外部モニタリング、トラブルシューティング、および診断ツールの使用方法

大規模な企業やサービスプロバイダーでは、高いネットワーク可用性が求められます。ネットワーク管理者は、ネットワーク可用性を維持するうえでさまざまな課題に直面しています。課題には、予定外のダウンタイム、専門知識の不足、不十分なツール、複雑なテクノロジー、ビジネス統合、競争の激しい市場などがあります。これらの課題に対応して解決するには、ネットワークモニタリング、問題診断、およびトラブルシューティングが不可欠です。

モニタリングでは、ネットワークアクティビティおよびデバイスのステータスを調査して、異常なイベントおよび動作を識別します。ネットワークおよびシステムの障害（停止や低下など）を迅速に診断および修正することによりサービスアベイラビリティが向上するため、問題を切り分け、分析、および修正するためのツールが不可欠です。

デバイスイベントをモニタリングするための主なSecurity Managerツールは、ヘルスとパフォーマンスのモニタ（第71章「ヘルスとパフォーマンスのモニタリング」を参照）とイベントビューア（第69章「イベントの表示」を参照）です。

ヘルスとパフォーマンスのモニタ、およびイベントビューアに加え、次のトピックでは、Security Managerで使用できるその他のモニタリング、トラブルシューティング、および診断ツールについて説明します。

ダッシュボードの概要

バージョン4.5以降、Security Managerクライアントには新しい起動ポイント（構成可能なダッシュボード）があります。このトピックでは、このダッシュボードについての概要を説明します。

このダッシュボードは、Security Managerクライアントの起動時にデフォルトのクライアントアプリケーションとして選択できる6つのクライアントアプリケーションの1つです（他には、Configuration Manager、Event Viewer、Report Manager、Health and Performance Manager、Image Managerがあります。CSM Mobileと呼ばれるモバイルデバイス用に設計されたアプリケーションもあります）。このダッシュボードを使用することによって、Security Managerの他の領域にある、IPS Health Monitorページ、Report Manager、Health and Performance MonitorおよびIP Intelligence設定などのタスクを実行できます。

ダッシュボードには、次の表に示すウィジェットが含まれています。ウィジェットは、IPS、ファイアウォール、またはその両方の各用途別に分類されています（これらのウィジェットのすべてがデフォルトで表示されるわけではありません）。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成して、タブとして表示できます。元のダッシュボードと、作成した新規や追加のダッシュボードの両方は、すべてカスタマイズ可能です。ダッシュボードをカスタマイズするには、使用可能なウィジェットのリストから任意のダッシュボードにウィジェットをドラッグアンドドロップします。

表 *1: IPS*、ファイアウォール、およびその両方に使用するウィジェット

IPS 用ウィジェット	• **IPSインスペクション負荷トレンド（IPS Inspection Load Trends）** • **IPS 攻撃者、攻撃対象、およびシグニチャに関する上位10のレポート（Top 10 Reports for IPS Attackers, Victims, and Signatures）** • **IPS欠落パケットトレンド（IPS Missed PacketTrends）** • **IPSライセンス（IPS License）** • **IPS更新パッケージ（IPS Update Packages）** • **古いIPSセンサー（IPS Sensors Out of Date）**
ファイアウォール用ウィジェット	• ファイアウォールの送信元、宛先、サービスに関する上位10のレポート（Top 10 Reports for Firewall Sources, Destinations, and Services） • ボットネットマルウェアサイト、ポート、ホストに関する上位10のレポート（Top 10 Reports for Botnet Malware Sites, Ports, and Hosts） • ファイアウォールCPU使用率トレンド（Firewall CPU Usage Trends）

IPS 用ウィジェット	• **IPSインスペクション負荷トレンド（IPS Inspection Load Trends）** • **IPS 攻撃者、攻撃対象、およびシグニチャに関する上位10のレポート（Top 10 Reports for IPS Attackers, Victims, and Signatures）** • **IPS欠落パケットトレンド（IPS Missed PacketTrends）** • **IPSライセンス（IPS License）** • **IPS更新パッケージ（IPS Update Packages）** • **古いIPSセンサー（IPS Sensors Out of Date）**
IPSおよびファイアウォールの両方に使用するウィジェット	• デバイスの健全性の概要（Device Health Summary） • メモリ使用量トレンド（Memory Usage Trends） • 展開 • IPインテリジェンス（IP Intelligence）

ダッシュボードとそのウィジェットの使用方法は、Security Manager を使用する目的によって異なります。たとえば、次の4つのウィジェットを使用して、デバイスの正常性の傾向を観察できます。

- IPSインスペクション負荷トレンド（IPS Inspection Load Trends）
- IPS欠落パケットトレンド（IPS Missed PacketTrends）
- メモリ使用量トレンド（Memory Usage Trends）
- ファイアウォールCPU使用率トレンド（Firewall CPU Usage Trends）

個々のウィジェットについて、次の表で説明します。主要なウィジェットの 1 つは、[デバイスの健全性の概要（Device Health Summary）] ウィジェットです。重要であることの理由の 1 つは、モバイルデバイス用に特別に設計された CSM Mobile を介してアクセスできる情報と同じ情報を提供することです。CSM Mobile の詳細については、CSM Mobile （20 ページ）を参照してください。CSM Mobile の有効化または無効化については、[CSM Mobile] ページを参照してください。

表 *2:* 個々のウィジェットの説明 ダッシュボード ウィジェット ダッシュボード内の ***IPS*** 用ウィジェット ダッシュボード内のファイアウォール用ウィジェット

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
IPS 攻撃者、攻撃対象、およびシグニチャに関する上位10のレポート（Top 10 Reports for IPS Attackers, Victims, and Signatures）	

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	ネットワーク内の IPS アラートの上位攻撃者、攻撃対象、およびシグニチャの分析に使用できる事前定義システムレポート。 **クリック可能なリンク**：[上位攻撃者（Top Attackers）] ウィジェットでは、IP アドレスはアクティブなハイパーリンクです。クリックすると IP インテリジェンスが表示されます。Security Manager の IP インテリジェンスの詳細については、 IP インテリジェンス（IP Intelligence） （51 ページ）を参照してください。 **クリック可能なリンク**：[上位シグニチャ（Top Signature）] ウィジェットでは、シグニチャ ID はアクティブなハイパーリンクです。クリックすると、シグニチャ情報が表示されます。 これらのレポートを使用するには、Report Manager を使用します（[起動（Launch）] > [Report Manager...]）。 これらの上位 10 レポートのいずれかから Event Viewer をクロス起動するには、特定の攻撃者、攻撃対象、またはシグニチャを選択し、発生数をクリックします。デフォルトでは、過去 24 時間の発生数がリストされます。必要に応じて、過去 1 時間に変更できます。 （注） Event Viewer をクロス起動すると、サマリーダッシュボードでは過去 24 時間または過去 1 時間であっても、Event Viewer のイベントクエリ時間は過去 10 分として表示されます。ドロップダウンリストを使用して、Event Viewer のイベントクエリ時間を過去 10 分間から別の値に変更できます。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
IPS欠落パケットトレンド（IPS Missed PacketTrends）	IPS欠落パケットトレンドの測定。欠落パケットのトレンドデータは、欠落したパケットに基づくアラートがある場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 （デバイスビューのIPSデバイス）[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）]の[IPSヘルスモニター（IPS Health Monitor）]ページでモニタリングパラメータを設定できます。
IPSライセンス（IPS License）	ライセンスが 30 日または 60 日で期限切れになる IPS デバイスを表示します（ドロップダウンリストを使用して、30 日または 60 日を選択します）。 ライセンスが 30 日または 60 日（選択した方）で期限切れになると、このウィジェットにはライセンスの有効期限が表示されます。
IPS更新パッケージ（IPS Update Packages）	Cisco.com またはローカル ダウンロード サーバーに存在するが、Security Manager サーバーにはダウンロードされていないセンサーの更新およびシグニチャの更新を表示します。 このような更新が多数ある場合、このウィジェットには最新の10件の更新のみが表示されます。
古いIPSセンサー（IPS Sensors Out of Date）	シグネチャの更新が必要なセンサー。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
ファイアウォールの送信元、宛先、サービスに関する上位 10 のレポート（Top 10 Reports for Firewall Sources, Destinations, and Services）	ファイアウォールACLイベントの上位の宛先、サービス、および送信元の識別に用できる事前定義システムレポート。この統計情報は、Event Manager サービスで収集されるイベント（Event Viewer に表示されるイベント）に基づいています。 これらのレポートを使用するには、Report Managerを使用します（[起動（Launch）] > [Report Manager...]）。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
ボットネットマルウェアサイト、ポート、ホストに関する上位10のレポート（Top 10 Reports for Botnet Malware Sites, Ports, and Hosts）	ボットネットトラフィックフィルタリングの分析に使用できる事前定義システムレポート。この統計情報は、ブロックリストおよびグレーリストにあるサイトについて Event Manager サービスで収集されるボットネットイベント（Event Viewer に表示されるイベント）に基づいています。 これらのレポートを使用するには、Report Manager（**[**起動（**Launch**）**]** > **[Report Manager]**）を使用します。
ファイアウォールCPU使用率トレンド（Firewall CPU Usage Trends）	ファイアウォールの CPU 使用率トレンドの測定。CPU 使用率トレンドデータは、ファイアウォールが CPU 使用率のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
デバイスの健全性の概要（Device Health Summary）	

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS** デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ **（デバイスビューの IPS デバイス）[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）] の [IPS**ヘルスモニター**（IPS Health Monitor）] ページでモニタリングパラメータを設定できます。**
	HPM によって生成された、現在の重大度の高いまたは中程度のアクティブなアラートを表示します。アラートは、Alert-Description、Predefined-Category、Device または Alert Technology 別にグループ化できます。 **クリック可能なリンク**：デバイス名はアクティブなハイパーリンクです。クリックすると、ダッシュボードに [デバイスの概要（Device Summary）] ダイアログボックスが表示されます。このリンクは、[_____ でグループ化（Group by _____）] ドロップダウンリストのすべてのオプション（[アラート（Alert）]、[カテゴリ（Category）]、[デバイス（Device）]、または [テクノロジー（Technology）]）で機能します。 これらのアラートを構成するには、HPM（[起動（Launch）] > [Health and Performance Monitor...]）を使用します。 （注） HPM でデバイスの監視をイネーブルにした後、実際の値が [デバイスの健全性の概要（Device Health Summary）] に表示されるまで、優先デバイスの場合は最大 5 分、非優先デバイスの場合は 10 分かかることがあります。 **アラートの確認**：アラートを確認するには、次の手順に従います。 **1.** [_____ でグループ化（Group by _____）] ドロップダウンリストを使用して、[アラート（Alert）]、[カテゴリ（Category）]、[デバイス（Device）]、または [テクノロジー（Technology）]）を選択します。。 **2.** 関心のあるアラート、カテゴリ、デバイス、またはテクノロジーを展開しま

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	す。これを行うと、Security Manager で監視している各デバイスのアラート、カテゴリ、デバイス、またはテクノロジーが表示されます。 **3.** [詳細（Detail）] アイコン（このトピックの最後に示しています）をクリックします。これにより、[アラート（Alert）] ダイアログボックスが開きます。 **4.** [アラートを確認（Acknowledge Alert）] をクリックします。 **アラートのクリア**：アラートをクリアするには、次の手順に従います。 **1.** [_____ でグループ化（Group by _____）] ドロップダウンリストを使用して、[アラート（Alert）]、[カテゴリ（Category）]、[デバイス（Device）]、または [テクノロジー（Technology）]）を選択します。。 **2.** 関心のあるアラート、カテゴリ、デバイス、またはテクノロジーを展開します。これを行うと、Security Manager で監視している各デバイスのアラート、カテゴリ、デバイス、またはテクノロジーが表示されます。 **3.** [詳細（Detail）] アイコン（このトピックの最後に示しています）をクリックします。これにより、[アラート（Alert）] ダイアログボックスが開きます。 **4.** [アラートのクリア（Clear Alert）] をクリックします。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS** デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	モバイルデバイスからもデバイス健全性の概要情報にアクセスできます。これを行うには、CSM Mobile アプリケーションを使用します。CSM Mobile から入手できる情報は、[デバイスの健全性の概要（Device Health Summary）] ウィジェットで入手できるものと同じです。CSM Mobile の有効化または無効化については、[CSM Mobile] ページを参照してください。
メモリ使用量トレンド（Memory Usage Trends）	IPS 健全性ステータスまたはファイアウォール健全性トレンドの測定。 IPS デバイスの場合、（デバイスビューの IPS デバイス）[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）] の [IPS ヘルスモニター（IPS Health Monitor ）] ページでモニタリングパラメータを設定できます。
展開	過去 24 時間のすべてのデバイスの展開ステータスを表示します。 Deployment Manager（[Configuration Manager] > [管理（Manage ）] > [展開（Deployments）]）を使用して展開ステータスを監視することもできます。 。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
IPインテリジェンス（IP Intelligence）	次の事項に関連する、IP アドレスについての情報。 • IP 位置情報 • DNS リバースルックアップによる FQDN • WHOIS 情報 Security Manager の IP インテリジェンス設定については、[Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [IPインテリジェンス設定（IP Intelligence Settings）] に移動します。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
CSM モニター	

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**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**）**] の [IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	サーバー情報を次の 3 つのカテゴリで表示します。 • CSMサーバー統計情報。この情報は、その名が示す通りです。たとえば、オペレーティングシステムの起動時間が表示されます。 • CSMユーザ関連情報。この情報には、ログインしているユーザ数という 1 つの項目のみが含まれます。 • CSM DB バックアップ関連情報。この情報は、[CMSモニター（CSM Monitor）] ウィジェットが未解決のバックアップロックファイルを検出したかどうかを示します。 未解決のバックアップロックファイルがあるかどうかを知ることは、次の理由で重要です。CSM バックアップを実行すると、次のようなエラーで失敗します。「ERROR(383): C:\PROGRA~2\CSCOpx\backup.LOCK file exists.」 次のような解決策が考えられます。Security Manager は、バックアップを開始する前に、バックアップディレクトリに新しいロックファイル（backup.LOCK)）を作成します。バックアップが中断または失敗した場合、このファイルはクリーンアップされません。Security Manager サーバーから現在の backup.LOCK ファイルを削除してから、バックアッププロセスを再度実行する必要があります。 [CMSモニター（CSM Monitor）] ウィジェットを使用すると、未解決のバックアップロック ファイルをより迅速かつ便利に検出できます。 詳細については、次の URL にある Cisco TAC のドキュメントを参照してくださ

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS** デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）[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**）]の[**IPS**ヘルスモニター（**IPS Health Monitor**）]ページでモニタリングパラメータを設定できます。
	い。 http://www.cisco.com/en/US/products/ps6498/products_tech_note09186a0080c13cdd.shtml

（注） 場合によっては、上位の感染ホストなどのダッシュボードレポートの外観が、 Report Managerによって生成されたレポートとわずかに異なります。これは並べ替えの違いによるものですが、データは同一です。このようなケースは、ダッシュボードレポートの複数のエントリに同じカウントがある場合に発生します。

ダッシュボードの基本的な操作を次の表に示します。

表 *3:* ダッシュボードの基本操作ダッシュボードの操作

ダッシュボードの起動	**Configuration Manager** またはその他の **Security Manager** クライアントアプリケーション>[起動（**Launch**）]>[ダッシュボード（**Dashboard**）]
新しいダッシュボードの追加	[ファイル（File）]>[新規ダッシュボード（New Dashboard）]

ダッシュボードの起動	**Configuration Manager** またはその他の **Security Manager** クライアント アプリケーション**>[**起動（**Launch**）**]>[**ダッシュボード（**Dashboard**）**]**
デフォルトビューのダッシュボードタブを再配置する	ダッシュボードのタブを再配置して、デフォルトビューを設定できます。たとえば、[IPS] タブを最初（左端） にしたい場合があります。 **1.** [サマリー（Summary）]、[ファイアウォール（Firewall）]、[IPS] など、関心のあるタブをクリックします。 **2.** 目的のタブが選択されたままの状態で右クリックすると、コンテキスト メニュー オプション [左に移動（Move to Left）]、[右に移動（Move to Right）]、[最初に移動（Move to First）]、[最後に移動（Move to Last）] が表示されます。 **3.** 選択する項目をクリックします。 **4.** 変更を保存する必要はありません。また、変更は永続的です。個々のダッシュボードタブは、次回ダッシュボードを起動したときに同じように配置されます。
別のダッシュボードを表示する	[サマリー（Summary）]、[ファイアウォール（Firewall）]、[IPS] など、目的のダッシュボードのタブをクリックします。
ウィジェットの表示または非表示	[ファイル（File）] > [ウィジェットを表示（Show Widgets）] または [ファイル（File）] > [ウィジェットを非表示（Hide Widgets）]
ウィジェットの追加	ドラッグアンドドロップによる方法： **1.** [ファイル（File）] > [ウィジェットを表示（ Show Widgets）] に移動します。 **2.** 目的のウィジェットを、ダッシュボードにドラッグアンドドラッグします。 メニューによる方法： **1.** [ファイル（File）] > [ウィジェットを表示（ Show Widgets）] に移動します。 **2.** 目的のウィジェットをクリックして選択します。 **3.** 説明バーで [追加（Add）] をクリックします。 **4.** 説明バーで [完了（Done）] をクリックします。 （**注**） メニューによる方法を使用すると、ウィジェットはダッシュボードの左上隅に追加されます。必要に応じて、すべてのウィジェットをドラッグアンドドロップして並べ替えることができます。

ダッシュボードの起動	**Configuration Manager** またはその他の **Security Manager** クライアントアプリケーション**>[**起動（**Launch**）**]>[**ダッシュボード（**Dashboard**）**]**
ウィジェットの削除	削除するウィジェットのタイトルバーにある [削除（Remove）] アイコンをクリックします。
ウィジェットの展開	ダッシュボードにウィジェットが表示されている場合は、下矢印で展開できます。ウィジェットのタイトルバーの右側にマウスポインタを合わせると、下矢印が表示されます。下矢印のツールチップには、「展開（Expand）」というラベルが付いています。 （注） ウィジェットを折りたたんで、ダッシュボードを終了し、ダッシュボードを再度起動したときは、特別な操作が必要となります。この場合、ウィジェットは引き続き折りたたまれていますが、（通常は展開に使用される）下矢印は表示されません。上矢印 （通常は折りたたむために使用）のみが表示されます。この場合、ウィジェットを展開するには、上矢印をクリックします。下矢印が再び表示されますので、通常どおり下矢印をクリックします。
ウィジェットを折りたたむ	ダッシュボードにウィジェットが表示されている場合は、上矢印で折りたたむことができます。ウィジェットのタイトルバーの右側にマウスポインターを合わせると、上矢印が表示されます。上矢印のツールチップには、「展開（Expand）」というラベルが付いています (「折りたたむ（Collapse）」ではありません）。
_____ でグループ化 （[デバイスの健全性の概要（Device Health Summary）] ウィジェットのみ）	次の選択肢を提供するドロップダウンリスト： • アラートでグループ化 • カテゴリでグループ化 • デバイスでグループ化 • テクノロジーでグループ化 （注） [_____でグループ化（Group by _____）] ドロップダウンリストで、デバイスの表示名（ハイパーリンクであることを示すために下線が引かれています）をクリックして、メモリやその他のパラメータについて、デバイスの健全性に関する情報ボックスを表示できます。情報ボックスにはアドレスフィールドがあります。アドレスは Host.Domain または IP アドレスのいずれかです。Host.Domain が構成されている場合、その情報が表示されます。それ以外の場合は、IPアドレスが表示されます。

ダッシュボードの多くのアイコンは、クリックすることで更新やダッシュボードの追加などの特定のアクションを実行できます。これらのクリック可能なアイコンのほとんどには、アイコンをクリックすると実行されるアクションを説明するツールチップがありますが、いくつかの

アイコンにはツールチップがありません。ダッシュボード内のツールチップのないクリック可能アイコンを次の表に示します。

表 *4:*ダッシュボード内のツールチップがないクリック可能アイコンダッシュボードアイコンダッシュボード内のツールチップがないアイコン

アイコン	表示	ウィジェット	説明
	三角形の黄色の背景に黒い感嘆符。	[展開（Deployment）] ウィジェット	[展開中（Deploying）] アイコン。 ジョブが展開中の状態であることを示します。このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）
	赤と黄色のドットが付いた白い長方形（ドキュメント）。	[展開（Deployment）] ウィジェット	[ステータスレポート（Status Report）] アイコン。 このアイコンをクリックして、詳細な展開ステータスレポートを表示します。
	灰色の縁取りのある緑の円の中に白いチェックマーク。	[展開（Deployment）] ウィジェット	[成功（Succeeded）] アイコン ジョブが成功状態であることを示します。このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）

アイコン	表示	ウィジェット	説明
	灰色の縁取りの赤い円の中に白い「X」。	[展開（Deployment）] ウィジェット	[失敗（Failed）] アイコン。 ジョブが失敗した状態であることを示します。このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）
	紙に注釈を付けている鉛筆とクリップボード。	[デバイスの健全性の概要（Device Health Summary）] ウィジェット	[詳細（Details）] アイコン このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）

CSM Mobile

バージョン 4.5 以降、Cisco Security Manager には CSM Mobile と呼ばれるアプリケーションがあります。

CSM Mobile では、モバイル デバイスからのデバイスのヘルスに関するサマリー情報にアクセスできます。この方法で入手できる情報は、[デバイスの健全性の概要（Device Health Summary）] ウィジェットで入手可能な情報と同じで、ヘルスとパフォーマンスのモニタによって生成される現在のシビラティ（重大度）が高または中程度のアクティブなアラートです。アラートは、Alert-Description、Predefined-Category、Device または Alert Technology 別にグループ化できます。ダッシュボードのデバイスの健全性の概要情報の詳細については、ダッシュボードの概要（2 ページ）を参照してください。

CSM Mobile のプリンシパル ユーザは、Apple iPad、Apple iPhone、Google Chrome ブラウザ、Apple Safari ブラウザを使用するユーザであることが想定されています。

CSM Mobile を使用するには、有効にする必要があります。CSM Mobile の有効化または無効化については、[CSM Mobile] ページを参照してください。

（注） CSM Mobile 機能が有効になっていない場合は、デフォルトの Security Manager ログイン ページ（CiscoWorks Common Services フレームワークソフトウェアによって提供される）にリダイレクトされます。エラーメッセージは表示されません。

CSM Mobile のホームページには、次のアラートカテゴリがあります。

- Device Not Reachable
- Interface Down
- Overall Device Health Alerts
- メモリ使用率が高い（High Memory Utilization）
- Firewall—High CPU Utilization
- IPS—High Inspection Load
- IPS—High Missed Packets
- IPS—Bypass Mode
- Other Alerts

CSM Mobile のナビゲーションおよびその他のタスクは、いくつかのシンプルな画面とアイコンを使用して実行できます。

- [ログイン（Login）]：「Cisco Security Manager Mobile - バージョン 4.5.0」と書かれた画面に、ユーザー名とパスワードのフィールドと、ログイン用のボタンがあります。
- [ログアウト（Logout）]：CSM Mobile ホームページ上にある、青色の背景の白い [X] アイコン。このアイコンは左上隅にあります。
- [更新（Refresh）]：CSM Mobile ホームページ上にある、青色の背景の白い円形の矢印アイコン。このアイコンは右上隅にあります。
- [アラートの詳細（Alert Detail）]：CSM Mobile ホームページのアラートタイプごとに、アラートカウントの右側にある灰色の矢印アイコン。
- CSM モバイルの [戻る（Back）] ボタン：各アラートの詳細ページにある、青い五角形の背景に白い角形矢印[アラートの詳細ページでのみ使用可能]。CSM Mobile の [戻る（Back）] ボタンは、ブラウザの戻るボタンと機能的に同等です。

（注） CSM Mobile の表示は自動的に更新されません。最新のアラートデータを取得するには、更新ボタンを手動でクリックする必要があります。

インベントリ ステータスの表示

表示することを許可されているすべてのデバイスのデバイス プロパティの概要を表示できます。概要には、デバイス アクセス情報およびすべてのデバイス設定が含まれています。概要では、どの設定がローカルであり、どの設定が共有ポリシーを使用しているかが示され、また有効なポリシー オブジェクト オーバーライドも示されます。デバイスへの設定展開のステータスを表示することもできます。

レポートは表形式であり、フィルタリング、ソート、並べ替え、およびカラムの削除によって情報を整理できます。また、表の内容を Security Manager サーバ上の Comma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートすることもできます。

ステップ 1 デバイスビューで、[ツール（Tools）]>[インベントリステータス（Inventory Status）] を選択して、[Inventory Status] ウィンドウ （23 ページ）を開きます。

ステップ 2 上部の表で、詳細なステータスを表示するデバイスを選択します。詳細情報が下部のペインのタブに表示されます。情報はフォルダに整理されています。[+] または [-] アイコンをクリックして、フォルダを開いたり閉じたりします。または、フォルダ名をダブルクリックします。次のタブを使用できます。

- [インベントリ（Inventory）]：選択したデバイスのデバイスプロパティ、展開方法、デバイス グループ メンバーシップ、およびモジュールの親デバイスに関する概要情報が表示されます。
- [Policy]：選択したデバイスに対して設定できるポリシーの現在のステータスが表示されます。ポリシーのステータスは、未割り当て（未定義）、ローカル ポリシー、または共有ポリシーです。
- [Policy Object Overrides]：選択したデバイスに対して定義されたオーバーライドを持つポリシー オブジェクトが表示されます。
- [ステータス（Status）]：選択したデバイスの Security Manager 展開ジョブからのステータスメッセージを、イベントタイプごとに整理して一覧表示します。

イベントは、管理対象のデバイスまたはコンポーネントが異常な状態になったことを示す通知です。1 つのモニタ対象デバイスまたはサービス モジュールで複数のイベントが同時に発生する場合もあります。

Security Manager では、各タイプの最近のイベントだけが表示されます。過去のステータス情報を表示するには、Deployment Manager を使用します。

ステップ 3 [閉じる（Close）] をクリックして、[インベントリステータス（Inventory Status）] ウィンドウを閉じます。

[Inventory Status] ウィンドウ

[Inventory Status] ウィンドウを使用して、表示することを許可されているデバイスのデバイス プロパティおよびステータスを表示します。このウィンドウでは、個々のデバイスごとにデバイス プロパティを開かなくても済むように、デバイス情報の概要が示されます。

デバイス プロパティ情報に加え、各デバイスのポリシーの設定方法（ローカル、共有、または未設定）および各デバイスのオーバーライドを持つポリシー オブジェクトに関する概要情報を表示できます。デバイスへの設定展開のステータスを表示することもできます。

[Inventory Status] ウィンドウには、2 つのペインがあります。上部のペインを使用して、すべてのデバイスの一覧を表示したり、属性をデバイスでソートしたり、特定のデバイスを除外したりします。下部のペインを使用して、上部のペインで選択したデバイスのデバイス プロパティの詳細を表示します。

ナビゲーション パス

[ツール（Tools）] > [インベントリステータス（Inventory Status）] を選択します。

関連項目

- インベントリ ステータスの表示 （22 ページ）
- 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

フィールド リファレンス

表 5 : [Inventory Status] ウィンドウ

要素	説明
すべてのデバイスのデバイス概要情報（上部のペイン）	
[Export] ボタン	インベントリを Comma-Separated Values（CSV; カンマ区切り値）ファイルとしてエクスポートするには、このボタンをクリックします。ファイル名を指定して、Security Manager サーバ上のフォルダを選択するように求められます。エクスポート ファイルは参照または分析に使用できます。
表示名	Security Manager に表示されるデバイス名。
展開	デバイスの設定展開のステータス。
OS タイプ	デバイスで実行されているオペレーティング システムのファミリ。IOS、IPS、ASA、FWSM、PIX など。
実行中 OS のバージョン	デバイスで実行されているオペレーティング システムのバージョン。

要素	説明
ターゲットOSバージョン	設定を適用するターゲットOSバージョン。設定は、このバージョンでサポートされているコマンドに基づきます。
Host Name.Domain Name	デバイスの DNS ホスト名および DNS ドメイン名。
IP Address	デバイスの管理 IP アドレス。
デバイスタイプ	デバイスのタイプ。
選択したデバイスの詳細（下部のペイン） 詳細情報が下部のペインのタブに表示されます。情報はフォルダに整理されています。[+]または[-]アイコンをクリックして、フォルダを開いたり閉じたりします。または、フォルダ名をダブルクリックします。	
インベントリ	選択したデバイスのデバイスプロパティ、展開方法、デバイスグループメンバーシップ、およびモジュールの親デバイスに関する概要情報が表示されます。
ポリシー	選択したデバイスに対して設定できるポリシーの現在のステータスが表示されます。ポリシーのステータスは、未割り当て（未定義）、ローカル ポリシー、または共有ポリシーです。
Policy Object Overrides	選択したデバイスに対して定義されたオーバーライドを持つポリシー オブジェクトが表示されます。ポリシー オブジェクト オーバーライドの詳細については、ポリシー オブジェクト オーバーライドのページを参照してください。
ステータス	選択したデバイスに対する展開ステータスメッセージが表示されます。 イベントはイベントタイプ別に整理されています。イベントの詳細には、タイムスタンプ、説明、および推奨するアクションが含まれています。タイムスタンプは、デバイスの最新のポーリング時刻ではなく、デバイスのステータスが最後に変更された時刻です。 ステータスメッセージの最も高い重大度レベルも表示されます。
ナビゲーション ボタン	インベントリ リスト内を移動するには、ナビゲーション ボタンをクリックします。ボタンの意味は、左から右の順で、リスト内の最初のデバイスに移動、前のデバイスに移動、次のデバイスに移動、最後のデバイスに移動です。中央のフィールドに、現在選択されているデバイスが行番号で示されます（たとえば、5/10は、リスト内の10個のデバイスのうちの5番めを意味します）。

デバイス マネージャの起動

デバイスマネージャを起動して、Security Manager からデバイスの設定とステータスを表示できます。ASA、ASA-SM、PIX、FWSM、IPS、およびIOS の各デバイスのデバイス マネージャを起動できます。

各デバイス マネージャには、デバイス上で実行されているサービスに関する情報およびシステムの全体的なヘルスのスナップショットを提供する複数のモニタリングおよび診断機能が含まれています。これらのデバイス マネージャを使用して、既存のデバイス設定の表示および現在のステータスのモニタを行うことができますが、デバイスに設定変更を適用することはできません。

（注） IPS 仮想センサーに対してデバイス マネージャを起動することはできません。

（注） Cisco Security Manager 4.16 では、JRE 1.7 ビルド 161 のアップグレードにより、一部の古いアプレットへのサポートが廃止されました。したがって、Cisco Security Manager 4.16 以降、PIX 6.3、IDS/IPS バージョン 5.x ～ 7.x、および FWSM 2.x を直接起動することはできません。

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

デバイスマネージャを起動するには、デバイスビューでデバイスを選択し、右クリックして [デバイスマネージャ（Device Manager）] を選択します。**[起動（Launch）] > [デバイスマネージャ（Device Manager）]** を選択してデバイスマネージャを起動することもできます。（これらのコマンドは、ASA CX デバイスを選択するとディセーブルになり、**Prime Security Manager** のコマンドがイネーブルになります。Cisco Prime Security Manager は、ASA CX デバイスの設定と管理に使用されます。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （33 ページ） を参照してください）。

Security Manager からデバイス マネージャを起動すると、デバイス マネージャ実行ファイルがクライアント システムにダウンロードされます。ネットワーク デバイスにデバイス マネージャをインストールする必要はありません。デバイス マネージャを最初に起動するときは、ソフトウェアをワークステーションにダウンロードするのに時間がかかります（経過表示バーが表示されます）（問題が発生した場合は、デバイス マネージャのトラブルシューティング （27 ページ）のヒントを確認してください）。

Security Manager によって、ネットワーク デバイス上で実行されているオペレーティング システムに基づいて、最適なデバイス マネージャ バージョンが選択されます。選択されたデバイ

スとのその後の通信は、ユーザにはまったく意識されません。接続はSecurity Managerサーバーを介して行われます。つまり、Security Manager サーバーはプロキシサーバーとして機能します。Security Manager からデバイス マネージャを起動することによって、クライアント システムとモニタ対象デバイスとの間で HTTPS 接続を開く必要がなくなります。

ヒント　デバイスマネージャ セッションを開始すると、Security Managerによって、デバイスで実行されているオペレーティング システム ソフトウェア バージョンに適切なマネージャのバージョンが開かれます（詳細については、「ASA and ASDM Compatibility Per Model」を参照してください）。ただし、使用している Security Manager バージョンのリリースよりもあとに新しいデバイス マネージャ バージョンがリリースされた場合、Security Managerによって、利用できる最新のデバイス マネージャ バージョンが開かれない場合があります。デバイスマネージャを起動するときは、そのバージョンを確認してください（たとえば、デバイスマネージャ ウィンドウで **[ヘルプ（Help）] > [バージョン情報（About）]** を選択します）。必要な機能を備えた、さらに新しいデバイスマネージャが使用可能な場合、その新機能を使用するには、Security Manager 以外でそのデバイスマネージャをインストールして使用する必要があります。

デバイスで実行されている外部デバイスマネージャを使用してデバイス設定を直接変更する場合、これらの変更は Security Manager によってアウトオブバンドと見なされ、次に Security Manager から設定を展開するときに上書きされる場合があることに注意してください。アウトオブバンド変更の詳細と、アウトオブバンド変更の識別および再作成については、次の項を参照してください。

- アウトオブバンド変更の処理方法について
- アウトオブバンド変更の検出および分析

Security Manager では、デバイスごとにデバイスマネージャのインスタンスが 1 つだけ起動されます。Security Managerを終了するか、アイドルセッションのタイムアウト時間が過ぎると、デバイスマネージャは終了します。複数のデバイス マネージャ ウィンドウを（異なるデバイスに接続して）同時に開くことができます。

次の表に、Security Manager から起動できるデバイス マネージャの概要を示します。

表 *6 : Security Manager* で使用可能なデバイス マネージャ

Device Manager	説明
IDM	IPS Device Manager（IDM）を使用すると、Security Manager インベントリの一部である IPS センサーおよびモジュールをモニタできます。 このデバイスマネージャの使用方法の詳細については、IDM のマニュアルを参照してください。

Device Manager	説明
PDM	PIX Device Manager（PDM）を使用すると、PIX 6.x デバイスおよび初期の FWSM（つまり、シングル コンテキスト モードまたはマルチ コンテキスト モードの FWSM リリース 1.1、2.2、および 2.3）をモニタできます。 このデバイスマネージャの使用方法の詳細については、PDM のマニュアルを参照してください。
ASDM	Adaptive Security Device Manager（ASDM）を使用すると、ASA、ASA-SM、PIX 7.x 以降、および FWSM 3.x 以降のデバイスをモニターできます。 このデバイスマネージャの使用方法の詳細については、ASDM のマニュアルを参照してください。
SDM	Security Device Manager（SDM）を使用すると、Cisco IOS ベースのリソースをモニタできます。SDM では、シスコ デバイスまたは Cisco コマンドライン インターフェイス（CLI）に関するこれまでの経験は必要ありません。Cisco SDM では、広範囲の Cisco IOS ソフトウェア リリースがサポートされます。 このデバイスマネージャの使用方法の詳細については、SDM のマニュアルを参照してください。

次の項では、デバイスマネージャのトラブルシューティングおよび使用について詳細に説明します。

- デバイス マネージャのトラブルシューティング （27 ページ）
- デバイス マネージャからのアクセス ルールの検索 （29 ページ）
- ASDM からアクセス ルールへのナビゲート （30 ページ）
- SDM からアクセス ルールへのナビゲート （32 ページ）

デバイス マネージャのトラブルシューティング

設定をデバイスに正常に展開できた場合、Security Manager でデバイスとのデバイス マネージャ セッションを開くことができます（デバイス マネージャの起動 （25 ページ）を参照）。

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

ただし、接続の確立または開かれたセッションの使用に問題がある場合は、次のトラブルシューティングに関するヒントを考慮してください。ヒントは、基本的なヒントと複数のデバイスマネージャの使用に関するヒントに分かれています。

デバイス マネージャのトラブルシューティングに関する基本的なヒント

- 一般に、Security Managerインベントリでデバイス用に設定されているクレデンシャルが、デバイスマネージャの起動に使用されます。ただし、SDMのいくつかのバージョンでは、デバイスマネージャの起動時にユーザ名およびパスワードを入力する必要があります。デバイスのクレデンシャルがないか、または有効ではないというエラーが表示された場合は、デバイスにログインできるユーザ名およびパスワードを使用して、[Device Properties Credentials] ページを更新します。デバイスビューで、デバイスを右クリックして、[デバイスプロパティ（Device Properties）] を選択します。詳細については、デバイス プロパティの表示または変更および[Device Credentials] ページを参照してください。
- CiscoWorks Common Services ロールのいずれかに関連付けられているすべてのユーザには、Security Manager からデバイス マネージャを起動する権限があります。ただし、Help Desk ロールと、定義済みのすべての Cisco Secure ACS ロールを除きます。適切な権限があることを確認してください。
- Security Manager とデバイス間のセキュアな通信を実現するには、SSL/HTTPS がターゲット デバイスでイネーブルである必要があります。デバイスで SSL がイネーブルになっていない場合、エラーメッセージが表示されます。詳細については、デバイスの通信要件についてを参照してください。
- デバイスマネージャサービス（**xdm-launcher.exe**）を起動するには、Security Manager システムおよびワークステーションで、Cisco Security Agent またはその他のアンチウイルスやネットワーク ファイアウォール ソフトウェアの変更が必要となる場合があります。
- ターゲット デバイスへのアクセスおよび通信に関して Security Manager が正しく設定されていることを確認します。特に、アイデンティティ、オペレーティング システム、クレデンシャルなどのデバイスのプロパティを確認します。目的のデバイスを選択し、右クリックして [デバイスプロパティ（Device Properties）] を選択します。[General] および [Credentials] ページで設定を確認します。[クレデンシャル（Credentials）] タブを選択して [接続のテスト（Test Connectivity）] をクリックすることにより、Security Manager がデバイスに接続できるかどうかをテストできます（デバイス接続のテストを参照）。

（注） [デバイスプロパティ（Device Properties）] の [全般（General）] タブの [オペレーティングシステム（Operating System）] フレームにある [実行中のOSのバージョン（Running OS Version）] フィールドが空白のときにパケットトレーサーを実行すると、CSMは、[実行中のOSのバージョン（Running OS Version）] フィールドを使用してデバイスのライブネスを正しくチェックできず、ASA デバイスが停止していると見なします。

- デバイス マネージャは、トランスペアレント モード（レイヤ 2 ファイアウォール）またはルーテッド モード（レイヤ 3 ファイアウォール）で実行されており、1 つのセキュリティ コンテキストまたは複数のセキュリティ コンテキストをサポートしている FWSM および ASA に対して起動できます。複数のセキュリティ コンテキストを実行している FWSM

およびASAデバイスの場合、セキュリティ コンテキストごとに一意の管理IPアドレスを定義する必要があります。

- プラットフォームがデバイスマネージャの起動に対してサポートされていないというメッセージが表示されたが、このガイドの情報ではプラットフォームはサポートされている場合、デバイスで実行されているオペレーティングシステムのバージョンと、使用しているSecurity Manager ソフトウェアのバージョンを考慮してください。最近のオペレーティングシステムを使用しているが、比較的古いバージョンの Security Manager を使用している場合は、Security Managerをアップグレード（またはサービスパックを適用）するか、Cisco Technical Support に問い合わせるか、あるいは最新のデバイスマネージャをネットワークデバイスにインストールしてSecurity Manager以外で使用する必要があることがあります。Security Manager以外でデバイス マネージャを使用する前に、デバイス マネージャの起動（25 ページ）でアウトオブバンド変更に関する情報を確認してください。

複数のデバイス マネージャ セッションのトラブルシューティングに関するヒント

- 複数のデバイス マネージャを起動すると、Security Manager サーバとクライアントの両方のパフォーマンスに影響することがあります。クライアントでは、メモリ要件およびパフォーマンスへの影響は、起動されるデバイス マネージャの数に比例します。サーバでは、デバイスマネージャの起動またはデバイスからの最新情報の取得に対する大量の要求が、パフォーマンスに悪影響を及ぼす可能性があります。
- すべてのクライアントから 1 つのデバイスに対して確立できる永続的な HTTPS 接続の最大数は、デバイスのタイプおよびモデルによって異なります。この制限を超えようとすると、エラー メッセージが表示されます。

たとえば、1 つの PIX 6.x では、複数のクライアントがそれぞれ 1 つのブラウザ セッションを開くことができ、最大 16 個の同時 PDM セッションがサポートされます。FWSM（1.1、2.2、または 2.3）では、モジュール全体で最大 32 個の PDM セッションと、コンテキストごとに最大 5 つの同時 HTTPS 接続が許可されます。

個別の制限については、該当するデバイスの資料を参照してください。

デバイス マネージャからのアクセス ルールの検索

アクセス ルールのセットが、各デバイス インターフェイスに関連付けられています。これらのルールは、順序が付けられたリストまたは表の形式で提供されます。このリストは Access-Control List（ACL; アクセス コントロール リスト）と呼ばれ、リスト内の各ルールは Access-Control Entry（ACE; アクセス コントロール エントリ）と呼ばれます。パケットを転送するかドロップするかを決定するときに、デバイスは、リストされている順序で各アクセス ルールに照らしてパケットをテストします。ルールが一致した場合、デバイスは指定されたアクションを実行します。その後の処理のためにデバイスへのパケットを許可するか、エントリを拒否します。パケットがどのルールとも一致しない場合、パケットは拒否されます。

ファイアウォールまたはルータでのアクティビティは、syslog メッセージを使用してモニタできます。デバイスでロギングがイネーブルの場合、syslog メッセージを生成するように設定さ

れたアクセス ルールが一致すると（たとえば、拒否されている IP アドレスから接続が試行された場合）、ログ エントリが生成されます。

（注） デバイスでログ エントリを生成するには、デバイスでロギングをイネーブルにする必要があります（ASA/PIX デバイスの場合は[Logging Setup] ページ、IOS デバイスの場合はロギング ポリシー（Cisco IOS ルータにおけるロギングを参照））。また、一致した場合にログ メッセージを生成するように個々のアクセス ルールを設定する必要があります（[Advanced]/[Edit Options] ダイアログボックスを参照）。

Security Manager から起動するデバイスマネージャで syslog メッセージをモニタリングできます。一部のデバイスマネージャでは、特定のメッセージを生成した Security Manager のアクセスルールをモニタリングウィンドウから検索できます。syslog エントリをトリガーしたアクセス ルールは、複数の一致があった場合でも、最初に一致したものが Security Manager で強調表示されます。

このアクセスルール検索は、IOS を実行しているすべての管理対象ルータの場合は SDM で使用可能であり、管理対象 PIX およびバージョン 8.0(3) 以降の ASA デバイス（ASA-SM を含む）、および FWSM バージョン 3.1 以降を実行しているデバイスの場合は ASDM で使用可能です。

次の項では、デバイス マネージャから Security Manager のアクセス ルールを検索する方法について説明します。

- ASDM からアクセス ルールへのナビゲート （30 ページ）
- SDM からアクセス ルールへのナビゲート （32 ページ）

ASDM からアクセス ルールへのナビゲート

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

Security Manager から起動された ASDM デバイス マネージャでは、[Real-time Log Viewer] ウィンドウおよび [Log Buffer] ウィンドウでシステム ログ メッセージをモニタできます。いずれかのウィンドウで表示された syslog メッセージを選択し、メッセージをトリガーした Security Manager のアクセス コントロール ルールにナビゲートして、必要に応じてルールを更新できます。

[Real-time Log Viewer] は、syslog メッセージが記録されたときにそれを表示できる独立したウィンドウです。独立した [Log Buffer] ウィンドウでは、syslog バッファ内に存在するメッセージを表示できます。

次の syslog メッセージ ID に関連付けられたアクセス ルールを検索できます。

- 106023：アクセスルールによってIPパケットが拒否されたときに生成されます。このメッセージは、ルールに対してロギングがイネーブルになっていない場合にも表示されます。
- 106100：一致したアクセスルールに対してロギングがイネーブルの場合（[Advanced]/[Edit Options] ダイアログボックスを参照）、このメッセージは、設定されているパラメータに応じて、トラフィックフローに関する情報を提供します。このメッセージは、拒否されたパケットだけを記録するメッセージ 106023 よりも多くの情報を提供します。

次の手順では、ASDM の [Real-time Log Viewer] または [ログバッファ（Log Buffer）] ウィンドウから Security Manager のアクセスルールを検索する方法について説明します。

関連項目

- デバイス マネージャからのアクセス ルールの検索 （29 ページ）
- SDM からアクセス ルールへのナビゲート （32 ページ）

ステップ 1 Security Manager デバイス インベントリで、PIX、ASA、ASA-SM または FWSM を選択します。

ステップ 2 [起動（Launch）] > [デバイスマネージャ（Device Manager）] を選択して ASDM を開始します。デバイスマネージャの起動の詳細については、デバイス マネージャの起動 （25 ページ）を参照してください。

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

ステップ 3 [ASDM] ウィンドウで、[モニタリング（Monitoring）] ボタンをクリックして [モニタリング（Monitoring）] パネルを表示します。左側のペインで [ロギング（Logging）] をクリックして、ログ表示オプションにアクセスします。

ステップ 4 [Real-time Log Viewer] または [ログバッファ（Log Buffer）] を選択します。

ステップ 5 [表示（View）] ボタンをクリックして、選択したログ表示ウィンドウを開きます。

（注） デバイスでロギングがイネーブルになっていない場合、[View] ボタンは表示されません。

ウィンドウに表示される各 syslog メッセージには、メッセージ ID 番号、メッセージが生成された日時、ロギング レベル、およびパケットが送受信されたネットワーク アドレスまたはホスト アドレスが含まれています。

ステップ 6 特定の syslog メッセージをトリガーしたアクセス ルールを表示するには、メッセージを選択し、ASDM ツールバーの [ルールの表示（Show Rule）] ボタンをクリックします（または、メッセージを右クリックして、ポップアップメニューから [CSMのルールに移動（Go to Rule in CSM）] を選択します）。

Security Manager クライアント ウィンドウがアクティブになり、[Access Rules] ページが表示されます。このページでは、ルール テーブル内のルールが強調表示されます。syslog エントリが現在の Security Manager アクティビティで参照されていないアクセス ルールによってトリガーされた場合、エラー メッセージが表示されます。

SDM からアクセス ルールへのナビゲート

Security Manager から起動された SDM デバイス マネージャでは、[Logging] ウィンドウの [Syslog] タブで、セキュリティ レベルで分類されたイベントのログを表示できます。syslog メッセージを選択し、メッセージをトリガーした Security Manager のアクセス コントロール ルールにナビゲートして、必要に応じてルールを更新できます。

SDM の [Monitor] > [Logging] オプションには、4 つのログ タブがあります。そのうち [Syslog] だけに、Security Manager アクセス ルール検索オプションがあります。ルータには、重大度レベルで分類されたイベントのログが含まれています。ログ メッセージが syslog サーバに転送されている場合でも、[Syslog] タブにはルータ ログが表示されます。

Cisco IOS デバイスでは、syslog メッセージは **log** または **log-input** キーワードを使用して設定されたアクセスルール用に生成されます。**log** キーワードでは、パケットがルールと一致したときにメッセージが生成されます。**log-input** キーワードでは、パケットの送信元および宛先 IP アドレスとポートに加えて、入力インターフェイスおよび送信元 MAC アドレスを含むメッセージが生成されます。同一のパケットが一致すると、メッセージは、直近の 5 分間に許可または拒否されたパケット数によって、5 分間隔で更新されます。

次の手順では、SDM の [ロギング（Logging）] パネルの [Syslog] タブから Security Manager のアクセスルールを検索する方法について説明します。

関連項目

- デバイス マネージャからのアクセス ルールの検索 （29 ページ）
- ASDM からアクセス ルールへのナビゲート （30 ページ）

ステップ 1 Security Manager デバイス インベントリで、IOS ルータを選択します。

ステップ 2 [起動（Launch）] > [デバイスマネージャ（Device Manager）] を選択して ASDM を開始します。デバイス マネージャの起動の詳細については、デバイス マネージャの起動 （25 ページ）を参照してください。

ステップ 3 [SDM] ウィンドウで、[モニタリング（Monitoring）] ボタンをクリックして [モニタリング（Monitoring）] パネルを表示します。左側のペインで [ロギング（Logging）] をクリックして、ログ表示オプションにアクセスします。

[Syslog] タブが表示された [Logging] ペインが表示されます。

ステップ 4 特定の syslog メッセージをトリガーしたアクセスルールを表示するには、メッセージを選択し、ログメッセージの表の上にある [CSMのルールに移動（Go to Rule in CSM）] ボタンをクリックします。

Security Manager クライアント ウィンドウがアクティブになり、[Access Rules] ページが表示されます。このページでは、ルール テーブル内のルールが強調表示されます。syslog エントリが現在の Security Manager アクティビティで参照されていないアクセス ルールによってトリガーされた場合、エラー メッセージが表示されます。

Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動

ASA CX は、高度なコンテキスト認識型セキュリティを実現する適応型セキュリティ アプライアンス モジュールであり、ASA プラットフォームを拡張して、アプリケーションの可視性と制御（「誰が、何を、どこで、いつ、どのように」についての詳細）を提供します。ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、および高度なマルウェア防御（AMP）などの次世代ファイアウォール サービスを提供します。

ASA CX デバイスは Cisco Prime Security Manager（PRSM）アプリケーションによって管理され、ASA FirePOWER モジュールは FireSIGHT Management Center アプリケーションによって管理されます。Cisco Security Manager で直接管理することはできません。とはいえ、Security Manager が拡張され、ASA デバイスでこれらのモジュールの存在を検出できるようになりました。Configuration Manager アプリケーションから PRSM と FireSIGHT Management Center を「クロス起動」したり、Security Manager と PRSM の間でポリシーオブジェクトデータを共有したりすることができます。

（注） PRSM と FireSIGHT Management Center はブラウザベースのアプリケーションです。つまり、ブラウザウィンドウ内で起動および動作します。そのため、Configuration Manager クライアントから PRSM または FireSIGHT Management Center をクロス起動すると、ホストシステムのデフォルトブラウザが開き、管理アプリケーションが開始されます。ただし、一部のブラウザは PRSM または FireSIGHT Management Center で認定されていないため、クロス起動の前に Security Manager クライアントのホストシステムでデフォルトのブラウザを変更しなければならない場合があります。詳細については、PRSM または FireSIGHT Management Center インストールガイドの「ブラウザ要件」を参照してください。

はじめる前に

PRSM または FireSIGHT Management Center を相互起動するには、Security Manager がモジュールの存在を認識している必要があります。そのような認識は、新しい ASA デバイス、または既存の ASA に追加されたモジュールのいずれかを検出することによって達成されます。このプロセスについては、ASA CX モジュールおよび FirePOWER モジュールの検出 （34 ページ）で概説されています。

また、「シングルサインオン」（SSO）を有効にして設定すると、Security Manager ユーザーがアプリケーションに別個にログインすることなく、PRSM または FireSIGHT Management Center に直接アクセスできるようになります。これを可能にするには、両方のアプリケーションで適切なユーザーログイン情報を定義する必要があります（PRSM または FireSIGHT Management Center の相互起動に SSO は必要ないことに留意してください）。詳細については、Security Manager の[シングルサインオンの設定（Single Sign-on Configuration）]ページと、『*User Guide for ASA CX and Cisco Prime Security Manager*』（『Cisco ASA CX Context-Aware Security End-User Guides』）の「Configuring Single Sign-On for Cisco Security Manager」を参照してください。

関連項目

- [シングルサインオンの設定（Single Sign-on Configuration）] ページ
- ASA CX モジュールおよび FirePOWER モジュールの検出 （34 ページ）
- PRSM とのデバイスインベントリおよびポリシーオブジェクトの共有 （36 ページ）

ASA CX デバイスまたは FirePOWER モジュールをモニタリングおよび管理するには、PRSM または FireSIGHT Management Center をクロス起動します。

ステップ 1 Configuration Manager のデバイスビューで、デバイスセレクタツリーまたはコンテンツ領域のデバイスのテーブルで、以前に検出された ASA CX デバイスまたは ASA with FirePOWER モジュールを選択します。

繰り返しになりますが、Security Manager での ASA CX デバイスまたは FirePOWER モジュールの検出については、 ASA CX モジュールおよび FirePOWER モジュールの検出 （34 ページ） で説明しています。

ステップ 2 選択したデバイスを右クリックし、ポップアップメニューから [Prime Security Manager] または [FireSIGHT Management Center] を選択します。または、Configuration Manager の [起動（Launch）] メニューからも [Prime Security Manager] や [FireSIGHT Management Center] を選択できます（これらのコマンドは、ASA CX、または FirePOWER モジュールを備えた ASA を選択した場合にのみ使用できます）。

ブラウザベースの PRSM または FireSIGHT Management Center のウィンドウが表示され、選択したデバイスのデバイス画面が表示されます。

（注） Security Manager が PRSM を起動するために使用する URL には、CX モジュールの管理 IP アドレス（デバイス検出中に取得）が組み込まれており、文字列 /admin/mgmt?rtp が含まれています。相互起動中に、このタイプの要求は、適切な PRSM 中央サーバーが存在する場合、そのサーバーにリダイレクトされます。それ以外の場合は、PRSM の「オンボックス」バージョンが起動されます（オンボックスバージョンの PRSM を自分で直接起動するには、ブラウザのアドレスフィールドに **https://***<management_IP_address>* と入力する必要があります。ここで *<management_IP_address>* は、目的の CX モジュールの管理アドレスです）。

PRSM の使用に関する情報は、cisco.com の『Cisco ASA CX Context-Aware Security End-User Guides』ページにあり、FireSIGHT Management Center の使用に関する情報は、cisco.com の『Cisco FireSIGHT Management Center』ページにあります。

ASA CX モジュールおよび FirePOWER モジュールの検出

Security Manager と PRSM の間でポリシーオブジェクトデータを共有し、Configuration Manager から PRSM または FireSIGHT Management Center を相互起動するには、Security Manager がモジュールを確実に認識している必要があります。

デバイスインベントリへのデバイスの追加で説明しているように、新規デバイスウィザードで関連するオプションを選択して新しい ASA デバイスを検出すると、CX モジュールまたは FirePOWER モジュールの検出が自動的に行われます。

すでにインベントリにある ASA デバイスに CX モジュールまたは FirePOWER モジュールを追加すると、次のように、ホスト ASA の既存のポリシーに影響を与えずに新しいモジュールを検出できます。

1. Configuration Manager のデバイスセレクタツリーで 1 つ以上の ASA デバイスを選択します。

   一度に複数のモジュールを検出できます。ASA ではないデバイス、または CX または FirePOWER モジュールを含まない ASA であるデバイスが選択されている場合、それらは無視されます。

2. 選択したデバイスを右クリックし、ポップアップメニューから [ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）] を選択します。

   [検出タスクの作成（Create Discovery Task）] ダイアログボックスまたは [バルク再検出（Bulk Rediscovery）] ダイアログボックスが表示され、[ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）] オプションが選択されています。他の検出オプションは使用できません。

   このダイアログボックスの使用方法の詳細は、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックスを参照してください。

3. [検出タスクの作成（Create Discovery Task）] ダイアログボックスで [OK] をクリックするか、[バルク再検出（Bulk Rediscovery）] ダイアログボックスで [完了（Finish）] をクリックしてダイアログボックスを閉じ、モジュールの検出を開始します。

   検出によって既存のポリシーが置き換えられるという警告が表示される場合があります。[はい（Yes）] をクリックして警告を閉じ、続行できます。

   [検出ステータス（Discovery Status）] ダイアログボックスが自動的に開き、検出の進行状況が表示されます。このプロセスの詳細については、ポリシー検出タスクのステータスの表示を参照してください。

CX モジュールまたは FirePOWER モジュールが ASA で検出されると、モジュール自体の管理 IP アドレスが取得され、[デバイスのプロパティ（Device Properties）] ウィンドウの [ASA-CX/FirePOWERモジュール（ASA-CX/FirePOWER Module）] セクションが更新されます。[デバイスのプロパティ（Device Properties）]：[全般（General）] ページを参照してください。管理 IP アドレスは、PRSM または FireSIGHT Management Center を相互起動するために使用されます。（Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （33 ページ）で説明しているように、Cisco Prime Security Manager（PRSM）は ASA CX デバイスの設定と管理に使用されるアプリケーションであり、FireSIGHT Management Center は ASA FirePOWER モジュールの設定と管理に使用されるアプリケーションです）。

（注） Security Manager が PRSM を起動するために使用する URL には、CX モジュールの管理 IP アドレス（デバイス検出中に取得）が組み込まれており、文字列 /admin/mgmt?rtp が含まれています。相互起動中に、このタイプの要求は、適切な PRSM 中央サーバーが存在する場合、そのサーバーにリダイレクトされます。それ以外の場合は、PRSM の「オンボックス」バージョンが起動されます。（オンボックスバージョンの PRSM を自分で直接起動するには、ブラウザのアドレスフィールドに **https://**<*management_IP_address*> と入力する必要があります。ここで <*management_IP_address*> は、目的の CX モジュールの管理アドレスです。）

検出プロセスが完了すると、CX モジュールがインストールされているすべての ASA は、さまざまな Security Manager 画面に、次の PRSM アイコンを提示したり含めたりして示されます。

。たとえば、デバイスセレクタでは、次の ASA CX アイコンが使用されます。

注意 また、選択したデバイスの右クリックメニューから [デバイス上のポリシーを検出（Discover Policies on Device(s)）] を選択するか、[ポリシー（Policy）] メニューから [デバイス上のポリシーを検出（Discover Policies on Device）] を選択して、既存の ASA における CX モジュールまたは FirePOWER モジュールの存在を検出することもできます。選択したデバイスの数と選択したコマンドに応じて、[検出タスクの作成（Create Discovery Task）] ダイアログボックスまたは [バルク再検出タスク（Bulk Rediscovery Task）] ダイアログボックスが開き、すべての検出、再検出オプションが使用可能になります。つまり、選択したデバイスですでに確立されている共有ポリシーを上書する可能性があります。既存のポリシーを確実に再検出する場合を除き、[ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）] を除くすべてのオプションの選択を解除してください。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出を参照してください。

PRSM とのデバイスインベントリおよびポリシーオブジェクトの共有

Cisco Security Manager の定義に従い Cisco Prime Security Manager（PRSM）にインポートするために、現在のデバイスインベントリおよびポリシーオブジェクトのセットをエクスポートできます。

デバイス インベントリのエクスポート

Cisco Security Manager デバイスインベントリを PRSM と共有するには、デバイス インベントリのエクスポートの説明に従い、インベントリをカンマ区切り値（CSV）ファイルとしてエク

スポートします。エクスポートファイルのフォーマットタイプには、必ず「Cisco Security Manager」を指定してください。

ネットワーク/ホストおよびサービスポリシーオブジェクトのエクスポート

PRSM にインポートするために、Cisco Security Manager ポリシーオブジェクト、具体的にはネットワーク/ホストオブジェクト、またはサービスオブジェクトをエクスポートするには、Cisco Security Manager サーバーホストで Perl スクリプトを実行して CSV ファイルを作成する必要があります（PRSM はポートリストオブジェクトをサポートしていません）。

Perl スクリプトは Cisco Security Manager サーバーのインストールに含まれており、その使用方法については、ポリシーオブジェクトのインポートおよびエクスポートを参照してください。基本的な手順は次のとおりです。

1. Cisco Security Manager サーバーを実行しているコンピュータにログインし、Cmd ウィンドウを開き、Perl スクリプトの場所に移動してから、コマンドプロンプトで Perl スクリプトコマンドを実行します。

ネットワーク/ホストオブジェクトをエクスポートするために使用されるコマンドの例を次に示します。perl PolicyObjectImportExport.pl -u *user* -p *password* -o export -t network -f C:\CSM_Net_objects.csv -e true

1. CSV ファイルを PRSM クライアントシステムにコピーします。

このファイルは、必要に応じて編集できます。

1. PRSM を起動し、CSV ファイルをインポートします。このプロセスの詳細については、PRSM ユーザーガイドの「Managing Policy Objects」の章にある「Importing Objects」セクションを参照してください。

Packet Tracer を使用した ASA または PIX の設定の分析

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

パケットトレーサは、ルーテッドモードで稼働していない、バージョン 7.2.1 以降を実行している ASA および PIX セキュリティアプライアンス用のポリシーデバッグツールです。

パケットトレーサは、アプライアンスで現在実行されているアクティブなポリシーを検査します。実際のトラフィックを生成しなくても、2 つのアドレス間でトラフィックがセキュリティアプライアンスをどのように通過するか（ドロップまたは許可）を分析できます。結果が予期しないものである場合は、問題がある場所を判別し、Security Manager で対応するポリシーを更新して解決できます。

パケットトレーサは、セキュリティアプライアンスのアクティブな設定による、シミュレートされたパケットの処理方法を段階的に分析します。また、ルートルックアップ、アクセスリス

ト、NAT 変換、VPN など、アクティブなファイアウォールモジュールを通過するパケットのフローをトレースします。アクティブなモジュールのセットは、設定されているパケットのタイプとアクティブな設定に基づいて変わります。たとえば、VPN ポリシーが設定されていない場合、VPN モジュールは評価されません。

ネットワークトラフィックを生成する代わりに、シミュレートされたパケットの通過を検査し、syslog メッセージを有効にして、生成される syslog メッセージを手動で確認できます。Packet Tracer では、パケットでアクティブな設定によって実施されたアクションが詳細に示されます。コンフィギュレーション コマンドによってパケットがドロップされた場合、「Drop-reason: (telnet-not-permitted) Telnet not permitted on least secure interface」などの理由が示されます。

セキュリティアプライアンスを通過するシミュレートされたパケットの寿命をトレースして、パケットの動作が予期したとおりかどうかを確認できます。Packet Tracer の用途は、次のとおりです。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用されるすべてのルール（ルールを定義する CLI を含む）を表示します。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスでパケットをトレースします。
- 明示的なアクセス ルールによってパケットがブロックまたは許可されている場合、ルールを編集できるように、ショートカットを使用してポリシーに移動できます。

ヒント：

- Packet Tracer は ASDM アプリケーションおよび ASA コマンドラインでも使用でき、Security Manager のバージョンは ASDM のバージョンと同じです。ASDM および CLI からパケットトレーサを使用して設定を分析する例については、「PIX/ASA 7.2(1) 以降：インターフェイス内通信」を参照してください。
- デバイスに対して Packet Tracer を使用する前に、デバイスをインベントリに追加したあとで少なくとも 1 回はポリシー変更を送信する必要があります。
- Packet Tracer では、デバイスで実行されているアクティブな設定だけが分析されます。このため、提案された設定がデバイスに展開されて実行される前に、Packet Tracer を使用してテストすることはできません。設定変更が保留中のデバイスで Packet Tracer を使用しないでください。変更を展開してから Packet Tracer を使用して、Packet Tracer の結果が有効になるようにしてください。

Packet Tracer を使用するには、次の手順を実行します。

ステップ 1 （デバイスビュー）ASA または PIX 7.2.1 以降のデバイスを右クリックし、ショートカットメニューで [パケットトレーサ（Packet Tracer）] を選択して [パケットトレーサ（Packet Tracer）] ウィンドウを開きます。

ステップ 2 [インターフェイス（Interfaces）] リストから、テストするインターフェイスを選択します。このリストには、デバイスで定義されているすべてのインターフェイスが含まれています。

ステップ 3 次のフィールドを設定して、トレースするパケットをモデル化します。

- [パケットタイプ（Packet Type）]：トレースするパケット（TCP、UDP、ICMP、IP、または ESP）を選択します。

（注） 4.16 以降、Cisco Security Manager は ASA 9.9.1 デバイスからの ESP パケットのトレースをサポートしています。

- [送信元、宛先IPアドレス（Source, Destination IP Address）]：次のアドレスタイプから選択し、通信（送信元から宛先へ）の両端のホスト IP アドレスを入力します。
  - ホストの IP アドレスIPv4 または IPv6 アドレスを使用できます。IPv6 を使用したパケットトレーサは、8.4(2) より前の ASA ソフトウェアバージョンを実行しているデバイスではサポートされていません。
  - ユーザ（送信元のみ）。例：DOMAIN\Administrator。ユーザーにマップされた IP アドレスがトレースに使用されます。このタイプのアドレスを使用するには、アイデンティティ オプションを設定することにより、アイデンティティ対応のファイアウォールを有効にする必要があります。
  - ホストの FQDN、つまり完全修飾ドメイン名。例：host.example.com。このタイプのアドレスを使用するには、DNS を設定する必要があります。
  - セキュリティ名（ASA 9.x 以降のみ）。
  - セキュリティタグ（ASA 9.x 以降のみ）。
- [送信元、宛先ポート（TCPおよびUDPのみ）（Source, Destination Port (TCP and UDP only)）]：トラフィックタイプを表すポート番号を入力（または選択）します。選択リストでは、指定アプリケーションの標準ポート番号と一致する名前が使用されています。たとえば、**http** を選択することと、**80** を入力することは同じです。
- [タイプ、コード、 ID（ICMPのみ）（Type, Code, ID (ICMP only)）]：ICMP パケットをモデル化する場合、次のフィールドすべてに値を入力する必要があります。
  - [タイプ（Type）]：ICMP パケットタイプを選択するか、同等の番号を入力します。リストには、主要な ICMP タイプがすべて含まれています。タイプと関連するコードの一覧については、http://www.ietf.org/rfc/rfc1700.txtで RFC 1700 を参照し、「ICMP Type Numbers」を検索してください。
  - [コード（Code）]：ゼロ以外のコードを持つパケットタイプをモデル化している場合以外は、**0** を入力します。これらは、宛先到達不能（タイプ 3、コード 0 ～ 12）、リダイレクト（タイプ 5、コード 0 ～ 3）、時間超過（タイプ 11、コード 0 ～ 1）、およびパラメータの問題（タイプ 12、コード 0 ～ 2）です。コードの説明については、RFC 1700 を参照してください。追加のコードが他の RFC に導入されている場合がある点に注意してください。
  - [ID]：限定された数のメッセージタイプに対してのみフィールドが使用される場合でも、ID の値を入力する必要があります。ID は、要求および応答バージョン（エコー、エコー要求など）を含む ICMP タイプに対して、応答を要求に一致させるために使用されます。値は 1 ～ 255 です。

- [プロトコル（IPのみ）Protocol (IP only)]：次のレベルのプロトコルを示す番号を入力します。プロトコルコードの一覧については、 http://www.ietf.org/rfc/rfc1700.txt で RFC 1700 を参照し、「Protocol Numbers」を検索してください。この項の執筆時点では、番号 1 ～ 54 および 61 ～ 100 が、許容範囲である 0 ～ 255 から実際のプロトコルに割り当てられている値を表しています。
- VLAN ID（1 ～ 4096）：フローの VLAN ID を入力します。VLAN ID は、パケットが属する VLAN を決定します。Cisco Security Manager により、ID 範囲が 1 ～ 4096 であることが検証されます。

（注） バージョン 4.13 以降、Cisco Security Manager パケットトレーサは透過的な FW デバイスをサポートします。VLAN ID は、デバイス 9.7.1 以降でパケットトレーサをサポートするためにバージョン 4.13 で導入された新しいパラメータです。

- 宛先 MAC：フローの宛先 MAC アドレスを入力します。Cisco Security Manager により、MAC アドレスのフォーマットが検証されます。
- [SPIの入力（ESPのみ）（Enter the SPI (ESP only)）]：セキュリティ パラメータ インデックスを入力します。これは、受信側のセキュリティ アソシエーションを識別するために（宛先 IP アドレスとともに）使用される任意の値です。0 ～ 4294967295 の数値を入力します。

ステップ 4 [パケットのトレース（Tracing Packet）] ドロップダウンリストから、該当するオプションを選択します。

- bypass-checks：シミュレートされたパケットのセキュリティチェックをすべてバイパスする
- decrypted：シミュレートされたパケットを復号された IPSec/SSL VPN として扱う
- persist：長期トレースを有効にし、クラスタでトレースを追跡する
- transmit：シミュレートされたパケットをデバイスから送信できるようにする

ステップ 5 トレースの経過を表示するには、[アニメーションの表示（Show animation）] を選択します。選択しない場合、トレースが完了するまでウィンドウは結果によって更新されません。

ステップ 6 [Start] をクリックして、パケットをトレースします。

ポリシーが検査され、結果がウィンドウの下部にグラフィカル情報と詳細情報という 2 つの形式で表示されます。グラフィカルビューには、パケットのパスで評価されたフェーズの概要が示されます。チェックマークはパケットがフェーズに合格したことを示し、赤い X はパケットがそのポイントでドロップされたことを示します。

詳細情報では、フェーズに対応するフォルダで結果が整理されます。[Action] カラムにフェーズの結果が示されます（合格した場合はチェックマーク、ドロップされた場合は赤い X）。フォルダを開くには、その見出しをクリックします。詳細情報には、評価された特定のコンフィギュレーション コマンドおよび**show** コマンドから取得されたデータを含めることができます。Result という名前の最後のフォルダでは、トレース結果の概要が示されます。

ヒント：

- 明示的なアクセス ルールによってパケットが許可または拒否される場合、そのルールにジャンプできます。Access-List フォルダを選択して開き、セクションの一番上にある [アクセスルールの表示（Show access rule）] リンクをクリックします。Access Rule ポリシーが表示され、そのルールが強調表示され

ます。必要に応じてルールを編集できます。暗黙的な廃棄ルールによってパケットがドロップされる場合、ルールがポリシー テーブルに存在しないため、[Show access rule] リンクは使用できません。

- 分析中にネットワーク障害によってデバイスがシャットダウンされるかデバイスに到達できない場合、「Device Connectivity is Failed」というエラーメッセージが表示されます。
- 新しいトレースを開始すると、表示されていた情報は自動的にクリアされます。[クリア（Clear）] をクリックしてもクリアできます。

ping、トレースルート、またはNSルックアップツールを使用した接続問題の分析

ping またはトレース ルートのツールを使用して、ネットワークの設定および接続の調査およびトラブルシューティングを行うことができます。通常は、Security Manager 内から特定の起動ポイントとパラメータを指定して、デバイスのこれらのコマンドを実行します。これにより、Security Manager で対応するコマンドが生成されます。一方、NS ルックアップは通常、Security Manager クライアントから実行します。

（注） バージョン 4.13 以降、Cisco Security Manager のトレースルートは IPv6 アドレスをサポートします。ASA バージョン 9.7.1 以降、IPv6 アドレスのトレースルートがサポートされています。

表 *7 : Ping*、トレースルート、および *NS* ルックアップ トラブルシューティング コマンドのプロファイル

Tool	Profile
Ping	ping を使用すると、特定のホストが IP ネットワーク上で到達可能かどうかをテストし、ローカルホストから宛先のコンピュータに送信されたパケットのラウンドトリップ時間を測定します。これには、ICMP メッセージを使用するローカルホスト独自のインターフェイスの測定も含まれる場合があります。 このツールの使用方法の詳細については、ping を使用した設定の分析 （42 ページ）を参照してください。
トレース ルート	トレースルートを使用すると、IP ネットワーク上でパケットが通過するルートが表示されます。システムは、行われたホップ数と通過した各デバイスのアドレスを返します。 このツールの使用方法の詳細については、TraceRoute を使用した設定の分析（44 ページ）を参照してください。

Tool	Profile
NS ルックアップ	NS ルックアップ（ネームスペース ルックアップ）を使用すると、デバイスから NS ルックアップ コマンドを発行するため、問い合わせされたデバイスが使用する DNS サーバの内容をテストできます。 このツールの使用方法の詳細については、NS ルックアップを使用した設定の分析 （46 ページ）を参照してください。

適用性

ping ツールは、ASA（7.0 ～ 8.3）、PIX（6.3(1-5) ～ 8.0(2-4)）、FWSM（2.2(1) ～ 4.1(1)）、およびすべての IOS のデバイスで適用可能です。IPS には適用できません。

トレース ルート ツールは、ASA（7.2(1) 以降）、PIX（6.3(1-5) ～ 8.0(2-4)）、およびすべての IOS のデバイスで適用可能です。これは FWSM にも IPS にも適用できません。

NS ルックアップツールは、Cisco Security Manager によって管理されるどのデバイスでもサポートされず、Windows API を使用して Cisco Security Manager クライアントから実行します。

ping を使用した設定の分析

ping ツールは、デフォルトで ICMP エコー要求およびエコー応答メッセージを使用して、リモート システムへの到達可能性をテストします。また、ping の実行に TCP を使用するように選択できます。一番簡単な形式で、ping は単純に IP パケットが宛先 IP アドレスに送信されて戻ってくることを確認します。ping が IP アドレスに送信されると、応答が返されます。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。Security Manager 内から、ping コマンドの発行元のネットワーク デバイスと、エコー要求のターゲットの両方を指定できます。このツールは、一般に 2 つの情報を返します。送信元が宛先に到達可能かどうか（推測によるこの逆への到達可能性も）と Round-Trip Time（RTT; ラウンドトリップ時間、ミリ秒単位）です。

ping 診断ツールは、次のようにさまざまな方法で使用できます。

- **セキュリティアプライアンスに対する ping の実行**：他のセキュリティアプライアンス上のインターフェイスに ping を実行して、インターフェイスが起動していて応答することを検証します。
- **2 つのインターフェイス間のループバックテスト**：同じセキュリティアプライアンス上の一方のインターフェイスから相手側のインターフェイスに ping を、外部ループバックテストとして起動して、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証します。
- **セキュリティアプライアンスを介した ping の実行**：ping ツールから発信した ping パケットは、デバイスとの中間にあるセキュリティアプライアンスをパススルーする場合があります。エコーパケットが返されるときも、そのインターフェイスのうち 2 つをパススルーします。これを使用して、中間にある装置のインターフェイス、動作、応答時間についての基本的なテストを実行できます。

- **中間の通信をテストするための ping の実行**：正しく機能していてエコー要求を返すことがわかっているネットワークデバイスに対して、セキュリティ アプライアンス インターフェイスから ping を開始します。エコーを受信した場合、物理的な接続と任意の中間デバイスの正常な動作を確認します。

ヒント　Event Manager 内から、イベントを右クリックし、ping ツールを開いて関連デバイスに ping を実行します。

ステップ 1　デバイスビューで、[ツール（Tools）] > [Ping、トレースルートおよびNSルックアップ...（Ping, TraceRoute and NS Lookup . . .）] を選択します。**...**

[Ping, TraceRoute and NS Lookup] ダイアログが表示されます。

ステップ 2　デバイスセレクタから、**Ping** コマンドの発行元にするデバイスを選択します。

選択したデバイスがダイアログボックスの右上に表示されます。

（注）　ping に TCP を使用するには、[Packet Type] で [TCP] を選択します（デフォルトのパケット タイプは ICMP です）。

ステップ 3　[Hostname/IPv4address] に ping の送信先にするホスト ネットワーク/ホスト ポリシー オブジェクトの IP アドレスを入力します。

または、[選択（Select）] をクリックして、ping の送信先にするホストネットワーク/ホストポリシーオブジェクトを定義するホストネットワーク/ホストオブジェクトを選択します。

ステップ 4　タイムアウト値を入力します（任意）。

ステップ 5　[Ping] をクリックします。

ウィンドウ下部の領域に結果が表示されます。

ping の実行結果の例：

例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping の実行結果が失敗の場合の例：

例：

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

[出力をクリア（Clear Output）] をクリックすると、ping の結果領域から以前の応答を削除できます。

ping コマンドの詳細については、Cisco.com の「Troubleshooting TCP/IP」を参照してください。

TraceRoute を使用した設定の分析

Traceroute ツールを使用して、パケットが宛先に到着するまでのルートを判断できます。このツールは、送信される各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。

Traceroute は、ネットワーク全体の TCP/IP 接続に関して役立つ情報を返します。次の表に、Traceroute ユーティリティによって返されるコードとその考えられる原因を示します。

表 *8 : Traceroute* の出力記号

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。
!A	ICMP が管理者によって禁止されています。
?	原因不明の ICMP エラーが発生しました。

ステップ 1 デバイスビューで、[ツール（Tools）] > [Ping、トレースルートおよびNSルックアップ...（Ping, TraceRoute and NS Lookup . . .）] を選択します。. . .

[Ping, TraceRoute and NS Lookup] ダイアログが表示されます。

ヒント Event Manager 内から、イベントを右クリックし、[TraceRoute] ページを開いて関連デバイスのルートをトレースします。

ステップ 2 [ルートのトレース（Trace Route）] タブを選択します。

[Trace Route] ページが表示されます。

ステップ 3 デバイス セレクタから、ルートのトレース元にするホストを選択します。

ステップ 4 [IPv4アドレス/ホスト名（IPv4 Address/Hostname）] を入力して、ルートのトレース先にするホストのアドレスまたは名前を指定します。

または、[選択（Select）] をクリックして、IP アドレスを定義するホストネットワーク/ホストオブジェクトを選択します。

（注） バージョン 4.13 以降、Cisco Security Manager のトレースルートは IPv6 アドレスをサポートします。バージョン 4.12 まで、syslog サーバーは IPv4 アドレスを持つデバイスで構成されていました。デバイスバージョン 9.7.1 以降、IPv6 アドレスのトレースルートがサポートされています。syslog サーバーは、IPv6 アドレスを持つデバイスで IPv6 syslog アドレスを使用して設定できます。

ステップ 5 必要に応じて、次のフィールドの値を指定します。

表 *9 : Traceroute* フィールド

フィールド	説明
[タイムアウト（Timeout）] :（任意）	接続がタイムアウトになるまでの応答の待機時間（秒単位）。デフォルトは 3 秒です。
[ポート（Port）]（任意）	UDP プローブ メッセージで使用される宛先ポート。デフォルトは 33434 です。
[ホップごとのプローブ数（Probes per hop）]（任意）	TTL の各レベルで送信するプローブの数。デフォルトは 3 です。
[TTL最小値（TTL Min）]（任意）	最初のプローブの TTL の最小値（デフォルトは 1 です）。
[TTL最大値（TTL Max）]（任意）	最初のプローブの TTL の最大値（デフォルトは 30 です）。

ステップ 6 必要に応じて、[送信元インターフェイスまたはIPアドレスの指定（Specify Source Interface or IP Address）] を選択してから次のいずれかを実行します。

- ドロップダウンリストから送信元の [インターフェイス（Interface）] を選択します。

（注） [IPアドレス/ホスト名（IP Address/ Hostname）] フィールドに IPv6 アドレスが指定されている場合、送信元の [インターフェイス（Interface）] フィールドは適用されません。

- [IPアドレス（IP Address）] を入力します。

ステップ 7 必要に応じて、[逆解決（Reverse Resolve）] を選択して、アドレスとホスト名の表示を入れ替えます。

ステップ 8 必要に応じて、[ICMP] を選択して、IP ではなくプロトコルを使用します。

ステップ 9 [トレース（Trace）] をクリックします。

traceroute は、パケットが宛先に到達するか、または TTL の最大値に達すると終了します。行われたホップおよび各ホップに対応するデバイスアドレスが表示されます。

NS ルックアップを使用した設定の分析

NS ルックアップ ツールを使用して、ホスト名を使用している場合はリモート ホスト アドレスを検索し、アドレスを使用している場合はホスト名を検索します。

ping ツールおよび Traceroute ツールとは異なり、NS ルックアップは、Security Manager クライアント上で実行されます。

ステップ 1 デバイスビューで、[ツール（Tools）] > [Ping、トレースルートおよびNSルックアップ...（Ping, TraceRoute and NS Lookup . . .）] を選択します。. . .

[Ping, TraceRoute and NS Lookup] ダイアログが表示されます。

ステップ 2 [NSルックアップ（NS Lookup）] タブを選択します。

ステップ 3 [IPv4Address/Hostname] にアドレスまたはホスト名を入力します。

または、[選択（Select）] をクリックして、IP アドレスを定義するホストネットワーク/ホストオブジェクトを選択します。

ステップ 4 必要に応じて、検索に特定の DNS サーバーを使用するには、DNS サーバーのサーバー名またはアドレスを入力します。

ステップ 5 [検索（Lookup）] をクリックします。

システムでは、検索に使用する DNS サーバだけでなく、特定のアドレス/ホスト名のペアも表示されます。

Packet Capture Wizard の使用

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行うために、キャプチャを設定、実行、表示、および保存できます。事前設定されたアクセス リストを使用するか、または 1 つ以上のインターフェイス上の送信元および宛先のアドレス/ポートなどのパケット パラメータの一致基準を使用して、キャプチャを実行できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを 1 回実行します。キャプチャを Cisco Security Manager クライアント コンピュータに保存して、パケット アナライザによるキャプチャの検査が可能です。

Packet Capture Wizard は、ASA クラスタでのパケットキャプチャもサポートしています。ASA クラスタの制御ユニットで Packet Capture Wizard を実行すると、選択したデバイスのみまたはクラスタ内のすべてのデバイスのデータをキャプチャするオプションが提供されます。クラスタのキャプチャを実行したら、クラスタのサマリー情報を表示したり、クラスタ内の特定デバイスのキャプチャバッファを表示またはダウンロードすることができます。

（注） ディレクタが変更されている場合は、Packet Capture Wizard を実行する前に Security Manager でディレクタを更新する必要があります。それを行わないと、メンバーのキャプチャにエラーが含まれます。[デバイスのプロパティ（Device Properties）]>[クラスタ情報（Cluster Information）]ページの [デバイスから取得（Retrieve From Device）] ボタンを使用すると、クラスタのディレクタを更新できます。詳細については、[グループ情報（Group Information）] ページを参照してください。

事前設定されたアクセス リストを使用するか、または 1 つ以上のインターフェイス上の送信元および宛先のアドレス/ポートなどのパケット パラメータの一致基準を使用して、キャプチャを実行できます。

次の点に注意してください。

- Packet Capture Wizard は、ファイアウォール デバイス（PIX、ASA、または FWSM）だけで使用できます。
- パケットの一致基準に基づいたパケット キャプチャは、ASA バージョン 7.2(3) 以降を実行するデバイスだけでサポートされます。他のデバイスについては、パケット キャプチャをアクセス リストに基づいて実行できるだけです。

Packet Capture Wizard を使用するには、次の手順に従います。

ステップ 1 次のいずれかの方法を使用して、Packet Capture Wizard を起動します。

- [ツール（Tools）] > [Packet Capture Wizard] を選択します。
- （デバイスビュー）ASA、PIX、または FWSM のデバイスを右クリックし、ショートカットメニューで [パケットキャプチャ（Packet Capture）] を選択します。ステップ 3 （47 ページ）に進みます。
- （イベントビューア）ASA、PIX、または FWSM のデバイスのイベントを右クリックし、ショートカットメニューで [パケットキャプチャ（Packet Capture）] を選択します。ステップ 3 （47 ページ）に進みます。

ステップ 2 [ツール（Tools）] メニューから Packet Capture Wizard を起動した場合は、パケットをキャプチャするデバイスを選択します。[Security Devices] リストには、パケット キャプチャが実行可能なデバイスだけが含まれています。

ステップ 3 ASA クラスタのディレクタユニットであるデバイスを選択した場合は、選択したデバイスについてのみキャプチャを実行するかクラスタ全体についてキャプチャを実行するかを指定し、[次へ（Next）] をクリックします。

ステップ 4 ドロップダウン リストから入力インターフェイスを選択します。

（注） 同じウィザードでは、同じインターフェイスを入力と出力の両方として選択できません。

ステップ 5 インターフェイスによって送信されたクラスタ コントロール プレーン パケットをキャプチャするには、[クラスタインターフェイスで制御パケットをキャプチャする（Capture control packets on cluster interface）] チェックボックスをオンにします。

（注） このオプションのフィールドは、クラスタ コントロール プレーン パケットのみをキャプチャするために、ASA 9.12.1 以降のデバイス用に Cisco Security Manager 4.19 で導入されました。この情報は、特にマルチコンテキストモードでクラスタでの問題をトラブルシューティングするときに役立ちます。

ステップ 6 [Packet Match Criteria] 領域で、次のいずれかの操作を実行します。

- パケットの照合に使用するアクセスリストを指定するには、[アクセスリスト（Access-List）] オプションボタンを選択して、ドロップダウンリストからアクセスリストを選択します。
- パケットパラメータを指定するには、[パケットパラメータ（Packet Parameters）] オプションボタンを選択して、次のフィールドを入力します。
  - [Source Host / Network] フィールドおよび [Destination Host / Network] フィールドに、それぞれ送信元および宛先を指定します。次のいずれかを使用して、送信元または宛先を指定できます。
  - [送信元ホスト/ネットワークオブジェクト（Source Host/ Network object）]。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。

（注） Cisco Security Manager 4.18 以降、パケットパラメータは All-Address（any）、All-IPv4-Address（any4）、および All-IPv6-Address（any6）でサポートされます。

- ホスト IP アドレス（10.10.10.100 など）。
- ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。
- キャプチャするプロトコル タイプをドロップダウン リストから選択します。指定できるキャプチャのプロトコル タイプは、ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp です。

プロトコルが ICMP の場合は、ドロップダウン リストから ICMP タイプを選択します。指定できるタイプは、ALL、alternate-address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable です。

プロトコルが TCP または UDP の場合は、送信元および宛先のポート サービスを指定します。指定できるオプションは次のとおりです。

- すべてのサービスを含めるには、[All Services] を選択します。
- 特定のサービスを指定するには、ドロップダウン リストから適切な演算子（=、!=、>、<、または range）を選択してから、aol、bgp、chargen、cifs、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nfs、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、whois、または www のいずれかを選択します。>、<、および range の演算子は、選択したサービスに割り当てられたポート番号に基づいて機能します。

range 演算子を使用する場合は、別のドロップダウン リストがイネーブルになります。2 つのドロップダウン リストを使用して、指定する範囲の開始サービスと終了サービスを選択します。対応するポート番号が小さい方のサービスを最初のドロップダウン リストに選択し、対応するポート番号の大きい方のサービスを 2 番めのドロップダウン リストに選択する必要があります。

ステップ 7 [次へ（Next）] をクリックして、[出力インターフェイスの選択（Select egress interface）] ステップに進みます。

ステップ 8 ドロップダウン リストから出力インターフェイスを選択します。

（注） 同じウィザードでは、同じインターフェイスを入力と出力の両方として選択できません。

ステップ 9 インターフェイスによって送信されたクラスタ コントロール プレーン パケットをキャプチャするには、[クラスタインターフェイスで制御パケットをキャプチャする（Capture control packets on cluster interface）] チェックボックスをオンにします。

（注） このオプションのフィールドは、クラスタ コントロール プレーン パケットのみをキャプチャするために、ASA 9.12.1 以降のデバイス用に Cisco Security Manager 4.19 で導入されました。この情報は、特にマルチコンテキストモードでクラスタでの問題をトラブルシューティングするときに役立ちます。

ステップ 10 [Packet Match Criteria] 領域で、次のいずれかの操作を実行します。

（注） 入力インターフェイスに選択した [Packet Match Criteria] オプション（アクセス リストまたはパケット パラメータ）は、出力インターフェイスにも使用されます。また、入力インターフェイスでの照合にパケット パラメータを使用した場合は、使用したプロトコル定義が出力インターフェイスにも使用されます。

- アクセス リストを使用してパケットを照合している場合は、ドロップダウン リストからアクセス リストを選択します。
- パケット パラメータを使用してパケットを照合している場合、入力に使用されるパラメータは、出力にも使用されます。

ステップ 11 [次へ（Next）] をクリックして、[バッファパラメータの設定（Set buffer parameters）] ステップに進みます。

ステップ 12 次のフィールドを設定して、バッファ パラメータを指定します。

[Buffer Parameters] 領域で、バッファ サイズとパケット サイズを指定します。バッファ サイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケット サイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケット サイズを使用することを推奨します。

- [10 秒ごとにキャプチャバッファを読み取る（Read capture buffer every 10 seconds）]：このオプションを選択にすると、10 秒ごとにキャプチャデータを自動的に取得します。このオプションを選択する場合は、循環バッファを使用する必要があります。
- [循環バッファを使用（Use a circular buffer）]：このオプションを選択すると、バッファが一杯になった後もパケットのキャプチャを継続します。この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

- [バッファサイズ（Buffer Size）]：キャプチャがパケットを保存するために使用可能なバイト数（1534 ～ 33554432）を入力します。
- [最大パケットサイズ（Maximum Packet Size）]：キャプチャが単一のパケットを保存するために使用可能なバイト数（14 ～ 1522）を入力します。最大値の 1522 を使用すると、可能な限り多くの情報をキャプチャします。

ステップ 13 [次へ（Next）] をクリックして [サマリー（Summary）] ステップに進みます。入力したトラフィックセレクタとバッファパラメータが表示されます。

ステップ 14 [次へ（Next）] をクリックして、[実行、表示、保存（Run, View & Save）] ステップに進みます。

ステップ 15 [Run, View & Save] ステップからは、次の操作を実行できます。

- パケットのキャプチャを開始するには、[キャプチャを開始（Start Capture）] をクリックします。
- パケットのキャプチャを停止するには、[キャプチャを停止（Stop Capture）] をクリックします。
- キャプチャされたパケットの次のセットを取得するには、次のいずれかを実行します。
  - 個別のデバイスの場合は、[キャプチャパケットの表示（Display Capture Packets）] をクリックして、キャプチャされたパケットの次のセットをデバイスから取得し、バッファステータスバーを更新します。このボタンは、[Set buffer parameters] ステップで [Read capture buffer every 10 seconds] オプションが選択されなかった場合だけイネーブルになります。
  - クラスタの場合は、[クラスタキャプチャサマリーの取得（Get Cluster Capture Summary）] をクリックして、キャプチャされたパケットの次のセットをクラスタ内のデバイスから取得し、バッファステータスバーを更新します。このボタンは、[Set buffer parameters] ステップで [Read capture buffer every 10 seconds] オプションが選択されなかった場合だけイネーブルになります。
- ASA クラスタのキャプチャを実行する場合、クラスタ内のデバイスのキャプチャバッファを操作するために次のオプションを使用できます。
  - クラスタ内のデバイスからキャプチャされたパケットを表示するには、[キャプチャバッファの取得（Get Capture Buffer）] の下にある [デバイス名（Device Name）] リストでデバイスを選択し、[キャプチャバッファの取得（Get Capture Buffer）] をクリックします。

選択したデバイスのキャプチャ情報が表示されます。このデータに対して実行できるアクションについては、このリストの他のオプションを参照してください。

- クラスタ内の特定デバイスまたはすべてのデバイスに関するキャプチャの内容を削除し、バッファに別のパケットをキャプチャするスペースを確保するには、[キャプチャバッファのクリア（Clear Capture Buffer）] の下にある [デバイス名（Device Name）] フィールドでデバイスを選択するか [-- すべて --（--All--）] を選択し、[キャプチャバッファのクリア（Clear Capture Buffer）] をクリックします。

（注） デバイスバッファをクリアする前に、キャプチャを保存することを推奨します。デバイスバッファをクリアする前にキャプチャを保存しないと、キャプチャされたデータは消失します。

- 外部パケット分析ツールを使用して対応する入力キャプチャまたは出力キャプチャを表示するには、[入力キャプチャ（Ingress Capture）] ウィンドウまたは [出力キャプチャ（Egress Capture）] ウィンド

ウの上にある [Network Sniffer を起動（Launch Network Sniffer）] ボタンをクリックします。パケットアナライザがインストールされていて、*.pcap ファイル拡張子に関連付けられている必要があります。

- パケットキャプチャデータを大きなウィンドウに並べてを表示するには、[データを大きなウィンドウで表示（View Data in Larger Window）] をクリックします。
- [キャプチャを保存（Save captures）] をクリックして、[キャプチャを保存（Save Capture）] ダイアログボックスを表示します。キャプチャしたパケットに含める形式として、ASCII または PCAP を選択します。入力キャプチャまたは出力キャプチャを保存するオプションがあります。
- 現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[デバイスバッファのクリア（Clear Device Buffer）] をクリックします。

（注） デバイスバッファをクリアする前に、キャプチャを保存することを推奨します。デバイスバッファをクリアする前にキャプチャを保存しないと、キャプチャされたデータは消失します。

- クラスタ内のデバイスに関してキャプチャされたパケットの次のセットを取得し、バッファステータスバーを更新するには、[キャプチャバッファのリフレッシュ（Refresh Capture Buffers）] をクリックして、

ステップ 16 [Finish] をクリックして、ウィザードを終了します。

IPインテリジェンス（IP Intelligence）

Cisco Security Manager によって管理されるネットワーク セキュリティ デバイスは、攻撃者または被害者のマシン、あるいはその両方の IP アドレス情報を含む大量のセキュリティログとセキュリティイベントを生成します。

IP アドレスに関する有用な詳細は、まとめて IP インテリジェンスと呼ばれ、ping、トレースルート、NS ルックアップなどのツールを使用して検出できます。ただし、これらのツールはやや初歩的なので、より高度なツールで補強することが望ましい場合がよくあります。

バージョン 4.5 以降、Security Manager は、IP アドレスに関する重要な詳細をリアルタイムで提供する、または生成されたレポートで提供する高度なツールを備えています。Security Manager では、これらの重要な詳細を次のカテゴリで提供しています。

- 逆引き DNS（FQDN）ルックアップサービス
- GeoIP ルックアップサービス
- Whois ルックアップサービス

（注） IPv6 アドレスの IP インテリジェンスはサポートされていません。

これらの IP インテリジェンスカテゴリについて、次の表で説明します。

表 *10 : IP* インテリジェンスカテゴリ

IP ルックアッププロバイダー	情報源	リアルタイムまたは手動/制限
逆引き DNS（FQDN）ルックアップサービス	DNS サーバー	リアルタイム （注） 外部 DNS 設定は設定可能な追加オプションですが、個々の状況を評価する必要があります。
GeoIP ルックアップサービス	外部のサードパーティ コマーシャル ベンダー	リアルタイム、Cisco Security Manager バージョン 4.18 まで。 GeoIP ルックアップサービスのデータベースは GeoIP2 にアップグレードされましたが、 Cisco Security Manager はまだアップグレードされていません。したがって、Cisco Security Manager の以前のバージョンの GeoIP の自動更新と、Cisco Security Manager 4.19 のデフォルトの GeoIP パッケージには、2018 年 12 月のデータベースのみが含まれます。

IP ルックアッププロバイダー	情報源	リアルタイムまたは手動/制限
Whois ルックアップサービス	サードパーティの Web サーバーである無料の whois サーバーによって提供されます。	リアルタイム 制限事項： • Whois は、クエリおよび応答プロトコルであり、登録されたユーザーやインターネットリソース（ドメイン名、IP アドレスブロック、自律システムなど）の割り当て先を保存するデータベースに照会するために幅広く使用されます。5 つの地域インターネットレジストリ（RIR）組織が IP アドレスの割り当てと登録を管理しています。 • ARIN（American Registry for Internet Numbers）、RIPE（Réseaux IP Européens Network Coordination Centre）、および APNIC（Asia-Pacific Network Information Centre）は、Security Manager が直接クエリを実行するために使用する 3 つの RIR であり、参照 URL も提供します。RIPE および APNIC では、解析エラーがある場合、直接の URL リンクのみが表示されます。 • 指定された URL をクリックすると、指定された IP アドレスの詳細が Web ブラウザに表示されます。IP アドレスが LACNIC（Latin America and Caribbean Network Information Centre）または AfriNIC（African Network Information Centre）に属している場合、Web ブラウザはそれぞれの RIR のホームページを表示します。 • 場合によっては（DNS クエリが Windows ファイアウォールによってブロックされている、または無効なプロキシが cco 設定ページで構成されているなど）、Whois が有効になっていても機能しないことがあります。そのような場合、「フェイルセーフ」メソッドとして、参照された URL のみを提供します。

IP インテリジェンスの検索を開始する前に、[Configuration Manager] > [ツール（Tools）] > [Security Manager管理（Security Manager Administration）]...> [IPインテリジェンス設定（IP Intelligence Settings）] で必要なサービスを有効にする必要があります。[IPインテリジェンス設定（IP Intelligence Settings）] ページ を参照してください。

IP インテリジェンス ルックアップは、次のいずれかの方法を使用して実行できます。

- [IPインテリジェンス（IP Intelligence）] ダイアログボックスを使用します。[Configuration Manager] > [ツール（Tools）] > [IPインテリジェンス（IP Intelligence）]... に移動し、表示される [IPインテリジェンス（IP Intelligence）] ダイアログボックスの検索フィールドに有

効な IPv4 アドレスを入力します（IP アドレスを入力した後、Enter キーを押す必要があります）。

- Security Manager インターフェイスで有効な IPv4 アドレスにマウスのカーソルを合わせて、「クイック起動」を使用します。これはイベントビューアなどで行うことができ、通常、IP アドレスが表示されるデータの一部であるすべての GUI テーブルで実行できます。GUI テーブルの 1 つのセルに複数の IP アドレスが表示されている場合は、最初の IP アドレスのみが表示されます。

（注） クイック起動を使用した場合、GUI に [IPインテリジェンス（IP Intelligence）] オプションが表示されるまで、1 ～ 2 秒の遅延が発生する場合があります。

（注） [Configuration Manager] > [ツール（Tools）] > [IPインテリジェンス（IP Intelligence）] の [IPインテリジェンス（IP Intelligence）]... ダイアログボックスで [クイック起動の有効化（Enable Quick Launch）] チェックボックスをオンまたはオフにすることで、クイック起動を有効または無効にすることができます。 。

- ダッシュボードで IP インテリジェンス ウィジェットを使用します（[起動（Launch）] > [ダッシュボード（Dashboard）]... 。この方法は、前述の [IPインテリジェンス（IP Intelligence）] ダイアログボックスを使用する場合と同等です。
- Report Manager（**[起動（Launch）] > [Report Manager]...**）を使用して、次のいずれかのレポートで IP インテリジェンスを確認します。
  - [FW/サマリーボットネット（FW/Summary Botnet）]：上位の感染ホスト
  - [FW/サマリーボットネット（FW/Summary Botnet）]：上位のマルウェア サイト
  - [FW]：上位の宛先
  - [FW]：上位のソース
  - [IPS]：ターゲット分析
  - [IPS]：上位の攻撃者
  - [IPS]：上位の被害者

（注） これらのレポートにはいくつかの注意点があります。1）Whois 情報は含まれません。2）**[Configuration Manager] > [ツール（Tools）] > [Security Manager管理（Security Manager Administration）]... > [IP インテリジェンス設定（IP Intelligence Settings）]** ですべてのプロバイダーを無効にしている場合、レポートには IP インテリジェンス関連の列が表示されません。3）すべてのサービスを有効にすると、逆引き DNS（FQDN）と GeoIP の詳細のみがレポートに表示されます。4）1 つのサービスのみを有効にすると、そのサービスのみがレポートに表示されます。

（注） PDF 形式と CSV 形式の両方で生成されたレポートには、IP インテリジェンスの詳細が含まれます。

（注） これらのすべてのレポートでは、必要なサービスが有効化されている必要があります。「[IPインテリジェンス設定（IP Intelligence Settings）] ページ」を参照してください。

CS-MARS と Security Manager の統合

Cisco Security Manager では、ネットワーク内のセキュリティ ポリシーおよびデバイス設定を集中管理できます。一方、Cisco Security Monitoring, Analysis and Response System（CS-MARS）は、デバイスをモニタしてイベント情報（syslog メッセージや NetFlow トラフィック レコードなど）を収集する別のアプリケーションであり、Security Manager よりも広範なネットワーク モニタリング機能を備えています。CS-MARS では、大量のネットワークおよびセキュリティ データが、使いやすい形式で集約および提供されます。CS-MARS レポートから取得された情報に基づいて、セキュリティ脅威に対抗するために Security Manager でデバイス ポリシーを編集できます。

特に、Security Manager を使用してファイアウォール アクセス ルールおよび IPS シグニチャを設定する場合、それらのポリシーに関連する情報を収集して Security Manager ユーザに対して使用可能にするように、CS-MARS を設定できます。CS-MARS サーバを Security Manager に登録することによって、ユーザは特定のアクセス ルールまたは IPS シグニチャから直接 CS-MARS レポート ウィンドウにナビゲートできます。このウィンドウには、そのルールまたはシグニチャのクエリー基準があらかじめ読み込まれています。

同様に、CS-MARS ユーザは、特定の CS-MARS イベントに関連する Security Manager ポリシーを表示できます。特定のイベントとそれをトリガーしたポリシーとの双方向マッピングと、ポリシーを即時に変更する機能を結合することによって、大規模または複雑なネットワークの設定およびトラブルシューティングに要する時間を大幅に削減できます。

この相互通信をイネーブルにするには、CS-MARS サーバを Security Manager に登録し、Security Manager サーバを CS-MARS サーバに登録する必要があります。また、特定のデバイスを各ア

プリケーションに登録する必要もあります。これにより、デバイスのファイアウォールアクセス ルールまたは IPS シグニチャを操作するときに、Security Manager ユーザは、そのルールまたはシグニチャに関連するリアルタイムおよび過去のイベント情報を迅速に表示できます。

次の項では、CS-MARS と Security Manager の相互通信をイネーブルにして使用する方法について説明します。

- CS-MARS と Security Manager を統合するためのチェックリスト （56 ページ）
- Security Manager ポリシーの CS-MARS イベントの検索 （62 ページ）
- CS-MARS イベントからの Security Manager ポリシーの検索 （67 ページ）

CS-MARS と Security Manager を統合するためのチェックリスト

CS-MARS と Security Manager 間の相互通信（ CS-MARS と Security Manager の統合 （55 ページ）を参照）をイネーブルにするには、アプリケーションを相互に識別させ、両方のアプリケーションによって管理されるデバイスが適切に設定されるようにする必要があります。次の表に、統合の手順を示します。

相互通信について問題がある場合は、 CS-MARS クエリーのトラブルシューティングに関するヒント （60 ページ）を参照してください。

表 *11 : CS-MARS と Security Manager* の統合

タスク	説明
Security Manager および CS-MARS にデバイスを追加する	Security Manager へのデバイスの追加については、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。CS-MARS インベントリへのデバイスの追加については、 Cisco Security MARS のデバイス設定ガイドを参照してください。 デバイスに相互通信を提供するには、デバイスが両方のアプリケーションによってサポートされている必要があります。サポートされているデバイス タイプは、一般に、[Firewall] > [Access Rules] または [IPS] > [Signatures] ポリシーを提供するデバイス タイプです（PIX、ASA および FWSM アプライアンス、Cisco IOS ルータ、Cisco IPS センサーとモジュール、Cisco Catalyst スイッチなどがあります）。
必要に応じてアプリケーションごとにデバイスを設定する	Security Manager の基本的な設定要件については、デバイスの通信要件についてを参照してください。CS-MARS の広範な要件については、Cisco Security MARS のデバイス設定ガイドを参照してください。

タスク	説明
Security Manager を CS-MARS に登録する	Security Manager と通信するための CS-MARS の設定については、Cisco Security MARS Local Controller および Global Controller のユーザ ガイドを参照してください。 Security Manager とのリンク専用の CS-MARS ユーザ アカウントを作成する場合があります。 CS-MARS ポリシー クエリーに応答するための Security Manager サーバの設定 （57 ページ）を参照してください。
CS-MARS コントローラを Security Manager に登録する	CS-MARS コントローラの Security Manager への登録については、Security Manager での CS-MARS サーバの登録 （58 ページ）を参照してください。
Security Manager で CS-MARS コントローラをデバイスにリンクする	Security Manager で、デバイスの [デバイスのプロパティ（Device Properties）] ページで [CS-MARSの検出（Discover CS-MARS）] をクリックして、特定のデバイスをモニターする CS-MARS コントローラをプロアクティブに検出できます（デバイスの CS-MARS コントローラの検出または変更 （59 ページ）を参照）。そのようにしない場合は、ユーザがデバイスのイベントを検索しようとしたときに、適切なコントローラが自動的に検出されます（複数のコントローラがデバイスをモニタしている場合、ユーザはコントローラを選択するように求められます）。

関連項目

- アクセス ルールの CS-MARS イベントの表示 （63 ページ）
- IPS シグニチャの CS-MARS イベントの表示 （66 ページ）
- Security Manager ポリシーの CS-MARS イベントの検索 （62 ページ）

CS-MARS ポリシー クエリーに応答するための Security Manager サーバの設定

CS-MARS は、ポリシー検索クエリーを実行してポリシー情報を取得できるように、Security Manager サーバへのアクセスを許可されている必要があります。

- サーバで Common Services AAA 認証を使用している場合（Cisco Secure ACS など）、CS-MARS が Security Manager サーバにクライアント アクセスできるように、管理アクセス設定を更新する必要があります。
- Security Manager で CS-MARS がクエリーの実行に使用できるユーザ アカウントを定義します。Security Manager サーバで特定の監査証跡を提供するために、別個のアカウントを作成することを推奨します。このアカウントを次の Common Services ロールの 1 つに割り当てる必要があります。
  - 承認者

- Network Operator
- ネットワーク管理者
- システム管理者（System Administrator）

Help Desk セキュリティ レベルのユーザは、CS-MARS 内のポリシー検索テーブルの表示だけを行うことができます。つまり、Security Manager をクロス起動してポリシーを変更することはできません。

（注） Security Manager サーバを CS-MARS に登録するときに、ポリシー テーブル検索のために Security Manager クレデンシャルを求める場合、認証用に Common Services で別の CS-MARS アカウントを用意する必要がなくなることがあります。

Common Services でのユーザーの追加およびロールの関連付けの詳細については、『*User Guide for CiscoWorks Common Services*』を参照してください。

関連項目

- Security Manager での CS-MARS サーバの登録 （58 ページ）
- デバイスの CS-MARS コントローラの検出または変更 （59 ページ）

Security Manager での CS-MARS サーバの登録

CS-MARS と Security Manager を同時に使用する場合は、 CS-MARS と Security Manager を統合するためのチェックリスト （56 ページ）の説明に従って、CS-MARS コントローラを Security Manager に登録し、これらのアプリケーション間の相互通信をイネーブルにする必要があります。

これにより、ユーザがデバイスのイベントを検索するときに、Security Manager によって、そのデバイスのイベントを収集している CS-MARS コントローラが識別されます。複数の CS-MARS コントローラによってデバイスのイベントが収集されている場合、ユーザは使用する CS-MARS コントローラを選択できます。各デバイスの [Device Properties] ウィンドウで、使用する正しい CS-MARS コントローラを指定することもできます（詳細については、デバイスの CS-MARS コントローラの検出または変更 （59 ページ）を参照してください）。

（注） Security Manager で明示的にサポートされている CS-MARS バージョンについては、製品の該当するバージョンの『Release Notes for Cisco Security Manager』を参照してください。明示的にはサポートされていないバージョンを使用する場合、4.3.4 または 5.3.4 よりも前の CS-MARS バージョンは使用できません。

ステップ 1 [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルで [CS-MARS] を選択して、[CS-MARS] ページを表示します。

ステップ 2 [追加（Add）] ボタンをクリックして、CS-MARS サーバーを追加します。[New CS-MARS Device] ダイアログボックスが開きます（詳細については、[New CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックスを参照してください）。

ステップ 3 [New CS-MARS Device] ダイアログボックスで、サーバの IP アドレスまたは完全修飾 DNS ホスト名と、サーバにログインするためのユーザ名およびパスワードを入力します。ローカル コントローラを追加する場合、入力するユーザ名はローカル アカウントとグローバル アカウントのいずれかです。[User Type] リストからアカウントのタイプを選択します。

ヒント CS-MARS Global Controller を使用している場合は、個別の Local Controller ではなく Global Controller を追加します。Global Controller を追加することによって、各 Local Controller を追加しなくても、Security Manager でデバイスの正しい Local Controller を識別できます。Global Controller を追加する場合は、Global Controller によってモニタされる個別の Local Controller を追加しないでください。

[デバイスから取得（Retrieve From Device）] をクリックして、サーバーの認証証明書を取得します。証明書が提示されたら、[承認（Accept）] をクリックします。

完了したら、[OK] をクリックします。[New CS-MARS Device] ダイアログボックスが閉じて、サーバが CS-MARS デバイス リストに追加されます。

ステップ 4 [CS-MARSの起動タイミング（When Launching CS-MARS）] リストから、ユーザーがイベントステータスを要求したときに CS-MARS サーバーにログインするように求められるようにするか、またはユーザーが Security Manager にログインしたときに提供されたクレデンシャルを使用して Security Manager が CS-MARS に自動的にログインするかを選択します。

Security Manager クレデンシャルの使用を選択した場合は、必要なユーザ アカウントを CS-MARS で設定する必要があります。詳細については、CS-MARS のマニュアルを参照してください。

ステップ 5 [CS-MARS] ページで [保存（Save）] をクリックして変更を保存します。

デバイスの CS-MARS コントローラの検出または変更

Cisco Security Monitoring, Analysis and Response System（CS-MARS）コントローラを使用してデバイスをモニタする場合、このコントローラを Security Manager に登録することにより、個々のデバイスのファイアウォール アクセスまたは IPS シグニチャ ルールに関連する syslog およびイベントを表示できます。

ルールに関連するイベントを表示しようとすると、Security Manager によって、デバイスをモニタする CS-MARS コントローラを自動的に検出できます。複数のコントローラによってデバイスがモニタされている場合は、使用するコントローラの選択を求められます。

デバイスの CS-MARS コントローラを、そのデバイスの [Device Properties] ウィンドウでプロアクティブに選択することもできます。同様に、デバイスに割り当てられている CS-MARS コントローラを変更する必要がある場合は、[Device Properties] ウィンドウで選択内容を変更できま

す。次の手順では、デバイスの CS-MARS コントローラをそのデバイスの [Device Properties] ウィンドウで検出または変更する方法について説明します。

はじめる前に

デバイスをモニターする CS-MARS コントローラが、[CS-MARS] 管理ページ（[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [CS-MARS]）で Cisco Security Manager に登録されている必要があります。詳細については、Security Manager での CS-MARS サーバの登録 （58 ページ）を参照してください。

ステップ 1 デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

ステップ 2 目次で [全般（General）] をクリックして、[全般（General）] プロパティページを開きます（[デバイスのプロパティ（Device Properties）] : [全般（General）] ページを参照）。

ステップ 3 [CS-MARSモニタリング（CS-MARS Monitoring）] グループで、[CS-MARSの検出（Discover CS-MARS）] をクリックします。Security Manager によって、デバイスをモニタしている登録済みコントローラが判別されます（存在する場合）。複数ある場合は、使用する CS-MARS コントローラを選択するように求められます。

CS-MARS クエリーのトラブルシューティングに関するヒント

CS-MARS と Security Manager を一緒に使用しているときに発生する可能性がある問題を識別して解決するには、次のトラブルシューティングに関するヒントを使用します。

- Security Manager サーバと CS-MARS 間の通信には、HTTPS が必要です。
- インターフェイス名は、Security Manager では大文字と小文字が区別されませんが、CS-MARS では区別されます。たとえば、「outside」と「Outside」は CS-MARS アプライアンスでは排他的と見なされますが、Security Manager では同一です。さらに、syslog メッセージでは、すべてのインターフェイス名に小文字が使用されます。その結果、CS-MARS で生成されたイベントから Security Manager ポリシーのクエリーを実行する場合、syslog イベントに記録されるインターフェイス名は、Security Manager のそのポリシーでのインターフェイス名と一致しない場合があります。この問題を回避するには、すべてのインターフェイス名、インターフェイス ロールの定義、CS-MARS で小文字を使用します。
- Security Manager ポリシーから CS-MARS イベントを照会するには、Security Manager クライアントが、ネットワーク アドレス変換（NAT）境界について、CS-MARS アプライアンスおよび Security Manager サーバと同じ側にある必要があります。

同様に、CS-MARS クライアントが NAT 境界について CS-MARS アプライアンスおよび Security Manager サーバと同じ側にない場合は、Security Manager ポリシーを検索できますが、読み取り専用モードになります。読み取り専用ポリシー検索テーブルからは Security Manager クライアントを起動できません。Security Manager クライアントを CS-MARS から起動して、一致したポリシーを変更する場合、クライアントは NAT 境界について CS-MARS アプライアンスおよび Security Manager サーバと同じ側にある必要があります。

- 複数の独立したセキュリティ コンテキストが存在する FWSM、PIX、および ASA デバイスの場合、CS-MARS イベントを照会するには、セキュリティ コンテキストごとに Security Manager で一意の管理 IP アドレスを定義する必要があります。また、各仮想コンテキストのホスト名およびレポート IP アドレスが、CS-MARS に追加される前に設定されている必要があります。設定されていないと、これらのコンテキストのポリシーからのイベント検索は失敗します。

- すべての IPS デバイスおよびサービス ポリシーについて、IPS ポリシーを検出しない場合、または設定済みのポリシーをデバイスから削除する場合は、デフォルトのシグニチャ ポリシーがデバイスに割り当てられます。デフォルトのシグニチャからイベント検索を実行しようとすると、「Policy not found」というエラーメッセージが表示されます。ただし、デフォルトのシグニチャを編集して保存すると、CS-MARS でイベントにナビゲートできます。

- Security Manager で定義されたアクセス ルールに対してオブジェクト グループ化またはルール最適化がイネーブルであり、デバイス上の関連付けられた access-list コマンドが最適化されたルールと一致しない場合、CS-MARS でイベントは表示されません。

- アクセス ルールに対してロギングがイネーブルになっていない場合は、警告メッセージが表示され、それらのルールのトラフィック フロー イベントだけを検索できます。

- デバイスでサポートされている場合は、Access-Control Entry（ACE; アクセス コントロール エントリ）によって生成された syslog メッセージについて CS-MARS を照会するときに、Security Manager によって ACE ハッシュコードが追加キーワードとして使用されます。大きな Access-Control List（ACL; アクセス コントロール リスト）には、このようなハッシュコードが数千含まれる場合もあります。キーワードの数か、または ACE やシグニチャの送信元、宛先、およびプロトコルの合計数がクエリー制限の 150 を超えた場合は、エラー メッセージが表示されます。エラー メッセージには、考えられる原因と推奨アクションが示されます。

- 次の状況で、ルールとレポートされるイベントとの間で同期の問題が発生する場合があります。

  - デバイスが Security Manager に追加されましたが、それに対する設定または変更がデータベースに保存されていません。これは、デバイスが CS-MARS に追加されて以降に変更されたが展開されていないアクセス ルールの場合に特に該当します。

  - Security Manager 内に対応するルールがないアクセス ルールがデバイス上に存在するか、またはその逆です。すべてのデバイスが Security Manager に追加され、Security Manager を使用してデバイス上にアクセス ルールが設定されるようにします。

- ルールが定義されていない、イベントをトリガーしている「間違った」方向のトラフィック。たとえば、インバウンド トラフィック ルールだけが定義されている高いセキュリティ レベルのインターフェイスでのアウトバウンド トラフィックがあります。

- CS-MARS からポリシー検索を実行し、Security Manager クライアントがアクティブである場合、クエリーは、開かれているアクティビティまたは設定セッション内のすべてのポリシーと、データベースに保存されているポリシー（コミットされた設定）に対して実行されます。Security Manager クライアントがアクティブではない場合は、コミットされたポリシーだけが考慮されます。

関連項目

- CS-MARS と Security Manager を統合するためのチェックリスト （56 ページ）
- Security Manager ポリシーの CS-MARS イベントの検索 （62 ページ）
- Security Manager での CS-MARS サーバの登録 （58 ページ）

Security Manager ポリシーの CS-MARS イベントの検索

CS-MARS と Security Manager を統合したあと、特定のファイアウォール アクセス ルールまたは IPS シグニチャに関連する CS-MARS 内のイベントを検索できます。

CS-MARS がイベントを受信すると、イベントは解析され、「セッション化」されて、イベントバッファに書き込まれてから、データベースに書き込まれます。セッション化には2つの形式があります。セッション指向プロトコル（TCP など）では、セッションには初期ハンドシェイクから接続のティアダウンまでが含まれます。セッションレス プロトコル（UDP など）では、セッションの開始時刻と終了時刻は、制限された時間内で追跡される最初と最後のパケットに基づきます。時間外のパケットは、他のセッションの一部と見なされます。

新しく受信したデータと完全に処理されたデータには違いがあるため、リアルタイムイベントまたは過去イベントのいずれも検索できます。

- [リアルタイム（Real-time）]：イベントをキャッシュ内に最大2分間保持するためセッション化には時間がかかります。そのため、リアルタイム イベント クエリを使用して解析直後にイベントを表示し、受信した最新データへのアクセスを可能にします。

リアルタイム イベントを照会すると、クエリーは Security Manager から取得されたポリシー値に基づいて自動的に実行され、結果は CS-MARS の [Query Results] ウィンドウに表示されます。このリアルタイム イベント ビューアを使用して、未処理イベントがセッション化される前の CS-MARS へのストリーミング中に、最大 5 秒の遅延で、CS-MARS トラフィックをほぼリアルタイムでモニタできます。セッション化されたイベントストリームの表示を選択することもできます。そのためには、[クエリ結果（Query Results）] ウィンドウで [編集（Edit）] をクリックし、[リアルタイム（Realtime）] ドロップダウンメニューから [セッション化されたイベント（Sessionized events）] を選択します。セッション内のイベント数が多い場合には、遅延が長くなる可能性があります。

- [履歴（Historical）]：過去のイベントのレポートは、リアルタイムモニタリングで可能な期間よりも長期にわたる傾向を識別するのに役立ちます。過去のイベントを照会すると、CS-MARS の [Query Criteria: Result] ウィンドウが開きます。クエリをすぐに実行するか、あとで実行するために基準を「レポート」として保存できます。過去のイベントの場合、[Result Format] は [All Matching Events] オプションであり、[Filter By Time] 値は過去 10 分に設定されます。

次の項では、イベント検索についてより詳細に説明します。

- アクセス ルールの CS-MARS イベントの表示 （63 ページ）
- IPS シグニチャの CS-MARS イベントの表示 （66 ページ）

アクセス ルールの CS-MARS イベントの表示

Security Manager の **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]** ポリシーから、アクセスルールを選択し、CS-MARSの関連するイベント情報を表示できます。ルールと一致するリアルタイム イベントまたは過去のイベント、トラフィック フロー、送信元アドレス、または宛先アドレスを表示できます。アクセス ルールをサポートする任意のデバイス（ASA、PIX、FWSM、ルータ、スイッチなど）のイベントを表示できます。

ファイアウォール アクセス ルールは、順序が付けられたリストまたは表の形式で提供されます。展開されると、このポリシーはAccess-Control List（ACL; アクセス コントロール リスト）となります。リスト内の各エントリは、Access-Control Entry（ACE; アクセス コントロール エントリ）と呼ばれます（詳細については、アクセス ルールについてを参照してください）。

パケットを転送するかドロップするかを決定するときに、デバイスは、リストされている順序で各アクセス ルールに照らしてパケットをテストします。アクセス ルールに対してロギングをイネーブルにすると、テストの結果はルールごとのログ設定に従って記録されます。ASA などの一部のデバイスでは、ロギングを明示的に設定しない場合でも、拒否されたアクセスのログ エントリが生成されます。ロギング オプションを含むアクセス ルールの作成の詳細については、アクセス ルールの設定を参照してください。

次のタイプのトラフィックのアクセス ルールに関連するリアルタイム イベントまたは過去のイベントについて、CS-MARS を照会できます。コマンドを使用するには、ルールを右クリックしてコンテキスト メニューから選択します。

- [フロー（Flow）]：トラフィックフローは、ルールの送信元と宛先のIPアドレス、プロトコル、およびポートによって定義されます。レポートされるフローイベントには、接続の設定およびティアダウンが含まれます。この情報を記録するには、アクセスルールに対してロギングをイネーブルにする必要があります。

フロー関連のイベントを表示するには、次の右クリック コマンドを使用します。

- **[MARSイベントを表示（Show MARS Events）] > [リアルタイム（Realtime）] > [このフローに一致（Matching this Flow）]**：このトラフィックフローと一致するイベントについて CS-MARS でリアルタイムクエリーの結果を表示します。いつでも CS-MARS ウィンドウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- **[MARSイベントを表示（Show MARS Events）] > [過去（Historical）] > [このフローに一致（Matching this Flow）]**：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、選択したルールのトラフィックフローに基づいて読み込まれます。必要に応じてルールパラメータとクエリー基準を編集し、[適用（Apply）] をクリックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。

- [ルール（Rule）]：ルールに対してロギングがイネーブルの場合（[Advanced]/[Edit Options] ダイアログボックスを参照）、イベントをログに記録するために、（デバイスが CS-MARS によってモニタされていると想定する場合は）デバイスから CS-MARS に syslog メッセージが送信されます。このクエリーには、使用可能なキーワード情報などのアクセスルールパラメータが含まれています。レポートされるイベントには、接続の設定およびティアダウンは含まれません。

ルール関連のイベントを表示するには、次の右クリック コマンドを使用します。

- **[MARSイベントを表示（Show MARS Events）] > [リアルタイム（Realtime）] > [このルールに一致（Matching this Rule）]**：このルール（フローパラメータおよびキーワード）と一致するイベントについて、CS-MARS でリアルタイムクエリーの結果を表示します。結果は 5 秒以内にスクロールを開始します。いつでも CS-MARS ウィンドウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- [MARSイベントを表示（Show MARS Events）] > [過去（Historical）] > [このフローに一致（Matching this Flow）]：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、アクセルルール（フローパラメータおよびキーワード）に基づいて読み込まれます。必要に応じてルールパラメータとクエリー基準を編集し、[適用（Apply）] をクリックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。

- [送信元または宛先（Source or Destination）]：アクセスルールエントリの [送信元（Source）] セルまたは [宛先（Destination）] セルを右クリックした場合、ルールの送信元または宛先の IP アドレスと一致するリアルタイムイベントまたは過去のイベントを表示するように選択することもできます。

送信元または宛先アドレスのイベントを表示するには、[Source] セルまたは [Destination] セルのアドレスを右クリックし、次のコマンドのいずれかを選択します（選択するセルによってコマンドは異なります）。

- **[MARSイベントを表示（Show MARS Events）] > [リアルタイム（Realtime）] > [この送信元/宛先に一致（Matching this Source/Destination）]**：送信元または宛先アドレスが一致するイベントについて、CS-MARS でリアルタイムクエリーの結果を表示します。いつでも CS-MARS ウィンドウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- **[MARSイベントを表示（Show MARS Events）] > [過去（Historical）] > [この送信元/宛先に一致（Matching this Source/Destination）]**：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、アクセスルールの送信元または宛先アドレスに基づいて読み込まれます。必要に応じてルールパラメータとクエリー基準を編集し、[適用（Apply）] をク

リックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。

トラフィック フローまたはアクセス ルール イベント クエリーの基準として、Security Manager から CS-MARS に次の情報が提供されます。

- [Device details]：ホスト名、ドメイン名、管理 IP アドレス、表示名などのデバイスに関する一般情報。
- [Source addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの送信元アドレス。
- [Destination addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの宛先アドレス。
- [Service]：プロトコルおよびポート情報。
- [イベントタイプ（Event Type）]：許可ルールの場合は「構築/ティアダウン/許可された IP 接続」、拒否ルールの場合は「セキュリティポリシーによってパケットを拒否」。
- [Keyword]（ルール イベントだけ。トラフィック フロー クエリーには提供されない）：論理演算子 OR で接続された ACL 名および ACE ハッシュコード（使用可能な場合）。

バージョン 7.0 以降の PIX および ASA デバイスでは、各アクセス ルールには MD5 ハッシュコードが割り当てられます。これは、そのルールによって生成される syslog に含まれています。大規模な ACL には数千のアクセス ルールを含めることができます。クエリーのキーワードとして使用すると、これらのハッシュコードは、より正確なイベント一致を生成するのに役立ちます。デバイスでハッシュコードがサポートされていない場合、キーワードがあいまいであるためクエリー結果が不正確な可能性があるという警告が表示されます。クエリーを続行し、クエリー キーワード リストを編集して送信し直します。

ヒント：

- 一度に照会できるアクセス ルールは 1 つだけです。
- セキュリティ デバイスで NAT または PAT が設定されている場合、送信元アドレスと宛先アドレスは変換前および変換後のアドレスにマッピングされ、Security Manager から CS-MARS にクエリーが送信されるときは変換後のアドレスが使用されます。インバウンド アクセス ルールの場合、宛先アドレスは変換前アドレスと見なされ、アウトバウンド アクセス ルールの場合、送信元アドレスは変換後アドレスと見なされます。
- デバイスが複数の CS-MARS コントローラによってモニタされている場合は、使用する CS-MARS インスタンスを選択するように要求されます。
- システムでのクレデンシャル検証の設定方法によっては、CS-MARS にログインするように要求される場合があります。詳細については、Security Manager での CS-MARS サーバの登録 （58 ページ）を参照してください。

関連項目

- [Access Rules] ページ
- CS-MARS イベントからの Security Manager ポリシーの検索 （67 ページ）
- アクセス ルールの CS-MARS イベントの表示 （63 ページ）

IPS シグニチャの CS-MARS イベントの表示

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

着信トラフィックを設定済みのシグニチャと比較することにより、IPS または IOS IPS デバイスによってネットワーク侵入が検出およびレポートされると、デバイス上で syslog メッセージが生成されます。デバイスが CS-MARS によってモニタされている場合、シグニチャに関連付けられたログがデバイスから取得されたあと、CS-MARS でインシデントが生成されます。特定のシグニチャに関連付けられたイベントを検索すると、攻撃を迅速に識別し、デバイス設定を調整して侵入を最小限に抑えるか、または防止できます。

レポートされたネットワーク侵入イベントを CS-MARS で表示するには、Security Manager のデバイスの Signatures ポリシーで 1 つ以上のエントリを選択し、CS-MARS の [Query] ページにナビゲートしてリアルタイム イベントおよび過去のイベントを表示します。

シグニチャのリアルタイム イベントを検索すると、クエリーが自動的に実行され、結果が CS-MARS に表示されます。ただし、シグニチャの過去のイベントを検索すると、Security Manager から CS-MARS に送信される値が、クエリー フィールドへの読み込みに使用されます。必要に応じてクエリー フィールドを変更し、クエリーを実行するか、あとで使用するために保存できます。

クエリー基準として、Security Manager から CS-MARS に次のシグニチャ情報が提供されます。

- [Device details]：ホスト名、ドメイン名、管理 IP アドレス、表示名などのデバイスに関する一般情報。
- [Keyword]：シグニチャ ID、サブシグニチャ ID、および仮想センサー名（該当する場合）。

仮想センサーの場合、センサーの名前がキーワード基準として他のデバイス情報およびシグニチャ パラメータとともに含まれます。

関連項目

- CS-MARS イベントからの Security Manager ポリシーの検索 （67 ページ）
- アクセス ルールの CS-MARS イベントの表示 （63 ページ）

ステップ 1 （デバイス ビュー）IPS または IOS IPS デバイスを選択して、[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）] を選択し、[Signatures] ページを表示します。

ステップ 2 シグニチャテーブルで目的のエントリを右クリックするか、または複数のエントリを選択してそのうちの 1 つを右クリックし、[MARS イベントの表示（Show MARS Events）] メニューから次のコマンドのいずれかを選択します。

- [リアルタイム（Realtime）]：このシグニチャと一致するイベントについて CS-MARS でリアルタイムクエリーの結果を表示します。5 秒以内にこの結果のスクロールが開始されます。CS-MARS へのストリーミング中の未処理イベントを表示するには、このオプションを使用します。

いつでも CS-MARS の [Query Results] ウィンドウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- [履歴（Historical）]：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、シグニチャパラメータに基づいて読み込まれます。必要に応じてパラメータとクエリー基準を編集し、[Apply] をクリックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。クエリーは編集でき、あとで再度実行する場合はレポートとして保存できます。

ヒント：

- シグニチャがディセーブルの場合、警告が表示され、イベント検索に進むかどうかが確認されます。
- デバイスが複数の CS-MARS コントローラによってモニタされている場合は、使用する CS-MARS インスタンスを選択するように要求されます。
- システムでのクレデンシャル検証の設定方法によっては、CS-MARS にログインするように要求される場合があります。詳細については、Security Manager での CS-MARS サーバの登録 （58 ページ）を参照してください。
- カスタムシグニチャはすべて、CS-MARS では「Unknown Device Event Type」イベントとして分類されます。
- IPS デバイスを Security Manager インベントリに追加するとき、または設定済みの IPS ポリシーをデバイスから削除するときに、IPS ポリシーを検索しない場合は、デフォルトのシグニチャがデバイスに割り当てられます。デフォルトのシグニチャからイベントを検索しようとすると、「Policy not found」というエラーメッセージが表示されます。ただし、デフォルトのシグニチャを編集して保存すると、CS-MARS で関連するイベントを照会できます。
- タイプが Packet Data および Context Data のイベントはシグニチャ ルールによってトリガーされないため、これらのイベントはクエリー結果に表示されません。

CS-MARS イベントからの Security Manager ポリシーの検索

『User Guide for Cisco Security MARS Local and Global Controllers』には、CS-MARS に表示されているイベントに基づいてポリシーを検索する方法についての詳細情報が記載されています。この情報には、起こりうる問題を解決するのに役立つ広範なトラブルシューティング情報と、相互作用をイネーブルにするために CS-MARS で設定する必要がある項目のチェックリストが含まれています。

ポリシー検索を実行する主な理由は、ポリシーが生成しているイベントに基づいてポリシーを調整することです。たとえば、アクセスルールにより、実際には許可すべきトラフィックがドロップされることがあります。イベントが表示中であるため、そのイベントを発生させているポリシーがあることがわかります。数回のクリックで、そのイベントから再設定する必要があるポリシーにたどり着くことができます。

デバイスで生成されたイベントに基づいてポリシーを検索するための一般的なプロセスは次のとおりです。ポリシー検索を実行するには、Security Manager クライアントがシステムにインストールされている必要があることに注意してください。

関連項目

- アクセス ルールの CS-MARS イベントの表示 （63 ページ）
- IPS シグニチャの CS-MARS イベントの表示 （66 ページ）

ステップ 1 CS-MARS の [Query Results] または [Incident Details] ページでイベントを検索します。

アクセス ルールの照会に使用できる syslog および NetFlow イベントの詳細については、次の項を参照してください。

- ポリシー検索に対してサポートされるシステム ログ メッセージ （69 ページ）
- CS-MARS での NetFlow イベント レポート （71 ページ）

ステップ 2 イベントの [Reporting Device] セルにある [Security Manager] アイコンをクリックします。CS-MARS の設定によっては、Security Manager へのログインを求められる場合があります。

Security Manager で複数のデバイスがイベントの特性と一致する場合は、デバイスを選択するように求められます。

ステップ 3 詳細情報が Security Manager から取得され、イベントがアクセス ルールに関するものか、または IPS シグニチャに関するものかに応じて表示されます。

- **アクセルルール**：アクセスルールが CS-MARS の読み取り専用ウィンドウに表示され、イベントと一致するルールが強調表示されます。

ルールを編集する場合は、ルール番号をクリックします。Security Manager クライアントの Access Rule ポリシーにルールが表示されます。ルールを編集して保存し、設定を展開できます。変更内容を展開するまで、デバイスに対して変更は行われません。

アクセス ルールの設定の詳細については、アクセス ルールの設定を参照してください。

- **IPS シグニチャ**：シグニチャ詳細が CS-MARS の読み取り専用ウィンドウに表示されます。

シグニチャを編集するには、[シグニチャの編集（Edit Signature）] をクリックします。シグニチャポリシーにシグニチャが表示され、変更できるようになります。詳細については、シグニチャ パラメータの編集（シグニチャの調整）を参照してください。

特定のアクションをイベントから削除するか、またはイベントを完全に削除してセンサーが処理できないようにする場合は、[フィルタの追加（Add Filter）] をクリックします。Security Manager で [Add Event Filter]

ダイアログボックスが開き、イベント フィルタを設定できます。詳細については、[Add Filter Item]/[Edit Filter Item] ダイアログボックスを参照してください。

アクセス ルールと同様に、変更内容は、新しい設定を展開するまで有効になりません。

ポリシー検索に対してサポートされるシステム ログ メッセージ

セキュリティ アプライアンスおよび IOS デバイスでアクセス ルールを設定するときに、[Advanced]/[Edit Options] ダイアログボックスで、システム ログ（syslog）メッセージを生成するロギング オプションを設定できます。複数のコンテキストを持つデバイスでは、各セキュリティ コンテキストに独自のロギング設定が含まれ、独自のメッセージが生成されます。Security Manager が CS-MARS と相互に機能するように設定されている場合、これらのメッセージは CS-MARS にレポートされ、レポートされた情報をルールごとに照会できます。

これらのメッセージ ID の詳細については、該当する製品マニュアルの『System Message Guide』を参照してください。

セキュリティ アプライアンス メッセージ

セキュリティ アプライアンス syslog メッセージはパーセント記号（%）で始まり、その構造は次のとおりです。

```
%{ASA | PIX | FWSM}-Level-Message_number: Message_text
```

次に例を示します。

```
%ASA-2-302013: Built outbound TCP connection 42210
for outside:9.1.154.12/23 (9.1.154.12/23) to inside:2.168.154.12/4402 (192.168.154.12/4402)
```

これらのメッセージの前に追加情報（日付やタイムスタンプなど）が付加されることに注意してください。具体的な追加情報は、デバイスのタイプによって異なります。

各メッセージは一意の 6 桁の数字（前の例では 302013）によって識別されます。Security Manager から CS-MARS へのクエリーでは、次のセキュリティ アプライアンス syslog メッセージ ID がサポートされます。セキュリティ アプライアンスのロギング レベルを変更した場合、これらのメッセージは新しいレベルで生成されます。

メッセージ ID	メッセージ
106023	IP パケットがアクセス ルールによって拒否されました。このメッセージは、ルールに対してロギングがイネーブルにされていない場合でも記録されます。これは、デフォルトのロギング オプションです。
106100	IP パケットがアクセス ルールによって許可または拒否されました。[Advanced]/[Edit Options] ダイアログボックスでルールに対して定義されているロギング レベルに基づいて、追加情報が提供されます。

メッセージ ID	メッセージ
302013	2 つのホスト間の TCP 接続が確立されました。
302014	2 つのホスト間の TCP 接続がティアダウンされました。
302015	2 つのホスト間の UDP 接続が確立されました。
302016	2 つのホスト間の UDP 接続がティアダウンされました。
302020	2 つのホスト間の ICMP 接続が確立されました。
302021	2 つのホスト間の ICMP 接続がティアダウンされました。

ルータ メッセージ

Cisco IOS ルータでも、アクセス ルールに対して syslog メッセージが生成されます。アクセス リストをトリガーする最初のパケットによって、即座にロギング メッセージが生成され、後続パケットは表示または記録されるまで5分間隔で収集されます。各ロギング メッセージには、アクセス リスト番号、パケットが許可されたか拒否されたか、パケットの送信元IPアドレス、および前の 5 分間隔で許可または拒否されたその送信元からのパケットの数が含まれます。

Security Manager から CS-MARS へのクエリーでは、次の IOS syslog メッセージ ID がサポートされます。

%SEC-6-IPACCESSLOGP	特定のアクセス リストのログ基準と一致するパケットが検出されました（TCP および UDP）。
%SEC-6-IPACCESSLOGS	特定のアクセス リストのログ基準と一致するパケットが検出されました（IP アドレス）。
%SEC-6-IPACCESSLOGDP	特定のアクセス リストのログ基準と一致するパケットが検出されました（ICMP）。
%SEC-6-IPACCESSLOGNP	特定のアクセス リストのログ基準と一致するパケットが検出されました（その他のすべての IPv4 プロトコル）。

（注） 過剰な数の syslog が生成されて CS-MARS にレポートされている場合は、[Advanced]/[Edit Options] ダイアログボックスを使用して、最も多くのメッセージを生成しているアクセス ルールのロギング レベルを変更します。生成されるメッセージのタイプを制限するために、デバイスのロギング ポリシーの変更を考慮することもできます。

CS-MARS での NetFlow イベント レポート

CS-MARS でのイベント レポートに、ASA 8.1+ デバイスからの NetFlow イベントを含めることができます。

NetFlow Security Event Logging では、高性能環境でセキュリティ テレメトリを効率的に配信するために、NetFlow バージョン 9 のフィールドおよびテンプレートが使用されます。NetFlow Security Event Logging は、syslog メッセージングよりも拡張性が高く、記録されるイベントについて同様に詳細な情報を提供します。ASA NetFlow 実装では、定期的な間隔でフローに関するデータがエクスポートされるのではなく、フローの寿命の中で重大なイベントだけがエクスポートされます。次のフロー イベントがエクスポートされます。

- フロー作成
- フロー ティアダウン
- アクセス ルールによって拒否されたフロー

ASA は syslog メッセージもエクスポートしますが、これには同じ情報が含まれています。デバイスで NetFlow をイネーブルにする場合、同等の syslog メッセージをディセーブルにすることを検討できます。同等の syslog メッセージをディセーブルにすると、同じイベントを表す NetFlow レコードと syslog メッセージの両方を生成および処理することによりパフォーマンスが低下する可能性を回避できます。次の表に、syslog メッセージおよび同等の NetFlow イベントを示します。NetFlow イベント ID および拡張イベント ID も示します。NetFlow と同等の syslog メッセージをディセーブルにする方法については、[Server Setup] ページを参照してください。

syslog ID	syslog の説明	NetFlow イベント ID	拡張イベント ID
302013302015302017302020	TCP、UDP、GRE、および ICMP 接続の作成。	1 = フロー作成	0 = 無視
302014302016302018302021	TCP、UDP、GRE、および ICMP 接続のティアダウン。	2 = フロー削除	0 = 無視、または > 2000 = ASP ドロップ理由
710003	デバイスインターフェイスへの接続の試行が拒否されました。	3 = フロー拒否	1003 = 設定により To-the-box フローが拒否されました。
106015	最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。	3 = フロー拒否	1004 = 最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。

syslog ID	syslog の説明	NetFlow イベント ID	拡張イベント ID
313001	デバイスへの ICMP パケットが拒否されました。	3 = フロー拒否	1003 = 設定により To-the-box フローが拒否されました。
313008	デバイスへの ICMP v6 パケットが拒否されました。	3 = フロー拒否	1003 = 設定により To-the-box フローが拒否されました。
106023	アクセス グループ コマンドでインターフェイスに付加されたアクセス リストによってフローが拒否されました。	3 = フロー拒否	1001 = フローが入力 ACL によって拒否されました。1002 = フローが出力 ACL によって拒否されました。
106100	アクセス ルールがヒットしました。	1 = フローが作成されました（ACL がフローを許可した場合）。3 = フローが拒否されました（ACL がフローを拒否した場合）。	0 = フローが ACL によって許可されている場合。1001 = フローが入力 ACL によって拒否されました。1002 = フローが出力 ACL によって拒否されました。

Flow Denied NetFlow イベントの場合、次の表に示すように、拡張イベント ID によって拒否の理由が示されます。

拡張イベント ID	イベント	説明
1001	フロー拒否	フローが入力 ACL によって拒否されました。
1002	フロー拒否	フローが出力 ACL によって拒否されました。
1003	フロー拒否	インターフェイス サービスへの接続の試みがセキュリティ アプライアンスによって拒否されました。たとえば、このメッセージは、セキュリティ アプライアンスが、権限のない SNMP 管理ステーションからの SNMP 要求を受信したときに（サービス SNMP とともに）表示されます。
1004	フロー拒否	最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。

拡張イベント ID	イベント	説明
> 2000	フロー削除	2000 を超える値は、フローが終了したさまざまな理由を表します。

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。