フェールオーバーの設定

[Failover] ページで、選択したセキュリティ アプライアンスのフェールオーバーを設定できます。[Failover] ページで設定できる内容およびページ全体の外観は、選択したデバイスのタイプ、動作モード（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）によって若干異なる場合があります。

つまり、フェールオーバーの設定方法は、セキュリティ アプライアンスの動作モードとセキュリティ コンテキストの両方に応じて異なります。

インターフェイスをフェールオーバー リンクとして割り当てる場合は、次の警告に注意してください。

- [AddInterface] と [Edit Interface] ダイアログボックスでインターフェイスを定義できますが、設定しないでください。特に、インターフェイス名は指定しないでください。このパラメータを指定すると、インターフェイスをフェールオーバー リンクとして使用できなくなります。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理を参照してください。
- IPv6 アドレスはフェールオーバー リンクではサポートされていません。
- ASA 5505 では、別のインターフェイスのバックアップとして割り当てられたインターフェイスは、フェールオーバー リンクとして使用できません（ただし、これを防ぐためのチェックは実行されません）。
- PPPoE 対応のインターフェイスをフェールオーバー リンクとして割り当てないでください。PPPoE とフェールオーバーを同じデバイス インターフェイスに設定しないでください（ただし、これを防ぐためのチェックは実行されません）。
- フェールオーバー インターフェイスでは、別のインターフェイスと同じ IP アドレス（特に、管理 IP アドレス）は使用できません（ただし、これを防ぐためのチェックは実行されません）。

また、インターフェイスをフェールオーバー リンクとして割り当てると、そのインターフェイスは [Interfaces] ページに表示されますが、[Interfaces] ページでそのインターフェイスを編集および削除することはできません。ただし、唯一の例外として、物理インターフェイスをステートフル フェールオーバー リンクとして設定している場合は、その速度とデュプレックスを設定できます。

この章は次のトピックで構成されています。

フェールオーバーについて

フェールオーバーを使用すると、同一の2台のセキュリティアプライアンスで、一方に障害が発生した場合にもう一方がファイアウォール動作を引き継げるように設定できます。セキュリティ アプライアンスのペアを使用すると、オペレータの介入なしに、システムのハイ アベイラビリティが実現されます。

リンクされたこれらのセキュリティアプライアンスは、専用リンクを介してフェールオーバー情報をやり取りします。このフェールオーバー リンクは、LAN ベースの接続であるか、または PIX セキュリティ アプライアンスの場合は専用シリアル フェールオーバー ケーブルです。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。

- 現在のフェールオーバー状態（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」とも呼ばれる）
- ネットワーク リンクの状態
- MAC アドレス交換
- 設定の複製
- 接続ごとの状態情報（ステートフル フェールオーバーの場合）

注意 フェールオーバー リンクを介して送信されたすべての情報は、フェールオーバー キーで通信を保護しないかぎり、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している場合、この情報には、トンネルの確立に使用されたユーザ名、パスワード、および事前共有キーが含まれます。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。特に、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している場合は、フェールオーバー キーを使用してフェールオーバー通信を保護することを推奨します。

Cisco セキュリティ アプライアンスは、次の 2 つのタイプのフェールオーバーをサポートします。

- **アクティブ/スタンバイ**：アクティブ セキュリティ アプライアンスは、すべてのネットワークトラフィックを検査し、一方スタンバイ セキュリティアプライアンスは、アクティブアプライアンスで障害が発生するまでアイドル状態のままとなります。アクティブ セキュリティ アプライアンスの設定に加えた変更は、フェールオーバー リンクを介してスタンバイ 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発生すると、スタンバイ セキュリティ アプライアンスがアクティブ装置になり、前にアクティブであった装置の IP アドレスと MAC アドレスを引き継ぎます。IP アドレスまたは MAC アドレスのこ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。

アクティブ/スタンバイ フェールオーバーを使用できるのは、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 モードで動作しているセキュリティ アプライアンスです。シングル コンテキスト モードでは、アクティブ/スタンバイ フェールオーバーだけを使用でき、すべてのフェールオーバー設定が [Failover] ページを使用して行われます。

（注） アクティブ/スタンバイ フェールオーバーを使用する場合、設定の変更はすべてアクティブ装置に対して行う必要があります。アクティブ装置は、これらの変更内容をスタンバイ装置に自動的に複製します。スタンバイ装置は、Security Manager デバイス リストにインポートまたは追加されません。また、認証証明書をアクティブ デバイスからスタンバイ デバイスに手動でコピーする必要があります。詳細については、アクティブ/スタンバイ フェールオーバー設定の追加手順 （12 ページ）を参照してください。

- **アクティブ/アクティブ**：両方のセキュリティアプライアンスが、一方がアクティブでもう一方がスタンバイになるようにそれぞれのロールを切り替えて、ネットワークトラフィックをコンテキストベースで検査します。これは、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 モードで動作するセキュリティ アプライアンスだけで使用できることを意味します。

ただし、アクティブ/アクティブ フェールオーバーが、マルチ コンテキスト モードでの必須のフェールオーバーというわけではありません。つまり、マルチ コンテキスト モードで動作しているデバイスでは、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 フェールオーバーを設定できます。いずれの場合も、システム コンテキストでシステム レベルのフェールオーバー設定を指定し、個々のセキュリティ コンテキストでコンテキスト レベルのフェールオーバー設定を指定します。

この項目の詳細については、アクティブ/アクティブ フェールオーバー （4 ページ）を参照してください。

さらに、フェールオーバーは、ステートレスまたはステートフルにすることができます。

- **ステートレス**：「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発生すると、アクティブな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**：フェールオーバーペアのアクティブ装置は、接続ごとの状態情報をスタンバイ装置に継続的に渡します。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を使用できます。サポートされるエンドユーザ アプリケーションは、現在の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。

詳細については、ステートフル フェールオーバー （6 ページ）を参照してください。

関連項目

- 基本的なフェールオーバー設定 （7 ページ）
- フェールオーバー ポリシー （13 ページ）

アクティブ/アクティブ フェールオーバー

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 モードで動作するセキュリティ アプライアンスだけで使用できます。アクティブ/アクティブ フェールオーバー設定では、両方のセキュリティ アプライアンスがコンテキストごとにネットワーク トラフィックを検査します。つまり、各コンテキストで、一方のアプライアンスがアクティブ デバイスで、もう一方のアプライアンスがスタンバイ デバイスとなります。

アクティブロールとスタンバイロールは、セキュリティコンテキストのセット全体でほぼ任意で割り当てられます。

セキュリティ アプライアンスでアクティブ/アクティブ フェールオーバーをイネーブルにするには、2 つのフェールオーバー グループのいずれかにセキュリティ コンテキストを割り当てる必要があります。フェールオーバー グループは、単に 1 つ以上のセキュリティ コンテキストの論理グループです。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 グループ割り当てを指定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、両方の装置が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状態で表示される装置が決まります。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。

（注） Cisco Security Manager は、アクティブ/アクティブ フェールオーバー モードのセキュリティ コンテキストを確実に管理するために、各コンテキストの管理インターフェイス用の IP アドレスを要求して、フェールオーバー ペアのアクティブなセキュリティ コンテキストと直接通信できるようにします。

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。

（注） アクティブ/アクティブ フェールオーバー設定のピア デバイスをブートストラップすると、そのブートストラップ設定は、それぞれのフェールオーバー ピア デバイスのシステム コンテキストにだけ適用されます。

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 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、引き続きスタンバイ装置上の現在の接続状態情報を更新します。フェールオーバーの発生時、サポートされるエンドユーザアプリケーションは、現在の通信セッションを保持するために再接続する必要がありません。

（注） ステート リンクおよび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、すべての状態情報をスタンバイ装置に渡すようにリンクを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 プラットフォームでだけ使用可能）ではなく、LAN フェールオーバー接続を使用している場合、ステートリンクおよびフェールオーバーリンクに同じインターフェイスを使用できます。ただし、スタンバイ装置に状態情報を渡すときは、専用のインターフェイスを使用することを推奨します。

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場合、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
- タイムアウト接続を含む、TCP 接続テーブル（HTTP を除く）
- HTTP 接続状態（HTTP レプリケーション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場合、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 レプリケーション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

基本的なフェールオーバー設定

次の手順では、基本的なフェールオーバー設定について説明します。インターフェイスをフェールオーバー リンクとして割り当てる場合は、次の警告に注意してください。

- [AddInterface] と [Edit Interface] ダイアログボックスでインターフェイスを定義できますが、設定しないでください。特に、インターフェイス名は指定しないでください。このパラメータを指定すると、インターフェイスをフェールオーバーリンクとして使用できなくなります。
- ASA 5505 では、別のインターフェイスのバックアップとして割り当てられたインターフェイスは、フェールオーバーリンクとして使用できません（ただし、これを防ぐためのチェックは実行されません）。
- PPPoE 対応のインターフェイスをフェールオーバー リンクとして割り当てないでください。PPPoE とフェールオーバーを同じデバイス インターフェイスに設定しないでください（ただし、これを防ぐためのチェックは実行されません）。
- フェールオーバー インターフェイスでは、別のインターフェイスと同じ IP アドレス（特に、管理 IP アドレス）は使用できません（ただし、これを防ぐためのチェックは実行されません）。

（注） フェールオーバー設定を保存すると、その設定はセキュリティ アプライアンスとフェールオーバー ピアの両方に適用されます。

はじめる前に

フェールオーバー設定が許可されたライセンスがデバイスにインストールされている必要があります。ASA 5505 と 5510 デバイスでは、このフェールオーバー ライセンスはオプションのライセンスです。フェールオーバーライセンスは、ASDM またはデバイスの CLI を使用して、Security Manager の外部にインストールする必要があります。また、デバイスプロパティの（デバイスを右クリックして [デバイスプロパティ（Device Properties）] を選択）の [全般（General）] ページで [ライセンスはフェールオーバーをサポート（License Supports Failover）] オプションを必ず選択します。デバイスをインベントリに追加するときにライセンスをインストールする場合や、ライセンスをインストールしてからデバイス ポリシーを再検出する場合、Security Manager はライセンスを識別して、このオプションを適切に設定します。

このオプションを選択しても、ライセンスがインストールされていない場合、展開は失敗します。このオプションを選択しないと、ポリシーを設定しても、Security Manager によってデバイスにフェールオーバー ポリシーが展開されません。

関連項目

- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理
- フェールオーバーについて （2 ページ）

- アクティブ/スタンバイ フェールオーバー設定の追加手順 （12 ページ）
- フェールオーバー ポリシー （13 ページ）

ステップ 1 デバイスビューが現在のアプリケーションビューであることを確認します。必要に応じて、ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

（注） デバイス ビューを使用したデバイス ポリシーの設定の詳細については、デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理を参照してください。

ステップ 2 設定するアプライアンスを選択します。

ステップ 3 デバイスポリシーセレクタで [プラットフォーム（Platform）] エントリを展開し、次に [デバイス管理（Device Admin）] を展開して、[フェールオーバー（Failover）] を選択します。

[Failover] ページが表示されます。

ステップ 4 （PIX のみ）[フェールオーバー方式（Failover Method）]（[シリアルケーブル（Serial Cable）] または [LANベース（LAN Based）]）を選択します。[Serial Cable] を選択する場合、[LAN Failover] 設定はディセーブルになります。2 台のデバイスを接続するケーブルが正しく接続されていることを確認します。

ステップ 5 [フェールオーバーの有効化（Enable Failover）] を選択して、このアプライアンス上でのフェールオーバーをイネーブルにします。

ステップ 6 （任意）[Settings] ボタンをクリックして、選択したデバイスの [Settings] ダイアログボックスを開きます。[Settings] ダイアログボックスの内容は、デバイスのタイプ、およびデバイスがシングル モードまたはマルチ モードのどちらで動作しているかによって異なります。一部のオプションが使用できない場合があります。次の項を参照してください。

- [Settings] ダイアログボックス （29 ページ）（ASA/PIX 7+）
- [Advanced Settings] ダイアログボックス （21 ページ）（FWSM）

ステップ 7 [ブートストラップ（Bootstrap）] ボタンをクリックして、[LANフェールオーバー用のブートストラップ設定（Bootstrap configuration for LAN failover）] ダイアログボックスを開きます。このダイアログボックスでは、LAN フェールオーバー設定内のプライマリデバイスとセカンダリデバイスに適用できるブートストラップ設定が示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）を参照してください。

ステップ 8 （マルチコンテキストデバイスのみ）[設定（Configuration）] セクションで、フェールオーバーモード（[アクティブ/アクティブ（Active/Active）] または [アクティブ/スタンバイ（Active/Standby）]）を選択します。

ステップ 9 （任意）次の手順を実行して、2 台のデバイス間の LAN フェールオーバー通信用のインターフェイスを設定します。

a) LAN ベースの通信用のデバイスインターフェイスを割り当て、次にキーボードの Tab キーを押してページを更新します。

PIX デバイスおよび ASA デバイスでは、このドロップダウン リストに、デバイスで定義されているインターフェイスが表示されます。ポート ID（gigabitethernet1 など）を入力するか、またはインターフェイスをすでに定義している場合はポートを選択できます。

FWSM では、このインターフェイス リストには VLAN ID は読み込まれません。ユーザは、使用する必要がある VLAN の数値 ID を入力する必要があります。

（注） いずれの場合も、名前付きインターフェイスは指定できず、PPPoE にはインターフェイスを設定できません。

b) [論理名（Logical Name）] にこのフェールオーバー インターフェイスの論理名を指定します。
c) [アクティブIP（Active IP）] にフェールオーバー通信用のアクティブ IP アドレスを入力します。
d) [スタンバイIP（Standby IP）] にフェールオーバー通信用のスタンバイ IP アドレスを入力します。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティ アプライアンスで使用されます。
e) [サブネットマスク（Subnet Mask）] に両方の IP アドレスのサブネットマスクを入力します。両方が同じサブネット上にある必要があります。

ステップ 10 （任意）次の手順を実行して、2 台のデバイス間のステートフルフェールオーバー通信用のインターフェイスを設定します。

a) 更新通信用のデバイスインターフェイスを割り当て、次にキーボード上の Tab キーを押してページを更新します。

ポート ID（gigabitethernet1 など）を入力するか、またはインターフェイスをすでに定義している場合は、ポートを選択できます。ただし、名前付きインターフェイスは指定できません。

（注） FWSM では、これは VLAN インターフェイスです。

b) [論理名（Logical Name）] にこのインターフェイスの論理名を指定します。
c) [アクティブIP（Active IP）] に接続更新用のアクティブ IP アドレスを入力します。
d) [スタンバイIP（Standby IP）] に更新通信用のスタンバイ IP アドレスを入力します。
e) [サブネットマスク（Subnet Mask）] に両方の IP アドレスのサブネットマスクを入力します。両方が同じサブネット上にある必要があります。
f) HTTP 接続情報を保持するには、[HTTPレプリケーションの有効化（Enable HTTP Replication）] を選択します。

HTTP を除くすべての TCP プロトコルに関する接続情報が、スタンバイ装置に伝達されます。HTTP 接続は一般に存続期間が短いため除かれます。フェールオーバー中に HTTP 接続を保持するには、このオプションを選択します。

ステップ 11 通信の暗号化キーを指定します。共有キーを入力し、次に [確認（Confirm）] フィールドに再度入力します。両方のデバイスで同じキーを必ず入力してください（3.1 よりも前のバージョンの FWSM では使用できません）。

共有キーには、最大 63 の英数字の任意の文字列を使用できます。[HEX] オプションが選択されている場合、共有キーは、厳密に 32 の 16 進数文字からなる任意の文字列となります（[HEX] オプションは、PIX/ASA バージョン 7.0.5 以降、および FWSM バージョン 3.1.3 以降でだけ使用できます）。

（注） この手順の実行は任意ですが、フェールオーバー通信を暗号化することを強く推奨します。

ステップ 12 非対称ルーテッドセッションのフェールオーバーの再接続タイムアウト値を指定するには、時間を hh:mm:ss（分と秒の値は省略可能）形式で [タイムアウト（Timeout）] フィールドに入力します。このフィールドが空白（デフォルト）または 0 の場合、再接続は行われません。この値を -1 に設定すると、タイムアウトがディセーブルになり、任意の時間が経過したあとでも接続を再開できます。

ステップ 13 (オプション)フェールオーバーペアと通信するように双方向フォワーディング検出（BFD）を設定でき、これを使用してフェールオーバーユニットの正常性を監視できます。[ヘルスチェックモニタリング（Health-Check Monitoring）] セクションから BFD テンプレートを作成または選択します。

（注） これは、ASA 9.7.1 以降を実行している Firepower フェールオーバーデバイスにのみ適用されます。

ヒント BFD フェールオーバーコマンドは、アクティブ/スタンバイモードでのみサポートされます。マルチコンテキストデバイスでは、BFD フェールオーバーコマンドはシステムコンテキストでのみサポートされます。BFD フェールオーバーコマンドは、透過モードではサポートされません。

ステップ 14 （FWSM だけ）設定されているインターフェイスが、[Interface Configuration] テーブルにリストされます。リストされているインターフェイスのフェールオーバー設定を編集するには、そのフェールオーバー設定を選択し、[Edit Row] ボタンをクリックして [Edit Failover Interface Configuration] ダイアログボックス （33 ページ）を開きます。

フェールオーバー グループ 2 へのセキュリティコンテキストの追加

新しいセキュリティコンテキストを既存のフェールオーバーグループ 2 に追加するには、新しいコンテキストコンフィギュレーションを展開ファイルに保存してから、適切なデバイスに手動で追加する必要があります。それ以外の場合、最初に展開が成功するまで、Security Manager はデバイスの管理コンテキストを介して新しいコンテキストとの通信を試みます。（グループ 1 と 2 の両方が同じデバイスでアクティブでない限り、）管理コンテキストを介してグループ 2 に到達できないため、これは失敗します。

次に、新しいセキュリティコンテキストを作成し、それをフェールオーバーグループ 2 に追加する手順を示します。

1. 新規セキュリティコンテキストを作成します。

   必ず、コンテキスト名、設定 URL を定義し、インターフェイスを割り当て、フェールオーバーグループ 2 を選択し、管理 IP アドレスを指定してください。詳細については、セキュリティ コンテキストの管理を参照してください。

2. これらの変更を保存して送信します。

3. 次のコンテキスト設定情報を提供し、各変更を保存します。

   - 新しいコンテキストの [デバイスプロパティ（Device Properties）] ウィンドウの [ログイン情報（Credentials）]ページで、ユーザー名とパスワードを入力します。詳細については、デバイス プロパティの表示または変更を参照してください。
   - コンテキストの[インターフェイス（Interfaces）]ページで、割り当てられたインターフェイスを編集して、名前、IP アドレス、およびサブネットマスクを指定します。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理を参照してください。

- コンテキストの [Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）で、インターフェイス設定を編集して、スタンバイ IP アドレスを提供します。
- [HTTP] ページで、[HTTPサーバーを有効にする（Enable HTTP Server）] をオンにして、HTTP アクセスを定義します。
- ログイン情報（Credentials）]ページで、コンテキストに接続するときに使用するユーザー名とパスワードを入力します。詳細については、デバイス クレデンシャルの設定を参照してください。

4. Configuration Manager の [ファイル（File）] メニューから [展開（Deploy）] を選択します。変更を送信し、[保存した変更の展開（Deploy Saved Changes）] ダイアログ ボックスで、この新しいコンテキストのみが選択されていることを確認してから、[展開メソッドの編集（Edit Deploy method）] をクリックします。[展開メソッドの編集（Edit Deploy method）] ダイアログ ボックスで、[メソッド（Method）] を [ファイル（File）] に変更し、[接続先（Destination ）] と [ファイル名（file name）] を指定します。[OK] をクリックして [展開メソッドの編集（Edit Deploy method）] ダイアログボックスを閉じ、[保存した変更の展開（Deploy Saved Changes）] ダイアログボックスの [展開（Deploy）] をクリックします。
5. 設定ファイルをデバイスにアップロードした後、CLI を使用してコンテキストの HTTP アクセスを有効にします。次に例を示します。
6. コンテキストの設定成が指定したファイルに保存されます。この手順の詳細については、ファイルへの展開を参照してください。

```
ciscoasa/group2(config-if)#  int g3/0
ciscoasa/group2(config-if)# nameif man
ciscoasa/group2(config-if)# security-level 100
ciscoasa/group2(config-if)# ip add 203.0.113.176 255.255.254.0 st 203.0.113.177
ciscoasa/group2(config-if)# exit
ciscoasa/group2(config)# http serv ena
ciscoasa/group2(config)# http 0.0.0.0 0.0.0.0 man
ciscoasa/group2(config)# username cisco pass cisco
ciscoasa/group2(config)#wr
```

このプロセスに従って、Security Manager を使用して、コンテキストへの新しい変更をコンテキストに正常に展開できます（コンテキストに到達しようとした場合、管理コンテキストの管理 IP アドレスを経由しません）。

代替方法

この問題に対する別のアプローチは、最初に新しいコンテキストをフェールオーバーグループ 1 に追加してから、Security Manager を介して設定を実行することです。ただし、このコンテキストをフェールオーバーグループ 2 に移動するには、両方のグループ（1 と 2）が同じデバイスでアクティブになっている必要があります。そうでない場合、次のエラーが報告されます。

```
"join-failover-group 2
ERROR: Command requires failover-group 2 and 1 to be in the same state or no nameif
comand for all interfaces in this context"
```

アクティブ/スタンバイ フェールオーバー設定の追加手順

Cisco Security Manager を使用すると、PIX/ASA/FWSM デバイスにインストールされている証明書を検証して、そのデバイスを認証できます。アクティブ/スタンバイ フェールオーバー設定でファイアウォールを設定する場合は、証明書をアクティブ デバイスからスタンバイ デバイスに手動でコピーして、フェールオーバーの発生後に Security Manager がスタンバイ デバイスと通信できるようにする必要があります。

次の手順では、ASDM を使用して、ネットワーク内のセキュリティ アプライアンスのアイデンティティ証明書、CA 証明書、およびキーをエクスポートまたは表示し、次に ASDM を使用してその情報をスタンバイ デバイスにインポートする方法について説明します。

- ファイルまたは PKCS12 データへの証明書のエクスポート （12 ページ）
- スタンバイ デバイスへの証明書のインポート （12 ページ）

ファイルまたは PKCS12 データへの証明書のエクスポート

トラストポイント設定をエクスポートするには、ASDM を使用して次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [機能（Features）] > [デバイス管理（Device Administration）] > [証明書（Certificate）] > [トラストポイント（Trustpoint）] > [エクスポート（Export）]** に移動します。

ステップ 2 [Trustpoint Name]、[Encryption Passphrase]、および [Confirm Passphrase] の各フィールドに入力します。これらのフィールドの詳細については、[Help] をクリックしてください。

ステップ 3 トラストポイント設定をエクスポートするための方法を選択します。

- [Export to a File]：ファイル名を入力するか、またはファイルを参照します。
- [Display the trustpoint configuration in PKCS12 format]：トラストポイント設定全体をテキスト ボックスに表示してから、インポートするためにコピーします。詳細については、[Help] をクリックしてください。

ステップ 4 [エクスポート（Export）] をクリックします。

スタンバイ デバイスへの証明書のインポート

トラストポイント設定をインポートするには、ASDM を使用して次の手順を実行します。

ステップ 1 [設定（Configuration）] > [機能（Features）] > [デバイス管理（Device Administration）] > [証明書（Certificate）] > [トラストポイント（Trustpoint）] > [インポート（Import）] に移動します。

ステップ 2 [Trustpoint Name]、[Decryption Passphrase]、および [Confirm Passphrase] の各フィールドに入力します。これらのフィールドの詳細については、[Help] をクリックしてください。この復号化パスフレーズは、このトラストポイントがエクスポートされたときに使用された暗号化パスフレーズと同じです。

ステップ 3 トラストポイント設定をインポートするための方法を選択します。

- [Import from a File]：ファイル名を入力するか、またはファイルを参照します。
- [Enter the trustpoint configuration in PKCS12 format]：エクスポート元からのトラストポイント設定全体をテキスト ボックスに貼り付けます。詳細については、[Help] をクリックしてください。

フェールオーバー ポリシー

この項では、さまざまなタイプのセキュリティ アプライアンスにおけるフェールオーバー設定を説明しているページを示します。ページは、デバイス タイプ別に整理されています。

PIX 6.x ファイアウォール

- [Failover] ページ（PIX 6.3） （14 ページ）
  - [Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3） （16 ページ）
  - [Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）

ファイアウォール サービス モジュール

- [Failover] ページ（FWSM） （17 ページ）
  - [Advanced Settings] ダイアログボックス （21 ページ）
  - [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （32 ページ）
  - [Edit Failover Interface Configuration] ダイアログボックス （33 ページ）
  - [Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）

適応型セキュリティ アプライアンスおよび PIX 7.0 ファイアウォール

- [Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）
  - [Settings] ダイアログボックス （29 ページ）
  - [Edit Failover Group] ダイアログボックス （35 ページ）
  - [Edit Failover Interface Configuration] ダイアログボックス （33 ページ）
  - [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （32 ページ）

• [Bootstrap Configuration for LAN Failover] ダイアログボックス　（37 ページ）

[Failover] ページ（PIX 6.3）

（注）　バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

[Failover] ページは、PIX 6.3.x ファイアウォールのフェールオーバー値を設定するために使用します。

ナビゲーション パス

デバイスビューで PIX 6.3.x デバイスを選択してから、デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）] を選択します。

関連項目

• フェールオーバーについて　（2 ページ）
• フェールオーバー ポリシー　（13 ページ）

フィールド リファレンス

表 *1 : [Failover]* ページ（*PIX 6.3*）

要素	説明
フェールオーバー	
Failover Method	フェールオーバーリンクのタイプを [シリアルケーブル（Serial Cable）] または [LANベース（LAN Based）] から選択します。[Serial Cable] を選択する場合、物理ケーブルが両方のデバイスに接続されていることを確認します。
Enable Failover	このデバイスで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。両方のデバイスのソフトウェア バージョン、アクティベーション キー タイプ、フラッシュ メモリ、およびメモリが同じであることを確認します。 PIX デバイスで [Failover Method] に [LAN Based] を選択している場合、次に論理 LAN フェールオーバー インターフェイスを設定する必要があります。また、任意でステートフル フェールオーバー インターフェイスを設定します。

要素	説明
[Bootstrap] ボタン	クリックすると、[Bootstrap Configuration for LAN Failover] ダイアログボックスが表示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）を参照してください。
Failover Poll Time	装置間での hello メッセージの間隔を指定します。値の範囲は 3 ～ 15 秒です。デフォルトは 15 です。
LAN-Based Failover これらのフィールドは [Failover Method] に [LAN Based] が選択されているときに使用できます。	
インターフェイス	LANベースのフェールオーバーに使用するインターフェイスを選択します。[未選択（Not Selected）] を選択すると、LANベースのフェールオーバーが無効になります。
共有キー 確認（Confirm）	プライマリ デバイスとスタンバイ デバイス間の通信を暗号化するために使用します。値には任意の英数文字列を指定できます。 [Confirm] フィールドに [Shared Key] をもう一度入力します。
Stateful Failover （任意） ステートフル フェールオーバー （6 ページ）を設定するには、次のパラメータを指定します。	
インターフェイス	ステートフルフェールオーバーに使用するインターフェイスを選択します。[未選択（Not Selected）] を選択すると、ステートフル フェールオーバーが無効になります。 （注） リストから高速 LAN リンクを選択する必要があります（100full、1000full、1000sxfull など）。
Enable HTTP Replication	選択すると、アクティブなHTTPセッションがスタンバイ ファイアウォールにコピーされます。選択しないと、HTTP 接続はフェールオーバー時に切断されます。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。
インターフェイス コンフィギュレーション このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスの [Standby IP Address] および [Active MAC Address] と [Standby MAC Address] を定義するには、リストからそれらを選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3） （16 ページ）を開きます。	

[Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[Edit Failover Interface Configuration] ダイアログボックスを使用して、選択した PIX 6.3.x デバイスのフェールオーバー インターフェイスを設定します。

（注） PPPoE にはフェールオーバー インターフェイスを設定できません。

ナビゲーション パス

[Edit Failover Interface Configuration] ダイアログボックスには、[Failover] ページ（PIX 6.3）（14 ページ）の [Interface Configuration] テーブルからアクセスできます。

関連項目

- フェールオーバー ポリシー （13 ページ）

フィールド リファレンス

表 2 : [Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3）

要素	説明
インターフェイス（Interface）	インターフェイスの名前。読み取り専用です。
Active IP Address	アクティブ インターフェイスの IP アドレスを表示します。このアドレスは、アクティブ デバイスと通信するためにスタンバイ デバイスによって使用されます。アドレスは、システムの IP アドレスと同じネットワーク上にある必要があります。 このインターフェイスのアクティブ IP アドレス。読み取り専用です。このアドレスは、アクティブデバイスと通信するためにスタンバイ デバイスによって使用されます。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、このフィールドはブランクです。 **ヒント** この IP アドレスを ping ツールで使用して、アクティブ デバイスのステータスを確認できます。

要素	説明
ネットマスク	アクティブ IP アドレスのサブネット マスク。読み取り専用です。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、このフィールドはブランクです。
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。このアドレスは、スタンバイ デバイスと通信するためにアクティブデバイスによって使用されます。アドレスは、システムの IP アドレスと同じネットワーク上にある必要があります。 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。 **ヒント** この IP アドレスを ping ツールで使用して、スタンバイ デバイスのステータスを確認できます。
フェールオーバー MAC アドレス これらのパラメータでは、フェールオーバー用に設定する物理インターフェイスの仮想MAC アドレスを定義できます。これらのアドレスはオプションです。	
Active MAC Address	アクティブ インターフェイスの MAC アドレスを 16 進数形式で指定します（0123.4567.89ab など）。
Standby MAC Address	スタンバイ インターフェイスの MAC アドレスを 16 進数形式で指定します（0123.4567.89ab など）。

[Failover] ページ（FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[フェールオーバー（Failover）] ページを使用して、選択した Firewall Services Module の基本的なフェールオーバー値を設定します。

ナビゲーション パス

この機能にアクセスするには、デバイスビューで FWSM を選択し、次に、デバイスポリシー セレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）]** を選択します。

関連項目

- フェールオーバー ポリシー （13 ページ）

- アクティブ/スタンバイ フェールオーバー設定の追加手順 （12 ページ）
- [Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）

フィールド リファレンス

表 3 : [Failover] ページ（FWSM）

要素	説明
Enable Failover	このデバイスで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。両方のデバイスのソフトウェア バージョン、アクティベーション キー、フラッシュ メモリ、およびメモリが同じであることを確認します。 次に論理 LAN フェールオーバー インターフェイスを設定する必要があります。また、任意でステートフル フェールオーバー インターフェイスを設定します。
設定ボタン	クリックすると、[Advanced Settings] ダイアログボックス （21 ページ）が表示されます。これは、フェールオーバーを実行するタイミングを定義します。
Configuration このセクションは、マルチコンテキスト モードで動作している FWSM 3.1.1 以降のデバイスでのみ表示されます。	
アクティブ/アクティブ	アクティブ/アクティブ フェールオーバー設定では、両方のセキュリティ アプライアンスがコンテキストごとにネットワーク トラフィックを検査します。つまり、各コンテキストで、一方のアプライアンスがアクティブ デバイスで、もう一方のアプライアンスがスタンバイ デバイスとなります。 デバイスでアクティブ/アクティブ フェールオーバーをイネーブルにするには、2 つのフェールオーバー グループのいずれかにセキュリティ コンテキストを割り当てる必要があります。フェールオーバー グループは、単に 1 つ以上のセキュリティ コンテキストの論理グループです。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 グループ割り当てを指定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。フェールオーバーグループへのコンテキストの割り当てについては、[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）を参照してください。

要素	説明
アクティブ/スタンバイ	アクティブ/スタンバイ設定では、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 アプライアンスで障害が発生するまではネットワーク トラフィックを処理しません。アクティブ セキュリティ アプライアンスの設定が変更されるたびに、設定情報がフェールオーバー リンクを介してスタンバイ 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発生すると、スタンバイ セキュリティ アプライアンスが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。
LAN Failover	
VLAN	フェールオーバー リンクに使用している VLAN インターフェイスの数値 ID（11 など）を入力します。このリストには、VLAN ID は自動的に読み込まれません。[未選択（Not Selected）] を強調表示して、目的の VLAN ID 番号を入力し、キーボードの Tab キーを押して関連フィールドをアクティブ化する必要があります。 フェールオーバー用に設定する場合、インターフェイスはスタンバイ デバイスに直接接続されます。
論理名 （Logical Name）	フェールオーバー VLAN インターフェイスの論理名を入力します。
Active IP Address	このインターフェイスのアクティブ IP アドレスを指定します。
Standby IP Address	このインターフェイスのスタンバイ IP アドレスを指定します。 フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティアプライアンスで使用され、アクティブ IP アドレスと同じサブネットに存在する必要があります。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。

要素	説明
[Bootstrap] ボタン	クリックすると、[Bootstrap Configuration for LAN Failover] ダイアログボックスが表示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）を参照してください。
Stateful Failover （任意） ステートフル フェールオーバー （6 ページ）を設定するには、次のパラメータを指定します。	
VLAN	フェールオーバー リンクに使用している VLAN インターフェイスの数値 ID（12 など）を入力します。このリストには、VLAN ID は自動的に読み込まれません。[未選択（Not Selected）] を強調表示して、目的の VLAN ID 番号を入力し、キーボードの Tab キーを押して関連フィールドをアクティブ化する必要があります。 フェールオーバー用に設定する場合、インターフェイスはスタンバイ デバイスに直接接続されます。
論理名（Logical Name）	ステートフル フェールオーバー VLAN インターフェイスの論理名を入力します。
Active IP Address	このインターフェイスのアクティブ IP アドレスを指定します。
Standby IP Address	このインターフェイスのスタンバイ IP アドレスを指定します。 フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティアプライアンスで使用され、アクティブ IP アドレスと同じサブネットに存在する必要があります。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。
Enable HTTP Replication	選択すると、ステートフル フェールオーバーで、アクティブ HTTP セッションをスタンバイ ファイアウォールにコピーできるようになります。選択しないと、HTTP 接続はフェールオーバー時に切断されます。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。

要素	説明
共有キー（Shared Key）（FWSM 3.1.1 以降のみ） このセクションのオプションを使用すると、共有暗号キーを提供して、アクティブ デバイスとスタンバイ デバイス間の通信を暗号化できます。 **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。このデバイスを VPN トンネルの終端に使用する場合、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。共有キーを使用して、フェールオーバー通信のセキュリティを確保することを推奨します。	
共有キー 確認（Confirm）	最大 63 文字の数字、文字、句読点の文字列を入力します。この文字列は暗号キーを生成するために使用されます。 [確認（Confirm）] フィールドにこの文字列をもう一度入力します。 [HEX] を選択する場合、[共有キー（Shared Key）] と [確認（Confirm）] のフィールドには、正確に 32 文字の 16 進数（0 ～ 9、a ～ f）を入力する必要があります。
インターフェイス コンフィギュレーション このテーブルは、シングルコンテキスト モードで動作しているデバイスまたは個々のセキュリティ コンテキストだけの [Failover] ページに表示されます。 このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスのモニタリングをイネーブルまたはディセーブルにするには、インターフェイスをリストから選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス （33 ページ）を開きます。[このインターフェイスの障害をモニターする（Monitor this interface for failure）] をオンまたはオフにします。	

[Advanced Settings] ダイアログボックス

[Advanced Settings] ダイアログボックスでは、選択した FWSM 用に追加のフェールオーバーを設定できます。

（注） 次のリファレンス テーブルは、[Advanced Settings] ダイアログボックスに表示される可能性があるすべてのフィールドを示しています。実際に表示されるフィールドは、動作モード（ルーテッドまたはトランスペアレント）とデバイスがシングル コンテキストとマルチ コンテキストのどちらをホストしているかによって異なります。

ナビゲーション パス

[Failover] ページ（FWSM） （17 ページ）の [Settings] ボタンをクリックして、[Advanced Settings] ダイアログボックスにアクセスできます。

関連項目

- フェールオーバー ポリシー （13 ページ）

フィールド リファレンス

表 4 : [Advanced Settings] ダイアログボックス

要素	説明
Interface Policy 障害が発生したインターフェイス オプションを選択して、適切な値を指定します。	
Number of failed interfaces	障害が発生したモニタ対象インターフェイスの数がこの値を超えると、セキュリティアプライアンスはフェールオーバーします。有効な値の範囲は 1 ～ 250 です。
障害が発生したインターフェイスのパーセンテージ（Percentage of failed interfaces）	障害が発生したモニタ対象インターフェイスの数がこのパーセンテージを超えると、セキュリティアプライアンスはフェールオーバーします。
Failover Poll Time これらのフィールドは、フェールオーバー リンクに送信される hello メッセージの頻度、および hello メッセージを受信していないときにピアの障害テストを実行するまでに待機する時間を定義します。	
Unit Failover	フェールオーバー装置間での hello メッセージの間隔。秒単位で 1 ～ 15 の値を入力するか、[msec] をオンにする場合は、ミリ秒単位で 500 ～ 999 の値を入力します。
Unit Hold Time	フェールオーバー リンク上で hello メッセージを待機する時間。この時間を過ぎると、装置はピアの障害テストを開始します。秒単位で 3 ～ 45 の値を入力します。この値は少なくとも [Unit Failover] 値の 3 倍である必要があります。
Monitored Interface	インターフェイス間でのポーリングの間隔。秒単位で 3 ～ 15 の値を入力します。

要素	説明
MAC Address Mapping	アクティブ/スタンバイ モードでは、このテーブルにはインターフェイスと仮想 MAC アドレスのマッピングが一覧表示されます。これは Security Manager の標準のテーブルです。テーブルの使用で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 インターフェイス マッピングを追加または編集するには、[Add Row] または [Edit Row] ボタンをクリックして、[Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （32 ページ）を開きます。
フェールオーバー グループ	アクティブ/アクティブ モードでは、このテーブルには両方のフェールオーバー グループが一覧表示されます。いずれかのグループのフェールオーバー パラメータを編集するには、グループをリストで選択して、[Edit Row] ボタンをクリックして、[Edit Failover Group] ダイアログボックス （35 ページ）を開きます。
Bridge Group Configuration	シングルコンテキスト トランスペアレント モードでは、このテーブルには現在定義されているすべてのブリッジ グループが一覧表示されます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理を参照）。スタンバイ IP アドレスをブリッジ グループに追加するには、グループをリストで選択して、[Edit Row] ボタンをクリックして、[Edit Failover Bridge Group Configuration] ダイアログボックス （23 ページ）を開きます。

[Edit Failover Bridge Group Configuration] ダイアログボックス

このダイアログボックスを使用して、スタンバイ IP アドレスをフェールオーバー ブリッジ グループに追加します。

ナビゲーション パス

[Edit Failover Bridge Group Configuration] ダイアログボックスには、次の場所からアクセスできます。

- ASA 上のトランスペアレント モードの個々のセキュリティ コンテキストに表示される [Failover] ページ。
- トランスペアレント モードの FWSM で表示される [Advanced Settings] ダイアログボックス （21 ページ）の [Bridge Group Configuration] テーブル。

関連項目

- フェールオーバー ポリシー （13 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）
- [Failover] ページ（FWSM） （17 ページ）

フィールド リファレンス

表 5 : [Edit Failover Bridge Group Configuration] ダイアログボックス

要素	説明
名前	ブリッジ グループを示します。編集はできません。
IPアドレス	ブリッジ グループに割り当てられている IP アドレスを示します。編集はできません。
ネットワーク マスク（Network Mask）	IP アドレスのサブネット マスクを示します。編集はできません。
Standby Address	スタンバイ ブリッジ グループの IP アドレスを入力します。このアドレスはプライマリ アドレスと同じサブネットにある必要があります。

[Failover] ページ（ASA/PIX 7.0 以降）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

[Failover] ページを使用して、ASA および PIX 7.0 以降のセキュリティ デバイスの基本的なフェールオーバー値を設定します。

（注） [Failover] ページに表示される機能とオプションは、選択したデバイスのタイプ、オペレーティング システムのバージョン、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）、およびセキュリティ コンテキスト（シングルまたはマルチ）によって異なります。したがって、次の表で説明されている要素によっては、現在選択しているデバイスの [Failover] ページに表示されないものもあります。

ナビゲーション パス

デバイスビューで ASA または PIX 7.0 以降を選択してから、デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）]** を選択します。

関連項目

- フェールオーバーについて （2 ページ）
- フェールオーバー ポリシー （13 ページ）

- アクティブ/スタンバイ フェールオーバー設定の追加手順 （12 ページ）

フィールド リファレンス

表 *6 : [Failover]* ページ（*ASA/PIX 7.0* 以降）

要素	説明
Failover Method	フェールオーバーリンクのタイプを [シリアルケーブル（Serial Cable）] または [LANベース（LAN Based）] から選択します。[Serial Cable] を選択する場合、物理ケーブルが両方のデバイスに接続されていることを確認します。 （注）　このオプションはPIXデバイスでのみ使用できます。
Enable Failover	このデバイスで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。両方のデバイスのソフトウェア バージョン、アクティベーション キー タイプ、フラッシュ メモリ、およびメモリが同じであることを確認します。 PIX デバイスで [Failover Method] に [LAN Based] を選択している場合およびすべての ASA では、次に論理 LAN フェールオーバー インターフェイスを設定する必要があります。また、任意でステートフル フェールオーバー インターフェイスを設定します。
[Bootstrap] ボタン	クリックすると、[Bootstrap Configuration for LAN Failover] ダイアログボックスが表示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）を参照してください。
設定ボタン	クリックすると、[Settings] ダイアログボックス （29 ページ）が表示されます。これは、フェールオーバーを実行するタイミングを定義します。
タイムアウト（Timeout）	フェールオーバーの [タイムアウト（Timeout）] では、システムが起動したときまたはアクティブになったときを起点として、、固定されたセッションが受け入れられる期間を指定します。これは、スタティック トランスレーション ルールとともに使用されます（詳細については、[Static Rules] タブを参照してください）。 非対称ルーテッド セッションのフェールオーバーの再接続タイムアウト値を指定するには、このフィールドに値を入力します。値は hh:mm:ss（時間:分:秒）の形式で入力します。分と秒は両方ともオプションです。 時間の有効な値 -1 ～ 1193 です。デフォルト値は 0 です。0 に設定すると、接続は再確立されません。この値を -1 に設定すると、タイムアウトがディセーブルになり、任意の時間が経過したあとでも再接続できます。

要素	説明
Configuration このセクションは、マルチコンテキスト モードで動作しているデバイスでのみ表示されます。	
アクティブ/アクティブ	アクティブ/アクティブ フェールオーバー設定では、両方のセキュリティ アプライアンスがコンテキストごとにネットワーク トラフィックを検査します。つまり、各コンテキストで、一方のアプライアンスがアクティブデバイスで、もう一方のアプライアンスがスタンバイ デバイスとなります。 セキュリティ アプライアンスでアクティブ/アクティブ フェールオーバーをイネーブルにするには、2つのフェールオーバー グループのいずれかにセキュリティ コンテキストを割り当てる必要があります。フェールオーバー グループは、単に 1 つ以上のセキュリティ コンテキストの論理グループです。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 グループ割り当てを指定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。フェールオーバー グループへのコンテキストの割り当てについては、[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）を参照してください。
アクティブ/スタンバイ	アクティブ/スタンバイ設定では、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で障害が発生するまではネットワーク トラフィックを処理しません。アクティブ セキュリティ アプライアンスの設定が変更されるたびに、設定情報がフェールオーバー リンクを介してスタンバイ 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発生すると、スタンバイ セキュリティアプライアンスが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。
LAN Failover	

要素	説明
インターフェイス	フェールオーバー リンクとして使用するインターフェイスを選択します。デバイス上の使用可能なすべてのインターフェイスが一覧表示されます。 フェールオーバー用に設定する場合、インターフェイスはスタンバイ デバイスに直接接続されます。 （注） フェールオーバー リンクとして EtherChannel インターフェイスを選択できます。フェールオーバーリンクとして割り当てられた他のタイプのインターフェイスと同様、EtherChannel インターフェイスに名前を付けることはできません。また、EtherChannel のメンバインターフェイスに名前を付けることもできません。さらに、アクティブ フェールオーバー リンクとして使用されている最中は、インターフェイス設定を変更することはできません。詳細については、EtherChannel の設定を参照してください。
論理名（Logical Name）	フェールオーバー インターフェイスの論理名を入力します。
Active IP Address	このインターフェイスのアクティブ IP アドレスを指定します。
Standby IP Address	このインターフェイスのスタンバイ IP アドレスを指定します。 フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティアプライアンスで使用され、アクティブ IP アドレスと同じサブネットに存在する必要があります。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。
Stateful Failover （任意） ステートフル フェールオーバー （6 ページ）を設定するには、次のパラメータを指定します。	

要素	説明
インターフェイス	ステートフル フェールオーバー リンクに使用するインターフェイスを選択します。デバイス上の使用可能なすべてのインターフェイスが一覧表示されます。 （注） ステートフル フェールオーバー リンクとして EtherChannel インターフェイスを選択できます。フェールオーバーリンクとして割り当てられた他のタイプのインターフェイスと同様、EtherChannel インターフェイスに名前を付けることはできません。また、EtherChannel のメンバインターフェイスに名前を付けることもできません。さらに、アクティブ フェールオーバー リンクとして使用されている最中は、インターフェイス設定を変更することはできません。詳細については、EtherChannel の設定を参照してください。
論理名（Logical Name）	アクティブ ファイアウォール デバイス上のインターフェイスの論理名を入力します。このインターフェイスは、フェールオーバー時にスタンバイ デバイスと通信します。ステートフル フェールオーバー用に設定されたインターフェイスは、スタンバイ デバイスに直接接続します。
Active IP Address	アクティブ インターフェイスの IP アドレスを指定します。
Standby IP Address	スタンバイ インターフェイスの IP アドレスを指定します。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。
Enable HTTP Replication	選択すると、アクティブな HTTP セッションがスタンバイ ファイアウォールにコピーされます。選択しないと、HTTP 接続はフェールオーバー時に切断されます。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。
キー（Key） このセクションのオプションを使用すると、アクティブ デバイスとスタンバイ デバイス間の通信を暗号化できます。タイプを選択して、共有暗号キーを生成する文字列を指定します。 **注意** フェールオーバー リンクおよびステートフル 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。このデバイスを VPN トンネルの終端に使用する場合、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。共有キーを使用して、フェールオーバー通信のセキュリティを確保することを推奨します。	

要素	説明
Any string 16 進数	[任意の文字列（Any string）] を選択すると、[共有キー（Shared Key）] フィールドには、最大 63 文字の数字、文字、句読点の任意の組み合わせを入力できます。この文字列は暗号キーを生成するために使用されます。 [HEX] を選択する場合、[共有キー（Shared Key）] と [確認（Confirm）] のフィールドには、正確に 32 文字の 16 進数（0 ～ 9、a ～ f）を入力する必要があります。この文字列は暗号キーとして使用されます。
共有キー 確認（Confirm）	キー タイプとして選択した [Any string] または [HEX] のいずれかに適した文字列を入力します。 [確認（Confirm）] フィールドに文字列をもう一度入力します。
インターフェイスコンフィギュレーション（Interface Configuration）（場合によっては [Monitor Interface Configuration] と表示） このテーブルは、シングルコンテキスト、トランスペアレント モードで動作している ASA 8.4.1 以降のデバイスおよび PIX/ASA デバイスの個々のコンテキストの [Failover] ページに表示されます。これらに表示されない場合は、[Settings] ダイアログボックス （29 ページ）に表示されます。 このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスのモニタリングをイネーブルまたはディセーブルにするには、インターフェイスをリストから選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス （33 ページ）を開きます。[このインターフェイスの障害をモニターする（Monitor this interface for failure）] をオンまたはオフにします。	

[Settings] ダイアログボックス

[Settings] ダイアログボックスでは、選択した ASA または PIX 7.x アプライアンスでフェールオーバーが発生するタイミングの基準を定義できます。

ナビゲーション パス

[Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）の [Settings] ボタンをクリックすると、[Settings] ダイアログボックスにアクセスできます。

（注） 次のリファレンス テーブルは、[Settings] ダイアログボックスに表示される可能性があるすべてのフィールドを示しています。実際に表示されるフィールドは、動作モード（ルーテッドまたはトランスペアレント）とデバイスがシングル コンテキストとマルチ コンテキストのどちらをホストしているかによって異なります。

関連項目

- フェールオーバー ポリシー （13 ページ）
- [Edit Failover Interface Configuration] ダイアログボックス （33 ページ）
- [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （32 ページ）
- [Bootstrap Configuration for LAN Failover] ダイアログボックス （37 ページ）

フィールド リファレンス

表 *7 : [Settings]* ダイアログボックス

要素	説明
Interface Policy	
Number of failed interfaces	障害が発生したモニタ対象インターフェイスの数がこの値を超えると、セキュリティ アプライアンスはフェールオーバーします。値の範囲は 1 ～ 250 です。
障害が発生したインターフェイスのパーセンテージ（Percentage of failed interfaces）	障害が発生したモニタ対象インターフェイスの数がこのパーセンテージを超えると、セキュリティ アプライアンスはフェールオーバーします。
Failover Poll Time	
Unit Failover	装置間での hello メッセージの間隔。値の範囲は 1 ～ 15 秒です。[単位をミリ秒に変更（Change units to msec）] オプションをオンにしている場合は 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を設定します。設定した時間内に受信しない場合、装置はピアの障害のテスト プロセスを開始します。値の範囲は 3 ～ 45 秒です。[msec] オプションをオンにしている場合は 800 ～ 999 ミリ秒です。[Unit Failover] の値の 3 倍より少ない値は入力できません。
Monitored Interface	インターフェイス間でのポーリングの間隔。値の範囲は 3 ～ 15 秒、またはミリ秒のオプションが選択されている場合は 500 ～ 999 ミリ秒です。

要素	説明
Interface Hold Time	データ インターフェイスが hello メッセージを受信する必要がある時間を設定します。この時間が過ぎると、ピアの障害が宣言されます。有効な値は 5 ～ 75 秒です。この値は少なくとも [Unit Failover] 値の 5 倍である必要があります。
リンクステート間隔（Link State Interval）	フェールオーバーペアの各 ASA がインターフェイスのリンクステートをチェックする間隔を設定します。デフォルトでは、リンクステート間隔の値は 500 ミリ秒です。polltime はカスタマイズできます。たとえば、polltime を 300 ミリ秒に設定すると、ASA ではインターフェイスの障害やトリガーのフェールオーバーをより早く検出できるようになります。有効な範囲は 300 ～ 799 ミリ秒です。 （注） [リンクステート間隔（Link State Interval）] は、ASA 9.7.1 以降で使用できます。
フェールオーバー グループ アクティブ/アクティブ モードでは、このテーブルには両方のフェールオーバー グループが一覧表示されます。いずれかのグループのフェールオーバーパラメータを編集するには、グループをリストで選択して、[Edit Row] ボタンをクリックして、[Edit Failover Group] ダイアログボックス （35 ページ）を開きます。	
MAC Address Mapping アクティブ/スタンバイ モードでは、このテーブルにはインターフェイスと仮想 MAC アドレスのマッピングが一覧表示されます。これは Security Manager の標準のテーブルです。テーブルの使用で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 インターフェイス マッピングを追加または編集するには、[Add Row] または [Edit Row] ボタンをクリックして、[Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （32 ページ）を開きます。	
Monitor Interface Configuration シングルコンテキスト モードでは、このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスのモニタリング用のスタンバイ IP アドレスを定義したり、インターフェイスのモニタリングをイネーブルまたはディセーブルにしたりするには、インターフェイスをリストから選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス （33 ページ）を開きます。	

要素	説明
管理 IP アドレス（Management IP Address） シングルコンテキストのトランスペアレントモードでは、このセクションには（[Management IP] ページで）デバイスに定義されている管理 IP アドレスとネットマスクが表示されます。これらの値は変更できません。	
スタンバイ（Standby）	スタンバイ装置の管理IPアドレスを入力します。このアドレスはプライマリ アドレスと同じサブネットにある必要があります。

[Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス

[Add Interface MAC Address] と [Edit Interface MAC Address] ダイアログボックスでは、フェールオーバー用に設定されている ASA、FWSM 3.x、PIX 7.x 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の仮想 MAC アドレスを定義できます（ASA 5505 デバイス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。この変更によりネットワーク トラフィックが中断される可能性があります。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 ペアはバーンドイン MAC アドレスを使用します。

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

ナビゲーション パス

[Add Interface MAC Address] と [Edit Interface MAC Address] ダイアログボックスは、 [Settings] ダイアログボックス （29 ページ）から開けます。

関連項目

- フェールオーバー ポリシー （13 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）
- [Edit Failover Group] ダイアログボックス （35 ページ）

フィールド リファレンス

表 8 : [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス

要素	説明
Physical Interface	フェールオーバー仮想 MAC アドレスを設定する物理インターフェイスを選択します。
MAC アドレス	
アクティブ インターフェイス（Active Interface）	アクティブ インターフェイスの仮想 MAC アドレスを 16 進数形式で入力します（0023.4567.89ab など）。
Standby Interface	スタンバイ インターフェイスの仮想 MAC アドレスを 16 進数形式で入力します（0023.4567.89ab など）。

[Edit Failover Interface Configuration] ダイアログボックス

[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モニタするかどうかを指定します。

（注） PPPoE にはフェールオーバー インターフェイスを設定できません。

ナビゲーション パス

[Edit Failover Interface Configuration] ダイアログボックスには、（ASA/PIX 7.0 以降では） [Settings] ダイアログボックス （29 ページ）、（FWSM では） [Advanced Settings] ダイアログボックス （21 ページ）からアクセスできます。また、シングルコンテキストのトランスペアレント モードで動作している ASA 8.4.1 以降のデバイスおよび個々の ASA/PIX セキュリティ コンテキストの [Failover] ページ自体からもアクセスできます。

関連項目

- フェールオーバー ポリシー （13 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）
- [Failover] ページ（FWSM） （17 ページ）
- [Edit Failover Group] ダイアログボックス （35 ページ）

フィールド リファレンス

表 9 : [Edit Failover Interface Configuration] ダイアログボックス

要素	説明
Interface Name	インターフェイスの名前。読み取り専用です。
Active IP Address	このインターフェイスのアクティブ IP アドレス。読み取り専用です。IP アドレスがインターフェイスで割り当てられていない場合、このフィールドはブランクです。たとえば、DHCP がインターフェイスでイネーブルの場合です。
Mask	アクティブ IP アドレスのサブネット マスク。読み取り専用です。IP アドレスがインターフェイスで割り当てられていない場合、このフィールドはブランクです。たとえば、DHCP がインターフェイスでイネーブルの場合です。
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。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。
このインターフェイスの障害をモニターする（Monitor this interface for failure）	このインターフェイスの障害をモニタするかどうかを指定します。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。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。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと（25 秒間）、そのインターフェイスでテストが開始します。モニター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。

要素	説明
ASR Group Number	このインターフェイスが非対称ルーティング グループの一部である場合、その ASR グループ番号を指定します。ASR グループ番号の有効な値は 1 ～ 32 です。 フェールオーバー設定の装置間で非対象ルーティング サポートを適切に機能させるためには、ステートフル フェールオーバーをイネーブルにする必要があります。

[Edit Failover Group] ダイアログボックス

[Edit Failover Group] ダイアログボックスを使用して、アクティブ/アクティブ フェールオーバー設定でセキュリティ コンテキストのグループのフェールオーバー パラメータを設定します。フェールオーバー グループへのコンテキストの割り当てについては、[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）または[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）を参照してください。

ナビゲーション パス

[Add Failover Group] ダイアログボックスには、PIX/ASA の [Settings] ダイアログボックス （29 ページ）または FWSM の [Advanced Settings] ダイアログボックス （21 ページ）からアクセスできます。

関連項目

- フェールオーバー ポリシー （13 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）
- [Failover] ページ（FWSM） （17 ページ）

フィールド リファレンス

表 10 : [Edit Failover Group] ダイアログボックス

要素	説明
Preferred Role	[Preferred Role]：同時に起動した場合や、[Preempt] オプションが選択されている場合、このフェールオーバー 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。[プライマリ（Primary）] または [セカンダリ（Secondary）] を選択します。 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間にトラフィックを分散させます。

要素	説明
Poll time interval for monitored interfaces	モニタされているインターフェイスのポーリング間隔を指定します。有効値の範囲は 3 ～ 15 秒（[msec] が選択されている場合は 500 ～ 999 ミリ秒）です。
保留時間（Hold Time）	グループが hello メッセージを受信する必要がある時間を指定します。この時間を経過すると、もう一方のグループの障害が宣言されます。有効な値は 5 ～ 75 秒です。
Preempt after Reboot	優先フェールオーバー デバイスがリブート後に引き継ぎを待機する秒数を指定します。この時間を経過すると、優先フェールオーバー デバイスは、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処理を引き継ぎます。有効な値は 0 ～ 1200 秒です。
Enable HTTP Replication	アクティブな HTTP セッションが、このフェールオーバー グループのスタンバイ デバイスにステートフル フェールオーバーの一部としてコピーされるかどうかを示します。HTTP レプリケーションを許可しない場合、HTTP 接続はフェールオーバー時に切断されます。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、[Failover] ページの HTTP レプリケーションの設定を上書きします。
Failover Criteria	このグループに対して障害が発生したインターフェイス基準を選択して、適切な値を指定します。 • [障害が発生したインターフェイスの数（Number of failed interfaces）]：この数のインターフェイスで障害が発生すると、フェールオーバーがトリガーされます。有効な値は 1 ～ 250 です。 • [障害が発生したインターフェイスのパーセンテージ（Percentage of failed interfaces）]：インターフェイスの総数に対してこのパーセンテージのインターフェイスで障害が発生すると、フェールオーバーがトリガーされます。有効な値は 1 ～ 100 です。
MAC Address Mapping このテーブルには、アクティブ MAC アドレスとスタンバイ MAC アドレスがマッピングされるインターフェイスが表示されます。	

[Failover] ページ（セキュリティ コンテキスト）

個々の ASA および PIX 7.0 以降のセキュリティコンテキストの [フェールオーバー（Failover）] ページには [インターフェイス設定（Interface Configuration）] テーブルが表示されます。このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。

テーブルでインターフェイスを選択して、[Edit Row] ボタンをクリックすると、[Edit Failover Interface Configuration] ダイアログボックス （33 ページ）が開きます。ここでは、スタンバイ

IP アドレスと ASR グループ番号を指定できます。また、インターフェイスのモニタリングをイネーブルまたはディセーブルにできます。

ASA 8.4.1 以降のデバイスにおける個々のトランスペアレントモード コンテキストの場合、[フェールオーバー（Failover）]ページには[ブリッジグループ設定（Bridge Group Configuration）]テーブルも表示されます。このテーブルには、現在定義されているすべてのフェールオーバー ブリッジ グループが一覧表示されます。

テーブルでエントリを選択して、[Edit Row] ボタンをクリックすると、[Edit Failover Bridge Group Configuration] ダイアログボックス （23 ページ）が開きます。ここでは、選択したブリッジ グループのスタンバイ IP アドレスを指定できます。

ナビゲーション パス

デバイスビューでセキュリティコンテキストを選択してから、デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）]** を選択します。

関連項目

- フェールオーバーについて （2 ページ）
- フェールオーバー ポリシー （13 ページ）
- ファイアウォール デバイスでのブリッジングについて

[Bootstrap Configuration for LAN Failover] ダイアログボックス

[Bootstrap Configuration for LAN Failover] ダイアログボックスでは、LAN フェールオーバー設定のプライマリおよびセカンダリ デバイスに適用できるブートストラップ設定が表示されます。

ナビゲーション パス

[Bootstrap Configuration for LAN Failover] ダイアログボックスには、[Failover] ページからアクセスできます。[Failover] ページの詳細については、次の項を参照してください。

- [Failover] ページ（PIX 6.3） （14 ページ）
- [Failover] ページ（FWSM） （17 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （24 ページ）

関連項目

- フェールオーバー ポリシー （13 ページ）
- アクティブ/スタンバイ フェールオーバー設定の追加手順 （12 ページ）

フィールド リファレンス

表 *11 : [Bootstrap Configuration for LAN Failover]* ダイアログボックス

要素	説明
プライマリ	プライマリ デバイスのブートストラップ設定が含まれています。プライマリ デバイスへのコンソール接続を開き、この設定を貼り付けて、プライマリ デバイスでフェールオーバーをアクティブにします。
セカンダリ（Secondary）	セカンダリ デバイスのブートストラップ設定が含まれています。プライマリ デバイスがアクティブになったあとに、セカンダリ デバイスへのコンソール接続を開き、次に、この設定を貼り付けて、セカンダリ デバイスでフェールオーバーをアクティブにします。

（注） アクティブ/アクティブ フェールオーバーの場合、ブートストラップ設定は、各フェールオーバー ピア デバイスのシステム コンテキストにだけ適用されます。

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