IPS 設定を開始する前に

Cisco Intrusion Prevention System（IPS; 侵入防御システム）センサーは、ネットワーク トラフィックの疑わしいアクティビティやアクティブなネットワーク攻撃のリアルタイム モニタリングを実行するネットワーク デバイスです。IPSセンサーは、ネットワーク パケットとフローを分析して、その内容がネットワークに対する攻撃を示しているように見えるかどうかを判断します。

Cisco Security Manager を使用して、センサーを設定および管理できます。センサーには、専用のスタンドアロン ネットワーク アプライアンス、Catalyst 6500 スイッチ モジュール、サポートされる ASA デバイスまたはルータで実行されているサービス モジュール、およびサービス統合型ルータで実行されている IPS 対応 Cisco IOS ソフトウェア イメージがあります。サポートされる IPS デバイスおよびソフトウェア バージョンの完全なリストについては、このバージョンの製品の『Supported Devices and Software Versions for Cisco Security Manager』を参照してください。

この章は次のトピックで構成されています。

IPS ネットワーク検知について

ネットワーク検知は、Cisco IPS センサー（アプライアンス、スイッチモジュール、ネットワーク モジュール、および SSM）と Cisco IOS IPS デバイス（IPS 対応のイメージがある Cisco IOS ルータと Cisco ISR）で実行できます。これらの検知プラットフォームは、Cisco Intrusion Prevention System のコンポーネントであり、Cisco Security Manager を通じて管理および設定できます。これらの検知プラットフォームは、ネットワーク トラフィックをリアルタイムでモニタおよび分析します。これは、ネットワーク フロー検証、広範囲に渡る埋め込み型シグニチャ ライブラリ、および異常検出エンジンに基づいて異常や悪用を探すことで行います。ただし、これらのプラットフォームは検出した侵入への対応方法が異なります。

ヒント Cisco IPS センサーと Cisco IOS IPS デバイスは、IPS デバイスまたは単純にセンサーと総称されることがあります。ただし、Cisco IOS IPS は、完全に専用の IPS ソフトウェアを実行せず、その設定に IPS デバイス固有のポリシーは含まれません。また、Cisco IOS IPS の方が、実行できる検知の量が限られています。次のセクションでは、Cisco IOS IPS ではなく、IOS ルータにインストールされているサービスモジュールを含め、専用の IPS デバイスの使用に焦点を当てます。Cisco IOS IPS に焦点を当てた説明については、Cisco.com の『Intrusion Prevention System (IPS) Cisco IOS Intrusion Prevention System Deployment Guide』および IOS IPS ルータの設定 http://www.cisco.com/go/iosips を参照してください。

IPS デバイスが不正なネットワーク アクティビティを検出した場合、接続の終了、関連するホストの永続的なブロックなどのアクションを実行できます。

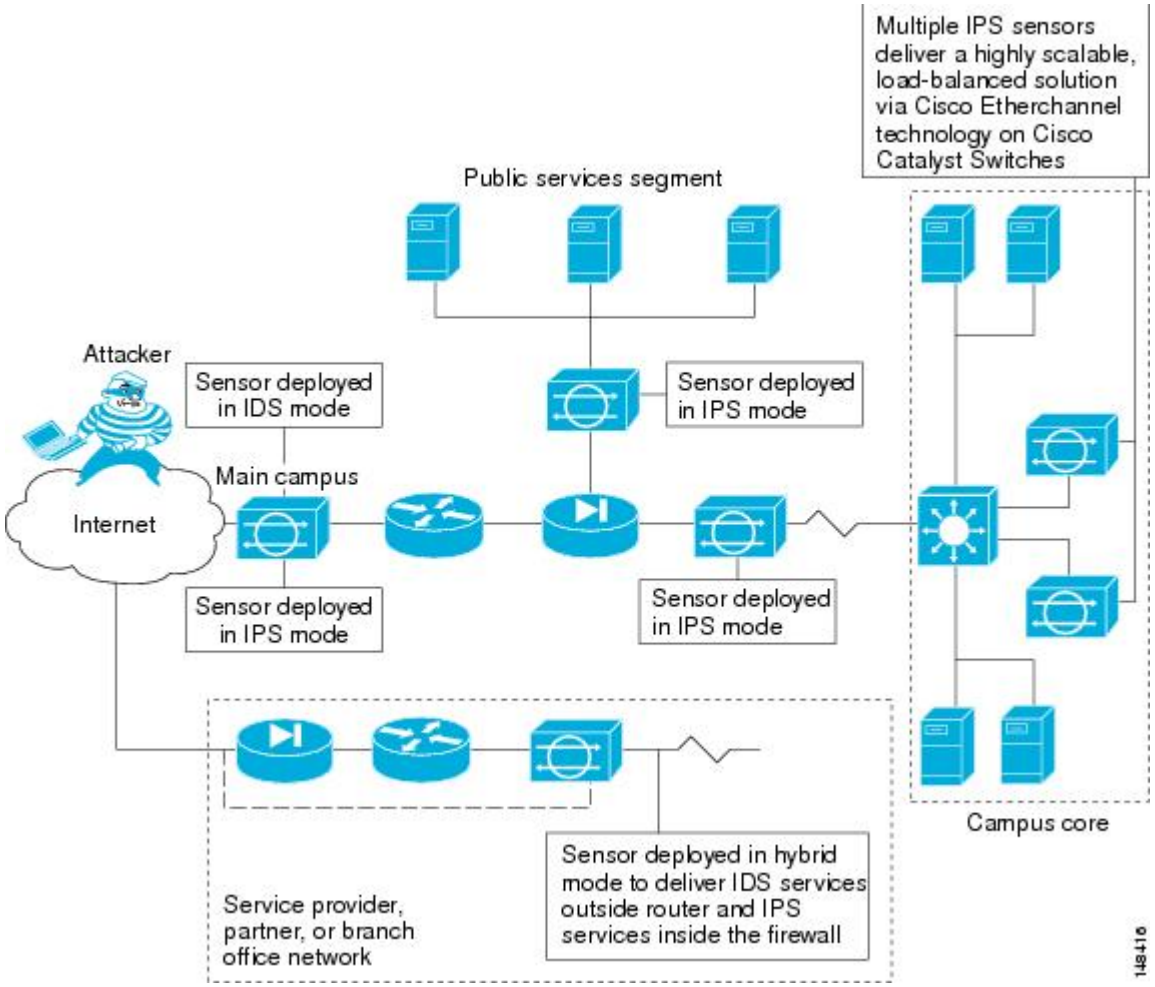
（注） 使用可能なアプライアンスとサービスモジュールの比較、デバイスインターフェイスの詳細など、IPS センサーの概要については、『*Installing Cisco Intrusion Prevention System Appliances and Modules*』の「Introduction the Sensor」を参照してください。各 IPS リリースのこれらのドキュメントのリストは、http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_installation_guides_list.html で入手できます。

ここでは、次の内容について説明します。

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。次の図に、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*：包括的な *IPS* 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。

センサーの適切な展開

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。
- ネットワークと、インターネットなどの他のネットワークとの間の接続。
- ネットワーク上の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。

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、イベント ビューアを使用して 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。

IPS 設定の概要

さまざまなデバイスに侵入防御システムを設定できます。設定の視点から、デバイスは2つのグループに分けられます。1 つは、完全な IPS ソフトウェアを実行する専用アプライアンスおよびサービス モジュール（ルータ、スイッチ、および ASA デバイスの場合）です。もう 1 つは、Cisco IOS ソフトウェア 12.4(11)T 以降（Cisco IOS IPS）を実行する IPS 対応ルータです。

次の手順は、専用アプライアンスおよびサービスモジュールでの IPS 設定の概要です。Cisco IOS IPS デバイス（ルータに設置されている IPS サービス モジュールを含みません）の場合は、Cisco IOS IPS 設定の概要を参照してください。

ステップ 1 デバイスを設置し、ネットワークに接続します。デバイス ソフトウェアをインストールし、基本的なデバイス構成を実行します。デバイス上で実行するすべてのサービスに必要なライセンスをインストールします。最初に実行する設定量は、Security Manager で設定する必要がある内容に影響します。

使用している IPS バージョンの『Installing Cisco Intrusion Prevention System Appliances and Modules』マニュアルの指示に従います。

ステップ 2 デバイスを Security Manager のデバイス インベントリに追加します（デバイス インベントリへのデバイスの追加を参照してください）。

ヒント モジュールが設置されているデバイスを追加するときに、ルータおよび Catalyst スイッチ モジュールを検出できます。ASA デバイスの場合は、サービス モジュールを別途追加する必要があります。

ステップ 3 インターフェイスの設定の説明に従って、インターフェイスを設定します。デバイスが機能するには、ネットワークに接続されているインターフェイスをイネーブルにする必要があります。

特定のタイプのサービス モジュールの場合は、追加のポリシーを設定します。

- ルータにホスティングしているサービスモジュール：ルータに [IPS モジュール（IPS Module）] インターフェイス設定ポリシーを設定します。詳細については、Cisco IOS ルータでの IPS モジュール インターフェイス設定を参照してください。
- IDSM：[IDSM 設定（IDSM Settings）] Catalyst プラットフォームポリシーを設定します。詳細については、IDSM 設定を参照してください。
- ASA デバイスの IPS モジュール：ホスト ASA の [プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）] ポリシーを設定して、検査するトラフィックを指定します。詳細については、ASA デバイスでの IPS モジュールについておよび[サービスポリシールール（Service Policy Rules）] ページを参照してください。

ステップ 4 [仮想センサー（Virtual Sensors）ポリシー] を使用して、インターフェイスを仮想センサーに割り当てます。これには、すべての IPS デバイスに存在する基本 vs0 仮想センサーが含まれます。仮想センサーの設定と仮想センサーへのインターフェイスの割り当てについては、仮想センサーの定義を参照してください。

必要な場合、デバイスがサポートしていれば、ユーザー定義の仮想センサーを作成して、1 つのデバイスに複数のセンサーのように機能させることもできます。ほとんどの IPS 設定は親デバイスで行われますが、シグニチャ、異常検出、イベント アクション用に独自の設定を仮想センサーごとに設定できます。詳細については、仮想センサーの設定を参照してください。

ステップ 5 基本的なデバイス アクセス プラットフォーム ポリシーを設定します。これらのポリシーによって、だれがデバイスにログインできるかが決定されます。

- [AAA]：このポリシーは、RADIUS サーバーを使用してデバイスへのアクセスを制御する場合に設定します。[ユーザーアカウント（User Accounts）] ポリシーで定義されたローカルユーザーアカウントと組み合わせて AAA 制御を使用できます。IPS デバイスの AAA アクセス コントロールの設定（27 ページ）を参照してください。
- [許可ホスト（Allowed Hosts）]：アクセスを許可されているホストのアドレス。許可されたホストとして Security Manager サーバーが含まれていることを確認してください。含まれていないと、Security Manager を使用してデバイスを設定できません。許可ホストの識別 （9 ページ）を参照してください。
- [SNMP]：SNMP アプリケーションを使用してデバイスを管理する場合は、このポリシーを設定します。SNMP の設定 （10 ページ）を参照してください。
- [パスワード要件（Password Requirements）]：ユーザーパスワードの許容される特性を定義できます。ユーザ パスワード要件の設定 （26 ページ）を参照してください。
- [ユーザーアカウント（User Accounts）]：デバイスで定義されているユーザーアカウント。IPS ユーザ アカウントの設定 （23 ページ）を参照してください。

ステップ 6 基本的なサーバ アクセス プラットフォーム ポリシーを設定します。次のポリシーにより、デバイスが接続できるサーバーが識別されます。

- [外部製品インターフェイス（External Product Interface）]：Management Center for Cisco Security Agents を使用する場合は、このポリシーを設定して、センサーがアプリケーションからホストポスチャをダウンロードできるようにします。外部製品インターフェイスの設定 （35 ページ）を参照してください。
- [NTP]：このポリシーは、ネットワーク タイム プロトコル サーバーを使用してデバイス時間を制御する場合に設定します。NTP サーバの識別 （30 ページ）を参照してください。
- [DNS]、[HTTP プロキシ（HTTP Proxy）]：[DNS] ポリシーおよび [HTTP プロキシ（HTTP Proxy）] ポリシーは、グローバル相関を設定する場合にのみ必要です。これらは、DNS 名を IP アドレスに解決できるサーバを特定します。ネットワークでプロキシを使用してインターネットに接続する必要がある場合は、[HTTP プロキシ（HTTP Proxy）] ポリシーを使用します。それ以外の場合は、[DNS] ポリシーを使用します。DNS サーバの識別 （31 ページ）または HTTP プロキシ サーバの識別（32 ページ）を参照してください。

ステップ 7 デフォルト以外のロギングが必要な場合は、[Logging] ポリシーを設定します。IPS ロギング ポリシーの設定 （39 ページ）を参照してください。

ステップ 8 IPS シグニチャおよびイベント アクションを設定します。イベント アクション ポリシーの設定は、カスタムのシグニチャの作成よりも簡単であるため、特定のシグニチャを編集する前に、イベント アクション フィルタを使用して、シグニチャの動作を変更するように上書きしてみてください。詳細は、次のトピックを参照してください。

- イベント アクション ルールの設定
- シグニチャの設定

ステップ 9 [Request Block] または [Request Rate Limit] イベント アクションのいずれかを使用する場合は、ブロッキングまたはレート制限ホストを設定します。IPS のブロッキングおよびレート制限の設定を参照してください。

ステップ 10 その他の必要な、高度な IPS サービスを設定します。次のトピックを参照してください。

- グローバル相関の設定
- 異常検出の設定

ステップ 11 デバイスを次のように保守します。

- 必要に応じて、設定を更新および再配布します。
- 更新したシグニチャおよびエンジン パッケージを適用します。更新の確認、更新の適用、および定期的な自動更新の設定については、IPS 更新の管理を参照してください。
- デバイス ライセンスを管理します。ライセンスを更新して再配布することも、ライセンスの更新を自動化することもできます。詳細は、次のトピックを参照してください。
  - IPS ライセンス ファイルの更新
  - IPS ライセンス ファイルの再展開
  - IPS ライセンス ファイル更新の自動化
- SSL（HTTPS）通信に必要な証明書を管理します。これらの証明書は有効期限があるため、約 2 年ごとに再生成する必要があります。証明書の再生成方法、およびデバイスで定義されている証明書を Security Manager の証明書ストアに保存されている証明書と同期させる方法については、IPS 証明書の管理を参照してください。

ステップ 12 デバイスを監視します。

- デバイスから生成されたアラートを表示するには、イベント ビューア アプリケーションを使用します。イベントビューアーは、Configuration Manager または Report Manager の [起動（Launch）] メニューか、Windows の [スタート（Start）] メニューから開くことができます。
  - Event Viewer の使用については、イベントの表示を参照してください。
  - IPS アラートをフィルタ処理する方法の例については、イベント テーブルからの false positive IPS イベントの削除を参照してください。

- Report Manager アプリケーションを使用して、IPS の使用に関するレポートを生成します。このレポートには、インラインモードと無差別モード、およびグローバル相関と従来のインスペクションが含まれます。上位攻撃者、攻撃対象、署名、ブロックされた署名を分析し、ターゲット分析を実行することもできます。次のトピックで、Report Manager および IPS レポートの詳細について説明します。
  - レポートの管理
  - 全般 IPS レポートについて
  - IPS 上位レポートについて
  - レポートの起動と生成

許可ホストの識別

[Allowed Hosts] ポリシーを使用して、IPS センサーにアクセスできるホストまたはネットワークを識別します。デフォルトでは、どのホストもセンサーへのアクセスを許可されないため、このポリシーにホストまたはネットワークを追加する必要があります。

具体的には、Security Manager サーバの IP アドレスまたはそのネットワーク アドレスを追加します。そうしないと、Security Manager はデバイスを設定できません。また、CS-MARS など、使用するその他すべての管理ホストのアドレスを追加します。

ヒント ホストアドレスだけを追加した場合、デバイスへのアクセスにはそれらのワークステーションだけを使用できます。あるいは、ネットワークアドレスを指定して、特定の「安全な」ネットワークアクセスに接続されているすべてのホストを許可することもできます。

ステップ 1 次のいずれかを実行して、[許可されたホスト（Allowed Hosts）] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [許可されたホスト（Allowed Hosts）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [許可されたホスト（Allowed Hosts）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次のいずれかを実行します。

- エントリを追加するには、[行の追加（Add Row] ボタンをクリックし、[アクセスリスト（Access List）] ダイアログボックスに入力します。

最大 512 のエントリを追加できます。

- エントリを編集するには、エントリを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- エントリを削除するには、エントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 3 エントリを追加または編集する場合は、[アクセスリストの追加または変更（Add or Modify Access List）] ダイアログボックスでホストまたはネットワークアドレスを指定してから、[OK] をクリックします。次の形式を使用して、アドレスを入力できます。

- ホストアドレス：10.100.10.10 などの単純な IP アドレス。
- ネットワーク アドレス：10.100.10.0/24 や 10.100.10.0/255.255.255.0 などのネットワーク アドレスおよびマスク。
- ネットワーク/ホストポリシーオブジェクト：[選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。このポリシーでオブジェクトを使用するには、値が単一の値（単一のネットワークまたは単一のホスト）になっている必要があります。

SNMP の設定

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。SNMP を使用すると、ネットワーク管理者は、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡大に対する計画を策定できます。

SNMP は、単純な要求/応答プロトコルです。ネットワーク管理システムが要求を発行し、管理対象デバイスが応答を返します。この動作は、Get、GetNext、Set、および Trap の 4 つのプロトコル操作のいずれかを使用することによって実装されます。

SNMP によるモニタリングのためにセンサーを設定することができます。SNMP は、ネットワーク管理ステーションがスイッチ、ルータ、センサーなどの多くのタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。

SNMP トラップを送信するようにセンサーを設定できます。SNMP トラップを使用すると、エージェントは非送信請求 SNMP メッセージを使用して管理ステーションに重要なイベントを通知できます。

トラップで指示される通知には次の利点があります。マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。ソリューションは、送信要求を行わずに、管理対象デバイス上のエージェントごとにマネージャに通知することです。イベントのトラップと呼ばれるメッセージを送信することで、この処理を行います。

イベントの受信後、マネージャはイベントを表示し、イベントに基づいてアクションを実行できます。たとえば、マネージャは、エージェントを直接ポーリングするか、他の関連デバイス エージェントをポーリングしてイベントの詳細情報を取得できます。

ヒント　トラップで指示された通知は、重要でないSNMP要求を排除することによって、ネットワークおよびエージェントのリソースを実質的に節約できます。ただし、SNMPポーリングを完全には排除できません。SNMP要求は、検出とトポロジ変更に必要です。また、管理対象デバイスエージェントは、デバイスに致命的な停止が生じた場合にはトラップを送信できません。

この手順では、トラップの設定など、SNMP管理ステーションでセンサーを管理できるようにIPS センサーで SNMP を設定する方法を説明します。

ステップ 1　次のいずれかを実行して、[SNMP] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2　[一般設定（General Configuration）] タブで、少なくとも次のオプションを設定します。使用可能なすべてのオプションの詳細な説明については、汎用 SNMP 設定オプション　（13 ページ）を参照してください。

- [SNMP Gets/Setsの有効化（Enable SNMP Gets/Sets）]：このオプションを選択して、SNMP 管理ワークステーションが情報を取得（get）したり、IPSセンサーの値を修正（set）したりできるようにします。このオプションをイネーブルにしない場合、管理ワークステーションはこのセンサーを管理できません。
- [読み取り専用コミュニティストリング（Read-Only Community String）]：センサーへの読み取り専用アクセスに必要なコミュニティストリング。管理ステーションからの SNMP get 要求は、センサーからの get 応答に対してこのストリングを提供する必要があります。このストリングによって、すべての SNMP get 要求にアクセスできます。
- [読み取り/書き込みコミュニティストリング（Read-Write Community String）]：センサーへの読み取り/書き込みアクセスに必要なコミュニティストリング。管理ステーションからのSNMP set要求は、センサーからの get 応答に対してこのストリングを提供する必要があります。また、get 要求で使用されることもあります。このストリングによって、すべての SNMP get 要求と set 要求にアクセスできます。

ステップ 3　[SNMPv3 ユーザー（SNMPv3 Users）] タブで、1 人以上の SNMPv3 ユーザを追加して、管理対象 IPS デバイスで SNMPv3 設定を構成します。バージョン 4.6 以降、Security Manager では、管理する IPS デバイスで SNMPv3 設定を構成できます。詳細については、SNMPv3 ユーザータブ　（14 ページ）を参照してください。

（注） SNMPv3 は IPS バージョン 7.2.2 以降でサポートされていますが、IPS バージョン 7.3.1 ではサポートされていません。ただし、Security Manager は IPS 7.3.1 デバイスを管理できます。Cisco Security Manager を使用して、SNMP ポリシーが設定されているバージョン 7.2.2 からバージョン 7.3.1 に IPS デバイスをアップグレードしようとすると、マウスオーバーのツールチップに「選択されたアップグレードは推奨されません。デバイスの SNMP ポリシーの割り当てを解除して展開し、7.3.1 へのアップグレードを続行します」と表示されます。バージョン 7.2.2 以降の IPS デバイスでの SNMPv3 ポリシーの管理については、Cisco Intrusion Prevention System 7.2(2) のリリースノートを参照してください。

ステップ 4 SNMP トラップを設定する場合は、[SNMPトラップ設定（SNMP Trap Configuration）] タブをクリックして、少なくとも次のオプションを設定します。使用可能なすべてのオプションの詳細な説明については、[SNMP Trap Configuration] タブ （16 ページ）を参照してください。

- [通知の有効化（Enable Notifications）]：センサーが SNMP トラップを送信できるようにするには、このオプションを選択します。
- [トラップ宛先（Trap Destinations）]：トラップの宛先となる SNMP 管理ステーションを追加します。[行の追加（+）（Add Row（+））]ボタンをクリックして新しい宛先を追加するか、宛先を選択して、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックして設定を変更します。

トラップ宛先を追加または編集する場合、入力したトラップ コミュニティ ストリングは、[SNMPトラップ設定（SNMP Trap Configuration）] タブで入力したデフォルトのコミュニティ ストリングよりも優先されます。コミュニティストリングがこの宛先に送信されたトラップに表示されます。これは、複数のエージェントから複数のタイプのトラップを受信する場合に役立ちます。たとえば、ルータまたはセンサーがトラップを送信する場合に、具体的にルータまたはセンサーを識別する何かをコミュニティ ストリングに入力すると、コミュニティ ストリングに基づいてトラップをフィルタリングすることができます。

宛先を削除するには、宛先を選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。

ステップ 5 トラップの宛先を設定する場合は、[SNMPトラップの要求（Request SNMP Trap）] アクションに必要なアラートを含める必要もあります。このアクションの追加には、次のオプションがあります。

- ((簡単な方法。）イベント アクション オーバーライドを作成して、指定したリスクレーティングのすべてのアラートに [SNMPトラップの要求（Request SNMP Trap）] アクションを追加します（[IPS] > [イベントアクション（Event Actions）]>[イベントアクションオーバーライド（Event Action Overrides）] ポリシー）。たとえば、リスクレーティングが 85 ～ 100 のすべてのアラートに対してトラップを生成できます。イベントアクション オーバーライドを使用すると、各シグニチャを個別に編集することなくアクションを追加できます。詳細については、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。
- （正確な方法。）シグニチャポリシーを編集して（[IPS] > [シグニチャ（Signatures）> [シグニチャ（Signatures）]）、トラップ通知を送信するシグニチャに [SNMPトラップの要求（Request SNMP Trap）] アクションを追加します。トラップは、トラップを送信するように設定したシグニチャだけに送信されます。

（注） シグニチャの送信元がデフォルトの場合は、アクションを変更する前に送信元をローカル送信元に変更する必要があります。ただし、シグニチャテーブルの [アクション（Action）] セルを右クリックして [アクションの編集（Edit Actions）] を選択し、[SNMP トラップの要求（Request SNMP Trap）]（およびその他の必要なアクション）を選択して [OK] をクリックすると、ソースは自動的にローカルに変更されます。

ステップ 6 SNMP 管理ステーションを [Allowed Hosts] ポリシーに追加します。管理ステーションは、センサーへのアクセスを許可されているホストである必要があります。許可ホストの識別 （9 ページ） を参照してください。

汎用 SNMP 設定オプション

[SNMP] ページの [一般設定（General Configuration）] タブを使用して、一般的な SNMP パラメータを設定して、IPS センサーに適用します。手順については、SNMP の設定 （10 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[General Configuration] タブを選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。[General Configuration] タブを選択します。

フィールド リファレンス

表 1 : [General Configuration] タブ、IPS センサーの [SNMP] ポリシー

要素	説明
Enable SNMP Gets/Sets	SNMP 管理ワークステーションで、IPS センサー上の情報の取得および値の修正（設定）をイネーブルにするかどうか。このオプションをイネーブルにしていない場合、管理ワークステーションはこのセンサーを管理できません。センサーは SNMP 要求に応答しません。
Read-Only Community String	センサーへの読み取り専用アクセスに必要なコミュニティ ストリング。管理ステーションからの SNMP get 要求は、センサーからの get 応答に対してこのストリングを提供する必要があります。このストリングによって、すべての SNMP get 要求にアクセスできます。このストリングを使用すると、センサーの識別に役立ちます。

要素	説明
Read-Write Community String	センサーへの読み取り/書き込みアクセスに必要なコミュニティストリング。管理ステーションからの SNMP set 要求は、センサーからの get応答に対してこのストリングを提供する必要があります。また、get要求で使用されることもあります。このストリングによって、すべての SNMP get 要求と set 要求にアクセスできます。このストリングを使用すると、センサーの識別に役立ちます。
Sensor Contact	このセンサーに責任を持つネットワーク管理者または担当者。
センサーの位置（Sensor Location）	建物の住所、名前、部屋番号など、センサーの物理的な場所。
Sensor Agent Port	センサーとの SNMP get/set 通信に使用するポート。デフォルトは 161 です。有効な範囲は 1 ～ 65535 です。 ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてリストからポートリストオブジェクトを選択するか、または新しいオブジェクトを作成します。ポート リスト オブジェクトでは、単一ポートが識別されます。
SNMPエージェントプロトコル（SNMP Agent Protocol）	SNMP に使用しているプロトコル（UDP（デフォルト）または TCP）。SNMP 管理ステーションで使用されるプロトコルを選択します。

SNMPv3 ユーザータブ

バージョン 4.6 以降、Security Manager では、管理する IPS デバイスで SNMPv3 設定を構成できます。SNMPv3 ユーザーを追加して、管理対象 IPS デバイスで SNMPv3 設定を指定する必要があります。

[SNMP] ページの [SNMPv3 ユーザー（SNMPv3 Users）] タブを使用して、SNMPv3 ユーザーを表示、追加、編集、または削除できます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMPv3 ユーザー（SNMPv3 Users）] タブを選択します。
- （ポリシービュー）**[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [SNMP]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[SNMPv3 ユーザー（SNMPv3 Users）] タブを選択します。

次のいずれかを実行します。

- SNMPv3 ユーザーを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [SNMPv3 ユーザーの追加（Add SNMPv3 User）] ダイアログボックスが開きます。ユーザーを作成するために必要な情報を入力します。設定の詳細については、[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックス （15 ページ）を参照してください。
- SNMPv3 ユーザーを編集するには、そのユーザーを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックして、[SNMPv3 ユーザーの編集（Edit SNMPv3 User）] ダイアログボックスに必要な変更を加えます。
- 既存の SNMPv3 ユーザーを削除するには、ユーザーを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

フィールド リファレンス

表 *2 : SNMPv3* ユーザー

要素	説明
User Name	SNMP エージェントに属するホスト上のユーザーの名前。
アクセス制御	SNMPv3 ユーザーのアクセス権限。
セキュリティ レベル（Security Level）	SNMPv3 ユーザーのセキュリティレベル。
認証プロトコル（Authentication Protocol）	認証プロトコルキーワードは、SNMPv3ユーザーの設定に使用される認証レベルです。
プライバシー プロトコル（Privacy Protocol）	プライバシー プロトコル キーワードは、SNMPv3 ユーザーの設定に使用されるプライバシーまたは暗号化アルゴリズムです。

[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックス

[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックスを使用して、管理対象 IPS デバイスの新しい SNMPv3 ユーザーを設定します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMPv3ユーザー（SNMPv3 Users ）] タブを選択し、[行の追加（Add Row ）]（+）ボタンをクリックします。
- （ポリシービュー）**[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [SNMP]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作

成します。[SNMPv3ユーザー（SNMPv3 Users）] タブを選択し、[行の追加（Add Row）]（+）ボタンをクリックします。

フィールド リファレンス

表 *3 : [SNMPv3*ユーザーの追加（*Add SNMPv3 Users*）*]* ダイアログボックス

要素	説明
User Name	新しい SNMPv3 ユーザーの名前を入力します。
アクセス制御	新しい SNMPv3 ユーザーのアクセス権限を選択します。
セキュリティ レベル（Security Level）	SNMPv3 ユーザーに対して、次のいずれかのセキュリティレベルを選択します。 • **NoAuthNoPriv**：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。 • **AuthNoPriv**：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。 • **AuthPriv**：認証とプライバシーが設定されます。メッセージが認証および暗号化されることを意味します。
認証プロトコル（Authentication Protocol）	使用される認証レベルを指定する認証プロトコルキーワードを選択します。デフォルト値はありません。
プライバシー プロトコル（Privacy Protocol）	使用するプライバシーまたは暗号化アルゴリズムを指定するプライバシー プロトコル キーワードを選択します。暗号化アルゴリズムには、AES キーワードを指定できます。デフォルト値はありません。
認証パスフレーズ（Authentication Passphrase）	認証ユーザーパスワードを指定する認証パスフレーズ引数を入力します。このパスワードは 8 文字以上にする必要があります。デフォルト値はありません。
プライバシーパスフレーズ（Privacy Passphrase）	暗号化ユーザーパスワードを指定するプライバシーパスフレーズ引数を入力します。このパスワードは 8 文字以上にする必要があります。デフォルト値はありません。

[SNMP Trap Configuration] タブ

[SNMP] ページの [SNMP トラップ通信（SNMP Trap Communication）] タブを使用して、トラップを設定してセンサーに適用し、トラップの送信先の受信者を指定します。手順については、SNMP の設定 （10 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMP Trap Configuration] タブを選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。[SNMP Trap Configuration] タブを選択します。

フィールド リファレンス

表 *4 : [SNMP*トラップ設定（*SNMP Trap Configuration***）*]* タブ、*IPS* センサーの *[SNMP]* ポリシー**

要素	説明
通知の有効化（Enable Notifications）	センサーで特定のタイプのイベントが発生したときに、センサーがトラップ通知をトラップの宛先に送信することをイネーブルにするかどうか。このオプションを選択しない場合、センサーはトラップを送信しません。 **ヒント** センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベントアクションとして [SNMPトラップを要求（Request SNMP Trap）] も選択する必要があります。トラップは、トラップを送信するように設定したシグニチャだけに送信されます。
Error Filter	イベントの重大度（重大、エラー、または警告）に基づいてSNMPトラップを生成するイベントのタイプ。必要な重大度をすべて選択します。複数の値を選択するには、Ctrl キーを押しながらクリックします。 センサーは、選択された重大度のイベント通知だけを送信します。
Enable Detail Traps	トラップにアラートのテキスト全体を含めるかどうか。このオプションを選択しない場合、スパースモードが使用されます。スパースモードでは、484 バイト未満のアラートのテキストが含まれます。
Default Trap Community String	[トラップ宛先（Trap Destinations）] テーブルでトラップの宛先に特定の文字列が設定されていない場合に、トラップに使用されるコミュニティ文字列。 **ヒント** すべてのトラップがコミュニティ ストリングを伝送します。デフォルトでは、宛先と同じコミュニティ ストリングを持つすべてのトラップが宛先で取得されます。その他すべてのトラップは、宛先によって廃棄されます。ただし、受け入れるトラップ文字列を判断するように宛先を設定できます。

要素	説明
[Trap Destinations] テーブル	トラップ通知を送信する SNMP 管理ステーション。テーブルには、管理ステーションの IP アドレス、このセンサーからトラップに追加されるコミュニティ ストリング、およびトラップの送信先のポートが表示されます。 • 宛先を追加するには、[行の追加（Add Row）] ボタンをクリックし、[SNMP トラップ通信の追加（Add SNMP Trap Communication）] ダイアログボックスに入力します（ [Add SNMP Trap Communication]/[Modify SNMP Trap Communication] ダイアログボックス （18 ページ）を参照）。 • 宛先を編集するには、その宛先を選択して [行の編集（Edit Row）] ボタンをクリックし、変更を行います。 • 宛先を削除するには、その宛先を選択して [行の削除（Delete Row）] ボタンをクリックします。

[Add SNMP Trap Communication]/[Modify SNMP Trap Communication] ダイアログボックス

[SNMP トラップ通信の追加または変更（Add or Modify SNMP Trap Communication）] ダイアログボックスを使用して、SNMP トラップの宛先を設定します。宛先は、IPS センサーからトラップを受信する必要がある SNMP 管理ステーションです。

ナビゲーション パス

IPS の [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] ポリシーに移動し、[SNMP トラップ設定（SNMP Trap Configuration）] タブを選択して [トラップの宛先（Trap Destinations）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、テーブルで宛先を選択して [行の編集（Edit Row）] ボタンをクリックします。詳細については、 [SNMP Trap Configuration] タブ （16 ページ）を参照してください。

フィールド リファレンス

表 5 : [Add SNMP Trap Communication]/[Modify SNMP Trap Communication] ダイアログボックス

要素	説明
IPアドレス	トラップ通知を受信する SNMP 管理ステーションの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。ネットワーク/ホスト オブジェクトでは、単一のホスト IP アドレスを指定する必要があります。
Trap Community String	トラップのコミュニティ ストリング。トラップ文字列を入力しない場合は、[SNMP Trap Communication] タブで定義されたデフォルトのトラップ文字列が、この宛先に送信されるトラップに使用されます。

要素	説明
トラップ ポート（Trap Port）	SNMP管理ステーションがトラップの受信に使用するポート。ポート リスト オブジェクトのポート番号または名前を入力するか、[Select] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。ポート リスト オブジェクトでは、単一ポートが識別されます。
SNMPv3ユーザー（SNMPv3 User）	[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックス（15 ページ）を使用して設定した SNMPv3 ユーザーのユーザー名を入力します。SNMPv3 ユーザーを関連付けない場合は、このフィールドを空白のままにします。 （注） 設定済みの SNMPv3 ユーザーではないユーザー名を入力すると、SNMP トラップ通信の設定の保存中にエラーメッセージが表示されます。また、最大 23 人の SNMPv3 ユーザーを追加できます。

ユーザ アカウントとパスワードの要件の管理

IPS デバイスに対して、ユーザ アカウントとパスワード、および一般的なパスワード要件を設定できます。ローカル ユーザ（デバイスで直接定義）を設定するか、RADIUS AAA サーバを使用するか、この両方を組み合わせることができます。使用されるポリシーは、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）] フォルダにある [AAA] ポリシー、[ユーザーアカウント（User Accounts）] ポリシー、および [パスワード要件（Password Requirements）] ポリシーです。

Security Manager でローカル ユーザ アカウントを作成または編集する場合は、入力するパスワードが、[Password Requirements] ポリシーで定義した要件を満たしている必要があります。これにより、新しいパスワードがセキュリティ要件を満たすことが保証されます。

ヒント パスワード要件を変更し、いずれかのローカル ユーザ アカウントに変更を加えた場合は、Security Manager によって管理されているパスワードを持つすべてのユーザ アカウントで新しい要件が満たされる必要があります。その理由は、いずれか1つのアカウントを再設定する必要がある場合に、Security Manager によってすべての管理対象アカウントのパスワードが再設定されるためです。

[User Accounts] ポリシーを使用して、IPS デバイスのローカル ユーザ アカウントを集中管理できます。共有ポリシーを使用すると、すべての IPS デバイスに同じパスワードを持つ同じアカウントが含まれる状態を確保するために役立ちます。ただし、パスワードは暗号化されているため、Security Manager はデバイスに定義されている実際のパスワードを検出できません。Security Manager でパスワードを定義する場合にだけ、Security Manager によってアカウントのパスワードが管理されます。Security Manager では、RADIUS AAA サーバで定義されたユーザ アカウントは管理しません。

ここでは、IPS ユーザ アカウント、および Security Manager の検出と展開の考慮事項について詳細に説明します。

IPS ユーザーロールについて

IPS ユーザ アカウントには 4 つのユーザ ロールがあります。

- **ビューア（Viewer）**：ユーザは、デバイス設定とイベントを表示できますが、自身のユーザパスワード以外の設定データは修正できません。
- **オペレータ（Operator）**：ユーザはすべてのデータを表示できるほか、次のオプションを修正できます。
  - シグニチャチューニング（優先順位、無効/有効）
  - 仮想センサーの定義
  - 管理対象ルータ。
  - ユーザ パスワード。
- **管理者（Administrator）**：ユーザはすべてのデータを表示できるほか、オペレータが修正できるすべてのオプションに加えて、次のオプションを修正できます。
  - センサー アドレッシング設定。
  - 設定エージェントまたはビュー エージェントとして接続が許可されたホストのリスト。
  - 物理的な検知インターフェイスの割り当て。
  - 物理インターフェイスの制御のイネーブル化またはディセーブル化。
  - ユーザとパスワードの追加および削除。
  - 新しい SSH ホスト キーおよびサーバ証明書の生成。
- **サービス（Service）**：サービス権限を持つユーザはセンサーに 1 人だけ存在できます。サービス ユーザは、IDM または IME にログインできません。サービス ユーザは、CLI ではなく bash シェルにログインします。サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。

（注） Service アカウントの目的は、通常は発生しない問題を Cisco テクニカル サポートがトラブルシューティングできるようにすることにあります。通常のシステム設定およびトラブルシューティングには必要ありません。サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

管理対象と管理対象外の IPS パスワードについて

各 IPS ローカル ユーザ アカウントには、デバイスへのセキュアなユーザ ログインを可能にするパスワードがあります。これらのユーザ パスワードは、IPS デバイスで暗号化されます。このため、IPS デバイスを Security Manager インベントリに追加すると、Security Manager は実際のユーザ パスワードを読み取れません。

Security Manager はパスワードを読み取れないため、新規に検出されたユーザ アカウントのパスワードをデバイスに展開できません。ユーザアカウントのパスワードが不明で使用不可の状態にならないように、Security Manager は検出されたユーザアカウントのパスワードに**管理対象外**というマークを付けます。パスワードのステータスは、[プラットフォーム（Platform）]> [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ユーザアカウント（User Accounts）] ポリシーの [管理対象のパスワード？（Is Password Managed?）] カラムに表示されます。

- [いいえ（No）] と表示されている場合、このアカウントのパスワードは Security Manager で設定されません。このポリシーを展開する場合、Security Manager はこのユーザ アカウントのパスワードの設定を試みません。
- [はい（Yes）] と表示されている場合、このアカウントのパスワードは Security Manager で設定または更新されています。このポリシーを展開する場合、Security Manager は、最後の展開後に変更されたパスワードだけでなく、すべての管理対象アカウントのパスワードを再設定します。

Security Manager は変更されていないパスワードも設定するため、すべての管理対象パスワードは [Password Requirements] ポリシーで定義されているパスワード要件を満たす必要があります。

このため、管理対象と管理対象外のアカウント パスワードを混在させることができます。たとえば、集中管理されている共有ユーザ アカウントのセットを使用し、これらのアカウントのパスワードを Security Manager で管理できます。他のアカウントは、個人ごとに固有にすることができます。これらのアカウントのパスワードを Security Manager で編集しない場合は、ユーザがデバイス上でパスワードを個別に管理できます。

ヒント　ユーザアカウントを Security Manager で管理しない場合は、[ユーザアカウントポリシー（User Accounts policy）] が空であることを確認するか、ポリシーの割り当てを解除します（ポリシーを右クリックし、[ポリシーの割り当て解除（Unassign Policy）] を選択します）。Security Manager は、ユーザアカウント設定を変更しません。

IPS パスワードの検出および展開方法について

ユーザ パスワードは IPS デバイスで暗号化されるため、Security Manager は、デバイスでポリシーを検出または設定を展開するときに、特に注意してこれらのパスワードを処理する必要があります。IPS デバイスでユーザ アカウントを検出または展開する場合、Security Manager は次の処理を行います。

- [検出（Discovery）] : IPS デバイスをインベントリに追加するとき、またはポリシーを再検出するとき、Security Manager は各ユーザーアカウントの現在のステータスを判断し、検出されたユーザー名とそれに関連付けられているロールでユーザーアカウントポリシーを更新し、ユーザーパスワードを管理対象外としてマークします（管理対象と管理対象外の IPS パスワードについて （21 ページ）を参照）。

アカウントステータスは動的で変化する可能性があるため、Security Manager を介して表示することはできません。ただし、[Discovery Status] ウィンドウに、検出時のステータスが表示されます。アカウントには次のステータスがあります。

- [アクティブ（Active）] : この状態は、アカウントが使用可能なことを示します。アクティブアカウントには、そのアカウントに割り当てられているユーザが認証トークンを使用してアクセスできます。
- [期限切れ（Expired）] : この状態は、アカウントの認証トークンが期限切れになっており、トークンが更新されるまで、トークンを使用してアカウントにアクセスできないことを示します。
- [ロック（Locked）] : この状態は、認証試行の失敗回数が多過ぎたために、このアカウントへのログインが無効になったことを示します。これらのアカウントのパスワードを更新する必要があります。

[展開（Deployment）] : ユーザーアカウントが [期限切れ（Expired）] または [ロック（Locked）] 状態にある場合に警告が表示されます。管理対象外のパスワードは、デバイスに展開されません。また、次の点に注意してください。

- デバイス上のいずれかのユーザアカウントに変更を加える場合は、管理対象パスワードを持つすべてのユーザ アカウントが再設定されます。[Password Requirements] ポリシーも変更した場合は、すべてのパスワードが新しいポリシーと比較され、新しい要件を満たす必要があります。
- デバイスの設定時に Security Manager が使用するようにデバイスのプロパティで定義されているユーザーアカウントのパスワードを変更した場合は、正常な展開後に、Security Manager がデバイスのプロパティのパスワードを新しいパスワードに更新します。パス

ワードを手動で更新する必要はありません。デバイスのプロパティを表示するには、[ツール（Tools）] > [デバイスプロパティ（Device Properties）] を選択します。

この動作は、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバイス通信（Device Communication）] ページの [デバイスへの接続方法（Connect to Device Using）] オプションに対して [Security Managerデバイスのクレデンシャル（Security Manager Device Credentials）] を選択したことを想定しています。ログインしているユーザのクレデンシャルを展開に使用している場合は、正常な展開後に、展開全体が失敗としてマークされ、接続の再確立方法がメッセージで説明されます。[Device Communication] ページを参照してください。

- アウトオブバンド変更検出を使用する場合は、パスワードに対する変更が検出されません。ただし、ユーザ名とロールに対する変更は検出されます。アウトオブバンド変更検出の詳細については、アウトオブバンド変更の検出および分析を参照してください。
- 設定をプレビューする場合、IPS（[Delta] > [User Passwords]）を選択してユーザ アカウントに対する変更を表示できます。ただし、パスワードはマスクされています。詳細については、設定のプレビューを参照してください。
- 設定をロールバックする場合、ユーザ アカウントはロールバックされません。ユーザ アカウントの現在のステータスと設定は変更されません。

ヒント IPS センサーは、SSH クライアントを介してデバイスにログインするときに、RSA 認証の公開キーを受け入れることができます。各ユーザには、認可されたキーのリストが関連付けられています。ユーザは、パスワードの代わりにこれらのキーを使用できます。Security Manager は、検出および展開時にこれらのキーを無視します。このため、キーが設定されている場合、Security Manager は設定を削除しません。

関連項目

- ポリシーの検出
- Workflow 以外のモードでの設定の展開
- Workflow モードでの設定の展開
- 設定のロールバックについて
- IPS および IOS IPS のロールバックについて

IPS ユーザ アカウントの設定

[User Accounts] ポリシーを使用して、IPS デバイスのローカル ユーザ アカウントを設定します。ユーザは、これらのアカウントを使用してデバイスにログインできます。新規ユーザの作成、ユーザ権限とパスワードの修正、およびユーザの削除を行うことができます。

ユーザ アカウント ポリシーには少なくとも次のアカウントが必要です。

- cisco：「cisco」という名前のアカウントがデバイスに存在する必要があり、削除できません。
- Security Manager が使用できる管理者アカウント：Security Manager が、設定するデバイスにログインできる必要があります。通常は、この目的のアカウントを作成します。ただし、Security Manager がデバイスにログインするために、設定を展開するユーザのユーザ アカウントを使用することもできます。この設定は、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [デバイス通信（Device Communication）] ページの [デバイスの接続に使用（Connect to Device Using）] オプションを使用して行うことができます。[Device Communication] ページを参照してください。

IPS ユーザ アカウントの設定は、見た目よりも複雑です。IPS ユーザ アカウントを設定する前に、次の項を参照してください。

- ユーザ アカウントとパスワードの要件の管理 （19 ページ）
- IPS ユーザーロールについて （20 ページ）
- 管理対象と管理対象外の IPS パスワードについて （21 ページ）
- IPS パスワードの検出および展開方法について （22 ページ）
- ユーザ パスワード要件の設定 （26 ページ）
- IPS デバイスの AAA アクセス コントロールの設定 （27 ページ）

ヒント

- Cisco IOS IPS デバイスでは、ルータに定義されているのと同じユーザ アカウントを使用します。この手順は、Cisco IOS IPS 設定には適用されません。
- デバイス プロパティで定義されたユーザのパスワード（Security Manager でデバイスに設定を展開するために使用）を変更する場合、Security Manager は、デバイス プロパティに定義された既存のクレデンシャルを使用してデバイスにログインし、変更を展開します。展開に成功したら、デバイス プロパティは、新しい設定を使用するように変更されます。デバイス プロパティのクレデンシャルの詳細については、[Device Credentials] ページを参照してください。

関連項目

- テーブルのフィルタリング
- テーブル カラムおよびカラム見出しの機能

ステップ 1 次のいずれかを実行して、[User Accounts] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ユーザーアカウント（User Accounts）] を選択します。

- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ユーザーアカウント（User Accounts）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ポリシーには、ユーザ名、ロール、（管理対象と管理対象外の IPS パスワードについて （21 ページ）で説明したように）パスワードが Security Manager で管理されるかどうかなど、既存のユーザ アカウントが表示されます。

ステップ 2 次のいずれかを実行します。

- ユーザーアカウントを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [Add User] ダイアログボックスが開きます。アカウントの定義に必要な情報を入力します。設定の詳細については、ユーザの追加またはユーザログイン情報の編集ダイアログボックス （25 ページ）を参照してください。
- ユーザーアカウントを編集するには、そのアカウントを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックして、[ユーザーの編集（Edit User）] ダイアログボックスに必要な変更を加えます。

ユーザ ロールをサービス ロールに、またはサービス ロールをユーザ ロールには変更できません。

- ユーザーアカウントを削除するには、そのアカウントを選択して [行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。cisco という名前のアカウントは削除できません。

ヒント すべてのパスワード変更は、[Password Requirements] ポリシーの要件を満たしている必要があります。要件ポリシーを変更した場合、すべての新規ユーザ アカウント、または編集したアカウントが、新規要件に対してテストされます。既存の編集していないユーザ アカウントのパスワードはテストされませんが、Security Manager は次の設定展開時にすべてのアカウントを展開するため、このポリシーで定義したユーザアカウントを変更する場合は、既存のユーザアカウントのパスワードもパスワード要件を満たしている必要があります。ポリシーを検証する場合は、パスワードの適合性がチェックされます。これは通常、データベースに変更を送信するときに行われます。詳細については、IPS パスワードの検出および展開方法について （22 ページ）を参照してください。

ユーザの追加またはユーザログイン情報の編集ダイアログボックス

[ユーザの追加（Add User）] または [ユーザログイン情報の編集（Edit User Credentials）] ダイアログボックスを使用して、IPS デバイスのユーザーアカウントを追加または編集します。

ナビゲーション パス

IPS プラットフォームの [ユーザーアカウント（User Accounts）] ポリシーで、[行の追加（+）（Add Row (+)）] ボタンをクリックして新しいアカウントを作成するか、既存のアカウントを選択して [行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。[User Accounts] ポリシーへのアクセス方法については、IPS ユーザ アカウントの設定 （23 ページ）を参照してください。

フィールド リファレンス

表 *6 : [Add User]/[Edit User]* ダイアログボックス

要素	説明
User Name	アカウントのユーザ名。名前は 1 ～ 64 文字で、大文字と小文字、数字、および ( ) + : , _ / -] + $ の特殊文字から構成できます。 アカウントを編集する場合、ユーザ名は変更できません。
パスワード 確認（Confirm）	このユーザ アカウントのパスワード。両方のフィールドにパスワードを入力します。 パスワードは、IPS デバイスの [Password Requirements] ポリシーに準拠する必要があります。 ユーザ パスワード要件の設定 （26 ページ）を参照してください。
ロール	このユーザのロール。これらのロールの説明については、IPS ユーザーロールについて （20 ページ）を参照してください。 **ヒント** ユーザアカウントを編集する場合、サービス ロールは選択できません。サービス ロールに割り当てられているアカウントを編集する場合、ロールは変更できません。

ユーザ パスワード要件の設定

IPS プラットフォームの [Password Requirements] ポリシーを使用して、ローカル IPS デバイス ユーザ アカウントのパスワードのルールを設定します。ユーザが作成するすべてのセンサー パスワードは、このポリシーに定義されている要件に準拠する必要があります。IPS ソフトウェア バージョン 6.0 以降を実行しているセンサーのパスワード要件を設定できます。

ヒント ここで定義する要件は、[User Accounts] ポリシーで受け入れることができるパスワードかどうかを決める条件になります（IPS ユーザ アカウントの設定 （23 ページ）を参照）。このポリシーを変更した場合は、変更されていないユーザアカウントにも適用できます。このポリシーに対する変更の展開の暗黙的な意味については、IPS パスワードの検出および展開方法について （22 ページ）を参照してください。

IPS パスワード要件を設定するには、次のいずれかのポリシーを選択します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [パスワード要件（Password Requirements）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [パスワード要件（Password Requirements）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

次の表で、設定できるパスワード要件オプションについて説明します。

表 7 : *[Password Requirements]* ポリシー

要素	説明
Attempt Limit	過剰な失敗試行によりユーザアカウントをロックする前にユーザがデバイスへのログイン試行を許可される回数。 デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。
Size Range	ユーザパスワードに対して許可される最小と最大のサイズ。最小と最大をハイフンで区切ります。範囲は 6 ～ 64 文字です。デフォルトは 8-64 です。 **ヒント** いずれかの最小文字数オプションにゼロ以外の値を設定した場合、[Size Range] フィールドに入力する最小サイズは、それらの値の合計以上である必要があります。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。
Minimum Digit Characters	パスワードに含まれる必要のある数字の最小数。
Minimum Uppercase Characters	パスワードに含まれる必要のある大文字の英字の最小数。
Minimum Lowercase Characters	パスワードに含まれる必要のある小文字の英字の最小数。
Minimum Other Characters	パスワードに含まれる必要のある英数字以外の印刷可能文字の最小数。
Number of Historical Passwords	各アカウントについてセンサーで記憶する過去のパスワードの数。新しいパスワードが記憶されているいずれかのパスワードと一致した場合は、アカウントのパスワードの変更試行に失敗します。0 を指定した場合、以前のパスワードは記憶されません。

IPS デバイスの AAA アクセス コントロールの設定

AAA ポリシーを使用して、IPS デバイスの AAA アクセス コントロールを設定します。AAA を設定するには、デバイスで IPS ソフトウェアリリース 7.0(4) 以降または 7.1.3 以降を使用する必要があります。たとえば、7.1.1 や 7.1.2 は AAA をサポートしていません。

デバイスへのユーザ アクセスの認証に RADIUS AAA サーバを使用するように、IPS デバイスを設定できます。AAA を設定することにより、デバイスで定義するローカル ユーザの数を減らし、既存の RADIUS 設定を活用できます。AAA サーバを設定する場合は、RADIUS サーバ

が使用できない場合のフォールバック メカニズムとしてローカル ユーザ アカウントを許可するように、デバイスを設定できます。

AAA の設定時に、AAA サーバ ポリシー オブジェクトを使用して RADIUS サーバを識別できます。ポリシーの作成時にオブジェクトを作成できます。そうしなかった場合は、Policy Object Manager で作成できます。AAA サーバ オブジェクトを設定する場合は、次の制限事項に従う必要があります。

- [ホスト（Host）]：IP アドレスを指定する必要があります。DNS 名は使用できません。
- [タイムアウト（Timeout）]：タイムアウト値を入力する場合は、1 ～ 512 秒の範囲で指定する必要があります。汎用 AAA サーバ オブジェクトではさらに大きい数字を使用できますが、IPS のタイムアウトの範囲はそれよりも制限されています。デフォルトは 3 です。
- [プロトコル（Protocol）]：サポートされるプロトコルは RADIUS のみです。
- [キー（Key）]：RADIUS サーバーで定義された共有秘密キーを指定する必要があります。このフィールドは、汎用 AAA サーバ オブジェクトの場合は任意ですが、IPS の場合、キーは必要です。
- [ポート（Port）]：RADIUS 認証/許可ポートが正しいことを確認します。AAA サーバ オブジェクトのデフォルト ポートが IPS のデフォルト（1812）と異なることに注意してください。IPS のデフォルトを使用する場合は、ポートを変更する必要があります。

AAA サーバ オブジェクトを設定する方法については、AAA サーバ オブジェクトの作成を参照してください。

ヒント 使用する認可方式に応じて、デバイス プロパティに設定されたユーザ アカウントが RADIUS サーバに存在するか、またはローカル ユーザ アカウントとして存在するか確認する必要があります。ローカル モードと AAA モードを切り替える場合、または AAA サーバを変更する場合は、使用しているユーザ アカウント データベースのいずれにもアカウントが定義されていることを確認する必要があります。ローカル フォールバックが設定された AAA を使用している場合、アカウントはすべてのデータベースで定義されている必要があります。このアカウントは、デバイスの Security Manager デバイス プロパティで定義されているパスワードと同じパスワードで存在している必要があります。そうでない場合、デバイスの展開が失敗します。検出および展開に使用するユーザ アカウントには管理者権限が必要です。

関連項目

- ユーザ アカウントとパスワードの要件の管理 （19 ページ）
- IPS ユーザ アカウントの設定 （23 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイス アクセス（Device Access）] > [AAA] を選択します。

- （ポリシービュー）[IPS]>[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[AAA] を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次の基本的なプロパティを設定します。

- [認証モード（Authentication Mode）]：ローカルモードと AAA モードのどちらを使用するか。Local モードでは、IPS デバイスで定義されたユーザ アカウントだけを使用します。AAA モードでは、RADIUS サーバがユーザ認証の基本手段です。ローカル ユーザ アカウントをフォールバック メカニズムとして設定できます。デフォルトは Local です。このポリシーのその他のオプションを設定するには、AAA を選択する必要があります。
- [プライマリRADIUSサーバー、セカンダリRADIUSサーバー（Primary RADIUS Server, Secondary RADIUS Server）]：メイン（プライマリ）AAA サーバーおよびバックアップ サーバー（使用する場合）。RADIUS サーバーを識別する AAA サーバー ポリシー オブジェクトの名前を入力します。または、[選択（Select）]をクリックして、オブジェクトのリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

ユーザの認証時に、IPS デバイスは、プライマリ サーバにユーザ認証の試行を送信します。セカンダリ サーバには、プライマリ サーバへの要求がタイムアウトになった場合にアクセスが行われます。

ステップ 3 デフォルト以外の値を設定する場合は、次の任意のプロパティを設定します。

- [コンソール認証（Console Authentication）]：コンソールを介して IPS デバイスにアクセスするユーザーを認証する方法。
  - [Local]：コンソール ポートを介して接続するユーザは、ローカル ユーザ アカウントを使用して認証されます。
  - [Local and RADIUS]：コンソール ポートを介して接続するユーザは、最初に RADIUS を使用して認証されます。RADIUS が失敗した場合は、ローカル認証が試行されます。
  - [RADIUS]：コンソール ポートを介して接続するユーザは、RADIUS によって認証されます。[Enable Local Fallback] も選択する場合は、ローカル ユーザ アカウントを使用してユーザを認証することもできます。
- [RADIUS NAS ID]：認証を要求するサービスを識別するネットワークアクセス ID。値には、すでに RADIUS サーバで設定されている NAS-ID、cisco-ips、NAS-ID 以外を指定できます。デフォルトは cisco-ips です。
- [ローカルへのフォールバックを有効化（Enable Local Fallback）]：すべての RADIUS サーバーが使用できない場合に、ローカルユーザーアカウント認証にフォールバックするかどうか。このオプションは、デフォルトで選択されます。RADIUS サーバがログインの試行に対して否定的な応答を示した場合、ローカル認証は試行されないことに注意してください。RADIUS サーバから応答を受信しなかった場合だけ、ローカル認証が試行されます。
- [デフォルトユーザーロール（Default User Role）]：RADIUS サーバーでロールを割り当てられていないユーザに割り当てるロール。Service 以外の Viewer、Operator、または Administrator をデフォルトのロールにできます。デフォルトのロールを割り当てない場合は、[Unspecified] を選択します（これが

デフォルトです）。ユーザ ロールの説明については、IPS ユーザーロールについて （20 ページ）を参照してください。

（注） ユーザ ロール設定はとても重要です。デフォルトのユーザ ロールを使用せず、RADIUS サーバでもユーザに対してロールを割り当てない場合、センサーは、RADIUS サーバがユーザ名およびパスワードを受け入れたとしてもユーザのログインを阻止します。

RADIUS サーバでユーザに対して明示的にロールを割り当てるには、そのアカウントの Accept Message を、ips-role=administrator、ips-role=operator、ips-role=viewer、または ips-role=service として設定します。ユーザ アカウントごとにそれぞれ Accept Message を設定します。例として、特定のユーザーの Reply 属性は、「Hello <user> your ips-role=operator」を返すように設定できます。

RADIUS サーバでサービス アカウントを設定する場合は、デバイス上でローカルに同じサービス アカウントを設定する必要もあります。サービス アカウントの場合は、ログイン時に RADIUS アカウントとローカル アカウントがチェックされます。

NTP サーバの識別

[NTP] ポリシーを使用して、ネットワーク タイム プロトコル（NTP）サーバを IPS デバイスのタイム ソースとして設定します。NTP を使用すると、ネットワーク デバイス間で時間が同期され、イベント分析に役立ちます。NTP は、IPS デバイスで時間を設定するための推奨される方法です。

Cisco IOS ルータを NTP サーバーとして設定する方法など、センサーに時間を設定する方法の詳細については、コマンド ライン インターフェイス バージョン 7.0 を使用した Cisco Intrusion Prevention System センサーの設定 [英語] の「Configuring Time」を参照してください。

ヒント IPS ソフトウェアの更新に問題がある場合は、IPS センサーで時刻をチェックします。センサーの時刻が、関連付けられている証明書の時刻よりも進んでいる場合、証明書は拒否され、センサー ソフトウェアの更新が失敗します。

ステップ 1 次のいずれかを実行して、[NTP] ポリシーを開きます。

- （デバイス ビュー）ポリシー セレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバー アクセス（Server Access）] > [NTP] を選択します。
- （ポリシー ビュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバー アクセス（Server Access）] > [NTP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [NTPサーバーIPアドレス（NTP Server IP Address）] フィールドに、NTP サーバーの IP アドレスを入力します。サーバーの単一のホストアドレスを識別するネットワーク/ホストオブジェクトの名前も入力できま

す。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。

（注） Cisco Security Manager 4.19 以降、ASA 9.12(1) 以降のすべてのデバイスに対して、IPV6 アドレスを使用して NTP サーバーを設定できます。

ステップ 3 NTP サーバーに認証が不要な場合は、[認証済みNTP（Authenticated NTP）] チェックボックスをオフにします。

NTP サーバに認証が必要な場合は、次のオプションを設定します。

- [認証済みNTP（Authenticated NTP）]：認証された接続を有効にするには、このオプションを選択します。
- [キー、確認（Key, Confirm）]：NTP サーバーのキー値。キーは、MD5 タイプのキー（数値または文字）です。これは、NTP サーバの設定に使用されたキーです。
- [キーID（Key ID）]：NTP サーバーのキー ID 値（1 ～ 65535 の数値）。

ヒント キーとキー ID は NTP サーバで設定します。これらを NTP サーバ設定から取得する必要があります。

DNS サーバの識別

IPS 7.0+ センサーでグローバル相関を設定する場合、センサーはグローバル相関の更新をダウンロードするときに更新サーバに正常に接続するために、ドメイン名を解決できる必要があります。[DNS] ポリシーを使用して、センサーがドメイン名から IP アドレスへの解決に使用できるドメイン ネーム システム（DNS）サーバを識別します。

ヒント インターネット接続の確立時にネットワークに HTTP プロキシが必要な場合は、[DNS] ポリシーの代わりに [HTTP Proxy] ポリシーを設定します。HTTP プロキシ サーバの識別 （32 ページ）を参照してください。

（注） AIP-SSC-5 サービス モジュールでは、DNS サーバはサポートされません。

ステップ 1 次のいずれかを実行して、HTTP プロキシ ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS] を選択します。

- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [プライマリ（Primary）]、[セカンダリ（Secondary）]、および [ターシャリ（Tertiary）] アドレスフィールドで、最大 3 つの DNS サーバーの IP アドレスを指定します。センサーでは、リストの順序でサーバが使用されます。1 つのサーバが応答しない場合は、次のサーバがアクセスされます。

サーバアドレスを含むネットワーク/ホスト オブジェクトの IP アドレスまたは名前を入力できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。ネットワーク/ホスト オブジェクトでは、単一のホスト アドレスを指定する必要があります。

HTTP プロキシ サーバの識別

IPS 7.0+ センサーにグローバル相関を設定し、ネットワークでインターネットへの接続に HTTP プロキシを使用する必要がある場合は、[HTTP Proxy] ポリシーを設定して、IPS センサーで使用できるプロキシを識別する必要があります。グローバル相関の更新をダウンロードする場合、IPS センサーはこのプロキシを使用して更新サーバに接続します。プロキシは、DNS 名を解決できる必要があります。

ヒント HTTP プロキシを使用しない場合は、IPS センサーが更新サーバのアドレスを解決できるように DNS サーバを設定します。DNS サーバの識別 （31 ページ）を参照してください。

（注） AIP-SSC-5 サービス モジュールでは、HTTP プロキシ サーバはサポートされません。

ステップ 1 次のいずれかを実行して、HTTP プロキシ ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [HTTPプロキシ（HTTP Proxy）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [HTTPプロキシ（HTTP Proxy）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次のオプションを設定します。

- [プロキシの有効化（Enable Proxy）]：設定したプロキシサーバーを介して接続するようにデバイスに通知するには、このオプションを選択します。

- [IPアドレス（IP Address）]：プロキシサーバーの IP アドレス、またはサーバーの IP アドレスを含むネットワーク/ホストオブジェクトの名前を入力します。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。ネットワーク/ホスト オブジェクトには、単一のホスト IP アドレスが含まれている必要があります。
- [ポート（Port）]：プロキシサーバーへの HTTP 接続に使用するポート番号を入力します。デフォルトは 80 です。

IPS SSHv2 の既知のホストキー

IPS SSHv2 の既知のホストキーポリシーを使用すると、SSHv2 サーバーホストキー（IPS センサーから SSH サーバーへの発信 SSHv2 接続）を設定できます。この機能は、Cisco IPS の 7.1(8) 以降のバージョンを実行している IPS センサーで使用できます。

ホストキーは、有効な IP アドレスを使用して IPS センサーから取得できます。把握している場合は手動で入力することもできます。ホストキーの取得には数秒かかる場合があります。

ステップ 1 次のいずれかを実行して、IPS SSHv2 の既知のホストキーポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [SSHv2の既知のホストキー（SSHv2 Known Host Keys）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [SSHv2の既知のホストキー（SSHv2 Known Host Keys）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

ステップ 2 [追加（Add）] ボタンをクリックして、[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックス （33 ページ）を開きます。

ステップ 3 行を選択してから [編集（Edit）] ボタンをクリックし、[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックス （33 ページ）を開きます。

[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックス

[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックスを使用して、IPS センサーから SSHv2 キーを取得するか、キーがわかっている場合は手動でキーを入力します。

ナビゲーション パス

[SSHv2既知ホストキー（SSHv2 Known Host Keys）] ポリシーから、[IPアドレス/公開キー（IP Address/Public Key）] テーブルにある [追加（Add）] ボタンをクリックするか、テーブルの行を選択して [編集（Edit）] ボタンをクリックします。[SSHv2既知ホストキー（SSHv2 Known Host Keys）] ポリシーについては、IPS SSHv2 の既知のホストキー （33 ページ）を参照してください。

フィールド リファレンス

表 *8 : [*既知のホスト*RSA*キーの追加または編集（*Add or Edit Known Host RSA Key*）*]* ダイアログボックス

要素	説明
IPアドレス	公開キーを取得する IPS センサーの IP アドレス。
公開キーの取得	[IPアドレス（IP Address）] フィールドで識別されたデバイスから公開キーの取得を開始します。 [公開キーの取得（Retrieve Public Key）] オプションは、デバイスビューで使用できます（共有ポリシービューには表示されません）。ただし、共有ポリシーに公開キーのインライン値を入力するか、デバイスビューで公開キーを取得し、[ポリシーの共有（Share Policy）] オプションを使用して共有することができます。
公開キー（3Public Key）	お客様が知っていて手動で入力できる公開キー。 共有ポリシーの場合、ホストキーのインライン値を入力できます。

IPS SSHv1 フォールバック設定の指定

IPS SSHv1 フォールバックポリシーは、Cisco IPS の 7.1(8) 以降のバージョンを実行している IPS センサーで使用できます。

ステップ 1 次のいずれかを実行して、SSHv1 フォールバックを有効または無効にします。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [設定（Settings）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [設定（Settings）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

ステップ 2 SSHv1 フォールバックを有効にするには、チェックボックスをクリックします。

ステップ 3 SSHv1 フォールバックを無効にするには、チェックボックスをオフにします。

外部製品インターフェイスの設定

[External Product Interface] ポリシーを使用して、Security Manager が Management Center for Cisco Security Agents（CSA MC）と連携する方法を設定します。

一般に、外部製品インターフェイスは、外部セキュリティおよび管理製品から情報を受信して処理するように設計されています。これらの外部セキュリティおよび管理製品は、センサー設定情報を自動的に拡張するために使用できる情報を収集します。Management Center for Cisco Security Agents は、IPS と通信するように設定できる唯一の外部製品です。IPS デバイスごとに最大 2 つの Management Center for Cisco Security Agents サーバを設定できます。

ヒント　Management Center for Cisco Security Agents は、アクティブな製品ではなくなりました。このポリシーは、このアプリケーションをまだ使用している場合にだけ設定します。詳細については、『Installing and Using Cisco Intrusion Prevention System Device Manager 6.0』の「About CSA MC」および http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html を参照してください。

Management Center for Cisco Security Agents は、ネットワーク ホストでセキュリティ ポリシーを強制します。これには 2 つのコンポーネントがあります。

- ネットワーク ホスト上に存在し、そのホストを保護するエージェント。
- エージェントを管理するアプリケーションである管理コンソール。セキュリティ ポリシーの更新をエージェントにダウンロードし、エージェントから操作情報をアップロードします。

はじめる前に

Security Manager がセンサーに外部製品との通信を許可するように、外部製品を許可ホストとして追加します。詳細については、許可ホストの識別　（9 ページ）を参照してください。

ステップ 1　次のいずれかを実行して、[External Product Interface] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [外部製品インターフェイス（External Product Interface）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [外部製品インターフェイスExternal Product Interface）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Management Center for Cisco Security Agents] タブには、外部アプリケーションの IP アドレス（またはネットワーク/ホストオブジェクト）、URL、およびポート、ログインに使用されるユーザ名とパスワード、接続がイネーブルになっているかどうかなどの既存の定義が表示されます。インターフェイス タイプは常に [Extended SDEE] です。

ステップ 2 次のいずれかを実行します。

- サーバーを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [External Product Interface] ダイアログボックスが開きます。サーバの識別に必要な情報を入力し、ポスチャ ACL を設定します。設定の詳細については、[Add External Product Interface]/[Edit External Product Interface] ダイアログボックス （36 ページ）を参照してください。

最大 2 台のサーバを追加できます。

- サーバーを編集するには、そのサーバーを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックして、[外部製品インターフェイス（External Product Interface）] ダイアログボックスに必要な変更を加えます。
- サーバーを削除するには、そのサーバーを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

[Add External Product Interface]/[Edit External Product Interface] ダイアログボックス

[Add External Product Interface]/[Edit External Product Interface] ダイアログボックスを使用して、Management Center for Cisco Security Agents（CSA MC）と IPS デバイスおよび関連ポスチャ ACL との間のインターフェイスを追加または修正します。

ナビゲーション パス

[外部製品インターフェイス（External Product Interface）] IPS プラットフォームポリシーで、[行の追加（Add Row）] をクリックするか、エントリを選択して [行の編集（Edit Row）] をクリックします。[External Product Interface] ポリシーを開く方法については、外部製品インターフェイスの設定 （35 ページ）を参照してください。

フィールド リファレンス

表 9 : [Add External Product Interface]/[Edit External Product Interface] ダイアログボックス

要素	説明
[外部製品のIPアドレス（External Product's IP Address）]	外部製品の IP アドレス、またはアドレスを含むネットワーク/ホスト ポリシー オブジェクト。IP アドレスまたはオブジェクト名を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
インターフェイス タイプ	物理インターフェイス タイプを識別します。これは常に [Extended SDEE] です。
Enable receipt of information	外部製品からセンサーに情報を渡せるかどうか。

要素	説明
SDEE URL	IPS が SDEE 通信を使用して情報を取得するために使用する CSA MC 上の URL。IPS が通信している CSA MC のソフトウェア バージョンに基づいて、URL を次のように設定する必要があります。 • CSA MC バージョン 5.0 の場合：/csamc50/sdee-server。 • CSA MC バージョン 5.1 の場合：/csamc51/sdee-server。 • CSA MC バージョン 5.2 以降の場合：/csamc/sdee-server（デフォルト値）。
[ポート（Port）]	通信に使用するポートまたはポートを識別するポート リスト オブジェクト。ポートまたはポートリスト名を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
ユーザー名 [パスワード（Password）]	外部製品にログインできるユーザ名とパスワード。
Enable receipt of host postures	CSA MC からのホスト ポスチャ情報の受信を許可するかどうか。このオプションをディセーブルにした場合、CSA MC から受信したホスト ポスチャ情報は削除されます。
[到達不能ホストのポスチャを許可（Allow unreachable hosts' postures）]	CSA MC が到達できないホストのホスト ポスチャ情報の受信を許可するかどうか。 CSA MC がホストポスチャに含まれるどの IP アドレスを使用してもホストとの接続を確立できない場合、そのホストは到達不能です。このオプションは、IP アドレスが IPS センサーから参照可能でないポスチャ、またはネットワーク上で重複している可能性のあるポスチャのフィルタリングに役立ちます。このフィルタは、CSA MC が到達できないホストには IPS でも到達できないようなネットワーク トポロジ（IPS と CSA MC が同じネットワーク セグメントにあるなど）に最適です。

要素	説明
[Posture ACL] テーブル	ポスチャ ACL とは、ネットワーク アドレス範囲です。その範囲に対してホスト ポスチャが許可または拒否されます。ポスチャ ACL を使用して、IPS で認識できない、またはネットワーク全体で重複している可能性がある IP アドレスを持つポスチャをフィルタリングします。 • ポスチャ ACL を追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [Add Posture ACL] ダイアログボックスが開きます。ポスチャ ACL の設定の詳細については、[Add Posture ACL]/[Modify Posture ACL] ダイアログボックス （38 ページ）を参照してください。 • ポスチャ ACL を編集するには、ポスチャ ACL を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • ポスチャ ACL を削除するには、ポスチャ ACL を選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。 • ACL のプライオリティを変更するには、その ACL を選択し、[Up] または [Down] ボタンをクリックします。ACL は順番に処理され、最初の一致に関連付けられているアクションが適用されます。
Enable receipt of watch listed addresses	CSA MC からのウォッチ リスト情報の受信を許可するかどうか。このオプションをディセーブルにした場合、CSA MC から受信したウォッチ リスト情報は削除されます。
Manual Watch List RR increase	手動ウォッチ リスト Risk Rating（RR; リスク レーティング）のパーセンテージ。デフォルトは 25 で、有効な範囲は 0 ～ 35 です。
Session-based Watch List RR Increase	セッション ベースのウォッチ リスト リスク レーティングのパーセンテージ。デフォルトは 25 で、有効な範囲は 0 ～ 35 です。
Packed-based Watch List RR Increase	パケット ベースのウォッチ リスト リスク レーティングのパーセンテージ。デフォルトは 10 で、有効な範囲は 0 ～ 35 です。

[Add Posture ACL]/[Modify Posture ACL] ダイアログボックス

[Add Posture ACL]/[Modify Posture ACL] ダイアログボックスを使用して、Management Center for Security Agents のポスチャ ACL を設定します。ポスチャ ACL とは、ネットワーク アドレス範囲です。その範囲に対してホスト ポスチャが許可または拒否されます。ポスチャ ACL を使用して、IPS で認識できない、またはネットワーク全体で重複している可能性がある IP アドレスを持つポスチャをフィルタリングします。

次のフィールドを設定して、ポスチャ ACL を定義します。

- [ネットワークアドレス（Network Address）]：ホストまたはネットワークの IP アドレスまたはホスト、または IP アドレスを指定するネットワーク/ホストオブジェクトの名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。
- [アクション（Action）]：ホストポスチャがネットワークアドレス上のホストで許可されるか拒否されるか。

ナビゲーション パス

[外部製品インターフェイス（External Product Interface）] ダイアログボックス（[Add External Product Interface]/[Edit External Product Interface] ダイアログボックス （36 ページ）を参照）で、[ポスチャACL（Posture ACL）] テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックするか、ポスチャ ACL を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

IPS ロギング ポリシーの設定

IPS プラットフォームの [Logging] ポリシーを使用して、トラフィック フロー通知と分析エンジンのグローバル変数を設定します。これらの設定は、IPS センサーの一般操作に適用されます。

トラフィック フロー通知では、センサーのインターフェイス上のトラフィック フローを扱う必要があります。インターフェイス上のパケットのフローをモニタし、そのフローが指定した間隔中に変更（開始および停止）された場合に通知を送信するようにセンサーを設定できます。特定の通知間隔内に欠落パケットのしきい値を設定でき、ステータスイベントがレポートされる前のインターフェイス アイドル遅延も設定できます。

分析エンジンは、パケット分析とアラート検出を実行します。指定したインターフェイスを流れるトラフィックをモニタします。分析エンジンには、[Maximum Open IP Log Files] という 1 つのグローバル変数だけがあります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [ロギング（Logging）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 10 : [IPS Logging] ページ

要素	説明
[Interface Notifications] タブ	

要素	説明
Missed Packets Threshold	通知を受信する前に発生する必要のある欠落パケットの割合。デフォルトは 0 で、範囲は 0 ～ 100 です。
通知間隔（Notification Interval）	欠落パケットのパーセンテージをチェックする時間の長さ（秒単位）。デフォルトは 30 で、有効な範囲は 5 ～ 3600 です。
Interface Idle Threshold	この時間が経過すると通知が生成される、インターフェイスがアイドルになってパケットを受信しない時間の長さ（秒単位）。デフォルトは 30 で、有効な範囲は 5 ～ 3600 です。
[Analysis Engine] タブ	
フロー深度の指定（Specify-Flow-Depth）	フローの検査深度を指定できます。フロー深度は、フローで検査されるバイト数です。新しい値は、新しいフローにのみ適用されます。有効な範囲は 0 ～ 4294967296 です。デフォルトは 0 です。
サービスアクティビティの有効化（Enable Service Activity）	サービスアクティビティを使用して、診断目的でサービスアクティビティに関する情報を収集できます。詳細はよりきめ細かく、ポートレベルの詳細があります。サービスアクティビティを有効にすると、システムのパフォーマンスに影響します。診断目的でのみ、サービスアクティビティの収集を一時的に有効にします。変更を有効にするには、サービスアクティビティを有効にした後、センサーをリブートする必要があります。
サービスアクティビティの制限（Service Activity Limit）	有効にするサービスの数の制限を設定します。有効範囲は 10 ～ 65536 です。デフォルトは 15 です。
（注） [フロー深度の指定（Specify-Flow-Depth）]、[サービスアクティビティの有効化（Enable Service Activity）]、および [サービスアクティビティの制限（Service Activity Limit）] フィールドは、バージョン 7.2(2) 以降の IPS デバイスに適用されます。	
Maximum Open IP Log Files	センサーで開くことのできる IP ログ ファイルの最大数。デフォルトは 20 で、範囲は 20 ～ 100 です。

IPS ヘルスモニター

[IPS ヘルスモニター（IPS Health Monitor）] ページで、IPS デバイスの正常性およびネットワーク セキュリティ ステータスを判断するために使用されるメトリック（パラメータ）を設定できます。IPS デバイスは、これらのメトリックを使用して、IPS イベントを送信するときに適

切なシビラティ（重大度）を割り当てます。結果は、Security Manager の Health and Performance Monitor（[起動（Launch）] > [Health and Performance Monitor]）に表示されます。

IPS Health Monitor は、IPS バージョン 6.1 以降の IPS デバイスとバージョン 4.4 以降の Security Manager でサポートされています。次の特殊なケースに注意してください。

1. 7.x を実行している IPS デバイスの場合、IPS セキュリティ設定ポリシーの 11 の設定項目はすべて、Security Manager GUI で適切に表示および監視されます。
2. 6.1 より前のバージョンを実行している IPS デバイスの場合、ネットワーク参加とグローバル相関のエントリは、Security Manager のデバイスビューに表示されません。
3. IPS ヘルスモニターの一部の設定項目は、デバイス側自体で保護されているエントリであり、編集できません。そのような場合は、Security Manager によって通知されます。

チェックボックスをオンにしてメトリックを選択しないと、Health and Performance Monitor に表示されません。デフォルト設定を受け入れるか、値を編集できます。メトリックを選択しないと、項目は無効になり、編集できません。

すべてのメトリックの中で最も重要な設定が、全体的な正常性になります。たとえば、選択されたメトリックが、1 つのクリティカルを除いてすべて正常であっても、全体的な正常性はクリティカルになります。IPS センサーの全体的な正常性ステータスが変化すると、IPS センサーは正常性およびセキュリティ ステータス イベントを送信します。

IPS センサーのセキュリティステータスは、仮想センサーによって検出されたイベントの脅威レーティングを使用して、仮想センサーごとに決定されます。仮想センサーが、その仮想センサーのしきい値を超える脅威レーティングを持つイベントを検出すると、その仮想センサーのセキュリティステータスが上昇します。しきい値を超えると、そのセキュリティステータスは、イベントがより高いレベルで検出されずに、設定された時間が経過するまで、クリティカルレベルで維持されます。

[IPS ヘルスモニター（IPS Health Monitor）] ページでメトリックを設定するには、次のいずれかのポリシーを選択します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ヘルスモニター（Health Monitor）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS] > [プラットフォーム（Platform）] >[デバイス管理（Device Admin）] > [ヘルスモニター（Health Monitor）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

（注） ポリシービューでは、共有 IPS ヘルスモニターポリシーが、6.1 より前のバージョンを実行している IPS デバイスに適用されている場合、検証が実行されません。Security Manager は、デバイスへの展開時にそのようなポリシーを無視し、展開ログにもそれらをキャプチャします。

次の表で、設定できる IPS ヘルスモニターメトリックについて説明します。

表 *11 : IPS* セキュリティ設定ポリシー

要素	説明
[検査負荷（Inspection Load）]	検査負荷のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。
[受信できなかったパケット（Missed Packet）]	受診できなかったパケットのしきい値のパーセントと、このメトリックがセンサーの全体的なヘルスレーティングに適用されるかどうかを設定できます。
メモリ使用率	メモリ使用量のしきい値のパーセントと、このメトリックがセンサーの全体的なヘルスレーティングに適用されるかどうかを設定できます。
シグニチャ アップデート	最後のシグニチャのアップデートが適用された時間のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。
ライセンスの期限切れ	ライセンスの有効期限のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。
[イベント取得（Event Retrieval）]	最後にイベントが取得された時間のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。 （注） イベント取得メトリックでは、IME などの外部モニタリング アプリケーションによって最後のイベントが取得された時間が記録されます。外部のイベント モニタリングを実行しない場合は、[イベント取得（Event Retrieval）] を無効にします。
ネットワーク参加	ネットワーク参加ヘルスメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。
グローバル相関	グローバル相関ヘルスメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。
アプリケーションの障害	センサーの全体的なヘルスレーティングにアプリケーションの障害を適用することを選択できます。
[バイパスモードの IPS（IPS in Bypass Mode）]	バイパスモードがアクティブであるかどうかを認識し、それをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。

要素	説明
[1 つ以上のアクティブインターフェイスがダウン（One or More Active Interfaces Down）]	1 つ以上のインターフェイスがダウンしているかどうかを認識し、それをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。
警告	警告しきい値の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。
重大	重大しきい値の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。

IPS セキュリティ設定の指定

IPS セキュリティ設定ポリシーを使用すると、IPS デバイスのセキュリティにとって重要な次の 2 つの項目を設定できます。

- パケットキャプチャロギングの許可（Permit packet capture logging）：この機能を使用すると、IPS デバイスは、ユーザーによる packet capture/display/iplog コマンドの任意の実行を防ぐことができます。以前のバージョンの Cisco Security Manager では、そのようなアクションにおいて、コマンドを実行したユーザーの痕跡が残りませんでした。
- 設定可能なアイドルタイムアウト（Configurable idle timeout）：この機能を設定している場合、指定した時間が経過すると IPS デバイスへの接続が終了します。その目的は、CLI セッションのセキュリティを強化することです。

（注） これらの設定は、IPS 7.1.3 以降で動作するデバイスで使用できます。

IPS セキュリティ設定を指定するには、次のいずれかのポリシーを選択します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [設定（Settings）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [設定（Settings）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

次の表で、定義できる IPS セキュリティ設定について説明します。

表 *12 : IPS* セキュリティ設定ポリシー

要素	説明
[パケットロギングの許可（Permit packet logging）]	パケットロギングを有効にするかどうか。packet capture/display/iplog コマンドに適用されます。

要素	説明
[CLI の非アクティブタイムアウト（分単位）（CLI Inactivity Timeout (In Minutes)）]	指定した時間が経過すると、IPSデバイスへの接続が終了します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。