センサーの概要

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、特に明記のない限り、*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、P.1-12 の「サポートしているセンサー」を参照してください。

この章は、次の項で構成されています。

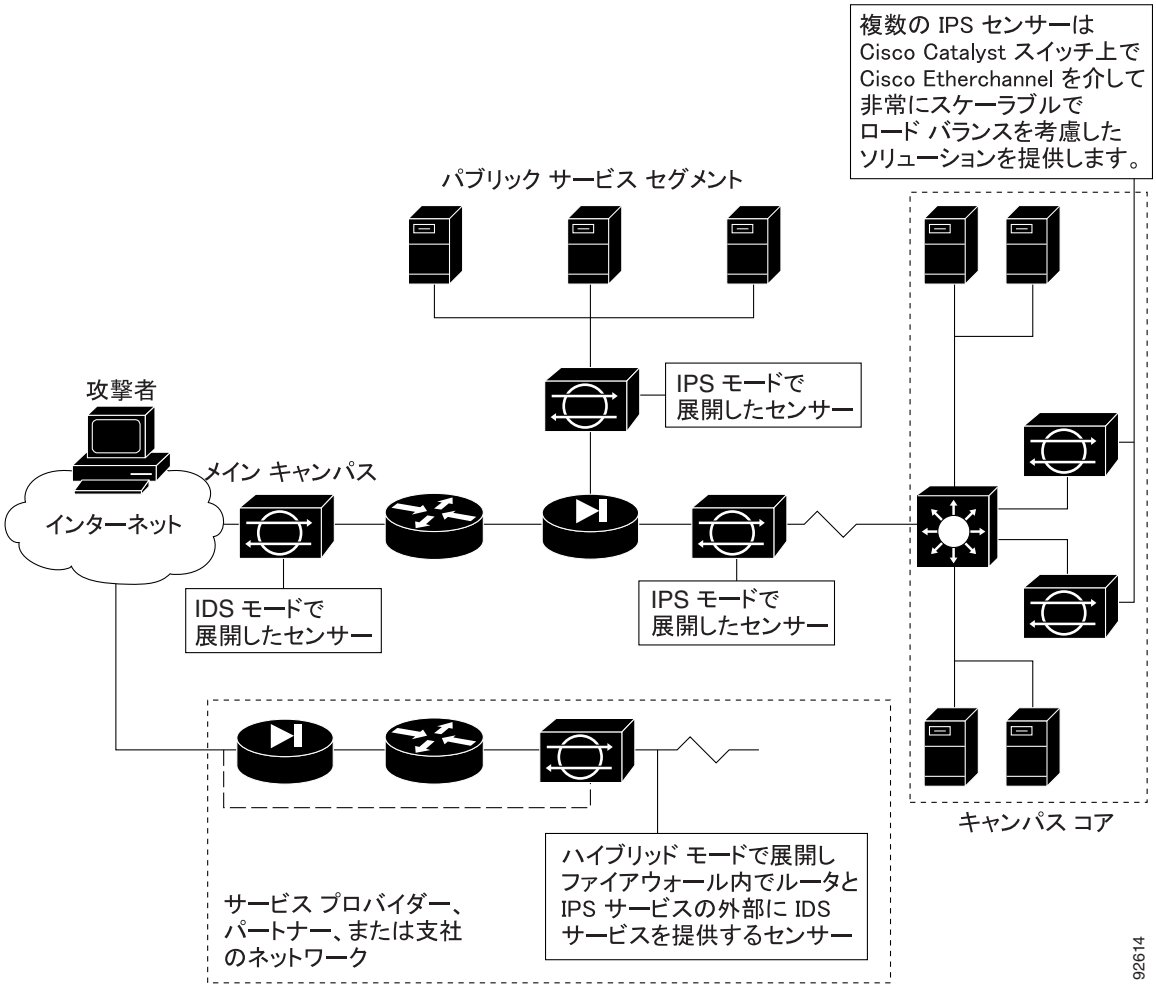
センサーの動作

この項では、センサーの動作について説明します。取り上げる事項は次のとおりです。

ネットワーク トラフィックの取り込み

センサーは、混合モードまたはインライン モードのいずれかで運用できます。図 1-1 に、ネットワークを保護するために、インライン（IPS）モードと混合（IDS）モードの両方で動作するセンサーの組み合せを展開する方法を示します。

図 1-1　展開ソリューションの全体図



（注）　IDS-4210 および NM-CIDS は、インライン モードでは動作しません。

コマンド / コントロール インターフェイスは、常にイーサネットです。このインターフェイスには、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（Cisco スイッチ、ルータ、およびファイアウォール）と通信できる割り当て済み IP アドレスがあります。このインターフェイスはネットワーク上で見ることができるので、データのプライバシーを保持するには、暗号化を使用する必要があります。SSH は CLI を保護するために使用し、TLS と SSL は、マネージャ ワークステーションを保護するために使用します。SSH および TLS と SSL は、マネージャ ワークステーション上において、デフォルトでイネーブルになっています。

攻撃に応答する場合、センサーは次の処置を実行できます。

- センシング インターフェイスを経由して 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するシグニチャ上においてのみ選択してください。非 TCP ベースのサービス上のアクションとして選択した場合、アクションは起こりません。さらに、TCP プロトコルには限界があるため、TCP リセットが違法なセッションを必ず切断するという保証はありません。IDS-4250-XL では、TCP リセットは、TCP リセット インターフェイスを通して送信されます。

- 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 が阻止する可能性があるのは、現在のトラフィックではなく、将来のトラフィックだけです。

- IP セッション ログ、セッションの再生、およびトリガー パケットの表示を生成する。

  IP セッション ログは、不正な使用に関する情報の収集に使用されます。IP ログ ファイルは、アプライアンスの検索対象として設定したイベントが発生したときに書き込まれます。
- 複数のパケット ドロップ アクションを行ってワームとウイルスを阻止する。

センサー インターフェイス

センサー インターフェイスには、最大速度とインターフェイスの物理位置に対応する名前が付けられています。物理位置は、ポート番号とスロット番号で構成されます。センサー 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。各 PCI 拡張スロットには、1 から始まるスロット番号が付けられています。スロット番号は一番下のスロットが 1 で、下から上に向かって大きくなります。特定のスロットを持つインターフェイスには、0 から始まるポート番号が付けられています。ポート番号は一番右のポートが 0 で、右から左に向かって大きくなります。たとえば、GigabitEthernet2/1 は、1 ギガビットの最大速度をサポートする右から 2 番目のインターフェイスで、下から 2 番目の PCI 拡張スロットにあります。IPS-4240 および IPS-4255 は、この規則の例外です。これらのセンサー上のコマンド / コントロール インターフェイスは、GigabitEthernet0/0 ではなく、Management0/0 と呼ばれます。

各物理インターフェイスは、コマンド / コントロール、センシング、および代替 TCP リセットの 3 つの役割のいずれかを実行します。

この項で取り上げる事項は次のとおりです。

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、センサーを設定するために使用されます。このインターフェイスは、センサーからセキュリティ イベントおよびステータス イベントを受信し、センサーに統計情報を照会します。

コマンド / コントロール インターフェイスは、恒常的にイネーブルです。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、センサーのモデルによって異なります。コマンド / コントロール インターフェイスを、センシング インターフェイスまたは代替 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
IDS-4210	FastEthernet0/1
IDS-4215	FastEthernet0/0
IDS-4235	GigabitEthernet0/1
IDS-4250	GigabitEthernet0/1
IPS-4240	Management0/0
IPS-4255	Management0/0
NM-CIDS	FastEthernet0/0
AIP SSM 10	GigabitEthernet0/0
AIP SSM 20	GigabitEthernet0/0
IDSM-2	GigabitEthernet0/2

センシング インターフェイス

センシング インターフェイスは、セキュリティ違反のトラフィックを分析するセンサーによって使用されます。センサーは、1 つ以上のセンシング インターフェイスを持ちます。この数は、センサーによって異なります。各センサーで使用可能なセンシング インターフェイスの数とタイプについては、P.1-5 の「インターフェイス サポート」を参照してください。

センシング インターフェイスは、混合モードで個別に運用できます。または、センシング インターフェイスをペアにして、インライン センシング モード用のインライン インターフェイスを作成することもできます。詳細については、P.1-10 の「混合モードの説明」、P.1-10 の「インライン インターフェイス モードの説明」、および P.1-10 の「インライン VLAN ペア モードの説明」を参照してください。

（注）　アプライアンスでは、すべてのセンシング　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。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、センシング インターフェイスは恒常的にイネーブルになっています。

一部のアプライアンスは、センサーにセンシング インターフェイスを追加するオプションの PCI インターフェイス カードをサポートします。これらのオプション カードの取り付けまたは取り外しは、センサーの電源が切れている間に行う必要があります。センサーは、サポートするインターフェイス カードの取り付けまたは取り外しを検出します。オプションの PCI カードを取り外すと、インターフェイス設定の一部が削除されます。削除される設定は、速度、デュプレックス、説明ス

トリング、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 ペアなどです。カードを再び取り付けると、これらの設定はデフォルト設定に戻ります。分析エンジンへの混合インターフェイスおよびインライン インターフェイスの割り当ては、分析エンジン設定からは削除されませんが、これらのカードを再び取り付けて、インライン インターフェイス ペアを再作成するまで無視されます。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Analysis Engine」または『*Installing and Using Cisco Intrusion Prevention System Device Manager Version 5.1*』を参照してください。

インターフェイス サポート

表 1-2 に、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 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 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

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 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	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
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 に取り付けることができます。S は、1 または 2 のいずれかのスロット番号を示します。

TCP リセット インターフェイス

この項では、TCP リセット インターフェイスについて説明します。また、どのような場合にそれらを使用するかについても説明します。取り上げる事項は次のとおりです。

代替 TCP リセット インターフェイスの説明

TCP リセット パケットを送信するようにセンサーを設定して、攻撃ホストとそのホストが意図するターゲット ホストの間のネットワーク接続をリセットすることができます。一部のインストレーションでは、インターフェイスが混合モードで動作しているときに、センサーは攻撃が検出されたセンシング インターフェイスで TCP リセット パケットを送信できない場合があります。このような場合、センシング 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と、混合モードで動作しているときにセンシング インターフェイスで送信されるはずだったすべての TCP リセットは、代わりに関連付けた代替 TCP リセット インターフェイス上で発信されます。詳細については、P.1-8 の「代替 TCP リセット インターフェイスの指定」を参照してください。

センシング 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関連付けた場合、その関連付けは、センサーが混合モードに設定されているときには適用されますが、センシング インターフェイスがインライン モードに設定されているときは無視されます。

IDSM-2 以外では、任意のセンシング インターフェイスを別のセンシング 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使用できます。IDSM-2 上の代替 TCP リセット インターフェイスは、ハードウェア制限があるために固定されています。

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
IDS-4210	なし[1]
IDS-4215	任意のセンシング インターフェイス
IDS-4235	任意のセンシング インターフェイス
IDS-4250	任意のセンシング インターフェイス
IPS-4240	任意のセンシング インターフェイス
IPS-4255	任意のセンシング インターフェイス
NM-CIDS	なし[2]
AIP SSM 10	なし[3]
AIP SSM 20	なし[4]
IDSM-2	System0/1[5]

1. IDS-4210 上のセンシング インターフェイスは 1 つだけです。
2. NM-CIDS 上のセンシング インターフェイスは 1 つだけです。
3. AIP SSM 10 上のセンシング インターフェイスは 1 つだけです。
4. AIP SSM 20 上のセンシング インターフェイスは 1 つだけです。
5. これは、Catalyst バックプレーン上の内部インターフェイスです。

代替 TCP リセット インターフェイスの指定

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。

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るのは、センシング インターフェイスだけです。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

センサー上のインターフェイスの設定については、次の制約事項があります。

- 物理インターフェイス
  - 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 上では、すべてのバックプレーン インターフェイスは、速度、デュプレックス、および状態の設定を固定しています。これらの設定は、すべてのバックプレーン インターフェイス上のデフォルト設定で保護されています。
  - バックプレーンではない 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。有効なデュプレックス設定は、全二重、半二重、および自動です。
  - 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、有効な速度設定は、1000 Mbps および自動です。
  - ギガビット銅インターフェイス（IDS-4235、IDS-4250、IPS-4240、および IPS-4255 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、全二重、半二重、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、速度を 1000 Mbps に設定すると、有効なデュプレックス設定は自動だけになります。
  - コマンド / コントロール インターフェイスをセンシング インターフェイスとして使用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
  - インライン インターフェイス ペアには、インターフェイスの物理インターフェイス タイプ（銅またはファイバ）、速度、またはデュプレックスの設定にかかわらず、センシング インターフェイスの任意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、およびデュプレックスの設定が異なるインターフェイスのペアは、完全にはテストされていない場合、または正式にはサポートされていない場合があります。詳細については、P.1-5 の「インターフェイス サポート」を参照してください。
  - コマンド / コントロール インターフェイスは、インライン インターフェイス ペアを構成できません。

- インライン インターフェイス ペアにおいて、物理インターフェイスをそれ自体とペアにすることはできません。
- 1 つの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 ペアだけを構成できます。
- インライン モードをサポートするセンサー プラットフォーム上に限り、バイパス モードを設定し、インライン インターフェイス ペアを作成することができます。
- 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**なし**以外の場合、物理インターフェイスはインライン インターフェイス ペアを構成できません。

- インライン VLAN インターフェイス ペア
  - VLAN をそれ自体とペアにすることはできません。
  - ある特定のセンシング インターフェイスにとって、1 つの VLAN は 1 つのインライン VLAN ペアだけを構成できます。ただし、ある特定の VLAN が、複数のセンシング インターフェイス上で 1 つのインライン VLAN ペアを構成することはできます。
  - インライン VLAN ペアの各 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 ペアを持つことができます。
- 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 インターフェイスだけに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**なし**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のために保護されています。
  - 同一の物理インターフェイスを、複数のセンシング インターフェイス用の代替 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しても、代替 TCP リセット インターフェイスとしても使用できます。
  - コマンド / コントロール インターフェイスを、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使用することはできません。
  - センシング インターフェイスを、それ自体の代替 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。
  - 代替 TCP リセット インターフェイスとして設定できるのは、TCP リセットの機能を持つインターフェイスだけです。

（注） この制約事項の例外は IDSM-2 です。双方のセンシング 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）。

インターフェイス モード

この項では、インターフェイス モードについて説明します。取り上げる事項は次のとおりです。

- 混合モードの説明（P.1-10）
- インライン インターフェイス モードの説明（P.1-10）
- インライン VLAN ペア モードの説明（P.1-10）

混合モードの説明

混合モードでは、パケットはセンサー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センサー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、センサーが阻止できないことです。混合センサー 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キング 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。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。これにより、センサーは、悪意のあるトラフィックが意図したターゲットに到達する前にそのトラフィック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） AIP 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。

（注） ペアの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アクセス ポートとして設定し、それら 2 つのポートのアクセス VLAN を異なるものにする必要があります。そのようにしないと、トラフィックはインライン インターフェイスを流れません。

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に、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 オン スティック」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されてから、ペアのもう一方の VLAN に転送されます。インライン VLAN ペアは、NM-CIDS、AIP SSM 10、および AIP SSM 20 を除いて、IPS 5.1 と互換性の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、センシング インターフェイスが 802.1q トランク ポートとして機能し、センサーがトランク上の VLAN のペアの間の VLAN ブリッジングを実行する、アクティブなセンシング モードです。センサーは、各ペアの各 VLAN 上で受信したトラフィックを検査し、ペアの VLAN のもう一方でパケットを転送するか、侵入の試みが検出された場合はそのパケットをド

ロップします。IPS センサーは、各センシング 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 で置き換えます。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 上で受信したパケットをすべてドロップします。

ネットワーク トポロジ

センサーを展開し、設定する前に、使用しているネットワークについて次の事項を理解しておく必要があります。

- 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

この知識があれば、センサーの所要台数、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 カードの規模とタイプ）、必要なマネージャ数を判断するのに役立ちます。

サポートしているセンサー

表 1-4 に、Cisco IPS 5.1 がサポートしているセンサー（アプライアンスおよびモジュール）を示します。

（注）　最新版の Cisco IPS ソフトウェアを入手する方法については、P.10-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

注意　サポートしていないセンサーに最新版のソフトウェア（バージョン　5.1）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。サポートし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。

表 1-4　サポートしているセンサー

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		
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	— — —
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9[1]	IDS-4FE-INT= —
IDS-4235	IDS-4235-K9 IDS-4235-TX-K9	IDS-4FE-INT= IDS-TX-INT=
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	IDS-4FE-INT= IDS-4250-SX-INT=[2] IDS-XL-INT= IDS-TX-INT= — —
IPS-4240	IDS-4240-K9 IPS-4240-DC-K9[3]	— —
IPS-4255	IDS-4255-K9	—
モジュール		
AIP SSM 10	ASA-SSM-AIP-10-K9	—
AIP SSM 20	ASA-SSM-AIP-20-K9	—
IDSM-2	WS-SVC-IDSM2-K9	—
NM-CIDS	NM-CIDS-K9	—

1. IDS-4215-4FE-K9 は、IDS-4215-K9 にオプションの 4FE カード（IDS-4FE-INT=）を工場で取り付けたものです。
2. IDS-4250 には、1 枚または 2 枚の IDS-4250-SX-INT カードを取り付けることができます。
3. IPS-4240-DC-K9 は、NEBS 準拠の製品です。

次の NRS および IDS アプライアンス モデルは旧モデルであり、このマニュアルではサポートしていません。

- NRS-2E
- NRS-2E-DM
- NRS-2FE
- NRS-2FE-DM
- NRS-TR
- NRS-TR-DM
- NRS-SFDDI
- NRS-SFDDI-DM
- NRS-DFDDI
- NRS-DFDDI-DM
- IDS-4220-E
- IDS-4220-TR
- IDS-4230-FE
- IDS-4230-SFDDI
- IDS-4230-DFDDI

（注）　WS-X6381 は IDSM ですが、旧モデルのため、このマニュアルではサポートしていません。

（注）　IDS-4210 で最新の IPS ソフトウェアをサポートするには、メモリのアップグレードが必要です。詳細については、P.2-4 の「メモリのアップグレード」を参照してください。

アプライアンス

この項では、Cisco 4200 シリーズ 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。

アプライアンスの概要

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。サポートしているアプライアンスのリストについては、P.1-12 の「サポートしているセンサー」を参照してください。

CLI、IDM、または ASDM を使用して、アプライアンスを設定できます。IPS マニュアルのリストおよびマニュアルへのアクセス方法については、アプライアンスに添付されている『*Documentation Roadmap for Cisco Intrusion Prevention System 5.1*』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。他の正当な接続は、それとは無関係に中断されることなく動作し続けます。

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、ファースト 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 4200 シリーズ 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

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。
- シスコシステムズは、Cisco IPS が動作していない場合のアプライアンスの使用を禁止しています。
- シスコシステムズは、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ない場合、禁止しています。

ターミナル サーバのセットアップ

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。

- IDS-4215、IPS-4240、および IPS-4255 の場合
  - RJ-45 接続の場合、180/ 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。
- その他のアプライアンスの場合は、すべて M.A.S.H. アダプタ（部品番号 29-4077-01）をアプライアンスの COM1 に接続して、次の操作を行います。
  - RJ-45 接続の場合、180/ ロールオーバー ケーブルを M.A.S.H. アダプタからターミナル 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 M.A.S.H. アダプタからターミナル サーバのポートに接続します。

ステップ 2　次のようにターミナル サーバ上にラインおよびポートを設定します。

a. イネーブル モードでは、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
```

b. IDS-4215、IPS-4240、または IPS-4255 用にターミナル サーバを設定する場合は、ステップ 3 に進みます。

それ以外の場合は、サポートしている他のすべてのアプライアンスに対して、すべての出力をターミナル サーバに送ります。CLI にログインして、次のコマンドを入力します。

```
sensor# configure terminal
sensor(config)# display-serial
```

出力は、シリアル ポートに送られます。**no display-serial** コマンドを使用して、出力をキーボードとモニタにリダイレクトします。

（注）　ターミナル サーバをセットアップし、**display-serial** コマンドを使用して、アプライアンスからの出力すべてをシリアル ポートに送ることができます。このオプションを使用すると、ブート処理中でも、シリアル ポートに接続したコンソールにシステム メッセージを表示できます。このオプションを使用する場合、出力はすべて、シリアル ポートに送られ、ローカルのキーボードおよびモニタ接続はディセーブルにされます。しかし、BIOS メッセージと POST メッセージは、ローカルのキーボードおよびモニタ上に表示されます。

（注） IDS-4215、IPS-4240、または IPS-4255 には、キーボード ポートまたはモニタ ポートがありません。したがって、**display-serial** および **no display-serial** コマンドは、これらのプラットフォームには適用されません。

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 セッションが正常に閉じられていることを確認してください。

ターミナル セッションが正常に終了していない場合、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) 信号を受信していない場合、ターミナル セッションは開いたままです。ターミナル セッションが正常に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、認証は実行されません。

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、常にセッションを終了してログイン プロンプトに戻ります。

注意 偶然に接続が切れたり、終了した場合は、接続を再確立し、正常に終了して、アプライアンスに対する不正なアクセスを防ぎます。

モジュール

この項では、モジュー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。

AIP SSM の概要

Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP SSM) は、Cisco ASA 5500 シリーズ Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）の IPS プラグイン モジュールです。ASA ソフトウェアは、ファイアウォール、VPN コンセントレータ、侵入検知および侵入防御のソフトウェア機能を 1 つのソフトウェア イメージに組み合せます。

AIP SSM には ASA-SSM-AIP-K9-10 および ASA-SSM-AIP-K9-20 の 2 つのモデルがあります。ASA-SSM-AIP-K9-10 は、約 100 Mbps のスループットをサポートし、ASA-SSM-AIP-K9-20 は、約 200 Mbps のスループットをサポートします。ASA のスロットに一度に装着できるモジュールは、1 つだけです。

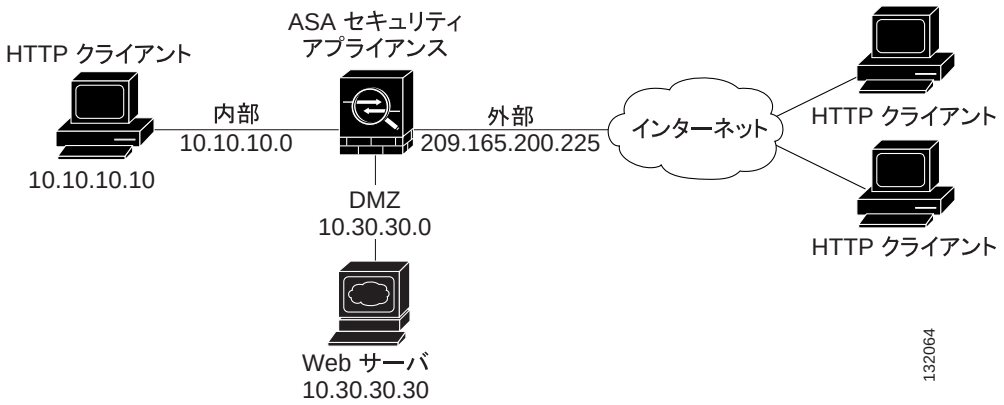
AIP SSM は、より詳細なセキュリティ検査を実施する高度な IPS ソフトウェアを、インライン モードまたは混合モードのどちらかで実行します。ASA は、パケットが出力インターフェイスを出る直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）、および他のファイアウォール ポリシーが適用された後に、パケットを AIP SSM に転送します。たとえば、アクセス リストによってブロックされたパケットは、AIP SSM に転送されません。

混合モードでは、IPS は GigabitEthernet インターフェイスを通してパケットを受け取り、侵入動作があるかどうかを検査し、侵入動作があった場合はアラートを生成します。インライン モードでは、侵入が検出されなかったパケットをすべて GigabitEthernet インターフェイスに送り返す手順が追加されます。

図 1-2 に、一般的な DMZ 構成の AIP SSM がある ASA を示します。DMZ は、プライベート（内部）ネットワークとパブリック（外部）ネットワーク間の中立地帯にある別個のネットワークです。Web サーバは DMZ インターフェイス上にあり、内部ネットワークと外部ネットワークの両方の HTTP クライアントが Web サーバに安全にアクセスできます。

図 1-2 では、内部ネットワーク上の HTTP クライアント（10.10.10.10）は、DMZ Web サーバ（30.30.30.30）と HTTP 通信を開始します。DMZ Web サーバへの HTTP アクセスは、インターネット上のすべてのクライアントに提供され、その他の通信はすべて拒否されます。ネットワークは、30.30.30.50 と 30.30.30.60 の間のアドレスの IP プール（DMZ インターフェイスに使用可能な一連の IP アドレス）を使用するように設定されます。

図 1-2　DMZ 構成



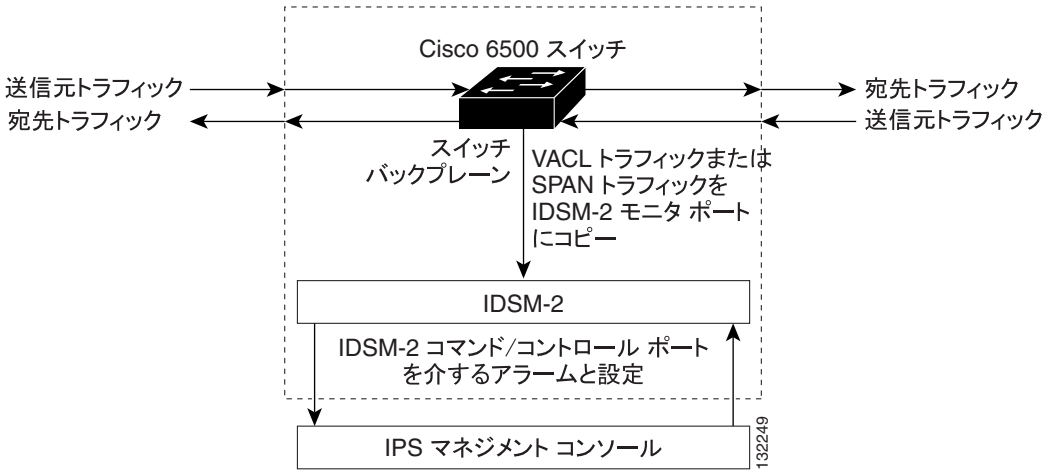
ASA のセットアップ方法については、『*Cisco ASA 5500 Quick Start Guide*』を参照してください。AIP SSM の設置方法については、P.6-4 の「AIP SSM の取り付け」を参照してください。AIP SSM が IPS トラフィックを受信するように設定する方法については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring AIP SSM」を参照してください。

IDSM-2 の概要

Cisco Catalyst 6500 シリーズの Intrusion Detection System Services Module（IDSM-2）は、Catalyst 6500 シリーズ スイッチおよび 7600 シリーズ ルータで侵入防御を実行するスイッチング モジュールです。IDSM-2 を設定するには、CLI または IDSM を使用します。IDSM-2 は、混合モードまたはインライン モードに設定できます。

IDSM-2 は、ネットワーク センシングを実行しています。つまりパケットの取り込みと分析を通して、リアルタイムでネットワーク パケットの監視を行っています。IDSM-2 は、ネットワーク パケットを取り込み、再構成し、代表的な侵入行為を示す攻撃シグニチャとパケット データを比較します。ネットワーク トラフィックの IDSM-2 へのコピーは、スイッチのセキュリティ VLAN に基づいて行われることも、スイッチの SPAN ポート機能を通して行われることもあります。これらの方法では、調査するスイッチ ポート、VLAN、またはトラフィック タイプに基づいて、IDSM-2 へのユーザ指定のトラフィックがルーティングされます（図 1-3 を参照してください）。

図 1-3　IDSM-2 のブロック ダイアグラム



IDSM-2 は、ネットワーク パケットのデータ部分またはヘッダー部分を検査することで、悪用のパターンを探します。コンテンツベースの攻撃では、悪意のあるデータはパケットのペイロードに含まれている可能性があります。一方、コンテキストベースの攻撃では、パケットのヘッダーに悪意のあるデータが含まれている可能性があります。

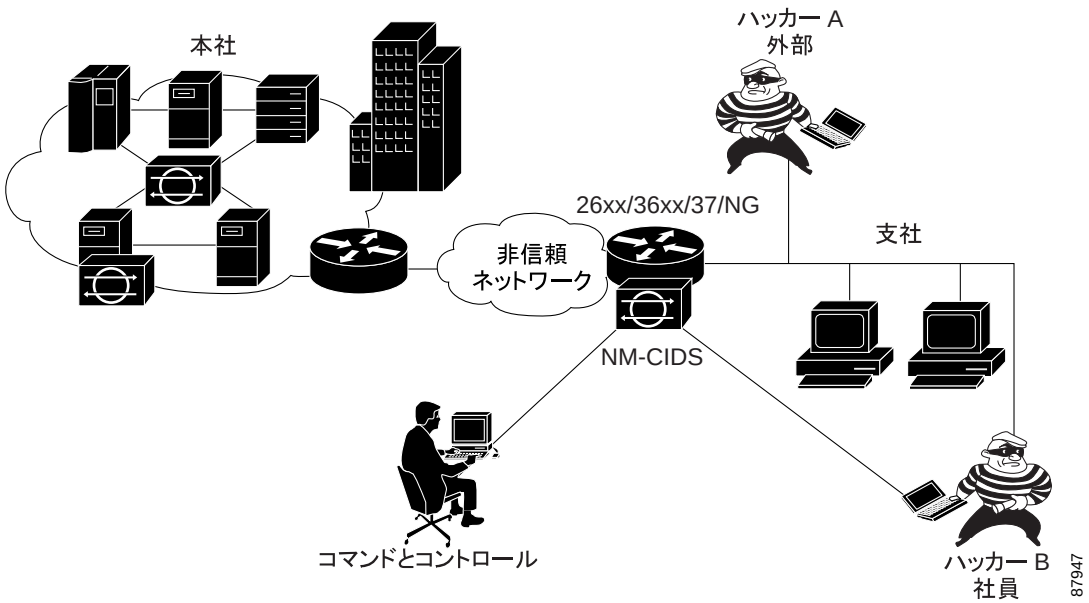
攻撃の可能性を検出したときにアラートを生成するよう IDSM-2 を設定できます。さらに、IDSM-2 を設定して、ソース VLAN に関する TCP リセットを送信し、IP ログを生成し、そして、ファイアウォールまたは他の管理対象装置上でブロッキングを行う対抗策を開始します。IDSM-2 が生成するアラートは、Catalyst 6500 シリーズのスイッチ バックプレーンを通して、IPS マネージャに生成されます。IPS マネージャにおいて、アラートはログに記録され、グラフィカル ユーザ インターフェイス上に表示されます。

NM-CIDS の概要

NM-CIDS（Cisco Intrusion Detection System Network Module）は、Cisco IDS の機能性を支社のルータに統合します。NM-CIDS の場合、全機能を持つ IDS をリモートの支社に導入できます。NM-CIDS は、Cisco 2600、3600、および 3700 シリーズ ルータのネットワーク モジュール スロットの 1 つに取り付けることができます。NM-CIDS は、最大 45 Mbps のネットワーク トラフィックを監視できます。サポートしているルータのリストについては、P.8-2 の「ソフトウェア要件およびハードウェア要件」を参照してください。NM-CIDS は、ルータあたり 1 台だけがサポートされています。図 1-4 に、支社環境におけるルータを示します。

（注）　NM-CIDS は、混合モード（IDS モード）のみで動作します。

図 1-4　支社ルータの NM-CIDS



NM-CIDS には内蔵 10/100 イーサネット ポートが 1 つあり、ルータのバックプレーンに接続されます。外部 10/100 ベース イーサネット ポートも 1 つあり、デバイス管理（他のルータやブロッキングを実行する PIX Firewalls の管理）および IDS マネージャによる NM-CIDS のコマンドとコントロールに使用されます。

NM-CIDS は、ルータと通信して、NM-CIDS の起動とシャットダウンに必要な制御情報や状態情報のやり取り、およびバージョン情報やステータス情報のやり取りを行います。NM-CIDS は、ルータ上の選択したインターフェイスから NM-CIDS 上の IDS インターフェイスに転送されたパケットを処理します。NM-CIDS は、取り込んだパケットを分析して、シグニチャと呼ばれる代表的な侵入行為のルール セットと比較します。取り込んだパケットがシグニチャ内の定義されている侵入パターンと一致したら、NM-CIDS は、攻撃をブロックするためにルータ上で ACL を変更するというアクション、および攻撃を起こしている TCP セッションを終了させるために TCP リセット パケットを発信者に送るというアクションのいずれかを実行します。

NM-CIDS は、取り込んだパケットを分析して悪意のある行為を識別するだけでなく、応答アクションとして設定できる IP セッションのログをシグニチャごとに取得することもできます。シグニチャが該当すると、指定した時間にセッション ログが tcpdump 形式で作成されます。Ethereal を使用してこれらのログを表示することも、IP セッションを TCP Replay などのツールを使用して再生することもできます。

イベントの管理および取得は、NM-CIDS から、CLI または IDM を通して行うことができます。

IDS 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、攻撃の後にログを正しく分析できません。NM-CIDS では、時刻を手動で設定できません。NM-CIDS は、取り付け先の Cisco ルータから時刻を取得します。ルータにはバッテリがないので、電源を切ると、設定した時刻を保持できません。ルータの電源投入またはリセットのたびにルータの時計を設定する必要があります。あるいは、ルータを設定して、NTP 時刻同期を使用することもできます。NTP 時刻同期を使用することを推奨します。NM-CIDS 自体、またはその取り付け先ルータのいずれかで、NTP 時刻同期を使用するように設定できます。詳細については、P.1-21 の「時刻源およびセンサー」を参照してください。

時刻源およびセンサー

この項では、センサーに信頼できる時刻源があることの重要性およびエラーが発生した場合の時刻の修正方法について説明します。

この項で取り上げる事項は次のとおりです。

センサー上の時刻の説明

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 Coordinated Universal Time（UTC; 世界標準時）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。詳細については、P.9-3 の「センサーの初期化」を参照してください。

センサーに時刻を設定する方法を要約して示します。

- アプライアンスの場合
  - **clock set** コマンドを使用して、時刻を設定する。これがデフォルトの方法です。

    手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Manually Setting the System Clock」を参照してください。
  - NTP を使用する。

    アプライアンスは、NTP 同期時刻源から時刻を取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP キー ID、および NTP キー値が必要です。初期化中に NTP をアプライアンスにセットアップすることも、CLI、IDM、または ASDM を通して NTP を設定することもできます。

    （注） NTP 同期時刻源を使用する方法を推奨します。

- IDSM-2 の場合
  - IDSM-2　は、自動的にその時計をスイッチ時刻と同期させることができる。これがデフォルトの方法です。

    （注） UTC 時刻は、スイッチと IDSM-2 の間で同期が取られます。時間帯とサマータイム設定は、スイッチと IDSM-2 間で同期が取られません。

注意　スイッチと IDSM-2 の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイム設定が IDSM-2 とスイッチとで一致していない場合、IDSM-2 の現地時間は不正確になる可能性があります。

- NTP を使用する。

  IDSM-2 は、その時刻を NTP 同期時刻源から取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP キー ID、および NTP キー値が必要です。初期化中に NTP を使用するように IDSM-2 を設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

  （注） NTP 同期時刻源を使用する方法を推奨します。

- NM-CIDS の場合
  - NM-CIDS は、自動的にその時計を取り付け先（親ルータ）のルータ シャーシの時計と同期させることができる。これがデフォルトの方法です。

    （注） UTC 時刻は、親ルータと NM-CIDS の間で同期が取られます。時間帯とサマータイム設定は、親ルータと NM-CIDS の間で同期が取られません。

注意 親ルータと NM-CIDS の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイムの設定が NM-CIDS とルータとで一致していない場合、NM-CIDS の現地時間は不正確になる可能性があります。

  - NTP を使用する。

    NM-CIDS は、その時刻を 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。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP キー ID、および NTP キー値が必要です。初期化中に NM-CIDS を NTP を使用するように設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

    （注） NTP 同期時刻源を使用する方法を推奨します。

- AIP SSM の場合
  - AIP SSM は、自動的にその時計を取り付け先の ASA の時計と同期させることができる。これがデフォルトの方法です。

    （注） UTC 時刻は、ASA と AIP SSM の間で同期が取られます。時間帯とサマータイム設定は、ASA と AIP SSM の間で同期が取られません。

注意 ASA と AIP SSM の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイムの設定が AIP SSM と ASA とで一致していない場合、AIP SSM の現地時間は不正確になる可能性があります。

－ NTP を使用する。

AIP SSM は、その時刻を 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。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP キー ID、および NTP キー値が必要です。初期化中に AIP SSM を NTP を使用するように設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

（注） NTP 同期時刻源を使用する方法を推奨します。

センサー上の時刻の修正

イベントには発生時の時刻が刻印されるため、時刻を誤って設定した場合、格納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。センサーの最初のセットアップ中に、時刻を午前 8 時と指定するところを午後 8 時と誤って設定した場合、エラーを修正したときに、修正した時刻が過去にさかのぼって設定されます。このため、新しいイベントの時刻が、古いイベントの時刻よりも以前になる場合があります。

たとえば、初期セットアップ中に、サマータイムをイネーブルにして中央時間にセンサーを設定し、現地時間が午後 8 時 4 分である場合、時刻は 20:04:37 CDT と表示され、UTC から 5 時間のオフセット（01:04:37 UTC、翌日）があります。一週間後の午前 9 時に、クロックに 21:00:23 CDT が表示されているエラーが見つかります。時刻を午前 9 時に変更すると、クロックには 09:01:33 CDT が表示されます。UTC からのオフセットは変更されていないため、UTC の時刻は 14:01:33 UTC である必要があります。このことによってタイムスタンプの問題が発生します。

イベント レコード上のタイムスタンプの統合性を保証するには、**clear events** コマンドを使用して、古いイベントのイベント アーカイブをクリアする必要があります。**clear events** コマンドの詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Clearing Events from the Event Store」を参照してください。

注意 個々のイベントは削除できません。

設置の準備

センサーを設置する準備をするには、次の手順を実行します。

ステップ 1　センサーに添付されている『*Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*』に記載されている安全上の注意事項を再度確認してください。

ステップ 2　IPS と関連資料、および Cisco.com における関連資料の所在を知るには、センサーに添付されている『*Documentation Roadmap for Cisco Intrusion Prevention System 5.1*』を参照してください。

ステップ 3　設置作業を実行する前に、Cisco.com から『*Release Notes for Cisco Intrusion Prevention System 5.1*』を入手して、熟読してください。

ステップ 4　センサーを開梱します。

ステップ 5　ESD 対策が施された環境にセンサーを置きます。

詳細については、P.1-25 の「設置場所および安全に関する推奨事項」を参照してください。

ステップ 6　センサーを安定した作業台に置きます。

ステップ 7　使用するセンサーのモデルに関連した章を参照します。

設置場所および安全に関する推奨事項

この項では、ESD 環境で電気、電源装置を取り扱う作業を行う場合の、設置場所のガイドラインおよび安全上の注意事項について説明します。取り上げる事項は次のとおりです。

設置場所のガイドライン

アプライアンスを机に置くか、またはラックに搭載します。システムが正常に動作するためには、アプライアンスの位置、および装置ラックまたは配線室の配置が非常に重要です。あまりに接近して配置された装置、不適切な通気、および手の届かないパネルは、システムの誤作動やシャットダウンの原因となり、アプライアンスのメンテナンスを困難にする可能性があります。

設置場所の配置および装置の位置を計画する場合は、次の注意事項に留意して、装置の故障を防ぎ、環境に起因するシャットダウンが起こらないようにしてください。既存の装置にシャットダウンまたは非常に重大な多くのエラーが発生する場合は、これらの注意事項が、障害の原因を分離し、将来の問題を防ぐのに役立つことがあります。

- 電気装置は熱を発生させます。空気の循環が適切でない場合、周囲の気温が、装置を仕様に合った動作温度まで冷却するのに適当でないことがあります。システムを運用する部屋に、適切な空気循環があることを確認してください。
- 機器への損傷を防ぐには、必ず ESD 防止手順に従ってください。静電放電による損傷は、即座のまたは断続的な機器障害の原因となる可能性があります。
- シャーシの上部パネルが固定されていることを確認します。シャーシは、冷却空気が内部を効率よく流れるように設計されています。シャーシが開いていると空気漏れが生じ、内蔵部品からの冷却空気の流れが妨げられたり、向きが変えられたりすることがあります。

ラック構成のガイドライン

装置ラックの構成を計画するには、次のガイドラインに従います。

- 閉鎖型ラックには、適切な通気が必要です。各シャーシは熱を発生させるため、ラックが過密にならないようにします。閉鎖型ラックには、冷却空気を供給するために、ルーバー付きの側面とファンが必要です。
- 開放型ラックにシャーシを搭載する場合は、ラックのフレームが吸気口や排気口をふさがないことを確認します。シャーシをスライドに取り付ける場合は、シャーシがラックに完全にはまったときに位置を確認します。
- 通気ファンが上部にある閉鎖型ラックの場合、ラックの底部付近で装置が発する過度の熱は上方に送られ、ラック内のその装置の上にある装置の吸気口に送られます。ラックの底部で、装置に対して適切な通気が行われるようにします。
- バッフルは、排気と吸気を分離するのに役立つことがあります。また、冷却空気をシャーシに取り込むのに役立つこともあります。バッフルの最適な配置は、ラック内のエアーフローのパターンによって異なります。さまざまな配置を試して、バッフルを効果的に配置してください。

電気の安全に関する推奨事項

警告　**シャーシの取り扱い作業または電源装置近くでの作業を行う前に、AC ユニットの電源コードを抜き、DC ユニットの回路ブレーカーの電源を切ります。**

電力を動力源にしている装置を取り扱うときは、次のガイドラインに従います。

- シャーシの内部にアクセスする必要がある手順を開始する前に、作業を行う部屋の緊急電源遮断スイッチの場所を確認してください。緊急電源遮断スイッチの場所を確認しておけば、電気の事故が発生した場合、迅速に電源を切ることができます。
- 作業場所に、危険な状況が発生する可能性がある場合は、一人で作業を行わないでください。
- 回路から電源が切断されているとは絶対に想定しないでください。必ず回路を確認してください。
- 濡れている床、接地されていない電源拡張ケーブル、擦り切れた電源コード、保安接地の欠如など、事故の原因となる可能性がある箇所が作業場所にないか、注意深く探してください。
- 電気の事故が発生した場合は、次のように対処します。
  - 自分自身が被災しないよう、十分注意してください。
  - システムの電源を切ります。
  - 可能な場合は、他の人に医療の援助を求めに行ってもらいます。不可能な場合は、被災者の状態を確かめてから救助を求めます。
  - 被災した人に人工呼吸が必要か、心臓マッサージが必要かを判断してから、適切な行動をとります。
- マークが付いた電力の範囲および製品使用説明書に記載されたシャーシを使用します。
- 『*Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*』に示されている地域および各国の電気工事規定に従ってセンサーを取り付けます。
- AC 入力電源装置が装備されているセンサー モデルは、アース タイプのコンセントにのみ適合するアース タイプのプラグが付いた 3 線電気コードが取り付けられて出荷されます。これは回避してはならない安全上の要点です。装置のアースは、地域および各国の電気工事規定に準拠していることが必要です。
- DC 入力電源装置が装備されているセンサー モデルは、DC 入力配線を使用して、15 アンペア以上を供給できる DC 電源上で終端する必要があります。15 アンペアの回路ブレーカーは、48 VDC ファシリティ電源で必要です。簡単にアクセスできる切断装置を、ファシリティ配線に組み込む必要があります。必ず、アース線コンジットをしっかりした接地場所に接続してください。指定のリング型端子を使用して、アース線をアース突起で終端することをお勧めします。このシステムへの DC 戻り線は、システム フレームおよびシャーシから絶縁しておく必要があります。

  DC 電源のその他のガイドラインは、『*Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor* 』マニュアルに記載されています。

電源装置のガイドライン

電源装置に関する次のガイドラインに従います。

- シャーシを取り付ける前に設置場所の電源を確認し、電源にスパイクやノイズがないことを保証します。必要に応じて電源調整器を取り付け、電源電圧の電圧レベルおよび電力レベルが適切に保たれるようにします。
- 落雷や電源の電圧の急激な変化による被害を避けるため、設置場所に適切なアースを取り付けます。
- AC 入力電源装置が装備されているシャーシには、次の事項が適用されます。
  - シャーシには、ユーザ選択可能な操作範囲はありません。AC 入力電源装置の正確な要件は、シャーシ上のラベルを参照してください。
  - いくつかのタイプの AC 入力電源装置コードが使用できます。設置場所に適したタイプのコードであることを確認します。
  - 設置場所に UPS を取り付けます。
  - 落雷や電源電圧の急激な変化による被害を防ぐため、設置場所に適切なアース　ファシリティを取り付けます。
- DC 入力電源装置が装備されているシャーシには、次の事項が適用されます。
  - 各 DC 入力電源装置には、専用の 15 アンペア サービスが必要です。
  - DC 電源ケーブルについては、14 AWG ワイヤ ケーブル以上をお勧めします。
  - このシステムへの DC 戻り線は、システム フレームおよびシャーシから絶縁しておく必要があります。

ESD 環境での作業

ESD の影響を受けやすい部品の取り扱いは、接地された静電気防止用の作業台（静電気防止用のワークベンチや静電気を散逸させるマットなど）にある承認済みの静電気保護ステーションでのみ行います。

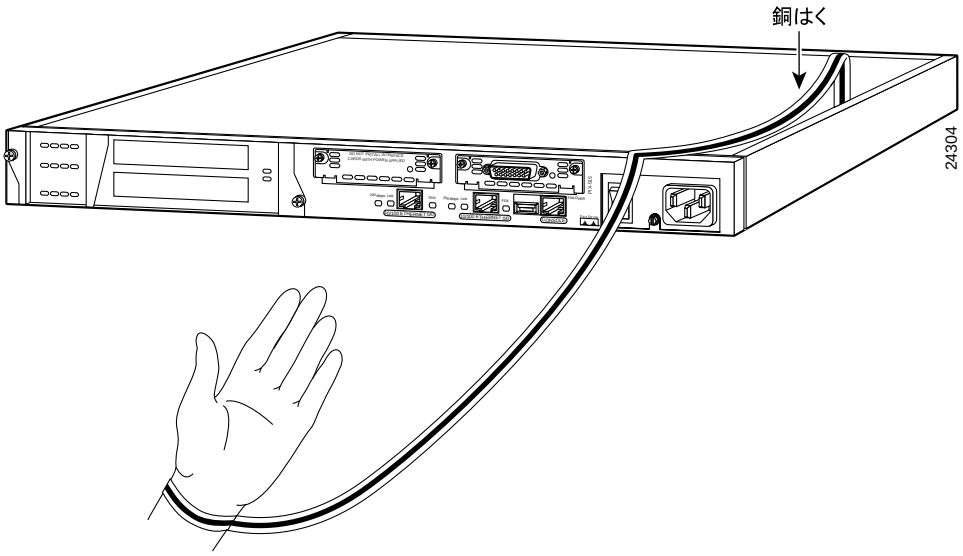
センサーのコンポーネントの取り外しと取り付けを行うには、次の手順を実行します。

ステップ 1　作業場所から静電気の発生源をすべて取り除きます。

ステップ 2　静電気防止用の作業台とリスト ストラップを使用します。

（注）　アップグレード部品に一般に付属している使い捨て式のリスト ストラップは、一度しか使用しないことを前提に設計されています。

ステップ 3　リスト ストラップを手首と作業台のターミナルに装着します。使い捨て式のリスト ストラップを使用している場合は、リスト ストラップをシャーシの塗装されていない金属面に直接接続します。



ステップ 4　アース ケーブルとワニロクリップを使用して、作業台をシャーシに接続します。

注意　コンポーネントの取り外し、取り付け、および修理を行うときは、必ず ESD 防止手順に従ってください。

（注）　コンポーネントをアップグレードする場合は、取り付けの準備が完了するまでコンポーネントを ESD 対応パッケージから取り出さないでください。

ケーブル ピン配置

この項では、10/100/1000BaseT、コンソール、RJ 45 ～ DB 9 ポート、および MGMT 10/100 イーサネット ポートのピン配置について説明します。この項で取り上げる事項は次のとおりです。

10/100BaseT コネクタおよび 10/100/1000BaseT コネクタ

センサーでは、10/100/1000BaseT ポートがサポートされます。100/1000Base-TX の運用には、少なくとも Category 5 ケーブルを使用する必要があります。10Base-TX の運用には、Category 3 ケーブルを使用できます。

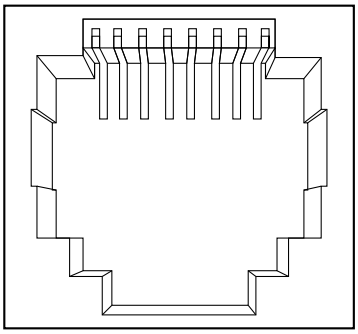
（注）　センサーには、10/100BaseT をサポートするもの（IDS-4210、IDS-4215、およびオプションの 4FE カード）と、10/100/1000BaseT をサポートするもの（IDS-4235、IDS-4250-TX、IPS-4240、および IPS-4255）があります。これは、銅アプライアンスにだけ該当します。ファイバ アプライアンスは、1000Base-SX だけをサポートします。

10/100/1000BaseT ポートは、標準 RJ-45 コネクタを使用し、MDI および MDI-X コネクタをサポートします。イーサネット ポートは通常 MDI コネクタを使用し、ハブ上のイーサネット ポートは通常 MDI-X コネクタを使用します。

イーサネット ストレート ケーブルは、MDI を MDI-X ポートに接続するのに使用します。クロス ケーブルは、MDI を MDI ポートに接続するか、または MDI-X を MDI-X ポートに接続するのに使用します。

図 1-5 に、10/100BaseT（RJ-45）ポートのピン配置を示します。

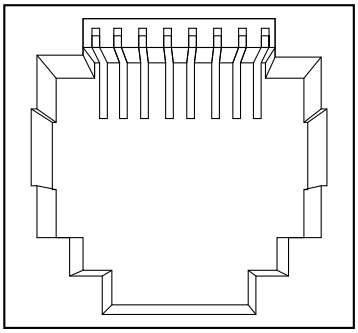
図 1-5　10/100 ポートのピン配置

ピン	ラベル	1 2 3 4 5 6 7 8
1	TD+	
2	TD-	
3	RD+	
4	NC	
5	NC	
6	RD-	
7	NC	
8	NC	

132412

図 1-6 に、10/100/1000BaseT（RJ-45）ポートのピン配置を示します。

図 1-6　10/100/1000 ポートのピン配置

ピン	ラベル	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

60915

コンソール ポート（RJ-45）

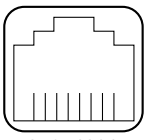
シスコ製品では、次のタイプの RJ-45 ケーブルが使用されます。

- ストレート型
- クロス型
- ロール型（コンソール）

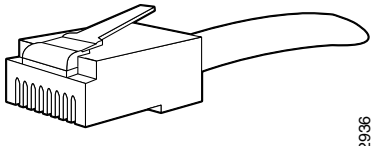
（注）　シスコではこれらのケーブルを提供していませんが、一般的に入手できます。

図 1-7 に、RJ 45 ケーブルを示します。

図 1-7　RJ-45 ケーブル



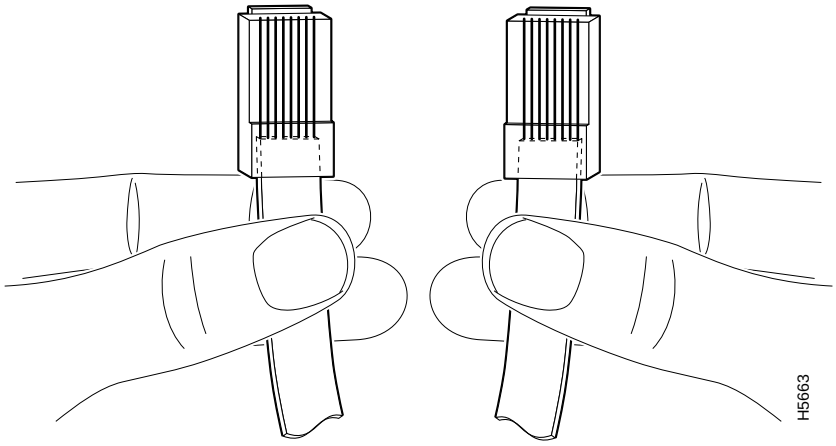
RJ-45 コネクタ



H2936

RJ-45 ケーブルのタイプを識別するには、図 1-8 に示すように、内部の色付きのワイヤが見えるようにケーブルの両端を並べて持ちます。

図 1-8　RJ-45 ケーブルの識別



色付きのワイヤの配列を調べて、次のように RJ-45 ケーブルのタイプを判別します。

- ストレート型：色付きのワイヤは、ケーブルの両端で同じ配列になっています。
- クロス型：ケーブルの一方の端の 1 番目（左端）の色付きのワイヤは、ケーブルのもう一方の端では 3 番目の色付きのワイヤになっています。
- ロール型：色付きのワイヤは、ケーブルの両端で逆の配列になっています。

RJ-45 ～ DB-9 または DB-25

表 1-5 に、RJ-45 ～ DB-9 または DB-25 のケーブル ピン配置を示します。

表 1-5　RJ-45 ～ DB-9 または DB-25 のケーブル ピン配置

信号	RJ-45 ピン	DB-9/DB-25 ピン
RTS	8	8
DTR	7	6
TxD	6	2
GND	5	5
GND	4	5
RxD	3	3
DSR	2	4
CTS	1	7