ヘルスとパフォーマンスのモニタリング

Health and Performance Monitor（HPM）アプリケーションを使用すると、デバイスのステータスとトラフィック情報をネットワークレベルで可視化することで、ASA デバイス、IPS デバイス、および VPN サービスの主要な正常性データとパフォーマンスデータを監視できます。

すべてのデバイス、ファイアウォールデバイス、IPS デバイス、VPN サマリなど、さまざまなビューが提供され、独自のカスタマイズされたビューを作成できます。デバイスアラートの設定可能なリストも利用できます。

この機能を使用して、主要なネットワークとデバイスのメトリックを監視することで、ネットワーク内のデバイスの誤動作やボトルネックをすばやく検出して解決できます。

この章は次のトピックで構成されています。

- Health and Performance Monitor の概要　（1 ページ）
- HPM アクセス制御　（4 ページ）
- 正常性とパフォーマンスのモニタリングの準備　（5 ページ）
- Health and Performance Monitor の起動　（6 ページ）
- 監視対象デバイスの管理　（6 ページ）
- HPM ウィンドウ　（7 ページ）
- デバイスのモニタリング　（27 ページ）
- アラートと通知　（41 ページ）
- SNMP トラップ転送通知　（56 ページ）

Health and Performance Monitor の概要

Health and Performance Monitor は、他のスタンドアロン Cisco Security Manager アプリケーション（ダッシュボード、Configuration Manager、イベントビューア、Report Manager、および Image Manager）から、または Windows のスタートメニューからアクセスする Cisco Security Manager クライアントのログイン画面から起動できるスタンドアロン アプリケーションです。

HPM アプリケーションは、イベントビューアおよび Report Manager アプリケーションを補完します。以下を参照してください。

- **イベントビューア**：ASA および FWSM デバイス、それぞれのセキュリティコンテキストの syslog（システムログ）イベント、さらに IPS デバイスおよび仮想センサーの Secure Device Event Exchange（SDEE）イベントを対象にネットワークをモニターします。対象イベントには、ファイアウォール トラフィック情報、NAT イベント、フェイルオーバーイベント、IPS アラートなどが含まれます。イベントビューアは、この情報を収集して表示し、さまざまなビューに編成します。詳細については、Event Viewer 機能の概要を参照してください。
- **Report Manager**：ASA および IPS デバイス、リモートアクセス IPsec および SSL VPN のネットワーク使用状況とセキュリティ情報を収集、表示、およびエクスポートします。各レポートには、上位の送信元、宛先、攻撃者、被害者などのセキュリティデータ、および上位の帯域幅、期間、スループットユーザーなどのセキュリティ情報が集約されます。データは、時間別、日別、および月別の期間でも集約されます。詳細については、レポート管理についてを参照してください。
- **Health and Performance Monitor**（HPM）：ネットワーク内の ASA および IPS デバイスの主要な正常性、パフォーマンス、および VPN データを監視および表示します。この情報には、メモリ使用量、インターフェイスステータス、ドロップされたパケット、トンネルステータスなど、重大な問題と重大ではない問題が含まれます。また、デバイスを通常または優先監視用に分類し、優先デバイスに異なるアラートルールを設定できます。

表示されたアラートにメモを追加したり、アラートを「確認」したり、削除したりできます。アラートがクリアされると、[アラート（Alerts）] の表示から削除されます。ただし、アラート情報はデータベースに 30 日間保持されます。メモの追加、アラートの確認とクリアの詳細については、アラート：確認応答とクリア （54 ページ）を参照してください。

（注） アラート：履歴 （55 ページ）の説明に従い、[アラート履歴（Alerts History）] ウィンドウを使用して、以前クリアされたアラートにアクセスして表示できます。

ここでは、次の内容について説明します。

- トレンド情報 （2 ページ）
- マルチコンテキストのモニタリング （3 ページ）

トレンド情報

Health and Performance Monitor は、監視対象デバイスを定期的にポーリングして、ステータスとパフォーマンスデータを取得します。この情報はアラートの生成に使用されるほか、集計データに基づいてリアルタイムビューと過去の傾向を表示するために使用されます。

特定のメトリックセットに関する傾向が、グラフで表示されます。現在選択されているデバイスの各傾向が、選択した時間間隔で生成されたグラフとして表されます。たとえば、CPU およびメモリ使用量の現在の値と週平均を比較することで、選択したデバイスの運用に関するコン

テキストが得られます。監視対象デバイスで利用可能な傾向の間隔は、1時間、24時間、および1週間です。

傾向の生成に使用される指標には、次のものがあります。

- CPU 使用率
- メモリ使用量（シングルコンテキスト デバイスのみ）
- 1 秒あたりの接続数（ファイアウォールデバイス）
- 1 秒あたりの翻訳数（ファイアウォールデバイス）
- インスペクションの負荷（IPS デバイス）
- 欠落したパケットの割合（IPS デバイス）
- VPN トンネルの数
- RA VPN セッションの数
- VPN の合計スループット
- ファイアウォールのスループット
- ドロップされたパケットの総数（ファイアウォール インターフェイス）

特定のデバイスのヘルスとパフォーマンスに関して、その他のグラフィック情報を確認するには、デバイス、クラスターノード、またはマルチコンテキストデバイスのシステムコンテキストのエントリを右クリックし、ポップアップメニューから [デバイスマネージャ（Device Manager）] を選択することで、関連するデバイスマネージャを起動できます。デバイスマネージャの詳細については、デバイス マネージャの起動を参照してください。

マルチコンテキストのモニタリング

Health and Performance Monitor は、単一および複数のコンテキストの ASA デバイスをモニターできます。マルチコンテキストデバイスの場合、各コンテキストがモニターされ、個別のデバイスとして表示されます。

各コンテキストは、該当するすべてのメトリックに対して個別にポーリングされます。HPM は、任意のデバイスから一度に最大 5 つのコンテキストをポーリングします。5 つ以上のコンテキストを持つデバイスの場合、データは5つのコンテキストの連続する各バッチから取得され、各バッチは連続するポーリングサイクル中に徐々にポーリングされます。これは、すべてのコンテキストが同時に更新されない可能性があることを意味します。

マルチコンテキストデバイスの場合、基本的な Device Health（メモリ使用量、デバイスステータスなど）は物理デバイスでのみ（つまり、システムコンテキストから）モニターされますが、トラフィックデータ（接続数、変換数、ドロップされた数）は、コンテキストレベルでモニターされます。

仮想コンテキストの場合、CPU使用率データはパターン分析にのみ使用され、アラート生成には使用されません。仮想コンテキストについては、インターフェイス ステータス アラートのみが生成されます。

HPM アクセス制御

ユーザー名に対して割り当てられる権限により、Health and Performance Monitor で行うことができる操作が制御されます。ローカルユーザーまたは他のタイプの ACS 以外のアクセスコントロールを使用している場合は、すべてのユーザーが HPM にアクセスできます。ただし、次のアクセス制限が課されます。

- Security Manager でヘルスとパフォーマンスのモニタリングを有効または無効にするには、[Health and Performance Monitor] ページで説明されているように、システム管理者権限が必要です。
- デバイスを監視対象として選択または選択解除するためには、監視対象デバイスの管理 （6 ページ） で説明されているように、システム管理者、ネットワーク管理者、または承認者権限が必要です。
- アラートと通知を構成するには、アラート：設定 （44 ページ） で説明されているように、システム管理者、ネットワーク管理者、または承認者権限も必要です。

ACS を使用して Security Manager へのアクセスを制御する場合は、次も制御できます。

- [表示（View）] > [Health and Performance Monitor] 権限（ACS の Role Management の一部）を使用して、Health and Performance Monitor アプリケーションへのアクセスを制御できます。この権限を使用して、特定のユーザーが HPM にアクセスできないようにしたり、イベントビューアまたは Report Manager へのアクセスを許可せずに HPM へのアクセスを許可するロールを作成したりすることができます。すべてのデフォルトの ACS ロールは、Health and Performance Monitor アプリケーションの使用が許可されています。
- [変更（Modify）] > [ポリシー（Policy）] > [HPMモニタリング（HPM Monitoring）] 特権を使用して、監視対象のデバイスを選択および選択解除できるユーザーを制御したり（監視対象デバイスの管理 （6 ページ）を参照）、アラートと通知を設定したり（アラート：設定 （44 ページ）を参照）、アラートに注釈を付けて確認したり（アラート：確認応答とクリア （54 ページ）を参照）することができます。ヘルプデスクとスーパー管理者を除くすべてのデフォルトの ACS ロールには、この権限があります。
- ユーザーは、少なくともデバイスの表示権限を持っている場合にのみ、デバイスの正常性とパフォーマンスの情報を表示できます。
- [Health and Performance Monitor] ページで説明されているように、HPM を有効化または無効化するヘルスとパフォーマンスのモニタリングの管理設定ページ（Security Manager の Configuration Manager 内）へのアクセスを制御できます。このページ（またはその他の管理設定ページ）にアクセスするには、ユーザーは[変更（Modify）]>[ポリシー（Policies）] >[HPM管理者（HPM Admin）]権限を持っている必要があります。ヘルプデスクを除くすべてのデフォルト ACS ロールがこのページを表示できますが、設定を変更できるのはシステム管理者だけです。

Cisco Security Manager と Cisco Secure ACS との統合の詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。

正常性とパフォーマンスのモニタリングの準備

Health and Performance Monitor（HPM）を使用するには、次のように Security Manager を設定し、HPM アプリケーションを有効にし、デバイスモニタリングを設定する必要があります。

- ACL ドロップパケット、スキャン脅威ドロップパケット、インスペクション ドロップ パケット、および SYN 攻撃ドロップパケットなどのメトリックを監視するには、基本脅威検出を ASA 8.0 以降のデバイスで有効にする必要があります（基本脅威検出は、デフォルトで有効になっています）。
- 電子メールでアラート通知を受信するには、Security Manager サーバーの [システム設定（System Preferences）] ページで、SMTP サーバーと管理者の電子メール ID を設定しておく必要があります。詳細については、『*Installation Guide for Cisco Security Manager*』を参照してください（Health and Performance Monitor アプリケーションからのアラート通知用電子メールアドレスの指定については、アラート：設定 （44 ページ）で説明されています）。
- [Health and Performance Monitor] ページで説明されているように、Security Manager で正常性とパフォーマンスのモニタリングを有効にする必要があります。
- 監視対象デバイスの管理 （6 ページ）で説明されているように、HPM で、通常モードと優先モードの両方でモニタリングするデバイスを指定します。

（注） ASA の読み取りタイムアウトを防ぐには、PIX ファイアウォール、ASA、および FWSM デバイスでの SSL（HTTPS）の設定で説明されているように、該当するデバイスが、サーバーとして動作するときに特定の SSL/TLS プロトコルバージョンのみを使用するように設定する必要があります。

- アラートと電子メール通知がトリガーされるタイミングを定義するデバイスのしきい値と状態変更ルールを有効にして設定します。このプロセスについては、アラート：設定 （44 ページ）で説明します。

（注） また、タイミングの同期のため、Network Time Protocol（NTP）サーバーを使用するようにモニタリング対象デバイスを設定することをお勧めします。詳細については、[NTP] ページを参照してください。

これらの手順を完了すると、HPM は指定されたデバイスのポーリングを開始し、正常性情報とアラートを表示します。

Health and Performance Monitor の起動

Health and Performance Monitor（HPM）を使用して、ネットワーク全体で監視対象のファイアウォールおよびIPSデバイスから収集されたステータス情報とアラートを表示します。モニタ対象のデバイスの選択の詳細については、監視対象デバイスの管理 （6 ページ）を参照してください。

HPM を起動するには、次のいずれかを実行します。

- Windows の [スタート] メニューから [すべてのプログラム] > [Cisco Security Manager Client] > [Cisco Security Manager Client] を選択し（コマンドパスは若干異なる場合があります）、ログイン時のデフォルトビューとして [Health and Performance Monitor] を選択します。
- Configuration Manager、イベントビューア、Image Manager、または Report Manager アプリケーションから、[起動（Launch）] > [Health and Performance Monitor] を選択します。
- Configuration Manager または Image Manager ウィンドウのクイック起動ツールバーにある [Health and Performance Monitor] ボタンをクリックします。

現在 Security Manager アプリケーションにログインしていない場合は、ログインするように求められます（Security Manager クライアント アプリケーションの起動とログインの詳細については、Security Manager へのログインおよび終了を参照してください）。それ以外の場合、他のアプリケーションへのログインに使用したのと同じユーザーアカウントを使用して、HPM ウィンドウ （7 ページ）が開きます。

（注） 前述のように、HPM は他の Security Manager クライアント アプリケーションから「相互起動」できます。[起動（Launch）] メニューから目的のアプリケーションを選択するか、適切なクイック起動ボタンをクリックすることにより、Health and Performance Monitor から他のクライアント アプリケーションを同様に相互起動できます。

監視対象デバイスの管理

HPM デバイスセレクタは、「通常」と「優先」の両方の監視リストにデバイスを追加および削除するために使用されます。また、デバイスセレクタを使用して、2 つのリスト間でデバイスを転送できます。

（注） HPM でデバイスの監視を有効にした後、HPM パラメータの実際の値が [デバイスの概要（Device 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。

HPM デバイスセレクタを使用するには、次の手順を実行します。

ステップ 1 [ツール（Tools）] メニューから [デバイスセレクタ（Device Selector）] を選択して、[デバイスセレクタ（Device Selector）] ウィンドウを開きます。デバイス管理画面が表示されます。

左側の [すべてのデバイス（All Devices）] セクションには、Cisco Security Manager インベントリ内の監視可能なすべての ASA デバイスと IPS デバイスが一覧表示されます。（例：HPM は、バージョン 7.0.1 以降の IPS センサーの監視のみをサポートします。以前の IPS バージョンはデバイスセレクタに表示されません）。

現在、通常監視リストと優先監視リストに割り当てられているすべてのデバイスが、ウィンドウの右側にある 2 つのセクションに表示されます。

ステップ 2 [通常（Normal）] リストにデバイスを追加するには、[すべてのデバイス（All Devices）] リストでデバイスを選択し、[すべてのデバイス（All Devices）] リストと [通常監視対象デバイス（Normal Monitored Devices）] リストの間にある [>] ボタンをクリックします。

デバイスを [優先監視対象デバイス（Priority Monitored Devices）] リストに移動する手順も同じです。[すべてのデバイス（All Devices）] リストと [優先監視対象デバイス（Priority Monitored Devices）] リストの間にある [>] ボタンを使用します。

ステップ 3 いずれかの [監視対象（Monitored）] リストからデバイスを削除して [すべてのデバイス（All Devices）] リストに戻すには、デバイスを選択して適切な [<] ボタンをクリックします。

ステップ 4 1 つの [監視対象（Monitored）] リストから別のリストにデバイスを転送するには、そのエントリを強調表示し、[上へ（Up）] または [下へ（Down）] ボタンをクリックして、上位または下位のリストに移動します。

ステップ 5 ウィンドウの下部にある [次へ（Next）] をクリックして、[VPNセレクタ（VPN-selector）] 画面を表示します。

すべての監視対象デバイスと個々のコンテキスト（ある場合）が一覧表示されます。各エントリには、リモートアクセス（RA）用のチェックボックスと、サイト間（S2S）VPN 選択用のチェックボックスが含まれています。

（注） Cisco Security Manager 4.10 以降、ASA 9.5(2) 以降のすべてのコンテキストがデバイスセレクタに一覧表示されます。デバイスセレクタで対応するチェックボックスをオンにすることで、すべてのユーザーコンテキストの RA およびサイト間 VPN を監視できるようになりました。

リストフィルターフィールドの使用 （25 ページ）の説明に従い、このページの [リストフィルタ（List Filter）] フィールドを使用してリストをフィルタ処理できます。

ステップ 6 適切なボックスをオンにして、特定のデバイスで監視する VPN のタイプを選択します。

ステップ 7 [保存（Save）] をクリックして変更を保存して適用し、デバイスセレクタを閉じます。

HPM ウィンドウ

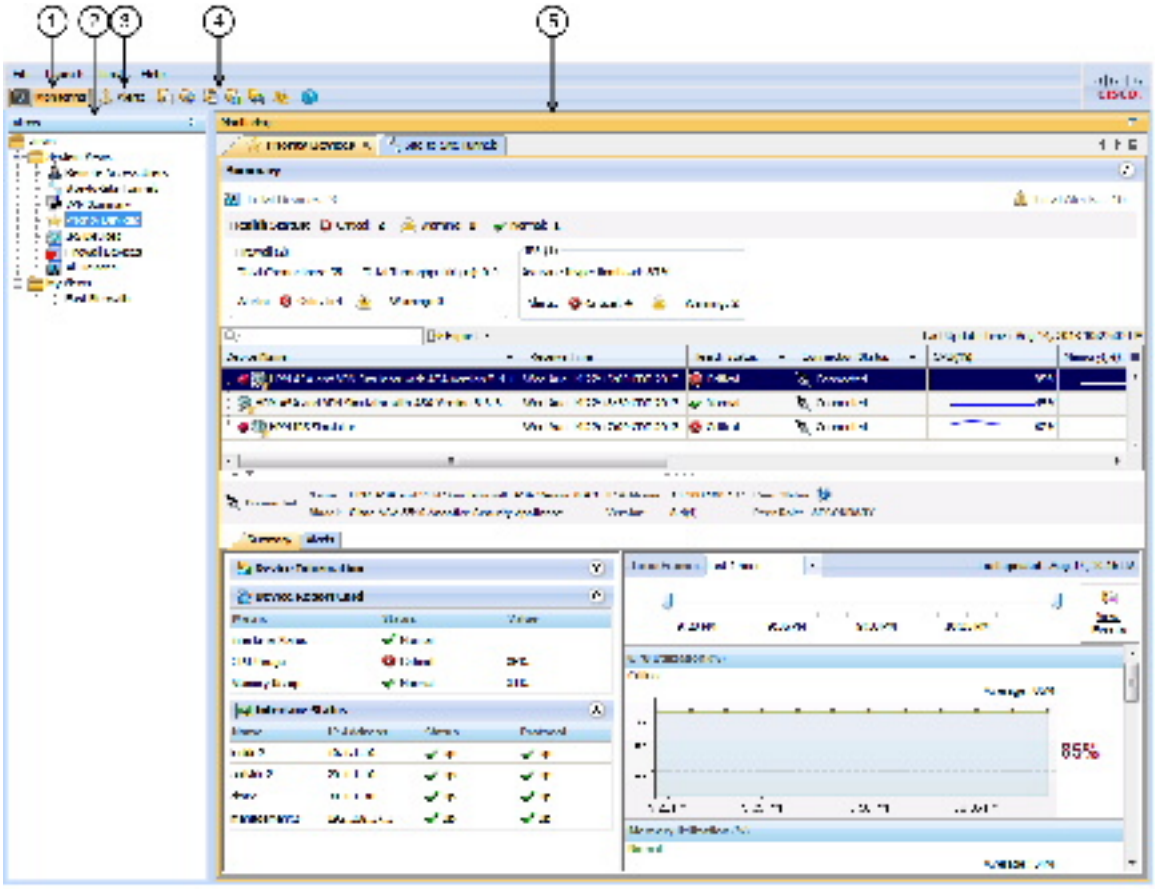
[ヘルスとパフォーマンスのモニタ（HPM）アプリケーション（Health and Performance Monitor (HPM) application）] ウィンドウでは、監視対象のファイアウォールおよび IPS デバイスから収

集されたステータス情報とアラート、およびネットワーク全体のリモートアクセス（RA）およびサイト間（S2S）VPN 情報を表示できます。

（注） 監視するデバイスの指定については、監視対象デバイスの管理 （6 ページ）を参照してください。

次の図は、[HPM] ウィンドウの主な機能を示しています。

図 *1 : [*ヘルスとパフォーマンスのモニタ（*Health and Performance Monitor***）*]* ウィンドウ**



[ヘルスとパフォーマンスのモニタ（Health and Performance Monitor）] ウィンドウ

1	**モニタリングボタン。**	**4**	**クイック起動ボタン。**
2	ビュー	5	モニタリング/アラート表示エリア。
3	アラートボタン。		

[HPM] ウィンドウは、次の 3 つの主要な要素で構成されています。

- **監視ボタン（1）**：このボタンをクリックして、デバイスとVPNの正常性とパフォーマンスのデータを表示します。詳細については、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）を参照してください。
- **ビュー（2）**：モニタリングビューでは、HPMメインウィンドウの左ペインに使用可能なビューのリストが表示されます。詳細については、デバイスビューの管理 （27 ページ）を参照してください。

次の図に示します。

- **アラートボタン（3）**：このボタンをクリックすると、ウィンドウの表示エリアにアラートのテーブルが表示されます。詳細については、HPM ウィンドウ：アラートディスプレイ （42 ページ）を参照してください。
- **クイック起動ボタン（4）**：任意のボタンをクリックして、関連するSecurity Managerクライアント アプリケーションを相互起動します。
- **モニタリング/アラート表示エリア（5）**：ウィンドウのこのセクションには、デバイスとVPNのモニタリング情報、またはモニタリング対象デバイスによって生成されたアラートのテーブルが表示されます。[モニタリング（Monitoring）] ボタンと [アラート（Alerts）] ボタンを使用して、これら 2 つの表示を切り替えることができます。

テーブル列の操作

HPM に表示されるさまざまな情報テーブルは、次のようにカスタマイズできます。

- 特定の列のエントリが昇順または降順になるようにテーブルをソートします。
  - 列の見出しで、ドロップダウン メニュー ボタン以外の任意の場所をクリックすると、列のエントリが昇順になるようにテーブルがソートされます（小さな灰色の上矢印で示されます）。
  - 見出しを再度クリックすると、エントリが降順にソートされます（小さな灰色の下矢印で示されます）。
  - 見出しを再度クリックすると、テーブルが元の表示順序に戻ります（矢印アイコンが削除されます）。
- さまざまな列を表示したり非表示にします。表示できる列は各テーブルで異なります。
- 列にフィルタを適用します。つまり、指定した条件に一致するエントリのみがテーブルに表示されるようにします。

ここでは、次の内容について説明します。

- テーブル列の表示と非表示 （10 ページ）
- 列ベースのフィルタリング （22 ページ）

テーブル列の表示と非表示

情報のさまざまな列を非表示および表示することで、HPM に表示される各種テーブルをカスタマイズできます。表示可能な列はテーブルごとに異なります。

（注） 列見出しは、列ベースのフィルタリング （22 ページ）で説明されているように、選択したパラメータに従ってエントリを非表示または表示することにより、テーブルをさらにフィルタ処理するために使用できるメニューです。

テーブルに表示される特定の列を表示または非表示にするには、次の手順を実行します。

1. 列見出しの右側にある [列（Columns）] ボタンをクリックして、[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開きます。

現在のビューで使用できるすべての列が一覧表示されます。

1. 表示および非表示にする列を選択または選択解除します。
2. [OK] をクリックして、ダイアログボックスを閉じます。

このテーブルには、選択した列のみが表示されます。

次のトピックでは、さまざまなテーブルで使用できる個々の列について説明します。

- テーブル列：デバイス関連のビュー （10 ページ）
- テーブル列：VPN 関連のビュー （16 ページ）
- アラートテーブル列 （21 ページ）

テーブル列：デバイス関連のビュー

情報のさまざまな列を非表示および表示することにより、デバイス関連のビューの [モニタリング（Monitoring）] ペインに表示されるテーブルをカスタマイズできます。表示可能な列は、ビューごとに異なります。

[表示する列を選択（Choose Columns to Display）] ダイアログボックスのエントリの順序には、列の表示順序が反映されています（ただし、次の表の行の順序には、列の表示順序が必ずしも反映されていません）。[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開く方法については、テーブル列の表示と非表示 （10 ページ）を参照してください。

次の表は、デバイス関連のモニタリングビュー（[優先デバイス（Priority Devices）]、[IPS デバイス（IPS Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[すべてのデバイス（All Devices）]）およびこれらのシステムビューに基づくすべてのカスタムビューで使用可能なすべてのデータ列を示します。リストされている列の一部は、そこに示されているように、特定のビューでは使用できません。

表 *1:* デバイス関連のビューで使用可能なテーブル列

列名	ビューで使用可能	説明
デバイス名（Device Name）	IPS、ファイアウォール	デバイスに割り当てられている名前（つまり、[デバイスのプロパティ（Device Properties）] ウィンドウの [デバイスのプロパティ（Device Properties）]：[全般（General）] ページで定義されているホスト名）。列ベースのフィルタリング （22 ページ）を利用できます。 名前の前にデバイスタイプを示すアイコンが付いています。このアイコンの前にデバイスアラートインジケータが表示される場合もあります。赤色のドットは 1 つ以上の重大なアラート（および、場合によっては警告）を示し、黄色のドットは 1 つ以上の警告のみを示します。このエリアは、アラートのないデバイスの場合は空白になります。 ドットにマウスのポインタを合わせると、そのデバイスに関する重大なアラートの数と警告の数を表示するポップアップが表示されます。 デバイスアイコン自体に金色の星が付加されている場合は、優先監視対象デバイスであることを示しています。
Receive Time	IPS、ファイアウォール	このエントリのポーリング日時（形式：曜日 MMM DD HH:MM:SS タイムゾーン YYYY）。
IPアドレス	IPS、ファイアウォール	このデバイスの IP アドレス。列ベースのフィルタリング （22 ページ）を利用できます。
ヘルス ステータス	IPS、ファイアウォール	デバイスの現在の全体的な正常性（[クリティカル（Critical）]、[警告（Warning）]、または [正常（Normal）]）。列ベースのフィルタリング （22 ページ）を利用できます。 （注） 全体的な正常性は、正常性メトリックの中で最も重要なメトリックで定義されます。たとえば、デバイスで選択されたメトリックが、1 つのクリティカルを除いてすべて正常であっても、全体的な Device Health はクリティカルになります。

列名	ビューで使用可能	説明
接続ステータス	IPS、ファイアウォール	HPM がデバイスに接続可能またはデバイスをポーリング可能かどうかを示します（[接続済み（Connected）]、[認証エラー（Authentication Error）]、[証明書の不一致エラー（Certificate Mismatch Error）]、[接続エラー（Connection error）]、[読み取り操作中のタイムアウト（Timeout during Read operation）]、または [サービスが利用できません（Service unavailable）]）。列ベースのフィルタリング （22 ページ）を利用できます。 （注） デバイスが HPM（[ツール（Tools）] > [デバイスセレクタ（Device Selector）]）で通常または優先監視対象デバイスとして選択されていない場合、このステータスは適用されません。監視対象デバイスの選択に対する変更が有効になり、画面に反映されるまで数分かかる場合があります。 「接続済み」ではないデバイスについて表示される情報は、接続が失敗する前の、示されている受信時間のものです。
[メモリ（%）（Memory (%)）]	IPS、ファイアウォール	メモリの総使用可能容量に対する使用率。
[CPU（%）]	IPS、ファイアウォール	CPU の総使用可能容量に対する使用率。
モデル	IPS、ファイアウォール	デバイスのタイプとモデル番号。ASA 5510、IPS 4270 などです。
バージョン	IPS、ファイアウォール	このデバイスで実行されているソフトウェアのバージョン。列ベースのフィルタリング （22 ページ）を利用できます。
[検査負荷（%）（Inspection Load (%)）]	IPS	ポーリング時のデバイスの検査負荷（パーセンテージ）。
[受信できなかったパケット（%）（Missed Packet(%)）]	IPS	検査されたパケットの総数に対するドロップされたパケットの割合。
[センサーアプリケーションのステータス（Sensor App Status）]	IPS	現在のセンサーアプリ（分析エンジン）のステータス（[稼働（Up）]または [ダウン（Down）]）。列ベースのフィルタリング （22 ページ）を利用できます。

列名	ビューで使用可能	説明
[メインアプリのステータス（Main App Status）]	IPS	現在のメインアプリのステータス（[稼働（Up）]または [ダウン（Down）]）。列ベースのフィルタリング（22 ページ）を利用できます。
[コラボレーションアプリケーションのステータス（Collaboration App Status）]	IPS	現在のコラボレーションアプリのステータス（[稼働（Up）] または [ダウン（Down）]）。
[ライセンス有効期限ステータス（License Expiration Status）]	IPS	センサーに設定されている赤色および黄色のしきい値に基づくセンサーのライセンスステータス（[正常（Normal）]、[警告（Warning）]、または [クリティカル（Critical）]）。列ベースのフィルタリング （22 ページ）を利用できます。
[バイパスモード状態（In Bypass Mode）]	IPS	センサーでバイパスモードが有効になっているかどうか（[はい（Yes）] または [いいえ（No）]）。列ベースのフィルタリング （22 ページ）を利用できます。
[イベント取得ステータス（Event Retrieval Status）]	IPS	IPS イベント取得のステータス（[正常（Normal）]、[警告（Warning）]、または [クリティカル（Critical）]）。列ベースのフィルタリング （22 ページ）を利用できます。
[グローバル相関ステータス（Global Correlation Status）]	IPS	グローバル相関に参加しているセンサーの場合、その更新ステータス（[正常（Normal）]（前回の更新が成功）、[警告（Warning）]（過去 1 日間つまり 86,400 秒以内に更新が成功していない）、または [クリティカル（Critical）]（過去 3 日間つまり 259,200 秒以内に更新が成功していない））。列ベースのフィルタリング （22 ページ）を利用できます。
シグニチャ アップデート	IPS	このセンサーに適用された最新のシグニチャアップデートの数（たとえば、S574）。列ベースのフィルタリング （22 ページ）を利用できます。
ファイアウォールモード	Firewall	このデバイスの動作モード（[ルーテッド（Routed）]、[トランスペアレント（Transparent）]、または [混合（Mixed）]）。列ベースのフィルタリング （22 ページ）を利用できます。
コンテキスト モード	Firewall	このデバイスのコンテキストモード（[シングル（Single）] または [マルチ（Multiple）]）。列ベースのフィルタリング （22 ページ）を利用できます。

列名	ビューで使用可能	説明
接続（Connections）	Firewall	デバイスがポーリングされたときのアクティブな接続の数。
Xlates	Firewall	アドレス変換カウンタ。
[接続数/秒（Connections/second）]	Firewall	1 秒あたりの確立された接続の数。
[変関数/秒（Translations/second）]	Firewall	1 秒あたりの変換数。
フェールオーバー ステータス	Firewall	このデバイスがフェールオーバーペアの一部である場合、その現在の状態（[アクティブ（Active）] または [スタンバイ（Standby）]）。列ベースのフィルタリング （22 ページ）を利用できます。
[フェールオーバー ホスト ロール（Failover Host Role）]	Firewall	このデバイスがフェールオーバーペアの一部である場合、その現在のロール（[プライマリ（Primary）] または [セカンダリ（Secondary）]）。列ベースのフィルタリング （22 ページ）を利用できます。
[フェールオーバーピア ロール（Failover Peer Role）]	Firewall	このデバイスがフェールオーバーペアの一部である場合、そのピアデバイスの現在のロール（[プライマリ（Primary）] または [セカンダリ（Secondary）]）。列ベースのフィルタリング （22 ページ）を利用できます。
[フェールオーバー ピア ステータス（Failover Peer Status）]	Firewall	このデバイスがフェールオーバーペアの一部である場合、そのピアの現在のステータス（[アクティブ（Active）] または [スタンバイ準備完了（Standby Ready）]）。列ベースのフィルタリング （22 ページ）を利用できます。
Used Memory (MB)	Firewall	デバイスがポーリングされたときのメモリ使用容量（メガバイト単位）。列ベースのフィルタリング （22 ページ）を利用できます。
[空きメモリ（MB）（Free Memory (MB)）]	Firewall	デバイスがポーリングされたときのメモリ使用可能容量（メガバイト単位）。列ベースのフィルタリング （22 ページ）を利用できます。
[最大接続数（Max. Connections）]	Firewall	接続のピーク数。ASA グループでは使用できません。

列名	ビューで使用可能	説明
[Xlate の最大数（Max. Xlates）]	Firewall	アドレス変換のピーク数。ASA グループでは使用できません。
Throughput (Kbps)	Firewall	デバイスの平均スループット（キロビット/秒単位）。ASA 9.0 以降のクラスタの場合、これはグループに含まれるすべてのインターフェイスの総スループットです。
[ACL ドロップパケット（ACL Dropped Packets）]	Firewall	アクセス制御リストルールに違反したためにドロップされたパケットの数。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[スキャン脅威ドロップパケット（Scanning Threat Dropped Packets）]	Firewall	スキャン脅威検出が有効になっている場合、スキャン脅威インスペクションに失敗したためにドロップされたパケットの数。有効になっていない場合は、[適用なし（NA）] と表示されます。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[インスペクション ドロップ パケット（Inspection Dropped Packets）]	Firewall	アプリケーションインスペクションが有効になっている場合、アプリケーションインスペクションに不合格になったためにドロップされたパケット数。有効になっていない場合は、[適用なし（NA）] と表示されます。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[SYN 攻撃ドロップパケット（Syn Attack Dropped Packets）]	Firewall	SYN フラッディングのためにドロップされたパケットの数。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[総インターフェイス ドロップ パケット（Total Interface Dropped Packets）]	Firewall	すべてのインターフェイスでドロップされたパケットの総数。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。 （注） インターフェイスごとのドロップされたパケットの数は、選択したデバイスの [詳細（detail）] セクションに表示されるタブ付きの [インターフェイス（Interface）] パネルで確認できます。
[分析エンジンメモリ（%）（Analysis Engine Memory (%)）]	IPS	現在使用中の分析エンジンに割り当てられているメモリの割合。

列名	ビューで使用可能	説明
[グループでのロール（Role in Group）]	Firewall	ASA ロードバランシンググループのこのメンバーのロール（[グループ（Group）]、[制御（Control）]、または [データ（Data）]）。 グループは、複数のノードを持つ単一のデバイスとして Security Manager によって管理されます。そのため、各グループは HPM に単一のエントリとして表示されます。これを展開するとノードのリストを表示できます。
* これらの列はすべて、[すべてのデバイス（All Devices）] ビューと [優先デバイス（Priority Devices）] ビューで使用できます。		

テーブル列：VPN 関連のビュー

情報のさまざまな列を非表示および表示することにより、VPN 関連のビューの [モニタリング（Monitoring）]ペインに表示されるテーブルをカスタマイズできます。表示可能な列は、ビューごとに異なります。

[表示する列を選択（Choose Columns to Display）] ダイアログボックスのエントリの順序には、列の表示順序が反映されています（ただし、次の表の行の順序には、列の表示順序が必ずしも反映されていません）。[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開く方法については、テーブル列の表示と非表示 （10 ページ）を参照してください。

次の表に、VPN 関連のモニタリングビューで使用可能なすべてのデータ列を示します。[リモートアクセスユーザー（RA）（Remote Access Users (RA）]、[サイト間トンネル（S2S）（Site-to-Site Tunnels (S2S)）]、[VPNサマリー（VPN Summary）]、およびこれらのシステムビューに基づくすべてのカスタムビュー。表示されている列の一部は、示されているように、特定のビューでは使用できません。

デバイスがトラップメッセージを送信すると、Cisco Security Manager はトラップをキャプチャし、Health and Performance Monitoring アプリケーションの [サイト間トンネル（Site to Site Tunnels）] ページに送信します。Cisco Security Manager バージョン 4.16 までは、IPv4 経由でのみトラップメッセージを送信するためにデバイスが使用されていました。Cisco Security Manager 4.17 以降、SNMP トラップは IPv6 を使用してキャプチャされるため、Cisco Security Manager はトラップメッセージを受信します。また、デバイスの IPv6 アドレスをデバイスの詳細にマッピングし、Health and Performance Monitoring アプリケーションの [サイト間トンネル（Site to Site Tunnels）] ページにトラップに関するアラートを表示します。ステータスは、数回の更新サイクルの後、Health and Performance Monitoring アプリケーションに表示されます。

（注） Cisco Security Manager バージョン 4.9 以降、Health and Performance Monitoring アプリケーションは、IPv4 ベースのトンネルに加えて、IPv6 アドレスが設定されているサイト間トンネルを監視および表示します。また、電子メールとトラップの通知には、IPv4 アドレスに加えて IPv6 アドレスが含まれるようになりました。

表 *2 : VPN* 関連のビューで使用可能なテーブル列

列名	ビューで使用可能	説明
Receive Time	RA、S2S、VPNサマリー（VPN Summary）	このエントリのポーリング日時（形式：曜日 MMM DD HH:MM:SS タイムゾーン YYYY）。
ファイアウォール名（Firewall Name）	RA、S2S、VPNサマリー（VPN Summary）	Cisco Security Manager インベントリで提供されるこのデバイスの名前。列ベースのフィルタリング （22 ページ）を利用可能。
ユーザー名	RA	このセッションを確立するために使用されるユーザーログイン名。列ベースのフィルタリング （22 ページ）を利用可能。
ユーザーグループポリシー（User Group Policy）	RA	このユーザーが属する ASA VPN ユーザーグループの名前。列ベースのフィルタリング （22 ページ）を利用可能。
ゲートウェイ	RA	ユーザーが接続している VPN ゲートウェイの IP アドレス。列ベースのフィルタリング （22 ページ）を利用可能。
割り当てられている IP	RA	このセッションのリモートクライアントに割り当てられたプライベート IP アドレス。「内部」または「仮想」IP アドレスとも呼ばれています。
Public IP	RA	クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。列ベースのフィルタリング （22 ページ）を利用可能。
接続開始時間（Connection Initiation Time）	RA	接続が開始された日時（HH:MM:SS 曜日 MMM DD YYYY）。時刻は 24 時間形式の協定世界時（UTC）で表示されます。
期間	RA	セッションの開始から最新のデバイスポーリングまでの経過時間（HH:MM:SS）。

列名	ビューで使用可能	説明
クライアントバージョン（Client Version）	RA	リモートピアで実行されている VPN クライアントソフトウェアとバージョン。AnyConnect Windows 3.0、Mozilla 4.0 など。列ベースのフィルタリング （22 ページ）を利用可能。
エンドポイントOS（EndPoint OS）	RA	リモートピアで使用中のオペレーティングシステム。Windows、Windows NT など。列ベースのフィルタリング （22 ページ）を利用可能。
認証方式	RA	ユーザーパスワード、証明書、または事前共有キー。列ベースのフィルタリング （22 ページ）を利用可能。
暗号化（Encryption）	RA、S2S	このセッションが使用しているデータ暗号化アルゴリズム。列ベースのフィルタリング （22 ページ）を利用可能。
トンネル タイプ	RA、VPNサマリー（VPN Summary）（[タイプ（Type）] のみ）	トンネルまたは接続のタイプ。クライアントレス、IPsec、および Secure Client が含まれます。列ベースのフィルタリング （22 ページ）を利用できます。
Throughput (Kbps)	RA、S2S	受信バイト数と送信バイト数（キロビット/秒）。
セッションID（Session ID）	RA	このセッションに割り当てられた識別子。
非アクティブ時間（Inactive Time）	RA	このセッションが非アクティブだった時間。
IPアドレス	S2S、VPNサマリー（VPN Summary）	このデバイスの IP アドレス。列ベースのフィルタリング （22 ページ）を利用可能。
Local Endpoint	S2S	ローカル トンネル インターフェイスの IP アドレス。
リモートエンドポイント	S2S	リモート トンネル インターフェイスの IP アドレス。
ローカルサブネット（Local Subnet）	S2S	ローカルで保護されたサブネットのアドレス。
リモートサブネット（Remote Subnet）	S2S	リモートで保護されたサブネットのアドレス。

列名	ビューで使用可能	説明
アップタイム（Uptime）	S2S	このトンネルの現在の継続時間。
[接続時間（Connection Time）]	S2S	接続が開始された日時（HH:MM:SS 曜日 MMM DD YYYY）。時刻は 24 時間形式の協定世界時（UTC）で表示されます。
ステータス	S2S	トンネル接続ステータス。[アップ（Up）] または [ダウン（Down）] になります。トンネルが指定された回数ダウンすると、アラートが発行されます。詳細については、列ベースのフィルタリング （22 ページ）を参照してください。 **ヒント** [ステータス（Statu）] 列の [ダウン（Down）] 通知ハイパーリンクをクリックして、イベントビューアでそのデバイスの IPSec VPN イベントを表示できます。イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。
ヘルス ステータス	VPNサマリー（VPN Summary）	基礎となるデバイスの現在の全体的な正常性：[クリティカル（Critical）]、[警告（Warning）]、または [正常（Normal）]。列ベースのフィルタリング （22 ページ）を利用可能。 **（注）** 全体的な正常性は、正常性メトリックの中で最も重要なメトリックで定義されます。たとえば、デバイスで選択されたメトリックが、1 つのクリティカルを除いてすべて正常であっても、全体的な Device Health はクリティカルになります。
接続ステータス	VPNサマリー（VPN Summary）	リモート接続ステータス。常に [接続済み（Connected）] になります（HPM は以前の接続に関する情報を表示できません）。列ベースのフィルタリング （22 ページ）を利用可能。

列名	ビューで使用可能	説明
モニタリングタイプ（Monitoring Type）	VPNサマリー（VPN Summary）	監視されている VPN 接続のタイプ。 列ベースのフィルタリング （22 ページ） を利用可能。
アクティブセッション（Active Sessions）	VPNサマリー（VPN Summary）	現在アクティブなセッション（S2S、IPSec RA、クライアントベースの SSL RA、およびクライアントレス SSL RA）。
ピークセッション数（Peak Sessions）	VPNサマリー（VPN Summary）	同時セッションのピーク数（S2S、IPSec RA、クライアントベースの SSL RA、およびクライアントレス SSL RA）。
ユーザ総数	VPNサマリー（VPN Summary）	現在のリモートユーザーの合計（S2S、IPSec RA、クライアントベースの SSL RA、およびクライアントレス SSL RA）。
非アクティブセッション	VPNサマリー（VPN Summary）	非アクティブセッションの数。
合計VPNスループット（Kbps）（Total VPN Throughput (Kbps)）	VPNサマリー（VPN Summary）	すべての VPN トラフィックの合計。つまり、RA と S2S のスループット値の合計（キロビット/秒）。 列ベースのフィルタリング （22 ページ） を利用可能。
ACL Name	サイト間トンネル（Site-to-Site Tunnels）	バージョン 4.9 以降、Cisco Security Manager では、選択したサイト間トンネルに関連付けられているアクセス制御リスト（ACL）名を表示できます。この列名はデフォルトで選択されています。 （注） Health and Performance アラートの表示で、トンネルアップ/ダウンアラートの [説明（Description）] 列に ACL 名も表示されるようになりました。同様に、電子メールおよびトラップ通知の [説明（Description）] 列にも ACL 名が表示されます。
備考	サイト間トンネル（Site-to-Site Tunnels）	（任意）この列には、[ACL名（ACL Name）] に対応する注釈が表示されます。 （注） アラート、電子メール、およびトラップ通知には、説明フィールドの一部として [注釈（Remarks）] は含まれていません。

列名	ビューで使用可能	説明
制限事項： Cisco Security Manager Daemon Manager サービスが開始されると、HPM アプリケーションは Configuration Archive の最新の構成を使用して、サイト間 VPN トンネルに関連付けられた [ACL名（ACL Name）] と [注釈（Remarks）] を抽出します。VPN トンネルが HPM によって識別されると、抽出されたデータを使用して、S2S ビューに [ACL名（ACL Name）] と [注釈（Remarks）] の列が表示されます。HPM でデータが使用可能になる前に VPN トンネルが起動した場合、次の UI 更新まで、 [ACL名（ACL Name）] と [注釈（Remarks）] の列にデータが表示されないことがあります。同様に、HPM によってデータが抽出される前にアラートが生成された場合、アラートの表示の [説明（Description）] 列に [ACL名（ACL Name）] が表示されないことがあります。これは、以前のバージョンから Cisco Security Manager バージョン 4.9 へのアップグレード中に発生する可能性があります。次回のポーリングで同じアラートが表示された場合、[ACL名（ACL Name）] が [説明（Description）] に追加されます。 **ヒント**： [注釈（Remarks）] 列の内容に相違がある場合があります。Configuration Archive の最新の構成に [注釈（Remarks）] が含まれているか確認します。アウトオブバンドの変更により [注釈（Remarks）] が追加または更新された場合は、デバイスを再検出する必要があります。		

アラートテーブル列

情報のさまざまな列を非表示または表示することにより、アラートテーブルをカスタマイズできます。

[表示する列を選択（Choose Columns to Display）] ダイアログボックスのエントリの順序には、列の表示順序が反映されています（ただし、次の表の行の順序には、列の表示順序が必ずしも反映されていません）。[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開く方法については、テーブル列の表示と非表示 （10 ページ）を参照してください。

表 *3:* アラートテーブルで使用可能なデータ列

列名	説明
デバイス名（Device Name）（常に選択）	このアラートがトリガーされたデバイスの名前で、Cisco Security Manager インベントリで提供されます。列ベースのフィルタリング （22 ページ）で利用可能。
ノード	このアラートが ASA ロードバランシングクラスタのメンバーによって生成された場合のノード名です。列ベースのフィルタリング （22 ページ）で利用可能。
デバイスタイプ	デバイスのタイプ：ASA または IPS。列ベースのフィルタリング （22 ページ）で利用可能。

列名	説明
重大度	アラートの重大度：[クリティカル（Critical）]、[警告（Warning）]、または [正常（Normal）]。 列ベースのフィルタリング （22 ページ）で利用可能。
ステータス	現在のデバイスステータス：アクティブまたは確認済み。 列ベースのフィルタリング （22 ページ）で利用可能。
説明	アラートの説明。例、「Device Health がクリティカル」または「デバイスポーリング：認証エラー」など。
最初の確認	このアラートが最後に記録された日時（day-of-week MMM DD、YYYY HH:MM:SS AM/PM）。時間はユーザーのタイムゾーンに基づいています。 列ベースのフィルタリング （22 ページ）で利用可能。
最後の確認日時	このアラートが最後に記録された日時（day-of-week MMM DD、YYYY HH:MM:SS AM/PM）。時間はユーザーのタイムゾーンに基づいています。 列ベースのフィルタリング （22 ページ）で利用可能。
注記	アラートの確認時に、注釈を付けることができます。すべての注釈はこのフィールドに表示されます。詳細については、 アラート：確認応答とクリア （54 ページ）を参照してください。

列ベースのフィルタリング

特定の列の内容に基づいて HPM 内のさまざまなテーブルをフィルタ処理できます。列フィルタを適用すると、その列に指定された基準を持つエントリのみが含まれるようにテーブルがフィルタ処理されます。

（注） テーブルの表示を変更する他の方法については、 テーブル列の操作 （9 ページ）参照してください。

ヒント

- 列フィルタは累積的です。フィルタ処理されたテーブルにエントリが表示されるには、すべての列フィルタ基準を満たす必要があります。論理和を取った列フィルタのセットは作成できません。
- すべてではありませんが、ほとんどのカラムの内容に対してフィルタリングできます。カラムに下矢印がない場合は、そのカラムに対してはフィルタリングできません。たとえば、[すべてのデバイス（All Devices）] ビューの [受信時間（Receive Time）] ではフィルタ処理できません。
- フィルタアイコン（じょうご）はフィルタリングされたカラムの見出しに表示されます。

- 使用可能なカラムの詳細については、テーブル列の表示と非表示 （10 ページ）を参照してください。

特定の列パラメータに従ってテーブルをフィルタ処理するには、次の手順を実行します。

列の見出しの下向き矢印をクリックし、ドロップダウンメニューから次のいずれかを選択します。

- [すべて（All）]：この列からフィルタを削除または「元に戻す」には、[すべて（All）]を選択します。テーブルが更新され、このパラメータのすべてのエントリが表示されます。たとえば、[アラート（Alerts）]テーブルの [重大度（Severity）] 列をフィルタ処理して [クリティカル（Critical）] アラートのみを表示した場合、このオプションを選択すると、すべての [クリティカル（Critical）] アラートと [警告（Warning）] アラートが再表示されます。
- [カスタム（Custom）]：[カスタム（Custom）] を選択すると、その列の情報に基づいてカスタムフィルタを作成できる [カスタムフィルタ（Custom Filter）] ダイアログボックスが開きます。詳細については、カスタムフィルタ処理 （23 ページ）を参照してください。
- 特定のエントリ：ドロップダウンメニューには、列に関連するすべての値が含まれています。1 つの値を選択して、そのエントリのグループのみを表示します。たとえば、[アラート（Alerts）]テーブルの [重大度（Severity）] 列から [クリティカル（Critical）] を選択して、テーブルをフィルタ処理し、[クリティカル（Critical）] アラートのみ表示します。

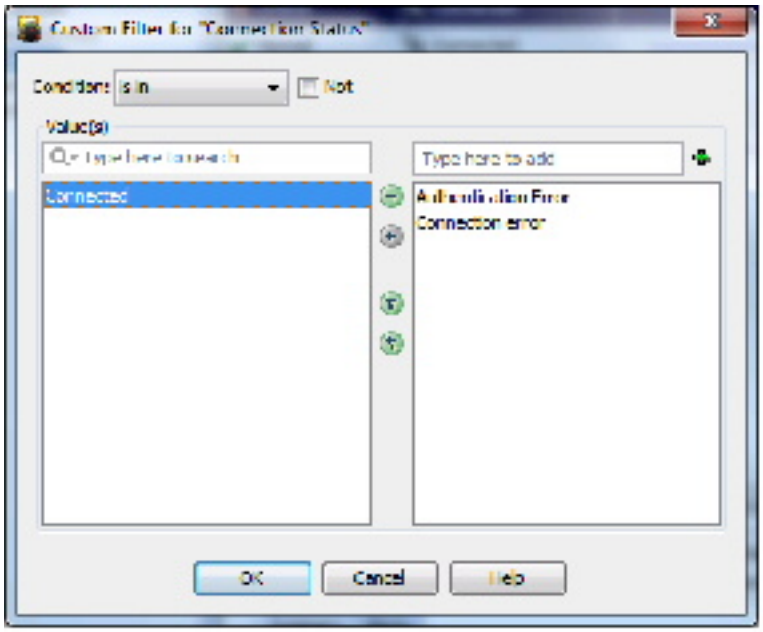
カスタムフィルタ処理

次の手順では、列のドロップダウンリストから単純に値を選択しない、カスタム列ベースのフィルタを作成する方法について説明します。他の列ベースのフィルタリングオプションについては、HPM ウィンドウ：アラートディスプレイ （42 ページ）を参照してください。

ステップ 1 列の見出しの下向き矢印をクリックし、ドロップダウンメニューから [カスタム（Custom）] を選択します。

選択した列に対して [カスタムフィルタ（Custom Filter）] ダイアログボックスが開きます。

ステップ 2 [Custom Filter] ダイアログボックスで目的の値を選択します。次の図に、このダイアログボックスの一般的な例を示します。



以下は、[カスタムフィルタ（Custom Filter）] ダイアログボックスに表示される可能性のあるコントロールです（すべてのインスタンスにすべてのコントロールが表示されるわけではありません）。

- [条件（Condition）]：選択した [値（Values）] に適用される条件を選択します。

通常、これは **is in** です。つまり、選択した各 [値（Values）] は、そのエントリがフィルタ処理されたテーブルに表示されるためには、列に「含まれている」必要があります。

- [否定（Not）]：負の条件を作成するには、このボックスをオンにします。

is in が条件として選択されている場合、選択された [値（Values）] が列に存在できないことを意味します。つまり、列にこれらの [値（Values）] を持つエントリが表示されないように、テーブルがフィルタ処理されます。

- [値（Values）] リスト：ダイアログボックスのいくつかのインスタンスには、選択する [値（Values）] の 1 つのリストが表示されるので、目的のオプションをオンにします。

使用可能な [値（Values）] と選択された [値（Values）] のリスト：ほとんどの場合、ダイアログボックスには、前の図に示すように 2 つの [値（Values）] のリストが表示されます。カスタムフィルタの値を選択するには、列で使用可能な値が含まれている左側のリストでその値を強調表示し、右矢印をクリックして右側の選択された値のリストに追加します。複数の値を選択できます。

使用可能な [値（Values）] リストの項目は、送信元テーブルの選択した列に現在表示されている値によって決定されます。

使用可能な値が多数ある場合は、リストの上にある [リストフィルタ（List Filter）] フィールドに特定の値を入力して検索できます。詳細については、リストフィルターフィールドの使用　（25 ページ）を参照してください。

次の方法を使用して、値の選択または選択解除をすることもできます。

- 選択した [値（Values）] リストの上にあるテキストフィールドに値の名前を入力し、[+] ボタンをクリックします。選択した [値（Values）] にその値が追加されます。この方法は、使用可能な [値（Values）] が多数ある場合、または使用可能な [値（Values）] リストにない値をフィルタ処理する場合に役立ちます。
- 他方のリストに移動する、一方のリストの項目をダブルクリックします。
- いずれかの二重矢印ボタンをクリックして、選択した値に関係なく、すべての項目を 1 つのリストから別のリストに移動します。

ステップ 3 [OK] をクリックして、ダイアログボックスを閉じます。

テーブルが更新され、現在適用されているすべてのフィルタを満たすエントリのみが表示されます。

リストフィルターフィールドの使用

[リストフィルタ（List Filter）] フィールドは、[モニタリング（Monitoring）] 画面のデバイスおよびVPN リストの上、[アラート（Alerts）] 画面のアラートテーブルの上、デバイス セレクタの [VPN] ページのデバイスリストの上、および [クリアされたアラートの表示（View Cleared Alerts）] ウィンドウにあります。いずれの場合も、[リストフィルタ（List Filter）] フィールドを使用して、指定したテキスト文字列を含む関連テーブル内のエントリをすばやく見つけることができます。

（注） 見つかったテキストは、エントリに関連付けられたデータフィールドの一部にすることができます。たとえば、[アラートリストフィルタ（Alerts List Filter）] フィールドに「ライセンス（license）」と入力すると、アラートテーブルがフィルタリングされ、差し迫ったライセンスの期限切れに関連するアラートのみが表示されます。（関連するデータカラム（この例では [詳細（Detail）]）が表示されていなくても、一致したエントリが一覧表示されるため、混乱が生じる可能性があります。テーブルのカラムを非表示にする方法の詳細については、テーブル列の表示と非表示 （10 ページ）を参照してください）。

図 *2 :* ヘルスとパフォーマンスの監視：*[リストフィルタ（List Filter）]* フィールド

1	[フィルタパラメータ（Filter-parameters）] ボタン	2	[Clear] ボタン

デバイスリスト、VPNリスト、アラートテーブル、または[クリアされたアラートの表示（View Cleared Alerts）]ウィンドウで特定のテキスト文字列を検索するには、次の手順を実行します。

- [リストフィルタ（List Filter）]フィールドをクリックしてテキストカーソルを置き、入力を開始します。

これらは「ライブフィルター」フィールドです。つまり、各文字を入力すると、現在のテキスト文字列を含まないエントリがリストまたはテーブルから削除されます。たとえば、アラートの広範なリストに「Device Health Critical,」のステータスが 1 つあり、他のアラートには、*hea* という文字を含むテキスト文字列が含まれていないとします。[リストフィルタ（List Filter）]フィールドを使用して、その 1 つのアラートをすばやく見つけたいので、「health」という単語の入力を開始します。最初の 3 文字を入力した後に表示されるのは、そのアラートだけです。

[リストフィルタ（List Filter）] フィールドをクリアするには：

- フィールドの右側にある [クリア（clear）] ボタンをクリックします。

このボタンは、フィールドへの入力を開始すると表示されます。（文字を強調表示して、キーボードの Delete キーまたは Backspace キーを押すこともできます）。

[リストフィルタ（List Filter）]フィールドをクリアすると、リスト内のすべてのエントリが再び表示されます。

検索する情報（カラム）を指定し、大文字と小文字を区別するか区別しないかを選択し、ワイルドカードまたは正規表現を許可し、返される文字列のどこに文字を配置すべきかを指定することにより、フィルタ結果を調整できます。

リストフィルタ条件を変更するには、次の手順を実行します。

1. [リストフィルター（List Filer）] フィールドの左側にある [filter-parameters] ボタン（虫眼鏡）をクリックして、パラメータメニューを開きます。
2. オプションを選択します。

メニューは 4 つのセクションで構成されています。

- 使用可能なすべての情報タイプのリスト：これらのエントリは、その特定のリストまたはテーブルに表示できるカラムに対応しています。[すべて（All）]を選択するか、個別のエントリを選択することができます。
- [大文字と小文字を区別する（Case sensitive）]および[大文字と小文字を区別しない（Case insensitive）]：いずれかを選択します。[大文字と小文字を区別する（Case sensitive）]を選択した場合、見つかったテキストは、入力した文字だけでなく、大文字と小文字も入力されたものと一致する必要があります。

- [ワイルドカードを使用する（Use wildcards）] および [正規表現を使用する（Use regular expression）] : いずれかを選択します。次のワイルドカードが認識されます。
- *****（アスタリスク）：文字列内のその位置にある 0 個以上の文字に一致します。
- **?**（疑問符）：文字列内のその位置にある 1 文字に一致します。
- [最初から一致（Match from start）]、[完全一致（Match exactly）]、および [一部が一致（Match anywhere）] : 1 つを選択します。[最初から一致（Match from start）]とは、入力した文字列がエントリの先頭で見つかる必要があることを意味します。ただし、より大きな文字セットの一部でも可能です。[完全一致（Match exactly）] では、入力した文字列がカラムエントリ全体と完全に一致する必要があります。[一部が一致（Match anywhere）] とは、文字列がエントリ内のどこかで見つかることを意味し、より大きな文字セットの一部でも可能です。
- 別のパラメータを変更するには、手順 1 と 2 を繰り返します。

デバイスのモニタリング

[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）で説明するように、HPM モニタリング画面には、ビュー制御、ビューパネル、現在選択されているデバイスに関する詳細情報が表示されます。

モニタリング画面に切り替えるには、次の手順を実行します。

- HPM メニューバーの下にある [モニタリング（Monitoring）] ボタンをクリックします。

([アラート（Alerts）]画面に戻るには、[アラート（Alerts）] ボタンをクリックします。)

（注） 監視するデバイスの指定については、デバイスビューの管理 （27 ページ）を参照してください。

ここでは、次の内容について説明します。

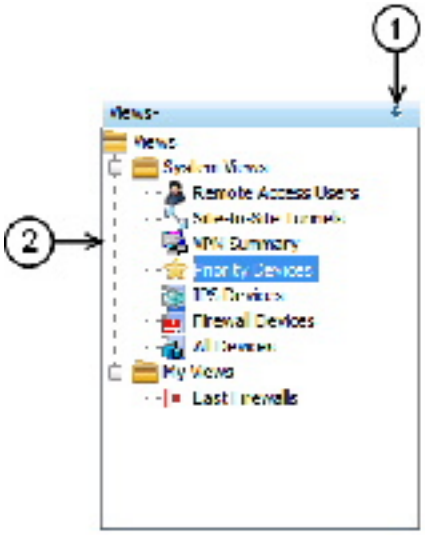
- デバイスビューの管理 （27 ページ）
- [HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）

デバイスビューの管理

「ビュー」は、HPM アプリケーションの [モニタリング（Monitoring）] ペインに表示される情報をフィルタ処理および整理するための手段を提供します。すべてのデバイス、ファイアウォールデバイス、リモートアクセスユーザーの詳細など、さまざまなシステムビューが提供されます。また、カスタムビューを作成して、地理的なデバイスの場所など、その他の方法で情報を整理することもできます。

HPM のメインウィンドウの左ペインには、次の図に示すように使用可能なビューのリストが表示されます。

図 *3 : Health and Performance Monitor* : *[ビュー（Views）]* ペイン *[ビュー（Views）]* ペインには、次のコントロールが含まれています。



- **(1) プッシュピンボタン**：ビューリストの表示を制御するには、プッシュピンボタンをクリックします。リストが HPM ウィンドウのペインとして表示されている場合（ピンが垂直）、このボタンをクリックするとペインがウィンドウの左端に折りたたまれ、ラベルの付いたタブが残ります。[モニタリング（Monitoring）] ペインが展開され、HPM ウィンドウ全体に表示されます。

タブの上にマウスポインタを合わせると、ビューリストを「ポップアウト」表示にできます。ポインタがタブまたはリスト領域にある限り、リストは表示されたままになります（ピンは水平）。また、タイトルバーの任意の場所（ピン自体を除く）をクリックして、リストを「ポップアウト」表示のままにすることもできます。

ピンをもう一度クリックすると、ビューリストが開いたペインとして再確立されます。[モニタリング（Monitoring）] ペインが縮小し、リストのための場所が確保されます。

- (2) ビューのリスト：リストは、[システムビュー（System Views）] と [マイビュー（My Views）] のフォルダに整理されます。ビュー：開閉 （29 ページ）で説明されているように、いずれかのフォルダのエントリをクリックすると、そのビューが [モニタリング（Monitoring）] ウィンドウで開きます。[マイビュー（My Views）] フォルダに新しいビューを作成する方法については、ビュー：カスタム （31 ページ）を参照してください。
- 右クリック ショートカット メニュー：[ビュー（Views）] リストのエントリを右クリックすると、ビュー関連のコマンドのポップアップメニューにアクセスできます。
  - [編集（Edit）]：既存のカスタムビューの名前と説明を編集します。ビュー：カスタム （31 ページ）を参照してください。

- [名前を付けて保存（Save As）]：ビューを新しいカスタムビューとして保存します。ビュー：カスタム （31 ページ）を参照してください。
- [削除（Delete）]：そのカスタムビューを削除します。
- [デフォルトのビューとして設定（Set as default view）]：HPM アプリケーションを起動するたびに常に表示されるビューを指定するには、このコマンドを使用します。

ここでは、次の内容について説明します。

- ビュー：開閉 （29 ページ）
- ビュー：水平または垂直方向に並べて表示 （30 ページ）
- ビュー：フローティングとドッキング （31 ページ）
- ビュー：カスタム （31 ページ）

ビュー：開閉

使用可能なすべてのビューは、HPM ウィンドウの左側にある [ビュー（Views）]ペインに一覧表示されます。[モニタリング（Monitoring）]ペインには、開いているビューが表示されます。各ビューは個別のタブ付きパネルとして表示されます（このウィンドウの詳細については、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）を参照してください）。

（注） ビューを切り離して、別のウィンドウに「フロート」できます。詳細については、ビュー：フローティングとドッキング （31 ページ）を参照してください。

[モニタリング（Monitoring）]ペインに新しいビューを表示するには、次の手順を実行します。

- [ビュー（Views ）] リストで目的のエントリをクリックします。

ビューは [モニタリング（Monitoring）] ペインにタブ付きパネルとして表示されます。また、自動的に選択されて表示されます

開いている別のビューに切り替えるには、次の手順を実行します。

- [モニタリング（Monitoring）] ペインで目的のタブをクリックすると、そのビューが表示されます。
- 任意のタブを右クリックし、[次へ（Next）] または [前へ（Previous）] を選択して、そのタブ付きビューの右側または左側にビューを表示します。
- タブの右側にある [スクロールバック（Scroll Back）] ボタンと [スクロールフォワード（Scroll Forward）] ボタンをクリックして、現在のビューの左側または右側にビューを表示します

ビューを閉じるには、次の手順を実行します。

- 該当タブの [閉じる（Close）] ボタンをクリックします。
- タブを右クリックし、[閉じる（Close）] を選択します。
- タブを右クリックし、[その他を閉じる（Close Others）]を選択して、右クリックしたビュー以外の開いているすべてのビューを閉じます。
- 任意のタブを右クリックし、[すべて閉じる（Close All）] を選択して、開いているすべてのビューを閉じます。

ビュー：水平または垂直方向に並べて表示

[モニタリング（Monitoring）] ペイン全体に 1 つのビューを表示するのではなく、簡単に比較できるように、2 つ以上のビューを水平または垂直に並べて表示できます。

たとえば、2 つのビューを水平に並べて表示すると、一方のビューが [モニタリング（Monitoring）]ペインの上半分に表示され、もう一方のビューが下半分に表示されます。同様に、2 つのビューを垂直に並べると、ペインの左半分が 1 つのビューで占められ、もう一方のビューによって右半分が占められます。さらに、3 つ以上のビューを並べて表示することもできます。ペインは、ビューごとに均等に分割されます。

2 つの水平または垂直のタイルを作成するには：

- いずれかのタブを右クリックし、[新規水平グループ（New Horizontal Group）] または [新規垂直グループ（New Vertical Group）] を選択します。

選択したビューとその他のビューは、[モニタリング（Monitoring）] ペインを均等に共有するように、選択に応じて水平または垂直に配置されます。

これらのコマンドのいずれかを選択したときに3つ以上のビューが開いている場合は、選択されているビューがタイルとして表示され、タブ付きビューの残りのグループがもう一方のタイルとして表示されることに注意してください。その後必要に応じて、残りのタブ付きビューでこのプロセスを繰り返し、表示されるタイルの数を増やすことができます。

既存のタイルを別のタイルに移動することもできます。

- タブを右クリックし、[次のタググループに移動（Move to Next Tab Group）] または [前のタブグループに移動（Move to Previous Tab Group）] を選択します。

選択したビューは、次のタイル（タイルの向きに応じて下または右）または前のタイル（上または左）に追加されます。これらのコマンドは、このような移動が可能なようにビューが配置されている場合にのみ使用できます。

ビューの方向を水平から垂直に、またはその逆に切り替えて変更するには：

- 任意のタブを右クリックし、[タブグループの方向を変更（Change Tab Groups Orientation）] を選択します。

このコマンドは、2 つ以上のビューが並べて表示されている場合にのみ使用できます。

ビュー：フローティングとドッキング

タブ付きビューを切り離し、別個のウィンドウとして「フローティング」させたり、フローティングビューを「ドッキング」し、タブ付きビューとして [モニタリング（Monitoring）] ペインに戻したりすることができます。

ビューをフローティングウィンドウとして切り離すには：

- タブを右クリックし、[フローティング（Floating）] を選択します。

標準ウィンドウが開き、選択したビューが表示されます。

[モニタリング（Monitoring）] ペインから、すでに開いているフローティング ビュー ウィンドウに別のタブ付きビューを移動するには、次の手順を実行します。

- タブを右クリックし、[フローティングの移動先（Floating to）] サブメニューからウィンドウを選択します。

右クリックしたビューは、別のタブ付きパネルとして既存のウィンドウに追加されます。

フローティングビューを [モニタリング（Monitoring）] ペインにタブ付きパネルとして戻すには：

- ウィンドウでビューのタブを右クリックし、[ドッキング（Docking）] を選択します。

フローティングビューが [モニタリング（Monitoring）] ペインに戻ります。

（注） 標準ウィンドウとして、他のウィンドウと同様に、フローティングビューを最小化、最大化したり、閉じたりすることができます。

ビュー：カスタム

Health and Performance Monitor には、7 つのシステムビューがあります。さらに、既存のビューに基づいたカスタムビューをいくつでも作成できます。カスタムビューを編集および削除することもできます。

さまざまなビューが [モニタリング（Monitoring）] 画面の [ビュー（View）] ペインに表示され、[システムビュー（System Views）] と [マイビュー（My Views）]（後者のフォルダにはカスタムビューが含まれています）という 2 つのフォルダに編成されています。[モニタリング（Monitoring）] 画面については、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ） で説明しています。

新しいカスタムビューを作成するには、次の手順に従います。

1. [ビュー（View）] リストで、新しいビューの基になるビューを選択します。

システムビューまたは既存のカスタムビューを、基になるビューにすることができます。

1. [ファイル（File）] メニューの [名前を付けて保存（Save As）] を選択して、[ビューに名前を付けて保存（Save View As）] ダイアログボックスを開きます。

選択したビューを右クリックし、ポップアップメニューから [名前を付けて保存（Save As）] を選択してダイアログボックスを開くこともできます。

1. [名前（Name）] に新しいビューの名前を指定し、オプションで [説明（Description）] に説明を入力します。
2. このビューでモニターするデバイスを指定します。ダイアログボックスのデバイスセレクタ領域のエントリをオンまたはオフにします。
3. [保存（Save）] をクリックしてダイアログボックスを閉じ、新しいビューを [マイビュー（My View）] フォルダに追加します。

既存のカスタム ビューを編集するには、次の手順に従います。

1. [マイビュー（My View）] で、ビューを選択します。
2. [ファイル（File）] メニューの [編集（Edit）] を選択して、[ビューに名前を付けて保存（Save View As）] ダイアログボックスを開きます。

選択したビューを右クリックして、ポップアップメニューから [編集（Edit）] を選択することもできます。

1. [名前（Name）] と [説明（Description）] を編集します。
2. このビューでモニターされるデバイスを変更するには、デバイスセレクタのエントリをオンまたはオフにします。
3. [Save] をクリックして、ダイアログボックスを閉じます。

既存のカスタム ビューを削除するには、次の手順に従います。

1. [マイビュー（My View）] で、ビューを選択します。
2. [ファイル（File）] メニューから [削除（Delete）] を選択します。

選択したビューを右クリックして、ポップアップメニューから [削除（Delete）] を選択することもできます。

1. ビューを削除することを確認します。

該当するビューは、[ビュー（Views）] リストから削除されます。

[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ

[HPM] ウィンドウには、モニタリングと警告という 2 つの異なる情報が表示されます。[モニタリング（Monitoring）] ボタンをクリックして、[モニタリング（Monitoring）] ディスプレイにアクセスします。

[モニタリング（Monitoring）] ディスプレイは、[ビュー（Views）] と [モニタリング（Monitoring）] という 2 つの主要なペインで構成されています。[ビュー（Views）] ペインに

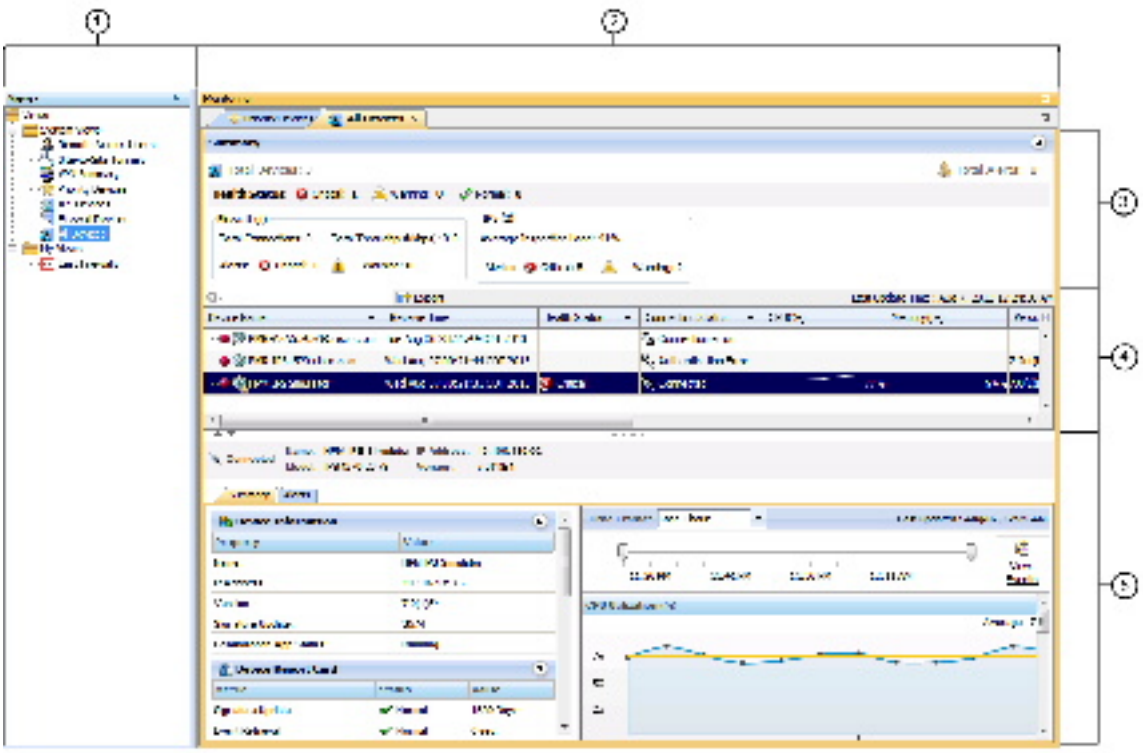
は、使用可能なビューのリストが表示されます。このリストのエントリをクリックして、そのビューを [モニタリング（Monitoring）] ペインのタブ付きパネルとして開きます。

[モニタリング（Monitoring）] ペインには複数のタブ付きビューが表示され、そのほとんどに複数のセクションが表示されます。タブをクリックすると、そのビューが前面に表示されます。

（注） モニタリングビュー：VPN、RA および S2S （39 ページ）で説明されているように、[リモートアクセスユーザー（Remote Access Users）] ビューと [サイト間トンネル（Site-to-Site Tunnels）] ビューには、それぞれ情報のテーブルが 1 つだけ表示されます。以下の説明は、主にその他の利用可能なシステムビューに焦点を当てています。

次の図は、[モニタリング（Monitoring）] ディスプレイとパネルセクションの主な機能を示しています。

図 *4 : Health and Performance Monitor* : *[モニタリング（Monitoring）]* ディスプレイ



1	**[ビュー（Views）] リスト。**	4	**デバイスまたはVPNのステータス。**
2	[モニタリング（Monitoring）] ビューのコントロール。	5	選択したデバイスの詳細情報。
3	全デバイスの概要。		

[モニタリング（Monitoring）] ディスプレイは、5 つの主な要素で構成されています。

- [ビュー（Views）] リスト（1）：このペインには、使用可能なすべてのビューが一覧表示されます。このリストのエントリをクリックすると、そのビューが [モニタリング（Monitoring）] ペインで開きます。このビューは、Health and Performance Monitor の一部として提供される [システムビュー（System Views）] と、ユーザーが作成したカスタムビューである [マイビュー（My Views）] で編成されます。[ビュー（Views）] ペインについてはデバイスビューの管理 （27 ページ）、カスタムビューの管理についてはビュー：カスタム （31 ページ）を参照してください。
- [モニタリング（Monitoring）] ビューのコントロール（2）：開いている各ビューのラベル付きタブがここに表示されます。任意のタブをクリックすると、そのビューが前面に表示されます。[後ろにスクロール（Scroll Backward）] ボタンと [前にスクロール（Scroll Forward）] ボタンを使用して、タブ付きビューから別のタブ付きビューへと前後に移動することもできます。または、右側の [リストの表示（Show List）] ドロップダウンメニューを開き、ラベルを選択してアクティブビューにします。
- 全デバイスまたは VPN の概要（3）：このビューに表示されるすべてのデバイスまたは VPN の集約情報を提供します。このセクションを展開するか折りたたむには、右側のボタンをクリックします。デバイス概要セクションについては、モニタリングビュー：デバイスまたは VPN サマリー （34 ページ）で詳しく説明されています。
- デバイスステータスリスト（4）：このビューに含まれるすべてのデバイスまたは VPN がここに一覧表示されます。このリストの詳細については、モニタリングビュー：デバイスまたは VPN ステータスリスト （35 ページ）を参照してください。 リストフィルターフィールドの使用 （25 ページ）で説明されているように、このセクションの [リストフィルタ（List Filter）] フィールドを使用してリストをフィルタリングします。
- 選択されたデバイスまたは VPN の詳細（5）：このセクションには、デバイスリストで現在強調表示されているデバイスまたは VPN に関する詳細情報が表示されます。詳細セクションについては、 モニタリングビュー：デバイスまたは VPN の詳細 （36 ページ）で詳しく説明されています。

ここでは、次の内容について説明します。

- モニタリングビュー：デバイスまたは VPN サマリー （34 ページ）
- モニタリングビュー：デバイスまたは VPN ステータスリスト （35 ページ）
- モニタリングビュー：デバイスまたは VPN の詳細 （36 ページ）
- モニタリングビュー：VPN、RA および S2S （39 ページ）
- HPM データのエクスポート （40 ページ）

モニタリングビュー：デバイスまたは VPN サマリー

HPM モニタリング画面には、タブ付きのビューが表示されます。各ビューには、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）で説明されているように、現在選択されているデバイスまたは VPN に関する詳細情報が表示されます。ここで説明され

ているように、すべてのデバイス関連ビュー（つまり、リモートアクセスユーザーとサイト間トンネルビューを除くすべて）には、概要セクションが含まれています。

このデバイスサマリー（VPNサマリー）は、タイトルバーの右側にあるボタンをクリックして表示または非表示にすることができ、現在のビューに関連するすべてのデバイスまたは VPN のヘルスステータスとアラートステータスを集約したスナップショットを表示します。たとえば、[ファイアウォールデバイス（Firewall Devices）] パネルを表示している場合、ステータスの概要は、監視対象のすべてのファイアウォールデバイスについてのみ表示されます。

モニタリングビュー：デバイスまたは VPN ステータスリスト

[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）には、（特定のデバイスビューまたは [VPNサマリー（VPN Summary）] ビューで）現在選択されているデバイスまたはVPN に関する詳細情報が表示されます。すべてのデバイス関連ビューと [VPNサマリー（VPN Summary）] ビューには、現在のビューに関連する監視対象デバイスまたは VPN のテーブルが含まれています。

このテーブルには、すべての監視対象デバイスまたは VPN の「概要」ステータス情報が表示されます。それぞれ、このテーブルのエントリで表されます。ASA クラスタは展開可能なエントリとして表示されます。クラスタエントリの前にある [+] アイコンをクリックして展開し、各クラスタノードのインデントされたエントリを表示します。

この場合もやはり、リストには、現在のビューに関連する要素のみが含まれています。たとえば、[ファイアウォールデバイス（Firewall Devices）] ビューのリストには、IPS デバイスのエントリは含まれません。[リモートアクセスユーザー（Remote-Access Users）] および [サイト間トンネル（Site-to-Site Tunnels）] ビューには、このステータス表示は含まれません。

テーブルの列のサイズを変更したり、列の表示と非表示を切り替えたりできます。列の見出しは、選択したパラメータに従ってデバイスを非表示または表示することで、テーブルをフィルタ処理するために使用できるメニューです。これらのオプションの詳細については、テーブル列の表示と非表示 （10 ページ）を参照してください。

このリストのエントリを選択すると、モニタリングビュー：デバイスまたはVPN の詳細 （36 ページ）で説明されているように、そのデバイスの詳細情報がテーブルの下のデバイス詳細領域に表示されます。

ヒント [すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[IPSデバイス（IPS Devices）]、および [優先デバイス Priority Devices）] ビュー（および任意のカスタムデバイス関連ビュー）では、強調表示されたエントリを右クリックし、ポップアップメニューから [デバイスマネージャ（Device Manager）] を選択して、そのデバイスに適切な外部デバイスマネージャ（つまり、ASA の ASDM と IPS センサーの IDM）を開き、そのデバイスの正常性データとパフォーマンスデータを「ドリルダウン」できます。デバイスマネージャの詳細については、デバイス マネージャの起動を参照してください。

モニタリングビュー：デバイスまたは VPN の詳細

[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）には、現在選択されているデバイスまたは VPN に関するビューと詳細情報が表示されます。すべてのデバイス関連ビューと VPN サマリービューには、その上のデバイス ステータス テーブルで現在選択されている、個々のデバイスまたは VPN に関する詳細情報の 3 つまたは 4 つのタブ付きパネルが表示されます（[リモートアクセスユーザー（Remote-Access Users）] および [サイト間トンネル（Site-to-Site Tunnels）] ビューには、この詳細パネルは表示されません）。

ビューのタイプごとに表示される情報は次のとおりです。

[すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[IPS デバイス（IPS Devices）]、[優先デバイス（Priority Devices）]、およびカスタムデバイス関連のビューの場合、タブ付きパネルは次のとおりです。

- [概要（Summary）]：[概要（Summary）] タブは、デバイスとデバイスのステータスに関する情報を提供する 4 つのセクションで構成されています。
  - [デバイス情報（Device Information）]：このセクションには、デバイス名、IP アドレス、デバイスタイプ、モデル番号などのデバイス固有の情報の読み取り専用リストが表示されます。フェールオーバー情報の読み取り専用リストも表示されます。ASA クラスタが選択されている場合、[フェールオーバー（Failover）] リストはクラスタ関連情報のリストに置き換えられます。
  - [デバイスレポートカード（Device Report Card）]：このセクションには、デバイスの現在のステータスを示す一連のメトリックが表示されます。ここに表示されるメトリックの詳細については、テーブル列：デバイス関連のビュー （10 ページ）を参照してください。
  - [インターフェイスステータス（Interface Status）]：このセクションには、デバイスで定義されているすべてのインターフェイスのリストと、現在のステータス情報が表示されます。
  - [デバイス正常性グラフ（Device Health Graphs）]：このセクションは、CPU やメモリの使用量などの特定のメトリックのグラフィック表示を使用して、デバイスステータスの「スナップショット」を提供します。また、デバイス固有のトラフィック情報、たとえば、ファイアウォールデバイスの平均接続数と変換数（最新のポーリング期間中）、IPS センサーの平均検査負荷と欠落したパケットの割合（最新のポーリング期間中）も表示されます。これらのグラフに使用する期間（過去 1 時間、過去 24 時間、または過去 7 日間）を [期間（Time Frame）] リストから指定できます。グラフの上にあるスライダバーを使用して、特定の期間に焦点を合わせることができます。選択したデバイスのイベントを表示するには、[イベントの表示（View Events）] ボタンをクリックします。イベントビューアが開き、[イベントモニタリング（Event Monitoring）] ウィンドウに、選択したデバイスでフィルタリングされたイベントと、スライダバーで指定された期間が一覧表示されます。

（注） IPSデバイスの場合、特定の正常性メトリックのしきい値を、個々のデバイス（つまり、HPMの外部）で個別に設定する必要があります。したがって、たとえばHPMに何も表示されないまま、IPSデバイスの正常性が重大な状態になる可能性があります。詳細については、アラート設定：IPS （46ページ）を参照してください。

- [アラート（Alerts）]：[アラート（Alerts）]タブには、選択したデバイスのすべてのアラートが一覧表示されます。アラートごとに、複数の列の情報を表示または非表示にすることができます。アラートの詳細については、アラートと通知 （41ページ）を参照してください。このタブ内のフィールドの詳細については、HPMウィンドウ：アラートディスプレイ （42ページ）を参照してください。

[すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、および[優先デバイス（Priority Devices）]の場合、タブ付きパネルは次のとおりです。

- [概要（Summary）]：[概要（Summary）]タブは、デバイスとデバイスのステータスに関する情報を提供する4つのセクションで構成されています。
  - [デバイス情報（Device Information）]：このセクションには、デバイス名、IPアドレス、デバイスタイプ、モデル番号などのデバイス固有の情報の読み取り専用リストが表示されます。フェールオーバー情報の読み取り専用リストも表示されます。ASAクラスタが選択されている場合、[フェールオーバー（Failover）]リストはクラスタ関連情報のリストに置き換えられます。
  - [デバイスレポートカード（Device Report Card）]：このセクションには、デバイスの現在のステータスを示す一連のメトリックが表示されます。ここに表示されるメトリックの詳細については、テーブル列：デバイス関連のビュー （10ページ）を参照してください。
  - [インターフェイスステータス（Interface Status）]：このセクションには、デバイスで定義されているすべてのインターフェイスのリストと、現在のステータス情報が表示されます。
  - [デバイス正常性グラフ（Device Health Graphs）]：このセクションは、CPUやメモリの使用量などの特定のメトリックのグラフィック表示を使用して、デバイスステータスの「スナップショット」を提供します。また、デバイス固有のトラフィック情報、たとえば、ファイアウォールデバイスの平均接続数と変換数（最新のポーリング期間中）、IPSセンサーの平均検査負荷と欠落したパケットの割合（最新のポーリング期間中）も表示されます。これらのグラフに使用する期間（過去1時間、過去24時間、または過去7日間）を[期間（Time Frame）]リストから指定できます。グラフの上にあるスライダバーを使用して、特定の期間に焦点を合わせることができます。選択したデバイスのイベントを表示するには、[イベントの表示（View Events）]ボタンをクリックします。イベントビューアが開き、[イベントモニタリング（Event Monitoring）]ウィンドウに、選択したデバイスでフィルタリングされたイベントと、スライダバーで指定された期間が一覧表示されます。

[VPNサマリー（VPN Summary）] ビューの場合、タブ付きパネルは次のとおりです。

（注） IPS デバイスの場合、特定の正常性メトリックのしきい値を、個々のデバイス（つまり、HPM の外部）で個別に設定する必要があります。したがって、たとえば HPM に何も表示されないまま、IPS デバイスの正常性が重大な状態になる可能性があります。詳細については、アラート設定：IPS （46 ページ）を参照してください。

- [アラート（Alerts）]：[アラート（Alerts）] タブには、選択したデバイスのすべてのアラートが一覧表示されます。アラートごとに、複数の列の情報を表示または非表示にすることができます。アラートの詳細については、アラートと通知 （41 ページ）を参照してください。このタブ内のフィールドの詳細については、HPM ウィンドウ：アラートディスプレイ （42 ページ）を参照してください。
- [フローオフロード（Flow-offload）]：[フローオフロード（Flow-offload）] タブには、オフロードエンジンに関する基本情報、オフロードコアの負荷率、アクティブなオフロードフローに関する情報（作成されたオフロードフローの数、オフロードアクティブフロー、それらの書き換えルールおよびデータ）が表示されます。
- [フローオフロード統計（Flow-offload Statistics）]：[フローオフロード統計（Flow-offload Statistics）] タブには、送信、受信、およびドロップされたパケットの数と、使用された仮想 NIC の統計が表示されます。

[VPNサマリー（VPN Summary）] ビューの場合、タブ付きパネルは次のとおりです。

- [VPNの使用状況（VPN Usage）]：アクティブなサイト間トンネル、アクティブなリモートアクセスセッション、合計スループットなどの情報を示すいくつかのグラフ。これには、アクティブなサイト間トンネル、アクティブ IPSec リモートアクセスユーザー、アクティブ SSL VPN クライアントレスユーザー、およびアクティブ SSL VPN とそのクライアントユーザーの履歴傾向情報が含まれます。
- [クラスタリソースの使用状況（Cluster Resource Usage）]：クラスタリソースの使用状況の詳細（リソース名、その現状、ピーク、および使用制限）を表示します。拒否されたパケットとコンテキストの数も表示します。この機能は、Cisco Firepower 9K デバイスにのみ適用されます。
- [クラスタ分散の詳細（Cluster Distribution Details）]：VPN のクラスタモードを表示します。集中型の場合、接続先モードが VPN 分散型ではないことを示すエラーメッセージが表示されます。分散されている場合は、メンバー I およびメンバー II の詳細が個別に表示されます。この機能は、Cisco Firepower 9K デバイスにのみ適用されます。
- [ライセンス情報（License Information）]：上のテーブルでの選択に応じて、VPN タイプ別のライセンス情報の読み取り専用リスト、または IPSec および SSL ライセンスと負荷情報のリスト。マルチモードデバイスのシステムコンテキストの場合、VPN ライセンスと割り当てが表示されます。個々のコンテキストについて、VPN 割り当ての制限と VPN ライセンスの使用状況が表示されます。
- [その他の詳細（Other Details）]：証明書とトラストポイントの詳細のリスト。

VPN モニタリングの対象デバイスの選択に関する詳細については、監視対象デバイスの管理（6 ページ）を参照してください。

モニタリングビュー：VPN、RA および S2S

HPM モニタリングディスプレイには、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （32 ページ）で説明されているように、さまざまなデバイスおよび VPN に関連したデータビューが表示されます。これには、リモート アクセス ユーザー ビューとサイト間トンネルビューが含まれます。これらのビューは、他のビューとは異なり、単に現在のユーザーとトンネルのテーブルです。

VPN モニタリングの対象デバイスの選択に関する詳細については、監視対象デバイスの管理（6 ページ）を参照してください。

両方のビューで、テーブルの列のサイズを変更したり、列の表示と非表示を切り替えたりできます。列の見出しは、選択したパラメータに従ってエントリを非表示または表示することにより、テーブルをフィルタリングするために使用できるメニューです。これらのオプションの詳細については、テーブル列の表示と非表示 （10 ページ）を参照してください。

リモート アクセス ユーザー ビューには、HPM によってモニタリングされているデバイスを使用してネットワーク リソースに現在ログインしているリモートアクセスユーザーが一覧表示されます。リモートアクセスユーザー情報は、他のビューの標準である 5 分ではなく、20 分ごとに更新されることに注意してください（通常のモニタリングの場合、優先モニタリングの間隔は 15 分です）。また、リモートアクセスユーザーは履歴データやトレンド分析データを利用できません。

さらに、VPN サマリービューとリモート アクセス ユーザー ビューの RA ユーザー数が一致しない場合があります。これは、VPN サマリーが 10 分/5 分（通常/優先）間隔で更新されるためです。

ヒント リモート アクセス ユーザー ビューで、ユーザーエントリを右クリックし、ポップアップメニューから [ユーザーのログオフ（Log Off User）] を選択して、リモートアクセス接続を終了できます。

サイト間トンネルビューは、すべてのモニタリング対象デバイスを使用した現在の VPN トンネル情報を提供します。デバイスまたはコンテキストのトンネルアップ/ダウンアラートを有効にするには、[SNMP Credentials] ダイアログボックスで説明されているように、デバイスで SNMPv3 を設定する必要があることに注意してください。

ヒント サイト間トンネルビューで、[ステータス（Statu）] 列の [ダウン（Down）] 通知ハイパーリンクをクリックして、イベントビューアでそのデバイスの IPSec VPN イベントを表示できます。イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。

ASA 9.0+ デバイスのクラスタの場合、VPN 処理はノード間でロードバランシングされず、クラスタ内の集中サポートに限定されるため、ディレクタデバイスのみの情報が表示されます。

（注） VPN ポーリングは一定の時間間隔で行われるため、その時間間隔内のステータスの変更をログに記録することはできません。たとえば、サイト間トンネルがポーリングの直後にダウンし、次のポーリングの直前に復旧した場合、そのステータスの変化は検出できません。

HPM データのエクスポート

現在のビューに含まれるデバイスステータス情報の「スナップショット」を PDF、HTML、または CSV（カンマ区切り値）ファイルとして保存できます。

（注） Security Manager バージョン 4.9 以降、PDF、HTML、または CSV 形式でエクスポートされたデータには、IPv6 トンネル情報も含まれます。

次に、現在のビューデータを PDF、HTML、または CSV ファイルにエクスポートする手順について説明します。

関連項目

- HPM ウィンドウ （7 ページ）
- テーブル列の表示と非表示 （10 ページ）

ステップ 1 適切なタブをクリックして、エクスポートするビュー（[優先デバイス（Priority Devices）]、[VPNサマリー（VPN Summary）]、[すべてのデバイス（All Devices）] など）を表示します。

ヒント 特定のビューに含まれるエントリすべてのサブセットのデータをエクスポートするには、目的のデバイスのみを含むカスタムビューを作成します。詳細については、ビュー：カスタム （31 ページ）を参照してください。

ステップ 2 [リストフィルタ（List Filter）] フィールド（デバイスまたは VPN ステータスリストの上）の横にある [エクスポート（Export）] ボタンの横にある下矢印をクリックし、ドロップダウンメニューから [PDF形式（As PDF）]、[HTML形式（As HTML）]、または [CSV形式（As CSV）] を選択します。

[エクスポート（Export）] ダイアログボックスが開きます。

ステップ 3 ダイアログボックスの該当する列をオンにして、エクスポートする特定の情報を選択します。

次のトピックでは、さまざまなビューで使用できる個々の列について説明します。

- テーブル列：デバイス関連のビュー （10 ページ）
- テーブル列：VPN 関連のビュー （16 ページ）

ステップ 4 [エクスポート（Export）] ドロップダウンリストから [PDF形式（As PDF）] を選択した場合、[エクスポート（Export）] ダイアログボックスの下部で、PDF ファイルの目的の [ページサイズ（Page Size）]（A1、A2、A4、レター、またはリーガル）を選択できます。

PDF ファイルのページが選択したサイズになり、表示される情報はそれに応じて書式設定されます。

ステップ 5 [エクスポート（Export）] ドロップダウンリストから [CSV形式（As CSV）] を選択した場合、Security Manager は、必要に応じて保存できる CSV ファイルに情報をエクスポートします。バージョン 4.8 以降、Security Manager には、[トレンドチャートのエクスポート（Export Trend Charts）] チェックボックスが用意されています。これを選択すると、トレンド情報をCSVファイル形式でエクスポートできます。チェックボックスの選択後、過去 1 時間、過去 24 時間、過去 7 日間の利用可能な時間範囲からタイムフレームを選択できます。

ステップ 6 [エクスポート（Export）] をクリックすると、[エクスポート（Export）] ダイアログボックスが閉じます。

[ファイルの保存（File Save）] ダイアログボックスが開きます。

ステップ 7 ファイルの名前を入力し、保存する場所を指定します。

デフォルトのファイル名は、現在のシステム時刻（長整数型）です。これを説明的な名前に変更することもできます。Windows システムの場合、デフォルトの場所は My Documents です。任意の場所を指定できます。

ステップ 8 [保存（Save）] をクリックして [保存（Save）] ダイアログボックスを閉じ、選択したデータをエクスポートします。

アラートと通知

Health and Performance Monitor（HPM）では、監視対象デバイスのパフォーマンスと正常性に関するトレンド情報、アラート、および通知が提供されます。個々のデバイスおよびデバイスグループのステータスを迅速にスキャンすることにより、ネットワークユーザーとデバイスリソースの使用率を含む、ネットワークの全体的な正常性を監視できます。

特定のデバイスレベルのトレンド情報は、毎時、毎日、および毎週の間隔で利用できます。アラートは目立つように表示され、関連する HPM データに簡単にナビゲートできます。個々のアラートを確認して注釈を付けることもできます。

（注） クラスタのノードが削除され、そのクラスタが Cisco Security Manager で再検出されると、そのノードはHPMのモニタリング対象から除外されます（現在有効になっている場合）。ただし、そのノードで生成されたアラートは引き続き HPM に表示されます。アラートは手動で HPM からクリアする必要があります。

それらのアラートは、設定したしきい値と状態変更ルールに基づいています。さまざまなメトリックの [クリティカル（Critical）]、[警告（Warning）]、および [正常（Normal）] のレベルを定義するしきい値を指定し、インターフェイス障害など、特定の状態変更のルールを設定できます。

さらに、デバイスモニタリングには2つのレベルがあります。最初は、すべてのデバイスが監視されていません。ただし、監視対象のデバイスを「通常」レベルまたは「優先度」レベルで指定できます。レベルごとに個別のアラート定義のセットを定義します。優先デバイスはより頻繁にポーリングおよびレポートされ(「通常の」デバイスの場合は10分間隔であるのに対して5分間隔)、障害パラメータはより厳格です。

また、電子メールアラート通知を有効にできます。設定されている場合、アラートが生成されるたびに、指定されたアドレスに電子メールが送信されます。アラートのカテゴリ（ファイアウォールおよびIPS）ごとに複数のアドレスを指定できます。

（注） 電子メール通知は、アラートが初めて記録されたとき、およびアラートの重大度が警告から重大に変更されたときに送信されます（逆の場合は送信されません）。デバイスが通常の状態に戻った場合、通知は発行されません。

ここでは、次の内容について説明します。

- HPM ウィンドウ：アラートディスプレイ （42 ページ）
- アラート：設定 （44 ページ）
- アラート：表示 （53 ページ）
- アラート：表示 （53 ページ）

HPM ウィンドウ：アラートディスプレイ

HPM ウィンドウには、モニタリングと警告という 2 つの異なる情報が表示されます。[アラート（Alerts）] ボタンをクリックして [アラート（Alerts）] 画面にアクセスします。

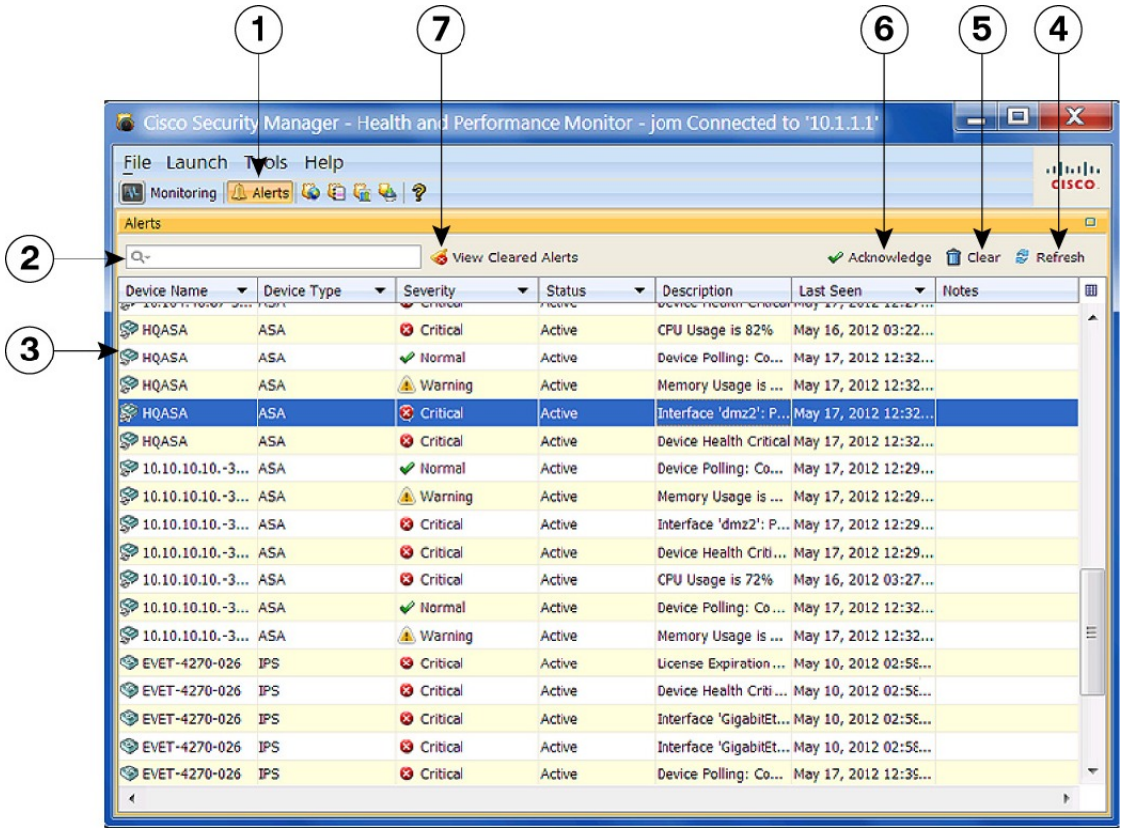
（注） アラートデータのデバイス固有のビューは、特定のデバイスの詳細情報を表示するときに [アラート（Alerts）] タブで使用できます（モニタリングビュー：デバイスまたは VPN の詳細 （36 ページ）を参照）。いくつかの例外を除き、デバイス固有のアラートビューでは、プライマリ [アラート（Alerts）] 画面と同じ機能の多くを実行できます。

次の図は、[アラート（Alerts）] 画面の主な機能を示しています。

関連項目

- アラート：設定 （44 ページ）

図 5 : [ヘルスとパフォーマンスのモニタ（*Health and Performance Monitor*）]：[アラート（*Alerts*）]画面



1	**[アラート（Alerts）]ボタン**	5	**[クリア（Clear）]ボタン**
2	[リストフィルタ（List Filter）]フィールド	6	[確認（Acknowledge）]ボタン
3	[アラート（Alerts）]テーブル	7	[クリアされたアラートの表示（View Cleared Alerts）]ボタン
4	[更新（Refresh）]ボタン		

[アラート（Alerts）]画面は、次の 7 つの主要要素で構成されています。

（注） これらの要素については、[リストのフィルタ（List Filter）]フィールドと[クリアされたアラートの表示（View Cleared Alerts）]ボタンを除き、特定デバイスの詳細情報を表示するときに[アラート（Alerts）]タブで同じ要素を使用できます（モニタリングビュー：デバイスまたはVPNの詳細 （36 ページ）を参照）。

- [アラート（Alerts）]ボタン（1）：HPM ウィンドウには、デバイスおよび VPN の監視情報か、監視対象デバイスによって生成されたアラートのテーブルが表示されます。アラートテーブルを表示するには、この[アラート（Alerts）]ボタンをクリックしてください。

- [リストのフィルタ（List Filter）] フィールド（2）：このフィールドを使用すると、テーブルに表示されるアラートをフィルタ処理できます。指定されたテキストを含むアラートのみがリストされます。詳細については、リストフィルターフィールドの使用 （25 ページ）を参照してください。
- [アラート（Alerts）] テーブル（3）：このテーブルには、現在監視されているすべてのデバイスに関するすべてのアラートがリストされます。表示されるアラートは、[リストのフィルタ（List Filter）] フィールドを使用してフィルタ処理できます。また、アラートごとに、複数の列の情報を表示または非表示にすることもできます。詳細については、アラートと通知 （41 ページ）を参照してください。
- [更新（Refresh）] ボタン（4）：通常のポーリングサイクルより前にすべてのアラートを更新するには、このボタンをクリックします。
- [クリア（Clear）] ボタン（5）：1 つ以上のアラートが選択されている場合、このボタンをクリックして [クリア（Clear）] ダイアログボックスを開くことができます。ダイアログボックスを閉じて、強調表示されたアラートをテーブルからクリアするには、ダイアログボックスの [クリア（Clear）] ボタンをクリックします。

（注） アラートのクリアと確認の詳細については、アラート：確認応答とクリア （54 ページ）を参照してください。

- [確認（Acknowledge）] ボタン（6）：1 つ以上のアラートが選択されている場合、このボタンをクリックして [クリア（Acknowledge）] ダイアログボックスを開くことができます。必要に応じて、選択したアラートに適用されるメモを入力できます。ダイアログボックスを閉じて、強調表示されたすべてのアラートを確認済みとしてマークするには、[確認（Acknowledge）] ボタンをクリックします。

ヒント 以前に確認したアラートにメモを追加できます。そのアラートの [メモ（Note）] フィールドをクリックして、[メモの入力（Enter Notes）] ダイアログボックスを開きます。これは、[メモの入力（Enter Notes）] ダイアログボックスにアクセスする唯一の方法です。

- [クリアされたアラートの表示（View Cleared Alerts）] ボタン（7）：このボタンをクリックすると、[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウが開き、以前にクリアされたアラートにアクセスして確認することができます。対象のデバイスと時間範囲を指定してください。このウィンドウの使用方法の詳細については、アラート：履歴（55 ページ）を参照してください。

アラート：設定

HPM によって提供されるアラートと電子メール通知は、[アラート設定（Alerts Configuration）] ダイアログボックスで設定するしきい値と状態変更ルールに基づいています。

[アラート設定（Alerts Configuration）] ダイアログボックスは、3 つのタブ付きパネルで構成されています。IPS センサー関連のアラートの場合は [IPS]、ファイアウォール関連のアラートの場合は [FW]、トンネルステータスアラートの場合は [VPN] です。各パネルには、セクションのオプションのグループが表示されます。特定のセクションを表示または非表示にするには、展開/折りたたみボタンを使用します。

（注） 該当するセクションを展開せずに、特定のアラートを有効または無効にすることができます。セクションの見出しの前にあるボックスをオンまたはオフにするだけです。現在の設定が使用および保持されます。

デバイスモニタリングには、通常または「標準」の優先順位と「アクティブ」な優先順位の 2 つのレベルがあります。アクティブな優先順位のデバイスはより頻繁にポーリングされて報告され、障害パラメータはより厳格になります。すべてのモニタリング対象デバイスの最大 10% を優先モニタリング対象として指定できます。デバイス選択の詳細については、監視対象デバイスの管理 （6 ページ）を参照してください。

次の手順に従って、標準デバイスと優先デバイス両方のアラートレポートと通知を設定します。

ステップ 1 [ツール（Tools）] メニューから [アラート設定（Alert Configuration）] を選択して、[アラート設定（Alert Configuration）] ダイアログボックスを開きます。

ステップ 2 [IPS] パネルで、IPS 関連のアラートを設定します。必要に応じて、[IPS] タブをクリックしてパネルを表示します。

1. IPS アラートが生成された場合の電子メール通知を有効にするには、[電子メールアドレス（Email Addresses）] フィールドに 1 つ以上の有効なアドレスを入力します。複数のアドレスはコンマで区切ります。
2. セクション見出しのチェックボックスを使用して、特定のアラートを有効または無効にします。セクションを展開して、アラート定義を更新します。IPS パラメータについては、アラート設定：IPS （46 ページ）で説明されています。

（注） 電子メール通知は、アラートが初めて記録されたとき、およびアラートの重大度が警告から重大に変更されたときに送信されます（逆の場合は送信されません）。デバイスが通常の状態に戻った場合、通知は発行されません。

ステップ 3 [FW] パネルで、ファイアウォール関連のアラートを設定します。[FW] タブをクリックしてパネルを表示します。

1. ファイアウォールアラートが生成された場合の電子メール通知を有効にするには、[電子メールアドレス（Email Addresses）] フィールドに 1 つ以上の有効なアドレスを入力します。複数のアドレスはコンマで区切ります。
2. セクション見出しのチェックボックスを使用して、特定のアラートを有効または無効にします。セクションを展開して、アラート定義を更新します。FW パラメータについては、アラート設定：ファイアウォール （48 ページ）で説明されています。

ステップ 4 [VPN] パネルで、トンネルステータスアラートを設定します。[VPN] タブをクリックしてパネルを表示します。

1. トンネルダウンアラートが生成された場合の電子メール通知を有効にするには、[電子メールアドレス（Email Addresses）] フィールドに 1 つ以上の有効なアドレスを入力します。複数のアドレスはコンマで区切ります。
2. セクション見出しのチェックボックスを使用して、トンネルステータスアラートを有効または無効にします。セクションを展開して、アラート定義を更新します。VPN パラメータについては、アラート設定：VPN （50 ページ）で説明されています。

（注） デバイスまたはコンテキストに対してこれらのトンネルステータスアラートを有効にするには、S2S ポーリングのための SNMP の設定 （51 ページ）で説明されているように、まずデバイスで SNMP を設定する必要があります。

ステップ 5 [保存（Save）] をクリックして変更を保存し、ダイアログボックスを閉じます。

アラート設定：IPS

（注） バージョン 4.17 以降、Cisco Security Manager は IPS デバイスをサポートしていません。

モニタリング対象の IPS デバイスから収集されるアラートとステータス情報は、[アラート設定（Alerts Configuration）] ダイアログボックスの [IPS] パネルで設定されます。ダイアログボックスの開き方、IPS パネルへのアクセス、IPS 関連の通知用の電子メールアドレスの指定については、アラート：設定 （44 ページ）を参照してください。

IPS アラートの設定パラメータは、展開したり折りたたんだりできるセクションにグループ化されています。各セクションには、見出しの横にチェックボックスがあります。このチェックボックスを使用して、アラートを有効または無効にします。各セクションを展開すると、アラートの定義に使用される設定にアクセスできます。

次の表で、IPS アラートおよびステータスの設定パラメータについて説明します。各パラメータは、優先デバイスと標準デバイスに対して個別に設定できます（優先モニタリングと標準モニタリングの対象となるデバイスの指定については、監視対象デバイスの管理 （6 ページ）で説明しています）。

（注） 次に挙げる一部のアラート設定では、モニタリング対象の IPS センサー自体で特定の関連パラメータを設定する必要があります。たとえば、特定のセンサーで **license-expiration-policy**（**health-monitor** コマンド）が有効になっていない場合、ライセンス有効期限メッセージはそのセンサーによって生成されないため、HPM はそのセンサーに関するアラートを集計しません。

表 *4 : IPS* アラートの設定

設定	説明
[コラボレーションアプリケーションのステータス（Collaboration App Status）]	コラボレーション アプリケーションによって生成されたエラーが集計されます。アラートと通知は、集計されたエラーの数が指定された発生回数の値に達すると生成されます。
[センサーアプリケーションのステータス（Sensor App Status）]	センサーアプリケーションによって生成されたエラーが集計されます。アラートと通知は、イベントの数が指定された発生回数の値に達すると生成されます。
[バイパスモード（Bypass Mode）]	バイパスモードがトリガーされるたびに、この設定に関する発生回数1が記録されます。アラートと通知は、発生回数が指定された値に達すると生成されます。
インターフェイス ステータス	有効になっている各インターフェイスのステータスは定期的にポーリングされます。任意のインターフェイスに対するポーリング結果「ダウン」は、そのインターフェイスでの発生回数1として記録されます。アラートと通知は、発生回数が指定された値に達すると生成されます。
ライセンスの期限切れ	ライセンスの期限切れのしきい値は、各 IPS センサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。
メモリ使用率	メモリ使用率のしきい値は、各IPSセンサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。 メモリ使用率メッセージごとに発生回数 1 が記録されます。アラートと通知は、発生回数がここで指定された値に達すると生成されます。
[受信できなかったパケット数（Missed Packets）]	受信できなかったパケット数のしきい値は、各IPSセンサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。 受信できなかったパケットメッセージごとに発生回数1が記録されます。アラートと通知は、発生回数がここで指定された値に達すると生成されます。
[検査負荷（Inspection Load）]	トラフィック検査負荷のしきい値は、各 IPS センサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。 負荷超過メッセージごとに発生回数1が記録されます。アラートと通知は、発生回数が指定された値に達すると生成されます。

アラート設定：ファイアウォール

モニタリング対象のファイアウォールデバイスから収集されるアラートおよびステータス情報は、[アラート設定（Alerts Configuration）] ダイアログボックスの [FW] パネルで設定されます。ダイアログボックスを開く方法、[FW] パネルにアクセスする方法、セクションを展開する方法と折りたたむ方法、およびFW関連の通知用電子メールアドレスを提供する方法については、監視対象デバイスの管理 （6 ページ）を参照してください。

ファイアウォールアラートの設定パラメータは、展開したり折りたたんだりできるセクションにグループ化されています。各セクションには、見出しの横にチェックボックスがあります。このチェックボックスを使用して、アラートを有効または無効にします。各セクションを展開すると、アラートの定義に使用される設定にアクセスできます。

一部のセクションの見出しには、[デバイスの正常性を判断する際に考慮（Consider for Device Health）]チェックボックスも含まれています。これらのボックスのいずれかをオンにすると、各デバイスの全体的な正常性を判断するときに、その特定の情報が考慮されるようになります。

次の表で、FW アラートおよびステータスの設定パラメータについて説明します。

表 *5:* ファイアウォールアラートの設定

設定	説明
フェールオーバーピアのステータス	デバイスのフェールオーバーピアへのリンクのステータスは、定期的にポーリングされます。送信試行の失敗は、それぞれ発生回数1として集計されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）]を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。
インターフェイス ステータス	有効になっている各インターフェイスのステータスは定期的にポーリングされます。任意のインターフェイスに対するポーリング結果「ダウン」は、そのインターフェイスでの発生回数1として記録されます。このモニタリングは、スタンドアロンデバイスごと、およびASAクラスタのノードごとに実行されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）]を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。 （注） デバイスの正常性の計算にこれらのデータを含めるには、ヘッダーの [デバイスの正常性を判断する際に考慮（Consider for Device Health）] をオンにします。

マスターの変更	発生回数は、ASA クラスタの制御ユニットノードとして指定されたデバイスが変更されるたびに集計されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）] を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。
クラスタノードのステータス	発生回数は、ASA クラスタノードの接続ステータスが変更（起動または停止）されるたびに集計されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）] を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。
CPU 使用率	発生回数は、CPU 使用率が指定されたしきい値のパーセンテージを超えるたびに集計されます。これはスタンドアロンデバイスごと、シングル コンテキスト クラスタのノードごとに実行されます。またマルチコンテキストクラスタのノードごとに（システムコンテキストに関してのみ）実行されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 （注） デバイスの正常性の計算にこれらのデータを含めるには、ヘッダーの [デバイスの正常性を判断する際に考慮（Consider for Device Health）] をオンにします。 優先デバイスと標準デバイスでは、CPU 使用率の [重大（Critical）] アラートと [警告（Warning）] アラートのいずれかまたは両方を有効にすることができます。 **1.** 該当するボックスをオンにして、[しきい値（Threshold）] フィールドと [発生回数（Occurrence）] フィールドを有効にします。 **2.** 上矢印または下矢印をクリックするか、既存の値を強調表示したり数値を入力したりすることで、[しきい値（Threshold）] のパーセンテージを指定します。 **3.** [発生回数（Occurrence）] フィールドで、指定したしきい値を超えてから重大アラートまたは警告アラートが発行される回数を指定します。

メモリ使用率	発生回数は、メモリ使用率が指定されたしきい値のパーセンテージを超えるたびに集計されます。これはスタンドアロンデバイスごと、シングル コンテキスト クラスタのノードごとに実行されます。またマルチコンテキストクラスタのノードごとに（システムコンテキストに関してのみ）実行されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 （注） デバイスの正常性の計算にこれらのデータを含めるには、ヘッダーの [デバイスの正常性を判断する際に考慮（Consider for Device Health）] をオンにします。 優先デバイスと標準デバイスでは、メモリ使用率の [重大（Critical）] アラートと [警告（Warning）] アラートのいずれかまたは両方を有効にすることができます。 1. 該当するボックスをオンにして、[しきい値（Threshold）] フィールドと [発生回数（Occurrence）] フィールドを有効にします。 2. 上矢印または下矢印をクリックするか、既存の値を強調表示したり数値を入力したりすることで、[しきい値（Threshold）] のパーセンテージを指定します。 3. [発生回数（Occurrence）] フィールドで、指定したしきい値を超えてから重大アラートまたは警告アラートが発行される回数を指定します。

アラート設定：VPN

監視対象デバイスおよびコンテキストでのサイト間（S2S）トンネルのアラートの生成は、[アラート設定（Alerts Configuration）] ダイアログボックスの [VPN] パネルで有効化し、設定します。ダイアログボックスを開く方法、VPN パネルにアクセスする方法、および VPN 関連の通知用電子メールアドレスを提供する方法については、アラート：設定 （44 ページ）を参照してください。

ヒント VPN アラートが有効になっている場合、HPM は、通常/優先順位の指定に従って、監視対象のデバイスとコンテキストを通常間隔および優先間隔（それぞれ 10 分と 5 分）でポーリングします。また、トラップの処理直後に HPM トンネルのステータスを更新する SNMP モニタリングを有効にすることもできます。HPM の SNMP 処理を有効にする方法の詳細については、S2S ポーリングのための SNMP の設定 （51 ページ）を参照してください。

トンネルステータスの設定パラメータは、展開したり折りたたんだりできるセクションにグループ化されています。展開すると、アラート設定にアクセスできます。見出しの横にあるチェックボックスを使用して、アラートを有効または無効にします。

使用可能な VPN アラートパラメータについては、以下の表で説明します。

表 *6 : VPN* アラートの設定

設定	説明

Tunnel Status	監視対象の各 S2S トンネルのステータスは、定期的なポーリングまたは SNMP トラップ処理に基づいて、起動または停止するたびに更新されます。任意のトンネルに対するポーリング結果「ダウン」は、発生回数 1 として記録されます。発生回数がここで指定した値に達すると、アラートが生成されます。 優先デバイスと標準デバイスで、重大と警告の両方のトンネルダウンアラートを個別に設定できます。[重大（Critical）] または [警告（Warning）] を選択して、生成されるアラートのタイプを指定し、[発生回数（Occurrence）] フィールドで、クリティカルまたは警告アラートが発行される前に、ポーリングされたときにトンネルがダウンする回数を指定します。

S2S ポーリングのための SNMP の設定

正常性とパフォーマンスのモニタリング（HPM）アプリケーションは、SNMP を使用して、アップ/ダウンステータス更新のためサイト間（S2S）VPN トンネルをポーリングします。監視対象デバイスおよびコンテキストでのサイト間（S2S）トンネルのアラートの生成は、[HPMアラート設定（HPM Alerts Configuration）] ダイアログボックスの [VPN] パネルで設定します。ダイアログボックスを開く方法、VPN パネルにアクセスする方法、および VPN 関連の通知用 E メールアドレスを提供する方法については、アラート：設定 （44 ページ）を参照してください。

ここでは、S2S ポーリングを提供するために Security Manager で SNMP を設定する方法について概説します。基本的な手順は以下のとおりです。

1. デバイスまたは個々のコンテキストに対して [SNMP] ページで SNMP を有効にして設定します。具体的には、[SNMPサーバーを有効にする（Enable SNMP Servers）] をオンにして、[読み取りコミュニティ文字列（Read Community String）] を指定して確認します。
2. [SNMP Trap Configuration] ダイアログボックスで、[その他（Other）] パネルの [IPSECの開始（IPSEC Start）] および [IPSECの停止（IPSEC Stop）] を確認します。
3. [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスで、インターフェイス名、IP アドレス、コミュニティ文字列を指定（および確認）し、SNMP バージョン（1 または 2c）を選択します。

バージョン 1、2c、および 3 は S2S ポーリングでサポートされていますが、次のセクションで説明するように、バージョン 3 は個別に設定する必要があります。

1. [SNMP Credentials] ダイアログボックスで、デバイスまたは個々のコンテキストの SNMP ログイン情報を設定します。

バージョン 1 および 2c の場合は、RO コミュニティ文字列を指定して確認します。

バージョン 3 の場合、Security Manager は 3 つのモードをサポートします。どれを使用するかは、入力に応じて決まります。

- noauthnopriv（認証なし、プライバシーなし）：ユーザ名は必須ですが、その他は任意。
- authnopriv（認証あり、プライバシーなし）：ユーザ名、パスワード、認証アルゴリズム、およびエンジン ID が必要。

- authpriv（認証あり、プライバシーあり）：ユーザ名、パスワード、認証アルゴリズム、プライバシーパスワード、プライバシーアルゴリズム、およびエンジン ID が必要。

ここでも、次のセクションで説明するように、SNMP v3 の設定は個別に実行されます。

Security Manager デバイスの SNMP v3 の設定

Security Manager で SNMP v3 を直接設定することはできません。 CLI コマンドを使用するか、FlexConfig を設定する必要があります。手順は次のとおりです。

1. SNMP サーバーグループを設定します。

```
snmp-server group group-name v3 [auth | noauth | priv]
```

auth キーワードは、パケット認証を有効にします。noauth キーワードは、パケット認証や暗号化が使用されていないことを示します。priv キーワードは、パケット暗号化と認証を有効にします。auth または priv キーワードには、デフォルト値がありません。

1. 新しい SNMP ユーザを定義します。

```
snmp-server user username group-name{v3 [encrypted]
[auth {md5 | sha]} auth-password
[priv [des | 3des | aes] [128 | 192 | 256] priv-password]
```

v3 キーワードは、SNMP バージョン 3 のセキュリティモデルを使用することを指定し、encrypted、priv、および auth キーワードの使用を有効化します。encrypted キーワードは、パスワードが暗号化された形式であることを示します。暗号化されたパスワードは、16進数の形式である必要があります。

auth キーワードは、使用する認証レベル（md5 または sha）を指定します。

priv キーワードは、暗号化レベルを指定します。auth または priv キーワードには、デフォルト値がありません。

暗号化アルゴリズムには、des、3des、または aes を指定できます。また、使用する AES 暗号化アルゴリズムのバージョンとして、128、192、256 のいずれかを指定することもできます。auth-password は、認証ユーザ パスワードを指定します。priv-password は、暗号化ユーザ パスワードを指定します。

1. SNMP 通知の受信者を指定します。

```
snmp-server host interface {hostname | ip_address} [version 3 username]
```

トラップの送信元となるインターフェイスを示します。デバイスに接続できる NMS または SNMP マネージャの名前と IP アドレスを指定します。

関連項目

- SNMP の設定

アラート：表示

監視対象デバイスに対して生成されたすべてのアラートは、HPM ウィンドウの代替画面に表として表示されます。デバイスがステータス情報をポーリングされると、アラートテーブルが自動的に更新されます。右側のテーブルの上にある [更新（Refresh）] ボタンをクリックして、テーブルを更新することもできます。

これらのアラートは、設定したしきい値と状態変更ルールに基づいています。詳細については、アラート：設定 （44 ページ）を参照してください。

（注） 監視対象デバイスの指定については、監視対象デバイスの管理 （6 ページ）を参照してください。

[アラート（Alerts）] 画面に切り替えるには、次の操作を実行します。

- HPM メニューバーの下にある [アラート（Alerts）] ボタンをクリックします

（[モニタリング（Monitoring）] ボタンをクリックするとモニタリング画面に戻ります）。

（注） 特定のデバイスの詳細を表示しているときに、[アラート（Alerts）] タブから特定のデバイスに適用されるアラートを表示することもできます（モニタリングビュー：デバイスまたはVPNの詳細 （36 ページ）を参照）。

アラートリストは、行と列で構成される基本的なテーブルであり、各行は特定のデバイスからの 1 つのアラートを表します。各列には、そのアラートに関する特定の情報（デバイス名、アラートの重大度、記録時間など）が表示されます（アラート画面の詳細については、HPM ウィンドウ：アラートディスプレイ （42 ページ）を参照してください）。

（注） 列見出しは、選択したパラメータに従ってアラートを非表示または表示することにより、テーブルをフィルタ処理するために使用できるメニューです。たとえば、特定のデバイスのアラートのみを表示してから、そのデバイスの重大なアラートのみを選択することができます。詳細については、テーブル列の操作 （9 ページ）を参照してください。

ヒント トンネルアップ/ダウンアラートの [説明（Description）] 列のハイパーリンクをクリックして、イベントビューアでそのデバイスの IPSec VPN イベントを表示できます。イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のアップ/ダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。

アラートテーブルでは、スクロールだけでなく、特定のアラートのセットを表示することもできます。

- このテーブルの上にある [リストをフィルタ処理（List Filter）] フィールドを使用して、リストをフィルタリングします。詳細については、リストフィルターフィールドの使用（25 ページ）を参照してください。
- [クリアされたアラートの表示（View Cleared Alerts）] ウィンドウを使用して、指定した時間範囲で選択された一連のデバイスについて、以前にクリアされたアラートを表示します。詳細については、アラート：履歴 （55 ページ）を参照してください。

また、アラートの確認、アラートのクリア、アラートノートの編集を行うこともできます。

- アラート：確認応答とクリア （54 ページ）で説明されているように、アラートを確認またはクリアできます。
- 既存のアラートメモに追加するには、テーブル内の該当するエントリの [メモ（Notes）] フィールドをクリックして、[メモの入力（Enter Notes）] ダイアログボックスを開きます。このダイアログボックスは、メモを表示してアラートに追加するために使用します。テーブルで既存のメモを含む単一のアラートが選択されている場合にのみ使用できます。

アラート：確認応答とクリア

アラート：表示 （53 ページ）で説明されているように、監視対象デバイスに対して生成されたすべてのアラートが [アラート（Alerts）] テーブルに表示されます。個々のアラートにメモを追加したり、アラートを個別またはグループで確認または消去したりできます。

アラートを選択するには、[アラート（Alerts）] テーブルでそのエントリをクリックします。Shift キーを押しながら別のアラートをクリックして、2 つの間のグループを選択できます。また、Ctrl キーを押しながらさまざまな行をクリックして、連続していない複数のアラートを選択できます。

テーブルでアラートを選択すると、次のことができます。

- [確認（Acknowledge）] ボタンをクリックして [アラートの確認（Acknowledge Alert）] ダイアログボックスを開きます。これを使用してメモを追加し、選択したアラートを確認済みとしてマークします。一度に複数のアラートを確認できます。

このダイアログ ボックスの [メモ（Notes）] フィールドにテキストを入力し（これはオプションです）、[OK] をクリックします。ダイアログボックスが閉じ、アラートが確認済みとしてマークされ、[メモ（Notes）] カラムにタイムスタンプが表示されます。

- [クリア（Clear）] ボタンをクリックして [アラートのクリア（Clear Alert）] ダイアログボックスを開き、メモを追加し、選択したエントリを [アラート（Alerts）] テーブルから削除します。

このダイアログ ボックスの [メモ（Notes）] フィールドにテキストを入力し（これはオプションです）、[OK] をクリックします。ダイアログボックスが閉じ、選択したアラートが [アラート（Alerts）] テーブルから削除されます。

（注） 関連するしきい値を変更すると、アラートは HPM によって自動的にクリアされます。クリアしたアラートと同様に、これらのアラートは [クリアされたアラートの表示（View Cleared Alerts）] ウィンドウで確認できます（アラート：履歴 （55 ページ）を参照）。

クリアされたアラートに関するメモやその他の情報は、[アラート（Alerts）] データベースに 30 日間保存されます。

アラート：履歴

モニタリング対象デバイスに対して生成されたすべてのアラートは、[HPM] ウィンドウに表として表示されます。アラート：表示 （53 ページ）で説明されているように、表示されている列パラメータでテーブルをフィルタリングできます。

[クリアされたアラートの表示（View Cleared Alerts）] ボタンを使用して、以前にクリアされたアラートにアクセスして確認することができます。対象となるデバイスのセットと時間範囲を指定してください（アラートのクリアについては、アラート：確認応答とクリア （54 ページ）で説明されています）。

（注） クリアされたアラートに関するメモやその他の情報は、アラートデータベースに 30 日間保持されます。生成から 30 日を超えたアラートにはアクセスできません。

[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウを開いて使用するには、次の手順に従います。

1. [アラート（Alerts）] 画面で、[リストフィルタ（List Filter）] フィールドの横にある [クリアされたアラートの表示（View Cleared Alerts）] ボタンをクリックして、[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウを開きます（[HPM] ウィンドウの [アラート（Alerts）] 画面へのアクセスに関する詳細については、アラート：表示 （53 ページ）を参照してください）。
2. アラートの表示設定を指定します。これらの設定により、表示するアラートのセットが定義されます。
   - 対象のデバイスを指定します。[すべて（All）] のデバイスがデフォルトで選択されています。特定のデバイスセットを選択するには：
   - [選択（Select）] ボタンをクリックして、[デバイスの選択（Select Device）] ダイアログボックスを開きます。
   - 目的のデバイスを選択します。除外するデバイスの選択を解除します。
   - [OK] をクリックして [デバイスの選択（Select Devices）] ダイアログボックスを閉じます。

- 表示するアラートのタイプを指定します。[重大（Critical）]、[警告（Warning）]、[正常（Normal）] を選択または選択解除します。
- [開始（From）] の日時および [終了（To）] の日時を選択して、目的の [時間範囲（Time Range）] を定義します。この範囲内に [最初の確認（First Seen）] 時刻が入っているすべてのアラートが表示されます。

[開始（From）] と [終了（To）] にはそれぞれ、月と日の選択に使用される標準のドロップダウンカレンダーが表示されます。

各カレンダーの下の時間フィールドを使用して、正確な開始時刻または終了時刻をそれぞれ指定します。数字を強調表示して上矢印または下矢印をクリックするか、目的の数字を入力します。[現在（Now）] ボタンをクリックして、現在の時刻を指定することもできます。

1. [検索（Search）] ボタンをクリックして、定義済みのアラートセットを表示します。

[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウには、クリアされたアラートの表示をフィルタリングするために使用できる [リストフィルタ（List Filter）] フィールドがあることに注意してください。このフィールドの使用方法については、リストフィルターフィールドの使用 （25 ページ）で説明されています。

このテーブルをフィルタリングする他の方法については、テーブル列の操作 （9 ページ）を参照してください。

SNMP トラップ転送通知

4.6 以前のバージョンの Security Manager では、ASA、IPS、および VPN に関して Health and Performance Monitor のアラートが生成されると、電子メール通知がユーザーに送信されていました。

このフレームワークは、Security Manager 4.7 で、電子メール通知に加えて SNMP トラップ通知を送信するように拡張されました。Security Manager 4.7 はアラートをトラップに変換し、それらを中央 SNMP トラップサーバーに送信します。SNMP v1、v2c、および v3 がサポートされています。アラートが最初に生成されるとトラップが生成され、重大度が増加するとトラップが再生成されます。その結果、電子メール通知の場合と同様に、トラップが最大 2 回生成されます。

SNMP トラップ転送通知には、次の前提条件があります。

1. SNMP トラップ受信者（サーバー）を使用できる。また、特定の Security Manager インストールに複数のサーバーを使用できる。
2. ASA デバイスを使用できる。
3. IPS 7.0.x 以降を実行する IPS センサーを使用できる。
4. Health and Performance Monitor が有効になっている。

ヒント　Health and Performance Monitor が有効になっていることを確認するには、[Configuration Manager] > [ツール（Tools）] > [Security Manager 管理（Security Manager Administration...）] > [Health and Performance Monitor] に移動します。

1. Health and Performance Monitor で ASA デバイスおよび IPS センサーデバイスの通常または優先監視が有効になっている。
2. ファイアウォール、IPS、および VPN のアラート設定が有効になっている。

ヒント　ファイアウォール、IPS、および VPN のアラート設定を有効にするには、[Health and Performance Monitor] > [ツール（Tools）] > [アラート設定（Alert Configuration）] に移動します。

MIB ドキュメント

ここでは、Security Manager がトラップ通知の送信に使用する MIB と、特定のアラート情報を取得するためにユーザーが検索する必要がある OID について説明します。

SNMP トラップの場合、Security Manager は「CISCO-DEVICE-EXCEPTION-REPORTING-MIB」を使用します。

次のリストには、OID の詳細とそれに含まれる情報が示されています。

- iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0（HPM サーバーの稼働時間を示します）：「システム稼働時間 = 現在の Security Manager サーバー時間 - HPM サービス起動時間」で計算されます。
- snmpTrapOID（1.3.6.1.4.1.9.9.224.2.0.1）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.2（「memory usage」のようなアラートルール名をリストします）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.3（定数値 1、IP アドレスタイプを示します）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.4（デバイス表示名：デバイスタイプおよびクラスタノード（存在する場合）とデバイスの名前）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.5（アラートの重大度）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.6（アラートのタイムスタンプ）：現在の Security Manager サーバー時間 - アラートが最初に生成された時間
- .1.3.6.1.4.1.9.9.224.1.1.5.1.7（アラートを説明する最大 1024 文字の文字列）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.8（Security Manager サーバー名）

ここでは、次の内容について説明します。

- [SNMP トラップエントリ（SNMP Trap Entries）] ダイアログボックス （58 ページ）

• [SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックス （59 ページ）

[SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックス

SNMP トラップ転送通知の開始点として [SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックスを使用します。

ナビゲーション パス

ヘルスとパフォーマンスのモニターで、[ツール（Tools）] メニューから [SNMPトラップの設定（SNMP Trap Configuration）] を選択します。[SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックスには、次の領域が含まれています。

- 現在設定されているトラップを表示する [設定（Settings）] テーブル。
- SNMP トラップエントリを操作するための追加、編集、およびその他のオプション。

フィールド リファレンス

表 *7 : [SNMP*トラップエントリ（*SNMP Trap Entries***）*]* ダイアログボックスの *[*設定（***Settings***）*]* テーブルとその他のオプション**

フィールド	説明
[トラップの転送先（Forward Trap To）] テーブル	
[ステータス（Status）] 列	[Enabled] と [Disabled] があります。常に最大 5 つのトラップ転送ホストを有効にできます。
[IP/ホスト（IP/Host）]列	中央 SNMP トラップサーバーの IP アドレスまたはホスト名。パフォーマンスの問題を避けるため、ローカルホストおよび Security Manager サーバーは、両方とも SNMP サーバーとして使用できません。
[ポート（Port）] 列	中央 SNMP トラップサーバーが使用するポート
[SNMPバージョン（SNMP Version）] 列	v1、v2c、または v3。デフォルトは v2c です。
[Username] カラム	SNMP サーバーに対する認証用のユーザ名
[認証アルゴリズム（Authentication Algorithm）] 列	MD5 または SHA
[暗号化アルゴリズム（Encryption Algorithm）] 列	DES、3DES、AES128、AES192、および AES256

フィールド	説明
追加（Add）	新しい設定の追加に使用します。[追加（Add）] ボタンをクリックすると、[トラップ設定の追加（Add Trap Settings）] ダイアログボックスが開きます。
Edit	既存の設定の編集に使用します。[編集（Edit）] ボタンをクリックすると、[トラップ設定の編集（Edit Trap Settings）] ダイアログボックスが開きます。
設定のコピー（Copy Settings）	既存の構成のすべての設定をコピーするために使用されます。[設定のコピー（Copy Settings）] ボタンをクリックすると、[SNMPトラップ設定のコピー（Copy SNMP Trap Settings）] ダイアログボックスが開きます。
削除（Delete）	既存の設定の削除に使用します。
有効	既存の設定の有効化に使用します。
無効	既存の設定の無効化に使用します。

[SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックス

[SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックスを使用して、SNMP トラップを追加、編集、およびその他の方法で操作および設定します。

ナビゲーション パス

ヘルスとパフォーマンスのモニターで、[ツール（Tools）] メニューから [SNMPトラップの設定（SNMP Trap Configuration）] を選択します。次に、[追加（Add）]、[編集（Edit）]、または [設定のコピー（Copy Settings）] を選択します。

[SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックスには、次のエリアがあります。

- IP/ホストおよびポートエリア
- FW アラート、IPS アラート、および VPN アラートのトラップ設定エリア
- SNMP オプションのトラップ設定エリア

フィールド リファレンス

表 *8 : [SNMP*トラップエントリの追加/編集/コピー（*Add/Edit/Copy SNMP Trap Entries*）*]* ダイアログ ボックスの *[*トラップ設定（*Trap Settings*）*]* エリアおよびその他のオプション

フィールド	説明
トラップの設定	次のトピックで説明されている、FW、IPS、および VPN のすべてまたは選択したアラートのみを選択するために使用されます。 • アラート設定：ファイアウォール （48 ページ） • アラート設定：IPS （46 ページ） • アラート設定：VPN （50 ページ）
SNMP オプション	
RO Community String （SNMP バージョン V1 と V2C のみ）	SNMP バージョン v1 または v2c で認証に使用されるパスワード。
グループ タイプ （SNMP バージョン v3 のみ）	NOAUTH、AUTH、または PRIV。
エンジンID（Engine ID） （SNMP バージョン v3 のみ）	v3 で認証に使用される SNMPEngineID 識別子。
ユーザー名 （SNMP バージョン v3 のみ）	SNMP サーバーに対する認証用のユーザー名
認証パスワード（Authentication Password） （SNMP バージョン v3 のみ）	SNMP サーバーに対する認証用のパスワード
認証プロトコル（Authentication Protocol） （SNMP バージョン v3 のみ）	MD5 または SHA。
Encryption Password （SNMP バージョン v3 のみ）	MD5 または SHA 暗号化のパスワード。
暗号化プロトコル（Encryption Protocol） （SNMP バージョン v3 のみ）	DES、3DES、AES128、AES192、および AES256。

注：AES192、AES256、または 3DES を使用するには、次の手順に従う必要があります。

1. http://www.oracle.com/technetwork/ > [ダウンロード（Downloads）] > [Java SE] > [JDK/JRE 7用Java暗号拡張（ JCE）無制限の強度の司法管轄権ポリシーファイル（Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 7）] から、無制限の強度の暗号ポリシー .jar ファイルをダウンロードします。（[ダウンロード（download）] ボタンをクリックして、ライセンス契約に同意し、ファイルをダウンロードします。）
2. Security Manager サーバーの CSCOpx\MDC\vms\jre\lib\security フォルダにある local_policy.jar および US_export_policy.jar を置き換えます。
3. Security Manager サーバーを再起動します。

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。