



インターフェイスの設定

この章では、さまざまなインターフェイス モードとセンサー上のインターフェイスの設定方法について説明します。この章は、次の項で構成されています。

- [インターフェイスの説明 \(P.3-2\)](#)
- [混合モードの説明 \(P.3-3\)](#)
- [インライン インターフェイス モードの説明 \(P.3-3\)](#)
- [インライン VLAN ペア モードの説明 \(P.3-4\)](#)
- [インターフェイス サポート \(P.3-5\)](#)
- [インターフェイスの設定上の制限 \(P.3-7\)](#)
- [サマリー \(P.3-9\)](#)
- [インターフェイスの設定 \(P.3-10\)](#)
- [インライン インターフェイス ペアの設定 \(P.3-14\)](#)
- [インライン VLAN ペアの設定 \(P.3-17\)](#)
- [バイパス モードの設定 \(P.3-21\)](#)
- [トラフィック フロー通知の設定 \(P.3-23\)](#)

インターフェイスの説明

コマンド/コントロール インターフェイスは、特定のインターフェイスに恒常的にマッピングされます。この物理インターフェイスは、使用しているセンサーのタイプによって異なります。センシング インターフェイスは、混合モード、インライン インターフェイス モード、またはインライン VLAN ペア モードで動作するように設定できます。インライン インターフェイス モードをサポートするセンサーでは、センシング インターフェイスを「インラインペア」と呼ばれる論理インターフェイスのペアにできます。VLAN をサポートするセンサーでは、VLAN をインライン VLAN ペアにできます。センサーがトラフィックを監視する前に、インターフェイス、インターフェイス ペア、または VLAN ペアをイネーブルにする必要があります。



(注)

アプライアンスでは、センシング インターフェイスはデフォルトでディセーブルになっています。モジュールでは、センシング インターフェイスは常にイネーブルで、ディセーブルにはできません。

インライン VLAN ペア (on-a-stick) 機能の追加により、各センシング インターフェイスは混合モード、インライン インターフェイス モード、インライン VLAN ペア モードの3つのモードのいずれかで動作するようになりました。複数のセンシング インターフェイスを備えたセンサー上では、同一センサー上でモードを任意に組み合わせて使用できます。

- センシング インターフェイスがインライン インターフェイス ペアの別のセンシング インターフェイスとペアになり、そのサブインターフェイス タイプが `none` に設定されている (デフォルト) 場合、そのセンシング インターフェイスはインラインモードになります。
- センシング インターフェイスのサブインターフェイス タイプがインライン VLAN ペアに設定されている場合、そのセンシング インターフェイスはインライン VLAN ペア モードになります。
- デフォルト、つまり他の2つのどちらのモードでもない場合、センシング インターフェイスは混合モードです。

センシング インターフェイスには IP アドレスが割り当てられていないため、攻撃者からは見えません。このため、センサーは、見張っていることを攻撃者に気づかれずにデータ ストリームを監視できます。混合モードは、ネットワークに出入りするすべてのパケットがセンサーを通過する必要があるインライン インターフェイス モードと対照的です。詳細については、[P.3-3 の「混合モードの説明」](#)、[P.3-3 の「インライン インターフェイス モードの説明」](#)、および [P.3-4 の「インライン VLAN ペア モードの説明」](#) を参照してください。

センサーは、デフォルトの仮想センサーに割り当てられているインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア上のトラフィックのみを監視します。詳細については、[P.4-3 の「インターフェイスの仮想センサーへの割り当て」](#) を参照してください。

SensorApp が動作していない場合にもトラフィックがインライン ペアを経由して流れるようにセンサーを設定するには、バイパス モードをイネーブルにします。バイパス モードでは、再設定、サービス パックのインストール、またはソフトウェア障害時のデータフローの中断が最小限に抑えられます。

センサーは、シャーシの電源が切れている間に、インストールされているモジュールのインターフェイスを検出します。それらのインターフェイスは、次回センサーを起動するときに設定できます。モジュールが取り外されている場合、センサーは次の起動時に、インターフェイスがないことを検出します。インターフェイス設定は保持されますが、インターフェイスが存在しない場合はセンサーによって無視されます。

次のインターフェイス設定イベントは、ステータス イベントとして報告されます。

- リンク アップまたはリンク ダウン

- トラフィックの開始または停止
- バイパスモードの自動アクティブ化または非アクティブ化
- パケット失敗率のしきい値の超過

混合モードの説明

混合モードでは、パケットはIPSを経由して流れません。センサーは、実際に転送されたパケットではなく、監視したトラフィックのコピーを分析します。混合モードで運用する利点は、転送されたトラフィックでパケットのフローにIPSが影響を与えないことです。ただし、混合モードで運用する場合の短所は、悪意のあるトラフィックがアトミックアタック（シングルパケット攻撃）などの特定の種類の攻撃のために意図したターゲットに到達するのを、IPSが阻止できないことです。混合IPSデバイスによって実行される応答アクションはイベント後の応答であるため、多くの場合、攻撃に応答するには、ルータやファイアウォールなど他のネットワークングデバイスによるサポートが必要です。このような応答アクションは一部の種類の攻撃を防ぐことができますが、アトミックアタックの場合、混合モードベースのセンサーが管理対象デバイス（ファイアウォール、スイッチ、ルータなど）にACL修正を適用する前に、シングルパケットがターゲットシステムに到達する可能性があります。

インラインインターフェイスモードの説明

インラインインターフェイスモードで動作すると、IPSは直接トラフィックフローに挿入され、パケット転送速度に影響を与えます。パケット転送速度は遅延を加えられることによって遅くなります。インラインIPSはファーストパスにあります。ファーストパスでは、センサーが、意図したターゲットに到達する前に悪意のあるトラフィックを廃棄することによって攻撃を阻止し、保護サービスを提供できます。インラインデバイスは、レイヤ3および4で情報を処理するだけでなく、より高度な埋め込み型攻撃のパケットの内容およびペイロードも分析します（レイヤ3～7）。このより詳細な分析では、通常は従来のファイアウォールデバイスを通過する攻撃をシステムが識別し、停止またはブロックすることができます。

インラインインターフェイスモードでは、パケットはセンサーのペアの1つ目のインターフェイスを経由して入り、ペアの2つ目のインターフェイスを経由して出ます。パケットは、シグニチャによって拒否または変更されない限り、ペアの2つ目のインターフェイスに送信されます。



(注) ASA SSMは、センシングインターフェイスが1つしかない場合にもインラインで動作するように設定できます。

インライン VLAN ペア モードの説明

物理インターフェイス上で VLAN をペアに関連付けることができます。これは「inline on a stick」として知られています。ペアの VLAN のいずれかで受信されたパケットは、分析された後、別の VLAN にペアで転送されます。インライン VLAN ペアは、NM-CIDS、AIP SSM 10、および AIP SSM 20 を除く、IPS 5.1 と互換性があるすべてのセンサーでサポートされています。

インライン VLAN ペア モードは、アクティブ センシング モードです。このモードでは、センシング インターフェイスが 802.1q トランク ポートとして動作し、センサーがトランク上の VLAN ペア間の VLAN ブリッジングを実行します。センサーは、ペアごとに各 VLAN 上で受信するトラフィックを調べ、そのパケットをペアの他方の VLAN へ転送するか、または侵入の試行が検出された場合はパケットを破棄することができます。IPS センサーでは、各センシング インターフェイスで最大 255 個の VLAN ペアを同時にブリッジするように設定できます。センサーは、受信した各パケットの 802.1q ヘッダー内の VLAN ID フィールドをセンサーがパケットを転送する出力 VLAN の ID に置き換えます。センサーは、インライン VLAN ペアに割り当てられていない VLAN 上で受信されたパケットをすべてドロップします。

インターフェイス サポート

表 3-1 は、IPS 5.1 を実行するアプライアンスおよびモジュールのインターフェイス サポートを示します。

表 3-1 インターフェイス サポート

ベース シャーシ	追加された PCI カード	インラインをサポートするインターフェイス	可能なポートの組み合わせ	インラインをサポートしていないインターフェイス
IDS-4210	—	なし	なし	すべて
IDS-4215	—	なし	なし	すべて
IDS-4215	4FE	FastEthernet0/1 4FE FastEthernetS/0 ¹ FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3 0/1<->1/0 0/1<->1/1 0/1<->1/2 0/1<->1/3	FastEthernet0/0
IDS-4235	—	なし	なし	すべて
IDS-4235	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4235	TX (GE)	TX オンボード + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 または GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	—	なし	なし	すべて
IDS-4250	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4250	TX (GE)	TX オンボード + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 または GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	SX	なし	なし	すべて
IDS-4250	SX + SX	2 SX GigabitEthernet1/0 GigabitEthernet2/0	1/0<->2/0	GigabitEthernet0/0 GigabitEthernet0/1

表 3-1 インターフェイス サポート (続き)

ベース シャーシ	追加された PCI カード	インラインをサポートするインターフェイス	可能なポートの組み合わせ	インラインをサポートしていないインターフェイス
IDS-4250	XL	XL GigabitEthernet2/0 の 2 SX GigabitEthernet2/1	2/0<->2/1	GigabitEthernet0/0 GigabitEthernet0/1
IDSM-2	—	ポート 7 および 8 GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2
IPS-4240	—	4 オンボード GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4255	—	4 オンボード GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
NM-CIDS	—	なし	なし	すべて
AIP SSM 10	—	GigabitEthernet0/1	セキュリティ コンテキスト による	GigabitEthernet0/0
AIP SSM 20	—	GigabitEthernet0/1	セキュリティ コンテキスト による	GigabitEthernet0/0

1. 4FE カードはスロット 1 または 2 のどちらかにインストールできます。S はスロット番号を示しており、1 または 2 のどちらかになります。

インターフェイスの設定上の制限

センサー上のインターフェイスの設定については、次の制限があります。

- インライン モードをサポートするセンサー プラットフォームでは、バイパス モードを設定してインラインインターフェイス ペアを作成することしかできません。
- インライン インターフェイス ペアには、物理インターフェイスのタイプ（銅または光ファイバ）、速度、またはインターフェイスの二重通信設定に関係なく、任意のセンシング インターフェイスの組み合わせを含めることができます。ただし、メディア タイプ、速度、および二重通信設定の異なるインターフェイスの組み合わせについては、テストが不完全だったり、正式にサポートされていない場合があります。
- モジュール（IDSM-2、NM-CIDS、AIP SSM 10、および AIP SSM 20）、IPS-4240、および IPS-4255 では、すべてのバックプレーン インターフェイスの速度、二重通信、状態の設定は固定です。これらの設定は、すべてのバックプレーン インターフェイスのデフォルト設定内で保護されています。
- NM-CIDS 上で、センシング インターフェイスとして機能する同一バックプレーン インターフェイスは、RBCP 制御トラフィックも伝送します。このインターフェイスがダウンすると、モジュールも失敗します。バックプレーン インターフェイスは保護されているため、このインターフェイスがダウン状態になるよう設定することはできません。ただし、Linux `ifconfig` ユーティリティを使用してこのインターフェイスのダウン状態を設定している場合、RBCP 通信は失敗します。
- 代替 TCP リセット インターフェイス
 - 代替 TCP リセット インターフェイスはセンシング インターフェイスにしか割り当てできません。管理インターフェイスを代替 TCP リセット インターフェイスとして設定することはできません。代替 TCP リセット インターフェイス オプションは、デフォルトとして **none** に設定されており、センシング インターフェイスを除くすべてのインターフェイス用に保護されています。
 - 同じ物理インターフェイスを複数のセンシング インターフェイスの代替 TCP リセット インターフェイスとして割り当てることができます。
 - 物理インターフェイスは、センシング インターフェイスと代替 TCP リセット インターフェイスの両方として機能できます。
- インライン VLAN ペア内で VLAN を指定する順序は重要ではありません。
- インライン VLAN ペア モードのセンシング インターフェイスは、1 ~ 255 個のインライン VLAN ペアを保持できます。

次のインターフェイスの組み合わせは無効です。

- 管理インターフェイスはセンシング インターフェイスとして機能することはできません。
- 管理インターフェイスは、センシング インターフェイスの代替 TCP リセット インターフェイスとして機能することはできません。
- 管理インターフェイスは、インライン インターフェイス ペアのメンバにすることはできません。
- 物理インターフェイスとインライン インターフェイス ペア内のそれ自体とをペアにすることはできません。
- 物理インターフェイスは、最大 1 つのインライン インターフェイス ペアのメンバにすることができます。
- センシング インターフェイスは、それ自身の代替 TCP リセット インターフェイスとしては機能できません。
- TCP リセットに対応しているインターフェイスのみを代替 TCP リセット インターフェイスとして設定できます。



(注) この制限事項の例外が IDSM-2 です。両方のセンシング インターフェイスに対する代替 TCP リセット インターフェイスの割り当ては System0/1 です (保護されています)。

- VLAN はそれ自体とペアにすることはできません。
- 特定のセンシング インターフェイスの場合、VLAN は最大 1 つのインライン VLAN ペアのメンバにすることができます。ただし、特定の VLAN を複数のセンシング インターフェイスのインライン VLAN ペアのメンバにすることができます。
- 物理インターフェイスは、インライン インターフェイス ペアのメンバにすることはできません。ただし、物理インターフェイスのサブインターフェイス モードが **none** の場合は除きます。
- 非バックプレーン FastEthernet インターフェイスの場合、有効な速度設定は 10 Mbps、100 Mbps、および自動です。有効な二重通信設定は、全、半、自動です。
- ギガビット ファイバ インターフェイス (IDS-4250 上の 1000-SX および XL) の場合、有効な速度設定値は 1000 Mbps および自動のみです。
- ギガビット 銅線 インターフェイス (IDS-4235 および IDS-4250 上の 1000-TX) の場合、有効な速度設定値は 10 Mbps、100 Mbps、1000 Mbps、および自動です。
- ギガビット (銅線またはファイバ) インターフェイスの場合は、速度が 1000 Mbps に設定されている場合、有効な二重通信設定値は自動のみです。

サマリー

この項では、Summary パネルについて説明します。取り上げる事項は次のとおりです。

- 概要 (P.3-9)
- サポートされるユーザのロール (P.3-9)
- フィールド定義 (P.3-9)

概要

Summary パネルには、センシング インターフェイスをどのように設定したか、つまり、混合モードに設定したインターフェイス、インライン ペアに設定したインターフェイス、およびインライン VLAN ペアに設定したインターフェイスが表示されます。インターフェイス設定を変更すると、このパネルの内容も変更されます。



注意

1 つの物理インターフェイスを混合モード、インライン ペア モード、またはインライン VLAN ペア モードのいずれかで動作するように設定できますが、これらのモードを組み合わせたインターフェイスを設定することはできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

フィールド定義

Summary パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：インターフェイスの名前。
混合インターフェイスでは、この値は **FastEthernet** または **GigabitEthernet** になります。インライン インターフェイスでは、ペアに割り当てた名前になります。
- **Details**：インターフェイスが混合またはインラインであるかどうかを示し、VLAN ペアの有無を示します。
- **Description**：インターフェイスの説明。
- **Assigned Virtual Sensor**：インターフェイスまたはインターフェイス ペアが仮想センサー vs0 に割り当て済みであるかどうかを示します。

インターフェイスの設定

この項では、センサー上のインターフェイスの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要 (P.3-10)
- TCP リセットの説明 (P.3-10)
- サポートされるユーザのロール (P.3-11)
- フィールド定義 (P.3-11)
- インターフェイスの設定 (P.3-13)

概要

Interfaces パネルには、センサー上の既存の物理インターフェイスとそれらに関連する設定が表示されます。センサーはインターフェイスを検出し、インターフェイス リストを Interfaces パネルに代入します。

センサーがトラフィックを監視するように設定するには、インターフェイスをイネーブルにする必要があります。setup コマンドを使用してセンサーを初期化したときに、インターフェイスまたはインライン ペアをデフォルトの仮想センサー vs0 に割り当て、そのインターフェイスまたはインライン ペアをイネーブルにしています。インターフェイス設定を変更する必要がある場合は、Interfaces パネルから変更できます。インターフェイスまたはインライン ペアの仮想センサー vs0 への割り当ては、Edit Virtual Sensor ダイアログボックスの **Configuration > Analysis Engine > Virtual Sensor > Edit** で実行できます。

TCP リセットの説明

次の場合には、代替 TCP リセット インターフェイスを指定する必要があります。

- スイッチが SPAN または VACL キャプチャを使用して監視され、スイッチが SPAN または VACL キャプチャ ポートで着信パケットを受け入れない場合。
- スイッチが複数の VLAN の SPAN キャプチャまたは VACL キャプチャのどちらかを使用して監視され、スイッチが 802.1q ヘッダーのある着信パケットを受け入れない場合。



(注) TCP リセットには、リセットを送信する VLAN を指定する 802.1q ヘッダーが必要です。

- 接続の監視にネットワーク タップが使用される場合。



(注) タップは、センサーからの着信トラフィックを許可しません。

センシング インターフェイスは代替 TCP リセット インターフェイスとしてのみ割り当てることができます。管理インターフェイスを代替 TCP リセット インターフェイスとして設定することはできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

センサー上のインターフェイスを編集するには、管理者である必要があります。

フィールド定義

この項では、インターフェイスのフィールド定義を示します。取り上げる事項は次のとおりです。

- [Interfaces パネル \(P.3-11\)](#)
- [Edit Interface ダイアログボックス \(P.3-12\)](#)

Interfaces パネル

Interfaces パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Name**：インターフェイスの名前。
すべてのインターフェイスで、この値は **FastEthernet** または **GigabitEthernet** になります。
- **Enabled**：インターフェイスをイネーブルにするかどうかを指定します。
- **Media Type**：メディア タイプを示します。
メディア タイプのオプションは次のとおりです。
 - **TX**：銅メディア
 - **SX**：光ファイバ メディア
 - **XL**：ネットワーク アクセラレータ カード
 - **Backplane interface**：モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。
- **Duplex**：インターフェイスの二重通信設定を示します。
二重通信タイプのオプションは次のとおりです。
 - **Auto**：インターフェイスを自動ネゴシエーション二重に設定します。
 - **Full**：インターフェイスを全二重に設定します。
 - **Half**：インターフェイスを半二重に設定します。
- **Speed**：インターフェイスの速度設定を示します。
速度タイプのオプションは次のとおりです。
 - **Auto**：インターフェイスを自動ネゴシエーション速度に設定します。
 - **10 MB**：インターフェイスを 10 MB に設定します (TX インターフェイスの場合のみ)。
 - **100 MB**：インターフェイスを 100 MB に設定します (TX インターフェイスの場合のみ)。
 - **1000**：インターフェイスを 1 GB に設定します (ギガビット インターフェイスの場合のみ)。
- **Alternate TCP Reset Interface**：これを選択すると、代替インターフェイスが混合モニタリングに使用され、シグニチャ反応によってリセット アクションがトリガーされた場合、代替インターフェイス上の TCP リセットが送信されます。
- **Description**：インターフェイスの説明を入力します。

ボタンの機能：

- **Select All**：リストにあるすべてのエントリを選択できます。
- **Edit**：Edit Interface ダイアログボックスを開きます。
このダイアログボックスで、このインターフェイスに関連付けられた値の一部を変更できます。
- **Enable**：インターフェイスをイネーブルにします。
- **Disable**：インターフェイスをディセーブルにします。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Edit Interface ダイアログボックス

Edit Interface ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Name**：インターフェイスの名前。
すべてのインターフェイスで、この値は FastEthernet または GigabitEthernet になります。
- **Description**：インターフェイスの説明を入力します。
- **Media Type**：メディア タイプを示します。
メディア タイプは次のとおりです。
 - **TX**：銅メディア
 - **SX**：光ファイバ メディア
 - **XL**：ネットワーク アクセラレータ カード
 - **Backplane interface**：モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。
- **Enabled**：インターフェイスをイネーブルにするかどうかを指定します。
- **Duplex**：インターフェイスの二重通信設定を示します。
二重通信タイプは次のとおりです。
 - **Auto**：インターフェイスを自動ネゴシエーション二重に設定します。
 - **Full**：インターフェイスを全二重に設定します。
 - **Half**：インターフェイスを半二重に設定します。
- **Speed**：インターフェイスの速度設定を示します。
速度タイプは次のとおりです。
 - **Auto**：インターフェイスを自動ネゴシエーション速度に設定します。
 - **10MB**：インターフェイスを 10 MB に設定します (TX インターフェイスの場合のみ)。
 - **100 MB**：インターフェイスを 100 MB に設定します (TX インターフェイスの場合のみ)。
 - **1000**：インターフェイスを 1 GB に設定します (ギガビット インターフェイスの場合のみ)。
- **Use Alternate TCP Reset Interface**：これを選択すると、代替インターフェイスが混合モニタリングに使用され、シグニチャ反応によってリセット アクションがトリガーされた場合、代替インターフェイス上の TCP リセットが送信されます。
 - **Select Interface**：TCP リセットを送信するインターフェイスを設定します。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

インターフェイスの設定

インターフェイスをイネーブルまたはディセーブルにする、またはインターフェイス設定を編集するには、次の手順を実行します。

ステップ 1 管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2 **Configuration > Interface Configuration > Interfaces** の順にクリックします。

Interfaces パネルが表示されます。

ステップ 3 行を選択またはダブルクリックして、**Enable** をクリックします。

インターフェイスがイネーブルになります。インターフェイスがトラフィックを監視するためには、そのインターフェイスを仮想センサーに割り当てる必要があります。手順については、[P.4-3](#) の「[インターフェイスの仮想センサーへの割り当て](#)」を参照してください。

ステップ 4 インターフェイスに関連付けられている値の一部を編集するには、インターフェイスを選択して、**Edit** をクリックします。

Edit Interface ダイアログボックスが表示されます。

ステップ 5 **Description** フィールドの説明を変更できます。また、**No** または **Yes** チェックボックスをオンにすることで、状態を **enabled** から **disabled** に変更できます。**Use Alternative TCP Reset Interface** を選択することで、インターフェイスが代替 TCP リセットを使用するように設定できます。

ステップ 6 **OK** をクリックします。

変更内容が Interfaces パネルのリストに表示されます。



ヒント 変更を元に戻す場合は、**Reset** をクリックします。

ステップ 7 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

インライン インターフェイス ペアの設定

この項では、インライン インターフェイス ペアの設定方法について説明します。取り上げる事項は次のとおりです。

- [概要 \(P.3-14\)](#)
- [サポートされるユーザのロール \(P.3-14\)](#)
- [フィールド定義 \(P.3-14\)](#)
- [インライン インターフェイス ペアの設定 \(P.3-15\)](#)

概要

センサーがインライン モニタリングに対応している場合、センサー上でインターフェイスのペアを作成できます。



(注)

AIP SSM には、モニタリング用のインライン ペアは必要ありません。物理インターフェイスを仮想センサーに追加するだけです。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

インターフェイス ペアを設定するには、管理者である必要があります。

フィールド定義

この項では、インターフェイス ペアのフィールド定義を示します。取り上げる事項は次のとおりです。

- [Interface Pairs パネル \(P.3-14\)](#)
- [Add and Edit Interface Pair ダイアログボックス \(P.3-15\)](#)

Interface Pairs パネル

Interface Pairs パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Pair Name**：インターフェイス ペアに指定する名前。
- **Paired Interfaces**：ペアを作成した2つのインターフェイス (GigabitEthernet0/0<->GigabitEthernet0/1 など)。
- **Description**：このインターフェイス ペアの説明を追加します。

ボタンの機能：

- **Select All**：すべてのインターフェイス ペアを選択します。
- **Add**：Add Interface Pair ダイアログボックスを開きます。

このダイアログボックスでは、新しいインターフェイス ペアを追加できます。

- **Edit** : Edit Interface Pair ダイアログボックスを開きます。
このダイアログボックスでは、インターフェイス ペアの値を編集できます。
- **Delete** : 選択したインターフェイス ペアを削除します。
- **Apply** : 変更を適用し、変更された設定を保存します。
- **Reset** : 編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Add and Edit Interface Pair ダイアログボックス

Add and Edit Interface Pair ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明 :

- **Interface Pair Name** : インターフェイス ペアに指定する名前。
- **Select two interfaces** : リストからペアを作成する2つのインターフェイスを選択します (GigabitEthernet0/0<->GigabitEthernet0/1 など)。
- **Description** : このインターフェイス ペアの説明を追加します。

ボタンの機能 :

- **OK** : 変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel** : 変更を廃棄しダイアログボックスを閉じます。
- **Help** : この機能のヘルプ トピックを表示します。

インライン インターフェイス ペアの設定

インライン インターフェイス ペアを設定するには、次の手順を実行します。

ステップ 1 管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2 **Configuration > Interface Configuration > Interface Pairs** の順にクリックします。

Interface Pairs パネルが表示されます。

ステップ 3 インライン インターフェイス ペアを追加するには、**Add** をクリックします。

Add Interface Pair ダイアログボックスが表示されます。

ステップ 4 **Interface Pair Name** フィールドに名前を入力します。

インライン インターフェイス名は、作成した名前になります。

ステップ 5 **Select two interfaces** フィールドで、ペアを作成する2つのインターフェイスを選択します。

たとえば、GigabitEthernet0/0 と GigabitEthernet0/1 のように選択します。

ステップ 6 必要であれば、**Description** フィールドにインライン インターフェイス ペアの説明を追加できます。

ステップ 7 **OK** をクリックします。

Interface Pairs パネルのリストに、新しいインライン インターフェイス ペアが表示されます。

■ インライン インターフェイス ペアの設定

ステップ 8 インライン インターフェイス ペアを編集するには、これを選択し、**Edit** をクリックします。

Edit Interface Pair ダイアログボックスが表示されます。

ステップ 9 このダイアログボックスで、名前の変更、新しいインライン インターフェイス ペアの選択、説明の編集ができます。

ステップ 10 **OK** をクリックします。

Interface Pairs パネルのリストに、編集されたインライン インターフェイス ペアが表示されます。

ステップ 11 インライン インターフェイス ペアを削除するには、これを選択し、**Delete** をクリックします。

削除されたインライン インターフェイス ペアは、Interface Pairs パネルのリストに表示されなくなります。



ヒント 変更を元に戻す場合は、**Reset** をクリックします。

ステップ 12 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

インライン VLAN ペアの設定

この項では、インライン VLAN ペアの設定方法について説明します。取り上げる事項は次のとおりです。

- [概要 \(P.3-17\)](#)
- [サポートされるユーザのロール \(P.3-17\)](#)
- [フィールド定義 \(P.3-17\)](#)
- [インライン VLAN ペアの設定 \(P.3-19\)](#)

概要

VLAN Pairs パネルには、各物理インターフェイスの既存のインライン VLAN ペアが表示されます。インライン VLAN ペアを作成するには、**Add** をクリックします。



(注)

別のインターフェイスとペアになっているインターフェイスや、混合モードで動作し仮想センサーに割り当てられているインターフェイスでは、インライン VLAN ペアは作成できません。

混合モードで動作するインターフェイスに対してインライン VLAN ペアを作成するには、仮想センサーからそのインターフェイスを除外してから、インライン VLAN ペアを作成します。インライン VLAN ペアを作成するときに、インターフェイスが別のインターフェイスとペアになっていたり、混合モードになっていたりすると、エラーメッセージが表示されます。



(注)

センサーが「on-a-stick」機能をサポートしていない場合、VLAN Pairs パネルは表示されません。AIP SSM と NM-CIDS は、インライン VLAN ペアをサポートしていません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

インライン VLAN ペアを設定するには、管理者である必要があります。

フィールド定義

この項では、インライン VLAN ペアのフィールド定義を示します。取り上げる事項は次のとおりです。

- [VLAN Pairs パネル \(P.3-18\)](#)
- [Add and Edit VLAN Pair ダイアログボックス \(P.3-18\)](#)

VLAN Pairs パネル

Interface Pairs パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Name**：インライン VLAN ペアの名前。
- **Subinterface (VLAN Pair)**：インライン VLAN ペアのサブインターフェイス番号。
値は 1 ～ 255 です。
- **VLAN1**：VLAN1 の VLAN 番号を表示します。
値は 1 ～ 4095 です。
- **VLAN2**：VLAN2 の VLAN 番号を表示します。
値は 1 ～ 4095 です。
- **Description**：インライン VLAN ペアの説明。

ボタンの機能：

- **Select All**：すべての VLAN ペアを選択します。
- **Add**：Add VLAN Pair ダイアログボックスを開きます。
このダイアログボックスでは、新しい VLAN ペアを追加できます。
- **Edit**：Edit VLAN Pair ダイアログボックスを開きます。
このダイアログボックスで、VLAN ペアの値を編集できます。
- **Delete**：選択した VLAN ペアを削除します。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Add and Edit VLAN Pair ダイアログボックス

Add and Edit Inline VLAN Pair ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：



(注) VLAN はそれ自体とペアにすることはできません。

- **Interface Name**：インライン VLAN ペアを作成するために使用可能なインターフェイスを選択します。
- **Subinterface Number**：サブインターフェイス番号を割り当てます。
1 から 255 までの数字を割り当てることができます。
- **VLAN 1**：インライン VLAN ペアの最初の VLAN を指定します。
1 から 4095 までの任意の VLAN を割り当てることができます。
- **VLAN 2**：インライン VLAN ペアの 2 番目の VLAN を指定します。
1 から 4095 までの任意の VLAN を割り当てることができます。
- **Description**：インライン VLAN ペアの説明を追加します。



(注) サブインターフェイス番号と VLAN 番号は、各物理インターフェイスで一意である必要があります。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

インライン VLAN ペアの設定

インライン VLAN ペアを設定するには、次の手順を実行します。

-
- ステップ 1** 管理者特権を持つアカウントを使用して IDM にログインします。
- ステップ 2** **Configuration > Interface Configuration > VLAN Pairs** の順にクリックします。
- VLAN Pairs パネルが表示されます。
- ステップ 3** インライン VLAN ペアを追加するには、**Add** をクリックします。
- Add Inline VLAN Pair ダイアログボックスが表示されます。
- ステップ 4** **Interface Name** リストからインターフェイスを選択します。
- ステップ 5** **Subinterface Number** フィールドに、インライン VLAN ペアのサブインターフェイス番号 (1 ~ 255) を入力します。
- ステップ 6** **VLAN 1** フィールドに、インライン VLAN ペアの最初の VLAN (1 ~ 4095) を指定します。
- ステップ 7** **VLAN 2** フィールドに、インライン VLAN ペアの 2 番目の VLAN (1 ~ 4095) を指定します。
- ステップ 8** 必要であれば、**Description** フィールドにインライン VLAN ペアの説明を追加できます。
- ステップ 9** **OK** をクリックします。
- VLAN Pairs パネルのリストに、新しいインライン VLAN ペアが表示されます。
- ステップ 10** インライン VLAN ペアを編集するには、これを選択し、**Edit** をクリックします。
- Edit Inline VLAN Pair ダイアログボックスが表示されます。
- ステップ 11** このダイアログボックスでサブインターフェイス番号の変更、VLAN 番号の変更、説明の編集ができます。
- ステップ 12** **OK** をクリックします。
- VLAN Pairs パネルのリストに、編集されたインライン VLAN ペアが表示されます。
- ステップ 13** VLAN ペアを削除するには、これを選択し、**Delete** をクリックします。
- 削除された VLAN ペアは、VLAN Pairs パネルのリストに表示されなくなります。



ヒント 変更を元に戻す場合は、**Reset** をクリックします。

ステップ 14 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

バイパス モードの設定

この項では、バイパス モードの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要 (P.3-21)
- サポートされるユーザのロール (P.3-21)
- フィールド定義 (P.3-22)

概要

バイパス モードは、診断ツールおよびフェールオーバー保護メカニズムとして使用できます。すべての IPS 処理サブシステムをバイパスし、トラフィックが直接インライン ペアに流れることが可能なモードにセンサーを設定できます。このバイパス モードにより、アップグレードのためにセンサーのプロセスが一時的に停止した場合や、センサーのモニタリング プロセスが失敗した場合でも、センサーへのパケットフローは続行します。オン、オフ、自動の3つのモードがあります。デフォルトでは、バイパス モードは自動に設定されています。



(注)

バイパス モードは、初めはインラインでペアを組んでいるインターフェイスに対してのみ適用されてきました。不具合のため、混合モードには適用されません。今後のバージョンでこの不具合に対応できる可能性があります。混合モードでは、バイパス モードを自動またはオフに設定し、オンで使用しないことをお勧めします。



注意

センサーをバイパス モードにすると、セキュリティに影響を及ぼします。バイパス モードをオンにすると、トラフィックはセンサーをバイパスし検査されないため、センサーは悪意のある攻撃を防止できません。



(注)

バイパス モードが機能するのは、オペレーティング システムの実行中だけです。センサーの電源を切ったり、センサーがシャットダウンされたりすると、バイパス モードは機能しません。つまり、トラフィックはセンサーに渡されなくなります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

センサー上のバイパス モードを設定するには、管理者である必要があります。

フィールド定義

Bypass パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Auto**：センサーのモニタリング プロセスがダウンしている場合を除き、トラフィックがセンサーに流れて検査されます。
センサーのモニタリング プロセスがダウンしていると、センサーが再び動作するようになるまで、トラフィックはセンサーをバイパスします。センサーが動作を再開すると、トラフィックを検査します。自動モードは、センサーがアップグレード中でもトラフィックのフローが継続するので、センサー アップグレードのときに役立ちます。また、モニタリング プロセスが失敗した場合でも、トラフィックのフローを継続するのに役立ちます。
- **Off**：バイパス モードをディセーブルにします。
トラフィックはセンサーに流れて検査されます。センサーのモニタリング プロセスがダウンしていると、トラフィックのフローが停止します。つまり、インライン トラフィックの検査は必ず行われます。
- **On**：トラフィックは **SensorApp** をバイパスし、検査は行われません。つまり、インライン トラフィックの検査は行われません。

ボタンの機能：

- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

トラフィック フロー通知の設定

この項では、トラフィック フロー通知の設定方法について説明します。取り上げる事項は次のとおりです。

- [概要 \(P.3-23\)](#)
- [サポートされるユーザのロール \(P.3-23\)](#)
- [フィールド定義 \(P.3-23\)](#)
- [トラフィック フロー通知の設定 \(P.3-23\)](#)

概要

センサーがインターフェイスの packets フローを監視し、指定された時間間隔内で packets フローに変化があった（開始や停止）場合、通知を送信するように設定できます。特定の通知間隔内の非受信 packets しきい値を設定できます。また、ステータス イベントが報告されるまでのインターフェイスアイドル遅延も設定できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

トラフィック フロー通知を設定するには、管理者である必要があります。

フィールド定義

Traffic Flow Notifications パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Missed Packets Threshold**：通知が送信される前に、指定された時間内で受信できなかった packets の率。
- **Notification Interval**：センサーが未受信 packets 率をチェックする時間間隔。
- **Interface Idle Threshold**：通知が送信される前に、インターフェイスがアイドル状態で packets を受信していない時間（秒数）。

ボタンの機能：

- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

トラフィック フロー通知の設定

トラフィック フロー通知を設定するには、次の手順を実行します。

ステップ 1 管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2 **Configuration > Interface Configuration > Traffic Flow Notifications** の順にクリックします。

Traffic Flow Notifications パネルが表示されます。

■ トラフィック フロー通知の設定

- ステップ 3** 通知を受信する前に発生した未受信パケット率を選択し、**Missed Packets Threshold** フィールドにその値を入力します。
- ステップ 4** 未受信パケット率をチェックする秒数を選択し、**Notification Interval** フィールドにその値を入力します。
- ステップ 5** 通知を受信する前に、インターフェイスがアイドル状態でパケットを受信していない状況を許可する時間（秒数）を選択し、**Interface Idle Threshold** フィールドにその値を入力します。



ヒント 変更を元に戻す場合は、**Reset** をクリックします。

- ステップ 6** **Apply** をクリックし、変更を適用して、変更された設定を保存します。
-