CHAPTER 13

フェールオーバーの設定

この章では、FWSM のフェールオーバー機能について説明します。2 つの FWSM を設定することで、1 つに障害が発生しても、もう 1 つに操作を引き継がせることができます。フェールオーバー機能はルーテッド ファイアウォール モードと透過ファイアウォール モードの両方で使用でき、コンテキスト モードはシングルでもマルチでもかまいません。

この章で説明する内容は、次のとおりです。

フェールオーバーの設定例については、「フェールオーバーの設定例」（p.B-20）を参照してください。

フェールオーバーの概要

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 FWSM が必要です。アクティブ インターフェイスと装置がヘルス モニタされ、特定のフェールオーバー条件に合致するかどうかが判断されます。これらの条件に合致すると、フェールオーバーが発生します。

FWSM では、アクティブ / アクティブ フェールオーバーとアクティブ / スタンバイ フェールオーバーの 2 つのフェールオーバー設定がサポートされます。各フェールオーバー設定には、フェールオーバーを決定および実行するための独自の方法があります。

アクティブ / アクティブ フェールオーバーでは、両方の装置がネットワーク トラフィックを転送することができます。従って、負荷分散をネットワーク上で設定できます。アクティブ / アクティブ フェールオーバーは、マルチコンテキスト モードで動作する装置でのみ使用できます。

アクティブ / スタンバイ フェールオーバーでは、1 つの装置のみがトラフィックを転送し、もう 1 つの装置はスタンバイ状態で待機します。アクティブ / スタンバイ フェールオーバーは、シングル コンテキスト モードまたはマルチコンテキスト モードのいずれでも使用できます。

いずれのフェールオーバー設定も、ステートフルまたはステートレス（標準）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。

フェールオーバーのシステム要件

ここでは、FWSM のフェールオーバー設定のソフトウェア要件とライセンス要件について説明します。内容は次のとおりです。

ソフトウェア要件

フェールオーバー設定をした 2 つの装置は、同じメジャー（最初の番号）ソフトウェア バージョンおよびマイナー（2 番めの番号）ソフトウェア バージョンを持つ必要があります。ただし、アップグレード プロセス中は異なるソフトウェア バージョンを使用できます。たとえば、ある装置を Version 3.1(1) から Version 3.1(2) にアップグレードして、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。長期的な互換性を確保するために、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推奨します。

ライセンス要件

両装置とも同じライセンスを持つ必要があります。

フェールオーバー リンクとステート リンク

ここでは、フェールオーバー設定での 2 つの装置間の専用接続である、フェールオーバー リンクとステート リンクについて説明します。内容は次のとおりです。

フェールオーバー リンク

フェールオーバー ペアの 2 つの装置はフェールオーバー リンク経由で常時通信を行い、それぞれの装置の動作ステータスを把握します。フェールオーバー リンク経由で通信する情報は次のとおりです。

- 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 ステータス
- MAC アドレス交換
- 設定の複製と同期化

注意　フェールオーバー キーで通信をセキュリティ保護している場合を除き、フェールオーバーおよびステートフル フェールオーバー リンク間の情報はすべてクリア テキストで送信されます。

フェールオーバー リンクでは、標準のネットワーキング インターフェイスとしては設定しない、フェールオーバー通信専用の特別な VLAN インターフェイスを使用します。この VLAN は、フェールオーバー リンク（および任意で使用するステート リンク）だけに使用する必要があります。フェールオーバー リンク VLAN を他の VLAN と共有すると、断続的なトラフィック障害や ping エラーおよび ARP エラーが発生することがあります。シャーシ間のフェールオーバーでは、フェールオーバー リンク用としてスイッチ上の専用インターフェイスを使用します。

マルチコンテキスト モードで動作するシステムでは、システム コンテキストにフェールオーバー リンクが常時設定されます。このインターフェイス（および使用する場合はステート リンク）は、システム コンテキストで設定可能な唯一のインターフェイスです。他のすべてのインターフェイスは、セキュリティ コンテキスト内で割り当てられ、設定されます。

（注）　フェールオーバー 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。

ステート リンク

ステートフル フェールオーバーを使用するには、すべてのステート情報を渡すためのステート リンクを設定する必要があります。このリンクはフェールオーバー リンクと同じでもかまいませんが、ステート リンク用に別の VLAN および IP アドレスを割り当てることを推奨します。ステート トラフィックはサイズが大きいことがあるので、別のリンクを使用した方がパフォーマンスは向上します。

ステート リンク インターフェイスは標準ネットワーキング インターフェイスとしては設定されず、ステートフル フェールオーバー通信のためにのみ使用されます。ステート リンクとフェールオーバー リンクを共有する場合は、任意でフェールオーバー通信にも使用されます。

マルチコンテキスト モードでは、システム コンテキストにステート リンクが常時設定されます。システム コンテキストのインターフェイスは、このインターフェイスとフェールオーバー インターフェイスだけです。他のすべてのインターフェイスは、セキュリティ コンテキスト内で割り当てられ、設定されます。

（注） 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。

注意 フェールオーバー キーで通信をセキュリティ保護している場合を除き、フェールオーバーおよびステートフル フェールオーバー リンク間の情報はすべてクリア テキストで送信されます。

シャーシ内およびシャーシ間のモジュール配置

プライマリとセカンダリの FWSM は、同じスイッチ内または 2 台の異なるスイッチに搭載できます。ここでは、各オプションについて説明します。

- シャーシ内フェールオーバー（p.13-4）
- シャーシ間フェールオーバー（p.13-5）

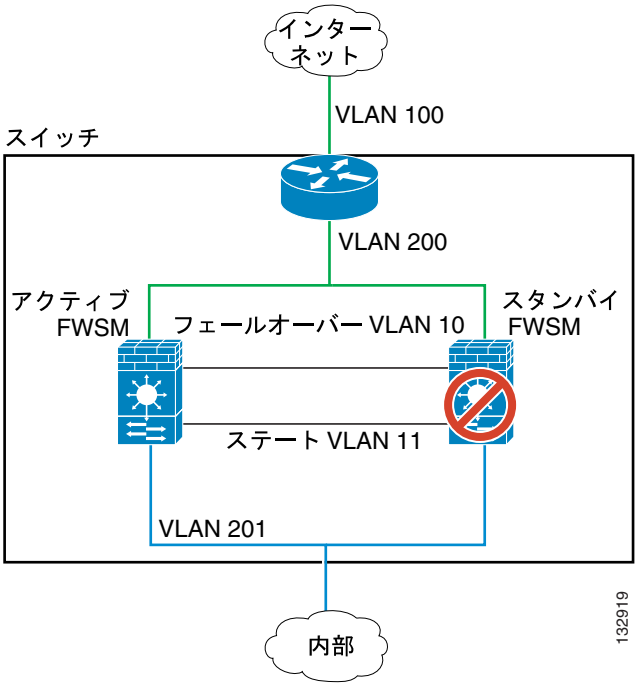
シャーシ内フェールオーバー

セカンダリ FWSM をプライマリ FWSM と同じスイッチに搭載した場合は、モジュール レベルの障害から保護する必要があります。モジュール レベルの障害のほか、スイッチ レベルの障害を保護するには、「シャーシ間フェールオーバー」（p.13-5）を参照してください。

両方の FWSM に同じ VLAN が割り当てられますが、ネットワーキングに参加するのはアクティブ モジュールだけです。スタンバイ モジュールは、トラフィックを転送しません。

図 13-1 に、一般的なスイッチ間の構成を示します。

図 13-1　スイッチ内フェールオーバー



シャーシ間フェールオーバー

スイッチレベルの障害から保護するため、セカンダリ FWSM を別のスイッチに搭載することができます。FWSM は直接スイッチとフェールオーバーを調整するのではなく、スイッチと協調してフェールオーバー操作を行います。スイッチのフェールオーバー設定については、スイッチのマニュアルを参照してください。

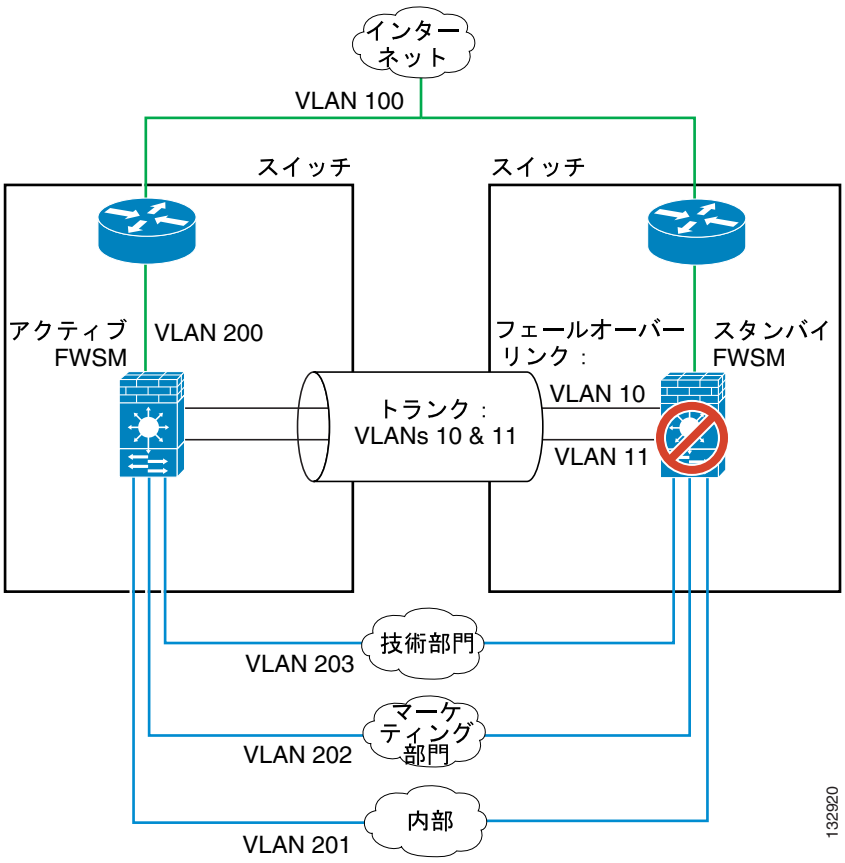
FWSM 間でフェールオーバー通信を行うには、2 台のスイッチ間に、フェールオーバーおよびステート VLAN を伝送するトランク ポートを設定することを推奨します。トランクにより、2 つの装置間のフェールオーバー通信の障害リスクは最小限に抑えられます。

他の VLAN については、両方のスイッチがすべてのファイアウォール VLAN にアクセスでき、モニタ対象 VLAN が両方のスイッチ間で正常に hello パケットを渡すことができるようにします。

図 13-2 に、スイッチと FWSM の一般的な冗長構成を示します。2 台のスイッチ間のトランクは、フェールオーバー FWSM VLAN（VLAN 10 と 11）を転送します。

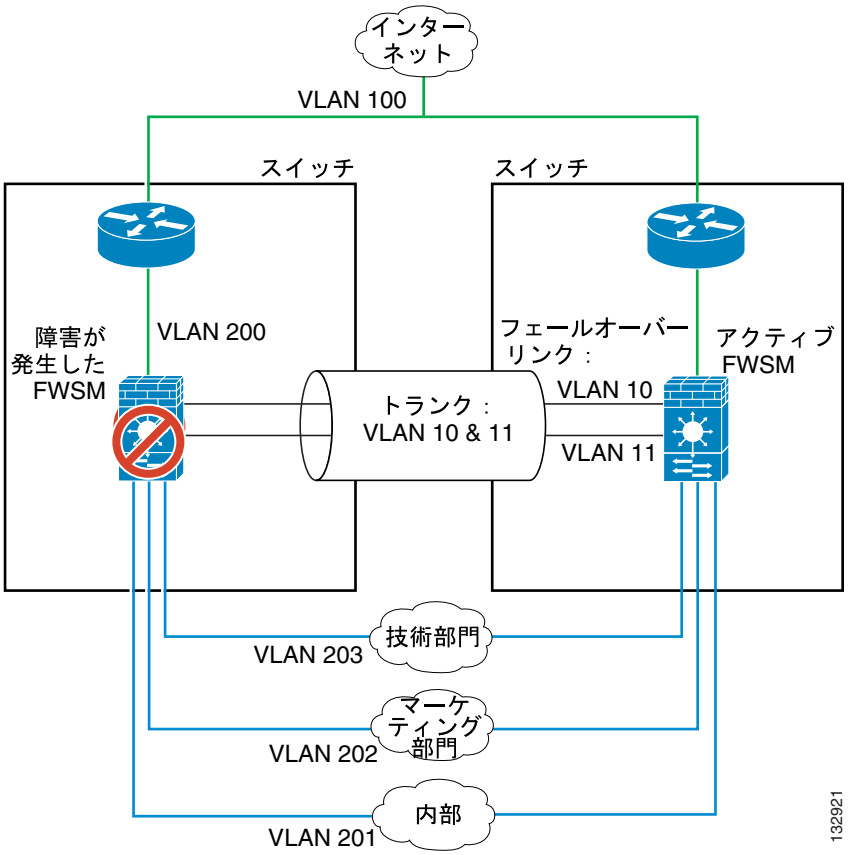
（注）　FWSM　のフェールオーバーはスイッチのフェールオーバーに依存しない独立した機能ですが、スイッチのフェールオーバーが発生した場合には、FWSM もそれに対応します。

図 13-2　　標準操作



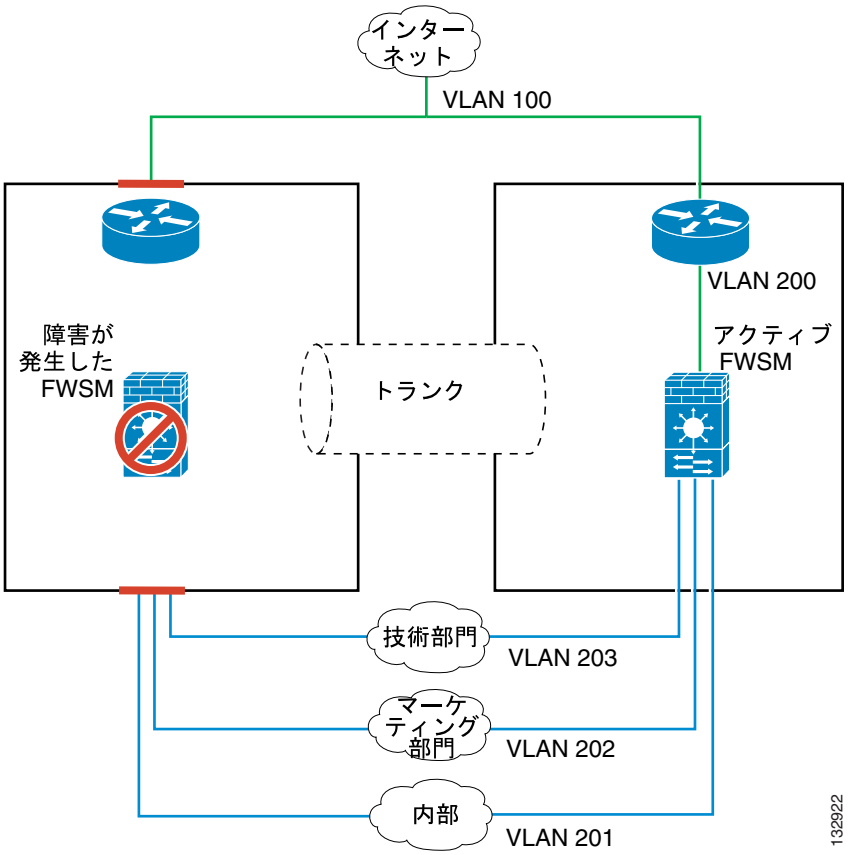
プライマリ FWSM に障害が発生すると、セカンダリ FWSM がアクティブになってファイアウォール VLAN を通過します（図 13-3）。

図 13-3　FWSM の障害



スイッチ全体に障害が発生し、FWSM にも障害が発生した場合（電源切断など）には、スイッチと FWSM の両方でセカンダリ ユニットへのフェールオーバーが実行されます（図 13-4）。

図 13-4　スイッチの障害



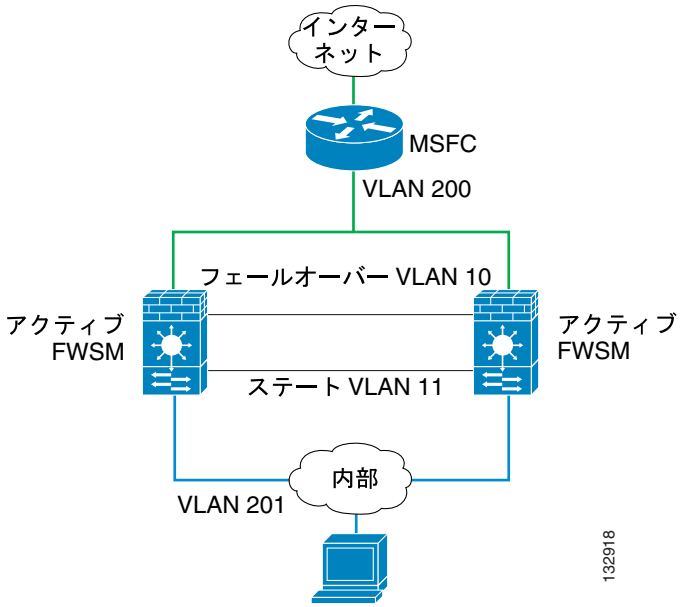
透過ファイアウォールの要件

透過モードでフェールオーバー機能を使用しているときにループを回避するには、BPDU の送信をサポートするスイッチ ソフトウェアを使用し、BPDU が許可されるように FWSM を設定する必要があります。BPDU が自動的に許可されるスイッチ ソフトウェアのバージョンについては、「スイッチ ハードウェアおよびソフトウェアの互換性」（p.A-2）を参照してください。

FWSM 経由の BPDU を許可するには、EtherType ACL を設定して、「EtherType アクセス リストの追加」（p.10-10）の説明のとおりに、両方のインターフェイスに適用します。

両モジュールが相手の存在を検出したり、フェールオーバー リンクが不正であったりするなど、両方のモジュールが同時にアクティブのときに、ループが発生することがあります。両方の FWSM が 2 つの同じ VLAN 間でパケットをブリッジングするので、外部宛ての内部パケットが両方の FWSM によって無限に複製され、ループが発生します（図 13-5 を参照）。BPDU がタイミングよく交換された場合は、スパニングツリー プロトコルによって、これらのループが遮断されます。ループを遮断するには、VLAN 200 と VLAN 201 間で送信される BPDU をブリッジングする必要があります。

図 13-5　透過モード時の潜在的なループ



アクティブ / スタンバイ フェールオーバーとアクティブ / アクティブ フェールオーバー

ここでは、各フェールオーバーの設定について詳しく説明します。内容は次のとおりです。

- アクティブ / スタンバイ フェールオーバー（p.13-9）
- アクティブ / アクティブ フェールオーバー（p.13-13）
- 使用するフェールオーバー タイプの決定（p.13-17）

アクティブ / スタンバイ フェールオーバー

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。内容は次のとおりです。

- アクティブ / スタンバイ フェールオーバーの概要（p.13-9）
- 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.13-10）
- デバイスの初期化と設定の同期化（p.13-10）
- コマンドの複製（p.13-11）
- フェールオーバーのトリガー（p.13-11）
- フェールオーバーの動作（p.13-12）

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、障害が発生した装置の機能を、スタンバイ FWSM に引き継ぐことができます。アクティブ ユニットに障害が発生すると、その装置はスタンバイ ステートに移行し、逆にスタンバイ ユニットがアクティブ ステートに移行します。アクティブになった装置は障害が発生した装置の IP アドレス（透過ファイアウォールの場合は管理 IP アドレス）と MAC アドレスを推定して、トラフィックの転送を開始します。スタンバイ ステートに移行した装置は、スタンバイ IP アドレス /MAC アドレスを引き継ぎます。ネットワーク デバイスは MAC/IP アドレスのペアの変更を知らないため、ネットワーク上で ARP エントリの変更やタイムアウトは発生しません。

（注）　マルチコンテキスト モードでは、FWSM 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が、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 ステータスとアクティブ / スタンバイ ステータス

フェールオーバーの 2 台の装置の主要な違いは、一方がアクティブで一方がスタンバイであること、すなわち、どちらの IP アドレスを使用し、どちらの装置がアクティブにトラフィックを転送するか、ということです。

ただし、プライマリ（設定に指定されている）かセカンダリかによって、両装置に多少の違いがあります。

- 両方の装置を同時に起動した場合、（動作状態が同じであれば）プライマリ ユニットが常にアクティブになります。
- プライマリ ユニットの MAC アドレスは常にアクティブ IP アドレスと組み合わされます。例外が発生するのは、セカンダリ ユニットがアクティブになり、フェールオーバー リンクでプライマリ MAC アドレスを取得できない場合です。この場合、セカンダリ モジュールの MAC アドレスが使用されます。

デバイスの初期化と設定の同期化

設定の同期化は、フェールオーバー ペアの一方または両方のデバイスが起動するときに行われます。設定は常に、アクティブ ユニットからスタンバイ ユニットに同期されます。スタンバイ ユニットの初期起動が完了すると、実行コンフィギュレーションが消去され（アクティブ ユニットとの通信に必要なフェールオーバー コマンドを除く）、アクティブ ユニットはスタンバイ ユニットに設定全体を送信します。

アクティブ ユニットは次のように決定されます。

- 装置の起動時にすでにアクティブに実行しているピアが検出された場合、この装置がスタンバイ ユニットになります。
- 装置の起動時にピアが検出されなかった場合、この装置がアクティブ ユニットになります。
- 両方の装置を同時に起動する場合、プライマリ ユニットがアクティブ ユニットになり、セカンダリ ユニットがスタンバイ ユニットになります。

（注）　セカンダリ ユニットの起動時にプライマリ ユニットが検出されなかった場合、セカンダリ ユニットがアクティブ ユニットになります。セカンダリ ユニットは、アクティブ IP アドレスに独自の MAC アドレスを使用します。ただし、プライマリ ユニットが使用可能になると、セカンダリ ユニットは MAC アドレスをプライマリ ユニットの MAC アドレスに変更します。これにより、ネットワーク トラフィックが一時停止することがあります。

設定の同期化が開始されると、アクティブ ユニットの FWSM コンソールで「Beginning configuration replication: Sending to mate」というメッセージが表示され、同期化が終了すると「End Configuration Replication to mate」というメッセージが表示されます。設定の同期化の間、アクティブ ユニットに入力されたコマンドがスタンバイ ユニットに正しく複製されず、スタンバイ ユニットに入力されたコマンドがアクティブ ユニットから複製された設定によって上書きされることがあります。設定の複製プロセス中に、フェールオーバー ペアの各装置にコマンドを入力することは避けてください。設定の大きさによっては、複製に数秒から数分かかることがあります。

アクティブ ユニットに **write standby** コマンドを入力すると、スタンバイ ユニットの実行コンフィギュレーションが消去され（アクティブ ユニットとの通信に必要なフェールオーバー コマンドを除く）、アクティブ ユニットはスタンバイ ユニットに設定全体を送信します。

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。1 つのコンテキスト内で **write standby** コマンドを入力すると、そのコンテキストの設定だけが複製されます。

スタンバイ ユニットでは、複製された設定は実行メモリにのみ保存されます。同期後の設定をフラッシュ メモリに保存する手順は、次のとおりです。

- シングルコンテキスト モードで、アクティブ ユニットに **write memory** コマンドを入力します。コマンドがスタンバイ ユニットに複製され、設定がフラッシュ メモリに書き込まれます。
- マルチコンテキスト モードで、システム実行スペースからアクティブ ユニットに **write memory all** コマンドを入力します。このコマンドにより、システム コンフィギュレーションとすべてのコンテキスト コンフィギュレーションが保存されます。コマンドがスタンバイ ユニットに複製され、設定がフラッシュ メモリに書き込まれます。外部サーバ上にスタートアップ コンフィギュレーションのあるコンテキストには、ネットワーク経由でどちらの装置からでもアクセスできるので、各装置に個別に保存する必要はありません。または、アクティブ ユニットから外部サーバにディスク上のコンテキストをコピーし、さらにスタンバイ ユニット上のディスクにコピーすることもできます。これらは装置をリロードしたときに使用可能になります。

コマンドの複製

アクティブ ユニット上に入力されたコマンドは、フェールオーバー リンクを経由してスタンバイ ユニットに送信されます。コマンドの複製は、常にアクティブ ユニットからスタンバイ ユニットへと行われます。複製されたコマンドは、スタンバイ ユニットの実行コンフィギュレーションに保存されます。実行コンフィギュレーションをアクティブ ユニットのスタートアップ コンフィギュレーションに保存すると、実行コンフィギュレーションがスタンバイ ユニットのスタートアップ コンフィギュレーションに保存されます。ただし、コマンドを複製するために、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。

（注）　**mode** コマンドはセカンダリ ユニットには複製されません。

スタンバイ ユニット上での変更は、アクティブ ユニットには複製されません。スタンバイ ユニット上でコマンドを入力すると、FWSM に、「`**** WARNING **** Configuration Replication is NOT performed from Standby module to Active module. Configurations are no longer synchronized.`」（警告：スタンバイ ユニットからアクティブ ユニットへの設定の複製は実行できません。設定は同期化されません）というメッセージが表示されます。このメッセージは、設定に影響しないコマンドを多数入力した場合にも表示されます。

フェールオーバーのトリガー

装置の障害は、次のいずれかの状況で発生します。

- 装置にハードウェア障害または電源障害が発生した場合
- 装置にソフトウェア障害が発生した場合
- モニタ対象のインターフェイスの多くで障害が発生した場合
- アクティブ ユニット上に **no failover active** コマンドが入力された場合、またはスタンバイ ユニット上に **failover active** コマンドが入力された場合

フェールオーバーの動作

アクティブ / スタンバイ フェールオーバーでは、フェールオーバーは装置単位で発生します。マルチコンテキスト モードで実行されているシステムであっても、アクティブ / スタンバイ フェールオーバーでは、個別のコンテキストまたはコンテキスト グループのフェールオーバーを行うことはできません。

表 13-1 に、各障害イベントのフェールオーバーの動作を示します。各障害イベントについて、フェールオーバー ポリシー（フェールオーバーあり / フェールオーバーなし）、アクティブ ユニットにより実行される動作、スタンバイ ユニットにより実行される動作、フェールオーバー状態および動作に関するコメントを示します。

表 13-1　フェールオーバーの動作

障害イベント	ポリシー	アクティブ ユニットの動作	スタンバイ ユニットの動作	説明
アクティブ ユニットの障害（電源またはハードウェア）	フェールオーバー	適用外	アクティブになる アクティブ ユニットを障害装置としてマークする	モニタ対象インターフェイスまたはフェールオーバー リンク上で、hello メッセージが受信されません。
以前のアクティブ ユニットの回復	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 ユニットの障害（電源またはハードウェア）	フェールオーバーなし	スタンバイ ユニットを障害装置としてマークする	適用外	スタンバイ ユニットが障害装置してマークされた場合、インターフェイスの障害数がスレッシュホールドを超過しても、アクティブ ユニットはフェールオーバーを試行しません。
運用中のフェールオーバー リンクの障害	フェールオーバーなし	フェールオーバー インターフェイスを障害としてマークする	フェールオーバー インターフェイスを障害としてマークする	フェールオーバー リンクがダウンしていると、スタンバイ ユニットへのフェールオーバーを実行できないので、フェールオーバー リンクをできるだけ早く回復させる必要があります。
起動時のフェールオーバー リンクの障害	フェールオーバーなし	フェールオーバー インターフェイスを障害としてマークする	アクティブになる	起動時にフェールオーバー リンクがダウンした場合、両方の装置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	ステート情報が更新されず、フェールオーバーが発生するとセッションは終了します。
アクティブ ユニットのインターフェイス障害がスレッシュホールドを超過	フェールオーバー	アクティブ ユニットを障害装置としてマークする	アクティブになる	なし
スタンバイ ユニットのインターフェイス障害がスレッシュホールドを超過	フェールオーバーなし	動作なし	スタンバイ ユニットを障害装置としてマークする	スタンバイ ユニットが障害装置としてマークされた場合、インターフェイスの障害数がスレッシュホールドを超過しても、アクティブ ユニットはフェールオーバーを試行しません。

アクティブ / アクティブ フェールオーバー

ここでは、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。内容は次のとおりです。

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 フェールオーバーは、FWSM のマルチコンテキスト モードでのみ使用できます。アクティブ / アクティブ フェールオーバーの設定では、両方の FWSM がネットワーク トラフィックを転送できます。

アクティブ / アクティブ フェールオーバーでは、FWSM のセキュリティ コンテキストを *フェールオーバー グループ*に分割します。フェールオーバー グループは、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です。FWSM に最大 2 つのフェールオーバー グループを作成できます。管理コンテキストは常にフェールオーバー グループ 1 のメンバーで、デフォルトでは、割り当てられていないセキュリティ コンテキストもすべてフェールオーバー グループ 1 のメンバーです。

フェールオーバー グループは、アクティブ / アクティブ フェールオーバーでのフェールオーバーの基本単位となります。インターフェイス障害モニタリング、フェールオーバー、アクティブ / スタンバイ ステータスはすべて、装置ではなくフェールオーバー グループの属性です。プライマリ ユニットの MAC アドレスは、アクティブ コンテキストのすべてのインターフェイスで使用されます。

アクティブ フェールオーバー グループに障害が発生すると、スタンバイ ステートに移行し、関連するスタンバイ フェールオーバー グループがアクティブになります。アクティブになったフェールオーバー グループのインターフェイスは、障害が発生したフェールオーバー グループのインターフェイスの MAC アドレスと IP アドレスを推定します。スタンバイ ステートに移行したフェールオーバー グループのインターフェイスは、スタンバイ フェールオーバー グループの MAC アドレスと IP アドレスを引き継ぎます。

（注） 装置上のフェールオーバー　グループの障害は、その装置に障害が発生していることを意味するものではありません。装置には、トラフィックを転送する別のフェールオーバー グループが存在する可能性があります。

フェールオーバー グループを作成する場合、アクティブ ステートのフェールオーバー グループ 1 を持つ装置上に作成する必要があります。

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

アクティブ / スタンバイ フェールオーバーと同様、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 ユニットに指定され、もう 1 つの装置がセカンダリ ユニットに指定されます。アクティブ / スタンバイ フェールオーバーとは異なり、両方の装置を同時に起動したときにアクティブになる装置は決まっていません。代わりに、プライマリ / セカンダリの指定で、ペアに実行コンフィギュレーションを提供する装置、および両方の装置を同時に起動したときにフェールオーバー グループがアクティブ ステートとして表示される装置が決まります。

設定内の各フェールオーバー グループには、プライマリ ユニットまたはセカンダリ ユニットのプリファレンスが指定されます。このプリファレンスにより、両方の装置を同時に起動したときに、フェールオーバー グループのコンテキストがアクティブ ステートになるフェールオーバー ペアの装置が決まります。ペアの 1 つの装置上で両方のフェールオーバー グループをアクティブ ステートにして、もう 1 つの装置にスタンバイ ステートのフェールオーバー グループを含めることもできます。ただし、一般的な設定では、各フェールオーバー グループに別々のロール プリファレンスに割り当てて、それぞれを別の装置上でアクティブにし、デバイス間のトラフィックを分散させています。

（注）　FWSM では負荷分散サービスは提供されていません。負荷分散は、FWSM にトラフィックを転送するルータで処理する必要があります。

デバイスの初期化と設定の同期化

設定の同期化は、フェールオーバー ペアの一方または両方の装置が起動するときに行われます。

ピア装置が使用できない間、装置を起動すると、フェールオーバー グループおよび装置のプライマリ / セカンダリ指定に関係なく、両方のフェールオーバー グループがその装置上でアクティブになります。設定の同期化は行われません。ピア装置が使用できない理由として、ピア装置の電源が切られている、ピア装置が障害ステートにある、装置間のフェールオーバー リンクが確立されていない、などがあります。

ピア装置がアクティブの間、（両方のフェールオーバー グループをアクティブにして）装置を起動すると、起動している装置はアクティブ ユニットに接続して実行コンフィギュレーションを取得します。デフォルトでは、各フェールオーバー グループおよび装置のプライマリ / セカンダリ指定に関係なく、フェールオーバー グループはアクティブ ユニット上でアクティブのままです（**preempt** コマンドで設定されていないかぎり）。次のいずれかが発生するまで、フェールオーバー グループは最初の装置上でアクティブのままになります。

- フェールオーバー状態により、フェールオーバー　グループがピア装置上でアクティブになった。
- **no failover active** コマンドを使用して、フェールオーバー グループをピア装置上で強制的に手動でアクティブにした。
- フェールオーバー グループの優先装置が使用可能になったときに、**preempt** コマンドにより、その装置上でフェールオーバー グループを強制的にアクティブにした。

両方の装置を同時に起動すると、プライマリ ユニットがアクティブ ユニットになります。セカンダリ ユニットは、プライマリ ユニットから実行コンフィギュレーションを取得します。設定が同期されると、各フェールオーバー グループはその優先装置上でアクティブになります。

コマンドの複製

両方の装置が実行されたあと、一方の装置からもう一方の装置に、次のようにコマンドが複製されます。

- セキュリティ コンテキスト内で入力されたコマンドは、セキュリティ コンテキストがアクティブ ステートに表示される装置からピア装置に複製されます。

（注）　所属するフェールオーバー グループが装置上でアクティブ ステートであれば、コンテキストはその装置上でアクティブ ステートとみなされます。

- システム実行スペースで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートの装置からフェールオーバー グループ 1 がスタンバイ ステートの装置に複製されます。
- 管理コンテキストで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ ステートの装置からフェールオーバー グループ 1 がスタンバイ ステートの装置に複製されます。

コマンドを適切な装置に入力せず、コマンドの複製が失敗した場合、設定は同期されません。次回、設定の同期化を行なったときに、それらの変更内容が失われる可能性があります。

（注）　**mode** コマンドは複製されません。

write standby コマンドを使用して、同期されなかった設定を再度同期化することができます。アクティブ / アクティブ フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- **write standby** コマンドをシステム実行スペースに入力すると、FWSM のシステム コンフィギュレーションおよびすべてのセキュリティ コンテキストの設定がピア装置に書き込まれます。これには、スタンバイ ステートのセキュリティ コンテキストの設定情報も含まれます。コマンドは、フェールオーバー グループ 1 がアクティブ ステートになっている装置のシステム実行スペースに入力する必要があります。
- **write standby** コマンドをセキュリティ コンテキストに入力すると、そのセキュリティ コンテキストの設定だけがピア装置に書き込まれます。コマンドは、セキュリティ コンテキストがアクティブ ステートに表示される装置上のセキュリティ コンテキストに入力する必要があります。

ピア装置への複製の場合、複製されたコマンドはフラッシュ メモリには保存されず、実行コンフィギュレーションに追加されます。複製されたコマンドを両方の装置のフラッシュ メモリに保存するには、変更を加えた装置上で **write memory** コマンドまたは **copy running-config startup-config** コマンドを使用します。コマンドがピア装置に複製され、設定がそのピア装置上のフラッシュ メモリに保存されます。

フェールオーバーのトリガー

アクティブ / アクティブ フェールオーバーでは、次のいずれかのイベントが発生した場合、装置レベルでフェールオーバーをトリガーできます。

- 装置にハードウェア障害が発生した場合
- 装置に電源障害が発生した場合
- 装置にソフトウェア障害が発生した場合
- システム実行スペースに **no failover active** コマンドまたは **failover active** コマンドが入力された場合

次のいずれかのイベントが発生した場合、フェールオーバー グループ レベルでフェールオーバーがトリガーされます。

- フェールオーバー グループに属するコンテキストの、非常に多くのモニタ対象インターフェイスで障害が発生した場合
- **no failover active group** *group_id* コマンドが入力された場合

フェールオーバー グループに障害が発生する前に、障害が発生する必要のあるフェールオーバー グループ内のインターフェイスの数または割合を指定して、各フェールオーバー グループのフェールオーバー スレッシュホールドを設定します。フェールオーバー グループにはマルチコンテキストを含めることが可能で、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可能であるため、シングルコンテキストのすべてのインターフェイスに障害が発生しても、関連するフェールオーバー グループには障害を発生させません。

インターフェイスおよび装置のモニタリングの詳細については、「フェールオーバーのヘルス モニタ」（p.13-18）を参照してください。

フェールオーバーの動作

アクティブ / アクティブ フェールオーバーの設定では、フェールオーバーはシステム単位ではなくフェールオーバー グループ単位で発生します。たとえば、両方のフェールオーバー グループをプライマリ ユニット上でアクティブに指定すると、フェールオーバー グループ 1 に障害が発生した場合、フェールオーバー グループ 2 はプライマリ ユニット上でアクティブのままになります。他方、フェールオーバー グループ 1 はセカンダリ ユニット上でアクティブになります。

（注）　アクティブ / アクティブ フェールオーバーを設定する場合、両方の装置の合計トラフィックが各装置の容量内に収まるようにしてください。

表 13-2 に、各障害イベントのフェールオーバーの動作を示します。各障害イベントについて、ポリシー（フェールオーバーが発生するかどうか）、アクティブ フェールオーバー グループの動作、スタンバイ フェールオーバー グループの動作を示します。

表 13-2　アクティブ / アクティブ フェールオーバーのフェールオーバー動作

障害イベント	ポリシー	アクティブ グループの動作	スタンバイ グループの動作	説明
装置に電源障害またはソフトウェア障害が発生	フェールオーバー	スタンバイ ユニットを障害装置としてマークする	アクティブになる アクティブ ユニットを障害装置としてマークする	フェールオーバー ペア内の装置に障害が発生すると、その装置上のすべてのアクティブ フェールオーバー グループが障害フェールオーバー グループとしてマークされ、ピア装置上でアクティブになります。
アクティブ フェールオーバー グループのインターフェイス障害がスレッシュホールドを超過	フェールオーバー	アクティブ グループを障害グループとしてマークする	アクティブになる	なし
スタンバイ フェールオーバー グループのインターフェイス障害がスレッシュホールドを超過	フェールオーバーなし	動作なし	スタンバイ グループを障害グループとしてマークする	スタンバイ フェールオーバー グループが障害フェールオーバー グループとしてマークされた場合、インターフェイスの障害数がスレッシュホールドを超過しても、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試行しません。
以前のアクティブ フェールオーバー グループの回復	フェールオーバーなし	動作なし	動作なし	**preempt** コマンドで設定された場合を除き、フェールオーバー グループは現在の装置上でアクティブのままになります。
起動時のフェールオーバー リンクの障害	フェールオーバーなし	アクティブになる	アクティブになる	起動時にフェールオーバー リンクがダウンした場合、両方の装置上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。

表 13-2　アクティブ / アクティブ フェールオーバーのフェールオーバー動作（続き）

障害イベント	ポリシー	アクティブ グループの動作	スタンバイ グループの動作	説明
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	ステート情報が更新されず、フェールオーバーが発生するとセッションは終了します。
運用中のフェールオーバー リンクの障害	フェールオーバーなし	適用外	適用外	各装置はフェールオーバー インターフェイスを障害としてマークします。フェールオーバー リンクがダウンしていると、スタンバイ ユニットへのフェールオーバーを実行できないので、フェールオーバー リンクはできるだけ早く回復させる必要があります。

使用するフェールオーバー タイプの決定

選択するフェールオーバー タイプは、FWSM の設定および FWSM の使用方法によって異なります。

FWSM をシングルモードで実行している場合、アクティブ / スタンバイ フェールオーバーのみ使用可能です。アクティブ / アクティブ フェールオーバーは、FWSM をマルチコンテキスト モードで実行している場合のみ使用できます。FWSM をマルチコンテキスト モードで実行している場合、アクティブ / アクティブ フェールオーバーまたはアクティブ / スタンバイ フェールオーバーのいずれの設定も可能です。

アップストリーム ルータを使用して負荷分散を行っている場合は、アクティブ / アクティブ フェールオーバーを使用します。負荷分散を行わない場合は、アクティブ / アクティブ フェールオーバーまたはアクティブ / スタンバイ フェールオーバーのいずれかを使用します。

表 13-3 で、各フェールオーバー タイプの設定でサポートされる一部の機能を比較します。

表 13-3　フェールオーバーの設定でサポートされる機能

機能	アクティブ/アクティブ	アクティブ/スタンバイ
シングルコンテキスト モード	不可	可
マルチコンテキスト モード	可	可
負荷分散ネットワーク コンフィギュレーション	可	不可
装置のフェールオーバー	可	可
コンテキスト グループのフェールオーバー	可	不可
個別コンテキストのフェールオーバー	不可	不可

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

FWSM は、標準フェールオーバーとステートフル フェールオーバーの 2 つのタイプのフェールオーバーをサポートします。ここは、次の内容について説明します。

標準フェールオーバー

フェールオーバーが発生すると、アクティブな接続はすべて切断されます。新しいアクティブ ユニットが接続を引き継ぐときに、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の場合、アクティブ ユニットは各接続ステート情報をスタンバイ ユニットに渡し続けます。フェールオーバー発生後は、新しいアクティブ ユニットで同じ接続情報を使用できます。同じ通信セッションを保持するために、サポート対象のエンドユーザ アプリケーションを再接続する必要はありません。

スタンバイ ユニットに渡されるステート情報には、次のデータが含まれます。

- NAT 変換テーブル
- TCP 接続ステート
- UDP 接続ステート
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（透過ファイアウォール モードで実行している場合）
- HTTP 接続ステート（HTTP の複製がイネーブルになっている場合）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース

ステートフル フェールオーバーがイネーブルの場合、次の情報はスタンバイ ユニットには渡されません。

- HTTP 接続テーブル（HTTP の複製がイネーブルの場合を除く）
- ユーザ認証（uauth）テーブル
- ルーティング テーブル

（注） Cisco IP SoftPhone セッション中にフェールオーバーが発生した場合、通話セッション ステート情報はスタンバイ ユニットに複製されるため、通話はアクティブのままになります。通話が中断されると、IP SoftPhone クライアントは CallManager との接続を失います。これは、スタンバイ ユニットに CTIQBE ハングアップ メッセージに関するセッション情報がないためです。IP SoftPhone クライアントは一定時間内に CallManager から応答を受信しない場合、CallManager を到達不能とみなして自らを登録解除します。

フェールオーバーのヘルス モニタ

FWSM は、各装置について、全体の動作状態とインターフェイスの動作状態をモニタします。FWSM が各装置の状態を判別するために実行するテストの詳細については、次の項目を参照してください。

- 装置のヘルス モニタ（p.13-18）
- インターフェイスのモニタ（p.13-19）

装置のヘルス モニタ

FWSM は、フェールオーバー リンクをモニタすることによって、他方の装置の状態を判別します。一方の装置がフェールオーバー リンク上で hello メッセージを受信しない場合、その装置はフェールオーバー インターフェイスを含めたすべてのインターフェイスに ARP 要求を送信します。FWSM はユーザによって設定可能な回数だけ、再試行します。FWSM の動作は、他方の装置からの応答状態によって異なります。具体的には、次のように動作します。

- FWSM がいずれかのインターフェイスから応答を受信した場合、フェールオーバーは実行されません。
- FWSM がどのインターフェイスからも応答を受信しない場合、スタンバイ ユニットがアクティブ モードに切り替わり、他方の装置は障害装置としてマークされます。
- FWSM がフェールオーバー リンク上でのみ応答を受信しない場合には、フェールオーバーは実行されません。フェールオーバー リンクは障害としてマークされます。フェールオーバー リンクがダウンしていると、スタンバイ ユニットへのフェールオーバーを実行できないので、フェールオーバー リンクはできるだけ早く回復させる必要があります。

（注）　障害がないと判断された装置が、障害状態から回復しない場合は、**failover reset** コマンドを入力してステートをリセットできます。ただし、フェールオーバーの条件が存続している場合には、装置は再び障害状態になります。

インターフェイスのモニタ

コンテキスト全体で最大 250 のインターフェイスをモニタできます。1 つのコンテキストが共有インターフェイスをモニタするように設定できます（インターフェイスが共有されているため、全コンテキストがモニタされるため）。

装置がモニタ対象のインターフェイス上で hello メッセージを受信しない場合、次のテストを実行します。

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の正常な動作が確認されると、FWSM はネットワークのテストを実行します。ネットワークのテストは、ネットワーク トラフィックを生成して、障害のある装置（両方の場合もあり）を判別することが目的です。各テストの開始時に、各装置はインターフェイスの受信パケット カウントをクリアします。テストが完了すると、各装置はトラフィックを受信しているかどうかを確認します。受信していれば、インターフェイスは正常であるとみなされます。一方の装置がテスト用トラフィックを受信し、他方の装置が受信していない場合、トラフィックを受信していない装置に障害があると判断されます。どちらの装置もトラフィックを受信していない場合には、次のテストが実行されます。
2. ネットワーク動作のテスト — ネットワークの受信動作のテストです。装置は、最大 5 秒間、すべての受信パケットをカウントします。この間にパケットを受信すれば、インターフェイスは正常であるとみなされ、テストは終了します。トラフィックを受信しなかった場合、ARP テストが実行されます。
3. ARP テスト — 装置の ARP キャッシュから、最新の 2 つのエントリが読み取られます。1 つのエントリごとに、装置はこれらの宛先に ARP 要求を送信し、ネットワーク トラフィックを流すことを試みます。各要求の送信後、装置は最大 5 秒間、すべての受信トラフィックをカウントします。トラフィックを受信すれば、インターフェイスは正常であるとみなされます。トラフィックを受信しなかった場合、次の宛先に ARP 要求が送信されます。最後のエントリまで、まったくトラフィックを受信しなかった場合には、ping テストが実行されます。
4. ブロードキャスト ping テスト — このテストでは、ブロードキャスト ping 要求が送信されます。その後、装置は、最大 5 秒間すべての受信パケットをカウントします。この間にパケットを受信すれば、インターフェイスは正常であるとみなされ、テストは終了します。

特定のインターフェイスがすべてのネットワークのテストに失敗し、他方の装置では同じインターフェイスが正常にトラフィックを伝送している場合、テストに失敗したインターフェイスに障害があるとみなされます。障害のあるインターフェイス数がスレッシュホールドの値に達した場合、フェールオーバーが実行されます。他方の装置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、これらのインターフェイスはいずれも「不明（Unknown）」ステートとなり、フェールオーバー用の障害インターフェイスとしてはカウントされません。

インターフェイスは、トラフィックを受信すれば、再び正常な状態に戻ります。障害インターフェイス数がスレッシュホールド未満になると、障害状態の FWSM はスタンバイ モードに戻ります。

（注）　障害がないと判断された装置が、障害状態から回復しない場合には、**failover reset** コマンドを入力してステートをリセットできます。ただし、フェールオーバーの条件が存続している場合には、装置は再び障害状態になります。

フェールオーバーの設定

ここでは、フェールオーバーを設定する手順について説明します。内容は次のとおりです。

アクティブ / スタンバイ フェールオーバーの使用

ここでは、アクティブ / スタンバイ フェールオーバーの設定手順を説明します。内容は次のとおりです。

一般的なフェールオーバーの設定例については、「フェールオーバーの設定例」（p.B-20）を参照してください。

前提条件

作業を開始する前に、次のことを確認します。

- 両装置とも正規のライセンスを持っていること。
- プライマリ ユニットがシングルコンテキスト モードの場合、セカンダリ ユニットもシングルコンテキスト モードで、さらにプライマリ ユニットと同じファイアウォール モードでなければなりません。
- プライマリ ユニットがマルチコンテキスト モードの場合、セカンダリ ユニットもマルチコンテキスト モードでなければなりません。セカンダリ ユニット上でセキュリティ コンテキストのファイアウォール モードを設定する必要はありません。フェールオーバー リンクおよびステート リンクはシステム コンテキスト内に常時設定されているためです。セカンダリ ユニットは、プライマリ ユニットからセキュリティ コンテキスト コンフィギュレーションを取得します。

（注）　**mode** コマンドはセカンダリ ユニットには複製されません。

アクティブ / スタンバイ フェールオーバーの設定

ここでは、アクティブ / スタンバイ フェールオーバーの設定方法について説明します。プライマリ ユニットから実行コンフィギュレーションを取得する前にフェールオーバー リンクを認識するように、セカンダリ ユニットを設定する必要があります。

このセクションでは、次の内容について説明します。

プライマリ ユニットの設定

次の手順に従って、アクティブ / スタンバイ フェールオーバー設定内のプライマリ ユニットを設定します。これらの手順は、プライマリ ユニットでフェールオーバーをイネーブルにするための最小限の設定です。マルチコンテキスト モードでは、特に明記されていないかぎり、すべての手順をシステム実行スペースで行います。

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

ステップ 1　各インターフェイス（ルーテッド モード）および各管理アドレス（透過モード）のアクティブ IP アドレスとスタンバイ IP アドレスをまだ設定していない場合は、設定します。スタンバイ IP アドレスは、現在スタンバイ ユニットである FWSM で使用されます。この IP アドレスは、アクティブ IP アドレスと同じサブネットに属している必要があります。

（注）　フェールオーバー リンクまたはステート リンク（ステートフル フェールオーバーを使用する予定の場合）の IP アドレスは設定しないでください。

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

（注）　マルチコンテキスト モードでは、各コンテキスト内でインターフェイス アドレスを設定する必要があります。**changeto context** コマンドを使用して、コンテキスト間の切り替えを行います。コマンド プロンプトが `hostname/context(config-if)#` に変わります。*context* は現在のコンテキストの名前です。

ステップ 2　装置をプライマリ ユニットとして指定します。

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

ステップ 3　フェールオーバー インターフェイスを定義します。

a. フェールオーバー インターフェイスとして使用するインターフェイスを指定します。

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

if_name 引数は、名前を *vlan* 引数で指定されたインターフェイスに割り当てます。

b. 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。

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

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に属している必要があります。スタンバイ アドレスのサブネット マスクを特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、フェールオーバー実行後も変更されません。プライマリ ユニットは常にフェールオーバー リンクのアクティブ IP アドレスを使用し、セカンダリ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 4　（任意）ステートフル フェールオーバーをイネーブルにするには、ステート リンクを設定します。ステート リンクは未使用のインターフェイス上で設定する必要があります。

a. ステート リンクとして使用するインターフェイスを指定します。

```
hostname(config)# failover link if_name [vlan vlan]
```

（注） ステート リンクがフェールオーバー リンクを使用する場合、*if_name* 引数を指定するだけで済みます。

if_name 引数は、論理名を *vlan* 引数で指定されたインターフェイスに割り当てます。このインターフェイスはほかの目的には使用しないでください（フェールオーバー リンクを除く［任意］）。

b. アクティブ IP アドレスとスタンバイ IP アドレスをステート リンクに割り当てます。

（注） ステート リンクがフェールオーバー リンクを使用する場合、この手順は省略します。すでにフェールオーバー リンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定しているためです。

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

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に属している必要があります。スタンバイ アドレスのサブネット マスクを特定する必要はありません。

ステート リンクの IP アドレスおよび MAC アドレスは、フェールオーバー実行後も変更されません。プライマリ ユニットは常にアクティブ IP アドレスを使用し、スタンバイ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 5　次のコマンドを入力して、トンネル インターフェイスのモニタをイネーブルにします。

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

FWSM 上（すべてのコンテキスト全体）でモニタできるインターフェイスの最大数は、250 です。

（注） マルチコンテキスト モードでは、各コンテキスト内でインターフェイス モニタリングを設定する必要があります。**changeto context** コマンドを使用して、コンテキスト間の切り替えを行います。コマンド プロンプトが `hostname/context(config)#` に変わります。*context* は現在のコンテキストの名前です。

ステップ 6　フェールオーバーをイネーブルにします。

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

ステップ 7　設定を保存します。

```
hostname(config)# write memory
```

（注）　マルチコンテキスト モードでは、システム実行スペースに **write memory all** コマンドを入力してすべてのコンテキストのコンフィギュレーションを保存します。

セカンダリ ユニットの設定

セカンダリ ユニットに必要なのは、フェールオーバー インターフェイスの設定だけです。プライマリ ユニットと初回の通信を開始するには、セカンダリ ユニットにこれらのコマンドが必要です。プライマリ ユニットからセカンダリ ユニットに設定が送信されたあと、2 つの設定で唯一異なるのが、各装置をプライマリまたはセカンダリとして識別する **failover lan unit** コマンドです。

マルチコンテキスト モードでは、特に明記されていないかぎり、すべての手順をシステム実行スペースで行います。

セカンダリ ユニットを設定するには、次の手順を実行します。

ステップ 1　フェールオーバー インターフェイスを定義します。プライマリ ユニットに使用した設定と同じ設定を使用します。

a. フェールオーバー インターフェイスとして使用するインターフェイスを指定します。

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

if_name 引数は、名前を *vlan* 引数で指定されたインターフェイスに割り当てます。

b. 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。

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

（注）　このコマンドは、フェールオーバー インターフェイスの設定時にプライマリ ユニットに入力したとおりに入力します。

ステップ 2　（任意）この装置をセカンダリ ユニットとして指定します。

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

（注）　すでに設定してある場合を除き、デフォルトでは装置はセカンダリ ユニットとして指定されるため、この手順は任意となります。

ステップ 3　フェールオーバーをイネーブルにします。

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

フェールオーバーをイネーブルにすると、アクティブ ユニットからスタンバイ ユニットに、実行メモリ内の設定が送信されます。設定を同期化すると、アクティブ ユニットのコンソールに「Beginning Configuration replication: Sending to mate」および「End Configuration Replication to mate」というメッセージが表示されます。

ステップ 4　実行コンフィギュレーションで複製が完了したら、設定をフラッシュ メモリに保存します。

```
hostname(config)# write memory
```

任意のアクティブ / スタンバイ フェールオーバーの設定

フェールオーバーの初期設定時またはフェールオーバーの設定後に、次の任意のアクティブ / スタンバイ フェールオーバー設定を指定することができます。特に指定のないかぎり、コマンドはアクティブ ユニットに入力します。

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.13-25）
- インターフェイスおよび装置のポーリング間隔の設定（p.13-25）
- フェールオーバー条件の設定（p.13-25）

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

ステート情報の複製に HTTP 接続を含めるには、HTTP の複製をイネーブルにする必要があります。HTTP 接続は一般に存続時間が短く、HTTP クライアントは失敗した接続を再試行することが多いため、HTTP 接続は複製されたステート情報には自動的には含められません。

ステートフル フェールオーバーがイネーブルである場合、次のコマンドをグローバル コンフィギュレーション モードで入力して、HTTP ステートの複製をイネーブルにします。

```
hostname(config)# failover replication http
```

インターフェイスおよび装置のポーリング間隔の設定

FWSM は、フェールオーバーについて、装置とインターフェイスの両方をヘルス モニタします。装置とインターフェイスをヘルス モニタする際、hello メッセージの間隔を設定できます。ポーリング間隔を短くすると、インターフェイスまたは装置の障害をより速く検出できますが、システム リソースの消費量が大きくなります。

インターフェイスのポーリング間隔を変更するには、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。

```
hostname(config)# failover polltime interface seconds
```

装置のポーリング間隔を変更するには、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。

```
hostname(config)# failover polltime seconds
```

フェールオーバー条件の設定

デフォルトでは、モニタ対象インターフェイスの障害が 50% になるとフェールオーバーが実行されます。フェールオーバーを実行するために必要な、モニタ対象の障害インターフェイスの数または割合を指定できます。

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。

```
hostname(config)# failover interface-policy num[%]
```

インターフェイスの数を指定する場合、*num* 引数に 1 ～ 250 を指定できます。インターフェイスの割合を指定する場合、*num* 引数に 1 ～ 100 を指定できます。

アクティブ / アクティブ フェールオーバーの使用

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。

内容は次のとおりです。

一般的なフェールオーバーの設定例については、「フェールオーバーの設定例」（p.B-20）を参照してください。

前提条件

作業を開始する前に、次のことを確認します。

- 両装置とも正規のライセンスを持っていること。
- 両装置ともマルチコンテキスト モードであること。セカンダリ ユニット上でセキュリティ コンテキストのファイアウォール モードを設定する必要はありません。フェールオーバー リンクおよびステート リンクはシステム コンテキスト内に常時設定されているためです。セカンダリ ユニットは、プライマリ ユニットからセキュリティ コンテキスト コンフィギュレーションを取得します。

（注）　**mode** コマンドはセカンダリ ユニットには複製されません。

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。プライマリ ユニットから実行コンフィギュレーションを取得する前にフェールオーバー リンクを認識するように、セカンダリ ユニットを設定する必要があります。

ここでは、次の内容について説明します。

プライマリ ユニットの設定

アクティブ / アクティブ フェールオーバーの設定内のプライマリ ユニットを設定するには、次の手順に従います。

ステップ 1　システム実行スペースで基本フェールオーバー パラメータを設定します。

a. 装置をプライマリ ユニットとして指定します。

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

b. フェールオーバー リンクを指定します。

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

if_name 引数は、*vlan* 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。このインターフェイスはその他目的では使用しないでください（ステート リンクを除く［任意］）。

c. フェールオーバー リンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定します。

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

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に属している必要があります。スタンバイ IP アドレスのサブネット マスクを特定する必要はありません。フェールオーバー リンクの IP アドレスは、フェールオーバー実行後も変更されません。プライマリ ユニットは常にアクティブ IP アドレスを使用し、スタンバイ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 2　（任意）ステートフル フェールオーバーをイネーブルにするには、ステート リンクを設定します。ステート リンクは未使用のインターフェイス上で設定する必要があります。

a. ステート リンクとして使用するインターフェイスを指定します。

```
hostname(config)# failover link if_name [vlan vlan]
```

if_name 引数は、*vlan* 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。このインターフェイスはその他の目的では使用しないでください（フェールオーバー リンクを除く［任意］）。

（注）　ステート リンクがフェールオーバー リンクを使用する場合、*if_name* 引数を指定するだけで済みます。

b. アクティブ IP アドレスとスタンバイ IP アドレスをステート リンクに割り当てます。

（注）　ステート リンクがフェールオーバー リンクを使用する場合、この手順は省略します。すでにフェールオーバー リンクのアクティブ IP アドレスとスタンバイ IP アドレスを指定しているためです。

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

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に属している必要があります。スタンバイ アドレスのサブネット マスクを特定する必要はありません。

ステート リンクの IP アドレスは、フェールオーバー実行後も変更されません。プライマリ ユニットは常にアクティブ IP アドレスを使用し、スタンバイ ユニットは常にスタンバイ IP アドレスを使用します。

ステップ 3　フェールオーバー グループを設定します。最大 2 つのフェールオーバー グループを作成できます。指定されたフェールオーバー グループが存在しない場合、**failover group** コマンドはこのグループを作成し、フェールオーバー グループ コンフィギュレーション モードを開始します。

各フェールオーバー グループについて、**primary** または **secondary** コマンドを使用して、そのフェールオーバー グループでのプライマリ / セカンダリのプリファレンスを指定する必要があります。両方のフェールオーバー グループに同じプリファレンスを割り当ててもかまいません。負荷分散設定の場合は、各フェールオーバー グループに異なるプリファレンスを割り当てる必要があります。

次に、フェールオーバー グループ 1 にプライマリ プリファレンスを割り当て、フェールオーバー グループ 2 にセカンダリ プリファレンスを割り当てる例を示します。

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

ステップ 4　コンテキスト コンフィギュレーション モードで **join-failover-group** コマンドを使用して、各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。

割り当てられていないコンテキストは自動的にフェールオーバー グループ 1 に割り当てられます。管理コンテキストは常にフェールオーバー グループ 1 のメンバーです。

次のコマンドを入力して、各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。

```
hostname(config)# context context_name
hostname(config-context)# join-failover-group {1 | 2}
```

ステップ 5　フェールオーバーをイネーブルにします。

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

ステップ 6　インターフェイス上のモニタリングをイネーブルにするには、コンテキストに切り替えて、次のコマンドを入力します。

```
hostname(config)# changeto context context_name
hostname(config)# monitor-interface interface_name
```

FWSM 上（すべてのコンテキスト全体）でモニタできるインターフェイスの最大数は、250 です。

セカンダリ ユニットの設定

フェールオーバー リンクを認識するには、セカンダリ ユニットを設定する必要があります。これにより、セカンダリ ユニットはプライマリ ユニットと通信し、プライマリ ユニットから実行コンフィギュレーションを取得することができます。

アクティブ / アクティブ フェールオーバー コンフィギュレーションのセカンダリ ユニットを設定するには、次の手順に従います。

ステップ 1　フェールオーバー インターフェイスを定義します。プライマリ ユニットに使用した設定と同じ設定を使用します。

a. フェールオーバー インターフェイスとして使用するインターフェイスを指定します。

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

if_name 引数は、*vlan* 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。

b. 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。

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

（注） このコマンドは、フェールオーバー インターフェイスの設定時にプライマリ ユニットに入力したとおりに入力します。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットに属している必要があります。スタンバイ アドレスのサブネット マスクを特定する必要はありません。

ステップ 2　（任意）この装置をセカンダリ ユニットとして指定します。

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

（注） すでに設定してある場合を除き、デフォルトでは装置はセカンダリ ユニットとして指定されるため、この手順は任意となります。

ステップ 3　フェールオーバーをイネーブルにします。

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

フェールオーバーをイネーブルにすると、アクティブ ユニットからスタンバイ ユニットに、実行メモリ内の設定が送信されます。設定を同期化すると、アクティブ ユニットのコンソールに「Beginning Configuration replication: Sending to mate」および「End Configuration Replication to mate」というメッセージが表示されます。

ステップ 4　実行コンフィギュレーションで複製が完了したら、次のコマンドを入力して、設定をフラッシュ メモリに保存します。

```
hostname(config)# write memory
```

ステップ 5　必要に応じて、プライマリ ユニット上でアクティブな任意のフェールオーバー グループを、強制的にセカンダリ ユニット上でアクティブ ステートにすることができます。フェールオーバー グループをセカンダリ ユニット上で強制的にアクティブにするには、プライマリ ユニットのシステム実行スペースで次のコマンドを入力します。

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

group_id 引数には、セカンダリ ユニット上でアクティブにするグループを指定します。

アクティブ / アクティブ フェールオーバーの任意の設定

フェールオーバーの初期設定時またはフェールオーバーの設定後に、次の任意のアクティブ / アクティブ フェールオーバー設定を指定することができます。特に指定のないかぎり、コマンドは、アクティブ ステートのフェールオーバー グループ 1 を持つ装置に入力する必要があります。

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 グループ プリエンプションの設定

フェールオーバー グループにプライマリまたはセカンダリの優先度を割り当てることで、両方の装置を同時に起動したときに、フェールオーバー グループがアクティブになる装置を指定します。ただし、一方の装置を他方より先に起動すると、その装置上で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。もう一方の装置がオンラインになると、この装置を優先するフェールオーバー グループはすべて、手動で強制しないか、フェールオーバーが発生するか、**preempt** コマンドでフェールオーバー グループが設定されない限り、この装置上ではアクティブにはなりません。**preempt** コマンドにより、指定した装置が使用可能になると、フェールオーバー グループはこの装置上で自動的にアクティブになります。

次のコマンドを入力して、指定したフェールオーバー グループにプリエンプションを設定します。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# preempt [delay]
```

任意で *delay* 値を入力することができます。この値は、フェールオーバー グループが指定した装置上で自動的にアクティブになるまで、現在の装置上でアクティブのままでいる秒数を指定します。

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

ステート情報に HTTP 接続を含めるには、HTTP の複製をイネーブルにする必要があります。HTTP 接続は一般に存続時間が短く、HTTP クライアントは失敗した接続を再試行することが多いため、HTTP 接続は複製されたステート情報には自動的には含められません。**replication http** コマンドを使用して、ステートフル フェールオーバーがイネーブルの場合に、フェールオーバー グループに HTTP ステート情報を複製させることができます。

フェールオーバー グループによる HTTP ステートの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。このコマンドは、コマンドが設定されたフェールオーバー グループにのみ影響します。両方のフェールオーバー グループによる HTTP ステートの複製をイネーブルにするには、各グループにこのコマンドを入力します。このコマンドは、システム実行スペースに入力する必要があります。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# replication http
```

インターフェイスおよび装置のポーリング間隔の設定

フェールオーバー グループのインターフェイスをヘルス モニタする際、hello メッセージの間隔を設定できます。インターフェイスのポーリング間隔を短くすると、フェールオーバーを速く実行できますが、システム リソースの消費量が大きくなります。

デフォルトのインターフェイス ポーリング間隔を変更するには、次のコマンドを入力します。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# polltime interface seconds
```

装置のポーリング間隔は、ピア装置の動作状態を判断するために、フェールオーバー リンクで 送信する hello メッセージの間隔を指定します。装置のポーリング間隔を短くすると、装置の障害をより速く検出できますが、システム リソースの消費量が大きくなります。装置のポーリング間隔を変更するには、グローバル コンフィギュレーション モードでシステム実行スペースに次のコマンドを入力します。

```
hostname(config)# failover polltime seconds
```

フェールオーバー条件の設定

デフォルトでは、モニタ対象インターフェイスの障害が 50% になるとフェールオーバーが実行されます。フェールオーバーを実行するために必要な、モニタ対象の障害インターフェイスの数または割合を指定できます。フェールオーバー条件は、フェールオーバー グループ単位で指定します。

指定したフェールオーバー グループのデフォルトのフェールオーバー条件を変更するには、次のコマンドを入力します。

```
hostname(config)# failover group {1 | 2}
hostname(config-fover-group)# interface-policy num[%]
```

インターフェイスの数を指定する場合、*num* 引数に 1 ～ 250 を指定できます。インターフェイスの割合を指定する場合、*num* 引数に 1 ～ 100 を指定できます。

フェールオーバー通信の認証 / 暗号化の設定

共有秘密鍵または 16 進数鍵を指定することで、フェールオーバー ピア間の通信の暗号化および認証を実行できます。

注意　フェールオーバー キーで通信をセキュリティ保護している場合を除き、フェールオーバーおよびステートフル フェールオーバー リンク間の情報はすべてクリア テキストで送信されます。FWSM を使用して VPN トンネルを終端する場合、この情報には任意のユーザ名、パスワードおよびトンネルの確立に使用した事前共有鍵が含まれます。この機密データをクリア テキストで伝送すると、重大なセキュリティ リスクが生じる可能性があります。FWSM を使用して VPN トンネルを終端している場合、フェールオーバー通信をフェールオーバー キーでセキュリティ保護することを推奨します。

アクティブ / スタンバイ フェールオーバー ペアのアクティブ ユニット上、またはアクティブ / アクティブ フェールオーバー ペア内のアクティブ ステートのフェールオーバー グループ 1 を持つ装置上で、次のコマンドを入力します。

```
hostname(config)# failover key {secret | hex key}
```

secret 引数は、暗号化鍵の生成に使用する共有秘密鍵を指定します。値には、数字、文字、句読点の任意の組み合わせの 1 ～ 63 文字を指定できます。***hex key*** 引数は、16 進数の暗号化鍵を指定します。このキーには 32 ビットの 16 進文字（0 ～ 9、a ～ f）を指定する必要があります。

（注）　フェールオーバー キーが既存のフェールオーバーの設定のために、ピア装置にクリア テキストで複製されないようにするには、アクティブ ユニット（または、アクティブ ステートのフェールオーバー グループ 1 を持つ装置のシステム実行スペースで）でフェールオーバーをディセーブルにして、両方の装置にフェールオーバー キーを入力してから、フェールオーバーを再びイネーブルにします。フェールオーバーが再びイネーブルになると、フェールオーバー通信はフェールオーバー キーで暗号化されます。

新しいフェールオーバーの設定では、**failover key** コマンドが初期フェールオーバー ペアの設定の一部でなければなりません。

フェールオーバーの設定の確認

ここでは、フェールオーバーの設定を確認する手順について説明します。内容は次のとおりです。

- フェールオーバー ステータスの表示（p.13-32）
- モニタ対象インターフェイスの表示（p.13-40）
- フェールオーバーの設定の表示（p.13-41）
- フェールオーバー機能のテスト（p.13-41）

フェールオーバー ステータスの表示

ここでは、フェールオーバー ステータスを確認する方法について説明します。各装置で **show failover** コマンドを入力してフェールオーバー ステータスを確認できます。表示される情報は、アクティブ / スタンバイ フェールオーバーまたはアクティブ / アクティブ フェールオーバーのどちらを使用しているかによって異なります。

ここでは、次の内容について説明します。

- アクティブ / スタンバイのフェールオーバー ステータスの表示（p.13-33）
- アクティブ / アクティブのフェールオーバー ステータスの表示（p.13-37）

アクティブ / スタンバイのフェールオーバー ステータスの表示

次に、アクティブ / スタンバイ フェールオーバーの **show failover** コマンドの出力例を示します。表 13-4 で、表示される情報について説明します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan 100(up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                Interface inside (10.130.9.3): Normal
                Interface outside (10.132.9.3): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                Interface inside (10.130.9.4): Normal
                Interface outside (10.132.9.4): Normal

Stateful Failover Logical Update Statistics
        Link : fover Vlan100 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         1950       0          1733       0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

マルチコンテキスト モードでは、セキュリティ コンテキストで **show failover** コマンドを使用すると、そのコンテキストのフェールオーバー情報が表示されます。この情報は、シングルコンテキスト モードでこのコマンドを使用した場合に表示される情報とほぼ同じです。装置のアクティブ / スタンバイ ステータスではなく、コンテキストのアクティブ / スタンバイ ステータスが表示されま

す。表 13-4 で、表示される情報について説明します。

```
Failover On
Last Failover at: 04:03:11 UTC Jan 4 2003
        This context: Negotiation
                Active time: 1222 (sec)
                Interface outside (192.168.5.121): Normal
                Interface inside (192.168.0.1): Normal
        Peer context: Not Detected
                Active time: 0 (sec)
                Interface outside (192.168.5.131): Normal
                Interface inside (192.168.0.11): Normal

Stateful Failover Logical Update Statistics
        Status: Configured.
        Stateful Obj    xmit       xerr       rcv        rerr
        RPC services    0          0          0          0
        TCP conn        99          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         22          0          0          0
        Xlate_Timeout   0          0          0          0
        GTP PDP         0          0          0          0
        GTP PDPMCB      0          0          0          0
```

表 13-4　show failover コマンドの出力の説明

フィールド	説明
Failover	• オン • オフ
Failover Unit	プライマリまたはセカンダリ
Failover LAN Interface	フェールオーバー リンク名を表示します。
Unit Poll frequency	ピア装置に hello メッセージを送信する間隔（秒）、およびピアの障害を宣言するまでにピア装置がフェールオーバー リンク上で hello メッセージを受信する時間（秒）を指定します。
Interface Poll frequency	*n* 秒 **failover polltime interface** コマンドで設定した秒数が表示されます。デフォルトは 15 秒です。
Interface Policy	フェールオーバーをトリガーするために必要な、障害インターフェイスの数または比率を表示します。
Monitored Interfaces	モニタ可能な最大インターフェイス数のうち、モニタ対象のインターフェイス数を表示します。
failover replication http	ステータス フェールオーバーに対して HTTP ステートの複製がイネーブルかどうかを示します。
Last Failover at	最終フェールオーバー日時を次の形式で示します。 *hh*:*mm*:*ss* **UTC** *DayName Month Day yyyy* UTC（協定世界時）は GMT（グリニッジ標準時）に相当します。
This host Other host	各ホストについて、次の情報が表示されます。
Primary または Secondary	• アクティブ • スタンバイ

表 13-4　show failover コマンドの出力の説明（続き）

フィールド	説明
Acitive time	*n*（秒） 装置がアクティブな時間。累積時間なので、スタンバイ ユニットが以前にアクティブだった場合、その時間が表示されます。
Interface *name* (*n.n.n.n*):	各インターフェイスについて、装置上で現在使用されている IP アドレスと、次のいずれかの状態が表示されます。 • Failed — インターフェイスに障害が発生しています。 • No Link — インターフェイス ライン プロトコルがダウンしています。 • Normal — インターフェイスは正常に動作しています。 • Link Down — インターフェイスは管理者によって明示的に閉じられています。 • Unknown — FWSM はこのインターフェイスのステータスを判別できません。 • Waiting — 他の装置上のネットワーク インターフェイスのモニタリングは、まだ開始されていません。
Stateful Failover Logical Update Statistics	ステートフル フェールオーバー機能の関連フィールドが表示されます。Link フィールドにインターフェイス名が示されている場合、ステートフル フェールオーバーの統計情報が表示されます。
Link	• *interface_name* — ステートフル フェールオーバー リンクに使用されているインターフェイス • Unconfigured — ステートフル フェールオーバーが使用されていません。 • up — インターフェイスは開かれて機能しています。 • down — インターフェイスは管理者によって明示的に閉じられているか、物理的にダウンしています。 • failed — インターフェイスに障害が発生しているため、ステートフル データは転送されません。
Stateful Obj	各フィールド タイプに、次の統計情報が表示されます。これらは 2 つの装置間で送信されたステート情報パケット数のカウンタです。必ずしも装置を通過するアクティブな接続が表示されるわけではありません。 • xmit — 他方の装置への送信パケット数 • xerr — 他方の装置へのパケット送信中に発生したエラー数 • rcv — 受信パケット数 • rerr — 他方の装置からのパケット受信中に発生したエラー数
General	すべてのステートフル オブジェクトの合計
sys cmd	論理更新システム コマンド：LOGIN、Stay Alive など
up time	アクティブ ユニットからスタンバイ ユニットに渡される動作時間
RPC services	リモート プロシージャ コールの接続情報
TCP conn	TCP 接続情報
UDP conn	動的な UDP 接続情報
ARP tbl	動的な ARP テーブル情報

表 13-4　show failover コマンドの出力の説明（続き）

フィールド	説明
L2BRIDGE tbl	レイヤ 2 ブリッジ テーブル情報（透過ファイアウォール モード限定）
Xlate_Timeout	接続変換のタイムアウト情報を示します
VPN IKE upd	IKE 接続情報
VPN IPSEC upd	IPSec 接続情報
VPN CTCP upd	cTCP トンネル接続情報
VPN SDI upd	SDI AAA 接続情報
VPN DHCP upd	トンネル経由の DHCP 接続情報
GTP PDP	GTP PDP 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
GTP PDPMCB	GTP PDPMCB 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
Logical Update Queue Information	各フィールド タイプに、次の統計情報が表示されます。 • Cur — 現在のパケット数 • Max — 最大パケット数 • Total — 合計パケット数
Recv Q	受信キューのステータス
Xmit Q	送信キューのステータス

アクティブ / アクティブのフェールオーバー ステータスの表示

次に、アクティブ / アクティブ フェールオーバーの **show failover** コマンドの出力例を示します。表 13-5 で、表示される情報について説明します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan 100 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : fover Vlan100 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         1973       0          1895       0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

次に、アクティブ / アクティブ フェールオーバーの **show failover group** コマンドの出力例を示します。表示される情報は、**show failover** コマンドの情報とほぼ同じですが、指定したグループに限定されます。表 13-5 で、表示される情報について説明します。

```
hostname# show failover group 1

  Last Failover at: 04:09:59 UTC Jan 4 2005

  This host:    Secondary
                State:          Active
                Active time:    186 (sec)

                admin Interface outside (192.168.5.121): Normal
                admin Interface inside (192.168.0.1): Normal


  Other host:   Primary
                State:          Standby
                Active time:    0 (sec)

                admin Interface outside (192.168.5.131): Normal
                admin Interface inside (192.168.0.11): Normal

  Stateful Failover Logical Update Statistics
        Status: Configured.
        RPC services    0          0          0          0
        TCP conn        33         0          0          0
        UDP conn        0          0          0          0
        ARP tbl         12         0          0          0
        Xlate_Timeout   0          0          0          0
        GTP PDP         0          0          0          0
        GTP PDPMCB      0          0          0          0
```

表 13-5　show failover コマンドの出力の説明

フィールド	説明
Failover	• オン • オフ
Failover Unit	プライマリまたはセカンダリ
Failover LAN Interface	フェールオーバー リンク名を表示します。
Unit Poll frequency	ピア装置に hello メッセージを送信する間隔（秒）、およびピアの障害を宣言するまでにピア装置がフェールオーバー リンク上で hello メッセージを受信する時間（秒）を指定します。
Interface Poll frequency	*n* 秒 **failover polltime interface** コマンドで設定した秒数が表示されます。デフォルトは 15 秒です。
Interface Policy	フェールオーバーをトリガーするために必要な、障害インターフェイスの数または比率を表示します。
Monitored Interfaces	モニタ可能な最大インターフェイス数のうち、モニタ対象のインターフェイス数を表示します。
Group 1 Last Failover at : Group 2 Last Failover at :	各グループの最終フェールオーバー日時を次の形式で示します。 *hh*:*mm*:*ss* **UTC** *DayName Month Day yyyy* UTC（協定世界時）は GMT（グリニッジ標準時）に相当します。
This host : Other host :	各ホストについて、次の情報が表示されます。

表 13-5　show failover コマンドの出力の説明（続き）

フィールド	説明
Role	プライマリまたはセカンダリ
System State	• アクティブまたはスタンバイ準備完了 • アクティブ時間（秒）
Group 1 State Group 2 State	• アクティブまたはスタンバイ準備完了 • アクティブ時間（秒）
context Interface *name* (*n.n.n.n*)	各インターフェイスについて、装置上で現在使用されている IP アドレスと、次のいずれかの状態が表示されます。 • Failed — インターフェイスに障害が発生しています。 • No Link — インターフェイス ライン プロトコルがダウンしています。 • Normal — インターフェイスは正常に動作しています。 • Link Down — インターフェイスは管理者によって明示的に閉じられています。 • Unknown — FWSM はこのインターフェイスのステータスを判別できません。 • Waiting — 他の装置上のネットワーク インターフェイスのモニタリングは、まだ開始されていません。
Stateful Failover Logical Update Statistics	ステートフル フェールオーバー機能の関連フィールドが表示されます。Link フィールドにインターフェイス名が示されている場合、ステートフル フェールオーバーの統計情報が表示されます。
Link	• *interface_name* — ステートフル フェールオーバー リンクに使用されているインターフェイス。 • Unconfigured — ステートフル フェールオーバーが使用されていません。 • up — インターフェイスは開かれて機能しています。 • down — インターフェイスは管理者によって明示的に閉じられているか、物理的にダウンしています。 • failed — インターフェイスに障害が発生しているため、ステートフル データは転送されません。
Stateful Obj	各フィールド タイプに、次の統計情報が表示されます。これらは 2 つの装置間で送信されたステート情報パケット数のカウンタです。必ずしも装置を通過するアクティブな接続が表示されるわけではありません。 • xmit — 他方の装置への送信パケット数 • xerr — 他方の装置へのパケット送信中に発生したエラー数 • rcv — 受信パケット数 • rerr — 他方の装置からのパケット受信中に発生したエラー数
General	すべてのステートフル オブジェクトの合計
sys cmd	論理更新システム コマンド：LOGIN、Stay Alive など
up time	アクティブ ユニットからスタンバイ ユニットに渡される動作時間
RPC services	リモート プロシージャ コールの接続情報
TCP conn	TCP 接続情報
UDP conn	動的な UDP 接続情報

表 13-5　show failover コマンドの出力の説明（続き）

フィールド	説明
ARP tbl	動的な ARP テーブル情報
L2BRIDGE tbl	レイヤ 2 ブリッジ テーブル情報（透過ファイアウォール モード限定）
Xlate_Timeout	接続変換のタイムアウト情報を示します。
VPN IKE upd	IKE 接続情報
VPN IPSEC upd	IPSec 接続情報
VPN CTCP upd	cTCP トンネル接続情報
VPN SDI upd	SDI AAA 接続情報
VPN DHCP upd	トンネル経由の DHCP 接続情報
GTP PDP	GTP PDP 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
GTP PDPMCB	GTP PDPMCB 更新情報。この情報は、GTP 検査がイネーブルの場合にのみ表示されます。
Logical Update Queue Information	各フィールド タイプに、次の統計情報が表示されます。 • Cur — 現在のパケット数 • Max — 最大パケット数 • Total — 合計パケット数
Recv Q	受信キューのステータス
Xmit Q	送信キューのステータス

モニタ対象インターフェイスの表示

モニタ対象インターフェイスのステータスを表示するには、次のコマンドを入力します。シングル コンテキスト モードでは、このコマンドをグローバル コンフィギュレーション モードで入力します。マルチコンテキスト モードでは、このコマンドをコンテキスト内で入力します。

```
primary/context(config)# show monitor-interface
```

次に例を示します。

```
hostname/context(config)# show monitor-interface
        This host: Primary - Active
                Interface outside (192.168.1.2): Normal
                Interface inside (10.1.1.91): Normal
        Other host: Secondary - Standby
                Interface outside (192.168.1.3): Normal
                Interface inside (10.1.1.100): Normal
```

フェールオーバーの設定の表示

実行コンフィギュレーションのフェールオーバー コマンドを表示するには、次のコマンドを入力します。

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

すべてのフェールオーバー コマンドが表示されます。マルチコンテキスト モードで実行する装置では、このコマンドをシステム実行スペースで入力します。**show running-config all failover** コマンドを入力すると、実行コンフィギュレーションのフェールオーバー コマンドが表示され、デフォルト値を変更していないコマンドが含められます。

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手順は、次のとおりです。

ステップ 1　異なるインターフェイスのホスト間で FTP（他の方法でも可）を使用してファイルを送信し、アクティブ ユニットまたはフェールオーバー グループが正常にトラフィックを転送しているかどうかをテストします。

ステップ 2　次のコマンドを入力して、スタンバイ ユニットへの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 フェールオーバーの場合、アクティブ ユニットに次のコマンドを入力します。

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

- アクティブ / アクティブ フェールオーバーの場合、ホストに接続しているインターフェイスを含むフェールオーバー グループがアクティブになっている装置に次のコマンドを入力します。

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

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

ステップ 4　テストに失敗した場合は、**show failover** コマンドを入力して、フェールオーバーのステータスを確認します。

ステップ 5　終了後、次のコマンドを入力して、装置またはフェールオーバー グループをアクティブ ステータスに戻すことができます。

- アクティブ / スタンバイ フェールオーバーの場合、アクティブ ユニットに次のコマンドを入力します。

  ```
  hostname(config)# failover active
  ```

- アクティブ / アクティブ フェールオーバーの場合、ホストに接続しているインターフェイスを含むフェールオーバー グループがアクティブな装置に次のコマンドを入力します

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

フェールオーバーの制御とモニタ

ここでは、フェールオーバーを制御およびモニタする方法について説明します。内容は次のとおりです。

フェールオーバーの強制実行

スタンバイ ユニットまたはスタンバイ フェールオーバー グループを強制的にアクティブにするには、次のいずれかのコマンドを入力します。

- アクティブ / スタンバイ フェールオーバーの場合：

  次のコマンドをスタンバイ ユニットに入力します。

  ```
  hostname# failover active
  ```

  または、次のコマンドをアクティブ ユニットに入力します。

  ```
  hostname# no failover active
  ```

- アクティブ / アクティブ フェールオーバーの場合：

  次のコマンドを、スタンバイ ステートのフェールオーバー グループを持つ装置のシステム実行スペースに入力します。

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

  または、次のコマンドを、アクティブ ステートのフェールオーバー グループを持つ装置のシステム実行スペースに入力します。

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

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

  ```
  hostname# failover active
  ```

フェールオーバーのディセーブル化

フェールオーバーをディセーブルにするには、次のコマンドを入力します。

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

アクティブ / スタンバイ ペアのフェールオーバーをディセーブルにすると、各装置のアクティブ ステートとスタンバイ ステートが、再起動するまで保持されます。たとえば、スタンバイ ユニットはスタンバイ モードのままなので、両方の装置によるトラフィック転送は開始されません。（フェールオーバーをディセーブルにした状態で）スタンバイ ユニットを強制的にアクティブにする場合は、「フェールオーバーの強制実行」（p.13-42）を参照してください。

アクティブ / アクティブ ペアのフェールオーバーをディセーブルにすると、どの装置を優先するように設定されたかに関係なく、現在アクティブなすべての装置上で、フェールオーバー グループはアクティブ ステートのままになります。no failover コマンドは、システム実行スペースに入力する必要があります。

設定の同期化のディセーブル化

FWSM を複雑な設定にアップグレードすると、管理アプリケーションの接続が失われることがあります。このような場合には、スタンバイ FWSM に、不完全なコンフィギュレーション ファイルが適用されます。設定の自動同期化をディセーブルに設定しておけば、スタンバイ FWSM に不完全な設定が適用されるのを防止できます。ソフトウェア イメージをアップグレードする場合、またはアクティブ FWSM の設定を変更する場合には、スタンバイ FWSM に完全なコンフィギュレーション ファイルが同期化されるように、設定の同期化をディセーブルにする必要があります。設定が完了したことを確認したあと、設定の同期化を再びイネーブルに設定します。

設定の同期化をディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# failover suspend-config-sync
```

設定の同期化を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

障害が発生した装置またはフェールオーバー グループの復元

障害が発生した装置を障害前のステートに復元するには、次のコマンドを入力します。

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

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 グループを障害前のステートに復元するには、次のコマンドを入力します。

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

障害が発生した装置またはグループを障害前のステートに復元しても、自動的にアクティブにはなりません。復元された装置またはグループは、フェールオーバー（強制実行または自然実行）によってアクティブにされるまで、スタンバイ ステートのままになります。**preempt** コマンドで設定されたフェールオーバー グループは例外です。前にアクティブであった場合、フェールオーバー グループが **preempt** コマンドで設定されていて、優先装置上で障害が発生したのであれば、このフェールオーバー グループはアクティブになります。

フェールオーバー動作のモニタ

フェールオーバーが実行されると、両方の FWSM からシステム メッセージが送信されます。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.13-43）
- デバッグ メッセージ（p.13-44）
- SNMP（p.13-44）

フェールオーバー システム メッセージ

FWSM は、クリティカル状態を示すプライオリティ レベル 2 で、フェールオーバー関連のシステム メッセージを多数生成します。これらのメッセージを表示するには、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*』を参照し、ロギングをイネーブルにして、システム メッセージの説明を参照してください。

（注）　スイッチオーバーの過程では、フェールオーバーが論理的にシャット ダウンされて、インターフェイスが開かれ、システム ログ メッセージ 411001 および 411002 が生成されます。これが標準動作です。

デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

（注）　デバッグの出力は CPU 処理でハイ プライオリティが割り当てられているため、システム パフォーマンスに大きな影響を及ぼす可能性があります。このため、**debug fover** コマンドは、特定の問題のトラブルシューティングまたは Cisco TAC によるトラブルシューティング セッションを行う場合にのみ使用してください。

SNMP

フェールオーバーに関する SNMP の Syslog トラップを受信するには、SNMP エージェントから SNMP 管理ステーションに SNMP トラップを送信するように設定し、Syslog ホストを定義し、Cisco syslog MIB を SNMP 管理ステーションにコンパイルします。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **snmp-server** コマンドと **logging** コマンドを参照してください。