



## **Cisco Wide Area Application Service モニタ リング ガイド**

### **Cisco Wide Area Application Services Monitoring Guide**

ソフトウェア バージョン 4.3.1

2010 年 11 月 30 日

**【注意】シスコ製品をご使用になる前に、安全上の注意**  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊  
社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

*Cisco Wide Area Application Service モニタリング ガイド*

© 2010 Cisco Systems, Inc.

All rights reserved.

Copyright © 2010–2011, シスコシステムズ合同会社.

All rights reserved.



## CONTENTS

はじめに	v	
対象読者	v	
マニュアルの構成	vi	
関連資料	vi	
表記法	vii	
マニュアルの入手方法およびテクニカル サポート	vii	
<b>CHAPTER 1</b>	<b>WAAS Central Manager を使用した WAAS のモニタリング</b>	<b>1-1</b>
WAAS ネットワーク ヘルスのモニタリング	1-1	
WAAS ダッシュボードの使用	1-2	
アラームの表示	1-3	
WAE デバイス ステータスの表示	1-8	
最適化のモニタリング	1-8	
システム動作のモニタリング	1-10	
トポロジのモニタリング	1-11	
監査証跡ログ、システム メッセージ、および WAAS Central Manager ログのモニタリング	1-12	
システム プロパティの表示	1-13	
WAAS デバイス ヘルスのモニタリング	1-14	
[Device Dashboard] の表示	1-14	
最適化レポートの表示	1-15	
接続統計情報の表示	1-15	
アクセラレーション レポートの表示	1-17	
CPU 統計情報の表示	1-18	
ディスク ヘルスとステータスの表示	1-19	
デバイス ピアリング ステータスの表示	1-19	
デバイス ログの表示	1-20	
WAAS Central Manager GUI からの CLI コマンドの実行	1-20	
show cms info コマンド出力	1-21	
show wccp service コマンド出力	1-22	
show wccp gre コマンド出力	1-22	
show statistics connection コマンド出力	1-23	
show statistics connection optimized cifs コマンド出力	1-24	
show statistics accelerator cifs detail コマンド出力	1-24	
show statistics dre コマンド出力	1-25	

show statistics tfo コマンド出力	1-25
show interface gig 1/0 コマンド出力	1-26
show tech-support コマンド出力	1-27

---

## 2      **トラフィック代行受信のモニタリング**

WCCPV2 代行受信の確認
show ip wccp IOS コマンド出力
show wccp WAAS コマンド出力
インライン代行受信の確認

---

## CHAPTER 3      **SNMP を使用した WAAS のモニタリング**

サポートされる MIB に関する情報
サポートされる MIB のダウンロード
SNMP トラップの表示とイネーブル化
一般的な SNMP MIB OID に関する情報
SNMP トリガーの表示と設定

---

## CHAPTER 4      **XML API を使用した WAAS のモニタリング**

XML ベースの API に関する情報
トラフィック アクセラレーション サービスの使用
イベントおよびステータス サービスの使用
soapUI を使用した WAAS API インターフェイスへのアクセス

---

## CHAPTER 5      **Cisco ネットワーク解析モジュールを使用した WAAS のモニタリング**

NAM に関する情報
データを NAM にエクスポートするよう WAAS デバイスを設定
WAAS デバイスをモニタするよう NAM を設定
NAM を使用した WAAS デバイスのモニタに関する情報
モニタする WAAS デバイスのデータ ソースの指定



## はじめに

---

この「はじめに」では、『Cisco Wide Area Application Service モニタリングガイド』の対象読者、編成、および表記法について説明します。また、関連情報の取得方法も記載されています。

## 対象読者

このマニュアルは、次の領域に固有の知識を持つ、経験を積んだシステム管理者とネットワーク管理者を対象としています。

- ネットワーキングおよびデータ通信
- ネットワーク セキュリティ
- ルータおよびスイッチの設定

## マニュアルの構成

このマニュアルは次のように構成されています。

章	説明
第 1 章「WAAS Central Manager を使用した WAAS のモニタリング」	WAAS Central Manager を使用して WAAS デバイスをモニタする方法について説明します。
第 2 章「トラフィック代行受信のモニタリング」	トラフィック代行受信のさまざまなモニタ方法について説明します。
第 3 章「SNMP を使用した WAAS のモニタリング」	SNMP を使用して WAAS デバイスをモニタする方法について説明します。
第 4 章「XML API を使用した WAAS のモニタリング」	WAAS XML API を使用して WAAS デバイスをモニタする方法について説明します。
第 5 章「Cisco ネットワーク解析モジュールを使用した WAAS のモニタリング」	Cisco Network Analysis を使用して WAAS デバイスをモニタする方法について説明します。

## 関連資料

Cisco WAAS ソフトウェアの詳細については、次のマニュアルを参照してください。

- 『[Release Note for Cisco Wide Area Application Services](#)』
- 『[Cisco Wide Area Application Services Quick Configuration Guide](#)』
- 『[Cisco Wide Area Application Services Configuration Guide](#)』
- 『[Cisco Wide Area Application Services Command Reference](#)』
- 『[Cisco Wide Area Application Services API Reference](#)』
- 『[Cisco Wide Area Application Services Upgrade Guide](#)』
- 『[Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade](#)』
- 『[Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later](#)』
- 『[Cisco WAAS on Service Modules for Cisco Access Routers](#)』
- 『[Cisco SRE Service Module Configuration and Installation Guide](#)』
- 『[Configuring Cisco WAAS Network Modules for Cisco Access Routers](#)』
- 『[WAAS Enhanced Network Modules](#)』
- 『[Cisco Wide Area Application Services Online Help](#)』
- 『[Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems](#)』
- 『[Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines](#)』
- 『[Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide](#)』
- 『[Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide](#)』
- 『[Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series](#)』
- 『[Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide](#)』

- 『Cisco Wide Area Application Engine 7326 Hardware Installation Guide』
- 『Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide』
- 『Installing the Cisco WAE Inline Network Adapter』
- 『Using Cisco NAM 4.1 Reporting with Cisco WAAS』
- 『Cisco Wide Area Application Services vWAAS Installation and Configuration Guide』

## 表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード	太字
値を指定する変数	イタリック体
表示されるセッションおよびシステム情報	screen フォント
入力する情報	太字の screen フォント
入力する変数	イタリック体の screen フォント
メニュー項目およびボタン名	太字
段落でのメニュー項目の選択	[Option] > [Network Preferences]
テーブルでのメニュー項目の選択	[Option] > [Network Preferences]



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『What's New in Cisco Product Documentation』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。







# CHAPTER 1

## WAAS Central Manager を使用した WAAS のモニタリング

この章では、WAAS Central Manager を使用して、WAAS 環境のネットワーク ヘルス、デバイス ヘルス、およびトラフィック代行受信をモニタする方法について説明します。

この章の構成は、次のとおりです。

- 「WAAS ネットワーク ヘルスのモニタリング」(P.1-1)
- 「WAAS デバイス ヘルスのモニタリング」(P.1-14)

WAAS Central Manager の使用に関する詳細については、『Cisco Wide Area Application Services Configuration Guide』の「[Monitoring and Troubleshooting Your WAAS Network](#)」の章を参照してください。

## WAAS ネットワーク ヘルスのモニタリング

ここでは、WAAS Central Manager を使用して、WAAS 環境のヘルスをモニタする方法について説明します。セキュアな Web ブラウザから、次のようにしてポート 8443 のホスト名または IP アドレスのいずれかを使用して、WAAS Central Manager にログインします。

`https://CM-Host-Name_or_IP Address:8443`

WAAS Central Manager にログインするには、正しいユーザ名とパスワード資格情報が必要です。

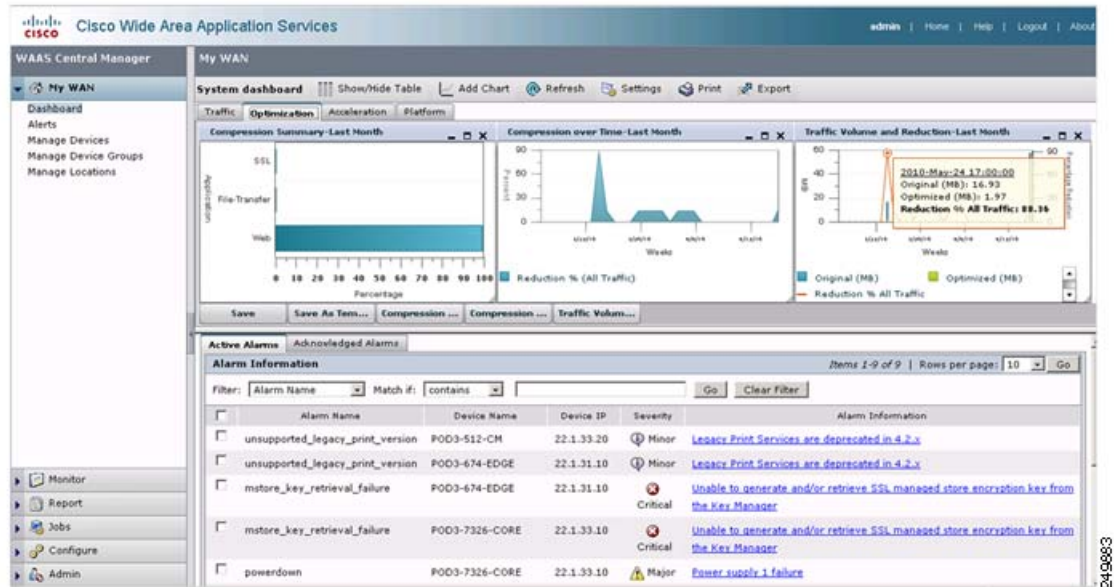
ここでは、次の内容について説明します。

- 「WAAS ダッシュボードの使用」(P.1-2)
- 「アラームの表示」(P.1-3)
- 「WAE デバイス ステータスの表示」(P.1-8)
- 「最適化のモニタリング」(P.1-8)
- 「トポロジのモニタリング」(P.1-11)
- 「監査証跡ログ、システム メッセージ、および WAAS Central Manager ログのモニタリング」(P.1-12)
- 「システム プロパティの表示」(P.1-13)

## WAAS ダッシュボードの使用

[My WAN] > [Dashboard] を選択して、ご使用の WAAS ネットワークに関する全般情報と詳細情報を表示できます。デフォルトで [Optimization] タブが表示される [System Dashboard] ウィンドウが表示されます (図 1-1 を参照)。

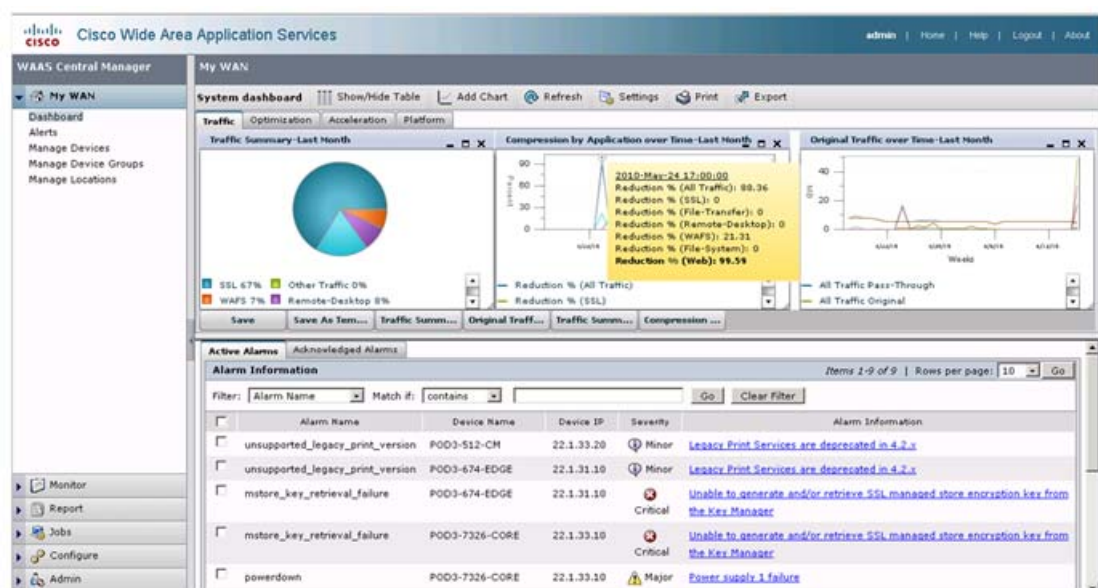
図 1-1 WAAS Central Manager : [Dashboard Optimization] タブ



チャートには、WAAS の全体的なネットワーク ヘルスのスナップショットが示されています。各タブでは、さまざまなレポート オプションを使用できます。チャートを選択して、特定のタイム フレーム用にカスタマイズできます。チャートまたはチャート上の交差点をナビゲートすると、役に立つ追加情報が表示されます。

図 1-2 に、[Traffic] タブをクリックすると表示できるトラフィック ダッシュボードの例を示します。

図 1-2 WAAS Central Manager : [Dashboard Traffic] タブ



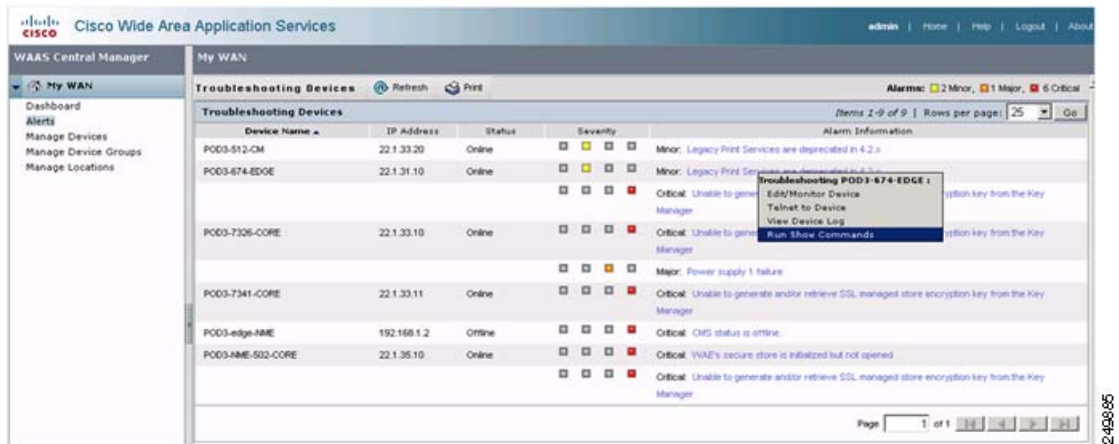
ダッシュボードには、存在する可能性があるネットワーク全体のアラームも表示されます。アラームのハイパーリンクにナビゲートするか、単にクリックすると、追加情報が示されます。[Active Alarms] タブから、アラームの確認応答を行うことができます。その後、アラームは [Acknowledged Alarms] タブに移動されます。

アラームは、問題が WAAS 環境に与える可能性がある影響に応じて、[Critical]、[Major]、または [Minor] に分類されます。フィルタ オプションを使用して、アラームを重大度、デバイスの IP アドレスまたは名前など別に表示できます。フィルタの一致基準では大文字と小文字が区別されます。

## アラームの表示

[My WAN] > [Alerts] を選択して、アラームを表示できます。[Troubleshooting Devices] ウィンドウが表示されます (図 1-3 を参照)。

図 1-3 WAAS Central Manager : [Troubleshooting Devices]



画面には、デバイスごとに処置を行うか、アラームの確認応答を行うことができる未処理のアラームのわかりやすい全体図が示されます。

一般的なアラームは次のとおりです。

#### アラーム 17001 (join\_timeout) : 「WCCP service join timeout.」

[Severity] : [Major]

カテゴリ : 通信

説明 : デバイスが 10 分以内に WCCP サービス グループに参加できません。WAAS WAE が参加するまで、WAE へのトラフィックのリダイレクトを行うことはできません。

処置 : このアラームを表すファーム内のすべての WAE で WCCP をディセーブルにして、5 分待機してから、これらの WAE で WCCP を再度イネーブルにして、WCCP 設定を再開します。

#### アラーム 17002 (rtr\_unreachable) : 「WCCP Router Unreachable Alarm.」

[Severity] : [Major]

カテゴリ : 通信

説明 : デバイスが 30 秒を超えてルータから ISU を受信できません。ルータと WAE 間のネットワーク接続が停止しているか、WAE での WCCP 設定がルータの設定と整合していません。この状況によって、WCCP ファーム内のルータに参加できなくなります。

処置 : アラームを出したルータと WAE で設定を確認します。アラームを出した WAE とルータ間の接続を確認します。

#### アラーム 17003 (rtr\_unusable) : 「WCCP Router Unusable Alarm.」

[Severity] : [Minor]

カテゴリ : 通信

説明 : 一致しない機能が原因で、デバイスが WCCP ファームに参加できません。割り当て方式、リダイレクト方式、またはリターン方式が、ルータによって提供される機能と一致しません。

処置 : WAE またはルータで機能設定を確認して、ファームでサポートされる機能と一致するよう変更します。

**アラーム 17004 (missing\_assignment) : 「WCCP Missing Assignment alarm.」**

[Severity] : [Major]

カテゴリ : 通信

説明 : デバイスは WCCP ファームに参加していますが、割り当てがありません。デバイスへのトラフィックのリダイレクトは行われません。これが発生する考えられる理由には、次のことがあります。1 : マスクの割り当てを使用する場合は、デバイスのマスク値がファームの残りとの整合していない。2 : デバイスが、ファームでの重みがより高い他のデバイスへの割り当てをすべて失った。3 : デバイスが、ファーム内のすべてのルータと通信できないため、割り当てを付与されない。ファームでの変更後 3 分以内に WAE で割り当てを取得しないと、アラームが出されます。

処置 : 設定と、すべてのルータへの接続を確認して、必要に応じて是正処置を行います。

**アラーム 17005 (mask\_mismatch) : 「Configured mask mismatch for WCCP.」**

[Severity] : [Major]

カテゴリ : 通信

説明 : 設定済みのマスクがファームの作動可能マスクと一致しないため、デバイスが WCCP ファームに参加できません。WAAS WAE が参加するまで、WAE へのトラフィックのリダイレクトを行うことはできません。

処置 : すべての WAE で WCCP マスク設定を調べて、同じマスクで設定されていることを確認します。

**アラーム 330001 (svcdisabled) : 「-service name- service has been disabled.」**

[Severity] : [Critical]

カテゴリ : 処理

説明 : 指定されたサービスの再開をノード マネージャが試行しましたが、サービスは再開し続けました。再開回数が内部制限を超え、サービスがディセーブルにされました。

処置 : サービスを再度イネーブルにするには、デバイスのリロードが必要な可能性があります。

**アラーム 330002 (servicedead) : 「-service name- service failed.」**

[Severity] : [Critical]

カテゴリ : 処理

説明 : 重要なサービスで障害が発生しました。このサービスの再開を試行しますが、デバイスは低下状態で実行される可能性があります。

処置 : デバイスは、不安定さを回避するために自動的にリブートすることがあります。Syslog で、サービスの障害の原因に関連するメッセージを調べます。

**アラーム 335000 (alarm\_overload) : 「Alarm Overload State has been entered.」**

[Severity] : [Critical]

カテゴリ : Quality Of Service

説明 : Node Health Manager は、オーバーロードしきい値を超えるレートでデバイスがアラームを出していることを示すためにこのメッセージを出します。

処置 : デバイスにアクセスして、アラームを出しているサービスを判別します。個々のサービスの問題を解決するために是正処置を行います。

**アラーム 335001 (keepalive) : 「Keepalive failure for -application name-.Timeout = n seconds.」**

[Severity] : [Critical]

カテゴリ : Quality Of Service

説明 : Node Health Manager は、アプリケーションが過去  $n$  秒間に Node Health Manager に対してキープアライブを発行していないことを示すためにこのメッセージを出します。アプリケーションのヘルスに問題があります。

処置 : デバイスにアクセスして、特定のアプリケーションの状態を判別します。アプリケーションの正しい実行を妨げている問題を解決するために是正処置を行います。

**アラーム 445000 (disk\_failure) : 「A disk has failed.」**

[Severity] : [Critical]

カテゴリ : 装置

説明 : System Monitor は、デバイスに接続されているいずれかのディスクで重大エラーが発生していることを示すためにこのメッセージを発行します。

処置 : デバイスにアクセスして、**show disk details** CLI コマンドを実行します。問題が解決しない場合は、ディスクを交換します。

**アラーム 445001 (core\_dump) : 「A user core file has been generated.」**

[Severity] : [Major]

カテゴリ : 処理

説明 : System Monitor は、1 つ以上のソフトウェア モジュールがコア ファイルを生成したことを示すためにこのメッセージを発行します。

処置 : デバイスにアクセスして、/local1/core\_dir ディレクトリを確認し、FTP からコア ファイルを取得して、Cisco TAC にご連絡ください。

**アラーム 445013 (powerdown) : 「Power supply is down.」**

[Severity] : [Major]

カテゴリ : 処理

説明 : System Monitor は、いずれかの電源装置が停止していることを示しています。

処置 : 電源装置を確認します。

**アラーム 445019 (license\_failure) : 「WAAS product license is missing.」**

[Severity] : [Critical]

カテゴリ : 処理

説明 : System Monitor は、WAAS 製品ライセンスを購入していないか、License Management システムが設定されていないことを示しています。

処置 : **show license** CLI コマンドを実行して、License Management システムが設定されていることを確認します。WAAS 製品ライセンスを購入して、**license add** コマンドを使用して License Management システムを設定します。

**アラーム 445022 (eth\_detection\_failed) : 「Detection of one of the network interfaces has failed.」**

[Severity] : [Critical]

カテゴリ : 装置

説明：System Monitor は、システム ネットワーキング ハードウェアで重大エラーが発生していることを示しています。インターフェイスと関連機能は正しく機能しません。

処置：デバイスをリブートします。アラームが消えない場合は、BIOS 設定をデフォルトにリセットしてから、再度リブートします。アラームが消えない場合は、Cisco TAC にご連絡ください。

#### アラーム 700002 (cms\_clock\_alarm) : 「Device clock is not synchronized with the primary CM.」

[Severity] : [Major]

カテゴリ：環境

説明：このデバイスが WAE である場合は、クロックをプライマリ WAAS Central Manager と同期して、統計情報、ステータス モニタリング、およびイベント スケジューリングのような時間に依存する機能を正しく機能させる必要があります。このデバイスがスタンバイ WAAS Central Manager である場合は、クロックをプライマリ WAAS Central Manager と同期して、WAAS Central Manager フェールオーバーを機能させる必要があります。

#### アラーム 700006 (cms\_wae\_secure\_store) : 「Secure Store is initialized but not opened.」

[Severity] : [Critical]

カテゴリ：環境

説明：WAE のセキュア ストアは初期化されていますが、ユーザによって開かれていません。WAE は、WAAS Central Manager からの更新に、事前展開、動的共有、および WAFS コア パスワードとユーザ設定に対する更新が含まれている場合、セキュア ストアが開くまで、そのような更新を拒否します。

処置：**cms secure-store open** CLI コマンドを使用するか、WAAS Central Manager GUI でパスワードを入力して、セキュア ストアを開きます。

#### アラーム 700008 (mstore\_key\_retrieval\_failure) : 「CMS/Management agent failed to generate and/or retrieve SSL managed store encryption key from Key Manager.」

[Severity] : [Critical]

カテゴリ：処理

説明：このアラームは、次のいずれかの問題を示しています。

- WAAS Central Manager デバイスに到達できない。
- WAAS Central Manager のセキュア ストアは初期化されているが、開いていない。
- WAAS Central Manager デバイスでの Key Manager プロセスが実行されていないか、応答していない。
- Key Manager が、キーの生成または取得要求を処理できない。この問題が発生すると、WAAS デバイスは、WAAS Central Manager から受信した設定更新に SSL 証明書とキー ペア情報が含まれている場合に、そのような更新を処理できません。

処置：WAAS Central Manager デバイスが到達可能かどうか（ポート 443 での WAE から WAAS Central Manager への TCP 接続）を確認します。次のログ ファイルで、エラーに関する追加情報を調べます。

- WAE の場合：WAE の /local1/errorlog/kc.log
- WAAS Central Manager の場合：/local1/errorlog/km/km.log

処置：デバイスまたはプライマリ WAAS Central Manager のクロックを修正します。

アラーム状態の全リストについては、Cisco.com の [WAAS 4.2.1 Software Download](#) 領域にある『Alarm Book』を参照してください。



## WAE デバイス ステータスの表示

[Cisco WAAS Central Manager devices] ページには、その特定の WAAS Central Manager に登録されており、ネットワーク全体に配置されている各 Cisco WAE のクイック ステータスの概要が表示されます。デバイスを管理するには、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます (図 1-4 を参照)。

図 1-4 WAAS Central Manager : [Manage Devices]

Device Name	Service	IP Address	CMS Status	Device Status	Location	Software Version	Hardware Type
POD1-612-EDGE2-POD3-...	CM (Standby)	22.1.33.21	Online	Online		4.2.1	OE612
POD3-512-CM	CM (Primary)	22.1.33.20	Online	Online		4.2.1	OE512
POD3-674-EDGE	Print, Application Accelerator	22.1.31.10	Online	Online	ibon	4.2.1	OE674
POD3-7326-CORE	Application Accelerator	22.1.33.10	Online	Online	POD3-7326-CORE-location	4.2.1	OE7326
POD3-7341-CORE	Application Accelerator	22.1.33.11	Online	Online	POD3-7341-CORE-location	4.2.1	OE7341
POD3-edge-NME	Application Accelerator	192.168.1.2	Offline	Offline	POD3-edge-NME-location	4.2.0	NM-WAE
POD3-NME-502-CORE	Application Accelerator	22.1.35.10	Online	Online	test-loc	4.2.1	NM-WAE
SRE-900	Application Accelerator	192.168.1.2	Online	Online	SRE-900-location	4.2.1	SM-WAE

各デバイスによって、オンラインまたはオフラインのいずれかの CMS ステータスが報告されます。これは、その時点の Cisco WAE の状態を管理者に警告します。Central Management System (CMS) サービスがディセーブルになっているか、その特定の Cisco WAE へのネットワーク接続が使用不可の場合は、オフラインとして報告されます。WAAS Central Manager は、設定データをオフラインの Cisco WAE と同期できず、新規のレポートデータを取得できません。

デバイスがオフラインとして表示される場合は、Telnet または SSH を使用してデバイスにアクセスし、**show cms info** コマンドを入力することで、ステータスを確認します。さらに、**show stat connection** などのコマンドを使用して、デバイスがトラフィック最適化に参加していることを確認する必要があります。

[Devices] ウィンドウには、デバイス名、サービス モード、IP アドレス、ソフトウェア バージョンなどの重要な情報も表示されます。理想的には、WAAS ネットワーク内のすべての WAE が同じ OS バージョンを実行している必要があります。最小でも、プライマリ WAAS Central Manager とセカンダリ WAAS Central Manager (存在する場合) は同じバージョンになっている必要があります。

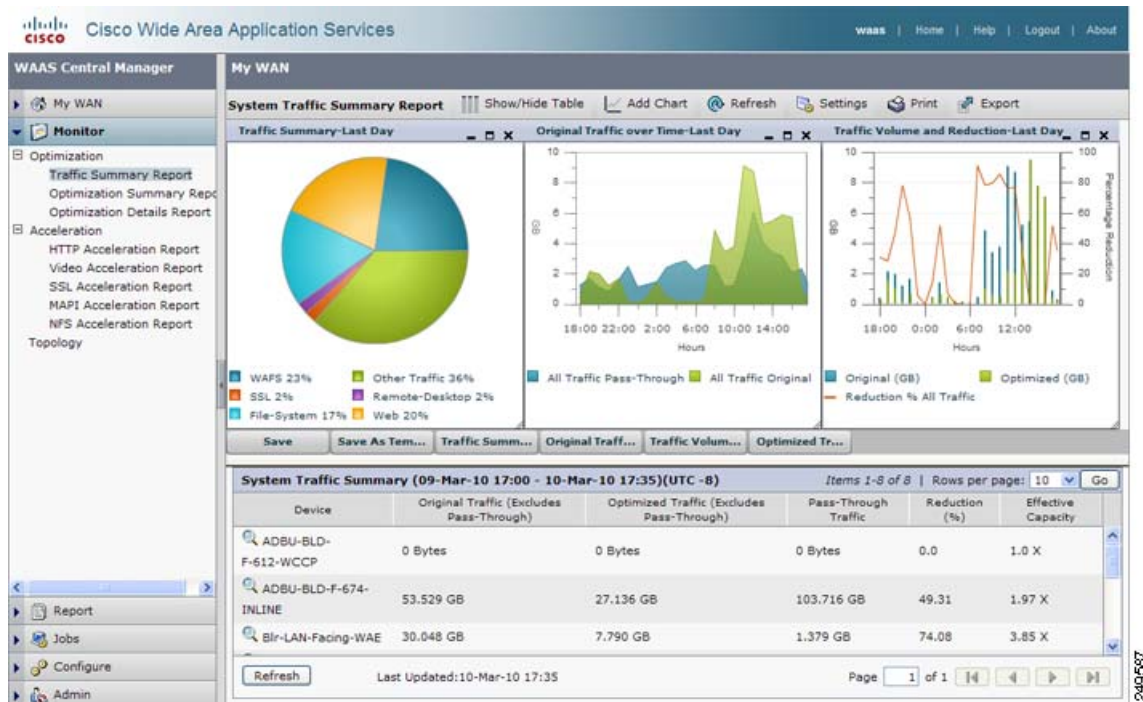
デバイス ヘルスは、デバイス ステータスによって示され、未処理のアラームが強調表示されます。デバイス アイコンをクリックすることで、そのデバイスにナビゲートできます。大規模の配置では、[Filter] オプションを使用して、デバイス名、サービス モード、およびステータス別にデバイスを表示します。

## 最適化のモニタリング

システム全体のトラフィック統計情報にアクセスするには、[My WAN] > [Monitor] > [Optimization] > [Traffic Summary Report] を選択します。[System Traffic Summary Report] ウィンドウが表示されます (図 1-5 を参照)。



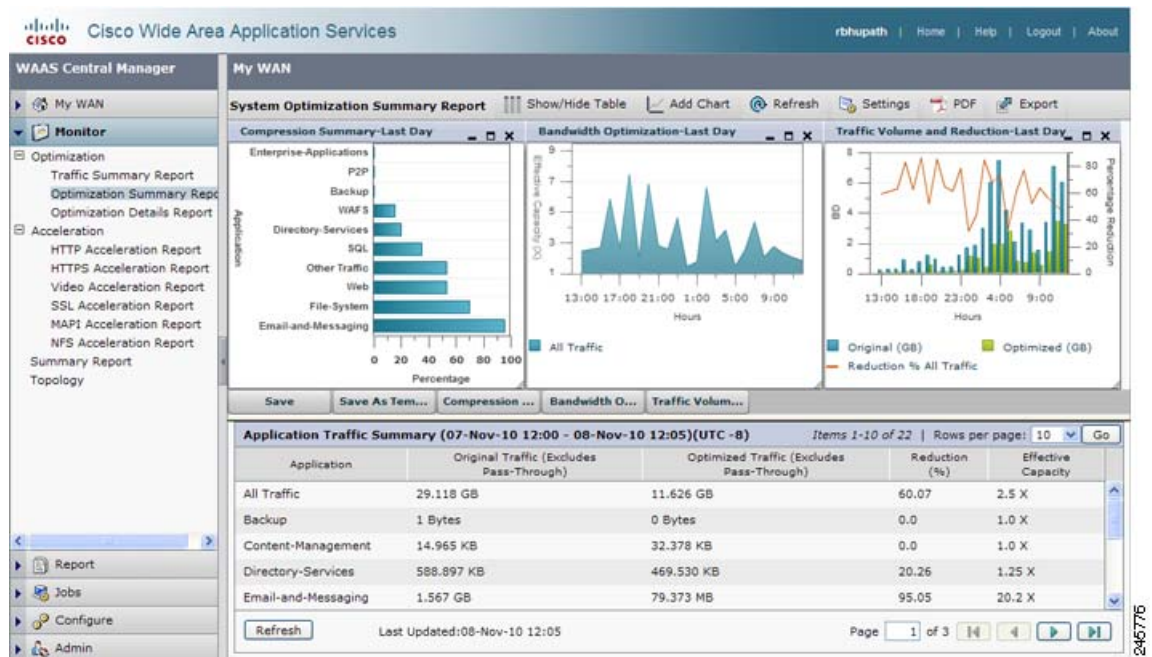
図 1-5 WAAS Central Manager : [System Traffic Summary Report]



最適化とプロトコルに固有のアプリケーション アクセラレータの両方のアクセラレーション レポートで、いくつかのレポート オプションを使用できます。[System Traffic Summary] テーブルには、WAAS デバイスが最適なトラフィック アクセラレーション用に正しく設定されているかどうかを判別するのに役立つ、デバイスレベルの最適化統計情報が示されます。

システム全体の最適化統計情報にアクセスするには、[My WAN] > [Monitor] > [Optimization] > [Optimization Summary Report] を選択します。[System Optimization Summary Report] ウィンドウが表示されます (図 1-6 を参照)。

図 1-6 最適化概要レポート



[System Optimization] レポートには、アプリケーション レベルの最適化レポートが示され、削減率と有効容量が強調表示されます。このデータを使用して、ポリシーを変更し、最適化オプションを調整できます。

[Acceleration] レポートには、デバイスレベルのアプリケーション アクセラレータに固有の統計情報が示されます。

## システム動作のモニタリング

システム動作をモニタリングするには、[My WAN] > [Monitor] > [Summary Report] を選択します。[Summary Report] が表示されます。

図 1-7 [Summary Report]

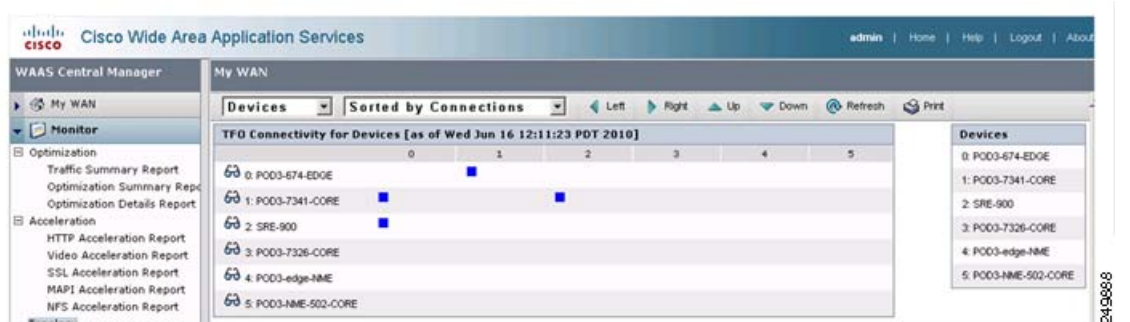


サマリー レポートはシステム動作のモニタリングに使用できる事前定義されたレポートです。サマリー レポートをカスタマイズして必要なチャートを表示できます。[Add Chart] オプションを使用してこのレポートに表示するチャートを選択します。レポートには 12 までのチャートが表示できます。[Settings] オプションを使用してチャートの設定をカスタマイズできます。

## トポロジのモニタリング

ピアリング関係を表示するには、[My WAN] > [Monitor] > [Topology] を選択します。[TFO Connectivity for Devices] ウィンドウが表示されます（図 1-8 を参照）。ピア間の最適化には、双方向関係が必要です。

図 1-8 WAAS Central Manager : [TFO Connectivity for Devices]

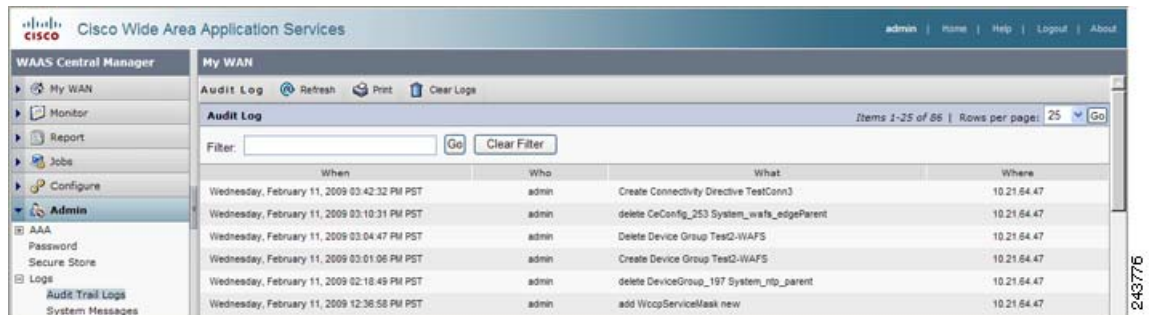


トポロジ情報は、トラブルシューティングと配置のサイズ変更（特にサイト間の通信が必要な大規模な配置の場合）で重要です。

## 監査証跡ログ、システム メッセージ、および WAAS Central Manager ログのモニタリング

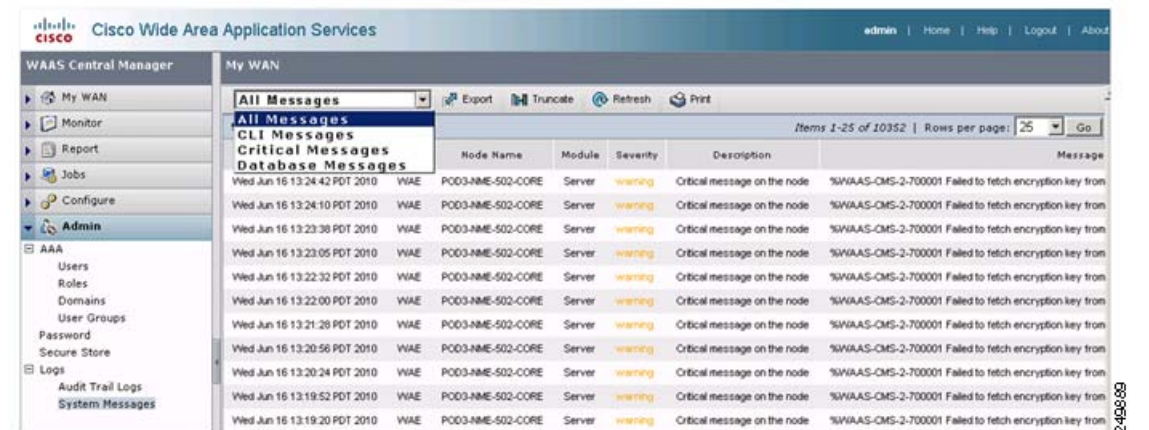
監査証跡ログを表示して、WAAS Central Manager GUI を使用して作成した特定のユーザによって実行された最後のアクションを追跡できます。このログを使用して、WAAS デバイス用に 2 つの異なるタイプの管理者ユーザ アカウント（デバイススペースの CLI アカウントとロールベースのアカウント）を一箇所で作成して管理できます。監査証跡ログを表示するには、[My WAN] > [Admin] > [Logs] > [Audit Trail Logs] を選択します。[Audit Trail Logs] ウィンドウが表示されます（図 1-9 を参照）。

図 1-9 WAAS Central Manager : [Audit Trail Logs]



システム全体のシステム ログを表示するには、[My WAN] > [Admin] > [Logs] > [System Messages] を選択します。[System Messages] ウィンドウが表示されます（図 1-10 を参照）。CLI メッセージ、重大メッセージ、またはデータベース メッセージを表示するには、[System Messages] を選択します。

図 1-10 WAAS Central Manager : [System Messages]



可能なエラーの完全なリストについては、Cisco.com の [WAAS 4.2.1 Software Download](#) エリアにある『Error Message Book』を参照してください。

WAAS Central Manager ログを表示するには、[My WAN] > [Devices] > [WAAS-CM] > [Admin] > [Logs] を選択します。[System Messages Log] ウィンドウが表示されます（図 1-11 を参照）。



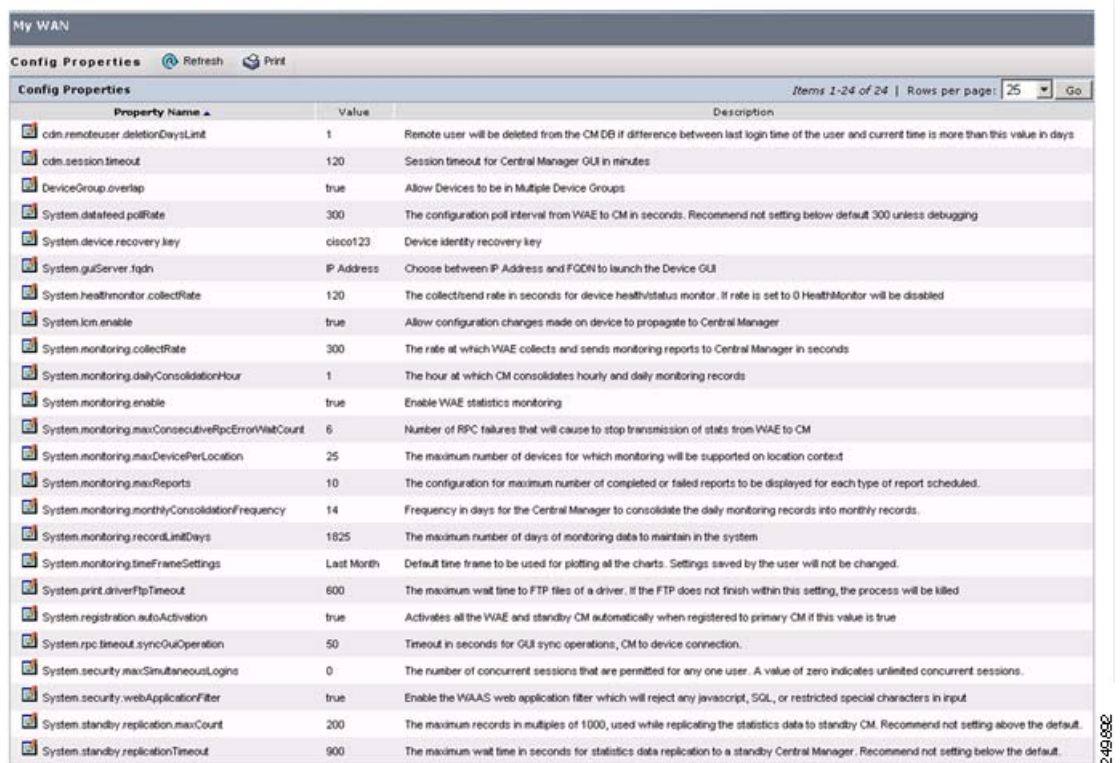
図 1-11 図 8 : WAAS Central Manager : [System Messages Log]



## システム プロパティの表示

現在のシステム プロパティを表示して変更するには、[My WAN] > [Configure] > [System Properties] を選択します。[Config Properties] ウィンドウが表示されます (図 1-12 を参照)。このウィンドウから、設定済みのシステム プロパティを変更して、システムのデフォルトの動作を変更できます。詳細については、『Cisco Wide Area Application Services Configuration Guide』の「[Configuring Other System Settings](#)」の章を参照してください。

図 1-12 WAAS Central Manager : [System Properties]



## WAAS デバイス ヘルスのモニタリング

WAAS Central Manager を使用して、WAAS ネットワーク内のすべてのデバイスをモニタおよび設定できます。WAAS Central Manager は、WAAS デバイス設定に関する詳細情報、デバイス ハードウェア統計情報、およびトラフィック最適化レポートを提供します。

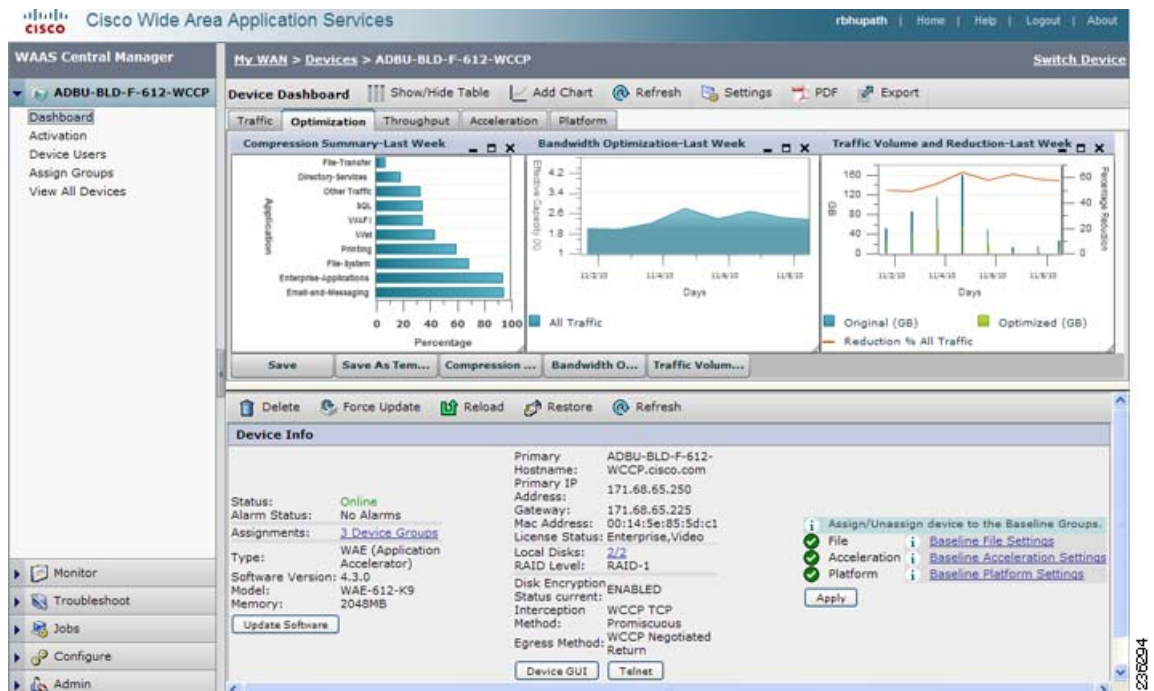
ここでは、次の内容について説明します。

- 「[Device Dashboard] の表示」 (P.1-14)
- 「最適化レポートの表示」 (P.1-15)
- 「接続統計情報の表示」 (P.1-15)
- 「アクセラレーション レポートの表示」 (P.1-17)
- 「CPU 統計情報の表示」 (P.1-18)
- 「ディスク ヘルスとステータスの表示」 (P.1-19)
- 「デバイス ピアリング ステータスの表示」 (P.1-19)
- 「デバイス ログの表示」 (P.1-20)
- 「WAAS Central Manager GUI からの CLI コマンドの実行」 (P.1-20)

### [Device Dashboard] の表示

デバイスを個別に管理するには、[My WAN] > [Devices] > [Device\_Name] を選択します。[Device Dashboard] ウィンドウが表示されます (図 1-13 を参照)。

図 1-13 WAAS Central Manager : [Device Dashboard]

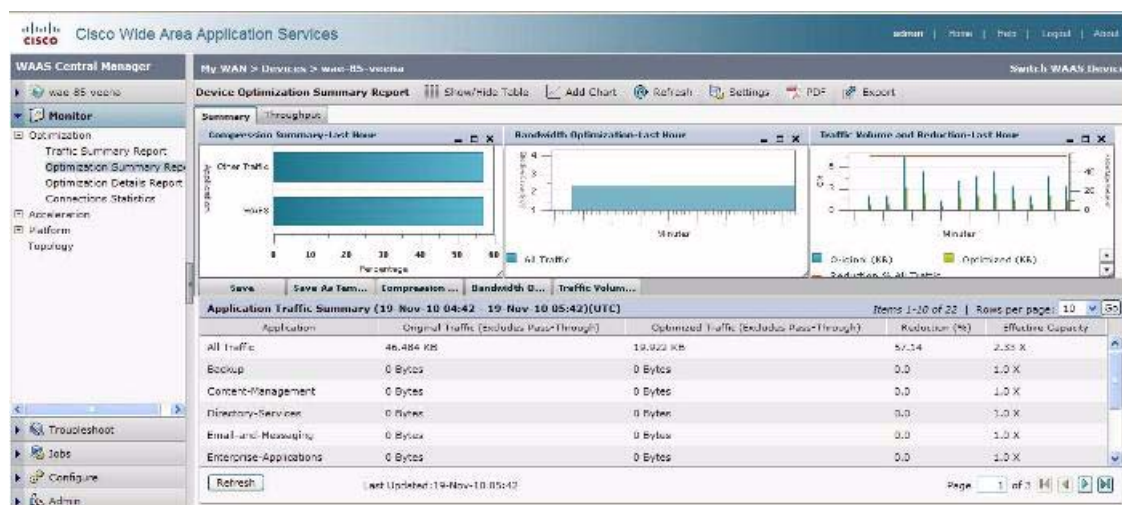


[Device Dashboard] には、WAAS ハードウェアとソフトウェア、設定済みの代行受信メカニズムなど、デバイスの概要が示されます。チャートをカスタマイズして、カスタム設定を保存できます。デバイスの GUI またはデバイスへの Telnet にアクセスすることもできます。

## 最適化レポートの表示

最適化レポートを表示するには、[My WAN] > [Devices] > [Device\_Name] > [Monitor] > [Optimization] > [Optimization Summary Report] を選択します。[Device Optimization Summary Report] ウィンドウが表示されます (図 1-14 を参照)。

図 1-14 WAAS Central Manager : [Device Optimization Summary Report]



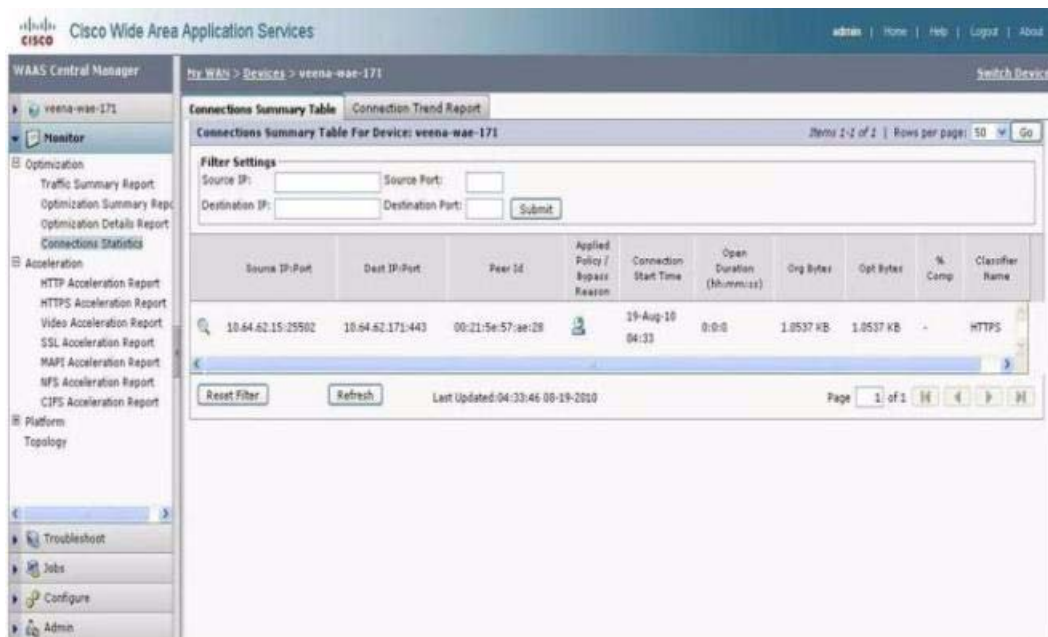
このレポートにはサマリー レポートとスループット レポートが含まれます。最適化レポートには、事前定義されたアプリケーションのトラフィック最適化統計情報、および最大の最適化が実現されるアプリケーションと追加の微調整が必要な可能性があるアプリケーションに関する見識が示されます。

最適化レポートの詳細については、『Cisco Wide Area Application Services Configuration Guide』の「[Monitoring and Troubleshooting Your WAAS Network](#)」の章を参照してください。

## 接続統計情報の表示

接続ごとの統計情報を表示するには、[My WAN] > [Devices] > [Device\_Name] > [Monitor] > [Optimization] > [Connection Statistics] を選択します。接続統計情報レポートにはデバイスの [Connections Summary Table] (図 1-15 を参照) と [Connection Trend Report] (図 1-15 を参照) が表示されます。

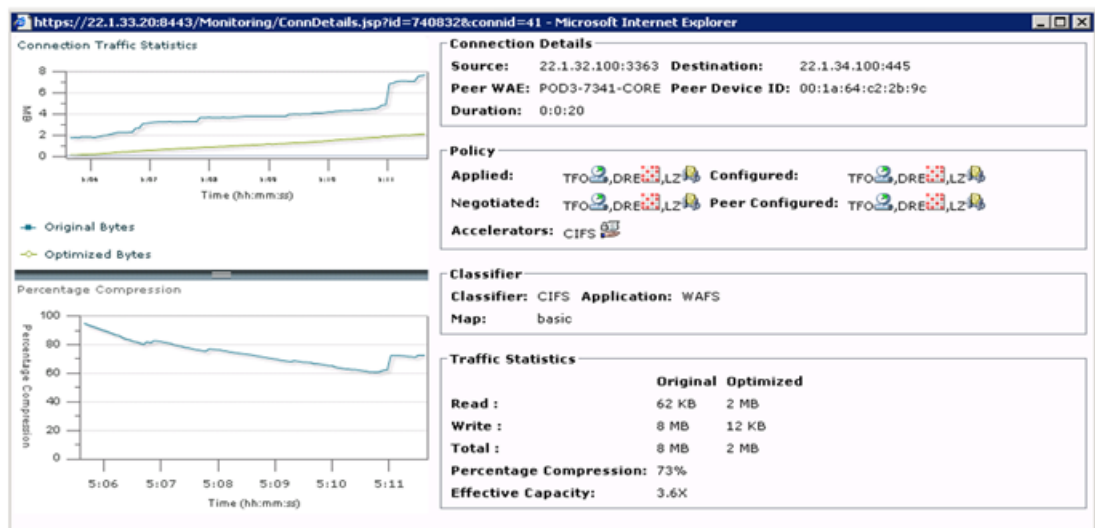
図 1-15 WAAS Central Manager : [Connections Summary Table]



[Connections Summary Table] には、選択した WAE 別にアクティブなすべてのフローの一覧が示されます。出力では、トラフィックのタイプ、ピア ID、圧縮率、適用されるポリシーなどを強調表示することでフローに関する重要な詳細が示されます。

フローごとに追加の詳細を表示するには、虫眼鏡アイコンをクリックします。フローの詳細ポップアップウィンドウが開き、トラブルシューティングまたはレポート作成に使用できる、ある時間にわたる接続統計情報が示されます (図 1-16 を参照)。このポップアップウィンドウは自動的に更新されます。

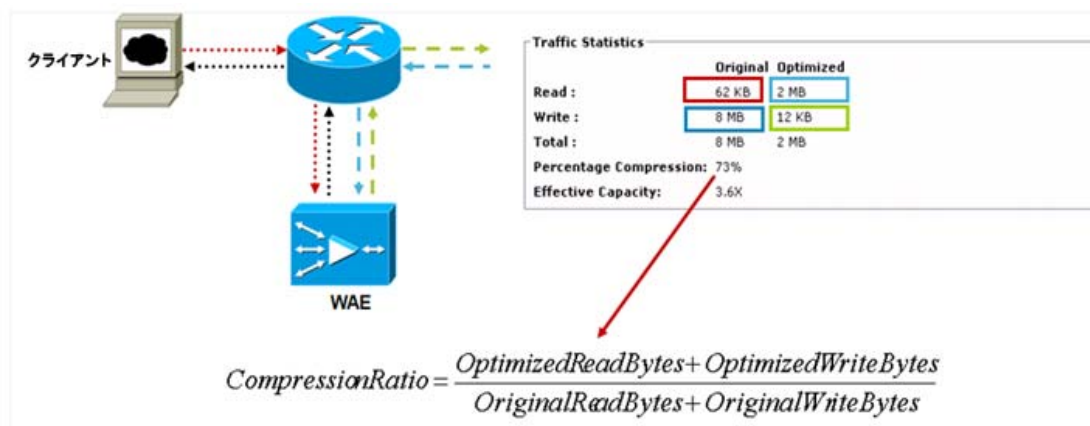
図 1-16 WAAS Central Manager : [Flow Details Pop-Up] ウィンドウ



トラフィック統計情報は、圧縮率、有効容量、および元のソケットと最適化済みソケットのバイト値を提供します。図 1-17 で、表示されるデータの解釈方法について説明します。

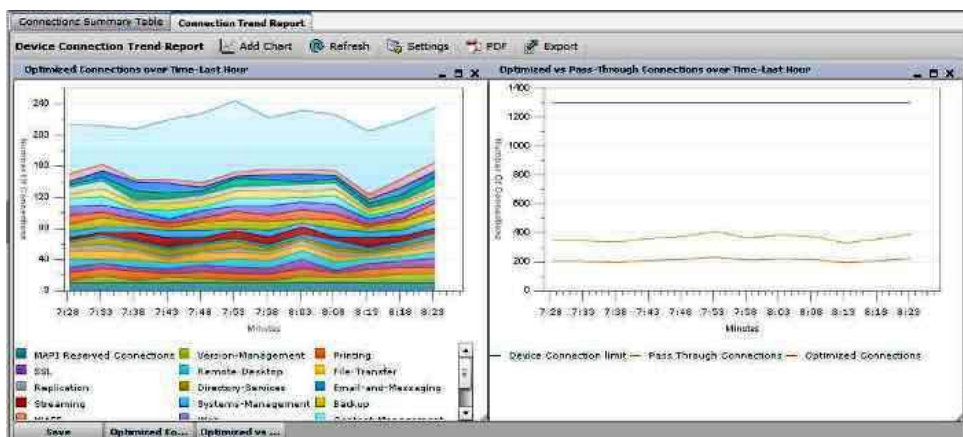


図 1-17 トラフィック統計情報の解釈



[Connection Trend Report] にはデバイス上で処理され、最適化されたすべてのトラフィックのパススルー接続に関するデータが示されます。このデータを使用してデバイス上のすべてのアプリケーションの接続傾向をモニタリングできます。

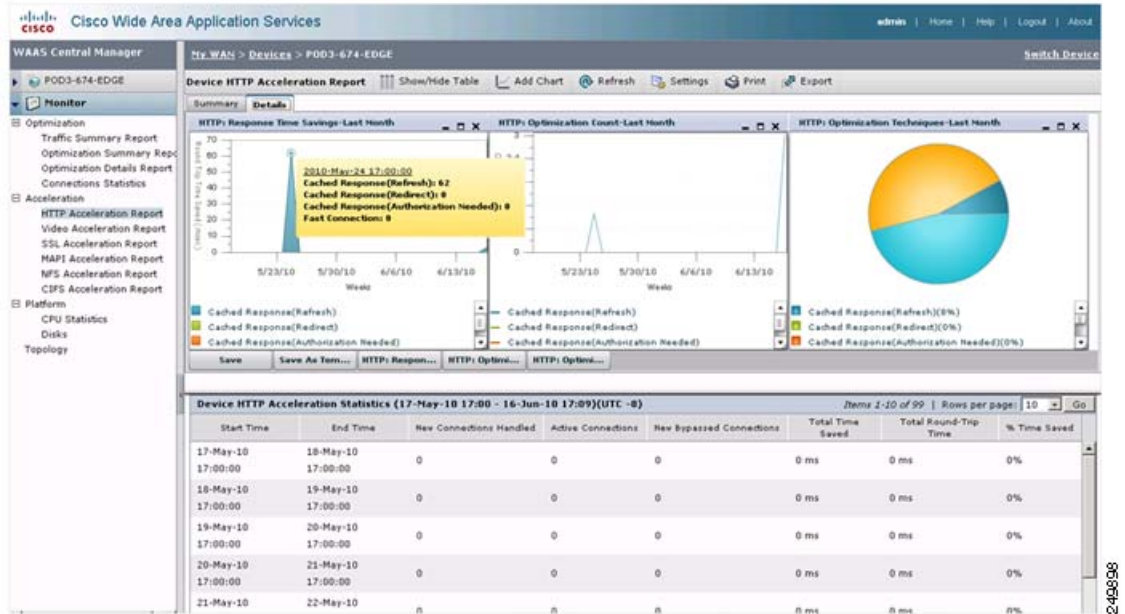
図 1-18 [Connection Trend Report]



## アクセラレーション レポートの表示

アプリケーション最適化装置のアクセラレーション レポートを表示するには、[My WAN] > [Devices] > [Device\_Name] > [Monitor] > [Acceleration] > [HTTP Acceleration Report] を選択します。[Device HTTP Acceleration Report] ウィンドウが表示されます (図 1-19 を参照)。

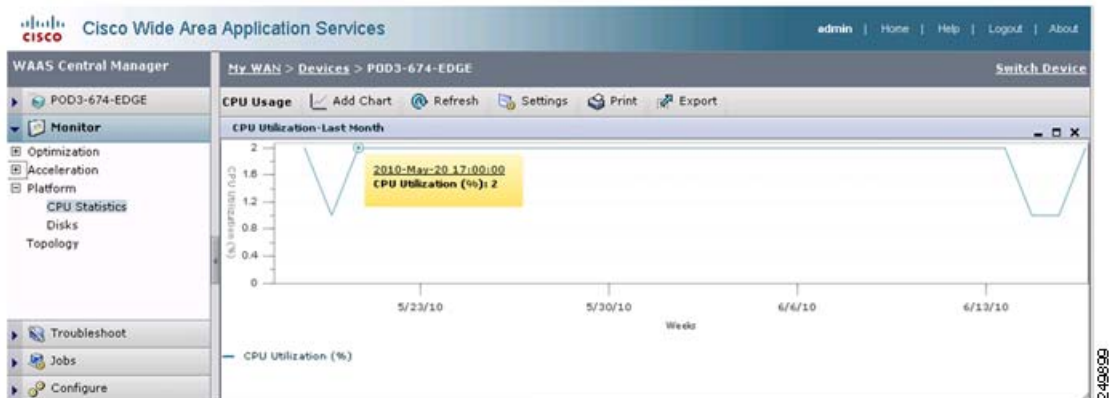
図 1-19 WAAS Central Manager : [Device HTTP Acceleration Report]



## CPU 統計情報の表示

WAAS デバイスの CPU 使用率を表示するには、[My WAN] > [Devices] > [Device\_Name] > [Monitor] > [Platform] > [CPU Statistics] を選択します。[CPU Usage] ウィンドウが表示されます（図 1-20 を参照）。

図 1-20 WAAS Central Manager : [CPU Usage]



完全なビューについては、CPU グラフの時間の長さを週または月に変更します。高い CPU 使用率は、必ずしも問題が発生していることを意味しているわけではありません。これは、最適化の低下を除外するために、他の統計情報と組み合わせて調べる必要があります。考慮すべき他の要因には、最適化の低下または低い圧縮などがあります。

## ディスク ヘルスとステータスの表示

個々の WAE のディスク ステータスを確認するには、[My WAN] > [Devices] > [Device Name] > [Monitor] > [Platform] > [Disk] を選択します。デバイスの [Disk Information] ウィンドウが表示されます（図 1-21 を参照）。

図 1-21 WAAS Central Manager : [Disk Information]

The screenshot shows the Cisco Wide Area Application Services (WAAS) Central Manager interface. The breadcrumb navigation is: My WAN > Devices > ADBU-BLD-F-674-INLINE. The main content area displays the Disk Information for the device ADBU-BLD-F-674-INLINE. It includes a table of Physical Disks and a section for Disk Information.

Name	Serial Number	Size	Present	Operational Status	Administrative Status
disk00	BJ5037BH	286102MB	YES	Online	ENABLED
disk01	BJ50379M	286102MB	YES	Online	ENABLED
disk02	BJ502YHW	286102MB	YES	Online	ENABLED

Below the table, the Disk Information section shows the following details:

- Disk Encryption Status current: ENABLED
- Disk Encryption Status future: ENABLED
- Extended Object Cache Status current: DISABLED
- Extended Object Cache Status future: DISABLED
- Raid Level: RAID-5
- Raid Device Name: Drive 1
- Raid Status: Okay
- Raid Device Size: 571890MB

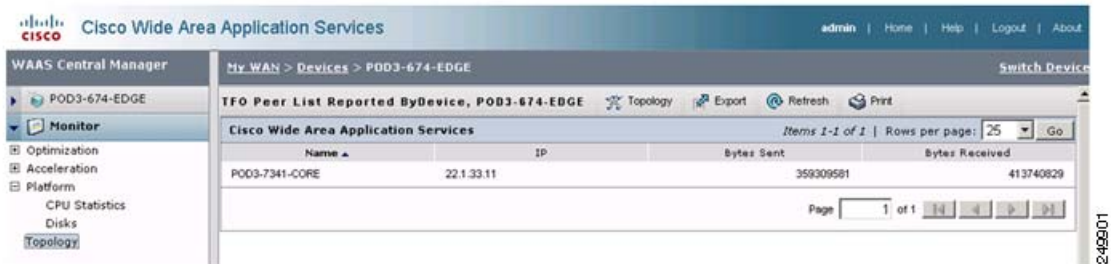
動作上のステータスは、[Online]、[Defunct]、[Missing]、[<null>]、または [Rebuilding] です。通常の作動条件下では、動作上のステータスは [Online] でなければなりません。[Rebuilding] ステータスは、RAID ペアが進行中であり、しばらく（ディスク サイズと WAE のハードウェア プラットフォームによって異なる）してからクリアする必要があることを示しています。

ビューには、ディスク サイズ、RAID、ディスクの暗号化、および拡張 CIFS キャッシュ機能のステータスも表示されます。

## デバイス ピアリング ステータスの表示

任意の時点におけるデバイス ピアリング ステータスを表示して、トラフィック フローとこれらのトラフィック フローの最適なアクセラレーションを検証するには、[My WAN] > [Devices] > [Device Name] > [Monitor] > [Topology] を選択します。デバイスの [TFO Peer List] ウィンドウが表示されます（図 1-22 を参照）。

図 1-22 WAAS Central Manager : [TFO Peer List]



ピア リストには、ピアごとに送受信されたデータに関する詳細が示されます。すべてのトラフィックは、データ センターからブランチ サイトに向かって流れている必要があるため、ブランチ サイトの WAE での受信数はより高い必要があります。

全体的なトポロジを表示するには、[Topology] アイコンをクリックします。

## デバイス ログの表示

デバイス ログを表示するには、[My WAN] > [Devices] > [Device Name] > [Admin] > [Logs] を選択します。[System Message Log] ウィンドウが表示されます（図 1-23 を参照）。

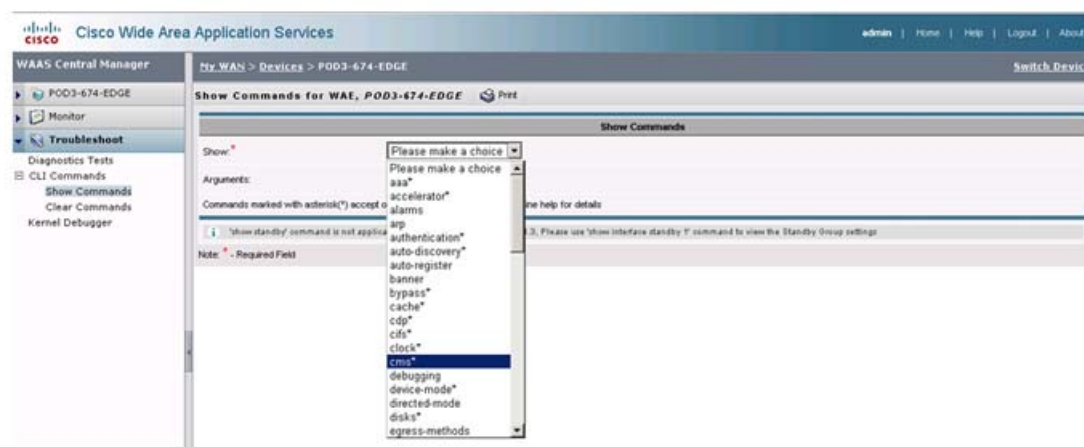
図 1-23 WAAS Central Manager : [System Message Log]



## WAAS Central Manager GUI からの CLI コマンドの実行

さまざまな CLI `show` コマンドを実行して、役に立つ追加情報を表示するには、[My WAN] > [Devices] > [Device Name] > [Troubleshoot] > [CLI Commands] > [Show Commands] を選択します。[Show Commands for WAAS] ウィンドウが表示されます（図 1-24 を参照）。

図 1-24 WAAS Show コマンド



コマンド出力を表示するには、コマンドのドロップダウンリストから **show** コマンドを選択して、任意のオプションのコマンド引数を指定します。出力はポップアップ ウィンドウで表示されます。その後に表示されるセクションでは、一部の **show** コマンドの出力に関する説明が示されます。コマンドオプションと出力に関する詳細については、『*Cisco Wide Area Application Services Command Reference*』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。

- 「[show cms info コマンド出力](#)」 (P.1-21)
- 「[show wccp service コマンド出力](#)」 (P.1-22)
- 「[show wccp gre コマンド出力](#)」 (P.1-22)
- 「[show statistics connection コマンド出力](#)」 (P.1-23)
- 「[show statistics connection optimized cifs コマンド出力](#)」 (P.1-24)
- 「[show statistics accelerator cifs detail コマンド出力](#)」 (P.1-24)
- 「[show statistics dre コマンド出力](#)」 (P.1-25)
- 「[show statistics tfo コマンド出力](#)」 (P.1-25)
- 「[show interface gig 1/0 コマンド出力](#)」 (P.1-26)
- 「[show tech-support コマンド出力](#)」 (P.1-27)

## show cms info コマンド出力

**show cms info** コマンド出力は、WAE 登録情報と、WAAS Central Manager との最後の設定同期時刻を提供します。これは、アプリケーション ポリシー設定の問題の疑いがある場合に役立ちます (図 1-25 を参照)。

図 1-25 コマンド出力 : show cms info

```

Output of command - show cms info

Device registration information :
Device Id                = 740832
Device registered as     = WAAS Application Engine
Current WAAS Central Manager = 22.1.33.20
Registered with WAAS Central Manager = 22.1.33.20
Status                   = Online
Time of last config-sync = Wed Jun 16 21:27:45 2010

CMS services information :
Service cms_ce is running

```

## show wccp service コマンド出力

**show wccp service** コマンド出力は、WAE がサービス グループ 61 と 62 に対して設定されているかどうかを示します (図 1-26 を参照)。

図 1-26 コマンド出力 : show wccp service

```

Output of command - show wccp service

Services configured on this Wide Area Engine
TCP Promiscuous 61
TCP Promiscuous 62

```

## show wccp gre コマンド出力

**show wccp gre** コマンド出力には、3 つの受信パケット数カウンタが含まれています。そのうちの 1 つは、増加して、WAE がリダイレクト パケットを受信していることを示している必要があります (図 1-27 を参照)。



図 1-27 コマンド出力 : show wccp gre

Output of command - show wccp gre	
Transparent GRE packets received:	1616200
Transparent non-GRE packets received:	0
Transparent non-GRE non-WCCP packets received:	0
Total packets accepted:	1082524
Invalid packets received:	0
Packets received with invalid service:	0
Packets received on a disabled service:	0
Packets received too small:	0
Packets dropped due to zero TTL:	0
Packets dropped due to bad buckets:	0
Packets dropped due to no redirect address:	0
Packets dropped due to loopback redirect:	0
Pass-through pkts dropped on assignment update:	0
Connections bypassed due to load:	0
Packets sent back to router:	0
GRE packets sent to router (not bypass):	0
Packets sent to another WAE:	0

デバイスに高い負荷がかかっている、新しいフローを最適化できない場合は、[Bypass Due to Load] カウンタが増加します。このカウンタのゼロ以外の値は、デバイスで過負荷が生じているか、過負荷状態になったため、さらに調査が必要であることを示しています。

## show statistics connection コマンド出力

**show statistics connection** コマンド出力には、現在の最適化されたフロー、自動検出フロー、パストルーフロー、および予約済みフローが表示されます (図 1-28 を参照)。アクティブ接続ごとに削減率も表示されます。

図 1-28 コマンド出力 : show statistics connection

Output of command - show statistics conn						
Current Active Optimized Flows:						3
Current Active Optimized TCP Plus Flows:						1
Current Active Optimized TCP Only Flows:						1
Current Active Optimized TCP Preposition Flows:						0
Current Active Auto-Discovery Flows:						0
Current Reserved Flows:						15
Current Active Pass-Through Flows:						0
Historical Flows:						28
D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio						
A:AOIH,C:CIFS,E:EPH,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO						
ConnID	Source IP:Port	Dest IP:Port	PeerID	Accel	RR	
1	22.1.34.100:42300	22.1.32.100:3389	00:1a:64:c2:2b:9c	T	00.0%	
2	22.1.34.100:42308	22.1.31.10:50139	00:1a:64:c2:2b:9c	TDL	48.4%	
11	22.1.32.100:4009	22.1.34.100:445	00:1a:64:c2:2b:9c	TCDL	12.4%	

各フローの追加の詳細を表示するには、次のようにしてオプションの **conn-id** 引数を含めます。

**show statistics connection conn-id conn-id-number**

## show statistics connection optimized cifs コマンド出力

**show statistics connection optimized cifs** コマンド出力には、CIFS アプリケーション アクセラレータによって最適化される接続が表示されます (図 1-29 を参照)。

図 1-29 コマンド出力 : show statistics connection optimized cifs

```

Output of command - show statistics connection opt cifs

Current Active Optimized Flows:                3
  Current Active Optimized TCP Plus Flows:      1
  Current Active Optimized TCP Only Flows:      1
  Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows:           0
Current Reserved Flows:                        15
Current Active Pass-Through Flows:             0
Historical Flows:                              28

D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID      Source IP:Port      Dest IP:Port      PeerID Accel RR
-----
  11         22.1.32.100:4009    22.1.34.100:445  00:1a:64:c2:2b:9c TCDL 12.34
  
```

## show statistics accelerator cifs detail コマンド出力

**show statistics accelerator cifs detail** コマンド出力には、CIFS アプリケーション アクセラレータの統計情報が表示されます。これは、CIFS アプリケーション アクセラレータによって処理される接続をトラブルシューティングする際に役立ちます (図 1-30 を参照)。

図 1-30 コマンド出力 : show statistics accelerator cifs detail

```

Output of command - show statistics accelerator cifs det

CIFS:
  Global Statistics
  -----
  Time Accelerator was started:                Sat Jun  5 05:48:47 2010
  Time Statistics were Last Reset/Cleared:      Sat Jun  5 05:48:47 2010
  Total Handled Connections:                    7
  Total Optimized Connections:                  3
  Total Connections Handed-off with Compression Policies Unchanged: 0
  Total Dropped Connections:                   0
  Current Active Connections:                  1
  Current Pending Connections:                 0
  Maximum Active Connections:                  3
  Number of local reply generating requests:    9716
  Number of remote reply generating requests:  7930
  The Average time to generate a local reply (msec): 3
  Average time to receive remote reply (ms):   10503
  
```

出力では、アプリケーション アクセラレータによって処理される、現在アクティブなフローと履歴フローが強調表示されます。アプリケーション アクセラレータによっては、アプリケーションに固有の最適化の詳細を示す追加情報を使用できます。



## show statistics dre コマンド出力

**show statistics dre** コマンド出力には、エンコードとデコードの両方についての圧縮率が表示され、DRE の存続期間、使用可能なキャッシュ サイズ、および使用率に関する詳細が含まれています (図 1-31 を参照)。

図 1-31 コマンド出力 : show statistics dre

```

Output of command - show statistics dre

Cache:
Status: Usable, Oldest Data (age): 50d
Total usable disk size: 116735 MB, Used: 0.63%
Hash table RAM size: 436 MB, Used: 0.00%

Connections: Total (cumulative): 31 Active: 3

Encode:
Overall: msg: 6201, in: 798 KB, out: 157 KB, ratio: 80.25%
DRE: msg: 154, in: 6673 B, out: 9973 B, ratio: 0.00%
DRE Bypass: msg: 6064, in: 791 KB
LZ: msg: 6124, in: 858 KB, out: 156 KB, ratio: 81.75%
LZ Bypass: msg: 77, in: 0 B
Avg latency: 0.128 ms Delayed msg: 0
Encode th-put: 1004 KB/s
Message size distribution:
0-1K=100% 1K-5K=0% 5K-15K=0% 15K-25K=0% 25K-40K=0% >40K=0%

Decode:
Overall: msg: 25377, in: 358 MB, out: 645 MB, ratio: 44.52%
DRE: msg: 25251, in: 357 MB, out: 643 MB, ratio: 44.51%
DRE Bypass: msg: 26539, in: 1527 KB
LZ: msg: 20110, in: 296 MB, out: 296 MB, ratio: 0.29%
LZ Bypass: msg: 5267, in: 63570 KB
Avg latency: 0.450 ms
Decode th-put: 57907 KB/s
Message size distribution:
0-1K=3% 1K-5K=14% 5K-15K=23% 15K-25K=13% 25K-40K=14% >40K=30%

```

出力には、エンコードとデコードの両方についての LZ 圧縮率も含まれています。

## show statistics tfo コマンド出力

**show statistics tfo** コマンド出力には、WAE によって処理される合計接続数、アクティブな接続数、保留中の接続数、およびバイパス接続数が表示されます (図 1-32 を参照)。

図 1-32 コマンド出力 : show statistics tfo

Output of command - show statistics tfo	
Total number of connections	: 31
No. of active connections	: 3
No. of pending (to be accepted) connections	: 0
No. of bypass connections	: 1
No. of normal closed conns	: 25
No. of reset connections	: 3
Socket write failure	: 0
Socket read failure	: 0
WAN socket close while waiting to write	: 0
A0 socket close while waiting to write	: 0
WAN socket error close while waiting to read	: 0
A0 socket error close while waiting to read	: 0
DRE decode failure	: 0
DRE encode failure	: 0
Connection init failure	: 0
WAN socket unexpected close while waiting to read	: 0
Exceeded maximum number of supported connections	: 0
Buffer allocation or manipulation failed	: 0
Peer received reset from end host	: 3
DRE connection state out of sync	: 0
Memory allocation failed for buffer heads	: 0
Unoptimized packet received on optimized side	: 0

出力には、接続リセットの原因を示す接続リセット数も示されます。



(注) 接続リセット数は、WAAS アプライアンス外の問題を示していることがあるため、この数には特に注意してください。

## show interface gig 1/0 コマンド出力

**show interface gig 1/0** コマンド出力は、インターフェイス ステータス、速度とデュプレックス、送受信されたパケット、および発生したエラーを示しています (図 1-33 を参照)。

図 1-33 コマンド出力 : show interface gig 1/0

```
Output of command - show interface gigabit 1/0
Type: Ethernet
Ethernet address: 00:1A:64:C3:08:2C
Maximum Transfer Unit Size: 1500
Metric: 1
Packets Received: 3418168
Input Errors: 233971
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 233971
Packet Sent: 2876215
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length: 1000
Collisions: 0
Interrupts: 16
Flags: UP BROADCAST RUNNING SLAVE MULTICAST
Link State: Interface is up, line protocol up
Mode: full-duplex, 100baseTX
```

速度とデュプレックスの不一致は、パフォーマンス低下の最も一般的な理由の 1 つです。

## show tech-support コマンド出力

**show tech-support** コマンド出力には、さまざまな CLI コマンドの主要な出力が表示され、タスクのモニタリングとトラブルシューティングに使用できます (図 1-34 を参照)。

図 1-34 コマンド出力 : show tech-support

```
Output of command - show tech-support
----- version and hardware -----
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2010 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software (WAAS-FULL-K9) Release 4.2.1 (build b13 Apr 20 2010)
Version: oe674-4.2.1.13

Compiled 20:45:22 Apr 20 2010 by danaster

Device Id: 00:1a:64:c3:08:2c
System was restarted on Sat Jun 5 05:46:01 2010.
The system has been up for 1 week, 4 days, 17 hours, 48 seconds.
```





## CHAPTER 2

# トラフィック代行受信のモニタリング

この章では、トラフィック代行受信を使用して、WAAS デバイスをモニタする方法について説明します。この章の構成は、次のとおりです。

- 「WCCPv2 代行受信の確認」(P.2-1)
- 「インライン代行受信の確認」(P.2-7)

## WCCPv2 代行受信の確認

ここでは、WCCP 代行受信が正しく機能している場合に使用可能ないくつかの IOS コマンドおよび WAAS WCCP コマンドについて説明します。

ここでは、次の内容について説明します。

- 「show ip wccp IOS コマンド出力」(P.2-1)
- 「show wccp WAAS コマンド出力」(P.2-6)

## show ip wccp IOS コマンド出力

**show ip wccp IOS** コマンド出力には、多数のルータ、WAE またはサービス グループ、リダイレクトされるパケット、および転送方式とリターン方式を含む、WCCP インベントリが示されます。これは、WCCP 代行受信が正しく動作しているかどうかを確認するために最も一般的に使用される CLI コマンドです。

コマンド構文は次のとおりです。

```
show ip wccp [service_group#] [detail]
```

次の例は、コマンドをオプションの引数とキーワードと一緒に使用方法と、オプションの引数とキーワードを指定せずにコマンドを使用する方法の両方を示しています。

図 2-1 では、サービス グループ 61 に登録されている 1 つの代行受信ルータと 1 つの WAE が存在することを示す、**show ip wccp IOS** コマンド出力の領域が強調表示されています。

図 2-1 コマンド出力の例 1 : show ip wccp

```

Router# show ip wccp
Global WCCP information:
  Router information:
    Router Identifier:          10.88.81.242
    Protocol Version:          2.0

  Service Identifier: 61
  Number of Service Group Clients: 1
  Number of Service Group Routers: 1
  Total Packets s/w Redirected: 68755
  Process: 2
  CEF: 68753
  Service mode: Open
  Service access-list: -none-
  Total Packets Dropped Closed: 0
  Redirect access-list: -none-
  Total Packets Denied Redirect: 0
  Total Packets Unassigned: 0
  Group access-list: -none-
  Total Messages Denied to Group: 0
  Total Authentication failures: 0
  Total Bypassed Packets Received: 0

--More--

```

クライアント = WAE

246915

図 2-2 では、Total Packets s/w Redirect カウンタがソフトウェアベースのプラットフォーム（たとえば、Cisco ISR）で増加していることを示す、**show ip wccp IOS** コマンド出力の領域が強調表示されています。

図 2-2 コマンド出力の例 2 : show ip wccp

```
Router# show ip wccp
Global WCCP information:
  Router information:
    Router Identifier:          10.88.81.242
    Protocol Version:          2.0

  Service Identifier: 61
    Number of Service Group Clients: 1
    Number of Service Group Routers: 1
    Total Packets s/w Redirected: 68755
    Process: 2
    CEF: 68753
  Service mode: Open
  Service access-list: -none-
  Total Packets Dropped Closed: 0
  Redirect access-list:
  Total Packets Denied Redirected:
  Total Packets Unassigned:
  Group access-list:
  Total Messages Denied to Group:
  Total Authentication failures: 0
  Total Bypassed Packets Received: 0
--More--
```

カウンタがソフトウェアベースのプラットフォーム（例：ISR）で増加していることを確認する

図 2-3 では、Total Packets s/w Redirect カウンタがハードウェアベースのプラットフォーム（たとえば、Cisco Catalyst 6500）で増加していないことを示す、**show ip wccp** IOS コマンド出力の領域が強調表示されています。



図 2-3 コマンド出力の例 3 : show ip wccp

```

Router# show ip wccp
Global WCCP information:
  Router information:
    Router Identifier:          10.88.81.242
    Protocol Version:          2.0

  Service Identifier: 61
    Number of Service Group Clients: 1
    Number of Service Group Routers: 1
    Total Packets s/w Redirected: 102
    Process: 1
    CEF: 101
    Service mode: Open
    Service access-list: -none-
    Total Packets Dropped Closed: 0
    Redirect access-list:
    Total Packets Denied Redirected:
    Total Packets Unassigned:
    Group access-list:
    Total Messages Denied to Group:
    Total Authentication failures: 0
    Total Bypassed Packets Received: 0
--More--

```

←

カウンタがハードウェアベースのプラットフォーム (例: ISR) で増加していないことを確認する

24/09/17

**show ip wccp service\_group# detail** IOS コマンド出力は、状態、使用されるリダイレクト方式とリターン方式、および接続時間などに関する情報を提供します。図 2-4 は、デフォルトのリダイレクト方式と割り当て方式が使用されるソフトウェアベースのプラットフォームの出力例を示しています。



図 2-4 コマンド出力の例 1 : show ip wccp service\_group# detail

```

Router# show ip wccp 61 detail
WCCP Client information:
  WCCP Client ID:      10.88.81.242
  Protocol Version:    2.0
  State:               Usable
  Redirection:         GRE
  Packet Return:       GRE
  Assignment:          HASH
  Initial Hash Info:   FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Assigned Hash Info:  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Hash Allotment:      256 (100.00%)
  Packets s/w Redirected: 68755
  Connect Time:        3w6d
  Bypassed Packets
  Process:             2
  CEF:
  Errors:
    
```

サービスグループでの WAE の状態を確認する

割り当てられているハッシュバケットの%

サービスグループでの現在の時間

図 2-5 は、L2 リダイレクトとマスク割り当て用に設定されているハードウェアベースのプラットフォームの出力例を示しています。CLI 出力は若干異なり、これらの設定済みのパラメータを反映しています。

図 2-5 コマンド出力の例 2 : show ip wccp service\_group# detail

```

Cat6k# sh ip wccp 61 det
WCCP Client information:
  WCCP Client ID:      10.88.80.135
  Protocol Version:    2.0
  State:               Usable
  Redirection:         L2
  Packet Return:       GRE
  Packets Redirected:  0
  Connect Time:        1d18h
  Assignment:          MASK

Mask  SrcAddr  DstAddr  SrcPort  DstPort
----  -
0000: 0x00000f00 0x00000000 0x0000 0x0000

Value SrcAddr  DstAddr  SrcPort  DstPort CE-IP
-----
0000: 0x00000000 0x00000000 0x0000 0x0000
0001: 0x00000001 0x00000000 0x0000 0x0000 0x0A585087 (10.88.80.135)
0002: 0x00000040 0x00000000 0x0000 0x0000 0x0A585087 (10.88.80.135)
0003: 0x00000041 0x00000000 0x0000 0x0000 0x0A585087 (10.88.80.135)
    
```

サービスグループマスク

## show wccp WAAS コマンド出力

WAE CLI から使用可能な `show wccp WAAS` コマンドを使用して、WCCP が正しく設定され動作していることを確認できます。

コマンド構文は次のとおりです。

```
show wccp {services | status | routers | gre}
```

図 2-6 は、`show wccp services`、`show wccp status`、および `show wccp routers` の各 WAAS コマンドの出力例を示しています。

図 2-6 コマンド出力 : `show wccp services`、`show wccp status`、および `show wccp routers`

```

WAE-612# show wccp services
Services configured on this File Engine
  TCP Promiscuous 61
  TCP Promiscuous 62

WAE-612# show wccp status
WCCP version 2 is enabled and currently active

WAE-612# show wccp routers

Router Information for Service: TCP Promiscuous 61
Routers Seeing this Wide Area Engine (1)
  Router Id      Sent To      Recv ID      AssKeyIP      AssKeyCN      MemberCN
  44.77.22.3    10.88.80.129 00090C46     10.88.80.133 1              5
Routers not Seeing this Wide Area Engine
-NONE-
Routers Notified of from other WAE's
-NONE-
Multicast Addresses Configured
-NONE-

```

WCCP が設定されイネーブルになっていることを確認する

WCCP 対応ルータとの双方向通信を確認する

249592

図 2-7 は、`show wccp gre WAAS` コマンドの出力例を示しています。

図 2-7 コマンド出力 : `show wccp gre`

```

WAE-612# show wccp gre
Transparent GRE packets received: 5531561
Transparent non-GRE packets received: 0
Transparent non-GRE non-WCCP packets received: 0
Total packets accepted: 5051
Invalid packets received: 0
Packets received with invalid service: 0
Packets received on a disabled service: 0
Packets received too small: 0
Packets dropped due to zero TTL: 0
Packets dropped due to bad buckets: 0
Packets dropped due to no redirect address: 0
Packets dropped due to loopback redirect: 0
Pass-through pkts dropped on assignment update: 0
Connections bypassed due to load: 0
Packets sent back to router: 0
GRE packets sent to router (not bypass): 0
Packets sent to another WAE: 0
GRE fragments redirected: 0
GRE encapsulated fragments received: 0
Packets failed encapsulated reassembly: 0
Packets failed GRE encapsulation: 0
--More--

```

WCCP リダイレクトが動作している場合は、これらのいずれかのカウンタは増加している必要がある

## インライン代行受信の確認

図 2-8 と図 2-9 は、`show interface` コマンドを使用して、インライン代行受信設定と正しい操作を確認する方法を示しています。

図 2-8 コマンド出力の例 1 : `show interface`

```

WAE-612# show interface inlineGroup 1/0
Interface is in intercept operating mode.
Standard NIC mode is off.
Disable bypass mode is off.
VLAN IDs configured for inline interception: All
Watchdog timer is enabled.
Timer frequency: 1600 ms.
Autoreset frequency 500 ms.
The watchdog timer will expire in 1452 ms.
WAE-612#

```

代行受信動作モードまたはバイパス動作モード

VLAN を確認する

2つの動作モードの違いは次のとおりです。

- 代行受信動作モード：パケットは、最適化のために WAAS に渡されます。

- バイパス動作モード：障害または管理シャットダウン中の InLineGroup でのポート間のメカニカルなバイパス。

図 2-9 コマンド出力の例 2 : show interface

```

WAE-612# show interface inlinePort 1/0/wan
Device name      : eth4. Bypass master interface.
Packets Received : 54231
Packets Intercepted: 0
Packets Bridged  : 54231
Packets Forwarded : 0
Packets Dropped  : 0
Packets Received on native      : 0
Active flows for this interface : 0
...

WAE-612# show interface inlinePort 1/0/lan
Device name      : eth5. Bypass slave interface.
Packets Received : 334602
Packets Intercepted: 0
Packets Bridged  : 334599
Packets Forwarded : 0
Packets Dropped  : 3
Packets Received on native      : 0
Active flows for this interface : 0
...
WAE-612#

```

「sh int inlinep」を使用して、任意の Inline-Port のデバイス名を判別する。パケットのキャプチャにはデバイス名を必要とする

InlinePort インターフェイスで代行受信されたトラフィックは、増加している（つまり検査されている）ように見える必要がある

ブリッジされたトラフィックが TCP でないか、または検査されていない

WCCP のトラブルシューティングに関する詳細については、Cisco DocWiki で入手可能な『[WAAS Troubleshooting Guide](#)』を参照してください。





## CHAPTER 3

# SNMP を使用した WAAS のモニタリング

この章では、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) を使用して WAAS デバイスをモニタする方法について説明します。SNMP は、SNMP エージェントからの WAAS デバイスの外部モニタリングを可能にする、相互運用可能な標準ベースのプロトコルです。

SNMP の使用と設定に関する詳細については、『Cisco Wide Area Application Services Configuration Guide』の「[Configuring SNMP Monitoring](#)」の章を参照してください。

この章の構成は、次のとおりです。

- 「サポートされる MIB に関する情報」(P.3-1)
- 「サポートされる MIB のダウンロード」(P.3-3)
- 「SNMP トラップの表示とイネーブル化」(P.3-3)
- 「一般的な SNMP MIB OID に関する情報」(P.3-5)
- 「SNMP トリガーの表示と設定」(P.3-6)

## サポートされる MIB に関する情報

ここでは、次に示すように、WAAS によってサポートされる Cisco に固有の MIB について説明します。

MIB	説明
ACTONA-ACTASTOR-MIB	CIFS トランスペアレント アクセラレータに関する統計情報と、WAAS 内のレガシー モード WAFS コンポーネントの統計情報とログトラップを提供します。
CISCO-CDP-MIB	ローカル インターフェイスの ifIndex 値を表示します。リピータポートに ifIndex 値が割り当てられていない 802.3 リピータでは、この値はポートの固有値であり、リピータでサポートされる ifIndex 値より大きくなります。この例では、特定のポートが cdpInterfaceGroup と cdpInterfacePort の対応する値によって示されています。この場合、これらの値は、RFC 1516 のグループ番号値とポート番号値に対応します。

MIB	説明
<b>CISCO-CONFIG-MAN-MIB</b>	<p>次のようなさまざまな場所に存在する設定データのモデルを表します。</p> <ul style="list-style-type: none"> <li>• <b>running</b> : 実行中のシステムによって使用中</li> <li>• <b>terminal</b> : 接続されているハードウェア</li> <li>• <b>local</b> : NVRAM またはフラッシュ メモリにローカルに保存済み</li> <li>• <b>remote</b> : ネットワーク上のサーバに保存済み</li> </ul> <p>この MIB には、設定に明確に関連する操作のみが含まれています。ただし、一部のシステム機能は一般的なファイルの保存と転送に使用できません。</p>
<b>CISCO-CONTENT-ENGINE-MIB</b>	<p>Cisco Systems の Cisco WAAS デバイス用の MIB モジュール。この MIB の次のオブジェクトがサポートされます。</p> <ul style="list-style-type: none"> <li>• <b>cceAlarmCriticalCount</b></li> <li>• <b>cceAlarmMajorCount</b></li> <li>• <b>cceAlarmMinorCount</b></li> <li>• <b>cceAlarmHistTableSize</b></li> </ul>
<b>EVENT-MIB</b>	<p>ネットワーク管理のためにイベント トリガーとアクションを定義します。MIB は RFC 2981 として公開されます。</p>
<b>HOST-RESOURCES-MIB</b>	<p>ホスト システムを管理します。ホストという用語は、インターネットに接続されている他の類似したコンピュータと通信する、任意のコンピュータを意味します。HOST-RESOURCES-MIB は、主要な機能が通信サービスであるデバイス（ターミナルサーバ、ルータ、ブリッジ、モニタリング機器）に必ずしも適用されるとは限りません。この MIB は、すべてのインターネット ホスト（たとえば、UNIX のバリエーションを実行するパーソナル コンピュータやシステム）に共通する属性を提供します。</p>
<b>IF-MIB</b>	<p>64 ビットのインターフェイス カウンタを含み、インターフェイス関連の統計情報のクエリをサポートします。これらのカウンタにはデバイスのインターフェイスで送受信されたオクテット、ユニキャスト、マルチキャスト、およびブロードキャスト パケットが含まれます。ifCounterDiscontinuityTime を除き、ifXEntry のすべてのオブジェクトがサポートされています。この MIB は、RFC 2233 で文章化されています。</p>
<b>MIB-II</b>	<p>RFC 1213 に記載されており、TCP/IP ベースのインターネットでネットワーク管理プロトコルとともに使用するためのインターネット標準の MIB。この MIB は、ダウンロードサイトの v1 ディレクトリの RFC1213-MIB ファイルにあります(他の MIB は v2 ディレクトリにあります)。</p>
<b>SNMP-COMMUNITY-MIB</b>	RFC 2576 に記載されています。
<b>SNMP-FRAMEWORK-MIB</b>	RFC 2571 に記載されています。
<b>SNMP-NOTIFICATION-MIB</b>	RFC 3413 に記載されています。
<b>SNMP-TARGET-MIB</b>	RFC 3413 に記載されています。
<b>SNMP-USM-MIB</b>	RFC 2574 に記載されています。

MIB	説明
SNMPv2-MIB	RFC 1907 に記載されています。この MIB では次の通知がサポートされます。 <ul style="list-style-type: none"><li>• coldStart</li><li>• linkUp</li><li>• linkDown</li><li>• authenticationFailure</li></ul>
SNMP-VACM-MIB	RFC 2575 に記載されています。

## サポートされる MIB のダウンロード

サポートされる MIB ファイルはすべて、次の Cisco FTP の場所からダウンロードできます。

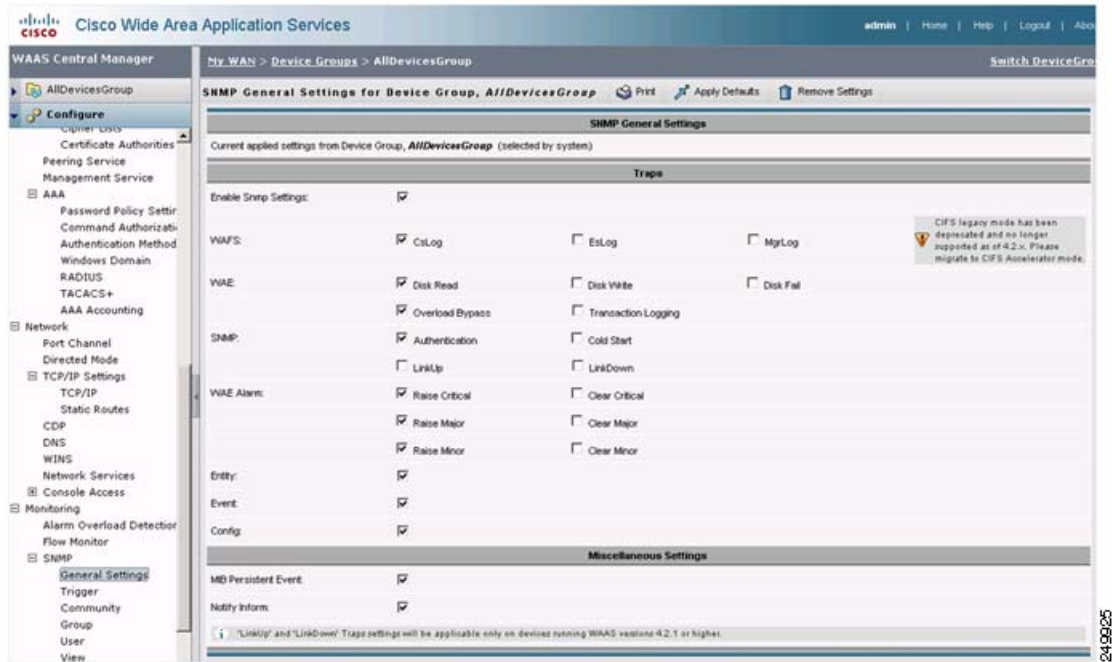
- <ftp://ftp.cisco.com/pub/mibs/v2>
- <ftp://ftp.cisco.com/pub/mibs/v1>

それぞれの MIB で定義される MIB オブジェクトは MIB ファイルで説明されており、明確です。

## SNMP トラップの表示とイネーブル化

WAAS システムで使用可能な SNMP トラップ オプションを表示するには、[My WAN] > [Device Group] > [AllDevicesGroup] > [Configure] > [Monitoring] > [SNMP] > [General Settings] を選択します。[SNMP General Settings] ウィンドウが表示されます (図 3-1)。

図 3-1 [SNMP General Settings] ウィンドウ



[SNMP General Settings] ウィンドウから SNMP トラップをイネーブルにする方法については、『Cisco Wide Area Application Services Configuration Guide』の「[Configuring SNMP Monitoring](#)」の章を参照してください。



## 一般的な SNMP MIB OID に関する情報

ここでは、一般的な SNMP トラップ OID について説明します。

オブジェクト	<b>cceAlarmCriticalRaised</b>
OID	<b>1.3.6.1.4.1.9.9.178.2.0.7</b>
ステータス	最新
MIB	<b>CISCO-CONTENT-ENGINE-MIB</b> : サポート イメージの表示
トラップ コンポーネント	<b>cceAlarmHistId</b> <b>cceAlarmHistModuleId</b> <b>cceAlarmHistCategory</b> <b>cceAlarmHistInfo</b> <b>cceAlarmHistTimeStamp</b>
説明	モジュールが重大アラームを出しました。
オブジェクト	<b>coldStart</b>
OID	<b>1.3.6.1.6.3.1.1.5.1</b>
ステータス	最新
MIB	<b>SNMPv2-MIB</b> : サポート イメージの表示
説明	通知発信元アプリケーションをサポートする SNMP エンティティが自動的に再初期化されています。このエンティティの設定は変更された可能性があります。
オブジェクト	<b>cceAlarmCriticalCleared</b>
OID	<b>1.3.6.1.4.1.9.9.178.2.0.8</b>
ステータス	最新
MIB	<b>CISCO-CONTENT-ENGINE-MIB</b> : サポート イメージの表示
トラップ コンポーネント	<b>cceAlarmHistId</b> <b>cceAlarmHistModuleId</b> <b>cceAlarmHistCategory</b> <b>cceAlarmHistInfo</b> <b>cceAlarmHistTimeStamp</b>
説明	モジュールが重大アラームをクリアしました。
オブジェクト	<b>cceFailedDiskName</b>

OID	1.3.6.1.4.1.9.9.178.1.5.1
タイプ	OCTET STRING
権限	accessible-for-notify
ステータス	最新
MIB	<a href="#">CISCO-CONTENT-ENGINE-MIB</a> : サポート イメージの表示
説明	ディスクの障害イベントが発生したディスクの名前。
オブジェクト	ciscoContentEngineDiskFailed
OID	1.3.6.1.4.1.9.9.178.2.0.6
ステータス	最新
MIB	<a href="#">CISCO-CONTENT-ENGINE-MIB</a> : サポート イメージの表示
トラップ コンポーネント	cceFailedDiskName
説明	Content Engine データ ドライブで障害が発生しました。このオブジェクトによって、ciscoContentEngineDataDiskFailed が置き換えられます。エラーに関する追加情報は Syslog に記録されます。

## SNMP トリガーの表示と設定

WAAS システムで SNMP トリガーを表示して設定できます。特定の設定に関係のある他の MIB オブジェクトについて追加の SNMP トラップを生成するようカスタム トリガーを設定できます。

WAE には 6 個のデフォルトのトリガーがあります。デフォルトのトリガーを削除して、設定を保存した場合、デバイスをリロードすると削除したトリガーが元に戻ります。図 3-2 に、デフォルトのトリガーを示します。

### 手順

**ステップ 1** [My WAN] > [Device Group] > [AllDevicesGroup] > [Configure] > [Monitoring] > [SNMP] > [Trigger] を選択します。

デフォルトのトリガーと設定済みのトリガーのリストが示された [Trigger List Entries] ウィンドウが表示されます (図 3-2)。

図 3-2 SNMP のトリガー リスト

MIB Name	Wild Card	Frequency	Test	Sample Type	Threshold Value	MIB Var1	MIB Var2	MIB Var3	Comments
daysLeft.0		120	less than	absolute	10				less than 10 days left for the WAF's license
exCnOpenFiles.0		60	greater than	absolute	4500				More than 4500 currently opened files
exCnConnectedSessionCount.0		120	greater than	absolute	2250				More than 2250 sessions (+users) are currently connected
exCnMibsConnected.1		60	equal	absolute	0				one of the CoreServers is disconnected
exEvictedAge.0		60	less than	absolute	120960000				Time spent in cache by the last evicted resource is less than 2 weeks (120960000 ticks)
exValid.0		120	equal	absolute	0				WAF's license file is not valid

**ステップ 2** トリガーを作成するには、[Trigger List Entries] ウィンドウで [Create] アイコンをクリックします。[Create new SNMP Trigger] ウィンドウが表示されます (図 3-3)。

図 3-3 SNMP トリガーの作成

Creating new SNMP Trigger for Device Group: AllDevicesGroup

**SNMP Trigger**

MIB Name:

Wild Card:

Frequency:  (60 to 600)

Test:

Sample Type:

Threshold Value:  (0 to 2147483647)

MIB Var1:

MIB Var2:

MIB Var3:

Comments:

Note: \* - Required Field

**ステップ 3** 新規 SNMP トリガーを設定します。

SNMP トリガーの設定については、『Cisco Wide Area Application Services Configuration Guide』の「[Configuring SNMP Monitoring](#)」の章を参照してください。





## CHAPTER 4

# XML API を使用した WAAS のモニタリング

この章では、WAAS API を使用して WAAS デバイスをモニタする方法と、soapUI を WAAS API インターフェイスで使用方法について説明します。

この章の構成は、次のとおりです。

- 「XML ベースの API に関する情報」 (P.4-1)
- 「トラフィック アクセラレーション サービスの使用」 (P.4-2)
- 「イベントおよびステータス サービスの使用」 (P.4-2)
- 「soapUI を使用した WAAS API インターフェイスへのアクセス」 (P.4-3)

## XML ベースの API に関する情報

WAAS Central Manager Web サービスは、デバイスのステータスと情報、アラーム、および統計情報のモニタリングをサポートする XML ベースの API を備えています。デバイス設定はサポートされません。

XML API に関する詳細については、『*Cisco Wide Area Application Services API Reference*』を参照してください。

次のサービスが提供されます。

- デバイス設定サービス (DeviceConf)
- トラフィック アクセラレーション サービス (TrafficStats)
- CIFS 統計情報サービス (CIFStats)
- ビデオ ストリーミング統計情報サービス (VideoStats)
- HTTP および HTTPS 統計情報サービス (HttpStats および HttpsStats)
- MAPI 統計情報サービス (MapiStats)
- NFS 統計情報サービス (NfsStats)
- SSL 統計情報サービス (SslStats)
- イベント サービス (AlarmStatus)
- ステータス サービス (DeviceStatus)

WAAS Central Manager モニタリング API 実装で特定のサービスに対して定義された WSDL ファイルを取得するには、次のようにサービスに ?wsdl サフィクスを付けて URL を送信します

```
https://<host/ip>:8443/ws/service_name?wsdl
```

サービスで情報を照会するには、XML 形式の SOAP 要求を次の URL のサービスに送信します。

`https://<host/ip>:8443/ws/service_name`

## トラフィック アクセラレーション サービスの使用

トラフィック アクセラレーション サービス (TrafficStats Web サービス) を使用して、個々の WAE、デバイス グループ、および WAAS ネットワークに関するトラフィックとアプリケーション統計情報を取得できます。このサービスは、次の 1 つ以上のアクションを実行します。

- `retrieveTrafficStats` : WAAS デバイス、デバイス グループ内の WAE、またはシステム全体のすべての WAE のいずれかで収集された統計情報全体を取得します。
- `getMonitoredApplications` : システムの有効範囲内で認識されているすべてのタイプのアプリケーションのリストを取得します。
- `retrieveAppTrafficStats` : WAAS デバイス、デバイス グループ内の WAE、またはシステム全体のすべての WAE のいずれかで収集されたトラフィック統計情報全体を取得します。トラフィックは、指定されたアプリケーション名に基づいてさらにフィルタリングされます。
- `retrieveCPUUtilization` : 指定された WAE の CPU 使用率情報を取得します。
- `retrieveConnection` : 現在の時間の全体的な接続の詳細を取得します。
- `retrieveConnectionTrendStats` : デバイス上で収集されたアプリケーションの全体的な接続傾向の詳細を取得します。
- `retrievePeakThroughPutStats` : デバイス上で収集されたピーク スループット値を取得します。
- `retrieveAverageThroughPutStats` : デバイス上で収集された平均スループット値を取得します。

## イベントおよびステータス サービスの使用

イベントおよびステータス サービス (AlarmStatus Web サービス) を使用して、アラーム情報、デバイス ステータス、およびディスク ステータスを取得できます。このサービスは、次の 1 つ以上のアクションを実行します。

- `retrieveAllAlarms` : すべてのアラームを取得します。
- `retrieveAlarmByName` : WAE または WAE グループの名前、オブジェクト タイプ、またはアラーム名でフィルタリングされたすべてのアラームのリストを取得します。
- `retrieveAlarmBySeverity` : アラームの重大度でさらにフィルタリングされた、指定された WAE または WAE グループのすべてのアクティブなアラームのリストを取得します。
- `getDeviceStatus` : デバイス ステータスを取得します。
- `getDiskStatus` : 物理ディスク ステータスを取得します。
- `getDiskInformation` : ディスクに関する情報を取得します。
- `getDiskEncryptStatus` : ディスクの暗号化ステータスを取得します。
- `getMonitoredAOs` : WAAS デバイス、デバイス グループ内の WAE、またはシステム全体のすべての WAE のいずれかに関するアプリケーション アクセラレーションの動作ステータスを取得します。
- `getMonitoredAOsByWaeIDs` : デバイス ID のリストに関するアプリケーション アクセラレーションの動作ステータスを取得します。

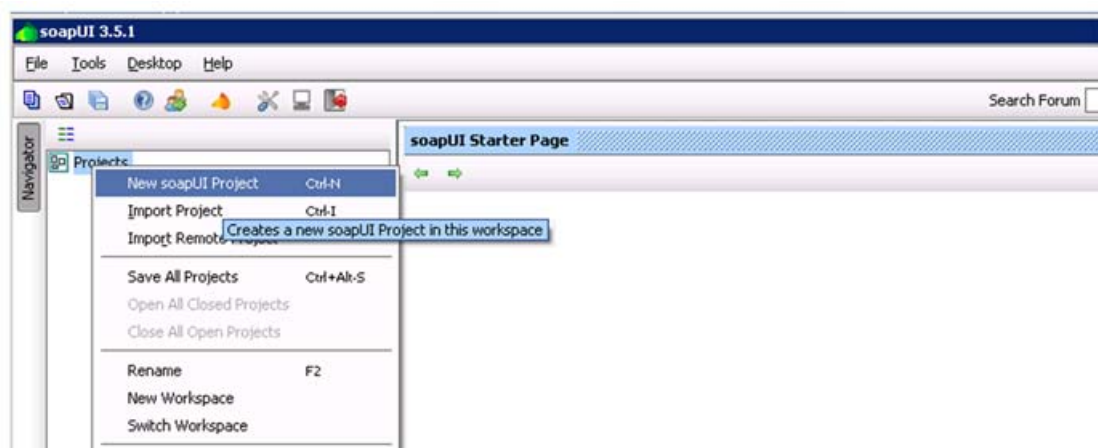
# soapUI を使用した WAAS API インターフェイスへのアクセス

WAAS API インターフェイスには、soapUI、WebInject、ApacheCXF などのサードパーティ製のツールを使用してアクセスできます。soapUI の Web サイト (<http://www.soapui.org/>) では、クライアント PC にダウンロードしてインストールできる無償のソフトウェア バージョンが提供されています。この手順では、soapUI をインストールして起動した後でこのソフトウェアを使用してプロジェクトを作成する方法について説明します。

## 手順

- ステップ 1** プロジェクトを右クリックして、プロジェクトを作成します (図 4-1)。たとえば、WAAS-Project です。

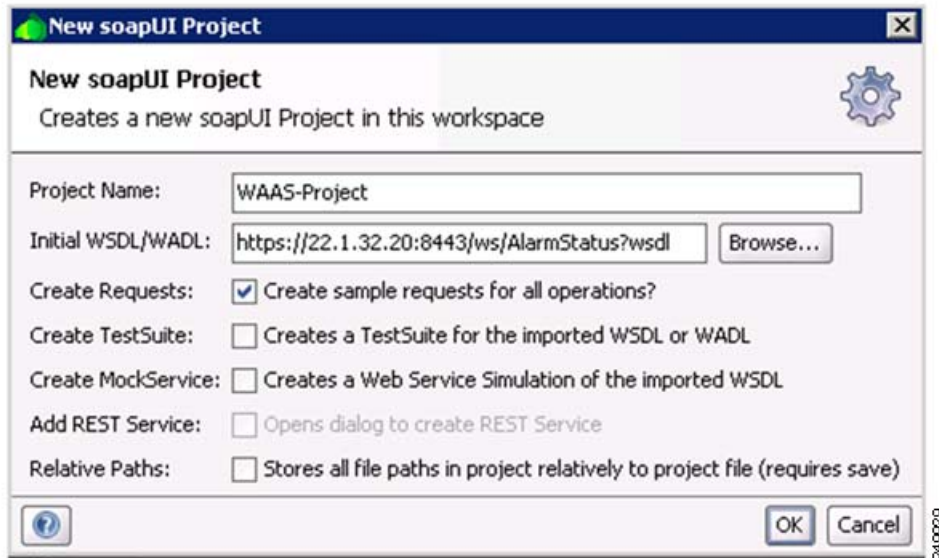
図 4-1 soapUI : 新規プロジェクトの作成



[New soapUI Project] ポップアップ ウィンドウが表示されます。

- ステップ 2** [New soapUI Project] ポップアップ ウィンドウ (図 4-2) で、次の手順を実行します。
- WSDL URL を入力します。
  - [Create Requests] チェックボックスをオンにします。
  - [OK] をクリックします。データの収集中に進行状況ウィンドウが表示されます。ロードには数秒かかることがあります。

図 4-2 soapUI : [New Project] ポップアップ ウィンドウ

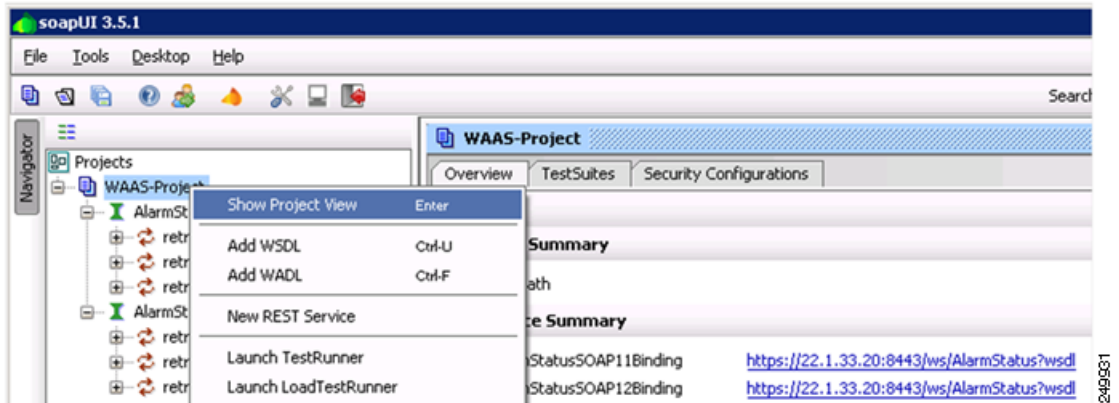


WSDL のロード後に、使用可能なナビゲーション オプションが表示されます。

**ステップ 3** 次の手順を実行して、セキュリティ資格情報を指定します。

- a. 新規プロジェクト (WAAS-Project など) を右クリックして、ポップアップ メニューを表示して、メニューから [Show Project View] をクリックします (図 4-3)。

図 4-3 soapUI : [Show Project View]

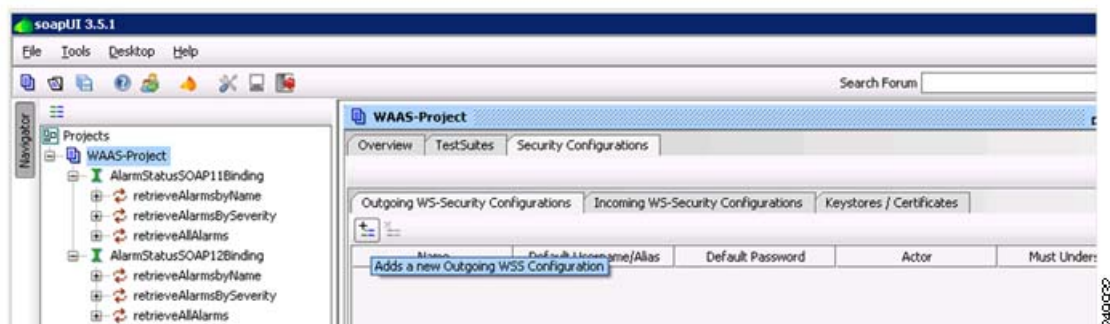


プロジェクト ウィンドウが表示されます。

- b. プロジェクト ウィンドウで、[Security Configurations] タブをクリックして新規 WSS を追加し、[Outgoing WS-Security Configurations] タブの下にあるプラス記号 (+) をクリックします (図 4-4)。



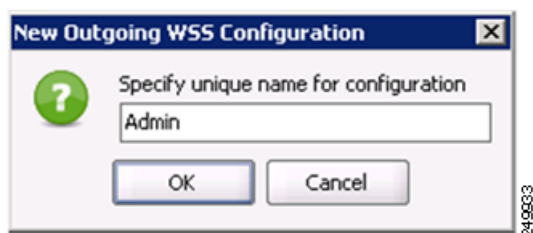
図 4-4 soapUI : [Add New WSS]



[New Outgoing WSS Configuration] ポップアップ ウィンドウが表示されます。

- c. [New Outgoing WSS Configuration] ポップアップ ウィンドウで、新規 WSS の名前 (Admin など) を入力して、[OK] をクリックします (図 4-5)。

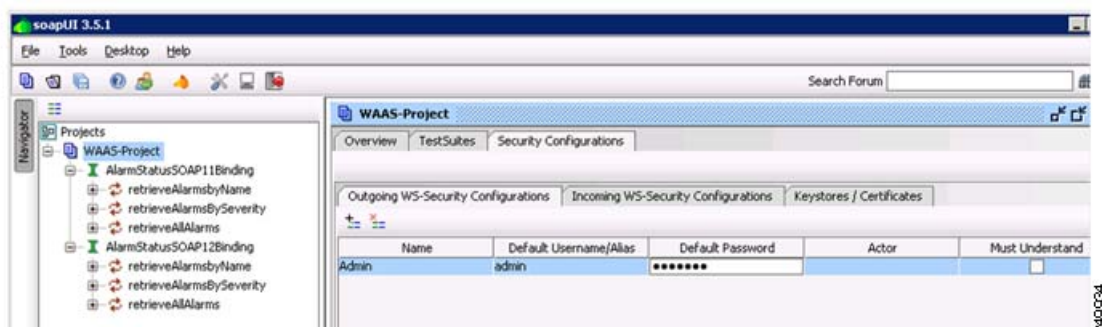
図 4-5 soapUI : [New Outgoing WSS Configuration] ポップアップ ウィンドウ



ポップアップ ウィンドウが閉じ、[Outgoing WS-Security Configuration] タブに新規 WSS が表示されます。

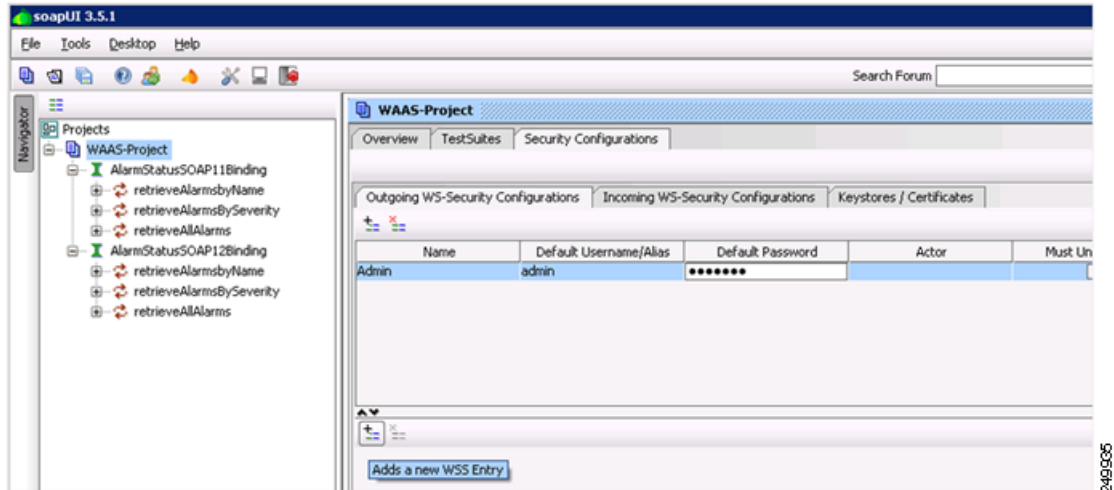
- d. [Outgoing WS-Security Configuration] タブで、デバイスのユーザ名とパスワードを入力します (図 4-6)。

図 4-6 soapUI : [WSS Username and Password]



- e. 下部ペインにあるプラス記号 (+) をクリックして、新規 WSS エントリを追加します (図 4-7)。

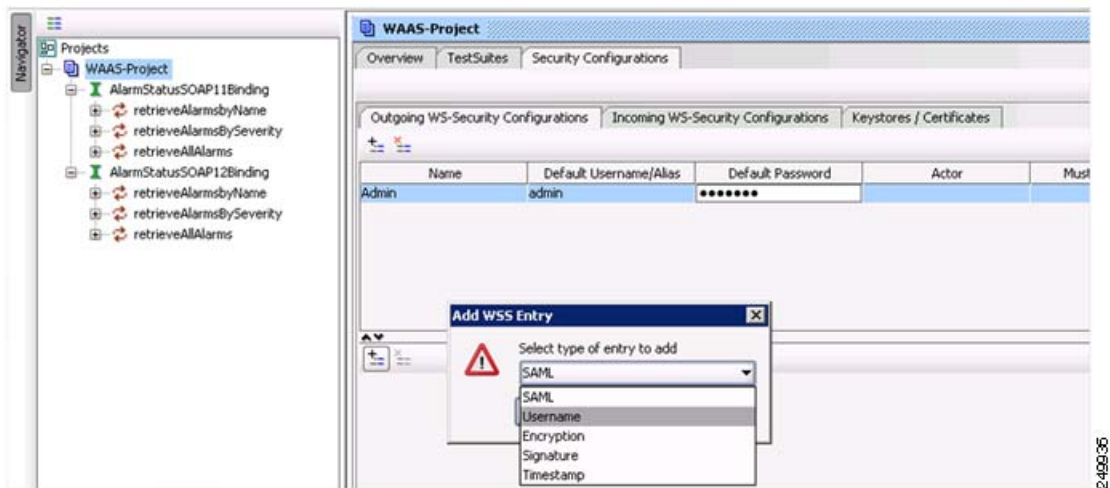
図 4-7 soapUI : [Add WSS Entry]



[Add WSS Entry] ポップアップ ウィンドウが表示されます。

- f. [Add WSS Entry] ポップアップ ウィンドウの [Select Type of Entry to Add] ドロップダウン リストで、[Username] を選択します (図 4-8)。

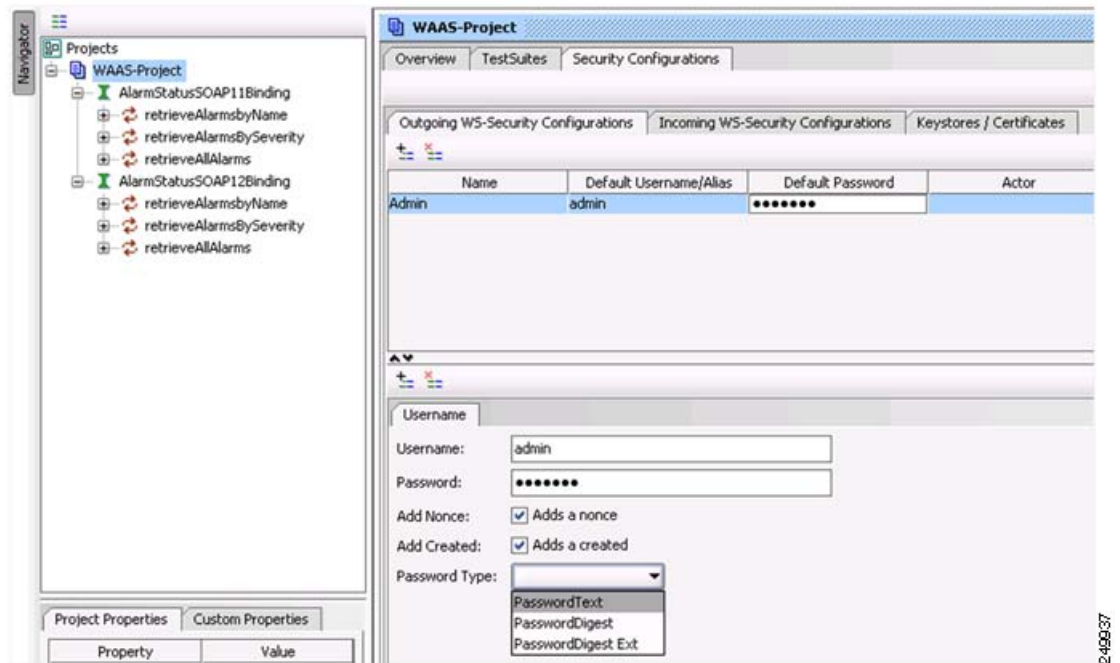
図 4-8 soapUI : [Add WSS Entry]



ポップアップ ウィンドウが閉じ、[Outgoing WS-Security Configuration] タブの下部ペインに、すでにユーザ名とパスワードが読み込まれた [Username] タブが表示されます。

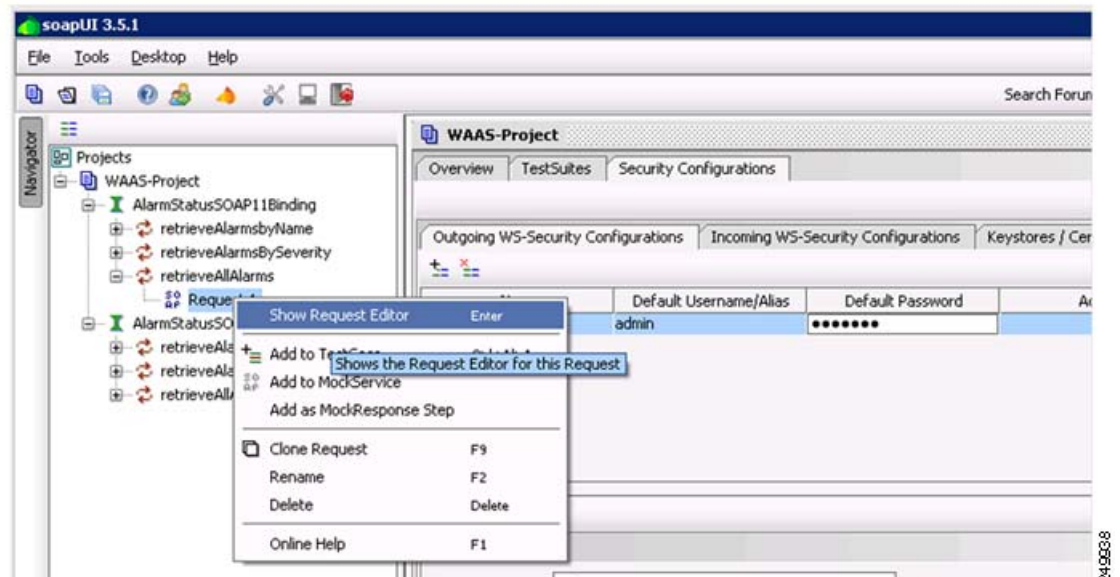
- g. [Username] タブの [Password Type] ドロップダウン リストで、[PasswordText] を選択します (図 4-9)。

図 4-9 soapUI : [Password Type]



**ステップ 4** 左側の [Projects] ツリーで、+ をクリックしてリストされているいずれかの項目を展開し、[Request x] をダブルクリックしてポップアップメニューを表示して、メニューから [Show Request Editor] を選択します (図 4-10)。

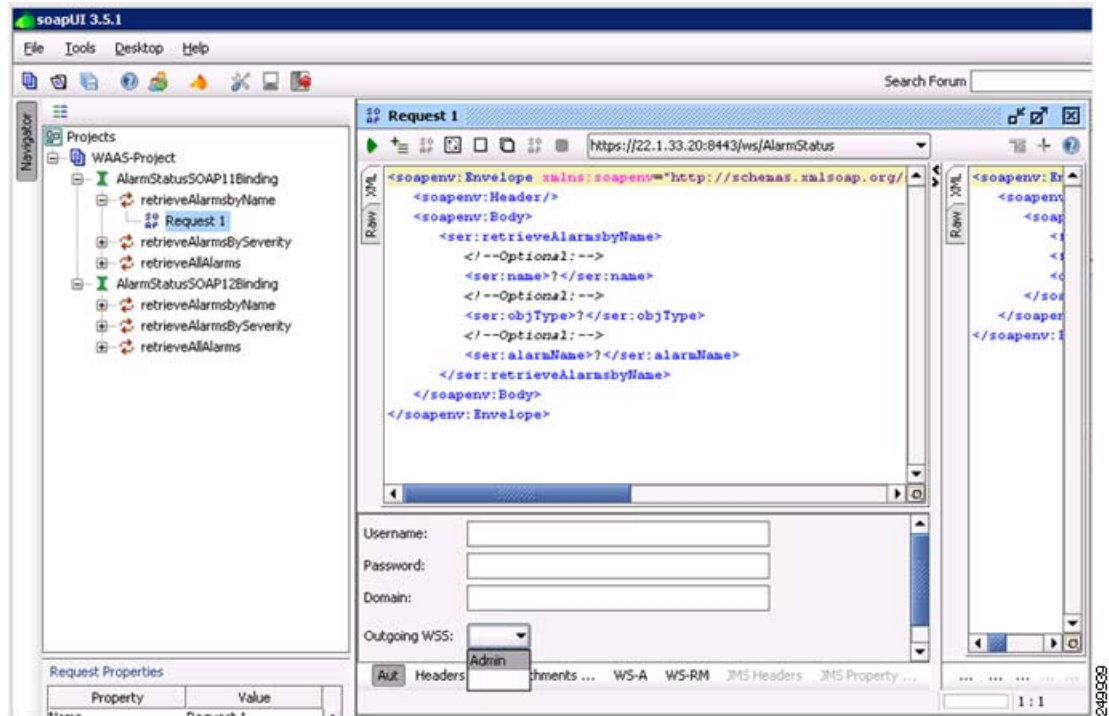
図 4-10 soapUI : [Show Request Editor]



[Request Editor] ウィンドウが表示されます。

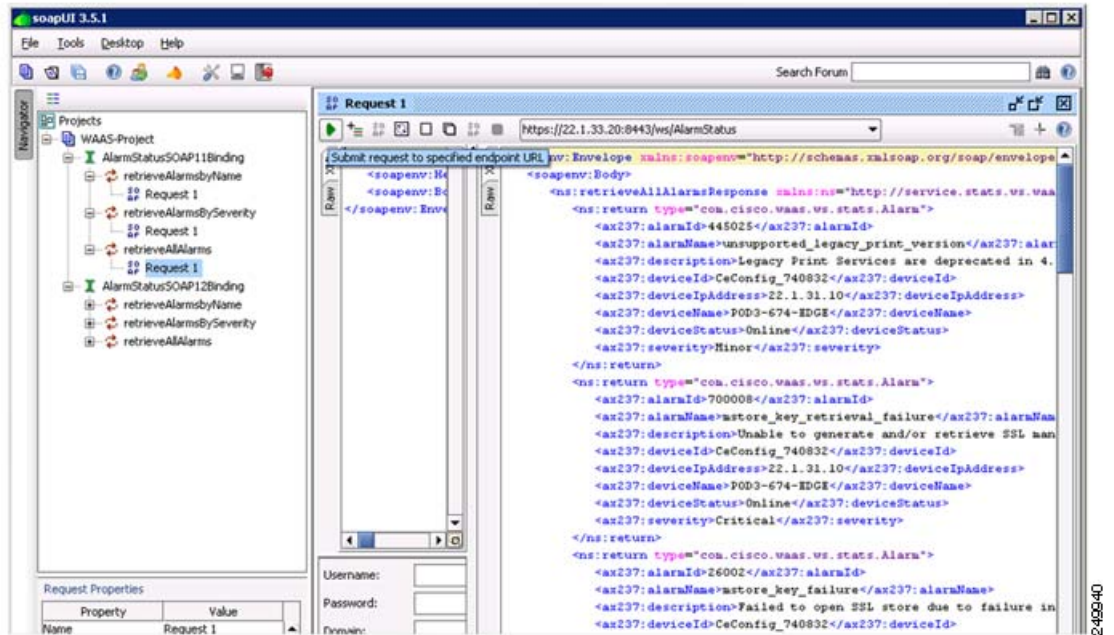
- ステップ 5** [Request Editor] ウィンドウで、下部にある [Aut] をクリックして、[Outgoing WSS] ドロップダウンリストから [Admin] を選択します (図 4-11)。

図 4-11 soapUI : [Request Editor]



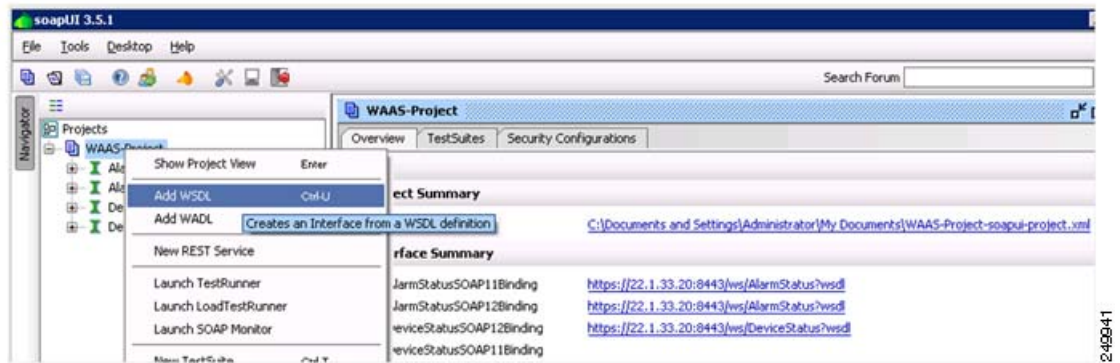
- ステップ 6** WSDL URL を確認して、[Submit] をクリックしてデバイスを照会します。要求が完了すると、XML 形式のデータが表示されます (図 4-12)。

図 4-12 soapUI : [Data in XML Format]



**ステップ 7** (オプション) 他の WSDL を追加するには、プロジェクトを右クリックしてポップアップメニューを表示して、メニューから [Add WSDL] を選択します (図 4-13)。

図 4-13 soapUI : [Add WSDL]



■ soapUI を使用した WAAS API インターフェイスへのアクセス





# CHAPTER 5

## Cisco ネットワーク解析モジュールを使用した WAAS のモニタリング

この章では、WAAS デバイスのモニタに使用できる Cisco Network Analysis Module (NAM; ネットワーク解析モジュール) について説明します。

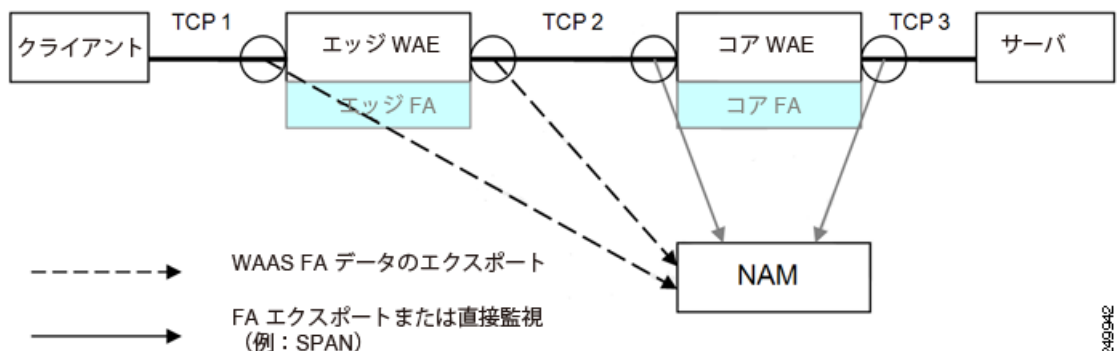
この章の構成は、次のとおりです。

- 「NAM に関する情報」(P.5-1)
- 「データを NAM にエクスポートするよう WAAS デバイスを設定」(P.5-2)
- 「WAAS デバイスをモニタするよう NAM を設定」(P.5-3)

### NAM に関する情報

NAM は、クライアントとアプリケーション サーバ間の TCP パケットの交換を分析することによって、ネットワークと Application Response Time (ART; アプリケーション応答時間) をモニタします。NAM バージョン 4 は、WAAS FlowAgent から受信したデータを処理および分析して、WAAS の最適化済みフローの ART を正確に計算するよう拡張されています。FlowAgent は、TCP パケットデータを収集して、フロー データを分析と報告のために NAM に送信するために WAAS デバイスで実行されます (図 5-1)。

図 5-1 WAAS デバイスの NAM モニタリング



NAM は、次のモニタリング機能を備えています。

- Client-Edge 接続のモニタリング: クライアントと WAAS エッジデバイス間の TCP 接続 (上の図の接続 TCP-1) をモニタすることによって、次の ART メトリックを測定できます。

## ■ データを NAM にエクスポートするよう WAAS デバイスを設定

- クライアントで発生する Total Delay (TD; 合計遅延)
- クライアントで発生する合計トランザクション時間
- 圧縮前の帯域幅使用状況 (バイト/パケット)
- トランザクションと接続の数
- 2つのセグメント (Client-Edge と Edge-Server) にわかれたネットワーク RTT
- Edge-Core でカスタマイズされた接続のモニタリング: エッジおよびコア WAAS デバイス間のスプーフィングされた TCP 接続 (上の図の接続 TCP-2) をモニタすることによって、追加の ART メトリックとして圧縮後の帯域幅使用状況 (バイト/パケット) を測定できます。
- Edge-Core 接続のモニタリング: コア WAAS デバイスとサーバ間の TCP 接続 (上の図の接続 TCP-3) をモニタすることによって、次の追加の ART メトリックを測定できます。
  - アプリケーション (サーバ) の遅延 (プロキシ アクセラレーションまたはキャッシング サーバなし)
  - コア WAAS デバイスとサーバ間のネットワーク RTT

次の項では、NAM によるモニタリングをイネーブルにするよう WAAS を設定する方法と、特定の WAAS 機能をモニタするよう NAM を設定する方法について説明します。

NAM の詳細については、次のマニュアルの URL を参照してください。

- 完全な NAM マニュアルセット :  
[http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html)
- 『Cisco WAAS NAM Virtual Service Blade Installation and Configuration Guide』 :  
[http://www.cisco.com/en/US/docs/net\\_mgmt/network\\_analysis\\_module\\_virtual\\_blade/4.2/install/guide/waas/waas42install.htm](http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_virtual_blade/4.2/install/guide/waas/waas42install.htm)

## データを NAM にエクスポートするよう WAAS デバイスを設定

ここでは、WAAS フロー レコード データを NAM にエクスポートするよう WAAS デバイスを設定する方法について説明します。

### 手順

- ステップ 1** WAAS Central Manager から、[My WAN] > [Device Group] > [AllDevicesGroup] > [Configure] > [Monitoring] > [Flow Monitor] を選択します。
- [Flow Monitoring Settings] ウィンドウが表示されます (図 5-2)。

図 5-2 WAAS Central Manager : [Flow Monitoring Settings]



**ステップ 2** [Flow Monitoring Settings] ウィンドウから、次の操作を行います。

- a. [Enable] チェックボックスをオンにして、データのエクスポートをイネーブルにします。
- b. [Destination] ボックスに NAM IP アドレスを入力します。
- c. [Submit] をクリックします。

これで、WAAS でフロー レコード データをエクスポートする準備ができました。NAM でモニタする WAAS データを指定するには、「[WAAS デバイスをモニタするよう NAM を設定](#)」(P.5-3) を参照してください。

## WAAS デバイスをモニタするよう NAM を設定

ここでは、NAM でモニタできる WAAS データ ソース機能の概要と、NAM でモニタする WAAS データの指定方法について説明します。



(注)

エクスポートがイネーブルにされた WAAS デバイスを NAM に追加する必要はありません。NAM はそのようなデバイスを自動的に検出できるためです。

ここでは、次の内容について説明します。

- 「[NAM を使用した WAAS デバイスのモニタに関する情報](#)」(P.5-3)
- 「[モニタする WAAS デバイスのデータ ソースの指定](#)」(P.5-6)

## NAM を使用した WAAS デバイスのモニタに関する情報

NAM では、WAAS データ ソースを使用して、さまざまな WAAS セグメント (クライアント、クライアント WAN、サーバ WAN、およびサーバ) から収集されたトラフィックをモニタします。それぞれの WAAS セグメントは、データ ソースによって表されます。モニタ対象 ART メトリックに加えて、WAAS データ ソースのその他のトラフィック統計情報 (アプリケーション、ホスト、および変換情報など) をモニタして報告するよう NAM を設定できます。

WAAS デバイスをモニタするよう NAM を設定

データ ソースの使用は、WAAS の配置シナリオに依存します。表 5-1 で、一般的ないくつかの WAAS 配置シナリオと適用可能なデータ ソースについて説明します。

表 5-1 WAAS 配置シナリオ

配置シナリオ	エッジ WAE データ ソース	コア WAE データ ソース
<ul style="list-style-type: none"> <li>分岐内のクライアント</li> <li>コア（データ センター）内のサーバ</li> <li>コア内の NAM</li> </ul>	クライアント	サーバ サーバ WAN
<ul style="list-style-type: none"> <li>分岐内のクライアント</li> <li>コア（データ センター）内のサーバ</li> <li>コア内の NAM</li> </ul>	クライアント クライアント WAN	サーバ
<ul style="list-style-type: none"> <li>分岐内のサーバ</li> <li>コア（データ センター）内のクライアント</li> <li>コア内の NAM</li> </ul>	サーバ	クライアント クライアント WAN
<ul style="list-style-type: none"> <li>分岐内のサーバ</li> <li>コア（データ センター）内のクライアント</li> <li>分岐内の NAM</li> </ul>	サーバ サーバ WAN	クライアント
<ul style="list-style-type: none"> <li>分岐とコア（データ センター）内のサーバとクライアント</li> <li>コア内の NAM</li> </ul>	クライアント サーバ	クライアント サーバ クライアント WAN サーバ WAN
<ul style="list-style-type: none"> <li>分岐とコア（データ センター）内のサーバとクライアント</li> <li>分岐内の NAM</li> </ul>	クライアント サーバ クライアント WAN サーバ WAN	クライアント サーバ

NAM バージョン 4.1 以降では、図 5-3 に示されているように、関連データと結合セグメントはクライアントサーバごとに 1 行で表示されます。

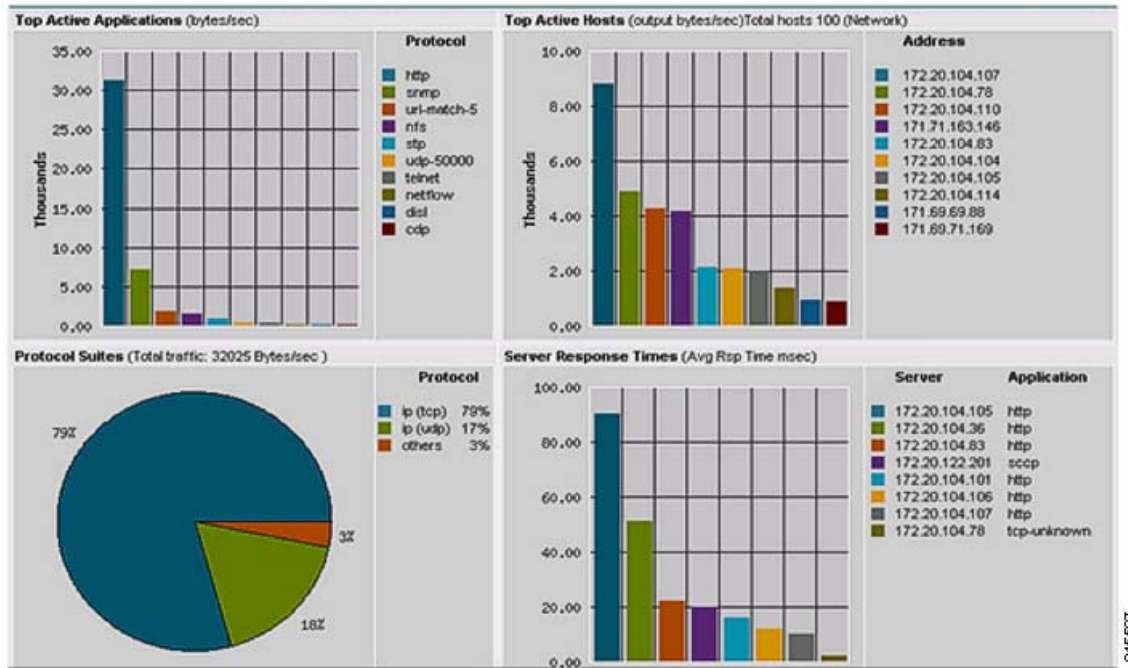
図 5-3 NAM サンプル データ ソースの表示

The screenshot shows the NAM interface with the following data table:

#	Branch	Server	Client	App	Network Delay (ms)			Total Delay (ms)	Transaction Time (ms)		Traffic Volume (bytes)			
					Client	WAN	Server		Avg	Max	Client	WAN	Server	
1.	WAE-172.20.107.117	172.20.107.123	171.69.155.57	http	2	8	2	7	99	170	3455	764,852	71,585	761,735

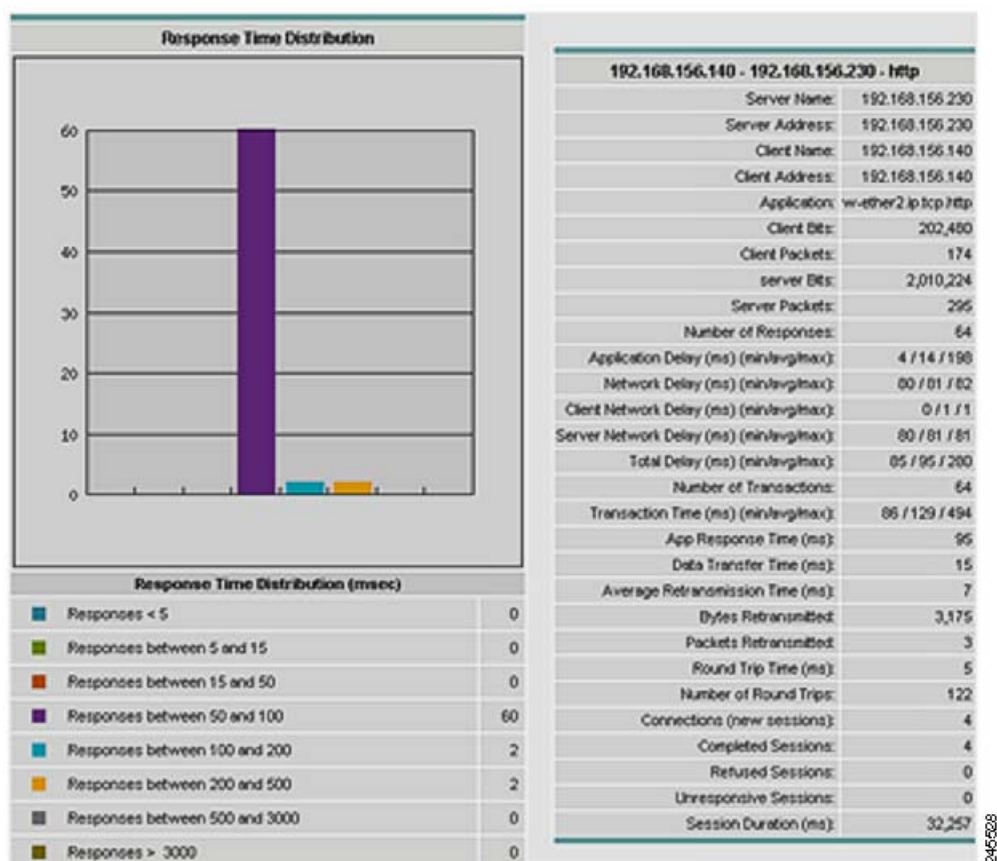
NAM は、ネットワーク アプリケーション、使用中のプロトコル、および最もアクティブなクライアントとサーバまたは最も使用率の高いクライアントとサーバに関するデータを表示できます (図 5-4 を参照)。

図 5-4 NAM ネットワーク アプリケーション、プロトコル、ホスト、およびサーバのレポート



さまざまなレポートを生成して、クライアント、サーバ、またはアプリケーションの応答時間と、上位のアクティブなアプリケーション、アクティブなホストなどを表示できます (図 5-5 を参照)。

図 5-5 NAM 応答時間のレポート



## モニタする WAAS デバイスのデータ ソースの指定

次の WAAS データ ソースをモニタするよう NAM を設定できます。

- クライアント：クライアントから発生した元の（LAN 側の）TCP フローをモニタのために NAM にエクスポートします。
- クライアント WAN：クライアントから発生した最適化済みの（WAN 側の）TCP フローをモニタのために NAM にエクスポートします。
- サーバ WAN：サーバからの最適化済みの（WAN 側の）TCP フローをモニタのために NAM にエクスポートします。
- サーバ：サーバからの元の（LAN 側の）TCP フローをモニタのために NAM にエクスポートします。
- パススルー：（NAM 4.1 以降だけ）WAAS を横断するフローを最適化せずにエクスポートします。

WAAS デバイスをモニタするよう NAM を設定する方法については、Cisco.com でホワイト ペーパー『[Using Cisco NAM 4.1 Reporting with Cisco WAAS](#)』を参照してください。

NAM の設定および使用に関する追加情報については、『[User Guide for Cisco Network Analysis Module Traffic Analyzer](#)』を参照してください。