IDSM

この章では、Intrusion Detection System Module（IDSM; 侵入検知システム モジュール）（WS-X6381-IDS）について説明します。

侵入検知システム モジュールは、Cisco Secure Intrusion Detection System（Cisco Secure IDS）の一部であり、Cisco Secure Policy Manager（Cisco Secure PM）によって管理されます（図 9-1 を参照）。Cisco Secure PM は、分散ネットワーク全体のセキュリティを管理するためのグラフィカル インターフェイスを提供します。IDSM は、ネットワーク パケットのリアルタイム モニタリングなどのネットワーク センシングを実行します。これはパケットのキャプチャおよび解析を含みます。

（注） スーパーバイザ エンジンとモジュールの特定の組み合わせは、ご使用のシャーシでサポートされない場合があります。サポートされていないモジュールとスーパーバイザ エンジンに関する具体的な情報については、システムで稼働するソフトウェア バージョンのリリース ノートを参照してください。

IDSM はネットワーク パケットをキャプチャして再構成し、このデータを侵入の代表例を示す一連の基準と照合します。ネットワーク トラフィックは、スイッチ内のセキュリティ VACL に基づいて IDSM にコピーされるか、スイッチの SPAN ポート機能を使用して IDSM に転送されます。どちらの方法でも、スイッチ ポートと VLAN 上の指定したタイプのトラフィック、またはトラフィック タイプの検査が可能です。

IDSM はネットワーク パケットのデータ部分またはヘッダ部分を検査することによって、悪用パターンを探します。コンテンツ ベースの攻撃はデータ部分から仕掛けられ、コンテキスト ベースの攻撃はヘッダ部分から仕掛けられます。

攻撃を検知すると、IDSM はアラームを発行します。IDSM が発行するアラームは、Cisco 7600 シリーズ ルータ バックプレーンを通じて Cisco Secure PM に送られてログが取られ、また GUI（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。アラーム関連の通信は、Cisco Secure IDS 通信サービス プロトコルによって処理されます。これは、IDSM から Cisco Secure PM にアラームを伝送する専用プロトコルです。

前面パネルには、STATUS LED、HD（ハード ドライブ）LED、SHUTDOWN ボタン、および PCMCIA スロットがあります（図 9-1 を参照）。

図 9-1　IDSM（WS-X6381-IDS）

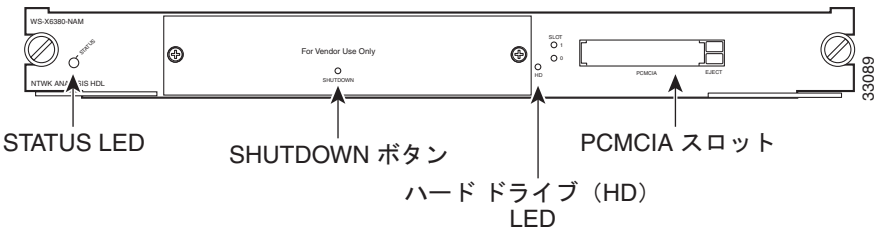

表 9-1 に、STATUS LED が示す IDSM の状態を示します。

表 9-1　IDSM の STATUS LED の説明

色 / 状態	説明
グリーン	すべての診断テストが正常に終了し、モジュールは動作可能。
レッド	各ポートのテストを除く診断テストでエラーが発生
オレンジ	モジュールは起動中でセルフテスト診断シーケンス中
	IDSM はディセーブル状態
消灯	IDSM の電源はオフ

SHUTDOWN ボタンは、IDSM を手動でシャットダウンするために使用します。損傷を防ぐため、適切にモジュールのシャットダウンを行う必要があります。スイッチング モジュールを正しくシャットダウンするには、Cisco 7600 シリーズ ルータのコンソールから IDSM セッションを開き、**shutdown** コマンドを実行します。IDSM が **shutdown** コマンドに応答しない場合は、SHUTDOWN ボタンを押して IDSM を手動でシャットダウンします。

注意　スイッチから IDSM を取り外すには、モジュールが完全にシャットダウンするまで待つ必要があります。シャットダウン手順を経ないで取り外すと、モジュールを損傷することがあります。

SHUTDOWN ボタンを押して IDSM の電源を切るには、ゼムクリップなど、細く尖ったものを使用してください。シャットダウン処理には、数分間かかることがあります。

HD（ハード ドライブ）アクティビティ LED が点灯している場合は、ハード ドライブが使用中です。

PCMCIA スロットには、最大 2 つの標準 PCMCIA カードを搭載できます。これは今後使用できるように装備されています。