



# ハイ アベイラビリティのためのフェールオーバー

この章では、ASA のハイアベイラビリティを達成するために、アクティブ/スタンバイまたはアクティブ/アクティブフェールオーバーを設定する方法について説明します。

- [フェールオーバーについて \(1 ページ\)](#)
- [フェールオーバーのライセンス \(28 ページ\)](#)
- [フェールオーバー のガイドライン \(29 ページ\)](#)
- [フェールオーバーのデフォルト \(34 ページ\)](#)
- [アクティブ/スタンバイ フェールオーバーの設定 \(34 ページ\)](#)
- [アクティブ/アクティブ フェールオーバーの設定 \(40 ページ\)](#)
- [オプションのフェールオーバー パラメータの設定 \(46 ページ\)](#)
- [フェールオーバー の管理 \(56 ページ\)](#)
- [フェールオーバーのモニタリング \(63 ページ\)](#)
- [フェールオーバーの履歴 \(65 ページ\)](#)

## フェールオーバーについて

フェールオーバーの設定では、専用フェールオーバーリンク（および任意でステートリンク）を介して相互に接続された 2 つの同じ ASA が必要です。アクティブユニットおよびインターフェイスのヘルスがモニターされて、所定のフェールオーバー条件に一致しているかどうか判断されます。所定の条件に一致すると、フェールオーバーが行われます。

## フェールオーバー モード

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

- アクティブ/スタンバイフェールオーバーでは、一方のデバイスがアクティブユニットとしてトラフィックを通過させます。もう一方のデバイスはスタンバイユニットとなり、ア

クティブにトラフィックを通過させません。フェールオーバーが発生すると、アクティブユニットからスタンバイユニットにフェールオーバーし、そのスタンバイユニットがアクティブになります。シングルまたはマルチ コンテキスト モードでは、ASA のアクティブ/スタンバイ フェールオーバーを使用できます。

- アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つのフェールオーバーグループに分割します。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。一方のグループは、プライマリ ASA でアクティブになるよう割り当てられます。他方のグループは、セカンダリ ASA でアクティブになるよう割り当てられます。フェールオーバーが行われる場合は、フェールオーバーグループ レベルで行われます。

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

## フェイルオーバーのシステム要件

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

### ハードウェア要件

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

- 同じモデルであること。

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

- インターフェイスの数とタイプが同じであること。

プラットフォーム モードと Firepower 4100/9300 シャーシ Firepower 2100 では、フェイルオーバー を有効にする前に、すべてのインターフェイスが FXOS で同一に事前構成されている必要があります。フェイルオーバーを有効にした後でインターフェイスを変更する場合は、スタンバイユニットの FXOS でそのインターフェイスを変更してから、アクティブユニットで同じ変更を行います。FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

- 同じモジュール（存在する場合）がインストールされていること。

- 同じ RAM がインストールされていること。

フェイルオーバー コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュメモリを取り付けた装置に、ソフトウェアイメージファイルおよびコンフィギュレーションファイルを格納できる十分な容量があることを確認してください。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

## ソフトウェア要件

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

- コンテキスト モードが同じであること（シングルまたはマルチ）。
- 単一モードの場合：同じファイアウォールモードにあること（ルーテッドまたはトランスペアレント）。

マルチコンテキスト モードでは、ファイアウォール モードはコンテキスト レベルで設定され、混合モードを使用できます。

- ソフトウェアバージョンが、メジャー（最初の番号）およびマイナー（2番目の番号）ともに同じであること。ただし、アップグレードプロセス中は、異なるバージョンのソフトウェアを一時的に使用できます。たとえば、ある装置をバージョン 8.3(1) からバージョン 8.3(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。
- 同じセキュアクライアント イメージがあること。中断のないアップグレードを実行するときにフェールオーバー ペアのイメージが一致しないと、アップグレードプロセスの最後のリブート手順でクライアントレス SSL VPN 接続が切断され、データベースには孤立したセッションが残り、IP プールではクライアントに割り当てられた IP アドレスが「使用中」として示されます。
- 同じ FIPS モードであること。
- (Firepower 4100/9300) 同じフローオフロードモードを使用し、両方とも有効または無効になっている。

## ライセンス要件

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

## フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2つの装置間の専用接続です。シスコでは、フェールオーバーリンクまたはステートフルフェールオーバーリンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で `eth0` を使用していた場合は、デバイス 2 でも同じインターフェイス (`eth0`) を使用します。



**注意** フェールオーバー リンクおよびステートフルリンク経由で送信される情報は、IPsec トンネルまたはフェールオーバー キーを使用して通信を保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザー名、パスワード、および事前共有キーが含まれています。この機密データをクリアテキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信を IPsec トンネルまたはフェールオーバー キーによってセキュリティ保護することをお勧めします。

## フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

### フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

### フェールオーバー リンクのインターフェイス

使用されていないデータインターフェイス（物理、サブインターフェイス、または EtherChannel）はいずれもフェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワークインターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステートフルリンク用としても使用できます）。ほとんどのモデルでは、以下で明示的に説明されていない限り、フェールオーバー用の管理インターフェイスを使用できません。

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

フェールオーバー リンクについては、次のガイドラインを参照してください。

- **5506-X ~ 5555-X** : 管理インターフェイスをフェールオーバー リンクとして使用できません。データ インターフェイスを使用する必要があります。5506H-X は唯一の例外で、フェールオーバー リンクとして管理インターフェイスを使用できます。
- **5506H-X** : フェールオーバー リンクとして管理 1/1 インターフェイスを使用できます。フェールオーバー用に設定した場合は、デバイスをリロードして変更を反映させる必要があります。この場合、管理プロセスに管理インターフェイスが必要であるため、ASA Firepower モジュールも使用できません。
- **Firepower 4100/9300** : フェールオーバーリンクに管理タイプのインターフェイスを使用することはできません。
- リンクのサイジングについては、次のガイドラインを参照してください。

表 1: フェールオーバーリンクのサイズ

| モデル                        | 結合フェールオーバーリンクとステートリンクのインターフェイスサイズ                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall 200               | 1 Gbps                                                                                                                                                                                            |
| Firepower 1010             | 1 Gbps                                                                                                                                                                                            |
| Firepower 1100             | 1 Gbps                                                                                                                                                                                            |
| Cisco Secure Firewall 1200 | 1 Gbps                                                                                                                                                                                            |
| Cisco Secure Firewall 3100 | Cisco Secure Firewall 3105 : 1 Gbps<br>Cisco Secure Firewall 3110 : 1 Gbps<br>Cisco Secure Firewall 3120 : 1 Gbps<br>Cisco Secure Firewall 3130 : 10 Gbps<br>Cisco Secure Firewall 3140 : 10 Gbps |
| Firepower 4100             | 10 Gbps                                                                                                                                                                                           |
| Cisco Secure Firewall 4200 | 10 Gbps                                                                                                                                                                                           |
| Firewall 6100              | 10 Gbps                                                                                                                                                                                           |
| Firepower 9300             | 10 Gbps                                                                                                                                                                                           |

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



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

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

## フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- ASA のフェールオーバー インターフェイスと同じネットワークセグメント（ブロードキャストドメインまたは VLAN）に他のデバイスのないスイッチを使用する。
- イーサネット ケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらのユニットのものを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASA は、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

## ステートフル フェールオーバー リンク

ステートフルフェールオーバーを使用するには、接続ステート情報を渡すためのステートフルフェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

### フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。ただし、設定が大規模でトラフィックが膨大なネットワークを使用している場合は、ステートリンクとフェールオーバー リンク専用のインターフェイスを検討する必要があります。

### 専用のインターフェイス

ステートリンク専用のデータインターフェイス（物理、または EtherChannel）を使用できます。専用のステートリンクの要件については [フェールオーバー リンクのインターフェイス（4 ページ）](#)、ステートリンクの接続については [フェールオーバー リンクの接続（6 ページ）](#) を参照してください。

長距離のフェールオーバーを使用する場合のステートリンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

## フェールオーバー リンクとデータ リンクの中断の回避

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

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

### シナリオ 1：非推奨

単一のスイッチまたはスイッチセットが 2 つの ASA 間のフェールオーバー インターフェイスとデータインターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンクがダウンすると、両方の ASA がアクティブになります。したがって、次の図で示されている次の 2 つの接続方式は推奨しません。

図 1: 単一のスイッチを使用した接続：非推奨

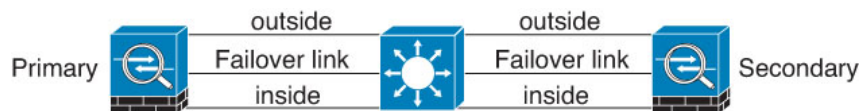
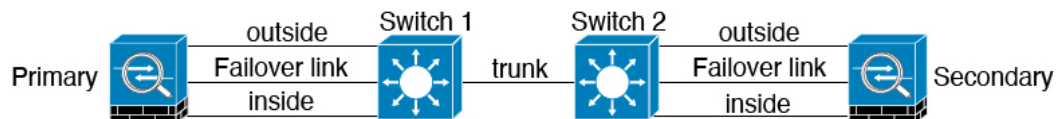


図 2: 2つのスイッチを使用した接続：非推奨



### シナリオ 2：推奨

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

図 3:異なるスイッチを使用した接続

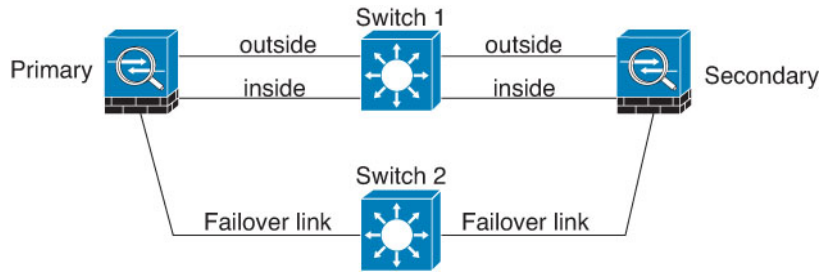
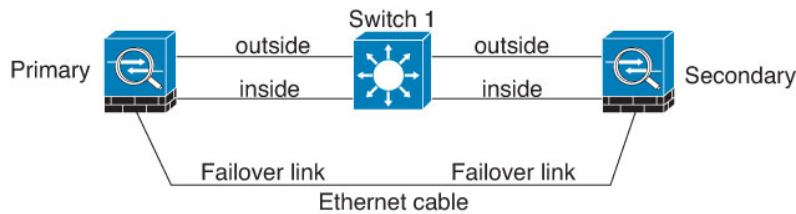


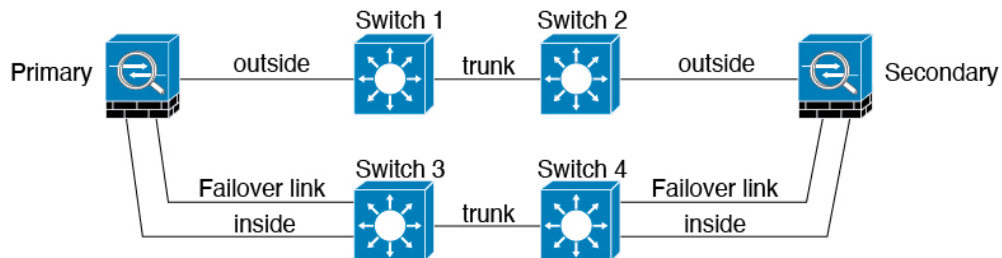
図 4: ケーブルを使用した接続



### シナリオ 3 : 推奨

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

図 5:セキュアスイッチを使用した接続



## フェールオーバーの MAC アドレスと IP アドレス

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



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

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

### アクティブ/スタンバイ IP アドレスと MAC アドレス

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

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

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

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



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

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。セカンダリ装置がプライマリ装置より先にオンラインになった場合でも、セカンダリ装置がアクティブ装置であるときに正しい MAC アドレスを使用するように、プライマリ装置とセカンダリ装置の両方で仮想 MAC アドレスを設定することをお勧めします。仮想 MAC

アドレスを設定しなかった場合、トラフィックフローを復元するために、接続されたルータの ARP テーブルをクリアする必要がある場合があります。ASA は MAC アドレスを変更するときに、スタティック NAT アドレスに対して Gratuitous ARP を送信しません。そのため、接続されたルータはこれらのアドレスの MAC アドレスの変更を認識できません。

### アクティブ/アクティブ IP アドレスと MAC アドレス

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

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

### 仮想 MAC アドレス

ASA には、仮想 MAC アドレスを設定する複数の方法があります。1 つの方法のみ使用することをお勧めします。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。手動の方法には、次で説明されている自動生成方法に加えて、インターフェイスモード **mac-address** コマンド、**failover mac address** コマンドが含まれ、アクティブ/アクティブフェールオーバーの場合は、フェールオーバー グループ モード **mac address** コマンドが含まれます。

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

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

### フェールオーバーでの MAC アドレス テーブルの更新

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

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

## ステートレス フェールオーバーとステートフル フェールオーバー

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



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

### ステートレス フェールオーバー

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



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

### ステートフル フェールオーバー

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

## サポートされる機能

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

- NAT 変換テーブル
- TCP 接続と UDP 接続、および状態。他のタイプの IP プロトコルおよび ICMP は、新しいパケットが到着したときに新しいアクティブユニットで確立されるため、アクティブ装置によって解析されません。
- HTTP 接続テーブル（HTTP 複製を有効にしない場合）。
- HTTP 接続状態（HTTP 複製が有効化されている場合）：デフォルトでは、ステートフルフェールオーバーが有効化されているときには、ASA は HTTP セッション情報を複製しません。HTTP レプリケーションを有効にすることをお勧めします。
- SCTP 接続状態ただし、SCTP インスペクションのステートフル フェールオーバーはベストエフォートです。フェールオーバー中、SACK パケットが失われると、失われたパケットが受信されるまで、新しいアクティブユニットはキューにある他のすべての順序が不正なパケットを破棄します。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションとピンホール。
- ICMP 接続状態：ICMP 接続の複製は、個々のインターフェイスが非対称ルーティンググループに割り当てられている場合にだけ有効化されます。
- スタティックおよびダイナミック ルーティング テーブル：ステートフルフェールオーバーはダイナミック ルーティング プロトコル（OSPF や EIGRP など）に参加するため、アクティブ装置上のダイナミック ルーティング プロトコルによる学習ルートが、スタンバイ装置のルーティング情報ベース（RIB）テーブルに維持されます。フェールオーバーイベントで、アクティブなセカンダリ ユニットには最初にプライマリ ユニートをミラーリングするルールがあるため、パケットは通常は最小限の中断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルートエントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれています。



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

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

## サポートされない機能

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

- ユーザー認証 (uauth) テーブル
- マルチキャスト ルーティング。
- 選択された次のクライアントレス SSL VPN 機能 :
  - スマートトンネル
  - ポート転送
  - プラグイン
  - Java アプレット
  - IPv6 クライアントレスまたはセキュアクライアントセッション
  - Citrix 認証 (Citrix ユーザーはフェールオーバー後に再認証が必要です)

## フェールオーバーのブリッジ グループ要件

ブリッジグループを使用する場合は、フェールオーバーに関して特別な考慮事項があります。

### アプライアンス、ASA のブリッジグループ必須要件

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

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

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

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

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

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

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

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

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

## フェールオーバーのヘルス モニタリング

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

## 装置のヘルス モニターリング

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

- ASAがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- ASAがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- ASAがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

## ハートビートモジュールの冗長性

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

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

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



- (注)
- HA が有効な場合、追加のハートビートモジュールは常にデフォルトで有効になっています。データプレーンの追加のハートビートモジュールのポーリング間隔を設定する必要はありません。このモジュールは、コントロールプレーンに設定したものと同一ハートビート間隔を使用します。
  - この機能は、バージョン 7.3 では使用できません。

## インターフェイス モニタリング

最大 1025 のインターフェイスを監視できます（マルチコンテキスト モードでは、すべてのコンテキスト間で分割）。重要なインターフェイスをモニターする必要があります。たとえば、マルチコンテキストモードでは、共有インターフェイスを監視するように1つのコンテキストを設定する場合があります（インターフェイスが共有されているため、すべてのコンテキストがそのモニタリングによる利点を得ることができます）。

ユニットは、モニター対象のインターフェイス上で15秒間 **hello** メッセージを受信しなかった場合に（デフォルト）、インターフェイステストを実行します。（この時間を変更するには、**failover polltime interface** コマンド、アクティブ/アクティブフェールオーバーの場合は **polltime interface** コマンドを参照してください）1つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、ASA はテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**failover interface-policy** コマンド、またはアクティブ/アクティブフェールオーバーの場合は **interface-policy** コマンドを参照）、さらに、アクティブユニットでスタンバイユニットよりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

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

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、ASA は IPv4 を使用してヘルス モニタリングを実行します。インターフェイスに IPv6 アドレスだけが設定されている場合、ASA は ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリングテストを実行します。ブロードキャスト ping テストの場合、ASA は IPv6 全ノードアドレス (FE02::1) を使用します。



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

## インターフェイス テスト

ASAでは、次のインターフェイステストが使用されます。各テストの時間は約1.5秒（デフォルト）、またはフェールオーバー インターフェイスの保留時間の1/16です（**failover polltime interface** コマンドを参照するか、アクティブ/アクティブフェールオーバーの場合は **interface-policy** コマンドを参照）。

1. リンクアップ/ダウンテスト：インターフェイスステータスのテストです。リンクアップ/ダウンテストでインターフェイスがダウンしていることが示された場合、ASAは障害が発生し、テストが停止したと見なします。ステータスがアップの場合、ASAはネットワーク アクティビティを実行します。
2. ネットワークアクティビティテスト：ネットワークの受信アクティビティのテストです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると思われ見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思われ見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASAはARPテストを開始します。
3. ARPテスト：ARPが正しく応答するかどうかをテストします。各ユニットは、ARPテーブル内の最新のエントリのIPアドレスに対して単一のARP要求を送信します。ユニットがテスト中にARP応答またはその他のネットワークトラフィックを受信する場合、インターフェイスは動作していると思われ見なされます。ユニットがARP応答を受信しない場合、ASAは、ARPテーブル内の「次の」エントリのIPアドレスに対して単一のARP要求を送信します。ユニットがテスト中にARP応答またはその他のネットワークトラフィックを受信する場合、インターフェイスは動作していると思われ見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思われ見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASAはブートストラップ ping テストを開始します。
4. ブロードキャストPingテスト：ping応答が正しいかどうかをテストします。各ユニットがブロードキャストpingを送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると思われ見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると思われ見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARPテストを使用してテストが再開されます。両方の装置がARPおよびブロードキャストpingテストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

## インターフェイス ステータス

モニタ対象のインターフェイスには、次のステータスがあります。

- **Unknown** : 初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合があります。
- **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** は管理上ダウンしています。
- **No Link** : インターフェイスの物理リンクがダウンしています。
- **Failed** : インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

## フェールオーバー 時間

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

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

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。デフォルト値を変更するには、フェールオーバーが発生するしきい値として、障害が発生したインターフェイスの数またはモニター対象インターフェイスの割合を設定します。アクティブデバイスでしきい値を超えると、フェールオーバーが発生します。スタンバイデバイスでしきい値を超えると、ユニットが **Fail** 状態に移行します。

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

表 2:

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



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

表 3: ASA

| フェールオーバー条件                                                                                         | 最小      | デフォルト | 最大数  |
|----------------------------------------------------------------------------------------------------|---------|-------|------|
| アクティブユニットの電源の喪失、ハードウェアのダウン、ソフトウェアのリロードまたはクラッシュにより、モニター対象インターフェイスまたはフェールオーバーリンクでhelloメッセージを受信しなくなる。 | 800 ミリ秒 | 15 秒  | 45 秒 |
| アクティブ ユニット メインボード インターフェイスリンクがダウンする。                                                               | 500 ミリ秒 | 5 秒   | 15 秒 |
| アクティブ ユニットの 4GE モジュール インターフェイス リンクがダウンする。                                                          | 2 秒     | 5 秒   | 15 秒 |
| アクティブ ユニットのインターフェイスは実行されているが、接続の問題によりインターフェイステストを行っている。                                            | 5 秒     | 25 秒  | 75 秒 |

## 設定の同期

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

### コンフィギュレーションの複製の実行

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

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

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

スタンバイ/セカンドユニットが初期スタートアップを完了すると、実行コンフィギュレーションを削除し（アクティブ ユニットとの通信に必要な **failover** コマンドを除く）、アクティブ ユニットはコンフィギュレーション全体をスタンバイ/セカンドユニットに送信します。複製が開始されると、アクティブユニットの ASA コンソールに「Beginning configuration replication: Sending to mate,」というメッセージが表示され、完了すると ASA に「End Configuration Replication to mate,」というメッセージが表示されます。コンフィギュレーションのサイズによって、複製には数秒から数分かかります。

コンフィギュレーションを受信する装置の場合、コンフィギュレーションは実行メモリにだけ存在します。[コンフィギュレーションの変更の保存](#)に従ってコンフィギュレーションをフラッシュメモリに保存する必要があります。たとえば、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブ状態であるユニット上のシステム実行スペースに **write memory all** コマンドを入力します。コマンドはピア装置に複製され、コンフィギュレーションがフラッシュメモリに書き込まれます。



(注) 複製中、コンフィギュレーションを送信しているユニット上に入力されたコマンドは、ピアユニットに正常に複製されず、コンフィギュレーションを受信するユニット上に入力されたコマンドは、受信したコンフィギュレーションによって上書きできます。コンフィギュレーションの複製処理中には、フェールオーバーペアのどちらの装置にもコマンドを入力しないでください。

## ファイルの複製

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

- セキュアクライアント イメージ
- CSD イメージ
- セキュアクライアント プロファイル

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

- アクティブ装置で **write standby** コマンドを入力します。
- アクティブ装置でプロファイルを再適用します。

- スタンバイ装置をリロードします。
- ローカル認証局 (CA)
- ASA イメージ
- ASDM イメージ

## コマンドの複製

起動した後、アクティブユニットで入力したコマンドはただちにスタンバイユニットに複製されます。コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

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

コマンドの複製を行うのに適切な装置上でコマンドを入力しなかった場合は、コンフィギュレーションは同期されません。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

- すべてのコンフィギュレーション コマンド (**mode**、**firewall**、および **failover lan unit** を除く)
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

スタンバイ ASA に複製されないコマンドは、次のとおりです。

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

## 設定同期の最適化

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

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

### 設定同期の最適化のガイドラインと制限事項

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

### 設定同期の監視

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

設定同期の最適化をモニタリングするには、次のコマンドを使用します。

- **show failover config-sync checksum**

デバイスのステータスとチェックサムに関する情報を表示します。

- **show failover config-sync configuration**

デバイスの設定とチェックサムに関する情報を表示します。

- **show failover config-sync status**

設定同期最適化機能のステータスを表示します。



(注) **show failover state** コマンドの構成状態は、HA 参加中の構成同期状態のステータスを表示します。この状態には、再同期が開始されるまで、その後の設定の展開または変更、およびデバイスの複製は反映されません。

## アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ ASA に引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。ただし、セカンダリ装置の設定を保持するために、障害が発生した装置を交換する前に、スタンバイ装置をプライマリに設定する必要があります。



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

## プライマリ/セカンダリの役割とアクティブ/スタンバイ ステータス

フェールオーバーペアの2つのユニットの主な相違点は、どちらのユニットがアクティブでどちらのユニットがスタンバイであるか、つまりどちらの IP アドレスを使用するか、およびどちらのユニットがアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリ ユニット（設定で指定）とセカンダリ ユニットとの間には、いくつかの相違点があります。

- 両方のユニット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 ユニットが常にアクティブ ユニットになります。
- プライマリ ユニットの MAC アドレスは常に、アクティブ IP アドレスと結び付けられています。このルールの例外は、セカンダリ ユニットがアクティブであり、フェールオーバー リンク経由でプライマリ ユニットの MAC アドレスを取得できない場合に発生します。この場合、セカンダリ ユニットの MAC アドレスが使用されます。

## 起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。

- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

## フェールオーバー イベント

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

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ ユニットが行うアクション、スタンバイ ユニットが行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 4: フェールオーバー イベント

| 障害イベント                        | ポリシー       | アクティブユニットのアクション                  | スタンバイユニットのアクション                  | 注意                                                                                   |
|-------------------------------|------------|----------------------------------|----------------------------------|--------------------------------------------------------------------------------------|
| アクティブ ユニットが故障（電源またはハードウェア）    | フェールオーバー   | 適用対象外                            | アクティブになる<br>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                         | 動作なし                             | なし。                                                                                  |
| スタンバイ ユニットが故障（電源またはハードウェア）    | フェールオーバーなし | スタンバイに故障とマークする                   | 適用対象外                            | スタンバイユニット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、アクティブユニットはフェールオーバーを行いません。                |
| 動作中にフェールオーバーリンクに障害が発生した       | フェールオーバーなし | フェールオーバーリンクに故障とマークする             | フェールオーバーリンクに故障とマークする             | フェールオーバー リンクがダウンしている間、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、できるだけ早くフェールオーバー リンクを復元する必要があります。 |
| スタートアップ時にフェールオーバー リンクに障害が発生した | フェールオーバーなし | アクティブになる<br>フェールオーバーリンクに故障とマークする | アクティブになる<br>フェールオーバーリンクに故障とマークする | スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置がアクティブになります。                                      |

| 障害イベント                           | ポリシー           | アクティブユニット<br>のアクション | スタンバイユニット<br>のアクション | 注意                                                                    |
|----------------------------------|----------------|---------------------|---------------------|-----------------------------------------------------------------------|
| ステート リンクの障害                      | フェール<br>オーバーなし | 動作なし                | 動作なし                | ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。                                |
| アクティブ ユニット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<br>オーバー   | アクティブに故障と<br>マークする  | アクティブになる            | なし。                                                                   |
| スタンバイ ユニット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<br>オーバーなし | 動作なし                | スタンバイに故障<br>とマークする  | スタンバイユニット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、アクティブユニットはフェールオーバーを行いません。 |

## アクティブ/アクティブ フェールオーバーの概要

この項では、アクティブ/アクティブ フェールオーバーについて説明します。

### アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチコンテキストモードの ASA でのみ使用できます。アクティブ/アクティブフェールオーバーでは、ASA のセキュリティ コンテキストを 2 つまでのフェールオーバー グループに分割します。

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

管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティコンテキストもまた、デフォルトでフェールオーバーグループ1のメンバです。アクティブ/アクティブ フェールオーバーが必要であるが複数コンテキストは必要ない場合、最もシンプルな設定は他のコンテキストを1つ追加し、それをフェールオーバーグループ2に割り当てることです。



- (注) アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。



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

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

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの 1 つの装置がプライマリ ユニットの指定され、もう 1 つの装置がセカンダリ ユニットの指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリまたはセカンダリの指定時に、次の 2 つの点を判定します。

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

## 起動時のフェールオーバー グループのアクティブ装置の決定

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

- ピア装置が使用できないときに装置がブートされると、両方のフェールオーバーグループがピア装置でアクティブになります。
- ピア装置がアクティブ（両方のフェールオーバーグループがアクティブ状態）の場合に装置がブートされると、フェールオーバーグループは、アクティブ装置でアクティブ状態のままになります。これは、次のいずれかの状態になるまで、フェールオーバーグループのプライマリ プリファレンスまたはセカンダリ プリファレンスには関係ありません。
  - フェールオーバーが発生した。
  - 手動でフェールオーバーを強制実行した。
  - フェールオーバーグループのプリエンプションを設定した。この設定により、優先する装置が使用可能になると、フェールオーバーグループはその装置上で自動的にアクティブになります。

## フェールオーバー イベント

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリユニットで両方のフェールオーバーグループをアクティブと指定し、フェールオーバーグループ1が故障すると、フェールオーバーグループ2はプライマリユニットでアクティブのままですが、フェールオーバーグループ1はセカンダリユニットでアクティブになります。

フェールオーバー グループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバー グループが故障と判断されない可能性があります。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブフェールオーバー グループのアクション、およびスタンバイ フェールオーバー グループのアクションを示します。

表 5: フェールオーバー イベント

| 障害イベント                                  | ポリシー       | アクティブグループのアクション      | スタンバイグループのアクション            | 注記                                                                                            |
|-----------------------------------------|------------|----------------------|----------------------------|-----------------------------------------------------------------------------------------------|
| 装置で電源断またはソフトウェア障害が発生した                  | フェールオーバー   | スタンバイになる<br>故障とマークする | アクティブになる<br>アクティブに故障とマークする | フェールオーバーペアの装置が故障すると、その装置のアクティブフェールオーバーグループはすべて故障とマークされ、ピア装置のフェールオーバーグループがアクティブになります。          |
| アクティブフェールオーバーグループにおけるしきい値を超えたインターフェイス障害 | フェールオーバー   | アクティブグループに故障とマークする   | アクティブになる                   | なし。                                                                                           |
| スタンバイフェールオーバーグループにおけるしきい値を超えたインターフェイス障害 | フェールオーバーなし | 動作なし                 | スタンバイグループに故障とマークする         | スタンバイフェールオーバーグループが故障とマークされている場合、インターフェイスフェールオーバー障害しきい値を超えても、アクティブフェールオーバーグループはフェールオーバーを行いません。 |

| 障害イベント                        | ポリシー       | アクティブグループのアクション | スタンバイグループのアクション | 注記                                                                                                            |
|-------------------------------|------------|-----------------|-----------------|---------------------------------------------------------------------------------------------------------------|
| 以前にアクティブであったフェールオーバー グループの復旧  | フェールオーバーなし | 動作なし            | 動作なし            | フェールオーバー グループのプリエンプションが設定されている場合を除き、フェールオーバー グループは現在の装置でアクティブのままです。                                           |
| スタートアップ時にフェールオーバー リンクに障害が発生した | フェールオーバーなし | アクティブになる        | アクティブになる        | スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置の両方のフェールオーバー グループがアクティブになります。                                             |
| ステート リンクの障害                   | フェールオーバーなし | 動作なし            | 動作なし            | ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。                                                                        |
| 動作中にフェールオーバー リンクに障害が発生した      | フェールオーバーなし | 適用対象外           | 適用対象外           | 各装置で、フェールオーバー リンクが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。 |

## フェールオーバーのライセンス

ほとんどのモデルでは、フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

| モデル            | ライセンス要件                                                                                 |
|----------------|-----------------------------------------------------------------------------------------|
| ASA 仮想         | <a href="#">ASAv のフェールオーバー ライセンス</a> を参照してください。                                         |
| Firepower 1010 | 両方のユニットの Security Plus ライセンス。 <a href="#">Firepower 1010 のフェールオーバー ライセンス</a> を参照してください。 |
| Firepower 1100 | <a href="#">Firepower 1100 のフェールオーバー ライセンス</a> を参照してください。                               |

| モデル                                  | ライセンス要件                                                                        |
|--------------------------------------|--------------------------------------------------------------------------------|
| Cisco Secure Firewall 1210/1220      | <a href="#">Cisco Secure Firewall 1210/1220 のフェールオーバーライセンス</a> を参照してください。      |
| Cisco Secure Firewall 1230/1240/1250 | <a href="#">Cisco Secure Firewall 1230/1240/1250 のフェールオーバーライセンス</a> を参照してください。 |
| Cisco Secure Firewall 3100/4200      | 「 <a href="#">Secure Firewall 3100 のフェールオーバーライセンス</a> 」を参照してください。              |
| Firepower 4100/9300                  | 「 <a href="#">Firepower 4100/9300のフェールオーバーライセンス</a> 」を参照してください。                |
| ISA 3000                             | 両方のユニットの Security Plus ライセンス。<br><br>(注)<br>各ユニットに同じ暗号化ライセンスが必要です。             |



- (注) 有効な永続キーが必要です。まれに、ISA 3000 で、PAK 認証キーを削除できることもあります。キーがすべて0の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

## フェールオーバーのガイドライン

### コンテキストモード

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

### モデルのサポート

- 200/ 1010/ 1210// 1220 :
  - フェールオーバーを使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。フェールオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常のフェールオーバーのネットワーク設定では、両方のユニットのアクティブなスイッチポートがネットワークループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニターできますが、スイッチポートはモニターできません。理論的には、1つのスイッチポートをVLANに配置し

て、フェールオーバーを正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。

- ファイアウォールインターフェイスはフェールオーバーリンクとしてのみ使用できます。
- FirePOWER 9300：シャード間フェールオーバーを使用して最良の冗長性を確保することを推奨します。
- Microsoft Azure や Amazon Web Services などのパブリッククラウドネットワーク上の ASA 仮想では、レイヤ2接続が必要なため、通常のフェールオーバーはサポートされません。代わりに、[パブリッククラウドでのハイアベイラビリティのためのフェールオーバー](#)を参照してください。

### ハイアベイラビリティを実現するためのASA仮想のフェールオーバー

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

### その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチポートが、トポロジの変化を検出すると30～50秒間ブロッキング状態になる可能性があります。ポートがブロッキングステートである間のトラフィック損失を防ぐには、スイッチでSTP PortFast機能を有効にします。

#### **interface interface\_id spanning-tree portfast**

この回避策は、ルーテッドモードおよびブリッジグループインターフェイスの両方に接続されているスイッチに適用されます。PortFast機能を設定すると、リンクアップと同時にポートがSTPフォワーディングモードに遷移します。ポートは引き続きSTPに参加しています。したがって、ポートがループの一部になる場合、最終的にはSTPブロッキングモードに遷移します。

- ASAフェールオーバーペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュアポートで設定または学習されたセキュアMACアドレスが別のセキュアポートに移動し、スイッチのポートセキュリティ機能によって違反フラグが付けられた場合に発生します。
- すべてのコンテキストにわたり、1台の装置の最大1025のインターフェイスをモニタできます。
- アクティブ/スタンバイフェールオーバーとVPN IPsecトンネルの場合、SNMPを使用してVPNトンネル上でアクティブユニットとスタンバイユニットの両方をモニターすることはできません。スタンバイユニットにはアクティブVPNトンネルがないため、NMSに

向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。

- 正常なアクティブ/スタンバイ状態の間にフェールオーバーがトリガーされない場合、スタンバイユニットのどのインターフェイスもシャットダウンされません。ただし、HA がアクティブ/障害状態の間にこれが発生すると、フェールオーバー LAN と状態インターフェイスを除くすべてのインターフェイス（管理インターフェイスを含む）が、障害が発生したユニットでシャットダウンされます。これは、フェールオーバーが無効になった後に、障害が発生したインターフェイスがアクティブになった場合に発生する可能性のあるトラフィックの問題を防ぐために行われます。フェールオーバー LAN および状態インターフェイスは稼働したままとなり、進行中のフェールオーバー通信が確保されます。
- アクティブ/アクティブフェールオーバーでは、同じコンテキスト内の2つのインターフェイスを同じ ASR グループ内で設定することはできません。
- アクティブ/アクティブフェールオーバーでは、最大2つのフェールオーバーグループを定義できます。
- アクティブ/アクティブフェールオーバーでフェールオーバーグループを削除する場合は、フェールオーバーグループ1を最後に削除する必要があります。フェールオーバーグループ1には常に管理コンテキストが含まれます。フェールオーバーグループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバーグループ1になります。コンテキストが明示的に割り当てられているフェールオーバーグループは削除できません。
- フェールオーバーの直後に、syslog メッセージの送信元アドレスが数秒間フェールオーバーインターフェイスアドレスになります。
- （フェールオーバー中に）コンバージェンスを向上させるには、どの設定やインスタンスにも関連付けられていない HA ペアのインターフェイスをシャットダウンする必要があります。
- 共有フェールオーバーおよび状態インターフェイスを使用する高可用性展開では、スタンバイユニットが同期設定状態にあるとき、フェールオーバーインターフェイスを介した接続に障害が発生し、最終的にスタンバイユニットがアクティブ状態に切り替わるときに、スプリットブレインが発生します。これは、モニター対象のインターフェイスがある場合でも同様です。

フェールオーバーインターフェイスを介した接続は、次の状況で失敗する可能性があります。

- スタンバイユニットがリブートした後、スタンバイユニットが同期設定状態にある間、フェールオーバーインターフェイスを介した接続は失敗します。
- スタンバイユニットで以前無効にしたフェールオーバーを有効にすると、スタンバイユニットが同期設定状態にある間、フェールオーバーインターフェイスを介した接続が失敗します。

スプリットブレインを回避するには、フェールオーバーおよび状態インターフェイスを使用します。フェールオーバーインターフェイス上の接続障害が解消されない場合は、新しいアクティブ（前にスタンバイだった）ユニットをネットワークから分離します。

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

例：

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

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

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

- フェイルオーバーのユニットは、クロックを動的に同期しません。同期が行われるときのイベントの例を次に示します。
  - 新しい フェイルオーバー ペアが作成される。

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

フェールオーバー LAN リンクがダウンしている場合、設定はピアユニットに複製されない可能性があるため、設定を展開することは推奨されません。
  - Cisco ASA の OSPF では、近くのスイッチがダウンし、Cisco ASA インターフェイスが同じスイッチに接続されている場合、ファイアウォール内のインターフェイスもダウンしてスイッチの障害が発生します。これは予期された動作です。これにより、設計どおりに高可用性フェールオーバーがトリガーされます。
  - OSPF では、フェールオーバー後、ピアデバイスとの OSPF 接続が無効になります。無効な接続を終了してから、新しい OSPF 接続を確立します。
  - スタンバイの Cisco ASA が別のスイッチに接続されている場合は、インターフェイスが起動すると、ルーティングテーブルは、アクティブの Cisco ASA のルーティングテーブルとは異なります。これにより、ルートと隣接関係（アジャセンシー）が更新されるまでの短時間（約 15 ～ 17 秒）の障害が発生します。

- トランスペアレントモードでは、アクティブユニットでホットスタンバイルータ（HSRP）の MAC アドレスが失われるという問題が発生した場合は、MAC アドレスのスタティックマッピングを作成します。

## フェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートフル フェールオーバーでの HTTP 複製は行われません。
- 単一のインターフェイス障害でフェールオーバーが行われます。
- インターフェイスのポーリング時間は 5 秒です。
- インターフェイスのホールド時間は 25 秒です。
- 装置のポーリング時間は 1 秒です。
- 装置のホールド時間は 15 秒です。
- 仮想 MAC アドレスはマルチコンテキストモードで無効化されていますが。
- すべての物理インターフェイスをモニタリングします。

## アクティブ/スタンバイ フェールオーバーの設定

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

### アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定

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

#### 始める前に

- フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。ポイントツーポイント接続に 31 ビットサブネット マスクを使用する場合、スタンバイ IP アドレスを設定しないでください。いずれかのインターフェイスが DHCP 用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。

- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

## 手順

**ステップ 1** この装置をプライマリ装置に指定します。

**failover lan unit primary**

**ステップ 2** フェールオーバー リンクとして使用するインターフェイスを指定します。

**failover lan interface if\_name interface\_id**

例 :

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

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

*if\_name* 引数は、インターフェイスに名前を割り当てます。

*interface\_id* 引数には、データ物理インターフェイス、サブインターフェイス、または EtherChannel インターフェイス ID を指定できます。Firepower 1010 および Cisco Secure Firewall 1210/1220 では、インターフェイスはファイアウォール インターフェイス ID です。スイッチポート ID または VLAN ID を指定することはできません。Firepower 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。

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

**failover interface ip failover\_if\_name {ip\_address mask | ipv6\_address / prefix} standby ip\_address**

例 :

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

または :

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

このアドレスは未使用のサブネット上になければなりません。このサブネットは IP アドレスが 2 つだけの 31 ビット (255.255.255.254) にすることができます。169.254.1.0/24 および fd00:0:0:0::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

**ステップ 4** フェールオーバー リンクをイネーブルにします。

**interface failover\_interface\_id**

**no shutdown**

例 :

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

**ステップ 5** (オプション) ステートリンクに別のインターフェイスを使用する場合は、そのインターフェイスを指定します。

**failover link if\_name interface\_id**

例 :

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

別のインターフェイスを指定しない場合、フェールオーバーリンクがステートリンクに使用されます。

*if\_name* 引数は、インターフェイスに名前を割り当てます。

*interface\_id* 引数には、物理インターフェイス、サブインターフェイス、または EtherChannel インターフェイス ID を指定できます。Firepower 1010 および Cisco Secure Firewall 1210/1220 では、インターフェイスはファイアウォールインターフェイス ID です。スイッチポート ID または VLAN ID を指定することはできません。

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

**failover interface ip state\_if\_name {ip\_address mask | ipv6\_address/prefix} standby ip\_address**

例 :

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

または :

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

このアドレスは、フェールオーバーリンクとは異なる未使用のサブネット上になければなりません。このサブネットは IP アドレスが 2 つだけの 31 ビット (255.255.255.254) にすることができます。169.254.1.0/24 および fd00:0:0::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステートリンクを共有する場合は、この手順をとばしてください。

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

```
interface state_interface_id
```

```
no shutdown
```

例：

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

ステート リンクを共有する場合は、この手順をとばしてください。

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

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

```
failover ipsec pre-shared-key [0 | 8] key
```

例：

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

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

マスターパスフレーズ ([マスターパスフレーズの設定](#)を参照) を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は (たとえば **more system:running-config** の出力からのコピー)、キーワード **8** を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

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

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

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバーキーを削除する必要があります。

フェールオーバー LAN-to-LAN トンネルは、IPsec (その他の VPN) ライセンスには適用されません。

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

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

例：

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

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

マスター パスフレーズ（[マスター パスフレーズの設定](#)を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

**failover key** の共有秘密は、**show running-config** の出力に \*\*\*\*\* と表示されます。このマスクされたキーはコピーできません。

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

**ステップ 9** フェールオーバーをイネーブルにします。

**failover**

**ステップ 10** システム コンフィギュレーションをフラッシュ メモリに保存します。

**write memory**

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

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

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

## アクティブ/スタンバイ フェールオーバーのセカンダリ装置の設定

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

### 始める前に

- いずれかのインターフェイスが DHCP 用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

### 手順

**ステップ 1** **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。 [アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定 \(34 ページ\)](#) を参照してください。

次に例を示します。

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

**ステップ 2** フェールオーバー コンフィギュレーションが同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

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

# アクティブ/アクティブ フェールオーバーの設定

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

## アクティブ/アクティブ フェールオーバーのプライマリ装置の設定

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

### 始める前に

- マルチ コンテキスト モードの有効化または無効化に従って、マルチ コンテキスト モードをイネーブルにします。
- ルーテッドモードおよびトランスペアレントモードのインターフェイスに従って、フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。ポイントツーポイント接続に 31 ビットサブネットマスクを使用する場合、スタンバイ IP アドレスを設定しないでください。いずれかのインターフェイスが DHCP 用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

### 手順

**ステップ 1** この装置をプライマリ装置に指定します。

```
failover lan unit primary
```

**ステップ 2** フェールオーバー リンクとして使用するインターフェイスを指定します。

```
failover lan interface if_name interface_id
```

例：

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

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

*if\_name* 引数は、インターフェイスに名前を割り当てます。

*interface\_id* 引数には、物理インターフェイス、サブインターフェイス、または EtherChannel インターフェイス ID を指定できます。Firepower 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。

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

**standby failover interface ip if\_name {ip\_address mask | ipv6\_address/prefix } standby ip\_address**

例 :

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

または :

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

このアドレスは未使用のサブネット上になければなりません。このサブネットは IP アドレスが 2 つだけの 31 ビット (255.255.255.254) にすることができます。169.254.1.0/24 および fd00:0:0::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

**ステップ 4** フェールオーバー リンクをイネーブルにします。

**interface failover\_interface\_id**

**no shutdown**

例 :

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

**ステップ 5** (オプション) ステートリンクに別のインターフェイスを使用する場合は、そのインターフェイスを指定します。

**failover link if\_name interface\_id**

例 :

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

フェールオーバーリンクとは別のステートリンクを使用することをお勧めします。別のインターフェイスを指定しない場合、フェールオーバーリンクがステートリンクに使用されます。

*if\_name* 引数は、インターフェイスに名前を割り当てます。

*interface\_id* 引数には、物理インターフェイス、サブインターフェイス、または EtherChannel インターフェイス ID を指定できます。

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

このアドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。このサブネットは IP アドレスが 2 つだけの 31 ビット (255.255.255.254) にすることができます。169.254.1.0/24 および fd00:0:0::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステート リンクを共有する場合は、この手順をとばしてください。

**failover interface ip state if\_name {ip\_address mask | ipv6\_address/prefix} standby ip\_address**

例 :

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

または :

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

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

**interface state\_interface\_id**

**no shutdown**

例 :

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

ステート リンクを共有する場合は、この手順をとばしてください。

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

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

**failover ipsec pre-shared-key [0 | 8] key**

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

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

マスターパスフレーズ ([マスターパスフレーズの設定](#)を参照) を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は (たとえば **more system:running-config** の出力からのコピー) 、キーワード **8**

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

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

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

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバーキーを削除する必要があります。

フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。

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

**failover key [0 | 8] {hex key | shared\_secret}**

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

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

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

マスター パスフレーズ（[マスター パスフレーズの設定](#)を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

**failover key** の共有秘密は、**show running-config** の出力に **\*\*\*\*\*** と表示されます。このマスクされたキーはコピーできません。

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

**ステップ 9** フェールオーバー グループ 1 を作成します。

**failover group 1**

**primary**

**preempt [delay]**

例：

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

通常、プライマリ装置にグループ 1 を割り当て、セカンダリ装置にグループ 2 を割り当てます。グループの **primary** または **secondary** の設定にかかわらず、両方のフェールオーバー グループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。**preempt** コマンドは、指定された装置が使用可能になったときに、フェールオーバー グループがその装置で自動的にアクティブになるようにします。

オプションの **delay** 値に秒数を入力して、その時間フェールオーバー グループが現在の装置でアクティブ状態に維持され、その後に指定された装置で自動的にアクティブになるようにできます。有効な値は 1 ～ 1200 です。

ステートフルフェールオーバーがイネーブルの場合、プリエンブションは、フェールオーバーグループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

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

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

**failover group 2**

**secondary**

**preempt [delay]**

例：

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

**ステップ 11** 特定のコンテキストのコンテキスト コンフィギュレーション モードに入り、そのコンテキストをフェールオーバー グループに割り当てます。

**context name**

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

例：

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

コンテキストごとにこのコマンドを繰り返します。

未割り当てのコンテキストはすべて、自動的にフェールオーバー グループ 1 に割り当てられます。管理コンテキストは常にフェールオーバー グループ 1 のメンバーです。グループ 2 に割り当てることはできません。

**ステップ 12** フェールオーバーをイネーブルにします。

**failover**

**ステップ 13** システム コンフィギュレーションをフラッシュ メモリに保存します。

**write memory**

#### 例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

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

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

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

## アクティブ/アクティブ フェールオーバーのセカンダリ装置の設定

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

#### 始める前に

- マルチ コンテキスト モードの有効化または無効化に従って、マルチ コンテキスト モードをイネーブルにします。
- いずれかのインターフェイスが DHCP 用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。

- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

## 手順

**ステップ 1** **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。また、プライマリ装置から複製されるので、**failover group** コマンドおよび **join-failover-group** コマンドを入力する必要もありません。[アクティブ/アクティブ フェールオーバーのプライマリ装置の設定 \(40 ページ\)](#) を参照してください。

次に例を示します。

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

**ステップ 2** フェールオーバー コンフィギュレーションがプライマリ装置と同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

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

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

```
failover active group 2
```

# オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

## フェールオーバー基準とその他の設定の構成

この項で変更可能な多くのパラメータのデフォルト設定については、[フェールオーバーのデフォルト \(34 ページ\)](#) を参照してください。アクティブ/アクティブモードでは、ほとんどの条件をフェールオーバー グループごとに設定します。

### 始める前に

- マルチ コンテキスト モードのシステム実行スペースで次の設定を行います。
- ユニットのヘルス モニタリングの Bidirectional Forwarding Detection (BFD) については次の制限を参照してください。
  - FirePOWER 9300 および 4100 のみ
  - アクティブ/スタンバイのみ
  - ルーテッド モードのみ

### 手順

**ステップ 1** 装置のポーリング時間およびホールド時間を変更します。

**failover polltime [unit] [msec] poll\_time [holdtime [msec] time]**

例 :

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

**polltime** の範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。**holdtime** の範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ユニットのポーリング時間の 3 倍未満のホールド時間の値を入力することはできません。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間で検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

1 回のポーリング期間中に、装置がフェールオーバー通信インターフェイスで **hello** パケットを検出しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

アクティブ/アクティブモードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

**ステップ 2** ユニットのヘルス モニタリングの BFD を設定します。

CPU の使用率が高い場合、通常のユニットのモニタリングにより誤ってアラームが発生する可能性があります。BFD メソッドは分散されているため、CPU の使用率が高い場合でも動作に影響はありません。

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

**bfd-template single-hop** *template\_name*

**bfd interval min-tx** *milliseconds***min-rx** *milliseconds* **multiplier** *multiplier\_value*

例 :

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

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

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

- b) ヘルス モニタリングの BFD を有効化します。

**failover health-check bfd** *template\_name*

例 :

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

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

**failover polltime link-state msec** *poll\_time*

例 :

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

範囲は 300 ～ 799 ミリ秒です。デフォルトでは、フェールオーバーのペアの ASA では、インターフェイスのリンク ステートが 500 ミリ秒ごとに確認されます。 **polltime** はカスタマイズできます。たとえば、**polltime** を 300 ミリ秒に設定すると、ASA ではインターフェイスの障害やトリガーのフェールオーバーをより早く検出できるようになります。

アクティブ/アクティブモードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

### ステップ 4 セッションの複製レートを、1 秒間の接続数で設定します。

**failover replication rate** *conns*

例 :

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

最小および最大レートはモデルによって異なります。デフォルトは最大レートです。アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

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

**failover standby config-lock**

デフォルトでは、スタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションは、警告メッセージ付きで許可されます。

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

**failover group {1 | 2}**

例 :

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

- ステップ 7**    HTTP ステート複製をイネーブルにします。

- アクティブ/スタンバイ モードの場合

**failover replication http**

- アクティブ/アクティブ モードの場合

**replication http**

HTTP 接続がステート情報複製に含まれるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP ステート複製を有効にすることをお勧めします。

(注)

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

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

- アクティブ/スタンバイ モードの場合

**failover interface-policy num [%]**

例 :

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

- アクティブ/アクティブ モードの場合

**interface-policy num [%]**

例：

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

デフォルトでは、1つのインターフェイス障害でフェールオーバーが行われます。  
インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 1025 を設定できます。  
インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

#### ステップ9 インターフェイスのポーリング時間とホールド時間を変更します。

- アクティブ/スタンバイ モードの場合

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

例：

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

- アクティブ/アクティブ モードの場合

**polltime interface [msec] polltime [holdtimetime]**

例：

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

- *polltime* : hello パケットをピアに送信するまで待機する時間を設定します。*polltime* に有効な値は 1 ～ 15 秒で、オプションの **msec** キーワードを使用する場合は 500 ～ 999 ミリ秒です。デフォルトは 5 秒です。
- *holdtimetime* : ピア ユニットからの最後に受信した hello メッセージとインターフェイステストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイステストの期間を *holdtime*/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、*polltime* の 5 倍です。*polltime* の 5 倍よりも短い *holdtime* 値は入力できません。

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

1.  $x = (\text{holdtime}/\text{polltime})/2$ 、最も近い整数に丸められます。（0.4 以下は切り下げ、0.5 以上は切り上げ。）
2.  $y = x * \text{polltime}$

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

#### ステップ10 インターフェイスの仮想 MAC アドレスを設定します。

- アクティブ/スタンバイ モードの場合

**failover mac address phy\_if active\_mac standby\_mac**

例：

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

- アクティブ/アクティブ モードの場合

**mac address phy\_if active\_mac standby\_mac**

例：

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

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

*active\_mac* および *standby\_mac* 引数は、H.H.H 形式（H は 16 ビットの 16 進数）の MAC アドレスです。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。

*active\_mac* アドレスはインターフェイスのアクティブ IP アドレスに関連付けられ、*standby\_mac* はインターフェイスのスタンバイ IP アドレスに関連付けられます。

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

**show interface** コマンドを使用して、インターフェイスが使用している MAC アドレスを表示します。

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

## インターフェイス モニタリングの設定

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

重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。

装置ごとに最大 1025 のインターフェイスをモニターできます（マルチ コンテキスト モードのすべてのコンテキストにわたって）。

### 始める前に

マルチ コンテキスト モードで、各コンテキスト内のインターフェイスを設定します。

## 手順

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

**[no] monitor-interface {if\_name}**

例：

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

## 非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）

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

返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスでは同じ内部ネットワークに接続している一方、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフェイスがセッション情報を持たないパケットを受信すると、同じグループ（この場合 ASR グループ 1）内のスタンバイ コンテキストの他のインターフェイスのセッション情報をチェックします。一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

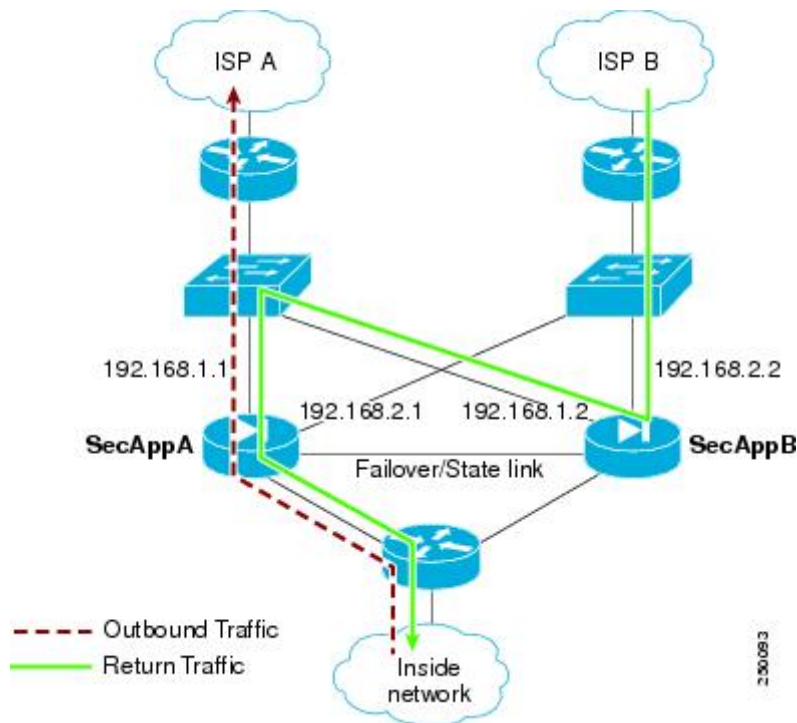
- 着信トラフィックがピア装置に発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。



- (注) この機能は、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

次の図に、非対称にルーティングされたパケットの例を示します。

図 6: ASR の例



1. アウトバウンドセッションが、アクティブな SecAppA コンテキストを持つ ASA を通過します。このパケットは、インターフェイス外の ISP-A (192.168.1.1) から送信されます。
2. 非対称ルーティングがアップストリームのどこかで設定されているため、リターントラフィックは、アクティブな SecAppB コンテキストを持つ ASA のインターフェイス外部の ISP-B (192.168.2.2) 経由で戻ります。
3. 通常、リターントラフィックは、そのインターフェイス 192.168.2.2 上にリターントラフィックに関するセッション情報がないので、ドロップされます。しかし、このインターフェイスは、ASR グループ 1 の一部として設定されています。装置は、同じ ASR グループ ID で設定された他のインターフェイス上のセッションを探します。
4. このセッション情報は、SecAppB を持つ装置上のスタンバイ状態のインターフェイス outsideISP-A (192.168.1.2) にあります。ステートフル フェールオーバーは、SecAppA から SecAppB にセッション情報を複製します。
5. ドロップされる代わりに、レイヤ 2 ヘッダーはインターフェイス 192.168.1.1 の情報で書き直され、トラフィックはインターフェイス 192.168.1.2 からリダイレクトされます。そこか

ら、発信元の装置のインターフェイスを経由して戻ります（SecAppA の 192.168.1.1）。この転送は、必要に応じて、セッションが終了するまで続行されます。

### 始める前に

- ステートフル フェールオーバー：アクティブ フェールオーバー グループにあるインターフェイスのセッションのステート情報を、スタンバイ フェールオーバー グループに渡します。
- replication http：HTTP セッションのステート情報は、スタンバイ フェールオーバー グループに渡されないため、スタンバイ インターフェイスに存在しません。ASA が非対称にルーティングされた HTTP パケットを再ルーティングできるように、HTTP ステート情報を複製する必要があります。
- プライマリ装置およびセカンダリ装置の各アクティブ コンテキスト内でこの手順を実行します。
- コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキストインターフェイスも ASR グループに含めることはできません。

### 手順

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

**interface** *phy\_if*

例：

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

**ステップ 2** インターフェイスの ASR グループ番号を設定します。

**asr-group** *num*

例：

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

*num* 範囲に有効な値は、1 ～ 32 です。

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

**interface** *phy\_if*

例：

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

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

**asr-group num**

例：

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

例

2 つの装置に次のコンフィギュレーションがあります（コンフィギュレーションは関連するコマンドだけを示します）。図の「SecAppA」というラベルの付いたデバイス は、フェールオーバー ペアのプライマリ装置です。

プライマリ装置のシステム コンフィギュレーション

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

SecAppA コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/2
```

```
nameif outsideISP-A
security-level 0
ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
asr-group 1
interface GigabitEthernet0/3
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

### SecAppB コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/4
nameif outsideISP-B
security-level 0
ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
asr-group 1
interface GigabitEthernet0/5
nameif inside
security-level 100
ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

## フェイルオーバーの管理

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

## フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次の手順を実行します。

### 始める前に

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

### 手順

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

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

- アクティブ/スタンバイ モードのスタンバイ装置の場合

**failover active**

- アクティブ/アクティブ モードのスタンバイ装置の場合

**failover active [group group\_id]**

例 :

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

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

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

- アクティブ/スタンバイ モードのアクティブ装置の場合

**no failover active**

- アクティブ/アクティブ モードのアクティブ装置の場合

**no failover active [group group\_id]**

例 :

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

## フェールオーバーのディセーブル化

1 つまたは両方の装置でフェールオーバーをディセーブルにすると、リロードするまで各装置のアクティブおよびスタンバイ状態が維持されます。アクティブ/アクティブフェールオーバーペアの場合、どの装置を優先するように設定されていようと、フェールオーバーグループはアクティブであるすべての装置でアクティブ状態のまま維持されます。

フェールオーバーをディセーブルにする際、次の特性を参照してください。

- スタンバイ装置/コンテキストはスタンバイ モードのまま維持されるので、両方の装置はトラフィックの転送を開始しません（これは疑似スタンバイ状態と呼ばれます）。
- スタンバイ装置/コンテキストは、アクティブ装置/コンテキストに接続されていない場合でもそのスタンバイ IP アドレスを引き続き使用します。
- スタンバイ装置/コンテキストによる、フェールオーバー上における接続に対するリッセンは継続されます。フェールオーバーをアクティブ装置/コンテキストで再度イネーブルにすると、そのコンフィギュレーションの残りが再同期化された後に、スタンバイ装置/コンテキストが通常のスタンバイ状態に戻ります。

- スタンバイ装置で手動でフェールオーバーをイネーブルにしてアクティブ化しないでください。代わりに、[フェールオーバーの強制実行（56 ページ）](#)を参照してください。スタンバイ装置でフェールオーバーをイネーブルにすると、MAC アドレスの競合が発生し、IPv6 トラフィックが中断される可能性があります。
- 完全にフェールオーバーをディセーブルにするには、**no failover** コンフィギュレーションをスタートアップ コンフィギュレーションに保存してからリロードします。

### 始める前に

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

### 手順

**ステップ 1** フェールオーバーをディセーブルにします。

**no failover**

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

**write memory**

**reload**

## 障害が発生した装置の復元

障害が発生した装置を障害のない状態に復元するには、次の手順を実行します。

### 始める前に

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

### 手順

**ステップ 1** 障害が発生したユニットを障害が発生していない状態に復元します。

- アクティブ/スタンバイ モードの場合

**failover reset**

- アクティブ/アクティブ モードの場合

**failover reset [group group\_id]**

例：

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

障害が発生した装置を障害のない状態に復元しても、その装置が自動的にアクティブになるわけではありません。復元された装置は、（強制または自然な形での）フェールオーバーによってアクティブになるまではスタンバイ状態のままです。例外は、フェールオーバー グループ（アクティブ/アクティブ モードのみ）にフェールオーバー プリエンブションが設定されている場合です。以前アクティブであったフェールオーバー グループにプリエンブションが設定されており、障害が発生した装置が優先装置の場合、そのフェールオーバー グループはアクティブになります。

**group group\_id** を指定した場合、このコマンドは障害が発生したアクティブ/アクティブ フェールオーバー グループを障害のない状態に復元します。

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

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

## コンフィギュレーションの再同期

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

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

複製されたコマンドは、実行コンフィギュレーションに保存されます。

## フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

### 手順

**ステップ 1** FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置が予期したとおりにトラフィックを渡しているかどうかをテストします。

**ステップ 2** アクティブ装置で次のコマンドを入力し、フェールオーバーを強制実行します。

アクティブ/スタンバイ モード

```
ciscoasa(config)# no failover active
```

アクティブ/アクティブ モード

```
ciscoasa(config)# no failover active group group_id
```

**ステップ 3** FTP を使用して、2 つの同じホスト間で別のファイルを送信します。

**ステップ 4** テストが成功しなかった場合は、**show failover** コマンドを入力してフェールオーバー ステータスを確認します。

**ステップ 5** テストが終了したら、新しくアクティブになった装置で次のコマンドを入力すると、装置をアクティブ ステータスに復元できます。

アクティブ/スタンバイ モード

```
ciscoasa(config)# no failover active
```

アクティブ/アクティブ モード

```
ciscoasa(config)# failover active group group_id
```

(注)

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

## リモート コマンドの実行

リモートコマンドを実行すると、コマンドラインに入力されたコマンドを特定のフェールオーバー ピアに送信できます。

### コマンドの送信

コンフィギュレーションコマンドはアクティブ装置またはコンテキストからスタンバイ装置またはコンテキストに複製されるため、いずれの装置にログインしているかにかかわらず、**failover exec** コマンドを使用して正しい装置にコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ装置にログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ装置に送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置やコンテキストへの設定コマンドの送信には、**failover exec** コマンドを使用しないでください。これらの設定の変更はアクティブ装置に複製されないため、2 つの設定が同期されなくなります。

configuration、exec、および **show** コマンドの出力は、現在のターミナルセッションで表示されるため、**failover exec** コマンドを使用し、ピア装置で **show** コマンドを発行して、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

## 手順

**ステップ 1** マルチ コンテキスト モードの場合は、**changeto contextname** コマンドを使用して、設定したい コンテキストに変更します。**failover exec** コマンドを使用して、フェールオーバー ピアでコンテキストを変更することはできません。

**ステップ 2** 次のコマンドを使用して、所定のフェールオーバー装置にコマンドを送信します。

```
ciscoasa(config)# failover exec {active | mate | standby}
```

**active** または **standby** キーワードを使用すると、その装置が現在の装置であっても、コマンドは指定された装置で実行されます。**mate** キーワードを使用すると、コマンドはフェールオーバー ピアで実行されます。

コマンドモードを変更するコマンドによって、現在のセッションのプロンプトが変更されることはありません。コマンドが実行されるコマンドモードを表示するには、**show failover exec** コマンドを使用する必要があります。詳細については、[コマンドモードの変更 \(7-53 ページ\)](#) を参照してください。

## コマンド モードの変更

**failover exec** コマンドは、お使いのターミナルセッションのコマンドモードとは異なるコマンドモード状態を維持します。デフォルトでは、**failover exec** コマンドモードは、指定されたデバイスのグローバル コンフィギュレーション モードで開始されます。このコマンドモードを変更するには、**failover exec** コマンドを使用して適切なコマンド (**interface** コマンドなど) を送信します。**failover exec** を使用してモードを変更しても、セッションプロンプトは変更されません。

たとえば、フェールオーバーペアのアクティブユニットのグローバルコンフィギュレーションモードにログインし、**failover exec active** コマンドを使用してインターフェイス コンフィギュレーションモードを変更した場合、ターミナルプロンプトはグローバルコンフィギュレーションモードのままですが、**failover exec** を使用して入力されるコマンドは、インターフェイス コンフィギュレーションモードで入力されます。

次の例は、ターミナルセッションモードと **failover exec** コマンドモードの違いを示しています。この例で、管理者はアクティブ装置の **failover exec** モードを、インターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーションモードに変更します。その後、**failover exec active** を使用して入力されたすべてのコマンドがインターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーションモードに送信されます。次に、管理者は **failover exec active** を使用して、そのインターフェイスに IP アドレスを割り当てます。プロンプトはグローバル コンフィギュレーションモードを示していますが、**failover exec active** モードはインターフェイス コンフィギュレーションモードです。

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

デバイスとの現在のセッションのコマンドモードを変更しても、**failover exec** コマンドで使用するコマンドモードには影響しません。たとえば、アクティブ装置のインターフェイス コンフィギュレーションモードで、**failover exec** コマンドモードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。その結果、デバイスとのセッションはインターフェイス コンフィギュレーションモードのままで、**failover exec active** を使用して入力されたコマンドは、指定されたルーティングプロセスを実行するためルータ コンフィギュレーションモードに送信されます。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

**show failover exec** コマンドを使用すると、指定したデバイスにコマンドモードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。**show failover exec** コマンドでは、**failover exec** コマンドと同じキーワード、つまり **active**、**mate**、または **standby** が使用されます。各デバイスの **failover exec** モードは個別に追跡されます。

次に、スタンバイ装置に入力された **show failover exec** コマンドの出力例を示します。

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

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

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

## セキュリティに関する注意事項

**failover exec** コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防ぐためには、フェールオーバー リンクの暗号化をイネーブルにする必要があります。

## リモート コマンドの実行に関する制限事項

リモートコマンドの使用には、次の制限事項があります。

- ゼロダウンタイムアップグレード手順を使用して1台の装置だけをアップグレードする場合は、**failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキストヘルプは、*cmd\_string* 引数のコマンドでは使用できません。

- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしている装置でそのコンテキストに変更する必要があります。
- 次のコマンドを **failover exec** コマンドと一緒に使用することはできません。
  - **changeto**
  - **debug (undebug)**
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在の装置が特権 EXEC モードのときに **failover exec mate configure terminal** を入力すると、**show failover exec mate** の出力に、failover exec セッションがグローバル コンフィギュレーションモードであることが示されます。ただし、ピア装置で **failover exec** を使用してコンフィギュレーションコマンドを入力した場合、現在の装置でグローバルコンフィギュレーションモードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** コマンドのような、再帰的な failover exec コマンドは入力できません。
- ユーザーの入力または確認が必要なコマンドでは、**noconfirm** オプションを使用する必要があります。たとえば、mate をリロードするには、次を入力します。  
**failover exec mate reload noconfirm**

## フェールオーバーのモニタリング

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

### フェールオーバー メッセージ

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

### フェールオーバーの syslog メッセージ

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



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

## フェールオーバー デバッグ メッセージ

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



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

## SNMP のフェールオーバー トラップ

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

## フェールオーバー ステータスのモニタリング

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

- **show failover**

装置のフェールオーバー状態についての情報を表示します。

- **show failover group**

装置のフェールオーバー状態に関する情報を表示します。表示される情報は、**show failover** コマンドの場合と似ていますが、指定されたグループに対象が限定されます。

- **show monitor-interface**

モニター対象インターフェイスの情報を表示します。

- **show running-config failover**

実行コンフィギュレーション内のフェールオーバー コマンドを表示します。

## フェールオーバーの履歴

| 機能名                                 | リリース   | 機能情報                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アクティブ/スタンバイ フェールオーバー                | 7.0(1) | この機能が導入されました。                                                                                                                                                                                                                                                                                                                                             |
| アクティブ/アクティブ フェールオーバー                | 7.0(1) | この機能が導入されました。                                                                                                                                                                                                                                                                                                                                             |
| フェールオーバー キーの 16 進数値サポート             | 7.0(4) | フェールオーバー リンクの暗号化用に 16 進数値が指定できるようになりました。<br><br><b>failover key hex</b> コマンドが変更されました。                                                                                                                                                                                                                                                                     |
| フェールオーバー キーのマスターパスフレーズのサポート         | 8.3(1) | フェールオーバー キーが、実行コンフィギュレーションとスタートアップコンフィギュレーションの共有キーを暗号化するマスターパスフレーズをサポートするようになりました。一方の ASA から他方に共有秘密をコピーする場合、たとえば、 <b>more system:running-config</b> コマンドを使用して、正常に暗号化共有キーをコピーして貼り付けることができます。<br><br>(注)<br><b>failover key</b> の共有秘密は、 <b>show running-config</b> の出力に ***** と表示されます。このマスクされたキーはコピーできません。<br><br><b>failover key [0   8]</b> コマンドが変更されました。 |
| フェールオーバーに IPv6 のサポートが追加             | 8.2(2) | 次のコマンドが変更されました。 <b>failover interface ip</b> 、 <b>show failover</b> 、 <b>ipv6 address</b> 、 <b>show monitor-interface</b>                                                                                                                                                                                                                                 |
| 「同時」ブートアップ中のフェールオーバーグループのユニットの設定の変更 | 9.0(1) | 以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバーグループを優先ユニットでアクティブにする <b>preempt</b> コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバーグループが最初に起動するユニットでアクティブになるように変更されました。                                                                                                                                                                                               |

| 機能名                                                         | リリース   | 機能情報                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フェールオーバー リンクおよびステート リンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート | 9.1(2) | <p>フェールオーバーキーに独自の暗号化を使用する代わりに (<b>failover key</b> コマンド)、フェールオーバー リンクおよびステート リンクの暗号化に IPsec LAN-to-LAN トンネルが使用できるようになりました。</p> <p>(注)<br/>フェールオーバー LAN-to-LAN トンネルは、IPsec (その他の VPN) ライセンスには適用されません。</p> <p><b>failover ipsec pre-shared-key</b>、<b>show vpn-sessiondb</b> の各コマンドが導入または変更されました。</p> |
| ハードウェア モジュールのヘルス モニタリングの無効化                                 | 9.3(1) | <p>ASA はデフォルトで、インストール済みハードウェア モジュール (ASA FirePOWER モジュールなど) のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。</p> <p><b>monitor-interface service-module</b> コマンドが変更されました。</p>                                                                           |
| フェールオーバーペアのスタンバイ装置またはスタンバイ コンテキストのコンフィギュレーション変更のロック         | 9.3(2) | <p>通常のコन्フィギュレーションの同期を除いてスタンバイ装置上で変更ができないように、スタンバイ装置 (アクティブ/スタンバイ フェールオーバー) またはスタンバイ コンテキスト (アクティブ/アクティブフェールオーバー) のコンフィギュレーション変更をロックできるようになりました。</p> <p><b>failover standby config-lock</b> コマンドが導入されました。</p>                                                                                       |
| ASA 5506H のフェールオーバー リンクとして、管理 1/1 インターフェイスを使用可能             | 9.5(1) | <p>管理 1/1 インターフェイスは、ASA 5506H に限りフェールオーバーリンクとして設定できるようになりました。この機能により、デバイスの他のインターフェイスをデータインターフェイスとして使用できます。この機能を使用した場合、ASA FirePOWER モジュールは使用できません。このモジュールでは管理 1/1 インターフェイスを通常の管理インターフェイスとして維持することが必須です。</p> <p>次のコマンドが変更されました。 <b>failover lan interface</b>、<b>failover link</b></p>               |

| 機能名                                                                                        | リリース   | 機能情報                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| キャリア グレード NAT の強化がフェールオーバーおよび ASA クラスタリングでサポート                                             | 9.5(2) | <p>キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます (RFC 6888 を参照してください)。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。</p> <p>次のコマンドが変更されました。 <b>show local-host</b></p>                                              |
| アクティブ/スタンバイフェールオーバーを使用するときのセキュアクライアントからのダイナミック ACL における同期時間の改善                             | 9.6(2) | <p>フェールオーバーペアでセキュアクライアントを使用するとき、関連付けられているダイナミック ACL (dACL) におけるスタンバイユニットへの同期時間が改善されました。以前は、大規模な dACL の場合、スタンバイユニットが可用性の高いバックアップを提供するのではなく同期作業で忙しい間は、同期時間が長時間に及ぶことがありました。</p> <p>変更されたコマンドはありません。</p>                                               |
| マルチコンテキストモードのセキュアクライアント接続のステートフルフェールオーバー                                                   | 9.6(2) | <p>マルチコンテキストモードでセキュアクライアント 接続のステートフルフェールオーバーがサポートされるようになりました。</p> <p>変更されたコマンドはありません。</p>                                                                                                                                                          |
| より迅速に検出を行うためのインターフェイスのリンクステートモニタリングを設定可能                                                   | 9.7(1) | <p>デフォルトでは、フェールオーバーペアの ASA は、500 ミリ秒ごとにインターフェイスのリンク ステートをチェックします。ポーリングの間隔を 300 ミリ秒から 799 ミリ秒の間で設定できるようになりました。たとえば、ポーリング時間を 300 ミリ秒に設定すると、ASA はインターフェイス障害やトリガーのフェールオーバーをより迅速に検出できます。</p> <p>次のコマンドが導入されました。 <b>failover polltime link-state</b></p> |
| FirePOWER 9300 および 4100 でのアクティブ/スタンバイ フェールオーバー ヘルス モニタリングで、双方向フォワーディング検出 (BFD) がサポートされました。 | 9.7(1) | <p>FirePOWER 9300 および 4100 上のアクティブ/スタンバイペアの 2 つのユニット間のフェールオーバー ヘルスチェックに対して、双方向フォワーディング検出 (BFD) を有効にできるようになりました。ヘルス チェックに BFD を使用すると、デフォルトのヘルスチェックより信頼性が高まり、CPU の使用を抑えることができます。</p> <p>次のコマンドが導入されました。 <b>failover health-check bfd</b></p>         |

| 機能名                     | リリース    | 機能情報                                                                                                                                                                                                                                                                     |
|-------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| フェールオーバー遅延の無効化          | 9.15(1) | ブリッジグループまたは IPv6 DAD を使用する場合、フェールオーバーが発生すると、新しいアクティブユニットは、スタンバイユニットがネットワークタスクを完了してスタンバイ状態に移行するまで、最大3000ミリ秒待機します。その後、アクティブユニットはトラフィックの受け渡しを開始できます。この遅延を回避するために、待機時間を無効にすると、スタンバイユニットが移行する前にアクティブユニットがトラフィックの受け渡しを開始します。<br><br>新規/変更されたコマンド： <b>failover wait-disable</b> |
| HA ピアリングを高速化する設定同期最適化機能 | 9.18(1) | 設定同期最適化機能により、 <b>config-hash</b> 値を交換して参加ユニットとアクティブユニットの設定を比較できます。アクティブユニットと参加ユニットの両方で計算されたハッシュが一致する場合、参加ユニットは完全な設定同期をスキップして HA に再参加します。この機能により、さらに迅速な HA ピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。                                                                      |
| ハートビートモジュールの冗長性         | 9.20(1) | ASA 高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳や CPU の過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。                                                                                                                                 |

## 翻訳について

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

## 翻訳について

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

## 翻訳について

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