CHAPTER 10

トレンド レポートの使用

（注） サポートされるサービスおよびプラットフォームの詳細については、「モニタリングおよびレポートでサポートされるサービスとプラットフォーム」（P.1-5）を参照してください。

ここでは、Performance Monitor で使用できるレポートの機能について、および生成した履歴トレンド レポートを使用および保存する方法について説明します。

レポートのオプションについて

サポートされているすべてのサービス タイプについて、レポートを設定および生成できます。レポートは、4 つの広義のカテゴリ、および 30 を超える狭義のサブカテゴリに分類されます。

（注） RAS VPN サービスとサイト間 VPN サービスのみ、4 つの広義のレポート カテゴリをすべてサポートしています。ほとんどの場合、サブカテゴリはサービスに特有です。

サブカテゴリは、検証済みのデバイスについて、またはサポートされているデバイスにおける狭い範囲の条件について、長期間のトレンドを測定します。Failure（障害）カテゴリの中のサブカテゴリは、障害の中の特別な種類を表す、というように、サブカテゴリはカテゴリに特有です。1 つのレポートに対して選択できるサブカテゴリの数は、1 ～ 4 で、選択するサブカテゴリによって異なります。

レポートのカテゴリには次のものがあります。

カテゴリ名	参考
Failure	「障害レポートのサブカテゴリについて」（P.10-2）を参照してください。
Performance	「パフォーマンス レポートのサブカテゴリについて」（P.10-3）を参照してください。
Throughput	「スループット レポートのサブカテゴリについて」（P.10-5）を参照してください。
Usage	「使用状況レポートのサブカテゴリについて」（P.10-6）を参照してください。

障害レポートのサブカテゴリについて

障害レポートで生成されるそれぞれの折れ線グラフには、表 10-1 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- 障害レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- 障害レポートに表示されるグラフについて説明します。

（注）　履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-17）を参照してください。

表 10-1　障害レポートの設定サブカテゴリ

障害レポートのサブカテゴリ	該当するサービス	説明
（注）　障害レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイルまたはカウントのいずれかを表します。		
[% of Inbound Conn Failures]	リモート アクセス VPN	グラフは、失敗した受信接続の長期間のトレンドを、リモート アクセス VPN の全デバイスに対するすべての受信接続の割合（パーセンテージ）として示します。
[% of Phase 1 Conn Failures]	リモート アクセス VPN	グラフは、失敗したフェーズ 1（IKE）接続の長期間のトレンドを、フェーズ 1 の全接続の割合（パーセンテージ）として示します。
[% of Phase 2 Conn Failures]	リモート アクセス VPN	グラフは、失敗したフェーズ 2（IPSec）接続の長期間のトレンドを、フェーズ 2 の全接続の割合（パーセンテージ）として示します。
[% Of Conns Dropped By All Virtual Servers]	ロード バランシング	グラフは、ドロップした仮想サーバ接続の長期間のトレンドを、全接続の割合（パーセンテージ）として示します。
[% Of Failed Conns Per Module]	ロード バランシング	グラフは、失敗したロードバランシング接続の長期間のトレンドを、CSM サービス モジュールの全接続の割合（パーセンテージ）として示します。
[% Of Inbound Conn Failures]	サイト間 VPN	グラフは、失敗した受信フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルの長期間のトレンドを、すべての受信交換の割合（パーセンテージ）として示します。
[% Of Outbound Conn Failures]	サイト間 VPN	グラフは、失敗した送信フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルの長期間のトレンドを、すべての送信交換の割合（パーセンテージ）として示します。
[% of Total Conn Failures]	サイト間 VPN	グラフは、失敗したフェーズ 1（IKE）およびフェーズ 2（IPSec）接続の長期間のトレンドを、すべての受信および送信交換の割合（パーセンテージ）として示します。
（注）　少数のデータ ポイントをベースにする場合には、通常、トレンド レポートはあまり有用ではありません。日付の範囲およびトレンドのタイプによって、データ ポイントの数が決まります。たとえば、期間が 2 日に満たないデータに対して Daily のトレンド タイプを適用した場合、データ ポイントは 1 つだけになります。1 つのデータ ポイントのみからトレンドをグラフ化することはできません。		

パフォーマンス レポートのサブカテゴリについて

パフォーマンス レポートで生成されるそれぞれの折れ線グラフには、表 10-2 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- パフォーマンス レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- パフォーマンス レポートに表示されるグラフについて説明します。

（注） 履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-17）を参照してください。

表 10-2　パフォーマンス レポートの設定サブカテゴリ

パフォーマンス レポートの サブカテゴリ	該当するサービス	説明
（注） パフォーマンス レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイル値またはカウントのいずれかを表します。		
[Bandwidth Usage]	リモート アクセス VPN	グラフは、使用された全帯域幅容量の平均パーセンテージに関する長期間のトレンドを示します。これは、インターフェイス速度を係数とし、受信および送信パケットの合計として計算されます。
[CPU Usage]	• ファイアウォール • リモート アクセス VPN • サイト間 VPN • SSL	グラフは、使用された全 CPU 能力の平均パーセンテージに関する長期間のトレンドを示します。
[CPU Usage Rev]	サイト間 VPN	グラフは、使用された全 CPU 能力の平均パーセンテージに関する長期間のトレンドを示します。 **（注）** [CPU Usage Rev] サブカテゴリを選択したときにレポートに何も示されない場合は、代わりに [CPU Usage] サブカテゴリを使用してください。
[FTP Fixup]	ファイアウォール	グラフは、[FTP Fixup]（FTP トラフィックに適用される、PIX OS のインスペクション機能）に対する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[HTTP Fixup]	ファイアウォール	グラフは、[HTTP Fixup]（HTTP トラフィックに適用される、PIX OS のインスペクション機能）に対する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[Memory Usage]	• ファイアウォール • サイト間 VPN • SSL	グラフは、使用されたプロセッサ メモリ容量の平均パーセンテージに関する長期間のトレンドを示します。

表 10-2　パフォーマンス レポートの設定サブカテゴリ （続き）

パフォーマンス レポートの サブカテゴリ	該当するサービス	説明
[SSL Connections]	SSL	グラフは、アクティブな SSL 接続の合計数に関する長期間のトレンドを示します。
[TCP Fixup]	ファイアウォール	グラフは、[TCP Fixup]（TCP トラフィックに適用される、PIX OS のインスペクション機能）に対する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[TCP Intercept]	ファイアウォール	グラフは、[TCP Intercept]（TCP サービスに対する Denial of Service（DoS; サービス拒否）攻撃を回避する PIX OS の機能）に関する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[Throughput]	SSL	グラフは、インターフェイス速度を係数として、全パブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを示します。
[Total IfErrors]	ファイアウォール	グラフは、ファイアウォールのインターフェイス エラーの数について長期間のトレンドを示します。
[Total Throughput]	ファイアウォール	グラフは、インターフェイス速度を係数として、全パブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを示します。
[URL Access]	ファイアウォール	グラフは、PIX OS の **show perfmon** コマンドの出力に基づいて、1 秒あたりに URL（Web サイト）がアクセスされた平均回数の長期間のトレンドを示します。
[URL Request]	ファイアウォール	グラフは、PIX OS の **show perfmon** コマンドの出力に基づいて、1 秒あたりに URL（Web サイト）が要求された平均回数の長期間のトレンドを示します。
[Xlates]	ファイアウォール	グラフは、ファイアウォールを介して 1 秒あたりに行われた TCP および UDP NAT 変換の平均回数の長期間のトレンドを示します。 **（注）** 変換は、内部アドレスから外部アドレスへのマッピングで、NAT では 1 対 1、PAT では多対 1 にすることができます。1 つのホストで、さまざまな宛先に対して複数の接続を持つことができますが、変換は 1 つだけです。xlate のカウント数が、内部ネットワーク上のホスト数よりもかなり多くなっていることに気付いた場合は、内部ホストのいずれか 1 つが侵害されている可能性があります。

（注） 少数のデータ ポイントをベースにする場合には、通常、トレンド レポートはあまり有用ではありません。日付の範囲およびトレンドのタイプによって、データ ポイントの数が決まります。たとえば、期間が 2 日に満たないデータに対して Daily のトレンド タイプを適用した場合、データ ポイントは 1 つだけになります。1 つのデータ ポイントのみからトレンドをグラフ化することはできません。

スループット レポートのサブカテゴリについて

スループット レポートで生成されるそれぞれの折れ線グラフには、表 10-3 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- スループット レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- スループット レポートに表示されるグラフについて説明します。

（注） 履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-17）を参照してください。

表 10-3　スループット レポートの設定サブカテゴリ

スループット レポートの サブカテゴリ	該当するサービス	説明
（注） スループット レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイル値またはカウントのいずれかを表します。		
[Throughput]	• リモート アクセス VPN • サイト間 VPN	グラフは、インターフェイス速度を係数として、全パブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを示します。
[Throughput Per Accelerator]	リモート アクセス VPN	グラフは、Scalable Encryption Processor（SEP）アクセラレータ カードでの受信および送信オクテットの合計（kbps）の長期間のトレンドを、SEP カードの速度を係数として示します。 **（注）** グラフの各線は、個別の SEP カードを表します。VPN 3005 コンセントレータまたは VPN 3015 コンセントレータには SEP カードがないため、このレポートではこれらのデバイスは対象外になります。[Throughput Per Accelerator] を選択した場合は、他のレポート サブカテゴリを選択できません。
[Throughput Per Interface]	• リモート アクセス VPN • サイト間 VPN	グラフは、1 つのデバイスのパブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを、インターフェイス速度を係数として示します。 **（注）** グラフの各線は、個別のインターフェイスを表します。[Throughput Per Interface] を選択した場合は、他のレポート サブカテゴリを選択できません。
[% Of Crypto Packet Drop]	サイト間 VPN	グラフは、ドロップした暗号化パケットの長期間のトレンドを、暗号化および復号化された全パケットの割合（パーセンテージ）として示します。
[% Of Crypto Packet Errors]	リモート アクセス VPN	グラフは、フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルでエラーとなった暗号化パケットの長期間のトレンドを、暗号化された全パケットの割合（パーセンテージ）として示します。
[% Of Packets Dropped]	• リモート アクセス VPN • サイト間 VPN	グラフは、フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルでドロップしたパケットの長期間のトレンドを、すべての受信および送信パケットの割合（パーセンテージ）として示します。

使用状況レポートのサブカテゴリについて

使用状況レポートで生成されるそれぞれの折れ線グラフには、表 10-4 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- 使用状況レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- 使用状況レポートに表示されるグラフについて説明します。

（注） 履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-17）を参照してください。

表 10-4　使用状況レポートの設定サブカテゴリ

使用状況レポートのサブカテゴリ	該当するサービス	説明
（注） 使用状況レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイルまたはカウントのいずれかを表します。		
[Number of Tunnels]	サイト間 VPN	グラフは、サイト間 VPN に対してフェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルを組み合わせた数の長期間のトレンドを示します。
[Number of Users]	リモート アクセス VPN	グラフは、すべての RAS デバイスにおけるアクティブなセッションの集約数について、長期間のトレンドを示します。
[# Of Conns Per Module]	ロード バランシング	グラフは、特定のシャーシ内の各 CSM モジュールに対して、接続の平均数に関する長期間のトレンドを示します。 **（注）** グラフの各線は、個別のサービス モジュールを表します。[# Of Conns Per Module] を選択した場合は、他のレポート サブカテゴリを選択できません。
[# Of Conns Per Virtual Server]	ロード バランシング	グラフは、特定のシャーシに関連付けられている各仮想サーバに対して、接続数の長期間のトレンドを示します。 **（注）** グラフの各線は、個別の仮想サーバを表します。[# Of Conns Per Virtual Server] を選択した場合は、他のレポート サブカテゴリを選択できません。
（注） 少数のデータ ポイントをベースにする場合には、通常、トレンド レポートはあまり有用ではありません。日付の範囲およびトレンドのタイプによって、データ ポイントの数が決まります。たとえば、期間が 2 日に満たないデータに対して Daily のトレンド タイプを適用した場合、データ ポイントは 1 つだけになります。1 つのデータ ポイントのみからトレンドをグラフ化することはできません。		

レポートの設定と生成

ネットワーク内でサポートされているサービスに対して、履歴レポートを設定および生成することができます。

手順

ステップ 1　[Report] > [Service Type] > [Configure Report] を選択します。[Service Type] は、オプション バーで選択するサービスです。

[Configure Report] ページには、オブジェクト セレクタ、選択したサービスに適用されるアクション ボタン、リスト、およびレポートのカテゴリが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　[All] タブがアクティブになっていない場合は、このタブをクリックして、選択ツリー内のデバイス グループおよび個々のデバイスのリストを表示します。レポートの対象にする情報が定義されているデバイスを選択します。1 つのデバイス グループをすると、そのグループ内のすべてのデバイス、および階層内でのそのグループの下位グループが選択されます。

レポートを設定する前に、少なくとも 1 つのデバイスをツリーから選択する必要があります。次のレポート サブカテゴリで選択が必要なデバイスは *1 つだけ*です。

- [Remote Access] : [Throughput] : [Throughput Per Accelerator]
- [Remote Access] : [Throughput] : [Throughput Per Interface]
- [Site-To-Site] : [Throughput] : [Throughput Per Interface]
- [Load Balancing] : [Usage] : [# Of Conns Per Virtual Server]
- [Load Balancing] : [Usage] : [# Of Conns Per Module]
- [Load Balancing] : [Failure] : [% Of Conns Dropped By All Virtual Servers]
- [Load Balancing] : [Failure] : [% Of Failed Conns Per Module]

ステップ 3　レポート カテゴリを選択し、サブカテゴリを選択してから [>>]（追加）をクリックして、[Selected List] に移動します。誤ったサブカテゴリを選択してしまった場合は、[<<]（削除）をクリックします。

次のルールに従って、複数のレポート タイプを選択できます。

- いずれのレポートについても、4 つを超えるサブカテゴリは選択できません。
- 1 つのレポートに対して 2 つを超えるサブカテゴリは選択できません（ただし、選択したすべてのサブカテゴリがパーセント単位で測定している場合は除きます）。このような場合は、最大 4 つのサブカテゴリを選択できます。
- 選択したサブカテゴリのうち、いずれか 1 つがパーセント単位で測定している場合は、2 つを超えるサブカテゴリは選択できません。
- 「レポートのオプションについて」（P.10-1）およびその各項に説明があるとおり、サブカテゴリを 1 つしか選択できない場合があります。

レポートには 30 を超えるサブカテゴリがあります。レポート タイプの説明については、次の各項を参照してください。

- 「障害レポートのサブカテゴリについて」（P.10-2）
- 「パフォーマンス レポートのサブカテゴリについて」（P.10-3）
- 「スループット レポートのサブカテゴリについて」（P.10-5）
- 「使用状況レポートのサブカテゴリについて」（P.10-6）

ステップ 4　[Trending Type] リストから間隔を選択します。トレンドのオプションには、次のものがあります。

- [Hourly]：レポートは、指定したカレンダー日付の範囲に対して、1 時間間隔でモニタした値を示します。
- [Daily]：レポートは、指定したカレンダー日付の範囲に対して、1 日間隔でモニタした値を示します。
- [Weekly]：レポートは、指定したカレンダー日付の範囲に対して、1 週間間隔でモニタした値を示します。
- [Monthly]：レポートは、指定したカレンダー日付の範囲に対して、1 か月間隔でモニタした値を示します。

ステップ 5　レポートの対象とするデータについて、開始（[From]）と終了（[To]）の日付を選択します。

ステップ 6　次のいずれかを実行します。

- レポートを生成して新しいブラウザ ウィンドウで表示するには、[View] をクリックします。
- レポートを生成し、1 回または繰り返しの E メール配信オプションを設定するには、[Email] をクリックします。繰り返しの E メール ジョブを設定する場合は、レポートに何時間分のデータを含めるかを指定できます。
- レポートを生成してそれをファイルに保存するには、ファイル形式を選択して [Export] をクリックします。使用できる形式には、次のものがあります。
  - CSV：データをカンマ区切りの ASCII リストでエクスポートします。ほとんどのスプレッドシート アプリケーションは、CSV を表形式で表示できます。
  - XML：データを Extensible Markup Language（XML）でエクスポートします。XML は、Web ブラウザ、ワード プロセッサ、または XML ファイルを表示する他のアプリケーションで確認できます。
  - PDF：データを Portable Document Format（PDF）形式でエクスポートします。PDF は、Adobe Acrobat Reader アプリケーション、または PDF ファイルを表示する他のアプリケーションで確認できます。

履歴レポートについて

生成したレポートには、選択したサブカテゴリの履歴トレンドを示すグラフが表示されます。Performance Monitor はレポートに対して、指定したトレンド タイプおよび日付範囲を適用します。特定のグラフの詳細については、「レポートのオプションについて」（P.10-1）およびその各項を参照してください。

[Performance Monitor Report] ページの [Details] エリアには、対象レポートのユーザ名、トレンド タイプ、および日付範囲が表示されます。

関連トピック

- 「レポートの設定と生成」（P.10-7）

RAS VPN の上位 10 ユーザ レポートの表示

すべての RAS デバイス間で、ネットワーク内の RAS VPN の上位 10 ユーザの履歴レポートを表示できます。

（注）　Performance Monitor は、Easy VPN RAS セッションについてこの情報を表示できません。

手順

ステップ 1　[Reports] > [Remote Access] > [Top 10 Users] を選択します。

デフォルトでは、[Top 10 Users] ページに、スループット レベルが最も高い RAS ユーザが 10 人表示され、最近 24 時間の時間ごとのデータ ポイントが示されます。対象の 24 時間で RAS VPN に接続していたユーザが 10 人未満の場合は、10 人よりも少ない人数が表示されます。

レポートの情報は、デバイスごとのユーザ アクティビティ ランキングをベースにしています。

ステップ 2　必要な場合はレポート基準を修正し、[Go] をクリックして結果を確認してください。次のいずれかの方法で実行できます。

- トレンド タイプを変更します。次のいずれかを選択します。
  - [Hourly]：モニタされた値を 1 時間間隔で表示します。
  - [Daily]：モニタされた値を 1 日間隔で表示します。
  - [Weekly]：モニタされた値を 1 週間間隔で表示します。
  - [Monthly]：モニタされた値を 1 か月間隔で表示します。
- [From] フィールドと [To] フィールドに異なる日付を入力し、レポート日付の別の範囲を指定します。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS VPN ユーザ セッション レポートの表示

指定した複数のユーザ、または 1 人のユーザについて、VPN セッションへの長期間のリモート アクセスを表すレポートを表示できます。

ヒント　いくつかのマルチユーザ セッションのクエリーでは、結果として大きい値が返されることがあります。クエリーの結果として 10,000 を超える値が返される場合は、[User Session Report] ページでブラウザをロードするために数分かかります。このような遅延が問題となる場合は、特定のデバイスを選択し、クエリーを発行する前に開始時間と終了時間を調整することを推奨します。

はじめる前に

この機能では、Syslog メッセージを Performance Monitor へ送信するよう、VPN 3000 コンセントレータ、ASA および PIX デバイスを設定する必要があります。

- アプライアンスおよびファイアウォールの設定については、「ASA アプライアンス、PIX デバイス、およびファイアウォール サービス モジュールのセットアップ」（P.2-5）を参照してください。
- VPN コンセントレータの設定については、「VPN 3000 コンセントレータのセットアップ」（P.2-6）を参照してください。
- Performance Monitor が処理可能な Syslog メッセージのリストについては、「通知の操作」（P.12-1）を参照してください。

手順

ステップ 1　[Reports] > [Remote Access] > [User Session Report] を選択します。

[User Session Report] ページにはオブジェクト セレクタがあります。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　複数のユーザ、または 1 人のユーザのどちらに対してセッション レポートを表示するかを決定し、次のいずれかを実行します。

- すべてのユーザのセッションが含まれている情報を表示するには、[Search All Users] を選択します。
- ユーザ セッションの検索対象を 1 人のユーザに制限するには、ツリーでクラスタ ペアレントを選択します。
- ユーザ セッションの検索対象を 1 つのデバイスに制限するには、ツリーでデバイスを選択します。
- 検索対象を 1 人のユーザのセッションに制限するには、[User Name] テキスト ボックスにユーザ名を入力します。

ステップ 3　Performance Monitor がセッションを検索する間隔を定義するには、次の両方を実行します。

- [Start Time] エリアで、カレンダー日付を選択し、HH:MM:SS 形式で時間を入力します。[Start Time] エリアの値は、Performance Monitor がセッション情報を検索する間隔の始まりを定義します。
- [End Time] エリアで、カレンダー日付を選択し、HH:MM:SS 形式で時間を入力します。[End Time] エリアの値は、Performance Monitor がセッション情報を検索する間隔の終わりを定義します。

ステップ 4　次のいずれか、または両方を実行します。

- 新しいブラウザ ウィンドウにレポートを表示するには、[View] をクリックします。
- レポートをエクスポートするには、ファイル形式（CSV または XML）を選択して [Export] をクリックします。

  CSV を選択すると、以前にサーバを「信頼できるソース」として指定していない場合には、Performance Monitor で、CiscoWorks Server の証明書を承認するよう要求されることがあります。この証明書を承認すると、Performance Monitor は、デフォルトのスプレッドシート アプリケーションにエクスポートされた CSV データを表示します。証明書を承認しなかった場合は、CSV ファイルをローカルに保存するためのファイル名とパスの指定を、Performance Monitor から求められます。

  XML を選択すると、XML のエクスポートによって新しいブラウザ ウィンドウが開きます。このウィンドウから、表示された結果を保存できます。エクスポートしたレポートのローカル コピーを保存するには、[File] > [Save As] を選択します。

レポートの内容について、表 10-5 に示します。

ユーザ セッション レポートの形式

表 10-5　ユーザ セッション レポートの形式

エレメント	説明
[Username] カラム	1 人のユーザを検索し、一致したユーザ名が見つかった場合には、検索クエリーとして入力した認証済みのユーザ名が表示されます。 特定の期間におけるすべてのユーザのセッションを検索した場合は、[Username] カラムに、その期間のすべてのセッションに関連付けられている認証済みのすべてのユーザ名が含まれていることがあります。
[IP Address] カラム	対象のセッションに関連付けられているユーザの IP アドレスが表示されます。特定のユーザの IP アドレスは、特にダイナミック アドレッシングを使用しているネットワークでは、セッションによって変わることがあります。
[State] カラム	対象のユーザ セッションの最も新しいステータス（Active または Completed）が表示されます。
[VPN Device Name] カラム	対象のセッションが実行された（またはアクティブなセッションの場合は、実行している）VPN コンセントレータの DNS 名が表示されます。
[Start Time] カラム	対象のセッションが開始された日付と時間が、MM/DD/YYYY HH:MM:SS の形式で表示されます。
[End Time] カラム	対象のセッションが終了した日付と時間が、MM/DD/YYYY HH:MM:SS の形式で表示されます。 [End Time] の値が赤の場合は、正確な終了時刻が不明です。このような場合に表示された値は、Performance Monitor のポーリングでセッションがアクティブでなくなったと判断された時刻です。
[Duration] カラム	セッションの期間が、日、時間、分、および秒で表示されます。 正確な終了時刻がわからない場合は、[Duration] カラムの値が赤になります。このような場合に表示された値は、Performance Monitor のポーリングでセッションがアクティブでなくなったと判断された期間です。
[Last Verified] カラム	デバイスのポーリングで、対象のセッションに対して最後に情報を提供した時刻が、MM/DD/YYYY HH:MM:SS 形式で表示されます。
[Bytes In] カラム	ユーザが対象セッションでネットワークを介して受信した、トンネリングされたバイト数の合計数が表示されます。
[Bytes Out] カラム	ユーザが対象セッションでネットワークを介して送信した、トンネリングされたバイト数の合計数が表示されます。

サイト間 VPN の上位 10 トンネル レポートの表示

すべてのデバイス間で、ネットワーク内のサイト間 VPN の上位 10 トンネルの履歴レポートを表示できます。

手順

ステップ 1　[Reports] > [Site-to-Site] > [Top 10 Tunnels] を選択します。

デフォルトでは、[Top 10 Tunnels] ページに、スループット レベルが最も高いトンネルが 10 個表示され、最近 24 時間の時間ごとのデータ ポイントが示されます。対象の 24 時間で、スループットを測定できたトンネルが 10 個未満の場合は、10 個よりも少ない数が表示されます。

テーブルのカラムの説明については、表 10-6 を参照してください。

ステップ 2　必要な場合はレポート基準を修正し、[Go] をクリックして結果を確認してください。次のいずれかの方法で実行できます。

- トレンド タイプを変更します。次のいずれかを選択します。
  - [Hourly]：モニタされた値を 1 時間間隔で表示します。
  - [Daily]：モニタされた値を 1 日間隔で表示します。
  - [Weekly]：モニタされた値を 1 週間間隔で表示します。
  - [Monthly]：モニタされた値を 1 か月間隔で表示します。
- [From] フィールドと [To] フィールドに異なる日付を入力し、レポート日付の別の範囲を指定します。

参考

表 10-6　[Top 10 Tunnels] ページ

エレメント	説明
[Device Name] カラム	対象デバイスの DNS 名または IP アドレスが表示されます。
[Local Endpoint] カラム	トンネルが終了したローカル エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。 **（注）** Performance Monitor の内部で、「ローカル」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。
[Remote Endpoint] カラム	トンネルが終了したリモート エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。 **（注）** Performance Monitor の内部で、「リモート」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。
[Local Subnet] カラム [Remote Subnet] カラム [Protocol] カラム	次の 3 つのカラムの値は全体として、1 つのトンネルのアクセス リストを定義しています。 • [Local Subnet]：ローカル エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Remote Subnet]：リモート エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Protocol]：トンネル プロトコルおよび使用したポート（TCP 80 など）が表示されます。
[Throughput (Kbps)] カラム	トンネルの開始以降の、トンネルを介した受信および送信オクテットの合計（kbps）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

スケジュールされた E メール ジョブの操作

スケジュールされた E メール ジョブを表示および削除できます。Performance Monitor は、これらのジョブによって履歴レポートを配信します。

手順

ステップ 1　[Reports] > [Service Type] > [Scheduled Email Jobs] を選択します。[Service Type] は、オプション バーで選択するサービスです。

ステップ 2　リストから 1 つのジョブを選択します。

ステップ 3　次のいずれかを実行します。

- [Email Job Details] ウィンドウでジョブを表示するには、[View] をクリックします。
- ジョブを削除するには、[Delete] をクリックします。ジョブを削除すると、元に戻すことはできません。

参考

表 10-7　E メール ジョブ

エレメント	説明
[Job Name] カラム	ジョブの名前が表示されます。名前は次の要素で構成されます。 • CiscoWorks のユーザ名：Admin など。 • 特定のサービス タイプ：RAS など。 • [Schedule Email Report] ウィンドウの [Job Name] フィールドで入力した値。
[Recurring] カラム	次のいずれかが表示されます。 • [Yes]：ジョブが繰り返しスケジュールされます。 • [No]：ジョブは 1 回だけスケジュールされます。
[Next Schedule] カラム	繰り返しスケジュールされるジョブだけに、ジョブが次回実行される日付と時間が表示されます。
[Last Run Status] カラム	E メールが正常に送信されたか、配信に失敗したかを示すメッセージが表示されます。
[Last Run Time] カラム	スケジュールされていた対象の E メール ジョブが最後に実行された時刻が、MM/DD/YYYY HH:MM:SS 形式で表示されます。

関連トピック

- 「レポートの設定と生成」（P.10-7）
- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）