レポートの管理

Re

Report Manager アプリケーションを使用して、デバイス、およびリモート アクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。

この章は次のトピックで構成されています。

port Manager アプリケーションを使用して、デバイス、およびリモートアクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。

この章は次のトピックで構成されています。

レポート管理について

Report Manager アプリケーションを使用して、デバイス、およびリモート アクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。これらのレポートは、ご使用のネットワークに関する有益な情報を提供します。

Report Manager は、Event Manager サービスによってモニタ対象デバイスから収集される情報を集約します。このため、デバイスに関するレポートを表示するには、Event Viewer のデバイスもモニタリングする必要があります。一部の統計情報（VPN 統計情報など）は、通常の 5 分間隔のポーリングによってデバイスから直接取得されます。集約データには、15 分、毎時、毎日、および毎月の間隔で集約されるデータがあり、90 日間保持されます。15 分の集約データ

は最大3日間、毎時のデータは最大1週間保持されます。データ集約の詳細については、Report Manager データ集約について （5 ページ）を参照してください。

Report Manager を使用して、以下に関するレポートを作成できます。

- ASA ソフトウェアリリース 8.0 以降を実行する適応型セキュリティアプライアンス（ASA）。VPN レポートの場合、ASA ソフトウェア 7.x リリースもサポートされます。

（注） VPN レポートは、VPN 設定をサポートしていない Cisco Catalyst 6500 シリーズ ASA Services Modules（ASA-SM; ASA サービス モジュール）では使用できません。その他のタイプのレポートは、ASA-SM で使用できます。

- IPS ソフトウェアリリース 6.1 以降を実行する IPS デバイス（IOS IPS デバイス以外）。これには、ASA、ルータ、およびスイッチに取り付けられた専用 IPS モジュールが含まれます。
- サポートされる ASA デバイスでホストされているリモート アクセス IPsec および SSL VPN。

（注） Event Viewer は FWSM を処理しますが、Report Manager は FWSM イベントについては報告しません。

次のトピックでは、Report Manager および使用可能なレポートをさらに詳細に説明し、Security Manager で使用可能なその他のタイプのレポートについても説明します。

- Security Manager で使用可能なレポートのタイプについて （2 ページ）
- Report Manager レポート用のデバイスの準備 （4 ページ）
- Report Manager データ集約について （5 ページ）
- Report Manager のアクセス コントロールについて （7 ページ）
- Report Manager の事前定義システム レポートについて （17 ページ）

Security Manager で使用可能なレポートのタイプについて

Security Manager は、さまざまなレポート機能を提供します。以下に、使用可能なレポートのタイプを示します。

- **セキュリティおよび使用状況のレポート（Report Manager アプリケーション）**：Report Manager アプリケーションを使用して、Event Manager サービスによってモニター対象デバイスから収集された集約情報を表示できます。デバイスから直接取得される情報もあります。これらのレポートは、ネットワーク セキュリティおよびリモート アクセス IPsec および SSL VPN の使用状況に関する情報を提供します。

- **アクティビティ（設定セッション）変更レポート**：これらのレポートは、特定アクティビティ（Workflow モード）または設定セッション（Workflow 以外のモード）内で変更されたポリシーに関する詳細情報を提供します。詳細については、変更レポートの表示を参照してください。
- **アウトオブバンド変更レポート**：これらのレポートは、デバイスに存在する設定と Security Manager で管理されるデバイスの設定の間の不整合を識別します。この情報を使用して、設定を展開する前にこれらの不整合に事前に対処できます。この場合、展開ジョブで選択する動作に応じて、変更が上書きされるか、または展開が失敗します。詳細については、アウトオブバンド変更の検出および分析を参照してください。
- **監査レポート**：このレポートは、Security Manager およびデータベースに含まれているオブジェクトに対する変更内容に関する情報を提供します。このレポートには、ランタイム環境（ログインや認証の失敗など）、オブジェクトに対する変更（アクティビティの変更や展開など）、および管理対象デバイスに対する変更（インベントリの追加や削除など）に関する情報が含まれています。詳細については、監査レポートの生成を参照してください。
- **インベントリステータス**：このレポートは、ポリシー展開ステータスに関する情報を提供します。詳細については、インベントリ ステータスの表示を参照してください。
- **ポリシー検出ステータスレポート**：デバイスからポリシーを検出するときに（インベントリへの追加時または管理対象デバイスのポリシーの再検出時のいずれか）、ポリシー検出に関する情報はあとで表示できるように保持されます。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。
- **展開ステータスレポート**：管理対象デバイスに設定を展開するときに、展開に関する情報はあとで表示できるように保持されます。詳細については、ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示を参照してください。
- **トラブルシューティングのための展開および検出ステータスレポート**：展開およびポリシー検出ステータスレポートを Cisco Technical Support（TAC）への送信に適した形式でエクスポートし、問題のトラブルシューティングに役立てることができます。これらのレポートがユーザ独自の目的に役立つ場合もあります。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成を参照してください。
- **エクストラネット VPN 設定概要**：エクストラネット VPN 設定概要の PDF ファイルを印刷または生成できます。この概要には、接続に使用されている事前共有キーが含まれている場合があります。この情報を使用して、ご使用のネットワークとパートナーまたはサービス プロバイダーのネットワークの間の現在の接続記録を維持できます。詳細については、[VPNトポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）]を参照してください。
- **ポリシーオブジェクト使用状況レポート**：このレポートは、ポリシーオブジェクトの使用場所（そのポリシーオブジェクトがポリシーまたは別のポリシーオブジェクトによって参照されているインスタンスなど）を示します。この情報を使用すると、提案されたオブジェクトに対する変更が、そのオブジェクトのすべての使用ケースで目的の効果を提供するかどうかの判別に役立ちます。ポリシーや別のポリシーオブジェクトによってアクティブに使用されているオブジェクトは削除できないため、この情報はオブジェクトを削除す

る場合にも役立ちます。詳細については、オブジェクト使用状況レポートの生成を参照してください。

- **ポリシー オブジェクト オーバーライド レポート**：このレポートは、ポリシーオブジェクトに対して現在定義されているデバイスレベルのオーバーライドをすべて表示します（オーバーライドを許可するようにそのオブジェクトが定義されている場合）。このレポートからオーバーライドの作成および削除を行うこともできます。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集および[Policy Object Overrides] ウィンドウを参照してください。
- **デバイスマネージャレポート**：Security Manager には、ほとんどのサポート対象デバイスについて、Adaptive Security Device Manager（ASDM）などの個々のデバイスマネージャの読み取り専用バージョンが含まれています。これらのデバイスマネージャを Security Manager の Configuration Manager アプリケーションから直接開始し、それらのデバイスマネージャで使用できる任意のタイプのレポートを使用できます。これらのレポートは単一のデバイスに対するものであり、Report Manager を介して使用できるレポートを増強できます。Event Viewer または Report Manager では直接サポートされていないデバイスのステータス情報を提供することもできます。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。

Report Manager レポート用のデバイスの準備

Report Manager でデバイスに関するレポートを表示する前に、Security Manager にイベントを送信するようにデバイスを設定し、そのデバイスをモニタするように Security Manager を設定する必要があります。Report Manager は Event Viewer でモニタリングしているデバイスに関するレポートのみを提供できるため、レポートのためのデバイス設定はイベントモニタリングのための設定と同じです。

ステップ 1 Security Manager にイベントを送信するようにデバイスを設定します。次のタイプのデバイスで Report Manager を使用できます。

- ASA 8.0 以降：詳細な設定手順については、イベント管理のための ASA と FWSM デバイスの設定を参照してください。
- IPS 6.1 以降：詳細な設定手順については、イベント管理のための IPS デバイスの設定を参照してください。

ステップ 2 モニタするデバイスの選択の説明に従って、デバイスがイベント管理用に選択されていることを確認します。

ステップ 3 Event Manager サービスの開始、停止、および設定の説明に従って、Event Manager サービスがイネーブルであることを確認します。

Report Manager データ集約について

Report Managerは、Event Managerサービスによってモニタ対象デバイスから収集される情報を集約します。このため、デバイスに関するレポートを表示するには、Event Viewerのデバイスもモニタリングする必要があります。

Report Managerは、2つの方法を使用してデータを収集します。まず、Event Managerサービスは、関連するイベントをReport Managerに提供し、次にReport Managerが定義済みのレポートと現在設定されているカスタムレポートに基づき、それらのイベントを保存する必要があるかどうかを決定します。次に、VPN統計情報などの一部の統計情報は、通常のポーリングを使用して5分間隔でデバイスから直接取得されます。

表 *1 : Report Manager* のデータ ソース

レポート（**Reports**）	データ ソース（**Data Sources**）
FW レポート	
上位ソース 上位接続先 最上位サービス（Top Services）	構築された Syslog： 302013、302015、302017、302020 syslog を拒否： 106001、106006、106007、106010、106011、106014、106015、106016、106017
上位マルウェア サイト（Top Malware Sites） 上位マルウェアポート 上位感染ホスト	BOTNET Syslog： 338001、338002、338003、338004、338005、338006、338007、338008、338201、338202、338203、338204
IPS レポート	
すべての IPS レポート	すべての IPS アラート
VPN レポート	

上位帯域幅ユーザ（フルクライアント）
上位継続時間ユーザ（フルクライアント）
上位スループットユーザ（フルクライアント）
	ASA バージョン 8.3 以前：
	`show vpn-sessiondb full svc`
	ASA バージョン 8.4.1 以降：
	`show vpn-sessiondb full anyconnect`

レポート（Reports）	データ ソース（Data Sources）

上位帯域幅ユーザ（IPSec-RA）
上位継続時間ユーザ（IPSec-RA）
上位スループットユーザ（IPSec-RA）
	ASA バージョン 8.3 以前：
	`show vpn-sessiondb full remote`
	ASA バージョン 8.4.1 以降：
	`show vpn-sessiondb full ra-ikev1-ipsec`

上位帯域幅ユーザ（クライアントレス） 上位継続時間ユーザ（クライアントレス） 上位スループットユーザ（クライアントレス）	すべての ASA バージョンの場合： `show vpn-sessiondb full webvpn`
ユーザ レポート	上記すべての show コマンド。
VPN デバイス使用状況レポート	上記すべての show コマンド。

Report Managerは、15分、毎時、毎日、および毎月の間隔で、この収集情報を集約します。15分の集約データは1日、毎時のデータは最大5日間、その他のデータは90日間保持されます。

集約スケジュールは固定された時刻に発生します。15 分の集約は正時からの時間で 00 分、15 分、30 分、および45 分に発生します。毎時の集約は正時（00 分）に発生します。毎日の集約は日付が変わるときに発生します（0 時になると、その日付が集約されます）。毎月の集約は月が変わるときに発生します。

集約サイクルは、レポートに表示される内容に影響します。

- レポートデータは直前のデータを対象にするわけではありません。代わりに、選択された期間について、最後に完了した期間全体を対象にします。たとえば、1 日のレポートは昨日を対象にします。今日のデータは含まれません。つまり、1 日のレポートは、レポート生成時刻から始まる直前の 24 時間ではありません。
- カスタム期間を使用してレポートを設定する場合、15分より短い期間を選択することはできません。レポートには、少なくとも 15 分の集約データが必ず含まれます。分のエントリは、最も近い集約時刻（つまり、00、15、30、または45）に丸められます。開始と終了が当日であるカスタム レポートの場合にのみ、分の値を設定できます。

また、毎時のデータは最大で5日間しか保持されないため、過去5日間についてのみ、カスタム期間内の時間を指定できます。

- デバイスがモニタされている期間より長い期間のレポートを生成することはできません。たとえば、初めてEvent Managerサービスを開始する場合、月が変わるまでは毎月のレポートを生成できません。これは、数日のみである場合（たとえば、29日にサービスを開始する場合）も、ほとんど月全体である場合（たとえば、月の最初の日にサービスを開始する場合）もあります。

このルールに対する例外は、カスタム期間レポートです。カスタム期間レポートは毎日の集約データを使用して生成されるため、任意のカスタム期間を選択できます。

（注） 最初の月の集約データは、1 か月に相当するデータよりもかなり少ない可能性があることに注意してください。毎月のレポートを比較する場合、実際に（例として）30 日間のデータと 15 日間のデータを比較していると、これは重大な相違に見える可能性があります。

事前定義システム レポートのデフォルトの時間間隔の設定、および個々のレポートの時間間隔の設定を行うことができます。次のトピックでは、時間コントロールについて説明します。

- レポートのデフォルト設定値の設定 （37 ページ）
- レポート設定の編集 （28 ページ）

Report Manager のアクセス コントロールについて

ユーザ名に対して割り当てられるユーザ権限により、Report Manager 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、またはその他のタイプの非 ACS アクセス コントロールを使用する場合は、すべてのユーザが Report Manager およびすべてのレポート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。

- 事前定義システム レポートのデフォルト設定値を設定するには、システム管理者権限またはネットワーク管理者権限が必要です。 レポートのデフォルト設定値の設定 （37 ページ）を参照してください。
- 別のユーザーのスケジュールに対して、参照、イネーブル化またはディセーブル化、生成された結果の表示、または削除を行うには、システム管理者権限またはネットワーク管理者権限が必要です。次のトピックを参照してください。
  - レポート スケジュールの表示 （42 ページ）
  - スケジューリングされたレポートの結果の表示 （44 ページ）
  - レポート スケジュールのイネーブル化およびディセーブル化 （45 ページ）
  - レポート スケジュールの削除 （46 ページ）
- サーバーに設定されているすべてのカスタムレポートのリストの参照、または別のユーザーのカスタムレポートの削除を行うには、システム管理者権限またはネットワーク管理者権限が必要です。 カスタム レポートの管理 （41 ページ）を参照してください。

ACS を使用して Security Manager へのアクセスを制御する場合、Report Manager へのユーザ アクセスを制御することもできます。ACS を使用する場合、次のようになります。

- View Report Manager 権限を使用して、Report Manager 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、特定のユーザが Report Manager にアクセスできないようにしたり、Event Viewer へのアクセスを許可せずに Report Manager 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。

- ユーザは、少なくともデバイスに対する表示権限がある場合にのみ、そのデバイスのレポートを表示できます。

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。

Report Manager の概要

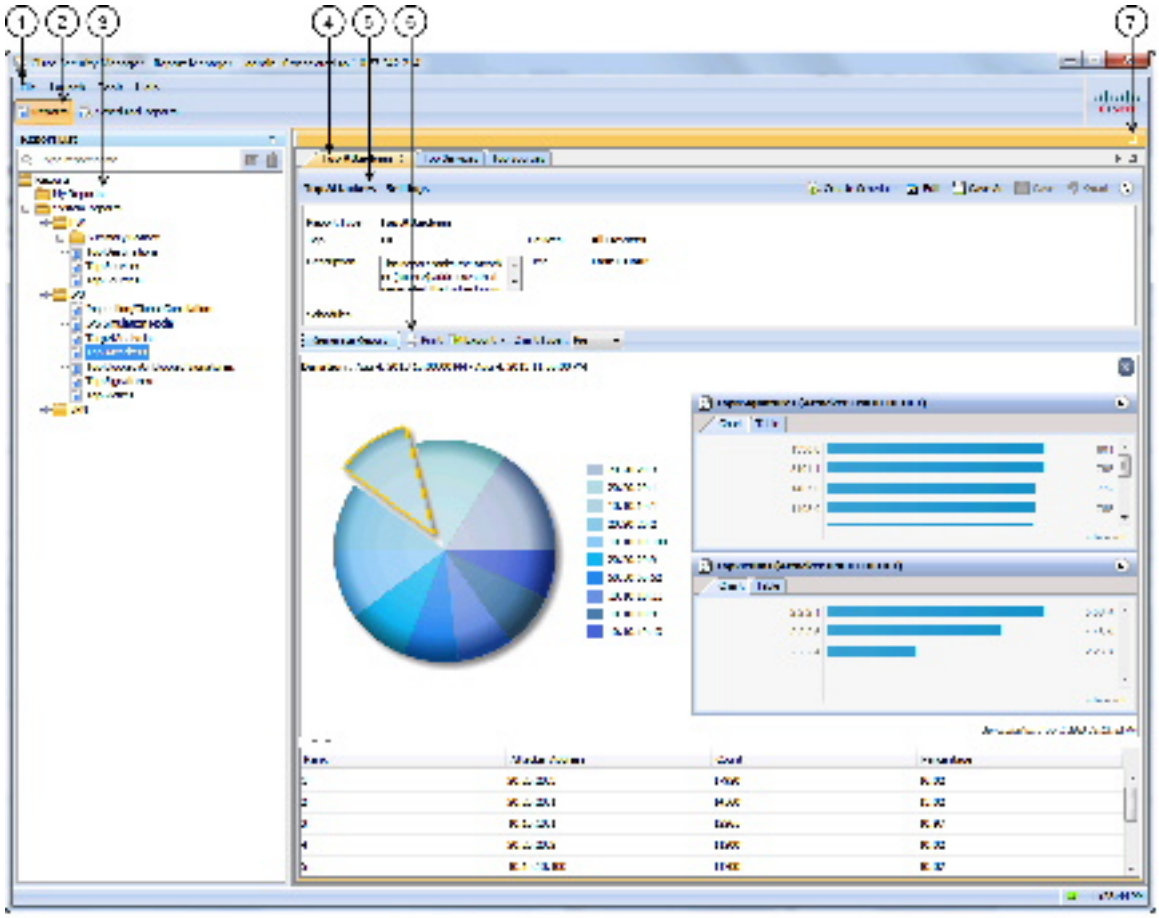
Report Manager を使用して、ASA デバイスと IPS デバイス、およびリモート アクセス IPsec と ASA デバイスでホストされる SSL VPN に関する、セキュリティおよび使用状況のレポートを作成します。サポートされるデバイス、および Report Manager を使用して生成できるレポートの詳細については、レポート管理について （1 ページ）を参照してください。

Report Manager を開くには、次のいずれかを実行します。

- Windows のスタートメニューから [スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Security Managerクライアント（Cisco Security Manager Client）] > [Report Manager] を選択するか（コマンドパスは異なる場合があります）、デスクトップの [Report Manager] アイコンをダブルクリックします。ログインを求められます。Cisco Security Manager クライアント アプリケーションの開始方法の詳細については、Security Manager へのログインおよび終了を参照してください。
- Configuration Manager アプリケーションまたはイベントビューア アプリケーションから **[起動（Launch）] > [Report Manager]** を選択します。他のアプリケーションへのログインに使用したアカウントと同じユーザ アカウントを使用して Report Manager が開きます。

次の図とその後のリストで、Report Manager の基本を説明します。

図 *1 : Report Manager* のメイン ウィンドウ



次のリストで、メイン Report Manager ウィンドウとそのコールアウトをさらに詳細に説明します。

- **メニューバー（1）**：Report Manager でアクションを実行するための一般的なコマンド。コマンドの説明については、Report Manager のメニュー （11 ページ）を参照してください。
- **メインウィンドウのタブ（2）**：次のタブで構成されるメインウィンドウの領域：
  - [Reports]：[Reports] タブを使用して、オンデマンドでのレポートの生成、カスタム レポートの作成、およびその他のレポート指向タスクの実行を行います。上の図と、このトピックのほとんどの情報は、[Reports] タブに関連しています。[Reports] タブから実行できるタスクについては、Report Manager でのレポートの使用 （25 ページ）を参照してください。
  - [Scheduled Reports]：[Scheduled Reports] タブを使用して、レポート スケジュールを表示および管理します。[Scheduled Reports] タブの詳細については、レポート スケジュールの表示 （42 ページ）を参照してください。[Scheduled Reports] タブから実行でき

るタスクについては、レポートのスケジュール設定 （42 ページ）を参照してください。

- **レポートリスト（3）**：[レポート（Reports）] タブの左側のペインは、レポートのリストです。このリストはフォルダに編成されています。[System Reports] は事前定義レポートで、[My Reports] フォルダにはユーザが作成するカスタム レポートが含まれます。レポートをダブルクリックして開くか、レポートを選択して**[ファイル（File）]>[開く（Open）]**を選択するか、またはレポートを右クリックして [レポートを開く（Open Report）] を選択します。レポート リストの使用方法の詳細については、Report Manager のレポート リストについて （12 ページ）を参照してください。
- **レポートペイン（4、5、6、7）**：[レポート（Reports）] タブの右側のペインには、開いているレポートが表示されます。開いている各レポートは別々のタブで表されます（開いているレポートは最大 5 つです）。このスペースにレポートを水平または垂直に配置可能で、別のウィンドウにレポートをフローティングすることも可能であることに注意してください。レポートの配置方法またはフローティング方法の詳細については、レポート ウィンドウの配置 （38 ページ）を参照してください。

ペインの上の最大化コントロール（7）を使用して、そのペインがワークスペース全体を占めるようにする（レポートリストは非表示）ことができます。ペインの最大化後、コントロールはメイン ウィンドウを2つのペインで構成されるビューに戻すための復元コントロールに変わります。

右矢印と左矢印、および [Show List] アイコン ボタンを使用して、開いているレポート間のスクロール、またはレポートへの直接移動を行うことができます。ただし、目的のレポート名が表示されているタブをクリックすることが、レポートに移動する最も簡単な方法です。

レポート ペインには、開いている各レポートに対して次の領域が含まれています。

- - レポート設定ペイン（5）：レポートの上部には、レポートの生成に使用される基準であるレポート設定が表示されます。見出しをクリックするか、または展開/縮小アイコン ボタンをクリックすることにより、設定ペインを開閉できます。見出しには、レポートに対して実行できるコマンドが表示されているツールバーが含まれています。設定ペインの詳細については、レポート設定ペインについて （13 ページ）を参照してください。
  - 生成済みレポート ペインおよびレポート ツールバー（6）：設定ペインの下に、レポートデータの生成および操作に使用する追加のツールバーがあります。これらのコントロールを使用して、レポート設定で定義された基準を使用したレポートの生成、レポートの印刷、レポートの PDF 形式または CSV 形式へのエクスポート、またはレポートに表示されるグラフィックのタイプの変更を行います。

レポート ペインの下部は実際のレポートです。この領域は、[Generate Report] ボタンをクリックするまでは空です。レポートの上部には情報のグラフィカル表現が表示され、ページの下部には表形式のデータが表示されます。詳細については、「生成済みレポート ペインおよびツールバーについて （15 ページ）」および「レポートの起動と生成 （25 ページ）」を参照してください。

Report Manager のメニュー

次の表で、Report Manager のメニューのコマンドを説明します。

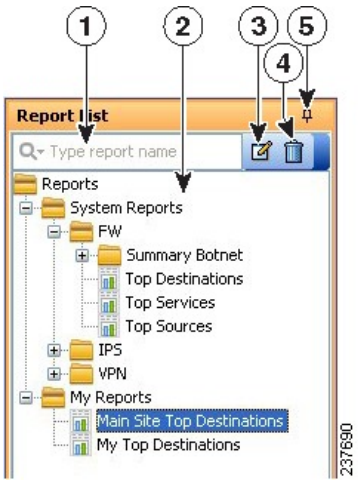
表 *2 : Report Manager* のメニューのリファレンス

メニュー	コマンド	説明
ファイル（File）	オープン（Open）	[Reports] タブのレポートリストで選択されたレポートを開きます。 レポートの起動と生成 （25 ページ）を参照してください。
	保存	レポート設定に対する変更内容を保存します。このコマンドは、カスタム レポートの場合にのみ使用できます。 レポートの保存 （39 ページ）を参照してください。
	名前を付けて保存	レポートを新規レポートとして保存します。このコマンドを使用して、既存のレポートから新規レポートを作成します。 レポートの保存 （39 ページ）を参照してください。
	Close Report Close All Reports	アクティブな開いているレポートを閉じるか、または開いているレポートをすべて閉じます。 レポート ウィンドウの終了 （40 ページ）を参照してください。
	終了（Exit）	Report Manager を終了します。
ラウンチ	ダッシュボード 設定マネージャ（Configuration Manager） イベントビューア Health and Performance Monitor Image Manager	指定された Security Manager アプリケーションを開きます。
Tools	Default Report Settings	事前定義システム レポートのデフォルト設定を設定します。 レポートのデフォルト設定値の設定 （37 ページ）を参照してください。
	Custom Report List	サーバに設定されているカスタム レポートを、ユーザが作成したものだけではなくすべて表示します。このウィンドウからレポートを管理できます。 カスタム レポートの管理 （41 ページ）を参照してください。

メニュー	コマンド	説明
ヘルプ	Help about this page	現在メイン ウィンドウに表示されているページに関連したトピックのオンライン ヘルプを開きます。
	About Report Manager	アプリケーションの著作権、バージョン、およびライセンス情報を表示します。

Report Manager のレポート リストについて

次の図に示すように、Report Manager の [Reports] タブの左側のペインには、使用可能なレポートのリストが表示されます。



レポート リストには、次のコントロールが含まれています（図のコールアウトで示されています）。

- **クイック フィルタ検索ボックス（1）**：クイックフィルタ検索ボックスを使用して、リスト内のレポートを検索します。入力すると、リストはフィルタリングされます。ただし、フォルダは自動的には開かれません。デフォルトでは、レポート名内の任意の位置にあるテキスト文字列を検索します。ただし、クイック フィルタ ボックスで下矢印をクリックすると、検索文字列の評価方法を変更するさまざまなオプションを選択できます。
- **レポートのリスト（2）**：このリストはフォルダに編成されています。システムレポートは事前定義レポート（Report Manager の事前定義システム レポートについて （17 ページ）で説明）で、My Reports フォルダにはユーザが作成するカスタムレポートが含まれます。レポートをダブルクリックして開くか、またはレポートを選択して [ファイル（File）] > [開く（Open）] を選択します。詳細については、レポートの起動と生成 （25 ページ）を参照してください。
- **右クリックのショートカットメニュー（表示されません）**：レポートを右クリックすると、レポートを開く、スケジュールを作成する、新規レポートとしてレポートを保存するなど、実行可能な追加のコマンドのリストが表示されます。

- **編集ボタン（3）**：[編集（Edit）]ボタンをクリックして、選択したカスタムレポートの名前を変更します。カスタム レポートのみを編集できます。詳細については、レポートの名前変更 （40 ページ）を参照してください。
- **削除ボタン（4）**：[削除（Delete）]ボタンをクリックして、選択したカスタムレポートを削除します。カスタム レポートのみを削除できます。詳細については、レポートの削除（41 ページ）を参照してください。
- **Push Pin ボタン（5）**：[プッシュピン（Push Pin）]アイコンをクリックして、レポートリストペインを開くか閉じるかを制御します。ピンが垂直である場合、レポートリストは開いたままです。ただし、レポートペイン（右側のペイン）を最大化する場合は除きます。ピンが水平である場合、レポート リストは左マージンに縮小され、リストを開くには左マージンでレポート リストの見出しをクリックする必要があります。

関連項目

- Report Manager の概要 （8 ページ）
- レポート管理について （1 ページ）
- Report Manager でのレポートの使用 （25 ページ）
- レポート スケジュールの表示 （42 ページ）
- レポートのスケジュール設定 （42 ページ）
- レポート ウィンドウの配置 （38 ページ）

レポート設定ペインについて

レポートが開いている場合、[Reports]タブの右側の上部にレポート設定が表示されます。これらの設定は、レポートの生成に使用する基準を定義します。次の図に、レポート設定ペインの例を示します。

図 *2 : Report Manager* のレポート設定

レポート リストには、次のコントロールが含まれています（図のコールアウトで示されています）。

- [レポート（Report）]タブ（3）：正確には設定の一部ではありませんが、各レポートは独自のタブに表示されます。これらの設定はタブの上部にあります。タブ自体を右クリックすると、レポート ウィンドウを配置できるようにするコマンドのメニューが表示されます。詳細については、レポート ウィンドウの配置 （38 ページ）を参照してください。
- 見出しとツールバー（2）：設定ペインの上部には、見出し（たとえば、「Top Sources - Settings」）、および設定を操作するためのボタンの行が表示されています。見出しをクリックするか、またはツールバーの一番右側の上矢印ボタンをクリックすることにより、ペインを開閉できます。その他のボタンには、次の機能があります。
  - [Create Schedule] ボタン：これらの設定に基づいて自動的にレポートを生成する新規スケジュールを作成します。詳細については、レポート スケジュールの設定 （43 ページ）を参照してください。

    [Edit] ボタン：レポート設定を編集します。詳細については、レポート設定の編集 （28 ページ）を参照してください。
  - [Save As] ボタン：レポートを新規レポートとして保存します。事前定義システム レポートの設定を編集し、変更内容を保存する場合は、[Save As] を使用してカスタム レポートを作成する必要があります。詳細については、レポートの保存 （39 ページ）およびカスタム レポートの作成 （27 ページ）を参照してください。
  - [Save] ボタン：設定に対する変更内容を保存します。カスタム レポートの場合にのみ、変更内容を保存できます。詳細については、レポートの保存 （39 ページ）を参照してください。
  - [Reset] ボタン：前回保存された値に設定をリセットします。
  - [Expand/Collapse] ボタン（二重の上矢印と下矢印）：レポート設定ペインの開閉を切り替えます。
- 設定表示（1）：見出しとツールバーの下には、レポート設定の概要が示されます。情報には、レポートのタイプ、レポートに含まれるデバイス、時間範囲、説明、レポートに定義されているスケジュール、およびレポートに固有のその他のプロパティが含まれます。

説明を変更するには、[Description] 編集ボックスに直接変更内容を入力します。

関連項目

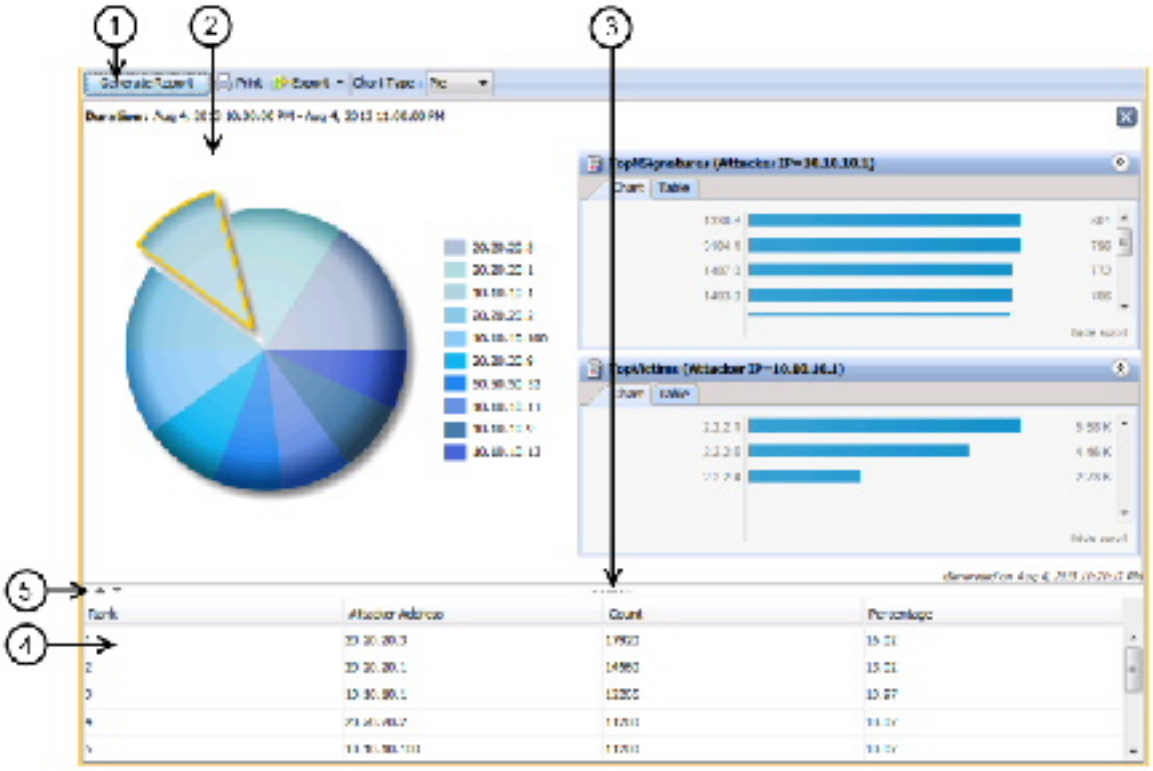
- レポートの起動と生成 （25 ページ）
- 生成済みレポート ペインおよびツールバーについて （15 ページ）
- Report Manager の概要 （8 ページ）
- レポート管理について （1 ページ）
- Report Manager でのレポートの使用 （25 ページ）
- レポート スケジュールの表示 （42 ページ）
- レポートのスケジュール設定 （42 ページ）

生成済みレポート ペインおよびツールバーについて

レポートが開いている場合、[Reports] タブの右側の下部に生成済みレポートとレポート ツールバーが表示されます。このペインには、[Generate Report] ボタンをクリックした結果が表示されます。

次の図に、生成済みレポート ペインと関連ツールバーの例を示します。

図 *3 : Report Manager* の生成済みレポート ペインとツールバー



レポート リストには、次のコントロールが含まれています（図のコールアウトで示されています）。

- **レポートツールバー（1）**：生成済みレポートペインの上部に、レポートを生成および操作するためのコントロールの行があります。これらのコントロールには次の機能があります。
  - [Generate Report] ボタン：レポート設定（上部のペイン）で定義された基準に基づいてレポートを生成します。詳細については、レポートの起動と生成 （25 ページ）を参照してください。
  - [Print] ボタン：生成されたレポートを印刷します。詳細については、レポートの印刷（34 ページ）を参照してください。

- [Export] ボタン：レポートをエクスポートします。ボタンの下矢印をクリックして、作成するファイルのタイプを選択します。タイプは、[PDFとして（As PDF）]（Adobe Acrobat の場合）または [CSVとして（As CSV）]（カンマで区切られた値の場合）です。詳細については、レポートのエクスポート （35 ページ）を参照してください。
- [Chart Type]：レポートの上部に表示されるグラフのタイプを決定します。一般には、円グラフ、棒グラフ、および XY（線形）グラフを使用できます。場合によっては、一部のグラフ タイプを選択できないことがあります。詳細については、レポートの起動と生成 （25 ページ）を参照してください。

- **グラフィカルビュー（2、3、5）**：生成されたレポートの上部には、レポートデータが色分けされたグラフで表示され、また配色を示す凡例が含まれます。また、レポートが生成された日付と時刻も含まれています。

（注） 上位の宛先、上位のサービス、上位の送信元のファイアウォールレポートと上位の攻撃者、上位のシグネチャ、上位の被害者 IPS レポートでは、円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのデータポイントの詳細を表示できます。たとえば、上位のシグネチャレポートの円グラフのスライスをクリックすると、選択したシグネチャの上位の攻撃者と上位の被害者のレポートの詳細が表示されます。詳細については、レポートデータへのドリルダウン （33 ページ）を参照してください。

グラフィカル ビューの下部には、次のコントロールがあります。

- 上矢印と下矢印（5）：グラフィックの左側にあるこれらのアイコンボタンを使用すると、レポートのグラフィカル部分を開くこと、および閉じることができます。
- ウィンドウサイズコントロール（3）：ウィンドウの中央のグラフィックの下にある水平方向のダッシュの上にマウスポインタを移動すると、ポインタをクリックして移動し、レポートのグラフィカル部分のサイズを変更できます。領域のサイズを拡大または縮小すると、グラフィックは自動的にサイズ変更されます。実際、テーブルの上部の任意の部分の上にマウス ポインタを移動すると、このコントロールにアクセスできます。
- **表形式のビュー（4）**：レポートの下部には、そのレポートに対して収集されたデータを表示するテーブルがあります。このデータはグラフィックの生成に使用されます。テーブルのカラムは、レポートのタイプによって異なります。

見出しをクリックして、テーブルをカラムでソートできます。3 つのソート順序があり、カラムの見出しをクリックすると、これらの順序が循環して切り替わります。矢印が、昇順（上矢印）、降順（下矢印）、およびソートなし（空）の、各ソート順序を示します。Ctrl を押した状態でクリックすると、別のカラムに別のソート順序を作成できます。これは、最初のソートカラムで 1 つ以上のエントリが繰り返される場合にのみ効果があります。番号は、そのカラムが 1 番め、2 番め、3 番めなどの、どのソート基準であるかを示しています。

関連項目

- レポート設定ペインについて （13 ページ）
- Report Manager の概要 （8 ページ）
- レポート管理について （1 ページ）
- Report Manager でのレポートの使用 （25 ページ）
- レポート スケジュールの表示 （42 ページ）
- レポートのスケジュール設定 （42 ページ）

Report Manager の事前定義システム レポートについて

Report Manager にはいくつかの事前定義システム レポートが組み込まれており、ネットワークの分析に使用できます。これらのレポートをカスタマイズして、特定のデバイスと期間の集合に焦点を当てたり、その他の設定可能パラメータに焦点を当てたりすることができます。

ここでは、次の内容について説明します。

- ファイアウォール トラフィック レポートについて （17 ページ）
- ファイアウォール サマリー ボットネット レポートについて （18 ページ）
- VPN 上位レポートについて （20 ページ）
- 全般 VPN レポートについて （21 ページ）
- IPS 上位レポートについて （22 ページ）
- 全般 IPS レポートについて （24 ページ）

ファイアウォール トラフィック レポートについて

Report Manager には、ファイアウォール ACL イベントの上位の宛先、サービス、およびソースの識別に使用できる事前定義システム レポートが組み込まれています。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。

[システムレポート（System Reports）] > [FW] フォルダで、以下のレポートを使用できます。

- [上位の宛先（Top Destinations）]：このレポートでは、Cisco Security Manager によって受信されたすべての built/deny ファイアウォールイベントのセッションの宛先がランク付けされます。このレポートには、宛先 IP アドレス、各アドレスに対するイベント数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の宛先を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その宛先に関連付けられた上位の送信元と上位のサービスに

関するレポート情報を表示できます（レポートデータへのドリルダウン （33 ページ）を参照）。

- [上位の送信元（Top Sources）]：このレポートでは、Cisco Security Manager によって受信されたすべての built/deny ファイアウォールイベントのセッションの送信元がランク付けされます。このレポートには、送信元 IP アドレス、各アドレスに対するイベント数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の送信元を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その送信元に関連付けられた上位の宛先と上位のサービスに関するレポート情報を表示できます（レポートデータへのドリルダウン （33 ページ）を参照）。
- [上位のサービス（Top Services）]：このレポートでは、Cisco Security Manager によって受信されたすべての built/deny ファイアウォールイベントの宛先サービスがランク付けされます。TCP サービスおよび UDP サービスにはポート番号が含まれています。このレポートには、サービス、各サービスに対するイベント数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定のサービスを表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのサービスに関連付けられた上位の宛先と上位の送信元に関するレポート情報を表示できます（レポートデータへのドリルダウン （33 ページ）を参照）。

レポートに含めるアドレスまたはサービスの数およびレポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （37 ページ）で説明されているようにシステム デフォルトで定義されます。

レポート設定の編集およびレポートのカスタムバージョンの作成を行うこともできます。次のトピックで説明されているように、レポートを絞り込んで、ソースアドレス、宛先アドレス、またはサービスの特定の集合に焦点を当てたり、アクションの許可または拒否のみに焦点を当てたり、ファイアウォールデバイスのサブセットに焦点を当てるようにレポートを制限したりすることができます。

- レポート設定の編集 （28 ページ）
- カスタム レポートの作成 （27 ページ）

ファイアウォール サマリー ボットネット レポートについて

Report Manager には、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 レポートが組み込まれています。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。

ボットネットの詳細については、Botnet Traffic Filter についてを参照してください。

[システムレポート（System Reports）] > [FW] > [サマリーボットネット（Summary Botnet）] フォルダで、次のレポートを使用できます。

- **上位感染ホスト（Top Infected Hosts）**：このレポートは、Security Manager によって受信されたすべてのボットネットイベントに基づいて、感染したホストからブラックリストま

たはグレーリストのサイトへのトラフィックについて上位感染ホストをランク付けします。このレポートには、感染したホストの IP アドレスとそのイベントが検出されたファイアウォールインターフェイス名（カッコ内）、各アドレスについてブロックリストまたはグレーリストのサイトに記録された接続数のカウント、ボットネットトラフィックフィルタリングによってブロックされた（ドロップされた）接続数のカウント、およびレポート内のすべてのカウントの合計に比較したカウントのパーセンテージが表示されます。

- **上位マルウェアポート（Top Malware Ports）**：このレポートは、Security Manager によって受信されたすべてのボットネットイベントに基づいて、感染したホストからブラックリストまたはグレーリストのサイトへのトラフィックについて上位宛先ポートをランク付けします。このレポートには、宛先マルウェアポート、各ポートについてブロックリストまたはグレーリストのサイトに記録された接続数のカウント、ボットネット トラフィック フィルタリングによってブロックされた（ドロップされた）接続数のカウント、およびレポート内のすべてのカウントの合計に比較したカウントのパーセンテージが表示されます。

- **上位マルウェアサイト（Top Malware Sites）**：このレポートは、Security Manager によって受信されたすべてのボットネットイベントに基づいて、すべてのインバウンドセッションとアウトバウンドセッションについて、上位ボットネットサイト（ブラックリストまたはグレーリストのサイト）をランク付けします。このレポートには、次の情報が表示されます。

  - IP アドレス（IP Address）：ボットネットイベントで悪意のあるホストとして示されている IP アドレス（ブロックリストまたはグレーリストのいずれか）。
  - マルウェア サイト（Malware Site）：動的なフィルタ データベースに登録されていて、トラフィックの宛先となったドメイン名または IP アドレス。
  - リストサイト（List Type）：サイトがブラックリストまたはグレイリストのどちらにあるか。
  - 記録された接続数（Connections Logged）：各サイトについて記録またはモニタされた接続数のカウント。
  - ブロックされた接続数（Connections Blocked）：各サイトについてボットネット トラフィック フィルタリングによってブロックされた（ドロップされた）接続数のカウント。
  - 脅威レベル（Threat Level）：サイトのボットネット脅威レベル（「非常に低い」から「非常に高い」まで、または「なし」）。
  - カテゴリ（Category）：ボットネットデータベースに定義されている、サイトが引き起こす脅威のカテゴリ（ボットネット、トロイの木馬、スパイウェアなど）。

レポート内のホスト数、ポート数、またはサイト数、およびレポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （37 ページ）で説明されているように、システムデフォルトで定義されています。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタム バージョンの作成を行うこともできます。

- レポート設定の編集　（28 ページ）
- カスタム レポートの作成　（27 ページ）

VPN 上位レポートについて

Report Manager には、帯域幅使用状況、ネットワークへの接続期間、およびデータ スループットに基づいて、上位のリモート アクセス VPN ユーザを識別するために使用される事前定義システム レポートが組み込まれています。ユーザによる接続のタイプに基づいて、別々のレポートが提供されます。

これらのレポートは、**Cisco Secure Client の AnyConnect VPN モジュール**、[Cisco VPN Client（IPsec）リモートアクセスVPN（Cisco VPN Client (IPsec) Remote Access VPN）]、および [クライアントレスSSL VPN（Clientless SSL VPN）] の [システムレポート（System Reports）] > [VPN（VPN）] フォルダで使用できます。

次のレポートは各フォルダで使用できます。各レポートはフォルダ名で示される接続タイプに固有です。接続タイプはレポート名のカッコ内にも含まれています。

- **帯域幅が上位のユーザー（Top Bandwidth Users）**：このレポートは、帯域幅消費量が最大である VPN ユーザーをランク付けします。このレポートには、ユーザ名、合計送受信バイト数での帯域幅、および報告された各ユーザによる使用帯域幅のパーセンテージが表示されます。
- **接続時間が上位のユーザー（Top Duration Users）**：このレポートは、ネットワークへの接続時間が最も長かったVPNユーザーをランク付けします。このレポートには、ユーザー名、*days hours:minutes:seconds* という形式での接続時間、および報告された各ユーザーの期間のパーセンテージが表示されます。チャートには、期間は秒単位で表示されます。
- **スループットが上位のユーザー（Top Throughput Users）**：このレポートは、最高のスループットレートでデータを送受信した VPN ユーザーをランク付けします。このレポートには、ユーザ名、各ユーザのスループット（kbps 単位）、および報告された各ユーザのスループットのパーセンテージが表示されます。スループットは、8.0 *（バイト単位でのユーザの帯域幅）/（秒単位でのユーザの接続時間 * 1000.0）として計算されます。

レポートに含めるユーザ数およびレポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定　（37 ページ）で説明されているようにシステム デフォルトで定義されます。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタム バージョンの作成（特定のユーザに焦点を当てることも含む）を行うこともできます。

- レポート設定の編集　（28 ページ）
- カスタム レポートの作成　（27 ページ）

全般 VPN レポートについて

Report Manager には、ネットワークにおける一般的なリモート アクセス VPN 使用状況の分析に使用できる事前定義システム レポートが組み込まれています。これらのレポートは、VPN で使用される接続タイプに固有ではありません。

[システムレポート（System Reports）] > [VPN] フォルダで、次のレポートを使用できます。

- **接続プロファイルレポート**：このレポートは、各リモートアクセス接続プロファイルのユーザ数、セッション、帯域幅使用率とスループット使用状況の概要を提供します。

デフォルトのレポートには、直前の 1 時間のすべてのデバイスに関するこの情報が含まれます。レポートは、さまざまな方法でカスタマイズできます（レポート設定の編集 （28 ページ）を参照）。

- **ユーザレポート**：このレポートは、各リモートアクセス VPN ユーザの帯域幅使用率、接続時間、およびスループット使用状況の概要を提供します。このレポートには、ユーザ名、合計送受信バイト数での帯域幅、*days hours:minutes:seconds* 形式での接続時間、および各ユーザのスループット（kbps）が表示されます。スループットは、8.0 *（バイト単位でのユーザの帯域幅）/（秒単位でのユーザの接続時間 * 1000.0）として計算されます。

Security Manager 4.7 以降、ユーザレポートは**ユーザレベルの詳細**と**セッション レベルの詳細**の両方を提供します。

- • **ユーザレベルの詳細**：**ユーザレベルの詳細**は、特定のユーザーについて、ユーザのすべてのセッションの合計値（ユーザー名、セッション合計数、帯域幅、期間、およびスループット）を表します: 。

（注） Cisco Security Manager 4.13 以降、パブリック IP および割り当てられた IP の詳細は、一般的な VPN レポートのユーザレベルの詳細の一部としても表示されます。

- • **セッションレベルの詳細**：ツリーを展開すると、特定のユーザが VPN 接続を持つ各セッションについて**セッションレベルの詳細**が表示されます。セッションレベルの詳細には、セッション ID、ログイン時間、ログアウト時間、帯域幅、スループット、およびセッションの期間が含まれます。（ここで、ログアウト時間は、式**ログアウト時間 = ログイン時間 + 期間**を使用して計算されます。）

デフォルト レポートには、すべての接続テクノロジーとすべてのユーザの情報が含まれています。単一のテクノロジータイプまたは 1 つ以上の特定ユーザに焦点を当てるようにレポートをカスタマイズできます（レポート設定の編集 （28 ページ）を参照）。

ユーザレポートの [条件（Criteria）] セクションには、テクノロジー（すべて、クライアントレス、フルクライアント、および IPSec RA）、ユーザー名、およびユーザーセッション時間（<=、>= （時間））のフィルターがあります。

- **VPN デバイス使用率レポート**：このレポートは、リモートアクセス VPN 接続をホストする各デバイスの使用率の統計の概要を提供します。このレポートには、デバイス（Security Manager の表示名を使用）、レポート時間範囲内の任意の時点における VPN へのログインユーザの平均数、VPN のすべてのユーザの合計帯域幅（バイト）（送信および受信）、*days hours:minutes:seconds* 形式の合計接続時間、およびこのレポート期間内の任意の時点における平均スループット（kbps）が表示されます。

デフォルト レポートには、すべての接続テクノロジーの情報が含まれています。単一のテクノロジー タイプに焦点を当てるようにレポートをカスタマイズできます（レポート設定の編集（28 ページ）を参照）。

レポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （37 ページ）で説明されているようにシステムデフォルトで定義されます。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタムバージョンの作成を行うこともできます。

- レポートのデフォルト設定値の設定 （37 ページ）
- カスタム レポートの作成 （27 ページ）

IPS 上位レポートについて

（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。

Report Manager には、ネットワーク内の IPS アラートの攻撃者、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 レポートが組み込まれています。

[システムレポート（System Reports）] > [IPS] フォルダで、次のレポートを使用できます。

- [上位攻撃者（Top Attackers）]：このレポートは、記録された IPS アラート数が最も多い攻撃者（送信元）のアドレスをランク付けします。このレポートには、攻撃者 IP アドレス、各アドレスに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の攻撃者を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その攻撃者に関連した上位のシグニチャと上位の攻撃対象に関するレポート情報を表示できます（レポートデータへのドリルダウン （33 ページ）を参照）。

デフォルト レポートには、ブロックされたアクションとブロックされなかったアクションの両方について、すべての攻撃者、攻撃対象、およびシグニチャの情報が含まれています。攻撃者、攻撃対象、またはシグニチャのサブセットに焦点を当てるようにレポートをカスタマイズしたり、ブロックされたアクションのみ、またはブロックされなかったアクションのみに分析を制限したりすることができます（レポート設定の編集 （28 ページ）を参照）。

- [上位攻撃対象（Top Victims）]：このレポートは、記録された IPS アラート数が最も大きい攻撃対象（宛先）のアドレスをランク付けします。このレポートには、攻撃対象アドレ

ス、各アドレスに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の攻撃対象を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その攻撃対象に関連した上位のシグニチャと上位の攻撃者に関するレポート情報を表示できます（レポートデータへのドリルダウン （33 ページ）を参照）。

デフォルト レポートには、ブロックされたアクションとブロックされなかったアクションの両方について、すべての攻撃者、攻撃対象、およびシグニチャの情報が含まれています。攻撃者、攻撃対象、またはシグニチャのサブセットに焦点を当てるようにレポートをカスタマイズしたり、ブロックされたアクションのみ、またはブロックされなかったアクションのみに分析を制限したりすることができます（レポート設定の編集 （28 ページ）を参照）。

- [上位シグニチャ（Top Signatures）]：このレポートは、発行したアラートの数が最も大きいシグニチャをランク付けします。このレポートには、シグニチャ ID 番号、シグニチャの名前、各シグニチャに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定のシグニチャを表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのシグニチャに関連した上位の攻撃対象と上位の攻撃者に関するレポート情報を表示できます（レポートデータへのドリルダウン （33 ページ）を参照）。

デフォルト レポートには、ブロックされたアクションとブロックされなかったアクションの両方について、すべての攻撃者、攻撃対象、およびシグニチャの情報が含まれています。攻撃者、攻撃対象、またはシグニチャのサブセットに焦点を当てるようにレポートをカスタマイズしたり、ブロックされたアクションのみ、またはブロックされなかったアクションのみに分析を制限したりすることができます（レポート設定の編集 （28 ページ）を参照）。

- [上位ブロック/非ブロックシグニチャ（Top Blocked/Unblocked Signatures）]：このレポートは、ブロックした攻撃者の数が最も大きいシグニチャをランク付けします。このレポートには、シグニチャ ID 番号、シグニチャの名前、各シグニチャに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。

デフォルト レポートには、ブロックされたアクションのみが表示されます。ただし、ブロックされなかったアクションのみ、またはブロックされたアクションとブロックされなかったアクションの組み合わせを表示するように、レポートをカスタマイズできます（レポート設定の編集 （28 ページ）を参照）。

特定の攻撃者または攻撃対象のアドレス、またはシグニチャのサブセットに制限されたブロック リストまたは非ブロック リストを表示する場合は、上位ブロック/非ブロック シグニチャ（Top Blocked/Unblocked Signatures）レポートではなく上位シグニチャ（Top Signatures）レポートを使用します。ブロックされたシグニチャのみ、またはブロックされなかったシグニチャのみを表示するようにレポートをカスタマイズします。

- [IPSターゲット分析（IPS Target Analysis）：このレポートは、シグニチャおよび攻撃の頻度による上位ターゲットを提示します。このレポートには、アラートを生成したシグニチャ、アラートの数、および攻撃対象 IP アドレスが表示され、[Top Signatures] レポートと [Top Victims] レポートの集約ビューに基づいています。このレポートには、最大で 10

個のシグニチャと5個の攻撃者が含まれています。情報は散布図にプロットされます。これは、そのレポートに対して使用できる唯一のグラフィカル表現です。

レポートに含めるアドレスまたはシグニチャの数およびレポート期間の定義に使用されるパラメータは、レポート スケジュールの設定 （43 ページ）で説明されているようにシステム デフォルトで定義されます。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタム バージョンの作成を行うこともできます。

- レポート設定の編集 （28 ページ）
- カスタム レポートの作成 （27 ページ）

全般 IPS レポートについて

（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。

Report Manager には、ネットワークにおける一般的な IPS アクティビティの分析に使用できる事前定義システム レポートが組み込まれています。

[システムレポート（System Reports）] > [IPS] フォルダで、次のレポートを使用できます。

- [検査/グローバル相関（Inspection/Global Correlation）]：このレポートでは、グローバル相関によって生成されたアラートと従来の IPS 検査によって生成されたアラートの比較が示されます。このレポートには、IPS 検査方式（グローバル相関または検査のいずれか）あたりのアラートの数およびパーセンテージが表示されます。
- [IPSシミュレーションモード（IPS Simulation Mode）]：このレポートでは、インライン（IPS）モードと無差別（IDS または IPS シミュレーション）モードのアラートの比較が示されます。このレポートには、モードに基づくアラートの数とパーセンテージが表示されます（非シミュレーション カウント（インライン）またはシミュレーション モード カウント（無差別）のいずれか）。IPSセンサーは、無差別モードで発生する攻撃を直接ブロックすることはできません。

IPS イベントを処理する際、Cisco Security Manager の Report Manager コンポーネントはイベントを個別に報告します。 Cisco Security Manager のイベント ビューア コンポーネントにアラートが表示されます。イベント ビューア コンポーネントで、IPS Summarizer はイベントを単一のアラートにグループ化するため、IPS センサーが送信するアラートの数が減少します。

ヒント Cisco IPS Manager Express（IME）と Cisco Security Manager は、まったく同じ方法ではイベントを要約しません。

レポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （37 ページ）で説明されているようにシステムデフォルトで定義されます。次のトピックで説明さ

れているように、レポート設定の編集およびレポートのカスタムバージョンの作成を行うこともできます。

- レポート設定の編集　（28 ページ）
- カスタム レポートの作成　（27 ページ）

Report Manager でのレポートの使用

Report Manager アプリケーションを使用して、デバイス、およびリモート アクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。次のトピックで、レポート作成の基本を説明します。レポート スケジュールの使用については、レポートのスケジュール設定　（42 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。

- レポートの起動と生成　（25 ページ）
- カスタム レポートの作成　（27 ページ）
- レポート設定の編集　（28 ページ）
- レポートデータへのドリルダウン　（33 ページ）
- レポートの印刷　（34 ページ）
- レポートのエクスポート　（35 ページ）
- レポートのデフォルト設定値の設定　（37 ページ）
- レポート ウィンドウの配置　（38 ページ）
- レポートの保存　（39 ページ）
- レポートの名前変更　（40 ページ）
- レポート ウィンドウの終了　（40 ページ）
- レポートの削除　（41 ページ）
- カスタム レポートの管理　（41 ページ）

レポートの起動と生成

レポートはスタティックではありません。レポートを開くと、そのレポートの生成に使用するデータを定義する設定は含まれていますが、レポートにデータは含まれていません。したがって、レポートを表示するには、レポートを開いてから生成する必要があります。この手順では、このプロセスを説明します。

関連項目

- Report Manager の概要　（8 ページ）

- カスタム レポートの作成 （27 ページ）
- レポート ウィンドウの配置 （38 ページ）
- Report Manager のトラブルシューティング （46 ページ）

ステップ 1 Report Manager で、次のいずれかを実行してレポートを開きます。

- レポート リスト（左側のペイン）内のレポートの名前をダブルクリックします。
- レポートリスト内のレポートを選択し、[ファイル（File）] > [開く（Open）] を選択します。
- レポートリスト内のレポートを右クリックし、[レポートを開く（Open Report）] を選択します。

レポート設定ペインが開いていてレポート コンテンツ領域が空の状態で、レポートが開きます。

ヒント 同時に開いていることができるレポートは、最大で5つです。設定ツールバーの任意の領域（別の機能を実行するボタンではない領域）をクリックすることにより、レポート設定ペインを縮小して、生成されたレポートを表示するための領域を増やすこともできます。

ステップ 2 （任意）レポート設定に目的の値（たとえば、レポートに対する目的の時間枠）が含まれていることを確認します。システム レポートの設定値は、システム デフォルト（ レポートのデフォルト設定値の設定 （37 ページ）の説明に従って設定可能）に基づいています。カスタム レポートの設定値は、そのレポートに対して前回保存された設定値です。

設定を変更する必要がある場合は、設定ツールバーで [編集（Edit）] ボタンをクリックし、[設定の編集（Edit Settings）] ダイアログボックスで変更します。詳細については、 レポート設定の編集 （28 ページ） を参照してください。

ヒント 変更内容を永続的にする場合は、必ずその変更内容を保存してください。システム レポートの設定値を変更して保持する場合は、[Save As] を使用して新規カスタム レポートを作成する必要があります。システム レポートの設定値をデフォルト設定値から変更することはできません。

ステップ 3 設定ペインの下にある [レポートの生成（Generate Report）] ボタンをクリックして、レポートデータベースからレポートデータを取得し、取得した情報を表示します。この情報は次の2つの形式で表示されます。

- グラフィカル：レポートの上部に、データのグラフィカル表現が表示されます。レポートデータの上の [チャート（Chart）] メニューから、さまざまなタイプのグラフを選択できます（円グラフ、XY（線形グラフの場合）、または棒グラフ）。レポートに10項目よりも多い項目が含まれている場合（たとえば、25個の値を表示するように上位レポートを設定した場合）、10番目以降の値はすべて、チャートでは「others」として要約表示されます。

（注） 上位の宛先、上位のサービス、上位の送信元のファイアウォールレポートと上位の攻撃者、上位のシグネチャ、上位の被害者 IPS レポートでは、円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのデータポイントの詳細を表示できます。たとえば、上位のシグネチャレポートの円グラフのスライスをクリックすると、選択したシグネチャの上位の攻撃者と上位の被害者のレポートの詳細が表示されます。詳細については、 レポートデータへのドリルダウン （33 ページ） を参照してください。

IPS ターゲット分析（IPS Target Analysis）レポートなどの一部のレポートは、散布図を使用します。これらのレポートの場合、別のグラフィック タイプを選択するオプションはありません。

- 表形式：グラフィックの下のテーブルには、グラフィックの生成に使用されたデータがリストされます。テーブルのカラムは、レポートのタイプに基づいて異なります。以下に、いくつかの一般的なカラムを示します。各レポートの内容の詳細については、Report Manager の事前定義システム レポートについて （17 ページ）を参照してください。
  - [Rank]：情報の順序は大きさ順。たとえば、ファイアウォール上位宛先レポートの場合、ランク 1 は、その宛先が評価対象イベントで最も使用されていることを示しています。
  - （レポート対象の特性の名前）：レポートでターゲットとする特性に基づく名前を持つカラムが必ず存在します。たとえば、[Source/Destination]（IP アドレス）、[Service]（プロトコルおよびポート）、または [User]（ユーザ名）などです。
  - [Count]：その項目がイベントまたは関連統計情報に現れる回数。
  - [Percentage]：報告された特性の、レポート内のその特性の総計に対する比率。この比率は、レポートに含まれる数値のみが含まれます。したがって、たとえば、上位 10 件のレポートと上位 25 件のレポートで、同じ項目に対して異なるパーセンテージが得られる可能性があります。

ステップ 4 （任意）必要に応じて、レポートの印刷、または PDF ファイルまたは Comma-Separated Values（CSV; カンマ区切り値）ファイルへのエクスポートを行うことができます。

- レポートを印刷するには、[印刷（Print）] ボタンをクリックしてプリンタを選択します。詳細については、レポートの印刷 （34 ページ）を参照してください。
- レポートをエクスポートするには、[エクスポート（Export）] ボタンをクリックしてファイルタイプ（PDF または CSV）を選択します。詳細については、レポートのエクスポート （35 ページ）を参照してください。

ヒント レポートを閉じるときに、レポート データは保持されません。表示されている情報を保持する場合は、レポートを印刷またはエクスポートする必要があります。

カスタム レポートの作成

通常の分析または表現を必要とする特定の特性をターゲットとするカスタム レポートを作成できます。たとえば、さまざまなファイアウォールデバイスのグループに対して別々の上位宛先（Top Destination）ファイアウォール レポートを作成し、別々の物理サイトのアクティビティを別々に分析できるようにすることができます。カスタム レポートを使用して、通常は上位レポートに含まれないソース、宛先、またはサービスを分析することもできます。

ヒント 新規に作成されたカスタム レポートでデータを使用できるまでに最大 1 時間かかる可能性があります。レポートの作成後にレコードが見つからないというメッセージが表示される場合は、1 時間待ってから、レポートの期間が直前の 1 時間（Last 1 Hour）であることを確認してください。

関連項目

- レポートの起動と生成 （25 ページ）
- Report Manager の概要 （8 ページ）

ステップ 1 レポート リストで、カスタム レポートが基づくレポートを選択します。レポートをダブルクリックするか、レポートを選択して [ファイル（File）] > [開く（Open）] を選択するか、右クリックして [レポートを開く（Open Report）] を選択して、レポートを開きます。

ステップ 2 設定ツールバーで [編集（Edit）]（鉛筆）ボタンをクリックし、[設定の編集（Edit Settings）] ダイアログ ボックスを開きます。

（注） レポート リストの上の [Edit] ボタンはクリックしないでください。その [Edit] ボタンでは、レポートの名前のみを変更できます。

[Edit Settings] ダイアログボックスは、2 つのペインに分かれています。左側のペインには使用可能な設定ページがリストされ、右側のペインには左側のペインで選択されているページの設定が表示されます。

ステップ 3 目的のレポート パラメータを定義するように設定値を設定します。詳細については、レポート設定の編集（28 ページ）を参照してください。

ステップ 4 設定ツールバーで [名前を付けて保存（Save As）] ボタンをクリックするか、[ファイル（File）] > [名前を付けて保存（Save As）] を選択します。

ステップ 5 レポートの名前と説明（任意）を入力し、[OK] をクリックします。

レポート名は最大 64 文字で、英数字、スペース、ハイフン（-）、および下線文字（_）を含みます。説明には、最大 1024 文字を使用できます。

レポート設定の編集

レポートの生成に使用する基準を定義する設定を変更できます。カスタム レポートの場合、変更内容を保存できます。

事前定義システム レポートの場合、変更内容を直接保存することはできません。代わりに、[Save As] を使用して、更新された設定を使用する新規カスタム レポートを作成できます。また、レポートのデフォルト設定値の設定 （37 ページ）で説明されているように、レポート設定を編集するのではなく、すべての事前定義システム レポートで使用されるデフォルト設定を変更することもできます。

関連項目

- レポートの起動と生成　（25 ページ）
- Report Manager の概要　（8 ページ）
- カスタム レポートの作成　（27 ページ）
- Report Manager データ集約について　（5 ページ）
- レポート ウィンドウの配置　（38 ページ）

ステップ 1 Report Manager で、設定を変更するレポートを開きます。レポートをダブルクリックして開くか、レポートをダブルクリックして[ファイル（File）]>[開く（Open）]を選択するか、またはレポートを右クリックして [レポートを開く（Open Report）] を選択します。

レポートの上部に設定ペインが開いた状態で、レポートが開きます。設定ペインには、レポートのタイプ、レポートに含まれるデバイス、時間範囲、説明、レポートに対して定義されているスケジュール、およびそのレポートに固有のその他のプロパティが表示されます。

ステップ 2 （任意）レポート設定ペインの [Description] 編集ボックスに入力することにより、説明を変更します。

ステップ 3 設定ツールバーで [編集（Edit）]（鉛筆）ボタンをクリックし、[設定の編集（Edit Settings）] ダイアログボックスを開きます。

（注）　レポート リストの上の [Edit] ボタンはクリックしないでください。その [Edit] ボタンでは、レポートの名前のみを変更できます。

[Edit Settings] ダイアログボックスは、2 つのペインに分かれています。左側のペインには使用可能な設定ページがリストされ、右側のペインには左側のペインで選択されているページの設定が表示されます。

ステップ 4 次のように、目的のページで設定を編集します。

- [デバイス（Devices）]：レポートに含めるモニタ対象デバイスを変更します。デフォルトは[すべてのデバイス（All Devices）] です。

モニタ対象デバイスのサブセットをレポートに反映させる場合は、[デバイスのフィルタ（Filter Devices）] を選択し、リストから目的のデバイスを選択するか、コンテキストを作成します。デバイスがイタリック体である場合、そのデバイスが現在は Event Viewer でモニタ対象として選択されていないことを意味します。これらのデバイスを選択すると、そのデバイスが選択された期間にモニタリングされた場合はレポートにそのデバイスのデータが組み込まれます。フォルダを選択して、フォルダ内のすべてのデバイスを選択できます。

デバイス リストは、適切なタイプのデバイスのみを表示するように事前にフィルタリングされます。たとえば、ファイアウォール レポートの設定を編集している場合、IPS デバイスは選択可能なデバイスのリストに表示されません。

（注）　Cisco Security Manager 4.10 以降では、ASA 9.5(2) 以降で作成されたすべてのコンテキストが [デバイスのフィルタ（Filter Devices）] の下にリストされます。

- [時間（Time）]：レポートに含めるイベントとデータの選択に使用する期間を変更します。時間はSecurity Managerサーバの時間に基づいています。次のいずれかのオプションを選択して、期間を定義します。
  - [Last 1 Hour]：00分から始まる直前の1時間全体。たとえば、現在の時刻が午前11:45である場合、直前の1時間（Last 1 Hour）のレポートには10:00から11:00までのデータが表示されます。
  - [Last 1 Day]：直前の1日全体（0時から0時まで）。たとえば、現在の日付が火曜日である場合、直前の1日（Last 1 Day）のレポートには月曜日のデータが表示されます。
  - [Last 1 Week]：前の月曜日から日曜日まで。
  - [Last 1 Month]：前月。たとえば、現在の日付が9月29日である場合、直前の1か月（Last 1 Month）のレポートには8月のデータが表示されます。
  - [Custom]：[Start Date]カレンダーと[End Date]カレンダーを使用して、そのレポートに対する目的の開始時刻と終了時刻を選択します。カレンダーウィジェットで、下矢印をクリックして目的の日時を選択し、[OK]をクリックします。レポート可能なデータは90日間保持されます。したがって、90日よりも前にさかのぼる日付は選択できません。さらに、5日間を超えてさかのぼる開始日を選択すると、時刻を指定できません。開始日に現在の日付を選択する場合、開始日と終了日両方の分の値も指定できますが、レポートデータは15分ごと（各正時からの時間で00分、15分、30分、および45分）に集約されるため、分のエントリはこれらの数値で最も近い値に丸められます。許可される時間選択は、Report Managerデータ集約について （5ページ）で説明されているように、データの集約方法に基づいています。
- [基準（Criteria）]：レポートの定義に使用するその他の基準を変更します。[Criteria]設定ページで使用可能な属性は可変です。場合により、選択可能な基準はありません。以下に、可能な基準のリストを示します。
  - [上位（Top）]（すべての「上位」レポート）：レポートに含める対象項目数。たとえば、[Top 10]ファイアウォール宛先は、設定されている時間範囲内のファイアウォールイベントについて最も頻度が高い10件の宛先を戻します。10、20、25、または50を選択します。
  - [Service]（ボットネット以外のファイアウォールレポート）：レポートに含めるサービス。サービスを指定するには、フィールドの横の[Edit]ボタンをクリックし、目的のサービスポリシーオブジェクトを選択します。複数のオブジェクトを選択できます。
  - [Source IP]、[Destination IP]（ボットネット以外のファイアウォールレポート）：ソースと宛先のIPアドレスフィールドは分かれていますが、機能的には同じです。これらのフィールドは、レポートに含めるソースまたは宛先のIPアドレスを定義します。個々のアドレス（10.100.10.10など）を入力することも、アドレスの範囲（10.100.10.10-10.100.10.20など）を入力することもできます。IPv4アドレスとIPv6アドレスの両方が受け入れられます。カンマで複数のアドレスを区切ります。

フィールドの横の[Edit]ボタンをクリックしてダイアログボックスを開き、そこでアドレスとアドレス範囲の複雑なリストをより簡単に作成できます。ただし、ネットワーク/ホストオブジェクトを使用してアドレスを定義することはできません。

（注） [Service]、[Source IP]、および [Destination IP] の各基準の値をすべて単一レポートで指定することは行わないでください。レポートが基づく基準（たとえば、上位サービス（Top Services）レポートの場合は [Service]）と、その他の 1 つの基準を指定できます。3 つの値すべてを指定すると、そのレポートには常にデータが含まれません。

- [Permit/Deny]（ボットネット以外のファイアウォール レポート）：イベントで反映されるアクション。一致するトラフィックの許可（[Permit]）、一致するトラフィックの拒否（[Deny]）、またはその両方（[All]）のいずれか。デフォルトは [All] です。
- [Signature ID]（IPS 上位攻撃者、上位シグニチャ、上位攻撃対象）：レポートに含めるシグニチャ。シグニチャを指定するには、フィールドの横の [Edit] ボタンをクリックし、目的のシグニチャを選択します。フォルダを選択して、フォルダ内のすべてのシグニチャを選択できます。

（注） 事前定義システム レポートでは、[Signature ID]、[Attacker IP]、および [Victim IP] の各基準すべての値を指定することはできません。レポートのキー属性の値（たとえば、上位攻撃対象レポートの場合は [Victim IP]）と、その他の値を 1 つ指定できます。3 つの基準すべての値を設定する場合は、カスタム レポートを作成する必要があります。

- [Attacker IP]、[Victim IP]（IPS 上位攻撃者、上位シグニチャ、上位攻撃対象）：攻撃者と攻撃対象の IP アドレス フィールドは分かれていますが、機能的には同じです。これらのフィールドは、レポートに含める攻撃者（ソース）または攻撃対象（宛先）の IP アドレスを定義します。個々のアドレス（10.100.10.10 など）を入力することも、アドレスの範囲（10.100.10.10-10.100.10.20 など）を入力することもできます。IPv4 アドレスと IPv6 アドレスの両方が受け入れられます。カンマで複数のアドレスを区切ります。

フィールドの横の [Edit] ボタンをクリックしてダイアログボックスを開き、そこでアドレスとアドレス範囲の複雑なリストをより簡単に作成できます。ただし、ネットワーク/ホスト オブジェクトを使用してアドレスを定義することはできません。

- [Blocked]（IPS 上位攻撃者、上位ブロック/非ブロック シグニチャ、上位シグニチャ、上位攻撃対象）：イベントが、ドロップされたトラフィック（[Blocked]）、ドロップされなかったトラフィック（[Unblocked]）、または両方（[All]）の、どちらに起因するか。
- [ユーザー名（Username）]（接続プロファイル レポートおよびユーザー レポート）：レポートに含めるユーザの名前。デフォルトは空のリストで、すべてのユーザが含まれます。レポートで特定のユーザに焦点を当てる場合は、テーブルの下の [Add]（+）ボタン、[Edit]（鉛筆）ボタン、または [Delete]（ゴミ箱）ボタンを使用して、目的のユーザ リストを作成します。Security Manager のバージョン 4.7 以降、ユーザー名フィルタは大文字/小文字の区別、ワイルドカード文字、および「NOT」操作のサポートをサポートします。このトピックの最後の段落にある「**大文字/小文字の区別の有効化**」と「**ワイルドカードのサポートの無効化**」を参照してください。
- [テクノロジー（Technology）]（接続プロファイル レポート、ユーザ レポート、および VPN デバイス使用状況レポート）：レポートに含めるリモート アクセス テクノロジーのタイプ：すべて、クライアントレス（SSL VPN）、フルクライアント（SSL VPN）、IPsec RA（IPsec リモートアクセス VPN）。
- [接続プロファイル（Connection Profile）]（接続プロファイル レポート）：クライアントレス（SSL VPN）、フル クライアント（SSL VPN）、または IPsec RA（IPsec リモートアクセス VPN）トポロジの接続プロファイルを追加または編集することにより、Report Manager で接続プロファイル レポートをカスタマイズできます。詳細については、[Connection Profiles] ページおよび接続プロファイルの設

定（ASA、PIX 7.0+）を参照してください。Security Manager のバージョン 4.7 以降、接続プロファイルフィルタは大文字/小文字の区別、ワイルドカード文字、および「NOT」操作のサポートをサポートします。このトピックの最後の段落にある「**大文字/小文字の区別の有効化**」と「**ワイルドカードのサポートの無効化**」を参照してください。

- グループポリシー（接続プロファイルレポート）：フィルタで 1 つまたは複数のグループポリシーを指定して、指定したグループポリシーでログインしたユーザのレポートを生成することにより、Report Manager で接続プロファイルレポートをカスタマイズできます。詳細については、リモート アクセス VPN のグループ ポリシーの設定を参照してください。Security Manager のバージョン 4.7 以降、グループポリシーフィルタは大文字/小文字の区別、ワイルドカード文字、および「NOT」操作のサポートをサポートします。このトピックの最後の段落にある「**大文字/小文字の区別の有効化**」と「**ワイルドカードのサポートの無効化**」を参照してください。
- ユーザーセッションの継続時間（接続プロファイルレポートおよびユーザレポート）：タイトルが示すように、ユーザーセッションの継続時間を <= または >= 時間として指定できます。

ステップ 5 [設定の編集（Edit Settings）] ダイアログボックスで [OK] をクリックして、変更内容を実装します。

これで、[Generate Report] ボタンをクリックして設定で定義されたデータを取得し、レポートに表示できます。[Save] または [Save As] を使用して、変更内容を設定に永続的に保存することもできます。

大文字/小文字の区別を有効にする

Security Manager のバージョン 4.7 以降、ユーザー名フィルタ、接続プロファイルフィルタ、およびグループポリシーフィルタで、大文字/小文字を区別できます。大文字/小文字の区別はデフォルトで無効になっています。使用する場合は、次の手順に従って有効にする必要があります。これら 3 つのフィルタのいずれかに対して有効にすると、それら 3 つすべてに対して有効になることに注意してください。

1. reporting.properties ファイルを見つける。デフォルトの場所は NMSROOT/MDC/reports/config です。（NMSROOT のデフォルト値は C:\Program Files\CSCOpx です）
2. パラメータ reports.reportgeneration.vpnUserReport.casesensitive.enable=true を設定する
3. CsmReportServer である Report Manager サービスを再起動する。

ワイルドカードサポートの無効化

Security Manager のバージョン 4.7 以降、ユーザー名フィルタ、接続プロファイルフィルタ、およびグループポリシーフィルタで、ワイルドカードをサポートしています。ワイルドカードサポートは、デフォルトで有効になっています。使用したくない場合は、次の手順に従って無効にする必要があります。これら 3 つのフィルタのいずれかを無効にすると、3 つすべてが無効になることに注意してください。

1. reporting.properties ファイルを見つける。デフォルトの場所は NMSROOT/MDC/reports/config です。（NMSROOT のデフォルト値は C:\Program Files\CSCOpx です）
2. パラメータ reports.reportgeneration.vpnUserReport.wildcard.enable=false を設定します。
3. CsmReportServer である Report Manager サービスを再起動する。

レポートデータへのドリルダウン

上位の宛先、上位のサービス、上位の送信元ファイアウォールレポート、および上位の攻撃者、上位のシグネチャ、上位の攻撃対象IPSレポートでは、レポートデータをドリルダウンできます。

ドリルダウン対応レポートの1つをドリルダウンするには、そのレポートの円グラフ、XYグラフ、または棒グラフのデータポイントをクリックします。たとえば、上位のシグネチャレポートの円グラフのスライスをクリックすると、選択したシグネチャの上位の攻撃者と上位の被害者のレポートの詳細が表示されます。

（注） レポートに使用するフィルタ条件は、関連するドリルダウンレポートで表示されるデータに影響します。レポートデータにフィルタを適用すると、レポートデータをドリルダウンするときに、1つのドリルダウンレポートのみが表示されます。

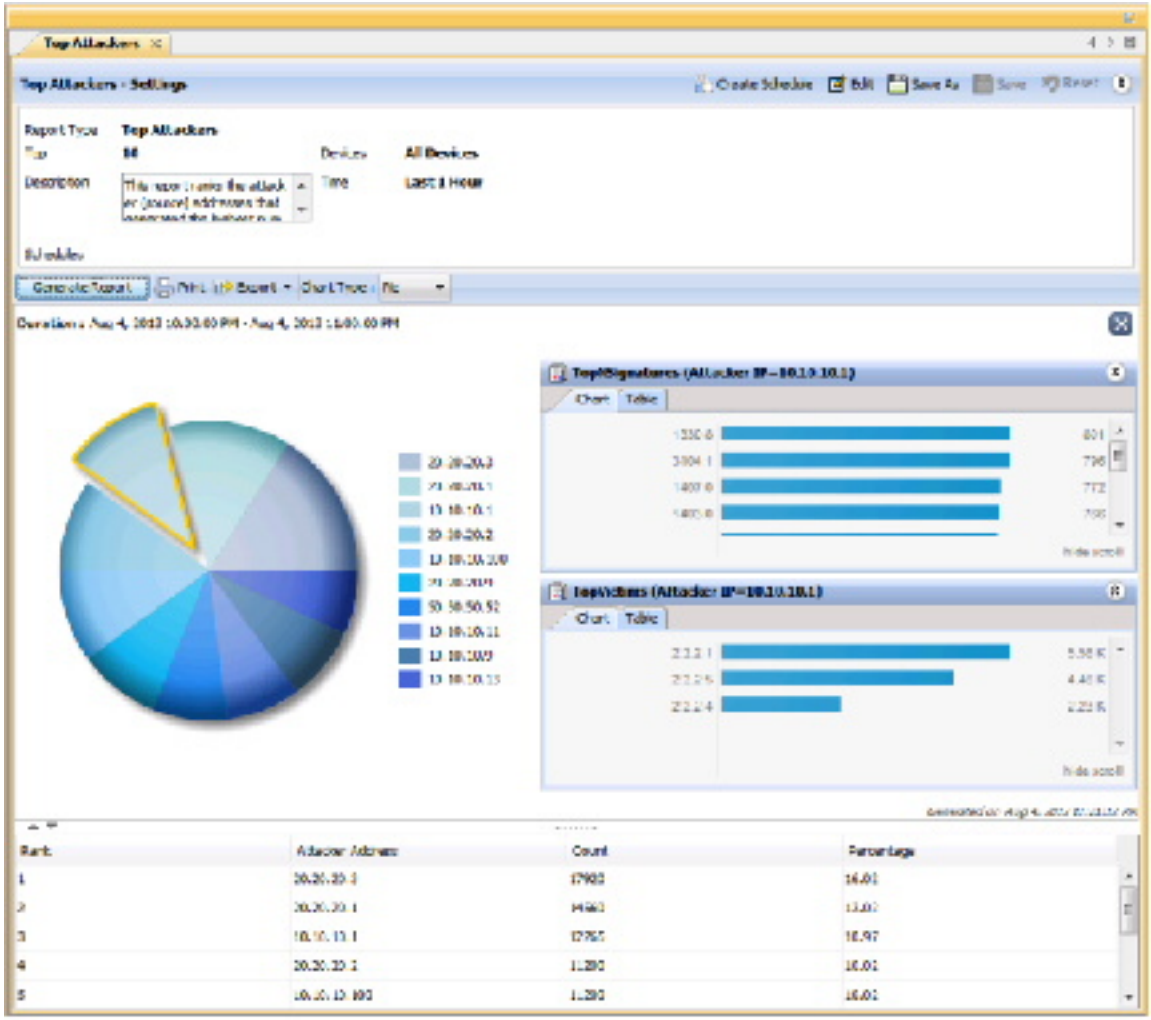
次の表は、サポートされているレポートタイプごとに表示されるドリルダウンレポートを示しています。

レポート名	表示されるドリルダウンレポート
Firewall	
上位ソース	上位宛先（Top Destinations）、上位サービス（Top Services）
上位接続先	上位送信元（Top Sources）、上位サービス（Top Services）
最上位サービス（Top Services）	上位送信元（Top Sources）、上位宛先（Top Destinations）
IPS	
上位シグニチャ（Top Signature）	上位攻撃者（Top Attackers）、上位攻撃対象（Top Victim）
上位攻撃者（Top Attackers）	上位攻撃者（Top Attackers）、上位攻撃対象（Top Victim）
上位攻撃対象（Top Victim）	上位シグニチャ（Top Signature）、上位攻撃者（Top Attackers）

ドリルダウンレポートごとに、ドリルダウンデータのグラフまたは表を表示できます。サポートされているレポートのいずれかで特定のデータポイントにドリルダウンした場合、ドリルダウンレポートのグラフと表形式のデータが、印刷したレポートとエクスポートしたレポートデータに含まれます。

次の図は、[上位攻撃者（Top Attackers）] レポートのドリルダウンレポートデータの例を示しています。

図 *4:* 上位の攻撃者のドリルダウン レポート



関連項目

- レポートの起動と生成　（25 ページ）
- ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要

レポートの印刷

レポートの起動と生成　（25 ページ）の説明に従ってレポートを生成したあとで、そのレポートを印刷できます。

（注） 上位宛先、上位サービス、または上位送信元ファイアウォールレポート、または上位攻撃者、上位シグネチャ、または上位攻撃対象 IPS レポートで特定のデータポイントのドリルダウンレポートを開いている場合、ドリルダウンレポートのグラフと表形式のデータは、印刷されたレポートに含まれます。詳細については、レポートデータへのドリルダウン （33 ページ）を参照してください。

レポートを印刷するには、レポートの上にある [印刷（Print）] ボタンをクリックします。プリンタを選択するプロンプトが表示されます。

レポートのエクスポート

レポートの起動と生成 （25 ページ）の説明に従ってレポートを生成したあとで、そのレポートを Adobe Acrobat（PDF）ファイルまたは Comma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートできます。

エクスポートされたファイルには、次の情報が含まれています。

- レポートの作成時刻。
- レポートの生成に使用した設定。
- （PDF のみ）レポートデータのグラフィカル表現。
- 表形式のレポート データ。PDF では、情報はテーブルとして表されます。CSV では、情報はカンマ区切りで、最初の行がカラムの見出しになります。

（注） 上位宛先、上位サービス、または上位送信元ファイアウォールレポート、または上位攻撃者、上位シグネチャ、または上位攻撃対象 IPS レポートで特定のデータポイントのドリルダウンレポートを開いている場合、ドリルダウンレポートのグラフと表形式のデータは、エクスポートに含まれます。詳細については、レポートデータへのドリルダウン （33 ページ）を参照してください。

レポートをエクスポートするには、レポートの上の [エクスポート（Export）] ボタンで下矢印をクリックし、[PDFとして（As PDF）] または [CSVとして（As CSV）] のいずれかを選択します。レポートのフォルダを選択するプロンプトが表示されます。デフォルトのファイル名が指定されていますが、そのファイル名を変更できます。

レポートエクスポートエラーのトラブルシューティング

デバイスステータスレポートをエクスポートしようとすると、次のエラーが表示されます。

「Windows は 'acrord32' を見つけることができません。名前を正しく入力したことを確認してから、やり直してください。」

まず、サーバーに Adobe Reader がインストールされていない場合に上記のエラーが発生します。Adobe がインストールされていないため、Windows は acrord32.exe ファイルを見つけることができません。

次に、Adobe Reader がインストールされている場合でも、上記のエラーがスローされる場合があります。これは、Windows XP、Vista、7、8.1、および 10 に存在する問題です。これは、Adobe Reader の起動に失敗したことが原因です。これは既知のエラーであり、Adobe Reader だけでなく、すべてのアプリケーションで発生する可能性があります。Microsoft はまだこれに対するパッチを提供していません。

この問題が発生する可能性のある報告された理由は次のとおりです。

1) 破損したレジストリエントリ

2) Adobe のインストール中の問題

3) デフォルトの Adobe Reader の削除

<B>症状：</B>

デバイスステータスレポートをエクスポートしようとすると、次のエラーが表示されます。

「Windows は 'acrord32' を見つけることができません。名前を正しく入力したことを確認してから、やり直してください。」

<B>条件：</B>

まず、サーバーに Adobe Reader がインストールされていない場合に上記のエラーが発生します。Adobe がインストールされていないため、Windows は acrord32.exe ファイルを見つけることができません。

次に、Adobe Reader がインストールされている場合でも、上記のエラーがスローされる場合があります。これは、Windows XP、Vista、7、8.1、および 10 に存在する問題です。これは、Adobe Reader の起動に失敗したことが原因です。これは既知のエラーであり、Adobe Reader だけでなく、すべてのアプリケーションで発生する可能性があります。Microsoft はまだこれに対するパッチを提供していません。

<B>回避策：</B>

1) Adobe Reader がインストールされていない場合はインストールします

2) Adobe Reader がインストールされていてもエラーがスローされる場合は、ファイルが保存されている場所に移動して実行します

Adobe Reader アクションで開きます。エラーがスローされても、ファイルは作成されますが、フォーマットはなしになります。

形式）。そのため、PDF リーダーを使用して開くことができます。

<B>問題の詳細：</B>

レポートのデフォルト設定値の設定

Report Managerがシステム レポートに対して使用するデフォルト設定を制御できます。デフォルトを変更すると、すべてのシステム レポートの設定が自動的に変更されますが、変更内容はカスタム レポートとして保存したレポート（[My Reports] フォルダ内）には適用されません。これらの設定を変更するには、システム管理者権限またはネットワーク管理者権限が必要です。

レポートを表示している間に、任意のシステム レポートを編集してこれらの設定に別の値を指定できます。その目的は、レポートを表示している間の一時的な使用、または [My Reports] フォルダ内のカスタム レポートとしての保存のいずれかです。

（注） レポートの作成後はフィルタを適用できないため、[マイレポート（My Reports）] または [カスタムレポート（Custom Reports）] でレポートを作成する際には、レポートの作成時に必要なフィルタが適用されていることを確認してください。

ヒント システムレポートの設定を変更する場合、[レポート設定（Report Settings）] ツールバーで [リセット（Reset）] ボタンをクリックすると、レポートをデフォルト設定に戻すことができます。

ステップ 1 Report Manager で、[ツール（Tools）] > [デフォルトのレポート設定（Default Report Settings）] を選択し、[デフォルトのレポート設定（Default Report Settings）] ダイアログボックスを開きます。

ステップ 2 次のいずれかのオプションを設定します。

- [上位（Top）]：いずれかの「上位」レポートに表示される結果の数。上位レポートには、レポートがターゲットとするタイプの最新の発生項目が表示されます。たとえば、20 を選択すると、ファイアウォール上位宛先（Top Destinations）レポートには、Security Manager に報告されたイベント内で発生時刻が最新 20 個のトラフィック宛先が表示されます。デフォルトは 10 です。

各追加項目の詳細情報はレポートテーブルに表示されますが、10 よりも大きい値を選択すると、10 番目の後の項目はすべて、チャートでは「others」として要約表示されます。

- [時間範囲（Time Range）]：レポートに含めるイベントの時間枠：
  - [Last 1 Hour]：00 分から始まる直前の 1 時間全体。たとえば、現在の時刻が午前 11:45 である場合、直前の 1 時間（Last 1 Hour）のレポートには 10:00 から 11:00 までのデータが表示されます。
  - [Last 1 Day]：直前の 1 日全体（0 時から 0 時まで）。たとえば、現在の日付が火曜日である場合、直前の 1 日（Last 1 Day）のレポートには月曜日のデータが表示されます。
  - [Last 1 Week]：前の月曜日から日曜日まで。
  - [Last 1 Month]：前月。たとえば、現在の日付が 9 月 29 日である場合、直前の 1 か月（Last 1 Month）のレポートには 8 月のデータが表示されます。

時間範囲設定の意味の詳細については、 Report Manager データ集約について （5 ページ）を参照してください。

- [デフォルトの電子メールアドレス（Default Email Address）]：スケジューリングされたレポートのデフォルトの宛先として使用される電子メールアドレス。

インストール時のデフォルト値に戻す場合は、[デフォルトの復元（Restore Defaults）]をクリックします。

ステップ 3 [適用（Apply）]をクリックして変更内容を保存し、[閉じる（Close）]をクリックしてダイアログボックスを閉じます。

レポート ウィンドウの配置

同時に最大で 5 つのレポート ウィンドウを開いていることができます。レポートは、メイン Report Manager ウィンドウの右側のペインにタブ付きウィンドウとして開かれます。複数の領域がある場合は、最も最近に使用された領域（「タブ付きグループ」）に開かれます。次の図に示すように、レポート ウィンドウのタブを右クリックすると、ウィンドウを配置するためのコマンドが表示されます。

ユーザの要件に基づいてレポート ウィンドウを配置するための多数のオプションがあります。たとえば、2 つのレポートを横に並べて比較したり、レポートを閉じないでメイン ウィンドウから除去したりすることができます。

次の方法を使用してレポート ウィンドウを配置し、目的の表示にすることができます。

- レポートのフローティング：レポートを閉じずにメイン Report Manager ウィンドウから除去するには、レポートタブを右クリックし、[フローティング（Floating）]を選択します。レポートは独自のウィンドウに移動します。

すでにレポートをフローティングしている場合は、[フローティング先（Floating to）] を選択し、既にフローティングされているウィンドウの 1 つを選択します。レポートがそのウィンドウ内の新しいタブになります。

- レポートのドッキング：フローティングレポートをメイン Report Manager ウィンドウに戻すには、レポートタブを右クリックし、[ドッキング（Docking）] を選択します。
- 横に並べて比較するためのレポートの水平配置：レポートをフローティングせずに、簡単に比較できるようにするためにレポートを垂直または水平に配置するには、レポートタブ

を右クリックし、[新しい横方向グループ（New Horizontal Group）] または [新しい縦方向グループ（New Vertical Group）] を選択します。これらのコマンドは、現在のタブ付きグループを選択されたレイアウトに分割します。これらのコマンドを使用するには、少なくとも 2 つのレポートが開いている必要があります。レポートを 3 つ以上開いていて、それらすべてを別々のウィンドウに配置する場合は、コマンドを複数回使用する必要があります。

- 異なるタブ付きグループへのレポートの移動：開いているレポートが複数あり、それらのレポートが水平または垂直のグループに配置されている場合は、レポートタブを右クリックして [次のタブグループに移動（Move to Next Tab Group）] または [前のタブグループに移動（Move to Previous Tab Group）] を選択することにより、グループ間でレポートを移動できます。これらのコマンドは、移動できるような方法でレポートが配置されている場合にのみ表示されます。
- グループの向きの変更：レポート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）] を選択することにより、水平方向のレイアウトと垂直方向のレイアウトを切り替えることができます。

レポートの保存

レポートの設定を編集する場合、それらの変更内容を永続的にするにはレポートを保存する必要があります。ただし、事前定義システム レポートに対する変更内容を保存するには、レポートをカスタム レポートとして保存する必要があります。

ヒント レポートを保存すると、そのレポートを定義している設定が保存されます。レポートの生成内容は保存されません。レポートの生成内容（つまり、グラフとレポートデータ）を保存する場合は、レポートを保存するのではなくエクスポートする必要があります。

- カスタム レポートに対する変更内容を保存するには、Report Manager で次のいずれかを実行します。
  - メニューバーから **[ファイル（File）] > [保存（Save）]** を選択する。
  - レポート設定ツールバーで [名前を付けて保存（Save As）] ボタンをクリックする。
- 変更内容を新規カスタム レポートとして保存するには、次のいずれかを実行して、[Save Report As] ダイアログボックスを開きます。
  - メニューバーから **[ファイル（File）] > [名前を付けて保存（Save As）]** を選択する。
  - レポート設定ツールバーで [名前を付けて保存（Save As）] ボタンをクリックする。
  - レポートリストでレポートを右クリックして、[名前を付けて保存（Save As）] を選択する。

次に、レポートの名前とレポートの説明（任意）を入力し、[OK] をクリックします。レポートがレポート リストの [My Reports] フォルダに追加されます。

（注） レポート名は最大 64 文字で、英数字、スペース、ハイフン（-）、および下線文字（_）を含みます。説明には、最大 1024 文字を使用できます。

レポートの名前変更

カスタム レポートの名前は変更できますが、事前定義システム レポートの名前は変更できません。

関連項目

- Report Manager の概要 （8 ページ）
- Report Manager のレポート リストについて （12 ページ）

ステップ 1 Report Manager で、名前を変更するレポートをレポート リストから選択します。レポートを開く必要はありません。単にリスト内で選択します。

ステップ 2 レポートリストの上の [編集（Edit）]（鉛筆）ボタンをクリックしてダイアログボックスを開きます。そこで、レポート名を変更できます。

ステップ 3 新しい名前を入力し、[OK] をクリックします。

レポート名は最大 64 文字で、英数字、スペース、ハイフン（-）、および下線文字（_）を含みます。

レポート ウィンドウの終了

レポート タブの X アイコンをクリックすることにより、任意のレポートを閉じることができます。フロートしたレポートの場合、単にそのウィンドウのタイトルバーの [X] アイコンをクリックします。

ヒント レポートを閉じるときに、生成されたレポートデータは保持されません。生成されたデータを保持する場合は、レポート ウィンドウを閉じる前に、レポートを印刷またはエクスポートする必要があります。

次の方法を使用して、Report Manager を終了せずにレポート ウィンドウを閉じることもできます。

- レポートを閉じる：[ファイル（File）]>[レポートを閉じる（Close Report）] を選択して、現在表示されているウィンドウを閉じるか、または目的のレポートタブを右クリックして [閉じる（Close）] を選択します。

- すべてのレポートを閉じる：[ファイル（File）] > [すべてのレポートを閉じる（Close All Reports）] を選択するか、または任意のレポートタブを右クリックして [すべてを閉じる（Close All）] を選択します。
- 1 つのレポートを除いてすべてのレポートを閉じる：開いたままにしておくレポートのレポートタブを右クリックし、[他を閉じる（Close Others）] を選択します。

レポートの削除

カスタム レポートは削除できますが、事前定義システム レポートは削除できません。

カスタムレポートを削除するには、削除するレポートをレポートリストで選択し、レポートリストの上の [削除（Delete）]（ゴミ箱）ボタンをクリックします。削除の確認が求められます。

ヒント レポートを削除すると、そのレポートのスケジュールもすべて削除されます。

別のユーザのカスタムレポートを削除する必要がある場合は、カスタム レポートの管理 （41 ページ）を参照してください。

カスタム レポートの管理

システム管理者権限またはネットワーク管理者権限がある場合は、この Security Manager サーバ上のすべての Report Manager ユーザによって作成されたカスタム レポートのリストを表示できます。

カスタムレポートのリストを表示するには、[ツール（Tools）] > [カスタムレポートリスト（Custom Report List）] を選択して [カスタムレポートの管理（Manage Custom Reports）] ダイアログボックスを開きます。リストには、レポート名、レポートのタイプ、レポートで分析されるデバイスのタイプ、カスタム レポートを作成したユーザのユーザ名が表示されます。

次のコントロールを使用して、このページのカスタム レポートを管理できます。

- **ページネーションコントロール**：多数のカスタムレポートがある場合、ページネーションコントロールを使用してリスト内を移動します。ボタンをクリックして、最初のページ、前のページ、次のページ、または最後のページに移動できます。または [Page X of Y] 編集ボックスにページ番号を入力できます。編集ボックスで下矢印をクリックして、ページ番号ではなくレコード番号で処理するように編集ボックスを変更することもできます。
- [削除（Delete）] ボタン：選択されたレポートを削除するには、このボタンをクリックします。そのレポートを使用するスケジュール（およびスケジュールの結果）もすべて削除されます。
- [リフレッシュ（Refresh）]ボタン：最新の情報を使用してリストを更新するには、このボタンをクリックします。

レポートのスケジュール設定

定期的に Report Manager からレポートを生成するようにスケジュールを作成できます。

ここでは、次の内容について説明します。

レポート スケジュールの表示

Report Manager で設定されているレポート スケジュールのリストを表示できます。システム管理者権限またはネットワーク管理者権限がある場合、リストには、そのユーザが設定したか別のユーザが設定したかには関係なく、サーバで設定されているすべてのスケジュールが含まれています。それより低い権限を持つユーザは、自身のスケジュールのみを参照できます。

レポートスケジュールのリストを表示するには、[スケジュール設定されたレポート（Scheduled Reports）] タブを選択し、必要に応じて、[スケジュールリスト（Schedule List）] サブタブを選択します。リストには、スケジュール名、説明、スケジュールによって生成されるレポート、レポート生成の頻度、レポートの送信先電子メールアドレス（ある場合）、スケジュールがイネーブルまたはディセーブルのどちらであるか、およびスケジュールを作成したユーザのユーザ名が表示されます。

次のコントロールを使用して、このページのレポート スケジュールを管理できます。

- **ページネーション コントロール**：多数のスケジュールがある場合、ページネーション コントロール（テーブルの下の左側）を使用してリスト内を移動します。ボタンをクリックして、最初のページ、前のページ、次のページ、または最後のページに移動できます。または [Page X of Y] 編集ボックスにページ番号を入力できます。編集ボックスで下矢印をクリックして、ページ番号ではなくレコード番号で処理するように編集ボックスを変更することもできます。
- [追加（Add）] ボタン：新規スケジュールを追加するには、このボタンをクリックします。詳細については、 レポート スケジュールの設定 （43 ページ）を参照してください。
- [編集（Edit）] ボタン：選択されたスケジュールを編集するには、このボタンをクリックします。詳細については、 レポート スケジュールの設定 （43 ページ）を参照してください。
- [削除（Delete）] ボタン：選択されたスケジュールを削除するには、このボタンをクリックします。詳細については、 レポート スケジュールの削除 （46 ページ）を参照してください。

- [リフレッシュ（Refresh）]ボタン：最新の情報を使用してリストを更新するには、このボタンをクリックします。
- [イネーブル（Enable）] ボタン：選択されたスケジュールをイネーブルにするには、このボタンをクリックします。このボタンは、選択されたスケジュールがディセーブルの場合にのみアクティブです。詳細については、レポート スケジュールのイネーブル化およびディセーブル化 （45 ページ）を参照してください。
- [ディセーブル（Disable）]ボタン：選択されたスケジュールをディセーブルにするには、このボタンをクリックします。このボタンは、選択されたスケジュールがディセーブルの場合にのみアクティブです。詳細については、レポート スケジュールのイネーブル化およびディセーブル化 （45 ページ）を参照してください。

レポート スケジュールの設定

設定された時刻に自動的にレポートを生成するようにスケジュールを作成できます。生成されたレポートは、指定された受信者に電子メールで送信され、また、Report Manager で表示できるように保管されます。レポートをスケジューリングすることにより、ネットワーク セキュリティおよび使用状況の定期的なマイルストーン ビューを簡単かつ効率的に作成できます。この手順では、レポートのスケジュールのセットアップ方法を説明します。

関連項目

- Report Manager の概要 （8 ページ）
- レポートの起動と生成 （25 ページ）
- レポート スケジュールの表示 （42 ページ）
- Report Manager のトラブルシューティング （46 ページ）

ステップ 1 Report Manager で、次のいずれかを実行します。

- [Reports] タブで、レポート リスト（左側のペイン）でレポートの名前ダブルクリックすることにより、新規スケジュールを作成するレポートを開きます。次に、レポート設定ツールバーで[スケジュールの作成（Create Schedule）] ボタンをクリックします。

（注） [Reports] タブから既存のスケジュールを編集することはできません。

- [レポート（Reports）]タブで、スケジュールを作成するレポートを右クリックし、[スケジュールの作成（Create Schedule）] を選択します。レポートがまだ開いていない場合は、開かれます。
- [スケジュール設定されたレポート（Scheduled Reports）]タブの[スケジュールリスト（Schedule List）]サブタブで、スケジュールのリストの下にある [追加（Add）] ボタンをクリックし、新規スケジュールを作成します。既存のスケジュールを編集するには、リストでレポートを選択して [編集（Edit）] ボタンをクリックします。

[Add or Edit Report Schedule] ダイアログボックスが開きます。

ステップ 2 ダイアログボックスで次のオプションを設定します。

- [スケジュール名（Schedule Name）]：スケジュールの名前（最大 64 文字）。
- [レポート名（Report Name）]：スケジュールで生成するレポートの名前を選択します。レポート設定ペインからスケジュールを作成する場合、名前は事前に選択されており、ユーザはその名前を変更できません。
- [スケジュール（Schedule）]：レポートの生成頻度（毎日、毎週（週に 1 回）、または毎月（月に 1 回））を選択します。次に、レポートを生成する日時を入力します。
  - [Daily schedules]：スケジュールが [Monday through Friday]（5 日間）または [Monday through Sunday]（7 日間全体）のどちらであるかを選択します。レポートを生成する時刻（24 時間表記）を入力します。
  - [Weekly schedules]：曜日を選択し、24 時間表記で時刻を入力します。
  - [Monthly schedules]：レポートの生成が、月の最初の日、最後の日、またはカスタムの、いずれであるかを選択します。[Custom] を選択する場合は、日付番号を入力します。次に、24 時間表記で時刻を入力します。
- [電子メールの送信先（Email To）]：レポートの送信先の電子メールアドレス。カンマで複数のアドレスを区切ります。レポートを電子メールで送信しない場合は、そのフィールドが空であることを確認してください。電子メールを正常に送信するには、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定で説明されているように、Security Manager サーバに SMTP を設定する必要があることに注意してください。

何らかの理由でレポートを生成できない場合、その失敗に関する通知がこれらの電子メールアドレスに送信されます。

- [レポート形式のエクスポート（Export Report Format）]：レポートを Adobe Acrobat（PDF）形式またはカンマ区切り値（CSV）形式で生成するかを指定します。PDF にはグラフィックが含まれますが、CSV には含まれません。エクスポート形式の詳細については、レポートのエクスポート （35 ページ）を参照してください。
- [説明（Description）]：スケジュールの説明。
- [ステータス（Status）]：スケジュールが有効（レポートが生成される）または無効（レポートが生成されない）であるかを指定します。

ステップ 3 [OK] をクリックして、スケジュールを保存します。[Schedules] タブのスケジュール リストに新規スケジュールが追加されます。

スケジューリングされたレポートの結果の表示

通常、レポート スケジュールには生成されたレポートの送信先電子メール アドレスが含まれています。Report Manager でスケジュールから生成されたレポートを表示することもできま

す。システム管理者権限またはネットワーク管理者権限がある場合、他のユーザーのスケジュールによって生成された結果を表示できます。

ヒント　Report Manager は、スケジュールによって生成された最後のレポートのコピーを維持します。以前に生成されたレポートを取得することはできません。

関連項目

- Report Manager の概要　（8 ページ）
- レポートの起動と生成　（25 ページ）
- レポート スケジュールの表示　（42 ページ）
- Report Manager のトラブルシューティング　（46 ページ）

ステップ 1　Report Manager で、[スケジュール設定されたレポート（Scheduled Reports）] タブを選択します。

ステップ 2　[結果（Results）] サブタブを選択します。

表示する権限があるすべての結果が、このタブにリストされます。このリストには、スケジュール名、生成されたレポートの名前、レポート生成の頻度、前回のスケジュール実行（レポートが生成されたとき）の日時、レポート生成のステータス（[Success] または [Failed]）、生成されたレポート（[Last Report] カラム内）へのリンク、およびスケジュールを作成したユーザのユーザ名が表示されます。

ヒント　レポートのステータスが [Failed] である場合は、リンクをクリックして失敗の理由を参照します。

ステップ 3　[Last Report] カラムでレポートへのアイコン リンクをダブルクリックし、レポートを開きます。レポートを表示しているときに、そのレポートをワークステーションに保存できます。

探しているレポートが見つからない場合は、[リフレッシュ（Refresh）] ボタンをクリックして最新の情報でリストを更新します。

レポート スケジュールのイネーブル化およびディセーブル化

レポート スケジュールをイネーブルまたはディセーブルにして、スケジュールに基づいてレポートが生成されるかどうかを変更できます。スケジュールをディセーブルにすることにより、スケジュールを削除せずにレポートが生成されないようにすることができます。システム管理者権限またはネットワーク管理者権限がある場合、別のユーザのスケジュールをイネーブルまたはディセーブルにすることができます。

関連項目

- Report Manager の概要　（8 ページ）
- レポート スケジュールの表示　（42 ページ）

ステップ 1 Report Manager で、[スケジュール設定されたレポート（Scheduled Reports）] タブを選択し、必要に応じて、[スケジュールリスト（Schedule List）] サブタブを選択します。このタブには、現在定義されていて表示権限があるスケジュールがすべてリストされます。

ステップ 2 ステータスを変更するスケジュールを選択し、[有効（Enable）] ボタンまたは [無効（Disable）] ボタンのいずれかをクリックします。

レポート スケジュールの削除

レポート スケジュールが不要になったら、それらのスケジュールを削除できます。システム管理者権限またはネットワーク管理者権限がある場合、別のユーザーのスケジュールを削除できます。

ヒント スケジュールからレポートを生成しないが、スケジュール定義を保持しておく場合は、スケジュールをディセーブルにすることができます。ディセーブルになったスケジュールは、レポートを生成しません。

ステップ 1 Report Manager で、[Scheduled Reports] タブを選択し、必要に応じて、[Schedule List] サブタブを選択します。このタブには、現在定義されていて表示権限があるスケジュールがすべてリストされます。

ステップ 2 スケジュールを選択し、リストの下の [削除（Delete）] ボタンをクリックします。削除の確認が求められます。

スケジュールを削除すると、そのスケジュールの結果もすべてサーバから削除され、[Results] タブから除去されます。

Report Manager のトラブルシューティング

以下に、Report Manager アプリケーション使用時に発生する可能性があるいくつかの問題と、いくつかの問題解決方法を示します。

問題：Report Manager が開かず、「Not able to connect to server」というメッセージが表示される。

解決策：Report Manager で、csmReportServer プロセス、rptDbEngine プロセス、および rptDbMonitor プロセスを開始する必要があります。Report Manager は、Event Management サービス VmsEventServer にも依存しています。Security Manager サーバですべてのサービスが開始されており、正しく実行していることを確認してください。

プロセスの現在の状態を表示するには、http://SecManServer:1741（SecManServer はサーバーの DNS 名）を使用して Security Manager Web インターフェイスにログインします。Security

Management Suite ホームページから、[サーバー管理（Server Administration）] リンクをクリックして [管理（Admin）] ページで CiscoWorks Common Services を開きます。ウィンドウの左側の TOC で [プロセス（Processes）] をクリックして、現在の状態を表示するプロセスのリストを開きます。これらのプロセスを選択し、[開始（Start）] をクリックして開始します。必要に応じて、これらのプロセスを停止してから再起動することができます。プロセスが完全に再起動するまで待機してから、再度 Report Manager を開いてみます。

問題：レポートの生成時に、「No records found」というメッセージが表示される。

解決策：このメッセージは、そのレポートタイプと設定されている設定値に関連したイベントレコードがイベント データ ストレージ ロケーションに存在しないか、または必要な Report Manager 集約サイクルが完了していないことを示しています。以下を調べます。

- モニタするデバイスの選択の説明に従って、モニタリングに適したタイプのデバイスが選択されていることを確認します。
- これらのデバイスが Security Manager へのイベント送信用に適切に設定されていること、およびデバイスからのイベントが Event Viewer に表示されていることを確認します。デバイスと Security Manager が同じ syslog ポートを使用していることを確認します。デバイスの設定については、イベント管理のための ASA と FWSM デバイスの設定およびイベント管理のための IPS デバイスの設定を参照してください。Security Manager が使用している syslog ポートを確認するには、Configuration Manager の [ツール（Tools）] > [Security Manager 管理（Security Manager Administration）] > [イベント管理（Event Management）] ページの設定を表示します。
- IPS デバイスの場合、証明書が期限切れになっていないことを確認します。Configuration Manager で [管理（Manage）] > [IPS] > [IPS証明書（IPS Certificates）] を選択することにより証明書テーブルを確認し、必要な場合は証明書を再生成します。
- レポート設定で、レポート対象の集約データが存在しない期間が指定されている可能性があります。データは、15 分ごと、1 時間ごと（正時）、および 1 日ごと（0 時）に集約されます。レポートの時間のパラメータを変更してみてください。レポート設定の編集（28 ページ）を参照してください。以下の点に注意してください。
  - 直前の 1 時間（Last 1 Hour）のレポートを表示するには、最初に Event Manager サービスを開始したあとで時間の変更（正時）が発生している必要があります。たとえば、10:05 にサービスを開始する場合、毎時のレポートは 11:00 のあとでのみ使用できます。
  - 直前の 1 日（Last 1 Day）のレポートを表示するには、最初に Event Manager サービスを開始したあとで日付の変更が発生している必要があります。たとえば、10:05 にサービスを開始する場合、毎日のレポートを参照するには 0 時を過ぎるまで待つ必要があります。
  - 直前の 1 週間（Last 1 Week）のレポートを表示するには、すべての曜日のサイクルが少なくとも 1 回発生している必要があります。毎週のレポートは、毎日のレポートに基づいています。
  - 直前の 1 か月（Last 1 Month）のレポートを表示するには、サービス開始後に少なくとも 1 つの月全体が経過している必要があります。

- カスタム期間レポートを表示するには、その日付のサイクルが少なくとも 1 回発生している必要があります。

- 新規カスタム レポートを作成する場合、データを使用できるまでに最大 1 時間かかる可能性があります。また、レポートの経過時間が他の期間のデータに対して十分になるまでは、期間が直前の 1 時間（Last 1 Hour）であることを確認してください。

問題：特定のデバイスのレポートを取得できない。

解決策：以下を調査します。

- モニタするデバイスの選択で説明されているように、そのデバイスがレポーティング時間フレームにおけるイベント管理用に選択されている必要があります。デバイスが選択されている場合でも、Report Manager が Event Viewer でサポートされるすべてのデバイスをサポートするとは限りません。サポートされるデバイス タイプについては、レポート管理について （1 ページ）を参照してください。

- レポート設定でそのデバイスが除外されている可能性があります。レポートですべてのデバイスを考慮するようにレポート設定が指定している場合を除き、デバイス選択にそのデバイスが含まれていることを確認します。レポート設定の編集 （28 ページ）を参照してください。

- レポート設定で、そのデバイスのデータが存在しない期間が指定されている可能性があります。レポートの時間のパラメータを変更してみてください。レポート設定の編集 （28 ページ）を参照してください。

- ユーザの組織で Cisco Secure ACS を使用してアプリケーションへのアクセスを制御している場合は、少なくともデバイスに対する表示権限がある場合にのみ、そのデバイスに関するレポートを表示できます。必要な権限があるかどうかを確認してください。

問題：シグニチャ、攻撃対象 IP、および攻撃者 IP のそれぞれに対して値を指定したあとで、特定の IPS 事前定義レポートのデータが表示されない。

解決策：上位攻撃者、上位攻撃対象、および上位シグニチャの各事前定義レポートには、シグニチャ、攻撃対象 IP アドレス、および攻撃者 IP アドレスの各基準が含まれています。ただし、3 つの基準すべてを事前定義レポート内で設定することはできません。代わりに、レポートが基づく基準（たとえば、上位攻撃対象レポートの攻撃対象 IP アドレス）と、残りの値を 1 つのみ設定できます。この制限は、[Blocked] や [Top] などの他の基準には適用されないことに注意してください。

問題：サービス、ソース IP、および宛先 IP のそれぞれに対して値を指定したあとで、特定のファイアウォール事前定義レポートのデータが表示されない。

解決策：上位宛先、上位サービス、および上位ソースの各事前定義レポートには、サービス、ソース IP アドレス、および宛先 IP アドレスの各基準が含まれています。ただし、3 つの基準すべてを事前定義レポート内で設定することはできません。代わりに、レポートが基づく基準（たとえば、上位サービス レポートのサービス）と、残りの値を 1 つのみ設定できます。この制限は、[Permit/Deny] や [Top] などの他の基準には適用されないことに注意してください。

問題：VPN レポートの統計情報を取得できない。

解決策：VPN 統計情報は、イベント データ ストレージ ロケーションに格納されているイベントからではなく、デバイスから直接部分的に取得されます。統計情報を取得するには、Report Managerがデバイスにログインしてshowコマンドを使用できる必要があります。ご使用のVPNデバイスのデバイス プロパティが、ログインするための正しいクレデンシャルを持っていることを確認してください。

問題：スケジュール設定されたレポートが受信者に送信されない。

解決策：SMTP サーバーが正しく設定されていること、および Security Manager に対して有効なソース電子メールアドレスが設定されていることを確認してください。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定を参照してください。

問題：デバイスステータスレポートをエクスポートすると、次のエラーが表示される。「Windows は 'acrord32' を見つけることができません。名前を正しく入力したことを確認してから、やり直してください。」

解決策：以下を実行します。

- サーバーに Adobe Reader をインストールします（まだインストールされていない場合）。Adobe Reader がインストールされていない場合、MS-Windows は acrord32.exe ファイルを見つけることができません。
- Adobe Reader がインストールされていても、Windows XP、Vista、7、8.1、または 10 を使用している場合は、エラーがスローされることがあります。これは Microsoft Windows の既知のエラーです。Microsoft は、このエラーに対するパッチをまだ提供していません。次の手順を実行します。
  - エクスポートされたレポートファイルが保存されている場所に移動します。右クリックして、[プログラムから開く] > [Adobe Reader] を選択します。エラーは発生していますが、ファイルは定義された形式なしで作成されます。そのため、PDF リーダーを使用して開くことができます。

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。