CHAPTER 14

ハイ アベイラビリティ

ここでは、次の内容について説明します。

フェールオーバーについて

[Failover] ペインには、セキュリティ アプライアンスでフェールオーバーを構成するための各種設定が含まれています。ただし、[Failover] ペインは、マルチ モードであるかシングル モードであるかによって変化し、マルチ モードのときは使用しているセキュリティ コンテキストに基づいて変化します。

フェールオーバーを使用すると、2 台のセキュリティ アプライアンスを設定して、一方に障害が発生した場合にもう一方がその動作を引き継ぐようにすることができます。ペアになっているセキュリティ アプライアンスを使用することで、オペレータの介入を必要としない高可用性を実現できます。セキュリティ アプライアンスは、専用のフェールオーバー リンクでフェールオーバー情報を伝達します。このフェールオーバー リンクには、LAN ベースの接続、または PIX セキュリティ アプライアンス プラットフォームでは専用シリアル フェールオーバー ケーブルのいずれかを使用できます。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。

- フェールオーバーの状態（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
- コンフィギュレーションの複製

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。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

セキュリティ アプライアンスは、Active/Standby と Active/Active の 2 つのフェールオーバー タイプをサポートします。また、フェールオーバーは、ステートフルにもステートレスにもできます。フェールオーバーのタイプの詳細については、次の項目を参照してください。

- 「Active/Standby フェールオーバー」（P.14-2）
- 「アクティブ/アクティブ フェールオーバー」（P.14-2）
- 「ステートレス（標準）フェールオーバー」（P.14-3）
- 「ステートフル フェールオーバー」（P.14-3）

Active/Standby フェールオーバー

Active/Standby コンフィギュレーションでは、アクティブ セキュリティ アプライアンスが、フェールオーバー ペアを通過するすべてのネットワーク トラフィックを処理します。スタンバイ セキュリティ アプライアンスは、アクティブ セキュリティ アプライアンスに障害が発生するまでネットワーク トラフィックを処理しません。アクティブ セキュリティ アプライアンスのコンフィギュレーションが変更されると、その都度コンフィギュレーション情報がフェールオーバー リンク経由でスタンバイ セキュリティ アプライアンスに送信されます。

フェールオーバーが実行されると、スタンバイ セキュリティ アプライアンスはアクティブ装置になります。前のアクティブ装置の IP アドレスと MAC アドレスが使用されます。IP アドレスまたは MAC アドレスの変更はネットワーク上の他のデバイスには認識されないため、ARP エントリがネットワーク上で変更されたりタイムアウトしたりすることはありません。

Active/Standby フェールオーバーは、シングル モードでもマルチ モードでも、セキュリティ アプライアンスで使用できます。

アクティブ/アクティブ フェールオーバー

Active/Active フェールオーバー コンフィギュレーションでは、両方のセキュリティ アプライアンスがネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードのセキュリティ アプライアンスでのみ使用できます。

セキュリティ アプライアンスで Active/Active フェールオーバーをイネーブルにするには、フェールオーバー グループを作成する必要があります。フェールオーバー グループを作成しないでフェールオーバーをイネーブルにすると、アクティブ/スタンバイ フェールオーバーがイネーブルになります。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。セキュリティ アプライアンスには、2 つのフェールオーバー グループを作成できます。フェールオーバー グループ 1 がアクティブ状態になる装置にフェールオーバー グループを作成する必要があります。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。

アクティブ/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 ペアの各装置には、プライマリまたはセカンダリのどちらかが指定されます。アクティブ/スタンバイ フェールオーバーとは異なり、両方の装置が同時に起動した場合にどちらの装置がアクティブになるかは指示されていません。設定の各フェールオーバー グループには、プライマリまたはセカンダリ ロール プリファレンスが設定されます。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、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。ペアの一方の装置にアクティブ状態の両方のフェールオーバー グループを含めて、もう一方の装置にスタンバイ状態のフェールオーバー グループを含めることができます。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 プリファレンスを割り当てて、それぞれを別の装置上でアクティブにすることでデバイスにトラフィックを分散させます。

初期設定同期は、一方または両方の装置が起動すると実行されます。この同期は、次のように実行されます。

- 両方の装置が同時に起動した場合、設定はプライマリ装置からセカンダリ装置に同期されます。
- 一方の装置がすでにアクティブであるときに、もう一方の装置が起動した場合は、起動した装置が、すでにアクティブな装置から設定を受信します。

両方の装置が動作中になった後で、次のように、コマンドが一方の装置からもう一方の装置に複製されます。

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

（注） あるコンテキストがある装置でアクティブ状態と見なされるのは、そのコンテキストが属するフェールオーバー グループがその装置上でアクティブ状態である場合です。

- システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から、フェールオーバー グループ 1 がスタンバイ状態である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 がアクティブ状態である装置から、フェールオーバー グループ 1 がスタンバイ状態である装置に複製されます。

コマンドの複製の実行に適切な装置上でコマンドを入力しなかった場合は、設定が非同期になります。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバー グループをアクティブと指定した場合にフェールオーバー グループ 1 で障害が発生すると、フェールオーバー グループ 2 はプライマリ装置でアクティブのままですが、フェールオーバー グループ 1 はセカンダリ装置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構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

ステートレス（標準）フェールオーバー

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

ステートフル フェールオーバー

（注） ステートフル フェールオーバーは、ASA 5505 シリーズ適応型セキュリティ アプライアンスではサポートされていません。

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場合、フェールオーバー ペアのアクティブ装置は接続ごとのステート情報をスタンバイ装置に常に渡しています。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

（注）　ステートおよび LAN 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。

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 リンクがすべてのステート情報をスタンバイ装置に渡すように設定する必要があります。シリアル フェールオーバー インターフェイス（PIX セキュリティ アプライアンス プラットフォームだけで使用可）ではなく、LAN フェールオーバー接続を使用している場合、フェールオーバー リンクとしてステート リンクに同じインターフェイスを使用できます。ただし、スタンバイ装置にステート情報を渡すときは、専用のインターフェイスを使用することをお勧めします。

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、次の情報がスタンバイ装置に渡されます。

- NAT 変換テーブル
- タイムアウト接続などの TCP 接続テーブル（HTTP を除く）
- HTTP 接続状態（HTTP 複製がイネーブルの場合）
- H.323、SIP、および MGCP UDP メディア接続
- システム クロック
- ISAKMP および IPSec SA テーブル

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、次の情報はスタンバイ装置にコピーされません。

- 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
- ARP テーブル
- ルーティング テーブル

High Availability and Scalability Wizard を使用したフェールオーバーの設定

High Availability and Scalability Wizard では、Active/Active フェールオーバー コンフィギュレーション、および Active/Standby フェールオーバー コンフィギュレーション、または VPN Cluster Load Balancing コンフィギュレーションを作成するプロセスの手順が示されます。

High Availability and Scalability Wizard の使用の詳細については、次の項目を参照してください。

- 「High Availability and Scalability Wizard へのアクセスと使用」（P.14-5）
- 「High Availability and Scalability Wizard を使用した Active/Active フェールオーバーの設定」（P.14-5）
- 「High Availability and Scalability Wizard を使用した Active/Standby フェールオーバーの設定」（P.14-6）
- 「High Availability and Scalability Wizard を使用した VPN ロード バランシングの設定」（P.14-7）
- 「High Availability and Scalability Wizard のフィールド情報」（P.14-7）

High Availability and Scalability Wizard へのアクセスと使用

High Availability and Scalability Wizard を開くには、ASDM メニューバーで [Wizards] > [High Availability and Scalability Wizard] の順に選択します。ウィザードの最初の画面が表示されます。

ウィザードの次の画面に移動するには、[Next] ボタンをクリックします。次の画面に移動する前に、各画面の必須フィールドへの入力を完了する必要があります。

ウィザードの前の画面に戻るには、[Back] ボタンをクリックします。ウィザードの後の画面に入力した情報に前の画面で行った変更が反映されていない場合でも、ウィザードを進んでいけば入力した情報は画面上に残っています。情報を再度入力する必要はありません。

[Cancel] をクリックすると、変更内容を保存せずにいつでもウィザードを終了できます。

ウィザードの最後にコンフィギュレーションをセキュリティ アプライアンスに送信するには、[Finish] をクリックします。

High Availability and Scalability Wizard を使用した Active/Active フェールオーバーの設定

次の手順では、High Availability and Scalability Wizard を使用した Active/Active フェールオーバーの設定の概要を説明します。手順の各ステップは、ウィザード画面に対応しています。各ステップを実行したら、次のステップに進む前に [Next] をクリックします（ただし、最終ステップを除きます）。また、各ステップには、実行に必要な追加情報への参照も含まれています。

ステップ 1　[Choose the type of failover configuration] 画面で [Configure Active/Active] フェールオーバーを選択します。

この画面の詳細については、「Choose the Type of Failover Configuration」（P.14-8）を参照してください。

ステップ 2　[Check Failover Peer Connectivity and Compatibility] 画面にフェールオーバー ピアの IP アドレスを入力します。[Test Compatibility] をクリックします。すべての互換性テストに合格するまで、次の画面に進むことはできません。

この画面の詳細については、「Check Failover Peer Connectivity and Compatibility」（P.14-9）を参照してください。

ステップ 3　セキュリティ アプライアンスまたはフェールオーバー ピアがシングル コンテキスト モードである場合、[Change Device to Multiple Mode] 画面でマルチ コンテキスト モードに変更します。セキュリティ アプライアンスをマルチ コンテキスト モードに変更すると、リブートされます。リブートが完了すると、ASDM は自動的にセキュリティ アプライアンスとの通信を再確立します。

この画面の詳細については、「Change Device to Multiple Mode」（P.14-9）を参照してください。

ステップ 4　（PIX 500 シリーズ セキュリティ アプライアンスのみ）[Select Failover Communication Media] 画面で、ケーブルベース フェールオーバーまたは LAN ベース フェールオーバーを選択します。

この画面の詳細については、「Select Failover Communication Media」（P.14-10）を参照してください。

ステップ 5　[Context Configuration] 画面で、フェールオーバー グループにセキュリティ コンテキストを割り当てます。この画面では、コンテキストを追加または削除できます。

この画面の詳細については、「Security Context Configuration」（P.14-10）を参照してください。

ステップ 6　[Failover Link Configuration] 画面でフェールオーバー リンクを定義します。

この画面の詳細については、「Failover Link Configuration」（P.14-11）を参照してください。

ステップ 7　（ASA 5505 セキュリティ アプライアンスでは使用不可）[State Link Configuration] 画面でステートフル フェールオーバー リンクを定義します。

この画面の詳細については、「State Link Configuration」（P.14-12）を参照してください。

ステップ 8　[Standby Address Configuration] 画面で、スタンバイ アドレスをセキュリティ アプライアンス インターフェイスに追加します。

この画面の詳細については、「Standby Address Configuration」（P.14-12）を参照してください。

ステップ 9　[Summary] 画面でコンフィギュレーションを確認します。必要に応じて [Back] ボタンを使用し、前の画面に戻って変更します。

この画面の詳細については、「Summary」（P.14-15）を参照してください。

ステップ 10　[Finish] をクリックします。

フェールオーバー コンフィギュレーションがセキュリティ アプライアンスとフェールオーバー ピアに送信されます。

High Availability and Scalability Wizard を使用した Active/Standby フェールオーバーの設定

次の手順では、High Availability and Scalability Wizard を使用した Active/Standby フェールオーバーの設定の概要を説明します。手順の各ステップは、ウィザード画面に対応しています。各ステップを実行したら、次のステップに進む前に [Next] をクリックします（ただし、最終ステップを除きます）。また、各ステップには、実行に必要な追加情報への参照も含まれています。

ステップ 1　[Choose the type of failover configuration] 画面で [Configure Active/Standby] フェールオーバーを選択します。[Next] をクリックします。

この画面の詳細については、「Choose the Type of Failover Configuration」（P.14-8）を参照してください。

ステップ 2　[Check Failover Peer Connectivity and Compatibility] 画面にフェールオーバー ピアの IP アドレスを入力します。[Test Compatibility] をクリックします。すべての互換性テストに合格するまで、次の画面に進むことはできません。

この画面の詳細については、「Check Failover Peer Connectivity and Compatibility」（P.14-9）を参照してください。

ステップ 3　（PIX 500 シリーズ セキュリティ アプライアンスのみ）[Select Failover Communication Media] 画面で、ケーブルベース フェールオーバーまたは LAN ベース フェールオーバーを選択します。

この画面の詳細については、「Select Failover Communication Media」（P.14-10）を参照してください。

ステップ 4　[Failover Link Configuration] 画面でフェールオーバー リンクを定義します。

この画面の詳細については、「Failover Link Configuration」（P.14-11）を参照してください。

ステップ 5　（ASA 5505 セキュリティ アプライアンスでは使用不可）[State Link Configuration] 画面でステートフル フェールオーバー リンクを定義します。

この画面の詳細については、「State Link Configuration」（P.14-12）を参照してください。

ステップ 6　[Standby Address Configuration] 画面で、スタンバイ アドレスをセキュリティ アプライアンス インターフェイスに追加します。

この画面の詳細については、「Standby Address Configuration」（P.14-12）を参照してください。

ステップ 7　[Summary] 画面でコンフィギュレーションを確認します。必要に応じて [Back] ボタンを使用し、前の画面に戻って変更します。

この画面の詳細については、「Summary」（P.14-15）を参照してください。

ステップ 8　[Finish] をクリックします。

フェールオーバー コンフィギュレーションがセキュリティ アプライアンスとフェールオーバー ピアに送信されます。

High Availability and Scalability Wizard を使用した VPN ロード バランシングの設定

次の手順では、High Availability and Scalability Wizard を使用した VPN クラスタ ロード バランシングの設定の概要を説明します。手順の各ステップは、ウィザード画面に対応しています。各ステップを実行したら、次のステップに進む前に [Next] をクリックします（ただし、最終ステップを除きます）。また、各ステップには、実行に必要な追加情報への参照も含まれています。

ステップ 1　[Choose the type of failover configuration] 画面で [Configure VPN Cluster Load Balancing] フェールオーバーを選択します。

この画面の詳細については、「Choose the Type of Failover Configuration」（P.14-8）を参照してください。

ステップ 2　[VPN Cluster Load Balancing Configuration] 画面で VPN ロード バランシング設定を実行します。

この画面の詳細については、「VPN クラスタ ロード バランシングの設定」（P.14-13）を参照してください。

ステップ 3　[Summary] 画面でコンフィギュレーションを確認します。必要に応じて [Back] ボタンを使用し、前の画面に戻って変更します。

この画面の詳細については、「Summary」（P.14-15）を参照してください。

ステップ 4　[Finish] をクリックします。

フェールオーバー コンフィギュレーションがセキュリティ アプライアンスとフェールオーバー ピアに送信されます。

High Availability and Scalability Wizard のフィールド情報

High Availability and Scalability Wizard では、次のダイアログが使用できます。ウィザードの実行中に、すべてのダイアログボックスが表示されるわけではありません。表示される各ダイアログボックスは、設定するフェールオーバーのタイプと、その設定を行っているハードウェア プラットフォームによって異なります。

Choose the Type of Failover Configuration

[Choose the Type of Failover Configuration] 画面では、設定するフェールオーバーのタイプを選択できます。

フィールド

[Choose the Type of Failover Configuration] には、次の情報フィールドが表示されます。これらの情報フィールドは、セキュリティ アプライアンスのフェールオーバー機能の決定に役立ちます。

- [Hardware Model]：（*表示専用*）セキュリティ アプライアンスのモデル番号を表示します。
- [No. of Interfaces]：（*表示専用*）セキュリティ アプライアンスで使用可能なインターフェイスの数を表示します。
- [No. of Modules]：（*表示専用*）セキュリティ アプライアンスに取り付けられているモジュールの数を表示します。
- [Software Version]：（*表示専用*）セキュリティ アプライアンス上のプラットフォーム ソフトウェアのバージョンを表示します。
- [Failover License]：（*表示専用*）デバイスにインストールされたフェールオーバー ライセンスのタイプを表示します。フェールオーバーを設定するには、アップグレードしたライセンスの購入が必要になる場合があります。
- [Firewall Mode]：（*表示専用*）ファイアウォール モード（ルーテッドまたはトランスペアレント）およびコンテキスト モード（シングルまたはマルチ）を表示します。

設定しているフェールオーバー コンフィギュレーションのタイプを選択します。

- [Configure Active/Active Failover]：セキュリティ アプライアンスに Active/Active フェールオーバーを設定します。
- [Configure Active/Standby Failover]：セキュリティ アプライアンスに Active/Standby フェールオーバーを設定します。
- [Configure VPN Cluster Load Balancing]：セキュリティ アプライアンスがクラスタの一部として VPN ロード バランシングに参加するように設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Check Failover Peer Connectivity and Compatibility

[Check Failover Peer Connectivity and Compatibility] 画面では、選択したフェールオーバー ピアが到達可能で、現在の装置と互換性があることを確認できます。接続および互換性テストが失敗した場合、ウィザードの先に進む前に、問題を修正する必要があります。

フィールド

- [Peer IP Address]：ピア装置の IP アドレスを入力します。このアドレスはフェールオーバー リンクのアドレスでなくても構いませんが、ASDM アクセスがイネーブルになっているインターフェイスでなければなりません。
- [Test Compatibility]：このボタンをクリックして、次の接続テストおよび互換性テストを実行します。
  - ASDM からピア装置への接続テスト
  - ファイアウォール デバイスからピア ファイアウォール デバイスへの接続テスト
  - ハードウェア互換性テスト
  - ソフトウェア バージョンの互換性
  - フェールオーバー ライセンスの互換性
  - ファイアウォール モードの互換性

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Change Device to Multiple Mode

[Change Device to Multiple Mode] ダイアログボックスは、Active/Active フェールオーバー コンフィギュレーションでだけ表示されます。Active/Active フェールオーバーでは、セキュリティ アプライアンスがマルチ コンテキスト モードになっている必要があります。このダイアログボックスでは、シングルコンテキスト モードのセキュリティ アプライアンスをマルチ コンテキスト モードに変換します。

シングルコンテキスト モードからマルチ コンテキスト モードに変換するとき、セキュリティ アプライアンスは、現在実行しているコンフィギュレーションからシステム コンフィギュレーションと管理コンテキストを作成します。管理コンテキスト コンフィギュレーションは、admin.cfg というファイルに格納されます。変換プロセスでは、以前のスタートアップ コンフィギュレーションが保存されないので、スタートアップ コンフィギュレーションが実行中のコンフィギュレーションと異なる場合は、異なる部分が失われます。

セキュリティ アプライアンスをシングルコンテキスト モードからマルチ コンテキスト モードに変換すると、セキュリティ アプライアンスはリブートされます。ただし、High Availability and Scalability Wizard では、新規作成された管理コンテキストとの接続が復元され、このダイアログボックスで [Devices Status] フィールドのステータスが報告されます。

次に進む前に、現在のセキュリティ アプライアンスとピア セキュリティ アプライアンスの両方をマルチ コンテキスト モードに変換する必要があります。

フィールド

- [Change *device* To Multiple Context]：セキュリティ アプライアンスをマルチ コンテキスト モードに変更します。*device* の部分には、セキュリティ アプライアンスのホスト名が入ります。
- [Change *device* (peer) To Multiple Context]：ピア装置をマルチ コンテキスト モードに変更します。*device* の部分には、セキュリティ アプライアンスのホスト名が入ります。
- [Device Status]：（*表示専用*）マルチ コンテキスト モードへの変換中にセキュリティ アプライアンスのステータスが表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Select Failover Communication Media

[Select Failover Communication Media] は、PIX 500 シリーズ セキュリティ アプライアンスだけに表示されます。この画面では、フェールオーバー リンクにフェールオーバー ケーブルを使用するか、LAN ベースの接続を使用するかを選択できます。

フィールド

- [Use Failover Cable]：フェールオーバー通信に専用フェールオーバー ケーブルを使用するには、このオプションを選択します。
- [Use LAN-based connection]：フェールオーバー通信にネットワーク接続を使用するには、このオプションを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Security Context Configuration

[Security Context Configuration] 画面は、Active/Active コンフィギュレーションにだけ表示されます。[Security Context Configuration] 画面では、セキュリティ コンテキストをフェールオーバー グループに割り当てることができます。この画面では、デバイスで現在設定されているセキュリティ コンテキストが表示され、必要に応じて新しいセキュリティ コンテキストを追加したり、既存のコンテキストを削除したりできます。この画面でセキュリティ コンテキストを作成できますが、作成したコンテキ

ストにインターフェイスを割り当てたり、作成したコンテキストの他のプロパティを設定したりできません。コンテキスト プロパティを設定し、インターフェイスをコンテキストに割り当てるには、[System] > [Security Contexts] ペインを使用する必要があります。

フィールド

- [Name]：セキュリティ コンテキストの名前を表示します。名前を変更するには、名前をクリックして新しい名前を入力します。
- [Failover Group]：コンテキストの割り当て先であるフェールオーバー グループを表示します。セキュリティ コンテキストのフェールオーバー グループを変更するには、フェールオーバー グループをクリックし、ドロップダウン リストから新しいフェールオーバー グループ番号を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Failover Link Configuration

[Failover Link Configuration] 画面は、LAN ベースのフェールオーバーを設定している場合にだけ表示されます。ケーブルベースのフェールオーバーを PIX 500 シリーズ セキュリティ アプライアンスで設定している場合は表示されません。

フィールド

- [LAN Interface]：フェールオーバー通信に使用するインターフェイスをドロップダウン リストから選択します。
- [Logical Name]：インターフェイスの名前を入力します。
- [Active IP]：アクティブ状態のフェールオーバー グループ 1 がある装置上のフェールオーバー リンクに使用する IP アドレスを入力します。
- [Standby IP]：スタンバイ状態のフェールオーバー グループ 1 がある装置上のフェールオーバー リンクに使用する IP アドレスを入力します。
- [Subnet Mask]：アクティブ IP アドレスまたはスタンバイ IP アドレスのサブネット マスクを入力または選択します。
- [Secret Key]：（任意）フェールオーバー通信の暗号化に使用するキーを入力します。このフィールドを空白のままにした場合、コンフィギュレーション内のパスワードまたはキーをはじめ、コマンド複製中に送信されるフェールオーバー通信は、クリア テキストになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

State Link Configuration

[State Link Configuration] 画面は、ASA 5505 プラットフォーム上で実行している ASDM のウィザードには表示されません。

[State Link Configuration] 画面では、ステートフル フェールオーバーをイネーブルにして、ステートフル フェールオーバー リンク プロパティを設定できます。

フィールド

- [Use the LAN link as the State Link] : LAN ベースのフェールオーバー リンクでステート情報を渡すには、このオプションを選択します。このオプションは、ケーブルベースのフェールオーバー向けに設定された PIX 500 シリーズ セキュリティ アプライアンスでは使用できません。
- [Disable Stateful Failover] : ステートフル フェールオーバーをディセーブルにするには、このオプションを選択します。
- [Configure another interface for Stateful failover] : 未使用のインターフェイスをステートフル フェールオーバー インターフェイスとして設定するには、このオプションを選択します。
  - [State Interface] : ステートフル フェールオーバー通信に使用するインターフェイスをドロップダウン リストから選択します。
  - [Logical Name] : ステートフル フェールオーバー インターフェイスの名前を入力します。
  - [Active IP] : アクティブ状態のフェールオーバー グループ 1 がある装置上のステートフル フェールオーバー リンクの IP アドレスを入力します。
  - [Standby IP] : スタンバイ状態のフェールオーバー グループ 1 がある装置上のステートフル フェールオーバー リンクの IP アドレスを入力します。
  - [Subnet Mask] : アクティブ IP アドレスまたはスタンバイ IP アドレスのサブネット マスクを入力または選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Standby Address Configuration

[Standby Address Configuration] 画面を使用して、セキュリティ アプライアンス上のインターフェイスにスタンバイ アドレスを割り当てます。

フィールド

- [Device/Interface]：（Active/Standby フェールオーバー）フェールオーバー装置上で設定されたインターフェイスを表示します。デバイス名の横のプラス記号（+）をクリックすると、そのデバイス上のインターフェイスが表示されます。デバイス名の横のマイナス記号（-）をクリックすると、そのデバイス上のインターフェイスが非表示になります。
- [Device/Group/Context/Interface]：（Active/Active フェールオーバー）フェールオーバー装置上で設定されたインターフェイスを表示します。インターフェイスはコンテキストでグループ化され、コンテキストはフェールオーバー グループでグループ化されます。デバイス、フェールオーバー グループ、コンテキスト名の横のプラス記号（+）をクリックすると、リストが展開されます。デバイス、フェールオーバー グループ、コンテキスト名の横のマイナス記号（-）をクリックすると、リストが折りたたまれます。
- [Active IP]：このフィールドをダブルクリックして、アクティブ IP アドレスを編集または追加できます。また、このフィールドに移動すると、ピア装置上の対応するインターフェイスが [Standby IP] フィールドに表示されます。
- [Standby IP]：このフィールドをダブルクリックすると、スタンバイ IP アドレスを編集または追加できます。また、このフィールドに移動すると、ピア装置上の対応するインターフェイスが [Active IP] フィールドに表示されます。
- [Is Monitored]：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するには、このチェックボックスをオンにします。チェックボックスをオフにすると、ヘルス モニタリングがディセーブルになります。デフォルトでは、物理インターフェイスのヘルス モニタリングはイネーブルに、仮想インターフェイスのヘルス モニタリングはディセーブルになっています。
- [ASR Group]：非同期グループ ID をドロップダウン リストから選択します。この設定は、物理インターフェイスにだけ使用可能です。仮想インターフェイスの場合、このフィールドには「None」が表示されます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

VPN クラスタ ロード バランシングの設定

リモートクライアント コンフィギュレーションで、複数のセキュリティ アプライアンスを同じネットワークに接続してリモート セッションを処理している場合、これらのデバイスでセッション負荷を分担するように設定できます。この機能は、*ロード バランシング*と呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。これによって、システム リソースを効率的に利用でき、パフォーマンスと可用性が向上します。

[VPN Cluster Load Balancing Configuration] 画面を使用して、このデバイスがロード バランシング クラスタに参加するのに必要なパラメータを設定します。

（注） VPN ロード バランシングを使用するには、Plus ライセンスの ASA モデル 5510、あるいは ASA モデル 5520 または 5540 が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロード バランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

ロード バランシングをイネーブルにするには、次の手順を実行します。

- 共通仮想クラスタ IP アドレス、UDP ポート（必要に応じて）、およびクラスタの IPSec 共有秘密情報を確立することによりロード バランシング クラスタを設定する。これらの値は、クラスタ内のすべてのデバイスで同一です。
- デバイスでロード バランシングをイネーブルにし、デバイス固有のプロパティを定義することにより、参加デバイスを設定する。これらの値はデバイスによって異なります。

（注） ロード バランシングは、Cisco VPN Client（リリース 3.0 以降）、Cisco VPN 3002 Hardware Client（リリース 3.5 以降）、または Easy VPN クライアントとして動作している ASA 5505 で開始されたリモート セッションだけで有効です。LAN 間接続を含む他のすべてのクライアントは、ロード バランシングがイネーブルなセキュリティ アプライアンスに接続できますが、ロード バランシングには参加できません。

ロード バランシングを実装するには、同じプライベート LAN 間ネットワーク上の複数のデバイスを、論理的に*仮想クラスタ*としてグループ化します。

フィールド

- [Cluster IP Address]：仮想クラスタ全体を表す単一の IP アドレスを指定します。仮想クラスタ内のすべてのセキュリティ アプライアンスが共有するパブリック サブネットのアドレス範囲内で、IP アドレスを選択します。
- [Cluster UDP Port]：このデバイスが参加する仮想クラスタの UDP ポートを指定します。デフォルト値は 9023 です。別のアプリケーションでこのポートが使用されている場合は、ロードバランシングに使用する UDP の宛先ポート番号を入力します。
- [Enable IPSec Encryption]：IPSec 暗号化をイネーブルまたはディセーブルにします。このチェックボックスをオンにする場合は、共有秘密情報を指定し、確認する必要もあります。仮想クラスタ内のセキュリティ アプライアンスは、IPSec を使用して LAN-to-LAN トンネルを介して通信します。デバイス間で通信されるすべてのロード バランシング情報が暗号化されるようにするには、このチェックボックスをオンにします。

（注） 暗号化を使用する場合、事前にロードバランシング内部インターフェイスを設定しておく必要があります。そのインターフェイスがロードバランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

クラスタの暗号化を設定したときにロードバランシング内部インターフェイスがイネーブルに設定されたが、仮想クラスタへのデバイス参加を設定する前にディセーブルにされた場合は、[Participate in Load Balancing Cluster] チェックボックスをオンにしたときにエラー メッセージが表示され、そのクラスタに対して暗号化はイネーブルになりません。

  - [Shared Secret Key]：IPSec 暗号化をイネーブルにするときに、IPSec ピア間の共有秘密情報を指定します。ボックスに入力する値は、連続するアスタリスク文字として表示されます。

- [Priority Of This Device]：クラスタ内でこのデバイスに割り当てられる優先順位を指定します。指定できる範囲は 1 ～ 10 です。プライオリティは、起動時または既存のマスターで障害が発生したときに、このデバイスが仮想クラスタ マスターになる可能性を表します。優先順位を高く設定すれば（10 など）、このデバイスが仮想クラスタ マスターになる可能性が高くなります。

（注） 仮想クラスタ内のデバイスを異なるタイミングで起動した場合、最初に起動したデバイスが、仮想クラスタ マスターの役割を果たすと想定されます。仮想クラスタにはマスターが必要であるため、起動したときに仮想クラスタ内の各デバイスはチェックを行い、クラスタに仮想マスターがあることを確認します。仮想マスターがない場合、そのデバイスがマスターの役割を果たします。後で起動し、クラスタに追加されたデバイスは、セカンダリ デバイスになります。仮想クラスタ内のすべてのデバイスが同時に起動されたときは、最高の優先順位が設定されたデバイスが仮想クラスタ マスターになります。仮想クラスタ内の複数のデバイスが同時に起動され、いずれも最高の優先順位が設定されている場合、最も低い IP アドレスを持つデバイスが仮想クラスタ マスターになります。

- [Public Interface Of This Device]：このデバイスのパブリック インターフェイスの名前または IP アドレスを指定します。
- [Private Interface Of This Device]：このデバイスのプライベート インターフェイスの名前または IP アドレスを指定します。
- [Send FQDN to client]：このチェックボックスをオンにすると、VPN クラスタ マスターが VPN クライアント接続をクラスタ デバイスにリダイレクトするときに、外部 IP アドレスの代わりにクラスタ デバイスのホスト名とドメイン名を使用して完全修飾ドメイン名が送信されるようになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

Summary

[Summary] 画面では、これまでのウィザード パネルで実行した設定手順の結果が表示されます。

フィールド

設定内容は画面中央に表示されます。設定を確認して [Finish] をクリックすると、設定内容がデバイスに送信されます。フェールオーバーを設定している場合、設定内容はフェールオーバー ピアにも送信されます。設定を変更する必要がある場合は、[Back] をクリックして変更する必要のある画面まで戻ります。変更を行ったら [Next] をクリックして [Summary] 画面まで戻ります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

[Failover] ペインのフィールド情報

フェールオーバー ペインに表示される内容は、現在のモード（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）およびシステム実行スペースにいるか、セキュリティ コンテキスト内に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。

- [Failover]（シングル モード）
- [Failover]（マルチ モード、セキュリティ コンテキスト）
- [Failover]（マルチ モード、システム）

[Failover]（シングル モード）

[Failover] ペインには、シングルコンテキスト モードで Active/Standby フェールオーバーを設定できるタブが含まれています。フェールオーバーの詳細については、フェールオーバーについてを参照してください。[Failover] ペインの各タブでの設定の詳細については、次の情報を参照してください。ルーテッド ファイアウォール モードであるか、トランスペアレント ファイアウォール モードであるかによって、[Interfaces] タブが変わります。

- [Failover]: [Setup]
- [Failover]: [Interfaces]（ルーテッド ファイアウォール モード）
- [Failover]: [Interfaces]（トランスペアレント ファイアウォール モード）
- [Failover]: [Criteria]
- [Failover]: [MAC Addresses]

[Failover]: [Setup]

このタブを使用して、セキュリティ アプライアンスでフェールオーバーをイネーブルにします。また、ステートフル フェールオーバーを使用している場合、このタブではフェールオーバー リンクおよびステート リンクも指定できます。

一般的なフェールオーバーの設定方法の詳細については、「フェールオーバーについて」を参照してください。

フィールド

- [Enable Failover]：このチェックボックスをオンにすると、フェールオーバーがイネーブルになり、スタンバイ セキュリティ アプライアンスを設定できます。

（注）　フェールオーバー インターフェイスの速度と二重通信の設定は、フェールオーバーがイネーブルになっても変わりません。フェールオーバー インターフェイスの速度や二重通信の設定を変更するには、フェールオーバーをイネーブルにする前に、[Configuration] > [Interfaces] ペインで設定しておく必要があります。

ASDM では、フェールオーバーをイネーブルにするときに、ピア装置を設定するかどうかを確認するダイアログボックスが表示されます。このダイアログボックスは、Preferred Role 設定、または PIX セキュリティ アプライアンス プラットフォームでの（シリアル ケーブル フェールオーバーではなく）Enable LAN 設定が変更されたときにも表示されます。

  - [Peer IP Address]：ASDM が接続されているピア装置での IP アドレスを入力します。このフィールドは、[Do you want to configure the failover peer firewall] ダイアログボックスに表示されます。

- [Use 32 hexadecimal character key]：[Shared Key] ボックスに 16 進数値の暗号キーを入力するには、このチェックボックスをオンにします。[Shared Key] ボックスに英数字の共有秘密情報を入力する場合は、このチェックボックスをオフにします。
- [Shared Key]：フェールオーバー共有秘密情報またはフェールオーバー ペア間での暗号化および認証済み通信のためのキーを指定します。

  [Use 32 hexadecimal character key] チェックボックスをオンにした場合、16 進数の暗号キーを入力してください。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。

  [Use 32 hexadecimal character key] チェックボックスをオフにした場合は、英数字の共有秘密情報を入力してください。共有秘密情報は、1 ～ 63 文字で入力できます。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。
- [Enable LAN rather than serial cable failover]:（PIX セキュリティ アプライアンス プラットフォームのみ）LAN フェールオーバーをイネーブルにするには、このチェックボックスをオンにします。フェールオーバー リンクとして専用シリアル ケーブルを使用するには、このチェックボックスをオフにします。
- [LAN Failover]：LAN フェールオーバーを設定するためのフィールドが含まれます。
  - [Interface]：フェールオーバー通信に使用するインターフェイスを指定します。フェールオーバーには専用インターフェイスが必要ですが、ステートフル フェールオーバーとインターフェイスを共有できます。

    このリストには、未設定のインターフェイスまたはサブインターフェイスだけが表示され、LAN フェールオーバー インターフェイスとして選択できます。インターフェイスを LAN フェールオーバー インターフェイスに指定すると、そのインターフェイスは [Configuration] > [Interfaces] ペインでは編集できません。
  - [Active IP]：アクティブ装置のフェールオーバー インターフェイスの IP アドレスを指定します。
  - [Subnet Mask]：プライマリ装置およびセカンダリ装置のフェールオーバー インターフェイスのマスクを指定します。
  - [Logical Name]：フェールオーバー通信に使用するインターフェイスの論理名を指定します。
  - [Standby IP]：セカンダリ装置がプライマリ装置との通信に使用する IP アドレスを指定します。
  - [Preferred Role]：このセキュリティ アプライアンスの優先の役割が、LAN フェールオーバーのプライマリ装置であるか、セカンダリ装置であるかを指定します。
- [State Failover]：ステートフル フェールオーバーの設定のためのフィールドが含まれます。

（注）　ステートフル フェールオーバーは、ASA 5505 プラットフォームでは使用できません。この領域は、ASA 5505 セキュリティ アプライアンスで実行している ASDM には表示されません。

- [Interface]：ステート通信に使用するインターフェイスを指定します。選択できるのは、未設定のインターフェイスまたはサブインターフェイス、LAN フェールオーバー インターフェイス、または [Use Named] オプションです。

（注）　LAN フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスには、2 つの個別の専用インターフェイスを使用することをお勧めします。

  未設定のインターフェイスまたはサブインターフェイスを選択した場合、そのインターフェイスのアクティブ IP、サブネット マスク、スタンバイ IP、および論理名を入力する必要があります。

  LAN フェールオーバー インターフェイスを選択した場合は、アクティブ IP、サブネット マスク、論理名、およびスタンバイ IP の値を指定する必要はありません。LAN フェールオーバー インターフェイスに指定されている値が使用されます。

  [Use Named] オプションを選択した場合、[Logical Name] フィールドは、名前のついたインターフェイスのドロップダウン リストになります。このリストからインターフェイスを選択します。アクティブ IP、サブネット マスク、スタンバイ IP の値を指定する必要はありません。そのインターフェイスに指定された値が使用されます。[Interfaces] タブで選択したインターフェイスにスタンバイ IP アドレスを指定してください。

（注）　ステートフル フェールオーバーでは、大量のトラフィックが生成されることがあるため、ステートフル フェールオーバーと通常トラフィックの両方のパフォーマンスが、名前付きインターフェイスを使用することで影響を受けることがあります。

- [Active IP]：プライマリ装置のステートフル フェールオーバー インターフェイスの IP アドレスを指定します。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスまたは [Use Named] オプションが選択されている場合、このフィールドはグレー表示されます。
- [Subnet Mask]：プライマリ装置およびセカンダリ装置のステートフル フェールオーバー インターフェイスのマスクを指定します。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスまたは [Use Named] オプションが選択されている場合、このフィールドはグレー表示されます。
- [Logical Name]：フェールオーバー通信に使用される論理インターフェイスを指定します。[Interface] ドロップダウン リストで [Use Named] オプションを選択した場合、このフィールドには、名前付きインターフェイスのリストが表示されます。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスが選択されている場合、このフィールドはグレー表示されます。
- [Standby IP]：セカンダリ装置がプライマリ装置との通信に使用する IP アドレスを指定します。[Interface] ドロップダウン リストで LAN フェールオーバー インターフェイスまたは [Use Named] オプションが選択されている場合、このフィールドはグレー表示されます。
- [Enable HTTP replication]：このチェックボックスをオンにすると、ステートフル フェールオーバーによるアクティブ HTTP セッションからスタンバイ ファイアウォールへのコピーがイネーブルになります。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [Interfaces]（ルーテッド ファイアウォール モード）

このタブを使用して、セキュリティ アプライアンス上の各インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスを監視するかどうかを指定します。

一般的なフェールオーバーの設定方法の詳細については、「フェールオーバーについて」を参照してください。

フィールド

- [Interface]：セキュリティ アプライアンスのインターフェイスを一覧表示し、そのアクティブ IP アドレス、スタンバイ IP アドレス、モニタリング ステータスを示します。
  - [Interface Name column]：インターフェイス名を示します。
  - [Active IP column]：このインターフェイスのアクティブ IP アドレスを示します。
  - [Standby IP Address]：スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。
  - [Is Monitored column]：このインターフェイスの障害を監視するかどうかを指定します。
- [Edit]：選択したインターフェイスの [Edit Failover Interface Configuration]（ルーテッド ファイアウォール モード）ダイアログボックスを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Edit Failover Interface Configuration]（ルーテッド ファイアウォール モード）

[Edit Failover Interface Configuration] ダイアログボックスは、インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスをモニタするかどうかを指定する場合に使用します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Active IP Address]：このインターフェイスの IP アドレスを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Subnet Mask]：このインターフェイスのマスクを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Standby IP Address]：スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。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]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。
  - [Failed]：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [Interfaces]（トランスペアレント ファイアウォール モード）

このタブを使用してスタンバイ管理 IP アドレスを定義し、セキュリティ アプライアンス上のインターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface]：セキュリティ アプライアンスのインターフェイスを一覧表示し、そのモニタリング ステータスを示します。
  - [Interface Name column]：インターフェイス名を示します。
  - [Is Monitored column]：このインターフェイスの障害を監視するかどうかを指定します。
- [Edit]：選択したインターフェイスの [Edit Failover Interface Configuration]（トランスペアレント ファイアウォール モード）ダイアログボックスを表示します。
- [Management IP Address]：セキュリティ アプライアンスまたはトランスペアレント ファイアウォール モードのコンテキストのアクティブおよびスタンバイ管理 IP アドレスを示します。
  - [Active]：アクティブ管理 IP アドレスを示します。
  - [Standby]：スタンバイ フェールオーバー装置の管理 IP アドレスを指定します。
- [Management Netmask]：アクティブおよびスタンバイ管理 IP アドレスに関連付けられたマスクを示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Edit Failover Interface Configuration]（トランスペアレント ファイアウォール モード）

[Edit Failover Interface Configuration] ダイアログボックスを使用して、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。インターフェイスのポーリング時間中、セキュリティ アプライアンスのフェールオーバー ペア間で Hello メッセージが交換されます。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]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。

– [Failed] : インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [Criteria]

このタブを使用して、障害が発生するときのインターフェイスの数、ポーリング間に待機する時間など、フェールオーバーの基準を定義します。保持時間では、装置がフェールオーバーする前にポーリングへの応答を受信しないまま待機する間隔が指定されます。

フィールド

- [Interface Policy] : モニタリングでインターフェイスの障害が検出されたときのフェールオーバーのポリシーを定義するためのフィールドが含まれます。
  - [Number of failed interfaces that triggers failover] : 障害の発生した監視対象インターフェイスの数がこのコマンドで設定した値を超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。値の範囲は 1 ～ 250 です。
  - [Percentage of failed interfaces that triggers failover] : 障害の発生した監視対象インターフェイスの数がこのコマンドで設定したパーセンテージを超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。
- [Failover Poll Times] : フェールオーバー リンクで Hello メッセージが送信される頻度、およびオプションで、Hello メッセージが受信されない場合にピアの障害をテストする前に待機する時間を定義するためのフィールドが含まれます。
  - [Unit Failover] : 装置間の Hello メッセージの間の時間。範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。
  - [Unit Hold Time] : 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必要がある時間（それ以外の場合は、装置がピアの障害のテスト プロセスを開始する）を設定します。範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。
  - [Monitored Interfaces] : インターフェイス間でのポーリングの間の時間。範囲は 1 ～ 15 秒または 500 ～ 999 ミリ秒です。
  - [Interface Hold Time] : データ インターフェイスがそのデータ インターフェイス上で Hello メッセージを受信し、その後ピアの障害発生が宣言される時間を設定します。有効な値は 5 ～ 75 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]: [MAC Addresses]

[MAC Addresses] タブでは、Active/Standby フェールオーバー ペアのインターフェイスの仮想 MAC アドレスを設定できます。

（注）　このタブは、ASA 5505 プラットフォームでは使用できません。

アクティブ / スタンバイ フェールオーバーでは、プライマリ装置の 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。セカンダリ装置は、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済み MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から 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。

各インターフェイスに仮想 MAC アドレスを設定して、セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。仮想 MAC アドレスを指定しない場合、フェールオーバー ペアは焼き付け済み 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 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。

フィールド

- [MAC Addresses]：アクティブおよびスタンバイ仮想 MAC アドレスが設定されているセキュリティ アプライアンス上の物理インターフェイスを一覧表示します。
  - [Physical Interface column]：フェールオーバー仮想 MAC アドレスが設定されている物理インターフェイスを示します。
  - [Active MAC Address column]：アクティブ セキュリティ アプライアンス（通常プライマリ）の MAC アドレスを示します。
  - [Standby MAC Address column]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）の MAC アドレスを示します。
- [Add]：[Add Interface MAC Address] ダイアログボックスを表示します。仮想 MAC アドレスは、LAN 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 インターフェイスには割り当てることができません。詳細については、「Add/Edit Interface MAC Address」を参照してください。

- [Edit]：選択したインターフェイスに対して [Edit Interface MAC Address] ダイアログボックスを表示します。詳細については、「Add/Edit Interface MAC Address」を参照してください。
- [Delete]：現在選択されているインターフェイスを MAC アドレス テーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Interface MAC Address

[Add/Edit Interface MAC Address] ダイアログボックスを使用して、インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを定義します。

フィールド

- [Physical Interface]：フェールオーバー仮想 MAC アドレスを定義する物理インターフェイスを指定します。フェールオーバー中は、LAN 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 インターフェイスに対して MAC アドレスは変更されないので、これらのインターフェイスは選択できません。
- [MAC Addresses]：インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを指定するためのフィールドが含まれます。
  - [Active Interface]：アクティブ セキュリティ アプライアンス（通常プライマリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。
  - [Standby Interface]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]（マルチ モード、セキュリティ コンテキスト）

マルチ コンテキスト モードの [Failover] ペインに表示されるフィールドは、コンテキストがトランスペアレント ファイアウォール モードであるか、ルーテッド ファイアウォール モードであるかによって変わります。

ここでは、次の内容について説明します。

- [Failover] : [Routed]
- [Failover] : [Transparent]

[Failover] : [Routed]

このペインを使用して、セキュリティ コンテキストの各インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface table] : セキュリティ アプライアンスのインターフェイスを一覧表示し、そのアクティブ IP アドレス、スタンバイ IP アドレス、モニタリング ステータスを示します。
  - [Interface Name column] : インターフェイス名を示します。
  - [Active IP column] : このインターフェイスのアクティブ IP アドレスを示します。
  - [Standby IP Address] : スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。
  - [Is Monitored column] : このインターフェイスの障害を監視するかどうかを指定します。
- [Edit] : 選択したインターフェイスの [Edit Failover Interface Configuration] ダイアログボックスを表示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Edit Failover Interface Configuration

[Edit Failover Interface Configuration] ダイアログボックスを使用して、インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Active IP Address]：このインターフェイスの IP アドレスを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Subnet Mask]：このインターフェイスのマスクを示します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Standby IP Address]：スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。インターフェイスのポーリング時間中、セキュリティ アプライアンスのフェールオーバー ペア間で Hello メッセージが交換されます。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]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。
  - [Failed]：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]：[Transparent]

このペインを使用して、セキュリティ コンテキストの管理インターフェイスのスタンバイ IP アドレスを定義し、セキュリティ コンテキストのインターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface]：セキュリティ コンテキストのインターフェイスを一覧表示し、そのモニタリング ステータスを示します。
  - [Interface Name]：インターフェイス名を示します。

  - [Is Monitored]：このインターフェイスの障害を監視するかどうかを指定します。
- [Edit]：選択したインターフェイスの [Edit Failover Interface Configuration] ダイアログボックスを表示します。
- [Management IP Address]：セキュリティ コンテキストのアクティブおよびスタンバイ管理 IP アドレスを示します。
  - [Active]：アクティブ フェールオーバー装置の管理 IP アドレスを示します。
  - [Standby]：スタンバイ フェールオーバー装置の管理 IP アドレスを指定します。
- [Management Netmask]：管理アドレスに関連付けられたマスクを示します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Edit Failover Interface Configuration

[Edit Failover Interface Configuration] ダイアログボックスを使用して、インターフェイスのステータスを監視するかどうかを指定します。

フィールド

- [Interface Name]：インターフェイス名を示します。
- [Monitor interface for failure]：このインターフェイスの障害を監視するかどうかを指定します。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。インターフェイスのポーリング時間中、セキュリティ アプライアンスのフェールオーバー ペア間で Hello メッセージが交換されます。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]：インターフェイスは管理上ダウンしています。
  - [No Link]：インターフェイスの物理リンクがダウンしています。
  - [Failed]：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	—	•	—

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover]（マルチ モード、システム）

このペインには、マルチ コンテキスト モードのセキュリティ アプライアンスの、システム コンテキストでのシステムレベル フェールオーバー設定を行うためのタブが含まれます。マルチ モードでは、Active/Standby フェールオーバーまたは Active/Active フェールオーバーを設定できます。アクティブ/アクティブ フェールオーバーは、デバイス マネージャでフェールオーバー グループを作成するときに、自動的にイネーブルになります。どちらのタイプのフェールオーバーの場合も、システム コンテキストでのシステムレベル フェールオーバー設定、および個々のセキュリティ コンテキストでのコンテキストレベル フェールオーバー設定を入力する必要があります。一般的なフェールオーバーの設定方法の詳細については、「フェールオーバーについて」を参照してください。

詳細については、次の項目も参照してください。

- [Failover] > [Setup] タブ
- [Failover] > [Criteria] タブ
- [Failover] > [Active/Active] タブ
- [Failover] > [MAC Addresses] タブ

[Failover] > [Setup] タブ

このタブを使用して、マルチ コンテキスト モードのセキュリティ アプライアンスでフェールオーバーをイネーブルにします。また、ステートフル フェールオーバーを使用している場合、このタブではフェールオーバー リンクおよびステート リンクも指定できます。

フィールド

- [Enable Failover]：このチェックボックスをオンにすると、フェールオーバーがイネーブルになり、スタンバイ セキュリティ アプライアンスを設定できます。

（注） インターフェイスの速度と二重通信の設定は、フェールオーバーがイネーブルになっても変更されません。フェールオーバー インターフェイスの速度や二重通信の設定を変更するには、フェールオーバーをイネーブルにする前に、[Configuration] > [Interfaces] ペインで設定しておく必要があります。

- [Use 32 hexadecimal character key]：[Shared Key] フィールドに 16 進数値の暗号キーを入力するには、このチェックボックスをオンにします。[Shared Key] フィールドに英数字の共有秘密情報を入力する場合は、このチェックボックスをオフにします。

- [Shared Key]：フェールオーバー共有秘密情報またはフェールオーバー ペア間での暗号化および認証済み通信のためのキーを指定します。

  [Use 32 hexadecimal character key] チェックボックスをオンにした場合、16 進数の暗号キーを入力してください。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。

  [Use 32 hexadecimal character key] チェックボックスをオフにした場合は、英数字の共有秘密情報を入力してください。共有秘密情報は、1 ～ 63 文字で入力できます。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。

- [Enable LAN rather than serial cable failover]:（PIX セキュリティ アプライアンス プラットフォームのみ）LAN フェールオーバーをイネーブルにするには、このチェックボックスをオンにします。フェールオーバー リンクとして専用シリアル リンクを使用するには、このチェックボックスをオフにします。

- [LAN Failover]：LAN フェールオーバーを設定するためのフィールドが含まれます。
  - [Interface]：フェールオーバー通信に使用するインターフェイスを指定します。フェールオーバーには専用インターフェイスが必要ですが、同じインターフェイスをステートフル フェールオーバーにも使用できます。

    このリストには、コンテキストに割り当てられていない、未設定のインターフェイスまたはサブインターフェイスだけが表示され、LAN フェールオーバー インターフェイスとして選択できます。インターフェイスを LAN フェールオーバー インターフェイスとして設定すると、[Configuration] > [Interfaces] ペインで編集したり、コンテキストに割り当てたりできません。
  - [Active IP]：アクティブ装置のフェールオーバー インターフェイスの IP アドレスを指定します。
  - [Subnet Mask]：アクティブ装置のフェールオーバー インターフェイスのマスクを指定します。
  - [Logical Name]：フェールオーバー インターフェイスの論理名を指定します。
  - [Standby IP]：スタンバイ装置の IP アドレスを指定します。
  - [Preferred Role]：このセキュリティ アプライアンスの優先の役割が、LAN フェールオーバーのプライマリ装置であるか、セカンダリ装置であるかを指定します。

- [State Failover]：ステートフル フェールオーバーの設定のためのフィールドが含まれます。
  - [Interface]：フェールオーバー通信に使用するインターフェイスを指定します。未設定のインターフェイス、サブインターフェイス、または LAN フェールオーバー インターフェイスを選択できます。

    LAN フェールオーバー インターフェイスを選択した場合、インターフェイスには、LAN 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 トラフィックの両方を処理できる十分な容量が必要です。また、アクティブ IP、サブネット マスク、論理名、スタンバイ IP の値は指定する必要はありません。LAN フェールオーバー インターフェイスに指定されている値が使用されます。

    （注）　LAN フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスには、2 つの個別の専用インターフェイスを使用することをお勧めします。
  - [Active IP]：アクティブ装置のステートフル フェールオーバー インターフェイスの IP アドレスを指定します。
  - [Subnet Mask]：アクティブ装置のステートフル フェールオーバー インターフェイスのマスクを指定します。
  - [Logical Name]：ステートフル フェールオーバー インターフェイスの論理名を指定します。
  - [Standby IP]：スタンバイ装置の IP アドレスを指定します。

– [Enable HTTP replication]：このチェックボックスをオンにすると、ステートフル フェールオーバーによるアクティブ HTTP セッションからスタンバイ ファイアウォールへのコピーがイネーブルになります。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover] > [Criteria] タブ

このタブを使用して、障害が発生するときのインターフェイスの数、ポーリング間に待機する時間など、フェールオーバーの基準を定義します。保持時間では、装置がフェールオーバーする前にポーリングへの応答を受信しないまま待機する間隔が指定されます。

（注）　Active/Active フェールオーバーを設定している場合、インターフェイス ポリシーの定義にこのタブを使用しないでください。各フェールオーバー グループのインターフェイス ポリシーを定義するには、[Failover] > [Active/Active] タブを使用します。Active/Active フェールオーバーでは、各フェールオーバー グループに定義されたインターフェイス ポリシー設定がこのタブでの設定を上書きします。Active/Active フェールオーバーをディセーブルにした場合は、このタブの設定が使用されます。

フィールド

- [Interface Policy]：モニタリングでインターフェイスの障害が検出されたときのフェールオーバーのポリシーを定義するためのフィールドが含まれます。
  - [Number of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定した値を超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。値の範囲は 1 ～ 250 です。
  - [Percentage of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定したパーセンテージを超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。
- [Failover Poll Times]：フェールオーバー リンクで Hello メッセージが送信される頻度、およびオプションで、Hello メッセージが受信されない場合にピアの障害をテストする前に待機する時間を定義するためのフィールドが含まれます。
  - [Unit Failover]：装置間の Hello メッセージの間の時間。範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。

- [Unit Hold Time]：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必要がある時間（それ以外の場合は、装置がピアの障害のテスト プロセスを開始する）を設定します。範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ポーリング時間の 3 倍より少ない値は入力できません。
- [Monitored Interfaces]：インターフェイス間でのポーリングの間の時間。範囲は 1 ～ 15 秒または 500 ～ 999 ミリ秒です。
- [Interface Hold Time]：データ インターフェイスがそのデータ インターフェイス上で Hello メッセージを受信し、その後ピアの障害発生が宣言される時間を設定します。有効な値は 5 ～ 75 秒です。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover] > [Active/Active] タブ

このタブを使用して、フェールオーバー グループを定義し、セキュリティ アプライアンスで Active/Active フェールオーバーをイネーブルにします。Active/Active フェールオーバー コンフィギュレーションでは、両方のセキュリティ アプライアンスがネットワーク トラフィックを渡すことができます。Active/Active フェールオーバーは、マルチ モードのセキュリティ アプライアンスでだけ使用できます。

フェールオーバー グループは、1 つのセキュリティ コンテキストの論理グループにすぎません。セキュリティ アプライアンスには、2 つのフェールオーバー グループを作成できます。フェールオーバー ペアのアクティブ装置にフェールオーバー グループを作成する必要があります。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。

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

フィールド

- [Failover Groups]：現在セキュリティ アプライアンスに定義されているフェールオーバー グループを一覧表示します。
  - [Group Number]：フェールオーバー グループ番号を指定します。この番号は、コンテキストをフェールオーバー グループに割り当てるときに使用されます。
  - [Preferred Role]：同時に起動したり、preempt オプションが指定されたりしたときに、フェールオーバー グループがアクティブ状態として表示される、フェールオーバー ペアのプライマリ装置またはセカンダリ装置を指定します。ペアの一方の装置にアクティブ状態の両方の

フェールオーバー グループを含めて、もう一方の装置にスタンバイ状態のフェールオーバー グループを含めることができます。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 プリファレンスを割り当てて、それぞれを別の装置上でアクティブにすることでデバイスにトラフィックを分散させます。

  - [Preempt Enabled]：このフェールオーバー グループの優先フェールオーバー デバイスである装置がリブート後にアクティブ装置になるかどうかを指定します。
  - [Preempt Delay]：優先フェールオーバー デバイスが、このフェールオーバー グループのアクティブ装置として引き継ぐ前に、リブート後に待機する秒数を指定します。値の範囲は 0 ～ 1200 秒です。
  - [Interface Policy]：グループがフェールオーバーする前に許可される監視対象インターフェイス障害の数または障害のパーセンテージのいずれかを指定します。範囲は 1 ～ 250 回の障害、または 1 ～ 100% です。
  - [Interface Poll Time]：インターフェイス間のポーリング間隔の時間を指定します。1 ～ 15 秒の範囲で指定できます。
  - [Replicate HTTP]：ステートフル フェールオーバーがアクティブ HTTP セッションをこのフェールオーバー グループのスタンバイ ファイアウォールにコピーするかどうかを示します。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。この設定は、[Setup] タブの HTTP レプリケーションの設定を上書きします。

- [Add]：[Add Failover Group] ダイアログボックスを表示します。存在するフェールオーバー グループが 2 つに満たない場合にだけ、このボタンがイネーブルになります。詳細については、「Add/Edit Failover Group」を参照してください。
- [Edit]：選択したフェールオーバー グループに対して [Edit Failover Group] ダイアログボックスを表示します。詳細については、「Add/Edit Failover Group」を参照してください。
- [Delete]：現在選択されているフェールオーバー グループをフェールオーバー グループ テーブルから削除します。このボタンは、リストの最終フェールオーバー グループが選択されている場合にだけイネーブルになります。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Failover Group

[Add/Edit Failover Group] ダイアログボックスを使用して、Active/Active フェールオーバー コンフィギュレーションにフェールオーバー グループを定義します。

フィールド

- [Preferred Role]：フェールオーバー グループがアクティブ状態として表示される、フェールオーバー ペアのプライマリ装置またはセカンダリ装置を指定します。ペアの一方の装置にアクティブ状態の両方のフェールオーバー グループを含めて、もう一方の装置にスタンバイ状態のフェールオーバー グループを含めることができます。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 プリファレンスを割り当てて、それぞれを別の装置上でアクティブにすることでデバイスにトラフィックを分散させます。
- [Preempt after booting with optional delay of]：このチェックボックスをオンにすると、フェールオーバー グループの優先フェールオーバー デバイスである装置が、リブート後にアクティブ装置になります。また、このチェックボックスをオンにすると、デバイスがアクティブ装置になる前に待機しなければならない時間を指定できる [Preempt after booting with optional delay of] フィールドとともに、リブート後に Preempt もイネーブルになります。
- [Preempt after booting with optional delay of]：優先フェールオーバー デバイスである装置が、いずれかのフェールオーバー グループのアクティブ装置として引き継ぐ前に、リブート後に待機する秒数を指定します。値の範囲は 0 ～ 1200 秒です。
- [Interface Policy]：モニタリングでインターフェイスの障害が検出されたときのフェールオーバーのポリシーを定義するためのフィールドが含まれます。これらの設定は、[Criteria] タブのインターフェイス ポリシー設定を上書きします。
  - [Number of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定した値を超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。値の範囲は 1 ～ 250 です。
  - [Percentage of failed interfaces that triggers failover]：障害の発生した監視対象インターフェイスの数がこのコマンドで設定したパーセンテージを超えたとき、セキュリティ アプライアンスはフェールオーバーを行います。
- [Poll time interval for monitored interfaces]：インターフェイス間でのポーリングの間の時間。1 ～ 15 秒の範囲で指定できます。
- [Enable HTTP replication]：このチェックボックスをオンにすると、ステートフル フェールオーバーによるアクティブ HTTP セッションからスタンバイ ファイアウォールへのコピーがイネーブルになります。HTTP の複製を許可しない場合、HTTP 接続はフェールオーバーで切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。この設定は、[Setup] タブの HTTP レプリケーションの設定を上書きします。
- [MAC Addresses]：アクティブおよびスタンバイ仮想 MAC アドレスが設定されているセキュリティ アプライアンス上の物理インターフェイスを一覧表示します。
  - [Physical Interface]：フェールオーバー仮想 MAC アドレスが設定されている物理インターフェイスを示します。
  - [Active MAC Address]：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上のインターフェイスおよびフェールオーバー グループの MAC アドレスを表示します。
  - [Standby MAC Address]：フェールオーバー グループがスタンバイ状態になっている装置上のインターフェイスおよびフェールオーバー グループの MAC アドレスを表示します。
- [Add]：[Add Interface MAC Address] ダイアログボックスを表示します。仮想 MAC アドレスは、LAN 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 インターフェイスには割り当てることができません。詳細については、「Add/Edit Interface MAC Address」を参照してください。
- [Edit]：選択したインターフェイスに対して [Edit Interface MAC Address] ダイアログボックスを表示します。詳細については、「Add/Edit Interface MAC Address」を参照してください。
- [Delete]：現在選択されているインターフェイスを MAC アドレス テーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Interface MAC Address

[Add/Edit Interface MAC Address] ダイアログボックスを使用して、フェールオーバー グループのインターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを定義します。インターフェイスに仮想 MAC アドレスを指定しない場合、次のようにデフォルトの仮想 MAC アドレスが指定されます。

- アクティブ ユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number.failover_group_id*01
- スタンバイ装置のデフォルト MAC アドレス：00a0.c9:*physical_port_number.failover_group_id*02

（注） 同じネットワーク上にアクティブ/アクティブ フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上で MAC アドレスが重複することを回避するには、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

これらの MAC アドレスは、インターフェイスの物理 MAC アドレスを上書きします。

フィールド

- [Physical Interface]：フェールオーバー仮想 MAC アドレスを定義する物理インターフェイスを指定します。フェールオーバー中は、LAN 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 インターフェイスに対して MAC アドレスは変更されないので、これらのインターフェイスは選択できません。
- [MAC Addresses]：インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを指定するためのフィールドが含まれます。
  - [Active Interface]：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上のインターフェイスおよびフェールオーバー グループの MAC アドレスを指定します。各インターフェイスには、MAC アドレスを 2 つまで指定できます。それぞれ各フェールオーバー グループのための MAC アドレスで、物理 MAC アドレスを上書きします。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。
  - [Standby Interface]：フェールオーバー グループがスタンバイ状態になっている装置上のインターフェイスおよびフェールオーバー グループの MAC アドレスを指定します。各インターフェイスには、MAC アドレスを 2 つまで指定できます。それぞれ各フェールオーバー グループのための MAC アドレスで、物理 MAC アドレスを上書きします。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

[Failover] > [MAC Addresses] タブ

[MAC Addresses] タブでは、Active/Standby フェールオーバー ペアのインターフェイスの仮想 MAC アドレスを設定できます。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置の 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。セカンダリ装置は、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済み MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から 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。

各インターフェイスに仮想 MAC アドレスを設定して、セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。仮想 MAC アドレスを指定しない場合、フェールオーバー ペアは焼き付け済み 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 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。

Active/Active フェールオーバーでは、このタブで設定された MAC アドレスは無効になります。代わりに、フェールオーバー グループで定義された MAC アドレスが使用されます。

フィールド

- [MAC Addresses]：アクティブおよびスタンバイ仮想 MAC アドレスが設定されているセキュリティ アプライアンス上の物理インターフェイスを一覧表示します。
  - [Physical Interface]：フェールオーバー仮想 MAC アドレスが設定されている物理インターフェイスを示します。
  - [Active MAC Address]：アクティブ セキュリティ アプライアンス（通常プライマリ）の MAC アドレスを示します。
  - [Stanby MAC Address]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）の MAC アドレスを示します。
- [Add]：[Add/Edit Interface MAC Address] ダイアログボックスを表示します。
- [Edit]：選択したインターフェイスの [Add/Edit Interface MAC Address] ダイアログボックスを表示します。

- [Delete]：現在選択されているインターフェイスを MAC アドレス テーブルから削除します。確認されず、やり直しもできません。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。

Add/Edit Interface MAC Address

[Add/Edit Interface MAC Address] ダイアログボックスを使用して、インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを定義します。

フィールド

- [Physical Interface]：フェールオーバー仮想 MAC アドレスを定義する物理インターフェイスを指定します。フェールオーバー中は、LAN 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 インターフェイスに対して MAC アドレスは変更されないので、これらのインターフェイスは選択できません。
- [MAC Addresses]：インターフェイスのアクティブおよびスタンバイ仮想 MAC アドレスを指定するためのフィールドが含まれます。
  - [Active Interface]：アクティブ セキュリティ アプライアンス（通常プライマリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。
  - [Standby Interface]：スタンバイ セキュリティ アプライアンス（通常セカンダリ）上のインターフェイスの MAC アドレスを指定します。MAC アドレスは、16 進数形式（0123.4567.89AB など）で入力します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	—	—	•

詳細情報

フェールオーバーの詳細については、「フェールオーバーについて」を参照してください。