センサーの概要

内容

この章では、センサーの概要、およびセンサーを設置するときに知っておくべき情報について説明します。このガイドでは、明記されていない限り、*センサー*という用語はすべてのモデルを指します。サポートしているセンサーとその型番全体のリストについては、「サポートされるセンサー」（P.1-19）を参照してください。

この章の内容は、次のとおりです。

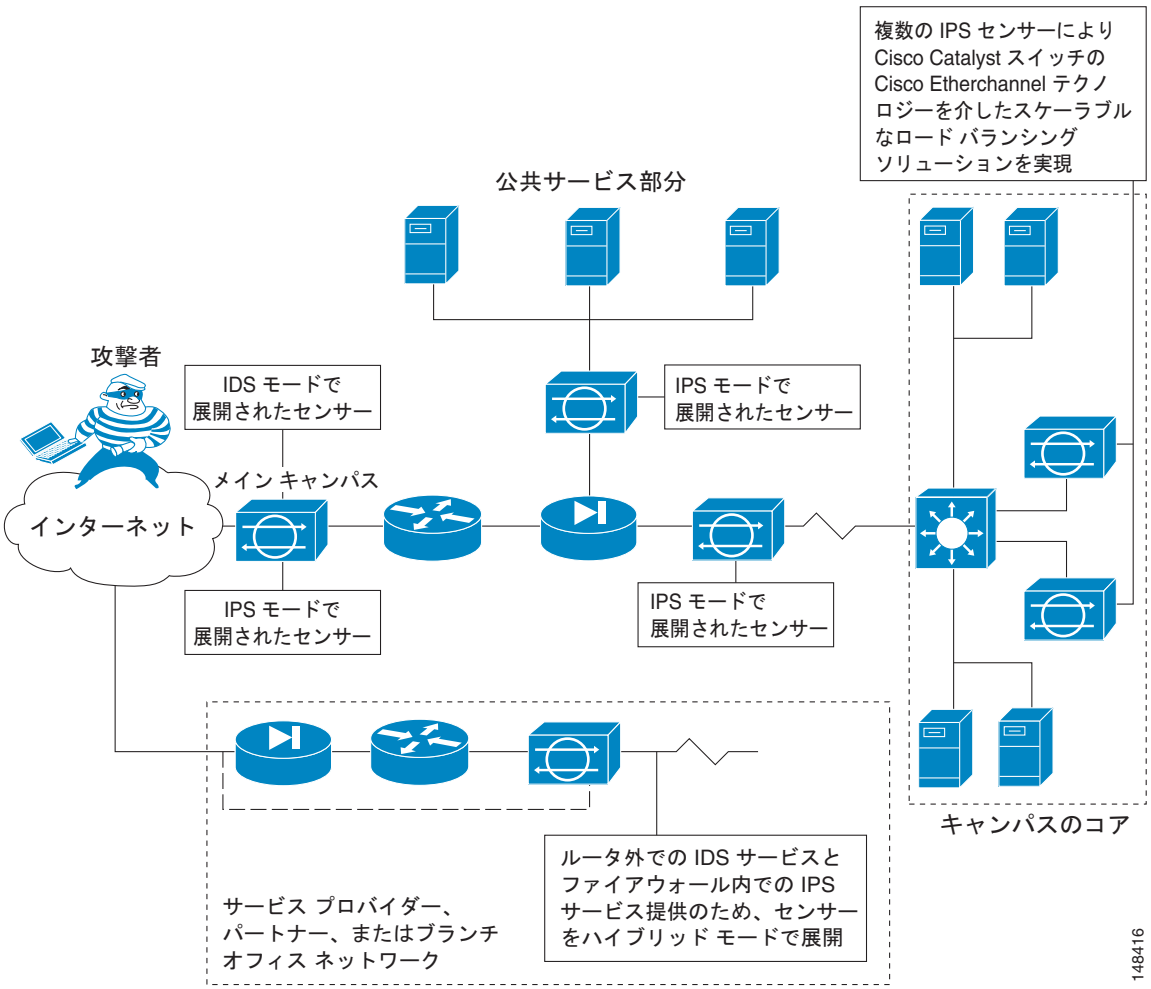
センサーの動作

ここでは、センサー機能について説明します。内容は次のとおりです。

ネットワーク トラフィックのキャプチャ

センサーは、無差別モードまたはインライン モードで動作できます。図 1-1（P.1-2）に、インライン（IPS）モードと無差別モード（IDS）モードの両方で動作するセンサーの組み合わせを展開してネットワークを保護する方法を示します。

図 1-1　包括的な展開ソリューション



コマンドおよび制御インターフェイスは常に Ethernet です。このインターフェイスには IP アドレスが割り当てられており、この IP アドレスによってマネージャ ワークステーションまたはネットワーク デバイス（シスコのスイッチ、ルータ、およびファイアウォール）と通信できます。このインターフェイスはネットワーク上で参照できるため、暗号化を使用してデータのプライバシーを維持する必要があります。CLI を保護するには SSH を使用し、マネージャ ワークステーションを保護するには TLS/SSL を使用します。SSH および TLS/SSL は、マネージャ ワークステーションでデフォルトでイネーブルになります。

攻撃に対応する場合、センサーは次の処理を行うことができます。

- 検知インターフェイスを介して TCP リセットを挿入する。

（注）　TCP リセット アクションは、TCP ベースのサービスに関連付けられているシグニチャでだけ選択する必要があります。TCP ベース以外のサービスでアクションとして選択した場合、アクションは実行されません。また、TCP プロトコルの制限により、TCP リセットでは攻撃セッションのティアダウンが保証されません。

- センサーが管理するスイッチ、ルータ、およびファイアウォールの ACL を変更する。

（注）　ACL は、現在のトラフィックではなく今後のトラフィックだけをブロックできます。

- IP セッション ログ、セッション リプレイ、およびトリガー パケット表示を生成する。

  IP セッション ログを使用して、不正な使用に関する情報を収集します。IP ログ ファイルは、アプライアンスで検索するように設定されているイベントが発生した場合に書き込まれます。
- 複数のパケット ドロップ アクションを実装して、ワームやウイルスを停止する。

ネットワーク トポロジ

センサーを展開および設定する前に、ネットワークについて次のことを理解する必要があります。

- ネットワークの規模と複雑さ。
- 他のネットワーク（およびインターネット）との接続
- ネットワーク トラフィックの量とタイプ

この知識は、必要なセンサーの数、各センサーのハードウェア設定（たとえば、ネットワーク インターフェイス カードのサイズとタイプ）、および必要なマネージャの数を判断するのに役立ちます。

センサーの適切な展開

IPS センサーは、常にファイアウォールや適応型セキュリティ アプライアンスなどの境界フィルタリング デバイスの背後に配置する必要があります。境界デバイスは、セキュリティ ポリシーに一致するようにトラフィックをフィルタリングして、許容されるトラフィックだけがネットワークに入れるようにします。適切な配置によって、アラートの数が大幅に削減され、セキュリティ違反の調査に使用できる対処可能データ量が増えます。IPS センサーをファイアウォールの前面のネットワークのエッジに配置した場合、センサーは、ネットワークの実装にとって重要な意味がない場合でも、すべての単一スキャンおよび攻撃の試行に対してアラートを生成します。（大規模なエンタープライズ環境では）実際にはクリティカルまたは対処可能でない数百、数千、または数百万のアラートが環境に生成されます。このタイプのデータの分析には、時間とコストがかかります。

IPS の調整

IPS を調整すると、表示されるアラートに、実際に対処可能な情報が反映されます。IPS を調整しないと、偽陽性とも呼ばれる良性のイベントが大量に表示され、ネットワークでのセキュリティ調査が困難になります。false positive はすべての IPS デバイスで副次的に発生しますが、Cisco IPS デバイスはステートフルで標準化されており、攻撃評価に脆弱性シグニチャを使用するため、Cisco IPS デバイスでは発生頻度がはるかに低くなります。Cisco IPS デバイスは、ハイリスクのイベントを識別するリスク レーティングと、リスク レーティングに基づいて IPS シグニチャ アクションを実施するためのルールを展開できるポリシーベースの管理も提供します。

IPS センサーを調整するときは、次のヒントに従います。

- センサーは、ネットワーク上の境界フィルタリング デバイスの背後に配置する。センサーを適切に配置すると、検査する必要のあるアラートの数を 1 日に数千単位で削減できます。

- デフォルトのシグニチャを設定したままセンサーを展開する。

  デフォルトのシグニチャ セットでは、非常に高いセキュリティ保護ポスチャが提供されます。シスコのシグニチャ チームは、センサーに非常に高い保護を与えるデフォルトのテストに多くの時間を費やしました。これらのデフォルトが失われたと思われる場合は、復元できます。

- リスク レーティングが 90 を超えるパケットをドロップするようにイベント アクションのオーバーライドが設定されていることを確認する。これはデフォルトであり、ハイリスク アラートが即時に停止されるようにします。
- 次のいずれかの方法で、脆弱性スキャナやロード バランサなどの特殊なソフトウェアが原因の false positive をフィルタで除外する。
  - スキャナおよびロード バランサの IP アドレスからのアラートを無視するようにセンサーを設定できる。
  - これらのアラートを許可するようにセンサーを設定し、IME を使用して false positive をフィルタで除外できる。
- Informational アラートをフィルタリングする。

  このような低い優先度のイベント通知は、別のデバイスが IPS で保護されているデバイスを探査しているときに発生することがあります。これらの Informational アラートから送信元 IP アドレスを調べ、送信元を判断します。

- 残りの対処可能なアラートを分析する。
  - アラートを調べる。
  - 攻撃元を突き止める。
  - 宛先ホストを突き止める。
  - より多くの情報を提供するように IPS ポリシーを修正する。

詳細情報

- リスク レーティングの詳細については、「リスク レーティングの計算」を参照してください。
- シスコのシグニチャの詳細については、IDM および IME の場合は、「シグニチャの定義」を参照してください。CLI については、「シグニチャの定義」を参照してください。
- イベント アクション オーバーライドの詳細については、IDM および IME の場合は、「イベント アクション オーバーライドの設定」を参照してください。CLI については、「イベント アクション オーバーライドの設定」を参照してください。

センサーのインターフェイス

ここでは、センサー インターフェイスについて説明します。内容は次のとおりです。

センサー インターフェイスについて

センサーのインターフェイスは、インターフェイスの最大速度および物理的な場所に従って名前が付けられています。物理的な場所は、ポート番号とスロット番号で構成されています。センサーのマザーボードに組み込まれたすべてのインターフェイスは、スロット 0 にあります。インターフェイス カード拡張スロットには、一番下のスロットをスロット 1 として、下から上に向かって順にスロット番号が付けられています。各物理インターフェイスは、VLAN グループ サブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスの VLAN のグループで構成されます。

インターフェイスには、次の 3 つの役割があります。

- コマンド/コントロール
- 検知
- 代替 TCP リセット

特定のインターフェイスに割り当てることができるロールには制約があります。また、複数のロールを担うインターフェイスもあります。検知インターフェイスを、他の検知インターフェイスに対する TCP リセット インターフェイスとして設定できます。TCP リセット インターフェイスは、同時に IDS（無差別）検知インターフェイスとしても機能します。次の制約事項が適用されます。

- 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 モードでは、TCP リセットは常に検知インターフェイス上で送信されるため、検知インターフェイスに割り当てられた TCP リセット インターフェイスは、これらのモードでは影響を与えません。
- ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）には 1 つの検知インターフェイスしかないため、ASA IPS モジュールで代替 TCP リセット インターフェイスを指定することはできません。
- IPS 4510 および IPS 4520 では、SensorApp がダウンすると、インターフェイス関連の設定は許可されません。

コマンド/コントロール インターフェイス

コマンド/コントロール インターフェイスは、IP アドレスを持ち、センサーの設定に使用されます。このインターフェイスは、センサーからセキュリティ イベントとステータス イベントを受信し、センサーに統計情報を問い合わせます。コマンド/制御インターフェイスは、常にイネーブルです。このインターフェイスは特定の物理インターフェイス（センサーのモデルによって異なる）に常時マッピングされています。コマンド/制御インターフェイスを検知インターフェイスや代替 TCP リセット インターフェイスとして使用することはできません。

表 1-1 に、各センサーのコマンド/コントロール インターフェイスを示します。

表 1-1　コマンド/コントロール インターフェイス

センサー	コマンド/コントロール インターフェイス
ASA 5512-X IPS SSP	Management 0/0
ASA 5515-X IPS SSP	Management 0/0
ASA 5525-X IPS SSP	Management 0/0
ASA 5545-X IPS SSP	Management 0/0
ASA 5555-X IPS SSP	Management 0/0
ASA 5585-X IPS SSP-10	Management 0/0
ASA 5585-X IPS SSP-20	Management 0/0

表 1-1　コマンド/コントロール インターフェイス （続き）

センサー	コマンド/コントロール インターフェイス
ASA 5585-X IPS SSP-40	Management 0/0
ASA 5585-X IPS SSP-60	Management 0/0
IPS 4345	Management 0/0
IPS 4360	Management 0/0
IPS 4510	Management 0/0[1]
IPS 4520	Management 0/0[1]

1. 4500 シリーズ センサーには 2 つの管理ポート（Management 0/0 および Management 0/1）がありますが、Management 0/1 は将来使用するために予約されています。

センシング インターフェイス

検知インターフェイスは、セキュリティ違反に関してトラフィックを分析するために、センサーによって使用されます。センサーには、1 つ以上の検知インターフェイスがあり、その数はセンサーによって異なります。検知インターフェイスは、無差別モードで個別に動作させるか、またはペアにしてインライン インターフェイスを作成できます。

（注）　アプライアンスでは、すべての検知インターフェイスがデフォルトでディセーブルになっています。これらのインターフェイスを使用するには、イネーブルにする必要があります。モジュールでは、検知インターフェイスは常にイネーブルです。

センサーに検知インターフェイスを追加するオプションのインターフェイス カードをサポートするアプライアンスもあります。これらのオプションのカードは、センサーの電源がオフのときに着脱する必要があります。センサーは、サポートされているインターフェイス カードの着脱を検出します。オプションのインターフェイス カードを取り外すと、速度、デュプレックス、記述文字列、インターフェイスのイネーブル/ディセーブル状態、インライン インターフェイス ペアの組み合わせなど、インターフェイスの設定の一部が削除されます。これらの設定は、カードを再挿入すると、デフォルト設定に復元されます。無差別およびインライン インターフェイスの分析エンジンへの割り当ては分析エンジンの設定から削除されませんが、これらのカードが再挿入され、もう一度インライン インターフェイスのペアを作成するまで無視されます。

インターフェイス サポート

表 1-2 では、Cisco IPS 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 サポートについて説明します。

表 1-2　インターフェイス サポート

ベース シャーシ	追加されたインターフェイス カード	インターフェイス サポート インライン VLAN ペア（検知ポート）	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
ASA 5512-X IPS SSP	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
ASA 5515-X IPS SSP	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
ASA 5525-X IPS SSP	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
ASA 5545-X IPS SSP	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
ASA 5555-X IPS SSP	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
ASA 5585-X IPS SSP-10	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
ASA 5585-X IPS SSP-20	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0

表 1-2　インターフェイス サポート （続き）

ベース シャーシ	追加されたインターフェイス カード	インターフェイス サポート インライン VLAN ペア（検知ポート）	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
ASA 5585-X IPS SSP-40	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
ASA 5585-X IPS SSP-60	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel 0/0	Management 0/0
IPS 4345	—	ギガビット イーサネット 0/0 ギガビット イーサネット 0/1 ギガビット イーサネット 0/2 ギガビット イーサネット 0/3 ギガビット イーサネット 0/4 ギガビット イーサネット 0/5 ギガビット イーサネット 0/6 ギガビット イーサネット 0/7	すべての検知ポートをまとめてペアにすることが可能	Management 0/0 Management 0/1[1]

表 1-2　インターフェイス サポート （続き）

ベース シャーシ	追加されたインターフェイス カード	インターフェイス サポート インライン VLAN ペア（検知ポート）	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
IPS 4360	—	ギガビット イーサネット 0/0 ギガビット イーサネット 0/1 ギガビット イーサネット 0/2 ギガビット イーサネット 0/3 ギガビット イーサネット 0/4 ギガビット イーサネット 0/5 ギガビット イーサネット 0/6 ギガビット イーサネット 0/7	すべての検知ポートをまとめてペアにすることが可能	Management 0/0 Management 0/1[1]

表 1-2　インターフェイス サポート （続き）

ベース シャーシ	追加されたインターフェイス カード	インターフェイス サポート インライン VLAN ペア（検知ポート）	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
IPS 4510	—	ギガビット イーサネット 0/0 ギガビット イーサネット 0/1 ギガビット イーサネット 0/2 ギガビット イーサネット 0/3 ギガビット イーサネット 0/4 ギガビット イーサネット 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	すべての検知ポートをまとめてペアにすることが可能	Management 0/0 Management 0/1[2]
IPS 4520	—TX	ギガビット イーサネット 0/0 ギガビット イーサネット 0/1 ギガビット イーサネット 0/2 ギガビット イーサネット 0/3 ギガビット イーサネット 0/4 ギガビット イーサネット 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	すべての検知ポートをまとめてペアにすることが可能	Management 0/0 Management 0/1[2]

1. 現在ハードウェア バイパスをサポートしていません。
2. 将来的な使用のために予約されています。

TCP リセット インターフェイス

ここでは、TCP リセット インターフェイスとこれらを使用する必要がある場合について説明します。次の項目について説明します。

代替 TCP リセット インターフェイスについて

（注）　代替 TCP リセット インターフェイスの設定は、リセットがインライン インターフェイスまたはインライン VLAN ペア モードでインラインで送信されるため、これらのモードで無視されます。

攻撃者のホストと攻撃のターゲット ホストとの間のネットワーク接続をリセットするために、TCP リセット パケットを送信するようにセンサーを設定できます。一部のインストールでは、インターフェイスが無差別モードで動作している場合、攻撃が検出された検知インターフェイスと同じインターフェイスでセンサーが TCP リセット パケットを送信できないことがあります。このような場合は、検知インターフェイスを代替 TCP リセット インターフェイスに関連付けることができます。これにより、無差別モードで動作している場合に通常は検知インターフェイスで送信されるすべての TCP リセットを、関連付けた代替 TCP リセット インターフェイスで送信できます。

検知インターフェイスが代替 TCP リセット インターフェイスに関連付けられている場合、センサーが無差別モードに設定されるとその関連付けが適用されますが、検知インターフェイスがインライン モードに設定されると無視されます。すべての検知インターフェイスは、別の検知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なることができます。

（注）　ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）には 1 つの検知インターフェイスしかないため、ASA IPS モジュールで代替 TCP リセット インターフェイスを指定することはできません。

表 1-3 に、代替 TCP リセット インターフェイスを示します。

表 1-3　代替 TCP リセット インターフェイス

センサー	代替 TCP リセット インターフェイス
ASA 5512-X IPS SSP	なし
ASA 5515-X IPS SSP	なし
ASA 5525-X IPS SSP	なし
ASA 5545-X IPS SSP	なし
ASA 5555-X IPS SSP	なし
ASA 5585-X IPS SSP-10	なし
ASA 5585-X IPS SSP-20	なし
ASA 5585-X IPS SSP-40	なし
ASA 5585-X IPS SSP-60	なし
IPS 4345	任意の検知インターフェイス
IPS 4360	任意の検知インターフェイス

表 1-3　代替 TCP リセット インターフェイス （続き）

センサー	代替 TCP リセット インターフェイス
IPS 4510	任意の検知インターフェイス
IPS 4520	任意の検知インターフェイス

代替 TCP リセット インターフェイスの指定

（注）　ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）には 1 つの検知インターフェイスしかないため、ASA IPS モジュールで代替 TCP リセット インターフェイスを指定することはできません。

次の場合、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 キャプチャでモニタされていて、スイッチがその SPAN または VACL ポートで着信パケットを受け入れない場合。
- 複数の VLAN でスイッチが SPAN または VACL キャプチャでモニタされていて、スイッチが 802.1q ヘッダー付きの着信パケットを受け入れない場合。TCP リセットでは、リセットを送信する VLAN を判断するために 802.1q ヘッダーが必要です。
- 接続のモニタにネットワーク タップが使用されている場合。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。

注意　検知インターフェイスだけを代替 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。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。

インターフェイスの制約事項

センサーでのインターフェイスの設定に適用される制約は次のとおりです。

- 物理インターフェイス
  - ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）上で、すべてのバックプレーン インターフェイスの速度、デュプレックス、および状態設定は固定されます。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で保護されます。
  - バックプレーン以外の FastEthernet インターフェイスでは、有効な速度設定は、10 Mbps、100 Mbps、および自動です。有効なデュプレックス設定は、全、半、および自動です。
  - ギガビットの銅インターフェイス（IPS 4345、IPS 4360、IPS 4510、および IPS 4520 上の 1000-TX）の場合、有効な速度設定は、10 Mbps、100 Mbps、1000 Mbps、および自動です。有効なデュプレックス設定は、全、半、および自動です。
  - ギガビット（銅またはファイバ）インターフェイスの場合、速度は 1000 Mbps に設定されている場合、有効なデュプレックス設定は自動だけです。
  - コマンド/コントロール インターフェイスを検知インターフェイスとして機能させることはできません。

- インライン インターフェイス ペア
  - 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（銅またはファイバ）、インターフェイスの速度やデュプレックス設定に関係なく、任意の検知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、異なるメディア タイプ、速度、デュプレックス設定のインターフェイスの組み合わせは十分にテストまたはサポートされていない場合があります。
  - コマンド/コントロール インターフェイスを、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。
  - インライン インターフェイス ペアで物理インターフェイスをそれ自身とペアにすることはできません。
  - 物理インターフェイスは、1 つのインライン インターフェイス ペアのみのメンバにすることができます。
  - バイパス モードだけを設定でき、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のみインライン インターフェイス ペアを作成できます。
  - 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** に設定されていない限り、物理インターフェイスをインライン 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。
  - ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）に 1 つの検知インターフェイスしかない場合でも、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
  - VLAN をそれ自身とペアにすることはできません。
  - インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。
  - 特定の検知インターフェイスについて、VLAN を 1 つのインライン VLAN ペアだけのメンバにすることができます。ただし、その VLAN は、複数の検知インターフェイスで 1 つのインライン VLAN ペアのメンバにできます。
  - インライン VLAN ペアで 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 モードの検知インターフェイスは、1 ～ 255 のインライン VLAN ペアを持つことができます。
  - ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）は、インライン VLAN ペアをサポートしていません。
  - IPS 4510 および IPS 4520 の場合、システム全体で作成できるインライン VLAN ペアの最大数は 150 です。その他のすべてのプラットフォームでは、各インターフェイスの制限値は 255 です。
- 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、検知インターフェイスにのみ割り当てることができます。コマンド/コントロール 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で **none** に設定され、検知インターフェイス以外のすべてのインターフェイスに対して保護されています。
  - 複数の検知インターフェイスに対して同じ物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割り当てることができます。
  - 物理インターフェイスは、検知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。
  - コマンド/コントロール インターフェイスは、検知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させることはできません。

  - 検知インターフェイスは、独自の代替 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。
  - 代替 TCP リセット インターフェイスとして TCP リセットが可能なインターフェイスだけを設定できます。
  - ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）には 1 つの検知インターフェイスしかないため、ASA IPS モジュールで代替 TCP リセット インターフェイスを指定することはできません。
- VLAN グループ
  - 無差別モード、インライン インターフェイス ペア モード、またはインライン VLAN ペア モードに 1 つのインターフェイスを設定できますが、これらのモードを組み合わせることはできません。
  - 各インターフェイスの複数のグループに 1 つの VLAN を追加することはできません。
  - 複数の仮想センサーに 1 つの VLAN グループを追加することはできません。
  - 1 つのインターフェイスに追加できるユーザ定義 VLAN グループは最大 255 です。
  - 物理インターフェイスをペアにする場合、インターフェイスを分割することはできません。ペアは分割できます。
  - 複数のインターフェイスで 1 つの VLAN を使用できますが、この構成に対して警告を受け取ります。
  - 分割されているかどうかに関係なく、1 つ以上の物理インターフェイスとインライン VLAN ペアの任意の組み合わせに仮想センサーを割り当てることができます。
  - 物理インターフェイスと論理インターフェイスの両方を VLAN グループに分割できます。
  - CLI、IDM、および IME は、ダングリング参照を削除するように求めます。ダングリング参照をそのままにして、設定の編集を続けることができます。
  - CLI、IDM、および IME では、分析エンジンでインターフェイス設定と競合する設定変更を行うことはできません。
  - CLI では、分析エンジン設定で競合の原因となる設定変更をインターフェイス設定で行うことができます。IDM と IME では、分析エンジン設定で競合の原因となるインターフェイス設定の変更を行うことは *できません*。
  - ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）は、VLAN グループ モードをサポートしていません。

インターフェイス モード

ここでは、インターフェイス モードについて説明します。内容は次のとおりです。

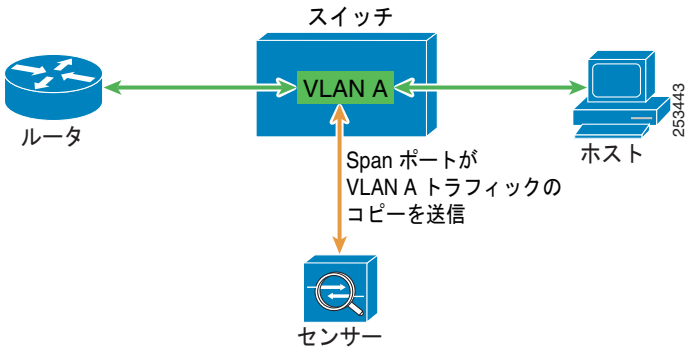
無差別モード

無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されるパケットではなく、モニタ対象のトラフィックのコピーを分析します。無差別モードで運用する利点は、転送されるトラフィックでパケットのフローにセンサーが影響を与えないことです。ただし、無差別モードで運用するときは、アトミック アタック（シングル パケット攻撃）などの特定のタイプの攻撃の場合に、悪意のあるトラフィックがターゲットに到達することをセンサーで阻止できないという短所があります。無差別モードのセンサー 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、攻撃に対応するために、ルータやファイアウォールなど、他のネットワーキング デバイスによるサポートが必要となります。このような応答アクションは一部の攻撃を防ぐことはできますが、アトミック アタックでは、無差別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。

デフォルトでは、すべての検知インターフェイスは無差別モードです。インターフェイスをインライン インターフェイス モードから無差別モードに変更するには、変更対象のインターフェイスを含むすべてのインライン インターフェイスを削除し、インターフェイス設定からそのインターフェイスのすべてのインライン VLAN ペアのサブインターフェイスを削除します。

図 1-2 に無差別モードを示します。

図 1-2　　無差別モード



IPv6、スイッチ、および VACL キャプチャなし

Catalyst スイッチの VACL は IPv6 をサポートしていません。トラフィックを無差別モードで設定されたセンサーにコピーする最も一般的な方法は、VACL キャプチャを使う方法です。IPv6 サポートが必要な場合は、SPAN ポートを使用できます。

ただし、次の設定を使用しない限り、スイッチでは最大 2 つのモニタ セッションしか設定できません。

- モニタ セッション
- 1 つ以上のセンサーに複数トランク
- トランク ポートごとに、1 つの IPS 内の複数の異なるセンサーまたは仮想センサーに対して多くの VLAN のモニタリングを実行できる VLAN を制限

次の設定では、1 つの SPAN セッションを使用して、指定された任意の VLAN 上のトラフィックすべてを指定されたすべてのポートに送信します。各ポート設定では、特定の 1 つの VLAN または複数の VLAN だけに通過を許可します。したがって、1 つの SPAN 設定行を使用して、異なる VLAN から異なるセンサーまたは仮想センサーすべてにデータを送信できます。

```
clear trunk 4/1-4 1-4094
```

```
set trunk 4/1 on dot1q 930
set trunk 4/2 on dot1q 932
set trunk 4/3 on dot1q 960
set trunk 4/4 on dot1q 962
set span 930, 932, 960, 962 4/1-4 both
```

（注）　VLAN ごとに異なる IPS ポリシーを割り当てる場合や 1 つのインターフェイスで処理できない大きな帯域幅をモニタする必要がある場合に SPAN/モニタ設定は役立ちます。

詳細情報

無差別モードの詳細については、「無差別モード」（P.1-15）を参照してください。

インライン インターフェイス ペア モード

インライン インターフェイス ペア モードで運用する場合は、IPS が直接トラフィック フローに挿入され、パケット転送速度に影響を与えます。遅延が加わるため、パケット転送速度は遅くなります。その結果、センサーは、悪意のあるトラフィックがターゲットに到達する前にそのトラフィックをドロップして攻撃を阻止できるため、保護サービスが提供されます。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か、その両方を行うことができます。

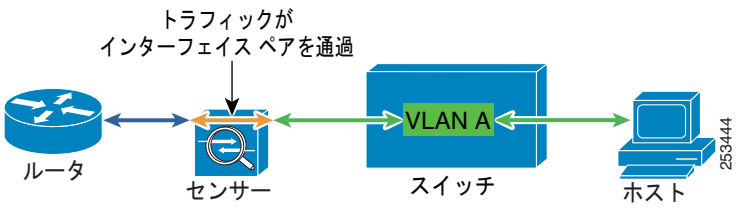
インライン インターフェイス ペア モードでは、パケットはセンサーのペアの 1 つめのインターフェイスを経由して入り、ペアの 2 つめのインターフェイスを経由して出ます。パケットは、シグニチャによって拒否または変更されないかぎり、ペアの 2 つめのインターフェイスに送信されます。

（注）　ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）に 1 つの検知インターフェイスしかない場合でも、インラインで動作するように設定できます。

（注）　ペアになっているインターフェイスが同じスイッチに接続されている場合は、それらのインターフェイスをスイッチ上で 2 つのアクセス ポートとして設定し、それぞれが異なる VLAN アクセスを持つようにする必要があります。このようにしないと、トラフィックはインライン インターフェイスを通過しません。

図 1-3 にインライン インターフェイス ペア モードを示します。

図 1-3　インライン インターフェイス ペア モード



インライン VLAN ペア モード

（注）　ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）は、インライン VLAN ペアをサポートしていません。

（注）　IPS 4510 および IPS 4520 の場合、システム全体で作成できるインライン VLAN ペアの最大数は 150 です。その他のすべてのプラットフォームでは、各インターフェイスの制限値は 255 です。

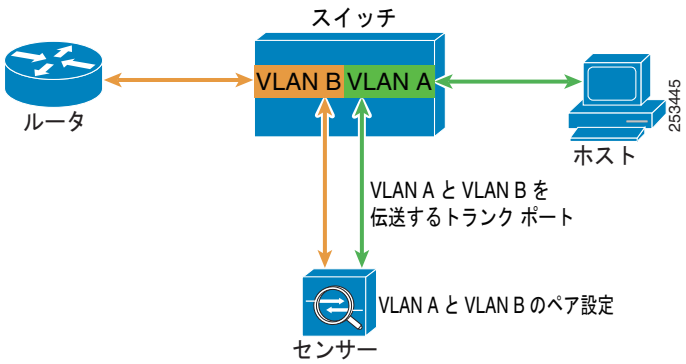
物理インターフェイス上で、VLAN をペアで関連付けることができます。これは、インライン VLAN ペア モードと呼ばれます。ペアの一方の VLAN で受信されたパケットは、分析後にペアのもう一方の VLAN に転送されます。

インライン VLAN ペア モードは、アクティブ検知モードです。このモードでは、検知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 のペア間の 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検査し、そのパケットをペアのもう一方の VLAN に転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。IPS センサーは、各検知インターフェイス上で最大 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すべての VLAN で受信したすべてのパケットをドロップします。

（注）　インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。

図 1-4 にインライン VLAN ペア モードを示します。

図 1-4　インライン VLAN ペア モード



VLAN グループ モード

（注）　ASA IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）は、VLAN グループ モードをサポートしていません。

各物理インターフェイスまたはインライン インターフェイスは、VLAN グループ サブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスの VLAN のグループで構成されます。分析エンジンは複数の仮想センサーをサポートします。各センサーはこれらの 1 つ以上のインターフェイスをモニタできます。これにより、複数のポリシーを同じセンサーに適用できます。この利点は、わずかなインターフェイスしかないセンサーを多くのインターフェイスがあるかのように使用できる点にあります。

（注）　インライン VLAN ペアに含まれている物理インターフェイスは、VLAN グループに分けることはできません。

VLAN グループ サブインターフェイスによって、物理インターフェイスまたはインライン インターフェイスと VLAN セットが関連付けられます。VLAN を複数の VLAN グループ サブインターフェイスのメンバにすることはできません。各 VLAN グループ サブインターフェイスは、1 ～ 255 の数値で識別されます。サブインターフェイス 0 は、仮想化されていない物理インターフェイスまたは論理インターフェイス全体を表すために使用される予約済みのサブインターフェイス番号です。サブインターフェイス 0 を作成、削除、または変更することはできません。また、サブインターフェイス 0 に関する統計情報は報告されません。

未割り当て VLAN グループは、別の VLAN グループに明示的に割り当てられていないすべての VLAN を含んでいる状態で維持されます。未割り当て VLAN グループ内の VLAN を直接指定することはできません。別の VLAN グループ サブインターフェイスに VLAN が追加されたり、または別の VLAN グループ サブインターフェイスから VLAN が削除されたりすると、未割り当て VLAN グループは更新されます。

通常、802.1q トランクのネイティブ VLAN 内のパケットには、そのパケットが属する VLAN 番号を示す 802.1q カプセル化ヘッダーがありません。各物理インターフェイスには、デフォルトの VLAN 変数が関連付けられており、この変数をネイティブ VLAN の VLAN 番号または 0 に設定する必要があります。値 0 は、ネイティブ VLAN が不明であるか、またはネイティブ VLAN の指定の有無は関係ないことを示しています。デフォルトの VLAN 設定が 0 の場合は、次の処理が行われます。

- 802.1q カプセル化のないパケットによってトリガーされたアラートには、VLAN 値 0 が報告されます。
- 802.1q カプセル化のないトラフィックは未割り当て VLAN グループに関連付けられ、ネイティブ VLAN として他の VLAN グループに割り当てることができません。

（注）　スイッチのポートは、アクセス ポートまたはトランク ポートとして設定できます。アクセス ポートでは、すべてのトラフィックは、アクセス VLAN と呼ばれる 1 つの VLAN 内にあります。トランク ポートでは、ポートで複数の VLAN を伝送することができ、各パケットには VLAN ID を含む 802.1q ヘッダーと呼ばれる特別なヘッダーが付加されます。このヘッダーは、一般に VLAN タグと呼ばれます。ただし、トランク ポートには、ネイティブ VLAN と呼ばれる特別な VLAN があります。ネイティブ VLAN 内のパケットには、802.1q ヘッダーは付加されていません。

VLAN グループの展開

インライン ペアの VLAN グループは、VLAN ID を変換しません。したがって、論理インターフェイスで VLAN グループを使用するには、2 つのスイッチ間にインライン ペア インターフェイスが存在する必要があります。アプライアンスの場合、2 つのペアを同じスイッチに接続し、それらをアクセス ポートにして、2 つのポートに対して別々にアクセス VLAN を設定できます。この設定では、センサーは 2 つの VLAN 間を接続します。これは、2 つのポートはそれぞれアクセス モードであり、1 つの VLAN だけを伝送するためです。この場合、2 つのポートは異なる VLAN に存在する必要があります。センサーはこれら 2 つの VLAN をブリッジし、2 つの VLAN 間を流れるすべてのトラフィックをモニタします。

2 つのスイッチ間にアプライアンスを接続することもできます。2 つの方法があります。第 1 の方法では、2 つのポートがアクセス ポートとして設定されるため、1 つの VLAN を伝送できます。この方法では、センサーは 2 つのスイッチ間で 1 つの VLAN をブリッジします。

第 2 の方法では、2 つのポートはトランク ポートとして設定されるため、複数の VLAN を伝送できます。この設定では、センサーは 2 つのスイッチ間で複数の VLAN をブリッジします。複数の VLAN がインライン インターフェイス ペアで伝送されるため、VLAN をグループに分けることができ、各グループを仮想センサーに割り当てることができます。

サポートされるセンサー

注意　サポートされていないセンサーに最新版のソフトウェアをインストールすると、予期せぬ結果が生じる可能性があります。サポートされていないプラットフォームにインストールしたソフトウェアは、サポートの対象外です。

特定の IPS ファイル名および各センサーがサポートする IPS バージョンのリストについては、次の URL にある IPS バージョンのリリース ノートを参照してください。

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_release_notes_list.html

表 1-4 に、Cisco IPS によってサポートされているセンサー（IPS アプライアンスおよびモジュール）を示します。

表 1-4　サポートされるセンサー

モデル名	部品番号	オプションのインターフェイス
アプライアンス		
IPS 4345	IPS-4345-K9	—
IPS 4360	IPS-4360-K9	—
IPS 4510	IPS 4510-K9	—
IPS 4520	IPS 4520-K9	—
モジュール		
ASA 5512-X	ASA5512-K7 ASA5512-K8 ASA5512-DC-K8	ASA-IC-6GE-CU-A= ASA-IC-6GE-SFP-A=
ASA 5515-X	ASA5515-K7 ASA5515-K8 ASA5515-DC ASA5515-DC-K8	ASA-IC-6GE-CU-A= ASA-IC-6GE-SFP-A=
ASA 5525-X	ASA5525-K7 ASA5525-K8 ASA5525-K9 ASA5525-DC	ASA-IC-6GE-CU-B= ASA-IC-6GE-SFP-B=

表 1-4　サポートされるセンサー （続き）

モデル名	部品番号	オプションのインターフェイス
アプライアンス		
ASA 5545-X	ASA5545-K7 ASA5545-K8 ASA5545-K9 ASA5545-DC-K8 ASA5545-CU-2AC-K9	ASA-IC-6GE-CU-C= ASA-IC-6GE-SFP-C=
ASA 5555-X	ASA5555-K8 ASA5555-CU-2AC-K9	ASA-IC-6GE-CU-C= ASA-IC-6GE-SFP-C=
ASA 5585-X IPS SSP-10	ASA-SSP-IPS10-K9	—
ASA 5585-X IPS SSP-20	ASA-SSP-IPS20-K9	—
ASA 5585-X IPS SSP-40	ASA-SSP-IPS40-K9	—
ASA 5585-X IPS SSP-60	ASA-SSP-IPS60-K9	—

詳細情報

最新版の Cisco IPS ソフトウェアを入手する方法については、「Cisco IPS ソフトウェアの入手方法」（P.C-1）を参照してください。

IPS アプライアンス

ここでは、Cisco アプライアンスについて説明します。取り上げる事項は次のとおりです。

IPS アプライアンスの導入

（注）　現在サポートされている Cisco IPS アプライアンスは、IPS 4345、IPS 4360、IPS 4510、および IPS 4520 です。

IPS アプライアンスは、高性能のプラグアンドプレイ デバイスです。アプライアンスは、ネットワークベースのリアルタイム侵入防御システムである IPS のコンポーネントです。アプライアンスの設定には、IPS CLI、IDM、IME、ASDM、または CSM を使用できます。IPS のマニュアルのリストおよびアクセス方法については、『*Documentation Roadmap for Cisco Intrusion Prevention System 7.2*』を参照してください。

ネットワーク トラフィックを取り込み、分析すると同時に、認識したシグニチャに応答するようにアプライアンスを設定できます。これらの応答には、イベントのログ取得、イベントのマネージャへの転送、TCP リセットの実行、IP ログの生成、アラート用トリガー パケットの取り込み、ルータの再設定などがあります。アプライアンスは、ワーム、スパイウェア、アドウェア、ネットワーク ウイルス、アプリケーションの不正使用などの脅威を検出、分類、および阻止するのに役立てることによって、重要な保護を提供します。

アプライアンスは、ネットワークの重要な地点に設置された後、広範囲に渡る埋め込み型シグニチャ ライブラリに基づいて異常動作と悪用行為を探すことで、ネットワーク トラフィックの監視およびリアルタイム分析を実行します。システムが不正行為を検出した場合、アプライアンスは、特定の接続を終了し、攻撃中のホストを恒常的にブロックし、事故のログを取得し、マネージャにアラートを送信します。その他の正規の接続は、中断することなく独立した動作を継続します。

アプライアンスは、特定のデータ レートに対して最適化され、イーサネット構成、ファスト イーサネット構成、およびギガビット イーサネット構成にパッケージ化されます。スイッチド環境では、アプライアンスは、スイッチの SPAN ポートまたは VACL キャプチャ ポートに接続する必要があります。

Cisco IPS アプライアンスは、次の機能を提供します。

- 最大 8 つのインターフェイスを使用した複数のネットワーク サブネットの保護
- 混合モードとインライン モードの両方での同時二重動作
- 幅広いパフォーマンス オプション：80 Mbps ～ 数ギガビット
- センサーとともにパッケージ化された埋め込み型 Web ベース管理ソリューション

詳細情報

- サポートされるアプライアンスの一覧については、「サポートされるセンサー」（P.1-19）を参照してください。
- IPS 4345 および IPS 4360 の詳細については、第 3 章「IPS 4345 および IPS 4360 の設置」を参照してください。
- IPS 4510 および IPS 4520 の詳細については、第 4 章「IPS 4510 および IPS 4520 の設置」を参照してください。
- ASA 5585-X IPS SSP の詳細については、第 5 章「ASA 5585-X IPS SSP の取り付けおよび取り外し」を参照してください。

アプライアンスの制約事項

アプライアンスの使い方と動作については、次の制約事項があります。

- アプライアンスは、汎用のワークステーションではありません。
- シスコは、Cisco IPS を実行せずにアプライアンスを使用することを禁止しています。
- シスコは、アプライアンス内のハードウェアまたはソフトウェアを修正またはインストールすることは、Cisco IPS の正常な操作に含まれる場合を除き、禁止しています。

ターミナル サーバへのアプライアンスの接続

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- RJ-45 接続を行うターミナル サーバの場合、ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

- ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

ステップ 2　ターミナル サーバで、ラインとポートを設定します。イネーブル モードで次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションは確実に正しく終了してください。ターミナル セッションが正しく終了されていない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号が受信されていない場合、ターミナル セッションは開いたままです。ターミナル セッションが正しく終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証が実行されません。

注意　接続を確立するために使用したアプリケーションを終了する前に、必ずセッションを終了してログイン プロンプトに戻ってください。

注意　誤って接続が切断されたり終了した場合は、接続を再確立し、正しく終了して、アプライアンスに対する不正なアクセスを防ぎます。

時刻源とセンサー

ここでは、エラーがある場合に、センサーの信頼できる時刻源を持つことの重要性と時間を修正する方法について説明します。次の項目について説明します。

センサーおよび時刻源

（注）　センサー上の時間を調整するには、NTP サーバを使用することを推奨します。認証された NTP または認証されていない NTP を使用できます。認証された NTP には、NTP サーバの IP アドレス、キー ID、およびキー値が必要です。NTP は初期化中にセットアップできます。また、CLI、IDM、IME、または ASDM を介して NTP を設定することもできます。

センサーには、信頼できる時刻源が必要です。すべてのイベント（アラート）に、正しい UTC と現地時間のタイムスタンプが必要です。タイムスタンプがないと、攻撃の後でログを正しく分析できません。センサーを初期化するときに、時間帯とサマータイム設定をセットアップします。ここでは、センサーに時刻を設定するためのさまざまな方法を概説します。

IPS スタンドアロン アプライアンス

- **clock set** コマンドを使用して、時刻を設定する。これはデフォルトです。
- アプライアンスが NTP 同期時刻源から時間を取得するように設定できます。

（注）　現在サポートされている Cisco IPS アプライアンスは、IPS 4345、IPS 4360、IPS 4510、および IPS 4520 です。

ASA IPS モジュール

- ASA 5500-X IPS SSP および ASA 5585-X IPS SSP は、インストールされている適応型セキュリティ アプライアンスのクロックに自動的にクロックを同期させます。これはデフォルトです。
- これらは、時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように設定できます。

IPS モジュールのシステム クロックと親デバイスのシステム クロックとの同期

IPS モジュール（ASA 5500-X IPS SSP および ASA 5585-X IPS SSP）は、IPS がブートアップするたび、および親シャーシのクロックが設定されるたびに、親シャーシのクロック（スイッチ、ルータまたは適応型セキュリティ アプライアンス）にクロックを同期させます。IPS のクロックと親シャーシのクロックは、時間の経過とともにずれが生じる傾向があります。誤差は、1 日で数秒になることがあります。この問題を回避するには、IPS のクロックと親シャーシのクロックの両方が外部 NTP サーバと同期するようにします。NTP サーバに IPS クロックのみ同期させた場合、または親シャーシ クロックのみ同期させた場合、時刻の差異が発生します。

センサーと NTP サーバの同期の確認

Cisco IPS では、無効な NTP キー値や ID などの誤った NTP 設定をセンサーに適用できません。誤った設定を適用しようとすると、エラー メッセージが表示されます。NTP 設定を確認するには、**show statistics host** コマンドを使用してセンサーの統計情報を収集します。NTP 統計情報セクションには、NTP サーバとセンサーの同期に関するフィードバックを含む NTP 統計情報が表示されます。

NTP 設定を確認するには、次の手順を実行します。

ステップ 1　センサーにログインします。

ステップ 2　ホストの統計情報を生成します。

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
```

```
        2 10373  9014   yes   yes  none    reject   reachable  1
      status = Not Synchronized
   ...
```

ステップ 3　数分後にもう一度、ホストの統計情報を収集します。

```
sensor# show statistics host
   ...
   NTP Statistics
           remote           refid      st t when poll reach   delay   offset  jitter
      *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
       LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
      ind assID status  conf reach auth condition  last_event cnt
        1 10372  f624   yes   yes   ok   sys.peer   reachable  2
        2 10373  9024   yes   yes  none    reject   reachable  2
      status = Synchronized
```

ステップ 4　ステータスが [Not Synchronized] のままの場合は、NTP サーバが正しく設定されていることを NTP サーバの管理者に確認してください。

センサーの時刻の修正

イベントには発生時の時刻がスタンプされるため、時刻を誤って設定した場合、保存されたイベントの時刻は不正確になります。イベント ストアのタイムスタンプは、常に UTC 時刻に基づいています。元のセンサーのセットアップ中に、時刻を 8:00 a.m. ではなく 8:00 p.m. に設定した場合、エラーを訂正すると、訂正された時刻がさかのぼって設定されます。そのため、新しいイベントに古いイベントの時刻よりも過去の時刻が記録される場合があります。

たとえば、初期セットアップ中にセンサーを中部時間に設定し、さらにサマータイムを有効にした場合、現地時間が 8:04 p.m. であれば、時刻は 20:04:37 CDT として表示され、UTC からのオフセットは -5 時間になります（翌日の 01:04:37 UTC）。1 週間後の 9:00 a.m. に、21:00:23 CDT と表示された時計を見て誤りに気づいたとします。それから時刻を 9:00 a.m. に変更します。時計は現在 09:01:33 CDT と表示されています。UTC からのオフセットは変更されていないため、UTC 時刻は 14:01:33 UTC になります。ここにタイムスタンプの問題が生じる原因があります。

イベント レコードのタイムスタンプの整合性を維持するには、**clear events** コマンドを使用して、古いイベントのイベント アーカイブを消去する必要があります。

（注）　イベントは、個別には削除できません。

詳細情報

イベントのクリアの手順には、「イベント ストアからのイベントのクリア」を参照してください。