



CHAPTER 3

アクティブ/スタンバイ フェールオーバーの設定

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

- 「フェールオーバーおよびハイ アベイラビリティの概要」 (P.3-1)
- 「アクティブ/スタンバイ フェールオーバーの前提条件」 (P.3-15)
- 「ガイドラインと制限事項」 (P.3-16)
- 「アクティブ/スタンバイ フェールオーバーの設定」 (P.3-16)
- 「フェールオーバーの制御」 (P.3-24)
- 「アクティブ/スタンバイ フェールオーバーのモニタリング」 (P.3-26)
- 「アクティブ/スタンバイ フェールオーバーの機能履歴」 (P.3-27)

フェールオーバーおよびハイ アベイラビリティの概要

ハイ アベイラビリティを設定するには、専用のフェールオーバー リンクで相互に接続されている 2 台の同じ ASA 1000V が必要です。アクティブ インターフェイスおよび ASA 1000V のヘルスがモニタされて、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。

ASA 1000V では、アクティブ/スタンバイ フェールオーバーがサポートされます。アクティブ/スタンバイ フェールオーバーでは、1 つの ASA 1000V だけがトラフィックを渡し、もう 1 つの ASA 1000V はスタンバイ状態で待機します。ASA 1000V のアクティブ/スタンバイ フェールオーバー ペアに通常割り当てられるインターフェイスは、GigabitEthernet0/2 です。

- 「フェールオーバーのシステム要件」 (P.3-2)
- 「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」 (P.3-6)
- 「ステートレス (標準) フェールオーバーとステートフル フェールオーバー」 (P.3-9)
- 「フェールオーバー コンフィギュレーションでの Auto Update サーバ サポート」 (P.3-10)
- 「フェールオーバー ヘルスのモニタリング」 (P.3-13)
- 「フェールオーバー メッセージ」 (P.3-15)

フェールオーバーのシステム要件

それぞれの ASA 1000V を別個の Nexus 1000V にインストールする必要があります。

フェールオーバー コンフィギュレーションの 2 つの ASA 1000V は、メジャー（最初の番号）ソフトウェア バージョンおよびマイナー（2 番目の番号）ソフトウェア バージョンが同じでなければなりません。ただし、アップグレード プロセス中に、異なるバージョンのソフトウェアを使用し、フェールオーバーをアクティブのままにすることができます。長期的に互換性を維持するために、両方の ASA 1000V 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。

フェールオーバー ペアでのソフトウェアのアップグレードについては、「フェールオーバー ペアのゼロ ダウンタイム アップグレードの実行」(P.32-5) を参照してください。

アクティブ/スタンバイ フェールオーバーに関する情報

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

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

アクティブ/スタンバイ フェールオーバーの概要

アクティブ/スタンバイ フェールオーバーでは、スタンバイ ASA 1000V を使用して、障害の発生した ASA 1000V の機能を引き継ぐことができます。アクティブ ASA 1000V が故障すると、スタンバイ状態に変わり、そしてスタンバイ ASA 1000V がアクティブ状態に変わります。アクティブになる ASA 1000V は、故障した ASA 1000V の IP アドレスおよび MAC アドレスを使用してトラフィックの送信を開始します。現在スタンバイ状態の ASA 1000V が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

プライマリ/セカンダリ ステータスとアクティブ/スタンバイ ステータス

フェールオーバー ペアの 2 台の ASA 1000V の主な違いは、どちらの ASA 1000V がアクティブでどちらの ASA 1000V がスタンバイであるか、つまりどちらの IP アドレスを使用し、どちらの ASA 1000V がアクティブにトラフィックを渡すかという点です。

ただし、どちらがプライマリで（コンフィギュレーションで指定）とどちらがセカンダリかによっては、ASA 1000V 間にいくつかの相違点があります。

- 両方の ASA 1000V が同時に起動された場合（動作ヘルスが同等であれば）、常にプライマリ ASA 1000V がアクティブ ASA 1000V になります。
- プライマリ ASA 1000V 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。この規則の例外は、セカンダリ ASA 1000V 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 ASA 1000V 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 ASA 1000V の MAC アドレスが使用されます。

デバイスの初期化とコンフィギュレーションの同期

コンフィギュレーションの同期は、フェールオーバー ペア的一方または両方のデバイスがブートされると行われます。コンフィギュレーションは、常にアクティブ ASA 1000V からスタンバイ ASA 1000V に同期されます。スタンバイ ASA 1000V は、その初期スタートアップを完了すると、自分の実行コンフィギュレーションをクリアし（アクティブ ASA 1000V との通信に必要なフェールオーバー コマンドを除く）、アクティブ ASA 1000V は自分のコンフィギュレーション全体をスタンバイ ASA 1000V に送信します。

アクティブ ASA 1000V は、次の条件で判別されます。

- ASA 1000V 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、それがスタンバイ ASA 1000V になります。
- ASA 1000V がブートして、ピアが検出されない場合、それがアクティブ ASA 1000V になります。
- 両方の ASA 1000V が同時にブートされた場合は、プライマリ ASA 1000V がアクティブ ASA 1000V になり、セカンダリ ASA 1000V がスタンバイ ASA 1000V になります。



(注)

プライマリ ASA 1000V が検出されず、セカンダリ ASA 1000V がブートされると、それがアクティブ ASA 1000V になります。アクティブ IP アドレスには、セカンダリ装置自体の MAC アドレスを使用します。しかし、プライマリ ASA 1000V が使用可能になると、セカンダリ ASA 1000V は MAC アドレスをプライマリ ASA 1000V の MAC アドレスに変更します。これによって、ネットワーク トラフィックが中断されることがあります。これを回避するには、フェールオーバー ペアを仮想 MAC アドレスで設定します。詳細については、「[仮想 MAC アドレスの設定](#)」(P.3-23) を参照してください。

複製が開始されると、アクティブ ASA 1000V のコンソールに「Beginning configuration replication: Sending to mate」というメッセージが表示され、複製が完了すると、ASA 1000V に「End Configuration Replication to mate」というメッセージが表示されます。複製中、アクティブ ASA 1000V に入力されたコマンドがスタンバイ ASA 1000V に適切に複製されないことがあり、またスタンバイ ASA 1000V に入力されたコマンドが、アクティブ ASA 1000V から複製されているコンフィギュレーションによって上書きされることがあります。コンフィギュレーションの複製処理中には、フェールオーバー ペアのどちらの ASA 1000V にもコマンドを入力しないでください。コンフィギュレーションのサイズによって、複製は数秒で済むことも数分かかることもあります。

スタンバイ ASA 1000V の場合、コンフィギュレーションは実行メモリだけに存在します。ASA 1000V のフェールオーバー ペアを同じモード（両方 VMMC または両方 ASDM）で配置して、セキュリティ ポリシー コンフィギュレーションがフェールオーバー ペア全体で一貫しているようにする必要があります。モードが混在している場合は、次のエラー メッセージが表示されます。

```
Mate's device manager mode (ASDM|VMMC) is not compatible with my mode (ASDM|VMMC).
Failover will be disabled.
```

同期後にコンフィギュレーションをフラッシュ メモリに保存するには、アクティブ ASA 1000V で **write memory** コマンドを入力します。コマンドはスタンバイ ASA 1000V 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。

コマンドの複製

コマンドの複製は、常に、アクティブ ASA 1000V からスタンバイ ASA 1000V に向かって行われます。アクティブ ASA 1000V にコマンドを入力すると、そのコマンドがフェールオーバー リンクを通してスタンバイ ASA 1000V に送信されます。コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

スタンバイ ASA 1000V に複製されるコマンドは、次のとおりです。

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

- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

スタンバイ ASA 1000V に複製されないコマンドは、次のとおりです。

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



(注)

スタンバイ ASA 1000V で行われた変更は、アクティブ ASA 1000V へは複製されません。スタンバイ ASA 1000V にコマンドを入力すると、「**** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit.Configurations are no longer synchronized.」というメッセージが表示されます。このメッセージは、コンフィギュレーションに影響しない数多くのコマンドを入力したときにも表示されます。

アクティブ ASA 1000V で **write standby** コマンドを入力すると、スタンバイ ASA 1000V では実行コンフィギュレーション（アクティブ ASA 1000V との通信に使用するフェールオーバー コマンドを除く）がクリアされ、アクティブ ASA 1000V からコンフィギュレーション全体がスタンバイ ASA 1000V に送信されます。

複製されたコマンドは、実行コンフィギュレーションに保存されます。



(注)

スタンバイ フェールオーバーによって、次のファイルおよびコンフィギュレーション コンポーネントは複製されません。

- ASA 1000V イメージ
- ASDM イメージ

スタンバイ ASA 1000V のフラッシュ メモリに複製されたコマンドを保存するには、アクティブ ASA 1000V で **copy running-config startup-config** コマンドを入力します。コマンドはスタンバイ ASA 1000V 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。

フェールオーバーのトリガー

次のいずれかのイベントが発生した場合、ASA 1000V に障害が発生する可能性があります。

- ハードウェア障害または電源障害が発生した。
- ソフトウェア障害が発生した。

- 多くのモニタ対象インターフェイスが故障した。
- フェールオーバーを強制実行した。(「フェールオーバーの強制実行」(P.3-25) を参照)。

フェールオーバーのアクション

表 3-1 に、各障害イベントに対するフェールオーバー アクションを示します。この表には、各障害イベントに対して、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 ASA 1000V が行うアクション、スタンバイ ASA 1000V 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 3-1 フェールオーバー動作

障害の状況	ポリシー	アクティブ アクション	スタンバイ アクション	注釈
アクティブ ASA 1000V に障害が発生した	フェールオーバー	n/a	アクティブになる アクティブに故障とマークする	モニタ対象インターフェイスまたはフェールオーバー リンクで hello メッセージは受信されません。
以前にアクティブであった ASA 1000V 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 ASA 1000V に障害が発生した	フェールオーバーなし	スタンバイに故障とマークする	n/a	スタンバイ ASA 1000V が障害とマークされている場合、インターフェイス障害のしきい値を超えても、アクティブ ASA 1000V はフェールオーバーを行いません。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー インターフェイスに故障とマークする	フェールオーバー インターフェイスに故障とマークする	フェールオーバー リンクがダウンしている間、ASA 1000V はスタンバイ ASA 1000V にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	フェールオーバー インターフェイスに故障とマークする	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の ASA 1000V がアクティブになります。
ステートフル フェールオーバー リンクに障害が発生した	フェールオーバーなし	動作なし	動作なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
アクティブ ASA 1000V でのインターフェイス障害のしきい値を超過	フェールオーバー	アクティブに故障とマークする	アクティブになる	なし。
スタンバイ ASA 1000V でのインターフェイス障害のしきい値を超過	フェールオーバーなし	動作なし	スタンバイに故障とマークする	スタンバイ ASA 1000V が障害とマークされている場合、インターフェイス障害のしきい値を超えても、アクティブ ASA 1000V はフェールオーバーを行いません。

オプションのアクティブ/スタンバイ フェールオーバー設定

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

- ステートフル フェールオーバーでの HTTP 複製：ステート情報の複製に接続を含めることができます。
- インターフェイス モニタリング：ASA 1000V の最大 250 のインターフェイスをモニタし、フェールオーバーに影響を与えるインターフェイスを制御できます。
- インターフェイス ヘルス モニタリング：ASA 1000V がより早くインターフェイスの障害を検出して対応できるようにします。
- フェールオーバー基準の設定：インターフェイス数またはモニタされているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。

仮想 MAC アドレスの設定：プライマリ ASA 1000V よりも前にオンラインになった場合でも、セカンダリ ASA 1000V がアクティブ ASA 1000V であるときは、セカンダリで正しい MAC アドレスを使用するようにします。

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

この項では、フェールオーバー リンクおよびステートフル フェールオーバー リンクについて説明します。これらのリンクは、フェールオーバー コンフィギュレーションで 2 台の ASA 1000V 間の専用接続です。ここでは、次の内容について説明します。

- 「フェールオーバー リンク」(P.3-6)
- 「ステートフル フェールオーバー リンク」(P.3-7)
- 「フェールオーバー リンクの中断の回避」(P.3-8)

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 ASA 1000V は、フェールオーバー リンク経由で常に通信して、各 ASA 1000V の動作ステータスを確認します。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。

- ASA 1000V 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



注意

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。

フェールオーバー リンクとしてデバイスの GigabitEthernet 0/2 インターフェイスを使用できます。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（および、オプションでステートフル フェールオーバー リンク）専用とする必要があります。

スイッチを使用してフェールオーバー リンクを接続します。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）上で他のデバイスを ASA 1000V のフェールオーバー インターフェイスとしては使用しません。

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、ステートフル フェールオーバー リンクを設定してすべてのステート情報を渡す必要があります。ステートフル フェールオーバー リンクを設定する方法としては、次の 3 つのオプションがあります。

- ステートフル フェールオーバー リンクに、専用のイーサネット インターフェイスを使用できます。これは、名前が *FOLink* の GigabitEthernet0/2 インターフェイスとして定義されています。このインターフェイスは vPath カプセル化によるパケットを受信しません。

ASDM 経由でポリシーを管理している場合は、最初の配置後、インターフェイス ロールを変更できます。

- フェールオーバー リンクを共有できます。
- 内部インターフェイスなど、通常のデータ インターフェイスを共有できます。しかし、このオプションはお勧めしません。

スイッチを使用して専用ステート リンクを接続します。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）上で他のデバイスを ASA 1000V のフェールオーバー インターフェイスとしては使用しません。



(注)

ASA 1000V に直接接続されている Cisco スイッチ ポートの PortFast オプションをイネーブルにします。

データ インターフェイスをステートフル フェールオーバー リンクとして使用する場合、そのインターフェイスをステートフル フェールオーバー リンクと指定すると、次の警告が表示されます。

```
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
Sharing Stateful failover interface with regular data interface is not
a recommended configuration due to performance and security concerns.
***** WARNING ***** WARNING ***** WARNING ***** WARNING *****
```

データ インターフェイスとステートフル フェールオーバー インターフェイスを共有すると、リプレイ攻撃を受けやすくなる場合があります。さらに、大量のステートフル フェールオーバー トラフィックがインターフェイスで送信され、そのネットワーク セグメントでパフォーマンス上の問題が発生することがあります。



(注)

ステートフル フェールオーバー リンクが通常のデータ インターフェイスに設定されていない限り、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変更されません。

**注意**

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。

フェールオーバー リンクの中断の回避

ASA 1000V は、プライマリおよびセカンダリ ASA 1000V の間のメッセージの転送にフェールオーバー インターフェイスを使用するので、フェールオーバー インターフェイスがダウン（つまり、物理リンクがダウンしているか、インターフェイスの接続に使用しているスイッチがダウン）している場合、フェールオーバー インターフェイスのヘルスが復元されるまで、ASA 1000V のフェールオーバー動作が影響を受けます。

すべての通信がフェールオーバー ペアの ASA 1000V 間で断ち切られれば、両方の ASA 1000V が予期されるアクティブ状態になります。通信が復元され、2 台のアクティブ ASA 1000V がフェールオーバー リンクまたは任意のモニタ対象インターフェイスを介して通信を再開すると、プライマリ ASA 1000V がアクティブのままになり、セカンダリ ASA 1000V がスタンバイ状態にすぐに戻ります。この関係は、プライマリ ASA 1000V のヘルスに関係なく確立されます。

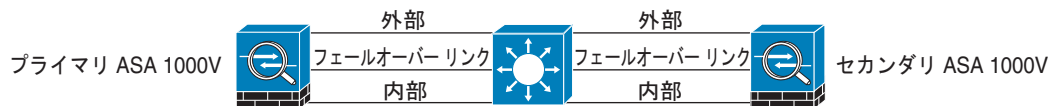
この動作が原因で、ネットワークを分割中にセカンダリ アクティブ ASA 1000V によって適切に渡されたステートフルフローは中断されます。この中断を回避するには、フェールオーバー リンクおよびデータ インターフェイスは、異なるパスを通過して、すべてのリンクで同時に障害が発生する可能性を減らす必要があります。1 組のフェールオーバー リンクがダウンしている場合、ASA 1000V はインターフェイスのヘルスをサンプリングし、データ インターフェイスを使用してピアとこの情報を交換して、アクティブ ASA 1000V の方がダウンしているインターフェイスが多ければ、スイッチオーバーを実行します。その後、フェールオーバー動作は、フェールオーバー リンクのヘルスが復元されるまで停止されます。

ネットワーク トポロジに応じて、ASA 1000V のフェールオーバー ペアには複数のプライマリ/セカンダリ障害シナリオがあります。それらのシナリオについて次に説明します。

シナリオ 1：非推奨

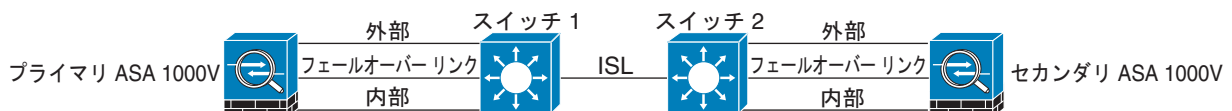
単一のスイッチまたはスイッチ セットが 2 つの ASA 1000V 間のフェールオーバー インターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンクがダウンすると、両方の ASA 1000V がアクティブになります。したがって、[図 3-1](#) および [図 3-2](#) で示されている次の 2 つの接続方式は推奨しません。

図 3-1 単一のスイッチを使用した接続：非推奨



332063

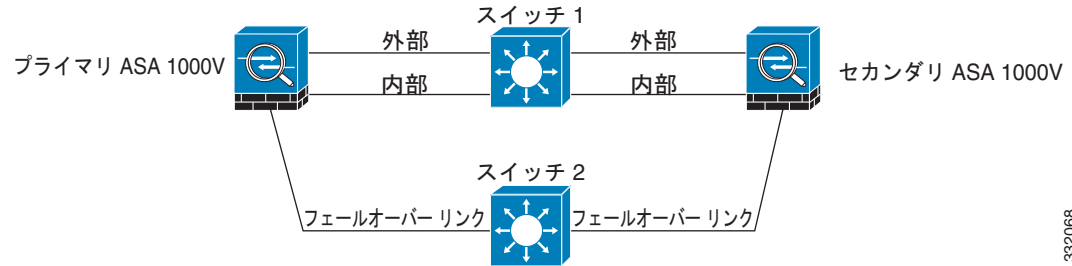
図 3-2 2 つのスイッチを使用した接続：非推奨



332064

シナリオ 2：推奨

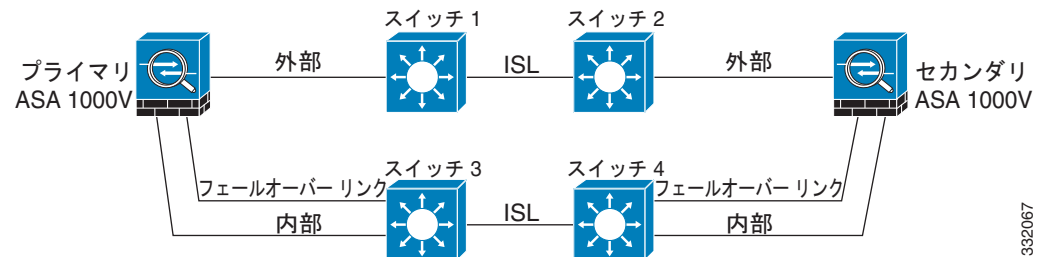
ASA 1000V のフェールオーバー ペアでフェールオーバー インターフェイス障害が発生しないように、フェールオーバー インターフェイスがデータ インターフェイスと同じスイッチを使用しないようにすることをお勧めします（前述の接続を参照）。代わりに、[図 3-3](#) に示すように、2 つの ASA 1000V フェールオーバー インターフェイスを接続する別のスイッチを使用します。

図 3-3 異なるスイッチを使用した接続

332068

シナリオ 3：推奨

ASA 1000V 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、[図 3-4](#) に示すように、フェールオーバー インターフェイスはいずれかのスイッチ（できればネットワーク内のセキュア側のスイッチ）に接続できます。

図 3-4 セキュアなスイッチを使用した接続

332067

ステートレス（標準）フェールオーバーとステートフル フェールオーバー

ASA 1000V は、標準およびステートフルという 2 つのタイプのフェールオーバーをサポートします。ここでは、次の内容について説明します。

- 「[ステートレス（標準）フェールオーバー](#)」 (P.3-9)
- 「[ステートフル フェールオーバー](#)」 (P.3-10)

ステートレス（標準）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 ASA 1000V が引き継いだ後、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イネーブルになっている場合、アクティブ ASA 1000V は接続ごとのステート情報をスタンバイ ASA 1000V に常に渡しています。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 ASA 1000V で使用できます。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。

ステートフル フェールオーバーがイネーブルになっているとき、次のステート情報がスタンバイ ASA 1000V に渡されます。

- NAT 変換テーブル
- TCP 接続状態
- UDP 接続状態
- ARP テーブル
- HTTP 接続状態 (HTTP 複製がイネーブルの場合)
- ISAKMP および IPSec SA テーブル
- SIP シグナリング セッション

ステートフル フェールオーバーがイネーブルになっているとき、次のステート情報はスタンバイ ASA 1000V に渡されません。

- HTTP 接続テーブル (HTTP 複製がイネーブルでない場合)
- ユーザ認証 (uauth) テーブル
- 検査対象のプロトコルは高度な TCP ステート トラッキングの対象となり、これらの接続の TCP ステートは自動的に複製されません。スタンバイ ASA 1000V への接続は複製されますが、TCP ステートを再確立するベスト エフォート型の試行が行われます。
- DHCP サーバアドレスのリース
- モジュールのステート情報。

フェールオーバー コンフィギュレーションでの Auto Update サーバ サポート

Auto Update サーバを使用して、ソフトウェア イメージとコンフィギュレーション ファイルを、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の ASA 1000V に配置できます。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 Auto Update をイネーブルにするには、フェールオーバー ペアのプライマリ ASA 1000V に Auto Update サーバのコンフィギュレーションを入力します。詳細については、「[Auto Update サポートの設定](#)」(P.32-8)を参照してください。

フェールオーバー コンフィギュレーションの Auto Update サーバ サポートには、次の制限と動作が適用されます。

- 新しいプラットフォーム ソフトウェア イメージをロードする際、フェールオーバー ペアはトラフィックの転送を停止します。
- LAN ベースのフェールオーバーを使用する場合、新しいコンフィギュレーションによってフェールオーバー リンクのコンフィギュレーションが変更されてはいけません。フェールオーバー リンクのコンフィギュレーションが変更されると、ASA 1000V 間の通信は失敗します。
- Auto Update サーバへの Call Home を実行するのはプライマリ ASA 1000V だけです。Call Home を実行するには、プライマリ ASA 1000V がアクティブ状態である必要があります。そうでない場合、ASA 1000V は自動的にプライマリ ASA 1000V にフェールオーバーします。

- ソフトウェア イメージまたはコンフィギュレーション ファイルをダウンロードするのは、プライマリ ASA 1000V だけです。その後、ソフトウェア イメージまたはコンフィギュレーション ファイルはセカンダリ ASA 1000V にコピーされます。
- インターフェイスの MAC アドレスは、プライマリ ASA 1000V から取得します。
- Auto Update サーバまたは HTTP サーバに保存されたコンフィギュレーション ファイルは、プライマリ ASA 1000V 専用です。

Auto Update プロセスの概要

次に、フェールオーバー コンフィギュレーションでの Auto Update プロセスの概要を示します。このプロセスは、フェールオーバーがイネーブルであり、動作していることを前提としています。ASA 1000V がコンフィギュレーションを同期化している場合、何かの理由でスタンバイ ASA 1000V に障害が発生している場合、または、フェールオーバー リンクがダウンしている場合、Auto Update プロセスは実行できません。

1. 両方の ASA 1000V は、プラットフォームおよび ASDM ソフトウェア チェックサムとバージョン情報を交換します。
2. プライマリ ASA 1000V は Auto Update サーバにアクセスします。プライマリ ASA 1000V がアクティブ状態でない場合、ASA 1000V はまずプライマリ ASA 1000V にフェールオーバーしてから、Auto Update サーバにアクセスします。
3. Auto Update サーバは、ソフトウェア チェックサムと URL 情報を返します。
4. プライマリ ASA 1000V が、アクティブまたはスタンバイ ASA 1000V のプラットフォーム イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
 - a. プライマリ ASA 1000V は、Auto Update サーバの URL を使用して、HTTP サーバから適切なファイルを取得します。
 - b. プライマリ ASA 1000V は、そのイメージをスタンバイ ASA 1000V にコピーしてから、自身のイメージをアップデートします。
 - c. 両方の ASA 1000V に新しいイメージがある場合は、セカンダリ (スタンバイ) ASA 1000V が最初にリロードされます。
 - セカンダリ ASA 1000V のブート時にヒットレス アップグレードが可能な場合は、セカンダリ ASA 1000V がアクティブ ASA 1000V になり、プライマリ ASA 1000V がリロードされます。リロードが終了すると、プライマリ ASA 1000V がアクティブ ASA 1000V になります。
 - スタンバイ ASA 1000V のブート時にヒットレス アップグレードができない場合は、両方の ASA 1000V が同時にリロードされます。
 - d. セカンダリ (スタンバイ) ASA 1000V だけに新しいイメージがある場合は、セカンダリ ASA 1000V だけがリロードされます。プライマリ ASA 1000V は、セカンダリ ASA 1000V のリロードが終了するまで待機します。
 - e. プライマリ (アクティブ) ASA 1000V だけに新しいイメージがある場合は、セカンダリ ASA 1000V がアクティブ ASA 1000V になり、プライマリ ASA 1000V がリロードされます。
 - f. もう一度アップデート プロセスが手順 1 から開始されます。
5. ASA 1000V が、プライマリまたはセカンダリ ASA 1000V の ASDM イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
 - a. プライマリ ASA 1000V は、Auto Update サーバから提供された URL を使用して、HTTP サーバから ASDM イメージ ファイルを取得します。
 - b. プライマリ ASA 1000V は、必要に応じて ASDM イメージをスタンバイ ASA 1000V にコピーします。

- c. プライマリ ASA 1000V は、自身の ASDM イメージをアップデートします。
 - d. もう一度アップデート プロセスが手順 1 から開始されます。
6. プライマリ ASA 1000V が、コンフィギュレーションをアップデートする必要があると判断した場合は、次の処理が実行されます。
 - a. プライマリ ASA 1000V は、指定された URL を使用して、コンフィギュレーション ファイルを取得します。
 - b. 両方の ASA 1000V で同時に、古いコンフィギュレーションが新しいコンフィギュレーションに置換されます。
 - c. もう一度アップデート プロセスが手順 1 から開始されます。
 7. チェックサムがすべてのイメージおよびコンフィギュレーション ファイルと一致している場合、アップデートは必要ありません。このプロセスは、次のポーリング時間まで中断されます。

Auto Update プロセスのモニタリング

debug auto-update client または **debug fover cmd-exe** コマンドを使用して、Auto Update プロセスで実行される処理を表示できます。次に、**debug auto-update client** コマンドの出力例を示します。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
  Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
  Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
  Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msec
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
```

```

auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419

```

Auto Update プロセスが失敗すると、次の syslog メッセージが生成されます。

```
%ASA-4-612002: Auto Update failed: file version: version reason: reason
```

file は、どのアップデートに失敗したかによって、「image,」、「asdm,」、または「configuration,」のいずれかになります。*version* は、アップデートのバージョン番号です。*reason* は、アップデートが失敗した原因です。

フェールオーバー ヘルスのモニタリング

ASA 1000V は、各 ASA 1000V 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します。ASA 1000V がテストを実行して、各 ASA 1000V の状態を判断する方法の詳細については、次の項を参照してください。

- [「ASA 1000V ヘルス モニタリング」 \(P.3-13\)](#)
- [「インターフェイスのモニタリング」 \(P.3-14\)](#)

ASA 1000V ヘルス モニタリング

ASA 1000V は、フェールオーバー リンクをモニタして相手 ASA 1000V のヘルスを判断します。ASA 1000V がフェールオーバー リンクで 3 回連続して hello メッセージを受信しないとき、ASA 1000V は、フェールオーバー インターフェイスを含む各インターフェイスでインターフェイス hello メッセージを送信し、ピア インターフェイスが応答するかどうかを検証します。ASA 1000V が行うアクションは、相手 ASA 1000V 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 1000V がフェールオーバー インターフェイスで応答を受信した場合は、フェールオーバーを行いません。
- ASA 1000V がフェールオーバー リンクで応答を受信せず、他のインターフェイスで応答を受信した場合、ASA 1000V 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、ASA 1000V 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 1000V 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 ASA 1000V がアクティブ モードに切り替わり、相手 ASA 1000V を障害に分類します。

hello メッセージの頻度と、フェールオーバーが行われる前の保持時間を設定できます。ポーリング時間が速くて保持時間が短いほど、ASA 1000V の障害が短時間で検出され、フェールオーバーの実行が迅速になりますが、キープアライブ パケットを遅延させるネットワーク輻輳が原因で「偽の」障害が生じる可能性もあります。

インターフェイスのモニタリング

最大 250 のインターフェイスをモニタできます。重要なインターフェイスをモニタする必要があります。

設定した保持時間が半分経過しても ASA 1000V がモニタ対象のインターフェイスで hello メッセージを受信しない場合は、次のテストが実行されます。

1. リンク アップ/ダウン テスト：インターフェイスのステータスのテスト。リンク アップ/ダウン テストでインターフェイスが動作していることが示された場合、ASA 1000V はネットワーク テストを実行します。一連のテストの目的は、障害が発生している（いずれかにある場合）ASA 1000V を判別するためのネットワーク トラフィックを生成することです。各テストの開始時に、各 ASA 1000V はインターフェイスの受信パケット カウントをクリアします。各テストの終了時には、各 ASA 1000V はトラフィックを受信したかどうかをチェックします。トラフィックを受信していれば、インターフェイスは正常に動作していると思なされます。一方の ASA 1000V だけがテスト用のトラフィックを受信していて、もう一方の ASA 1000V は受信していない場合は、トラフィックを受信しなかった ASA 1000V に障害が発生していると思なされます。どちらの ASA 1000V もトラフィックを受信しなかった場合は、次のテストが使用されます。
2. ネットワーク アクティビティ テスト：受信ネットワーク アクティビティ テスト。ASA 1000V では、受信したすべてのパケットを最大 5 秒間カウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。トラフィックが受信されなかった場合、ARP テストが開始します。
3. ARP テスト：取得したエントリの最後の 2 つの ASA 1000V ARP キャッシュの読み取り。ASA 1000V は、1 回に 1 つ、これらのマシンに ARP 要求を送信し、ネットワーク トラフィックを発生させます。要求を送信するたびに、ASA 1000V では、受信したすべてのトラフィックを最大 5 秒間カウントします。トラフィックが受信されれば、インターフェイスは正常に動作していると思なされます。トラフィックが受信されなければ、ARP 要求が次のマシンに送信されます。リストの最後まで、まったくトラフィックが受信されなかった場合、ping テストが開始します。
4. ブロードキャスト ping テスト：ブロードキャスト ping 要求の送信で構成される ping テスト。ASA 1000V では、受信したすべてのパケットを最大 5 秒間カウントします。この時間間隔の間にパケットが受信されると、インターフェイスが正常に動作しているものと見なされ、テストは停止します。

1 つのインターフェイスに対するネットワーク テストがすべて失敗したが、相手 ASA 1000V のこの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、そのインターフェイスは故障していると思なされます。故障したインターフェイスがしきい値を超えている場合は、フェールオーバーが行われます。相手 ASA 1000V のインターフェイスもすべてのネットワーク テストに失敗した場合、両方のインターフェイスが「未知」状態になり、フェールオーバー制限に向けてのカウントは行いません。

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 1000V 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。



(注)

障害が発生した ASA 1000V 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** コマンドを入力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、ASA 1000V は再び障害状態になります。

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 1000V がシステム メッセージを送信します。ここでは、次の内容について説明します。

- 「フェールオーバー システム メッセージ」 (P.3-15)
- 「デバッグ メッセージ」 (P.3-15)
- 「SNMP」 (P.3-15)

フェールオーバー システム メッセージ

ASA 1000V 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、複数のシステム 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。ロギングをイネーブルにするには、第 29 章「ロギングの設定」を参照してください。



(注)

切り替え中、フェールオーバー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 411001 および 411002 メッセージを生成します。このアクティビティは正常です。

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、**debug fover** コマンドは、特定の問題に対するトラブルシューティングや、Cisco TAC とのトラブルシューティングセッション中に限定して使用してください。

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。詳細については、第 30 章「SNMP の設定」を参照してください。

アクティブ/スタンバイ フェールオーバーの前提条件

両方の ASA 1000V が同じ ASA 1000V であり、専用のフェールオーバー リンク（オプションで、ステートフル フェールオーバー リンク）で相互に接続されている必要があります。

ガイドラインと制限事項

- フェールオーバー ペアの両方の ASA 1000V からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。
- スタンバイ IP アドレスは、現在スタンバイ ASA 1000V である ASA 1000V で使用されます。スタンバイ IP アドレスは、アクティブ ASA 1000V で対応しているインターフェイスのアクティブ IP アドレスと同じサブネット内にある必要があります。
- フェールオーバー ペアのアクティブ ASA 1000V でコンソール端末のページ設定を変更した場合、アクティブなコンソール端末のページ設定は変更されますが、スタンバイ ASA 1000V の設定は変更されません。アクティブ ASA 1000V で発行されたデフォルト コンフィギュレーションは、スタンバイ ASA 1000V の動作にも影響を与えます。
- インターフェイス モニタリングをイネーブルにすると、1 台の ASA 1000V で最大 250 のインターフェイスをモニタできます。
- デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、ASA 1000V は HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドを使用すると、ステートフル フェールオーバー環境で HTTP セッションのステートフルな複製がイネーブルになりますが、システムのパフォーマンスが低下する可能性があります。

アクティブ/スタンバイ フェールオーバーの設定

この項では、アクティブ/スタンバイ フェールオーバーを設定する方法について説明します。ここでは、次の内容について説明します。

- 「[アクティブ/スタンバイ フェールオーバーの設定のタスク フロー](#)」 (P.3-16)
- 「[プライマリ ASA 1000V の設定](#)」 (P.3-17)
- 「[セカンダリ ASA 1000V の設定](#)」 (P.3-19)
- 「[オプションのアクティブ/スタンバイ フェールオーバー設定値の設定](#)」 (P.3-20)

アクティブ/スタンバイ フェールオーバーの設定のタスク フロー

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

-
- | | |
|--------|--|
| ステップ 1 | 「 プライマリ ASA 1000V の設定 」 (P.3-17) に従って、プライマリ ASA 1000V を設定します。 |
| ステップ 2 | 「 セカンダリ ASA 1000V の設定 」 (P.3-19) に従って、セカンダリ ASA 1000V を設定します。 |
| ステップ 3 | (任意) 「 オプションのアクティブ/スタンバイ フェールオーバー設定値の設定 」 (P.3-20) に従って、オプションのアクティブ/スタンバイ フェールオーバー設定を行います。 |
-

プライマリ ASA 1000V の設定

この項の手順に従って、LAN ベースのアクティブ/スタンバイ フェールオーバー コンフィギュレーションでプライマリ ASA 1000V を設定します。この手順では、プライマリ ASA 1000V 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低限のコンフィギュレーションを示します。

制限事項

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

前提条件

すべての IP アドレスのスタンバイ アドレスを第 4 章「インターフェイスの設定」に従って設定します。

手順の詳細

	コマンド	目的
ステップ1	<code>failover lan unit primary</code>	ASA 1000V をプライマリ ASA 1000V として指定します。
ステップ2	<code>failover lan interface if_name interface_id</code> 例: <code>hostname(config)# failover lan interface folink gigabitEthernet0/2</code>	フェールオーバー インターフェイスとして使用するインターフェイスを指定します。このインターフェイスは、他の目的に使用しないでください（オプションのステートフル フェールオーバー リンクは除く）。 <code>if_name</code> 引数は、 <code>interface_id</code> 引数で指定されたインターフェイスに名前を割り当てます。 インターフェイス ID は、イーサネット インターフェイスです。
ステップ3	<code>failover interface ip if_name [ip_address mask standby ip_address]</code> 例: <code>hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2</code>	アクティブおよびスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。 スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。 フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。フェールオーバーリンクのアクティブ IP アドレスは、常にプライマリ ASA 1000V に存在し、スタンバイ IP アドレスは、セカンダリ ASA 1000V に存在します。
ステップ4	<code>interface interface_id no shutdown</code> 例: <code>hostname(config)# interface gigabitEthernet0/2 hostname(config-if)# no shutdown</code>	インターフェイスをイネーブルにします。

■ アクティブ/スタンバイ フェールオーバーの設定

コマンド	目的
<p>ステップ5 <code>failover link if_name interface_id</code></p> <p>例: <pre>hostname(config)# failover link statelink gigabitEthernet0/2</pre></p>	<p>(任意) ステートフル フェールオーバー リンクとして使用するインターフェイスを指定します。このインターフェイスは、他の目的に使用しないでください (オプションのフェールオーバー リンクは除く)。</p> <p>(注) ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、<code>if_name</code> 引数を指定することだけが必要です。</p> <p><code>if_name</code> 引数は、<code>interface_id</code> 引数で指定されたインターフェイスに論理名を割り当てます。<code>interface_id</code> 引数は、物理ポート名 (Ethernet1 など) にすることも、すでに作成されているサブインターフェイス (Ethernet0/2.3 など) にすることもできます。このインターフェイスは、イーサネット インターフェイスです。フェールオーバー コンフィギュレーションでは、インターフェイス名の代わりに、インターフェイス ID (たとえば、<code>gigabitEthernet0/2</code>) を使用します。</p>
<p>ステップ6 <code>failover interface ip if_name [ip_address mask standby ip_address]</code></p> <p>例: <pre>hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2</pre></p>	<p>(任意) アクティブおよびスタンバイ IP アドレスをステートフル フェールオーバー リンクに割り当てます。</p> <p>(注) ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、この手順をスキップします。インターフェイスのアクティブおよびスタンバイ IP アドレスは、すでに定義しています。</p> <p>スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。スタンバイ アドレスのサブネット マスクを指定する必要はありません。</p> <p>ステートフル フェールオーバー リンク IP アドレスおよび MAC アドレスは、データ インターフェイスを使用しない限り、フェールオーバー時に変更されません。アクティブ IP アドレスは常にプライマリ ASA 1000V に存在し、スタンバイ IP アドレスはセカンダリ ASA 1000V に存在します。</p>
<p>ステップ7 <code>interface interface_id</code> <code>no shutdown</code></p> <p>例: <pre>hostname(config)# interface gigabitEthernet0/2 hostname(config-if)# no shutdown</pre></p>	<p>(任意) インターフェイスをイネーブルにします。</p> <p>ステートフル フェールオーバー リンクがフェールオーバー リンクまたはデータ インターフェイスを使用する場合は、この手順をスキップします。インターフェイスは、すでにイネーブルです。</p>
<p>ステップ8 <code>failover</code></p> <p>例: <pre>hostname(config)# failover</pre></p>	<p>フェールオーバーをイネーブルにします。</p>
<p>ステップ9 <code>copy running-config startup-config</code></p> <p>例: <pre>hostname(config)# copy running-config startup-config</pre></p>	<p>システム コンフィギュレーションをフラッシュ メモリに保存します。</p>

セカンダリ ASA 1000V の設定


セカンダリ ASA 1000V 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 ASA 1000V には、プライマリ ユニットと初期に通信するために、これらのコマンドが必要です。コンフィギュレーションがプライマリ ASA 1000V からセカンダリ ASA 1000V に送信された後に、2つのコンフィギュレーション間で永続的に異なるのは、**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 ASA 1000V がプライマリまたはセカンダリとして識別されます。

前提条件

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

手順の詳細

セカンダリ ASA 1000V を設定するには、次の手順を実行します。

	コマンド	目的
ステップ1	<pre>failover lan interface if_name interface_id</pre> <p>例:</p> <pre>hostname(config)# failover lan interface folink gigabitEthernet0/2</pre>	<p>フェールオーバー インターフェイスとして使用するインターフェイスを指定します。(プライマリ ASA 1000V に使用したものと同一設定を使用します)。</p> <p><i>if_name</i> 引数は、<i>interface_id</i> 引数で指定されたインターフェイスに名前を割り当てます。</p> <p>このインターフェイスは、イーサネット インターフェイスです。フェールオーバー コンフィギュレーションでは、インターフェイス名の代わりに、インターフェイス ID (たとえば、<i>gigabitEthernet0/2</i>) を使用します。</p>
ステップ2	<pre>failover interface ip if_name [ip_address mask standby ip_address]</pre> <p>例:</p> <pre>hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2</pre>	<p>アクティブおよびスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。</p> <p>フェールオーバー ペアの両方の ASA 1000V からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。</p> <p> (注) プライマリ ASA 1000V にフェールオーバー インターフェイスを設定する場合 (同じ IP アドレスを含む)、プライマリ ASA 1000V でこのコマンドを入力するときは、正確に入力してください。</p>
ステップ3	<pre>interface interface_id</pre> <p>no shutdown</p> <p>例:</p> <pre>hostname(config)# interface gigabitEthernet0/2 hostname(config-if)# no shutdown</pre>	<p>インターフェイスをイネーブルにします。</p>

	コマンド	目的
ステップ4	<pre>failover lan unit secondary</pre> <p>例: hostname(config)# failover lan unit secondary</p>	<p>(任意) この ASA 1000V をセカンダリ ASA 1000V として指定します。</p> <p> (注) ASA 1000V 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。</p>
ステップ5	<pre>failover</pre> <p>例: hostname(config)# failover</p>	<p>フェールオーバーをイネーブルにします。</p> <p>フェールオーバーをイネーブルにすると、アクティブ ASA 1000V では実行メモリ内のコンフィギュレーションがスタンバイ ASA 1000V に送信されます。コンフィギュレーションの同期時に、メッセージ「Beginning configuration replication: Sending to mate」および「End Configuration Replication to mate」がアクティブ ASA 1000V のコンソールに表示されます。</p>
ステップ6	<pre>copy running-config startup-config</pre> <p>例: hostname(config)# copy running-config startup-config</p>	<p>コンフィギュレーションをフラッシュ メモリに保存します。</p> <p>実行コンフィギュレーションの複製が完了した後で、コマンドを入力します。</p>

オプションのアクティブ/スタンバイ フェールオーバー設定値の設定

ここでは、次の内容について説明します。

- 「ステートフル フェールオーバーでの HTTP 複製のイネーブル化」 (P.3-21)
- 「インターフェイス モニタリングのディセーブル化とイネーブル化」 (P.3-21)
- 「フェールオーバー基準の設定」 (P.3-22)
- 「ASA 1000V およびインターフェイスのヘルス ポーリング時間の設定」 (P.3-22)
- 「仮想 MAC アドレスの設定」 (P.3-23)

フェールオーバー ペアのプライマリ ASA 1000V を最初に設定する（「[プライマリ ASA 1000V の設定](#)」 (P.3-17) を参照）場合、または、初期コンフィギュレーションの後でフェールオーバー ペアのアクティブ ASA 1000V を設定する場合は、オプションのアクティブ/スタンバイ フェールオーバーを設定できます。

ステートフル フェールオーバーでの HTTP 複製のイネーブル化

HTTP 接続がステート情報複製に含まれるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP 接続は通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP 接続は複製されるステート情報に自動的に含まれません。

ステートフル フェールオーバーがイネーブルの場合に、HTTP ステート複製をイネーブルにするには、次のコマンドを入力します。

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

インターフェイス モニタリングのディセーブル化とイネーブル化

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

1 台の ASA 1000V で最大 256 のインターフェイスをモニタできます。デフォルトでは、イーサネット インターフェイスのモニタリングはイネーブルに、サブインターフェイスのモニタリングはディセーブルになっています。

インターフェイス ポーリング頻度ごとに、ASA 1000V フェールオーバー ペア間で hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ~ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと (25 秒間)、そのインターフェイスでテストが開始します。

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

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

■ アクティブ/スタンバイ フェールオーバーの設定

シングル コンフィギュレーション モードの ASA 1000V の特定のインターフェイスのヘルス モニタリングをイネーブルまたはディセーブルにするには、次のいずれかのコマンドを入力します。

<pre>no monitor-interface if_name</pre> <p>例: hostname(config)# no monitor-interface lanlink</p>	インターフェイスのヘルス モニタリングをディセーブルにします。
<pre>monitor-interface if_name</pre> <p>例: hostname(config)# monitor-interface lanlink</p>	インターフェイスのヘルス モニタリングをイネーブルにします。

フェールオーバー基準の設定

インターフェイス数またはモニタされているインターフェイスの割合を指定して、この数または割合を超えたインターフェイスに障害が発生した場合にフェールオーバーが発生するようにできます。デフォルトでは、1つのインターフェイス障害でフェールオーバーが行われます。

デフォルトのフェールオーバー基準を変更するには、次のコマンドを入力します。

コマンド	目的
<pre>failover interface-policy num[%]</pre> <p>例: hostname (config)# failover interface-policy 20%</p>	<p>デフォルトのフェールオーバー基準を変更します。</p> <p>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 ~ 256 を設定できます。</p> <p>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。</p>

ASA 1000V およびインターフェイスのヘルス ポーリング時間の設定

ASA 1000V は、各データ インターフェイスから hello パケットを送信して、インターフェイスヘルスをモニタします。ASA 1000V は、フェールオーバー リンクを通して hello メッセージを送信し、ASA 1000V のヘルスをモニタします。保持時間の半分以上が経過しても ASA 1000V がピア ASA 1000V の対応するインターフェイスから hello パケットを受信しない場合、追加のインターフェイスのテストが開始されます。hello パケットまたはテストの正常終了の結果が指定した保持時間内に受信されない場合、インターフェイスは失敗としてマークされます。失敗したインターフェイスの数がフェールオーバー基準を満たしている場合、フェールオーバーが発生します。

ポーリング時間および保持時間を短縮すると、ASA 1000V はインターフェイスの障害に対してより迅速な検出と応答を実行できますが、多くのシステム リソースを消費することがあります。ポーリング時間と保持時間を延長すると、ASA 1000V がネットワーク上でフェールオーバーし、長時間の遅延が発生するのを防止できます。

コマンド	目的
<pre>failover polltime interface [msec] time [holdtime time]</pre> <p>例:</p> <pre>hostname (config): failover polltime interface msec 500 holdtime 5</pre>	<p>インターフェイスのポーリング時間と保持時間を変更します。</p> <p>ポーリング時間の有効な値は 1 ～ 15 秒で、オプションの msec キーワードを使用すると、500 ～ 999 ミリ秒です。hello パケットを受信できなかったときからインターフェイスが失敗としてマークされるまでの時間が、保持時間によって決まります。保持時間に有効な値は、5 ～ 75 秒です。ポーリング時間の 5 倍に満たない保持時間は入力できません。</p> <p>インターフェイス リンクがダウンしていると、インターフェイスのテストは実行されず、障害のあるインターフェイスの数が設定されたフェールオーバー基準に合致するか、または基準を超過している場合、スタンバイ ASA 1000V は、1 つのインターフェイス ポーリング期間内でアクティブになります。</p>
<pre>failover polltime [unit] [msec] poll_time [holdtime [msec] time]</pre> <p>例:</p> <pre>hostname(config)# failover polltime unit msec 200 holdtime msec 800</pre>	<p>装置のポーリング時間と保持時間を変更します。</p> <p>ユニットのポーリング タイムの 3 倍未満の値を holdtime の値として入力することはできません。ポーリング時間が短いほど、ASA 1000V は短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。</p> <p>1 回のポーリング期間中に、装置がフェールオーバー通信インターフェイスで hello パケットを検出しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。</p> <p>コンフィギュレーションには、failover polltime [unit] コマンドと failover polltime interface コマンドの両方を含めることができます。</p>

仮想 MAC アドレスの設定

アクティブ/スタンバイ フェールオーバーでは、プライマリ ASA 1000V の MAC アドレスは常にアクティブ IP アドレスに関連付けられています。セカンダリ ASA 1000V は、最初にブートされてアクティブになると、そのインターフェイスの焼き付け MAC アドレスを使用します。プライマリ ASA 1000V がオンラインになると、セカンダリ ASA 1000V はプライマリ ASA 1000V から MAC アドレスを取得します。この変更によって、ネットワークトラフィックが中断することがあります。

プライマリ ASA 1000V よりも前にオンラインになった場合でも、セカンダリ ASA 1000V がアクティブ ASA 1000V であるときは、セカンダリが正しい MAC アドレスを使用するように、各インターフェイスの仮想 MAC アドレスを設定できます。仮想 MAC アドレスを指定しない場合、フェールオーバーペアは焼き付け NIC アドレスを MAC アドレスとして使用します。



(注)

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

インターフェイスの仮想 MAC アドレスを設定するには、アクティブ ASA 1000V で次のコマンドを入力します。

コマンド	目的
<p>failover mac address <i>phy_if active_mac standby_mac</i></p> <p>例: hostname (config): failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8</p>	<p>インターフェイスの仮想 MAC アドレスを設定します。</p> <p><i>phy_if</i> 引数は、インターフェイスの名前 (Ethernet1 など) です。 <i>active_mac</i> および <i>standby_mac</i> 引数は、H.H.H 形式 (H は 16 ビットの 16 進数) の MAC アドレスです。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。</p> <p><i>active_mac</i> アドレスはインターフェイスのアクティブ IP アドレスに関連付けられ、<i>standby_mac</i> はインターフェイスのスタンバイ IP アドレスに関連付けられます。</p> <p>ASA 1000V に仮想 MAC アドレスを設定するには複数の方法があります。仮想 MAC アドレスを設定するために複数の方式を使用した場合、ASA 1000V は次の優先順位で、インターフェイスに割り当てる仮想 MAC アドレスを決定します。</p> <ol style="list-style-type: none"> 1. mac-address コマンド (インターフェイス コンフィギュレーション モード) のアドレス 2. mac-address auto コマンドが生成したアドレス 3. failover mac address コマンドのアドレス 4. 焼き付け MAC アドレス <p>show interface コマンドを使用して、インターフェイスが使用している MAC アドレスを表示します。</p>

フェールオーバーの制御

この項では、フェールオーバーの制御およびモニタの方法について説明します。次の項目を取り上げます。

- 「フェールオーバーの強制実行」 (P.3-25)
- 「フェールオーバーのディセーブル化」 (P.3-25)
- 「障害が発生した ASA 1000V の復元」 (P.3-25)

フェールオーバーの強制実行

スタンバイ ASA 1000V を強制的にアクティブにするには、次のいずれかのコマンドを入力します。

コマンド	目的
failover active 例: hostname# failover active	フェールオーバー ペアのスタンバイ ASA 1000V で入力された場合に、フェールオーバーを強制実行します。スタンバイ ASA 1000V がアクティブ ASA 1000V になります。
no failover active 例: hostname# no failover active	フェールオーバー ペアのアクティブ ASA 1000V で入力された場合に、フェールオーバーを強制実行します。アクティブ ASA 1000V がスタンバイ ASA 1000V になります。

フェールオーバーのディセーブル化

フェールオーバーをディセーブル化するには、次のコマンドを入力します。

コマンド	目的
no failover 例: hostname (config)# no failover	フェールオーバーをディセーブルにします。アクティブ/スタンバイ ペアでフェールオーバーをディセーブルにすると、再起動されるまで各 ASA 1000V のアクティブおよびスタンバイ状態が維持されます。たとえば、スタンバイ ASA 1000V はスタンバイ モードのまま維持されるので、両方の ASA 1000V はトラフィックの転送を開始しません。(フェールオーバーがディセーブル化されていても) スタンバイ ASA 1000V をアクティブにするには、「 フェールオーバーの強制実行 」(P.3-25) を参照してください。

障害が発生した ASA 1000V の復元

障害が発生した ASA 1000V を障害のない状態に復元するには、次のコマンドを入力します。

コマンド	目的
failover reset 例: hostname (config)# failover reset	障害が発生した ASA 1000V を障害のない状態に復元します。障害が発生した ASA 1000V を障害のない状態に復元しても、それ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 ASA 1000V は、フェールオーバー (強制または成り行き) によってアクティブになるまではスタンバイ状態のままです。

フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

-
- ステップ 1** FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ ASA 1000V 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 ASA 1000V で次のコマンドを入力し、フェールオーバーを強制実行します。
- ```
hostname(config)# no failover active
```
- ステップ 3** FTP を使用して、2 つの同じホスト間で別のファイルを送信します。
- ステップ 4** テストが成功しなかった場合は、**show failover** コマンドを入力してフェールオーバー ステータスを確認します。
- ステップ 5** テストが終了したら、新しくアクティブになった ASA 1000V で次のコマンドを入力すると、ASA 1000V をアクティブ ステータスに復元できます。
- ```
hostname(config)# no failover active
```
-

アクティブ/スタンバイ フェールオーバーのモニタリング



(注)

フェールオーバー イベントが発生した後、デバイスのモニタリングを継続するには、ASDM を再起動するか、または [Devices] ペインにリストされる別のデバイスに切り替えて、元の ASA 1000V に戻す必要があります。この操作が必要なのは、ASDM がデバイスから切断されて再接続された場合、接続のモニタリングが再確立されないためです。

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

コマンド	目的
<code>show failover</code>	ASA 1000V のフェールオーバー状態についての情報を表示します。
<code>show monitor-interface</code>	モニタ対象インターフェイスの情報を表示します。
<code>show running-config failover</code>	実行コンフィギュレーション内のフェールオーバー コマンドを表示します。

モニタリング コマンドの出力の詳細については、コマンドリファレンスを参照してください。

アクティブ/スタンバイ フェールオーバーの機能履歴

表 3-2 に、この機能のリリース履歴を示します。

表 3-2 アクティブ/スタンバイ フェールオーバーの機能履歴

機能名	リリース	機能情報
ASA 1000V のフェールオーバーのサポート	8.7(1)	ASA 1000V のアクティブ/スタンバイ フェールオーバーペアに割り当てられるインターフェイスは、GigabitEthernet0/2 です。

