CHAPTER 4

インターフェイスの設定

この章では、インターフェイス コンフィギュレーションを実行するためのタスクについて説明します。次の項目を取り上げます。

- 「インターフェイスに関する情報」（P.4-1）
- 「ガイドラインと制限事項」（P.4-4）
- 「デフォルト設定」（P.4-5）
- 「VNMC との通信の設定」（P.4-5）
- 「インターフェイスの設定」（P.4-6）
- 「インターフェイスのモニタリング」（P.4-11）
- 「インターフェイスの機能履歴」（P.4-12）

インターフェイスに関する情報

- 「Ethernet Interfaces」（P.4-1）
- 「セキュリティ プロファイル インターフェイス」（P.4-2）
- 「インターフェイスにセキュリティ ポリシーを適用する方法」（P.4-3）
- 「to-the-box トラフィック」（P.4-3）
- 「vPath タギング」（P.4-3）
- 「インターフェイスのセキュリティ レベル」（P.4-4）

Ethernet Interfaces

最初に ASA 1000V をプロビジョニングする場合は、ASA 1000V イーサネット インターフェイスの Nexus 1000V ポート プロファイルに対応するポート グループに、これらのインターフェイスを関連付けます。Nexus 1000V ポート プロファイルでは、インターフェイスに対する他のスイッチ パラメータを指定する他、VLAN にインターフェイスを関連付けます。複数のインターフェイスに同じポート プロファイルを割り当てると、これらのインターフェイスに同じスイッチポート設定を適用した効果があります。ポート プロファイル設定の詳細については、Nexus 1000V のドキュメントを参照してください。

それぞれの ASA 1000V は、データおよびフェールオーバー トラフィックに使用可能な 4 種類のイーサネット インターフェイスを提供します。管理用に 1 つ、通過トラフィック用に 2 つ、フェールオーバー リンク用に 1 つです。

- Management 0/0：管理専用トラフィック用、ASA 1000V を配置したときに指定した IP アドレスのパラメータで **management** という名前が指定されます。必要に応じて、この章を使用してこれらのパラメータを変更できますが、名前は固定されます。
- GigabitEthernet 0/0：この章に従って、このインターフェイスをデータ インターフェイスとして設定します。
- GigabitEthernet 0/1：この章に従って、このインターフェイスをデータ インターフェイスとして設定します。
- GigabitEthernet 0/2：フェールオーバー トラフィック用、ASA 1000V の配置時に指定した IP アドレスのパラメータによります。フェールオーバー リンク パラメータを変更するには、第 3 章「アクティブ/スタンバイ フェールオーバーの設定」を参照してください。

内部（高セキュリティ レベル）インターフェイスおよび *外部*（低セキュリティ レベル）インターフェイスとして 2 つのデータ インターフェイスを設定します。セキュリティ レベルの詳細については、「インターフェイスのセキュリティ レベル」（P.4-4）を参照してください。

セキュリティ プロファイル インターフェイス

セキュリティ プロファイル インターフェイスは、Nexus 1000V セキュリティ プロファイルに対応します。特定のネットワークでは、セキュリティ プロファイルは、他の仮想マシン（VM）から VM のクラスを分離することもできます。たとえば、アプリケーション サーバからの Web サーバの分離などです。セキュリティ プロファイルは、IP アドレスに基づく代わりに、VM のクラスに基づいてセキュリティ ポリシーを適用することができます。

- 「VNMC とのセキュリティ プロファイルの調整」（P.4-2）
- 「内部インターフェイスのセキュリティ プロファイル」（P.4-2）
- 「インターフェイス ベースのポリシー」（P.4-2）
- 「セキュリティ プロファイル インターフェイスのポート プロファイル」（P.4-3）

VNMC とのセキュリティ プロファイルの調整

ASA 1000V でセキュリティ プロファイル インターフェイスを作成すると、同じ名前のセキュリティ プロファイルが Cisco VNMC に自動的に追加され、Nexus 1000V のポート プロファイルで使用できるようになります。

内部インターフェイスのセキュリティ プロファイル

トラフィックが ASA 1000V の内部インターフェイスに入ると、ASA 1000V は、パケットに含まれるタグ（*vPath タギング*という。「vPath タギング」（P.4-3）を参照）に基づいてトラフィックのセキュリティ プロファイルを識別できます。ASA 1000V でセキュリティ プロファイルのトラフィックを受信できるのは、1 つのイーサネット インターフェイス上、つまりサービス インターフェイス（内部インターフェイスであることが必要です）上に限られます。サービス インターフェイスは自動的に内部インターフェイスになります。外部インターフェイスのトラフィックにタグは付きません。

インターフェイス ベースのポリシー

ASA オペレーティング システムにはインターフェイス ベースのセキュリティ ポリシーがあります。セキュリティ プロファイルは、ASA のインターフェイス ベースのポリシーを利用するために、ASA 内の「インターフェイス」として扱われます。セキュリティ プロファイルは、内部インターフェイスで送受信されるすべてのトラフィックのサブセットである、トラフィックのクラスです。

セキュリティ プロファイル インターフェイスのポート プロファイル

イーサネット インターフェイスのように、セキュリティ プロファイル インターフェイスは Nexus 1000V ポート プロファイルにも関連付けられます。セキュリティ プロファイルが内部イーサネット インターフェイスに関連付けられているように、セキュリティ プロファイルの Nexus 1000V ポート プロファイルは、内部インターフェイスのポート プロファイルと同じ VLAN 上に存在する必要があります。

インターフェイスにセキュリティ ポリシーを適用する方法

セキュリティ ポリシーでは、トラフィックの許容動作が決まります。パケットが外側から内側に許可されるかどうか、内部ネットワークで NAT を実行するかどうか、外部のサーバへのアクセス時に内部からのトラフィックに対してインスペクションを適用するかどうかなどです。機能によっては、機能を適用する 1 つ以上のインターフェイスの識別が必要な場合があります。

外部インターフェイスを参照する必要があるすべての機能は、外部イーサネット インターフェイスを直接参照する必要があります。セキュリティ プロファイルは内部インターフェイス（サービス インターフェイス）に関連付けられているだけなので、内部インターフェイスに適用されるすべての機能は、内部インターフェイスを直接参照するのではなく、特定のセキュリティ プロファイルを参照する必要があります。セキュリティ ポリシーの目的として、内部インターフェイスが別々のセキュリティ プロファイルに分かれます。

ただし、ルーティングや DHCP サーバなど、ネットワーク トポロジを制御する機能では、内部インターフェイスを直接参照する必要があります。

to-the-box トラフィック

to-the-box 管理トラフィックは、セキュリティ プロファイル インターフェイスではなく、内部イーサネット インターフェイスによって受信されます。同様に、from-the-box トラフィックは、内部インターフェイスから送信されます。

vPath タギング

Nexus 1000V は、ASA 1000V の内部インターフェイスと同じ宛先 MAC アドレスを持つトラフィックに、vPath タギングを適用します。

ASA 1000V が内部インターフェイスでタグ付けされていない通過トラフィックを受信した場合、ASA 1000V は、パケットをドロップします（ドロップされたパケットを表示するには、**show asp drop** コマンドを参照してください）。

ブロードキャストおよびマルチキャスト トラフィックはタグ付けされません（ARP および DHCP）。ブロードキャストおよびマルチキャスト トラフィックは、セキュリティ プロファイル インターフェイスではなく、ASA 1000V の内部イーサネット インターフェイスで処理されます。

インターフェイスのセキュリティ レベル

イーサネット インターフェイスとセキュリティ プロファイル インターフェイスは、セキュリティ レベルを使用します。

- 内部インターフェイスのセキュリティ レベルは 100（最高）です。このレベルをそのままにすることを推奨します。
- セキュリティ プロファイル インターフェイスのセキュリティ レベルは 0 です。このレベルをより高いセキュリティ レベル（たとえば、100）に変更する必要があります。
- 外部インターフェイスのセキュリティ レベルは 0（最低）です。このレベルをそのままにすることを推奨します。
- 管理インターフェイスのセキュリティ レベルは 0 です。このレベルをそのままにすることを推奨します。

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。同じセキュリティ レベルのインターフェイス間では通信できません。
- 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。
  - 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 ASA を通過することが許可されます。

ガイドラインと制限事項

フェールオーバーのガイドライン

フェールオーバー リンクを設定するには、第 3 章「アクティブ/スタンバイ フェールオーバーの設定」を参照してください。

その他のガイドライン

- Management 0/0 インターフェイスは管理専用インターフェイスとしてだけ設定できます。
- 最大 256 のセキュリティ プロファイル インターフェイスを作成できます。
- ASA 1000V では、ジャンボ イーサネット パケットがサポートされます。必要に応じて MTU および TCP の最大セグメント サイズを設定します。

デフォルト設定

デフォルトのセキュリティ レベル

- 内部インターフェイスのセキュリティ レベルは 100（最高）です。このレベルをそのままにすることを推奨します。
- セキュリティ プロファイル インターフェイスのセキュリティ レベルは 0 です。このレベルをより高いセキュリティ レベル（たとえば、100）に変更する必要があります。
- 外部インターフェイスのセキュリティ レベルは 0（最低）です。このレベルをそのままにすることを推奨します。
- 管理インターフェイスのセキュリティ レベルは 0 です。このレベルをそのままにすることを推奨します。

インターフェイスのデフォルトの状態

- イーサネット インターフェイス：ディセーブル。
- 管理インターフェイス：ASA 1000V の配置の一部としてイネーブルになります。
- セキュリティ プロファイル インターフェイス：ディセーブル。

デフォルトの速度およびデュプレックス

デフォルトでは、イーサネット インターフェイスの速度とデュプレックスはオートネゴシエーションに設定されます。

デフォルトの MAC アドレス

デフォルトでは、イーサネット インターフェイスは、ASA 1000V を配置したときに動的に割り当てられた MAC アドレスを使用します。すべての関連するセキュリティ プロファイル インターフェイスが同じ MAC アドレスを使用します。

VNMC との通信の設定

セキュリティ プロファイル インターフェイスを設定する前に VNMC との通信をイネーブルにする必要があります。

手順の詳細

	コマンド	目的
ステップ 1	**vnmc policy-agent** **例：** `hostname (config)# vnmc policy-agent`	ASA 1000V が VNMC と通信できるようにして、VNMC ポリシー エージェント コンフィギュレーション モードを開始します。
ステップ 2	**login username** *username* **password** *password* **例：** `hostname(config-vnmc-policy-agent)# login username exampleuser1 password cisco123`	VNMC のログイン クレデンシャルを指定します。アカウントには VNMC の管理者権限が必要です。

	コマンド	目的
ステップ 3	**shared-secret** *shared-secret* **例：** `hostname(config-vnmc-policy-agent)# shared-secret adamyauchrip`	VNMC への ASA 1000V の接続を暗号化するための共有秘密を指定します。共有秘密は、セキュリティ上の目的で非表示になります。 VNMC および ASA 1000V が同じキーを共有します。管理対象エンド ポイント（ASA 1000V）が VNMC に要求を送信すると、ASA 1000V は認証用のハッシュ値を含めます。VNMC は同じハッシュ生成アルゴリズムを使用して、要求が信頼できるソースからのものであるかどうかを判断できます。ハッシュ値を生成するために VNMC の IP アドレスが共有秘密情報とともに使用されるため、VNMC の IP アドレスは VNMC の実際の IP アドレスである必要があります（NAT で変更されない）。一方、IP アドレスのハッシュ確認は VNMC で失敗します。ASA 1000V と VNMC 間の NAT はサポートされていません。
ステップ 4	**registration host** *ip_address* **例：** `hostname(config-vnmc-policy-agent)# registration host 192.168.1.1`	VNMC を実行しているホストの IP アドレスまたはホスト名を指定します。
ステップ 5	**vnmc org** *org-path* **例：** `hostname(config)# vnmc org root/tenant1/datacenter1/application1/tier1`	組織パスを設定します。VSM で設定された組織階層と一致するように、ASA 1000V で組織階層を設定する必要があります。組織パスは次の形式でなければなりません。 **root**/*name_of_tenant*/*name_of_datacenter*/*name_of_application*/*name_of_tier* 最大 4 個のレイヤが許可され、組織パスが **root/** ディレクトリの下にある必要があります。 それぞれの ASA 1000V で、一意の組織パスを指定する必要があります。VNMC のこの ORG パスで割り当てられた別の ASA 1000V は存在できません。 **（注）** 次の手順に進む前に、VNMC ポリシー エージェントが開始されて、登録されていることを確認します。

インターフェイスの設定

ここでは、次の内容について説明します。

- 「内部および外部イーサネット インターフェイスの設定」（P.4-7）
- 「セキュリティ プロファイル インターフェイスの設定」（P.4-9）
- 「セキュリティ プロファイル インターフェイスのイーサネット インターフェイスへの関連付け」（P.4-9）
- 「vPath MTU の設定」（P.4-10）

内部および外部イーサネット インターフェイスの設定

この項では、内部インターフェイスと外部インターフェイスの名前、IPv4 アドレスなどのオプションを設定する方法について説明します。

管理インターフェイスのパラメータを変更する場合にも、この手順を使用できます。

ガイドラインと制限事項

フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバー リンクとステート リンクを設定するには、第 3 章「アクティブ/スタンバイ フェールオーバーの設定」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**interface gigabitethernet 0/**{**0** | **1**} **例：** `hostname(config)# interface gigabitethernet 0/0`	内部インターフェイスまたは外部インターフェイスに使用するイーサネット インターフェイスである、GigabitEthernet 0/0 または 0/1 のいずれかを指定します。
ステップ 2	**nameif** *name* **例：** `hostname(config-if)# nameif inside`	インターフェイスに名前を付けます。 *name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。
ステップ 3	次のいずれかを実行します。	
	ip address *ip_address* [*mask*] [**standby** *ip_address*] **例：** `hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2`	IP アドレスを手動で設定します。 **（注）** 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。 *ip_address* 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。 **standby** *ip_address* 引数は、フェールオーバーで使用します。詳細については、第 3 章「アクティブ/スタンバイ フェールオーバーの設定」を参照してください。
	ip address dhcp [**setroute**] **例：** `hostname(config-if)# ip address dhcp`	DHCP サーバから IP アドレスを取得します。 **setroute** キーワードを指定すると、ASA 1000V で DHCP サーバの提供するデフォルト ルートを使用できるようにします。 DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。 **ip address dhcp** コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスをイネーブルにしなかった場合、DHCP 要求が送信されないことがあります。

	コマンド	目的
ステップ 4	（任意） **speed** {**auto** | **10** | **100** | **1000** | **nonegotiate**} **例：** hostname(config-if)# speed 100	速度を設定します。**auto** 設定がデフォルトです。**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。
ステップ 5	（任意） **duplex** {**auto** | **full** | **half**} **例：** hostname(config-if)# duplex full	デュプレックスを設定します。**auto** 設定がデフォルトです。
ステップ 6	（任意） **mac-address** *mac_address* [**standby** *mac_address*] **例：** hostname(config-if)# mac-address 000C.F142.4CDE	プライベート MAC アドレスをこのインターフェイスに割り当てます。*mac_address* 引数は、H.H.H 形式で指定します。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。 自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。 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 ASA 1000V がフェールオーバーし、スタンバイ ASA 1000V がアクティブになると、新しいアクティブ ASA 1000V 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 ASA 1000V はスタンバイ アドレスを使用します。
ステップ 7	**no shutdown** **例：** hostname(config-if)# no shutdown	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。
ステップ 8	（任意） **mtu** *interface_id bytes* **例：** hostname(config)# mtu gigabitethernet0/1 9200	通常またはジャンボ イーサネット パケットの最大伝送単位（MTU）を、64 ～ 9216 バイトの範囲で設定します。デフォルトは 1500 バイトです。ジャンボ パケットの場合、この値をたとえば 9000 のように高く設定します。この値は、「vPath MTU の設定」（P.4-10）で設定する vPath MTU よりも大きい値には設定できません。最適なパフォーマンスを得るには、vPath MTU の最大値から 164 バイト（82 バイトの最大 vPath ヘッダーのサイズの 2 倍）を引いた値にインターフェイス MTU を設定します。インターフェイス名ではなく、インターフェイス ID を指定してください。
ステップ 9	外部インターフェイスを設定するには、他の使用可能なインターフェイスに対してこの手順を繰り返します。	

セキュリティ プロファイル インターフェイスの設定

セキュリティ プロファイル 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。

手順の詳細

	コマンド	目的
ステップ 1	**interface security-profile** *number* **例：** `hostname (config)# interface security-profile1`	セキュリティ プロファイル インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。*number* 引数は、1 ～ 256 のセキュリティ プロファイル インターフェイス ID を指定します。
ステップ 2	**nameif** *interface_name* **例：** `hostname (config-if)# nameif profile1-ifc`	インターフェイスに名前を付けます。この名前は、ASA 1000V のコンフィギュレーション内だけで使用されます。 *name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。
ステップ 3	**security-profile** *security_profile_name* **例：** `hostname(config-if)# security-profile test-profile-1`	セキュリティ プロファイルの名前を指定します。*security-profile_name* 引数は、1 ～ 256 文字の範囲で指定できます。セキュリティ プロファイル インターフェイスを追加する場合、この名前を使用して、VNMC のセキュリティ プロファイルが作成されます。 同一のセキュリティ プロファイル名を 2 つの異なるセキュリティ プロファイル インターフェイスに関連付けることはできません。このタイプの設定には、エラー メッセージが表示されます。 古いセキュリティ プロファイル名が取り除かれるまで、設定されたセキュリティ プロファイルの名前は変更できません。セキュリティ プロファイルがインターフェイスで削除されるとすぐに、そのセキュリティ プロファイル インターフェイスに基づくすべての接続がクリアされます。
ステップ 4	**no shutdown** **例：** `hostname(config-if)# no shutdown`	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。

セキュリティ プロファイル インターフェイスのイーサネット インターフェイスへの関連付け

内部インターフェイスをサービス インターフェイスとして識別することによって、すべてのセキュリティ プロファイルを内部インターフェイスに関連付ける必要があります。

手順の詳細

コマンド	目的
service-interface security-profile all *inside_interface_name* **例：** `hostname(config-if)# service-interface security-profile all inside`	セキュリティ プロファイル インターフェイスを内部イーサネット インターフェイスに関連付けます。

vPath MTU の設定

ASA 1000V は、vPath と呼ばれるパケット リダイレクションのメカニズムを使用して、仮想マシン（VM）からカプセル化パケットを受信します（「vPath タギング」（P.4-3）を参照）。vPath ヘッダーのサイズ（最大 82 バイト）が原因で、vPath ヘッダーが追加された後、ペイロードでフラグメンテーションが必要になる可能性があります。ASA 1000V には、これらの追加バイトを構成するために VM が MTU を小さくする必要がなく、このオーバーヘッドを透過的に処理する機能があります。ASA 1000V は、イーサネット上でフラグメントを送信する前に vPath カプセル化を追加するとき、アップリンク MTU を超過するパケットを 2 個の vPath フラグメントに分割できます。vPath フラグメントは、パケットが宛先 VM に配信される前に、Nexus 1000V スイッチの仮想イーサネット モジュール（VEM）によって再構成されます。

vPath の MTU 設定は、ASA 1000V から宛先 VM のパスの MTU に従うように、ASA 1000V の vPath モジュールがパケットをフラグメント化する方法を設定します。vPath モジュールは ASA 1000V の IP レイヤの下で動作し、このため、IP フラグメンテーションから独立しています（「内部および外部イーサネット インターフェイスの設定」（P.4-7）を参照）。ASA 1000V の VEM および vPath モジュールは、VM および ASA 1000V に対して有効な IP データグラム（フラグメントまたは別の方法）を示すために連動します。ASA 1000V は、vPath の追加オーバーヘッドをあらかじめ構成する TCP MSS 設定を適用します。

ASA 1000V および VM 間のパスに他のカプセル化が存在する場合があります。たとえば、VXLAN が ASA 1000V および VM 間で使用されている場合、追加の 50 バイトがパケットに使用されます。

追加のオーバーヘッドが存在する場合に vPath のフラグメンテーションを回避するには、次のいずれかを実行します。

- VXLAN カプセル化（50 バイト）に対応するように vPath MTU を小さくします。vPath MTU のデフォルト値は 9000 バイトで、これは、Nexus 1000V のアップリンク ポートのデフォルトの MTU と一致します。たとえば、vPath MTU を 8950 に設定します。
- vPath のフラグメンテーションを回避するためにアップリンクの MTU を増やし、VXLAN カプセル化を許可します。VXLAN カプセル化に対応するには、Nexus 1000V の MTU を 9050 に増やすことができます。
- 追加オーバーヘッドを構成するように、VM の MTU 設定を減らします。

手順の詳細

コマンド	目的
vpath path-mtu *bytes* **例：** `hostname(config)# vpath path-mtu 9200`	vPath MTU のしきい値を設定します。*bytes* 引数は、Nexus 1000V スイッチへの物理アップリンク インターフェイスで、送信できる MTU を 64 ～ 65535 の範囲で定義します。デフォルト値は 9000 バイトです。MTU は 164 バイト以上（最大 82 バイトの最大 vPath ヘッダーのサイズの 2 倍）にする必要があります。

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
show interface	インターフェイス統計情報を表示します。
show interface ip brief	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。
show interface security-profile	実行時ステータスとセキュリティ プロファイル インターフェイスの統計情報を表示します。
show running-config interface	現在の実行コンフィギュレーションのインターフェイス統計情報を表示します。
show running-config mtu	現在の実行コンフィギュレーションの MTU を表示します。
show running-config vnmc policy-agent	VNMC ポリシー エージェントの実行コンフィギュレーションを表示します。
show vm	メモリおよび CPU リソースの推奨値、および実行中の VM によるリアルタイムの実際の CPU リソースの使用状況を表示します。
show vnmc policy-agent	VNMC ポリシー エージェントのステータスを表示します。
show vsn ip-binding	設定されたセキュリティ プロファイル インターフェイスに一致している宛先 IP アドレスを表示します。
show vsn security-profile	すべての設定されたセキュリティ プロファイル インターフェイスのセキュリティ プロファイル ID を表示します。

インターフェイスの機能履歴

表 4-1 にリリース履歴を示します。

表 4-1　インターフェイスの機能履歴

機能名	リリース	機能情報
セキュリティ プロファイル インターフェイス	8.7(1)	セキュリティ プロファイル インターフェイスが導入されました。セキュリティ プロファイル インターフェイスは、Nexus 1000V セキュリティ プロファイルに対応します。特定のネットワークでは、セキュリティ プロファイルは、他の仮想マシン（VM）から VM のクラスを分離することもできます。たとえば、アプリケーション サーバからの Web サーバの分離などです。セキュリティ プロファイルは、IP アドレスに基づく代わりに、VM のクラスに基づいてセキュリティ ポリシーを適用することができます。 次のコマンドを導入または変更しました。**interface security-profile**、**security-profile**、**mtu**、**vpath path-mtu**、**clear interface security-profile**、**clear configure interface security-profile**、**show interface security-profile**、**show running-config interface security-profile**、**show interface ip brief**、**show running-config mtu**、**show vsn ip binding**、**show vsn security-profile**
サービス インターフェイス	8.7(1)	サービス インターフェイスは、セキュリティ プロファイル インターフェイスに関連付けられたイーサネット インターフェイスです。内部インターフェイスであることが必要なサービス インターフェイスを 1 つだけ設定できます。 コマンド **service-interface security-profile all** が導入されました。
VNMC ポリシー エージェント	8.7(1)	VNMC ポリシー エージェントは ASDM および VNMC モードの両方でポリシー設定をイネーブルにします。HTTPS 経由で Cisco VNMC から XML ベースの要求を受信し、ASA 1000V 設定に変換する Web サーバが含まれます。 次のコマンドが導入されました。**vnmc policy-agent**、**login**、**shared-secret**、**registration host**、**vnmc org**、**show vnmc policy-agent**、**show running-config vnmc policy-agent**、**clear configure vnmc policy-agent**