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、およびシステム設定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。

この章では、コンテキストに割り当てられている各インターフェイス（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 モードでインターフェイスを設定するには、第 5 章「インターフェイスの設定」を参照してください。

この章は、次の項で構成されています。

システム設定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。

この章は、次の項で構成されています。

（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を割り当てます。（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

物理インターフェイスは、デフォルトではすべてシャットダウンされます。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、インターフェイスはデフォルトで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、まずこの手順に従って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、オートネゴシエーションに設定されます。

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 の 2 つのコネクタ タイプがあります。RJ-45 がデフォルトです。

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 インターフェイスでは、速度は固定であり、二重通信はサポートされていませんが、インターフェイスをリンク パラメータ ネゴシエーションあり（デフォルト）またはネゴシエーションなしに設定することができます。

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、デフォルトのオート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、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネー

ブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、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およびイネーブル化

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、[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　（任意）メディア タイプ、デュプレックス、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。

RJ-45 がデフォルトです。

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 タイプに応じて [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。

使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、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 シリーズの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、デフォルトのオート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、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、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の物理インターフェイスからなるペアです。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。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、必要な場合はフェールオーバーととも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。

その後のすべてのセキュリティ アプライアンス コンフィギュレーションは、メンバ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を説明します。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.6-4）
- 「冗長インターフェイスで使用する場合の物理インターフェイスのガイドライン」（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います。

- フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、プライマリ ユニットに加えてセカンダリ ユニット上の基本的な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 リンク用に冗長インターフェイスを使用する場合は、2 つのユニット間にスイッチまたはハブを配置する必要があります。両ユニットは直接接続できません。スイッチやハブがなくても、プライマリ ユニット上のアクティブ ポートをセカンダリ ユニット上のスタンバイ ポートに直接接続できる場合もあります。
- 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モニタできます。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モニタしているときには、冗長インターフェイスで障害が発生しているように見えません。冗長インターフェイスで障害が発生しているように見えるのは、両方の物理インターフェイスで障害が発生したときだけです。

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、最初に追加された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でメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になった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 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（「インターフェイス パラメータの設定」（P.6-12）または「セキュリティ コンテキストの設定」（P.9-20）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使用する場合の物理インターフェイスのガイドライン

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います。

- 両方のメンバ インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。
- 物理インターフェイスを冗長インターフェイスに追加すると、名前、IP アドレス、およびセキュリティ レベルは削除されます。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

- 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。

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 モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。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 リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

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、1 つの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 でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上ある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 では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはセキュリティ 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。

この項では、次のトピックについて取り上げます。

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のイネーブル化については、「物理インターフェイスの設定」（P.6-2）を参照してください。冗長インターフェイスのイネーブル化については、「冗長インターフェイスの設定」（P.6-3）を参照してください）。

最大サブインターフェイス数

プラットフォームに許容されるサブインターフェイスの数を決定するには、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、そのサブインターフェイスに 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。

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] フィールドに、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 モードの場合、VLAN はシステム設定でしか設定できません。

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。

許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

ステップ 7　（任意）[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 モードの場合、システムの説明とコンテキストの説明に関係はありません。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。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 リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

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

この項では、次のトピックについて取り上げます。

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 とそれに続く ***.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であるかどうか（[Yes] または [No]）を示します。

  物理インターフェイスは、デフォルトではすべてシャットダウンされます。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、インターフェイスはデフォルトで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、それ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]：インターフェイスが冗長インターフェイスであるかどうか（[Yes] または [No]）を示します。
- [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であるかどうか（[Yes] または [No]）を示します。

- [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 リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。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、「VLAN サブインターフェイスと 802.1Q トランキングの設定」（P.6-6）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、「冗長インターフェイスの設定」（P.6-3）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 リンクとしてインターフェイスを割り当てた場合（[[Failover]: [Setup]] タブを参照）は、そのインターフェイスをこのペインで削除することはできません。

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
•	•	—	—	•

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場合、イネーブル状態の任意の物理インターフェイスをサブインターフェイスの追加先として選択できます。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、およびデュプレックスを設定できます。
- [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。

  物理インターフェイスは、デフォルトではすべてシャットダウンされます。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、インターフェイスはデフォルトで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、それ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 モードの場合、VLAN はシステム設定でしか設定できません。
- [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。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。
- [Description]：オプションの説明を 240 文字以内で入力します。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 リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。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 リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

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
•	•	—	—	•

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 の範囲で設定します。
- [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、インターフェイスはデフォルトで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、それ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]：オプションの説明を 240 文字以内で入力します。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 リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE

Failover Interface」などの固定の値になります。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 リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

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
•	•	—	—	•

Hardware Properties (System)

フィールド

- [Hardware Port]：*表示専用*。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。デフォルトの設定は RJ45 です。
- [Duplex]：インターフェイスのデュプレックス オプションが一覧表示されます。インターフェイス タイプに応じて [Full]、[Half]、または [Auto] があります。
- [Speed]：インターフェイスの速度オプションが表示されます。使用できる速度は、インターフェイス タイプによって異なります。常に 1000 Mbps である SFP インターフェイスでは、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 シリーズの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、デフォルトのオート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、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

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
•	•	—	—	•

コンテキストへのインターフェイスの割り当て

インターフェイスをコンテキストに割り当てるには、「セキュリティ コンテキストの設定」（P.9-20）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。この項では、次のトピックについて取り上げます。

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かかわらず、すべての割り当て済みのインターフェイスが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通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。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、それ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、インターフェイスのデフォルトの状態は次のとおりです。

- 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するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- 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するためには、物理インターフェイスもイネーブルになっている必要があります。

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、明示的にセキュリティ 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、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**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 が割り当てられる場合があります。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、「同じセキュリティ レベルの通信のイネーブル化」（P.6-14）を参照してください。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション 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間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション 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、着信データ接続だけがセキュリティ 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) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。

- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り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間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

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 address] > [Contexts] の下にあるコンテキスト名をダブルクリックします。

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] フィールドに、名前を 48 文字以内で入力します。

ステップ 4　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「デフォルトのセキュリティ レベル」（P.6-11）を参照してください。

ステップ 5　（任意）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。

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に対する IP アドレスを設定します。トランスペアレント 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、全体 セキュリティ アプライアンス 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。トランスペアレント ファイアウォール モードのセキュリティ アプライアンス全体またはコンテキスト全体の管理 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、この手順を使用します。

フェールオーバーとともに使用する場合は、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.** （任意）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.** （任意）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　（任意）[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 リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。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 リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

ステップ 9　（任意）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　（任意）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 MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、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、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古い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バーンドイン 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バーンドイン MAC アドレスを使用します。冗長インターフェイスは、追加し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でメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になった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 インターフェイスの MAC アドレスに関係なく、割り当てた 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。この機能を使用すると、セキュリティ アプライアンスはパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「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」（P.9-3）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には、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、「セキュリティ コンテキスト」（P.9-23）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して、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ができます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

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。同一セキュリティ レベルのインターフェイス間で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。インターフェイスごとに異なるレベルを使用し、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ようにすると、1 レベルにつき 1 つのインターフェイスしか設定できません（0 ～ 100）。

（注）　NAT 制御をイネーブルにする場合、同一セキュリティ レベルのインターフェイス間では NAT を設定する必要がありません。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

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)] フィールドの説明

この項では、次のトピックについて取り上げます。

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 とそれに続く *.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]：インターフェイス名を表示します。
- [Enabled]：インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示します。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、それ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。トランスペアレント モードの場合「native」が表示されます。トランスペアレント 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 モードの場合のみ。サブネット マスクを表示します。
- [Management Only]：インターフェイスでセキュリティ アプライアンスへのトラフィックが許可されるか、または管理のためだけかを示します。
- [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] : 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します。同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。
- [Enable traffic between two or more hosts connected to the same interface] : 同一インターフェイスを出入りするトラフィックをイネーブルにします。

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
•	•	—	•	—

[Edit Interface] > [General (Context)]

フィールド

- [Hardware Port] : *表示専用*。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。この設定に加えて、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）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、それ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、内部ネットワークから外部ネットワーク（低いセキュリティ レベル）に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が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。
- [IP Address] : ルーテッド モードの場合のみ。マルチ コンテキスト モードの場合は、コンテキスト設定で IP アドレスを設定します。
  - [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 アドレスを動的に設定します。

    [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 リースを更新します。

- [Description]：オプションの説明を 240 文字以内で入力します。改行を入れずに 1 行で入力します。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。

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
•	•	—	•	—

[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 モードの場合は、コンテキスト設定で MTU を設定します。
- [Mac Address Cloning]：手動で MAC アドレスを割り当てます。

  デフォルトでは、物理インターフェイスはバーンドイン 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バーンドイン 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。この機能を使用すると、セキュリティ アプライアンスはパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「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」（P.9-3）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には、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、「セキュリティ コンテキスト」（P.9-23）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して、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 モードで共有されないインターフェイスの場合は、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を推奨します。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

  - [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 アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。
  - [Standby Mac Address]：フェールオーバーを使用する場合は、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、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古い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
•	•	—	•	—