



CHAPTER 11

インターフェイス コンフィギュレーションの開始 (ASA 5510 以降)

この章では、ASA 5510 以降のインターフェイス コンフィギュレーションを開始するためのタスクについて説明します。イーサネット設定、冗長インターフェイス、および EtherChannel の設定が含まれています。



(注)

この章の内容が当てはまるのは、ASA 5500 シリーズ アプライアンスのみです。ASASM の場合は、インターフェイス コンフィギュレーションを開始するにはスイッチでスイッチ ポートおよび VLAN を設定してから、第 2 章「ASA サービス モジュールを使用するためのスイッチの設定」に従って VLAN を ASASM に割り当てます。インターフェイス コンフィギュレーションの実行方法については、第 13 章「インターフェイス コンフィギュレーションの実行 (ルーテッド モード)」を参照してください。第 14 章「インターフェイス コンフィギュレーションの実行 (トランスペアレント モード)」

ASA 5505 のコンフィギュレーションについては、次を参照してください。第 12 章「インターフェイス コンフィギュレーションの開始 (ASA 5505)」

マルチコンテキスト モードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

ASA クラスタ インターフェイスについては、特別な要件があるため、第 7 章「ASA のクラスタの設定」を参照してください。

この章の内容は、次のとおりです。

- 「ASA 5510 以降のインターフェイス コンフィギュレーションの開始に関する情報」 (P.11-2)
- 「ASA 5510 以降のインターフェイスのライセンス要件」 (P.11-8)
- 「注意事項と制限事項」 (P.11-10)
- 「デフォルト設定」 (P.11-12)
- 「インターフェイス コンフィギュレーションの開始 (ASA 5510 以降)」 (P.11-13)
- 「インターフェイスのモニタリング」 (P.11-36)
- 「ASA 5510 以降のインターフェイスの設定例」 (P.11-36)
- 「次の作業」 (P.11-37)
- 「ASA 5510 以降のインターフェイスの機能履歴」 (P.11-38)

ASA 5510 以降のインターフェイス コンフィギュレーションの開始に関する情報

この項では、次のトピックについて取り上げます。

- 「Auto-MDI/MDIX 機能」 (P.11-2)
- 「トランスペアレント モードのインターフェイス」 (P.11-2)
- 「管理インターフェイス」 (P.11-2)
- 「冗長インターフェイス」 (P.11-5)
- 「EtherChannel」 (P.11-5)

Auto-MDI/MDIX 機能

ASA 5500 シリーズの 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。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

トランスペアレント モードのインターフェイス

トランスペアレント モードのインターフェイスは、「ブリッジ グループ」に属しています。ブリッジ グループはネットワークごとに 1 つです。コンテキストまたはシングル モードごとに、それぞれ 4 つのインターフェイスからなる最大 8 個のブリッジ グループを設定できます。ブリッジ グループの詳細については、「トランスペアレント モードのブリッジ グループ」 (P.14-2) を参照してください。

管理インターフェイス

- 「管理インターフェイスの概要」 (P.11-2)
- 「管理スロット/ポート インターフェイス」 (P.11-3)
- 「管理専用トラフィックに対する任意のインターフェイスの使用」 (P.11-3)
- 「トランスペアレント モードの管理インターフェイス」 (P.11-4)
- 「冗長管理インターフェイスでのサポートなし」 (P.11-4)
- 「ASA 5512-X ~ ASA 5555-X の Management 0/0 インターフェイス」 (P.11-4)

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス

- 専用の管理スロット/ポートインターフェイス（使用しているモデルで使用できる場合）

第 43 章「管理アクセスの設定」の説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

管理スロット/ポートインターフェイス

表 11-1 に、モデルごとの管理インターフェイスを示します。

表 11-1 モデルごとの管理インターフェイス

モデル	通過トラフィックに対して設定可能 ¹	Management 0/0 ²	Management 0/1	Management 1/0	Management 1/1
ASA 5505	N/A	No	No	No	No
ASA 5510	Yes	Yes	No	No	No
ASA 5520	Yes	Yes	No	No	No
ASA 5540	Yes	Yes	No	No	No
ASA 5550	Yes	Yes	No	No	No
ASA 5580	Yes	Yes	Yes	No	No
ASA 5512-X	No	Yes	No	No	No
ASA 5515-X	No	Yes	No	No	No
ASA 5525-X	No	Yes	No	No	No
ASA 5545-X	No	Yes	No	No	No
ASA 5555-X	No	Yes	No	No	No
ASA 5585-X	Yes	Yes	Yes	Yes ³	Yes ³
ASASM	N/A	No	No	No	No

1. デフォルトでは、Management 0/0 インターフェイスは管理専用トラフィック用に設定されています（**management-only** コマンド）。ルーテッドモードでサポートされるモデルの場合、制限を削除してトラフィックを通過させることができます。使用しているモデルに他の管理インターフェイスが含まれている場合、それを通過トラフィックにも使用できます。ただし、管理インターフェイスは通過トラフィックには最適化されていない場合があります。
2. Management 0/0 インターフェイスは、デフォルトの出荷時のコンフィギュレーションの一部として、ASDM アクセス用に設定されています。詳細については、「工場出荷時のデフォルト コンフィギュレーション」(P.3-18) を参照してください。
3. SSP をスロット 1 に設置した場合は、Management 1/0 および 1/1 ではスロット 1 の SSP への管理アクセスのみが提供されます。



(注) IPS モジュールを設置した場合は、IPS モジュール管理インターフェイスでは、IPS モジュールの管理アクセスのみが提供されます。ASA 5512-X ~ ASA 5555-X では、IPS SSP ソフトウェア モジュールによって ASA と同じ物理的な Management 0/0 インターフェイスが使用されます。

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。これには、EtherChannel インターフェイスも含まれます（**management-only** コマンドを参照）。

トランスペアレント モードの管理インターフェイス

トランスペアレント ファイアウォール モードでは、許可される最大通過トラフィック インターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）、管理インターフェイスからなる EtherChannel インターフェイス（複数の管理インターフェイスがある場合）のいずれか）を個別の管理インターフェイスとして使用できます。他のインターフェイス タイプは管理インターフェイスとして使用できません。

使用しているモデルに管理インターフェイスが含まれていない場合は、データ インターフェイスからトランスペアレント ファイアウォールを管理する必要があります。

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ASA 5512-X ~ ASA 5555-X では、管理インターフェイスのサブインターフェイスは許可されないため、コンテキスト単位で管理を行うには、データ インターフェイスに接続する必要があります。

8.4(1) 以降では、管理インターフェイスは通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。



(注)

トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法で MAC アドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Cisco Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASAによって、データ インターフェイスではなく、管理インターフェイスを使用してスイッチにアクセスするように MAC アドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。

冗長管理インターフェイスでのサポートなし

冗長インターフェイスは、管理 スロット/ポート インターフェイスをメンバとしてサポートしません。また、管理以外のインターフェイスで構成される冗長インターフェイスを、管理専用として設定することはできません。

ASA 5512-X ~ ASA 5555-X の Management 0/0 インターフェイス

ASA 5512-X ~ ASA 5555-X の Management 0/0 インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません
- マルチキャスト MAC はサポートされません
- IPS SSP ソフトウェア モジュールによって Management 0/0 インターフェイスは共有されます。ASA と IPS モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。IPS オペレーティング システムで IPS の IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。

冗長インターフェイス

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。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 ASA 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、必要な場合はデバイスレベルの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。

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（「[MAC アドレスおよび MTU の設定](#)」(P.13-10) または「[マルチ コンテキストの設定](#)」(P.6-15) 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。

EtherChannel

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャンネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャンネル インターフェイスと呼びます）。ポートチャンネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

最大 48 個の EtherChannel を設定できます。

この項では、次のトピックについて取り上げます。

- 「[チャンネル グループのインターフェイス](#)」(P.11-5)
- 「[別のデバイスの EtherChannel への接続](#)」(P.11-6)
- 「[リンク集約制御プロトコル](#)」(P.11-7)
- 「[ロード バランシング](#)」(P.11-7)
- 「[EtherChannel MAC アドレス](#)」(P.11-8)

チャンネル グループのインターフェイス

チャンネル グループ 1 つにつき 8 個のインターフェイスをアクティブにすることができます。1 つのチャンネル グループに最大 16 個のインターフェイスを割り当てることができます。アクティブにできるインターフェイスは 8 個のみですが、残りのインターフェイスはインターフェイスに障害が発生した場合のスタンバイ リンクとして動作できます。

チャンネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャンネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

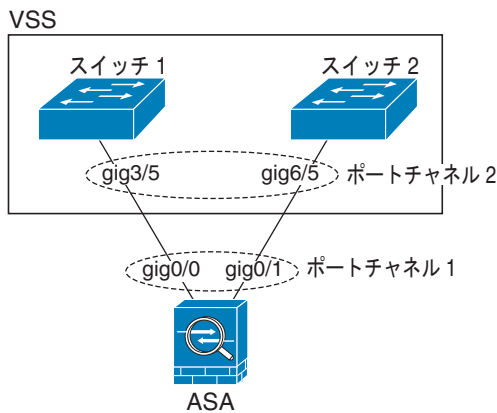
EtherChannel によって、チャンネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。ポートは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

ASA EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチに接続できます。

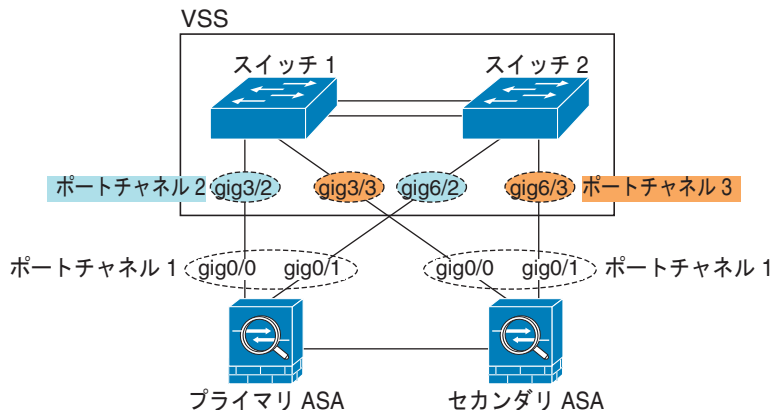
スイッチが仮想スイッチング システム (VSS) の一部である場合、同じ EtherChannel 内の ASA インターフェイスを VSS 内の個別のスイッチに接続できます。個別のスイッチは単一のスイッチのように動作するため、スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバーです (図 11-1 を参照)。

図 11-1 VSS への接続



ASA をアクティブ/スタンバイ フェールオーバー配置で使用する場合、ASA ごとに 1 つ、VSS 内のスイッチで個別の EtherChannel を作成する必要があります (図 11-1 を参照)。各 ASA で、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチ インターフェイスを両方の ASA に接続する単一の EtherChannel にグループ化できる場合でも (この場合、個別の ASA システム ID のため、EtherChannel は確立されません)、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ ASA に送信しないようにするためです。

図 11-2 アクティブ/スタンバイ フェールオーバーと VSS



リンク集約制御プロトコル

リンク集約制御プロトコル (LACP) では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ : LACP 更新を送受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ : LACP 更新を受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。
- オン : EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバ インターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

ASA は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します (この基準は設定可能です。「[EtherChannel のカスタマイズ](#)」(P.11-32) を参照してください)。ハッシュ結果は 3 ビットの値 (0 ~ 7) です。

8 個のハッシュ結果値は、チャネル グループのインターフェイス間でラウンドロビン方式で分散されます。最も小さい ID (スロット/ポート) のインターフェイスから開始されます。たとえば、ハッシュ結果が 0 のすべてのパケットは GigabitEthernet 0/0 に、ハッシュ結果が 1 のパケットは GigabitEthernet 0/1 に、ハッシュ結果が 2 のパケットは GigabitEthernet 0/2 に、というように送られます。

EtherChannel 内のアクティブ インターフェイスの数に関係なく 8 個のハッシュ結果値があるため、アクティブ インターフェイスの数によっては、パケットが均等に分散されない場合があります。

表 11-2 に、各アクティブ インターフェイス数について、インターフェイスごとのロード バランシング量を示します。太字のアクティブ インターフェイスは均等に分散されています。

表 11-2 インターフェイスごとの負荷分散

アクティブ インター フェイス数	インターフェイスごとの分散 %							
	1	2	3	4	5	6	7	8
1	100 %	—	—	—	—	—	—	—
2	50 %	50 %	—	—	—	—	—	—
3	37.5%	37.5%	25 %	—	—	—	—	—
4	25 %	25 %	25 %	25 %	—	—	—	—
5	25 %	25 %	25 %	12.5 %	12.5 %	—	—	—
6	25 %	25 %	12.5 %	12.5 %	12.5 %	12.5 %	—	—
7	25 %	12.5 %	12.5 %	12.5 %	12.5 %	12.5 %	12.5 %	—
8	12.5 %	12.5 %	12.5 %	12.5 %	12.5 %	12.5 %	12.5 %	12.5 %

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチ コンテキスト モードでは、EtherChannel ポート インターフェイスを含め、固有の MAC アドレスをインターフェイスに自動的に割り当てることができます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを手動で設定するか、またはマルチ コンテキスト モードで自動的に設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

ASA 5510 以降のインターフェイスのライセンス要件

モデル	ライセンス要件
ASA 5510	VLAN : 基本ライセンス : 50 Security Plus ライセンス : 100 インターフェイス速度 : 基本ライセンス : すべてのインターフェイスがファスト イーサネット。 Security Plus ライセンス : Ethernet 0/0 および 0/1 : ギガビット イーサネット、その他すべてはファスト イーサネット。 すべての種類のインターフェイス ¹ : 基本ライセンス : 52 Security Plus ライセンス : 120
ASA 5520	VLAN : 基本ライセンス : 150 すべての種類のインターフェイス ¹ : 基本ライセンス : 640
ASA 5540	VLAN : 基本ライセンス : 200 すべての種類のインターフェイス ¹ : 基本ライセンス : 840

モデル	ライセンス要件
ASA 5550	VLAN : 基本ライセンス : 400 すべての種類のインターフェイス ¹ : 基本ライセンス : 1640
ASA 5580	VLAN : 基本ライセンス : 1024 すべての種類のインターフェイス ¹ : 基本ライセンス : 4176
ASA 5512-X	VLAN : 基本ライセンス : 50 すべての種類のインターフェイス ¹ : 基本ライセンス : 328
ASA 5515-X	VLAN : 基本ライセンス : 100 すべての種類のインターフェイス ¹ : 基本ライセンス : 528
ASA 5525-X	VLAN : 基本ライセンス : 200 すべての種類のインターフェイス ¹ : 基本ライセンス : 928
ASA 5545-X	VLAN : 基本ライセンス : 300 すべての種類のインターフェイス ¹ : 基本ライセンス : 1328
ASA 5555-X	VLAN : 基本ライセンス : 500 すべての種類のインターフェイス ¹ : 基本ライセンス : 2128
ASA 5585-X	VLAN : 基本ライセンス : 1024 SSP-10 および SSP-20 のインターフェイス速度 : 基本ライセンス : ファイバ インターフェイスの場合 1 ギガビット イーサネット 10 GE I/O ライセンス (Security Plus) : ファイバ インターフェイスの場合 10 ギガビット イーサ ネット (SSP-40 および SSP-60 は 10 ギガビット イーサネットをデフォルトでサポートします)。 すべての種類のインターフェイス ¹ : 基本ライセンス : 4176

1. VLAN、物理、冗長、ブリッジグループ、および EtherChannel インターフェイスなど、すべてを合わせたインターフェイスの最大数。

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

マルチ コンテキスト モードでは、「[インターフェイス コンフィギュレーションの開始 \(ASA 5510 以降\)](#)」(P.11-13)に従って、システム実行スペースで物理インターフェイスを設定します。次に、[第 13 章「インターフェイス コンフィギュレーションの実行 \(ルーテッド モード\)」](#)または[第 14 章「インターフェイス コンフィギュレーションの実行 \(トランスペアレント モード\)」](#)に従って、コンテキスト 実行スペースで論理インターフェイス パラメータを設定します。

ファイアウォール モードのガイドライン

- トランスペアレント モードでは、コンテキストごとに、またはシングル モードのデバイスに対して、最大 8 個のブリッジグループを設定できます。
- 各ブリッジグループは、最大 4 つのインターフェイスを含むことができます。
- マルチ コンテキストのトランスペアレント モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。

フェールオーバーのガイドライン

- 冗長インターフェイスまたは EtherChannel インターフェイスをフェールオーバー リンクとして使用する場合、フェールオーバー ペアの両方の装置でその事前設定を行う必要があります。プライマリ装置で設定し、セカンダリ装置に複製されることは想定できません。これは、複製にはフェールオーバー リンク自体が必要であるためです。
- 冗長インターフェイスまたは EtherChannel インターフェイスをステート リンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。
- 冗長または EtherChannel インターフェイスをモニタすると、フェールオーバーが発生したかどうかわかります。それには、**monitor-interface** コマンドを使用します。必ず、論理冗長インターフェイス名を指定してください。アクティブなメンバ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または EtherChannel 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。すべての物理インターフェイスで障害が発生した場合にのみ、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているように見えます (EtherChannel インターフェイスでは、障害の発生が許容されるメンバインターフェイスの数を設定できます)。
- EtherChannel インターフェイスをフェールオーバー リンクまたはステート リンクに対して使用する場合、異常なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、変更時に EtherChannel をシャットダウンするか、フェールオーバーを一時的にディセーブルにする必要があります。どちらの操作でも、その間はフェールオーバーは行われません。
- フェールオーバーとフェールオーバー ステート リンクをポート チャネル リンク上で設定できますが、このポート チャネルを他のファイアウォール トラフィックと共有させることはできません。

クラスタリングのガイドライン

- 冗長または EtherChannel インターフェイスをクラスタ制御リンクとして使用するときは、そのリンクをクラスタ内のすべてのユニットで事前に設定する必要があります。プライマリユニットだけで設定してもメンバユニットに複製されることはありません。複製にはクラスタ制御リンクそのものが必要であるからです。
- スパンド EtherChannel を設定するには、「[スパンド EtherChannel の設定](#)」(P.7-35) を参照してください。
- 個別クラスタ インターフェイスを設定するには、「[個別インターフェイスの設定 \(管理インターフェイスの場合に推奨\)](#)」(P.7-33) を参照してください。

冗長インターフェイスのガイドライン

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- すべての ASA 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。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。
- 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は、管理スロット/ポートインターフェイスをメンバとしてサポートしません。また、管理以外のインターフェイスで構成される冗長インターフェイスを、管理専用として設定することはできません。
- フェールオーバーのガイドラインについては、「[フェールオーバーのガイドライン](#)」(P.11-10) を参照してください。
- クラスタリングのガイドラインについては、「[クラスタリングのガイドライン](#)」(P.11-11) を参照してください。

EtherChannel のガイドライン

- 最大 48 個の EtherChannel を設定できます。
- チャンネル グループ 1 つにつき 8 個のインターフェイスをアクティブにすることができます。1 つのチャンネル グループに最大 16 個のインターフェイスを割り当てることができます。アクティブにできるインターフェイスは 8 個のみですが、残りのインターフェイスはインターフェイスに障害が発生した場合のスタンバイ リンクとして動作できます。
- チャンネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャンネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。
- ASA 5500 EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチに接続できます。
- すべての ASA 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 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを ASA 上で設定することができます。

- 4GE SSM (これには ASA 5550 のスロット 1 の統合 4GE SSM も含まれます) 上のインターフェイスを EtherChannel の一部として使用することはできません。
- フェールオーバーのガイドラインについては、「[フェールオーバーのガイドライン](#)」(P.11-10) を参照してください。
- クラスタリングのガイドラインについては、「[クラスタリングのガイドライン](#)」(P.11-11) を参照してください。

デフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションについては、「[工場出荷時のデフォルト コンフィギュレーション](#)」(P.3-18) を参照してください。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。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。
- EtherChannel ポートチャネル インターフェイス：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ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。

デフォルトの速度および二重通信

- 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。
- ASA 5550 (スロット 1) および 4GE SSM の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。
- ASA 5580 および 5585-X のファイバインターフェイスでは、自動リンク ネゴシエーションの速度が設定されます。

デフォルトのコネクタ タイプ

ASA 5550 (スロット 1) と ASA 5510 以降の ASA 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。ASA を設定すると、ファイバ SFP コネクタを使用できます。

デフォルトの MAC アドレス

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。

インターフェイス コンフィギュレーションの開始 (ASA 5510 以降)

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 コンフィギュレーションを開始するためのタスク フロー」 (P.11-13)
- 「使用中のインターフェイスの冗長インターフェイスまたは EtherChannel インターフェイスへの変換」 (P.11-14)
- 「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」 (P.11-24)
- 「冗長インターフェイスの設定」 (P.11-27)
- 「EtherChannel の設定」 (P.11-29)
- 「VLAN サブインターフェイスと 802.1Q トランキングの設定」 (P.11-33)
- 「ジャンボ フレーム サポートのイネーブル化 (サポート対象のモデル)」 (P.11-35)

インターフェイス コンフィギュレーションを開始するためのタスク フロー



(注)

既存のコンフィギュレーションがあり、使用中のインターフェイスを冗長または EtherChannel インターフェイスに変換する場合は、中断を最小限にするために、コンフィギュレーションをオフラインで実行します。「使用中のインターフェイスの冗長インターフェイスまたは EtherChannel インターフェイスへの変換」 (P.11-14) を参照してください。

インターフェイス コンフィギュレーションを開始するには、次の手順を実行します。

- ステップ 1** (マルチ コンテキスト モード) この項のタスクはすべてシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- ステップ 2** 物理インターフェイスをイネーブルにし、必要に応じてイーサネット パラメータを変更します。「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」 (P.11-24) を参照してください。
デフォルトでは、物理インターフェイスはディセーブルになっています。
- ステップ 3** (任意) 冗長インターフェイス ペアを設定します。「冗長インターフェイスの設定」 (P.11-27) を参照してください。
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。
- ステップ 4** (任意) EtherChannel を設定します。「EtherChannel の設定」 (P.11-29) を参照してください。
EtherChannel によって、複数のイーサネット インターフェイスが 1 つの論理インターフェイスにグループ化されます。



(注) 4GE SSM (これには ASA 5550 のスロット 1 の統合 4GE SSM も含まれます) 上のインターフェイスを EtherChannel の一部として使用することはできません。

- ステップ 5** (任意) VLAN サブインターフェイスを設定します。「VLAN サブインターフェイスと 802.1Q トランキングの設定」(P.11-33) を参照してください。
- ステップ 6** (任意) 「ジャンボ フレーム サポートのイネーブル化 (サポート対象のモデル)」(P.11-35) に従って、ASA 5580 および 5585-X のジャンボ フレームのサポートをイネーブルにします。
- ステップ 7** (マルチ コンテキスト モードのみ) システム実行スペースでインターフェイス コンフィギュレーションを実行するには、第 6 章「マルチ コンテキスト モードの設定」に記載されている次のタスクを実行します。
- 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.6-20) を参照してください。
 - (任意) 固有の MAC アドレスをコンテキスト インターフェイスに自動的に割り当てるには、「コンテキスト インターフェイスへの MAC アドレスの自動割り当て」(P.6-24) を参照してください。
- MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。また、「MAC アドレスおよび MTU の設定」(P.13-10) に従って、コンテキスト内の MAC アドレスを手動で割り当てることもできます。
- ステップ 8** 第 13 章「インターフェイス コンフィギュレーションの実行 (ルーテッド モード)」または第 14 章「インターフェイス コンフィギュレーションの実行 (トランスペアレント モード)」に従って、インターフェイス コンフィギュレーションを実行します。

使用中のインターフェイスの冗長インターフェイスまたは EtherChannel インターフェイスへの変換

既存のコンフィギュレーションがあり、現在使用中のインターフェイスに対して冗長インターフェイスまたは EtherChannel インターフェイス機能を利用する場合は、論理インターフェイスに変換するときにある程度のダウンタイムが発生します。

ここでは、既存のインターフェイスを冗長インターフェイスまたは EtherChannel インターフェイスに最小限のダウンタイムで変換する方法の概要について説明します。詳細については、「冗長インターフェイスの設定」(P.11-27) および「EtherChannel の設定」(P.11-29) を参照してください。

- 「手順の詳細 (シングル モード)」(P.11-14)
- 「手順の詳細 (マルチ モード)」(P.11-20)

手順の詳細 (シングル モード)

次の理由から、コンフィギュレーションをオフラインでテキスト ファイルとして更新し、コンフィギュレーション全体を再インポートすることを推奨します。

- 冗長インターフェイスまたは EtherChannel インターフェイスのメンバとして名前付きインターフェイスは追加できないため、インターフェイスから名前を削除する必要があります。インターフェイスから名前を削除すると、その名前を参照していたコマンドは削除されます。インターフェイス名を参照するコマンドはコンフィギュレーション全体にわたっており、複数の機能に影響する

ため、CLI または ASDM で使用中のインターフェイス名を削除すると、新しいインターフェイス名に関係するすべての機能を再設定する間の重大なダウンタイムは言うまでもなく、コンフィギュレーションが大きく破壊されます。

- コンフィギュレーションをオフラインで変更すると、同じインターフェイス名を新しい論理インターフェイスに使用できるので、インターフェイス名を参照している機能コンフィギュレーションの変更が不要になります。変更が必要になるのは、インターフェイス コンフィギュレーションだけです。
- 実行コンフィギュレーションをクリアして新しいコンフィギュレーションをすぐに適用すると、インターフェイスのダウンタイムは最小になります。インターフェイスをリアルタイムで設定するのを待つことがありません。

-
- ステップ 1** ASA に接続します。フェールオーバーを使用する場合は、アクティブな ASA に接続します。
- ステップ 2** フェールオーバーを使用している場合、**no failover** コマンドを使用してフェールオーバーをディセーブルにします。
- ステップ 3** 実行コンフィギュレーションをコピーするために、**more system:running-config** コマンドを入力し、表示された出力をテキスト エディタにコピーします。
- 必ず、古いコンフィギュレーションの予備のコピーを保存しておいてください。編集時のエラーに備えるためです。
- ステップ 4** 冗長インターフェイスまたは EtherChannel インターフェイスに追加する使用中のインターフェイスごとに、新しい論理インターフェイスの作成で使用するために、**interface** コマンドの下のすべてのコマンドをインターフェイス コンフィギュレーション セクションの最後にカット アンド ペーストします。例外は次のコマンドのみであり、これらは物理インターフェイス コンフィギュレーションで使用されます。
- **media-type**
 - **speed**
 - **duplex**
 - **flowcontrol**



(注) EtherChannel インターフェイスまたは冗長インターフェイスに追加できるのは物理インターフェイスのみです。物理インターフェイスには VLAN を設定できません。

特定の EtherChannel インターフェイスまたは冗長インターフェイス内のすべてのインターフェイスについて、上記の値を必ず一致させてください。EtherChannel インターフェイスの二重通信の設定は [Full] または [Auto] である必要があります。

たとえば、次のインターフェイス コンフィギュレーションがあるとします。太字のコマンドは 3 つの新しい EtherChannel インターフェイスで使用するコマンドであり、インターフェイス セクションの最後にカット アンド ペーストする必要があります。

```
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 10.86.194.225 255.255.255.0
  no shutdown
!
interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 192.168.1.3 255.255.255.0
  no shutdown
```

```

!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address

```

ステップ 5 ペーストした各コマンドセクションの上に、次のコマンドのいずれかを入力して、新しい論理インターフェイスを作成します。

- **interface redundant number** [1-8]
- **interface port-channel channel_id** [1-48]

たとえば、次のように入力します。

...

```

interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown

```


ステップ 6 新しい論理インターフェイスに物理インターフェイスを割り当てます。

- 冗長インターフェイス：新しい **interface redundant** コマンドの下に次のコマンドを入力します。

```
member-interface physical_interface1
member-interface physical_interface2
```

物理インターフェイスは、同じタイプの任意の 2 つのインターフェイス（以前使用していたか、または未使用）です。管理インターフェイスを冗長インターフェイスに割り当てることはできません。

たとえば、既存の配線を利用するには、以前使用していたインターフェイスを引き続き、以前の役割のまま、内部および外部の冗長インターフェイスの一部として使用します。

```
interface redundant 1
  nameif outside
  security-level 0
  ip address 10.86.194.225 255.255.255.0
  member-interface GigabitEthernet0/0
  member-interface GigabitEthernet0/2
```

```
interface redundant 2
  nameif inside
  security-level 100
  ip address 192.168.1.3 255.255.255.0
  member-interface GigabitEthernet0/1
  member-interface GigabitEthernet0/3
```

- EtherChannel インターフェイス：EtherChannel に追加する各インターフェイス（以前使用していたか、または未使用）の下に次のコマンドを入力します。EtherChannel ごとに最大 16 個のインターフェイスを割り当てることができます。ただし、アクティブにすることができるのは 8 個のみであり、他は障害に備えてスタンバイ状態です。

```
channel-group channel_id mode active
```

たとえば、既存の配線を利用するには、以前使用していたインターフェイスを、以前の役割で、内部および外部の EtherChannel インターフェイスの一部として引き続き使用します。

```
interface GigabitEthernet0/0
  channel-group 1 mode active
  no shutdown
!
interface GigabitEthernet0/1
  channel-group 2 mode active
  no shutdown
!
interface GigabitEthernet0/2
  channel-group 1 mode active
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/3
  channel-group 1 mode active
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/4
  channel-group 2 mode active
  shutdown
  no nameif
```

```

no security-level
no ip address
!
interface GigabitEthernet0/5
  channel-group 2 mode active
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  channel-group 3 mode active
  no shutdown
!
interface Management0/1
  channel-group 3 mode active
  shutdown
  no nameif
  no security-level
  no ip address
...

```

ステップ 7 以前は使用されていなかったが論理インターフェイスの一部になった各インターフェイスをイネーブルにします。**shutdown** コマンドの前に **no** を追加します。

たとえば、最終的な EtherChannel の設定は次のとおりです。

```

interface GigabitEthernet0/0
  channel-group 1 mode active
  no shutdown
!
interface GigabitEthernet0/1
  channel-group 2 mode active
  no shutdown
!
interface GigabitEthernet0/2
  channel-group 1 mode active
  no shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/3
  channel-group 1 mode active
  no shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/4
  channel-group 2 mode active
  no shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/5
  channel-group 2 mode active
  no shutdown
  no nameif
  no security-level
  no ip address
!

```

```
interface Management0/0
  channel-group 3 mode active
  no shutdown
!
interface Management0/1
  channel-group 3 mode active
  no shutdown
  no nameif
  no security-level
  no ip address
!
interface port-channel 1
  nameif outside
  security-level 0
  ip address 10.86.194.225 255.255.255.0
!
interface port-channel 2
  nameif inside
  security-level 100
  ip address 192.168.1.3 255.255.255.0
!
interface port-channel 3
  nameif mgmt
  security-level 100
  ip address 10.1.1.5 255.255.255.0
```



(注) 他のオプションの EtherChannel パラメータは、新しいコンフィギュレーションをインポートした後で設定できます。「EtherChannel の設定」(P.11-29) を参照してください。

ステップ 8 ASA の CLI プロンプトで、接続（コンソールまたはリモート）に応じて次の手順を実行します。

- コンソール接続の場合
 - a. 変更したインターフェイス セクションを含め、新しいコンフィギュレーション全体をクリップボードにコピーします。
 - b. 実行コンフィギュレーションをクリアするために、次のとおりに入力します。
`hostname(config)# clear configure all`
ASA を通過するトラフィックは、このポイントで停止します。
 - c. 新しいコンフィギュレーションをプロンプトで貼り付けます。
ASA を通過するトラフィックが再開します。
- リモート接続：
 - a. 新しいコンフィギュレーションを TFTP または FTP サーバに保存します。ASA のスタートアップ コンフィギュレーションにコピーできるようにするためです。たとえば、PC 上で TFTP サーバまたは FTP サーバを実行できます。
 - b. 次のコマンドを入力してスタートアップ コンフィギュレーションをクリアします。
`hostname(config)# write erase`
 - c. 新しいコンフィギュレーションをスタートアップ コンフィギュレーションにコピーするために、次のとおりに入力します。
`hostname(config)# copy url startup-config`
「ファイルのダウンロード」(P.85-12) を参照してください。

- d. **reload** コマンドを使用して ASA をリロードします。実行コンフィギュレーションを保存しないでください。

ステップ 9 フェールオーバーを再度イネーブルにするために、**failover** コマンドを入力します。

手順の詳細 (マルチ モード)

次の理由から、システムおよびコンテキスト コンフィギュレーションをオフラインでテキスト ファイルとして更新し、それを再インポートすることを推奨します。

- 冗長インターフェイスまたは EtherChannel インターフェイスのメンバとして割り当て済みのインターフェイスは追加できないため、コンテキストからインターフェイスを割り当て解除する必要があります。インターフェイスを割り当て解除すると、そのインターフェイスを参照していたコンテキスト コマンドは削除されます。インターフェイスを参照するコマンドはコンフィギュレーション全体にわたっており、複数の機能に影響するため、CLI または ASDM で使用中のインターフェイスの割り当てを削除すると、新しいインターフェイスに関係するすべての機能を再設定する間の重大なダウンタイムは言うまでもなく、コンフィギュレーションが大きく破壊されます。
- コンフィギュレーションをオフラインで変更すると、同じインターフェイス名を新しい論理インターフェイスに使用できるので、インターフェイス名を参照している機能コンフィギュレーションの変更が不要になります。変更が必要になるのは、インターフェイス コンフィギュレーションだけです。
- 実行システム コンフィギュレーションをクリアして新しいコンフィギュレーションをすぐに適用すると、インターフェイスのダウンタイムは最小になります。インターフェイスをリアルタイムで設定するのを待つことはありません。

ステップ 1 ASA に接続し、システムに切り替えます。フェールオーバーを使用する場合は、アクティブな ASA に接続します。

ステップ 2 フェールオーバーを使用している場合、**no failover** コマンドを使用してフェールオーバーをディセーブルにします。

ステップ 3 システムで、実行コンフィギュレーションをコピーするために、**more system:running-config** コマンドを入力し、表示された出力をテキスト エディタにコピーします。

必ず、古いコンフィギュレーションの予備のコピーを保存しておいてください。編集時のエラーに備えるためです。

たとえば、次のインターフェイス コンフィギュレーションおよび割り当てがシステム コンフィギュレーションにあり、2 つのコンテキスト間に共有インターフェイスがあります。

システム

```
interface GigabitEthernet0/0
  no shutdown
interface GigabitEthernet0/1
  no shutdown
interface GigabitEthernet0/2
  shutdown
interface GigabitEthernet0/3
  shutdown
interface GigabitEthernet0/4
  shutdown
interface GigabitEthernet0/5
  shutdown
interface Management0/0
  no shutdown
interface Management1/0
```

```
shutdown
!
context customerA
  allocate-interface gigabitethernet0/0 int1
  allocate-interface gigabitethernet0/1 int2
  allocate-interface management0/0 mgmt
context customerB
  allocate-interface gigabitethernet0/0
  allocate-interface gigabitethernet0/1
  allocate-interface management0/0
```

ステップ 4 新しい EtherChannel インターフェイスまたは冗長インターフェイスを使用するすべてのコンテキスト コンフィギュレーションのコピーを取得します。を参照してください。「[コンフィギュレーションまたはその他のファイルのバックアップ](#)」(P.85-18)

たとえば、次のコンテキスト コンフィギュレーションをダウンロードします (インターフェイス コンフィギュレーションが表示されています)。

CustomerA コンテキスト

```
interface int1
  nameif outside
  security-level 0
  ip address 10.86.194.225 255.255.255.0
!
interface int2
  nameif inside
  security-level 100
  ip address 192.168.1.3 255.255.255.0
  no shutdown
!
interface mgmt
  nameif mgmt
  security-level 100
  ip address 10.1.1.5 255.255.255.0
  management-only
```

CustomerB コンテキスト

```
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 10.20.15.5 255.255.255.0
!
interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 192.168.6.78 255.255.255.0
!
interface Management0/0
  nameif mgmt
  security-level 100
  ip address 10.8.1.8 255.255.255.0
  management-only
```

ステップ 5 システム コンフィギュレーションで、「[冗長インターフェイスの設定](#)」(P.11-27) または「[EtherChannel の設定](#)」(P.11-29) に従って、新しい論理インターフェイスを作成します。論理インターフェイスの一部として使用する追加物理インターフェイスで **no shutdown** コマンドを入力してください。



(注) EtherChannel インターフェイスまたは冗長インターフェイスに追加できるのは物理インターフェイスのみです。物理インターフェイスには VLAN を設定できません。

特定の EtherChannel インターフェイスまたは冗長インターフェイス内のすべてのインターフェイスについて、速度や二重通信などの物理インターフェイス パラメータを必ず一致させてください。EtherChannel インターフェイスの二重通信の設定は [Full] または [Auto] である必要があります。

たとえば、新しいコンフィギュレーションは次のとおりです。

システム

```
interface GigabitEthernet0/0
  channel-group 1 mode active
  no shutdown
!
interface GigabitEthernet0/1
  channel-group 2 mode active
  no shutdown
!
interface GigabitEthernet0/2
  channel-group 1 mode active
  no shutdown
!
interface GigabitEthernet0/3
  channel-group 1 mode active
  no shutdown
!
interface GigabitEthernet0/4
  channel-group 2 mode active
  no shutdown
!
interface GigabitEthernet0/5
  channel-group 2 mode active
  no shutdown
!
interface Management0/0
  channel-group 3 mode active
  no shutdown
!
interface Management0/1
  channel-group 3 mode active
  no shutdown
!
interface port-channel 1
interface port-channel 2
interface port-channel 3
```

ステップ 6 コンテキストごとのインターフェイス割り当てを、新しい EtherChannel インターフェイスまたは冗長インターフェイスを使用するように変更します。「[セキュリティ コンテキストの設定](#)」(P.6-20) を参照してください。

たとえば、既存の配線を利用するには、以前使用していたインターフェイスを引き続き、以前の役割のまま、内部および外部の冗長インターフェイスの一部として使用します。

```
context customerA
  allocate-interface port-channel1 int1
  allocate-interface port-channel2 int2
  allocate-interface port-channel3 mgmt
context customerB
```

```
allocate-interface port-channel1
allocate-interface port-channel2
allocate-interface port-channel3
```



(注) まだ行っていない場合は、この機会を利用して、マップされた名前を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、**customerA** のコンフィギュレーションは変更の必要がなく、ASA で再適用する必要だけがあります。ただし、**customerB** のコンフィギュレーションは、インターフェイス ID をすべて変更する必要があります。**customerB** についてマップされた名前を割り当てると、コンテキスト コンフィギュレーションでのインターフェイス ID の変更は必要ですが、マッピングされた名前が今後のインターフェイスの変更役に役立つ場合があります。

ステップ 7 マップされた名前を使用しないコンテキストの場合、新しい EtherChannel インターフェイス ID または冗長インターフェイス ID を使用するようにコンテキスト コンフィギュレーションを変更します。(マップされたインターフェイス名を使用するコンテキストでは、変更は必要ありません)。

たとえば、次のように入力します。

CustomerB コンテキスト

```
interface port-channel1
  nameif outside
  security-level 0
  ip address 10.20.15.5 255.255.255.0
!
interface port-channel2
  nameif inside
  security-level 100
  ip address 192.168.6.78 255.255.255.0
!
interface port-channel3
  nameif mgmt
  security-level 100
  ip address 10.8.1.8 255.255.255.0
  management-only
```

ステップ 8 新しいコンテキスト コンフィギュレーション ファイルを古いファイルの上にコピーします。たとえば、コンテキストが FTP サーバにある場合は、FTP を使用して既存のファイル (必要に応じてバックアップを作成します) に上書きコピーします。コンテキストがフラッシュ メモリ内にある場合、**copy** コマンドを使用し TFTP サーバまたは FTP サーバを PC 上で実行するか、セキュア コピーを使用します。「[ファイルのダウンロード](#)」(P.85-12) を参照してください。この変更は、スタートアップ コンフィギュレーションのみに影響します。実行コンフィギュレーションでは古いコンテキスト コンフィギュレーションがまだ使用されています。

ステップ 9 ASA のシステム CLI プロンプトで、接続 (コンソールまたはリモート) に応じて次の手順を実行します。

- コンソール接続の場合
 - a. 変更したインターフェイス セクションを含め、新しいシステム コンフィギュレーション全体をクリップボードにコピーします。
 - b. 実行コンフィギュレーション (システムおよびコンテキストの両方) をクリアするために、次のとおりに入力します。

```
hostname(config)# clear configure all
```

ASA を通過するトラフィックは、このポイントで停止します。

- c. 新しいシステム コンフィギュレーションをプロンプトで貼り付けます。

新しいコンテキスト コンフィギュレーションがすべてリロードされます。リロードが終了すると、ASA を通過するトラフィックは再開されます。

- リモート接続 :
 - a. 新しいシステム コンフィギュレーションを TFTP または FTP サーバに保存します。ASA のスタートアップ コンフィギュレーションにコピーできるようにするためです。たとえば、PC 上で TFTP サーバまたは FTP サーバを実行できます。
 - b. 次のコマンドを入力してスタートアップ コンフィギュレーションをクリアします。


```
hostname(config)# write erase
```
 - c. 新しいシステム コンフィギュレーションをスタートアップ コンフィギュレーションにコピーするために、次のとおりに入力します。


```
hostname(config)# copy url startup-config
```

「ファイルのダウンロード」(P.85-12) を参照してください。
 - d. **reload** コマンドを使用して ASA をリロードします。実行コンフィギュレーションを保存しないでください。

ステップ 10 フェールオーバーを再度イネーブルにするために、**failover** コマンドを入力します。

物理インターフェイスのイネーブル化およびイーサネット パラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信（使用できる場合）を設定する。
- フロー制御のポーズ フレームのイネーブル化

前提条件

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ1	<pre>interface physical_interface</pre> <p>例:</p> <pre>hostname(config)# interface gigabitethernet 0/0</pre>	<p>設定するインターフェイスを指定します。</p> <p><i>physical_interface</i> ID には、タイプ、スロット、およびポート番号を <i>type[slot/port]</i> という形式で指定します。</p> <p>物理インターフェイスのタイプには、次のものがあります。</p> <ul style="list-style-type: none"> • ethernet • gigabitethernet • tengigabitethernet • management <p>タイプの後ろに <i>slot/port</i> を入力します。たとえば、gigabitethernet0/1 や ethernet 0/1 のように入力します。タイプと <i>slot/port</i> の間のスペースは任意です。</p>
ステップ2	<p>(任意)</p> <pre>media-type sfp</pre> <p>例:</p> <pre>hostname(config-if)# media-type sfp</pre>	<p>使用しているモデルで利用できる場合には、メディア タイプを SFP に設定します。デフォルトの RJ-45 に戻すには、media-type rj45 コマンドを入力します。</p>
ステップ3	<p>(任意)</p> <pre>speed {auto 10 100 1000 nonegotiate}</pre> <p>例:</p> <pre>hostname(config-if)# speed 100</pre>	<p>速度を設定します。</p> <p>銅線インターフェイスのデフォルト設定は auto です。</p> <p>SFP インターフェイスのデフォルト設定は no speed nonegotiate です。この設定では、速度が最大速度に設定され、フロー制御パラメータとリモート障害情報のリンク ネゴシエーションがイネーブルになります。nonegotiate キーワードは、SFP インターフェイスで使用できる唯一のキーワードです。speed nonegotiate コマンドは、リンク ネゴシエーションをディセーブルにします。</p>
ステップ4	<p>(任意)</p> <pre>duplex {auto full half}</pre> <p>例:</p> <pre>hostname(config-if)# duplex full</pre>	<p>銅線インターフェイスの二重通信を設定します。auto 設定がデフォルトです。</p> <p>(注) EtherChannel インターフェイスの二重通信の設定は [Full] または [Auto] である必要があります。</p>

コマンド	目的
<p>ステップ5 (任意)</p> <pre>flowcontrol send on [low_water high_water pause_time] [noconfirm]</pre> <p>例 :</p> <pre>hostname(config-if)# flowcontrol send on 95 200 10000</pre>	<p>1 ギガビットおよび 10 ギガビットのイーサネット インターフェイスでの、フロー制御のポーズ (XOFF) フレームをイネーブルにします。</p> <p>トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。ポーズ (XOFF) および XON フレームは、FIFO バッファ使用量に基づいて、NIC ハードウェアによって自動的に生成されます。バッファ使用量が高ウォーターマークを超えると、ポーズ フレームが送信されます。デフォルトの <i>high_water</i> 値は 128 KB (10 ギガビットイーサネット) および 24 KB (1 ギガビットイーサネット) です。0 ~ 511 (10 ギガビットイーサネット) または 0 ~ 47 KB (1 ギガビットイーサネット) に設定できます。ポーズの送信後、バッファ使用量が低ウォーター マークよりも下回ると、XON フレームを送信できます。デフォルトでは、<i>low_water</i> 値は 64 KB (10 ギガビットイーサネット) および 16 KB (1 ギガビットイーサネット) です。0 ~ 511 (10 ギガビットイーサネット) または 0 ~ 47 KB (1 ギガビットイーサネット) に設定できます。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。デフォルトの <i>pause_time</i> 値は 26624 です。この値は 0 ~ 65535 に設定できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。</p> <p>このコマンドを使用すると、次の警告が表示されます。</p> <pre>Changing flow-control parameters will reset the interface. Packets may be lost during the reset. Proceed with flow-control changes?</pre> <p>プロンプトを表示しないでパラメータを変更するには、noconfirm キーワードを使用します。</p> <p>(注) 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。</p>
<p>ステップ6</p> <pre>no shutdown</pre> <p>例 :</p> <pre>hostname(config-if)# no shutdown</pre>	<p>インターフェイスをイネーブルにします。インターフェイスをディセーブルにするには、shutdown コマンドを入力します。shutdown コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。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シャットダウンします。</p>

次の作業

オプション タスク :

- 冗長インターフェイス ペアを設定します。「冗長インターフェイスの設定」(P.11-27) を参照してください。

- EtherChannel を設定します。「[EtherChannel の設定](#)」(P.11-29) を参照してください。
- VLAN サブインターフェイスを設定します。「[VLAN サブインターフェイスと 802.1Q トランキングの設定](#)」(P.11-33) を参照してください。

必須タスク：

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。「[マルチ コンテキストの設定](#)」(P.6-15) を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 13 章「[インターフェイス コンフィギュレーションの実行 \(ルーテッド モード\)](#)」または第 14 章「[インターフェイス コンフィギュレーションの実行 \(トランスペアレント モード\)](#)」を参照してください。

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、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。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 ASA 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。

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設定](#)」(P.11-27)
- 「[アクティブ インターフェイスの変更](#)」(P.11-29)

冗長インターフェイスの設定

この項では、冗長インターフェイスを作成する方法について説明します。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。

注意事項と制限事項

- 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遅延値は設定可能ですが、デフォルトでは、ASA はそのメンバインターフェイスの物理タイプに基づくデフォルトの遅延値を継承します。
- 「[冗長インターフェイスのガイドライン](#)」(P.11-11) も参照してください。

前提条件

- 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。
- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。まず、その名前を削除する必要があります。名前を削除するには、**no nameif** コマンドを使用します。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

**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。

手順の詳細

	コマンド	目的
ステップ 1	<code>interface redundant number</code> 例: <code>hostname(config)# interface redundant 1</code>	論理冗長インターフェイスを追加します。 <i>number</i> 引数は、1 ~ 8 の整数です。 (注) 冗長インターフェイスの名前などの論理パラメータを設定する前に、少なくとも 1 つのメンバーインターフェイスを冗長インターフェイスに追加する必要があります。
ステップ 2	<code>member-interface physical_interface</code> 例: <code>hostname(config-if)# member-interface management 0/0</code>	最初のメンバインターフェイスを冗長インターフェイスに追加します。 物理インターフェイス ID の説明については、「 物理インターフェイスのイネーブル化およびイーサネットパラメータの設定 (P.11-24) 」を参照してください。 冗長インターフェイスは、管理スロット/ポートインターフェイスをメンバとしてサポートしません。 インターフェイスを追加すると、インターフェイスのコンフィギュレーション (IP アドレスなど) はすべて削除されます。
ステップ 3	<code>member-interface physical_interface</code> 例: <code>hostname(config-if)# member-interface management 1/0</code>	2 番目のメンバインターフェイスを冗長インターフェイスに追加します。 2 つ目のインターフェイスの物理タイプは、必ず最初のインターフェイスと同じにしてください。 メンバーインターフェイスを削除するには、 no member-interface physical_interface コマンドを入力します。冗長インターフェイスから両方のメンバインターフェイスは削除できません。冗長インターフェイスには、少なくとも 1 つのメンバインターフェイスが必要です。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

次の作業

オプション タスク :

- VLAN サブインターフェイスを設定します。「[VLAN サブインターフェイスと 802.1Q トランクリングの設定 \(P.11-33\)](#)」を参照してください。

必須タスク：

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます (固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます)。「[マルチ コンテキストの設定](#)」(P.6-15) を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 13 章「[インターフェイス コンフィギュレーションの実行 \(ルーテッド モード\)](#)」または第 14 章「[インターフェイス コンフィギュレーションの実行 \(トランスペアレント モード\)](#)」を参照してください。

アクティブ インターフェイスの変更

デフォルトでは、コンフィギュレーションで最初にリストされているインターフェイスが (使用可能であれば)、アクティブ インターフェイスになります。どのインターフェイスがアクティブかを表示するには、次のコマンドを入力します。

```
hostname# show interface redundantnumber detail | grep Member
```

たとえば、次のように入力します。

```
hostname# show interface redundant1 detail | grep Member
Members GigabitEthernet0/3 (Active), GigabitEthernet0/2
```

アクティブ インターフェイスを変更するには、次のコマンドを入力します。

```
hostname# redundant-interface redundantnumber active-member physical_interface
```

redundant number 引数には、冗長インターフェイス ID (**redundant1** など) を指定します。

physical_interface には、アクティブにするメンバインターフェイスの ID を指定します。

EtherChannel の設定

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

この項では、次のトピックについて取り上げます。

- 「[EtherChannel へのインターフェイスの追加](#)」(P.11-29)
- 「[EtherChannel のカスタマイズ](#)」(P.11-32)

EtherChannel へのインターフェイスの追加

ここでは、EtherChannel ポートチャネル インターフェイスを作成し、インターフェイスを EtherChannel に割り当てる方法について説明します。デフォルトでは、ポートチャネル インターフェイスはイネーブルになっています。

注意事項と制限事項

- 最大 48 個の EtherChannel を設定できます。
- チャンネル グループ 1 つにつき 8 個のインターフェイスをアクティブにすることができます。1 つのチャンネル グループに最大 16 個のインターフェイスを割り当てることができます。アクティブにできるインターフェイスは 8 個のみですが、残りのインターフェイスはインターフェイスに障害が発生した場合のスタンバイ リンクとして動作できます。

- 4GE SSM (これには ASA 5550 のスロット 1 の統合 4GE SSM も含まれます) 上のインターフェイスを EtherChannel の一部として使用することはできません。
- クラスタリング用にスパンド EtherChannel を設定するには、この手順の代わりに「[スパンド EtherChannel の設定](#)」(P.7-35) を参照してください。
- 「[EtherChannel のガイドライン](#)」(P.11-11) も参照してください。

前提条件

- チャンネル グループのすべてのインターフェイスは、同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。
- 名前が設定されている場合は、物理インターフェイスをチャンネル グループに追加できません。まず、その名前を削除する必要があります。名前を削除するには、**no nameif** コマンドを使用します。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。



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。

手順の詳細

	コマンド	目的
ステップ1	<pre>interface physical_interface</pre> <p>例:</p> <pre>hostname(config)# interface gigabitethernet 0/0</pre>	<p>チャンネル グループに追加するインターフェイスを指定します。<i>physical_interface</i> ID では、タイプ、スロット、ポート番号を <i>type[slot/port]</i> の形式で指定します。チャンネル グループのこの最初のインターフェイスによって、グループ内の他のすべてのインターフェイスのタイプと速度が決まります。</p> <p>トランスペアレント モードで、複数の管理インターフェイスがあるチャンネル グループを作成する場合は、この EtherChannel を管理専用インターフェイスとして使用できます。</p>
ステップ2	<pre>channel-group channel_id mode {active passive on}</pre> <p>例:</p> <pre>hostname(config-if)# channel-group 1 mode active</pre>	<p>1 ~ 48 の <i>channel_id</i> を指定して、この物理インターフェイスを EtherChannel に割り当てます。このチャンネル ID のポートチャンネル インターフェイスがコンフィギュレーションにまだ存在しない場合、ポートチャンネル インターフェイスが作成されます。</p> <pre>interface port-channel channel_id</pre> <p>active モードを使用することを推奨します。アクティブ、パッシブ、およびオンの各モードの詳細については、「リンク集約制御 プロトコル」(P.11-7) を参照してください。</p>

コマンド	目的
<p>ステップ3 (任意)</p> <pre>lacp port-priority number</pre> <p>例 :</p> <pre>hostname(config-if)# lacp port-priority 12345</pre>	<p>チャンネル グループ内の物理インターフェイスのプライオリティを、1 ~ 65535 の範囲で設定します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポート プライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID (スロット/ポート) で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。</p> <p>あるインターフェイスについて、インターフェイス ID は大きいですが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、lacp port-priority の値を、1/3 インターフェイスでは 12345 とし、0/7 インターフェイスではデフォルトの 32768 とします。</p> <p>EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。「EtherChannel のカスタマイズ」(P.11-32) の lacp system-priority コマンドを参照してください。</p>
<p>ステップ4 チャンネル グループに追加するインターフェイスごとに、ステップ 1 ~ 3 を繰り返します。</p>	<p>チャンネル グループの各インターフェイスのタイプと速度が同一であることが必要です。半二重はサポートされません。一致しないインターフェイスを追加すると、一時停止状態になります。</p>

次の作業

オプション タスク :

- EtherChannel インターフェイスをカスタマイズします。「[EtherChannel のカスタマイズ](#)」(P.11-32) を参照してください。
- VLAN サブインターフェイスを設定します。「[VLAN サブインターフェイスと 802.1Q トランクリンクの設定](#)」(P.11-33) を参照してください。

必須タスク :

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます (固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます)。「[マルチ コンテキストの設定](#)」(P.6-15) を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 13 章「[インターフェイス コンフィギュレーションの実行 \(ルーテッド モード\)](#)」または第 14 章「[インターフェイス コンフィギュレーションの実行 \(トランスペアレント モード\)](#)」を参照してください。

EtherChannel のカスタマイズ

この項では、EtherChannel のインターフェイスの最大数、EtherChannel をアクティブにするための動作インターフェイスの最小数、ロード バランシング アルゴリズム、およびその他のオプション パラメータを設定する方法について説明します。

手順の詳細

	コマンド	目的
ステップ 1	<pre>interface port-channel channel_id</pre> <p>例: hostname(config)# interface port-channel 1</p>	<p>ポートチャンネル インターフェイスを指定します。このインターフェイスは、チャンネル グループにインターフェイスを追加したときに自動的に作成されたものです。まだインターフェイスを追加していない場合は、このコマンドを実行するとポートチャンネル インターフェイスが作成されます。</p> <p>(注) 少なくとも 1 つのメンバ インターフェイスをポートチャンネル インターフェイスに追加してからでなければ、インターフェイスの論理パラメータ (名前など) は設定できません。</p>
ステップ 2	<pre>lacp max-bundle number</pre> <p>例: hostname(config-if)# lacp max-bundle 6</p>	<p>このチャンネル グループで許可されるアクティブ インターフェイスの最大数を 1 ~ 8 の範囲内で指定します。デフォルトは 8 です。</p>
ステップ 3	<pre>port-channel min-bundle number</pre> <p>例: hostname(config-if)# port-channel min-bundle 2</p>	<p>ポートチャンネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を、1 ~ 8 の範囲で指定します。デフォルトは 1 です。チャンネル グループ内のアクティブ インターフェイス数がこの値よりも小さい場合、ポートチャンネル インターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。</p>
ステップ 4	<pre>port-channel load-balance {dst-ip dst-ip-port dst-mac dst-port src-dst-ip src-dst-ip-port src-dst-mac src-dst-port src-ip src-ip-port src-mac src-port vlan-dst-ip vlan-dst-ip-port vlan-only vlan-src-dst-ip vlan-src-dst-ip-port vlan-src-ip vlan-src-ip-port}</pre> <p>例: hostname(config-if)# port-channel load-balance src-dst-mac</p>	<p>ロードバランシング アルゴリズムを設定します。デフォルトでは、ASA はパケットの送信元および宛先 IP アドレス (src-dst-ip) に従ってインターフェイスでのパケットの負荷を分散します。パケットの分類の基準となるプロパティを変更する場合は、このコマンドを使用します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロードバランシングの詳細については、「ロード バランシング」(P.11-7) を参照してください。</p>

コマンド	目的
<p>ステップ 5 <code>lACP system-priority number</code></p> <p>例 : <pre>hostname(config)# lACP system-priority 12345</pre></p>	<p>LACP システム プライオリティを 1 ~ 65535 の範囲で設定します。デフォルトは 32768 です。数字が大きいくほど、プライオリティは低くなります。このコマンドは、ASA に対してグローバルです。</p> <p>EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。EtherChannel 内でのインターフェイス プライオリティについては、「EtherChannel へのインターフェイスの追加 (P.11-29) の <code>lACP port-priority</code> コマンドを参照してください。</p>
<p>ステップ 6 (任意)</p> <p>ポートチャネル インターフェイスのイーサネット プロパティを設定します。この設定は、個別 インターフェイスに対して設定されたプロパティよりも優先されます。</p>	<p>これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。イーサネットのコマンドについては、「物理インターフェイスのイーサネットパラメータの設定 (P.11-24) を参照してください。</p>

次の作業

オプション タスク :

- VLAN サブインターフェイスを設定します。「[VLAN サブインターフェイスと 802.1Q トランキングの設定](#) (P.11-33) を参照してください。

必須タスク :

- マルチ コンテキスト モードの場合は、インターフェイスをコンテキストに割り当てます (固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます)。「[マルチ コンテキストの設定](#) (P.6-15) を参照してください。
- シングル コンテキスト モードの場合は、インターフェイス コンフィギュレーションを実行します。第 13 章「[インターフェイス コンフィギュレーションの実行 \(ルーテッド モード\)](#)」または第 14 章「[インターフェイス コンフィギュレーションの実行 \(トランスペアレント モード\)](#)」を参照してください。

VLAN サブインターフェイスと 802.1Q トランキングの設定

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、冗長インターフェイス、または EtherChannel 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 ASA 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。

注意事項と制限事項

- 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 VLAN サブインターフェイス数を決定するには、「[ASA 5510 以降のインターフェイスのライセンス要件](#) (P.11-8) を参照してください。

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスにも当てはまります。サブインターフェイスで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をイネーブルにする必要があるため、**nameif** コマンドを除外して、物理インターフェイスまたは冗長インターフェイスがトラフィックを通過させないようにしてください。物理インターフェイスまたは冗長インターフェイスでタグのないパケットを通過できるようにする場合は、通常どおりに **nameif** コマンドを設定できます。インターフェイス コンフィギュレーションの詳細については、第 13 章「インターフェイス コンフィギュレーションの実行 (ルーテッド モード)」または第 14 章「インターフェイス コンフィギュレーションの実行 (トランスペアレント モード)」を参照してください。
- (ASA 5512-X ~ ASA 5555-X) サブインターフェイスは Management 0/0 インターフェイスでは設定できません。

前提条件

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	<pre>interface {physical_interface redundant number port-channel number}.subinterface</pre> <p>例 :</p> <pre>hostname(config)# interface gigabitethernet 0/1.100</pre>	<p>新しいサブインターフェイスを指定します。物理インターフェイス ID については、「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」の説明を参照してください。</p> <p>redundant number 引数には、冗長インターフェイス ID (redundant 1 など) を指定します。</p> <p>port-channel number 引数は、port-channel 1 などの EtherChannel インターフェイス ID です。</p> <p>subinterface ID は、1 ~ 4294967293 の整数です。</p>
ステップ 2	<pre>vlan vlan_id</pre> <p>例 :</p> <pre>hostname(config-subif)# vlan 101</pre>	<p>サブインターフェイスの VLAN アドレスを指定します。vlan_id は、1 ~ 4094 の整数です。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。</p> <p>1 つの VLAN は 1 つのサブインターフェイスにだけ割り当てることができます。同じ VLAN を複数のサブインターフェイスに割り当ててはできません。VLAN を物理インターフェイスに割り当ててはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために no オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して vlan コマンドを入力すると、ASA によって古い ID が変更されます。</p>

次の作業

(任意) 「ジャンボ フレーム サポートのイネーブル化 (サポート対象のモデル)」(P.11-35) に従って、ジャンボ フレームのサポートをイネーブルにします。

ジャンボ フレーム サポートのイネーブル化 (サポート対象のモデル)

ジャンボ フレームとは、標準的な最大値 1518 バイト (レイヤ 2 ヘッダーおよび FCS を含む) より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能 (アクセス リストなど) の最大使用量が制限される場合があります。

サポート対象のモデルは次のとおりです。

- ASA 5512-X
- ASA 5515-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA 5580
- ASA 5585-X

前提条件

- マルチ コンテキスト モードでは、システム実行スペースでこのオプションを設定します。
- この設定を変更した場合は、ASA のリロードが必要です。
- ジャンボ フレームを送信する必要があるインターフェイスごとに MTU を必ず設定してください。MTU は、`mtu` コマンドを使用して、デフォルト値の 1500 よりも大きい値 (たとえば 9000) に設定します。「[MAC アドレスおよび MTU の設定](#)」(P.13-10) を参照してください。マルチ コンテキスト モードでは、各コンテキスト内で MTU を設定します。

手順の詳細

コマンド	目的
<code>jumbo-frame reservation</code>	ASA 5580 および 5585-X のジャンボ フレームのサポートをイネーブルにします。ジャンボ フレームをディセーブルにするには、このコマンドの <code>no</code> 形式を使用します。
例: <code>hostname(config)# jumbo-frame reservation</code>	

例

次に、ジャンボ フレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
hostname(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted.Command accepted.

hostnamehostname(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
```

```
hostname(config)# reload
Proceed with reload?[confirm] Y
```

インターフェイスのモニタリング

インターフェイスをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
<code>show interface</code>	インターフェイス統計情報を表示します。
<code>show interface ip brief</code>	インターフェイスの IP アドレスとステータスを表示します。
<code>show lacp</code> {[channel_group_number] {counters internal neighbor} sys-id}	EtherChannel の場合は、LACP 情報 (トラフィック統計情報、システム ID、ネイバーの詳細など) が表示されます。
<code>show port-channel</code> [channel_group_number] [brief detail port protocol summary]	EtherChannel の場合は、EtherChannel 情報が、詳細な 1 行サマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
<code>show port-channel</code> channel_group_number load-balance [hash-result {ip ipv6 l4port mac mixed vlan-only} parameters]	EtherChannel の場合は、ポートチャネル負荷分散情報が、指定のパラメータセットに対するハッシュ結果および選択されたメンバインターフェイスとともに表示されます。

ASA 5510 以降のインターフェイスの設定例

この項では、次のトピックについて取り上げます。

- 「物理インターフェイス パラメータの例」 (P.11-36)
- 「サブインターフェイス パラメータの例」 (P.11-36)
- 「マルチ コンテキスト モードの例」 (P.11-37)
- 「EtherChannel の例」 (P.11-37)

物理インターフェイス パラメータの例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
  speed 1000
  duplex full
  no shutdown
```

サブインターフェイス パラメータの例

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1.1
  vlan 101
  no shutdown
```

マルチ コンテキスト モードの例

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
interface gigabitethernet 0/1
  speed 1000
  duplex full
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
context contextA
  allocate-interface gigabitethernet 0/1.1
```

EtherChannel の例

次の例では、3 つのインターフェイスを EtherChannel の一部として設定します。また、システム プライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8 個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

次の作業

- 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ます（固有の MAC アドレスがコンテキスト インターフェイスに自動的に割り当てられます）。第 6 章「マルチ コンテキスト モードの設定」を参照してください。
 - 第 13 章「インターフェイス コンフィギュレーションの実行（ルーテッド モード）」または第 14 章「インターフェイス コンフィギュレーションの実行（トランスペアレント モード）」に従って、インターフェイス コンフィギュレーションを実行します。
- シングル コンテキスト モードの場合は、第 13 章「インターフェイス コンフィギュレーションの実行（ルーテッド モード）」または第 14 章「インターフェイス コンフィギュレーションの実行（トランスペアレント モード）」に従って、インターフェイス コンフィギュレーションを実行します。

ASA 5510 以降のインターフェイスの機能履歴

表 11-3 に、この機能のリリース履歴を示します。

表 11-3 インターフェイスの機能履歴

機能名	リリース	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 <ul style="list-style-type: none"> ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 ASA 5520 の VLAN 数が 25 から 100 に増えました。 ASA 5540 の VLAN 数が 100 から 200 に増えました。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
VLAN 数の増加	7.2(2)	VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 ASA は、Gigabit Ethernet (GE; ギガビットイーサネット) を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の Fast Ethernet (FE; ファストイーサネット) の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。speed コマンドを使用してインターフェイスの速度を変更します。また、show interface コマンドを使用して各インターフェイスの現在の設定速度を確認します。
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボ フレームとは、標準的な最大値 1518 バイト (レイヤ 2 ヘッダーおよび FCS を含む) より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能 (アクセス リストなど) の最大使用量が制限される場合があります。この機能は、ASA 5585-X でもサポートされます。 jumbo-frame reservation コマンドが導入されました。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。

表 11-3 インターフェイスの機能履歴 (続き)

機能名	リリース	機能情報
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ (XOFF) フレームをイネーブルにできるようになりました。 この機能は、ASA 5585-X でもサポートされます。 flowcontrol コマンドが導入されました。
1 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(5)/8.4(2)	すべてのモデルで 1 ギガビット インターフェイスのフロー制御のポーズ (XOFF) フレームをイネーブルにできるようになりました。 flowcontrol コマンドが変更されました。
EtherChannel サポート	8.4(1)	最大 48 個の 802.3ad EtherChannel (1 つあたりのアクティブ インターフェイス 8 個) を設定できます。 channel-group 、 lacp port-priority 、 interface port-channel 、 lacp max-bundle 、 port-channel min-bundle 、 port-channel load-balance 、 lacp system-priority 、 clear lacp counters 、 show lacp 、 show port-channel の各コマンドが導入されました。 (注) EtherChannel は ASA 5505 ではサポートされません。

