CHAPTER 6

マルチモードのインターフェイスの設定

この章では、物理イーサネット インターフェイスを設定してイネーブルにする方法、冗長インターフェイス ペアを作成する方法、およびシステム コンフィギュレーションにサブインターフェイスを追加する方法について説明します。ファイバと銅線の両方のイーサネット ポートがある場合（ASA 5510 以降のシリーズの適応型セキュリティ アプライアンスに搭載されている 4GE SSM など）、この章ではインターフェイス メディア タイプの設定方法について説明します。

また、この章では、コンテキストに割り当てられているインターフェイス（物理、冗長、またはサブインターフェイス）ごとに、名前、セキュリティ レベル、および IP アドレス（ルーテッド ファイアウォール モードのみ）の設定方法を説明します。

（注） シングルコンテキスト モードでのインターフェイスの設定方法については、第 5 章「インターフェイスの設定」を参照してください。

この章には、次の項があります。

システム コンフィギュレーションのインターフェイスの設定

マルチコンテキスト モードでは、物理インターフェイス パラメータを設定し、システム実行スペースに冗長インターフェイスとサブインターフェイスを追加します。

この章には、次の項があります。

（注）　フェールオーバーを使用する場合、Failover: Setup タブで、専用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る必要があります。また、オプションでステートフル フェールオーバー用のインターフェイスも割り当てます（フェールオーバーとステート トラフィックには同じインターフェイスを使用できますが、分けることをお勧めします）。物理インターフェイス、サブインターフェイス、または冗長インターフェイスは、コンテキストに割り当てられていなければ、フェールオーバーとステート リンクに使用できます。サブインターフェイスを使用するには、物理インターフェイスをコンテキストに割り当てないでください。

物理インターフェイスの設定

この項では、物理インターフェイス設定値を設定する方法について説明します。次の項目を取り上げます。

物理インターフェイスの概要

この項では、物理インターフェイスについて説明します。次の項目を取り上げます。

物理インターフェイスのデフォルトの状態

デフォルトでは、物理インターフェイスはすべてシャットダウンされています。トラフィックが物理インターフェイス（単独か冗長インターフェイス ペアの一部）またはサブインターフェイスを通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、インターフェイス（物理、冗長、またはサブインターフェイス）をコンテキストに割り当てると、デフォルトでインターフェイスはそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、まず次の手順に従ってその物理インターフェイスをシステム コンフィギュレーションでイネーブルにする必要があります。

デフォルトでは、銅線（RJ-45）インターフェイスの速度と二重通信は自動ネゴシエーションに設定されています。

コネクタ タイプ

ASA 5550 適応型セキュリティ アプライアンスと、ASA 5510 以降の適応型セキュリティ アプライアンスの 4GE SSM には、銅線 RJ-45 とファイバ SFP という 2 つのコネクタ タイプがあります。デフォルトは RJ-45 です。

ファイバ SFP コネクタを使用するには、メディア タイプを SFP に設定する必要があります。ファイバ インターフェイスの速度は固定で、二重通信はサポートされませんが、インターフェイスでリンク パラメータのネゴシエーションを行う（デフォルト）か行わないかを設定できます。

Auto-MDI/MDIX 機能

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、自動ネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度または二重通信のいずれかを自動ネゴシエーションに設定する必要があります。速度と二重通信の両方に固定値を明示的に設定して、両方の設定に関する自動ネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

物理インターフェイスの設定とイネーブル化

物理インターフェイスを設定してイネーブルにするには、次の手順を実行します。

ステップ 1　Configuration > Device List ペインで、アクティブなデバイスの IP アドレスの下にある **System** をダブルクリックします。

ステップ 2　Context Management > Interfaces ペインで、設定する物理インターフェイスをクリックして、**Edit** をクリックします。

ステップ 3　インターフェイスをイネーブルにするには、**Enable Interface** チェックボックスをオンにします。

ステップ 4　説明を追加するには、Description フィールドにテキストを入力します。

ステップ 5　（オプション）メディア タイプ、二重通信、および速度を設定するには、**Configure Hardware Properties** ボタンをクリックします。

a. ASA 5550 適応型セキュリティ アプライアンスまたは 4GE SSM を使用している場合は、Media Type ドロップダウン リストから **RJ-45** または **SFP** を選択できます。

デフォルトは RJ-45 です。

b. RJ-45 インターフェイスに二重通信を設定するには、Duplex ドロップダウン リストからインターフェイスに応じて Full、Half、または Auto を選択します。

c. 速度を設定するには、Speed ドロップダウン リストから値を選択します。

指定できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、常に 1000 Mbps です。また、速度を Negotiate または Nonegotiate に設定できます。Negotiate（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。Nonegotiate では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。
Auto-MDI/MDIX は、自動ネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度または二重通信のいずれかを自動ネゴシ

エーションに設定する必要があります。速度と二重通信の両方に固定値を明示的に設定して、両方の設定に関する自動ネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

d. **OK** をクリックして Hardware Properties の変更を受け入れます。

ステップ 6　**OK** をクリックして Interface の変更を受け入れます。

冗長インターフェイスの設定

論理冗長インターフェイスは、アクティブとスタンバイからなる物理インターフェイスのペアです。アクティブ インターフェイスに障害が発生すると、スタンバイ インターフェイスがアクティブになり、トラフィックの受け渡しを開始します。冗長インターフェイスを設定してセキュリティ アプライアンスの信頼性を高めることができます。この機能は、デバイス レベルのフェールオーバーとは別個のものですが、必要であればフェールオーバーと共に冗長インターフェイスも設定できます。最大 8 個の冗長インターフェイス ペアを設定できます。

後続のセキュリティ アプライアンスのコンフィギュレーションはすべて、メンバーの物理インターフェイスではなく論理冗長インターフェイスを参照します。

この項では、冗長インターフェイスを設定する方法について説明します。次の項目を取り上げます。

- 冗長インターフェイスの概要（P. 6-4）
- 冗長インターフェイスの追加（P. 6-5）

冗長インターフェイスの概要

この項では、冗長インターフェイスの概要について説明します。次の項目を取り上げます。

- 冗長インターフェイスのデフォルトの状態（P. 6-4）
- 冗長インターフェイスとフェールオーバーのガイドライン（P. 6-4）
- 冗長インターフェイスの MAC アドレス（P. 6-5）
- 冗長インターフェイスで物理インターフェイスを使用するためのガイドライン（P. 6-5）

冗長インターフェイスのデフォルトの状態

追加された冗長インターフェイスは、デフォルトでイネーブルになっています。ただし、トラフィックを通過させるには、メンバー インターフェイスもイネーブルにする必要があります。

冗長インターフェイスとフェールオーバーのガイドライン

メンバー インターフェイスを追加する場合は、次のガイドラインに従ってください。

- フェールオーバーまたはステート リンクに冗長インターフェイスを使用する場合、プライマリ装置だけでなくセカンダリ装置の基本コンフィギュレーションの一部として冗長インターフェイスを設定する必要があります。
- フェールオーバーまたはステート リンクに冗長インターフェイスを使用する場合、2 つの装置の間にスイッチまたはハブを設置する必要があります。2 つの装置を直接接続することはできません。スイッチまたはハブがない場合、プライマリ装置のアクティブなポートをセカンダリ装置のスタンバイ ポートに直接接続することもできます。
- フェールオーバーが発生しているかどうか冗長インターフェイスを監視できます。必ず論理冗長インターフェイス名を参照してください。

- アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーを監視していると、冗長インターフェイスに障害が発生したことは表示されません。物理インターフェイスの両方に障害が発生した場合だけ、冗長インターフェイスに障害が発生したことが表示されます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスは追加された最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーション内のメンバー インターフェイスの順序を変更すると、使用する MAC アドレスは、変更後の順序で先頭になるインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます（P.6-13 の「インターフェイス パラメータの設定」または P.9-22 の「セキュリティ コンテキストの設定」を参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

冗長インターフェイスで物理インターフェイスを使用するためのガイドライン

メンバー インターフェイスを追加する場合は、次のガイドラインに従ってください。

- 両方のメンバー インターフェイスの物理タイプが同じである必要があります。たとえば、両方ともイーサネットでなければなりません。
- 冗長インターフェイスに物理インターフェイスを追加すると、名前、IP　アドレス、およびセキュリティ レベルが削除されます。

注意　すでにコンフィギュレーションに設定されている物理インターフェイスを使用している場合、名前を削除するとそのインターフェイスを参照しているコンフィギュレーションはすべて消去されます。

- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

冗長インターフェイスの追加

最大 8 個の冗長インターフェイス ペアを設定できます。冗長インターフェイスを設定するには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、Configuration > Device List ペインで、アクティブなデバイスの IP アドレスの下にある **System** をダブルクリックします。

ステップ 2　Context Management > Interfaces ペインで、**Add > Redundant Interface** をクリックします。

ステップ 3　Redundant ID フィールドで、1 ～ 8 の整数を入力します。

ステップ 4　Primary Interface ドロップダウン リストから、プライマリにする物理インターフェイスを選択します。

サブインターフェイスを持たず、まだコンテキストに割り当てられていないインターフェイスを必ず選択してください。

ステップ 5　Secondary Interface ドロップダウン リストから、セカンダリにする物理インターフェイスを選択します。

ステップ 6　インターフェイスがまだイネーブルでない場合は、**Enable Interface** をオンにします。

このインターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このボックスをオフにします。

ステップ 7　説明を追加するには、Description フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチコンテキスト モードでは、システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクに設定すると、入力した説明は固定の説明に上書きされます。

ステップ 8　**OK** をクリックします。

VLAN サブインターフェイスと 802.1Q トランキングの設定

この項では、サブインターフェイスを設定する方法について説明します。次の項目を取り上げます。

サブインターフェイスの概要

サブインターフェイスを使用すると、物理インターフェイスまたは冗長インターフェイスを、異なる VLAN ID でタグ付けした複数の論理インターフェイスに分割できます。1 つ以上の VLAN サブインターフェイスを持つインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN によってトラフィックを物理インターフェイス上で分割できるため、物理インターフェイスやセキュリティ アプライアンスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチコンテキスト モードで特に便利です。

ここでは、次の項目について説明します。

サブインターフェイスのデフォルトの状態

追加されたサブインターフェイスは、デフォルトでイネーブルになっています。ただし、トラフィックを通過させるためには物理インターフェイスまたは冗長インターフェイスもイネーブルにする必要があります（物理インターフェイスをイネーブルにするには、P.6-2 の「物理インターフェイスの設定」を参照。冗長インターフェイスをイネーブルにするには、P.6-4 の「冗長インターフェイスの設定」を参照）。

最大サブインターフェイス数

使用するプラットフォームで許容されるサブインターフェイス数を判別するには、付録 A「機能のライセンスと仕様」を参照してください。

サブインターフェイスの追加

サブインターフェイスを追加して VLAN を割り当てるには、次の手順を実行します。

ステップ 1　まだシステム コンフィギュレーション モードに入っていない場合、Configuration > Device List ペインで、アクティブなデバイスの IP アドレスの下にある **System** をダブルクリックします。

ステップ 2　Context Management > Interfaces ペインで、**Add > Interface** をクリックします。

ステップ 3　Hardware Port ドロップダウン リストから、サブインターフェイスを追加する物理インターフェイスを選択します。

ステップ 4　インターフェイスがまだイネーブルでない場合は、**Enable Interface** をオンにします。

このインターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このボックスをオフにします。

ステップ 5　VLAN ID フィールドで、1 ～ 4095 の VLAN ID を入力します。

一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。マルチコンテキスト モードでは、VLAN はシステム コンフィギュレーションのみに設定できます。

ステップ 6　Subinterface ID フィールドに、サブインターフェイス ID を 1 ～ 4294967293 の整数で入力します。

許容されるサブインターフェイス数は、プラットフォームによって異なります。ID は、設定した後で変更することはできません。

ステップ 7　（オプション）Description フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。マルチコンテキスト モードでは、システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステートリンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクに設定すると、入力した説明は固定の説明に上書きされます。

ステップ 8　**OK** をクリックします。

Interface (System) のフィールドの説明

ここでは、次の項目について説明します。

Interfaces (System)

フィールド

- Interface：インターフェイス ID を表示します。すべての物理インターフェイスが自動的に一覧表示されます。サブインターフェイスは、インターフェイス ID の後の *.n* で示されます。*n* はサブインターフェイス番号です。
- Enabled：インターフェイスがイネーブルかどうかを Yes または No で示します。

  デフォルトでは、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブインターフェイスまたは冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、インターフェイスをコンテキストに割り当てると、デフォルトでインターフェイスはそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。
- Redundant：このインターフェイスが冗長インターフェイスかどうかを Yes または No で示します。
- Member：このインターフェイスが冗長インターフェイスのメンバーかどうかを Yes または No で示します。
- VLAN：サブインターフェイスに割り当てられた VLAN を示します。物理インターフェイスおよび冗長インターフェイスには「native」が表示されます。これはタグがないインターフェイスという意味です。
- Description：説明を表示します。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。この説明は編集できません。
- Add > Interface：サブインターフェイスを追加します。詳細については、P.6-6 の「VLAN サブインターフェイスと 802.1Q トランキングの設定」を参照してください。
- Add > Redundant Interface：冗長インターフェイスを追加します。詳細については、P.6-4 の「冗長インターフェイスの設定」を参照してください。
- Edit：選択したインターフェイスを編集します。
- Delete：選択したサブインターフェイスまたは冗長インターフェイスを削除します。物理インターフェイスまたはコンテキストで割り当てたインターフェイスは削除できません。フェールオーバー リンクまたはステート リンクに割り当てたインターフェイス（Failover: Setup タブを参照）は、このペインで削除できません。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	—	•

Add/Edit Interface (System)

フィールド

- Hardware Port：サブインターフェイスを追加すると、イネーブル状態の物理インターフェイスを選択でき、そこにサブインターフェイスが追加されます。インターフェイス ID が表示されない場合、インターフェイスがイネーブルになっているかどうかを確認してください。
- Configure Hardware Properties：物理インターフェイスでは、Hardware Properties (System) ダイアログボックスが開き、メディア タイプ、速度、および二重通信を設定できます。
- Enable Interface：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。

  デフォルトでは、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブインターフェイスまたは冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、インターフェイスをコンテキストに割り当てると、デフォルトでインターフェイスはそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。
- VLAN ID：サブインターフェイスでは、1 ～ 4095 の範囲の番号で VLAN ID を設定します。一部の VLAN ID は接続スイッチ用に予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。マルチコンテキスト モードでは、VLAN はシステム コンフィギュレーションのみに設定できます。
- Subinterface ID：サブインターフェイス ID を 1 ～ 4294967293 の範囲の整数で設定します。使用できるサブインターフェイスの数は、使用するプラットフォームによって異なります。ID は、設定した後で変更することはできません。
- Description：（オプション）240 文字以内で入力します。1 行で入力し、改行はできません。システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクに設定すると、入力した説明は固定の説明に上書きされます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	—	•

Add/Edit Redundant Interface (System)

フィールド

- Redundant ID：冗長インターフェイス ID を 1 ～ 8 で設定します。
- Primary Interface：プライマリ インターフェイスを設定します。このインターフェイスはデフォルトでアクティブになります。
- Secondary Interface：セカンダリ インターフェイスを設定します。
- Enable Interface：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。

  デフォルトでは、冗長インターフェイスはイネーブルになっています。イネーブルになっている冗長インターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、インターフェイスをコンテキストに割り当てると、デフォルトでインターフェイスはそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。
- Description：（オプション）240 文字以内で入力します。1 行で入力し、改行はできません。システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクに設定すると、入力した説明は固定の説明に上書きされます。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	—	•

Hardware Properties (System)

フィールド

- Hardware Port：表示のみ。インターフェイス ID を表示します。
- Media Type：メディア タイプを RJ45 または SFP に設定します。デフォルトは RJ45 です。
- Duplex：インターフェイスの二重通信オプションを一覧表示します。Full、Half、Auto があり、インターフェイス タイプによって異なります。
- Speed：インターフェイスの速度オプションを一覧表示します。指定できる速度は、インターフェイス タイプによって異なります。SFP インターフェイスでは、常に 1000 Mbps です。また、速度を Negotiate または Nonegotiate に設定できます。Negotiate（デフォルト）ではリンク ネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。Nonegotiate では、リンク パラメータのネゴシエーションを行いません。ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、自動ネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度または二重通信のいずれかを自動ネゴシエーションに設定する必要があります。速度と二重通信の両方に固定値を明示的に設定して、両方の設定に関する自動ネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	—	•

インターフェイスのコンテキストへの割り当て

インターフェイスをコンテキストに割り当てるには、P.9-22 の「セキュリティ コンテキストの設定」を参照してください。

各コンテキスト内でのインターフェイス パラメータの設定

各コンテキスト内で、各インターフェイスの名前、セキュリティ レベル、および IP アドレスを設定します。同じセキュリティ レベルの通信をイネーブルにすることもできます。ここでは、次の項目について説明します。

インターフェイス パラメータの概要

この項では、インターフェイス パラメータについて説明します。次の項目を取り上げます。

インターフェイスのデフォルトの状態

マルチコンテキスト モードでは、システム実行スペース内でのインターフェイスの状態に関係なく、割り当てられているインターフェイスはすべてデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを追加できるようにするには、インターフェイスをシステム実行スペース内でもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスはデフォルトで次の状態になっています。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過できるようにするには、メンバーの物理インターフェイスもイネーブルにする必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過できるようにするには、物理インターフェイスもイネーブルにする必要があります。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに名前「inside」を付けて、明示的なセキュリティ レベルを設定しないと、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します。

（注）　インターフェイスのセキュリティ　レベルを変更したときに、既存のインターフェイスがタイムアウトするまで待たずに新しいセキュリティ情報を使用したい場合は、**clear local-host** コマンドを使用して接続をクリアできます。

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 を割り当てる場合があります。DMZ などその他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、

P.6-15 の「同じセキュリティ レベルの通信のイネーブル化」を参照してください。

各レベルは、次の動作を制御します。

- ネットワーク アクセス：デフォルトでは、高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイス（発信）へのアクセスは、暗黙的に許可されます。高位のセキュリティ インターフェイス上のホストは、それより低いセキュリティ インターフェイス上のホストすべてにアクセスできます。アクセスは、インターフェイスにアクセスリストを適用すると制限できます。

  同じレベルのセキュリティ インターフェイスの場合、同じセキュリティ レベルまたはそれより低いレベルの他のインターフェイスへのアクセスは、暗黙的に許可されます。
- 検査エンジン：一部のアプリケーション検査エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイスの場合、検査エンジンはどちらの方向のトラフィックにも適用されます。
  - NetBIOS 検査エンジン：発信接続のみに適用されます。
  - SQL*Net 検査エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続のみセキュリティ アプライアンスを通過することが許可されます。
- フィルタリング：HTTP（S）フィルタリングおよび FTP フィルタリングは、発信接続（高位レベルから低位レベルへの接続）に対してのみ適用されます。

  同じセキュリティ レベルのインターフェイスの場合、どちらの方向のトラフィックにもフィルタリングが適用できます。
- NAT 制御：NAT 制御をイネーブルにする場合、低位のセキュリティ インターフェイス（外部）上のホストにアクセスする高位のセキュリティ インターフェイス（内部）上のホストに NAT を設定する必要があります。

  NAT 制御がない場合、または同じレベルのセキュリティ インターフェイスの場合は、任意のインターフェイス間で NAT を使用するように選択することも、NAT を使用しないように選択することもできます。外部インターフェイスに対して NAT を設定すると、特殊なキーワードが必要になる場合があることに留意してください。
- **established** コマンド：このコマンドを使用すると、高位レベルのホストから低位レベルのホストに接続がすでに確立されている場合に、低位のセキュリティのホストから高位のセキュリティのホストへのリターン接続が許可されます。

  同じセキュリティ レベルのインターフェイスでは、両方向に対して **established** コマンドが設定できます。

インターフェイス パラメータの設定

インターフェイスを追加または編集するには、次の手順を実行します。

ステップ 1　Configuration > Device List ペインで、アクティブなデバイスの *IP アドレス* > Contexts の下にあるコンテキスト名をクリックします。

ステップ 2　Device Setup > Interfaces ペインで、設定するインターフェイスをクリックし、**Edit** をクリックします。

Add/Edit Interface ダイアログボックスが、General タブが選択された状態で表示されます。

ステップ 3　Interface Name フィールドで、名前を 48 文字以内で入力します。

ステップ 4　Security level フィールドで、0（最小）～ 100（最大）のレベルを入力します。

詳細については、P.6-12 の「デフォルトのセキュリティ レベル」を参照してください。

ステップ 5　（オプション）このインターフェイスを管理専用インターフェイスとして設定するには、**Dedicate this interface to management-only** をオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。

ステップ 6　インターフェイスがまだイネーブルでない場合は、**Enable Interface** をオンにします。

このインターフェイスはデフォルトでイネーブルになっています。ディセーブルにするには、このボックスをオフにします。

ステップ 7　IP アドレスを設定するには、次のいずれかのオプションを使用します。

ルーテッド ファイアウォール モードでは､すべてのインターフェイスの IP アドレスを設定します。透過ファイアウォール モードでは、インターフェイスごとに IP アドレスを設定するのではなく、セキュリティ アプライアンス全体またはコンテキスト全体に IP アドレスを設定します。トラフィックを通過させない Management 0/0 管理専用インターフェイスの場合は例外となります。透過ファイアウォール モードでセキュリティ アプライアンス全体またはコンテキスト管理 IP アドレスを設定するには、管理 IP アドレス ペインを参照してください。Management 0/0 インターフェイスまたはサブインターフェイスの IP アドレスを設定するには、次の手順に従います。

フェールオーバーで使用する場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP はサポートされません。Configuration > Device Management > High Availability > Failover > Interfaces タブで、スタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、**Use Static IP** をクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、**Obtain Address via DHCP** をクリックします。
  a. （オプション）DHCP サーバからデフォルト ルートを取得するには、**Obtain Default Route Using DHCP** をオンにします。
  b. （オプション）リースを更新するには、**Renew DHCP Lease** をクリックします。

ステップ 8　（オプション）Description フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。システムの説明はコンテキストの説明に依存しません。フェールオーバーまたはステート リンクでは、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」など固定の説明が表示されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクに設定すると、入力した説明は固定の説明に上書きされます。

ステップ 9　（オプション）MTU を設定するには、**Advanced** タブをクリックして、MTU フィールドに 300 ～ 65,535 バイトの値を入力します。

デフォルトは 1500 バイトです。

ステップ 10　（オプション）MAC アドレスをこのインターフェイスに手動で割り当てるには、Advanced タブで、Active Mac Address フィールドに H.H.H 形式（H は 16 ビットの 16 進数）で MAC アドレスを入力します。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

フェールオーバーを使用する場合、Standby Mac Address フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新たなアクティブ装置はアクティブ MAC アドレスを使用して、ネットワークの中断を最小限に抑え、元のアクティブ装置はスタンバイ アドレスを使用します。

デフォルトでは、物理インターフェイスは焼き付け済み MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じ焼き付け済み MAC アドレスを使用します。冗長インターフェイスは追加された最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーション内のメンバー インターフェイスの順序を変更すると、使用する MAC アドレスは、変更後の順序で先頭になるインターフェイスの MAC アドレスと一致するように変更されます。このフィールドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバー インターフェイスの MAC アドレスに関係なく、割り当てられた MAC アドレスが使用されます。

コンテキスト間でインターフェイスを共有する場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すれば、セキュリティ アプライアンスで、該当するコンテキストへのパケットの分類が容易になります。固有の MAC アドレスが割り当てられていない共有インターフェイスも使用できますが、いくつか制限があります。詳細については、P.9-3 の「セキュリティ アプライアンスによるパケットの分類方法」を参照してください。コンテキストの共有インターフェイス用に手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、P.9-25 の「Security Contexts」を参照してください。MAC アドレスを自動生成する場合、このオプションを使用すれば生成されたアドレスを上書きできます。

共有しないインターフェイスについては、サブインターフェイスに固有の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーは MAC アドレスに基づいてアクセス コントロールを行っている場合があります。

ステップ 11　**OK** をクリックします。

同じセキュリティ レベルの通信のイネーブル化

デフォルトでは、セキュリティ レベルが同じインターフェイス同士は通信できません。同じセキュリティのインターフェイス間の通信を許可すると、101 を超える通信インターフェイスを設定できます。各インターフェイスで異なるセキュリティ レベルを使用したときに、同じセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

（注）　NAT 制御をイネーブルにした場合、同じセキュリティ レベルのインターフェイス間に NAT を設定する必要はありません。

同じセキュリティ レベルを持つインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。

同じインターフェイスに接続されているホスト間の通信をイネーブルにすることもできます。

- 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにするには、Configuration > Interfaces ペインで、**Enable traffic between two or more interfaces which are configured with same security level** をオンにします。
- 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、**Enable traffic between two or more hosts connected to the same interface** をオンにします。

Interface (Context) のフィールドの説明

ここでは、次の項目について説明します。

Interfaces (Context)

フィールド

- Interface：インターフェイス ID を表示します。割り当てられているすべてのインターフェイスが自動的に一覧表示されます。サブインターフェイスは、インターフェイス ID の後の *.n* で示されます。*n* はサブインターフェイス番号です。冗長インターフェイスは Redundant*n* と呼ばれます。
- Name：インターフェイスの名前を表示します。
- Enabled：インターフェイスがイネーブルかどうかを Yes または No で示します。デフォルトでは、すべてのインターフェイスはコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。
- Security Level：インターフェイスのセキュリティ レベルを 0 ～ 100 の範囲で示します。デフォルトのセキュリティ レベルは 0 です。
- IP Address：IP アドレスが表示されます。透過モードの場合「native」が表示されます。透過モードのインターフェイスは IP アドレスを使用しません。IP アドレスをコンテキストまたはセキュリティ アプライアンスに設定するには、管理 IP アドレス ペインを参照してください。
- Subnet Mask：ルーテッド モードのみ。サブネット マスクを表示します。
- Management Only：インターフェイスにセキュリティ アプライアンスへの、管理専用のトラフィックを許可する場合を示します。
- MTU：MTU を表示します。デフォルトでは、MTU は 1500 です。
- Active MAC Address：アクティブな MAC アドレスを示します。Edit Interface > Advanced (Context) タブで手動で割り当てると表示されます。
- Standby MAC Address：スタンバイ MAC アドレス（フェールオーバー用）を示します。手動で設定すると表示されます。
- Description：説明を表示します。
- Add：*適用されません。*サブインターフェイスと冗長インターフェイスは、システム実行スペースでのみ追加できます。
- Edit：選択したインターフェイスを編集します。
- Delete：*適用されません。* サブインターフェイスと冗長インターフェイスは、システム実行スペースでのみ削除できます。
- Enable traffic between two or more interfaces which are configured with same security levels：セキュリティ レベルが同じインターフェイス間の通信をイネーブルにします。同じセキュリティ レベルを持つインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。
- Enable traffic between two or more hosts connected to the same interface：同一インターフェイスの送受信トラフィックをイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	•	—

Edit Interface > General (Context)

フィールド

- Hardware Port：表示のみ。インターフェイス ID を表示します。
- Enable Interface：インターフェイスをイネーブルにすると、トラフィックが通過できるようになります。さらに、トラフィックがセキュリティ ポリシーに従って通過できるように、IP アドレス（ルーテッド モードの）と名前を事前に設定する必要があります。デフォルトでは、インターフェイスはコンテキスト内でイネーブルになっています。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。
- Interface Name：インターフェイス名を 48 文字以内で設定します。
- Dedicate this interface to management only：インターフェイスを設定してセキュリティ アプライアンスへのトラフィックだけを許可します。通過トラフィックは許可しません。
- Security Level：セキュリティ レベルを 0（最低）～ 100（最高）の範囲で設定します。セキュリティ アプライアンスは、内部インターフェイスから外部インターフェイス（低いセキュリティ レベル）へトラフィックを自由に流すことを許可します。他の多くのセキュリティ機能も、それぞれのインターフェイスの相対セキュリティ レベルに影響されます。
- IP Address：ルーテッド モードのみ。マルチコンテキスト モードでは、IP アドレスをコンテキスト コンフィギュレーションに設定します。
  - Use Static IP：IP アドレスを手動で設定します。

    IP Address：IP アドレスを設定します。

    Subnet Mask：サブネット マスクを設定します。
  - Obtain Address via DHCP：DHCP から IP アドレスをダイナミックに設定します。

    Obtain Default Route Using DHCP：デフォルト ルートを DHCP サーバから取得します。デフォルトのスタティック ルートの設定が不要になります。

    Renew DHCP Lease：DHCP のリース期間を更新します。
- Description：（オプション）240 文字以内で入力します。1 行で入力し、改行はできません。マルチコンテキスト モードでは、システムの説明はコンテキストの説明に依存しません。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	•	—

Edit Interface > Advanced (Context)

フィールド

- MTU：300 ～ 65,535 バイトの範囲で MTU を設定します。デフォルトは 1500 バイトです。マルチコンテキスト モードでは、MTU をコンテキスト コンフィギュレーションに設定します。
- Mac Address Cloning：MAC アドレスを手動で割り当てます。

  デフォルトでは、物理インターフェイスは焼き付け済み MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じ焼き付け済み MAC アドレスを使用します。

  マルチコンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すれば、セキュリティ アプライアンスで、該当するコンテキストへのパケットの分類が容易になります。固有の MAC アドレスが割り当てられていない共有インターフェイスも使用できますが、いくつか制限があります。詳細については、P.9-3 の「セキュリティ アプライアンスによるパケットの分類方法」を参照してください。コンテキストの共有インターフェイス用に手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、P.9-25 の「Security Contexts」を参照してください。MAC アドレスを自動生成する場合、このオプションを使用すれば生成されたアドレスを上書きできます。

  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 モードでの未共有インターフェイスの場合、固有の MAC アドレスをサブインターフェイスに割り当てることができます。たとえば、サービス プロバイダーは MAC アドレスに基づいてアクセス コントロールを行っている場合があります。

  - Active Mac Address：MAC アドレスを H.H.H 形式でインターフェイスに割り当てます。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。
  - Standby Mac Address：フェールオーバーで使用する場合は、スタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新たなアクティブ装置はアクティブ MAC アドレスを使用して、ネットワークの中断を最小限に抑え、元のアクティブ装置はスタンバイ アドレスを使用します。

モード

次の表に、この機能を使用できるモードを示します。

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
•	•	—	•	—