

# 分析ガイド

CA Application Delivery Analysis Multi-Port  
Monitor

バージョン 10.1



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により隨時、変更または撤回されることがあります。

CA の事前の書面による承諾を受ければ本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、

(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

## CAへの連絡先

テクニカルサポートの詳細については、弊社テクニカルサポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。



# 目次

---

<b>第 1 章: Multi-Port Monitor の概要</b>	<b>7</b>
<b>第 2 章: Web インターフェースにログインする方法</b>	<b>9</b>
<b>第 3 章: 分析の概要</b>	<b>11</b>
分析ページ.....	12
分析メニュー.....	13
事前定義済み分析.....	15
カスタム分析の作成.....	17
分析の複製.....	18
カスタム分析の削除.....	18
データ ビュー.....	19
<b>第 4 章: フィルタを使用した表示領域のデータのカスタマイズ</b>	<b>23</b>
現在のフィルタ条件の表示.....	26
分析フィルタ.....	26
分析フィルタの作成.....	27
分析フィルタのプロパティの変更.....	35
分析フィルタの削除.....	37
グローバルフィルタ.....	37
[グローバルフィルタ] ダイアログ ボックス.....	38
グローバルフィルタの変更.....	40
グローバルフィルタへの変更のクリア.....	41
<b>第 5 章: 表示領域のデータの理解</b>	<b>43</b>
グラフのタイプ.....	44
棒グラフ.....	45
トレンド折れ線グラフ.....	46
円グラフ.....	46
積み重ねトレンドグラフ.....	47
サマリ トレンドグラフ.....	47
データのタイプ.....	48

---

[トライフィック] タブ上のデータ .....	49
[TCP] タブ上のデータ .....	53
ネットワークとホストのバイト数 .....	59
データ テーブル内の列の追加または削除 .....	60
<b>第 6 章: データのエクスポート</b>	<b>61</b>
PDF ファイルへのデータのエクスポート .....	61
CSV ファイルへのデータのエクスポート .....	62
PCAP ファイルへのデータのエクスポート .....	63
電子メールによるデータの共有 .....	66
<b>付録 A: コマンド ライン構文</b>	<b>67</b>
<b>付録 B: 正規表現構文</b>	<b>69</b>

# 第 1 章: Multi-Port Monitor の概要

---

CA Application Delivery Analysis Multi-Port Monitor は、監視対象のデータセンターからセッション レベル パケットデータをキャプチャする強力なアプライアンスです。このアプライアンスでは、CA Application Delivery Analysis および CA Application Performance Management (CA APM) でレポートするためのデータをキャプチャします。

- TCP パケット ヘッダのデータは、CA Application Delivery Analysis がエンドツーエンドパフォーマンスを監視し、アプリケーション レスポンス時間を測定するのに役立ちます。
- 完全な HTTP パケットのデータは、CA APM がユーザ環境のトランザクションをマップしてエンドユーザ エクスペリエンスを監視し、サービス レベル アグリーメントを測定するのに役立ちます。

大量のデータセンター トラフィックを複数のポートからパッシブに監視することによって、Multi-Port Monitor はエンドツーエンドシステムパフォーマンスの連続的記録を保持するのを支援します。

監視対象のミラー ポートを通過するすべてのトラフィックからのパケット ヘッダが記録され、Multi-Port Monitor に短時間格納されます。1 分間のレポート間隔のデータは数日間保持され、分析に使用されます。メトリックは、レポート用に CA Application Delivery Analysis に、または CA APM でのレポート用に CA Transaction Impact Manager (CA TIM) に転送されます。

Multi-Port Monitor 分析のグラフおよびテーブルは、ホストごとのアクティビティおよびパフォーマンス データを表示します。分析は、セッション データ、ボリューム統計、およびレスポンス時間について複数のビューを提供します。また、トラブルシューティング用のワークフロー、データをエクスポートするための複数のオプション、およびフィルタ オプションを提供して、IT スタッフの問題診断および対応をサポートします。

Multi-Port Monitor にはその機能を監視するための機能があります。

- 論理ポートごとのハードウェアベース フィルタおよびパケットキャプチャ オプション。
- パフォーマンスを測定し、対象データのみをキャプチャするハードウェア フィルタ。
- 1つの Web ページから管理される複数のデータ フィード。
- SNMP トラップによる、データ監視またはキャプチャに影響する可能性があるエラーに関する自動通知送信。

Multi-Port Monitor には以下のコンポーネントが含まれます。

### アプライアンス

スイッチに出入りするトラフィックを監視するハードウェアおよびソフトウェア。以下の機能を実行します。

- パケットをキャプチャし、ストレージに書き込む。
- トラフィック統計を収集し、パフォーマンス情報用のパケットを分析する。
- ネットワーク、サーバ、およびアプリケーションのパフォーマンスに関する統計データを高パフォーマンス データベースに格納する。
- レポートと分析のために CA TIM または CA Application Delivery Analysis に統計データを送信する。

### Web インターフェース

ブラウザからアクセス可能な管理インターフェース。以下を実行できます。

- ドライブ、CPU、およびキャプチャ カードのステータスを含むアプライアンス統計を表示する。
- ポート定義、フィルタ オプション、安全なユーザ アカウントなどのシステム設定を構成する。
- キャプチャされたパケットに基づいており、フォーマットされたグラフまたはテーブルに表示されたパフォーマンス データを表示、フィルタ、およびソートする。
- ローカルに格納されたセッション レベルデータを [分析] タブ上で確認する。

# 第 2 章: Web インターフェースにログインする方法

---

データを分析するために Web インターフェースにログインします。

以下の手順に従います。

1. Web ブラウザで Web インターフェースにアクセスします。 ブラウザの [アドレス] フィールドに以下の構文を使用します。

`http://<ホスト名または IP アドレス>/`

Multi-Port Monitor の [ログイン] ページが開きます。

2. 割り当て済みのユーザ名およびパスワード（大文字と小文字を区別します）を使用してログインします。

Web インターフェースが開きます。



# 第3章: 分析の概要

---

分析は、Multi-Port Monitor アプライアンスに保存されているパケット レベル セッションデータへのトラブルシューティング パスの記述です。この記述は、データの一連の階層的に構成されたビューとして処理されます。

Multi-Port Monitor は 2 つのタイプの分析を提供します。

## 事前定義済み分析

CA Application Delivery Analysis レポートまたは CA APM の [障害詳細] ページからドリルインするときに使用される IPv4 ベースの TCP セッション レベル情報へのアクセスを提供します。

たとえば、CA Application Delivery Analysis コンポーネント レポートを検討し、192.94.5.6 ネットワークのデータを絞り込みます。[セッション分析] ボタンをクリックすると、選択したレポートの分析が Multi-Port Monitor [分析] ページに表示されます。選択したネットワークおよびタイムフレームによって、分析のセッション レベルデータがフィルタされます。

## カスタム分析

トラブルシューティング プロセスを迅速化するために、セッション レベル メトリックをフィルタし表示するためのオプションを提供します。Multi-Port Monitor ユーザはカスタム分析を作成、保存、再利用できます。

たとえば、CA Application Delivery Analysis からのドリルダウン (すなわちセッション分析) パスによって、状況に適用できない事前選択されたコンテキストに配置されます。分析を作成するか、保存された分析を開いて、目的のビューおよびその階層化された配置を選択する際のいくつかの手順を保存します。関連付けられたグラフおよびテーブルは、分析するデータに対して十分に絞り込んだ視点を提供します。

分析はすべて、 [分析] ページの表示領域の左側にある [分析] ペインに表示されます。

フィルタはビュー レベルで分析に追加され、同じ分析内のすべての下位ビューに適用されます。

新しい分析にはデフォルトデータ ビューが含まれません。新しい分析を適用する前に、データにビューを追加します。

このセクションには、以下のトピックが含まれています。

[分析ページ](#) (P. 12)

[分析メニュー](#) (P. 13)

[事前定義済み分析](#) (P. 15)

[カスタム分析の作成](#) (P. 17)

[分析の複製](#) (P. 18)

[カスタム分析の削除](#) (P. 18)

[データ ビュー](#) (P. 19)

## 分析ページ

セッション レベル ネットワーク データの詳細なビューは、Web インターフェースの [分析] ページに表示されます。 [分析] ページには 2 つのペインがあります。

### 表示領域

右側のペイン。グラフとデータ テーブルが表示されます。タブ付きビューにより、フォーマットされたパフォーマンス メトリックに容易にアクセスできます。グラフとテーブルは、異常値を検索するためにデータを表示し、グラフ形式を選択し、メトリックを並べ替えるための複数のオプションを提供します。

**注:** Multi-Port Monitor は 1 分単位の精度でデータをレポートしますが、パフォーマンス上の理由により収集したメトリックを 2 分間隔でデータベースにロードします。表示領域に最新の収集されたデータを表示する場合、この違いにより遅延が発生します。

### [分析]ペイン

左側のペイン。データ ビューを選択し、表示領域に表示されるデータをフィルタするオプションが表示されます。データ ビューの分析フィルタを作成でき、再使用可能なトラブルシューティング ワークフローとしてそれらを保存できます。アクティブ フィルタのリストが[分析]ペインの一番上に表示されます。プライマリ フィルタのタイプは以下のとおりです。

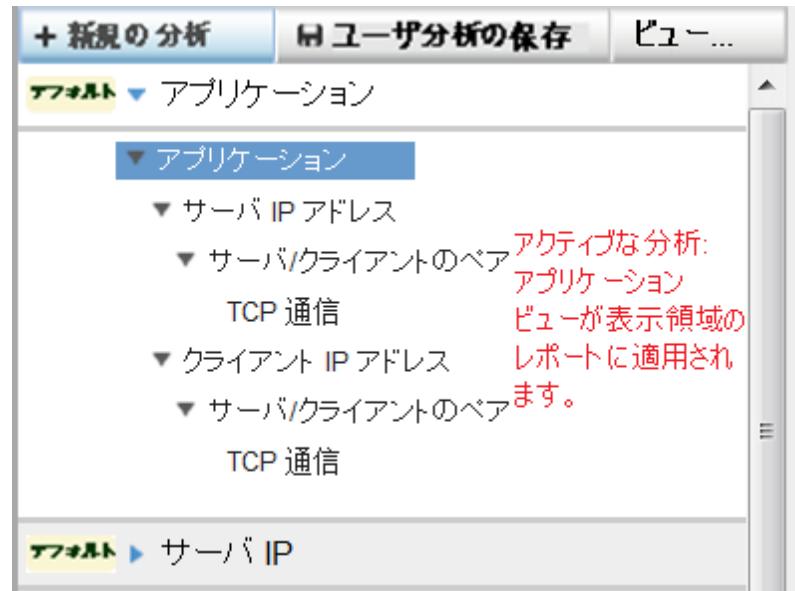
- [分析フィルタ](#) (P. 26)は、[分析フィルタの追加] をクリックするとデータに明示的に適用されます。表示領域のアイテムをダブルクリックすると、暗黙的に作成されます。
- [グローバル フィルタ](#) (P. 37)は、すべての分析に適用され、CA Application Delivery Analysis からのドリルダウン コンテキストに基づいています。

## 分析メニュー

分析を表示、作成、および変更するために分析メニューを使用します。デフォルトでは、メニューは[分析] ページの[分析] ペインに表示されます。メニューを非表示にして、グラフとテーブルに利用可能な表示画面を拡張できます。

[分析] ペインを非表示または表示するには、([分析メニュー] というラベルが付いた) [<<] または [>>] 記号をクリックします。

[分析] ペイン内では、アクティブな分析は青色に白いテキストで強調表示されます。アクティブな分析とそのフィルタは、表示領域内に表示できるレポートに適用されます。



アクティブな分析の子ビューは、さらに詳細なレベルまでレポートするために利用でき、一部の分析では TCP 通信レベルまで利用可能です。関連するフィルタは、表示領域に表示されるメトリックに特定のセッションを含むか除外するように設計されています。

関連付けられたビューを表示するには、分析を展開します。分析を展開するか折り畳むには、分析名の横の青い矢印をクリックします。アクティブな分析を折り畳んだり展開したりしても、フィルタは削除も追加もされません。

現在のタイムフレームに別のビューを適用して、別のコンテキストでデータを参照できます。別の分析を適用するには、[分析] ペインで展開して関連付けられたビューをクリックします。

## 事前定義済み分析

事前定義済み分析は、データの分析に役立つ並べ替えおよび表示オプションです。 [分析] メニューで「デフォルト」として指定されています。

分析フィルタの追加により、事前定義済み分析を一時的にカスタマイズできます。これらの変更は保存できません。現在のログインセッションでのみ保持されます。

分析はすべて高い詳細レベルまでデータをマイニングします。データのビューはそれぞれ事前定義済み分析と関連付けられます。分析を選択すると、階層構造内のビューのリストを表示するために展開されます。この構造は、監視対象のデータからアクセスできる高い詳細レベルを表します。ビューはそれぞれ、選択したタイムフレームのデータベースに格納されたより詳細なメトリックへのアクセスを提供します。

分析は、特定のアイテムの調査を支援することによりトラブルシューティング作業に役立ちます。分析では、初期データビューを調査中のアイテムに対応するものとして見なすと便利です。たとえば、クライアントIPアドレス分析は、IPアドレスがわかっているクライアントコンピュータで問題の原因を見つけるのに役立ちます。まず、クライアントビューが適用されます。クライアントをダブルクリックして、分析の次のビューにドリルダウンします。そのクライアントと通信したサーバがすべて表示されます。

Multi-Port Monitor は以下の事前定義済み分析を提供します。

### アプリケーション

問題があるアプリケーションを識別するために、この分析を使用します。この分析は、アプリケーションが実行されているサーバのIPアドレスおよびアプリケーションが使用するポート番号を識別します。以下のデータビューが含まれています。

サーバIPアドレス --> サーバ/クライアントのペア --> TCP通信

クライアントIPアドレス --> サーバ/クライアントのペア --> TCP通信

### サーバIPまたはクライアントIP

問題がある单一ホストを識別するために、この分析を使用します。以下のデータビューが含まれています。

サーバIPアドレス --> サーバ/クライアントのペア --> TCP通信

クライアントIPアドレス --> サーバ/クライアントのペア --> TCP通信

### ネットワーク

サブネット上の複数のホストの問題を識別するために、この分析を使用します。以下のデータ ビューが含まれています。

サーバ IP アドレス --> サーバ/クライアントのペア --> TCP 通信

クライアント IP アドレス --> サーバ/クライアントのペア --> TCP 通信

### IP Address

問題がある単一ホストを識別するために、この分析を使用します。以下のデータ ビューが含まれています。データ ビューはキャプチャされたデータの複数の可能なフィルタ パスに構成されています。

サーバ IP アドレス --> サーバ/クライアントのペア --> TCP 通信

クライアント IP アドレス --> サーバ/クライアントのペア --> TCP 通信

IP アドレス ペア --> IP セッション

### Protocol

単一のプロトコルを使用するトライフィックの問題を識別するために、この分析を使用します。以下のデータ ビューが含まれています。

IP アドレス --> IP アドレス ペア --> IP セッション

## カスタム分析の作成

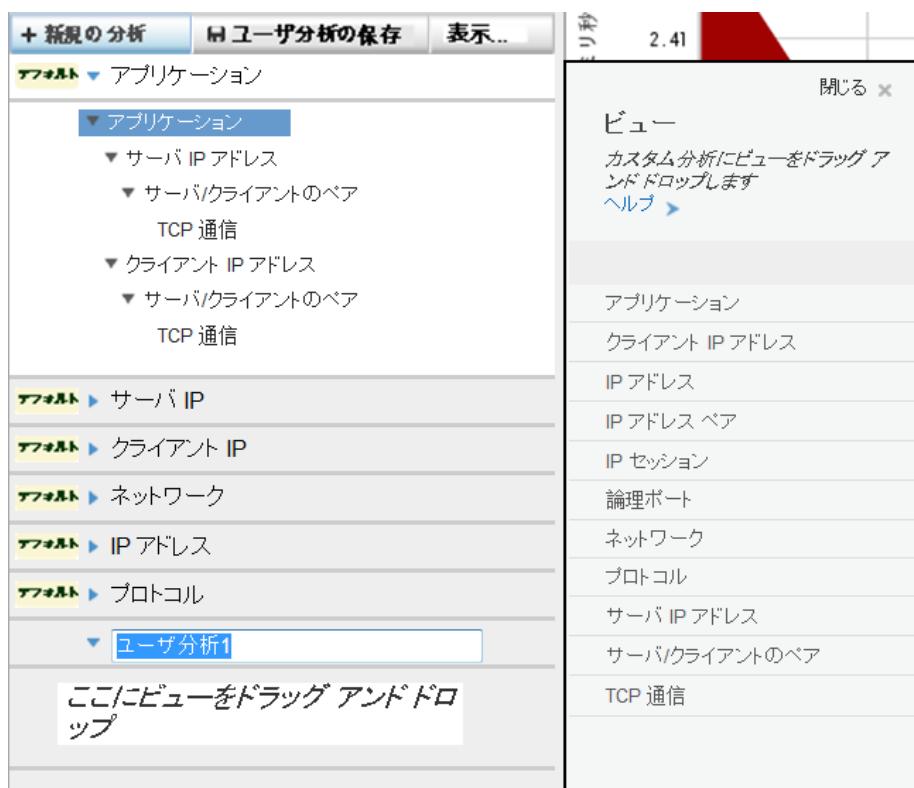
事前定義済み分析は永久的に変更することはできません。フィルタまたは分析ワークフローを保存するには、カスタム分析を作成します。

次の手順に従ってください:

1. [分析] ペインの [新規の分析] をクリックします。

新しいアイテムが [分析] ペインに表示されます。デフォルトの名前 (My Analysis 1) が強調表示されます。

[ビュー] ペインが [分析] ペインの右に表示されます。



2. 強調表示されたフィールドに新しい分析の名前を入力します。
3. [ビュー] ペインのカスタム分析に追加するビューを選択します。
4. [分析] ペインの [ここにビューをドラッグ アンド ドロップ] セクションにビューをドラッグします。
5. 手順 3 および 4 を繰り返して、分析にデータ ビューを追加します。ビューを高精度の階層フローに追加し、ビューが下位になると追加アイテムがフィルタで除外されるようにすることを推奨します。

6. (オプション) 高度なフィルタを追加します。ビューを右クリックし、[分析フィルタの追加] を選択します。

[分析フィルタの追加] ダイアログボックスが表示されます。フィールドの説明については、「[データ ビューのフィルタ \(P. 27\)](#)」を参照してください。

7. [ユーザ分析の保存] をクリックします。

カスタム分析が保存されます。複数の変更を同時に保存できます。

**重要:** 電子メールで送信された分析を表示している場合、[ユーザ分析の保存] をクリックすると保存された分析がすべて上書きされます。

## 分析の複製

カスタムおよび事前定義済み分析を複製できます。複製機能を使用して、分析に対する変更を保存できます。

次の手順に従ってください:

1. [分析] ペインで、複製する分析を右クリックします。
2. [複製] を選択します。

新しい分析が「My Analysis #」という命名規則で [分析] ペインに表示されます。

3. 複製された分析の新しい名前を入力します。

## カスタム分析の削除

カスタム分析を削除できます。事前定義済み分析は削除できません。

次の手順に従ってください:

1. [分析] ペインで、削除する分析の名前を右クリックします。
2. [分析の削除] を選択します。
3. 確認メッセージの [OK] をクリックします。

分析が [分析] ペインから削除されます。

## データビュー

データビューは、ネットワークパフォーマンスの領域を調査するのに役立ちます。事前定義済み分析にはデータビューが含まれます。独自のビューセットを持つカスタム分析を作成し、変更できます。

分析を作成すると、[ビュー]メニューが自動的に表示されます。また、[ビュー]ボタンをクリックして利用可能なデータビューのリストを参照することもできます。

以下のアイテムを使用してデータビューをカスタマイズできます。

- フィルタ（対象のトラフィックに焦点を当てる）。
- グラフ形式（対象のパフォーマンスマトリックをグラフで表示する）。
- データテーブル設定（対象のメトリックを選択的に表示する）。各ビューについて、デフォルトの並べ替え方法が適用されます。たとえば、プロトコル分析ではプロトコルは最も高いバイトレートから最も低いバイトレートに並べ替えられます。

データビューをカスタマイズできます。グラフ形式の変更など、一部の変更はビューに自動的に保存されます。

### アプリケーション

アプリケーションごとのレスポンス時間（トランザクション時間（ミリ秒））を強調表示します。アプリケーション名は CA Application Delivery Analysis 設定または既知のポート使用状況から取得されます。可能な場合は、アプリケーション名が表示されます。それ以外の場合は、ポート番号が表示されます。

デフォルトグラフは、レスポンス時間とその構成における傾向を表示します。トランザクション時間は、ネットワークラウンドトリップ時間、再送信、データ転送時間、およびサーバレスポンス時間に細分化されます。

### クライアント IP アドレス

クライアントごとのレスポンス時間（トランザクション時間（ミリ秒））を強調表示します。Multi-Port Monitor は、TCP 通信を開始する 3 方向ハンドシェークからクライアントコンピュータを識別します。グラフは、レスポンス時間とその構成における傾向を表示します。

### IP Address

([トライフィック] タブ) ホストの IP アドレスごとのスループット (バイト レート (ビット/秒) ) を最も高いバイト レートから最も低いバイト レートに並べ替えて強調表示します。グラフは、最も高いレートのホストへの、およびホストからの方向性のあるバイト レートを表示します。

### IP アドレス ペア

([トライフィック] タブ) ホスト IP アドレスの対話するペアごとのスループット (バイト レート (ビット/秒) ) を最も高いバイト レートから最も低いバイト レートに並べ替えて強調表示します。グラフは、最も高いレートのホストのペアへの、およびホストのペアからの方向性のあるバイト レートを表示します。

### IP セッション

([トライフィック] タブ) セッションごとのスループット (バイト レート (ビット/秒) ) を強調表示します。セッションはそれぞれホスト IP アドレスの対話するペアを表します。セッションは、最も高いバイト レートから最も低いバイト レートに並べ替えられます。グラフは、最も高いスループットの上位 10 個のセッションへの、およびセッションからのバイト レートの構成を表示します。

### 論理ポート

Multi-Port Monitor に到達する、論理ポートごと、すなわちスイッチ ミラー ポート セッションごとのレスポンス時間を強調表示します。グラフは、レスポンス時間 (バイト レートとして) における傾向を表示します。

### ネットワーク

ネットワークごとのレスポンス時間 (トランザクション時間 (ミリ秒) ) を強調表示します。ネットワークは CA Application Delivery Analysis 設定に基づいて識別されます。グラフは、レスポンス時間とその構成における傾向を表示します。

### Protocol

([トライフィック] タブ) ハードウェア フィルタを通過する各プロトコルのスループット (バイト レート (ビット/秒) ) を強調表示します。送受信されたバイトの総数および TCP バイトの数が表示されます。レイヤ 3 プロトコルも示されます。グラフは、一定期間のスループットの傾向 (バイト レートとして) を表示します。

### サーバ IP アドレス

サーバごとのレスポンス時間（サーバ レスポンス時間（ミリ秒））を強調表示します。グラフは、レスポンス時間とその構成における傾向を表示します。

### サーバ/クライアントのペア

ペアのホスト（クライアントとサーバ）ごとのレスポンス時間（トランザクション時間（ミリ秒））を強調表示します。グラフは、レスポンス時間とその構成における傾向を表示します。

### TCP 通信

セッションごとのレスポンス時間（トランザクション時間（ミリ秒））を強調表示します。セッションはそれぞれ、サーバホストとクライアントホストおよびポートで構成されます。グラフは、レスポンス時間とその構成における傾向を表示します。

#### 詳細:

[分析フィルタの作成 \(P. 27\)](#)

[現在のフィルタ条件の表示 \(P. 26\)](#)



# 第4章: フィルタを使用した表示領域のデータのカスタマイズ

---

Multi-Port Monitor は、[分析] ページの表示領域に表示されるセッション レベルメトリックの範囲を絞り込むいくつかの方法を提供します。以下のオプションは、選択した分析から表示されたデータに適用できます。

## データビュー

別のデータ ビューを選択して、現在のトラブルシューティング タスクに最も有用なネットワーク面に焦点を当てるすることができます。たとえば、アプリケーションのレスポンス時間が遅い場合は、[サーバ IP] ビューまたは [アプリケーション] ビューを選択し、関連付けられたメトリックを参照します。

ビュー内のデータをフィルタするには、[分析フィルタ](#) (P. 26)を使用します。

注: 分析フィルタは、キャプチャされたデータに適用するハードウェア フィルタとは異なります。ハードウェア フィルタは、データのキャプチャに影響します。分析フィルタは、データの表示に影響します。

## 特定コンテキスト フィルタリング

- データテーブル内の行または一連の行を選択します。右クリックして [フィルタとして適用] を選択し、現在の分析のデータの範囲を絞り込みます。複数行を強調表示するには、Ctrl キー+クリックまたは Shift キー+クリックを使用します。
- グラフの特定のセクションを選択するには、マウス ポインタを使用します。マウス ポインタを放し、[設定] をクリックします。グラフが更新されて、基準メトリックの例外を示す折れ線グラフの山など、絞り込まれたセグメントに焦点が当てられます。

### ドリルダウン フィルタリング

- データ テーブル内の行をダブルクリックして、分析の次のビューまで 1 レベル ドリルダウンします。
- APM 障害からドリルダウンして [分析] ページで関連付けられたデータを表示します。分析 フィルタは、障害のコンテキストに基づいて自動的に作成されます。
- CA Application Delivery Analysis レポートの [セッション分析] をクリックして、[分析] ページに関連付けられたデータを表示します。[分析] ページの [グローバル フィルタ](#) (P. 37) は CA Application Delivery Analysis レポートのコンテキストに基づいています。

### ズーム フィルタリング

折れ線グラフは、追加のフィルタ オプションを提供します。[ズーム イン] および [ズーム アウト] リンクにより、キャプチャされたデータのより小さいセグメントからパフォーマンス メトリックに詳細に焦点を当てることができます。

- [ズーム イン] は、データのより小さいセグメントがグラフに表示されるように現在のタイムフレームを縮小します。
- [ズーム アウト] は、タイムフレームを元に戻してデータのセグメントを広げます。

## タイムフレーム フィルタリング

〔サマリトレンド〕グラフ、〔トレンド折れ線〕グラフ、および〔積み重ねトレンド〕グラフの形式には、表示領域の上の時間ナビゲーションコンポーネントが含まれます。デフォルトのタイムフレームは 15 分です。期間セレクタでは、別のタイムフレームを正確に選択できます。

- 〔戻る〕と〔進む〕のボタンを使用して、キャプチャされたデータの時間を進めたり、さかのぼったりすることができます。この種の時間ナビゲーションでは、傾向データを表示し、各傾向が進むとその傾向を追跡できます。
- 日付、時間、および分は、他の日時パラメータを選択できるメニューです。
- 日付は、前方および後方に移動できるグラフィカルなカレンダーメニューです。
- 〔タイムフレーム〕リンクによって、「最後の 15 分」から「最後の 180 分」までより大きな時間セグメントにすばやくアクセスできます。

このセクションには、以下のトピックが含まれています。

[現在のフィルタ条件の表示 \(P. 26\)](#)

[分析フィルタ \(P. 26\)](#)

[グローバル フィルタ \(P. 37\)](#)

## 現在のフィルタ条件の表示

分析に適用されるフィルタに関する情報を表示するためのいくつかのオプションがあります。

- 以下の情報を参照するには、[分析] ペインまたは表示領域内の [フィルタの表示] リンクをクリックします。
  - CA Application Delivery Analysis レポートから継承されたすべてのグローバル フィルタのリスト。
  - 現在のデータ ビューに適用された分析フィルタのリスト。
- 分析では、フィルタされたデータ ビュー上にマウス ポインタを置きます。 フライオーバーテキストは、フィルタの条件および構文について説明します。
- 分析では、データ ビューを右クリックし、[分析フィルタの編集] を選択します。 [分析フィルタの編集] ダイアログ ボックスの [条件] フィールドでは、フィルタの条件および構文を識別します。
- 分析で、フィルタアイコンをクリックします。 [条件] フィールドでは、フィルタの条件および構文を識別します。

## 分析フィルタ

表示領域のデータを制限するためにデータ ビューに正規表現を適用できます。 この種のフィルタリングが分析フィルタです。

正規表現フィルタは、アクティブな分析のコンポーネントであるデータ ビューに直接適用されます。 分析カスタマイズの一部としてフィルタのみを保存できます。

## 分析フィルタの作成

表示領域のデータを制限するためにデータ ビューに正規表現を適用できます。この種のフィルタリングが分析フィルタです。

正規表現フィルタは、アクティブな分析のコンポーネントであるデータ ビューに直接適用されます。分析カスタマイズの一部としてフィルタのみを保存できます。

データ ビューに分析フィルタを追加すると、新規フィルタおよびすべての継承されたフィルタがビューに適用されます。[分析フィルタの追加] ダイアログ ボックスで継承されたフィルタを参照できます。

**注:** 新規フィルタは継承されたグローバル フィルタを変更しません。代わりに、グローバル フィルタを通過したデータに追加 フィルタを提供します。

次の手順に従ってください:

1. 分析内のビューを右クリックし、[分析フィルタの追加] を選択します。  
[分析フィルタの追加] ダイアログ ボックスが表示されます。同じ分析の別のビューから継承されたフィルタは、[継承された分析フィルタ] フィールドで示されます。
2. [パラメータ] フィールドからフィルタを選択します。各アイテムをクリックすると、[値] の適切な構文が含まれたヘルプが表示されます。
3. 演算子を選択します。
  - 等価 (=)
  - 不等価 (!=)
4. 値を入力して式を完成させます。ガイダンスについては、構文オンライン ヘルプを使用してください。

**注:** [値] フィールドに特定の式を使用するとフィルタは実質的に無効になります。「[予約済みフィルタ式 \(P. 29\)](#)」リストの式を使用しないでください。

5. [条件に追加] をクリックします。

フィルタステートメントが [条件] フィールドに表示されます。

**注:** フィルタステートメントを削除するには、[条件] フィールドの上の [クリア] をクリックします。また、[条件] フィールドに入力することによりステートメントを編集できます。

6. (オプション) ブール演算子を選択し、手順 3 ~ 5 を繰り返して、既存のフィルタステートメントと関連付けながら条件を追加します。

- AND (連結)
- OR (代替)

7. [OK] をクリックします。

フィルタが検証されます。有効な場合、表示領域のデータテーブルおよびグラフに適用されます。分析フィルタリングが適用されることを示すフィルタアイコンが [分析] ペインのビュー名の横に表示されます。

詳細情報:

[カスタム分析の作成 \(P. 17\)](#)

## 予約済みフィルタ式

以下のフィルタ式は予約済みです。 [分析フィルタの追加] ダイアログボックスの [値] フィールドに、これらの大文字と小文字を区別する式を使用しないでください。

ApplicationName、ApplicationTypeID、ApplicationNameTypeID  
ClientNetworkName、ClientNetwork  
HostName、Host  
L4Port  
LogicalPortName、LogicalPort  
L3ProtocolName、L3ProtocolNumber、L4ProtocolName、L4ProtocolNumber、  
L34ProtocolName、L34ProtocolNumber  
MAC  
NetworkName、Network  
PairName、Pair  
ServerName、Server  
SessionID、ToS、VLAN

パラメータに予約済みの式および「=」または「!=」が含まれる場合、分析フィルタ機能ではクエリの構文を作成できません。予約済みの式を使用する場合、リスト内で指定されている大文字/小文字とは異なる大文字/小文字を使用します。

## [パラメータ]フィールドと関連付けられた値

以下の表では、 [パラメータ] フィールドで選択したアイテムに基づいて変更される、 [値] フィールドの構文を説明します。

### アプリケーション名

アプリケーション名のフィルタ。表示領域のアプリケーション名は CA Application Delivery Analysis 設定または既知のポート使用状況から取得されます。名前または名前のカンマ区切りリストを入力します。ワイルドカードが使用できます。例：

Secure HTTP\*  
Secure HTTP (443)

### アプリケーション名/タイプ/ID

アプリケーション名、タイプ、および ID 番号を表す 3 つの値のフィルタ。[アプリケーション名]、[アプリケーションタイプ]、および [アプリケーション ID] 列が [列の編集] ダイアログボックスで有効な場合に、これらの値を表示できます。「名前/タイプ/ID」としてこの 3 つを指定します。例：

MySQL (3306)/Monitored/3

注：[アプリケーションタイプ/ID] および [アプリケーション名/タイプ/ID] パラメータには、内部的に割り当てられた値が必要です。右クリックメニューを使用してデータテーブルから直接その値を適用します。

### アプリケーション タイプ/ID

アプリケーションタイプ、および ID 番号を表す 2 つの値のフィルタ。[アプリケーションタイプ] および [アプリケーション ID] 列が [列の編集] ダイアログボックスで有効な場合に、これらの値を利用できます。「タイプ/ID」としてペアを指定します。例：

Monitored/10

### クライアント ネットワーク

クライアントネットワーク サブネットの IP アドレス、またはサブネットの IP アドレスのカンマ区切りリストのフィルタ。マスクをアドレスと区別するためにスラッシュ (/) を使用します。例：

192.3.45.0/24  
192.3.45.0/24,192.3.46.0/24,192.3.50.0/24

### クライアント ネットワーク名

CA Application Delivery Analysis で監視するために定義されたクライアントネットワークの名前、またはネットワークのカンマ区切りリストのフィルタ。

## ホスト

IP アドレスのフィルタ。以下の形式の任意の組み合わせで表されたデフォルトフィルタ パラメータです。

- 1 つの IP アドレス
- IP アドレスの範囲
- IP アドレスのカンマ区切りリスト
- アドレス範囲のカンマ区切りリスト

アドレス範囲にはハイフンを使用し、スペースは使用しません。例：

198.168.0.1, 198.165.0.1-198.165.1.255

## ホスト名

クライアントまたはサーバの DNS ホスト名のフィルタ。DNS ホスト名またはホスト名のカンマ区切りリストを入力します。ワイルドカード (\*) がサポートされています。このパラメータがデフォルトです。例：

exchangeserver1, \*noc\*, database\*

## レイヤ 3 プロトコル名

ネットワーク レイヤプロトコルのフィルタ。レイヤ 3 プロトコルの名前または名前のカンマ区切りリストを入力します。例：

IP

## レイヤ 3 プロトコル番号

ネットワーク レイヤプロトコルのフィルタ。レイヤ 3 プロトコルの 10 進数のレジストリ番号、またはレジストリのカンマ区切りリストを入力します。

## レイヤ 3/レイヤ 4 プロトコル名

レイヤ 3 および 4 からのプロトコルのペアのフィルタ。ペアのプロトコル名またはペアの名前のリストを入力します。ペアを区切るためにスラッシュ (/) を使用します。例：

IP/TCP

## レイヤ 3/レイヤ 4 プロトコル ペア

レイヤ 3 および 4 からのプロトコルのペアのフィルタ。プロトコル レジストリ番号のペア、または番号のペアのリストを入力します。ペアを区切るためにスラッシュ (/) を使用します。たとえば、IP/TCP の場合は次のようにになります。

2048/6

### レイヤ 4 ポート

トランスポート層のポート番号用のフィルタ。ポート番号、またはポート番号のカンマ区切りのリストを入力します。たとえば、**HTTPS** の場合は次のようにになります。

443

### レイヤ 4 プロトコル名

トランスポート層のプロトコル用のフィルタ。レイヤ 4 プロトコルの名前、または名前のカンマ区切りのリストを入力します。

### レイヤ 4 プロトコル番号

トランスポート層のプロトコル用のフィルタ。レイヤ 4 プロトコルの 10 進数のレジストリ番号、またはレジストリのカンマ区切りのリストを入力します。

### 論理ポート

論理ポート番号用のフィルタ。論理ポート番号、または番号のカンマ区切りのリストを入力します。このパラメータを使用すると、特定のソースからミラーリングされたデータのみを表示できます。

### 論理ポート名

Multi-Port Monitor アプライアンスに対して定義した論理ポート名用のフィルタ。論理ポート名、または名前のカンマ区切りのリストを入力します。

### MAC Address

MAC アドレス、または MAC アドレスのカンマ区切りのリスト用のフィルタ。例：

00:19:2f:aa:bb:cc

### ネットワーク名

CA Application Delivery Analysis ネットワーク名用のフィルタ。CA Application Delivery Analysis [環境管理] でネットワークを設定する場合は、それぞれの名前を指定できます。このフィールドにネットワーク名、または名前のカンマ区切りのリストを入力します。

## ネットワーク

ネットワーク サブネット用のフィルタ。ネットワーク サブネットの IP アドレス、またはサブネットのカンマ区切りのリストを入力します。マスクをアドレスと区別するためにスラッシュ (/) を使用します。例：

192.3.45.0/24  
192.3.45.0/24,192.3.46.0/24,192.3.50.0/24

## ペア

IP アドレスによる通信ホストのペア用のフィルタ。IP アドレスのペア、または IP アドレスのペアのカンマ区切りのリストを入力します。アドレスのペアの間にはスラッシュ (/) を使用します。例：

198.168.0.1/198.168.0.18

## ペア名

DNS ホスト名による通信ホストのペア用のフィルタ。ホスト名のペア、または値のペアのカンマ区切りのリストを入力します。ホスト名のペアの間にはスラッシュ (/) を使用します。例：

MyServer1/MyClient1

## サーバ

サーバ IP アドレス用のフィルタ。サーバの IP アドレス、またはアドレスのカンマ区切りのリストを入力します。ドット区切り表記を使用します。例：

192.3.45.0

## サーバ名

サーバホスト名用のフィルタ。ホスト名、またはホスト名のカンマ区切りのリストを入力します。

## セッション ID

TCP セッション ID 番号用のフィルタ。セッション ID 番号、または ID 番号のカンマ区切りのリストを入力します。

セッション ID は、[列の編集] ダイアログ ボックスで [セッション ID] 列が有効になっているときに使用可能な内部の識別子です。

### ToS

サービスのタイプのビット設定用のフィルタ。ToS 設定 (10 進数形式)、または設定のカンマ区切りのリストを入力します。以下の 0100 の例では、スループットを最大化します。

4

### VLAN 番号

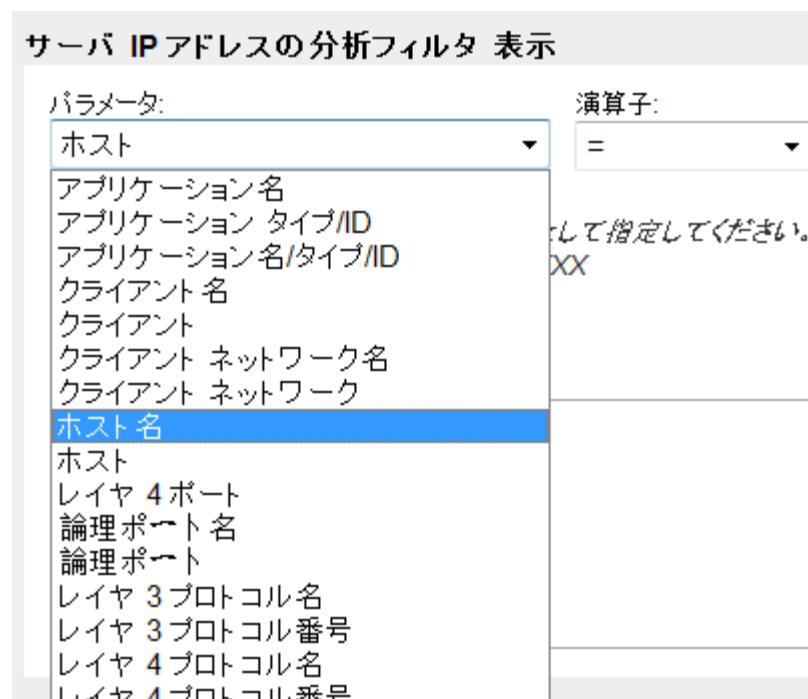
仮想 LAN ID 番号用のフィルタ。VLAN ID 番号、または番号のカンマ区切りのリストを入力します。

詳細:

[データ テーブル内の列の追加または削除 \(P. 60\)](#)

## フィルタでのデータベースのクエリ方法

一部の分析フィルタは、[分析フィルタの追加] ダイアログ ボックス内のペアになったセットです。たとえば、[ホスト] (IP アドレス) または [ホスト名] でフィルタできます。



有効なグラフを作成するために、これらのフィルタ パラメータはインテリジェントに適用されます。たとえば、[クライアント IP アドレス] ビューの [TCP] タブでデータをフィルタするには、[ホスト] パラメータを選択します。このデータには、フィルタ値に一致するクライアント アドレスのみが表示されます。次に、[サーバ IP アドレス] ビューと同じ [ホスト] フィルタを適用します。このデータには、値に一致するサーバアドレスのみが表示されます。

一部のデータ ビューでは、この方法で表示が制限されません。[プロトコル] および [アプリケーション] ビューでは、クライアントおよびサーバでフィルタします。[トライフィック] タブでは一般に、適用されるフィルタが少なくなります。

[ネットワーク] データ ビューや [ネットワーク] 分析フィルタでは、必ずしも CA Application Delivery Analysis で定義されているすべてのネットワークが検索されるとは限りません。CA Application Delivery Analysis はネットワークをクライアントまたはサーバネットワークのいずれかとして分類します。この分類は、キャプチャされたトランザクション内でこれらのホストが果たす役割に基づいています。ネットワークアドレスまたはネットワーク名の値と照合される [ネットワーク] および [ネットワーク名] フィルタは、デフォルトでクライアントネットワークに対して照合されます。ただし、選択されたデータ ビューやタブに基づく別のデータベース クエリも発行されます。

- [ネットワーク] ビューと [TCP] タブが選択されている場合は、値の照合のためにクライアントネットワークのみがクエリされます。
- [サーバ IP] ビューが選択されている場合は、サーバネットワークの照合のために [ネットワーク] および [ネットワーク名] 分析フィルタのみがクエリを送信します。

## 分析フィルタのプロパティの変更

データ ビューに適用される分析フィルタを変更できます。以下の詳細な手順を使用して、[分析] メニューからフィルタを変更できます。または、データ テーブルで右クリックのオプションを使用して、親のフィルタを変更できます。親のフィルタを変更すると、子のビューに適用されている分析フィルタがすべて上書きされます。

次の手順に従ってください:

1. 変更するフィルタを見つけます。フィルタ アイコン (F) によって、アクティブなフィルタが識別されます。

2. フィルタを右クリックし、[分析フィルタの編集] を選択します。

[分析フィルタの編集] ダイアログボックスでは、アクティブなフィルタが [条件] フィールド内に識別されます。[継承された分析フィルタ] フィールドには、同じ分析内の別のビューから継承されたフィルタが表示されます。

**注:** 分析内では、フィルタの継承が、前のビューから同じ分析内の以降のすべてのビューに下向きに続行されます。

3. 既存のフィルタステートメントに関係する条件を追加するには、[布尔値] 演算子を選択します。

- AND (連結)
- OR (代替)

4. [パラメータ] フィールドからフィルタを選択します。各項目をクリックすると、[値] フィールドの適切な構文が含まれたヘルプが表示されます。

5. 演算子を選択します。

- 等価 (=)
- 不等価 (!=)

6. 値を入力して式を完成させます。ガイダンスについては、構文オンラインヘルプを使用してください。

**注:** 特定の式は、[値] フィールドに指定したときにフィルタを無効にします。[予約済みフィルタ式 (P. 29)] リストの式を使用しないでください。

7. [条件に追加] をクリックします。

フィルタステートメントが [条件] フィールドに表示されます。

**注:** ステートメントを削除するには、[条件] フィールドの上の [クリア] をクリックします。また、[条件] フィールドに入力することによりステートメントを編集できます。

8. [OK] をクリックします。

変更されたフィルタが検証されます。有効な場合、このフィルタは表示領域内のデータ テーブルとグラフに適用されます。

#### 詳細情報:

[予約済みフィルタ式 \(P. 29\)](#)

[\[パラメータ\] フィールドと関連付けられた値 \(P. 29\)](#)

## 分析フィルタの削除

データ ビューに適用される分析フィルタを削除できます。現在のフィルタ条件を確認するには、マウス ポインタを使用してフィルタをポイントします。分析のための1つのフィルタまたはすべてのフィルタを削除できます。

次の手順に従ってください:

1. 削除するフィルタを見つけます。フィルタアイコン (▼) によって、フィルタが識別されます。

2. 1つのフィルタを削除するには、フィルタされたビューを右クリックし、[分析フィルタを削除] を選択します。

表示領域内のテーブルとグラフが、フィルタで除外されたデータを含むように更新されます。

3. すべてのフィルタを削除するには、分析の名前を右クリックし、[すべてのファイルを削除] を選択します。

表示領域内のテーブルとグラフが、フィルタで除外されたデータを含むように更新されます。

## グローバル フィルタ

グローバル フィルタは、セッション分析を開始したときに有効であった CA Application Delivery Analysis レポート コンテキストから継承されます。各グローバル フィルタ 設定はコンテキストを示します。

アクティブなグローバル フィルタのリストが [分析] ペインの一番上に表示されます。[ドメイン]、[アプリケーション]、[サーバ]、および [ネットワーク] グローバル フィルタが最初に表示され、次に、セッション分析の手順中に選択された [論理ポート] が表示されます。

Multi-Port Monitor データベースへのクエリによって、データがフィルタされます。これらのクエリは、フィルタのタイプや選択されたデータ ビューによって異なり、返されるデータを最適化するために選択されます。

- [ドメイン] グローバル フィルタは、指定されたドメインに重点を置いています。使用可能なドメインのリストは、CA Performance Center でユーザに割り当てられる ドメイン グループに基づきます。
- [サーバ] グローバル フィルタは、指定されたサーバに重点を置いています。
- [ネットワーク] グローバル フィルタは、そのネットワーク内の クラウド アントに重点を置いています。

グローバル フィルタは、表示領域に表示されるデータを制限するように変更できます。また、グローバル フィルタをクリアしてデフォルト設定に戻すこともできます。

### [グローバル フィルタ] ダイアログ ボックス

[グローバル フィルタ] ダイアログ ボックスには、以下の情報が表示されます。

#### ドメイン タブ

- 名前。ドメインの名前（ドメインが定義される場合）。使用可能なドメインのリストは、CA Performance Center でユーザに割り当てられる ドメイン グループに基づきます。

#### [アプリケーション] タブ

- 名前。アプリケーションの名前（使用可能な場合）。ポート番号が括弧内に表示されます。
- アプリケーション タイプ/ID。アプリケーション識別子。通常、アプリケーション タイプおよびその ID 番号を表す 2 つの値。各ペアによって、Multi-Port Monitor データベース内のアプリケーションが識別されます。

### [サーバ]タブ

[サーバ] タブには、ホストのリストが含まれています。監視対象トランザクションにおけるサーバの役割から、ホストとして識別されます。Multi-Port Monitor は、キャプチャされた通信データ内でサーバとクライアントを区別できます。

- 名前。 CA Application Delivery Analysis で設定されたサーバの名前（通常は、DNS ホスト名）。
- IP アドレス。サーバの IP アドレス。

### [ネットワーク]タブ

[ネットワーク] タブは、クライアントネットワークを識別します。CA Application Delivery Analysis でのネットワークの概念は、クライアント領域の監視と、それらの領域からのクライアント/サーバトランザクションの観測に基づいています。

- 名前。 CA Application Delivery Analysis で定義されたネットワークの名前。ネットワークは、CA Application Delivery Analysis のパフォーマンス監視の目的のためのクライアント領域として扱われます。
- サブネット。サブネット IP アドレスとマスクの組み合わせに基づいたクライアント領域。

### [論理ポート]タブ

- 名前。 Multi-Port Monitor の管理者によって定義された論理ポートの名前。デフォルトの名前は、ポート番号と同じです。
- 論理ポート。[論理ポート] ページに表示される論理ポートの番号。デフォルトの論理ポート定義は、アダプタ上のポート ID 番号に対応しています。

## グローバル フィルタの変更

分析に含まれるデータを制限するようにグローバル フィルタを変更できます。

注: [論理ポート] グローバル フィルタを変更すると、事実上、選択された分析のデータ セット全体が変更されます。

次の手順に従ってください:

1. [分析] ペインで、変更するグローバル フィルタの横にある [変更] をクリックします。  
[グローバル フィルタ] ダイアログ ボックスが表示されます。
2. 変更するグローバル フィルタに対応するタブをクリックします。たとえば、監視対象ネットワーク上で実行されているアプリケーションで分析をフィルタするには、[アプリケーション] タブをクリックします。  
このタブには、表示しているタイムフレームからキャプチャされたパケットにそのトラフィックが反映されている、すべての既知のアプリケーションのリストが表示されます。
3. リスト内のアプリケーションを選択します。たとえば、[簡易メール転送プロトコル] を選択します。  
選択したアプリケーションが [現在選択中] として表示されます。アプリケーションポート番号がかっこ内に表示されます。また、選択されたアプリケーションによって、[グローバル フィルタ] ダイアログ ボックス内の他のタブにある項目のリストもフィルタされます。
4. 分析に含まれるデータにさらに多くの制限を適用するには、別のタブをクリックします。  
たとえば、[サーバ] タブをクリックします。選択されたアプリケーション（この例では、SMTP）を実行しているサーバのみがリスト内に表示されます。サーバを選択します。
5. [OK] をクリックします。  
現在の分析のグラフやテーブルが、SMTP アプリケーションとそのアプリケーションサーバからのデータのみを表示するようにフィルタされます。

## グローバル フィルタへの変更のクリア

グローバル フィルタに加えた変更を削除（つまり、クリア）することができます。変更をクリアすることによって、グローバル フィルタがデフォルト設定の [すべて] に戻されます。

次の手順に従ってください：

1. [分析] ペインで、クリアするグローバル フィルタの横にある [変更] をクリックします。  
[グローバル フィルタ] ダイアログ ボックスが表示され、アクティブなグローバル フィルタが [現在選択中] として表示されます。
2. 選択されたフィルタの横にある [クリア] をクリックします。
3. 別のタブをクリックして、どのフィルタが選択されているかを確認し、手順 2 を繰り返します。
4. [OK] をクリックします。

データ テーブルとグラフが、フィルタで除外された情報を含むように更新されます。



# 第5章: 表示領域のデータの理解

---

表示領域には、グラフとデータ テーブルが含まれています。以下の項目は、グラフとテーブル内のデータに影響を与えます。

- ドメイン
- タイムフレーム
- グローバル フィルタ
- 分析 フィルタ
- データ テーブル内のアクティブなタブ（[TCP] または [トラフィック] タブのどちらか）

グラフの右下には、同じデータに他のグラフ形式を適用するために使用できる一連の形式ボタンが用意されています。[分析] ペインを非表示にすることによって、表示領域のサイズを拡張できます。[分析] ペインを非表示にするには、このペインにある[非表示] アイコン («) をクリックします。

グラフとテーブルは、その双方に常に補足的な形式でデータが表示されるようにリンクされています。テーブルには、グラフより多くのデータが表示されます。ただし、グラフには、テーブルに適用したフィルタ（ソート順序の変更や新しいページの選択など）が反映されます。

データ テーブルには、トラブルシューティングや分析のためのパフォーマンス データが表示されます。各列をソートして、外れ値や最小の結果を表示できます。次の2つのフィルタは、常にデータ テーブルに影響を与えます。

- 現在のタイムフレーム
- 現在の分析のフィルタ パラメータ

事前定義済みの分析には最小のフィルタが含まれており、データを管理可能な量に制限するために何らかのロジックが適用されます。この手法によってデータベース クエリが高速化されるだけでなく、標準的なユーザにとっての表示領域の整合性も向上します。

サマリ トレンド グラフを除くすべてのグラフには、テーブルの最初の 10 行のデータが表示されます。サマリ トレンド グラフには、すべてのテーブル行のデータが反映されます。[1 ページあたりの最大数] の設定を増やすことによって、より多くのテーブル行を表示できます。

このセクションには、以下のトピックが含まれています。

- [グラフのタイプ \(P. 44\)](#)
- [データのタイプ \(P. 48\)](#)

## グラフのタイプ

表示領域内のグラフは、以下の状況で更新されます。

- CA Application Delivery Analysis レポートからセッション分析を開始したとき。
- [分析] ペインでデータ ビューをクリックしたとき。
- 表示領域でデータ テーブル内の列を選択したとき。
- CA APM の障害からドリルダウンしたとき。

グラフとテーブルによって、相互にサポートされるフィルタ オプションが提供されます。データ テーブル内の列見出しをクリックすると、選択された項目で使用可能なすべての行をソートするようにテーブルが更新されます。グラフは、選択された項目を表示するように更新されます。

[TCP] または [トライフィック] タブをクリックすると、それに応じて、グラフ内のデータが自動的に変更されます。ほとんどのグラフは、トップ 10 エントリに制限されます。唯一の例外が、CA Application Delivery Analysis の規則に従い、データ テーブル全体のデータが含まれているサマリ トレンド グラフです。

各トレンド グラフを使用すると、タイムフレームおよびズーム オプションを選択できます。

## 棒グラフ

棒グラフの形式は、選択された期間全体にわたるデータの平均を表します。それぞれの棒がテーブルの各行のデータを表します。Y軸によって、各テーブル行が識別されます。1つの棒グラフには、最大10行を含めることができます。Y軸のラベルは、その行を識別する列を示します。たとえば、Y軸は[サーバIPアドレス]ビューの対応する各サーバ名を示します。X軸には通常、メトリック値とそれらの単位が表示されます。

このタイプのグラフ形式は、異なるエンティティからのパフォーマンスマトリックの比較に最も有効です。以下に例を示します。

- あるサーバと別のサーバのサーバレスポンス時間の比較。
- トップ10アプリケーションのTCPバイトレートの比較

棒の各部分によって、メトリックとその値を識別するためのライオーバーテキストが提供されます。この機能は、合計に対してどのコンポーネントメトリックが最も寄与したかを理解するために役立ちます。グラフ内の棒をクリックすると、データテーブル内の対応する行が強調表示されます。次に、そのテーブル行を右クリックして[フィルタとして適用]を選択すると、選択したエンティティにのみ関連付けられたデータを表示できます。

**重要:** 特定のメトリックは、サーバレスポンス時間などの1つの値として示されます。その他のメトリックは、トランザクション時間などの、複合形式で示されます。複合グラフは、メトリック全体の一部として選択されたメトリックとして表示されます。複合棒グラフには、各単位に対する1つの値の内訳が表示されます。

### トレンド折れ線グラフ

トレンド折れ線グラフの形式では、1本の線がデータテーブル内の各行のデータを表します。この線は、期間全体にわたって選択されたメトリックをプロットします。グラフあたり、最大 10 のデータ行がプロットされます。Y 軸によって、ミリ秒単位でのサーバレスポンス時間 (SRT) などの、メトリック値のバケットが識別されます。X 軸には、トレンドを示すための時間単位が表示されます。

このタイプのグラフ形式は、システムステータスやトレンドの簡単な概要を提供します。以下に例を示します。

- [サーバ IP アドレス] ビューにアクセスし、サーバレスポンス時間のトレンドを比較して、SRT 内の急上昇部分にドリルダウンできます。
- 1つの IP アドレスにフィルタを適用して、徐々に増加しているトランザクション時間の発生元を見つけることができます。

### 円グラフ

円グラフの形式は、扇形として選択されたメトリックのトップ 10 エントリを表します。各扇形は、全体に対するパーセンテージを示します。すべての扇形を合計すると、トップ 10 のテーブルエントリの選択されたメトリック合計の 100 パーセントになります。それぞれの扇形はデータテーブル内の 1 つの行を表します。

注: TCP バイトロスの割合など特定のメトリックは、円グラフ形式での表示に適していません。

トップ 10 エントリが常に、選択された期間中に観測されたすべてのアクティビティの 100 パーセントになるとは限りません。11 番目の扇形で、すべてのテーブル行の残りの合計を表すことができます（[その他]）。扇形ごとのライオーバーテキストによりホストを識別します。扇形をクリックすると、データテーブル内の関連付けられたホストが強調表示されます。次に、そのデータでフィルタを実行できます。[その他] の扇形へのドリルインはサポートされていません。

このタイプのグラフ形式は、選択されたメトリックへのホストの相対的な寄与度を比較するのに最も有効です。たとえば、特定のサーバに関してフィルタし、[サーバ/クライアントのペア] ビューを選択します。次に、[TCP バイト数] メトリックを選択し、サーバのデータボリュームにどのクライアントが最も寄与しているかを確認します。

## 積み重ねトレンド グラフ

積み重ねトレンド グラフの背後にある概念は、値が時間の経過と共にプロットされるという点を除き、円グラフの概念に似ています。テーブル行ごとに、異なる色の1本の線が表示されます。グラフあたり、最大10行がプロットされます。各線は塗りつぶされて積み上げられ、最も高いテーブル行がグラフの一番下にプロットされます。各線の下にある下向きの塗りつぶしは、データの各領域が、他の領域やより大きなメトリックにどのように関連しているかを確認するのに役立ちます。

[合計] のラベルが付いた太線は、プロットされたメトリックの100パーセントがY軸に沿ってどこに位置するかを識別します。この線をグラフから削除するには、凡例の横にある [非表示] リンクをクリックします。

このタイプのグラフは、一定期間にわたるパフォーマンスマトリックへの選択されたエンティティの相対的な寄与度を比較するのに最も有効です。たとえば、特定のサーバに関してフィルタし、[サーバ/クライアントのペア] ビューを選択します。[TCP バイト数] メトリックの積み重ねトレンド グラフは、異なるクライアントのデータ ボリュームが時間の経過と共に変化しているかどうかを示します。

積み重ねトレンド グラフは、特定のタイプのメトリック (TCP バイト ロスのパーセンテージなど) には適用できません。

## サマリトレンド グラフ

サマリトレンド グラフは、積み上げ形式を使用して、すべてのテーブル行のデータ ポイントおよびデータ テーブル内のすべてのページを表示します。このグラフには、選択されたメトリックの値の階層化されたビューが表示されます。各値は、0から上の境界線までの距離ではなく、上と下のメトリック境界線間の垂直距離に等しくなります。

このグラフ形式は積み上げトレンド グラフに似ていますが、以下の違いがあります。

- 積み上げトレンド グラフには、データ テーブルの現在のページについてのみ、データ テーブル内の1列を表す1つのメトリックが表示されます。
- サマリトレンド グラフには、すべての列にわたって値が平均された、すべての行およびテーブル列からの複数のメトリックが表示されます。

積み上げ形式は、複合データを示すのに有効です。各メトリックの値は、メトリック全体の一部として扱われます。各データ ポイントは、1つのメトリックのそのコンポーネント部分への内訳を示します。

異なる色の線は、TCP トランザクション応答時間の各コンポーネント（ネットワーク ラウンドトリップ時間、サーバ応答時間、データ転送時間）などの重要な値を構成するデータ ポイントを示します。

プロットされたメトリックにおけるトレンドを表すために、グラフは選択された期間にわたってプロットされ、その時間の値が X 軸上に示されます。

## データのタイプ

データ テーブルは、同じタイムフレームからキャプチャされたデータに関する異なる観点を提供する 2 つのタブ付きビューで構成されます。各ビューは異なるメトリックを表示し、フィルタを異なる方法で適用します。

### [TCP] タブ

[TCP] タブには、TCP ベースのアプリケーションに固有のデータ、および CA Application Delivery Analysis レポート用のメトリックが含まれます。このタブには、キャプチャされたパケットから計算されるパフォーマンスマetriックも含まれます。[名前] 列のラベルは、クライアントまたはサーバのどちらが表示されているかを示すために変更されます。

**注:** [TCP] タブは、CA Application Delivery Analysis からドリルダウンするとデフォルトで選択されます。一般に、[TCP] タブ上のデータの形式は、CA Application Delivery Analysis レポート内のデータの形式に非常に似ています。

## [トラフィック]タブ

[トラフィック] タブには、TCP アプリケーションに制限されない、他のすべての使用可能なデータが含まれています。[トラフィック] タブには、クライアントまたはサーバの概念は適用されません。そのため、[名前] 列には、選択されたビューに応じてクライアントとサーバの両方の名前が表示されることがあります。[トラフィック] タブにはまた、TCP 以外のトラフィックも含まれ、それによって追加のホストが含まれる場合があります。

テーブルの幅を削減するために、データ テーブルでは一部のパフォーマンスマトリックの名前が簡略化されます。メトリックのフルネームを確認するには、マウス ポインタを簡略化された列名またはそのチェックボックスの上に置きます。フライオーバーテキストによって、選択されたメトリックのフルネームが表示されます。

## [トラフィック]タブ上のデータ

データ テーブルの [トラフィック] タブは、監視対象ミラー ポートを通過するパケットの包括的なビューを提供します。このテーブルには、選択されたビューに適用可能な列のみが表示されます。以下のリストでは、[トラフィック] タブの可能性のあるすべての列について説明します。

### アプリケーション

アプリケーション名は CA Application Delivery Analysis 設定または既知のポート使用状況から取得されます。可能な場合は、アプリケーション名が表示されます。それ以外の場合、ポート番号がかっこ内に表示されます。

### アプリケーション ID

アプリケーションを識別する一組の値のうち 2 番目の値。内部識別子です。

### アプリケーション タイプ

Multi-Port Monitor データベース内のアプリケーションを識別します。ほとんどの場合、CA Application Delivery Analysis に関してこのアプリケーションの状態を示します。以下のいずれかのタイプになります。

- **n/a** : 不明なプロトコル。
- **監視対象** : アプリケーションは TCP を使用します。 CA Application Delivery Analysis はこのアプリケーションを監視します。  
複数の収集デバイスが 1 つの CA Application Delivery Analysis 管理コンソールにレポートする場合、別の収集デバイスが CA Application Delivery Analysis 用のこのアプリケーションを監視することができます。このアプリケーションタイプは、この Multi-Port Monitor のみがアクティブに監視するアイテムを示します。
- **監視対象外 UDP** : アプリケーションは CA Application Delivery Analysis で定義されていますが、 UDP を使用します。 CA Application Delivery Analysis は UDP を監視しません。
- **監視対象外 TCP** : アプリケーションは CA Application Delivery Analysis で定義されており、 TCP を使用します。ただし、 CA Application Delivery Analysis はアプリケーションを監視していません。
- **不明な TCP** : アプリケーションは TCP を使用しますが、 CA Application Delivery Analysis で定義されていません。 アプリケーション列には「Port X」が表示されます。
- **不明な UDP** : アプリケーションは CA Application Delivery Analysis によって監視されない UDP を使用します。 アプリケーションは、 CA Application Delivery Analysis で、または Multi-Port Monitor の既知の UDP ポートのリストで定義されていません。 アプリケーション列には「Port X」が表示されます。

### バイトレート

ビット/秒 (バイト/秒 x 8) で測定されるサーバの処理効率。サーバ負荷または使用率の状態が把握できるため、このスループット値はキャパシティ計画にとって重要です。

### バイトレート(送信側)、バイトレート(受信側)

選択したホストが送信または受信したデータのビット/秒 (バイト/秒 x 8) でのスループット。

## バイト

バイト単位のデータ ボリューム。選択した期間および選択したクライアント - サーバ セッション中に送受信したアプリケーション レイヤ の総バイト数です。

## バイト数(送信側)、バイト数(受信側)

バイト単位のデータ ボリューム。選択したホストが選択した期間中に送受信したアプリケーション レイヤ の総バイト数です。

## IP アドレス、IP アドレス 1、IP アドレス 2

ホストの IP アドレス。ペアになったデータ ビューに「1」または「2」の指定が表示され、ホスト間のデータ フローの方向を示します。

## レイヤ 3 プロトコル

ネットワーク レイヤ プロトコルの名前 (IP または ARP)、またはパケット ヘッダ内の Ethertype フィールドの ID 番号。IEEE 802 Ethertype 値が見つかったときは「Ethertype=X」を示します。

## レイヤ 3 プロトコル番号

ネットワーク レイヤ プロトコルの 10 進数のレジストリ番号 (例: IPv4 は 2048)。

## レイヤ 4 プロトコル

トランスポート層プロトコルの名前 (例: TCP)。

## レイヤ 4 プロトコル番号

トランスポート層プロトコルの 10 進数のレジストリ番号 (例: TCP は 6)。

## 論理ポート、論理ポート番号

テーブル内のデータのソースである Multi-Port Monitor アプライアンスの論理ポートおよびポート番号。

## MAC アドレス、MAC アドレス 1、MAC アドレス 2、IP アドレス MAC

選択したセッション中に示された IP アドレスが割り当てられているサーバの MAC (Media Access Control) アドレス。ペアになったデータ ビューに「1」または「2」の指定が表示され、ホスト間のデータ フローの方向を示します。

### 名前、名前 1 または 2、サーバ名、クライアント名

ホストの名前、クライアントまたはサーバいづれかの名前。一部のビューでは、クライアントまたはサーバの指定が表示されます。他のビューでは、クライアントまたはサーバの役割に関わらずホストが表示されます。ペアになったデータビューに「1」または「2」の指定が表示され、ホスト間のデータフローの方向を示します。

### ネットワーク名、ネットワーク名 1、ネットワーク名 2

ADA での監視用に定義されたネットワークの名前。ペアになったデータビューに「1」または「2」の指定が表示され、ネットワーク間のデータフローの方向を示します。

### ネットワークサブネット、ネットワークサブネット 1、ネットワークサブネット 2

ネットワークサブネットの IP アドレス。ペアになったデータビューに「1」または「2」の指定が表示され、サブネット間のデータフローの方向を示します。

### パケットレート

1 秒あたりのパケット数で測定されるサーバの処理効率。サーバ負荷または使用率の状態が把握できるため、このスループット値はキャパシティ計画にとって重要です。

### パケットレート(送信側)、パケットレート(受信側)

選択したホストが送受信したデータのパケット単位での 1 秒あたりのスループット。

### パケット数

パケット単位でのデータボリューム。選択した期間および選択したクライアントサーバセッション中に送受信されたパケットの総数。

### パケット数(送信側)、パケット数(受信側)

データボリューム。選択したホストが送受信したパケットの総数。

### ポート 1、ポート 2

通信またはセッションに関連するデータを送受信したホスト上のポート。

### セッション ID

TCP セッションの ID 番号。内部識別子です。

### ToS

IPv4 ヘッダ内の TOS (Type of Service) フィールドのビット設定。

### ToS の説明

「デフォルト トラフィック」や「最大スループット」など、TOS 設定の標準的な説明。

### TCP バイト

バイト単位での TCP データ ボリューム。選択したホストまたはホストのペアによって選択した期間中に送受信された TCP バイトの総数。

### TCP パケット

パケット単位での TCP データ ボリューム。選択したホスト（またはホストのペア）が選択した期間中に送受信した TCP パケットの総数。

### VLAN

仮想ローカルエリア ネットワークの ID 番号。

## [TCP] タブ上のデータ

データ テーブルの [TCP] タブでは TCP 以外のパケットが除外され、CA Application Delivery Analysis および CA APM がすべての Multi-Port Monitor 論理ポートから監視するデータが表示されます。このテーブルには、選択されたビューに適用可能な列のみが表示されます。以下のリストでは、[TCP] タブの可能性のあるすべての列について説明します。

### アプリケーション

アプリケーション名は CA Application Delivery Analysis 設定または既知のポート使用状況から取得されます。可能な場合は、アプリケーション名が表示されます。それ以外の場合、ポート番号がかっこ内に表示されます。

### アプリケーション ID

アプリケーションを識別する一組の値のうち 2 番目の値。内部識別子です。

### アプリケーション タイプ

Multi-Port Monitor データベース内のアプリケーションを識別します。ほとんどの場合、CA Application Delivery Analysis に関してこのアプリケーションの状態を示します。以下のいずれかのタイプになります。

- **n/a** : 不明なプロトコル。
- **監視対象** : アプリケーションは TCP を使用します。 CA Application Delivery Analysis はこのアプリケーションを監視します。  
複数の収集デバイスが 1 つの CA Application Delivery Analysis 管理コンソールにレポートする場合、別の収集デバイスが CA Application Delivery Analysis 用のこのアプリケーションを監視することができます。このアプリケーションタイプは、この Multi-Port Monitor のみがアクティブに監視するアイテムを示します。
- **監視対象外 UDP** : アプリケーションは CA Application Delivery Analysis で定義されていますが、 UDP を使用します。 CA Application Delivery Analysis は UDP を監視しません。
- **監視対象外 TCP** : アプリケーションは CA Application Delivery Analysis で定義されており、 TCP を使用します。ただし、 CA Application Delivery Analysis はアプリケーションを監視していません。
- **不明な TCP** : アプリケーションは TCP を使用しますが、 CA Application Delivery Analysis で定義されていません。 アプリケーション列には「Port X」が表示されます。
- **不明な UDP** : アプリケーションは CA Application Delivery Analysis によって監視されない UDP を使用します。 アプリケーションは、 CA Application Delivery Analysis で、または Multi-Port Monitor の既知の UDP ポートのリストで定義されていません。 アプリケーション列には「Port X」が表示されます。

### クライアント IP アドレス

クライアント - サーバセッションにおけるクライアントコンピュータの IP アドレス。

### クライアント名

クライアント - サーバセッション（通信ペア）におけるクライアントコンピュータのホスト名。

### クライアント ポート

データが送受信されたクライアント上のポート。

### CT 観測数

接続時間の計測値。選択した時間間隔に発生した監視対象 TCP 接続の数。メトリックの測定値と使用率レベルを適切に示します。たとえば、計測値が大きい場合は、イベントがユーザに影響を及ぼしている可能性があります。

### DTT

データ転送時間。サーバが応答を開始してからデータを送信し終えるまでの間の経過時間。応答のサイズ、使用可能な帯域幅、アプリケーションとネットワーク間のインタラクションなど、いくつかの要因がこの値に影響します。TCP ウィンドウに収まるデータよりも多い送信データがある場合、初期サーバ応答時間を除外し、NRTT のみを含みます。この値は、すべてのデータを配信するのに必要なネットワーク ラウンド トリップの数およびラウンド トリップあたりの遅延に関連しています。

### ENRTT

有効なネットワーク ラウンド トリップ時間。NRTT および再送遅延(再送信がトランザクションに対して引き起こす遅延)を含んでいます。ユーザが実際に経験する遅延を反映しており、再送信が引き起こすパフォーマンス低下のインジケータとして機能します。

### レイヤ 3 プロトコル

ネットワーク レイヤプロトコルの名前(IP または ARP)、またはパケットヘッダ内の Ethertype フィールドの ID 番号。IEEE 802 Ethertype 値が見つかったときは「Ethertype=X」を示します。

### レイヤ 3 プロトコル番号

ネットワーク レイヤプロトコルの 10 進数のレジストリ番号(例: IPv4 は 2048)。

### レイヤ 4 プロトコル

トランスポート層プロトコルの名前(例: TCP)。

### レイヤ 4 プロトコル番号

トランスポート層プロトコルの 10 進数のレジストリ番号(例: TCP は 6)。

### 論理ポート、論理ポート番号

テーブル内のデータのソースである Multi-Port Monitor アプライアンスの論理ポートおよびポート番号。

### NCT

ネットワーク接続時間。クライアントがサーバ接続応答を確認するまでにかかった時間。一般的に、ネットワーク遅延は、接続時間の遅延を引き起こします。NCTは、キャリア遅延のベースラインおよびNRTT値との比較対象として機能します。

### NRTT

ネットワークラウンドトリップ時間。パケットがネットワーク上のサーバとクライアント間を移動するのにかかった時間（再送信による遅延を除く）。アプリケーションおよびサーバの処理時間はこの値から除外されます。この値は、NCTの値と比較すると役立ちます。

### 再送信

再送遅延。再送信が原因のNRTTの追加の遅延。再送信はデータの損失後に再送信されるパケットです。データは、各トランザクションの実際の再送信時間ではなく、すべての計測の平均として表されます。再送遅延によりクライアントの確認応答に遅延が生じると、NRTTの値は増加します。このメトリックでは、TCP幅轍のため、損失がDTTに与える影響が明らかになりません。このメトリックは、クライアントからサーバにではなく、サーバからクライアントへのデータの損失のみを反映します。

### SCT

サーバ接続時間。サーバがクライアントからSYNパケットを受信した時点からサーバが最初のSYN/ACKを送信するまでの時間です。

TCP接続を開始するにはSYN、SYN/ACK、およびACKの3つのパケットを交換します。TCPヘッダにはSYN（同期）およびACK（確認）ビットがあります。最初のパケットにはSYNビットが設定されています。2番目のパケットには両方のビットが設定されています。3番目のパケットにはACKビットのみが設定されています。この交換により接続の初期シーケンス番号を確立します。

SCTとNCTは接続セットアップ時間メトリックを構成します。

### サーバIPアドレス

クライアント - サーバセッションにおけるサーバのIPアドレス。

### サーバのMAC、クライアントMAC

ホストを識別する一意のMAC（Media Access Control）アドレス。

**サーバ名**

クライアント - サーバ セッション（通信ペア）におけるサーバのホスト名。

**サーバのネットワーク名、クライアント ネットワーク名**

CA Application Delivery Analysis での監視用に定義されたネットワークの名前。ペアになったデータ ビューに「クライアント」または「サーバ」の指定が表示され、ネットワーク間のデータ フローの方向を示します。

**サーバのネットワーク サブネット、クライアント ネットワーク サブネット**

ネットワーク サブネットの IP アドレス。ペアになったデータ ビューに「クライアント」または「サーバ」の指定が表示され、サブネット間のデータ フローの方向を示します。

**Server Port**

データが送受信されたサーバ上のポート。

**SRT**

サーバ応答時間。サーバがクライアント要求に応答するのにかかった時間。サーバ速度、アプリケーション設計、および要求の量が SRT に影響します。

**TCP バイトロス**

送受信された TCP バイトの割合として表されるデータの損失。

**TCP バイトレート(送信側)、TCP バイトレート(受信側)**

ビット単位の TCP スループット。選択した期間中の選択したサーバおよびクライアントの間のデータ レート（ビット/秒（バイト/秒 x 8）単位）。

**TCP 再送バイト率**

データ合計に対する再送信されたデータの比率、監視対象ネットワークで失われたデータの割合、およびビット/秒での損失率。

**TCP バイト**

バイト単位での TCP データ ボリューム。選択した期間中にネットワーク上で観測されたアプリケーションレイヤバイトの総数です。

### TCP バイト数(送信側)、TCP バイト数(受信側)

バイト単位での TCP データ ボリューム。選択した期間中に選択したサーバがクライアントとの間で送受信したアプリケーション レイヤ バイトの総数。

### TCP パケット ロス

送受信された TCP パケットの割合として表されるデータの損失。

### TCP パケット レート

パケット単位の TCP スループット。選択した期間内のパケット/秒単位のデータ レート。ADA レポートは「データ レート」という用語を使用します。

### TCP パケット レート(送信側)、TCP パケット レート(受信側)

パケット単位の TCP スループット。選択した期間中の選択したサーバ およびクライアントの間のデータ レート (パケット/秒単位)。

### 再送信 TCP パケット レート

データ合計に対する再送信されたデータの比率、監視対象ネットワークで失われたデータの割合、およびパケット/秒での損失率。

### TCP パケット

パケット単位での TCP データ ボリューム。選択した期間中のネットワーク上の総パケット数です。TCP 受信確認などのゼロバイト パケットが含まれます。

### TCP パケット数(送信側)、TCP パケット数(受信側)

ビット単位での TCP スループット。選択した期間中のデータ転送速度 (バイト/秒 x 8) です。CA Application Delivery Analysis のレポートでは「データ転送速度」という用語を使用します。

### TCP 再送信 バイト数

データの損失が原因で再送信された TCP バイトの数。

### TCP 再送信 パケット数

データの損失が原因で再送信された TCP パケットの数。

### ToS

IPv4 ヘッダ内の TOS (Type of Service) フィールドのビット設定。

### ToS の説明

「デフォルト トライフィック」や「最大スループット」など、TOS 設定の標準的な説明。

### トランザクション時間

クライアントが要求（パケット レベルまたはトランザクション レベル）を送信した時点からクライアントが応答で最後のパケットを受信した時点までの時間。

### トランザクション時間観測数

トランザクション計測時間。選択した間隔中に発生した、監視対象 TCP トランザクションの数。メトリックの測定値と使用率レベルを適切に示します。たとえば、計測値が大きい場合は、イベントが多くのユーザに影響を及ぼしている可能性があります。

### VLAN

仮想ローカルエリア ネットワークの ID 番号。

## ネットワークとホストのバイト数

[TCP] タブには、クライアントネットワークの観点からのアクティビティが表示されます。[トライフィック] タブには、どの通信ホストがクライアントで、どれがサーバかには関係なく、一般的なネットワーク アクティビティが表示されます。同じサブネット内のホストのペアがデータを交換する場合は、同じ通信のバイト数が各タブで異なることがあります。

[トライフィック] タブでは、同じサブネット内の通信の総バイト数が、[TCP] タブに表示される合計の 2 倍として表示される場合があります。2 つのホスト間で交換される総バイト数は、ネットワークから出るとき、さらに再び入るときに集計されます。ホストごとに分けるのではなく、両方向が合計に含まれます。

クライアントの観点が反映される [TCP] タブでは、1 つのホストが送受信したバイト数が同じ期間に対して集計されます。その結果、[トライフィック] タブ上の総バイト数の値より小さい総バイト数の値が得られます。

## データテーブル内の列の追加または削除

デフォルトでは、[トラフィック] および [TCP] タブ上のデータテーブルから一部のデータが除外されます。データの追加列を含めることができます。

次の手順に従ってください:

1. [列の編集] をクリックします。  
[列の編集] ダイアログ ボックスが表示されます。
2. データテーブルに追加するメトリックのチェック ボックスを選択します。
3. データテーブルから削除するメトリックのチェック ボックスをクリックします。
4. デフォルトの列設定を復元するには、[デフォルト] をクリックします。
5. [Save] をクリックします。

加えた変更は、データテーブルが更新された後に反映されます。

# 第 6 章: データのエクスポート

---

このセクションには、以下のトピックが含まれています。

[PDF ファイルへのデータのエクスポート \(P. 61\)](#)

[CSV ファイルへのデータのエクスポート \(P. 62\)](#)

[PCAP ファイルへのデータのエクスポート \(P. 63\)](#)

[電子メールによるデータの共有 \(P. 66\)](#)

## PDF ファイルへのデータのエクスポート

分析内のグラフは、以下の制限の下に PDF 形式で共有できます。

- データ テーブルはエクスポートされません。
- グラフ内の色を説明している凡例はエクスポートされません。そのため、トレンド折れ線グラフと積み重ねトレンド グラフの形式では、ビューを電子メールによるリンクとして送信します。

エクスポートされた分析には、現在のグラフに適用されたすべてのフィルタが保存されます。

次の手順に従ってください:

1. エクスポートするデータを表示します。
  - a. [分析] ペインでデータ ビューをクリックします。
  - b. 追加のフィルタを適用するか、または選択された列でデータ テーブルをソートします。
2. [PDF へエクスポート] をクリックします。  
[ファイルのダウンロード] ダイアログ ボックスが表示されます。

3. ファイルを開くか、またはファイルを保存するかを選択します。
  - [開く] をクリックすると、PDF が Acrobat Reader アプリケーションで表示されます。
  - [保存] をクリックした場合は、[別名で保存] ダイアログ ボックスを使用してファイルの保存場所を参照し、[保存] をクリックします。

現在のグラフが、.pdf ファイル拡張子を持つファイルにエクスポートされます。ラベルによって、データ ビュー、アクティブなフィルタ、データのタイムフレーム、および PDF が生成された時刻が識別されます。

## CSV ファイルへのデータのエクスポート

分析内のデータ テーブルを、カンマ区切り値 (.csv) 形式のスプレッドシートにエクスポートできます。エクスポートされた分析には、データ テーブルに適用されたすべてのフィルタが保持されます。

ベスト プラクティスとして、スプレッドシートのサイズを制限するためには、データの正確なセグメントを選択します。

- 定義した論理ポートにハードウェア フィルタを適用します。
- 選択したデータ ビューにフィルタを適用します。
- [期間] セレクタを使用して、比較的短い期間を選択します。

次の手順に従ってください:

1. エクスポートするデータを表示します。
  - a. [分析] ペインでデータ ビューをクリックします。
  - b. 追加のフィルタを適用するか、または選択された列でデータ テーブルをソートします。
2. [CSV へエクスポート] をクリックします。

[CSV へエクスポート] ダイアログ ボックスが表示されます。
3. (オプション) [エクスポート行制限] フィールドで、エクスポートするデータ テーブル行の最大数を入力します。または、選択された期間からのデータ テーブル内のすべての行をエクスポートするには、[無制限] を選択します。

4. [OK] をクリックします。  
[ファイルのダウンロード] ダイアログ ボックスが表示されます。
5. ダウンロード時間を速くするために、[保存] をクリックします。  
注: ファイルを開くオプションは推奨されません。大量のデータをエクスポート中にこのオプションを選択すると、ダウンロード時間が長くなります。
6. ファイルの保存場所を入力または参照し、[OK] をクリックします。  
選択した詳細が、.csv ファイル拡張子を持つファイルにエクスポートされます。データベースで使用可能なデータ量や、指定した行制限によっては、このプロセスの完了に数分かかることがあります。

## PCAP ファイルへのデータのエクスポート

現在のビューのパケットキャプチャデータを、PCAP 形式のパケットキャプチャファイルにエクスポートできます。パケットキャプチャファイルは未処理キャプチャファイルから構築され、現在の分析に含まれているすべてのセッションのパケットを表示します。

PCAP 形式は、ネットワークトレースファイルや、パケットレベルのデータの検証および交換のためのその他の方法に広範に使用されています。PCAP は、WinPcap (Windows) や libpcap (UNIX) と互換性があります。これらのアプリケーションプログラミングインターフェースを使用しているアプリケーションは、PCAP を容易に読み取って表示します。

管理者および CA Application Delivery Analysis 調査役割の権限を持つユーザは、[PCAP へエクスポート] 機能を使用できます。デフォルトでは、IT エンジニアおよび IT 管理者の役割のみが、この機能へのアクセスを許可します。

## ヒント :

- PCAP ファイルのエクスポートは、完了に少し時間がかかることがあります。 [ファイルのダウンロード] ダイアログ ボックスを開くために必要な時間は、エクスポートされるデータ量によって異なります。
- [PCAP へエクスポート] 機能のパフォーマンスを向上させるには、分析のタイムフレームを狭くしください。 タイムフレームが狭いほど、関連するパケットのために検索される未処理キャプチャファイルの数が削減されます。 期間セレクタまたはグラフ時間コントロールを使用して、目的のタイムフレームにズームインします。
- PCAP にエクスポートする機能は、目的のデータを含む未処理キャプチャファイルが削除された場合は使用できません。 キャプチャファイルは、メトリックデータベース内のメトリックデータほど長くは保持されません。
- [最大バイト数/パケット] パラメータの [ヘッダのみ] オプションは、拡張ヘッダを含む IPv4 (TCP および UDP) ヘッダに適用されます。 非 IP トライフィックのエクスポート時に [ヘッダのみ] を選択する場合、レイヤ 2 MAC ヘッダのみが受信されます。 代わりに、バイト値 (128 など) を選択して、各フレームの詳細を表示します。
- セッション レベルパフォーマンス データは、Multi-Port Monitor の論理ポートで受信される IPv4 ベースのポート ミラー データにのみ利用可能です。
- PCAP ファイルは、プロトコルアナライザ、またはフリーウェア ツールである Wireshark などのパケットスニッファで表示できます。 プロトコルアナライザはネットワークを通過するデータ フローを観測し、各パケットのコピーを検査します。 プロトコルアナライザでは、パケットヘッダ内の各フィールドの内容がグラフィカルユーザインターフェースに表示され、このインターフェースを使用して、データのフィルタ、ソート、および分析を実行できます。
- プロトコルアナライザは、Multi-Port Monitor がキャプチャしたデータのトラブルシューティング や分析を実行するための便利なツールです。 プロトコルアナライザを使用するには、イーサネット、IP、およびレイヤ 4 プロトコルのパケット構造を理解している必要があります。

以下の手順に従います。

1. エクスポートするデータを表示します。
  - a. [分析] ペインでデータ ビューをクリックします。
  - b. 追加のフィルタを適用するか、または選択された列でデータ テーブルをソートします。
2. [PCAP へエクスポート] をクリックします。

[PCAP へエクスポート] ダイアログ ボックスに、エクスポートする パケット トレースの時間範囲が表示されます。
3. [論理ポート] フィールドで、エクスポートするデータを受信したポートを選択します。使用可能なポートごとに、セッションの数とトラフィック量 (バイト数) が表示されます。これらの統計は、現在のフィルタ (タイムフレームやビューなど) に基づいています。エクスポートするファイルのサイズを示しているわけではありません。

エクスポートされる PCAP ファイルごとに 1 つのポートのみを選択します。
4. [最大バイト数/パケット] フィールドで、各パケットから含める最大バイト数を選択します。デフォルトのオプションでは、ヘッダのみが PCAP ファイルに含まれます。
5. [OK] をクリックします。

[名前を付けて保存] ダイアログ ボックスが表示されます。
6. エクスポートされた PCAP ファイルを保存する場所を選択します。
7. [Save] をクリックします。

## 電子メールによるデータの共有

分析へのリンクの送信は多くの場合、データを共有するための最も迅速な方法です。 [電子メール] オプションでは、分析から URL を構成し、デフォルトのメールクライアントを使用して電子メールメッセージを作成します。

### 制限

- 電子メールクライアントが必須です。電子メール機能を使用するには、電子メールクライアントをインストールし、ユーザが Web インターフェースにアクセスするコンピュータ上に SMTP サーバを設定します。
- 受信者には、 [分析] ページを表示する権限を持つユーザ アカウントが必要です。
- 受信者は、基になるデータがデータベースからページされる前に、数日以内に分析を表示する必要があります。

次の手順に従ってください:

1. エクスポートするデータを表示します。
  - a. [分析] ペインでデータ ビューをクリックします。
  - b. 追加のフィルタを適用するか、または選択された列でデータ テーブルをソートします。
2. [電子メール] をクリックします。

メッセージングアプリケーションで空白のメッセージが開きます。メッセージの本文に URL が表示されます。件名に日付と時刻が表示されます。この日付と時刻は、分析のタイムフレームではなく、電子メールメッセージが生成された時点を表します。分析のタイムフレームは、[分析] ページの表示領域に示されます。
3. 受信者のアドレスを入力し、 [送信] をクリックします。

受信者に送信される電子メールには、分析のための URL へのリンクが含まれています。

# 付録 A: コマンドライン構文

---

Multi-Port Monitor アプライアンスのデフォルトのユーザ名とパスワードでは、スーパーユーザのアクセス権が提供されます。スーパーユーザコマンドを識別する「`sudo`」プレフィックスを使用して、Linux のコマンドラインインターフェースで以下の操作を実行できます。

`sudo /sbin/service nqmaintd status`

メンテナンス デーモン (`nqmaintd`) のステータスを確認します。

`sudo /sbin/service nqmaintd restart`

メンテナンス デーモンを再起動します。ステータス メッセージでプロセスが実行中であることが示されている場合にのみ使用してください。

`sudo /sbin/service nqmaintd start`

メンテナンス デーモンを起動します。ステータス メッセージでプロセスが停止していることが示されている場合にのみ使用してください。

`sudo /opt/NetQoS/scripts/stopprocs.sh`

すべてのデーモン (プロセス) を停止します。

`sudo /opt/NetQoS/scripts/startprocs.sh`

すべてのデーモン (プロセス) を起動します。

`sudo /sbin/shutdown -h now`

アプライアンスを直ちに停止します。アプライアンスを停止する前に、Multi-Port Monitor データベースを停止してください。

`sudo reboot`

アプライアンスを直ちに停止して再起動します。アプライアンスを停止する前に、Multi-Port Monitor データベースを停止してください。

`sudo /opt/NetQoS/scripts/doVerticaCmd.sh --shutdown`

Vertica メトリック データベースを停止します。また、Web インターフェースからデータベースを停止することもできます。

`sudo /opt/NetQoS/scripts/doVerticaCmd.sh --start`

Vertica メトリック データベースを開始します。

```
sudo /opt/NetQoS/scripts/doVerticaCmd.sh --status
```

Vertica メトリックデータベースのステータスを確認します。また、Web インターフェースからステータスを確認することもできます。

```
sudo /opt/NetQoS/tui/tui-setup.php
```

アプライアンス上でネットワーク設定ユーティリティを起動します。

```
sudo /opt/NetQoS/scripts/syncNapatechClock --force
```

Multi-Port Monitor キャプチャカード上のクロックをシステムクロックと直ちに同期します。このコマンドによって **nqcapd** プロセスと **nqmetricd** プロセスが一時的に停止され、それにより監視が中断されます。クロックが同期された後、両方のプロセスが再起動されます。

# 付録 B: 正規表現構文

---

高度なフィルタでは、[条件] フィールドに書き込まれた構文が、キャプチャカードの互換性のためのベンダー仕様に自動的に従います。生成された式（特に、式をグループ化するかつこの位置）を見直して、式が正しい順序で評価されることを確認してください。たとえば、以下のグループ化

(A OR B) AND C

は、このグループ化とは異なる結果になります。

A OR (B AND C)

この構文は、[条件] フィールドで編集できます。

Multi-Port Monitor のフィルタでは、条件に一致するパケットが含まれます。特定のホストまたはサブネットからパケットを除外するフィルタを作成する場合は、特に注意してください。式の構文について質問がある場合は、[CA テクニカル サポート](#)にお問い合わせください。

## 例

ホスト A (192.168.32.15) とホスト B (10.10.21.10) の間の通信を無視します。この通信は、週に 1 回実行され、そのたびにベースラインにひずみを生じさせる自動バックアッププロセスを表します。「その他のすべてのトラフィック」に関するレポートが必要です。また、除外されたペア以外のホストに転送されるトラフィックのすべてのパケットを保持することも必要です。そのため、以下のパケットを保持するフィルタを作成します。

- ホスト A がソースであるが、宛先がホスト B に等しくないすべてのパケット、または
- ホスト B がソースであるが、宛先がホスト A に等しくないすべてのパケット、または
- ホスト A およびホスト B の IP アドレスに等しくないソース アドレスを含むすべてのパケット（その他のすべてのトラフィック）

[条件] フィールドでは、正しい構文は以下のようになります。

**条件:**

```
((mlPSrcAddr==[192.168.32.15] AND mlPDestAddr!=[10.10.21.10]) OR (mlPSrcAddr==  
[10.10.21.10] AND mlPDestAddr!=[192.168.32.15])) OR (mlPSrcAddr!= [192.168.32.15],  
{10.10.21.10}))
```

英語で記述した場合、作成する式は以下のようになります。

(IP Source Address EQUALS 192.168.32.15 AND IP Destination Address does NOT EQUAL  
10.10.21.10) OR (IP Source Address EQUALS 10.10.21.10 AND IP Destination Address  
does NOT EQUAL 192.168.32.15) OR (IP Source Address does NOT EQUAL 192.168.32.15,  
10.10.21.10)

正規表現を使用して高度なフィルタを作成する場合、「==」を挿入するには  
[Equals] を選択します。「!=」を挿入するには [Not Equals] を選択します。