Cisco Wide Area Application Services
コンフィギュレーション ガイド

Cisco Wide Area Application Services Configuration Guide

ソフトウェア バージョン 4.2.1
2010 年 6 月 22 日

Text Part Number: OL-21609-01-J

【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/）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。

Cisco Wide Area Application Services コンフィギュレーション ガイド

CONTENTS

はじめに

ここでは、『*Cisco Wide Area Application Services Configuration Guide*』の対象読者、マニュアルの構成、および手順や情報を記述するための表記法について説明します。この章の構成は次のとおりです。

対象読者

このガイドは、Cisco Wide Area Application Services（WAAS）の設定と保守を担当する経験のあるネットワーク管理者を対象にしています。

インターネットに使用される基本概念や用語に精通し、ネットワーク内のデバイスが使用できるネットワーク トポロジとプロトコルを理解する必要があります。また、WAAS ネットワークが稼動する Microsoft Windows、Linux、または Solaris のようなオペレーティング システムの使用経験と知識が必要です。

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	タイトル	説明
第 1 章	「Cisco WAAS の概要」	WAAS 製品とその機能の概要を提供します。
第 2 章	「WAAS ネットワークの計画」	ネットワークに WAAS 製品を設置する前に読む必要がある一般的なガイドラインと準備情報を提供します。
第 3 章	「デバイス グループとデバイス位置の使用」	複数のデバイスを同時に管理し、設定しやすいように、グループを作成する方法について説明します。また、デバイスの位置についても説明しています。

章	タイトル	説明
第 4 章	「トラフィック代行受信の設定」	IP ベース ネットワークですべての TCP トラフィックを代行受信するための WAAS ソフトウェア サポートについて説明します。
第 5 章	「ネットワーク設定の構成」	DNS や CDP のような基本的なネットワーク設定を設定する方法について説明します。
第 6 章	「管理ログインの認証、許可、およびアカウンティングの設定」	WAAS ネットワーク内の Wide Area Application Engine（WAE）用の Authentication, Authorization, And Accounting（AAA; 認証、許可、アカウンティング）を集中的に設定する方法について説明します。
第 7 章	「管理者ユーザ アカウントおよびグループの作成と管理」	WAAS Central Manager GUI から、デバイスに基づく CLI アカウントとロールに基づくアカウントを作成する方法について説明します。
第 8 章	「WAAS デバイス用の IP ACL の作成および管理」	WAE 用の Internet Protocol（IP; インターネット プロトコル）Access Control List（ACL; アクセス コントロール リスト）を集中的に作成し、管理する方法について説明します。
第 9 章	「その他のシステム設定の構成」	NTP サーバの指定やデバイス上の時間帯の設定のような他のさまざまなシステム設定作業を実行する方法について説明します。
第 10 章	「WAE Device Manager GUI の使用方法」	WAE Device Manager GUI を使用して、ネットワーク内の個々の WAE を設定し、管理する方法について説明します。
第 11 章	「WAFS の設定」	ブランチ オフィスのユーザが集中管理されたデータセンターに保存されているデータにより効率的にアクセスできる Wide Area File Services（WAFS; 広域ファイル サービス）を設定する方法について説明します。WAFS 機能は、ブランチ オフィスのユーザ付近の WAE でデータをキャッシュして、WAN の遅延と帯域幅制限を解決します。
第 12 章	「アプリケーション アクセラレーションの設定」	WAAS システムで、WAN 経由で加速されるアプリケーション トラフィックの種類を決定するアプリケーション ポリシーを設定する方法について説明します。
第 13 章	「WAAS レガシー印刷サービスの設定および管理」	WAE をブランチ オフィスのプリント サーバとして使用できる WAAS レガシー印刷サービス機能を設定し、管理する方法について説明します。
第 14 章	「仮想ブレードの設定」	WAAS デバイスで他のコンピュータをエミュレートする、仮想ブレードの設定方法について説明します。
第 15 章	「WAAS システムの保守」	WAAS システムを保守するために実行する必要がある作業について説明します。

章	タイトル	説明
第 16 章	「WAAS ネットワークのモニタリングおよびトラブルシューティング」	WAAS システムの問題を特定し、解決するために使用できる WAAS Central Manager GUI のモニタリング ツールとトラブルシューティング ツールについて説明します。
第 17 章	「SNMP モニタリングの設定」	SNMP トラップ、受信者、コミュニティ ストリングおよびグループの関連性、ユーザ セキュリティ モデル グループ、ユーザ アクセス権を設定する方法について説明します。
付録 A	「定義済みのアプリケーション ポリシー」	システムに組み込まれているポリシーに基づいて、WAAS によって最適化またはパススルーされる事前定義済みのアプリケーションと分類子のリストを示します。
付録 B	「トランザクション ログ形式」	トランザクション ログの形式について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。

出力例では、次の表記法を使用しています。

`screen フォント`	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
`イタリック体の screen フォント`	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
`< >`	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
`[ ]`	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
`!、#`	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（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。

ヒント 「*問題の解決に役立つ情報*」を示しています。ヒントは、トラブルシューティングや操作でない場合もありますが、時間を節減できます。

関連資料

Cisco WAAS ソフトウェアおよびハード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 Upgrade Guide』*
- *『Cisco Wide Area Application Services Command Reference』*
- *『Cisco Wide Area Application Services Quick Configuration Guide』*
- *『Cisco Wide Area Application Services Configuration Guide』*（本書）
- *『Cisco Wide Area Application Services API Reference』*
- *『Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade』*
- *『Cisco WAAS Troubleshooting Guide for Release 4.1.3』*（およびそれ以降のリリース）
- *『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 のオンライン ヘルプ*
- *『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』*

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。

PART 1

WAAS の概要と計画

CHAPTER 1

Cisco WAAS の概要

この章では、Cisco Wide Area Application Service（WAAS）ソリューションの概要とワイドエリア ネットワークでのデータ伝送に関する最も一般的な課題に対応するための主な WAAS 機能について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

Cisco WAAS について

WAAS システムは、ネットワーク経由の TCP トラフィックを最適化する WAE と呼ばれる一連のデバイスから構成されます。クライアント アプリケーションとサーバ アプリケーションが相互に通信するとき、ネットワークは、クライアント アプリケーションと送信先サーバの代理として機能できるように、このトラフィックを WAE へ転送します。WAE は、トラフィックを検査し、組み込みアプリケーション ポリシーを使用して、トラフィックを最適化するか、最適化せずにネットワークを通過させるかを決定します。

WAAS Central Manager GUI を使用して、ネットワーク内の WAE とアプリケーション ポリシーを中央で設定し、モニタします。また、WAAS Central Manager GUI を使用すると、WAAS システムがカスタム アプリケーションやあまり使用しないアプリケーションを最適化できるように、新しいアプリケーション ポリシーを作成できます。

Cisco WAAS を使用すると、企業は次の目標を達成できます。

- ブランチ オフィスの社員が地理的に分散したネットワーク経由で LAN のように情報やアプリケーションにアクセスできる。
- アプリケーション サーバやファイル サーバをブランチ オフィスから集中管理されたデータセンターへ移行する。
- 高度な圧縮アルゴリズムを使用して、WAN の不必要な帯域幅使用量を最小限に抑える。

- ブランチ オフィスのユーザに印刷などのローカル サービスを仮想化する。Cisco WAAS を使用すると、仮想ブレードで WAE with Windows を設定できるので、印刷サービス、Active Directory サービス、DNS、DHCP サービスなどのローカル サービスを処理するために専用システムを配備する必要がありません。
- 次のような共通の問題を解決して、WAN 経由のアプリケーションのパフォーマンスを改善する。
  - データ レートが低い（帯域幅の制約）
  - フレームの配信が遅い（ネットワークの遅延が大きい）
  - パケット損失の確率が高い（信頼性が低い）

ここでは、次の内容について説明します。

Cisco WAAS による WAN に関する共通の問題の解決

表 1-1 に、Cisco WAAS の TCP 最適化手法とアプリケーション アクセラレーション機能の組み合わせが、WAN 経由のトラフィック伝送に関する共通の問題をどのように解決するかを示します。

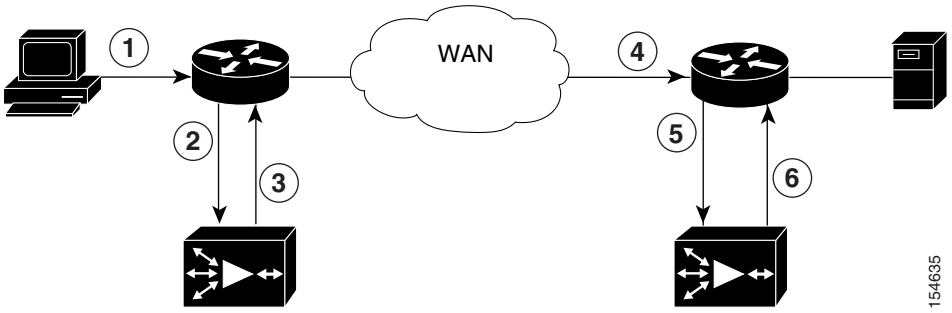
表 1-1　Cisco WAAS ソリューション

WAN に関する問題	WAAS による解決方法
ネットワークの遅延が大きい	インテリジェントなプロトコル アダプタが、通信量の多いアプリケーション プロトコルに共通する往復応答の数を減らします。
帯域幅の制約	ファイル サービス機能に付属しているデータ キャッシングとデータ圧縮が、WAN 経由で送信されるデータ量を減らすので、データ転送速度が上昇します。これらの機能は、WAN 経由で送信されるデータ量を減らして、輻輳したリンク上のアプリケーション応答時間を改善します。
リンクの使用率が低い	TCP 最適化機能が、WAN 経由で送信される TCP エラーの数を減らし、クライアントが一度に受信できるデータ量を決定する TCP ウィンドウ サイズを最大化して、ネットワーク スループットを改善します。
パケット損失	最適化された WAAS 内の TCP スタックが、頻発するパケット損失に関連する問題を解決し、WAN の状態から通信エンド ポイントを保護します。

トラフィック最適化プロセス

図 1-1 に、Cisco WAAS がアプリケーション トラフィックを最適化するプロセスを示します。

図 1-1　トラフィック最適化プロセス



次の手順は、WAAS ネットワークがブランチ オフィスのクライアントと送信先サーバ間の接続を最適化する方法を示しています。

1. ブランチ オフィスのクライアントが、ネイティブ アプリケーション ポート経由で送信先サーバとの接続を試みます。
2. WAAS ネットワークは、WCCP または PBR を使用してクライアント要求を代行受信します。または、Cisco WAE Inline Network Adapter とともに WAE に展開された場合は、WAAS はインライン モードを使用して要求を直接代行受信できます。インライン モードの詳細については、「TCP トラフィックの透過的な代行受信へのインライン モードの使用」（P.4-43）を参照してください。
3. ブランチ オフィスの WAE が、次の処理を実行します。

- トラフィックの TCP ヘッダーのパラメータを検査し、アプリケーション ポリシーを参照して、代行受信したトラフィックを最適化する必要があるかどうかを決定します。ブランチ オフィスの WAE は、送信先と送信元 IP アドレスのような TCP ヘッダー情報を使用して、トラフィックとアプリケーション ポリシーを照合します。定義済みポリシーのリストについては、付録 A「定義済みのアプリケーション ポリシー」を参照してください。
- ブランチ オフィスの WAE は、トラフィックを最適化する必要があると決定すると、トラフィックを最適化するためにネットワーク パス内の次の WAE に知らせる TCP ヘッダーに情報を追加します。

4. ブランチ オフィスの WAE が、ネットワーク経由でクライアント要求を元の送信先サーバへ転送します。
5. データセンターの WAE が、次の処理を実行します。

- 送信先サーバへ進むトラフィックを代行受信します。
- ブランチ オフィスの WAE との最適化された接続を確立します。データセンターの WAE が最適化を無効にしている場合、最適化された接続は確立されず、トラフィックは最適化されないままネットワークを通過します。

6. WAAS は、この接続用にブランチ オフィスの WAE と データセンターの WAE との間の以後のトラフィックを最適化します。

Cisco WAAS は、次の状況でトラフィックを最適化しません。

- WAE が（UDP や ICMP のような）TCP 以外のトラフィックを代行受信する。
- WAE に負荷がかかりすぎ、トラフィックを最適化するリソースがない。
- 代行受信したトラフィックが、トラフィックを最適化せずに通過させるというアプリケーション ポリシーに適合する。

（注）　最適化されていないトラフィックが WAE に到達すると、WAE は通過接続を使用してアプリケーションのパフォーマンスに影響を与えずにパススルー モードでトラフィックを転送します。

Cisco WAAS の主なサービス

Cisco WAAS は、WAN 経由トラフィックを最適化する次のサービスを提供します。

TFO の最適化

Cisco WAAS は、各種の Transport Flow Optimization（TFO; 転送フローの最適化）機能を使用して、WAAS デバイスが代行受信する TCP トラフィックを最適化します。TFO は、帯域幅制約、パケット損失、輻輳、および再送信のような負の WAN 条件から、通信中のクライアントとサーバを保護します。

TFO には、次の最適化機能があります。

ウィンドウの拡大縮小

ウィンドウの拡大縮小を使用すると、TCP パケットの受信側は、TCP 受信ウィンドウが 64 KB を超えることができることをアドバタイズできます。受信ウィンドウのサイズは、受信側が受信未確認データ用に使用できる容量を決定します。デフォルトで、TCP ヘッダーは受信ウィンドウのサイズを 64 KB に制限しますが、ウィンドウの拡大縮小を使用すると、TCP ヘッダーは受信ウィンドウ サイズを 64 KB を 1 GB まで拡大できます。

ウィンドウの拡大縮小を使用すると、TCP エンドポイントは、TCP ヘッダーに指定されたデフォルトのウィンドウのサイズに制限されず、ネットワークで使用できる帯域幅を利用できます。

ウィンドウの拡大縮小の詳細については、RFC 1323 を参照してください。

TCP の初期ウィンドウ サイズの最大化

WAAS は、TCP の初期ウィンドウの上限を 1 ～ 2 セグメントから 2 ～ 4 セグメント（約 4 KB）へ拡大します。TCP の初期のウィンドウ サイズを拡大すると、次の利点があります。

- 初期の TCP ウィンドウが 1 セグメントの場合、遅延 Acknowledgment（ACK; 確認応答）を使用する受信側は、ACK 応答を生成する前にタイムアウトを待つ必要があります。初期のウィンドウが 2 セグメント以上の場合、受信側は 2 番めのデータ セグメントが到着したあとで ACK 応答を生成するので、タイムアウトを待つ必要がありません。

- 小量のデータだけを送信する接続の場合、初期ウィンドウが大きいほど、送信時間が減ります。4 KB 未満の多くの電子メール（SMTP）と Web ページ（HTTP）転送の場合、初期ウィンドウが大きいほど、1 回のラウンドトリップ時間（RTT）が減ります。
- 大きな輻輳ウィンドウを使用する接続の場合、初期ウィンドウが大きいほど、初期の低速開始フェーズ中に最大 3 つの RTT タイムアウトと 1 つの遅延タイムアウトが除去されます。

この最適化機能の詳細については、RFC 3390 を参照してください。

バッファリングの強化

Cisco WAAS は、WAE がより積極的にブランチ オフィスのクライアントとリモート サーバからデータを取得できるように、TCP カーネルが使用するバッファリング アルゴリズムを強化します。このような強化により、接続に参加する 2 台の WAE のリンク使用率が最大に維持されます。

選択的受信確認

Selective Acknowledgement（SACK; 選択的受信確認）は、TCP が使用するデフォルトの復旧メカニズムより迅速によりパケット損失から回復できる効率的なパケット損失復旧再送信機能です。

デフォルトで、TCP は、受信側が受信しなかったパケットがあるかどうかを知るために送信側が往復を待つか、受信側が正しく受信した可能性があるセグメントを必要以上に再送信する累積的確認方式を使用します。

SACK を使用すると、受信側は正常に到着したすべてのセグメントについて送信側に知らせることができるので、送信側は実際に消失したセグメントだけを再送信するだけで済みます。

SACK の詳細については、RFC 2018 を参照してください。

BIC TCP

Binary Increase Congestion（BIC; 2 進増加輻輳）TCP は、ネットワークがパケット損失イベントからより迅速に回復できる輻輳管理プロトコルです。

ネットワークでパケット損失イベントが発生すると、BIC TCP は、受信側のウィンドウ サイズを減らし、この値を新しい最小ウィンドウの値として設定します。次に、パケット損失イベントが発生する直前のウィンドウ サイズを最大ウィンドウの値として設定します。パケット損失は最大ウィンドウ サイズで発生するため、ネットワークは、最小ウィンドウ サイズと最大ウィンドウ サイズの範囲にあるトラフィックをパケット損失なしに転送できます。

BIC TCP が更新された最大ウィンドウ サイズでパケット損失イベントを登録しない場合、そのウィンドウ サイズが新しい最小値になります。パケット損失イベントが発生する場合、そのウィンドウ サイズは新しい最大値になります。BIC TCP がウィンドウ サイズの最小値と最大値の新しい最適値を決定するまで、このプロセスが続行します。

圧縮

Cisco WAAS は、次の圧縮テクノロジーを使用して、WAN 経由で伝送されるデータのサイズを減らします。

- Data Redundancy Elimination（DRE; データ冗長性除去）
- LZ 圧縮

これらの圧縮テクノロジーは、WAN 経由でデータ ストリームを送信する前に冗長な情報を削除して、送信データのサイズを減らします。WAAS 圧縮は、転送するデータの量を減らすことで、ネットワーク使用率とアプリケーション応答時間を減らすことができます。

WAE は、圧縮を使用して TCP トラフィックを最適化するとき、ストリームに繰り返し現れるデータをそれよりはるかに短い参照で置き換えて、短くなったデータ ストリームを WAN 経由で送信します。受信側の WAE は、ローカルの冗長性ライブラリを使用して、送信先クライアントまたはサーバへ転送する前にデータ ストリームを再構築します。

WAAS の圧縮方式は、各 WAE が圧縮に参加する共有キャッシュ アーキテクチャに基づき、解除も同じ冗長性ライブラリを共有します。WAE で冗長性ライブラリを保存するキャッシュが一杯になると、WAAS は First In, First Out（FIFO; ファーストイン ファーストアウト）アルゴリズムを使用して、古いデータを廃棄し、新しいデータを保存します。

LZ 圧縮は、小型のデータ ストリームに作用し、限られた圧縮履歴を維持します。DRE は、大型のデータ ストリーム（数十から数百バイト）に作用し、はるかに大きな圧縮履歴を維持します。バージョンが更新されるたびにファイルが増分的に変更される場合や、ファイル ヘッダーやロゴのような特定の要素が多くのファイルで共通に使用される場合、ファイル システム操作で冗長データが大型化する傾向があります。

アプリケーション固有のアクセラレーション

WAN 経由のトラフィックのフローを高速化する TCP 最適化機能に加えて、Cisco WAAS には次のアプリケーション アクセラレーション機能があります。

- 動作予測とバッチ処理：WAAS デバイスは、WAN 経由のコマンド シーケンスを短いシーケンスに変換して、往復を減らすことができます。
- インテリジェントなメッセージ抑制：リモート アプリケーションの応答時間を短縮します。TFO が WAN 経由のトラフィックを最適化しても、ブランチ オフィスのクライアントとリモート サーバ間のプロトコル メッセージにより、アプリケーションの応答時間はまだ低速です。この問題を解決するため、各 WAAS デバイスには、クライアントがリモート サーバからの応答を待たなくてもいいように、メッセージにローカルに応答するアプリケーション プロキシが内蔵されています。アプリケーション プロキシは、キャッシング、コマンドのバッチ処理、予測、およびリソースのプリフェッチのような各種の手法を使用して、リモート アプリケーションの応答時間を短縮します。
- Wide Area File Services（WAFS）キャッシング：WAAS デバイスは、リモート ファイルやアプリケーション サーバからデータを取得する代わりにローカルにキャッシュされたデータを使用して、クライアント要求に応答できます。
- 事前配置：WAAS デバイスは、将来のクライアント要求を予期してリソース データとメタデータをプリフェッチできます。

Cisco WAAS は、アプリケーションインテリジェントなソフトウェア モジュールを使用して、これらのアクセラレーション機能を適用します。

典型的な Common Internet File System（CIFS; 共通インターネット ファイル システム）アプリケーションの使用例では、クライアントは、次の要求を送信する前に応答を待つ必要がある多数の同期要求を送信します。WAN 経由のデータを圧縮するだけでは、適切な応答時間を達成するには不十分です。

たとえば、5 MB の Word 文書を開くと、約 700 の CIFS 要求（550 の読み取り要求と 150 の他の要求）が生成されます。このすべての要求を 100 ms のラウンドトリップ WAN で送信すると、応答時間は少なくとも 70 秒（700 × 0.1 秒）になります。

WAAS のアプリケーション アクセラレーションによって CIFS プロトコルの同期効果が最小限に抑えられるので、アプリケーションの応答時間が減ります。各 WAAS デバイスは、アプリケーション ポリシーを使用して、特定のトラフィックの種類とアプリケーションを照合し、そのアプリケーション トラフィックを最適化し、高速化する必要があるかどうかを決定します。

使用できる WAAS アプリケーション アクセラレータは次のとおりです。

- CIFS：リモート ファイル サーバで交換された CIFS トラフィックを加速化します。詳細については、「デスクトップ アプリケーション用のファイル サービス」（P.1-7）を参照してください。
- NFS：リモート ファイル サーバで交換された Network File System（NFS; ネットワーク ファイル システム）バージョン 3 トラフィックを加速化します。Secure NFS トラフィックは加速化されません。
- HTTP：HTTP トラフィックを加速化します。
- SSL：暗号化された Secure Socket Layer（SSL; セキュア ソケット レイヤ）および Transport Layer Security（TLS; トランスポート レイヤ セキュリティ）トラフィックを加速化します。SSL アクセラレータは、WAAS 内でトラフィックの暗号化および複合化を行い、エンドツーエンドのトラフィック最適化を可能にします。SSL アクセラレータは、暗号化の証明書およびキーも安全に管理します。
- MAPI：Messaging Application Programming Interface（MAPI）プロトコルを使用する Microsoft Outlook Exchange トラフィックを加速化します。Microsoft Outlook 2000 ～ 2007 のクライアントがサポート対象です。メッセージ認証（署名）または暗号化を使用する安全な接続は加速化されず、MAPI over HTTP も加速化されません。
- ビデオ：RTSP over TCP を使用する Windows Media ビデオ ブロードキャストを加速化します。ビデオ アクセラレータは、自動的に、WAN からの 1 つのソース ビデオ ストリームを複数のストリームに分割し、LAN 上の複数のクライアントに供給します。ビデオ アクセラレータにより、UDP ストリームを要求するクライアントは、自動的にプロトコル切り替えを実行して TCP を使用します（クライアントとサーバの両方が TCP を許可する場合）。
- Windows プリント：クライアントとデータセンターにある Windows プリント サーバ間のプリント トラフィックを加速化します。Server Message Block（SMB; サーバ メッセージ ブロック）署名トラフィックは加速化されません。Windows プリント アクセラレータは、Windows 2000 および Windows Server 2003 プリント サーバをサポートします。Windows 2000、Windows XP、および Windows Vista が稼動するクライアントをサポートします。

アプリケーション アクセラレータを有効または無効にするには、「グローバル最適化機能の有効化と無効化」（P.12-2）を参照してください。

すべてのアプリケーション アクセラレータが動作するには、WAN リンクのどちらか一方の側にあるピア WAE の両方でアクセラレータを有効化する必要があります。

デスクトップ アプリケーション用のファイル サービス

ファイル サービス（CIFS アクセラレータ）機能を使用すると、WAE は、WAN 経由で要求をファイル サーバへ送信する代わりにクライアントのデータ要求を迅速に処理できるように、ローカル キャッシュにリモート ファイル サーバのデータを保存できます。WAE は、クライアントの要求をローカルに処理して WAN 経由で送信されるトラフィックを最小限に抑え、ブランチ オフィスのユーザがファイルや多くのデスクトップ アプリケーションにアクセスする時間を減らすので、企業は重要な情報をデータセンターに統合できます。

詳細については、第 11 章「WAFS の設定」を参照してください。

WAAS バージョン 4.1.1 以降は、相互に排他的な 2 つのファイル サービス モード（透過的 CIFS アクセラレータ モードおよびレガシー モード）をサポートしています。透過的 CIFS アクセラレータ モードでは、コア、エッジ、または接続の設定が不要です。レガシー モードは、WAAS バージョン 4.0.x と同様に設定します。これら 2 つのモードは、相互に排他的です。WAAS 4.0.x デバイスと相互作用する必要のない場合は、透過的 CIFS モードを使用することを推奨します。

（注）　レガシー モード WAFS は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー WAFS をお使いの場合は、透過的 CIFS アクセラレータに移行してください。

ファイル サービスには、次の機能があります。

- 事前配置：システム管理者は、頻繁に使用するファイルを中央のファイル サーバから選択した WAE のキャッシュに事前に「配置」できます。これにより、ユーザは最初からファイルに高速アクセスでき、使用可能な帯域幅の使用効率が上昇します。
- データの一貫性と並列性：データが最新であること（一貫性）を管理し、複数のクライアントによるデータへのアクセス（並列性）を制御して、WAAS システム全体にわたるデータの整合性を確保します。
- 自動検出：WAAS Central Manager で個々のファイル サーバを登録せずに、ファイル サービスを使用できます。自動検出機能が有効な場合、WAAS デバイスは、CIFS 要求を受信したときに、自動的に新しいファイル サーバを検出し接続します。

WAAS 印刷サービス

WAAS ソフトウェアには、次の印刷サービス オプションがあります。

- Windows プリント アクセラレータ：このオプションは、データセンターにプリント サーバがあり、ブランチ クライアントがローカルまたはリモート プリンタに印刷する場合に使用します。このサービスは、クライアントとデータセンターにある Windows プリント サーバ間のプリント トラフィックを加速化します。このオプションでは設定は必要ありませんが、CIFS アクセラレータと Windows プリント アクセラレータを有効にする必要があります。詳細については、「グローバル最適化機能の有効化と無効化」（P.12-2）を参照してください。
- 仮想ブレードに基づくプリント サーバ：このオプションは、別のプリント サーバ ハードウェアをインストールせずにブランチ オフィスにローカル プリント サーバを配備する場合に使用します。Windows プリント サーバをブランチ オフィスの WAE 上の仮想ブレードにインストールし、Windows プリント サーバの標準機能を使用して印刷を管理できます。詳細については、第 14 章「仮想ブレードの設定」を参照してください。
- レガシー WAAS プリント サービス：このレガシー サービスでは、WAAS に組み込まれている Samba および Common Unix Printing System（CUPS）ソフトウェアを使用し、ブランチ オフィスの WAE をローカル プリント サーバとして使用できます。詳細については、第 13 章「WAAS レガシー印刷サービスの設定および管理」を参照してください。

（注）　レガシー印刷サービスの機能は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー印刷サービスをお使いの場合は、Windows プリント アクセラレータに移行してください。

これら 3 つのサービスにより、ブランチ オフィスに別のハードウェア プリント サーバを設置する必要がなくなります。WAAS 印刷サービスは、Windows クライアントで使用でき、IP に基づく任意のネットワーク プリンタで動作します。

仮想化

WAAS ソフトウェアを使用すると、仮想ブレードを設定して、独自の操作環境で実行しているサービスを WAAS システムに追加できます。たとえば、WAE デバイスに仮想ブレードを設定して、印刷サービス、Active Directory サービス、DNS、DHCP サービスなどの Windows サービスを実行できます。

WAAS 仮想ブレードにより、WAE デバイス内に汎用コンピュータとして動作するエミュレート ハードウェア環境を実現できます。WAAS システムで使用するオペレーティング システムおよびアプリケーションをインストールし、ネットワーク上のユーザに追加サービスを提供できます。詳細については、第 14 章「仮想ブレードの設定」を参照してください。

WAAS インターフェイスの概要

WAAS ソフトウェアは、WAAS ネットワークの各種要素を管理、設定、モニタできる次のインターフェイスを提供しています。

- 「WAAS Central Manager GUI」（P.1-9）
- 「WAAS Device Manager GUI」（P.1-15）
- 「WAAS 印刷サービス管理 GUI」（P.1-16）
- 「WAAS CLI」（P.1-16）

WAAS Central Manager GUI

各 WAAS ネットワークには、ネットワーク内の他の WAAS デバイスを管理する 1 台のプライマリ WAAS Central Manager デバイスが必要です。WAAS Central Manager デバイスは、ネットワーク内の WAAS デバイスを設定、管理、モニタするための Web ベースのインターフェイスである WAAS Central Manager GUI を搭載しています。WAAS Central Manager は、専用の WAE デバイスに存在します。

WAAS Central Manager GUI を使用すると、管理者は次の作業を実行できます。

- 個々の WAAS デバイスまたはデバイス グループのシステム設定とネットワーク設定の構成
- WAAS デバイスが特定種類のトラフィックを代行受信したときに実行する処理を決定するアプリケーション ポリシーの作成と編集
- ファイル サービスと事前配置ポリシーの設定
- 同時に複数の WAE を管理し、構成するためのデバイス グループの作成
- WAAS ネットワーク内の最適化されたトラフィックに関する詳細なレポートの表示

（注）　WAAS Central Manager として設定された WAE では、ファイル サービス、印刷サービス、またはアプリケーション アクセラレーションを有効にすることができません。WAAS Central Manager の目的は、ネットワーク内の WAE を構成、モニタ、管理することです。

ここでは、次の内容について説明します。

- 「WAAS Central Manager GUI へのアクセス」（P.1-10）
- 「WAAS Central Manager GUI のコンポーネント」（P.1-10）
- 「WAAS Central Manager ナビゲーション ペイン」（P.1-12）
- 「WAAS Central Manager のタスクバー アイコン」（P.1-13）

WAAS Central Manager GUI へのアクセス

WAAS Central Manager GUI にアクセスするには、ブラウザで次の URL を入力します。

https://*WAE_Address*:8443/

*WAE_Address 値*は、WAAS Central Manager デバイスの IP アドレスまたはホスト名です。

管理者のデフォルトのユーザ名は *admin*、パスワードは *default* です。アカウントの作成とパスワードの変更については、第 7 章「管理者ユーザ アカウントおよびグループの作成と管理」を参照してください。

Web ブラウザが Unicode（UTF-8）文字コードを使用するように設定されていることを確認します。

WAAS Central Manager GUI を設定して、ユーザに許可される並列セッション数を制限できます。デフォルトでは、並列セッション数は無制限です。許可される並列セッション数を変更するには、「デフォルトのシステム設定プロパティの変更」（P.9-17）の説明に従って、System.security.maxSimultaneousLogins プロパティを適切に設定します。

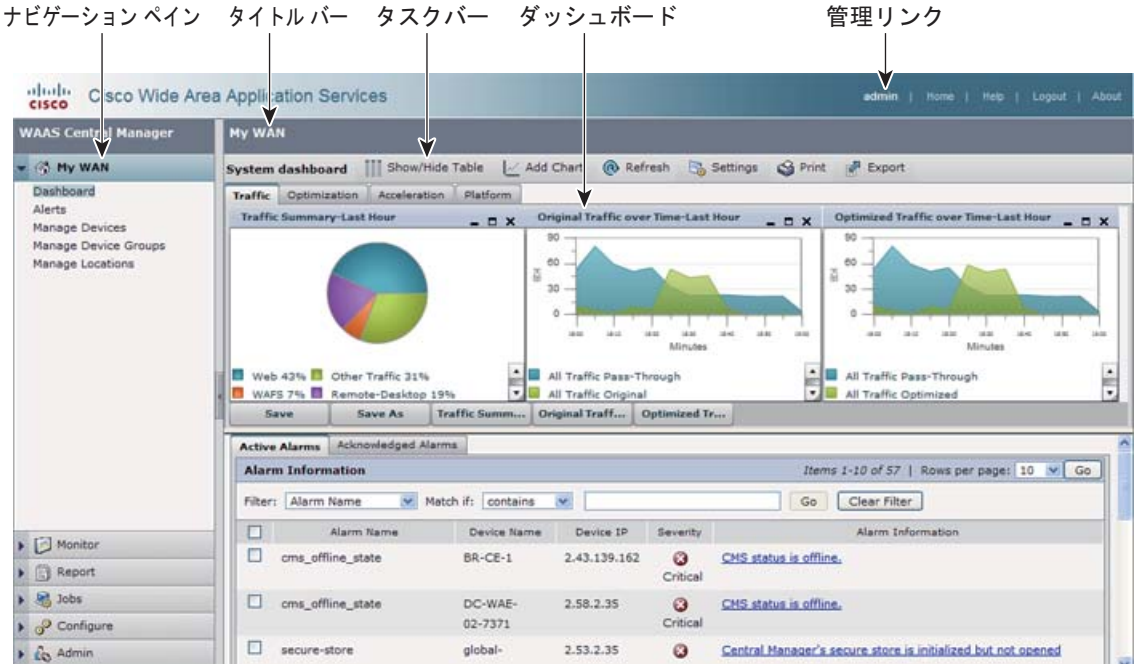
（注）　セッションを終了するには、Central Manager からログオフする必要があります。ユーザがログオフせずにブラウザを閉じたり、接続を切断すると、120 分後にタイムアウトになるまでセッションは閉じません。許可される並列セッションの数を超えた場合も、タイムアウトになるまで Central Manager GUI に再びアクセスできません。

（注）　アップグレード、ダウングレード、または新規インストールを行った場合、Internet Explorer のキャッシュをクリアしてから WAAS Central Manager に対するブラウザ セッションを再開する必要があります。

WAAS Central Manager GUI のコンポーネント

図 1-2 に、WAAS Central Manager GUI の主なコンポーネントを示します。

図 1-2　WAAS Central Manager GUI のコンポーネント



WAAS Central Manager GUI は、主に次のコンポーネントで構成されています。

- ナビゲーション ペイン：WAAS Central Manager の機能をグループ化する引出しで構成されています。詳細については、「WAAS Central Manager ナビゲーション ペイン」（P.1-12）を参照してください。
- タイトル バー：表示されているページのタイトル、および階層の前レベルにすばやく戻るためのブレッドクラム リンクを表示します（図 1-3 にブレッドクラム リンクを示します）。
- タスクバー：ダッシュボードのコンテンツに応じてさまざまな機能を実行するアイコンが表示されます。詳細については、「WAAS Central Manager のタスクバー アイコン」（P.1-13）を参照してください。
- ダッシュボード：メイン コンテンツを表示します。コンテンツは、ナビゲーション ペインで選択された機能によって変化します。
- 管理リンク：次のナビゲーション リンクで構成されます。
  - [Home]：システム ダッシュボードを表示します（図 1-2 を参照）。
  - [Help]：WAAS コンテキスト ヘルプの別ウィンドウを開きます。
  - [Logout]：現在のユーザを WAAS Central Manager からログアウトします。
  - [About]：バージョン番号を示す [WAAS About] ウィンドウを表示します。

WAAS Central Manager GUI は、次の 2 つのメイン コンテキストで構成されています。

- グローバル コンテキスト：最初はこのコンテキストが設定されており、特定のデバイスまたはデバイス グループは選択されていません。ナビゲーション ペインの 1 番上のドロワーには、[My WAN] が表示されます（図 1-2 を参照）。
- デバイス コンテキスト：[Manage Devices] ページまたは [Manage Device Groups] ページでデバイスまたはデバイス グループを選択した後は、このコンテキストが設定されます。ナビゲーション ペインの 1 番上のドロワーには、選択したデバイスまたはデバイス グループの名前が表示されます（図 1-3 を参照）。

図 1-3　WAAS Central Manager GUI：デバイス コンテキスト

デバイス コンテキストでは、WAAS Central Manager GUI に次の新規アイテムが追加されます。

- デバイス名：ナビゲーション ペインの 1 番上のドロワーに、選択したデバイスまたはデバイス グループの名前が表示されます。
- システム ダッシュボード リンク：[My WAN] にシステム ダッシュボードが表示され、グローバル コンテキストに戻ります。
- 現在の場所へのブレッドクラム：GUI での現在の場所へのパスを表示します。[Devices] リンクをクリックして、[Manage Devices] ページに戻ることができます。デバイス グループを管理している場合、このリンクの名前は [Device Groups] で、[Manage Device Groups] ページに戻ります。

- [Switch Device] リンク：デバイスを切り替えて、GUI の同じ機能のデバイス コンテキスト ページにとどまることができます。このリンクをクリックすると、[Switch Devices] ページが開きます（図 1-4 を参照）。別のデバイスに切り替えるには、デバイスの横のオプション ボタンを選択して [Switch] ボタンをクリックします。

  デバイス グループを管理している場合、このリンクの名前は Switch DeviceGroup で、デバイスと同様に別のデバイス グループに切り替えることができます。

図 1-4　[Switch Devices] ページ

WAAS Central Manager ナビゲーション ペイン

WAAS Central Manager GUI ナビゲーション ペインは、WAAS Central Manager の機能をグループ化するドロワーで構成されています。表 1-2 で、ナビゲーション ペインのドロワーについて説明します。

グローバル コンテキストが設定されている場合と比べて、特定のデバイスまたはデバイス グループが選択されている場合、ドロワーは異なる機能で構成されることがあります。

表 1-2　ドロワーの説明

ドロワー	説明
[My WAN] または [*Device name*]	WAAS ネットワーク全体のダッシュボードおよびアラート表示に移動し、WAAS サービスおよび一般設定を構成する特定のデバイスまたはデバイス グループを選択できます。詳細なデバイス情報とメッセージを表示して、場所を管理することも表示できます。 特定のデバイスまたはデバイス グループを選択した場合、このドロワーにはそのデバイスまたはデバイス グループの名前が付けられ、デバイスをアクティブ化したりグループまたはデバイスを割り当てることができます。すべてのデバイスのビューに戻るには、[View All Devices] を選択します。
[Monitor]	ネットワーク トラフィックおよび他のチャートやレポートを表示し、WAAS ネットワークの状態およびパフォーマンスをモニタできます（このドロワーは、グローバル レベルで、またはデバイス グループではなく個別デバイスが選択されている場合に限り表示されます）。
[Report]	WAAS ネットワークのレポートを管理およびスケジュールできます（このドロワーは、デバイスまたはデバイス グループが選択されていないグローバル レベルに限り表示されます）。
[Troubleshoot]	トラブルシューティング ツールを使用できます（このドロワーは、グローバル レベルではなく、デバイスまたはデバイス グループが選択されている場に限り表示されます）。
[Jobs]	ソフトウェア更新ジョブを管理できます。

表 1-2　ドロワーの説明 （続き）

ドロワー	説明
[Configure]	主な WAAS サービス（ファイル、印刷、およびアプリケーション アクセラレーション）およびその他の設定を構成できます。
[Admin]	ユーザ アカウント、パスワード、ライセンス、および仮想ブレードを管理したり、システム ログを表示したりできます。

WAAS Central Manager のタスクバー アイコン

表 1-3 で、WAAS Central Manager GUI にあるタスクバー アイコンについて説明します。

表 1-3　タスクバー アイコンの説明

タスクバー アイコン	機能
共通のアイコン	
（更新）	WAAS Central Manager GUI の現在のページを更新します。
（削除）	デバイス、デバイス グループ、印刷ドライバ、またはファイル サービス ポリシーなどの WAAS 要素を削除します。
（作成）	ファイル サービス ポリシーやアクセラレーション ポリシーなどの新しい WAAS 要素を作成します。
（詳細検索）	特定の項目を見つけやすくするために、表内の情報を選別します。
（すべてを表示）	すべての項目を（複数のページでなく）単一ページに表示します。
（印刷または表の印刷）	情報を印刷します。
（すべてを割り当て）	表内のすべての有効な項目を選択します。たとえば、WAAS プリント サーバへ印刷ドライバを配信している場合、このアイコンをクリックすると、プリント サーバがダウンロードする必要があるリスト内のすべてのドライバを選択できます。
（すべてを削除）	表で選択されているすべての項目の選択を解除します。
デバイスおよびデバイス グループ アイコン	
（有効でないすべての WAE の有効化）	WAAS ネットワーク内の有効でないすべての WAE を有効にします。詳細については、「すべての非アクティブ WAAS デバイスのアクティブ化」（P.15-32）を参照してください。

表 1-3　タスクバー アイコンの説明 （続き）

タスクバー アイコン	機能
（更新の強制）	WAAS Central Manager GUI に表示されるデバイス設定をデバイスに再適用します。一般に、WAAS Central Manager GUI で行った変更は、設定を確認するとただちにデバイスに適用されます。ただし、CLI エラーまたはデバイスのエラーにより、デバイスの設定が WAAS Central Manager GUI に表示される設定と異なる場合があります。データベース全体の強制更新アイコンは、WAAS Central Manager がデバイスを更新する 設定全体をにデバイスに適用し、設定が再適用されます。 デバイスの CLI エラーは、「システム メッセージ ログの表示」（P.16-61）に説明されている [System Message] ウィンドウに表示できます。 データベース全体の強制更新アイコンは、「[Device Dashboard] ウィンドウ」（P.16-9）に説明されている [Device Dashboard] ウィンドウに表示されます。
（リロード）	WAAS Central Manager GUI に表示される位置に応じて、WAE またはデバイス グループをリブートします。詳細については、「デバイスまたはデバイス グループのリブート」（P.15-33）を参照してください。
（強制グループ設定）	そのグループのすべてのデバイスに、デバイス グループ設定を強制します。詳細については、「グループ内のすべてのデバイスへのデバイス グループ設定の強制」（P.3-8）を参照してください。
（デフォルトの適用）	ウィンドウのフィールドにデフォルト設定を適用します。
（表のエクスポート）	表の情報を CSV ファイルにエクスポートします。
（基準グループの切り替え）	基準グループに関連付ける別のデバイス グループを選択できます。 詳細については、「サービス用の基準グループの切り替え」（P.3-13）を参照してください。
（グループ設定の変更）	デバイスのグループ設定に優先するデバイス固有の設定を指定できます。 詳細については、「デバイス上のデバイス グループ設定の変更」（P.3-9）を参照してください。
（デバイスの無効化）	WAE を無効にします。
（アプリケーション統計情報の更新）	アプリケーション統計情報を更新します。
（すべてを削除）	IP ACL 条件などの特定の種類のすべて WAAS 要素を削除します。
（すべてのデバイスを表示）	ナビゲーション ペインにすべての WAE デバイスまたはデバイス グループを表示します。
（ダッシュボード表示の設定）	[Device Dashboard] ウィンドウに表示するチャートを指定できるようにします。

表 1-3　タスクバー アイコンの説明 （続き）

タスクバー アイコン	機能
印刷サービス アイコン	
（故障したドライバのダウンロード再試行）	WAAS プリント サーバまたはデバイス グループへ配信できなかった印刷ドライバをダウンロードします。詳細については、第 13 章「WAAS レガシー印刷サービスの設定および管理」を参照してください。
（印刷サービス管理 GUI）	WAAS 印刷サーバ用の印刷サービス管理 GUI を開きます。この GUI から実行できる作業の詳細については、「Print Services Administration GUI の使用方法」（P.13-28）を参照してください。
アクセラレーション アイコン	
（デフォルト ポリシーと分類子の復元）	デバイスまたはデバイス グループにデフォルトの事前定義されたアプリケーション ポリシーを復元します。詳細については、「アプリケーション ポリシーと分類子の復元」（P.12-38）を参照してください。
（トポロジの表示）	WAE デバイス間のすべての TFO 接続を示すトポロジ マップを表示します。詳細については、「トポロジ レポート」（P.16-44）を参照してください。
（アプリケーション設定ページへ移動）	アプリケーションを作成するための設定ページを表示します。詳細については、「アプリケーションのリストの表示」（P.12-37）を参照してください。
システム メッセージ ログ アイコン	
（表の中断）	詳細については、「システム メッセージ ログの表示」（P.16-61）を参照してください。

WAAS Device Manager GUI

WAE Device Manager は、ネットワーク内の個々の WAE デバイスを構成、管理、およびモニタできる Web ベースの管理インターフェイスです。WAE Device Manager と WAAS Central Manager GUI の両方に同じデバイス設定が存在することがあります。そのため、できるだけ WAAS Central Manager GUI からデバイス設定を構成することを推奨します。

場合によって、特定の作業を実行するために WAE Device Manager GUI を使用する必要があります。たとえば、次の作業は、WAE Device Manager GUI から実行できますが、WAAS Central Manager GUI からは実行できません。

- WAE での印刷サービスの有効化
- デバイス サービスの停止

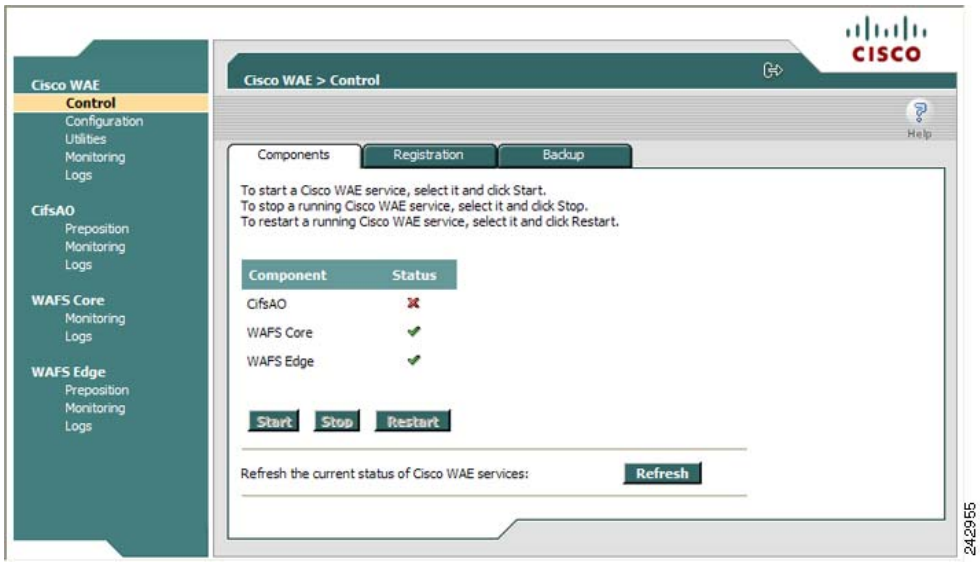
WAE Manager から実行できる作業の詳細については、第 10 章「WAE Device Manager GUI の使用方法」を参照してください。

特定のデバイス用の WAE Device Manager にアクセスするには、次の URL へ進みます。

https://*Device IP Address*:8443/mgr

図 1-5 に、WAE Device Manager ウィンドウの例を示します。

図 1-5　WAE Device Manager ウィンドウの例



WAAS 印刷サービス管理 GUI

印刷サービス管理 GUI は、個々の WAAS プリント サーバを構成し、処理中および完了したプリント ジョブのリストを表示できる Web ベースのインターフェイスです。

印刷サービス管理 GUI から、次の共通作業を実行できます。

- WAAS プリント サーバへのプリンタの追加
- 既存のプリンタの設定の変更
- 印刷クラスタのセットアップ
- 印刷ジョブの表示

印刷サービス管理 GUI は、WAAS Central Manager GUI または WAE Manager GUI からアクセスできます。詳細については、第 13 章「WAAS レガシー印刷サービスの設定および管理」を参照してください。

WAAS CLI

WAAS CLI を使用すると、コンソール接続または端末エミュレーション プログラムを通じて、WAE をデバイス単位で構成、管理、モニタすることができます。また、WAE への Lightweight Directory Access Protocol（LDAP）サインオンの設定など、CLI だけがサポートしている特定の機能を設定できます。可能な場合は、WAAS CLI でなく、WAAS Central Manager GUI を使用することを強く推奨します。

（注）　WAAS Central Manager で WAE を登録してから、WAE で CLI 設定の変更を行うまでに、約 10 分間（2 データ フィード ポール サイクル）待機する必要があります。これよりも前に CLI 設定の変更を行った場合、Central Manager が WAE を更新する際に上書きされます。すべての設定の変更は、Central Manager GUI を使用して行うことを強く推奨します。

WAAS CLI は、4 つのコマンド モードから編成されています。各コマンド モードには、WAE の設定、保守、およびモニタリング用のコマンド セットがあります。使用できるコマンドは、モードによって異なります。システム プロンプトで疑問符（?）を入力すると、各コマンド モードで使用可能なコマンドのリストを表示できます。

4 つの WAAS コマンド モードは次のとおりです。

- EXEC モード：システム動作の設定、表示、およびテスト用。このモードは、ユーザと特権の 2 つのアクセス レベルに分かれています。特権アクセス レベルを使用するには、ユーザ アクセス レベルのプロンプトで **enable** コマンドを入力し、パスワード プロンプトが表示されたら、特権 EXEC パスワードを入力します。
- グローバル コンフィギュレーション モード：装置全体に対する WAAS ソフトウェア機能の設定、表示、およびテスト用。このモードを使用するには、特権 EXEC モードから **configure** コマンドを入力します。
- インターフェイス コンフィギュレーション モード：特定のインターフェイスにおけるコンフィギュレーションの設定、表示、およびテスト用。このモードを使用するには、グローバル コンフィギュレーション モードから **interface** コマンドを入力します。
- その他のコンフィギュレーション モード：特定の機能を管理するために、グローバル コンフィギュレーション モードから、一部のコンフィギュレーション モードを使用できます。

CLI を使用して WAAS デバイスを構成する方法については、『*Cisco Wide Area Application Services Command Reference*』および『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。

Cisco WAAS の利点

ここでは、Cisco WAAS の利点について説明します。内容は、次のとおりです。

送信元 TCP/IP 情報の維持

多くの最適化製品が、ルータおよび他のネットワーク デバイスを通過するトンネルを作成するため、最適化されたデータに送信元 TCP/IP 情報が維持されません。そのため、重要なネットワーク サービス（QoS、NBAR など）が中断し、NetFlow のようなトラフィック分析ツールおよび ACL や IP に基づくファイアウォールのようなセキュリティ製品の機能の正常な動作が中断する場合があります。

他の最適化製品と異なり、Cisco WAAS は、ネットワークに円滑に統合され、最適化するトラフィックにすべての TCP/IP ヘッダー情報を保存するので、既存の分析ツールやセキュリティ製品は中断しません。

WAAS デバイスの自動検出

Cisco WAAS には、WAE がネットワーク上のピア WAE を自動的に検出できる自動検出機能があります。WAE は、ピア デバイスを自動検出したあとで、LAN と WAN TCP の接続を停止して分離し、異なる速度を解決するためにバッファ層を追加することができます。WAE がピア WAE との接続を確立すると、2 台のデバイスは TCP トラフィック用に最適化されたリンクを確立したり、最適化せずにトラフィックを渡すことができます。

ピア WAAS デバイスの自動検出は、独自の TCP オプションを使用して行われます。これらの TCP オプションは、WAAS デバイスだけに認識、理解され、WAAS 以外のデバイスでは無視されます。

ネットワークの集中モニタリングと管理

Cisco WAAS の Web ベースの管理ツール（WAAS Central Manager および WAE Device Manager GUI）を使用すると、IT 管理者は、各 WAAS デバイスの使用制限、バックアップ、障害復旧、復元、アクセス コントロール、およびセキュリティ ポリシーのようなポリシーを集中的に定義、モニタ、および管理することができます。また、IT 管理者は、次の作業を実行できます。

- 各 WAAS デバイスまたはデバイス グループのリモート配備、構成、およびモニタ
- 総合的な統計情報、ログ、および報告によるシステムのパフォーマンスと使用率の最適化
- SNMP ベースのモニタリング、トラップ、アラート、およびデバッグ モードのようなツールによる作業の問題解決

IT 管理者は、Cisco WAAS の次の機能を利用できます。

- ネイティブ プロトコル サポート：企業向けの基本的なファイル システム プロトコル（Windows/CIFS）の完全なエンド ツー エンドのサポートを提供します。各クライアントとファイル サーバ間には、セキュリティ、並列性、一貫性が維持されます。
- 透過性：アプリケーション、ファイル システム、およびプロトコルに対して完全に透過的なので、異機種環境を含む既存のネットワーク インフラストラクチャに円滑に統合できます。また、Cisco WAAS は、現在展開されているセキュリティ技術に影響しません。
- ブランチ オフィスのデータ保護：ブランチ オフィスのデータ保護を強化します。Cisco WAAS のファイル キャッシュは、オフィスの LAN でローカル ファイル サーバと同じように見えます。エンド ユーザは、Windows または UNIX ユーティリティを使用して、個人用ドキュメント フォルダをファイル キャッシュにマッピングできます。キャッシュにコピーしたユーザ データは、高速にアクセスできるようにブランチ オフィスの WAE にローカルに保存されます。マスター コピーは、良好に保護されたデータセンターに集中的に保存されます。
- 集中管理されたバックアップ：Cisco WAAS は、企業全体にわたるデータをデータセンターに統合するので、集中管理されたストレージ管理手順をブランチ オフィスのデータに簡単に適用できます。データが分散されている場合に比べ、バックアップと復元作業が簡素化、高速化され、信頼性が向上します。

  データが消失した場合、データセンターにバックアップ ファイルが存在するので、復旧用に迅速にアクセスできます。データセンターで中央管理されるストレージに対するバックアップの頻度が多いため、データ消失の量が大幅に減ります。このような集中管理されたストレージのバックアップにより、単体のファイル サーバや NAS アプライアンスでの作業に比べ、障害復旧の効率と経済性が大幅に上昇します。

- ストレージ管理の簡素化：ストレージをリモート地点から中央のデータ ファシリティに移行することでコストが削減され、企業全体のストレージ管理が簡単になります。
- WAN の適用：リモート ユーザが、データセンターに存在するファイルに、LAN アクセス並にアクセスできるようになります。WAAS は、WAE 間のトラフィック転送を最適化する独自のプロトコルを使用します。WAE 間の通信が中断すると自動的に Disconnected Mode（切断モード）に切り替わり、ネットワーク内のファイルの一貫性を損なう可能性がある操作を防止します。

最適化された読み取り / 書き込みキャッシュ

Cisco WAAS の Wide Area File Services（WAFS）機能は、ファイルをクライアントの付近でローカルに保存します。ファイルに行われた変更は、ただちにローカル ブランチ オフィスの WAE に保存され、ストリーム化されて中央のファイル サーバへ転送されます。中央に保存されたファイルは、ブランチ オフィスのユーザにはローカル ファイルのように見えるので、アクセス パフォーマンスが向上します。WAFS キャッシングには、次の機能があります。

- ローカル メタデータ処理とキャッシング：ファイル属性やディレクトリ情報のようなメタデータをローカルにキャッシュし、保存できるので、ユーザ アクセスを最適化できます。
- ファイルの一部のキャッシング：転送を最適化するために、ファイル全体でなく、書き込み要求で更新されたファイルのセグメントだけを伝送します。
- ライトバック キャッシュ：データセンターの WAE がブランチ オフィスの WAE からの書き込みをバッファに入れ、データ整合性を損なわずに更新をストリーム化し、非同期的にファイル サーバへ転送できるので、書き込み処理の効率が向上します。
- 事前ファイル読み取り：WAE は、アプリケーションが順次ファイル読み取りを実行しているときに、ユーザが要求するファイルを事前に読み取ることができるので、パフォーマンスが向上します。
- 負性キャッシング：WAE は欠落したファイルに関する情報を保存できるので、WAN 経由のラウンドトリップ回数が減ります。
- Microsoft Remote Procedure Call（MSRPC）の最適化：要求と応答のローカル キャッシングを使用して、WAN 経由のラウンドトリップ回数を減らします。
- メッセージの予測と減少の通知：アルゴリズムを使用して、特性を失わずに WAN 経由のラウンドトリップ回数を減らします。

ブランチ オフィスの WAE とデータセンターの WAE 間の WAN では独自の適応プロトコル層を使用し、クライアント側とサーバ側では標準の CIFS プロトコルを使用します。この独自のネットワーク プロトコルは、特に遅延が大きく、帯域幅に制約がある条件で、信頼性の高い効率的な WAN 経由通信を提供します。

Cisco WAAS プロトコルには、次の利点があります。

- 信頼性：内部メッセージ キューと順序を維持するので、一時的な接続解除、ネットワーク変動、およびメッセージ損失に対応できます。Cisco WAAS トランスポート層は、接続を再確立し、切断されたソケットで応答を受信しなかった要求を再送信して、一時的なネットワーク障害に対応します。
- 効率性：相互に依存する複数の要求と応答を 1 つのメッセージにグループ化する「複合要求」をサポートしています。複合メッセージ内の個別呼び出しの処理はシリアル化されるので、あるコマンドの出力を次のコマンドの入力として使用できます。
- リンク使用率の最適化：ブランチ オフィスの WAE とデータセンターの WAE 間の各リンク用に複数の並列 TCP 接続を使用します。要求と応答は、使用可能な任意の接続経由で配信できます。たとえば、データ配信の複数の要求（および応答）を複数の接続に分割することで、TCP パフォーマンスが低下する遅延と損失が大きい WAN 接続で、ネットワークを効率的に利用できます。

- コマンドの優先順位の設定：動作中のクライアントからの要求に高い優先順位を割り当てるので、ユーザが経験する WAN 遅延が減少します。バッチ タスク（事前配置など）は低い優先順位が割り当てられ、バックグラウンドで実行されます。
- 帯域幅の節減：すべての要求と応答は圧縮されます。メッセージは符号化されてから圧縮されるので、テキスト データとバイナリ データの両方の配信効率が向上します。プロトコル層は、メッセージの内容にかかわらず、自動的に圧縮を適用します。
- ファイアウォール対応：TCP/IP 上の階層構造であり、TCP ポート 4050 を使用します。ファイアウォールは、TCP ポート 4050 を開いてトラフィックが通過できるように設定する必要があります。

WCCP のサポート

シスコシステムズが開発した Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）は、1 台または複数のルータ（またはレイヤ 3 スイッチ）および 1 台または複数のアプリケーション アプライアンス、Web キャッシュ、および他のアプリケーション プロトコルのキャッシュ間の通信を規定しています。通信の目的は、ルータのグループを通過する選択した種類のトラフィックの透過的なリダイレクションを確立し、維持することです。選択したトラフィックは、アプライアンスのグループへリダイレクトされます。あらゆる種類の TCP トラフィックをリダイレクトできます。

WCCP v2 プロトコルは、自動フェールオーバーやロード バランシングのような便利な機能が組み込まれています。ルータは、WCCP キープアライブ メッセージを通じて、ルータに接続している各 WAE の状態をモニタし、WAE が停止している場合、WAE へのパケットのリダイレクションを中止します。ブランチ オフィスの WAE は、WCCP を使用して、シングル ポイント障害になることを回避します。また、ルータは、複数のブランチ オフィスの WAE の間でトラフィックの負荷を分散できます。

Cisco WAAS は、WCCP を使用して、TCP セッションの透過的な代行受信をサポートしています。ルータとブランチ オフィスの WAE の両方で WCCP が有効になると、新しいセッションだけが代行受信されます。既存のセッションには影響しません。

PBR のサポート

Policy-Based Routing（PBR; ポリシーベース ルーティング）を使用すると、組織は、トラフィックの分類に基づいて選択的にトラフィックをネクストホップへ転送するように、ネットワーク デバイス（ルータまたはレイヤ 4 ～レイヤ 6 スイッチ）を構成できます。WAAS 管理者は、PBR を使用して、既存のブランチ オフィス ネットワークとデータセンターに WAE を透過的に統合できます。PBR を使用すると、定義されたポリシーに基づいて一部またはすべてのパケットが通過するルートを確立できます。

PBR の詳細については、第 4 章「トラフィック代行受信の設定」を参照してください。

インライン代行受信のサポート

直接インライン トラフィック代行受信は、Cisco WAE Inline Network Adapter をインストールした WAE でサポートされています。トラフィックのインライン代行受信は、構成を簡素化し、ルータでの WCCP または PBR の設定の複雑さを軽減します。

Cisco WAE Inline Network Adapter は、トラフィックを透過的に代行受信し、最適化の必要のないトラフィックをブリッジングします。電源、ハードウェア、修復不可能なソフトウェア障害が発生した場合に自動的にトラフィックをブリッジングする、フェールセーフ機構の設計も使用します。

ある VLAN からのトラフィックだけを受信し、他のすべての VLAN のトラフィックはブリッジングされて処理されないように、Cisco WAE Inline Network Adapter を設定できます。

デバイスの故障に備えてアベイラビリティを高めるために、Cisco WAE Inline Network Adapter が搭載された WAE デバイスを連続的にクラスタ化できます。現在最適化を行っているデバイスが故障すると、クラスタ内の 2 つめの WAE が最適化サービスを提供します。スケーリングまたはロード バランシングのために WAE デバイスをシリアル インライン クラスタに配置することは、サポートされていません。

インライン モードの詳細については、「TCP トラフィックの透過的な代行受信へのインライン モードの使用」（P.4-43）を参照してください。

障害復旧と保護

Cisco WAAS は、WAFS が停止する確率と時間を最小限に抑えるハイ アベイラビリティ フェールオーバー（およびロード バランシング）機能を提供しています。

WAFS 用に設定された WAE が故障すると、その WAE と動作するように設定されたすべてのピア WAE が、別の WAE と動作するようにリダイレクトされます。この動作は、サービスを中断せず、ハイ アベイラビリティを維持します。

この変更がユーザに透過的にならない場合があります。そのため、クライアント接続が閉じられ、CIFS クライアントが接続を再確立する必要があります。このような変更が現在実行中のアプリケーションに影響をするかどうかは、使用しているアプリケーションの動作と特定の CIFS クライアントの動作に依存します。ただし、移行は、一般にクライアントには透過的です。

レガシー モードを使用しているときに、Edge WAE とコア クラスタ間の通信またはコアクラスタとファイル サーバ間の通信が中断すると、Cisco WAAS ネットワークは、完全な通信が復旧するまで、非接続状態で動作するように切り替わります。中断が短い場合、ネットワークは過渡的な非接続状態になり、すでに開いているファイルに対する読み取りコマンドのような一部のサービスとコマンドが限られた時間（通常は約 1 分）だけ有効になります。

ネットワーク障害が長時間続く場合、Cisco WAAS は完全な非接続状態に切り替わり、クライアントにはサービスが提供されません。このモードでは、システムは、接続が再確立されるまで、（キャッシュされたファイルを含む）任意のファイルへのアクセスを拒否します。ユーザには、Edge WAE が、接続しているネットワークが切断しているかのように応答するように見えます。

この方法は、データのセキュリティを維持するために必要です。サービス中断状態を強制しない場合、ファイル サーバにローカルに接続しているユーザはそのままファイル操作を継続できるので、ネットワークが中断したときに同じファイルをリモートに操作していた他のユーザとの競合が発生します。Cisco WAAS は、データの一貫性と並列性を損なう状況を防止するように設計されています。

（注）　切断操作は、CIFS レガシー モードだけで機能します。CIFS アクセラレータでは機能しません。

名前空間のサポート

レガシー CIFS ユーザが Edge WAE がキャッシュするファイル サーバにアクセスし、組織の名前空間に組み込むには、複数の方法があります。その 1 つは、ファイル サーバごとに固有の名前を作成するために、特定のサイト用のプレフィクス、拡張子、またはエイリアスを使用する方法です（エイリアスを使用すると、データセンターでローカル ファイル サーバを新しいサーバと交換した後でも古いファイル名を維持できます）。あるいは、キャッシュされるファイル サーバを DFS リンクとして DFS 名前空間に組み込む方法もあります。レガシー CIFS で DFS を使用するときは、Edge WAE（またはエッジ デバイス グループ）ごとに、DFS サイト名を手動で設定する必要があります。この情報により、DFS は、ユーザの要求を正しく転送できます。リモート ユーザは、適切な Edge WAE 経由でファイル サーバに接続し、ローカル ユーザは、WAE キャッシュを利用せずにファイルに直接アクセスできます。

RAID の対応

Cisco WASS は、ストレージ容量の増加や信頼性の向上に対応するために次の Redundant Array of Independent Disks（RAID; 冗長ディスク アレイ）機能を提供しています。

- RAID 5 を使用した論理ディスク処理 : WAAS のハードウェア機能として RAID 5 を使用した論理ディスク処理が実装されています。RAID 5 デバイスでは、単一の論理ディスク ドライブが作成できます。この論理ドライブには最大 6 台の物理ハード ディスク ドライブを搭載でき、ディスク容量を論理的に拡張します。

  RAID 5 を実装したシステムは、物理ドライブのどちらか 1 つが故障したりオフラインになったりしても動作し続けます。

- RAID 1 を使用した論理ディスク処理 : WAAS のソフトウェア機能として RAID 1 を使用した論理ディスク処理が実装されています。RAID 1 ではディスク ミラーリングを実行して、2 つ以上のドライブにデータを重複して書き込み、信頼性を向上させます。

  2 つのディスク ドライブに対して書き込み処理が行われるため、ファイルシステムの書き込み速度が低下することがあります。

- ディスクのホットスワップ機能のサポート : RAID 1 を実装した WAAS では、ディスク ハードウェアのホットスワップに対応しています。RAID 5 の場合も、RAID アレイのシャット ダウン後にディスク ハードウェアを活性挿抜することができます。RAID システムのディスクの取り外しおよび取り換え手順については、第 15 章「WAAS システムの保守」を参照してください。

円滑なセキュリティ

Cisco WAAS はディスクの暗号化をサポートします。暗号化により、導入した WAAS システムで送受信され、WAAS 永続ストレージに保存される機密情報が安全に保護されます。

Cisco WAAS では、すでに手一杯の状態の IT スタッフにさらに負担をかけるような保守作業は不要です。固有のユーザ管理階層を追加することを回避し、代わりにファイル サーバが維持しているユーザ、ユーザ認証、およびアクセス コントロール リストを利用します。セキュリティに関連するすべてのプロトコル コマンドは、送信元ファイル サーバと送信元ドメイン コントローラに直接委譲されます。ドメインと送信元ファイル サーバで認識されるユーザは、同じセキュリティ レベルで自動的に Cisco WAAS によって認識され、追加的な設定や管理は不要です。

Cisco WAAS は、アクセス コントロールと認証の決定を オリジン ファイル サーバに委譲します。

SNMP のサポート

Cisco WAAS は、SNMPv1、SNMPv2、および SNMPv3 を含む Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）をサポートしています。Cisco WAAS は、HP OpenView や IBM Tivoli NetView のような普及している多くの SNMP マネージャをサポートしています。

Cisco WAAS は、次の読み取り専用のプライベート MIB に基づいてパラメータをエクスポートします。

- ACTONA-ACTASTOR-MIB.my
- CISCO-CONTENT-ENGINE-MIB

さらに、Cisco WAAS は、トラップの設定など、これらの標準的な各 MIB の完全な機能をサポートしています。ほとんどの Cisco WAAS トラップは、WAAS Central Manager GUI に表示されるログにも記録されます。ただし、一部のトラップ（最大セッション数の超過など）は、SNMP マネージャだけに報告されます。

- MIB-2 一般的なネットワーク統計情報（RFC 1213 および 1157）：TCP/IP に基づくネットワークの基本的な管理用の重要なパラメータを含みます。
- ホスト リソース（RFC 1514）
- SNMPv3 MIB（RFC 2571 ～ 2576）
- DISMAN-EVENT-MIB（RFC 2981）
- ENTITY-MIB（RFC 2037）

Cisco WAAS は、SNMPv2 に基づくパラメータをサポートしているので、共通の SNMP 管理システムに統合できます。これらのパラメータを使用すると、システム管理者は、WAAS ネットワークの現在の状態とパフォーマンス レベルをモニタできます。

エクスポートされるパラメータは、次のカテゴリに分かれます。

- 一般的なパラメータ：バージョン、ビルド番号、およびライセンス情報を含みます。
- 管理パラメータ：Central Manager の位置を含みます。
- データセンター WAE パラメータ：一般的なパラメータ、ネットワーク接続パラメータ、およびエクスポートされるファイル サーバを含みます。
- ブランチ オフィス WAE パラメータ：一般的なパラメータ、ネットワーク接続パラメータ、および CIFS 統計情報、およびキャッシュ統計を含みます。

SNMP サポートの詳細については、第 17 章「SNMP モニタリングの設定」を参照してください。

CHAPTER 2

WAAS ネットワークの計画

この章では、Wide Area Application Service（WAAS）ネットワークを設定する前に注意すべき一般的なガイドライン、制約事項、および制限事項について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

WAAS ネットワークを計画するためのチェックリスト

企業やサービス プロバイダーは、WAAS ソフトウェアを実行する Cisco WAE を使用すると、ブランチ オフィスとデータセンター間のアプリケーション トラフィックのフローを最適化できます。WAE ノードは、ネットワーク接続されたアプリケーション クライアントとサーバの付近にある WAN エンドポイントに配備して、WAN 経由のアプリケーション トラフィックを代行受信して最適化します。WAE ノードは、指定された処理ポイントのネットワーク フローに挿入する必要があります。

WAAS ソフトウェアは、次の 3 つの典型的なネットワーク トポロジをサポートします。

- ハブ & スポーク構成：ハブ & スポーク構成ではサーバが集中管理され、ブランチ オフィスにはクライアントと少数のローカル サービス（たとえば、WAAS 印刷サービス）だけが配置されます。

- メッシュ構成：メッシュ構成では、任意の場所にクライアントとサーバを配置でき、クライアントは任意の数のローカル サーバやリモート サーバにアクセスできます。
- 階層型構成：階層型構成では、複数の地域や各国のデータセンターにサーバが配置され、さまざまなクライアントがアクセスします。データセンター間の接続は、ブランチ オフィスとの接続より高い帯域幅です。

構成は、クライアント/サーバ型のアクセス パターンに従い、物理ネットワークリンクと異なる場合がある WAAS 要素の接続に応じて異なります。詳細については、第 1 章「Cisco WAAS の概要」を参照してください。

計画のチェックリスト

WAAS ネットワークを計画するときは、ガイドラインとして次のチェックリストを使用してください。次のチェックリストが示すように、計画フェーズは、論理的に主に 3 つの計画作業カテゴリに分けることができます。

- 規模決定フェーズ
- 管理計画
- アプリケーション最適化計画

（注） 多少の相互依存性はありますが、特定の計画フェーズのすべての手順を完了しなくても、次の手順を開始できます。

ネットワークを計画するには、次のガイドラインに従ってください。

1. 次の作業を含む規模決定フェーズを完了します。

- 既存のネットワークで WAAS 最適化が必要な場所（たとえば、ブランチ オフィスとデータセンター）を決定します。
- それぞれの場所に必要な WAAS デバイスの台数とモデルを決定します。この選択プロセスで重要な要素は、WAN 帯域幅、ユーザ数、および予想される使用方法です。さまざまなハードウェア構成が可能です（たとえば、異なるハードディスク モデルやメモリのサイズ）。スケーラビリティとフェールオーバーが必要な場所には、WAE のクラスタを運用することを検討します。詳細については、「必要な WAAS デバイスの台数の計算」（P.2-17）を参照してください。
- 要件を満たすために十分なライセンスを購入したことを確認します。

2. 次のように管理を計画します。

- サイトとネットワークの計画を完了します（たとえば、IP アドレスとサブネット、ルータとデフォルト ゲートウェイの IP アドレス、およびデバイスのホスト名のような IP とルート指定情報を入手します）。『*Cisco Wide Area Application Services Quick Configuration Guide*』の「Checklist of WAAS Network System Parameters」の表を参照してください。
- WAAS Central Manager と WAE が使用するログイン認証とログイン許可の方法（たとえば、外部 RADIUS、TACACS+、Windows ドメイン サーバ）およびアカウント ポリシーを決定します。詳細については、第 6 章「管理ログインの認証、許可、およびアカウンティングの設定」を参照してください。
- セキュリティのために、WAE の初期設定を完了したあとで、定義済みの superuser アカウント用の定義済みのパスワードをただちに変更するように計画します。詳細については、「WAAS ログイン認証および許可」（P.2-26）を参照してください。
- WAAS デバイス用に管理アカウントを追加する必要があるかどうかを決定します。詳細については、第 7 章「管理者ユーザ アカウントおよびグループの作成と管理」を参照してください。

- WAE を論理グループに構成する必要があるかどうかを決定します。詳細については、「WAE の論理グループの作成」（P.2-27）を参照してください。
- どの管理アクセス方式を使用するかを決定します。デフォルトで Telnet が使用されますが、特定の構成では SSH の方が望ましい場合があります。詳細については、「WAAS デバイス用のログイン アクセス コントロール設定の構成」（P.6-7）を参照してください。

3. 次のようにアプリケーション最適化を計画します。

- ルータの相互運用性問題を決定し、解決します（たとえば、サポートされるハードウェアとソフトウェアのバージョン、代行受信が有効時のルータのパフォーマンス）。詳細については、「サイトとネットワークの計画」（P.2-4）を参照してください。
- データセンターやブランチ オフィスが複雑な場合は、適切な代行受信の位置を決定します（たとえば、既存のネットワークが階層的なトポロジを使用している場合）。
- どの WAAS サービスを展開するかを決定します（たとえば、Wide Area File Services（WAFS; 広域ファイル サービス）のサービス、WAAS 印刷サービス、および WAAS アプリケーション アクセラレーション）。さまざまな WAAS サービスの詳細については、第 1 章「Cisco WAAS の概要」を参照してください。
- インストールする WAAS ソフトウェア ライセンスを決定します。ソフトウェア ライセンスにより特定の WAAS サービスが有効になります。ソフトウェア ライセンスのインストールの詳細については、「ソフトウェア ライセンスの管理」（P.9-3）を参照してください。
- WAAS ネットワークでどのトラフィック代行受信方式を使用するかを決定します（たとえば、無差別モードには、インライン モード、Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）バージョン 2 または Policy-Based Routing（PBR; ポリシーベース ルーティング）、WAFS 専用トラフィックには NetBIOS）。詳細については、「サポートされるトラフィック リダイレクション方式」（P.2-18）を参照してください。

（注）　WCCP は、IPv4 ネットワークだけで動作します。

- トラフィック代行受信方式として TCP 無差別モード サービスを使用する計画の場合は、ルータで IP Access Control List（ACL; アクセス コントロール リスト）を使用する必要があるかどうかを決定します。

（注）　ルータで定義される IP ACL は、WAE で定義される ACL より優先します。詳細については、「ルータと WAE 上のアクセス リスト」（P.2-24）を参照してください。

- WAE で IP ACL または代行受信 ACL を定義する必要があるかどうかを決定します。詳細については、「ルータと WAE 上のアクセス リスト」（P.2-24）を参照してください。

（注）　WAE で定義される ACL は、WAE で定義される WAAS アプリケーション定義ポリシーより優先します。

- PBR を使用する場合は、WAE が使用できる次の PBR ホップを確認するためにどの PBR 方式を使用するかを決定します。詳細については、「PBR のネクストホップが使用できるかどうかを確認する方法」（P.4-40）を参照してください。
- WAAS ネットワークの主なアプリケーションを決定します。定義済みのアプリケーション定義ポリシーがこれらのアプリケーションも対象としているかどうかを確認します。対象としていない場合は、ポリシーを追加する必要があるかどうかを検討します。定義済みのアプリケーション定義ポリシーのリストについては、付録 A「定義済みのアプリケーション ポリシー」を参照してください。

- 印刷サービス設定を決定します。詳細については、第 13 章「WAAS レガシー印刷サービスの設定および管理」を参照してください。
- プロセスでファイル サーバを集中管理する場合は、ファイル システムの事前移行を検討します。詳細については、「データ移行プロセス」（P.2-28）を参照してください。
- サーバ、対象の WAFS ファイル サーバとして使用する WAFS ファイル サーバ、および希望するフィーチャ セット（たとえば、非接続モードやホーム ディレクトリ）を特定します。

計画作業を完了したら、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って WAAS ネットワークの基本的な設定を実行できます。

サイトとネットワークの計画

ネットワークに WAAS デバイスを設置して展開する前に、WAAS デバイスを統合するために必要なネットワークに関する情報を収集します。

典型的な分散組織レイアウトでは、WAAS デバイスを設置するネットワークには 2 つの種類があります。

- データセンター（セントラル オフィス）。このネットワークでは、同じ場所に配置された 1 台以上のデータセンターの WAE が、常駐ファイル サーバへのアクセスを提供します。データセンターでは、単体の WAE を配置したり、ハイ アベイラビリティやロード シェアリングのために 2 台 1 組の WAE を配置することができます。2 台 1 組の WAE 構成で、ハイ アベイラビリティは、データセンターでのトラフィック リダイレクション用に WCCP バージョン 2 または PBR を使用する場合にサポートされます。また、ロード シェアリングは、データセンターでのトラフィック リダイレクション用に WCCP バージョン 2 を使用する場合にだけサポートされます。
- ブランチ オフィス。このネットワークでは、ユーザがブランチ オフィスの WAE を使用して WAN 経由でファイル サーバにアクセスできます。ブランチ オフィスでは、単体のデバイスとして WAE を配置したり、ハイ アベイラビリティやロード シェアリング用に 2 台 1 組の WAE を配置することができます。2 台 1 組の WAE 構成で、ハイ アベイラビリティは、ブランチ オフィスでのトラフィック リダイレクション用に WCCP バージョン 2 または PBR を使用する場合にサポートされます。また、ロード シェアリングは、ブランチ オフィスでのトラフィック リダイレクション用に WCCP バージョン 2 を使用する場合にだけサポートされます。

コラボレーション ネットワークの場合は、同じ場所に配置したデータセンターの WAE とブランチ オフィスの WAE がネットワーク全体に展開されます。この場合、WAE は逆方向のデータを共有します（クロスリンク サーバが 2 台）。

WAE は、アプライアンスとして LAN に接続します。WAE は、パケット代行受信とリダイレクションを使用して、アプリケーション アクセラレーションと WAN 最適化を実現します。そのため、WAE を配置する各サイトでトラフィック代行受信と WAE へのリダイレクションを実行する必要があります。トラフィック代行受信とリダイレクションは、パケット フローの両方の方向で行われます。レイヤ 3 ヘッダーとレイヤ 4 ヘッダーが維持されるので、WAE とトラフィックを WAE にリダイレクトする WCCP または PBR 対応ルータの間でリダイレクションのループが発生しないように、ルータの第 3 のインターフェイス（またはサブインターフェイス）に WAE を接続する必要があります。この項目の詳細については、「第 3 のインターフェイスまたはサブインターフェイスを使用したルータと WAE の接続」（P.2-23）の手順を参照してください。

（注） WAE、ルータ、スイッチ、またはその他のデバイスでは半二重接続を使用しないことを強く推奨します。半二重接続の場合はパフォーマンスが低下するので、使用は避けてください。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を調べて、全二重接続が使用されていることを確認してください。

（注）　データセンターの WAE とブランチ オフィスの WAE は、ファイアウォールを使用する場合にだけ相互に通信します。Wide Area Files Services（WAFS; 広域ファイル サービス）をレガシー モードで展開する予定の場合、または directed モードを有効にする予定の場合、ポート 4050 を開くようにファイアウォールを設定する必要があります（directed モードの場合は UDP）。ただし、透過 CIFS アクセラレータを展開する予定の場合、または汎用 TCP 最適化だけを展開して directed モードは使用しない予定の場合、ポート 4050 を開くようにファイアウォールを設定する必要はありません。

ここでは、次の内容について説明します。

Windows ネットワークの統合

WAAS デバイスを Windows 環境に正しく統合するには、次の各項で説明するように、ネットワークのデータセンターの WAE 側とブランチ オフィスの WAE 側で準備を行う必要がある場合があります。ここでは、次の内容について説明します。

（注）　WAFS の統合が透過的でない場合は、WAAS デバイスはそのネットワークで Windows サーバの役割を果たさず、また Windows 環境でドメイン コントローラまたはマスター ブラウザとして機能しません。WAE ネットワーク内で、別の Windows マシンがそれらの役割を果たす必要があります。この注意点は、透過的な統合を使用する WCCP 環境や PBR 環境には無関係です。

データセンターの WAE の統合

データセンターの WAE を初期設定する前に、次のパラメータを知っている必要があります。

- WINS サーバ（該当する場合）
- DNS サーバと DNS ドメイン（該当する場合）
- ファイル サーバ ディレクトリ トラバース（読み取り専用）特権を持つブラウズするユーザ。一般にドメイン ユーザまたはサービス ユーザとしてセットアップされるこのユーザは、事前配置ポリシーを実行する必要があります。

DHCP を使用しないネットワークのデータセンターの WAE 側で Cisco WAAS を Windows 環境に正しく統合するには、データセンターの WAE の名前と IP アドレスを手動で DNS サーバに追加する必要があります。この作業は、WAAS デバイスを設置し、展開する前に行う必要があります。

（注）　ユーザのアクセス権は、既存のセキュリティ インフラストラクチャによって決定されます。

ブランチ オフィスの WAE の統合

ブランチ オフィスの WAE を初期設定する前に、次のパラメータを知っている必要があります。

- DNS サーバと DNS ドメイン
- Windows ドメイン名
- WINS サーバ（該当する場合）

ネットワークのブランチ オフィスの WAE 側で Windows 環境に Cisco WAAS を正しく統合するには、ネットワークに WAAS デバイスを設置し、展開する前に、次の予備的な作業を行う必要があります。

- 指定したドメイン内のすべてのブランチ オフィスの WAE が同じドメイン内のユーザのネットワーク ネイバーフッドに現れるようにするには、ドメインのマスター ブラウザまたはローカルのマスター ブラウザが有効になっていることを確認します。
- DHCP を使用しない場合は、ブランチ オフィスの WAE の名前と IP アドレスを手動で DNS サーバに追加する必要があります。

UNIX ネットワークの統合

WAAS デバイスを初期設定する前に、次のパラメータを知っている必要があります。

- DNS サーバと DNS ドメイン
- NIS サーバのパラメータ（該当する場合）
- データセンターの WAE 側で、ファイル サーバ ディレクトリ トラバース（読み取り専用）特権を持つブラウズする UID または GID。一般にドメイン ユーザまたはサービス ユーザとしてセットアップされるこの UID または GID は、一貫性ポリシーを定義するときにブラウズするために必要です。

Cisco WAAS を UNIX 環境に正しく統合するには、ネットワークのデータセンターの WAE 側とブランチ オフィスの WAE 側で次の作業を実行する必要があります。

- データセンターの WAE とブランチ オフィスの WAE の名前と IP アドレスを手動で DNS サーバに追加する必要があります。
- 別々のドメインを使用するときは、リモート オフィス（ブランチ オフィス）または中央のサーバで UNIX ユーザを定義できます。そのため、異なるドメインで同じユーザ名が定義される場合があります。ユーザは、ブランチ オフィスと中央で異なる定義にするか、片方だけで定義することができます。このような場合、NIS を使用するか、手動または自動で異なるドメイン間でマッピングして一貫性を保証できます。つまり、セントラル オフィスからリモート オフィスへユーザ ID を変換して、リモート サーバから中央のサーバへユーザをマップできます。

（注） 自動的な管理を使用してユーザをマップするには、最初にデータセンターの WAE（プライマリ）とブランチ オフィスの WAE（セカンダリ）で NIS サーバを構成する必要があります。

WAAS 環境で使用する WAFS 関連ポート

ここでは、クライアント、ファイル エンジンとして機能する WAE、および CIFS ファイル サーバ間で使用する Wide Area File Services（WAFS; 広域ファイル サービス）関連ポートについて説明します。WAFS 通信の大半は、ブランチ オフィスとセントラル オフィスの間で発生します。この通信は暗号化され、組織の VPN 経由で配信されます。すべての通信が内部的にトンネルされるため、ファイアウォールのポートを開放する必要がありません。

組織外部から管理作業や他の保守作業を行う必要がある場合にだけ、ファイアウォールの設定を変更する必要があります。

ポート 4050

Core WAE ゲートウェイと Edge WAE キャッシュ間の通信は、従来の WAFS 機能によって TCP/IP ポート 4050 経由で行われます。透過 CIFS アクセラレータを有効にすると、ポート 4050 は CIFS には使用されません。

ポート 139 およびポート 445

WAAS ネットワークに WAFS サービスだけを展開した場合、WAAS ネットワークは、ポート 139 とポート 445 を使用して、クライアントをブランチ オフィスの WAE に接続し、データセンターの WAE を関連するファイル サーバに接続します。使用するポートは、WAAS ネットワークの構成に依存します。

WCCP が有効であるか、またはインライン モードが使用されている場合、ブランチ オフィスの WAE はポート 139 または 445 でクライアント接続を受け入れます。WCCP がインライン モードでも有効でもない場合は、ブランチ オフィスの WAE はポート 139 でだけ接続を受け入れます。

WAAS ネットワークは、エンドツーエンドの通信に常に同じポートの使用を試みます。そのため、クライアントがポート 445 を使用してブランチ オフィスの WAE に接続する場合、関連するデータセンターの WAE は、同じポートを使用してファイル サーバとの接続を試みます。ポート 445 を使用できない場合、データセンターの WAE は、ポート 139 の使用を試みます。

一部の企業によっては、ポート 139 に関連するセキュリティ リスクを最小限に抑えるために、ポート 139 を閉じている所もあります。セキュリティ上の理由からポート 139 を閉じた場合、ポート 139 をバイパスするように WAAS ネットワークを設定できます。この場合、WAAS ネットワークに WAFS サービスだけを展開している場合は、次の手順を実行してポート 139 をバイパスし、ポート 445 を代用することができます。

- 『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、ルータとブランチ オフィスの WAE で WCCP バージョン 2 を有効にします。代わりに、Cisco WAE Inline Network Adapter がインストールされたブランチ オフィスの WAE でインライン モードを使用することもできます。

ポート 88 およびポート 464

Kerberos が有効になっており Windows ドメイン認証を使用している場合、WAE は、ポート 88 とポート 464 を使用してドメイン コントローラへクライアントを認証します。

ポート 50139

WAAS 印刷サービスを設定している場合、プリント サーバはポート 50139 で動作します。WAAS 印刷サービスの設定の詳細については、第 13 章「WAAS レガシー印刷サービスの設定および管理」を参照してください。

ファイアウォールと Directed モード

デフォルトでは、WAAS はピア WAE との新規 TCP 接続を透過的に設定します。これにより、WAAS デバイスがトラフィックを最適化しようとする際、ファイアウォール トラバースに関する問題が発生することがあります。WAE デバイスがトラフィックの最適化を阻止するファイアウォールの背後にあ

る場合、ピア WAE への通信に directed モードを使用できます。directed モードでは、ピア WAE に送信されるすべての TCP トラフィックは UDP にカプセル化されるため、ファイアウォールはトラフィックをバイパスするか、トラフィックを検査できます（UDP 検査ルールを追加して）。

2 つの WAE ピア間のすべてのファイアウォールを、ポート 4050 で、またはデフォルト以外のポートが使用されている場合は directed モードに設定されているすべてのカスタム ポートで、UDP トラフィックを通過させるように設定する必要があります。

Directed モードを使用する WAE が NAT デバイスの背後にある場合、WAE で NAT IP アドレスを設定する必要があります。

Directed モードの設定の詳細については、「directed モードの設定」（P.5-16）を参照してください。

ファイアウォールとスタンバイ Central Manager

プライマリ Central Manager とスタンバイ Central Manager は、ポート 8443 で通信します。ネットワークでプライマリ Central Manager とスタンバイ Central Manager との間にファイアウォールが存在する場合、ポート 8443 上のトラフィックを許可するようにファイアウォールを設定して、Central Manager 同士が通信を行い、同期を維持できるようにします。

自動登録と WAE について

自動登録は、自動的にネットワーク設定を構成し、WAAS Central Manager デバイスに WAE を登録します。起動時、WAAS ソフトウェアを実行するデバイス（WAAS Central Manager デバイスを除く）は、自動的に WAAS Central Manager デバイスを検出し、登録します。手動でデバイスを構成する必要はありません。この機能は、デバイスの大規模な自動展開を行う場合に便利です。WAE が登録されたら、WAAS Central Manager GUI を使用してリモートにデバイスを構成します。

『*Cisco Wide Area Application Services Quick Configuration Guide*』に示す構成例では、自動登録機能は WAE で無効になっており、設定ユーティリティを使用してデバイスの初期設定を実行します。

自動登録は、Dynamic Host Configuration Protocol（DHCP）を使用します。自動登録が機能するには、WAAS Central Manager のホスト名付きで構成され、ベンダー クラス オプション 43 を処理できる DHCP サーバが必要です。

（注）　自動登録に使用する DHCP の形式は、**ip address dhcp** インターフェイス コンフィギュレーション コマンドを使用して設定できるインターフェイス レベルの DHCP と同一では*ありません*（**ip address dhcp** インターフェイス コンフィギュレーション コマンドの説明については、『*Cisco Wide Area Application Services Command Reference*』を参照してください）。

ベンダー クラス オプション（オプション 43）情報は、RFC 2132 の規定に従って、カプセル化したベンダー固有オプションの形式で WAAS デバイスに送信する必要があります。RFC 2132 の関連するセクション「Section 8.4」の内容を次に示します。

> カプセル化したベンダー固有オプション フィールドは、DHCP オプション フィールドの構文と同一の構文でコード/長さ/値フィールドのシーケンスとして符号化する必要があります。ただし、次のような違いがあります。
>
> **a.** カプセル化したベンダー固有拡張フィールドには、「magic cookie」フィールドがあってはなりません。
>
> **b.** カプセル化したベンダー固有拡張フィールドでは、ベンダーが 0 または 255 以外のコードを再定義できます。ただし、第 2 節に規定されている「タグ - 長さ - 値」の構文に従う必要があります。

c. コード 255（END）は、存在する場合、ベンダー拡張フィールドの終了でなく、カプセル化したベンダー拡張フィールドの終了を表します。コード 255 が存在しない場合は、取り囲むベンダー固有情報フィールドの終了が、カプセル化したベンダー固有拡張フィールドの終了を表します。

DHCP サーバは、RFC 規格に従って、コード/長さ/値（コードと長さは 1 オクテット）の形式で WAAS Central Manager のホスト名情報を送信する必要があります。WAAS Central Manager のホスト名のコードは 0x01 です。DHCP サーバの管理と設定は、自動登録機能の対象ではありません。

（注）　WAE は、WAE をデバイス グループにまとめやすいように、オプション 60 のベンダー クラス ID として「CISCOCDN」を送信します。

また、DHCP サーバの提示が有効であると見なされるために、自動登録 DHCP に次のオプションも存在する必要があります。

- サブネット マスク（オプション 1）
- ルータ（オプション 3）
- ドメイン名（オプション 15）
- ドメイン名サーバ（オプション 6）
- ホスト名（オプション 12）

これに対し、インターフェイス レベルの DHCP では、提示が有効であると見なされるために、サブネット マスク（オプション 1）とルータ（オプション 3）だけが必要です。ドメイン名（オプション 15）、ドメイン名サーバ（オプション 6）、およびホスト名（オプション 12）はオプションです。ドメイン名サーバ（オプション 6）を除く上記のすべてのオプションが、システムの既存の設定を変更します。ドメイン名サーバ オプションは、既存のネーム サーバのリストに追加されます。ただし、ネーム サーバの個数は最大 8 個です。

デバイスの最初のインターフェイスでは、自動登録は、デフォルトで有効です。WAAS アプライアンスの場合、最初のインターフェイスは GigabitEthernet 1/0 です。NME-WAE モジュールでは、自動登録は設定したインターフェイス上で有効です。SM-SRE モジュールでは、自動登録はデフォルトでは無効になっています。

（注）　両方のデバイス インターフェイスがポートチャネル インターフェイスとして設定されている場合は、自動登録を無効にする必要があります。

DHCP サーバがない場合、デバイスは自動登録を完了できず、最終的にタイムアウトします。デバイスを起動し、手動での設定と登録を行ったあとで、自動登録を無効にすることができます。

自動登録を無効にする、または別のインターフェイスの自動登録を設定するには、グローバル コンフィギュレーション モードで **no auto-register enable** コマンドを使用します。

（注）　固定 IP アドレスが設定されている場合、またはインターフェイス レベルの DHCP が自動登録と同じインターフェイスで設定されている場合、自動登録は自動的に無効になります（「スタティック IP アドレスの選択または Interface-Level DHCP の使用」（P.2-10）を参照）。

次の例は、インターフェイス GigabitEthernet 1/0 の自動登録を無効にします。

```
WAE(config)# no auto-register enable GigabitEthernet 1/0
```

自動登録のステータスは、次の **show** EXEC コマンドを使用して取得できます。

```
WAE# show status auto-register
```

スタティック IP アドレスの選択または Interface-Level DHCP の使用

初期設定中、デバイス用の固定 IP アドレスを設定するか、DHCP を選択することができます。

DHCP は、ネットワーク管理者がネットワークを集中管理し、組織のネットワークでの IP アドレスの割り当てを自動化できる通信プロトコルです。組織がネットワークと接続できるようにコンピュータユーザをセットアップする場合、各デバイスに IP アドレスを割り当てる必要があります。DHCP を使用しない場合、各コンピュータの IP アドレスを手動で入力する必要があり、コンピュータをネットワークの別の部分にある別の場所に移動したときは、それに応じて IP アドレスを変更する必要があります。DHCP は、コンピュータをネットワークの別のサイトに接続すると、自動的に新しい IP アドレスを送信します。

構成済みの DHCP サーバがある場合、自動登録は、起動時に自動的にネットワーク設定を構成し、WAE を WAAS Central Manager デバイスに登録します。

構成済みの DHCP サーバがない場合、または DCHP サーバはあるが自動登録機能を使用したくない場合は、自動登録を無効にし、対話型設定ユーティリティまたは CLI を使用して手動で次のネットワーク設定を構成し、WAAS Central Manager デバイスに WAE を登録します。次の設定を構成します。

- イーサネット インターフェイス
- IP ドメイン名
- ホスト名
- IP ネーム サーバ
- デフォルト ゲートウェイ
- プライマリ インターフェイス

WAAS デバイスを起動すると、初回設定ユーティリティを起動し、基本設定を入力するためのプロンプトが表示されます。初回設定ユーティリティを使用して、WAE 用の基本的なデバイス ネットワーク設定をセットアップします。

相互運用性に関する問題の特定と解決

ここでは、相互運用性に関する問題を特定して解決する方法について説明します。内容は次のとおりです。

相互運用性とサポート

表 2-1 に、WAAS ソフトウェアがサポートするハードウェア、クライアント、およびブラウザを示します。

表 2-1　ハードウェア、クライアント、ブラウザのサポート

ハードウェアのサポート	特定の Cisco ルータにインストールされている WAE-512、WAE-612、WAE-674、WAE-7326、WAE-7341、WAE-7371、WAVE-274、WAVE-474、および WAVE-574 アプライアンス、または NME-WAE、SM-SRE-700、または SM-SRE-900 ネットワーク モジュール。専用のデバイスに WAAS Central Manager を展開する必要があります。
クライアントのサポート	ブランチ オフィスの WAE で動作する WAAS ソフトウェアは、次の CIFS クライアントと相互動作します：Windows 98/NT 4.0/2000/XP/7 および Windows Server 2003/2008 R2。
ブラウザのサポート	WAAS GUI は、Internet Explorer 5.5 以降を実行する必要があります。

ここでは、次の内容について説明します。

- 「WAAS GUI インターフェイス用の Unicode のサポート」
- 「Unicode サポートの制限事項」

WAAS GUI インターフェイス用の Unicode のサポート

WAAS ソフトウェアは、WAAS Central Manager と WAE Device Manager GUI インターフェイスで Unicode をサポートしています。

WAAS Central Manager では、Unicode 文字を含む事前配置ポリシーを作成できます。たとえば、名前に Unicode 文字を含むディレクトリ用の事前配置ポリシーを定義することができます。

具体的には、WAAS Central Manager GUI の次のフィールドが Unicode をサポートしています。

- 事前配置ポリシーのルート ディレクトリ フィールドとファイル パターン フィールド

WAE Device Manager GUI では、バックアップ設定ファイルの名前に Unicode 文字を入れることができます。さらに、WAE Device Manager GUI に付属しているログは、Unicode 文字を表示できます。

Unicode サポートの制限事項

Unicode のサポートには、次のような制限があります。

- ユーザ名には Unicode 文字を入れることができません。
- 一貫性などのポリシーを定義する場合、[Description] フィールドに Unicode 文字を使用できません。
- ファイル サーバ名 には Unicode 文字を入れることができません。

WAAS と Cisco IOS の相互運用性

ここでは、WCCP に基づく代行受信と透過転送を使用する基本的な WAAS 配備での WAAS ソフトウェアと Cisco IOS 機能の相互運用性について説明します。内容は、次のとおりです。

- 「WAAS による Cisco IOS トラフィック ポリシングと速度制限のサポート」（P.2-14）
- 「WAAS による Cisco IOS シグナリングのサポート」（P.2-14）
- 「WAAS による Cisco IOS リンク効率動作のサポート」（P.2-14）
- 「WAAS による Cisco IOS プロビジョニング、モニタリング、および管理のサポート」（P.2-14）
- 「WAAS と管理装置」（P.2-14）
- 「WAAS と MPLS」（P.2-15）

（注）　WAAS ソフトウェアは、Cisco IOS IP v6 とモバイル IP をサポートしていません。

Cisco IOS ソフトウェア Release 12.2 以降を使用することを推奨します。

WAAS による Cisco IOS QoS 分類機能のサポート

パケットは、パケットに定義されているポリシー フィルタを使用して（たとえば、QPM を使用して）分類できます。次のポリシー フィルタ プロパティを使用できます。

- 送信元 IP アドレスまたはホスト名：WAAS デバイスが送信元 IP アドレスを維持するため、WAAS でサポートされます。
- 送信元 TCP/UDP ポート（またはポート範囲）：WAAS デバイスが送信元ポートを維持するため、WAAS でサポートされます。
- 送信先 IP アドレスまたはホスト名：WAAS が送信先 IP を維持するため、WAAS でサポートされます。WAAS は、データセンターでの代行受信を使用して、ピア WAAS デバイスへトラフィックをリダイレクトします。
- 送信先 TCP/UDP ポート（またはポート範囲）：WAAS が送信先 IP を維持するため、WAAS でサポートされます。WAAS は、データセンターでの代行受信を使用して、ピア WAAS デバイスへトラフィックをリダイレクトします。
- DSCP/IP 優先（TOS）：WAAS が WAAS からルータへ返信される発信パケットに着信パケットの設定値をコピーするため、WAAS でサポートされます。WAAS は定期的に設定値のポールを実行しないため、接続確立時にパケットが（TCP パケット用に）色付けされない場合、設定値の伝達が遅れる場合があります。パケットは、最終的に正しく色付けされます。パケットが色付けされていない場合、WAAS ソフトウェアは色付けしません。

WAAS ソフトウェアは、IPv6 QoS、MPLS QoS、ATM QoS、フレームリレー QoS、およびレイヤ 2（VLAN）QoS をサポートしていません。

WAAS による Cisco IOS NBAR 機能のサポート

「WAAS による Cisco IOS QoS 分類機能のサポート」（P.2-12）に記載されているポリシー フィルタを使用して指定される従来のタイプの分類とは異なり、Network-Based Application Recognition（NBAR）分類ではペイロードを考慮する必要があります。ペイロードの変更により NBAR がパケットを分類できなくなる場合があるため、分類はペイロードを変更する代行受信者を追跡します。ただし、WAAS ソフトウェアは、NBAR をサポートしています。

次の例は、WAAS ソフトウェアが NBAR をサポートするフローを示しています。

1. TCP ストリーム S1 の一部であるパケット P1 がルータに入り、ルータの LAN インターフェイスで NBAR によってクラス C1 に属すると分類されます。P1 の分類がペイロード検査を含まない場合（たとえば、TCP/IP ヘッダーだけの場合）、WAAS ソフトウェアがこの情報を維持するため、処理は不要です。

2. P1 分類にペイロード検査が必要な場合、（他の内部マーキングメカニズムを使用する場合と異なり）パケットの TOS/DSCP ビットを使用して P1 にマークを付ける必要があります。
3. 次に、P1 が WCCP バージョン 2 を通じて代行受信され（やはり、LAN インターフェイスで、WCCP は NBAR のあとに処理されます）、WAE へリダイレクトされます。
4. WAAS は、ペイロードに最適化を適用し、着信 TCP ストリーム S1 から発信ストリーム S2 に DCSP ビット設定をコピーします（発信ストリーム S2 は、ローカル WAAS アプライアンスとリモート WAAS アプライアンス間で WAN 経由で確立されます）。一般に NBAR は分類を実行する前にペイロードを確認する必要があるため、WAAS が接続確立時に正しいビット設定を持つことはほとんどありません。そのため、WAAS ソフトウェアは、ポーリングを使用して、着信 TCP ストリームの DSCP ビットを検査し、WAAS デバイスからルータへ返信されるストリームにコピーします。
5. S2 がルータに再び入るとき、ペイロードが変更または圧縮されているため、NBAR は S2 を C1 に属すると分類しません。ただし、DSCP 設定が、すでにこれらのパケットに C1 に属するというマークを付けています。そのため、これらのパケットは、NBAR が分類したかのように正しく処理されます。

   フローが識別されないかぎり、NBAR は、パケットで分類を検索し続けます。圧縮されたパケットは分類されないため、パケット検査を実行する CPU に必要以上に負担がかかる場合があります。パフォーマンスが低下し、正確さが疑わしくなる可能性があるため、（「第 3 のインターフェイスまたはサブインターフェイスを使用したルータと WAE の接続」（P.2-23）の説明に従って）サブインターフェイスまたは別の物理インターフェイスを使用して、WAE をルータに接続することを強く推奨します。第 3 のインターフェイスまたはサブインターフェイスを使用して WAE をルータに接続すると、各パケットは一度だけ処理されるため、パフォーマンスと正確性の問題が解決されます。
6. 動的な分類のため、NBAR はフローごとに状態を維持します。特定のフローが分類されると、NBAR は詳細なパケット検査を停止します。ただし、他のフロー（たとえば、Citrix）については、分類がフローの中で動的に変化する場合があるため、NBAR はパケット検査を継続します。したがって、すべての NBAR 分類をサポートするには、WAAS への着信パケットの DSCP 設定をフロー当たり 1 回ポーリングするだけでは十分でなく、フローの変化を特定するために定期的にポーリングする必要があります。ただし、WAAS システムは、パケットがクラス C1 に属するパケットのシーケンス、C2 のシーケンスなどのように現れることを期待するため、このような動的な変化を追跡するにはポーリング方式で十分です。

（注） この動的な分類をサポートするには、「WAAS による Cisco IOS QoS 分類機能のサポート」（P.2-12）に記載されている DSCP/ToS 設定マーキングと、ポーリングによる動的な変化の追跡のサポートが必要です。

NBAR-WAAS 準拠性を保証するためにいくつかのルータ構成に従う必要があり、次のルータ構成に準拠していることを確認する必要があります。

- 分類が正しい DSCP マーキングに従っていることを確認します。
- 一般にルータ（ルータに設定されている IP アクセス リスト）が着信時にすでにパケットにマークされている DSCP/TOS 設定に抵触せず、NBAR がパケットのマークを削除しないことを確認します。

WAAS による Cisco IOS マーキングのサポート

WAAS ソフトウェアは、Cisco IOS マーキング機能をサポートしています。

WAAS による Cisco IOS キューイングのサポート

WAAS ソフトウェアは、輻輳を管理するために Cisco IOS キューイング機能をサポートしています。

WAAS による Cisco IOS 輻輳回避のサポート

WAAS ソフトウェアは、Cisco IOS 輻輳回避機能をサポートしています。

WAAS による Cisco IOS トラフィック ポリシングと速度制限のサポート

WAAS ソフトウェアは、Cisco IOS トラフィック ポリシングと速度制限機能を部分的にサポートしています。この Cisco IOS 機能は、発信インターフェイスで有効になっている場合、正しく動作します。ただし、この機能を着信インターフェイスで有効にすると、圧縮されているトラフィックと圧縮されていないトラフィックの両方が検査されるため、速度制限が不正確になります。

WAAS による Cisco IOS シグナリングのサポート

一般に、Cisco IOS シグナリング（RSVP）機能は、MPLS ネットワークに実装されます。WAAS ソフトウェアは MPLS RSVP メッセージと対話しないため、RSVP 機能はサポートされます。

WAAS による Cisco IOS リンク効率動作のサポート

WAAS ソフトウェアは、Cisco IOS リンク効率動作をサポートしています。

WAAS による Cisco IOS プロビジョニング、モニタリング、および管理のサポート

WAAS ソフトウェアは Cisco IOS AutoQoS 機能をサポートしていますが、追加設定が必要です。AutoQoS 機能は NBAR を使用してネットワーク上のさまざまなフローを発見するため、この機能は NBAR サポートと密接に関係しています。ただし、Cisco IOS AutoQoS 機能は厳密に発信機能（たとえば、インターフェイスの着信側では有効にできない）であり、発信インターフェイスでの NBAR の有効化はサポートされていないため、この状況は潜在的な問題になる場合があります。

この潜在的な問題を防止するには、分類とキューイングがマークされた値に基づいて実行されるように、次のインターフェイスで AutoQoS 機能の信用オプションを有効にします（NBAR は、このソリューションを使用する発信インターフェイスでは有効になっていません）。

- 入力ポリシーが作成され、パケットのマーキングが AutoQoS マーキングに従って実行される（たとえば、対話型ビデオ マークから af41 へ）必要がある LAN インターフェイス
- WAN 発信インターフェイス

WAAS と管理装置

WAAS ソフトウェアとともに管理装置を使用する場合は、次の事項に注意してください。

- ネイティブ（透過）モードで配置された場合、NetFlow などのテクノロジーに不可欠なパケット ヘッダー情報が WAAS によって維持されます。NetFlow は、隣接デバイス上で設定でき、WAAS デバイスに対する NetFlow の設定場所に応じたフロー レコード情報をエクスポートします。NetFlow が WAAS デバイスの LAN 側で設定された場合、元のフローに関する情報の入ったレコードが NetFlow によってエクスポートされます。NetFlow が WAAS デバイスの WAN 側で設定された場合、最適化されたパススルー フローに関する情報の入ったレコードが NetFlow によってエクスポートされます。
- 最適化されたトラフィックと最適化されていないトラフィックに関する統計情報を表示できます。
- IP Service Level Agreement（SLA; サービス レベル契約）はサポートされています。

- レイヤ 3 とレイヤ 4 に基づくポリシーは、完全にサポートされています。レイヤ 7 に基づくポリシーは、最初の少数のメッセージが最適化されていないため、部分的にサポートされています。
- Intrusion Detection System（IDS; 侵入検知システム）は、部分的にサポートされています。IDS が侵入文字列を検出できるように、最初の少数のメッセージは最適化されません。
- Cisco IOS セキュリティは、レイヤ 5 以上の参照可能性に依存する機能を除き、部分的にサポートされています。
- IP セキュリティと SSL VPN はサポートされています。
- ACL はサポートされています。ルータ上の IP ACL は、WAE で定義されている ACL より優先します。詳細については、「ルータと WAE 上のアクセス リスト」（P.2-24）を参照してください。
- WCCP 代行受信のあとで VPN が展開される場合、VPN はサポートされます。

（注）　WAAS デバイスは、WAN トラフィックを暗号化しません。追加的なセキュリティ対策が必要な場合は、VPN を使用する必要があります。ただし、VPN アプライアンスは、WAAS デバイスが暗号化されていないトラフィックだけを見るように、WAAS デバイスのあとでトラフィックを暗号化し、WAAS デバイスの前で複号化する必要があります。WAAS デバイスは、暗号化されたトラフィック圧縮できず、限られた TCP 最適化だけを提供します。

- Network Address Translation（NAT; ネットワーク アドレス変換）はサポートされています。ただし、ペイロードに基づく NAT はサポートされません。

WAAS と MPLS

WAAS ソフトウェアは、MPLS を部分的にサポートしています。WCCP は、MPLS ラベルが付いているパケットを処理する方法を知りません。そのため、WCCP リダイレクションは、クラウドの内側で機能しません（たとえば、WCCP リダイレクションは、中間の WAE では動作しません）。ただし、MPLS のクラウドの外にあるインターフェイスでリダイレクションが行われる場合、WAAS はサポートされます。

他の Cisco アプライアンスやソフトウェアとの WAAS の互換性

ファイアウォールがクライアントと WAE の片側の間に配置され、ルータがファイアウォールの反対側に配置される場合、デフォルト WCCP リダイレクションは動作しません。ただし、ファイアウォールの内側に 1 台のルータがあり、ファイアウォールの外部に別のルータがある場合、デフォルト WCCP に基づくリダイレクションは動作し、WAAS はサポートされます。ファイアウォール トラバースに関する問題を回避するために、directed モードを有効にすることもできます。詳細については、「directed モードの設定」（P.5-16）を参照してください。

ネットワークでの ACNS デバイスと WAAS デバイスの連結は、サポートされています。ACNS デバイスは、Web プロトコルを最適化し、Web コンテンツをローカルに処理できます。WAAS デバイスは、コンテンツ エンジンからの要求を最適化します。このコンテンツ エンジンが、上流のサーバまたは上流のコンテンツ エンジンからサービスを提供される必要がある ACNS デバイスです。ネットワークで ACNS デバイスと WAAS デバイスを連結すると、次の利点があります。

- ACNS がすでにネットワークに展開されている場合、WAAS も配備できます。
- ACNS がネットワークに展開されていないが、特定の ACNS 機能が必要な場合、ACNS を購入して WAAS とともに展開することができます。

WAAS デバイスとデバイス モード

専用のアプライアンスに WAAS Central Manager を展開する必要があります。WAAS Central Manager デバイスは WAAS ソフトウェアを実行しますが、その唯一の目的は管理機能を提供することです。WAAS Central Manager は、ネットワークで WAAS Central Manager に登録されている WAE と通信します。WAAS Central Manager GUI を使用して、WAE の設定を個別またはグループで集中管理できます。また、WAAS Central Manager は、登録された WAE 用の管理統計情報を収集してログに記録します。

WAE は WAAS ソフトウェアも実行しますが、その役割は WAAS ネットワークでアクセラレータとして機能することです。

WAAS ネットワークでは、次のいずれかのデバイス モードで WAAS デバイスを展開する必要があります。

- WAAS Central Manager モード : WAAS Central Manager デバイスが使用する必要があるモード
- WAAS アプリケーション アクセラレータ モード : WAAS ソフトウェアを実行するデータセンターの WAE およびブランチ オフィスの WAE である WAAS アクセラレータ用のモード

WAAS デバイスのデフォルトのデバイス モードは、WAAS アクセラレータ モードです。**device mode** グローバル コンフィギュレーション コマンドを使用すると、WAAS デバイスのデバイス モードを変更できます。

```
waas-cm(config)# device mode ?
  application-accelerator  Configure device to function as a WAAS Engine.
  central-manager          Configure device to function as a WAAS Central Manager.
```

たとえば、WAAS CLI を使用して、指定した WAAS Central Manager（waas-cm という名前の WAAS デバイス）用の基本的なネットワーク パラメータを指定し、それにプライマリ インターフェイスに割り当てると、**device mode** コンフィギュレーション コマンドを使用して中央マネージャとしてデバイス モードを指定できます。

```
waas-cm# configure
waas-cm(config)#
waas-cm(config)# primary-interface gigabitEthernet 1/0
waas-cm(config)# device mode central-manager
waas-cm(config)# exit
waas-cm# copy run start
waas-cm# reload
Proceed with reload?[confirm] y
Shutting down all services, will Reload requested by CLI@ttyS0.
Restarting system.
```

WAAS デバイスを初期設定する方法の詳細については、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。

（注） WAE ネットワーク モジュール（NME-WAE または SM-SRE ファミリのデバイス）を WAAS Central Manager モードで稼動するように設定することはできません。

Cisco WAE Inline Network Adapter のある WAE は、WAAS Central Manager モードで動作するように設定できますが、インライン代行受信機能は有効ではありません。

必要な WAAS デバイスの台数の計算

動作システムのしきい値を超えると、Cisco WAAS は期待されるサービス レベルに適合しない場合があります。そのため、パフォーマンスが低下する場合があります。

この制約の原因は、特定の Cisco WAAS デバイス（WAAS Central Manager、ブランチ オフィスの WAE、またはデータセンターの WAE）、Cisco WAAS システム全体、ハードウェアの制約、または分散したソフトウェア集合を接続するネットワークなどがあります。リソースを追加するか、ハードウェアやソフトウェアをアップグレードすると、制約を解決できる場合があります。

ネットワークを計画するときは、サポートする必要があるユーザ数、サポートする必要があるファイル数、およびキャッシュする必要があるデータ量のような動作容量を考慮してください。

また、WAAS ネットワークを計画するときは、次の補足的なガイドラインを参照してください。

- WAAS Central Manager の数：すべてのネットワークに、少なくとも 1 つの WAAS Central Manager が必要です。大型ネットワークの場合は、アクティブとスタンバイのバックアップ、ハイ アベイラビリティ、およびフェールオーバー用に 2 つの WAAS Central Manager を展開することを検討する必要があります。WAAS Central Manager は、専用のアプライアンスで展開します。
- WAE の台数：フローを最適化するために、ネットワークの両側に 1 台ずつの少なくとも 2 台の WAE が必要です（たとえば、ブランチ オフィスに 1 台、データセンターに 1 台）。冗長性を実現するために、1 つのサイトに複数の WAE を配置できます。
- ブランチ オフィスの WAE の台数：各リモートのオフィスに、少なくとも 1 台のブランチ オフィスの WAE が必要です。一般に、大型オフィスには複数の部門があり、ユーザはセントラル オフィスの異なるサーバを使用します。この場合、組織構造に従って各部門に 1 台のブランチ オフィスの WAE を配置すると、システム管理が簡単になります。特定の状況下では、WCCP バージョン 2 を使用して、複数のブランチ オフィス WAE をクラスタ化および設定し、フェールオーバー機能を提供することができます。ユーザ数が多い場合は、WCCP バージョン 2 を推奨します。
- データセンターの WAE の台数：各組織に少なくとも 1 台のデータセンターの WAE が必要です。

組織に必要な各コンポーネントの台数を決定するときは、次の要因を検討してください。

- システムに接続するユーザ数：システムの固定容量と動的容量に依存します。
  - 固定容量：容量に達する前にシステムに接続できるユーザ セッションの数を定義します。
  - 動的容量：サーバが処理するトラフィックの量（ネットワークで実行される作業の量）を定義します。たとえば、現在システムに接続しているユーザによるシステムの負荷を考慮してください。

（注） 動的容量は、各ユーザに固有の具体的な負荷の仮定に基づいて計算する必要があります。

- データセンターの WAE 経由でファイル サーバに接続する全ブランチ オフィスのユーザの総数：ユーザの数が 1 台のデータセンターの WAE がサポートできるユーザ数を超える場合は、1 台または複数の追加のデータセンターの WAE をネットワークに追加する必要があります。

  システム制限によるデータ損失を防止するために、WAAS は、レガシー WAFS 機能向けの Core WAE クラスタをサポートしています。この定義された Core WAE のグループは、次の目的で使用されます。

  - システム容量の拡張性の強化
  - 冗長性の実現

  WAFS の透過的 CIFS アクセラレータを使用する場合は、機能が停止しても WAAS システムが自動的に他の WAE 経由で要求をルーティングするため、Core WAE クラスタは必要ありません。

サポートされるトラフィック リダイレクション方式

WAAS ネットワークでは、最適化、冗長性の除去、および圧縮のために、ブランチ オフィスのクライアントとデータセンターのサーバ間のトラフィックを WAE にリダイレクトできます。トラフィックは、ルータに設定されているポリシーに基づいて代行受信され、WAE へリダイレクトされます。要求をローカル WAE に透過的にリダイレクトするネットワーク要素に WCCP バージョン 2 または PBR を使用するルータを使用すれば、トラフィックをローカル WAE またはレイヤ 4 ～ レイヤ 7 のスイッチ（たとえば、Catalyst 6500 シリーズの Content Switching Module（CSM）または Application Control Engine（ACE））に透過的にリダイレクトできます。

代わりに、Cisco WAE Inline Network Adapter がインストールされた WAE は、インライン モードで動作でき、ルータを通過する前にトラフィックを直接受信したり最適化することができます。

ここでは、次の内容について説明します。

WAAS ネットワーク用のトラフィック代行受信を設定する方法の詳細については、第 4 章「トラフィック代行受信の設定」を参照してください。

インライン代行受信を使用する長所と短所

インライン代行受信は、Cisco WAE Inline Network Adapter がインストールされた WAE アプライアンスの使用を必要とします。インライン モードでは、WAE は、物理的に透過的にトラフィックをクライアントとルータの間で代行受信できます。このモードを使用した場合、WAE デバイスを最適化するトラフィックのパスに物理的に配置します。通常は、スイッチとルータの間です。

トラフィックのリダイレクションが不要なため、トラフィックのインライン代行受信は、構成を簡素化し、ルータでの WCCP または PBR の設定の複雑さを軽減します。

Cisco WAE Inline Network Adapter には LAN/WAN イーサネット ポートの 1 つまたは 2 つのペアがあります。アダプタにポートの 2 つのペアがある場合、ネットワーク トポロジで必要であれば 2 つのルータに接続できます。さらに、一部の WAE モジュールには、2 つの Cisco WAE Inline Network Adapter をインストールできます。

Cisco WAE Inline Network Adapter は、トラフィックを透過的に代行受信し、最適化の必要のないトラフィックをブリッジングします。電源、ハードウェア、修復不可能なソフトウェア障害が発生した場合に自動的にトラフィックをブリッジングする、フェールセーフ機構の設計も使用します。

ある VLAN からのトラフィックだけを受信し、他のすべての VLAN のトラフィックはブリッジングされて処理されないように、Cisco WAE Inline Network Adapter を設定できます。

デバイスの故障に備えてアベイラビリティを高めるために、Cisco WAE Inline Network Adapter が搭載された WAE デバイスを連続的にクラスタ化できます。現在最適化を行っているデバイスが故障すると、クラスタ内の 2 つめの WAE が最適化サービスを提供します。スケーリングまたはロード バランシングのために WAE デバイスをシリアル インライン クラスタに配置することは、サポートされていません。

ピア WAE 上でのトラフィック代行受信メカニズムの任意の組み合わせがサポートされています。たとえば、インライン代行受信を、データセンター WAE 上のブランチ オフィス WAE と WCCP で使用できます。複雑なデータセンターの構成に対して、ハードウェアが加速化された WCCP 代行受信または Cisco Application Control Engine（ACE）でのロード バランシングの使用を推奨します。

インライン代行受信の詳細については、「TCP トラフィックの透過的な代行受信へのインライン モードの使用」（P.4-43）を参照してください。

次の 3 つの要素を一緒に使用すると、WCCP ベースのアプローチを使用しなくても、データ センターでのトラフィックの代行受信が容易に行えるようになります。

- 特定の WAE モデルでサポートされるデュアル インライン Cisco WAE Inline Network Adapter。4 つのインライン グループで、合計 8 つのポートを提供します。
- ハイ アベイラビリティをサポートするための 2 つの WAE でのシリアル インライン クラスタリング。
- どのトラフィックを代行受信し、どのトラフィックを通過させるのかを制御する代行受信 ACL。代行受信 ACL の詳細については、「代行受信アクセス コントロール リストの設定」（P.4-29）を参照してください。

WCCP に基づくルーティングを使用する長所と短所

WCCP は、1 台または複数のルータ（またはレイヤ 3 スイッチ）および 1 台または複数のアプリケーション アプライアンス、Web キャッシュ、および他のアプリケーション プロトコルのキャッシュ間の通信を規定しています。通信の目的は、ルータのグループを通過する選択した種類のトラフィックの透過的なリダイレクションを確立し、維持することです。選択したトラフィックは、アプライアンスのグループへリダイレクトされます。

WCCP では、クライアント要求を処理するために WAE へ透過的にリダイレクトすることができます。WAAS ソフトウェアは、すべての TCP トラフィックの透過的な代行受信をサポートしています。

基本的な WCCP を構成するには、データセンターのルータと WAE およびブランチ オフィスのルータと WAE で、WCCP バージョン 2 サービスを有効にする必要があります。WAE を起動し稼動させるために、使用可能な WCCP 機能またはサービスをすべて設定する必要はありません。

（注）　WCCP バージョン 1 は Web トラフィック（ポート 80）しかサポートしていないため、ルータと WAE が WCCP バージョン 1 の代わりに WCCP バージョン 2 を使用するように設定する必要があります。

WCCP は、PBR より設定がはるかに簡単です。ただし、一般にデータセンターとブランチ オフィスの端に存在するルータ上の WCCP を設定するには、ルータへの書き込みアクセスが必要です。また、WCCP を使用すると、WAE を稼動させるために、ルータと WAE 上の WCCP の基本的な設定を実行するだけで済むという利点もあります。

また、WCCP バージョン 2 プロトコルには、複数のデバイス間の自動的なフェールオーバーやロードバランシングのような魅力的な機能が内蔵されています。WCCP 対応ルータは、WCCP キープアライブ メッセージを使用して、ルータに接続している各 WAE の状態をモニタします。WAE が停止している場合、ルータは WAE へのパケット リダイレクションを停止します。WCCP バージョン 2 を使用すると、ブランチ オフィスの WAE は WAAS サービスのシングル ポイント障害になりません。また、ルータは、複数のブランチ オフィスの WAE の間でトラフィックの負荷を分散できます。

ルータと WAE の両方で CLI コマンドを使用して基本的な WCCP を設定できます。また、CLI コマンドを使用して WCCP 用にルータを設定し、WAAS Central Manager GUI を使用して WAE 上の基本的な WCCP を設定できます。『*Cisco Wide Area Application Services Quick Configuration Guide*』に記載されている設定例では、CLI を使用して WAE 上の基本的な WCCP を設定しています。

最初のブランチ オフィスの WAE とデータセンターの WAE では、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、WAAS CLI を使用して WCCP の基本的な初期設定を完了することを推奨します。WCCP 透過リダイレクションが正常に動作していることを確認したら、WAAS Central Manager GUI を使用して集中的にこの基本的な WCCP 設定を変更したり、WAE（または WAE のグループ）用に追加の WCCP 設定（ロード バランシングなど）を構成したりすること

ができます。詳細については、「WAE 用の WCCP 設定の管理」（P.4-12）を参照してください。ルータ上の基本的な WCCP を構成したら、「WCCP 対応ルータでの高度な WCCP 機能の設定」（P.4-7）の説明に従って、ルータ上の高度な WCCP 機能を構成できます。

PBR を使用する長所と短所

PBR を使用すると、組織は、トラフィックの分類に基づいて選択的にトラフィックをネクストホップへ転送するように、ネットワーク デバイス（ルータまたはレイヤ 4 ～レイヤ 6 スイッチ）を構成できます。WAAS 管理者は、PBR を使用して、既存のブランチ オフィス ネットワークとデータセンターに WAE を透過的に統合できます。PBR を使用すると、定義されたポリシーに基づいて一部またはすべてのパケットが WAE を通過するルートを確立できます。

PBR を構成するには、ルート マップを作成し、透過的なトラフィック リダイレクションを行いたいルータ インターフェイスにルート マップを適用する必要があります。ルート マップは、許可または拒否の明示的な基準を含むアクセス リストを参照します。アクセス リストは、WAE に「関連する」トラフィック（つまり、ネットワーク デバイスが透過的に代行受信し、ローカル WAE へリダイレクトする必要があるトラフィック）を定義します。ルート マップは、ネットワーク デバイスが「関連する」トラフィックを処理する方法（たとえば、パケットをネクストホップであるローカル WAE へ送信する）を定義します。

WCCP バージョン 2 の代わりに PBR を使用して透過的に IP/TCP トラフィックを WAE へリダイレクトする利点は、次のとおりです。

- PBR は、GRE オーバーヘッドがないため、WCCP バージョン 2 より高いパフォーマンスを提供します。
- ルータで Cisco Express Forwarding（CEF）が有効になっていると、デフォルトで PBR は CEF を使用します（PBR が CEF を使用すると、パケットの交換が高速化されます）。
- PBR は、適切なバージョンの Cisco IOS ソフトウェアが稼動する任意の Cisco IOS 対応ルータまたはスイッチに実装できます。Cisco IOS ソフトウェア Release 12.2 以降を使用することを推奨します。
- PBR は、複数のネクストホップ アドレスが定義されている場合、フェールオーバーを提供します。

WCCP バージョン 2 の代わりに PBR を使用して透過的に IP/TCP トラフィックを WAE へリダイレクトする主な短所は、次のとおりです。

- PBR は、等価コスト ルート間のロード バランシングをサポートしていません。そのため、PBR は、スケーラビリティを提供しません。
- PBR の設定は WCCP バージョン 2 よりも複雑です。WAAS トラフィックに PBR を設定する例については、「ポリシーベース ルーティングを使用した WAE へのすべての TCP トラフィックの透過的なリダイレクション」（P.4-34）を参照してください。

WAAS トラフィック用の WCCP または PBR ルーティングの設定

WAAS の主な機能は、WAN トラフィックを高速化することです。一般に、WAAS は、TCP トラフィックを高速化します。WAAS は、対称方式を使用してアプリケーションを最適化します。WAN の両側に、アプリケーション固有およびネットワーク固有の知能を持つ WAE が配置されます。これらの WAE は、ブランチ オフィスとデータセンターの両方で、データ パスの外部に配置されます。

ブランチ オフィスのクライアントとデータセンターのサーバ間のトラフィックは、トンネリングなしで設定された 1 組のポリシーに基づいて、WAE 経由で透過的にリダイレクトされます。ルータは、最適化、冗長性の除去、および圧縮のために、WCCP バージョン 2 または PBR を使用して、透過的にトラフィックを代行受信し、ローカル WAE へリダイレクトします。たとえば、Edge-Router1 は、PBR

または WCCP バージョン 2 を使用して、ブランチ オフィスのローカル WAE である Edge-WAE1 へ透過的にトラフィックをリダイレクトします。Core-Router1 は、PBR または WCCP バージョン 2 を使用して、データセンターのローカル WAE である Core-WAE1 へ透過的にトラフィックをリダイレクトします。

（注）　この構成例では、Edge-Router1 と Core-Router1 を、トラフィックをローカル WAE へリダイレクションできるレイヤ 4 ～ 7 スイッチで置き換えることができます。

図 2-1 に示すように、WAE（Edge-WAE1 と Core-WAE1）は、トラフィックの送信先と送信元から分離された帯域外ネットワークに存在する必要があります。たとえば、Edge-WAE1 は、クライアント（トラフィックの送信元）とは別のサブネットに存在し、Core-WAE1 は、ファイル サーバとアプリケーション サーバ（トラフィックの送信先）とは別のサブネットに存在します。さらに、WAE とルータ間の無限ルーティング ループを防止するために、トラフィックを WAE へリダイレクトするルータに WAE を接続する第 3 のインターフェイス（分離された物理インターフェイス）またはサブインターフェイスを使用する必要がある場合があります。この項目の詳細については、「第 3 のインターフェイスまたはサブインターフェイスを使用したルータと WAE の接続」（P.2-23）を参照してください。

図 2-1　PBR または WCCP バージョン 2 を使用してすべての TCP トラフィックを透過的に WAE へリダイレクトする例

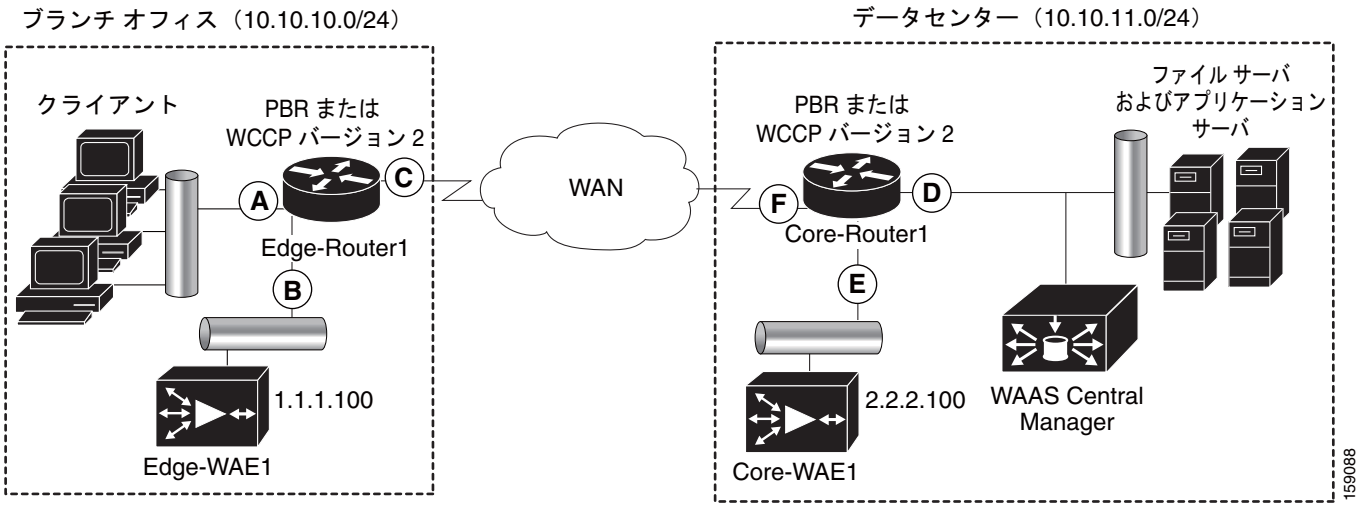


表 2-2 に、PBR または WCCP バージョン 2 を使用して、透過的にトラフィックを WAE へリダイレクトするために設定する必要があるルータ インターフェイスの概要を示します。

表 2-2　WCCP または PBR がトラフィックを WAE へリダイレクトするためのルータ インターフェイス

ルータ インターフェイス	説明
Edge-Router1	
A	発信トラフィックのリダイレクションを実行する Edge LAN インターフェイス（入力インターフェイス）
B	Edge-Router1 の LAN ポートにない第 3 のインターフェイス（分離された物理インターフェイス）またはサブインターフェイス。ブランチ オフィスの Edge-Router1 に Edge-WAE1 を接続するために使用します。
C	着信トラフィックのリダイレクションを実行する Edge-Router1 の Edge WAN インターフェイス（出力インターフェイス）
Core-Router1	

表 2-2　WCCP または PBR がトラフィックを WAE へリダイレクトするためのルータ インターフェイス （続き）

ルータ インターフェイス	説明
D	発信トラフィックのリダイレクションを実行する Core LAN インターフェイス（入力インターフェイス）
E	Core-Router1 上の LAN ポートにない第 3 のインターフェイスまたはサブインターフェイス。データセンターの Core-Router1 に Core-WAE1 を接続するために使用します。
F	着信トラフィックのリダイレクションを実行する Core-Router1 の Core WAN インターフェイス（出力インターフェイス）

このトラフィック リダイレクションは、トンネリングを使用しません。4 つ 1 組の情報（送信元 IP アドレス、送信元ポート番号、送信先 IP アドレス、および送信先ポート番号）が、TCP トラフィックの両端で維持されます。WAAS の主な機能が WAN 経由で転送するデータを減らして WAN トラフィックを加速することであるため、TCP トラフィックの元のペイロードは両端で維持されません。このようなペイロードの変更により、（NBAR のように）処理を実行するために実際のペイロードを見る必要がある（WCCP または PBR リダイレクションを実行する）ルータの機能に潜在的に影響する場合があります。この項目の詳細については、「WAAS と Cisco IOS の相互運用性」（P.2-11）を参照してください。

両側でトンネリングなしで WCCP または PBR を使用するには、トラフィックを代行受信し、近くのルータだけでなく、遠くのルータにもリダイレクトする必要があります。そのため、トンネルに基づくモードの 2 か所の代行受信地点に対して、4 か所の代行受信地点が必要です。

WCCP 対応ルータの発信インターフェイスまたは着信インターフェイスのどちらかで、パケット リダイレクションをイネーブルにすることができます。*発信*および*着信*という用語は、インターフェイスから見て定義されます。着信リダイレクションは、あるインターフェイスでトラフィックを受信した通りにリダイレクトすることを示します。発信リダイレクションは、あるインターフェイスでトラフィックを送信した通りにリダイレクトすることを示します。

WAAS ネットワークに WAN 最適化を展開している場合は、WCCP バージョン 2 と TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）用にルータと WAE を構成する必要があります。

（注） サービス 61 と 62 は、WAE での TCP 無差別の設定時に常に有効です。ネットワーク デバイス（ルータ、スイッチ、その他）での TCP 無差別の設定時に、シリーズ 61 と 62 は定義が必要であり、別々に設定される必要があります。サービス 61 は、送信元 IP アドレスでトラフィックを配信し、サービス 62 は、送信先 IP アドレスでトラフィックを配信します。

TCP 無差別モード サービスは、任意の TCP ポート宛てのすべての TCP トラフィックを代行受信し、透過的 WAE へリダイレクトします。WCCP 対応ルータは、サービス ID 61 および 62 を使用して、このサービスにアクセスします。

デフォルトで、IP プロトコル 6 が、TCP 無差別モード サービス用に指定されます。そのため、TCP 無差別モード サービスに設定されたルータは、任意の TCP ポート宛てのすべての TCP トラフィックを代行受信し、ローカル WAE へリダイレクトします。TCP 無差別モード サービスは WAE で設定されるため、WAE は、指定した WCCP ルータが透過的に WAE へリダイレクトするすべての TCP トラフィックを受け付けます（たとえば、Edge-WAE1 は、それにリダイレクトされたすべての TCP トラフィックを受け付けます）。ブランチ オフィスでは、エッジ ルータのエッジ LAN および WAN インターフェイスでパケットを代行受信し、TCP トラフィックをローカル WAE（ブランチ オフィスの WAE）へリダイレクトできます。データセンターでは、コア ルータのコア LAN および WAN インターフェイスでパケットを代行受信し、TCP トラフィックをローカル WAE（データセンターの WAE）へリダイレクトできます。詳細については、「WAAS ネットワークでの無差別 TCP デバイスとしての WAE の設定」（P.2-23）を参照してください。

可能な場合は、ブランチ ソフトウェア ルータの着信インターフェイスにパケット リダイレクションを設定してください。着信トラフィックは、Cisco Express Forwarding（CEF）、distributed Cisco Express Forwarding（dCEF）、高速スイッチング、またはプロセス転送を使用するように設定できます。

（注）　CEF は、WCCP に必要であり、ルータで有効になっている必要があります。

WCCP を使用してルータの発信または着信インターフェイスでパケット リダイレクションを有効にするには、**ip wccp redirect** インターフェイス コンフィギュレーション コマンドを使用します。

注意　**ip wccp redirect** インターフェイス コマンドは、**ip wccp redirect exclude in** コマンドに影響を及ぼす可能性があります。**ip wccp redirect exclude in** コマンドをインターフェイスに設定し、続けて、**ip wccp redirect in** コマンドを設定すると、**exclude in** コマンドが上書きされます。**exclude in** コマンドを設定すると、**redirect in** コマンドが上書きされます。

ここでは、次の内容について説明します。

- 「WAAS ネットワークでの無差別 TCP デバイスとしての WAE の設定」（P.2-23）
- 「第 3 のインターフェイスまたはサブインターフェイスを使用したルータと WAE の接続」（P.2-23）

WAAS ネットワークでの無差別 TCP デバイスとしての WAE の設定

指定した WCCP バージョン 2 ルータによって TCP トラフィックが透過的に WAE にリダイレクトされるように、WAE を無差別 TCP デバイスとして機能させるには、WAE で WCCP バージョン 2 サービス 61 および 62 を使用します。次のブランチ オフィスの WAE の WAAS CLI の出力例に示すとおり、WCCP サービス 61 および 62 は WAE 上では、標準名の tcp-promiscuous で表されます。

```
Edge-WAE1(config)# wccp ?
  access-list      Configure an IP access-list for inbound WCCP encapsulated
                   traffic
  flow-redirect    Redirect moved flows
  router-list      Router List for use in WCCP services
  shutdown         Wccp Shutdown parameters
  slow-start       accept load in slow-start mode
  tcp-promiscuous  TCP promiscuous mode service
  version          WCCP Version Number
```

WCCP サービス 61 および 62 は、WAAS Central Manager GUI では TCP Promiscuous という名前で表現されます（図 4-3 を参照）。

WAAS Central Manager GUI を使用して個々の WAE で TCP 無差別モード サービスを設定することもできますが、WAAS CLI を使用して WAE の基本的な初期設定を完了し、WAAS Central Manager GUI を使用して以後の設定変更を行うことを推奨します。WAAS Central Manager GUI を使用して以後の設定変更を行うと、それらの変更を WAE グループ（デバイス グループ）にも適用できます。WAAS ネットワーク用の基本的な WCCP 設定を実行する手順については、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。WAAS Central Manager GUI を使用して WAE または WAE のグループ用の基本的な WCCP 設定を変更する手順については、「WAE 用の WCCP 設定の管理」（P.4-12）を参照してください。

第 3 のインターフェイスまたはサブインターフェイスを使用したルータと WAE の接続

WCCP バージョン 2 または PBR を使用して透過的に TCP トラフィックを WAE へリダイレクトする予定の場合は、WAE がトラフィック リダイレクションを行うルータ インターフェイスと同じセグメントに接続しないことを確認してください。そうでない場合、ルータと WAE の間で無限ルーティング

ループが発生します。これらの無限ルーティング ループは、トラフィックを初めて WAE へリダイレクションしたあとで、代行受信とリダイレクションをバイパスするようにルータに通知する方法がないために発生します。ルータは、代行受信した同じトラフィックをローカル WAE へ継続的にリダイレクションし、そのために無限ルーティング ループが発生します。

（注）　WCCP GRE 返信および汎用 GRE 出力方式では、WAE をクライアントおよびサーバと同じ VLAN またはサブネットに配置することができます。これらの出力方式を構成する方法については、「代行受信接続の出力方法の設定」（P.4-30）を参照してください。

たとえば、PBR または WCCP トラフィック リダイレクションを行うブランチ オフィスの LAN ルータ インターフェイスと同じセグメント（サブネット）に Edge-WAE1 を接続すると、Edge-Router1 と Edge-WAE1 の間で無限のルーティング ループが発生します。PBR または WCCP トラフィック リダイレクションを行うデータセンターの LAN ルータ インターフェイスと同じセグメント（サブネット）に Core-WAE1 を接続すると、Core-Router1 と Core-WAE1 の間で無限のルーティング ループが発生します。

ルータとそのローカル WAE の間の無限ルーティング ループを防止するには、ルータの LAN ポートから第 3 のインターフェイス（独立した物理インターフェイス）またはサブインターフェイス（別の仮想サブインターフェイス）経由で WAE をルータに接続します。第 3 のインターフェイスまたはサブインターフェイスを使用して PBR または WCCP リダイレクションを実行するルータに WAE を接続すると、WAE が Cisco IOS 機能が有効になっていない独立した処理経路を持つことになります。さらに、この方法により、既存のネットワークに WAE を統合するプロセスが簡単になります。WAE は Cisco IOS 機能が有効になっていない第 3 のインターフェイスまたはサブインターフェイス経由でルータに接続するため、一般に Cisco IOS 機能が有効になっている既存のネットワーク要素（たとえば、Edge-Router1 または Core-Router1）は、これらのルータに WAE を接続しても影響を受けません。WAAS と Cisco IOS の相互運用性の詳細については、「WAAS と Cisco IOS の相互運用性」（P.2-11）を参照してください。

サブインターフェイスを使用して、TCP トラフィックを WAE へリダイレクトするルータにローカル WAE を正しく接続する方法の例については、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。

ルータと WAE 上のアクセス リスト

オプションで、ルータに定義されたアクセス リストに基づいて、トラフィックを WAE からリダイレクトするようにルータを設定できます。これらのアクセス リストのことを「リダイレクト リスト」と呼びます。透過的にトラフィックを WAE へリダイレクトするように設定するルータでアクセス リストを設定する方法については、「ルータ上の IP アクセス リストの設定」（P.4-10）を参照してください。

（注）　ルータ上の IP アクセス リストが最も高いプライオリティを持ち、WAE 上で定義された IP ACL がそれに続き、その後に WAE 上で定義された代行受信 ACL が続きます。

ここでは、次の内容について説明します。

WAE 上の IP ACL

集中管理される WAAS ネットワーク環境では、管理者がさまざまなデバイスやサービスへの不正アクセスを防止できる必要があります。WAAS ソフトウェアは、WAAS デバイス上の特定のインターフェイスへのアクセス、またはそれら経由のアクセスを制限できる標準および拡張の IP アクセス コントロール リスト（ACL）をサポートしています。詳細については、第 8 章「WAAS デバイス用の IP ACL の作成および管理」を参照してください。

（注）　インターフェイスに適用される IP ACL、および WCCP ACL は、WAE 上で定義されたどの代行受信 ACL および WAAS アプリケーション定義よりも優先されます。

WAE 上の代行受信 ACL

代行受信 ACL を設定することにより、すべてのインターフェイスでどの着信トラフィックが WAE デバイスにより代行受信されるかを制御できます。ACL により許可されたパケットは、WAE によって代行受信され、ACL によって拒否されたパケットは処理されずに WAE を通過します。WAE 上で代行受信 ACL を設定することにより、ルータの設定を変更することなく、トラフィックの代行受信を制御できます。

代行受信 ACL は、WCCP とインライン代行受信の両方で使用できます。

WAE 上で定義された代行受信 ACL は、WAE 上で定義されたどの WAAS アプリケーション定義よりも常に優先されますが、適用されるのはインターフェイス ACL と WCCP ACL の後です。

WAE の代行受信 ACL を設定する方法の詳細については、「代行受信アクセス コントロール リストの設定」（P.4-29）を参照してください。

（注）　代行受信 ACL は、固定バイパス リストとは排他的な機能です。両方のタイプのリストを同時に使用することはできません。固定バイパス リストではなく代行受信 ACL を使用することを推奨します。

WAE 上での固定バイパス リスト

代行受信 ACL の定義に加えて、WAE 上で固定バイパス リストを設定することもできます。固定バイパスを使用すると、WAE は、設定可能なクライアントとサーバの集合間でトラフィック フローの処理をバイパスできます。ブランチ オフィスの WAE に固定バイパス項目を設定すると、ルータの設定を変更することなく、トラフィックの代行受信を制御できます。また、ルータでも、最初にブランチ オフィスの WAE へリダイレクトすることなく、トラフィックをバイパスするようにアクセス リストを設定できます。

特定のクライアントから特定のサーバ（または特定のクライアントからすべてのサーバ）への接続を WAAS がアクセラレーションしないようにしたい場合、固定バイパスを使用できます。WAE または WAE のグループ用に固定バイパス リストを集中的に設定する方法については、「WAE 用の固定バイパス リストの設定」（P.4-28）を参照してください。

（注）　可能な限り、ACL（リダイレクト リスト）を WCCP 対応ルータ上で使用することを推奨します。この方法が、トラフィック代行受信を制御するのに最も効率的な方法です。一方、インライン代行受信を使用する場合は、WAE 上で固定バイパス リストまたは代行受信 ACL を使用できます。代行受信 ACL の方が柔軟性が高く、パススルー接続に関してより優れた統計結果が得られるため、代行受信 ACL を使

用することを推奨します。ルータ上で ACL を設定する方法については、「ルータ上の IP アクセス リストの設定」（P.4-10）を参照してください。WAE の代行受信 ACL を設定する方法の詳細については、「代行受信アクセス コントロール リストの設定」（P.4-29）を参照してください。

WAAS ログイン認証および許可

WAAS ネットワークでは、管理的ログイン認証と許可を使用して、設定、モニタリング、またはトラブルシューティング用に WAAS デバイスにアクセスしたい管理者からのログイン要求を制御します。

ログイン認証とは、WAAS デバイスが、デバイスにログインしようとしている管理者が有効なユーザ名とパスワード持っているかどうかを確認するプロセスです。ログインしようとする管理者は、デバイスに登録されたユーザ アカウントを持つ必要があります。ユーザ アカウント情報は、ユーザの管理ログインと設定特権を許可する役割を果たします。ユーザ アカウント情報は AAA データベースに保存され、AAA データベースが存在する特定の認証サーバにアクセスするように WAAS デバイスを設定する必要があります。ユーザがデバイスにログインしようとすると、デバイスは、その人物のユーザ名、パスワード、および特権レベルをデータベースに保存されたユーザ アカウント情報と比較します。

WAAS ソフトウェアは、次の Authentication, Authorization, And Accounting（AAA; 認証、許可、アカウンティング）サポートを、外部アクセス サーバ（たとえば、RADIUS、TACACS+、または Windows ドメイン サーバ）を持つユーザ、および AAA 機能を持つローカル アクセス データベースが必要なユーザに対して提供します。

- *認証*（または*ログイン認証*）は、ユーザが誰であるかを決定する処理です。ユーザ名とパスワードを検査します。
- *許可*（または*設定*）は、ユーザが許可されていることを決定する処理です。ネットワーク内で認証されたユーザに対して権限を許可または拒否します。一般に、認証の後で許可が実行されます。ユーザがログインするには、認証と許可の両方が必要です。
- *アカウンティング*は、システム アカウンティングを目的に管理ユーザの作業を追跡する処理です。WAAS ソフトウェアでは、TACACS+ による AAA アカウンティングがサポートされています。

詳細については、「WAAS デバイス用の AAA アカウンティングの設定」（P.6-33）を参照してください。

WAAS 管理者アカウント

集中管理される WAAS ネットワークでは、WAAS Central Manager にアクセスし、それと独立して WAAS Central Manager に登録された WAE にアクセスするための管理者アカウントを作成できます。WAAS 管理者には、2 種類のアカウントがあります。

- 役割に基づくアカウント：ユーザは、WAAS Central Manager GUI、WAAS Central Manager CLI、および WAE Device Manager GUI にアクセスできます。WAAS ソフトウェアには、管理者の役割に割り当てられるデフォルトの WAAS システム ユーザ アカウント（ユーザ名は admin、パスワードは default）があります。
- デバイスに基づく CLI アカウント：ユーザは、WAAS デバイスの WAAS CLI にアクセスできます。これらのアカウントのことを「ローカル ユーザ アカウント」と呼びます。

（注）　管理者は、コンソール ポートまたは WAAS Central Manager GUI を使用して WAAS Central Manager デバイスにログインできます。管理者は、コンソール ポートまたは WAE Device Manager GUI を使用して、データセンター WAE またはブランチ オフィス WAE として機能する WAAS デバイスにログインできます。

WAAS ソフトウェアが動作する WAAS デバイスには、最初にデバイスにアクセスするために使用できる定義済みの superuser アカウントが付属しています。認証と許可が設定される前にシステム管理者が WAAS デバイスにログインするとき、管理者は定義済みの superuser アカウントを使用して WAAS デバイスにアクセスできます（定義済みのユーザ名は admin、定義済みのパスワードは default です）。この定義済みの superuser アカウントを使用して WAAS デバイスにログインするとき、WAAS システム内のすべての WAAS サービスとエンティティへのアクセスが許可されます。

WAAS デバイスを初期設定した後で、各 WAAS デバイスで定義済みの superuser アカウント用のパスワードをただちに変更することを強く推奨します（定義済みのユーザ名は *admin*、パスワードは *default*、特権レベルは superuser、特権レベル 15 です）。WAAS Central Manager GUI を使用してパスワードを変更する手順については、「自身のアカウントのパスワードの変更」（P.7-7）を参照してください。

WAE の論理グループの作成

WAAS Central Manager に登録されている WAE の設定と保守を能率化するために、論理グループを作成し、1 台または複数の WAE をグループに割り当てることができます。グループは、複数の WAE を設定する時間を節減するだけでなく、設定が WAAS ネットワーク全体に一貫して適用されることを保証します。たとえば、グループ内のすべての WAE に必要な標準の Windows 認証設定を定義する WinAuth グループをセットアップすることができます。一旦 WinAuth 設定を定義すると、各 WAE で同じ設定を個別に定義する代わりに、WinAuth グループ内のすべての WAE に集中的にそれらの値を適用ができます。

WAAS Central Manager GUI を使用すると、次のようなデバイス グループにブランチ オフィスの WAE とデータセンターの WAE を簡単に編成できます。

- 標準デバイス グループ：共通の品質と機能を共有する WAE の集合。認証設定に基づいてグループをセットアップすることが、デバイス グループの例です。デバイス グループには、2 つの種類があります。
  - 設定グループ
  - Wide Area File Services（WAFS; 広域ファイル サービス）コア クラスタ（WAFS レガシー モードに対してだけ使用）

  デバイス グループを作成するときは、その WAE のグループをネットワーク内の他のグループから区別する固有の特性を識別する必要があります。たとえば、大規模な WAAS 構成では、WAAS ネットワーク内の別の WAE 集合と異なる 1 組の WAE を認証設定で構成する必要がある場合があります。この場合、それぞれが異なる認証設定を含む 2 つのデバイス グループを作成し、最も適切なグループに WAE を割り当てます。

  異なる時間帯に存在する WAE がある場合は、あるグループ内の WAE が別のグループ内の WAE の時間帯設定と異なる設定を持つように、地域に基づいてデバイス グループを作成することもできます。

  すべての WAE を同じ設定で構成できる小規模の WAAS 構成では、ただ 1 つの一般的なデバイス グループ（設定グループ）を作成するだけで済みます。この方法により、グループ用の設定を構成し、すべての WAE にそれらの設定を適用することができます。

  （注） AllDevicesGroup は、自動的にすべての WAE を含むデフォルトのデバイス グループです。AllDevicesGroup または他の任意のデバイス グループでは、グループ内のすべての WAE 全体で一貫させたい設定だけを設定する必要があります。単一の WAE に適用する設定は、デバイス グループでなく、そのデバイスだけで構成する必要があります。

- 基準グループ：複数の WAE に一貫した WAAS サービスを設定するために使用する特殊な種類のデバイス グループ。基準グループには、3 つの種類があります。
  - ファイル

- アクセラレーション
- プラットフォーム

たとえば、すべての WAE に同一のアプリケーション ポリシー集合を入れたい場合は、カスタム ポリシーと変更されたポリシーを含むアクセラレーション基準グループを作成することを推奨します。WAE をこのグループに割り当てると、WAE は自動的にグループからアプリケーション ポリシーを継承します。ポリシーを変更する必要があるときは、アクセラレーション基準グループに対して変更を行うと、変更がメンバー デバイスに伝達します。WAE は別々のデバイス グループに属することができるため、基準グループをセットアップすることは、異なるデバイス グループに存在する WAE 全体に一貫したサービス設定を適用する 1 つの方法です。

（注） デバイス グループには、ファイル設定とアクセラレーション設定を構成しないことを推奨します。その代わりに、この目的には、ファイル基準グループとアクセラレーション基準グループを使用してください。

デフォルトで、WAAS Central Manager を使用すると、（基準グループを含む）複数のデバイス グループにデバイスを割り当てることができます。デバイス グループを作成する前に、必ず、グループに入れる固有のプロパティを理解してください。

WAAS Central Manager を使用すると、WAAS デバイスに関連付けることができる位置を作成できます。最初にデバイスをアクティブにするとき、デバイスを位置に割り当てます。WAAS デバイスを位置に割り当てる主な目的は、WAAS デバイスをそれが存在する場所で識別できるようにすることです。デバイスはそれが属する位置から設定を継承しないため、位置はデバイス グループとは異なります。

『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、最初にデバイスをアクティブにするとき、デバイスを位置に割り当てます。WAE の論理グループを作成する方法の詳細については、第 3 章「デバイス グループとデバイス位置の使用」を参照してください。

データ移行プロセス

既存のネットワークが存在する場合は、WAAS ネットワークをセットアップする前にいくつかの手順を実行する必要があります。データ移行プロセスの最初の手順では、ブランチ オフィスのデータをバックアップし、データセンターに復元します。

データをデータセンターにバックアップしたら、最も高速のアクセスを提供したいファイルにキャッシュをプリロードします（これを「*事前配置*」と呼びます）。ブランチ オフィスのファイル サーバから WAE に、やはり同じブランチ オフィスに存在するファイルをセットアップします。次に、ブランチ オフィスからファイル サーバを撤去し、データセンターのファイル サーバを指し示すことができます。

データ移行プロセスの最後の手順では、WAFS ポリシーを設定します。

データ移行プロセスを実行するときは、次の制限に注意してください。

- 事前配置は、CIFS 環境だけで動作します。
- データセンターでのファイル サーバのトポロジは、ブランチ オフィスのファイル サーバに存在するトポロジと同じでなければなりません。
- リソース クレデンシャル（ACL など）は、自動的に移行されません。2 つの選択肢があります。
  - バックアップ ソフトウェアや復元ソフトウェアを使用して、ツリーの初期バックアップを対象サーバに復元できます。この方法により、ACL だけでなく、Rsync が差分計算の入力として取ることができる初期ファイル セットを作成できます。複製は、そのツリー内の既存の ACL を継承します。
  - あるいは、（データとアクセス権を含む）初回の Robocopy を実行し、Rsync を使用して同期反復を続行します。

複製のあとで、Microsoft 社のツールを使用して、複製したツリーに（データを含まず）ACL だけをコピーします。Robocopy.exe を使用してディレクトリ ツリーまたはファイル ACL をコピーし、Permcopy.exe を使用して共有アクセス権をコピーすることができます。

- 移行のサイズは、ブランチ オフィスの WAE のキャッシュ サイズ未満でなければなりません。

PART 2

WAAS の導入と設定

CHAPTER 3

デバイス グループとデバイス位置の使用

この章では、Wide Area Application Service（WAAS）ソフトウェアがサポートするデバイス グループの種類と、複数のデバイスをより簡単に同時に管理し、構成できるようにグループを作成する方法について説明します。また、デバイス位置を使用する方法についても説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

デバイス グループと基準グループについて

デバイス グループを作成するときは、そのデバイスのグループをネットワーク内の他のグループから区別する固有の特性を識別する必要があります。たとえば、大規模な WAAS 構成では、WAAS ネットワーク内の別のデバイス集合と異なる 1 組のデバイスを認証設定で構成する必要がある場合があります。この場合、それぞれが異なる認証設定を含む 2 つのデバイス グループを作成し、最も適切なグループにデバイスを割り当てます。

異なる時間帯に存在するデバイスがある場合は、あるグループ内のデバイスが別のグループ内のデバイスの時間帯設定と異なる設定を持つように、地域に基づいてデバイス グループを作成することもできます。

すべてのデバイスを同じ設定で構成できる小規模の WAAS 構成では、ただ 1 つの一般的なデバイス グループを作成するだけで済みます。この方法により、グループ用の設定を構成し、すべての WAAS デバイスにそれらの設定を適用することができます。

グループは、複数のデバイスを設定する時間を節減するだけでなく、設定が WAAS ネットワーク全体に一貫して適用されることを保証します。

WAAS Central Manager で WAE デバイスを登録すると、そのデバイスは、システムでの唯一のデフォルトのデバイス グループである AllDevicesGroup に自動的に参加します。追加のデバイス グループを作成する場合は、WAE デバイスを複数のグループ（デフォルトの All Devices グループと作成した新

しいデバイス グループ）に属するようにするかどうかを決定する必要があります。作成したデバイス グループだけにデバイスが属する場合は、必ず、デフォルトの All Devices グループからデバイスを削除してください。

WAAS デバイスは、次の種類のデバイス グループにまとめることができます。

- 標準デバイス グループ：共通の品質と機能を共有するデバイスの集合。すでに説明したように認証設定に基づいてグループをセットアップすることが、デバイス グループの例です。デバイス グループには、設定グループと WAFS コア クラスタの 2 種類があります。デバイス グループについては、「新しいデバイス グループの作成」（P.3-3）でさらに詳しく説明します。
- 基準グループ：複数のデバイスに一貫した WAAS サービスを設定するために使用する特殊な種類のデバイス グループ。基準グループには、ファイル、アクセラレーション、およびプラットフォームの 3 種類があります。

  デフォルトで、WAAS Central Manager に登録したすべてのデバイスが、3 つの基準グループすべてに割り当てられます。

  基準グループを使用すると、異なるデバイス グループに存在するデバイス全体に一貫したサービス設定を適用できます。

  たとえば、異なるデバイス グループに存在する WAAS デバイスがあり、すべてのデバイスが 同じアプリケーション ポリシーを共有するようにしたい場合、ポリシーの変更をアクセラレーション基準グループに対して行う必要があります。新しいポリシーを作成したり、既存のポリシーを変更すると、それらの変更は、アクセラレーション基準グループに属する各デバイスに配信されます。特定のデバイス グループのポリシーを変更する場合、他のグループに属するデバイスには影響しません。

デバイス グループの操作

ここでは、次の内容について説明します。

デバイス グループの作成

ここでは、次の内容について説明します。

表 3-1 で、新しいデバイス グループを作成するプロセスについて説明します。

表 3-1　デバイス グループを作成するためのチェックリスト

作業	追加情報と手順
1. 新しいデバイス グループを作成する。	グループ名および新しくアクティブにしたすべてのデバイスをこのグループに割り当てるかどうかなど、新しいグループに関する一般的な情報を定義します。 詳細については、「新しいデバイス グループの作成」（P.3-3）を参照してください。
2. 新しいデバイス グループの設定を構成する。	このデバイス グループに固有の設定を指定します。このグループに属するすべてのデバイスが、自動的にこれらの設定を継承します。 詳細については、「デバイス グループ用の設定の構成」（P.3-4）を参照してください。
3. デバイス グループにデバイスを割り当てる。	デバイスがグループ設定を継承できるように、グループにデバイスを割り当てます。 詳細については、「設定デバイス グループへのデバイスの割り当て」（P.3-5）を参照してください。

新しいデバイス グループの作成

デバイス グループを作成する前に、必ず、グループに入れる固有のプロパティを理解してください。たとえば、異なる認証設定や異なる時間帯設定を持つ 2 つのデバイス グループをセットアップできます。

デバイス グループを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。[Device Groups] ウィンドウが表示されます。

このウィンドウから、次の作業を実行できます。

- 変更するデバイス グループの横にある [Edit] アイコンをクリックします。
- 次の手順の説明に従って、新しいデバイス グループを作成します。

ステップ 2　タスクバーの [Create New Device Group] アイコンをクリックします。[Creating New Device Group] ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、デバイス グループの名前を入力します。

名前は、システムで他のデバイス グループからこのデバイス グループを区別できる固有の名前でなければなりません。名前には、英字、数字、ピリオド、ハイフン、アンダースコア、およびスペース以外の文字は使用できません。

ステップ 4　[Type] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [Configuration Group]：標準の種類のデバイス グループ。
- [Legacy WAFS Core Cluster]：レガシー モードを使用して Wide Area File Services（WAFS; 広域ファイル サービス）を設定するときだけ作成する必要がある特殊な種類のデバイス グループ。詳細については、「コア クラスタの設定」（P.11-11）を参照してください。

ステップ 5　[Automatically assign all newly activated devices to this group] チェックボックスを選択して、新たにアクティブにしたすべてのデバイスに対するデフォルトのデバイス グループとして、このデバイス グループを設定します。

[Baseline] チェックボックスは、選択しないでください。基準グループを作成する場合は、「基準グループ設定のカスタマイズ」（P.3-11）を参照してください。

（注）　デフォルトでは、システムはファイル、アクセラレーション、およびプラットフォーム基準グループで設定されています。これらの基準グループ タイプのうち 1 つしか設定できないため、グループの 1 つを削除しない限り、基準チェックボックスを選択することはできません。これらのグループの 1 つを再作成しない限り、[Is Baseline] チェックボックスを選択しても効果はありません。

ステップ 6　（任意）[Comments] フィールドに、グループに関するコメントを入力します。入力したコメントは [Device Group] ウィンドウに表示されます。

ステップ 7　[Submit] をクリックします。

ページが、追加オプションで更新されます。

（注）　[Pages configured for this device group] 矢印は、WAAS Central Manager GUI でこのデバイス グループ用に設定された設定ウィンドウを表示します。これは新しいデバイス グループであるため、このリストにはページが表示されません。

ステップ 8　（任意）次の手順を完了して、このデバイス グループのナビゲーション ペインをカスタマイズします。この機能を使用して、そのデバイス グループでは不要な設定ウィンドウの表示を消します。

a. [Select pages to hide from table of contents for this device group] 矢印をクリックします。

WAAS Central Manager GUI に、ウィンドウのリストが表示されます。

b. このデバイス グループでは非表示にするウィンドウを選択します。ウィンドウの横にあるフォルダ アイコンをクリックすると、そのチャイルド ウィンドウを表示できます。

c. [Submit] をクリックします。

ステップ 9　「デバイス グループ用の設定の構成」の項の説明に従って、このデバイス グループ用の設定を構成します。

デバイス グループ用の設定の構成

デバイス グループを作成したあとで、このグループ固有の設定を構成する必要があります。

すべての WAAS デバイスを含む一般的なデバイス グループがある場合は、すべてのデバイスに一貫する設定だけを構成してください。単一のデバイスに適用する設定は、デバイス グループでなく、そのデバイスだけで構成する必要があります。

（注）　デバイス グループには、ファイル設定とアクセラレーション設定を構成しないことを推奨します。その代わりに、この目的には、ファイル基準グループとアクセラレーション基準グループを使用してください。詳細については、「基準グループの操作」（P.3-10）を参照してください。

デバイス グループ用の設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。

[Device Groups] ウィンドウが表示されます。

ステップ 2　設定するデバイス グループの横にある [Edit] アイコンをクリックします。

[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　[Pages configured for this device group] 矢印ボタンをクリックして、すでに基準グループ用に設定されている設定ウィンドウを表示します。

そのデバイス グループ用に設定されたページのリストが表示されます。これが新しいデバイス グループである場合、またはこのデバイス グループ用にページが設定されていない場合、リストには何も表示されません。

ステップ 4　次の手順を完了して、このデバイス グループのナビゲーション ペインをカスタマイズします。

a.　[Select pages to hide from table of contents of this device group] 矢印をクリックします。

WAAS Central Manager GUI に、ウィンドウのリストが表示されます。

b.　このデバイス グループでは非表示にするウィンドウの横にあるチェックボックスを選択します。この機能を使用して、特定のデバイス グループ用に不要な設定ウィンドウを非表示にします。

ステップ 5　ナビゲーション ペインを使用して、このデバイス グループ用に変更したい各設定ウィンドウへ移動します。

このデバイス グループ用にウィンドウが設定されていない場合は、ウィンドウの一番上に「There are currently no settings for this group」メッセージが表示されます。

ステップ 6　設定ウィンドウで必要な変更を行い、完了したら [Submit] をクリックします。

特定の設定を構成すると、[Modifying Device Group] ウィンドウの [Pages configured for this device group] の下に、設定ウィンドウが表示されます。

ステップ 7　「設定デバイス グループへのデバイスの割り当て」（P.3-5）の説明に従って、この新しいグループにデバイスを割り当てます。

設定デバイス グループへのデバイスの割り当て

設定デバイス グループを作成したら、グループにデバイスを割り当てる必要があります。WAAS Central Manager GUI は、設定グループにデバイスを割り当てる 2 つの方法を提供します。最初にデバイスを選択してからグループにデバイスを割り当てる、または最初にデバイス グループを選択してからグループにデバイスを割り当てることができます。

この項の手順では、デバイスをグループに割り当てる方法について説明します。デバイスにグループを割り当てるには、[My WAN] > [Manage Devices] を選択し、グループに割り当てるデバイスの横にある [Edit] アイコンをクリックして、ナビゲーション ペインで [Assign Groups] を選択します。次に、下記のステップ 4 とステップ 5 に説明されている同じ方法を使用して、デバイスにグループを割り当てることができます。

WAAS Central Manager は、デバイス グループに割り当てることができません。WAAS Central Manager は、他のデバイスとは別に設定する必要があります。

（注）　デフォルトで、すべてのデバイスは、アクティブになったとき、自動的に AllDevicesGroup に参加します。デバイスが 2 つの異なるデバイス グループに属することを望まない場合は、AllDevicesGroup からデバイスの割り当てを解除し、別のデバイス グループにデバイスを割り当てる必要があります。

デバイス グループにデバイスを割り当てるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。

ステップ 2　デバイスを割り当てるデバイス グループの横にある [Edit] アイコンをクリックします。

[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Assign Devices] を選択します。

さまざまな位置に割り当てられた WAE デバイスを表示する [WAE Assignments] ウィンドウが表示されます。

割り当てウィンドウでは、リスト内の項目のビューをフィルタできます。フィルタにより、設定した基準に一致するリスト内の項目を見つけることができます。

ステップ 4　次のいずれかを実行して、デバイス グループにデバイスを割り当てます。

- タスクバーの をクリックして、使用できるすべてのデバイスをグループに割り当てます。
- グループに割り当てる各デバイスの横にある をクリックします。選択すると、アイコンは に変化します。

ステップ 5　[Submit] をクリックします。

割り当てたデバイスの横に、緑色のチェック マークが表示されます。

ステップ 6　デバイス グループから削除するデバイスの名前の横にある [Unassign] アイコン（緑色のチェック マーク）をクリックします。あるいは、タスクバーの [Remove all WAEs] アイコンをクリックして、選択したデバイス グループからすべてデバイスを削除することもできます。[Submit] をクリックします。

デバイス グループの削除

デバイス グループを削除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。[Device Groups] ウィンドウが表示されます。

ステップ 2　削除するデバイス グループの横にある [Edit] アイコンをクリックします。[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Delete Device Group] アイコンをクリックします。デバイス グループを削除するかどうかを確認するプロンプトが表示されます。

ステップ 4　操作を確認するには、[OK] をクリックします。

デバイス グループ割り当ての表示

WAAS Central Manager GUI を使用すると、デバイスが属するグループと特定のグループに属するデバイスを表示できます。この項では、この両方の手順について説明します。

デバイスが属するグループを表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　グループ割り当てを表示するデバイスの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　[Device Dashboard] ウィンドウの [Assignments] セクションで、デバイスが割り当てられているグループを表示するリンクをクリックします。

WAAS ネットワーク内のすべてのデバイス グループを表示する [Device Group Assignments] ページが表示されます。緑色のチェック マークが付いているデバイスは、このグループに割り当てられています。

あるいは、ナビゲーション ペインの [Assign Groups] オプションを選択して、[Device Group Assignments] ウィンドウへ直接進むことができます。

特定のグループに割り当てられたデバイスを表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。

ステップ 2　属するデバイスを表示するグループの横にある [Edit] アイコンをクリックします。

[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインから、[Assign Devices] を選択します。

WAAS ネットワーク上のすべてのデバイスを表示する WAE Assignments ウィンドウが表示されます。緑色のチェック マークが付いているデバイスは、このグループに割り当てられています。

デバイス グループ リストの表示

[Device Groups] ウィンドウは、WAAS ネットワークで作成されたすべてのデバイス グループを表示します。このリストを表示するには、WAAS Central Manager GUI で [My WAN] > [Manage Device Groups] を選択します。

このウィンドウは、各デバイス グループに関する次の情報を表示します。

- デバイス グループの種類（設定グループまたは WAFS コア クラスタ）
- デバイス グループの作成時に入力された任意のコメント

このウィンドウから、次の作業を実行できます。

- 新しいデバイス グループを作成する。詳細については、「新しいデバイス グループの作成」（P.3-3）を参照してください。
- 編集するグループの横にある [Edit] アイコンをクリックして、デバイス グループの設定を変更する。

デバイス グループ オーバーラップの有効化と無効化

デフォルトで、（基準グループを含む）複数のデバイス グループにデバイスを割り当てることができます。デバイスがただ 1 つのデバイス グループに属して複数のグループから設定を継承しないように、この機能性を無効にすることができます。

デバイス グループの重複を有効または無効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [System Properties] を選択します。

[Config Properties] ウィンドウが表示されます。

ステップ 2　プロパティ名 DeviceGroup.overlap の横にある [Edit] アイコンをクリックします。

[Modifying Config Property, DeviceGroup.overlap] ウィンドウが表示されます。

ステップ 3　[Value] ドロップダウン リストから、[true] または [false] を選択します（デフォルトは [true] です）。

デバイス グループの重複を無効にする（[false] に設定する）と、既存の重複デバイス グループは保持され、重複が有効になったまま処理されます。ただし、新しく追加されたデバイスは重複を許可されず、新しいデバイスは既存の重複グループに追加できません。

ステップ 4　[Submit] をクリックします。

グループ設定の変更

WAAS Central Manager GUI は、デバイスの現在のグループ設定を変更するために、次の方法を提供しています。

- 「グループ内のすべてのデバイスへのデバイス グループ設定の強制」（P.3-8）
- 「デバイス グループ優先の選択」（P.3-8）
- 「デバイス上のデバイス グループ設定の変更」（P.3-9）

グループ内のすべてのデバイスへのデバイス グループ設定の強制

グループ内のすべてのデバイスにデバイス グループ設定を強制するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。

[Device Groups] リスト ウィンドウが表示されます

ステップ 2　グループ内のすべてのデバイスに設定を強制するデバイス グループの横にある [Edit] アイコンをクリックします。

[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　タスクバーの [Force Group Settings] アイコンをクリックします。

WAAS Central Manager GUI は、次のメッセージを返します。

```
The action will apply all settings configured for this device group to all the WAEs
assigned to it. Do you wish to continue?
```

ステップ 4　デバイス グループ内のすべてのデバイスにグループ設定を強制するには、[OK] をクリックします。

ステップ 5　[Submit] をクリックします。

デバイス グループ優先の選択

設定が矛盾する複数のデバイス グループに属する場合、デバイスは、最後に変更されたデバイス グループから自動的に設定を継承します。デバイスが複数のデバイス グループに属するときにどのように設定を継承するかの詳細な説明については、「複数のデバイス グループにデバイスを割り当てる影響について」（P.3-10）を参照してください。

設定が矛盾する場合は、デバイスの設定をページ単位で編集し、優先させるデバイス グループの設定を選択できます。

デバイス グループ優先を選択するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

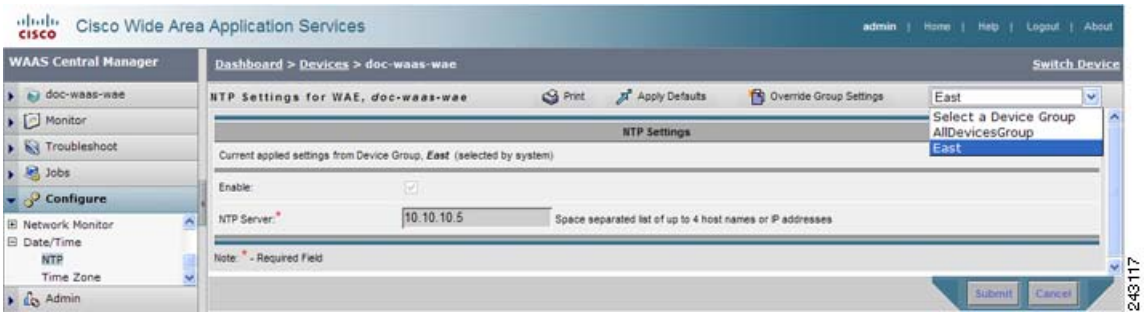
ステップ 2　デバイス グループ設定を行うデバイスの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインから、矛盾する設定を含む設定ウィンドウへ進みます。

図 3-1 に示すように、ウィンドウの一番上にあるタスクバーに、ドロップダウン リストが表示されます。このドロップダウン リストを使用すると、この設定ウィンドウが設定を継承するデバイス グループを選択できます。現在選択されているデバイス グループが、優先されるデバイス グループです。

図 3-1　　設定ウィンドウ用のデバイス グループ優先の指定



ステップ 4　ドロップダウン リストから、この設定ページが設定を継承するデバイス グループを選択し、[Submit] をクリックします。

設定ウィンドウは、選択したデバイス グループに関連する設定を反映するように変化します。

デバイス上のデバイス グループ設定の変更

WAAS Central Manager GUI を使用すると、デバイス グループ設定を変更し、そのデバイスに固有の新しい設定を指定できます。

デバイス上のデバイス グループ設定を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　グループ設定を変更するデバイスの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、変更するデバイス グループ設定を含む設定ウィンドウへ進みます。

ステップ 4　タスクバーの [Override Group Settings] アイコンをクリックします。

設定ウィンドウの設定が有効になります。

（注）　[Override Group Settings] アイコンは、関連するデバイス グループで変更された設定ウィンドウだけに表示されます。

ステップ 5　設定ウィンドウで必要な変更を行い、[Submit] をクリックします。

これで、デバイスは、自身が属するデバイス グループとは異なる値で設定されます。

（注）　[Force Settings on all Devices in Group] アイコンが、上書きされた設定ウィンドウのデバイス グループに表示されます。このアイコンをクリックしてデバイス グループ設定をデバイス グループのすべてのデバイスに適用できます。

ステップ 6　この設定ウィンドウにデバイス グループ設定を再適用するには、タスクバーのドロップダウン リストからデバイス グループを選択し、[Submit] をクリックします。

複数のデバイス グループにデバイスを割り当てる影響について

デバイスが複数のデバイス グループに属し、グループが正確に同じ設定になっていない場合、設定が矛盾する可能性があります。この場合、デバイスは、最後に変更されたデバイス グループから設定を継承します。ただし、どのように変更が実装されたかによっては、デバイスが複数のデバイス グループからの設定を保持できる場合があります。

次のシナリオで、デバイスが複数のデバイス グループからの設定を保持する方法について説明します。

処理 1：デバイス A をデバイス グループ 1（DG1）に割り当てる。

結果：デバイス A は、DG1 のすべての設定を自動的に継承します。

処理 2：デバイス A をデバイス グループ 2（DG2）に割り当てる。これで、デバイス A は、2 つのデバイス グループ（DG1 と DG2）に属することになります。

結果：デバイス A は DG2 からすべての設定を継承しますが、DG1 にも属しています。

処理 3：DG1 の標準時間帯をアメリカのニューヨークに変更する。

結果：デバイス A の時間帯がアメリカのニューヨークに変化しますが、デバイスは DG2 からの他のすべての設定を維持します。

このシナリオでは、デバイス A の設定は、DG1 と DG2 の組み合せです。デバイスがどのデバイス グループ設定を継承するかを指定する場合は、「グループ設定の変更」（P.3-8）に説明されている変更機能を使用できます。

基準グループの操作

基準グループは、複数のデバイスに一貫した WAAS サービスを設定するために使用する特殊な種類のデバイス グループです。WAAS Central Manager GUI は、次の 3 種類の基準グループを提供しています。

- ファイル：複数のデバイスに一貫したファイル サービスを設定します。
- アクセラレーション：複数のデバイスに一貫したアプリケーション ポリシーを設定します。
- プラットフォーム：複数のデバイスに一貫したプラットフォーム設定を設定します。

たとえば、すべてのデバイスに同一のアプリケーション ポリシー集合を入れたい場合は、カスタム ポリシーと変更されたポリシーを含むアクセラレーション基準グループを作成することを推奨します。すべてのデバイスをこのグループに割り当てると、デバイスは自動的にグループからアプリケーション ポリシーを継承します。ポリシーを変更する必要があるときは、アクセラレーション基準グループに対して変更を行うと、変更がすべてのデバイスに伝達されます。

デバイスは、複数の基準グループに属することができます。ただし、特定のサービスには、ある時点でただ 1 つの基準グループしか関連付けることができません。

基準グループは、デバイス グループと同じように設定し、同じように動作します。最初に基準グループを作成し、次にそのグループ用のサービス設定を構成または変更し、最後にデバイスをグループに割り当てます。

ここでは、次の内容について説明します。

デフォルトの基準グループの設定

表 3-2 に、WAAS システムに付属しているデフォルトの基準グループを設定するプロセスについて説明します。

表 3-2　デフォルトの基準グループを設定するためのチェックリスト

作業	追加情報と手順
1. 基準グループ設定をカスタマイズする。	新しくアクティブになったデバイスが自動的にグループに参加するかという基準グループの基本的なプロパティを変更します。 詳細については、「基準グループ設定のカスタマイズ」（P.3-11）を参照してください。
2. 基準グループ用のサービス設定を構成する。	基準グループに固有のサービス設定を構成します。このグループに属するすべてのデバイスが、自動的にこれらの設定を継承します。 詳細については、「基準グループのサービス設定の構成」（P.3-12）を参照してください。
3. 基準グループにデバイスを割り当てる。	デバイスがグループ設定を継承できるように、グループにデバイスを割り当てます。 詳細については、「設定デバイス グループへのデバイスの割り当て」（P.3-5）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。

基準グループ設定のカスタマイズ

基準グループを設定するには、最初に次のことを決定する基本設定をカスタマイズします。

- 新しくアクティブになったすべてのデバイスが、自動的に基準グループに参加するかどうか
- この基準グループで非表示にする設定ウィンドウ

基準グループ用の設定をカスタマイズするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、カスタマイズする基準グループを 3 つの中から 1 つ選択します。

- [File Services] 基準グループを選択する場合は、[Configure] > [File Services] > [Baseline Group] の順に選択します。

- [Acceleration Services] 基準グループを選択する場合は、[Configure] > [Acceleration] > [Baseline Group] の順に選択します。
- [Platform Services] 基準グループを選択する場合は、[Configure] > [Platform] > [Baseline Group] の順に選択します。

選択したサービスの [Selecting the (File、Acceleration、または Platform) Baseline Group] ウィンドウが表示されます。

（注） この基準グループにデバイス グループが割り当てられていない場合は、[Selecting the File Baseline Group] ウィンドウが表示されます。このウィンドウからこの基準グループに割り当てるデバイス グループを選択し、このセクションの残りの手順へ進みます。

ステップ 2　基準グループの名前を変更するには、提供されるフィールドに新しい名前を入力します。

名前は、システムで他の基準グループからこの基準グループを区別できる固有の名前でなければなりません。名前にはスペースや特殊文字は使用できません。

ステップ 3　[Automatically assign all newly activated devices to this group] チェックボックスを選択して、新しくアクティブにしたすべてのデバイス用のデフォルトのデバイス グループとして、この基準グループを設定します。すべてのデバイスがこの基準グループの設定を継承する場合だけ、このチェックボックスを選択してください。

ステップ 4　[Comments] フィールドに、この基準グループを説明するコメントを入力します。

入力したコメントは [Device Group] ウィンドウに表示されます。

ステップ 5　[Pages configured for this device group] 矢印をクリックして、WAAS Central Manager GUI でこの基準グループ用に設定されたウィンドウのリストを表示します。

ステップ 6　次の手順を完了して、この基準グループ用のナビゲーション ペインをカスタマイズします。

a. [Select pages to hide from table of contents of this device group] 矢印をクリックします。

WAAS Central Manager GUI に、ウィンドウのリストが表示されます。

b. この基準グループでは非表示にするウィンドウの横にあるチェックボックスを選択します。この機能を使用して、特定の基準グループ用に不要な設定ウィンドウを非表示にします。

ステップ 7　[Submit] をクリックします。

この基準グループでは非表示にするように選択したウィンドウが、ナビゲーション ペインから消えます。

ステップ 8　次の項の説明に従って、この基準グループ用の設定を構成します。

基準グループのサービス設定の構成

各基準グループは、他の基準グループと共有しない固有のサービス設定を反映するように構成する必要があります。たとえば、ファイル基準グループを使用してデバイス上のファイル サービスを構成し、アクセラレーション基準グループを使用してアプリケーション ポリシーを構成する場合、この 2 つの基準グループを異なるサービス設定で構成する必要があります。この場合、Edge Server サービスを有効にしてファイル基準グループを構成し、カスタムまたは変更されたアプリケーション ポリシーでアクセラレーション基準グループを構成することができます。

基準グループ用のサービス設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、設定したい基準グループを 3 つの中から 1 つ選択します。

- [File Services] 基準グループを選択する場合は、[Configure] > [File Services] > [Baseline Group] の順に選択します。
- [Acceleration Services] 基準グループを選択する場合は、[Configure] > [Acceleration] > [Baseline Group] の順に選択します。
- [Platform Services] 基準グループを選択する場合は、[Configure] > [Platform] > [Baseline Group] の順に選択します。

選択したサービスの [Modifying Device Group] ウィンドウが表示されます。

ステップ 2　[Pages configured for this device group] 矢印ボタンをクリックして、すでに基準グループ用に設定されている設定ウィンドウを表示します。

この基準グループ用に設定されたページのリストが表示されます。これが新しい基準グループである場合、またはこの基準グループ用にページが設定されていない場合、リストには何も表示されません。

ステップ 3　ナビゲーション ペインを使用して、この基準グループ用に変更する各設定ウィンドウへ移動します。

設定中の基準グループによっては、次の設定ウィンドウを変更する場合があります。

- [Configure] >[File Services]：ファイル基準グループ用のサービス設定を構成します。
- [Configure] >[Acceleration]：アクセラレーション基準グループ用のサービス設定を構成します。
- [Configure] >[General Settings]：プラットフォーム基準グループ用のサービス設定を構成します。

この基準グループ用に設定ウィンドウが設定されていない場合は、ウィンドウの一番上に「There are currently no settings for this group」メッセージが表示されます。

ステップ 4　設定ウィンドウで必要な変更を行った後、[Submit] をクリックします。

変更を適用すると、[Modifying Device Group] ウィンドウの [Pages configured for this device group] の下に、変更した設定ウィンドウが表示されます。

ステップ 5　「設定デバイス グループへのデバイスの割り当て」（P.3-5）の説明に従って、この新しいグループにデバイスを割り当てます。

サービス用の基準グループの切り替え

WAAS Central Manager GUI を使用すると、基準グループに関連するデバイス グループを切り替えることができます。基準グループを切り替えるときは、基準グループの代わりになる通常のデバイス グループを選択する必要があります。切り替え中に、選択したデバイス グループは基準グループに変換され、削除した基準グループは通常のデバイス グループに変換されます。

サービスから基準グループを削除し、その代わりに別の基準グループを関連付けるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File] または [Acceleration] または [Platform] > [Baseline Group] を選択します。

選択したサービス用の [Modify Device Group] ウィンドウが表示されます。

ステップ 2　タスクバーの [Switch Group] アイコンをクリックします。WAAS Central Manager GUI は、次のメッセージを返します。

```
This action will remove this device group as the Baseline Group for this service. You can
then select another device group or create a new one to the Baseline Group for this
service. Do you wish to Continue?
```

ステップ 3　サービスからデバイス グループを削除するには、[OK] をクリックします。

WAAS Central Manager GUI は、選択したサービスの [Selecting the Baseline Group] ウィンドウを表示します。

ステップ 4　次のように、[Select a Device Group to be the Baseline Group] ドロップダウン リストからデバイス グループを選択するか、[Create New Device Group] オプションを選択します。

- そのサービスの基準グループとしてデバイス グループを選択すると、そのデバイス グループの [Modify Device Group] ウィンドウへ移動します。
- [Create New Device Group] オプションを選択すると、[Create New Device Group] ウィンドウへ移動します。

デバイス位置の操作

WAAS Central Manager を使用すると、WAAS デバイスに関連付けることができる位置を作成できます。最初にデバイスをアクティブにするとき、デバイスを位置に割り当てます。デバイスを位置に割り当てる主な目的は、WAAS デバイスをそれが存在する場所で識別できるようにすることです。デバイスはそれが属する位置から設定を継承しないため、位置はデバイス グループとは異なります。

特定の場所のすべてのデバイスからのデータを集計したレポートを表示できます。詳細については「位置レベル レポート」（P.16-36）を参照してください。

「デバイス プロパティの変更」（P.9-1）の説明に従って、最初にデバイスをアクティブにするとき、デバイスを位置に割り当てます。

次の作業を実行すると、位置を操作できます。

- 「位置の作成」（P.3-14）
- 「位置の削除」（P.3-15）
- 「位置ツリーの表示」（P.3-15）

位置の作成

新しい位置を作成する、または既存の位置を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Locations] を選択します。[Locations] ウィンドウが表示されます。

ステップ 2　タスクバーで、[Create New Location] アイコンをクリックします。

[Creating New Location] ウィンドウが表示されます

ステップ 3　[Name] フィールドに、位置の名前を入力します。

名前には、文字、数字、ピリオド、ハイフン、アンダースコア、およびスペースを使用できます。

ステップ 4　[Parent Location] ドロップダウン リストから、親の位置（または [None]）を選択します。

親のない位置は、レベル 1 位置です。レベル 1 の親を持つ位置は、レベル 2 位置になり、以下同様です。親の位置（または [None]）を選択し、[Submit] をクリックして設定を保存すると、位置のレベルが表示されます。

ステップ 5　（任意）[Comments] フィールドに、位置に関するコメントを入力します。

ステップ 6　[Submit] をクリックします。

ステップ 7　位置を変更するには、[Locations] ウィンドウへ進み、変更する位置の名前の横にある [Edit] アイコンをクリックします。

ステップ 8　この位置にデバイスを割り当てます。詳細については、「デバイス プロパティの変更」（P.9-1）を参照してください。

位置の削除

必要に応じて、アクティブにした WAAS デバイスのルート位置以外の位置を削除できます。

（注）　位置にデバイスが割り当てられている場合は、デバイスを別の位置に割り当ててから元の位置を削除することができます。

位置を削除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Locations] を選択します。[Locations] ウィンドウが表示されます。

ステップ 2　削除する位置の横にある [Edit] アイコンをクリックします。

[Modifying Location] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Delete Location] アイコンをクリックします。位置を削除するかどうかを確認するプロンプトが表示されます。

ステップ 4　削除することを決定するには、[OK] をクリックします。位置が削除されます。

位置ツリーの表示

位置ツリーは、各位置に親を割り当てたときに設定したネットワーク トポロジを表します。WAAS Central Manager GUI は、WAAS ネットワークに設定されている位置の関係をグラフィック表現で表示します。

位置ツリーを表示するには、[My WAN] > [Manage Locations] を選択します。タスクバーで、[Location Trees] ボタンをクリックします。図 3-2 に示すように、位置ツリーが表示されます。

図 3-2　位置ツリーの例

CHAPTER 4

トラフィック代行受信の設定

この章では、IP および TCP ヘッダー情報に基づいて IP ベース ネットワークのすべての TCP トラフィックを代行受信し、Wide Area Application Engine（WAE）へリダイレクトする Wide Area Application Service（WAAS）ソフトウェア サポートについて説明します。この章では、トラフィックを WAE へ透過的にリダイレクトするための Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）、Policy-Based Routing（PBR; ポリシーベース ルーティング）、およびインライン モードの使用方法について説明します。

（注）この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従い、WAAS ネットワークの基本的な初期インストールと設定を完了しておく必要があります。この章で使用されている CLI コマンドの詳細なコマンド構文情報については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。WCCP の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』および『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章の構成は、次のとおりです。

要求リダイレクション方式

WAAS ネットワークでは、最適化、冗長性の除去、および圧縮のために、ブランチ オフィスのクライアントとデータセンターのサーバ間のトラフィックを WAE へリダイレクトできます。トラフィックは、ルータに設定されているポリシーに基づいて代行受信され、WAE へリダイレクトされます。要求を透過的にローカル WAE へリダイレクトするネットワーク要素は、WCCP バージョン 2 または PBR を使用してトラフィックを透過的にローカル WAE へリダイレクトするルータまたはレイヤ 4 ～ 7 のスイッチ（たとえば、Catalyst 6500 シリーズ Content Switching Module（CSM）や Application Control Engine（ACE））です。代わりに、Cisco WAE Inline Network Adapter のある WAE でインライン モードを使用して、トラフィックを直接代行受信できます。

WAAS ネットワークでは、次の 2 つのモードでトラフィックを代行受信できます。

- トランスペアレント モード（WCCP または PBR）
  - アプリケーション トラフィックの場合、クライアント アプリケーションやクライアント/サーバ アプリケーションの設定を変更する必要はありません。無差別 WCCP モードでは、ネットワーク要素によって、アプリケーション トラフィックが透過的にローカル WAE へリダイレクトされます。

    （注） TCP 無差別モード サービス（WCCP サービス 61 と 62）には、Common Internet File System（CIFS）プロトコルなどの、転送として TCP を使用するすべてのプロトコルが含まれています。ルータと WAE で TCP 無差別モードを有効にした場合、CIFS が TCP 上で実行されているために、CIFS トラフィックは Cisco WAE にリダイレクトされます。

  - CIFS トラフィックに対して、ブランチ オフィスの WAE は、システム設定とポリシーに基づいてトラフィックを高速化します。ファイル サーバが切断モードで設定され、ネットワークが切断されない限り、トランスペアレント モードで動作中の WAE がファイル サーバ名をアドバタイズすることはありません。クライアントとファイル サーバ間の CIFS トラフィックは、クライアント本来のサーバへの到達機能に依存します（直接 IP トラフィック経由または名前解決）。TCP 無差別モードで、ルータは CIFS トラフィック（TCP ポート 139 または 445）をローカルの WAE へリダイレクトし、そこで、その WAE のローカル ポリシーに基づいて最適化されます。ローカル プリント サービスが設定されている場合、このモードでブランチ オフィスの WAE によって提供される唯一のネーム サービスは、ローカル プリント サービスのためのものです。

    （注） ブランチ オフィスの WAE は、前述のトランスペアレント モードか、後述の非トランスペアレント モードのいずれかで動作します。このモードは、WAE で設定され、その WAE で高速化されるすべてのファイル サーバに適用されます。設定されたモードは Central Manager と WAE で保存されます。

- 非透過（明示）モード（WCCP バージョン 2 では無効、レガシー ファイル サービス モードを使用している場合に CIFS トラフィックだけを適用可能）
  - CIFS トラフィックでは、Edge WAE は、ブランチ オフィスのネットワークにファイル サーバ名を公開します。この公開された名前は、NetBIOS 名との競合のために、元のファイル サーバ名と同じではない場合があります。クライアント コンピュータは、Edge WAE によって公開された名前を使用して、高速化されたファイル サーバからドライブをマップする必要があります。これは、デフォルトのモードです。

  - アプリケーション トラフィック（CIFS ではない）に対して、トラフィックを最適化するために代行受信のあるフォームが必要です。WCCP、PBR、インライン モード、または CSM/ACE リダイレクションを設定する必要があります。そうでない場合は、CIFS ではないトラフィックは WAAS で最適化できません。

- インライン モード

  WAE は物理的にも透過的にもクライアントとルータ間のトラフィックを代行受信します。このモードを使用するには、Cisco WAE Inline Network Adapter が搭載された WAE を使用する必要があります。

表 4-1 に、WAAS でサポートされる透過トラフィック代行受信方式を示します。

表 4-1　サポートされる透過トラフィック代行受信方式

方式	説明
WCCP バージョン 2	アプリケーション トラフィックと Wide Area File Services（WAFS; 広域ファイル サービス）トラフィックの透過的な代行受信に使用します。ブランチ オフィスとデータセンターで、トラフィックをローカル WAE へ透過的にリダイレクトするために使用します。WCCP 対応ルータまたはレイヤ 3 スイッチが、透過的にトラフィックを代行受信し、ローカル WAE へリダイレクトします。 ブランチ オフィスのルータと WAE およびデータセンターのルータと WAE で、WCCP を設定する必要があります。詳細については、「WCCP を使用した WAE への透過的な TCP トラフィックのリダイレクション」（P.4-4）を参照してください。
PBR	ブランチ オフィスで、広域アプリケーションの最適化に使用します。ブランチ オフィスのルータは、PBR を使用してクライアントとサーバ両方のトラフィックを透過的に代行受信し、同じブランチ オフィスに存在する WAE へルーティングするように設定されます。 データセンターでは、データセンター アプリケーションの最適化に使用します。データセンター ルータや L3 スイッチは、透過的に代行受信したり、クライアントとサーバをデータセンター内で WAE にルーティングしたりするために、PBR を使用するように設定されている場合があります。ただし、PBR は、複数の WAE 間のロード バランシング（WCCP が行うような）をサポートしません。Cisco CSM や ACE などのロード バランサを使用した場合でもロード バランシングをサポートしません。「ポリシーベース ルーティングを使用した WAE へのすべての TCP トラフィックの透過的なリダイレクション」（P.4-34）を参照してください。
インライン	アプリケーション トラフィックと WAFS トラフィックの透過的な代行受信に使用します。「TCP トラフィックの透過的な代行受信へのインライン モードの使用」（P.4-43）を参照してください。
ACE または CSM	データセンターの最適化のために、Cisco Application Control Engine（ACE）または Catalyst 6500 シリーズ Content Switching Module（CSM）がデータセンターにインストールされています。ACE と CSM は、データセンター内の複数の WAE 間のトラフィックの代行受信とロード バランシングの両方を行うことができます。

WAE デバイスがトラフィックの最適化を阻止するファイアウォールの背後にある場合、WAN 経由のピア WAE 間の通信に directed モードを使用できます。詳細については、「directed モードの設定」（P.5-16）を参照してください。

WCCP を使用した WAE への透過的な TCP トラフィックのリダイレクション

WAAS ソフトウェアは、WCCP 標準バージョン 2 を使用して、リダイレクションを実行します。WCCP バージョン 2 の主な機能は、次のとおりです。

- WCCP サービスあたり最大 32 の WAE
- 複数のルータをサポート
- WAE と WCCP 対応ルータとの間のプロトコル メッセージのマルチキャスト
- プロトコル パケットの認証
- 非 HTTP トラフィックのリダイレクション
- パケット リターン（Generic Routing Encapsulation （GRE; 総称ルーティング カプセル化）を含む。WAE は、リダイレクトされたパケットを拒否し、転送するルータへ戻すことができる）
- L2 キャッシング（ルータと GRE を使用）およびマスキング（ロード バランシングを改善するため）
- 複数の転送方式
- サービス グループ内でのパケット分散方式のネゴシエーション
- WAE とサービス グループ間のコマンドとステータスの交換

（注） WCCP は、IPv4 ネットワークだけで動作します。

WAAS ソフトウェアは、WCCP TCP 無差別モード サービス（サービス 61 および 62）をサポートしています。この WCCP サービスでは、ルータと WAE で WCCP バージョン 2 が動作している必要があります。

TCP 無差別モード サービスとは、すべての TCP トラフィックを代行受信し、ローカル WAE へリダイレクトする WCCP サービスです。

また、WAAS ソフトウェアは、サービス パスワード、WAE フェールオーバー、フローの保護、代行受信 ACL、および固定的バイパスもサポートしています。

Cisco 2600、Cisco 2800、Cisco 3600、Cisco 3700、Cisco 3800、および Cisco 7600 シリーズ ルータがサポートされ、Cisco WAE で使用するために WCCP バージョン 2 サポートを手動で設定し、有効にすることができます。Catalyst 6000 および Catalyst 6500 シリーズ スイッチも、WCCP バージョン 2 をサポートしています。

（注） 2500、2600、および 3600 ルータを含む多数の従来の Cisco ルータは、Integrated Services Router（ISR）モデル 2800 および 3800 などの新しいルーティング プラットフォームに比べ、処理性能とメモリ レベルがはるかに劣っています。そのため、WCCPv2 または PBR を使用すると、ルータの CPU 使用率が高くなり、動作が不安定になる場合があります。これらのルータで動作するように WAAS を設定できますが、新しいルーティング プラットフォームと同じレベルのパフォーマンスや拡張性は実現できません。Cisco ISR は、ブランチ オフィス用のルーティング プラットフォームとして最適です。

WAE がサービス グループから除外されるなど動作が不安定になる場合は、ユーザ、サーバ、WAE、および WAN と接続するルータのすべての物理インターフェイスで、公平キュー方式、重み付き公平キュー方式、または速度制限を有効にしてください。公平キュー方式はサブインターフェイスでは設定できず、入力と出力の両方の物理インターフェイスで設定する必要があります。LAN や WAN インターフェイスでは、同様の公平さを提供する公平キュー方式以外のキュー方式がすでに設定されており、それで十分です。

さらに、ルータの LAN 側インターフェイスで受信できる帯域幅を制限すると、ルータのインターフェイス キューの混雑が軽減され、パフォーマンスが向上し、CPU 使用率が低下します。ルータの最大インターフェイス帯域幅を WAN 帯域幅容量の 10 倍以下に設定します。たとえば、WAN リンクが T1 である場合、LAN インターフェイスと WAE の LAN インターフェイス帯域幅を 10 × T1 = 10 × 1.544 Mbps（約 15 Mbps）に制限する必要があります。詳細については、Cisco IOS マニュアル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。

WCCP を設定するためのガイドライン

WCCP バージョン 2 を使用して WAE で透過的なリダイレクションを設定するときは、次の一般的なガイドラインに従ってください。

- 可能な場合は常に、着信インターフェイスでパケットを代行受信し、リダイレクトします。
- WAE をクライアントおよびサーバとして同一の VLAN またはサブネットに配置する場合は、WCCP GRE または汎用 GRE を出力方式として使用します。IP 転送出力方式を使用する場合は、このトポロジは利用できません。
- ブランチ オフィスの WAE は、パケットを暗号化したり圧縮したりせずに、内部 Network Address Translation（NAT; ネットワーク アドレス変換）ファイアウォール（存在する場合）の一部として動作する必要があります。
- Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータを使用している場合は、パケット転送方式としてレイヤ 2 リダイレクションを使用します。他の Cisco シリーズ ルータを使用している場合は、レイヤ 3 GRE パケット リダイレクションを使用します。
- Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）と WCCP を使用する場合、WAE のデフォルト ゲートウェイとして HSRP または Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）を設定し、HSRP グループのルータのプライマリ アドレスに WAE WCCP ルータリストを設定します。
- CEF は、WCCP に必要であり、ルータで有効になっている必要があります。
- ネットワークのクライアント側にブランチ オフィスの WAE を配置し、ルータを経由するクライアント側のパケット数を最小限に抑えます。
- Denial of Service（DoS; サービス拒絶）攻撃を避けるため、WCCP パスワードを使用します。詳細については、「ルータ上のサービス グループ パスワードの設定」（P.4-11）を参照してください。
- 新たに実装した場合は、WCCP リダイレクト リストを使用して、クライアントまたはサーバの読み込みを制限します。詳細については、「ルータ上の IP アクセス リストの設定」（P.4-10）を参照してください。
- WAE は、複数の WCCP 対応ルータからリダイレクトされたパケットを受け入れるように設定する必要があります。
- WAAS CLI または WAAS Central Manager GUI から、WAE で設定できる WCCP 設定とサービスのリストを迅速に表示できます。WAAS CLI から、**wccp** EXEC コマンドと疑問符（?）を入力します。WCCP バージョン 2 が有効になっている WAE の出力例は、次のとおりです。

```
WAE(config)# wccp ?
   access-list      Configure an IP access-list for inbound WCCP encapsulated traffic
   flow-redirect    Redirect moved flows
```

```
  router-list       Router List for use in WCCP services
  shutdown          Wccp Shutdown parameters
 tcp-promiscuous  TCP promiscuous mode service
  version           WCCP Version Number
```

- 基本 WCCP を設定するには、ネットワーク内の少なくとも 1 台のルータと、トラフィックをリダイレクトしたい WAE で、WCCP サービスを有効にする必要があります。WAE を起動し稼動させるために、使用可能な WCCP 機能またはサービスをすべて設定する必要はありません。ブランチ オフィスとデータセンターのルータおよび WAE で基本的な WCCP 設定を完了する方法の例については、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。
- WCCP バージョン 1 は Web トラフィック（ポート 80）しかサポートしていないため、ルータと WAE が WCCP バージョン 1 の代わりに WCCP バージョン 2 を使用するように設定する必要があります。
- ルータで WCCP を有効にしたら、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、ルータと WAE で TCP 無差別モード サービス（WCCP サービス 61 および 62）を設定する必要があります。
- WAE を TCP 無差別モードで機能させるには、WAE で WCCP バージョン 2 サービス 61 および 62 を使用します。この 2 つの WCCP サービスは、WAE では標準名の tcp-promiscuous で表されます。
- ルータと WAE の両方で CLI コマンドを使用して基本的な WCCP を設定できます。また、CLI コマンドを使用して WCCP 用にルータを設定し、WAAS Central Manager GUI を使用して WAE 上の基本的な WCCP を設定できます。『*Cisco Wide Area Application Services Quick Configuration Guide*』に記載されている設定例では、CLI を使用して WAE 上の基本的な WCCP を設定しています。

  最初のブランチ オフィスの WAE とデータセンターの WAE では、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、WAAS CLI を使用して WCCP の基本的な初期設定を完了することを推奨します。

  WCCP 透過リダイレクションが正常に動作していることを確認したら、WAAS Central Manager GUI を使用して集中的にこの基本的な WCCP 設定を変更したり、WAE（または WAE のグループ）用に追加の WCCP 設定（ロード バランシングなど）を構成したりすることができます。詳細については、「WAE 用の WCCP 設定の管理」（P.4-12）を参照してください。
- ルータ上の基本的な WCCP を構成したら、「WCCP 対応ルータでの高度な WCCP 機能の設定」（P.4-7）の説明に従って、ルータ上の高度な WCCP 機能を構成できます。
- 一貫性を確保するため、個々のデバイスでなく、デバイス グループ単位で WCCP 設定を行うことを推奨します。デバイス グループには、単一の WCCP サービス ファームの WAE だけが含まれるようにします。WCCP 設定は、ファームごとに異なる必要がある場合があるため、複数のファームに属する WAE が含まれているデバイス グループを使用して WCCP を設定しないようにしてください。
- 新規ルータを既存の WCCP ルータ ファームまたは WCCP サービス グループに追加すると、新規ルータは既存の接続をリセットします。WCCP がパス リダイレクションおよび割り当てを再確立するまで、パケットはクライアントに（予期したとおりに）直接送信されます。
- ルータは、WAE に設定されているリダイレクトおよび返信方式をサポートしている必要があります。設定されている方式がルータでサポートされていない場合、WAE は WCCP ルータ ファームに参加しません。ファーム内で異なるルータが組み合されている場合、設定されている方式をサポートするルータだけがファームに参加します。
- WAE の設定が異なる場合でも、厳密な割り当て方式のオプション（[Only Use Selected Assignment Method] チェックボックスをオンにする）を使用して WAE を設定していない限り、WAE はルータがサポートする割り当て方式にデフォルト設定されます。厳密な割り当て方式のオプションを使用するときは、WAE に設定されている割り当て方式がルータでサポートされている場合に限り、WAE はファームに参加します。

- WAE は、ファームに設定されているすべてのルータに認識されている場合に限り、WCCP ファームに参加します。いずれかのルータにリンク障害があれば、ファームは再設定され、WAE はファームから除去されます。

ファイル サーバ アクセス方式に関するガイドライン

一部のファイル サーバには複数のネットワーク インターフェイスがあり、複数の IP アドレスを通じて到達できます。このようなサーバの場合は、ブランチ オフィスの WAE の WCCP 受容リストに、使用できるすべての IP アドレスを追加する必要があります。このようにすると、クライアントは、登録されていない IP アドレスを使用してブランチ オフィスの WAE をバイパスすることがなくなります。WAE Device Manager GUI は、すべての IP アドレスを表示します。

一部のファイル サーバには、複数の NetBIOS 名と、ただ 1 つの IP アドレスがあります。このようなサーバの場合は、クライアントが UNC パス内の IP アドレス（つまり、¥¥server¥share でなく ¥¥IP_address¥share）を使用して接続すると、WAAS は、WAE Device Manager GUI でサーバ リストからこの IP アドレスと一致する最初の NetBIOS 名を選択します。WAAS は、その名前を使用して、データセンターの WAE とファイル サーバ間の NetBIOS ネゴシエーションを実行し、キャッシュにリソースを作成します。ファイル サーバが複数の NetBIOS 名を使用して（設定が異なる場合がある）仮想サーバを表し、プライマリ サーバ名として識別される 1 つの NetBIOS 名を持つ場合は、サーバ リストの先頭にその名前を置きます。

WCCP 対応ルータでの高度な WCCP 機能の設定

この項では、WAAS ネットワークで要求を WAE へ透過的にリダイレクトする WCCP 対応ルータで、高度な WCCP バージョン 2 機能を設定する方法について説明します。

- 「WCCP サービス グループをサポートするためのルータの設定」（P.4-7）
- 「ルータ上の IP アクセス リストの設定」（P.4-10）
- 「ルータ上のサービス グループ パスワードの設定」（P.4-11）
- 「ルータ上のループバック インターフェイスの設定」（P.4-12）
- 「WCCP コントロール パケット向けのルータ QoS の設定」（P.4-12）

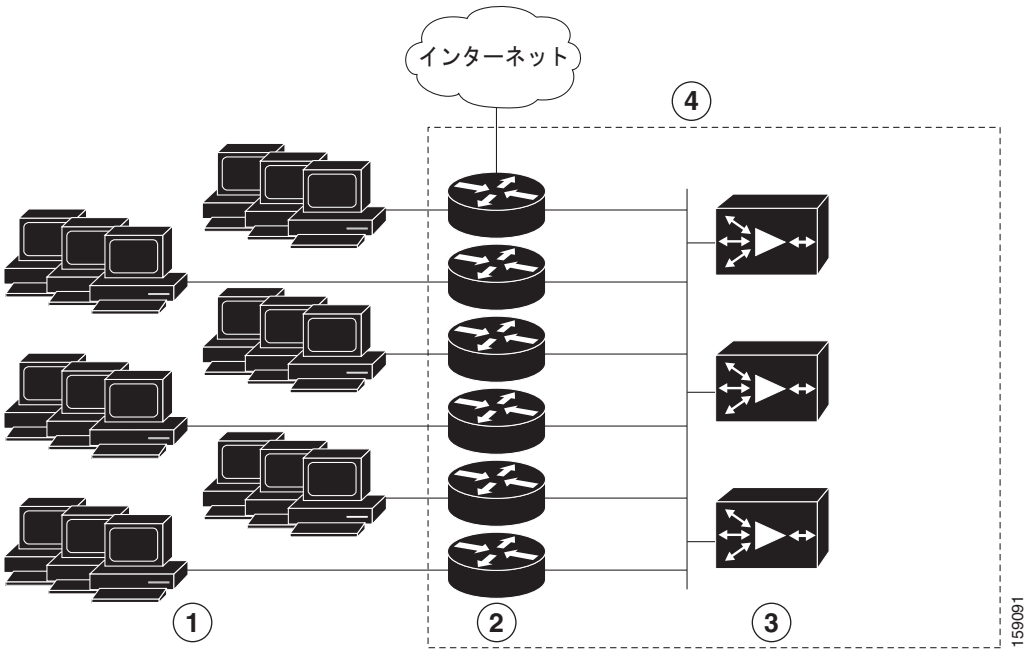
（注）　この項の手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従ってルータに基本 WCCP を設定しておく必要があります。

WCCP サービス グループをサポートするためのルータの設定

WCCP バージョン 2 を利用すると、WAE グループ内の 1 組のブランチ オフィスの WAE を複数のルータに接続することができます。グループ内の WAE、および同じ WCCP サービスを稼動している WAE グループに接続されている WCCP バージョン 2 対応ルータのことを「*サービス グループ*」と呼びます。

WCCP バージョン 2 対応ルータは、ブランチ オフィスの WAE との通信を通じて、使用できるブランチ オフィスの WAE を識別します。ルータとブランチ オフィスの WAE は相互に識別し、WCCP バージョン 2 を使用してサービス グループを形成します（図 4-1 を参照）。

図 4-1　WCCP バージョン 2 でのサービス グループ



1	ファイル サービスを要求するクライアント	3	ブランチ オフィスの WAE
2	Cisco ルータ	4	WAE サービス グループ

ブランチ オフィスの WAE のグループが存在する場合は、すべての WCCP バージョン 2 対応ルータによって認識され、最も小さい IP アドレスを持つ WAE がブランチ オフィスのリード WAE になります。

次の手順で、サービス グループ内の 1 つのブランチ オフィスの WAE をリードとして指定する方法を説明します。

1. 各ブランチ オフィスの WAE に、WCCP 対応ルータのリストが設定されます。

   複数の WCCP 対応ルータがグループにサービスを提供できます（最大 32 台のルータを指定できます）。サービス グループ内の使用可能なルータはいずれも、グループ内の各ブランチ オフィスの WAE にパケットをリダイレクトできます。

2. 各ブランチ オフィスの WAE は、自身が存在することを、ルータ リストの各ルータに通知します。ルータは、サービス グループ内のブランチ オフィスの WAE のビューとともに応答を返します。

3. グループ内のすべてのブランチ オフィスの WAE の間でビューの一貫性が確保されると、1 台のブランチ オフィスの WAE がブランチ オフィスのリード WAE として指定され、パケットをリダイレクトするために WCCP 対応ルータを配置する必要があるという内容のポリシーが設定されます。

ブランチ オフィスのリード WAE は、グループのブランチ オフィスの WAE にトラフィックを割り当てる方法を指定します。グループの WCCP 対応ルータがパケットをリダイレクトし、グループ内のブランチ オフィスの WAE がそれぞれの負荷をより適切に管理できるように、割り当て情報は指定されたブランチ オフィスのリード WAE からサービス グループ全体に渡されます。

WCCP は、サービス グループを使用して、グループ内の WCCP バージョン 2 対応ルータとブランチ オフィスの WAE 用の WAAS サービスを定義します。また、WCCP は、リアルタイムでこれらのグループへクライアント要求をリダイレクトします。

同じ WCCP サービス グループのメンバーとして設定され、リダイレクトされたトラフィックを受信するポートはすべて、次の特性を共有します。

- ポートはすべて、WAAS Central Manager GUI（「WAE 用の WCCP サービス マスクの表示または変更」（P.4-24））または **wccp service-number mask** グローバル コンフィギュレーション コマンドで設定されているとおり、同じハッシュまたはマスク パラメータを持ちます。
- 個々のポートの WCCP バージョン 2 サービスを、個別に停止または開始することはできません（WCCP バージョン 2 の制限）。

WCCP バージョン 2 対応ルータで、WCCP サービス グループのサポートを有効または無効にするには、**ip wccp** グローバル コンフィギュレーション コマンドを使用します。WCCP サービス グループのサポートを制御するためのルータの機能を削除するには、このコマンドの **no** 形式を使用します。

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*]

次の例は、マルチキャスト構成において、224.10.10.1 というグループ アドレスを持つルータ グループ内のルータで TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）を有効にする方法を示しています。

```
Router(config)# ip wccp 61 group-address 224.10.10.1
Router(config)# ip wccp 62 group-address 224.10.10.1
```

ユニキャスト構成の場合は、TCP 無差別モード サービスを次のように有効にします。

```
Router(config)# ip wccp 61
Router(config)# ip wccp 62
```

マルチキャスト構成の各 WAE で、次のように、WCCP ルータ リスト内のマルチキャスト アドレスだけを設定します。

```
WAE(config)# wccp router-list 1 224.10.10.1
```

ユニキャスト構成の各 WAE で、サービス グループ内のルータごとに 1 つずつ、WCCP ルータ リストの複数のユニキャスト ルータ アドレスを設定します。

さらに、マルチキャスト構成で、各ルータが 1 つのインターフェイスでマルチキャスト パケットを受信するように設定する必要があります。次のようなコマンドを使用します。

```
Router(config)# interface vlan817
Router(config-subif)# ip wccp 61 group-listen
Router(config-subif)# ip wccp 62 group-listen
Router(config-subif)# ip pim dense-mode
```

最後に、各ルータが適切なインターフェイスの着信方向で WCCP 代行受信に対応するように設定する必要があります。次のようなコマンドを使用します。

```
Router(config)# interface fa1/0.40
Router(config-subif)# ip wccp 61 redirect in
Router(config-subif)# exit
Router(config)# interface serial0
Router(config-subif)# ip wccp 62 redirect in
Router(config-subif)# exit
```

オンラインになった WAE は WCCP サービス グループに加入します。新しい WAE がサービス グループに参加すると、負荷を分散するためのハッシュ テーブルが更新され、以前は WAE1 へ転送されていたトラフィックを WAE2 へ転送できます。WAE2 に、すでに接続されているクライアントのパケットを WAE1 へ転送させるには、フローの保護を有効にする必要があります。その最終結果として、単一のセッションに属する要求はすべて、同じ WAE によって処理されます。管理者がフローの保護を無効にしている場合は、WAE をサービス グループに追加したときに、一部の既存のクライアントが切断されてしまうことがあります。

WAE をサービス グループから削除すると、そのクライアントは切断されます（そのクライアントを再接続すると、別の WAE に到達するか、使用可能な場合は元のファイル サーバに到達します）。

WAAS は、ブランチ オフィスの WAE が故障した場合にクライアントを他のブランチ オフィスの WAE に再接続して、WAE フェールオーバーをサポートしています。ブランチ オフィスの WAE は、故障すると、WCCP キープアライブの発行を停止します（高い CPU 負荷が続く場合も、その結果、キープアライブが失われ、フェールオーバーを実行するケースとして見なされる場合があります）。ルータは、キープアライブの消失を検出し、サービス グループからブランチ オフィスの WAE を削除します。指定したブランチ オフィスの WAE は、ブランチ オフィスの WAE の削除を反映して WCCP 設定ハッシュ テーブルを更新し、残っているブランチ オフィスの WAE の間でそのバケットを分割します。ブランチ オフィスのリード WAE が故障すると、指定した新しいブランチ オフィスのリード WAE が選択されます。クライアントは切断されますが、別のブランチ オフィスの WAE が以後の接続を処理します。

一旦、TCP のフローがブランチ オフィスの WAE によって代行受信されると、障害時の動作は、非トランスペアレント モードで発生する障害時の動作と同じになります。たとえば、データセンターの WAE の障害およびファイル サーバの障害のシナリオは、WCCP 代行受信を使用した場合の障害と異なる方法で処理されるわけではありません。

（注）　新規ルータを既存の WCCP ルータ ファームまたは WCCP サービス グループに追加すると、新規ルータは既存の接続をリセットします。WCCP がパス リダイレクションおよび割り当てを再確立するまで、パケットはクライアントに（予期したとおりに）直接送信されます。

ルータ上の IP アクセス リストの設定

オプションで、ルータに定義された Access Control List（ACL; アクセス コントロール リスト）に基づいて、トラフィックを WAE からリダイレクトするようにルータを設定できます。これらのアクセス リストのことを「リダイレクト リスト」と呼びます。

（注）　可能な場合は WCCP 対応ルータ上のリダイレクト リストを使用することを推奨します。トラフィック代行受信を制御するには、これが最も効率的な方法です。WAE 上では固定バイパス リストまたは代行受信 ACL も設定できますが、これらの 2 つの内、代行受信 ACL を使用することを推奨します。これは、代行受信 ACL の方が柔軟性が高く、パススルー接続についてより優れた統計情報が得られるためです。WAE の代行受信 ACL を設定する方法の詳細については、「代行受信アクセス コントロール リストの設定」（P.4-29）を参照してください。固定バイパス リストの設定方法については、「WAE 用の固定バイパス リストの設定」（P.4-28）を参照してください。また第 8 章「WAAS デバイス用の IP ACL の作成および管理」に示すとおり、WAE 上でインターフェイス ACL を設定して、WAE への管理アクセスを制御することもできます。

ルータで設定されるリダイレクト リストは最もプライオリティが高く、次に WAE の固定バイパス リストまたは代行受信 ACL となります。WAE で設定される代行受信 ACL は、WAE で定義されている任意のアプリケーション定義ポリシーよりも優先されます。

WCCP バージョン 2 対応ルータには、WAE への TCP トラフィックのリダイレクションを許可または拒否するためのアクセス リストを設定できます。次の例では、ルータは、次の条件に一致するトラフィックを WAE へリダイレクトしません。

- ホスト 10.1.1.1 から発信され、任意のその他のホスト宛てである
- 任意のホストから発信され、ホスト 10.255.1.1 宛てである

```
Router(config)# ip wccp 61 redirect-list 120
Router(config)# ip wccp 62 redirect-list 120
```

```
Router(config)# access-list 120 deny ip host 10.1.1.1 any
Router(config)# access-list 120 deny ip any host 10.1.1.1
Router(config)# access-list 120 deny ip any host 10.255.1.1
Router(config)# access-list 120 deny ip host 10.255.1.1 any
Router(config)# access-list 120 permit ip any
```

明示的に許可されないトラフィックは、暗黙的にリダイレクションが拒否されます。**access-list 120 permit ip any** コマンドは、明示的にすべてのトラフィック（任意の送信元から任意の宛先宛て）の WAE へのリダイレクションを許可しています。コマンドが入力された順番で条件に照合されるため、グローバル **permit** コマンドが最後に入力するコマンドとなります。

パケットのリダイレクションをアクセス リストに一致したパケットだけに制限するには、**ip wccp redirect-list** グローバル コンフィギュレーション コマンドを使用します。このコマンドを使用して、どのパケットを WAE へリダイレクトする必要があるかを指定します。

WCCP が有効になっていても、**ip wccp redirect-list** コマンドを使用しない場合は、WCCP サービスの条件に一致するすべてのパケットが WAE へリダイレクトされます。**ip wccp redirect-list** コマンドを指定すると、アクセス リストに一致するパケットだけがリダイレクトされます。

WCCP を使用して WAE への要求のリダイレクションを開始するために必要なコマンドは、**ip wccp** グローバル コンフィギュレーション コマンドと **ip wccp redirect** インターフェイス コンフィギュレーション コマンドだけです。WCCP 対応ルータのインターフェイスが、該当する発信パケットかどうかをチェックし、パケットを WAE へリダイレクトするように指定するには、**ip wccp redirect** インターフェイス コンフィギュレーション コマンドを使用します。**ip wccp** コマンドが有効でも、**ip wccp redirect** コマンドが無効の場合、WCCP 対応ルータは WAE を認識しますが、この WAE を使用しません。

名前または番号でアクセス リストを指定するには、グループ メンバシップの基準を定義する **ip wccp group-list** グローバル コンフィギュレーション コマンドを使用します。次の例では、**access-list 1 permit 10.10.10.1** コマンドを使用して、WCCP サービス グループへの参加を許可する WAE の IP アドレスを定義しています。

```
Router(config)# ip wccp 61 group-list 1
Router(config)# ip wccp 62 group-list 1
Router(config)# access-list 1 permit 10.10.10.1
```

ヒント　WCCP サービス ファームに複数の WAE が存在している場合は、ロード バランシング割り当てによって、パケットは WAE デバイス自体に送信され、そこからファーム内の別の WAE にリダイレクトされる可能性があり、それによってパフォーマンスが低下します。影響を受けるトラフィックには、管理トラフィック、レガシー CIFS トンネル トラフィックなどがあります。この状況を避けるため、WAE IP アドレスに送信されるトラフィックをリダイレクトから除外する WCCP リダイレクト リストを設定することを推奨します。

アクセス リストの詳細については、Cisco IOS IP アドレッシングおよびサービス ソフトウェアのマニュアルを参照してください。

ルータ上のサービス グループ パスワードの設定

セキュリティを目的として、WCCP バージョン 2 対応ルータとそれにアクセスする WAE に、サービス パスワードを設定できます。正しいパスワードが設定されたデバイスだけに、WCCP サービス グループへの参加が許可されます。

ルータで、WCCP 対応ルータのグローバル コンフィギュレーション モードから次のコマンドを入力して、TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）用のサービス グループ パスワードを指定します。

```
Router(config)# ip wccp 61 password [0-7] password
Router(config)# ip wccp 62 password [0-7] password
```

必須の *password* 引数は、WCCP バージョン 2 対応のルータに、指定したサービス グループから受信したメッセージに MD5 認証を適用するよう指示する文字列です。認証によって受け入れられなかったメッセージは、廃棄されます。*0* ～ *7* は、パスワードの暗号化に使用される HMAC MD5 アルゴリズムを示すオプションの値です。この値は、WAE の暗号化パスワードが作成されたときに生成されます。7 の値を推奨します。オプションの *password* 引数は、ルータと WAE 間の接続のセキュリティを確立するために、HMAC MD5 値と組み合わされるオプションのパスワード名です。

WAAS Central Manager GUI を使用して WAE（またはデバイス グループ）上のサービス グループ パスワードを指定する方法については、「WAE 上の WCCP 設定の表示と変更」（P.4-18）を参照してください。

ルータ上のループバック インターフェイスの設定

ルータのループバック インターフェイスのなかで最も大きい IP アドレスが、WAE へのルータの識別に使用されます。

次の例では、ループバック インターフェイスを設定し、コンフィギュレーション モードを終了し、実行中の設定を起動時設定として保存しています。

```
Router(config)# interface Loopback0
Router(config-if)# ip address 111.111.111.111 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

WCCP コントロール パケット向けのルータ QoS の設定

バージョン 4.2.1 以降、WAAS は Differentiated Services Code Point（DSCP）値 192 でマーキングした WCCP コントロール パケットを送信します（これ以前は、パケットはマーキングされませんでした）。ルータがこのプライオリティ値を活用するには、DSCP 値を調べて、ルータの Multilayer Switching（MLS; マルチレイヤ スイッチング）の Quality of Service（QoS）ポートの信頼状態を設定し、トラフィックを分類する必要があります。ルータを適切に設定するには、WAE に接続されたインターフェイス上で、インターフェイス コンフィギュレーション モードで **mls qos trust dscp** コマンドを使用します。

WAE 用の WCCP 設定の管理

ここでは、次の内容について説明します。

- 「WAE 用の WCCP ルータ リストの設定の変更」（P.4-25）
- 「WAE からの WCCP ルータ リストの削除」（P.4-26）
- 「WAE での追加 WCCP ルータ リストの定義」（P.4-26）
- 「WCCP の正常なシャットダウンのための WAE の設定」（P.4-28）
- 「WAE 用の固定バイパス リストの設定」（P.4-28）
- 「代行受信アクセス コントロール リストの設定」（P.4-29）

（注）　この項の手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、ルータと WAE 上の WCCP バージョン 2 と TCP 無差別モード サービスの基本的な設定など、WAAS ネットワークの初期設定が完了しているものとします。

ロード バランシングと WAE

WCCP 対応の複数の WAE を展開して、動的なロード バランシングを実装することで、サービス グループ内の個々の WAE に転送される負荷の調整を行うことができます。WCCP 対応ルータが受信した IP パケットは、WAE へ転送する必要のある要求であるかどうかがチェックされて判断されます。パケット検査には、要求と定義されたサービス基準との照合が含まれます。これらのパケットは、どの WAE（存在する場合）がリダイレクトされたパケットを受信する必要があるかを判断するために、ルータ上の処理ルーチンへ渡されます。

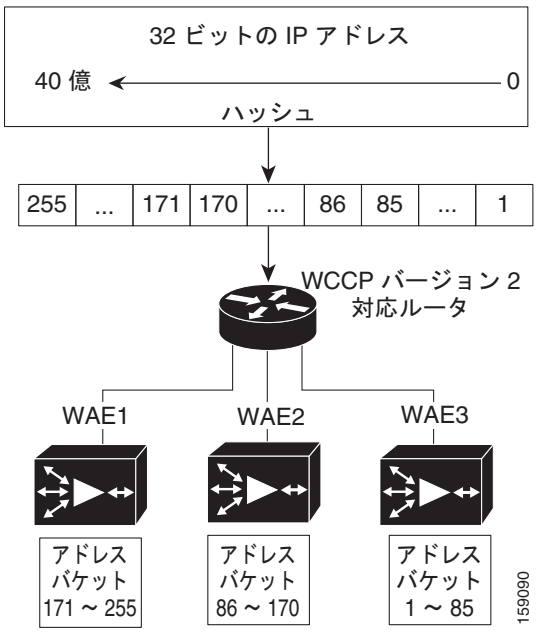
ロード バランシングを使用すると、複数の WAE 間でトラフィックの負荷バランスを取ることができます。ロード バランシングを使用すると、過負荷の WAE から、使用可能な容量を持つその他の WAE へ負荷を移動して、WAE に割り当てられている一連のハッシュ アドレス バケットを調整することができます。この技術では、ハッシュとマスキングの 2 つの割り当て方式が使用されます。

*割り当て方式*とは、WCCP が WAE 間に負荷を分散するために使用する方式を示します。2 つのロード バランシング割り当て方式は、ハッシュとマスキングです。マスク ロード バランシング方式が指定されていない場合は、ハッシュ ロード バランシング方式が使用されます。これは、デフォルトの方式です。

WCCP は、ハッシュ関数に基づくリダイレクションをサポートします。ハッシュ キーは、パケットの送信元または送信先 IP アドレスをベースにすることができます。WAFS の場合、ロード バランシング ハッシュは、送信元 IP アドレス（デフォルト）、送信先 IP アドレス、またはその両方に基づいています。

ハッシュ関数は、送信元 IP アドレスを使用して、パケットの割り当て先となるアドレス バケットを取得します。その後、この送信元アドレス バケットは、存在する WAE の数と WAE の使用状況に応じて、特定の WAE にマッピングされます（図 4-2 を参照）。

図 4-2　IP アドレスのハッシュによるロード バランシング



（注）　WAE が処理しないパケットは、送信元の同じルータへ返信されます。ルータは、正式にリダイレクトされたパケットを受信した場合に、それを再度リダイレクトする必要がないことを認識します。

送信先 IP アドレス ハッシュは、1 つの WAE が 1 つの特定のファイル サーバだけをキャッシュするように保証します。この方式により、ローカル一貫性ディレクティブをファイル サーバの内容に安全に適用できるため（内容に他の共同作業が行われていない場合）、パフォーマンス、WAN リンク、およびディスクの使用率が向上します。ただし、ファイル サーバ上のアクティビティは一様でないため、この方式では、負荷が不均等に分散されることがあります。

送信元 IP アドレスのハッシュの方が、ブランチ オフィスの WAE 上のキャッシュ間のセッション分散に適しています。この方式は、パフォーマンス、WAN リンク、およびディスク使用率に影響する場合があります（ロード バランシングを適用するときに考慮する必要がある要因については、前の説明を参照してください）。また、クライアントの IP アドレスが変更されると（DHCP 環境で動作中に発生する場合がある）、クライアントが別のブランチ オフィスの WAE に切り替えることがあります。これにより、クライアントのワーキング セットが新しいキャッシュに取り込まれるまで、クライアントのパフォーマンスが低下することがあります。

クライアント IP アドレスに基づくハッシュは、ハッシュ キーの局所性を一切保証しません。たとえば、同じサブネットのクライアント（同じ内容を共有し、同じ内容に対して共同作業している可能性がある）に、2 つの異なるハッシュ番号が割り当てられ、それによってそれぞれ異なるブランチ オフィスの WAE にリダイレクトされる場合もあれば、異なるサブネットのクライアントに同じハッシュ番号が割り当てられ、同じブランチ オフィスの WAE にリダイレクトされる場合もあります。クライアント IP アドレスに基づくハッシュは、一貫性を保証します。たとえば、同じ IP アドレスを使用しているクライアントは、同じブランチ オフィスの WAE にリダイレクトされます。

サービス ファームの中で、使用できる WAE の間で負荷を分散するハッシュ テーブルを作成するために、リード WAE が選択されます。リード WAE は、均等にバケットを分散します。送信元 IP アドレスがハッシュされ、その結果割り当てられたバケットに従い、パケットを処理する WAE が決定されます（フローの保護が、セッション全体を通じて同じ WAE が使用されるように保証します）。

WCCP は、マスク値割り当てによるリダイレクションをサポートします。この方式は、マスキングに依存して、リダイレクションに関する決定を下します。決定は、WCCP 対応ルータの特殊なハードウェア サポート機能を使用して実行されます。この方式は、ハードウェアがパケットを交換するため、非常に効率的です。

（注）　マスキング方式は、Catalyst 3750、Catalyst 4500、および Catalyst 6500 シリーズ スイッチ、Cisco 7600 シリーズ ルータ、および Cisco ASR 1000 シリーズ ルータとのロード バランシングに使用できます。また、IOS バージョン 12.4(20)T 移行を実行している Cisco 2800、3800、および 7200 シリーズ ルータとのロード バランシングに使用することもできます。

マスキングは、明示的に指定する必要があります。パケットの送信先または送信元の IP アドレスに基づいた 2 つのマスキングの値を指定できます。WAAS の場合、デフォルトのマスク値は、送信先 IP アドレスに基づいています。デフォルト値を使用するか、特定のマスク値を指定することで、マスクを有効にすることができます。デフォルトのマスク値（16 進数表記）は、次のとおりです。

- dst-ip-mask= 0x0
- src-ip-mask= 0xF00

最大 7 ビットのマスク値が指定できます。WAE は、2^7（128）通りの組み合せのテーブルを作成し、WAE の IP アドレスをその組み合せに割り当て、このテーブルを WCCP 対応ルータに送信します。ルータは、このテーブルを使用して、サービス グループ内のすべての WAE にトラフィックを分散します。WCCP サービス パラメータと一致する各パケットがこのテーブルと比較され、対応する WAE へ送信されます。

異なるマスクを持つ WAE がサービス ファームに存在している場合、ルータとの双方向通信を確立する最初の WAE によってファームのマスクが決定します。その他の WAE はいずれも、同一のマスクが設定されない限り、ファームに参加できません。

マスキングは通常、Catalyst 6500 シリーズ スイッチなど、ハードウェアによって加速化されるスイッチの WCCP リダイレクト機能を利用できるデータセンターで使用されます。データセンターにおけるロード バランシングの目的は、所定のクライアント サブネット（通常はブランチと同等）から開始されたすべての接続を 1 つのデータセンターの WAE に集め、Data Redundancy Elimination（DRE）の圧縮パフォーマンスを向上させることにあります。また、Catalyst 6500 シリーズ スイッチでのマスク割り当てには、ACL Ternary Content Address Memory（TCAM）が使用されます。WCCP リダイレクト リストと組み合せると、マスク割り当てに TCAM の大部分が使用される場合があります。TCAM の使用量を最小限に抑えるには、ケア ビットの少ないマスクを使用します。

WAAS バージョン 4.2.1 以降について上記の検討事項を考慮した結果、デフォルト マスクは src-ip-mask 0x1741 および dst-ip-mask 0x0（4.1x バージョン）から src-ip-mask 0xF00 および dst-ip-mask 0x0（4.2.1 以降のバージョン）に変更されました。現在のソース IP マスクは、旧バージョンのマスクが使用していた 6 ケア ビットではなく 4 ケア ビットだけを使用します。

通常のデータセンター WCCP 代行受信設定では（WAN のサービス 61 を使用した入力代行受信、LAN のサービス 62 を使用して入力代行受信）、このマスクでは /24 ブランチ サブネットのロード バランシングを行えます（/24 サブネットの最後の 4 ビットを抽出します）。1 つのブランチ サブネットからの接続は、1 つのデータセンター WAE へ固定されます。ネットワークにさまざまな IP アドレスが分散している場合（/16 サブネットなど）、アドレスの /16 ネットワーク部分からビットを抽出するマスク（src-ip-mask 0xF0000 など）を設定する必要があります。同様に、ブランチが他のブランチより多くのトラフィックを発生する場合、アドレスのホスト部分からもビットを抽出するマスク（0xF03 など）を作成できます。

パケット転送方式

WCCP 対応ルータは、次の 2 つのパケット転送方式のいずれかを使用して、代行受信した TCP セグメントを WAE へリダイレクションします。

- 総称ルーティング カプセル化（GRE）：WAE へのパスに多数のルータが存在する場合でも、パケットはその WAE に到達できます。
- レイヤ 2 リダイレクション：パケットは、レイヤ 2（MAC 層）で交換され、WAE に到達できます。

表 4-2 で、パケット転送方式について説明します。

表 4-2　パケット転送方式

パケット転送方式	ロード バランシング方式：ハッシュ	ロード バランシング方式：マスキング
GRE（レイヤ 3）	パケット リダイレクションは、ルータ ソフトウェアによって完全に処理されます。	パケット リダイレクションは、ルータ ソフトウェアによって処理されます。パケット転送方式として GRE が使用されている場合に、マスク割り当てを使用することは推奨しません。
レイヤ 2 リダイレクション	最初にリダイレクトされたパケットは、ルータ ソフトウェアによって処理されます。それ以降にリダイレクトされたパケットはすべて、ルータ ハードウェアによって処理されます。	すべてのパケットが、ルータ ハードウェアによって処理されます（特殊なハードウェアが必要となるため、現時点では、Catalyst6500 シリーズ スイッチまたは Cisco7600 シリーズ ルータだけでサポートされています）。

リダイレクション モードは、ブランチ オフィスの WAE によって制御されます。WCCP サービス グループに最初に加入したブランチ オフィスの WAE が、転送方式（GRE またはレイヤ 2 リダイレクション）と割り当て方式（ハッシュまたはマスキング）を決定します。「*マスク割り当て*」という用語は、WCCP レイヤ 2 Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）入力リダイレクションを指しています。

WCCP 出力リダイレクションにおいてマスキングを選択すると、ブランチ オフィスの WAE は、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）および Policy Feature Card（PFC; ポリシー フィーチャ カード）で使用されているオリジナルのハードウェア アクセラレーションに戻ります。

たとえば、WCCP はパケットをフィルタして、リダイレクトされたパケットのうち、どれがブランチ オフィスの WAE から戻されたパケットか、どれが戻されたパケットではないかを判別します。ブランチ オフィスの WAE でパケットを処理する必要がないと判断されたため、WCCP は戻されたパケットをリダイレクトしません。WCCP バージョン 2 は、ブランチ オフィスの WAE が処理しないパケットを、送信元のルータへ返信します。

ここでは、次の内容について説明します。

- 「パケットの拒否と返信の理由」（P.4-17）
- 「パケット転送方式としてのレイヤ 3 GRE」（P.4-17）
- 「パケット転送方法としてのレイヤ 2 リダイレクション」（P.4-18）

パケットの拒否と返信の理由

ブランチ オフィスの WAE は次の理由により、パケットを拒否して返信します。

- パケット処理が逆効果となるような特定の状況、たとえば、IP 認証がオンになっている場合などを、WAE が除外しているため。
- ブランチ オフィスの WAE によってキャッシュするように設定されていないサーバ宛ての CIFS パケットを、ブランチ オフィスの WAE が受信したため（WAFS レガシー モードのみ）。
- WAE で固定バイパス リストまたは代行受信 ACL を設定したため。

（注）　パケットは、WCCP 対応ルータとブランチ オフィスの WAE との間の接続の送信元にリダイレクトされます。使用されている Cisco IOS ソフトウェアのバージョンによって、この送信元は発信インターフェイスの場合もあれば、ルータ IP アドレスの場合もあります。後者の場合は、ブランチ オフィスの WAE のルータ リストに WCCP 対応ルータの IP アドレスが格納されていなければなりません。ルータ リストの詳細については、「WAE 用の WCCP ルータ リストの設定の変更」（P.4-25）を参照してください。

Cisco Express Forwarding（CEF）は、WCCP に必要であり、ルータで有効になっている必要があります。

また、WCCP を使用して、複数のルータ（ルータ リスト）が特定の WCCP サービス（たとえば、CIFS リダイレクション）をサポートするように設定することができます。

パケット転送方式としてのレイヤ 3 GRE

WCCP 対応ルータは、代行受信した要求を Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用してパケットをカプセル化することができます。このパケット転送方式では、WAE へのパスに複数のルータが存在する場合でも、パケットはその WAE に到達できます。パケット リダイレクションは、ルータ ソフトウェアによって完全に処理されます。

GRE は、WCCP 対応ルータでデータグラムを IP パケットにカプセル化し、その後 WAE にリダイレクトします（トランスペアレント プロキシ サーバ）。この中間の宛先で、データグラムはカプセル化が解除され、その後、WAAS ソフトウェアによって処理されます。要求をローカルに処理できない場合は、関連する WAE が元のサーバに接触して要求を完了できます。その場合、内部データグラムから見て、元のサーバへのトリップ分は 1 ホップと見なされます。通常、GRE を使用してリダイレクトされたトラフィックは、GRE トンネル トラフィックと呼ばれます。GRE を使用した場合、リダイレクションはすべて、ルータ ソフトウェアによって処理されます。

WCCP リダイレクションを使用する場合、ルータの接続の宛先ポート上の WCCP は有効になっているため、Cisco ルータは TCP SYN パケットを宛先へ転送しません。その代わり、WCCP 対応ルータが GRE トンネリングを使用してパケットをカプセル化し、この WCCP 対応ルータからリダイレクトされたパケットを受け入れるように設定された WAE へそのパケットを送信します。

リダイレクトされたパケットを受信すると、WAE は次のように処理します。

1. パケットから GRE レイヤを取り除きます。
2. 次のように、リダイレクトされたこのパケットを受け付けて内容の要求を処理するか、リダイレクトされたパケットを拒否するかを決定します。
   a. WAE は、要求を受け入れる必要があると判断した場合は、TCP SYN ACK パケットをクライアントへ送信します。WAE は、WAE がクライアントに見えない（透過的）ように、この応答パケットの中で送信元アドレスとして指定された元の送信先（元のサーバ）の IP アドレスを使用します。WAE は、クライアントからの TCP SYN パケットの送信先であるかのように動作します。

b. WAE は、要求を受け入れる必要がないと判断した場合は、GRE を使用して TCP SYN パケットを再度カプセル化し、WCCP 対応ルータへ返します。ルータは、WAE がこの接続に関与していないことを認識し、パケットを元の送信先（つまり、元のサーバ）へ転送します。

パケット転送方法としてのレイヤ 2 リダイレクション

レイヤ 2 リダイレクションは、WCCP 対応ルータまたはスイッチが、レイヤ 2 で WCCP トラフィック代行受信およびリダイレクションを部分的または完全に実装している内部ハードウェア スイッチを使用している場合に実現されます。このタイプのリダイレクションは、現在、Catalyst 6500 シリーズ スイッチと、Cisco 7200 および 7600 シリーズ ルータだけでサポートされています。レイヤ 2 リダイレクションでは、最初にリダイレクトされたトラフィック パケットがルータ ソフトウェアによって処理されます。それ以降のトラフィックは、ルータ ハードウェアによって処理されます。ブランチ オフィスの WAE は、特定のパケット フィールドにビット マスクを適用し、その後、マスク インデックス アドレス テーブルの形式でマスクの結果またはインデックスをサービス グループ内のブランチ オフィスの WAE にマッピングするよう、ルータまたはスイッチに指示します。リダイレクション プロセスは、スイッチング ハードウェアによって加速化されるため、レイヤ 2 リダイレクションの方がレイヤ 3 GRE に比べ効率的です。

（注）　WCCP は、WAE 上だけで使用が許可されており、リダイレクト ルータでの使用は許可されていません。WCCP が、ルータやスイッチの正常な動作を妨げることはありません。

WAE での WCCP フロー リダイレクション

フローの保護は、ブランチ オフィスの WAE がサービス グループに対して追加および削除されたときに、既存のクライアント TCP 接続に及ぼす影響を削減します。デフォルトでは、WCCP フロー リダイレクションは WAE で有効になっています。フローの保護は、ブランチ オフィスの WAE がサービス グループに対して追加および削除されたときに、既存のクライアント TCP 接続に及ぼす影響を削減します。フローの保護によってクライアントへの影響を削減できるのは、次のような状況の場合です。

- WAAS ネットワークの拡張：ブランチ オフィスの WAE がサービス グループに追加されると、以前に別のブランチ オフィスの WAE が処理していたトラフィックを、新たに起動したブランチ オフィスの WAE が受信します。さらに、そのトラフィックは、継続して処理するために、関連するブランチ オフィスの WAE へ転送されます。新しい接続は、新しいブランチ オフィスの WAE によって処理されます。
- ブランチ オフィスの WAE の交換後の障害：ブランチ オフィスの WAE で障害が発生すると、以前はそのブランチ オフィスの WAE または元のファイル サーバが処理していたトラフィックを、別のブランチ オフィスの WAE が受信できます。受信側のブランチ オフィスの WAE は、それ以前の 2 通りの使用例に従って動作します。

フローの保護を使用していない場合、上記の状況では、確立済みのクライアント接続は TCP RESET によって切断されます。フローの保護は、サポートされる WCCP サービスすべてに適用され、サービス単位で設定することはできません。

WAE 上の WCCP 設定の表示と変更

一貫性を確保するため、個々のデバイスでなく、デバイス グループ単位で WCCP を設定することを推奨します。デバイス グループには、単一の WCCP サービス ファームの WAE だけが含まれるようにします。

（注）　WCCP が設定されているデバイス グループに Cisco WAE Inline Network Adapter 搭載の WAE を追加しても、WCCP の設定はインライン WAE に自動的に適用されません。WCCP を使用するように インライン WAE を設定するには、手動で WCCP デバイス グループの設定が適用されるようにする必要があります。

（注）　この項の手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）の設定など、WAAS ネットワーク用の基本的な WCCP の設定はすでに完了しているものとします。

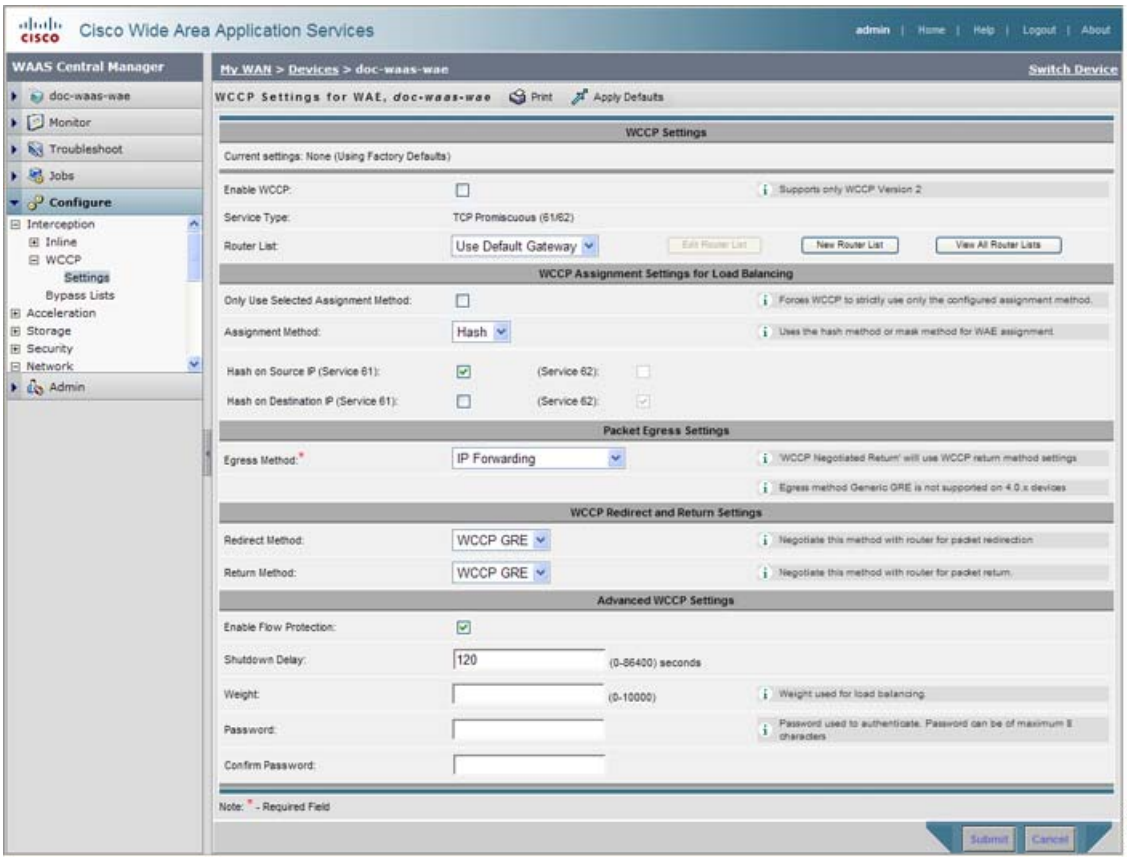
WAE（または WAE のグループ）用の WCCP の設定を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　WCCP 設定またはサービスを変更するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。[WCCP Settings] ウィンドウが表示されます（図 4-3 を参照）。

図 4-3　WCCP 設定の変更



ステップ 4　選択したデバイス（またはデバイス グループ）の現在の設定を確認します。

- 現在の設定を保持し、ウィンドウを閉じるには、[Cancel] をクリックします。
- 現在の設定を変更するには、この手順の残りの説明に従って現在の設定を変更します。

デフォルトで、WAE 上の WCCP は無効になっています。ただし、WAAS ネットワークでの WCCP の初期設定の一環として、WAE（ブランチ オフィスの WAE とデータセンターの WAE）とこれらの要求を透過的に WAE へリダイレクトするデータセンターとブランチ オフィスのルータで、WCCP バージョン 2 が有効になっている必要があります。WAAS ネットワークで基本的な WCCP 設定を実行する手順については、『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。

ステップ 5　[Enable WCCP] チェックボックスを選択して、選択したデバイス（またはデバイス グループ）の WCCP バージョン 2 を有効にします。または、チェックボックスの選択を解除して、選択したデバイス（またはデバイス グループ）の WCCP を無効にします。

（注） WCCP 環境で使用しているルータで、WCCP バージョン 2 をサポートするバージョンの Cisco IOS ソフトウェアが稼動していることを確認します。

ステップ 6　[Router List] ドロップダウン リストから適切な WCCP ルータ リスト番号を選択して、WCCP TCP 無差別モード サービスにルータ リストを関連付けます。デフォルトの [Use Default Gateway] を選択することもできます。デフォルトのルータ リストには、WAE デバイスのデフォルト ゲートウェイの単一 IP アドレスが含まれています。

ドロップダウン リストには、設定済みの WCCP ルータ リストだけが表示されます。WAAS ネットワークの初期設定の一環として、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、ブランチ オフィスの WAE 用の少なくとも 1 つの WCCP ルータ リストとデータセンターの WAE 用の別のルータ リストがすでに作成されている場合があります。WCCP ルータ リストの詳細については、次の項を参照してください。

- 「WAE 用の WCCP ルータ リストの設定の変更」（P.4-25）
- 「WAE からの WCCP ルータ リストの削除」（P.4-26）
- 「WAE での追加 WCCP ルータ リストの定義」（P.4-26）

ステップ 7　（任意）次のように、[WCCP Assignment Settings for Load Balancing] 領域で現在のロード バランシング設定を変更します。

a. 設定した割り当て方式だけを使用するように WCCP に強制するには、[Only Use Selected Assignment Method] チェックボックスを選択します。適用した後は、ハッシュ割り当てかマスク割り当てのいずれかのロード バランシング方式を選択します。

ブランチ オフィスの WAE グループ内の WCCP サービスごとにどちらか一方のロード バランシング方式（ハッシュまたはマスキング）を指定できます。

（注） [Only Use Selected Assignment Method] チェックボックスを選択した場合は、WAE で設定した割り当て方式がルータでサポートされている場合に限り、WAE は WCCP ファームに参加します。[Only Use Selected Assignment Method] チェックボックスの選択を解除した場合は、WAE がルータとは別に設定されている場合でも、WAE ではルータがサポートする割り当て方式が使用されます。

b. [Assignment Method] ドロップダウン リストから、使用する WAE ロード バランシング割り当て方式の種類を選択します（詳細については、「ロード バランシングと WAE」（P.4-13）を参照してください）。

- ハッシュ方式を使用する場合は、[Hash]（デフォルト）を選択します。次に、ステップ 8 とステップ 9 に従ってハッシュの動作を定義し、マスク設定は使用されていないのでステップ 13 に進みます。

– マスク方式を使用する場合は、[Mask] を選択します。次にステップ 10 に進み、サービス マスクを定義または編集します。

ステップ 8　（任意）送信元 IP アドレスの WCCP サービス 61 にロード バランシング ハッシュを定義するには、[Hash on Source IP] チェックボックスを選択します。このチェックボックスは、ハッシュ割り当て方式が使用されている場合だけ表示されます。

ステップ 9　（任意）宛先 IP アドレスの WCCP サービス 61 にロード バランシング ハッシュを定義するには、[Hash on Destination IP] チェックボックスを選択します。このチェックボックスは、ハッシュ割り当て方式が使用されている場合だけ表示されます。

（注）　ロード バランシングの詳細については、「ロード バランシングと WAE」（P.4-13）を参照してください。

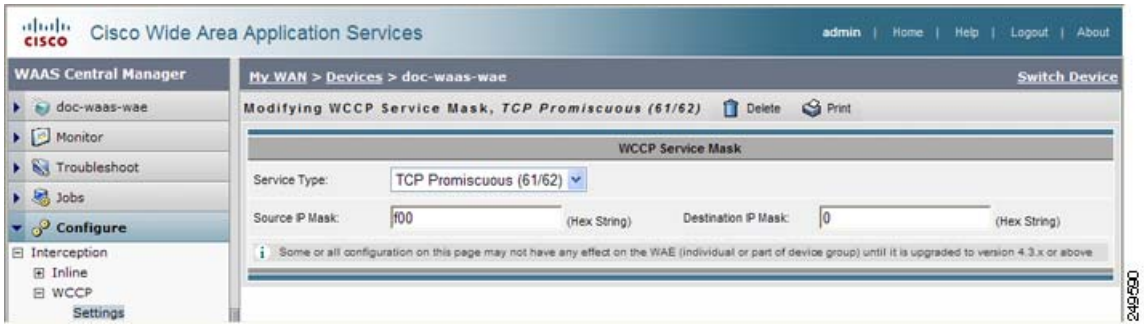
ステップ 10　（任意）選択した WCCP サービス用の既存のサービス マスクを変更するには、[Edit Mask] ボタンをクリックします。サービス マスクを変更する詳細については、「WAE 用の WCCP サービス マスクの表示または変更」（P.4-24）を参照してください（このボタンは、マスク割り当て方式が使用されている場合にだけ表示されます）。

ステップ 11　（任意）選択したサービス用に設定されているすべての WCCP サービス マスクのリストを表示するには、[View Masks Configured for All Services] ボタンをクリックします（このボタンは、マスク割り当て方式が使用されている場合にだけ表示されます）。[WCCP Service Mask Settings] ウィンドウが表示されます。

ステップ 12　[WCCP Service Mask Settings] ウィンドウから、次の作業を実行できます。

- WCCP サービス マスクを編集するには、変更するサービス マスクの横にある [Edit WCCP Service Mask] アイコンをクリックします。[Modifying WCCP Service Mask] ウィンドウが表示されます（図 4-4 を参照）。

図 4-4　WCCP サービス マスクの変更



次のように、変更したい設定の値を変更し、[Submit] をクリックします。

– [Source IP Mask] フィールドで、パケットの送信元 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x00000000 ～ 0xFE000000 です。デフォルト値は 0xF00 です。

（注）　4.1.x 以前のバージョンを実行する WAE にデフォルト マスクを適用した場合、マスクは、ソフトウェア バージョン 4.1.x 以前で設定されたデフォルト マスク（0x1741）とは異なります。

– [Destination IP Mask] フィールドで、パケットの送信先 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x0000000 ～ 0XFE000000 です。デフォルトは、0x00000000 です。

（注）　[Modifying WCCP Service] ウィンドウの [Edit Mask] ボタンをクリックして、サービス マスクを編集することもできます（図 4-3 を参照）。

- 既存の WCCP サービス マスクを削除するには、削除したいサービス マスクの横にある [Edit WCCP Service Mask] アイコンをクリックします。[Modifying WCCP Service Mask] ウィンドウが表示されます（図 4-4 を参照）。タスクバーの [Delete WCCP Service Mask] アイコンをクリックし、[Submit] をクリックします。

ステップ 13　（任意）[Packet Egress Settings] 領域の [Egress Method] ドロップダウン リストから、最適化されたパケットをルータまたはスイッチに返信するために使用する方式の種類を [IP Forwarding]（デフォルト）、[WCCP Negotiated Return]、または [Generic GRE] から選択します。出力方式の選択の詳細については、「代行受信接続の出力方法の設定」（P.4-30）を参照してください。

ステップ 14　（任意）次のように、[WCCP Redirect and Return Settings] 領域で、現在のパケット リダイレクトおよび返信方式の設定を変更します。

a. [Redirect Method] ドロップダウン リストから、使用するパケット リダイレクション（転送）方式の種類を選択します。

- レイヤ 3 GRE パケット リダイレクションを使用する場合は、デフォルトの [WCCP GRE] を選択します。
- WAE がデバイスとレイヤ 2 接続を確立していて、デバイスがレイヤ 2 リダイレクション用に設定されている場合に、WAE（またはデバイス グループ）が WCCP バージョン 2 スイッチまたはルータから透過的にリダイレクトされたトラフィックを受信できるようにするには、[L2] を選択します。

  ルータまたはスイッチ上の WCCP は、レイヤ 2 で WCCP のトラフィック代行受信およびリダイレクション機能をハードウェア内で部分的または完全に実装しているスイッチング ハードウェアを使用できます。その後、WAE が互換性のある Cisco スイッチに直接接続されている場合は、WAE はレイヤ 2 または MAC アドレス リライト リダイレクションを実行できます。リダイレクション処理は、スイッチング ハードウェアによって加速化されるため、この方式の方が、GRE を使用したレイヤ 3 リダイレクションより効率的です。WAE は、ルータまたはスイッチとのレイヤ 2 接続を保持している必要があります。スイッチと WAE 間の GRE トンネルは必須ではないため、スイッチは [L2] を選択して、カプセル化されたパケットを転送するカットスルー方式を使用できます。詳細については、「パケット転送方式」（P.4-16）を参照してください。

b. [Return Method] ドロップダウン リストから、最適化されていない（バイパスされた）パケットをルータに返信するために使用する方式の種類を選択します。

- GRE パケット返信を使用する場合は、デフォルトの [WCCP GRE] を選択します。
- パケット返信にレイヤ 2 リライトを使用する場合は、[L2] を選択します。

ステップ 15　（任意）次のように、[Advanced WCCP Settings] 領域で現在の詳細設定を変更します。

a. TCP フローを維持し、デバイス（またはデバイス グループ）が起動したときや新しいトラフィックが再割り当てされる際に過剰な負荷がかかるのを防止するには、[Enable Flow Protection] チェックボックスを選択します。詳細については、「WAE での WCCP フロー リダイレクション」（P.4-18）を参照してください。フローの保護はデフォルトで有効になります。

b. [Shutdown Delay] フィールドで、選択したデバイス（またはデバイス グループ）が WCCP の正常なシャットダウンを実行するのを待つ最大時間（秒）を指定します。デフォルトは、120 秒です。

WAE は、すべての接続が処理されるか、（この [Shutdown Delay] フィールドで指定した）WCCP バージョン 2 用の最大待ち時間が経過するまで再起動しません。

c. [Weight] フィールドで、ロード バランシングに使用される重み値を指定します。重み値の範囲は、0 ～ 10000 です。サービス グループ内の WAE の全重み値の合計が 100 以下である場合、重み値はそのまま、ロード バランシングのためにデバイスにリダイレクトされる合計負荷に対する比率となります。たとえば、重み値 10 の WAE は、すべての重み値の合計が 50 のサービス グループで合

計負荷の 10% を受け取ります。そのようなサービス グループの WAE に障害が発生した場合、別の WAE は障害前と同じ負荷パーセントを受け取り、障害のある WAE に割り当てられた負荷は受け取りません。

サービス グループで WAE のすべての重み値の合計が 101 ～ 10000 の間である場合、重み値は、サービス グループでのアクティブな WAE すべての合計の重み付けの割合として扱われます。たとえば、重み値 200 の WAE は、すべての重み値の合計が 800 のサービス グループで合計負荷の 25% を受け取ります。そのようなサービス グループの WAE に障害が発生した場合、別の WAE が障害のある WAE に割り当てられていた負荷を受け取ります。フェールオーバーの処理は、重みの合計が 100 以下の場合と異なります。

デフォルトで、重みは割り当てられず、トラフィックの負荷はサービス グループ内の WAE の間で均等に分散されます。

d. [Password] フィールドで、クラスタ内の WAE と指定したサービス用のルータ間の安全なトラフィックに使用するパスワードを指定します。クラスタ内の他のすべての WAE とルータを同じパスワードで有効にします。パスワードの長さは、8 文字以内です。[Confirm Password] フィールドに、パスワードを再入力します。

（注） CLI を使用してルータ上のサービス グループのパスワードを指定する方法については、「ルータ上のサービス グループ パスワードの設定」（P.4-11）を参照してください。

CLI から WCCP 設定を構成するには、**wccp flow-redirect**、**wccp router-list**、**wccp shutdown**、**wccp tcp-promiscuous**、および **wccp version** グローバル コンフィギュレーション コマンドを使用できます。

WAE 上の WCCP バージョン 2 の正常なシャットダウンの詳細については、「WCCP の正常なシャットダウンのための WAE の設定」（P.4-28）を参照してください。

既存の WCCP サービス用の WCCP サービス マスクの作成

WAE（または WAE のグループ）用の既存の WCCP サービス用のサービス マスクを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Devices Group]）を選択します。

ステップ 2　WCCP サービス マスクを作成したいデバイス（またはデバイスのグループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。[WCCP Settings] ウィンドウが表示されます。

ステップ 4　[Assignment Method] ドロップダウン リストから、[Mask] を選択します。

ステップ 5　[Create Mask] ボタンをクリックします。[Creating New WCCP Service Mask] ウィンドウが表示されます。

ステップ 6　[Source IP Mask] フィールドで、パケットの送信元 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x00000000 ～ 0xFE000000 です。デフォルト値は 0xF00 です。

（注）　4.1.x 以前のバージョンを実行する WAE にデフォルト マスクを適用した場合、マスクは、ソフトウェア バージョン 4.1.x 以前で設定されたデフォルト マスク（0x1741）とは異なります。

ステップ 7　[Destination IP Mask] フィールドで、パケットの送信先 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x0000000 ～ 0XFE000000 です。デフォルトは、0x00000000 です。

ステップ 8　[Submit] をクリックして、WCCP サービス マスク用の設定を保存します。

WAE 用の WCCP サービス マスクの表示または変更

WAE（または WAE のグループ）用に設定されている WCCP サービス用のサービス マスクを表示または変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Devices Group]）を選択します。

ステップ 2　WCCP サービス マスクを表示または変更するデバイス（またはデバイスのグループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。[WCCP Settings] ウィンドウが表示されます。

ステップ 4　[Assignment Method] ドロップダウン リストから、[Mask] を選択します。

ステップ 5　[Edit Mask] ボタンをクリックします。[Modifying WCCP Service Mask] ウィンドウが表示されます。

ステップ 6　[Source IP Mask] フィールドで、パケットの送信元 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x00000000 ～ 0xFE000000 です。デフォルト値は 0xF00 です。

（注）　4.1.x 以前のバージョンを実行する WAE にデフォルト マスクを適用した場合、マスクは、ソフトウェア バージョン 4.1.x 以前で設定されたデフォルト マスク（0x1741）とは異なります。

ステップ 7　[Destination IP Mask] フィールドで、パケットの送信先 IP アドレスと照合するために使用する IP アドレス マスク（16 進数）を指定します（たとえば、0xFE000000）。範囲は、0x0000000 ～ 0XFE000000 です。デフォルトは、0x00000000 です。

ステップ 8　[Submit] をクリックして、WCCP サービス マスク用の新しい設定を保存します。

設定されたマスクがファーム内の 1 つまたは複数のルータによってアドバタイズされたものと同じではないことを WAE が検出した場合、このマスクがファームへ加わることは許可されず、「Configured mask mismatch for WCCP」というメジャー アラームが出力されます。このアラームは、WAE がすでに他の WAE が設定されているファームに加わろうとし、これらの他の WAE が別のマスクを使用して設定されている場合に、出力されることがあります。ルータは、他の WAE が同じマスクをアドバタイズするのでない限り、これらの WAE がファームへ加わることを許可しません。

このアラームを解消するには、ファーム内のすべての WAE が同じマスクを使用して設定されていることを確認します。このアラームは、WAE で設定されているマスクが、ファーム内のすべてのルータのマスクに一致した場合にクリアされます。

WAE 用の WCCP ルータ リスト設定の表示

WAE（または WAE のグループ）用に現在定義されている WCCP ルータ リストのリストを集中的に表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　WCCP ルータ リストを表示するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。[WCCP Settings] ウィンドウが表示されます。

ステップ 4　[View All Router List] ボタンをクリックします。

選択したデバイス（またはデバイス グループ）用の [WCCP Router List Configurations] ウィンドウが表示されます。

WCCP ルータ リストの設定（各ルータ リストに入っている各ルータのルータ リストの番号と IP アドレス）が表示されます。

（注）　特定の WCCP ルータ リストの設定を変更するには、ルータ リストの横にある [Edit] アイコンをクリックし、表示される [Modifying Router List] を使用して、選択したルータ リストを変更します。ルータ リストを変更する詳細については、「WAE 用の WCCP ルータ リストの設定の変更」（P.4-25）を参照してください。WAE（または WAE のグループ）から WCCP ルータ リストを削除する方法については、「WAE からの WCCP ルータ リストの削除」（P.4-26）を参照してください。

CLI からルータ リストを表示するには、**show wccp routers** EXEC コマンドを使用できます。

WAE 用の WCCP ルータ リストの設定の変更

WAE（または WAE のグループ）用の WCCP ルータ リストの設定を集中的に変更する（たとえば、ルータ リストにルータを追加または削除する）には、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　ルータ リストの設定を変更するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。

[WCCP Settings] ウィンドウが表示されます。

ステップ 4　[Edit Router List] ボタンをクリックします。[Modifying WCCP Router List] ウィンドウが表示されます。

ステップ 5　選択したルータ リストにルータを追加するには、[Add Router] フィールドにルータの IP アドレスを入力し、[Add Router] ボタンをクリックします。

ステップ 6　選択したルータ リストからルータを削除するには、削除するルータの IP アドレスの横にあるチェックボックスを選択し、[Remove Router] ボタンをクリックします。

ステップ 7　[Submit] をクリックして、設定を保存します。

WAE からの WCCP ルータ リストの削除

ルータ リストを削除すると、このルータ リストを使用するように設定されていた WCCP バージョン 2 サービスも削除されます。設定されているルータ リストを削除する前に、WCCP サービスが別のルータ リストに関連付けられていることを確認してください。

WAE（または WAE のグループ）用の WCCP ルータ リストを集中的に削除する（たとえば、ルータ リストにルータを追加または削除する）には、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　WCCP ルータ リストを削除するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。[WCCP Settings] ウィンドウが表示されます。

ステップ 4　[Edit Router List] ボタンをクリックします。[Modifying WCCP Router List] ウィンドウが表示されます。

ステップ 5　ルータの IP アドレスの横にあるチェックボックスを選択して、[Remove Router] ボタンをクリックし、選択したルータ リストから表示されているすべてのルータを削除します。

ステップ 6　選択したルータ リスト（たとえば、ルータ リスト 2）からすべてのルータを削除したら、タスクバーの [Delete Router List] アイコンをクリックします

ルータ リスト設定を永続的に削除するかどうかを確認するダイアログボックスが表示されます。操作を確認するには、[OK] をクリックします。選択したデバイス（またはデバイス グループ）から、選択したルータ リストとそれに関連する WCCP サービスが削除されます。

WAE での追加 WCCP ルータ リストの定義

WAE の WCCP サービスの設定の一部として、WAE に対して TCP 無差別サービスをサポートする WCCP バージョン 2 が有効なルータのリストを作成する必要があります。WAAS CLI（**wccp router-list** グローバル コンフィギュレーション コマンド）または WAAS Central Manager GUI を使用して、WCCP ルータ リストを定義できます。

一般に、WAAS 管理者は、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、WAAS CLI を使用して WCCP ルータ リストの初期集合を定義します。WAAS CLI を使用して WCCP ルータ リストの初期設定を完了したら、WAAS Central Manager GUI を使用して、WAE 用の WCCP ルータ リスト設定を集中的に管理し、変更することを推奨します。

各 WAE には、WAE のデフォルト ゲートウェイとして定義されたルータの IP アドレスで設定されたデフォルト ルータ リスト（ルータ リスト 8）が含まれています。

（注）　この項の手順を実行する前に、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、TCP 無差別モード サービス（WCCP バージョン 2 サービス 61 および 62）の設定など、WAAS ネットワーク用の基本的な WCCP の設定はすでに完了しているものとします。

WAE（または WAE のグループ）用の追加 WCCP ルータ リストを集中的に定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

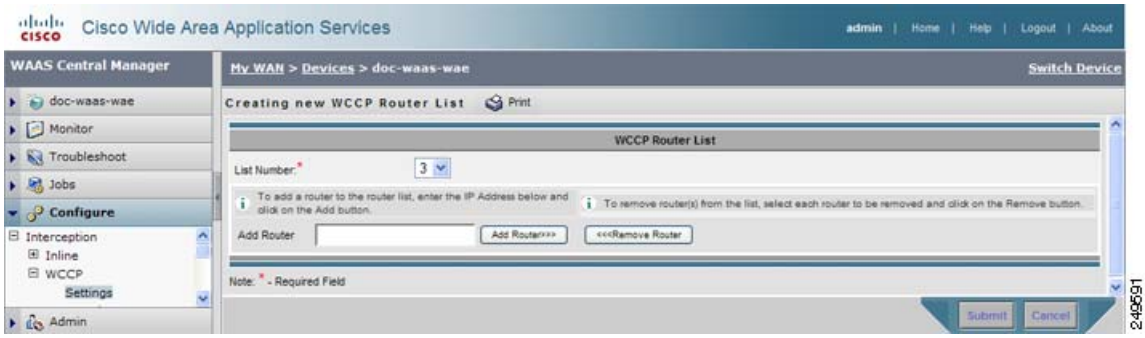
ステップ 2　WCCP ルータ リストを作成するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。[WCCP Settings] ウィンドウが表示されます。

ステップ 4　[New Router List] ボタンをクリックします。

[Creating New WCCP Router List] ウィンドウが表示されます（図 4-5 を参照）。

図 4-5　新しい WCCP ルータ リスト作成のサンプル画面



この例では、選択したデバイス（またはデバイス グループ）用にすでに 2 つの WCCP ルータ リストが定義されているため、[List Number] ドロップダウン リストであらかじめ [3] が選択されています。データセンターでは、トラフィックを透過的にデータセンターの WAE へリダイレクトするルータ リスト 1 が WCCP ルータ用にすでに定義されています。また、ブランチ オフィスでは、透過的にトラフィックを同じブランチ オフィスに存在するブランチ オフィスの WAE へリダイレクトするルータ リスト 2 が WCCP ルータ用に定義されています。

ステップ 5　[Add Router] フィールドで、ルータ リスト 3 に追加するルータの IP アドレスを指定します。

少なくとも 1 つの IP アドレスを入力する必要があります。追加するすべての IP アドレスが、ルータ リストの中で固有である必要があります。そうでない場合は、適用時にエラー メッセージが表示されます。

ステップ 6　ルータ リスト 3 に IP アドレスを追加するには、[Add] をクリックします。

このリストは、TCP 無差別モード サービス用に選択した WAE（または WAE のグループ）へ透過的にトラフィックをリダイレクトするすべての WCCP ルータの IP アドレスを表します。

ウィンドウが更新され、アドレスが番号順に表示されます。順序は、IP アドレスを入力した順序と一致しない場合があります。

ステップ 7　[Submit] をクリックして、ルータ リストを保存するか、ルータ IP アドレスに行った編集を保存します。

CLI からルータ リストを定義するには、**wccp router-list** グローバル コンフィギュレーション コマンドを使用できます。

WAE または WAE グループに WCCP ルータを作成した後は、『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、WCCP バージョン 2 が有効であり、この新しいルータ リストに含まれている WCCP ルータに設定されていることを確認します。

WCCP の正常なシャットダウンのための WAE の設定

TCP 接続の切断を防止するために、WAE は、WAE で WCCP バージョン 2 を無効にしたり、WAE をリロードしたりした後で、WCCP の正常なシャットダウンを実行します。

WAAS Central Manager GUI を使用すると、WAE で WCCP バージョン 2 を無効にすることができます。また、CLI を使用して（WAE で **no wccp version** CLI コマンドを入力して）、この作業をローカルに実行することもできます。

選択したデバイスまたはデバイス グループ用の WCCP を無効にするには、WAAS Central Manager の [WCCP Settings] ウィンドウの [Enable WCCP] チェックボックスの選択を解除します（図 4-3 を参照）。

WAE は、次のいずれかの状況になるまで起動しません。

- すべての接続がサービスを受けている。
- （[WCCP Configuration Settings] ウィンドウの [Shutdown Delay] フィールドまたは **wccp shutdown max-wait** コマンドで指定した）WCCP バージョン 2 の最大待ち時間が経過した（デフォルトは 120 秒）。

WCCP の正常なシャットダウンの間、WAE は継続して処理中のフローにサービスを提供しますが、新しいフローのバイパスを開始します。フローの数がゼロになると、リード WAE は、そのバケットを他の WAE に再度割り当ててグループから脱退します。WCCP を正常にシャットダウンすることなく WAE が機能停止またはリブートした場合は、TCP 接続が切断される可能性が残ります。

WAE の特定のポートで個々の WCCP サービスをシャットダウンできません。WAE の WCCP をシャットダウンする必要があります。WAE 上の WCCP がシャットダウンされると、WAE は自分の WCCP 構成の設定値を保存します。

WAE 用の固定バイパス リストの設定

固定バイパスを使用すると、設定可能な 1 組のクライアントとサーバ間のトラフィックのフローを WAE によってバイパス処理することができます。ブランチ オフィスの WAE に固定バイパス項目を設定すると、ルータの設定を変更することなく、トラフィックの代行受信を制御できます。ルータで、最初にトラフィックをブランチ オフィスの WAE へリダイレクトせず、トラフィックをバイパスするように、IP アクセス リストを個別に設定できます。通常、WCCP 受け入れリストは、加速化されるサーバのグループを定義します（暗黙的に、加速化されないサーバが定義されることとなります）。特定のクライアントから特定のサーバ（または特定のクライアントからすべてのサーバ）への接続を WAAS が加速化しないようにするには、固定バイパスを使用できます。

（注） WAE で固定バイパス リストまたは代行受信 ACL を使用するのではなく、可能な場合は WCCP 対応ルータの ACL を使用することを推奨します。この方法が、トラフィック代行受信を制御するのに最も効率的です。固定バイパス リストまたは代行受信 ACL の使用を決定した場合、代行受信 ACL を使用することを推奨します。これは、代行受信 ACL の方が柔軟性が高く、パススルー接続についてより優れた統計情報が得られるためです。ルータ上で ACL を設定する方法については、「ルータ上の IP アクセス リストの設定」（P.4-10）を参照してください。WAE の代行受信 ACL を設定する方法の詳細については、「代行受信アクセス コントロール リストの設定」（P.4-29）を参照してください。

WAE（または WAE のグループ）用の固定バイパス リストを集中的に設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　固定バイパス リストを作成するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Bypass Lists] を選択します。

ステップ 4　タスクバーで、[Create New WCCP/Inline Bypass List] アイコンをクリックします。[Creating new WCCP/Inline Bypass List] ウィンドウが表示されます

ステップ 5　[Client Address] フィールドに、クライアントの IP アドレスを入力します。

ステップ 6　[Server Address] フィールドに、サーバの IP アドレスを入力します。

ステップ 7　[Submit] をクリックして、設定を保存します。

CLI から固定バイパス リストを設定するには、**bypass static** グローバル コンフィギュレーション コマンドを使用できます。

固定バイパス リストの集約

各 WAE デバイスに固定バイパス リストを定義して、他の固定バイパス リストが定義されたデバイス グループに所属させることができます。

[WCCP Bypass Lists] ウィンドウの [Aggregate Settings] オプション ボタンは、各デバイスの固定バイパス リストを集約する方法を制御します。

- デバイスをそのデバイス自体および所属するデバイス グループに定義されているすべての固定バイパス リストで設定する場合は、[Yes] を選択します。
- デバイスをそのデバイス自体に定義されている固定バイパス リストだけに制限する場合は、[No] を選択します。

設定を変更すると次のメッセージが表示されます。「This option will take effect immediately and will affect the device configuration. Do you wish to continue?」。[OK] をクリックして続行します。

代行受信アクセス コントロール リストの設定

代行受信 ACL を設定することにより、すべてのインターフェイスでどの着信トラフィックが WAE デバイスにより代行受信されるかを制御できます。ACL により許可されたパケットは、WAE によって代行受信され、ACL によって拒否されたパケットは処理されずに WAE を通過します。

ブランチ オフィスの WAE に代行受信 ACL を設定すると、ルータの設定を変更することなく、トラフィックの代行受信を制御できます。ルータで、最初にトラフィックをブランチ オフィスの WAE へリダイレクトせず、トラフィックをバイパスするように、IP ACL を個別に設定できます。通常、WCCP 受け入れリストは、加速化されるサーバのグループを定義します（暗黙的に、加速化されないサーバが定義されることとなります）。代行受信 ACL を使用することで、ルータ設定の変更を望まないパイロット導入時などに、対象外のトラフィックを容易にバイパスできます。更に、フェーズにおけるさまざまな種類のトラフィックを許可して促進することで、パイロットから実稼動導入への移行を容易に行えます。

代行受信 ACL は、WCCP とインライン代行受信の両方で使用できます。

代行受信 ACL をインターフェイス ACL および WCCP ACL を併用した場合、最初にインターフェイス ACL が、2 番めに WCCP ACL が、最後に代行受信 ACL が適用されます。WAE で定義されているアプリケーション ポリシーは、すべての ACL がトラフィックをフィルタした後に適用されます。

（注）　代行受信 ACL は、固定バイパス リストとは排他的な機能です。両方のタイプのリストを同時に使用することはできません。固定バイパス リストではなく代行受信 ACL を使用することを推奨します。

代行受信 ACL を使用するには、まず ACL を定義し（第 8 章「WAAS デバイス用の IP ACL の作成および管理」を参照）、次にその ACL をデバイスに適用します。代行受信 ACL は、個々のデバイスにのみ設定でき、デバイス グループには設定できません。

WAE 向けに代行受信 ACL を設定するには、次の手順に従ってください。

ステップ 1　第 8 章「WAAS デバイス用の IP ACL の作成および管理」の手順に従って、代行受信に使用する ACL を作成します。ただし、この ACL をインターフェイスには適用しないでください。

ステップ 2　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します

ステップ 3　代行受信 ACL を使用するデバイスの名前の横にある [Edit] アイコンをクリックします。

ステップ 4　ナビゲーション ペインで、[Configure] > [Interception] > [Interception Access List] を選択します。

ステップ 5　[Interception Access List] フィールドの横にある矢印コントロールをクリックして、定義した ACL のドロップダウン リストを表示し、代行受信を適用する ACL を選択します。または、ACL の名前をフィールドに直接入力して、このページを送信した後、ACL を作成することもできます。このフィールドに入力した場合、表示される ACL のドロップダウン リストがフィルタされ、入力したテキストで始まるエントリだけが表示されます。

ACL の作成または編集が必要な場合は、このフィールドの横にある [Go to IP ACL] リンクをクリックすると、IP ACL 設定用ウィンドウが表示されます（[Configure] > [Network] > [TCP/IP Settings] > [IP ACL page] の順に選択して表示できます）。

ステップ 6　[Submit] をクリックして、設定を保存します。

CLI から代行受信 ACL を設定するには、**ip access-list** および **interception access-list** グローバル コンフィギュレーション コマンドを使用します。

接続が代行受信 ACL で通過されたかどうかを判別するには、**show statistics connection** EXEC コマンドを使用します。代行受信 ACL によるフローのパススルーは、接続タイプ「PT Interception ACL」で識別されます。

また、**show statistics pass-through** コマンドの「Interception ACL」カウンタにより、代行受信 ACL によるアクティブなパススルーと完了したパススルーの数がレポートされます。

代行受信接続の出力方法の設定

WAAS ソフトウェアでは、次の出力方式による WCCP 代行受信接続をサポートします。

- IP 転送
- WCCP GRE 返信
- 汎用 GRE

デフォルトの出力方式は IP 転送です。出力方式を設定しない場合、WAE では IP 転送を使用します。IP 転送出力方式では、WAE をクライアントおよびサーバとして同一の VLAN またはサブネットに配置することはできません。また、パケットが代行受信ルータに返信されるとは限りません。

WCCP GRE 返信および汎用 GRE 出力方式では、WAE をクライアントおよびサーバと同じ VLAN またはサブネットに配置することができます。発信パケットを GRE フレームにカプセル化することで、リダイレクションの繰り返しを防止します。Cisco IOS ルータは、これらの GRE フレームをバイパス フレームとして処理し、WCCP リダイレクションを適用しません。WCCP GRE 返信方式では、WAAS はルータ ID アドレスを GRE フレームの送信先として使用します。汎用 GRE 方式では、WAAS は WAE ルータ リストで設定されたルータのアドレスを使用します。

この技術によって、冗長なルータとルータのロード バランシングのサポートが可能となり、WAAS はフレームを送信元ルータに返信するための最善の努力をします。WAAS ネットワークに接続された複数のルータとともにこの機能を使用する場合は、たとえば、固定ルートを設定して、ルータ ID アドレスへの接続を確保する必要があります。ルータ ID は、最初のループバック インターフェイスまたは最もアクティブな物理インターフェイスのアドレスです。このアドレスは、**show wccp routers** EXEC コマンドの出力で確認できます。

WAAS は、次の論理に基づいて WCCP GRE および汎用 GRE のルータを選択します。

- WAAS ソフトウェアが DRE（データ冗長性除去）を実行して TCP フローを圧縮すると、出力されるパケット数は減少します。最適化されたデータを送信する単一パケットが、複数のルータからリダイレクトされた複数のパケットで受信されたオリジナル データを表す場合もあります。この最適化されたデータを送信するパケットは WAE から出力され、パケットを最後に WAE にリダイレクトしたルータに元のフロー方向で送信されます。
- WAE で受信された最適化データは、さまざまなルータから複数のパケットに入って送信される場合があります。WAAS は最適化されたデータをオリジナル データに戻し、複数のパケットとして送信します。オリジナル データを送信するパケットは WAE から出力され、パケットを最後に WAE にリダイレクトしたルータに元のフロー方向で送信されます。

WCCP GRE 返信方式および汎用 GRE 出力方式は類似していますが、汎用 GRE 出力方式は、Cisco 7600 シリーズ ルータまたは Catalyst 6500 シリーズ スイッチと Supervisor Engine 32 または 720 の組み合せなど、ルータまたはスイッチがハードウェアにより加速化された GRE パケット処理を行う構成で使用するように設計されています。さらに、汎用 GRE 出力方式は、ユーザがルータ上で設定する必要のある GRE トンネルを使用して、パケットを代行受信ルータに返信します（トンネルの WAE 側は自動的に設定されます）。汎用 GRE 出力方式は、WCCP GRE 代行受信方式が使用されている場合に限りサポートされます。

汎用 GRE 出力方式を使用するには、WAE 上に代行受信ルータを作成し（マルチキャスト アドレスはサポートされていません）、各ルータ上で GRE トンネル インターフェイスを設定する必要があります。ルータ上で GRE トンネル インターフェイスを設定する詳細については、「ルータ上の GRE トンネル インターフェイスの設定」（P.4-32）を参照してください。

WCCP バージョン 2 には、リダイレクト方式および返信方式をネゴシエートして代行受信接続を行う機能があります。WAAS ソフトウェアは、WCCP がネゴシエートする返信方式として WCCP GRE と WCCP レイヤ 2 をサポートしています。WCCP が WCCP レイヤ 2 返信をネゴシエートすると、WAE はデフォルトの出力方式として IP 転送を使用します。代行受信方式が WCCP レイヤ 2 に設定されていて、汎用 GRE を出力方式として設定する場合も（これらに互換性はありません）、WAE はデフォルトで IP 転送を使用します。WAE がデフォルトで IP 転送を使用する場合、WAE はマイナー アラームを記録します。これは、代行受信方式と出力方式が一致するように設定を修正したときにクリアされます。代行受信方式と出力方式が一致しない場合、**show egress methods** EXEC コマンドの出力には警告も表示されます。

CLI の設定に関係なく、WCCP バイパス トラフィックは WCCP GRE を返信方式として使用します。

WCCP ネゴシエートの返信方式および汎用 GRE 出力方式は、インライン モードの動作には適用されません。

WCCP 代行受信接続の出力方式を Central Manager GUI から設定する場合は、次の手順に従います。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　出力方式を設定するデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [WCCP] > [Settings] を選択します。[WCCP Settings] ウィンドウが表示されます（図 4-3 を参照）。

ステップ 4　[Packet Egress Settings] 領域の [Egress Method] ドロップダウン リストから、[IP Forwarding]、[WCCP Negotiated Return]、または [Generic GRE] を選択します。

ステップ 5　[Submit] をクリックします。

CLI で代行受信と WCCP GRE パケット返信による出力方式を設定するには、**egress-method** グローバル コンフィギュレーション コマンドを使用します。

```
WAE(config)# egress-method negotiated-return intercept-method wccp
```

CLI で代行受信と IP 転送による出力方式を設定するには、**egress-method** グローバル コンフィギュレーション コマンドを使用します。

```
WAE(config)# egress-method ip-forwarding intercept-method wccp
```

CLI で汎用 GRE 出力方式の代行受信および出力方式を設定するには、代行受信ルータ リストと汎用 GRE 出力方式を次のように設定します。

```
WAE(config)# wccp router-list 1 192.168.68.98
WAE(config)# egress-method generic-gre intercept-method wccp
```

ルータ リストには各代行受信ルータの IP アドレスが含まれている必要があります。マルチキャスト アドレスはサポートされていません。また、各ルータ上で GRE トンネル インターフェイスを設定する必要があります。ルータ上で GRE トンネル インターフェイスを設定する詳細については、「ルータ上の GRE トンネル インターフェイスの設定」（P.4-32）を参照してください。

特定 WAE で使用されている設定済みの出力方式を表示するには、**show egress-methods** EXEC コマンドを使用します。各接続セグメントの出力方式に関する情報を表示するには、**show statistics connection egress-methods** EXEC コマンドを使用します。

各受信代行ルータの汎用 GRE トンネル統計情報を表示するには、**show statistics generic-gre** EXEC コマンドを使用します。汎用 GRE 出力方式の統計情報を消去するには、**clear statistics generic-gre** EXEC コマンドを使用します。

ルータ上の GRE トンネル インターフェイスの設定

WAE で汎用 GRE 出力方式を使用する予定がある場合、各受信代行ルータ上で GRE トンネル インターフェイスを設定する必要があります。設定を簡易化するために、ファーム内の WAE ごとに 1 つのポイントツーポイント トンネルを作成するのではなく、ルータ上に 1 つのマルチポイント トンネルを作成することを推奨します。

ファームに WAE が 1 つしかない場合は、ポイントツーポイント トンネルを使用できますが、WAE トンネルと同一のトンネル ソースを持つトンネルがルータに設定されていないことを確認してください。

（注）　Catalyst 6500 シリーズ スイッチと Supervisor Engine 32 または 720 の組み合せでは、同じトンネル ソース インターフェイスを持つ複数の GRE トンネル（マルチポイントまたはポイントツーポイント）を設定しないでください。設定すると、スイッチの CPU の負荷が大きくなるおそれがあります。

トンネル インターフェイスには接続先であるレイヤ 3 ソース インターフェイスがあり、このソース インターフェイスは IP アドレスが WAE の代行受信ルータ リストで設定されているインターフェイスである必要があります。

ルーティング ループを回避するために、トンネル インターフェイスは WCCP 代行受信から排除する必要があります。コマンド **ip wccp redirect exclude in** を使用します。

ここでは、次の内容について説明します。

- 「マルチポイント トンネル設定」（P.4-33）
- 「ポイントツーポイント トンネルの設定」（P.4-33）

マルチポイント トンネル設定

ファーム内に 2 つの代行受信ルータと 2 つの WAE のある構成を考えてみます。各 WAE の構成は次のようになります。

```
wccp router-list 1 192.168.1.1 192.168.2.1
wccp tcp-promiscuous router-list-num-1
egress-method generic-gre intercept-method wccp
```

各ルータで WAE ファームへの単一 GRE マルチポイント トンネルを設定できます。

ルータ 1 の構成は次のようになります。

```
interface gigabitEthernet 1/1
ip address 192.168.1.1 255.255.255.0
...
interface Tunnel1
ip address 12.12.12.1 255.255.255.0
tunnel source GigabitEthernet1/1
tunnel mode gre multipoint
ip wccp redirect exclude in
end
```

ルータ 2 の構成は次のようになります。

```
interface Vlan815 1/0
ip address 192.168.2.1 255.255.255.0
...
interface Tunnel1
ip address 13.13.13.1 255.255.255.0
tunnel source vlan815
tunnel mode gre multipoint
ip wccp redirect exclude in
end
```

（注）　トンネル インターフェイスに IP アドレスをプロビジョニングすることは IP 対応にすることであり、通過パケットを処理および転送できるようになります。IP アドレスをプロビジョニングしない場合、トンネルを IP アンナンバード インターフェイスにすることで IP 対応にする必要があります。これにより、トンネルはポイントツーポイント トンネルに制限されます。

ポイントツーポイント トンネルの設定

ここでは、ルータ上のマルチポイント トンネルではなく、単一の WAE にポイントツーポイント トンネルを設定する方法について説明します。ポイントツーポイント トンネルを IP に対して有効にするには、アンナンバードにするか、IP アドレスを指定します。次のルータの設定例に、アンナンバード方式を示します。

```
interface gigabitEthernet 1/1
ip address 192.168.1.1 255.255.255.0
...
! Tunnel1 is an unnumbered point-to-point tunnel towards WAE1
interface Tunnel1
ip unnumbered GigabitEthernet1/1
tunnel source GigabitEthernet1/1
! tunnel destination is the IP address of WAE1
tunnel destination 10.10.10.10
ip wccp redirect exclude in
end
```

ポリシーベース ルーティングを使用した WAE へのすべての TCP トラフィックの透過的なリダイレクション

Cisco IOS ソフトウェア Release 11.0 で導入された PBR により、選択したパケットをネットワークの特定のパスで送信するポリシーが実装できるようになりました。

また、PBR は、Cisco IOS ソフトウェアを通じて可能になるキューイング手法と組み合せて使用すると、特定の種類のトラフィックが差別化された優先サービスを受信するようにパケットにマークを付ける方法も提供します。これらのキューイング手法は、ネットワークにルーティング ポリシーを実装するネットワーク管理者にとって、非常に強力で単純で柔軟なツールとなります。

PBR を使用すると、パケットをルーティングする前に、ルート マップを通過させることができます。PBR を設定するとき、一致基準とすべての一致節に適合する場合の処理を指定するルート マップを作成する必要があります。特定のインターフェイス上のそのルート マップ用に PBR を有効にする必要があります。指定したインターフェイスに到達し、一致節と一致するすべてのパケットが、PBR に支配されます。

1 つのインターフェイスにはただ 1 つのルート マップ タグしか指定できませんが、シーケンス番号を持つ複数のルート マップ項目を作成できます。項目は、最初の一致が現れるまで、シーケンス番号の順に評価されます。一致する項目がない場合、パケットは通常どおりにルーティングされます。

```
Router(config-if)# ip policy route--tag
```

ルート マップは、ルーティングするパケットの順序を決定します。

PBR を有効にして、一部またはすべてのパケットが WAAS を通過するルートを確立できます。WAAS プロキシ アプリケーションは、次のように、PBR がリダイレクトしたトラフィックと同じ方法で、PBR がリダイレクトしたトラフィックを受信します。

1. 次のように、ブランチ オフィスのルータ（Edge-Router1）で、関係するトラフィックを定義します。
   a. Edge-Router1 で、LAN インターフェイス（入力インターフェイス）に関係するトラフィックを指定します。

      拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別された送信先アドレスへのトラフィック）を定義します。

   b. Edge-Router1 で、WAN インターフェイス（出力インターフェイス）に関係するトラフィックを指定します。

      拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別されたリモート アドレスへのトラフィック）を定義します。
2. データセンターのルータ（Core-Router1）で、関係するトラフィックを指定します。

a. Core-Router1 で、LAN インターフェイス（入力インターフェイス）に関係するトラフィックを指定します。

拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別された送信先アドレスへのトラフィック）を定義します。

b. Core-Router1 で、WAN インターフェイス（出力インターフェイス）に関係するトラフィックを指定します。

拡張 IP アクセス リストを使用して、関係するトラフィック（すべてまたは選別されたローカル送信元アドレスから任意または選別されたリモート アドレスへのトラフィック）を定義します。

3. 次のように、ブランチ オフィスの Edge-Router1 にルート マップを作成します。
   a. Edge-Router1 の LAN インターフェイスに PBR ルート マップを作成します。
   b. Edge-Router1 の WAN インターフェイスに PBR ルート マップを作成します。
4. 次のように、データセンターの Core-Router1 にルート マップを作成します。
   a. Core-Router1 の LAN インターフェイスに PBR ルート マップを作成します。
   b. Core-Router1 の WAN インターフェイスに PBR ルート マップを作成します。
5. ブランチ オフィスの Edge-Router1 に PBR ルート マップを適用します。
6. データセンターの Core-Router1 に PBR ルート マップを適用します。
7. WAE の PBR ネクストホップが使用できるかどうかを検査するために使用する PBR 方式を決定します。詳細については、「PBR のネクストホップが使用できるかどうかを確認する方法」（P.4-40）を参照してください。

（注）　この項で参照する PBR コマンドの完全な説明については、『*Cisco Quality of Service Solutions Command Reference*』を参照してください。

図 4-6 に示すように、WAE（Edge-WAE1 と Core-WAE1）は、トラフィックの送信先と送信元から分離された帯域外ネットワークに存在する必要があります。たとえば、Edge-WAE1 は、クライアント（トラフィックの送信元）とは別のサブネットに存在し、Core-WAE は、ファイル サーバとアプリケーション サーバ（トラフィックの送信先）とは別のサブネットに存在します。さらに、ルーティング ループを防止するために第 3 のインターフェイス（別の物理インターフェイス）またはサブインターフェイスを通じてトラフィックを WAE へリダイレクトするルータに、WAE を接続する必要があります。この項目の詳細については、「第 3 のインターフェイスまたはサブインターフェイスを使用したルータと WAE の接続」（P.2-23）を参照してください。

図 4-6　PBR または WCCP バージョン 2 を使用してすべての TCP トラフィックを透過的に WAE へリダイレクトする例

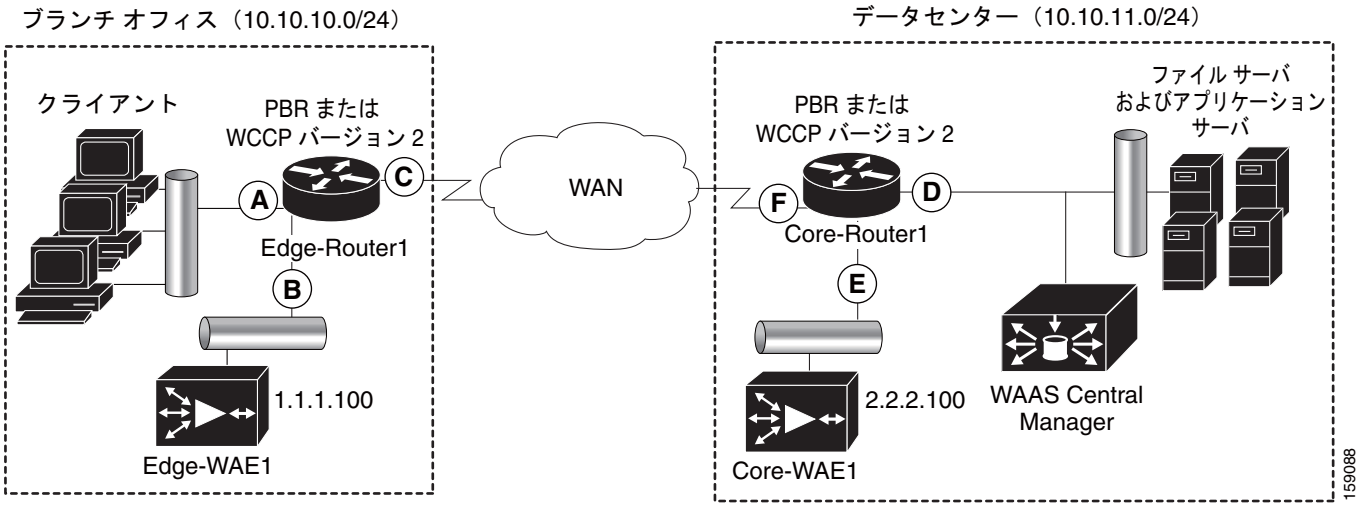


表 4-3 に、PBR または WCCP バージョン 2 を使用して、透過的にトラフィックを WAE へリダイレクトするために設定する必要があるルータ インターフェイスの概要を示します。

表 4-3　WCCP または PBR がトラフィックを WAE へリダイレクトするためのルータ インターフェイス

ルータ インターフェイス	説明
Edge-Router1	
A	発信トラフィックのリダイレクションを実行する Edge LAN インターフェイス（入力インターフェイス）。
B	Edge-Router1 の LAN ポートにない第 3 のインターフェイス（分離された物理インターフェイス）またはサブインターフェイス。ブランチ オフィスの Edge-Router1 に Edge-WAE1 を接続するために使用します。
C	着信トラフィックのリダイレクションを実行する Edge-Router1 の Edge WAN インターフェイス（出力インターフェイス）。
Core-Router1	
D	発信トラフィックのリダイレクションを実行する Core LAN インターフェイス（入力インターフェイス）。
E	Core-Router1 上の LAN ポートにない第 3 のインターフェイスまたはサブインターフェイス。データセンターの Core-Router1 に Core-WAE1 を接続するために使用します。
F	着信トラフィックのリダイレクションを実行する Core-Router1 の Core WAN インターフェイス（出力インターフェイス）。

（注） 図 4-6 では、冗長性（たとえば、冗長なルータ、スイッチ、WAE、WAAS Central Manager、およびルータ）が省略されています。

次の例は、（図 4-6 に示すように）ブランチ オフィスに 1 台の WAE、データセンターに 1 台の WAE が存在する WAAS ネットワークで、トラフィック リダイレクション方式として PBR を設定する方法を示しています。

（注）　ルータで PBR を設定するために使用するコマンドは、ルータにインストールされている Cisco IOS リリースによって変化します。ルータで使用している Cisco IOS リリース用に PBR を設定するために使用するコマンドについては、該当する Cisco IOS 設定ガイドを参照してください。

TCP トラフィックを透過的に WAE へリダイレクトするように PBR を設定するには、次の手順に従ってください。

ステップ 1　ブランチ オフィスの Edge-Router で、拡張 IP アクセス リストを使用して、LAN インターフェイス（入力インターフェイス A）に関係するトラフィックを指定します。

a. Edge-Router1 で、100 ～ 199 の範囲の拡張 IP アドレス リストを定義します。たとえば、Edge-Router1 でアクセス リスト 100 を作成します。

```
Edge-Router1(config)# ip access-list extended 100
```

b. Edge-Router1 で、この特定のインターフェイスに関係するトラフィックを指定します。

- たとえば、任意の TCP ポート上の任意のローカル送信元アドレスから任意の送信先への任意の IP/TCP トラフィック（任意のブランチ オフィス クライアント用のトラフィック）に「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 と 80 上の任意のローカル送信元アドレスから任意の送信先への IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any eq 135
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any eq 80
```

ステップ 2　ブランチ オフィスの Edge-Router1 で、拡張 IP アクセス リストを使用して、WAN インターフェイス（出力インターフェイス C）に関係するトラフィックを指定します。

a. Edge-Router1 で、100 ～ 199 の範囲の拡張 IP アドレス リストを定義します。たとえば、Edge-Router1 でアクセス リスト 101 を作成します。

```
Edge-Router1(config)# ip access-list extended 101
```

b. Edge-Router1 で、WAN インターフェイスに関係するトラフィックを指定します。

- たとえば、ローカル デバイスへの任意の IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 と 80 上の任意のローカル送信元アドレスと任意の送信先への IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255 eq 135
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255 eq 80
```

ステップ 3　データセンターの Core-Router1 で、拡張 IP アクセス リストを使用して、LAN インターフェイス（入力インターフェイス D）に関係するトラフィックを指定します。

a. Core-Router1 で、100 ～ 199 の範囲の拡張 IP アドレス リストを定義します。たとえば、Core-Router1 でアクセス リスト 102 を作成します。

```
Core-Router1(config)# ip access-list extended 102
```

b. Core-Router1 で、LAN インターフェイスに関係するトラフィックを指定します。

- たとえば、任意の TCP ポート上の任意のローカル デバイスから任意の送信先へ送信される任意の IP/TCP トラフィック（たとえば、データセンターの任意のファイル サーバまたはアプリケーション サーバから送信されるトラフィック）に「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 および 80 上の任意のローカル デバイスから任意の送信先への IP/TCP トラフィックに選択的に「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any eq 135
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any eq 80
```

ステップ 4　データセンターの Core-Router1 で、拡張 IP アクセス リストを使用して、WAN インターフェイス（出力インターフェイス F）に関係するトラフィックを指定します。

a. Core-Router1 で、100 ～ 199 の範囲の拡張アドレス リストを定義します。たとえば、Core-Router1 でアクセス リスト 103 を作成します。

```
Core-Router1(config)# ip access-list extended 103
```

b. Core-Router1 で、WAN インターフェイス用のトラフィックに「関係がある」というマークを付けます。

- たとえば、任意のローカル デバイスへ送信される任意の IP/TCP トラフィック（たとえば、データセンターの任意のファイル サーバまたはアプリケーション サーバへ送信されるトラフィック）に「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255
```

- あるいは、送信元 IP サブネット、送信先 IP アドレス、および TCP ポート番号を定義して、選択的にトラフィックに「関係がある」というマークを付けることができます。たとえば、TCP ポート 135 と 80 上の任意のローカル送信元アドレスへの IP/TCP トラフィックに「関係がある」というマークを付けます。

```
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255 eq 135
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255 eq 80
```

ステップ 5　ブランチ オフィスの Edge-Router1 に PBR ルート マップを定義します。

a. LAN インターフェイス（入力インターフェイス）用のルート マップを定義します。次の例で、WAAS-EDGE-LAN ルート マップが作成されます。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

b. WAN インターフェイス（出力インターフェイス）用のルート マップを定義します。

次の例では、WAAS-EDGE-WAN ルート マップが作成されます。

```
Edge-Router1(config)# route-map WAAS-EDGE-WAN permit
```

c. 一致基準を指定します。

match コマンドを使用して、Edge-Router1 が、どのトラフィックが WAN インターフェイスに関係があるかを決定するために使用する拡張 IP アクセス リストを指定します。**match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。

次の例で、Edge-Router1 は、WAN インターフェイスに関係があるトラフィックを決定するための基準として、アクセス リスト 101 を使用するように設定されます。

```
Edge-Router1(config-route-map)# match ip address 101
```

（注）　**ip address** コマンド オプションは、1 つまたは複数の標準または拡張アクセス リストで許可される送信元または送信先 IP アドレスを照合します。

d. 一致したトラフィックを処理する方法を指定します。

次の例で、Edge-Router1 は、指定した基準と一致するパケットをネクストホップ（IP アドレスが 1.1.1.100 の Edge-WAE1）へ送信するように設定されます。

```
Edge-Router1(config-route-map)# set ip next-hop 1.1.1.100
```

（注）　複数のブランチ オフィスの WAE がある場合、フェールオーバーの目的で別のブランチ オフィスの WAE の IP アドレスを指定して（たとえば、Edge-Router1 で **set ip next-hop 1.1.1.101** コマンドを入力して）、フェールオーバーの目的でネクストホップ アドレス 1.1.1.101（Edge-WAE2 の IP アドレス）を指定できます。**next-hop** コマンドは、ロード バランシングの目的でなく、フェールオーバーの目的で使用されます。

ステップ 6　データセンターの Core-Router1 にルート マップを作成します。

a. LAN インターフェイス（入力インターフェイス）でルート マップを定義します。

次の例で、WAAS-CORE-LAN ルート マップが作成されます。

```
Core-Router1(config)# route-map WAAS-CORE-LAN permit
```

b. WAN インターフェイス（出力インターフェイス）でルート マップを定義します。

次の例で、WAAS-CORE-WAN ルート マップが作成されます。

```
Core-Router1(config)# route-map WAAS-CORE-WAN permit
```

c. 一致基準を指定します。

match コマンドを使用して、Core-Router1 が、どのトラフィックが WAN インターフェイスに関係があるかを決定するために使用する拡張 IP アクセス リストを指定します。**match** コマンドを入力しない場合、ルート マップはすべてのパケットに適用されます。次の例で、Core-Router1 は、WAN インターフェイスに関係があるトラフィックを決定するための基準として、アクセス リスト 103 を使用するように設定されます。

```
Core-Router1(config-route-map)# match ip address 103
```

d. 一致したトラフィックを処理する方法を指定します。

次の例で、Core-Router1 は、指定した基準と一致するパケットをネクストホップ（IP アドレスが 2.2.2.100 の Core-WAE1）へ送信するように設定されます。

```
Core-Router1(config-route-map)# set ip next-hop 2.2.2.100
```

（注）　複数のデータセンターの WAE がある場合、フェールオーバーの目的で別のデータセンターの WAE の IP アドレスを指定して（たとえば、Core-Router1 で **set ip next-hop 2.2.2.101** コマンドを入力して）、フェールオーバーの目的でネクストホップ アドレス 2.2.2.101（Core-WAE2 の IP アドレス）を指定できます。**next-hop** コマンドは、ロード バランシングの目的でなく、フェールオーバーの目的で使用されます。

ステップ 7　ブランチ オフィスの Edge-Router1 の LAN インターフェイス（入力インターフェイス）と WAN インターフェイス（出力インターフェイス）にルート マップを適用します。

a. Edge-Router1 で、インターフェイス コンフィギュレーション モードを開始します。

```
Edge-Router1(config)# interface FastEthernet0/0.10
```

b. LAN ルータ インターフェイスが PBR 用の WAAS-EDGE-LAN ルート マップを使用するように指定します。

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-LAN
```

c. インターフェイス コンフィギュレーション モードを開始します。

```
Edge-Router1(config-if)# interface Serial0
```

d. WAN ルータ インターフェイスが PBR 用の WAAS-EDGE-WAN ルート マップを使用するように指定します。

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-WAN
```

ステップ 8　データセンターの Core-Router1 の LAN インターフェイス（入力インターフェイス）と WAN インターフェイス（出力インターフェイス）にルート マップを適用します。

a. Core-Router1 で、インターフェイス コンフィギュレーション モードを開始します。

```
Core-Router1(config)# interface FastEthernet0/0.10
```

b. LAN ルータ インターフェイスが PBR 用の WAAS-CORE-LAN ルート マップを使用するように指定します。

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-LAN
```

c. インターフェイス コンフィギュレーション モードを開始します。

```
Core-Router1(config-if)# interface Serial0
```

d. WAN ルータ インターフェイスが PBR 用の WAAS-CORE-WAN ルート マップを使用するように指定します。

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-WAN
```

PBR のネクストホップが使用できるかどうかを確認する方法

PBR を使用してトラフィックを透過的に WAE へリダイレクトするときは、次のいずれかの方法を使用して、WAE の PBR のネクストホップが使用できるかどうかを確認することを推奨します。選択する方法は、ルータで使用している Cisco IOS ソフトウェアのバージョンと WAE の配置によって異なります。ただし、可能な限り、方法 2 を使用してください。

- 方法 1：デバイスは、WAE を CDP ネイバー（直接接続されている）と見なすと、CDP と ICMP を使用して WAE が動作していることを確認できます。詳細については、「方法 1：CDP を使用して WAE が動作していることを確認する」（P.4-41）を参照してください。
- 方法 2（推奨方法）：Cisco IOS ソフトウェア Release 12.4 以降が動作しているデバイスが WAE を CDP ネイバーと見なさない場合は、IP Service Level Agreement（SLA; サービス レベル契約）を使用して、WAE が ICMP エコーを使用して動作していることを確認できます。詳細については、「方法 2：IP SLA を使用して、WAE が ICMP エコー検査を使用して動作していることを確認する（推奨方式）」（P.4-41）を参照してください。

- 方法 3：Cisco IOS ソフトウェア Release 12.4 以降が動作しているデバイスが WAE を CDP ネイバーと見なさない場合は、IP SLA を使用して、WAE が TCP 接続試行を使用して動作していることを確認できます。詳細については、「方法 3：IP SLA を使用して、WAE が TCP 接続試行を使用して動作していることを確認する」（P.4-42）を参照してください。

（注）　この項で、「デバイス」という用語は、PBR を使用してトラフィックを透過的に WAE へリダイレクトするように設定されたルータまたはスイッチのことを指しています。

PBR を使用するように設定されたデバイスが WAE を CDP ネイバーと見なすかどうかを確認するには、デバイスで **show cdp neighbors** コマンドを入力します。デバイスが WAE を CDP 隣接と見なす場合、WAE は **show cdp neighbors** コマンドの出力に表示されます。

方法 1：CDP を使用して WAE が動作していることを確認する

PBR を使用するように設定されたデバイスが WAE を CDP ネイバー（WAE がデバイスに直接接続されている）と見なす場合は、CDP と ICMP を使用して PBR のネクストホップとして WAE を使用できるかどうかを確認できます。

次の例は、この方法を使用して、PBR のネクストホップとして WAE を使用できるかどうかを確認する方法を示しています。CDP を使用する必要があるときに設定される LAN ルート マップと WAN ルート マップのそれぞれについて、次の設定プロセスを完了する必要があります。

CDP を使用して WAE が動作していることを確認するには、次の手順に従ってください。

ステップ 1　PBR が設定されているルータ（たとえば、ブランチ オフィスの Edge-Router1 ルータ）で、コンフィギュレーション モードを開始し、CDP を有効にします。

```
Edge-Router1(config)# cdp run
```

ステップ 2　すでにルータに作成されている WAAS-EGDE-LAN ルート マップ用のルート マップ コンフィギュレーション モードを有効にします。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

ステップ 3　CDP を使用して設定済みのネクストホップ アドレスが使用できるかどうかを確認するようにルータを設定します。

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability
```

ステップ 4　ルータが PBR を使用してトラフィックをリダイレクトするようにしたい WAE（たとえば、ブランチ オフィスの Edge-WAE1）で、CDP を有効にします。

```
Edge-WAE1(config)# cdp enable
```

PBR を設定し、複数の WAE があり、方法 1 を使用して PBR のネクストホップとして WAE が使用できることを確認する場合、前のプロセスを完了したら、追加の設定は不要です。

方法 2：IP SLA を使用して、WAE が ICMP エコー検査を使用して動作していることを確認する（推奨方式）

IP SLA と ICMP を使用して（推奨方式）、PBR のネクストホップとして WAE が使用できることを確認するには、次の手順に従ってください。

ステップ 1　ブランチ オフィスの Edge-Router1 ルータで、このルータですでに設定されている WAAS-EDGE-LAN ルート マップ用のルート マップ コンフィギュレーション モードを開始します。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

ステップ 2　トラフィックの一致条件を指定します。次の例では、一致条件にアクセス リスト番号 105 が指定されます。

```
Edge-Router1(config)# match ip address 105
```

ステップ 3　IP SLA 追跡インスタンス番号 1 を使用してネクストホップ WAE（たとえば、IP アドレスが 1.1.1.100 で Edge-WAE1 という名前のブランチ オフィスの WAE）が使用できることを確認するように、ルートマップを設定します。

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability 1.1.1.100 track 1
```

（注）　ブランチ オフィスのエッジ ルータと PBR を使用してトラフィックを WAE へリダイレクトするように設定されているデータセンターのコア ルータに設定されている各ルート マップについて、**set ip next-hop verify-availability** コマンドを入力します。

ステップ 4　IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
Edge-Router1(config-ip-sla)#
```

ステップ 5　指定のソース インターフェイスを使用し、Edge-WAE1 をエコーするようにルータを設定します。

```
Edge-Router1(config-ip-sla)# icmp-echo 1.1.1.100 source-interface FastEthernet 0/0.20
```

ステップ 6　20 秒周期でエコーを実行するようにルータを設定します。

```
Edge-Router1(config-ip-sla)# frequency 20
Edge-Router1(config-ip-sla)# exit
```

ステップ 7　ただちに開始し、継続的に動作するように、IP SLA 追跡インスタンス 1 のスケジュールを設定します。

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

ステップ 8　IP SLA 追跡インスタンス 1 で定義されているデバイスを追跡するように、IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config)# track 1 rtr 1
```

PBR を設定し、複数の WAE があり、方法 2 を使用して PBR のネクストホップとして WAE が使用できることを確認している場合は、WAE ごとに別々の IP SLA を設定し、IP SLA ごとに **track** コマンドを実行する必要があります。

方法 3：IP SLA を使用して、WAE が TCP 接続試行を使用して動作していることを確認する

PBR 用に設定され、Cisco IOS ソフトウェア Release 12.4 以降が動作しているデバイスが WAE を CDP ネイバーと見なさない場合は、IIP SLA を使用して、TCP 接続試行 を使用して WAE が動作していることを確認できます。IP SLA を使用して、60 秒の固定周期で TCP 接続試行を使用して、PBR のネクストホップとして WAE が使用できることをモニタできます。

PBR のネクストホップとして WAE が使用できることを確認するには、次の手順に従ってください。

ステップ 1　ブランチ オフィスの Edge-Router1 ルータで、このルータにすでに設定されている WAAS-EDGE-LAN ルート マップ用のルート マップ コンフィギュレーション モードを開始します。

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

ステップ 2　IP SLA 追跡インスタンス番号 1 を使用してネクストホップ WAE（たとえば、IP アドレスが 1.1.1.100 の Edge-WAE）が使用できることを確認するように、ルート マップを設定します。

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability 1.1.1.100 track 1
```

（注）　ブランチ オフィスのこのエッジ ルータと PBR を使用してトラフィックを透過的に WAE へリダイレクトするように設定されているデータセンターのコア ルータの各ルート マップについて、**set ip next-hop verify-availability** コマンドを入力します。

ステップ 3　IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
```

ステップ 4　指定した送信先ポートと送信元ポートを使用し、60 秒の固定周期で TCP 接続試行を使用して WAE が使用できることをモニタするように、ルータを設定します。

```
Edge-Router1(config-ip-sla)# tcp-connect 1.1.1.100 80 source-port 51883 control disable
Edge-Router1(config-ip-sla)# exit
```

ステップ 5　ただちに開始し、継続的に動作するように、IP SLA 追跡インスタンス 1 のスケジュールを設定します。

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

ステップ 6　IP SLA 追跡インスタンス 1 で定義されているデバイスを追跡するように、IP SLA 追跡インスタンス 1 を設定します。

```
Edge-Router1(config)# track 1 rtr 1
```

PBR を設定し、複数の WAE があり、方法 3 を使用して PBR のネクストホップとして WAE が使用できることを確認している場合は、WAE ごとに別々の IP SLA を設定し、IP SLA ごとに **track** コマンドを実行する必要があります。

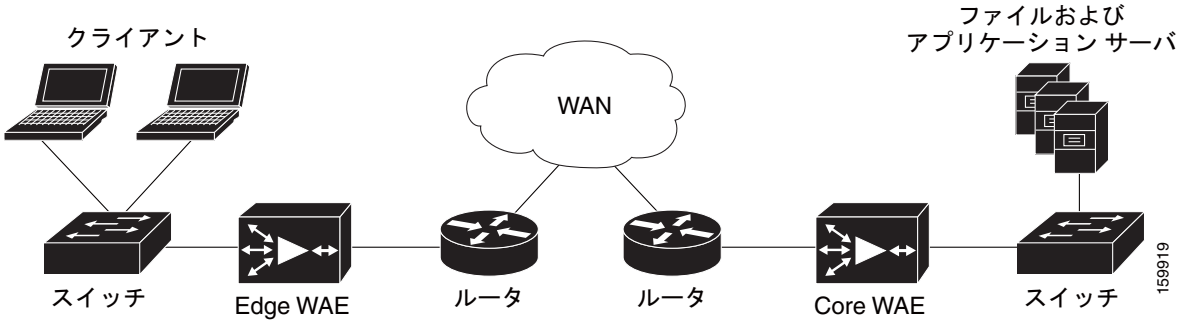
TCP トラフィックの透過的な代行受信へのインライン モードの使用

インライン モードを使用して、WAE は、物理的に透過的にトラフィックをクライアントとルータの間で代行受信できます。インライン モードを使用するには、Cisco WAE Inline Network Adapter がインストールされた WAE を使用する必要があります。このモードでは、WAE デバイスを最適化するトラフィックのパスに物理的に配置します。通常は、図 4-7 で表示したスイッチとルータの間です。トラフィックのリダイレクションは必要ありません。

（注）　インライン WAE デバイスを設置するときは、Cisco.com にある『*Installing the Cisco WAE Inline Network Adapter*』の「Cabling」の項で説明しているケーブルの要件に従う必要があります。

ピア WAE 上でのトラフィック代行受信メカニズムの任意の組み合わせがサポートされています。たとえば、インライン代行受信を、データセンター WAE 上のブランチ オフィス WAE と WCCP で使用できます。複雑なデータセンターの構成に対して、ハードウェアが加速化された WCCP 代行受信または Cisco Application Control Engine（ACE）でのロード バランシングの使用を推奨します。

図 4-7　　インライン代行受信



（注） インライン モードと WCCP リダイレクションは排他的です。WAE が WCCP 操作用に設定されている場合は、インライン モードを設定できません。インライン モードは、WAE デバイスに Cisco WAE Inline Network Adapter が搭載されたときのデフォルトのモードです。WCCP が設定されているデバイス グループに Cisco WAE Inline Network Adapter 搭載の WAE を追加しても、WCCP の設定はインライン WAE に自動的に適用されません。WCCP を使用するように インライン WAE を設定するには、手動で WCCP デバイス グループの設定が適用されるようにする必要があります。

（注） Cisco WAE Inline Network Adapter のある WAE は Central Manager として設定できますが、インライン代行受信機能は使用できません。

Cisco WAE Inline Network Adapter には、2 つまたは 4 つのイーサネット ポートがあります。4 つのイーサネット ポートがあるアダプタでは、ポートは 2 つの論理グループにグループ化されます。各グループには LAN 対応ポート 1 つと WAN 対応ポート 1 つがあります。通常、1 つのグループだけを使用し、LAN 対応ポートをスイッチに接続し、WAN 対応ポートをルータに接続します。4 つのポートがあるアダプタで、WAE を 2 つのルータに接続する必要があるネットワーク トポロジを使用する場合、インターフェイスの 2 番めのグループが提供されます。グループで 1 つのインターフェイスを入力するトラフィックは、同じグループの別のインターフェイス上のデバイスを終了させます。

WAE-7341/7371/674 は設置された 2 つの Cisco WAE Inline Network Adapter をサポートし、合計 8 つのインライン イーサネット ポートを提供します。

インライン インターフェイスに IP アドレスを割り当てることができますが、必須ではありません。詳細については、「インライン インターフェイスの IP アドレスの設定」（P.4-48）を参照してください。

Cisco WAE Inline Network Adapter を通過するトラフィックは、最適化のために、透過的に代行受信されます。最適化の必要のないトラフィックは、LAN/WAN インターフェイス間でブリッジされます。電源、ハードウェア、回復不能なソフトウェアの障害が発生した場合、ネットワーク アダプタは、自動的にバイパス モードで動作し始めます。この場合、すべてのトラフィックは各グループで LAN と WAN のインターフェイス間で機械的にブリッジングされます。WAE の電源を切るか起動したときに、Cisco WAE Inline Network Adapter もバイパス モードで動作します。さらに、手動で Cisco WAE Inline Network Adapter をバイパス モードに追加することもできます。

インライン モードはデフォルトで、すべての TCP トラフィックを受けるように設定されます。WAE が挿入されるネットワーク セグメントが 802.1Q のタグ付け（VLAN）トラフィックを実行中の場合、最初にすべての VLAN 上のトラフィックが受信されます。インライン代行受信は、各 VLAN に対して、有効または無効にできます。ただし、最適化のポリシーは、VLAN 上でカスタマイズできません。

Cisco WAE Inline Network Adapter が搭載された複数の WAE デバイスをシリアルでクラスタ化することにより、デバイスに障害が発生した場合のアベイラビリティを高めることができます。詳細については、「インライン WAE のクラスタリング」（P.4-51）を参照してください。

（注）　Cisco WAE Inline Network Adapter が搭載された WAE がバイパス モードに入ると、接続されたスイッチとルータのポートを再初期化しなければならない場合があり、これによって数秒間トラフィックの WAE の通過が中断される可能性があります。

WAE がループの作成ができないような設定で展開される場合（つまり、スイッチとルータ間にスタンダードな形式で展開される場合）、スイッチ ポート上の PortFast を WAE が接続されるように設定します。PortFast によって、ポートは、Spanning Tree Algorithm（STA; スパニング ツリー アルゴリズム）の最初の数ステージをスキップでき、より早くパケット転送モードに移行できます。

ここでは、次の内容について説明します。

インライン インターフェイス設定

インライン インターフェイス設定を行うには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します（[Device Groups] からインライン インターフェイスを設定できません）。

WAAS ネットワークに設定されているすべてのデバイスを表示する [Devices] ウィンドウが表示されます。

ステップ 2　インライン設定を変更するデバイスの横にある [Edit] アイコンをクリックします。

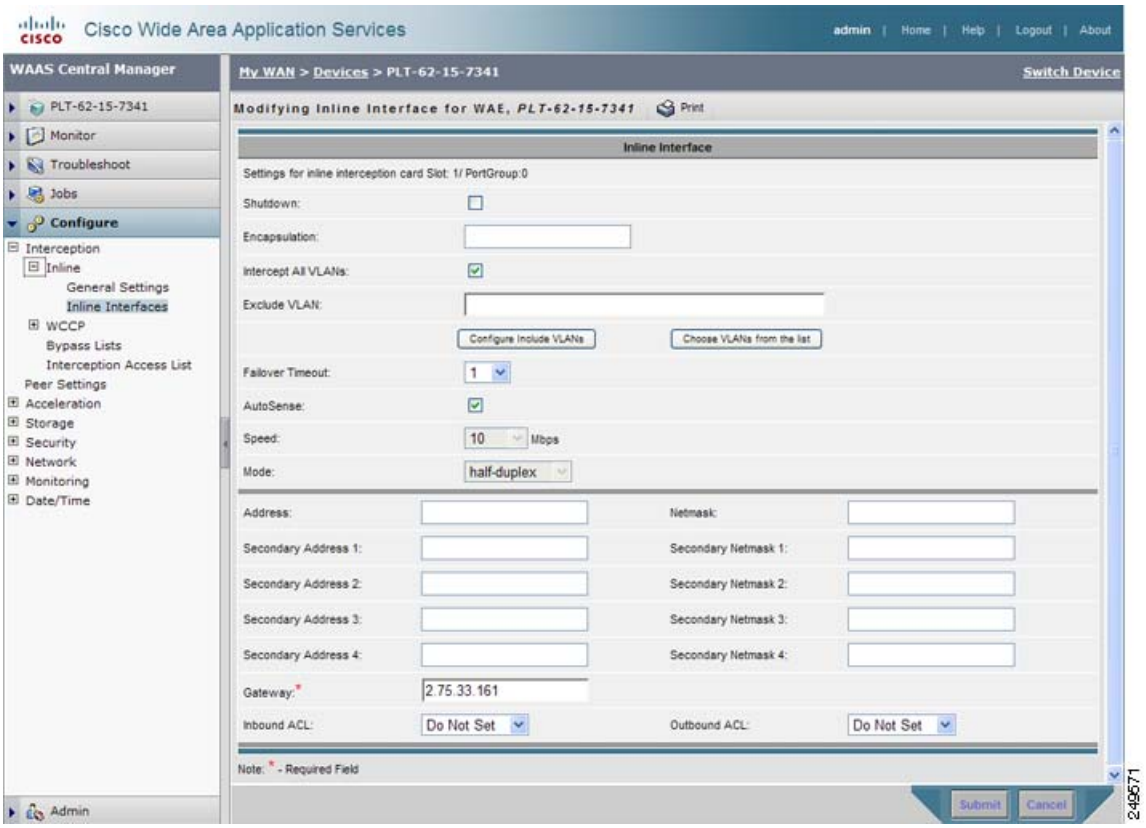
[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [Inline] > [Inline Interfaces] を選択します。

[Inline Interfaces] ウィンドウが開き、デバイス上のインライン インターフェイス グループが表示されます。変更するインライン インターフェイス グループの横にある [Edit Inline Interface] アイコンをクリックします。

[Modifying Inline Interface] ウィンドウが表示され、特定のスロットとグループ上のインライン インターフェイス設定が表示されます（図 4-8 を参照）。

図 4-8　[Modifying Inline Interface] ウィンドウ



ステップ 4　[Shutdown] チェックボックスを選択して、インターフェイスを停止します。この設定は、処理なしでトラフィックを LAN/WAN インターフェイス間でブリッジングします。

ステップ 5　[Encapsulation] フィールドで、WAE から出るトラフィックに割り当てる VLAN ID を入力します。VLAN ID は、ルータが予測する VLAN ID と一致するように設定する必要があります。

VLAN ID ドの詳細については、「インライン インターフェイスの IP アドレスの設定」（P.4-48）を参照してください。

ステップ 6　[Intercept all VLANs] チェックボックスをオンにして、インターフェイス グループのインライン代行受信を有効にします。デフォルトでインライン代行受信が有効な場合、WAE は Cisco WAE Inline Network Adapter を含みます。

（注）　インライン モードと WCCP リダイレクションは排他的です。WAE が WCCP 操作用に設定されている場合は、インライン モードを設定できません。インライン モードは、WAE デバイスに Cisco WAE Inline Network Adapter が搭載されたときのデフォルトのモードです。

ステップ 7　[Exclude VLAN] フィールドで、最適化から除外する 1 つまたは複数の VLAN 範囲のリストを入力します。ネイティブ VLAN を除外するには、「native」と入力します。各 VLAN 範囲をカンマで区切ります。または、次に示す手順に従って、VLAN 範囲をリストから選択できます。

a.　インライン代行受信に含める VLAN リストがわかっている場合は、[Configure Include VLANs] ボタンをクリックします。このボタンは、内包する VLAN をカンマで区切ったリストの入力を要求するスクリプトを実行します。スクリプトは、除外対象のすべての VLAN のインバース リストを生成し、その後、ウィンドウを更新し、リストを [Exclude VLAN] フィールドに入力します。

b. [Choose VLANs from the list] ボタンをクリックして、VLAN 範囲をピックします。[VLAN Range Assignments] ウィンドウが表示され、定義された VLAN 範囲を表示します。VLAN 範囲の定義については、「インライン サポートの VLAN の設定」（P.4-50）に説明があります。

c. 含める、または除外する VLAN 範囲を次の手順で選択します。

- このインライン インターフェイス グループの最適化に含めるそれぞれの VLAN 範囲の横にある ✖ をクリックします。アイコンは ✔ に変わります。最適化に含まれないすべての VLAN は、除外されます。
- このインライン インターフェイス グループの最適化から除外するそれぞれの VLAN 範囲の横にある ✖ をクリックします。アイコンは ✔ に変わります。
- タスクバーの ✔ をクリックして最適化する有効な VLAN 範囲を選択するか、タスクバーの ✖ をクリックして、すべての VLAN 範囲を最適化から除外します。

d. [Submit] をクリックします。

ステップ 8　[Failover Timeout] ドロップダウン リストから、秒数 [1]、[3]、[5]、または [10] を選択します。デフォルトは 1 秒です。この値は、バイパス モードで動作を開始する前に、WAE が待つ障害イベント後の秒数を設定します。バイパス モードでは、インターフェイス グループのいずれかのポートで受信されるすべてのトラフィックはグループの別のポートへ転送されます。

ステップ 9　ポートについて [Speed] と [Mode] を次のように設定します。

a. デフォルトで有効になっている [AutoSense] チェックボックスの選択を解除します。

b. [Speed] ドロップダウン リストから、伝送速度（[10]、[100]、または [1000] Mbps）を選択します。

c. [Mode] ドロップダウン リストから、送信モード（[full-duplex] または [half-duplex]）を選択します。

（注） WAE、ルータ、スイッチ、またはその他のデバイスでは半二重接続を使用しないことを強く推奨します。半二重接続の場合はパフォーマンスが低下するので、使用は避けてください。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を調べて、全二重接続が使用されていることを確認してください。

ステップ 10　IP アドレスを割り当てる場合は、[Address] フィールドにインライン インターフェイスの IP アドレスを入力します。

ステップ 11　[Netmask] フィールドに、インライン インターフェイスのサブネット マスクを入力します。

ステップ 12　[Secondary Address] フィールドと [Secondary Netmask] フィールドに最大 4 つまでのセカンダリ IP アドレスとそれに対応するサブネット マスクを入力します。

複数の IP アドレスを設定することで、デバイスを複数のサブネットに置くことができ、データをルータでリダイレクトせずに、直接 WAAS デバイスから情報を要求するクライアントへ転送できるので、デバイスを使用して応答時間を最適化することができます。また、WAAS デバイスとクライアントは同じサブネット上に設定されるため、クライアントから WAAS デバイスを認識できます。

ステップ 13　[Gateway] フィールドで、デフォルト ゲートウェイ IP アドレスを入力します。

ステップ 14　（任意）[Inbound ACL] ドロップダウン リストから、着信パケットに適用する IP ACL を選択します。

ドロップダウン リストには、システムに設定されているすべての IP ACL が表示されています。

ステップ 15　（任意）[Outbound ACL] ドロップダウン リストから、発信パケットに適用する IP ACL を選択します。

ステップ 16　[Submit] をクリックします。

CLI からインライン代行受信を設定するには、**interface InlineGroup** グローバル コンフィギュレーション コマンドを使用できます。

WAAS は VLAN ID を使用して、インライン インターフェイスで TCP フローの VLAN トラフィックを代行受信またはブリッジします。特定 TCP 接続で送信されたすべてのパケットの VLAN ID は一致する必要があります。異なる VLAN ID のパケットはブリッジされ、最適化されません。システムに、ある方向のトラフィック フローが他方向のトラフィック フローとは異なる VLAN ID を使用する非対称ルーティング トポロジが設定されている場合、トラフィックが最適化されていることを確認するために VLAN ID チェックを無効化できます。

VLAN ID チェックを設定にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します（[Device Groups] からネットワークを設定できません）。

WAAS ネットワークに設定されているすべてのデバイスを表示する [Devices] ウィンドウが表示されます。

ステップ 2　ネットワーク設定を変更するデバイスの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Interception] > [Inline] > [General Settings] を選択します。

[General Settings] ウィンドウが開き、VLAN ID 接続チェック コントロールが表示されます。

ステップ 4　VLAN ID 接続チェックを有効にするには、[VLAN ID Connection Check] チェックボックスを選択します。無効にするには、チェックボックスの選択を解除します。デフォルト設定では、有効になっています。

ステップ 5　[Submit] をクリックします。

CLI から VLAN ID チェックを設定するには、**inline vlan-id-connection-check** グローバル コンフィギュレーション コマンドを使用します。

インライン インターフェイスの IP アドレスの設定

インライン グループ インターフェイスに IP アドレスを割り当てることができますが、必須ではありません。「インライン インターフェイス設定」（P.4-45）で説明されている手順に従って、1 つのプライマリ IP アドレスと最大 4 つのセカンダリ IP アドレスを割り当てることができます。

インライン グループ インターフェイスを WAE のプライマリ インターフェイスとして設定するには、[Configure] > [Network] > [Network Interfaces] ウィンドウの [Primary Interface] ドロップダウン リストを使用します。

WAE のプライマリ インターフェイスがインライン グループ インターフェイスに設定され、管理トラフィックが個別の IP アドレス（同一のインライン グループ インターフェイスまたは組み込みインターフェイスのセカンダリ IP アドレス）に設定されているシナリオでは、WAAS Central Manager が管理トラフィック用に指定された IP アドレスの WAE と通信するように設定する必要があります。[*Device Name*] > [Activation] ウィンドウの [Management IP] フィールドで WAE 管理トラフィックの IP アドレスを設定します。

WAE と Cisco WAE Inline Network Adapter が、スイッチとルータ間の 802.1Q VLAN トランク回線に存在し、インライン インターフェイスに IP アドレスを設定している場合は、WAE の発信トラフィックに割り当てられる VLAN ID を設定する必要があります。VLAN ID は、ルータが予測する VLAN ID と一致するように設定する必要があります。

VLAN ID を割り当てるには、次のように、**encapsulation dot1Q** インターフェイス コマンドを使用します。

```
(config)# interface inlineGroup 1/0
```

```
(config-if)# encapsulation dot1Q 100
```

この例は、VLAN ID 100 を WAE の発信トラフィックに割り当てる方法を示しています。VLAN ID の範囲は、1 ～ 4094 です。

（注）　インライン トラフィックの VLAN ID を設定するには、**encapsulation dot1Q** インターフェイス コマンドを使用するか、または [Central Manager] ページ（[Configure] > [Interception] > [Inline] > [Inline Interfaces]）を使用します（「インライン インターフェイス設定」（P.4-45）を参照）。

VLAN ID がルータ サブインターフェイスによって予測された VLAN ID と一致しないと、インライン インターフェイス IP アドレスに接続できない場合があります。

インライン アダプタは、インライン グループ インターフェイスごとに 1 つの VLAN ID しかサポートしません。インライン インターフェイスの異なるサブネットのセカンダリ アドレスを設定している場合は、VLAN のルータ サブインターフェイスに同じセカンダリ アドレスを割り当てる必要があります。

IEEE 802.1Q トンネリングを使用すると、タグが追加されるときにフレーム サイズが 4 バイト増加します。したがって、デバイス MTU を最低でも 1504 バイト増やすことによって、トンネル化されたパケットが通過するすべてのスイッチでより大きなフレームを処理できるように設定する必要があります。

次の動作に関する考慮事項は、インライン インターフェイスでの IP アドレスの設定に適用されます。

- この機能は、ルーティング可能な基本インターフェイスをサポートし、組み込みインターフェイスに関連付けられたスタンバイ、ポート チャネル、および Cisco Discovery Protocol（CDP; シスコ検出プロトコル）といった追加機能はサポートしません。
- すべてのトラフィックに対してインライン インターフェイスを使用するように WAE を設定している場合は、インライン代行受信を有効にする必要があります。有効にしないと、WAE はトラフィックを受信しません。
- WAE が、すべてのトラフィックに対してインライン インターフェイスを使用するように設定されており、メカニカル バイパス モードに切り替わった場合は、インライン インターフェイス IP アドレスを介して WAE にアクセスできなくなります。インライン インターフェイスがバイパス モードの場合にデバイスを管理するには、コンソール アクセスが必要となります。
- WAE にインライン インターフェイスの IP アドレスが設定されている場合、インターフェイスはそのアドレス宛てのトラフィックと ARP ブロードキャストだけを受信でき、マルチキャスト トラフィックは受信できません。
- HSRP グループに参加している 2 つのルータが 2 つのインライン グループを介して直接接続されている、HSRP を使用した構成の場合、アクティブなルータが故障すると、HSRP はすべてのクライアントを対象として動作します。ただし、管理トラフィックもインライン インターフェイスを使用するように設定されている場合、管理トラフィック用の WAE 自身の IP アドレスにはこの冗長性は適用されません。アクティブなルータが故障した場合、インライン インターフェイスは物理的に故障したルータ インターフェイスに接続されているため、WAE インライン IP アドレスには接続できなくなります。この場合は、スタンバイ ルータに接続された 2 番めのインライン グループ インターフェイスを通じて WAE に接続できます。管理トラフィック用の WAE 自身の IP アドレスに冗長性が必要な場合は、インライン インターフェイスではなく組み込みインターフェイスの IP アドレスを使用することを推奨します。
- すべてのトラフィックに対してインライン インターフェイスを使用するように WAE を設定しており、組み込みインターフェイスには IP アドレスを割り当てていない場合に、WAE を 4.0.15 よりも前のバージョンにダウングレードすると、インライン インターフェイスに割り当てられた IP アドレスを使用している WAE 上の内部サービスは接続を失います。WAE をダウングレードする前に、組み込みインターフェイスに適切なネットワーク設定値を設定してください。

- WAAS Central Manager が 4.0.15 よりも前のバージョンのソフトウェアを実行している場合は、WAE が 4.0.15 以降のバージョンを実行しても、WAE のインライン インターフェイスへの IP アドレスの設定はサポートされません。
- WAE がすべてのトラフィックに対してインライン インターフェイスを使用するように設定されている構成で、WAAS Central Manager を 4.0.15 よりも前のバージョンにダウングレードすると、WAAS Central Manager はインライン インターフェイスをプライマリ インターフェイスとして認識できないため、WAE との通信は失われます。通信の喪失を回避するには、組み込みインターフェイスのいずれかで管理トラフィックを受信するように WAE を設定するか、[Device Name] > [Activation] ウィンドウの [Management IP] フィールドでインライン インターフェイス IP アドレスを代替管理アドレスとして設定します。

インライン サポートの VLAN の設定

最初、WAE はトラフィックをすべての VLAN から受信します。ある VLAN からのトラフィックを含めるまたは排除するように WAE を設定できます。排除された VLAN に対してトラフィックはグループで LAN/WAN インターフェイス間でブリッジングされ、処理されません。

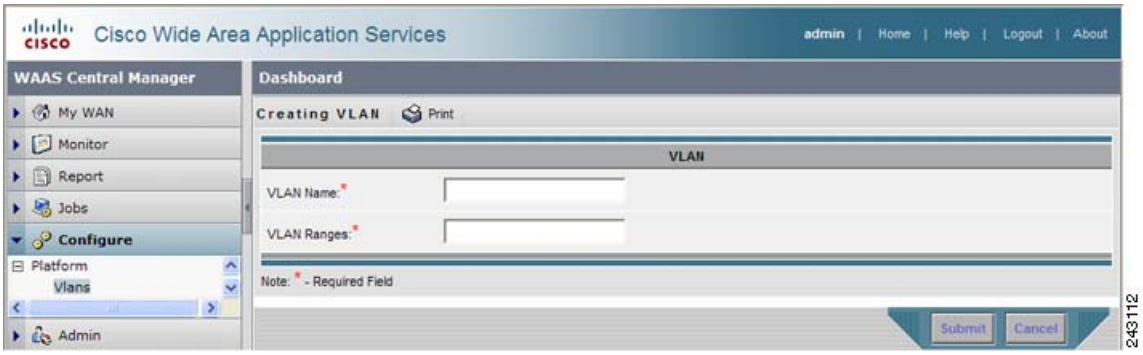
インラインをサポートするように VLAN を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Platform] > [Vlans] を選択します。

[Vlans] ウィンドウが表示され、定義された VLAN をリストします。修正する既存の VLAN の横にある [Edit Vlan] アイコンをクリックできます。

ステップ 2　タスクバーで、[Create New Vlan] アイコンをクリックします。[Creating Vlan] ウィンドウが表示されます（図 4-9 を参照）。

図 4-9　[Creating New Vlan] ウィンドウの例



ステップ 3　[Vlan Name] フィールドで、VLAN リストの名前を入力します。

ステップ 4　[VLAN Ranges] フィールドで、1 つまたは複数の VLAN 範囲のリストを入力します。各 VLAN 範囲をカンマで分離します（スペースはなし）。「インライン インターフェイス設定」（P.4-45）の説明に従って、インライン インターフェイス グループを設定するときに、VLAN 範囲のこのリストは、最適化に含めたり除外したりすることができます。このフィールドに「native」を指定できません。

ステップ 5　[Submit] をクリックします。

VLAN リスト作成のこの機能が提供され、VLAN リストをグローバルに設定できます。インライン インターフェイス用に VLAN を設定するには、この機能を使用する必要はありません。「インライン インターフェイス設定」（P.4-45）の説明に従って、インライン インターフェイス設定ウィンドウで VLAN を直接設定できます。

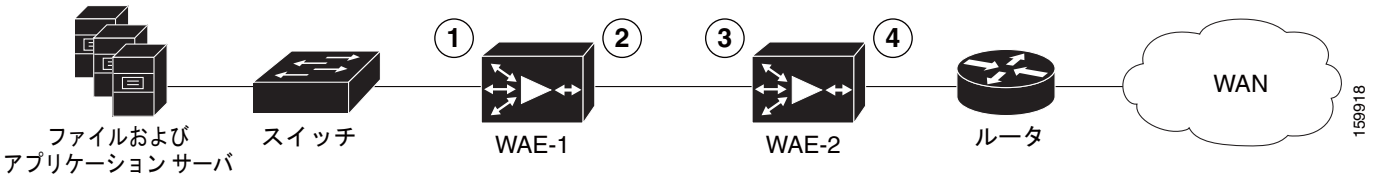
インライン WAE のクラスタリング

Cisco WAE Inline Network Adapter が搭載された 2 台の WAE デバイスをシリアルでクラスタ化することにより、デバイスに障害が発生した場合のデータセンターでのアベイラビリティを高めることができます。現在の最適化デバイスに問題が発生した場合、インライン グループはシャットダウンするか、またはデバイスが過負荷になり、クラスタ内の 2 番めの WAE デバイスが最適化サービスを提供します。拡張またはロード バランシングの目的でシリアル インライン クラスタに WAE デバイスを導入する方法は、サポートされていません。

（注）　個々のアプリケーション アクセラレータではなく、TFO 過負荷で過負荷フェールオーバーが発生します。これは、一時的な過負荷防止を目的としています。過負荷状態で WAE の実行を継続すると、頻繁に過負荷フェールオーバーが発生するため、推奨しません。

シリアル クラスタは、連続的にトラフィック パスで接続される 2 つの WAE デバイスで構成されます。1 つの Cisco WAE Inline Network Adapter の WAN ポートは、図 4-10 に示すように、次の Cisco WAE Inline Network Adapter の LAN ポートなどに接続されます。

図 4-10　インライン クラスタ



1	WAE-1 のインライン LAN ポート	**3**	WAE-2 のインライン LAN ポート
2	WAE-1 のインライン WAN ポート	**4**	WAE-2 のインライン WAN ポート

シリアル クラスタでは、スイッチとルータの間のすべてのトラフィックは、すべてのインライン WAE を通過します。図 4-10 では、TCP 接続は WAE-1 によって最適化されます。WAE-1 に障害が発生すると、トラフィックはバイパスされ、WAE-2 によって最適化されます。

シリアルでクラスタ化された WAE のポリシー設定は同じである必要があります。また、クラスタ内の両方の WAE に同じデバイスを使用することを推奨します。

各 WAE でインライン WAE をシリアルでクラスタ化する場合、クラスタ内の他の WAE のアドレスを非最適化ピアとして設定する必要があります。これにより、シリアル クラスタの 2 つのピア WAE 間の最適化が無効となります。これは、ユーザが WAN リンクの各側の WAE ピア間のみでの最適化を希望しているためです。

シリアル クラスタの WAE 間のピア最適化を無効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します（[Device Groups] からはピアを設定できません）。

WAAS ネットワークに設定されているすべてのデバイスを表示する [Devices] ウィンドウが表示されます。

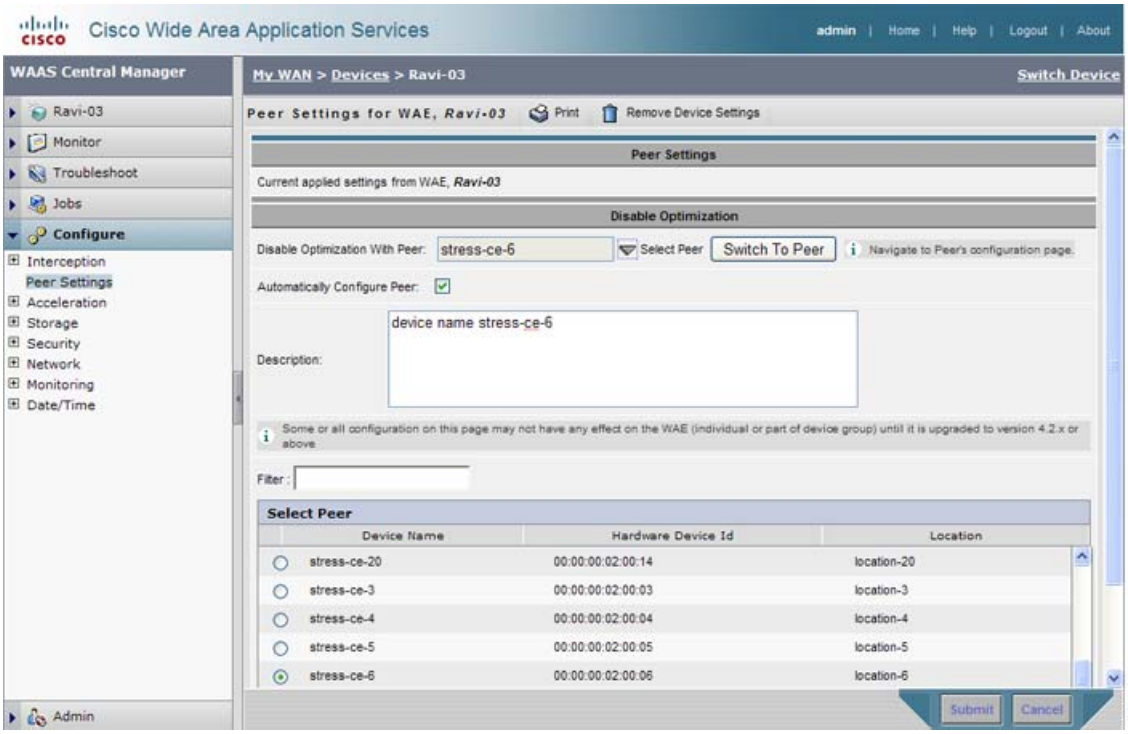
ステップ 2　ピア最適化を設定するデバイスの横にある [Edit] アイコンをクリックします。シリアル クラスタとしてペアになっている 2 つの WAE からいずれかを選択できます。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Peer Settings] を選択します。

[Peer Settings] ウィンドウが表示されます（図 4-11 を参照）。

図 4-11　ピアの設定



ステップ 4　[Select Peer] の三角形のコントロールをクリックすると、Central Manager を使用して登録されている他の WAE がウィンドウ下部に表示されます（[Select Peer] エリアを参照）。

ステップ 5　[Select Peer] エリアで、現在のデバイスのシリアル ピアの横にあるオプション ボタンをクリックします。ピア デバイスの名前が [Disable Optimization With Peer] フィールドに表示されます。

デバイス リストをフィルタする必要がある場合は、[Filter] フィールドに文字列を入力します。文字を入力すると、デバイス リストが動的にフィルタされ、デバイス名またはハードウェア デバイス ID にフィルタ文字列が含まれるデバイスのみが対象となります。

ステップ 6　[Automatically Configure Peer] チェックボックスを選択すると、Central Manager が同じ設定を使用して他のピアを設定し、現在のデバイスを使用して最適化を無効にすることができます。

このチェックボックスを選択しない場合、他のピアを手動で設定して、現在のデバイスを使用して最適化を無効にする必要があります。変更内容を送信した後、[Switch to Peer] ボタンをクリックして、このピア デバイスに関する同じ設定ページへ進みます。

ステップ 7　[Description] フィールドにピアの説明を入力します。デフォルトの説明は、ピアのデバイス名です。

ステップ 8　[Submit] をクリックします。

CLI からシリアル ピア最適化を無効にするには、**no peer device-id** グローバル コンフィギュレーション コマンドを使用します。シリアル ピア最適化を再度有効にするには、**peer device-id** グローバル コンフィギュレーション コマンドを使用します。

Central Manager に登録されているすべてのシリアル クラスタ ペアのステータスを表示するには、WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Peer Settings] を選択します。図 4-12 に示すように、[Peer Settings] ウィンドウが表示されます。

図 4-12　ピア設定ステータスの表示

ウィンドウには、ピア最適化を設定した各 WAE が表示されます。各シリアル クラスタ ペアに対して 2 つのエントリがあり、エントリの [Mutual Pair] カラムにチェック マークが付いていることを確認します。ペアの各 WAE にはエントリが設定されていることが必要です（たとえば、上図の最初と最後のエントリ）。

エントリの [Mutual Pair] カラムにチェック マークが付いていない場合は、シリアル ピアが設定されているが、このピアが最初のデバイスを使用してシリアル ピアとして同様に設定されていない WAE を示します。

CHAPTER 5

ネットワーク設定の構成

この章では、ネットワーク トラフィックをサポートするために追加のネットワーク インターフェイスの作成、DNS サーバの指定、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）の有効化、ファイアウォール トラバースに関する問題を回避するためにピア WAE で UDP カプセル化を使用してトラフィックを交換する directed 動作モードの構成など、基本的なネットワーク設定を構成する方法について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

ネットワーク インターフェイスの設定

初期設定時に、初期インターフェイスを選択し、DHCP 用に設定するか、固定 IP アドレスを指定しました。この項では、冗長性、ロード バランシング、およびパフォーマンス最適化用のオプションを使用して、追加のインターフェイスを設定する方法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。

- 「DHCP 用のインターフェイスの設定」（P.5-8）

WAAS CLI でなく、WAAS Central Manager GUI を使用して、ネットワーク設定を構成することを推奨します。ただし、CLI を使用する場合は、『*Cisco Wide Area Application Services Command Reference*』で **interface**、**ip address**、**port-channel**、および **primary-interface** コマンドを参照してください。

（注）　WAE、ルータ、スイッチ、またはその他のデバイスでは半二重接続を使用しないことを強く推奨します。半二重接続の場合はパフォーマンスが低下するので、使用は避けてください。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を調べて、全二重接続が使用されていることを確認してください。

スタンバイ インターフェイスの設定

この手順では、「スタンバイ インターフェイス」と呼ばれる論理インターフェイスを設定します。この論理インターフェイス用のパラメータを設定したあとで、物理インターフェイスをスタンバイ インターフェイスに関連付けて、スタンバイ グループを作成する必要があります（スタンバイ グループは、物理インターフェイスから構成されます）。WAAS Central Manager GUI で、物理インターフェイスをスタンバイ グループに参加させ、1 つの物理インターフェイスをプライマリに割り当てることによって、スタンバイ グループを作成します（「プライマリ スタンバイ インターフェイスの設定」（P.5-4）を参照してください）。

スタンバイ インターフェイスは、アクティブなインターフェイスが故障するまで、未使用の状態のままです。アクティブ ネットワーク インターフェイスに障害（ケーブルの問題、レイヤ 2 スイッチの障害、またはその他の障害が原因で）が発生し、そのインターフェイスがスタンバイ グループに属している場合は、スタンバイ インターフェイスがトラフィックを伝送し、障害の生じたインターフェイスの負荷を担うことができます。スタンバイ インターフェイスを設定すると、ある時点でただ 1 つのインターフェイスだけが使用中になります。

スタンバイ インターフェイスを設定するには、各物理インターフェイスをスタンバイ グループに割り当てる必要があります。次の動作に関する考慮事項は、スタンバイ グループに適用されます。

- スタンバイ グループは、物理インターフェイスから構成されます。
- Wide Area Application Service（WAAS）デバイス上のスタンバイ グループの最大数は 1 です。
- スタンバイ グループには、グループのすべてのメンバーが共有する固有のスタンバイ IP アドレスが割り当てられます。
- スタンバイ グループに属するインターフェイスの二重性と速度を設定すると、信頼性が向上します。
- スタンバイ グループに属する物理インターフェイスで、IP ACL を設定できます。
- スタンバイ グループの 1 つのインターフェイスがプライマリ スタンバイ インターフェイスに指定されます。プライマリ インターフェイスだけが、グループ IP アドレスを使用します。
- 使用中のインターフェイスに障害が発生した場合、そのスタンバイ グループにある別のインターフェイスが引き継ぎ、トラフィックを伝送します。
- スタンバイ グループのすべてのメンバーで障害が生じ、その後、1 つが回復した場合、WAAS ソフトウェアは、動作状態のインターフェイスでスタンバイ グループを起動します。
- スタンバイ グループ内のプライマリ インターフェイスは、実行時に変更できます（デフォルトの動作では、異なるインターフェイスがプライマリになった場合、現在使用中インターフェイスが優先的に使用されます）。
- 物理インターフェイスがスタンバイ グループのメンバーである場合、同時にポート チャネルのメンバーになることはできません。

- 1 つの IP アドレスをスタンバイ グループとポート チャネルの両方に割り当てることはできません。1 つの IP アドレスで設定できる仮想インターフェイスは 1 つだけです。
- VLAN タギング プロトコルを使用し、同じ VLAN タグを各インターフェイスに割り当てた場合、スタンバイ グループに属するインターフェイスは異なるスイッチに接続できます。

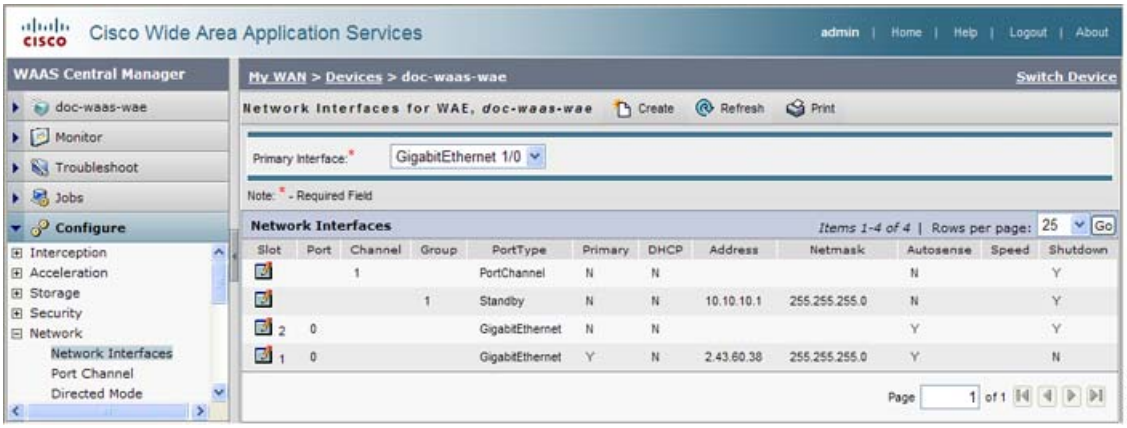
スタンバイ インターフェイスを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　スタンバイ インターフェイスを設定するデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。デバイス用の [Network Interfaces] ウィンドウが表示されます（図 5-1 を参照）。

図 5-1　[Device] ウィンドウのネットワーク インターフェイス



ステップ 4　タスクバーで、[Create New Interface] アイコンをクリックします。[Creating New Network Interface] ウィンドウが表示されます。

ステップ 5　[Port Type] ドロップダウン リストから、[Standby] を選択します。ウィンドウが更新され、スタンバイ グループ設定を構成するためのフィールドが表示されます。

ステップ 6　[Address] フィールドで、スタンバイ グループの IP アドレスを指定します。

ステップ 7　[Netmask] フィールドで、スタンバイ グループのネットマスクを指定します。

ステップ 8　[Shutdown] チェックボックスを選択して、ハードウェア インターフェイスを停止します。このオプションはデフォルトで無効になっています。

ステップ 9　[Gateway] フィールドで、デフォルト ゲートウェイ IP アドレスを入力します。インターフェイスが DHCP 用に設定されている場合、このフィールドは読み取り専用です。

ステップ 10　[Submit] をクリックします。

ステップ 11　「プライマリ スタンバイ インターフェイスの設定」（P.5-4）の説明に従って、インターフェイスの優先順位を設定します。

プライマリ スタンバイ インターフェイスの設定

WAAS Central Manager GUI を使用して論理スタンバイ インターフェイスを設定したあとで、物理インターフェイスをスタンバイ グループに参加させ、1 つの物理インターフェイスをプライマリ スタンバイ インターフェイスに設定することで、スタンバイ グループを設定します。スタンバイ グループのプライマリ インターフェイスは、スタンバイ グループの IP アドレスを使用します。インターフェイスをプライマリに設定する前に、スタンバイ インターフェイス設定されている必要があります（「スタンバイ インターフェイスの設定」（P.5-2）を参照してください）。

インターフェイスをスタンバイ グループに関連付け、プライマリ スタンバイ インターフェイスに設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

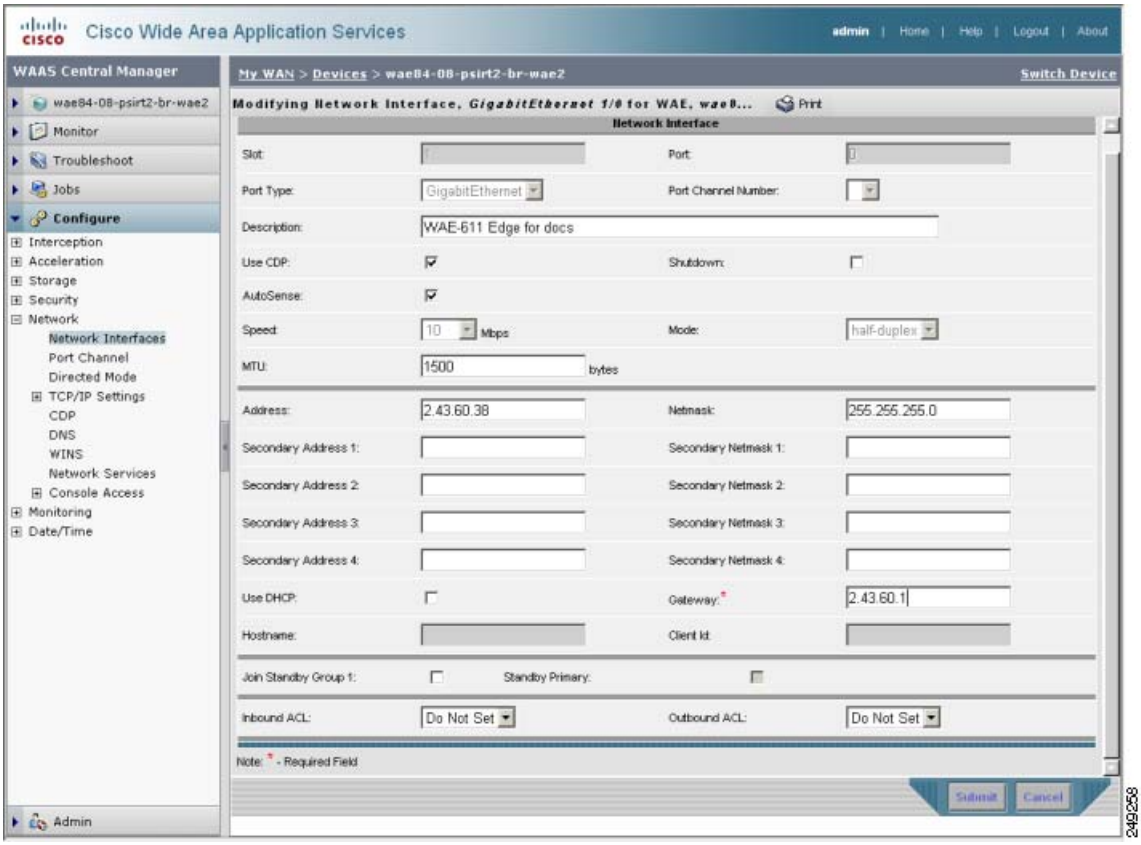
ステップ 2　スタンバイ インターフェイスを設定するデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。デバイス用の [Network Interfaces] ウィンドウが表示されます。

ステップ 4　スタンバイ グループに参加させる物理インターフェイスの横にある [Edit] アイコンをクリックします。[Modifying Network Interface] ウィンドウが表示されます（図 5-2 を参照）。

この手順で、論理インターフェイス（スタンバイまたはポート チャネル）を選択しないでください。

図 5-2　[Modifying Network Interface] ウィンドウ



ステップ 5　インターフェイスをスタンバイ グループに参加させ、プライマリ スタンバイ インターフェイスに指定するには、次の手順に従ってください。

a. [Join Standby Group 1] チェックボックスを選択します。

b. （任意）インターフェイスをスタンバイ グループのプライマリ（アクティブ）インターフェイスにする場合は、[Standby Primary] チェックボックスを選択します。

ステップ 6　[Submit] をクリックします。

1 つのインターフェイスへの複数の IP アドレスの設定

1 つのインターフェイスに、最大 4 つのセカンダリ IP アドレスを設定できます。この設定によりデバイスが複数のサブネットに存在でき、データをルータでリダイレクションせずに、WAAS デバイスから、情報を要求するクライアントへ直接転送できるので、デバイスを使用して応答時間を最適化できます。また、WAAS デバイスとクライアントは同じサブネット上に設定されるため、クライアントから WAAS デバイスを認識できます。

1 つのインターフェイスに複数の IP アドレスを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　インターフェイスを設定するデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。[Network Interfaces] リスト ウィンドウが表示されます。

ステップ 4　変更するギガビット イーサネット物理インターフェイス用の [Edit] アイコンをクリックします。[Modifying Network Interface] ウィンドウが表示されます。

（注）　この手順で、論理インターフェイス（スタンバイまたはポート チャネル）を選択しないでください。論理インターフェイスには、複数のインターフェイスを設定できません。

ステップ 5　[Secondary Address] および [Secondary Netmask] フィールド 1 ～ 4 で、インターフェイス用の最大 4 つの IP アドレスとセカンダリ ネットマスクを入力します。

ステップ 6　[Submit] をクリックします。

ギガビット イーサネット インターフェイス設定の変更

既存のギガビット イーサネット インターフェイスの設定を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

WAAS ネットワークに設定されているすべてのデバイス タイプを表示する [Devices] ウィンドウが表示されます。

ステップ 2　インターフェイス設定を変更するデバイスの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。

[Network Interfaces] ウィンドウが表示され、特定のスロットとポートに設定されているネットワーク インターフェイスが表示されます。

（注）　On an NME-WAE デバイスでは、ルータへの内部インターフェイスはスロット 1、ポート 0 に指定され、外部インターフェイスはスロット 2、ポート 0 に指定されます。設定の詳細については、『*Configuring Cisco WAAS Network Modules for Cisco Access Routers*』を参照してください。

ステップ 4　変更するギガビット イーサネット インターフェイスの横にある [Edit Network Interface] アイコンをクリックします。

[Modifying Network Interface] ウィンドウが表示され、特定のスロットとポート上のインターフェイス設定が表示されます（図 5-2 を参照）。

（注）　ウィンドウの一部のフィールドは、使用できません。スロット、ポート、およびポートの種類用のインターフェイス設定は、最初の起動時または WAAS CLI を使用して物理インターフェイス用に設定されます。

（注）　NME-WAE デバイスで内部インターフェイス（GigabitEthernet 1/0）を設定するときは、[Port Channel Number]、[AutoSense]、[Speed]、[Mode]、[Address]、[Netmask]、[Use DHCP]、および [Standby Group] フィールドまたはチェックボックスは変更できません。これらの値を変更して [Submit] をクリックすると、Central Manager はエラーを表示します。内部インターフェイスのこれらの設定は、ホスト ルータ CLI を使用しないと設定できません。詳細については、『*Configuring Cisco WAAS Network Modules for Cisco Access Routers*』を参照してください。

ステップ 5　インターフェイスで CDP を有効にするには、[Use CDP] チェックボックスを選択します。

有効にすると、CDP は、ネイバー デバイスのプロトコル アドレスを取得し、それらのデバイスのプラットフォームを検出します。また、ルータが使用するインターフェイスに関する情報を表示します。

[CDP Settings] ウィンドウから CDP を設定すると、CDP がすべてのインターフェイスでグローバルに有効になります。CDP 設定を構成する方法については、「CDP 設定の構成」（P.5-14）を参照してください。

ステップ 6　[Shutdown] チェックボックスを選択して、ハードウェア インターフェイスを停止します。

ステップ 7　速度とモードを自動ネゴシエーションするようにインターフェイスを設定するには、[AutoSense] チェックボックスを選択します。

このチェックボックスを選択すると、手動の [Speed and Mode] ドロップダウン リスト設定が無効になります。

（注）　自動感知が有効の場合、手動設定が変更されます。自動感知を開始するには、WAAS デバイスをリブートする必要があります。

ステップ 8　インターフェイスの伝送速度設定とモード設定を手動で構成するには、次の手順に従ってください。

a.　[AutoSense] チェックボックスの選択を解除します。

b.　[Speed] ドロップダウン リストから、伝送速度（[10]、[100]、または [1000] Mbps）を選択します。

c.　[Mode] ドロップダウン リストから、送信モード（[full-duplex] または [half-duplex]）を選択します。

全二重送信では、インターフェイスまたはケーブルを通じて、データを同時に両方の方向に伝送できます。半二重設定では、ある時点でデータが片方の方向だけに伝送されることが保証されます。全二重の方が高速ですが、インターフェイスがこのモードで効果的に動作できない場合があります。過度の衝突やネットワーク エラーが発生する場合は、インターフェイスを全二重でなく、半二重に設定してください。

（注） WAE、ルータ、スイッチ、またはその他のデバイスでは半二重接続を使用しないことを強く推奨します。半二重接続の場合はパフォーマンスが低下するので、使用は避けてください。各 Cisco WAE インターフェイスおよび隣接デバイス（ルータ、スイッチ、ファイアウォール、WAE）のポート設定を調べて、全二重接続が使用されていることを確認してください。

ステップ 9　[MTU] フィールドに値（バイト単位）を指定して、インターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズを設定します。

範囲は、88 ～ 1500 バイトです。MTU は、特定のデータ リンク接続を使用して転送できる IP データグラムの最大サイズです。

ステップ 10　[Address] フィールドに新しい IP アドレスを入力して、インターフェイス IP アドレスを変更します。

ステップ 11　[Netmask] フィールドに新しいネットマスクを入力して、インターフェイス ネットマスクを変更します。

ステップ 12　[Submit] をクリックします。

ポート チャネル設定の構成

WAFS ソフトウェアでは、最大 4 個の同じ速度のネットワーク インターフェイスを 1 つの仮想インターフェイスにグループ化することができます。このグループ化機能によって、2 つのギガビット イーサネット インターフェイスから構成される 1 つの仮想インターフェイスを設定または削除することができます。また、この機能は、Cisco ルータ、スイッチ、およびその他のネットワーキング デバイスやホストと相互運用可能で、各インターフェイスの現在のリンク ステータスに基づいて、EtherChannel、ロード バランシング、障害の自動検出と回復をサポートします。EtherChannel は、「ポート チャネル」とも呼びます。

ポート チャネル設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　インターフェイスを設定するデバイスの名前の横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。[Network Interfaces] ウィンドウが表示され、選択したデバイス用のすべてのインターフェイスが表示されます。

ステップ 4　タスクバーで、[Create New Interface] アイコンをクリックします。[Creating New Network Interface] ウィンドウが表示されます。

ステップ 5　[Port Type] ドロップダウン リストから、[Port Channel] を選択します。

ウィンドウが更新され、ネットワーク インターフェイス設定を構成するためのフィールドが表示されます。

ステップ 6　[Port Channel Number] ドロップダウン リストで、ポート チャネル インターフェイス番号 [1] を選択します（サポートされるポート チャネルは 1 つだけです）。

ステップ 7　[Shutdown] チェックボックスを選択して、このインターフェイスを停止します。このオプションはデフォルトで無効になっています。

ステップ 8　[Gateway] フィールドで、デフォルト ゲートウェイ IP アドレスを入力します。

ステップ 9　[Address] フィールドで、インターフェイスの IP アドレスを指定します。

ステップ 10　[Netmask] フィールドで、インターフェイスのネットマスクを指定します。

ステップ 11　（任意）[Inbound ACL] ドロップダウン リストから、着信パケットに適用する IP ACL を選択します。ドロップダウン リストには、システムに設定されているすべての IP ACL が表示されています。

ステップ 12　（任意）[Outbound ACL] ドロップダウン リストから、発信パケットに適用する IP ACL を選択します。

ステップ 13　[Submit] をクリックします。

次の動作に関する考慮事項は、ポート チャネル仮想インターフェイスに適用されます。

- 物理インターフェイスはポート チャネルまたはスタンバイ グループのメンバーになれますが、同時に両方のメンバーになることはできません。
- 1 つの IP アドレスをポート チャネルとスタンバイ グループの両方に割り当てることはできません。1 つの IP アドレスで設定できる仮想インターフェイスは 1 つだけです。

（注）　両方のデバイス インターフェイスがポートチャネル インターフェイスとして設定されている場合は、自動登録を無効にする必要があります。

DHCP 用のインターフェイスの設定

（注）　手動で DHCP 用にインターフェイスを設定する前に、自動登録を無効にする必要があります。

WAAS デバイスは、ネットワーク情報を要求するときに、設定されているクライアント ID とホスト名を DHCP サーバへ送信します。WAAS デバイスが送信しているクライアント ID 情報とホスト名情報を識別し、WAAS デバイスに割り当てられている特定のネットワーク設定を返信するように、DHCP サーバを設定できます。

DHCP 用のインターフェイスを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　インターフェイス設定を行うデバイスの名前の横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。[Network Interfaces] リスト ウィンドウが表示されます。

ステップ 4　変更するギガビット イーサネット物理インターフェイス用の [Edit] アイコンをクリックします。[Modifying Network Interface] ウィンドウが表示されます。

（注）　論理インターフェイスには DHCP を設定できないため、この手順では論理インターフェイス（スタンバイまたはポート チャネル）を選択しないでください。また、内部インターフェイスはホスト ルータ CLI を使用しないと設定できないため、NME-WAE デバイスでは内部インターフェイス（GigabitEthernet 1/0）を選択しないでください。詳細については、『*Configuring Cisco WAAS Network Modules for Cisco Access Routers*』を参照してください。

ステップ 5　ウィンドウを下方向へ移動し、[Use DHCP] チェックボックスを選択します。

このチェックボックスを選択すると、セカンダリ IP アドレスとネットマスクのフィールドが無効になります。

ステップ 6　[Hostname] フィールドで、WAAS デバイスまたは他のデバイスのホスト名を指定します。

ステップ 7　[Client Id] フィールドで、デバイス用に設定されているクライアント ID を指定します。

DHCP サーバは、WAAS デバイスがデバイス用のネットワーク情報を要求するとき、この ID を使用します。

ステップ 8　[Submit] をクリックします。

インターフェイス用のロード バランシング方式の設定

ロード バランシングを設定する前に、「ポート チャネル設定の構成」（P.5-7）の説明に従って、ポート チャネルが設定されていることを確認してください。

ロード バランシングを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　ロード バランシングを設定するポート チャネルを持つデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Port Channel] を選択します。

ステップ 4　[Load Balancing Method] ドロップダウン リストから、ロード バランシング方式を選択します。

- [round robin]：ラウンド ロビン方式によって、チャネル グループ内のすべてのインターフェイスにトラフィックを均等に分散できます。他のロード バランシング方式を使用すると、イーサネット フレームを送信するときに、（IP アドレスで）特定のインターフェイスを柔軟に選択できます。このオプションは、デフォルトで選択されています。
- [src-dst-ip-port]：分散機能は、送信元および宛先 IP アドレス / ポートの組み合わせに基づいて実行されます。WAAS バージョン 4.1.3 以降が稼動するデバイスでは、dst-ip 方式がこのロード バランシング方式に置き換わりました。

ステップ 5　[Submit] をクリックします。

CLI からロード バランシング方式を設定するには、**port-channel** グローバル コンフィギュレーション コマンドを使用できます。

TCP 設定の構成

クライアントとサーバ間のデータ トランザクションや照会では、ウィンドウとバッファのサイズが重要であるため、TCP スタック パラメータを調整してキャッシュ パフォーマンスを最大化します。

TCP パラメータは複雑であるため、これらのパラメータを調整するときは注意してください。ほとんどすべての環境で、デフォルトの TCP 設定は適切です。TCP 設定の調整は、適切な経験を持ち、TCP の動作を完全に理解しているネットワーク管理者が行ってください。

TCP および IP 設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　TCP 設定を構成する WAAS デバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [TCP/IP Settings] > [TCP/IP] を選択します。[TCP/IP Settings] ウィンドウが表示されます

ステップ 4　TCP 設定に必要な変更を行います。

このウィンドウの各 TCP フィールドの説明については、表 5-1 を参照してください。

ステップ 5　[Submit] をクリックします。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] をクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

表 5-1　TCP 設定

TCP 設定	説明
[TCP General Settings]	
[Enable Explicit Congestion Notification]	データ送信の遅延やパケット損失を軽減します。これにより、RFC 2581 に対応した TCP がサポートされます。このオプションはデフォルトで無効になっています。詳細については、「明示的輻輳通知について」（P.5-11）を参照してください。
[Initial Send Congestion Window Size]	初期の輻輳ウィンドウ サイズの値（セグメント数）。範囲は、1 ～ 10 セグメントです。デフォルトは、2 セグメントです。詳細については、「輻輳ウィンドウ」（P.5-11）を参照してください。
[ReTransmit Time Multiplier]	TCP アルゴリズムが決定する基数を 1 ～ 3 倍して、再送信タイマーの長さを変更するために使用する係数。デフォルトは 1 です。再送信タイマーの長さは変更されません。範囲は、1 ～ 3 です。詳細については、「再送信時間倍率」（P.5-11）を参照してください。 **（注）**　この係数の変更には、注意が必要です。信頼性の高い低速の接続で TCP を使用するときはスループットが向上しますが、信頼性の低いパケット配信環境では変更しないでください。
[Keepalive Probe Count]	接続が失敗と見なされる前に WAAS デバイスが接続を再試行できる回数。範囲は、1 ～ 120 回です。デフォルトは、4 回です。

表 5-1　TCP 設定 （続き）

TCP 設定	説明
[Keepalive Probe Interval]	WAAS デバイスがアイドル状態の接続を開いておく時間の長さ。デフォルトは、75 秒です。
[Keepalive Timeout]	WAAS デバイスが切断する前に接続を開いておく時間の長さ。範囲は、1 ～ 120 秒です。デフォルトは、90 秒です。
[Enable Path MTU Discovery]	さまざまなリンク間の転送パスに沿って許容可能な最大サイズの IP パケットを検出できるようにし、パケット サイズの正しい値を自動的に設定します。このオプションはデフォルトで無効になっています。詳細については、「パス MTU 検出」（P.5-12）を参照してください。

CLI から TCP 設定を構成するには、**tcp** グローバル コンフィギュレーション コマンドを使用できます。

CLI から MTU 検出ユーティリティを有効にするには、**ip path-mtu-discovery enable** グローバル コンフィギュレーション コマンドを使用できます。

ここでは、次の内容について説明します。

明示的輻輳通知について

TCP の Explicit Congestion Notification（ECN; 明示的輻輳通知）機能では、中間のルータが末端のホストに差し迫ったネットワーク輻輳を通知できます。また、この機能は、遅延やパケット損失の影響を受けやすいアプリケーションに関連する TCP セッションのサポートを強化します。ECN に関する主な問題は、ECN の動作に対応するために、ルータと TCP ソフトウェア スタックの両方の動作を変更する必要があることです。

輻輳ウィンドウ

輻輳ウィンドウ（*cwnd*）は、TCP 送信側が、TCP 伝送の受信側から Acknowledgment（ACK; 確認応答）を受信する前に、ネットワークへ送信できるデータ量を制限する TCP 状態変数です。TCP *cwnd* 変数は、TCP 輻輳回避アルゴリズムによって実装されます。輻輳回避アルゴリズムの目的は、送信側がデータのフロー全体の中で使用できるネットワーク容量の増減を自動的に感知して、送信速度を継続的に変更することです。（パケット損失として）輻輳が発生すると、送信速度が引き下げられ、送信側がネットワークの追加容量を継続的に検査しながら次第に引き上げられます。

再送信時間倍率

TCP 送信側は、タイマーを使用して、データ セグメントを送信してから、TCP 伝送の受信側から対応する ACK を受信するまでに経過する時間を測定します。この再送信タイマーがタイムアウトすると、送信側は、（TCP 輻輳制御に関する RFC 規格に従って）送信速度を下げる必要があります。ただし、

送信側は、ネットワーク輻輳に応えて送信速度を下げないため、ネットワークの現在の状態に関する有効な仮定を行うことができません。したがって、必要以上に大量のデータを送信してネットワークが輻輳するのを防止するために、送信側は、1 回の送信当たりの送信速度を 1 セグメントに下げるスロー スタート アルゴリズムを実装します（「TCP スロー スタート」（P.5-12）を参照してください）。

WAAS Central Manager GUI の [Retransmit Time Multiplier] フィールドを使用して、送信側の再送信タイマーを変更できます。再送信時間倍率は、輻輳制御用に使用している TCP アルゴリズム決定に従って、基数の 1 ～ 3 倍の範囲で再送信タイマーの長さを変更します。

再送信タイマーを調整するときは、パフォーマンスと効率に影響することに注意してください。再送信タイマーが短すぎると、送信側は必要以上にネットワークに重複データを送信し、再送信タイマーが長すぎると、送信側は必要以上にアイドル状態に留まり、データのフローが遅くなります。

TCP スロー スタート

スロー スタートは、TCP が使用する 4 つの輻輳制御アルゴリズムの中の 1 つです。スロー スタート アルゴリズムは、ネットワークの容量が不明なときに、TCP セッションの開始時にネットワークに送信するデータ量を制御します。

たとえば、TCP セッションの開始時にネットワークに大量のデータを送信すると、そのほとんどが失われる場合があります。その代わりに、TCP は、最初に控えめな量のデータを送信するので、送信が成功する確率が高くなります。次に、TCP は、ネットワークが輻輳している徴候がない限り、送信するデータ量を増やしてネットワークを検査します。

スロー スタート アルゴリズムは、最初に輻輳ウィンドウ（*cwnd*）変数で決定される速度でパケットを送信します（「輻輳ウィンドウ」（P.5-11）を参照してください）。アルゴリズムは、スロー スタートしきい値（*ssthresh*）変数で設定された制限値に到達するまで、送信速度を上げていきます。*ssthresh* 変数の値は、受信側の最大セグメント サイズ（RMSS）に初期設定されます。ただし、輻輳が発生すると、*ssthresh* 変数は、*cwnd* 変数の現在の値の半分に設定され、ネットワーク輻輳の新しい指標になります。

cwnd 変数の値は、送信側が送信できる最大セグメントのサイズである送信側の最大セグメント サイズ（SMSS）に初期設定されます。送信側は 1 つのデータ セグメントを送信し、輻輳ウィンドウは 1 セグメントのサイズに等しいため一杯になります。次に、送信側は、伝送の受信側からの対応する ACK を待ちます。ACK を受信したら、送信側が、1 SMSS 分だけ *cwnd* 変数の値を大きくすることによって、その輻輳ウィンドウ サイズを増やします。これで、送信側は、輻輳ウィンドウは再び一杯になる前に 2 つのセグメントを送信でき、これらのセグメントに対応する ACK を待ちます。スロー スタート アルゴリズムは、ACK を受信するたびに 1 SMSS だけ *cwnd* 変数の値を増やして、輻輳ウィンドウのサイズを増やしていきます。*cwnd* 変数の値が *ssthresh* 変数の値を超えると、TCP フロー制御アルゴリズムが、スロー スタート アルゴリズムから輻輳回避アルゴリズムへ変化します。

パス MTU 検出

WAAS ソフトウェアは、RFC 1191 に規定された IP パス MTU 検出方式をサポートしています。有効にすると、パス MTU 検出機能は、さまざまなリンク間の転送パスに沿って許容可能な最大サイズの IP パケットを検出し、パケット サイズの正しい値を自動的に設定します。リンクが処理できる最大 MTU を使用することで、送信側デバイスは、送信する必要があるパケットの数を最小限に抑えることができます。

IP パス MTU 検出は、ネットワークでリンクが停止し、別の異なる MTU サイズのリンクを使用しなければならない場合に有用です。また、IP パス MTU 検出は、接続が初めて確立され、送信側が中間に存在するリンクに関する情報を持っていない場合にも有用です。

（注）　IP パス MTU 検出は、送信側デバイスが開始するプロセスです。サーバが IP パス MTU 検出をサポートしていない場合、受信側デバイスには、サーバによって生成されるデータグラムの断片化を避ける手段がありません。

デフォルトで、この機能は無効になっています。この機能を無効にすると、送信側デバイスは、576 バイトかネクストホップ の MTU のどちらか小さい方のパケット サイズを使用します。この機能を有効または無効にしても、既存の接続に影響しません。

固定 IP ルートの設定

WAAS ソフトウェアを使用すると、ネットワークまたはホスト用の固定ルートを設定できます。指定した送信先のすべての IP パケットが、設定されたルートを使用します。

固定 IP ルートを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Devices Group]）を選択します。

ステップ 2　設定するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [TCP/IP Settings] > [Static Routes] を選択します。[IP Route Entries] ウィンドウが表示されます。

ステップ 4　タスクバーで、[Create New IP Route Entry] アイコンをクリックします。[Creating New IP Route] ウィンドウが表示されます。

ステップ 5　[Destination Network Address] フィールドに、送信先のネットワーク IP アドレスを入力します。

ステップ 6　[Netmask] フィールドに、送信先ホストのネットマスクを入力します。

ステップ 7　[Gateway's IP Address] フィールドに、ゲートウェイ インターフェイスの IP アドレスを入力します。

ゲートウェイ インターフェイスの IP アドレスは、いずれかのデバイスのネットワーク インターフェイスと同一のネットワークにある必要があります。

ステップ 8　[Submit] をクリックします。

CLI から固定ルートを設定するには、**ip route** グローバル コンフィギュレーション コマンドを使用できます。

IP ルートの集約

各 WAE デバイスに IP ルートを定義して、他の IP ルートが定義されたデバイス グループに所属させることができます。

[IP Route Entries] ウィンドウの [Aggregate Settings] オプション ボタンは、各デバイスの IP ルートを集約する方法を制御します。

- デバイスをそのデバイス自体および所属するデバイス グループに定義されているすべての IP ルートで設定する場合は、[Yes] を選択します
- デバイスをそのデバイス自体に定義されている IP ルートだけに制限する場合は、[No] を選択します。

設定を変更すると次のメッセージが表示されます。「This option will take effect immediately and will affect the device configuration. Do you wish to continue?」。[OK] をクリックして続行します。

CDP 設定の構成

CDP は、すべてのシスコ デバイス上で稼動するデバイス検出プロトコルです。CDP を使用すると、ネットワーク内の各デバイスは、ネットワーク内の他のすべてのデバイスに定期的にメッセージを送信します。すべてのデバイスは、その他のデバイスが送信した定期的なメッセージを受信して、ネイバー デバイスについて学習し、それらのインターフェイスのステータスを判断します。

CDP を使用して、ネットワーク管理アプリケーションは、ネイバー デバイスのデバイス タイプと Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）エージェント アドレスを学習できます。アプリケーションは、ネットワーク内に SNMP クエリーを送信できます。また、CiscoWorks2000 は、起動後に WAAS デバイスが送信した CDP パケットを使用して、WAAS デバイスを検出します。

デバイス関連の作業では、WAAS デバイス プラットフォームの存在、種類、およびバージョンをシステム マネージャに通知できるように、WAAS デバイス プラットフォームが CDP をサポートしている必要があります。

CDP 設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [CDP] を選択します。[CDP Settings] ウィンドウが表示されます

ステップ 4　[Enable] チェックボックスを選択して、CDP サポートを有効にします。デフォルトで、このオプションは有効になっています。

ステップ 5　[Hold Time] フィールドに、受信側が CDP パケットを保持する時間の長さを指定する時間（秒）を入力します。

範囲は、10 ～ 255 秒です。デフォルトは、180 秒です。

ステップ 6　[Packet Send Rate] フィールドに、CDP アドバタイズメントの間隔（秒）を入力します。

範囲は、5 ～ 254 秒です。デフォルトは、60 秒です。

ステップ 7　[Submit] をクリックします。

CLI から CDP 設定を構成するには、**cdp** グローバル コンフィギュレーション コマンドを使用できます。

DNS サーバの設定

DNS を使用すると、ネットワークは、要求に入っているドメイン名をそれに関連する IP アドレスに変換できます。WAAS デバイスで DNS を設定するには、次の作業を完了する必要があります。

- ネットワークが、要求されたドメイン名を、WAAS デバイスがドメイン名を解決するために使用する必要がある IP アドレスに変換するために使用する、DNS サーバのリストを指定します。
- WAAS デバイスで DNS を有効にします。

WAAS デバイス用の DNS サーバ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [DNS] を選択します。[DNS Settings] ウィンドウが表示されます。

ステップ 4　[Local Domain Name] フィールドに、ローカル ドメインの名前を入力します。最大 3 つのローカル ドメイン名を設定できます。リスト内の項目をスペースで区切ります。

ステップ 5　[List of DNS Servers] フィールドに、ネットワークがホスト名を IP アドレスに解決するために使用する DNS サーバのリストを入力します。

最大 3 台の DNS サーバを設定できます。リスト内の項目をスペースで区切ります。

ステップ 6　[Submit] をクリックします。

デフォルトおよびデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤色で表示されます。以前のウィンドウ設定に戻すには、[Reset] をクリックします。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

CLI から DNS ネーム サーバを設定するには、**ip name-server** グローバル コンフィギュレーション コマンドを使用できます。

Windows ネーム サービスの設定

デバイスまたはデバイス グループ用の Windows ネーム サービスを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　Windows ネーム サービスを設定するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [WINS] を選択します。[Windows Name Services Settings] ウィンドウが表示されます。

ステップ 4　[Workgroup or Domain Name] フィールドに、選択したデバイスまたはデバイス グループが存在するワークグループ（またはドメイン）の名前を入力します。

この名前は、127 文字以内の短縮形で入力する必要があります。有効な文字は、英数字、円（¥）、アンダースコア（_）、およびハイフン（-）です。

たとえば、ドメイン名が cisco.com の場合、短縮形は cisco です。

ステップ 5　ワークグループまたはドメインが Windows NT 4 ドメインの場合は、[NT] チェックボックスを選択します。たとえば、ドメイン名が cisco.com の場合、短縮形は cisco です。ワークグループまたはドメインが Windows 2000 または Windows 2003 ドメインの場合は、[NT] チェックボックスを選択しないでください。このオプションはデフォルトで無効になっています。

ステップ 6　[WINS server] フィールドに、Windows Internet Naming Service（WINS）サーバのホスト名または IP アドレスを入力します。

ステップ 7　[Submit] をクリックします。

CLI から Windows ネーム サービスを設定するには、**windows-domain** グローバル コンフィギュレーション コマンドを使用できます。

directed モードの設定

デフォルトでは、WAAS はピア WAE との新規 TCP 接続を透過的に設定します。これにより、WAAS デバイスがトラフィックを最適化しようとする際、ファイアウォール トラバースに関する問題が発生することがあります。WAE デバイスがトラフィックの最適化を阻止するファイアウォールの背後にある場合、ピア WAE への通信に directed モードを使用できます。directed モードでは、ピア WAE に送信されるすべての TCP トラフィックは UDP にカプセル化されるため、ファイアウォールはトラフィックをバイパスするか、トラフィックを検査できます（UDP 検査ルールを追加して）。

2 つの WAE ピア間のすべてのファイアウォールを、ポート 4050 で、またはデフォルト以外のポートが使用されている場合は directed モードに設定されているすべてのカスタム ポートで、UDP トラフィックを通過させるように設定する必要があります。また、directed モードで UDP トラフィックの送信が開始される前に、WAAS 自動ディスカバリ プロセスで TCP オプションが使用されるため、ファイアウォールは TCP オプションを通過させるように設定する必要があります。シスコのファイアウォールは、**ip inspect waas** コマンド（IOS 12.4(11)T2 以降の場合）または **inspect waas** コマンド（FWSM 3.2(1) 以降および PIX 7.2(3) 以降の場合）を使用することで、TCP オプションを許可するように設定できます。

WAN パケットは UDP を使用して WAE 間で直接ルーティングされますが、directed モードをアクティブにしたあと、WAE は LAN から送信されたパケットだけを透過的に代行受信します。

directed モードは、設定可能なすべてのトラフィック代行受信方法で動作します。directed モードでは、WAAS デバイス（または Cisco WAE Inline Network Adapter）をルーティング可能な非 NAT IP アドレスで設定する必要があります。directed モードをインライン モードとともに使用する場合、インターフェイス上で Cisco WAE Inline Network Adapter をルーティング可能 IP アドレスで設定する必要があります。このように設定しないと、トラフィックはブラック ホール化されます。

ピア WAE 接続のどちらかの端の WAE が directed モードに指定されていて、両方の WAE が directed モードをサポートする場合、明示的に directed モードが設定されていなくても、両方の WAE が directed モードを使用します。ピア WAE が directed モードをサポートしていない場合、ピアは最適化されていないトラフィックを通過させ、各 WAE が directed モードの試行に失敗したことを記述したトランザクション ログ エントリを作成します。

directed モード動作は、次の方法で起動できます。

- WAAS Central Manager GUI または CLI で、directed モードを明示的にアクティブにできます。
- ピア WAE が directed モードの使用を要求したときに、directed モードを自動的に起動できます。

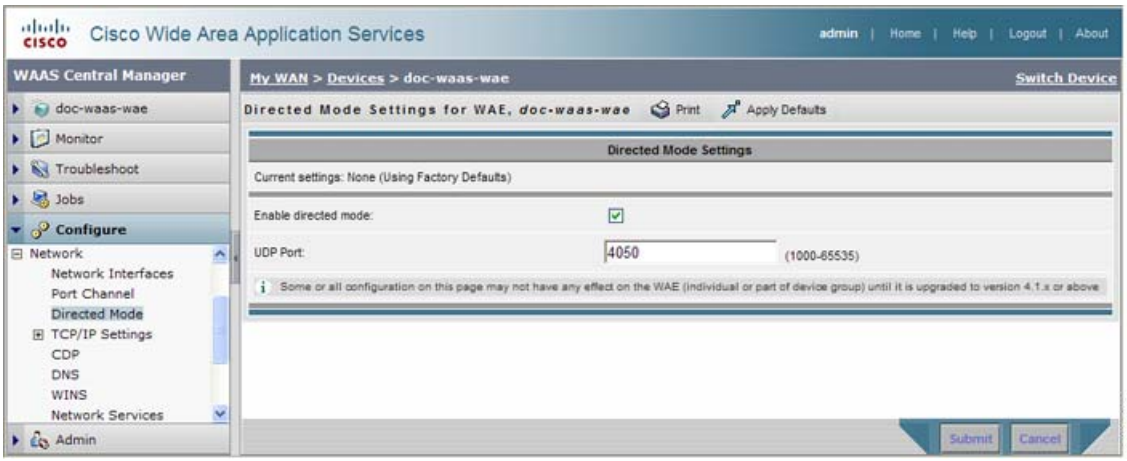
directed モードをアクティブにするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　directed モードを設定するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Directed Mode] を選択します。[Directed Mode Settings] ウィンドウが表示されます（図 5-3 を参照）。

図 5-3　[Directed Mode Settings] ウィンドウ



ステップ 4　[Enable directed mode] チェックボックスを選択して、directed モードをアクティブにします。

ステップ 5　[UDP Port] フィールドにポート番号を入力して、directed モード用のカスタム UDP ポートを設定します。デフォルトは、ポート 4050 です。

ステップ 6　[Submit] をクリックして、設定を保存します。

CLI から directed モードを設定するには、**directed-mode** グローバル コンフィギュレーション コマンドを使用します。

CHAPTER 6

管理ログインの認証、許可、およびアカウンティングの設定

この章では、Wide Area Application Service（WAAS）デバイス用の管理ログインの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）を設定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 Central Manager GUI を使用して、WAAS デバイス用の 2 種類の管理者ユーザ アカウント（デバイスに基づく CLI アカウントとロールに基づくアカウント）を一元的に作成し、管理します。詳細については、第 7 章「管理者ユーザ アカウントおよびグループの作成と管理」を参照してください。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

管理ログインの認証および許可について

WAAS ネットワークでは、管理的ログイン認証と許可を使用して、設定、モニタ、またはトラブルシューティング用に WAAS デバイスにアクセスしたい管理者からのログイン要求を制御します。

ログイン認証とは、WAAS デバイスが、デバイスにログインしようとしている管理者が有効なユーザ名とパスワード持っているかどうかを確認するプロセスです。ログインしようとする管理者は、デバイスに登録されたユーザ アカウントを持つ必要があります。ユーザ アカウント情報は、ユーザの管理ログインと設定特権を許可する役割を果たします。ユーザ アカウント情報は AAA データベースに保存され、AAA データベースが存在する特定の認証サーバにアクセスするように WAAS デバイスを設定する必要があります。ユーザがデバイスにログインしようとすると、デバイスは、そのユーザのユーザ名、パスワード、および特権レベルをデータベースに保存されたユーザ アカウント情報と比較します。

WAAS ソフトウェアは、外部アクセス サーバ（たとえば、RADIUS または TACACS+ サーバ）を持つユーザと AAA 機能を持つローカル アクセス データベースが必要なユーザに対して次の認証、許可、アカウンティング（AAA）サポートを提供します。

- 認証（またはログイン認証）は、ユーザが誰であるかを決定する処理です。ユーザ名とパスワードを検査します。
- 許可（または設定）は、ユーザが許可されていることを決定する処理です。ネットワーク内で認証されたユーザに対して権限を許可または拒否します。一般に、認証の後で許可が実行されます。ユーザがログインするには、認証と許可の両方が必要です。
- アカウンティングは、システム アカウンティングを目的に管理ユーザの作業を追跡する処理です。WAAS ソフトウェアでは、TACACS+ による AAA アカウンティングがサポートされています。詳細については、「WAAS デバイス用の AAA アカウンティングの設定」（P.6-33）を参照してください。

（注）　管理者は、コンソール ポートまたは WAAS Central Manager GUI を使用して WAAS Central Manager デバイスにログインできます。管理者は、コンソール ポートまたは WAE Device Manager GUI を使用して、データセンター WAE またはブランチ オフィス WAE として機能する WAAS デバイスにログインできます。

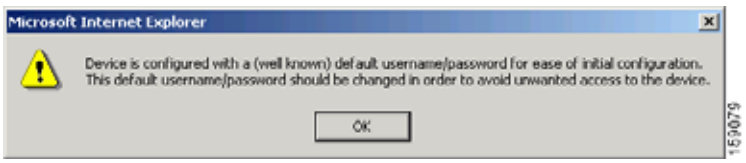
認証と許可が設定される前にシステム管理者が WAAS デバイスにログインするとき、管理者は定義済みの superuser アカウントを使用して WAAS デバイスにアクセスできます（定義済みのユーザ名は admin、定義済みのパスワードは default です）。この定義済みの superuser アカウントを使用して WAAS デバイスにログインするとき、WAAS システム内のすべての WAAS サービスとエンティティへのアクセスが許可されます。

（注）　WAAS デバイスごとに、ユーザ名が admin の 1 つの管理者アカウントが必要です。定義済みの superuser アカウントのユーザ名は変更できません。定義済みの superuser アカウントのユーザ名は admin である必要があります。

WAAS デバイスを初期設定した後で、各 WAAS デバイスで定義済みの superuser アカウント用のパスワードをただちに変更することを強く推奨します（定義済みのユーザ名は admin、パスワードは default、特権レベルは superuser、特権レベル 15 です）。

WAAS Central Manager デバイスでこの superuser アカウント用の定義済みのパスワードが変更されていない場合は、アカウントを使用して WAAS Central Manager GUI にログインするたびに、次のダイアログボックスが表示されます（図 6-1 を参照）。

図 6-1　superuser アカウント用の定義済みのパスワードを変更する必要があることを示すメッセージ



この superuser アカウント用の定義済みのパスワードが変更されていない場合は、アカウントを使用して WAAS デバイスの WAAS CLI にログインするたびに、コンソールに次のメッセージも表示されます。

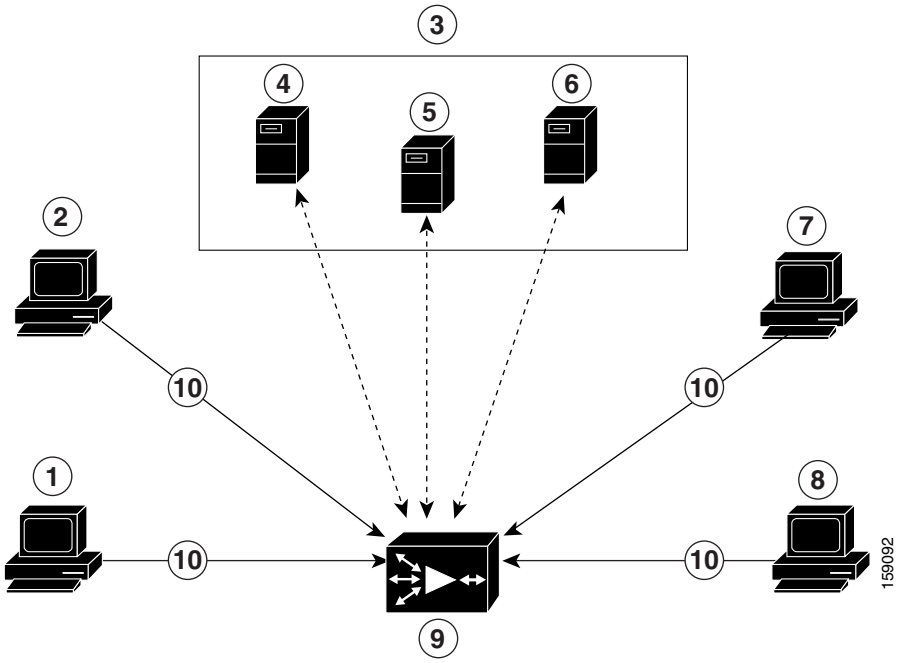
```
Device is configured with a (well known) default username/password
for ease of initial configuration. This default username/password
should be changed in order to avoid unwanted access to the device.
```

```
System Initialization Finished.
waas-cm#
```

WAAS Central Manager GUI を使用して定義済みの superuser アカウント用のパスワードを変更する手順については、「自身のアカウントのパスワードの変更」（P.7-7）を参照してください。

図 6-2 に、管理者が、コンソール ポートまたは WAAS GUI（WAAS Central Manager GUI または WAE Device Manager GUI）を使用して WAE にログインする方法を示します。WAAS デバイスが管理ログイン要求を受信すると、WAE は、ローカル データベースまたはリモート サードパーティ データベース（TACACS+、RADIUS、または Windows ドメイン データベース）をチェックし、ユーザ名とパスワードを確認し、管理者のアクセス特権を決定できます。

図 6-2　　認証データベースと WAE



1	FTP/SFTP クライアント	**6**	Windows ドメイン サーバ
2	WAAS Central Manager GUI または WAE Device Manager GUI	**7**	コンソールまたは Telnet クライアント
3	サードパーティ AAA サーバ	**8**	SSH クライアント
4	RADIUS サーバ	**9**	ローカル データベースとデフォルトの一次認証データベースを搭載する WAE
5	TACACS+ サーバ	**10**	管理ログイン要求

ユーザ アカウント情報は AAA データベースに保存され、AAA データベースが存在する特定の認証サーバにアクセスするように WAAS デバイスを設定する必要があります。WAAS デバイスへの管理ログイン アクセスを制御するために、次の認証および許可方式を任意に組み合わせて設定できます。

- ローカル認証および許可
- RADIUS
- TACACS+

- Windows ドメイン認証

（注） 外部認証サーバを使用して認証を設定する場合は、第 7 章「管理者ユーザ アカウントおよびグループの作成と管理」の説明に従って WAAS Central Manager でユーザ アカウントを作成する必要があります。ユーザ アカウントをローカル ユーザ アカウントにしないでください。つまり、アカウント作成時に [Local User] チェックボックスを選択しないでください。

デフォルトの AAA 設定の詳細については、「管理ログインの認証および許可のデフォルト設定」（P.6-4）を参照してください。AAA 設定の詳細については、「管理ログインの認証および許可の設定」（P.6-5）を参照してください。

管理ログインの認証および許可のデフォルト設定

デフォルトでは、WAAS デバイスはローカル データベースを使用して、管理ユーザのログイン認証および許可特権を取得します。

表 6-1 は、管理ログインの認証および許可のデフォルト設定を示しています。

表 6-1　管理ログインの認証および許可のデフォルト設定

機能	デフォルト値
管理ログインの認証	有効
管理設定の許可	有効
認証サーバが到達不能な場合の認証サーバのフェールオーバー	無効
TACACS+ ログイン認証（コンソールおよび Telnet）	無効
TACACS+ ログイン許可（コンソールおよび Telnet）	無効
TACACS+ キー	指定なし
TACACS+ サーバのタイムアウト	5 秒
TACACS+ 再送信の試行回数	2 回
RADIUS ログイン認証（コンソールおよび Telnet）	無効
RADIUS ログイン許可（コンソールおよび Telnet）	無効
RADIUS サーバの IP アドレス	指定なし
RADIUS サーバの UDP 許可ポート	ポート 1645
RADIUS キー	指定なし
RADIUS サーバのタイムアウト	5 秒
RADIUS 再送信の試行回数	2 回
Windows ドメイン ログイン認証	無効
Windows ドメイン ログイン許可	無効
Windows ドメイン パスワード サーバ	指定なし
Windows ドメイン領域（Kerberos 認証を使用するときに認証に使用される Kerberos 領域） **（注）** Kerberos 認証を有効にすると、デフォルトの**領域**は DOMAIN.COM になり、セキュリティは Active Directory サービス（ADS）になります。	空（から）の文字列
Windows ドメイン用の Windows Internet Naming Service（WINS）サーバのホスト名または IP アドレス	指定なし

表 6-1　管理ログインの認証および許可のデフォルト設定 （続き）

機能	デフォルト値
Window ドメインの管理グループ	定義済みの管理グループはありません。
Windows ドメインの NetBIOS 名	指定なし
Kerberos 認証	無効
Kerberos サーバのホスト名または IP アドレス（指定した Kerberos 領域用の Key Distribution Center（KDC; キー発行局）を稼動しているホスト）	指定なし
Kerberos サーバのポート番号（KDC サーバ上のポート番号）	ポート 88
Kerberos ローカル領域（WAAS 用のデフォルト領域）	kerberos-realm：空（から）の文字列
Kerberos 領域（ホスト名または DNS ドメイン名を Kerberos 領域にマップする）	空（から）の文字列

（注）　WAAS デバイス（RADIUS および TACACS+ クライアント）で RADIUS または TACACS+ キーを設定する場合は、必ず外部の RADIUS または TACACS+ サーバにも同一のキーを設定してください。

「管理ログインの認証および許可の設定」（P.6-5）の説明に従い、WAAS Central Manager GUI を使用してこれらのデフォルト値を変更します。

WAAS ソフトウェアには、Windows ドメイン認証を設定できる複数の Windows ドメイン ユーティリティが含まれます。WAAS CLI からこれらのユーティリティにアクセスするには、**windows-domain diagnostics** EXEC コマンドを使用します。

WAAS Central Manager GUI からこれらのユーティリティを起動する場合は、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　定義済みの順序でユーティリティを実行したいデバイスの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [Windows Domain] を選択します。

ステップ 4　表示されるウィンドウで、ウィンドウの一番下にある [Show Authentication Status] ボタンをクリックします。

管理ログインの認証および許可の設定

WAAS デバイスまたはデバイス グループ（WAE のグループ）用の管理ログイン認証および許可を一元的に設定する場合は、次の手順に従ってください。

ステップ 1　管理ログイン要求の認証時に WAAS デバイスで使用するよう設定するログイン認証方式を決定します（たとえば、ローカル データベースを 1 次ログイン データベースとして、RADIUS サーバを 2 次認証データベースとして使用します）。

ステップ 2　「WAAS デバイス用のログイン アクセス コントロール設定の構成」（P.6-7）の説明に従って、WAAS デバイス用のログイン アクセス コントロール設定を構成します。

ステップ 3　WAAS デバイスで管理ログイン認証サーバ設定を構成します（リモート認証データベースを使用する場合）。たとえば、次の項の説明に従って、WAAS デバイスが管理ログイン要求を認証するために使用する必要がある、リモート RADIUS サーバ、TACACS+ サーバ、または Windows ドメイン サーバの IP アドレスを指定します。

- 「RADIUS サーバ認証設定の構成」（P.6-12）
- 「TACACS+ サーバ認証設定について」（P.6-15）
- 「Windows ドメイン サーバ認証設定の構成」（P.6-17）

ステップ 4　次のログイン認証設定方式の中から、WAAS デバイスが管理ログイン要求を処理するために使用する必要がある 1 つまたはすべての方式を指定します。

- 管理ログイン認証方式を指定します。
- 管理ログイン許可方式を指定します。
- 管理ログイン認証サーバのフェールオーバー方式を指定します（任意）。

たとえば、WAAS デバイスが管理ログイン要求を処理するときに、どの認証データベースをチェックする必要があるかを指定します。「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（P.6-26）を参照してください。

注意　ローカル認証および許可を無効にする前に、RADIUS、TACACS+、または Windows ドメイン認証が設定され、正常に動作していることを確認します。ローカル認証を無効にし、RADIUS、TACACS+、または Windows ドメイン設定値が正しく設定されていない場合、もしくは RADIUS、TACACS+、または Windows ドメイン サーバがオンラインでない場合は、WAAS デバイスにログインできないことがあります。

WAAS Central Manager GUI または WAAS CLI を使用して、ローカルおよびリモート データベース（TACACS+、RADIUS、および Windows ドメイン）を有効または無効にすることができます。WAAS デバイスは、すべてのデータベースが無効になっているかどうかを確認し、無効な場合は、システムをデフォルトの状態に設定します（表 6-1 を参照）。管理認証と許可用に 1 つまたは複数の外部のサードパーティ データベース（TACACS+、RADIUS、または Windows ドメイン認証）を使用するように WAAS デバイスを設定した場合は、WAAS デバイスでもローカル認証方式と許可方式が有効であり、最後のオプションとしてローカル方式が指定されていることを確認します。このように指定されていないと、WAAS デバイスで、指定した外部のサードパーティ データベースに到達できない場合に、デフォルトでローカル認証方式と許可方式の段階に進みません。

デフォルトでは、最初にローカル ログイン認証が有効になります。ローカル認証および許可は、ローカルで設定されたログインとパスワードを使用して、管理ログインの試行を認証します。ログインとパスワードは、各 WAAS デバイスに対してローカルであり、個々のユーザ名にはマッピングされません。ローカル認証が無効な場合に、その他のすべての認証方式を無効にすると、ローカル認証は自動的に再度有効になります。

ローカル ログイン認証は、他の 1 つまたは複数の管理ログイン認証方式を有効にした後でだけ無効にできます。ただし、ローカル ログイン認証が無効な場合は、他のすべての管理ログイン認証方式を無効にしたときに、ローカル ログイン認証が自動的に再度有効になります。コンソール接続と Telnet 接続に異なる管理ログイン認証方式を指定することはできません。

管理ログインの認証方式と許可方式を同じ順序で設定することを強く推奨します。たとえば、管理ログイン認証と許可の両方の 1 次ログイン方式として RADIUS を使用し、2 次ログイン方式として TACACS+ を使用し、3 次ログイン方式として Windows を使用し、4 次ログイン方式としてローカル方式を使用するように、WAAS デバイスを設定します。

（注）　TACACS+ サーバは別の方式で認証されたユーザを許可しません。たとえば、Windows をプライマリ認証方式として設定し、TACACS+ をプライマリ許可方式として設定すると、TACACS+ 許可は失敗します。

ログイン認証方式と許可方式の優先順位リストの最後の方式として、ローカル方式を指定することを強く推奨します。この方法に従うと、指定した外部のサードパーティ サーバ（TACACS+、RADIUS、または Windows ドメイン サーバ）に到達可能できない場合でも、WAAS 管理者は、ローカル認証方式と許可方式を使用して WAAS デバイスにログインできます。

この項では、管理ログイン認証を一元的に設定する方法について説明します。内容は、次のとおりです。

- 「WAAS デバイス用のログイン アクセス コントロール設定の構成」（P.6-7）
- 「WAAS デバイス用のリモート認証サーバ設定の構成」（P.6-12）
- 「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（P.6-26）

WAAS デバイス用のログイン アクセス コントロール設定の構成

この項では、WAAS デバイスまたはデバイス グループ用のリモート ログイン設定とアクセス コントロール設定を一元的に構成する方法について説明します。内容は、次のとおりです。

- 「WAAS デバイス用のセキュア シェル設定の構成」（P.6-7）
- 「WAAS デバイス用の Telnet サービスの無効化と再有効化」（P.6-9）
- 「WAAS デバイスに対する Message of the Day 設定」（P.6-10）
- 「WAAS デバイス用の実行タイムアウト設定の構成」（P.6-11）
- 「WAAS デバイス用の回線コンソール キャリア検出の設定」（P.6-11）

WAAS デバイス用のセキュア シェル設定の構成

Secure Shell（SSH; セキュア シェル）は、サーバとクライアント プログラムから構成されます。Telnet のように、クライアント プログラムを使用して、SSH サーバが動作するマシンにリモートにログインできますが、Telnet と異なり、クライアントとサーバ間で伝達されるメッセージは暗号化されます。SSH の機能には、ユーザ認証、メッセージの暗号化、およびメッセージの認証があります。

（注）　WAAS デバイスの SSH 機能はデフォルトで無効に設定されています。

WAAS Central Manager GUI の SSH 管理ウィンドウを使用すると、設定、モニタ、またはトラブルシューティングのために特定の WAAS デバイスまたはデバイス グループにログインするときの暗号キーの長さ、ログイン許容時間、およびパスワードの最大試行回数を指定できます。

WAAS デバイスまたはデバイス グループで SSH 機能を一元的に有効にするには、次の手順に従ってください。

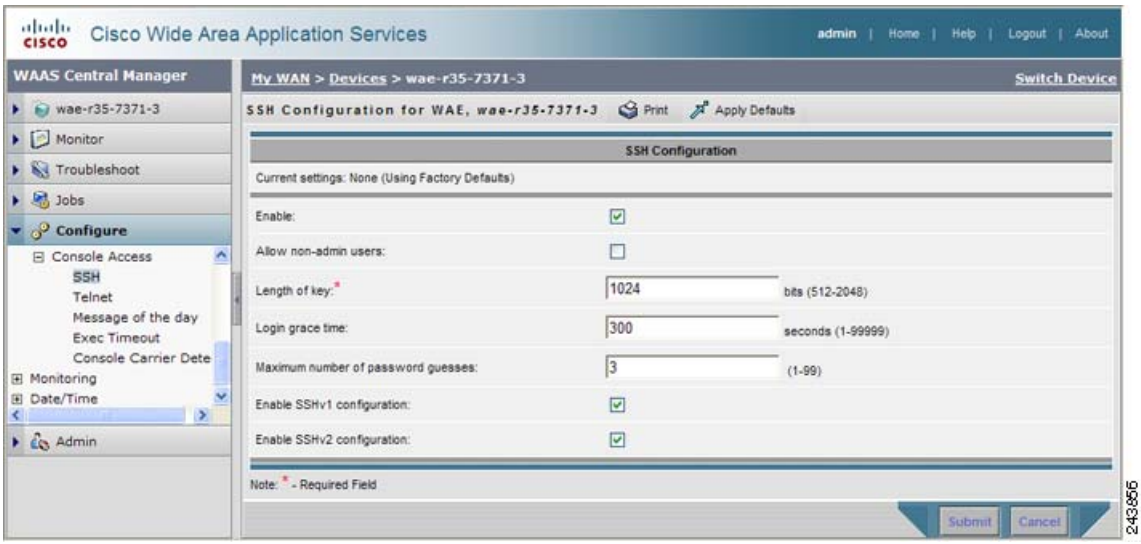
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　SSH を有効にしたいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Console] > [Access] > [SSH] を選択します。

[SSH Configuration] ウィンドウが表示されます（図 6-3 を参照）。

図 6-3　[SSH Configuration] ウィンドウ



ステップ 4　[Enable] チェックボックスを選択して、SSH 機能を有効にします。SSH は、安全で暗号化されたチャネルを通じて、選択した WAAS デバイス（またはデバイス グループ）へのログイン アクセスを可能にします。

ステップ 5　[Allow non-admin users] チェックボックスを選択して、非管理ユーザが SSH 経由で、選択したデバイス（またはデバイス グループ）にアクセスできるようにします。このオプションはデフォルトで無効になっています。

（注）　非管理ユーザとは、superuser ではない管理者です。superuser 以外の管理者はすべて、ログイン アカウントの特権レベルが 0 であるため、アクセスは WAAS デバイスだけに制限されています。superuser 管理者は、ログイン アカウントが最高の特権レベル、つまり特権レベル 15 であるため、WAAS デバイスへのフルアクセス権を持っています。

ステップ 6　[Length of key] フィールドで、SSH 暗号キーを作成するために必要なビット数を指定します。デフォルト値は、1024 です。

SSH を有効にするときは、クライアント プログラムがサーバの ID を確認するために使用する秘密キーとホストの公開キーの両方を必ず生成してください。SSH クライアントを使用して WAAS デバイスにログインすると、デバイスで動作する SSH デーモンの公開キーが、ホーム ディレクトリのクライアント マシン known_hosts ファイルに記録されます。その後に WAAS 管理者が [Length of key] フィールドにビット数を指定してホストの暗号キーを再生成する場合は、SSH クライアント プログラムを実行して WAAS デバイスにログインする前に、known_hosts ファイルから WAAS デバイスに関連する古い公開キー項目を削除する必要があります。古い項目を削除したあとで SSH クライアント プログラムを使用すると、known_hosts ファイルが WAAS デバイス用の新しい SSH 公開キーで更新されます。

ステップ 7　[Login grace time] フィールドで、クライアントとサーバ間のネゴシエーション（認証）フェーズ中に SSH セッションがタイムアウトする前にアクティブである時間（秒）を指定します。デフォルトは、300 秒です。

ステップ 8　[Maximum number of password guesses] フィールドで、1 接続当たりに許可する最大パスワード試行回数を指定します。デフォルト値は 3 です。

[Maximum number of password guesses] フィールドの値は、SSH サーバ側から許可するパスワード試行回数を指定しますが、SSH ログイン セッションの実際のパスワード試行回数は、SSH サーバと SSH クライアントが許可するパスワード試行回数の合計で決定されます。一部の SSH クライアントは、

SSH サーバがもっと多くの試行回数を許可する場合でも、許容される最大パスワード試行回数を 3 回（場合によっては 1 回）に制限します。許可するパスワード試行回数に *n* を指定すると、特定の SSH クライアントはこの数字を *n* + 1 として解釈します。たとえば、特定のデバイスの試行回数を 2 に設定すると、SSH クライアントからの SSH セッションでは、3 回のパスワード試行が許可されます。

ステップ 9　クライアントが SSH プロトコルのバージョン 1 を使用して接続することを許可するか、またはバージョン 2 を使用して接続することを許可するかを指定します。

- バージョン 1 を指定するには、[Enable SSHv1] チェックボックスを選択します。
- バージョン 2 を指定するには、[Enable SSHv2] チェックボックスを選択します。

（注）　SSH バージョン 1 とバージョン 2 を同時に有効にすることができます。あるいは、片方のバージョンだけを有効にすることができます。[Enable] チェックボックスの選択を解除して SSH 機能を無効にしない限り、両方の SSH バージョンを無効にすることはできません（ステップ 4 を参照）。

ステップ 10　[Submit] をクリックして、設定を保存します。

デフォルト設定またはデバイス グループ設定の適用後に保存されていない変更がある場合は、[Current Settings] 行に、「Click Submit to Save」メッセージが赤い色で表示されます。また、[Reset] ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

CLI から SSH 設定を構成するには、**sshd** および **ssh-key-generate** グローバル コンフィギュレーション コマンドを使用します。

WAAS デバイス用の Telnet サービスの無効化と再有効化

デフォルトでは、Telnet サービスは、WAAS デバイスで有効になっています。Telnet セッションでなく、コンソール接続を使用して、WAAS デバイス上のデバイス ネットワーク設定を定義する必要があります。ただし、コンソール接続を使用してデバイス ネットワーク設定を定義したあとに、Telnet セッションを使用してそれ以降の設定作業を行うことができます。

デバイスに Telnet で接続するために [Device Dashboard] ウィンドウで [Telnet] ボタンを使用する前に、Telnet サービスを有効にする必要があります。

（注）　Telnet は、Internet Explorer 7 または 8 ではサポートされていません。[Device Dashboard] から [Telnet] ボタンを使用する場合は、Internet Explorer 6 または異なる Web ブラウザを使用してください。

WAAS デバイスまたはデバイス グループで Telnet サービスを一元的に無効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　Telnet を無効にするデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Console Access] > [Telnet] を選択します。[Telnet Settings] ウィンドウが表示されます。

ステップ 4　選択したデバイス（またはデバイス グループ）用のリモート端末接続用の端末エミュレーション プロトコルを無効にするために、[Telnet Enable] チェックボックスの選択を解除します。

ステップ 5　[Submit] をクリックして、設定を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

あとでデバイス（またはデバイス グループ）で Telnet サービスを一元的に再有効化するには、[Telnet Settings] ウィンドウで [Telnet Enable] チェックボックスを選択し、[Submit] をクリックします。

CLI から Telnet を無効にするには、**no telnet enable** グローバル コンフィギュレーション コマンドを使用できます。また、Telnet を有効にするには、**telnet enable** グローバル コンフィギュレーション コマンドを使用できます。

WAAS デバイスに対する Message of the Day 設定

Message of the Day（MOTD）機能では、WAAS ネットワークの一部であるデバイスへのログイン時にユーザに情報を表示します。設定できるメッセージは、次の 3 種類です。

- MOTD バナー
- EXEC プロセス作成バナー
- ログイン バナー

（注）　SSH バージョン 1 クライアントを実行中でデバイスにログインしている場合、MOTD とログイン バナーは表示されません。デバイスへのログイン時にバナーを表示するには、SSH バージョン 2 を使用する必要があります。

MOTD 設定を行うには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　Message of The Day を設定する WAAS デバイスの横にある [Edit] アイコンをクリックします。選択したデバイス用の [Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Console Access] > [Message of the day] を選択します。選択したデバイス用の [MOTD Configuration] ウィンドウが表示されます。

ステップ 4　MOTD 設定を有効にするために、[Enable] チェックボックスを選択します。Message of the Day（MOTD）バナー、EXEC プロセス作成バナー、およびログイン バナーのフィールドが有効になります。

ステップ 5　Message of the Day（MOTD）バナーのフィールドで、デバイスにユーザがログインしたあとに MOTD バナーとして表示する文字列を入力します。

（注） [Message of the Day (MOTD) Banner] フィールド、[EXEC Process Creation Banner] フィールド、および [Login Banner] フィールドには、最大 1024 文字を入力できます。改行文字（または Enter キー）は、システムで ¥n と解釈されるため、2 文字として数えられます。MOTD テキストでは、`、%、^、" などの特殊文字を使用できません。テキストにこれらの特殊文字が含まれる場合、WAAS ソフトウェアは MOTD 出力からその文字を削除します。

ステップ 6　[EXEC Process Creation Banner] フィールドで、ユーザがデバイスの EXEC シェルに入力したときに EXEC プロセス作成バナーとして表示される文字列を入力します。

ステップ 7　[Login Banner] フィールドで、ユーザがデバイスにログインするときに、MOTD バナーのあとに表示される文字列を入力します。

ステップ 8　設定を保存するために、[Submit] をクリックします。

WAAS デバイス用の実行タイムアウト設定の構成

WAAS デバイスまたはデバイス グループで非アクティブな Telnet セッションを開いておく時間の長さを一元的に設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　実行タイムアウトを設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Console Access] > [Exec Timeout] を選択します。

ステップ 4　[Exec Timeout] フィールドで、アクティブ セッションがタイムアウトする時間（分）を指定します。デフォルト値は、15 分です。

WAAS デバイスとの Telnet セッションは、このフィールドに指定した時間の間、非アクティブのまま開いておくことができます。実行タイムアウト時間が経過すると、WAAS デバイスは自動的に Telnet セッションを閉じます。

ステップ 5　[Submit] をクリックして、設定を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

CLI から Telnet セッション タイムアウト を設定するには、**exec-timeout** グローバル コンフィギュレーション コマンドを使用できます。

WAAS デバイス用の回線コンソール キャリア検出の設定

WAAS デバイスをモデムに接続して呼び出しを受信する場合は、キャリア検出を有効にする必要があります。

（注）　デフォルトでは、この機能は、WAAS デバイスで無効になっています。

WAAS デバイスまたはデバイス グループ用のコンソール回線キャリア検出を一元的に有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Console Access] > [Console Carrier Detect] を選択します。[Console Carrier Detect Settings] ウィンドウが表示されます。

ステップ 4　[Enable console line carrier detection before writing to the console] チェックボックスを選択して、設定するためのウィンドウを有効にします。

ステップ 5　[Submit] をクリックして、設定を保存します。

キャリア検知ピンが配線されていない空のモデム ケーブルを使用すると、キャリア検知信号が検出されるまで WAE がコンソールで応答しないように見えることを説明するメッセージが表示されます。構成の不具合から回復するには、WAE をリブートし、キャリア検出設定を無視するように 0x2000 起動フラグを設定する必要があります。

ステップ 6　[OK] をクリックして作業を続行します。

CLI からコンソール回線キャリア検出を設定するには、**line console carrier-detect** グローバル コンフィギュレーション コマンドを使用できます。

WAAS デバイス用のリモート認証サーバ設定の構成

ログイン認証方式に 1 台または複数の外部認証サーバを含めることを決定した場合は、WAAS Central Manager GUI で認証方式を設定する前に、これらのサーバ設定を構成する必要があります。ここでは、次の内容について説明します。

RADIUS サーバ認証設定の構成

RADIUS は、Network Access Server（NAS; ネットワーク アクセス サーバ）が、ネットワーク デバイスに接続しようとしているユーザを認証するために使用するクライアント / サーバ認証および許可アクセス プロトコルです。NAS はクライアントとして機能し、ユーザ情報を 1 台以上の RADIUS サーバへ渡します。NAS は、1 台以上の RADIUS サーバから受信した応答に基づいて、ユーザにネットワーク アクセスを許可または拒否します。RADIUS は、RADIUS クライアントとサーバ間の転送に、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用します。

RADIUS 認証クライアントは、WAAS ソフトウェアを実行するデバイスに常駐します。有効にすると、これらのクライアントは認証要求を中央の RADIUS サーバへ送信します。RADIUS サーバには、ユーザ認証情報とネットワーク サービス アクセス情報が含まれています。

クライアントとサーバには、RADIUS キーを設定できます。クライアントにキーを設定する場合は、RADIUS サーバに設定されているキーと同じキーを設定する必要があります。RADIUS クライアントとサーバは、キーを使用して、送信されたすべての RADIUS パケットを暗号化します。RADIUS キーを設定しないと、パケットは暗号化されません。このキー自体は、ネットワーク経由で送信されません。

（注） RADIUS プロトコルの動作方法の詳細については、RFC2138、『*Remote Authentication Dial In User Service（RADIUS）*』を参照してください。

RADIUS 認証は、通常、管理者が、モニタ、設定、またはトラブルシューティングのためにデバイスを設定するために WAAS デバイスに最初にログインしたときに実行されます。RADIUS 認証は、デフォルトでは無効になっています。RADIUS 認証とその他の認証方式は同時に有効にすることができます。また、最初に使用する方式を指定することもできます。

複数の RADIUS サーバを設定できます。各サーバで順に認証試行が行われていきます。最初のサーバに到達不能の場合、ファーム内のその他のサーバでの認証試行が順に行われていきます。サーバに到達不能という以外の何らかの理由で認証に失敗した場合は、ファーム内の他のサーバでの認証試行は行われません。

ヒント WAAS Central Manager は、ユーザ認証情報をキャッシュしません。したがって、ユーザは、すべての要求について RADIUS サーバに対して再認証されます。多数の認証要求によるパフォーマンスの低下を防止するには、RADIUS サーバと同じ位置またはできるだけ近くに WAAS Central Manager デバイスを設置して、認証要求をできるだけ迅速に処理するようにします。

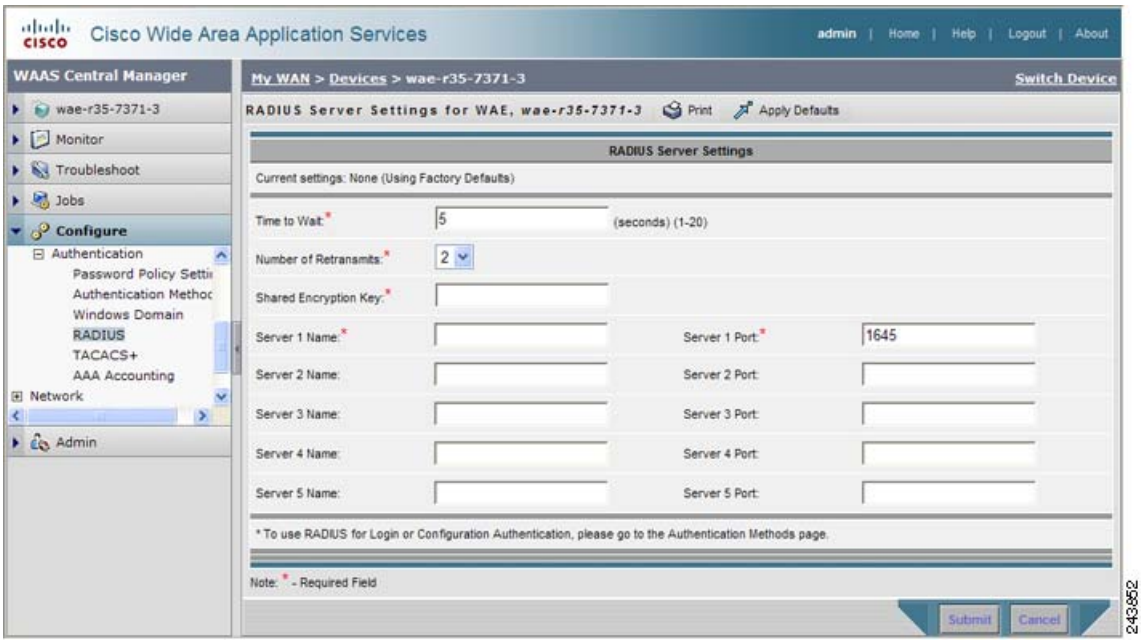
WAAS デバイスまたはデバイス グループ用の RADIUS サーバ設定を一元的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [RADIUS] を選択します。[RADIUS Server Settings] ウィンドウが表示されます（図 6-4 を参照）。

図 6-4　[RADIUS Server Settings] ウィンドウ



ステップ 4　[Time to Wait] フィールドに、デバイスまたはデバイス グループが、タイムアウトするまで RADIUS サーバから応答を待つ必要がある時間を指定します。範囲は、1 ～ 20 秒です。デフォルト値は 5 秒です。

ステップ 5　[Number of Retransmits] フィールドに、RADIUS サーバに接続するときに許可する再試行回数を指定します。デフォルト値は 2 回です。

ステップ 6　[Shared Encryption Key] フィールドに、RADIUS サーバと通信するために使用する秘密キーを入力します。

（注）　WAAS デバイス（RADIUS クライアント）で RADIUS キーを設定する場合は、必ず、外部の RADIUS サーバにも同一のキーを設定してください。左一重引用符（`）、二重引用符（"）、パイプ（|）、閉じ角カッコ（]）、または数字記号（#）の文字を使用しないでください。

ステップ 7　[Server Name] フィールドに、RADIUS サーバの IP アドレスまたはホスト名を入力します。5 つの異なるホストが許可されます。

ステップ 8　[Server Port] フィールドに、RADIUS サーバを受信する UDP ポート番号を入力します。少なくとも 1 つのポートを指定する必要があります。5 つの異なるポートが許可されます。

ステップ 9　[Submit] をクリックして、設定を保存します。

これで、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（P.6-26）の説明に従って、この WAAS デバイスまたはデバイス グループ用の管理ログイン認証および許可方式として、RADIUS を有効にすることができます。

CLI から RADIUS 設定を構成するには、**radius-server** グローバル コンフィギュレーション コマンドを使用できます。

TACACS+ サーバ認証設定について

TACACS+ は、ネットワーク デバイスと中央集中型データベースとの間で NAS 情報を交換し、ユーザまたはエンティティの ID を判断することで、ネットワーク デバイスへのアクセスを制御します。TACACS+ は、TACACS の拡張版であり、RFC1492 で規定されている UDP ベースのアクセス コントロール プロトコルです。TACACS+ は、TCP を使用して TACACS+ サーバとネットワーク デバイス上の TACACS+ デーモンとの間のすべてのトラフィックの安定した配信と暗号化を保証します。

TACACS+ は、固定パスワード、ワンタイム パスワード、チャレンジレスポンス認証などの多数のタイプの認証と連携して動作します。TACACS+ 認証は、通常、管理者が、モニタ、設定、またはトラブルシューティングに対して WAE を設定するために WAAS デバイスに最初にログインしたときに実行されます。

ユーザが限定されたサービスを要求した場合、TACACS+ は MD5 暗号化アルゴリズムを使用してユーザ パスワード情報を暗号化し、TACACS+ パケット ヘッダーに追加します。このヘッダー情報は、送信されたパケットのタイプ（たとえば、認証パケット）、パケットのシーケンス番号、使用されている暗号化タイプ、パケット長の合計を示しています。次に、TACACS+ プロトコルはパケットを TACACS+ サーバへ転送します。

TACACS+ サーバは、AAA 機能を提供できます。このサービスは、すべて TACACS+ の一部ですが、互いに独立しているため、特定の TACACS+ 設定では、3 つのサービスのいずれか、またはすべてを使用できます。

TACACS+ サーバは、パケットを受信すると、次のように処理します。

- ユーザ情報を認証し、ログイン認証が成功したか失敗したかどうかを、クライアントに通知します。
- 認証を続行することと、クライアントが追加情報を提供する必要があることを、クライアントに通知します。このチャレンジレスポンス プロセスは、ログイン認証が成功するか失敗するまで、何度も繰り返し実行できます。

クライアントとサーバには、TACACS+ キーを設定できます。WAAS デバイスで暗号キーを設定する場合は、TACACS+ サーバで設定した暗号キーと同じ暗号キーを設定する必要があります。TACACS+ クライアントとサーバは、暗号キーを使用して、送信されたすべての TACACS+ パケットを暗号化します。TACACS+ キーを設定しないと、パケットは暗号化されません。

TACACS+ 認証は、デフォルトでは無効になっています。TACACS+ 認証とローカル認証は同時に有効にすることができます。

1 つのプライマリ TACACS+ サーバと 2 つのバックアップ TACACS+ サーバを設定できます。まず、プライマリ サーバで認証試行が行われます。プライマリ サーバに到達不能の場合、ファーム内のその他のサーバでの認証試行が順に行われていきます。サーバに到達不能という以外の何らかの理由で認証に失敗した場合は、ファーム内の他のサーバでの認証試行は行われません。

TACACS+ データベースは、ユーザが WAAS デバイスにアクセスする前にユーザを検査します。TACACS+ は、Department of Defense（DoD; 米国国防総省）（RFC 1492）の原案から派生したものであり、シスコシステムズは非特権モードと特権モードのアクセス制御を強化するために TACACS+ を使用しています。WAAS ソフトウェアは、TACACS+ だけをサポートしています。TACACS や拡張 TACACS は、サポートしていません。

ユーザ認証に TACACS+ を使用している場合は、TACACS+ サーバで定義したユーザ グループと一致する WAAS ユーザ グループ名を作成できます。その後、TACACS+ サーバで定義したグループのメンバシップに基づいて、WAAS でユーザに動的にロールとドメインを割り当てることができます（「アカウントの操作」（P.7-3）を参照）。TACACS+ 設定ファイルで、次のように各ユーザに関連グループ名を指定する必要があります。

```
user = tacusr1 {
 default service = permit
 service = exec
 {
   waas_rbac_groups = admin,groupname1,groupname2
```

```
   priv-lvl = 15
 }
 global = cleartext "tac"
}
```

各ユーザの属するグループを、グループごとにカンマで区切って waas_rbac_groups 属性に表示します。

外部ユーザ グループに基づいてロールおよびドメインをダイナミックに割り当てるには、シェルのカスタム属性をサポートする TACACS+ サーバが必要です。たとえば、これらの属性は Cisco ACS 4.x でサポートされていますが、5.0 ではサポートされていません。

ヒント　WAAS Central Manager はユーザ認証情報をキャッシュしないので、ユーザはすべての要求について TACACS に対して再認証されます。多数の認証要求によるパフォーマンスの低下を防止するには、TACACS+ サーバと同じ場所またはできるだけ近くの場所に WAAS Central Manager デバイスを設置して、認証要求をできるだけ迅速に処理するようにします。

（注）　TACACS+ ユーザ認証を使用する場合は、ユーザ名を数字で始めたり、ユーザ名に数字だけを使用したりすることはできません。ユーザ名をこのように指定すると、ログインに失敗します。

TACACS+ サーバ設定の構成

WAAS ソフトウェアの CLI EXEC モードでは、システム動作の設定、表示、およびテストを実行できます。このモードは、ユーザと特権の 2 つのアクセス レベルに分かれます。特権レベルの EXEC モードにアクセスするには、ユーザ アクセス レベルのプロンプトで **enable** EXEC コマンドを入力し、パスワードの入力が求められたら特権 EXEC パスワード（superuser または admin 相当のパスワード）を指定します。

TACACS+ には、管理者が、管理レベルのユーザごとに異なる有効化パスワードを定義できる有効化パスワード機能があります。管理レベルのユーザが、管理者（admin）または管理者相当のユーザ アカウント（特権レベル 15）ではなく、通常レベルのユーザ カウント（特権レベル 0）で WAAS デバイスにログインした場合、そのユーザは、特権レベル EXEC モードにアクセスするために admin パスワードを入力する必要があります。

```
WAE> enable
Password:
```

（注）　このことは、WAAS ユーザがログイン認証に TACACS+ を使用している場合にも適用されます。

WAAS デバイスまたはデバイス グループ用の TACACS+ サーバ設定を一元的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [TACACS+] を選択します。[TACACS+ Server Settings] ウィンドウが表示されます

（注）　AAA Command Authorization が有効になっている場合は、TACACS+ サーバの設定を変更したり削除したりすることはできません。

ステップ 4　認証用に ASCII 形式のパスワードを使用するために、[Use ASCII Password Authentication] チェックボックスを選択します。

デフォルトのパスワード タイプは、Password Authentication Protocol（PAP; パスワード認証プロトコル）です。ただし、認証パケットを ASCII クリアテキストで送信する場合は、パスワード タイプを ASCII に変更できます。

ステップ 5　[Time to Wait] フィールドで、デバイスがタイムアウトを待つ時間の長さを指定します。範囲は、1 ～ 20 秒です。デフォルト値は 5 秒です。

ステップ 6　[Number of Retransmits] フィールドに、TACACS+ サーバに接続するときに許可する再試行回数を指定します。範囲は、1 ～ 3 回です。デフォルト値は 2 回です。

ステップ 7　[Security Word] フィールドに、TACACS+ サーバと通信するために使用する秘密キーを入力します。

（注）　WAAS デバイス（TACACS+ クライアント）で TACACS+ キーを設定する場合は、必ず、外部の TACACS+ サーバにも同一のキーを設定してください。左一重引用符（`）、二重引用符（"）、パイプ（|）、閉じ角カッコ（]）、または数字記号（#）の文字を使用しないでください。

ステップ 8　[Primary Server] フィールドに、TACACS+ サーバの IP アドレスまたはホスト名を入力します。

ステップ 9　[Secondary Server] フィールドに、TACACS+ サーバの IP アドレスまたはホスト名を入力します。

ステップ 10　[Tertiary Server] フィールドに、TACACS+ サーバの IP アドレスまたはホスト名を入力します。

（注）　最大 2 台のバックアップ TACACS+ サーバを指定できます。

ステップ 11　[Submit] をクリックして、設定を保存します。

これで、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（P.6-26）の説明に従って、この WAAS デバイスまたはデバイス グループ用の管理ログイン認証および許可方式として、TACACS+ を有効にすることができます。

CLI から TACACS+ 設定を構成するには、**tacacs** グローバル コンフィギュレーション コマンドを使用できます。

Windows ドメイン サーバ認証設定の構成

Windows ドメイン コントローラは、チャレンジ / レスポンスまたは共有秘密認証方式を使用して WAAS ソフトウェア サービスへのアクセスを制御するように設定できます。システム管理者は、FTP、SSH、または Telnet セッションを使用して、あるいは 1 つのユーザ アカウント（ユーザ名 / パスワード / 特権）でコンソールまたは WAAS Central Manager GUI を使用して、WAAS デバイスにログインできます。Windows ドメイン認証では、RADIUS および TACACS+ 認証方式を同時に設定できます。Windows ドメイン認証を有効にすると、さまざまな認証ログイン統計情報をログに記録するように設定できます。ログ ファイル、統計カウンタ、および関連情報は、いつでも消去できます。

WAAS ネットワークでは、次の場合に Windows ドメイン認証を使用します。

- WAAS Central Manager GUI へのログイン
- WAE Device Manager GUI へのログイン
- 任意の WAAS デバイスでの CLI 設定
- 切断モードの操作

WAAS Central Manager デバイス、個別の WAAS デバイス、またはデバイスのグループ用の Windows 認証を設定できます。WAAS デバイスで Windows ドメイン認証を設定するには、一連の Windows ドメイン認証設定を構成する必要があります。

（注）　Windows ドメイン認証は、WAAS デバイスに Windows ドメイン サーバが設定されていない限り、実行されません。デバイスが正しく登録されていない場合、認証と許可は実行されません。WAAS は、Windows Server 2000 または Windows Server 2003 だけで稼動している Windows ドメイン コントローラによる認証をサポートします。

NTLM 認証を使用している場合は、Windows 2000 よりも前のオペレーティング システムをサポートするオプションを使用して Windows ドメイン サーバをインストールする必要があります（Windows サーバの dcpromo ウィザードの [installation Permissions] 画面で、[Permissions compatible with pre-Windows 2000 server operating systems.] を選択します）。

ここでは、次の内容について説明します。

- 「WAAS デバイス上の Windows ドメイン サーバ設定の構成」（P.6-18）
- 「Windows ドメイン コントローラからの WAE の登録解除」（P.6-22）
- 「Edge WAE 用の自動マシン アカウント パスワード変更の無効化」（P.6-23）

WAAS デバイス上の Windows ドメイン サーバ設定の構成

認証に使用する Windows ドメイン コントローラの名前と IP アドレス、またはホスト名を知っている必要があります。

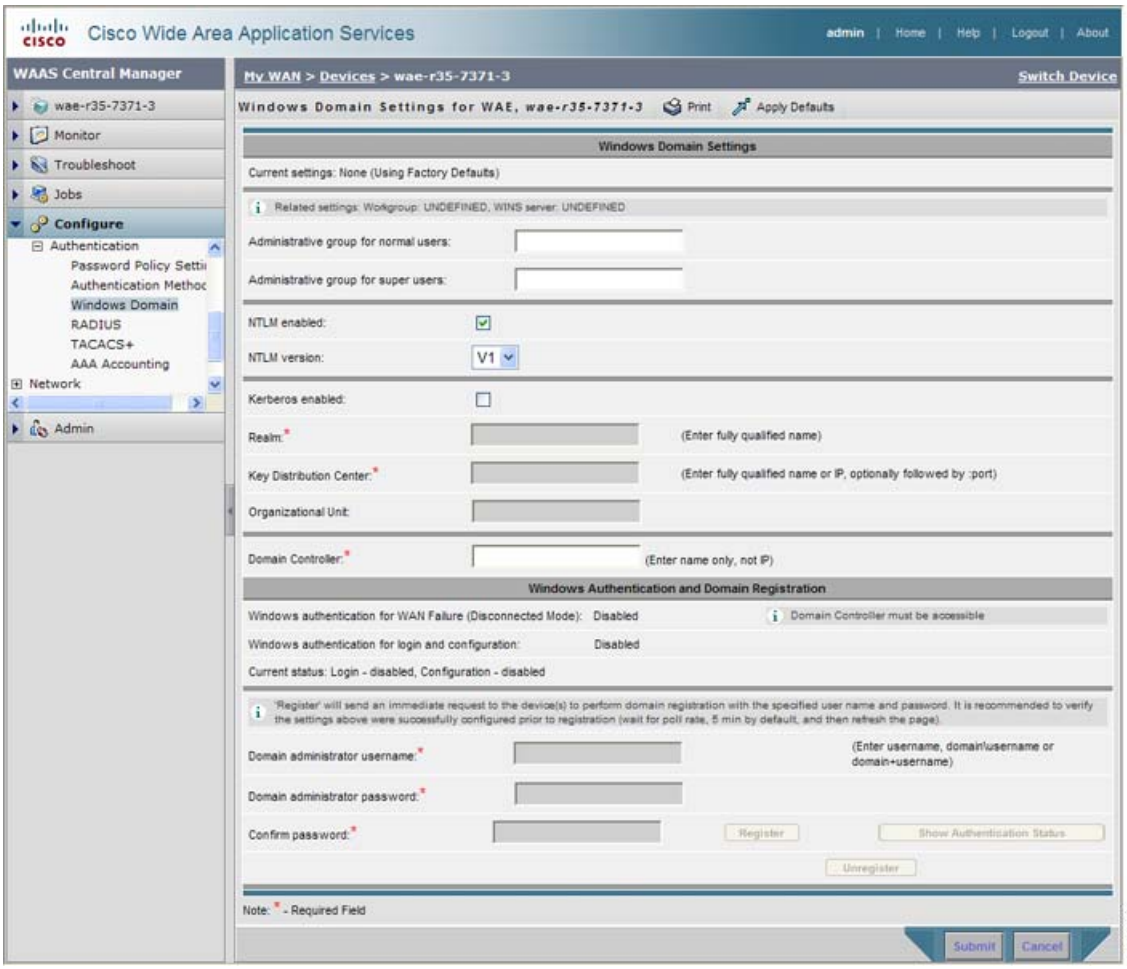
WAAS デバイスまたはデバイス グループ用の Windows ドメイン サーバ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [Windows Domain] を選択します。[Windows Domain Server Settings] ウィンドウが表示されます（図 6-5 を参照）。

図 6-5　[Windows Domain Server Settings] ウィンドウ



（注）　選択したデバイス（またはデバイス グループ）用に関連する WINS サーバおよびワークグループまたはドメイン名が定義されていない場合、図 6-5 に示すように、このウィンドウの一番上に、関連する設定が定義されていないことを知らせる情報メッセージが表示されます。これらの設定を定義するには、[Configure] > [Network] > [WINS] を選択します。

ステップ 4　[Administrative group for normal users] フィールドにグループの名前を入力して、選択したデバイス（またはデバイス グループ）へのアクセスに制限がある特権レベルが 0 の通常のユーザ（superuser でない管理者）用の管理グループを指定します。

（注）　デフォルトでは、WAE で設定された Windows ドメイン許可用のユーザ グループは、事前に定義されません。

ステップ 5　[Administrative group for superusers] フィールドにグループの名前を入力して、選択したデバイス（またはデバイス グループ）に完全にアクセスできる特権レベルが 15 の特権ユーザ（superuser である管理者）用の管理グループを指定します。

（注）　WAE で Windows ドメイン管理グループを設定することに加えて、Microsoft Windows 2000 または 2003 サーバで Windows ドメイン管理グループを設定する必要があります。Windows ドメイン管理特権ユーザ グループと通常のユーザ グループを作成する必要があります。特権ユーザ グループのグループ スコープが global に設定されていることを確認し、新しく作成した管理グループにユーザ メンバを割り当て、Windows ドメイン特権ユーザ グループにユーザ アカウント（たとえば、winsuper ユーザ）を追加します。Windows サーバで Windows ドメイン管理グループを設定する方法については、Microsoft 社のマニュアルを参照してください。

ユーザが Telnet セッション、FTP、または SSH セッションを使用してこの WAE にアクセスしようとすると、WAE は Active Directory ユーザ データベースを使用して管理アクセス要求を認証するように設定されます。

ステップ 6　次のように、選択したデバイス（またはデバイス グループ）への管理ログイン用の安全な共有認証方式として NTLM または Kerberos を選択します。

（注）　ユーザがドメイン アカウントにログインする Windows 2000 以上が動作する Windows システムには、Kerberos バージョン 5 が使用されます。

- NTLM を有効にするには、[NTLM enabled] チェックボックスを選択します。
- NTML バージョン 1 を選択するには、[NTLM enabled] チェックボックスを選択します。デフォルトでは、NTLM バージョン 1 が選択されます。

  NTLM バージョン 1 は、Active Directory を使用する Windows 98 や Windows NT などの従来のシステム、および Windows 2000、Windows XP、Windows 2003 などの最近の Windows システムを含むすべての Windows システムで使用されます。Windows 2000 SP4 または Windows 2003 のドメイン コントローラを使用する場合は、Kerberos の使用を推奨します。
- NTLM バージョン 2 を選択するには、ドロップダウン リストから [V2] を選択します。

  NTLM バージョン 2 は、Windows 98 と Active Directory を実行している Windows システム、Windows NT 4.0（Service Pack 4 以降）、Windows XP、Windows 2000、および Windows 2003 で使用されます。WAAS プリント サーバの NTLM バージョン 2 のサポートを有効にすると、NTLM または LM を使用するクライアントにアクセスできなくなります。

注意　すべてのクライアントのセキュリティ ポリシーが [Send NTLMv2 responses only/Refuse LM and NTLM] に設定されている場合にだけ、プリント サーバでの NTLM バージョン 2 サポートを有効にします。

- Kerberos を選択するには、[Kerberos enabled] チェックボックスを選択します。[Realm] フィールドに、WAAS デバイスが存在する領域の完全修飾名を入力します。[Key Distribution center] フィールドに、Kerberos 暗号キー配信局の完全修飾名または IP アドレスを入力します。必要に応じて、[Organizational Unit] フィールドに組織単位の名前を入力します。

  すべての Windows 2000 ドメインは、Kerberos 領域です。Windows 2000 ドメイン名は DNS ドメイン名でもあるため、Windows 2000 ドメイン名用の Kerberos 領域名は常に大文字です。この大文字の使用は、Kerberos バージョン 5 プロトコル資料（RFC-4120）での領域名として DNS 名を使用する勧告に従っており、Kerberos に基づく他の環境との相互運用性だけに影響します。

ステップ 7　[Domain Controller] フィールドに、Windows ドメイン コントローラの名前を入力します。

[Submit] をクリックすると、Central Manager が WAAS デバイスに要求を送って（バージョン 4.2.x 以上の場合）ドメイン コントローラ名を解決することにより、この名前を検証します。ドメイン コントローラが解決できない場合は、有効な名前を送信するように求められます。デバイスがオフラインの場

合は、デバイスの接続を確認するように求められます。デバイス グループを設定している場合、このページが受け付けられるまでは各デバイスでのドメイン コントローラ名の検証は行われず、デバイス上で解決できない場合は、このページでの設定変更はそのデバイスには適用されません。

ステップ 8　[Submit] をクリックします。

（注）　[Submit] をクリックし、指定した変更が WAAS Central Manager データベースにコミットされたことを確認してください。ステップ 9 で入力するドメイン管理者のユーザ名とパスワードは、WAAS Central Manager のデータベースに格納されません。

ステップ 9　選択したデバイス（またはデバイス グループ）を Windows ドメイン コントローラに登録するには、次の手順に従ってください。

a. [Domain Administrator username] フィールドに、指定した Windows ドメイン コントローラの管理ユーザ名（domain¥username またはドメイン名とユーザ名）を入力します。

b. [Domain Administrator password] フィールドに、指定した Windows ドメイン コントローラの管理パスワードを入力します。

c. [Confirm password] フィールドに、指定した Windows ドメイン コントローラの管理パスワードを入力します。

d. [Register] ボタンをクリックします。

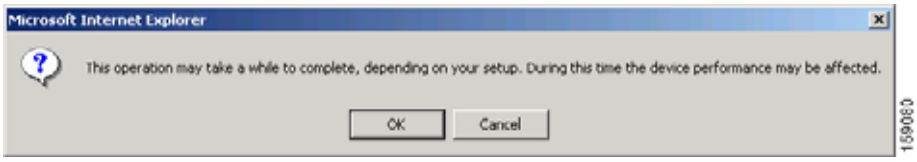
（注）　[Register] ボタンをクリックすると、WAAS Central Manager は、SSH を使用して、すぐに WAAS デバイス（またはデバイス グループ）へ登録要求を送信します（指定したドメイン管理者パスワードは、SSH で暗号化されます）。登録要求は、指定したドメイン管理者のユーザ名とパスワードを使用して、指定した Windows ドメイン コントローラへのドメイン登録を実行するように、デバイスに指示します。デバイスにアクセスできる場合（NAT の背後にあり、外部 IP アドレスを持っている場合）、登録要求はデバイス（またはデバイス グループ）によって実行されます。

e. 登録要求のステータスを確認するには、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（P.6-26）の説明に従って Windows をデバイスに対する認証および許可方式として設定し、数分経ってから [Show Authentication Status] ボタンをクリックします。

[Show Authentication Status] ボタンをクリックする前に、[Refresh Authentication Status] チェックボックスを選択できます。このボックスを選択すると、WAAS Central Manager は、ドメイン登録ステータスの更新をデバイスに問い合わせます。選択を外すと、Central Manager のローカル キャッシュのステータスが取得されます。

[Show Authentication Status] ボタンをクリックすると、認証要求ステータスを表示するかどうかを尋ねるダイアログ ボックスが表示されます（図 6-6 を参照）。

図 6-6　確認ダイアログボックス



f. [OK] をクリックして続行するか、[Cancel] をクリックして要求を取り消します。

要求が失敗した場合は、エラー ダイアログを受け取ります。数分経ってから、再試行して更新された認証ステータスを参照してください。

要求が正常に終了した場合、ドメイン登録ステータスは、図 6-5 の下部にある [Windows Authentication] と [Domain Registration] の見出しのすぐ下に表示されます。さらに、ウィンドウ認証と切断モードのステータスもこの部分に表示されます。

Windows のドメイン設定後に、Windows の認証を有効にするプロセスを完了するには、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（P.6-26）の説明に従って、[Authentication Methods] ウィンドウを使用して、Windows をデバイスに対する認証および許可方式としてと設定する必要があります。

WAAS CLI ではなく、WAAS Central Manager GUI を使用して、Windows ドメイン サーバ設定を構成することを推奨します。ただし、CLI を使用したい場合は、『*Cisco Wide Area Application Services Command Reference*』で **windows-domain** および **kerberos**（共有されたセキュアな認証方式として Kerberos を使用する場合）のコマンドを参照してください。

次に、次のコマンド（Kerberos 認証の場合）を使用して、設定した Windows ドメイン サーバに WAAS デバイスを登録し、検査します。

```
WAE# windows-domain diagnostics net  "ads join -U AdminUsername%AdminPassword"
WAE# windows-domain diagnostics net  "ads testjoin -U AdminUsername%AdminPassword"
```

NTLM 認証の場合は、次のコマンドを代わりに使用します。

```
WAE# windows-domain diagnostics net  "rpc join -U AdminUsername%AdminPassword"
WAE# windows-domain diagnostics net  "rpc testjoin -U AdminUsername%AdminPassword"
```

最後に、次のコマンドを使用して、管理ログイン認証および許可設定として Windows ドメインを有効にします。

```
WAE(config)# authentication login windows-domain enable primary
WAE(config)# authentication configuration windows-domain enable primary
```

切断モードで内容要求の認証を有効にするには、**authentication content-request windows-domain disconnected-mode enable** コンフィギュレーション コマンドを使用します。

Windows ドメイン コントローラからの WAE の登録解除

Windows ドメイン コントローラから WAE デバイスを登録解除する場合、Kerberos 共有認証方式を使用している場合は、WAAS Central Manager から直接登録解除を行うことができます。NTLM メソッドを使用している場合、WAAS Central Manager を使用して WAE を登録解除できません。ドメイン コントローラにログインし、デバイス登録を手動で削除する必要があります。

デバイスを登録解除する前に、デバイスに対するウィンドウズ認証を無効にする必要があります。

WAE デバイスを登録解除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　登録解除したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [Authentication Methods] を選択します。[Authentication and Authorization Methods] ウィンドウが表示されます（図 6-7（P.6-29）を参照）。

ステップ 4　[Authentication Login Methods] と [Authorization Methods] セクションの下で、WINDOWS に設定されたそれぞれのドロップダウン リストを別のものに変更します。設定の変更の詳細については、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（P.6-26）を参照してください。

ステップ 5　[Submit] をクリックして、設定を保存します。

ステップ 6　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [Windows Domain] を選択します。[Windows Domain Server Settings] ウィンドウが表示されます（図 6-5 を参照）。

ステップ 7　（任意）管理者のユーザ名とパスワードを [Domain administrator username] フィールド、[Domain administrator password] フィールド、および [Confirm password] フィールドに入力します。ユーザ名とパスワードは必須ではありませんが、登録解除を行うためにドメイン コントローラで必要となる場合があります。

ステップ 8　スクロール ダウンして [Unregister] ボタンをクリックします。

（注）　[Unregister] ボタンをクリックすると、WAAS Central Manager は SSH を使用してすぐに登録解除要求を WAAS デバイス（またはデバイス グループ）に送信します。登録解除要求によって、デバイスは指定された Windows ドメイン コントローラから登録解除するよう指示されます。

a.　登録解除要求のステータスを確認するには、数分経ってから [Show Authentication Status] ボタンをクリックします。認証要求のステータスを表示するためにこの要求を続行するかどうかを確認するダイアログボックスが表示されます（図 6-6 を参照）。

b.　[OK] をクリックして続行するか、[Cancel] をクリックして要求を取り消します。

CLI を使用して WAE デバイスを登録解除する場合、まず次のコマンドを使用して Windows 認証を無効にする必要があります。

```
WAE(config)# no authentication login windows-domain enable
WAE(config)# no authentication configuration windows-domain enable
```

次に、次のコマンドを使用して WAAS デバイスを Windows ドメイン サーバから登録解除します（Kerberos 認証の場合）。

```
WAE# windows-domain diagnostics net  "ads leave -U AdminUsername%AdminPassword"
```

NTLM 認証では、WAAS デバイスを登録解除する CLI コマンドがありません。

Edge WAE 用の自動マシン アカウント パスワード変更の無効化

認証用に Windows ドメイン コントローラが設定され、WAFS レガシー モードで動作している Edge WAE で切断モードが有効になっている WAAS ネットワークでは、WAN の障害時にドメイン コントローラは内容要求を認証します。デフォルトで、Windows ドメイン コントローラは、認証プロセスの一環として自動マシン アカウント パスワード変更を実行します。Edge WAE 用のマシン アカウント パスワードは 7 日周期で Edge WAE とドメイン コントローラの間で自動的にネゴシエートされ、変更されます。ただし、認証サービスが停止している場合、このプロセスは実行されず、Edge WAE 用のマシン アカウント パスワードは失効します。

この状況を回避するために、Edge WAE 用の自動マシン アカウント パスワード変更を無効にすることを推奨します。次の手順は、グループ ポリシー エディタを使用して、Windows XP および Windows Server 2003 用の自動マシン アカウント パスワード変更を無効にする方法を示しています。他の Windows オペレーティング システム用の自動マシン アカウント パスワード変更を無効にする方法の詳細については、Microsoft 社の [Help and Support] ページを参照してください。

グループ ポリシー エディタを使用して Edge WAE 用の自動的なマシン アカウント パスワード変更を無効にするには、次の手順に従ってください。

ステップ 1　Windows ドメイン コントローラで、[Start] をクリックし、[Run] を選択します。

ステップ 2　プロンプトで「**Gpedit**」と入力し、[OK] をクリックします。

ステップ 3　[Local Computer Policy]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Settings]、[Local Policies]、[Security] オプションを展開します。

ステップ 4　[Domain Member: Disable machine account password changes (DisablePasswordChange)] 設定を構成します。

LDAP サーバ署名

LDAP サーバ署名は、Microsoft Windows Server のネットワーク セキュリティ設定の設定オプションです。このオプションは、Lightweight Directory Access Protocol（LDAP）クライアント用の署名要件を制御します。LDAP 署名は、LDAP パケットがネットワークの途中で改変されていないことを確認し、パッケージ データが既知の送信元から送信されたことを保証するために使用されます。Windows Server 2003 の管理ツールは、LDAP 署名を使用して、管理ツールの実行インスタンスと管理対象サーバ間の通信の安全を確保します。

トランスポート レイヤ セキュリティ（TLS、RFC 2830）プロトコルを使用してインターネット通信のプライバシーを保護することで、クライアント/サーバアプリケーションは、盗聴、改変、またはメッセージの偽造を防止して通信できます。TLS v1 は、Secure Sockets Layer（SSL）に似ています。TLS は、通常の LDAP 接続（ldap//:389）で SSL と同じ暗号化を提供し、安全な接続（ldaps://:636）で動作します。TLS プロトコルは、サーバ証明書を使用して、暗号化された安全な接続を LDAP サーバに提供します。クライアント認証には、クライアント証明書と 1 組の暗号キーが必要です。

WAAS ソフトウェアでは、ドメイン セキュリティ ポリシー用の *LDAP サーバ署名要求*オプションを「Require signing（署名が必要）」に設定すると、Windows 2003 ドメインでのログイン認証がサポートされます。LDAP サーバ署名機能により、WAE はドメインに参加してユーザを安全に認証できます。

（注）　Windows ドメイン コントローラで LDAP 署名が必要となるように設定するときは、クライアント WAE でも LDAP 署名を設定する必要があります。LDAP 署名を使用するようにクライアントを設定しないと、サーバとの通信が影響を受け、ユーザ認証、グループ ポリシー設定、およびログイン スクリプトが失敗する場合があります。サーバの証明書を持つ Microsoft サーバに認証局サービスをインストールします（[Programs] > [Administrative Tools] > [Certification Authority]）。Microsoft サーバで LDAP サーバ署名要件プロパティを有効にします（[Start] > [Programs] > [Administrative Tools] > [Domain Controller Security Policy]）。表示されるウィンドウで、ドロップダウン リストから [Require signing] を選択し、[OK] をクリックします。

Windows ドメイン コントローラで LDAP 署名が必要となるように設定する方法については、Microsoft 社のマニュアル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。

- 「クライアント WAE 上での LDAP 署名の設定」（P.6-25）
- 「クライアント WAE 上の LDAP サーバ署名の無効化」（P.6-26）

クライアント WAE 上での LDAP 署名の設定

Windows 2003 ドメイン コントローラで、クライアント（WAE など）に LDAP 要求に署名することを要求するセキュリティ設定を構成できます。署名のないネットワーク トラフィックは、途中で傍受されたり、改変される可能性があり、一部の組織は、LDAP サーバでの中間者攻撃を防止するために LDAP サーバ署名を義務付けています。LDAP 署名は、個別の WAE 単位で設定できます。システム レベルでは設定できません。さらに、WAAS CLI を使用して WAE 上の LDAP 署名を設定する必要があります。WAAS GUI（WAAS Central Manager GUI または WAE Device Manager GUI）では、LDAP 署名を設定できません。

デフォルトで、LDAP サーバ署名は、WAE で無効になっています。WAE でこの機能を有効にするには、次の手順に従ってください。

ステップ 1　WAE で LDAP サーバ署名を有効にします。

```
WAE# configure terminal
WAE(config)# smb-conf section "global" name "ldap ssl" value "start_tls"
```

ステップ 2　WAE で設定を保存します。

```
WAE(config)# exit
WAE# copy run start
```

ステップ 3　WAE で、現在動作している LDAP クライアントの設定を確認します。

```
WAE# show smb-conf
```

ステップ 4　WAE を Windows ドメインに登録します。

```
WAE# windows-domain diagnostics net "ads join -U Administrator%password"
```

ステップ 5　WAE でユーザ ログイン認証を有効にします。

```
WAE# configure
WAE(config)# authentication login windows-domain enable primary
```

ステップ 6　WAE でユーザ ログイン許可を有効にします。

```
WAE(config)# authentication configuration windows-domain enable primary
```

ステップ 7　WAE でログインの認証と許可の現在の設定を確認します。

```
WAE# show authentication user
Login Authentication:    Console/Telnet/Ftp/SSH Session
------------------------------ ------------------------------
local                                enabled (secondary)
Windows domain           enabled (primary)
Radius                            disabled
Tacacs+                          disabled

Configuration Authentication: Console/Telnet/Ftp/SSH Session
------------------------------ ------------------------------
local                                 enabled (primary)
Windows domain           enabled (primary)
Radius                             disabled
Tacacs+                           disabled
```

この時点で、WAE は、Active Directory ユーザを認証するように設定されています。Active Directory ユーザは、Telnet、FTP、または SSH を使用して WAE に接続できます。また、WAAS GUI（WAAS CentralManager GUI または WAE Device Manager GUI）を使用して WAE にアクセスできます。

ステップ 8　Windows ドメイン ユーザ認証に関連する統計情報を表示します。ユーザ認証が行われるたびに、統計情報が追加されます。

```
WAE# show statistics windows-domain
Windows Domain Statistics
  ---------------------------------------------
  Authentication:
    Number of access requests:                    9
    Number of access deny responses:              3
    Number of access allow responses:             6
  Authorization:
    Number of authorization requests:             9
    Number of authorization failure responses:    3
    Number of authorization success responses:    6
  Accounting:
    Number of accounting requests:                0
    Number of accounting failure responses:       0
    Number of accounting success responses:       0

WAE# show statistics authentication
    Authentication  Statistics
    ------------------------------------
    Number of access requests:        9
    Number of access deny responses:  3
    Number of access allow responses: 6
```

ステップ 9　WAE に関する統計情報を消去するには、**clear statistics** EXEC コマンドを使用します。

- すべてのログイン認証統計情報を消去するには、**clear statistics authentication** EXEC コマンドを入力します。
- Windows ドメイン認証に関連する統計情報だけを消去するには、**clear statistics windows-domain** EXEC コマンドを入力します。
- すべての統計情報を消去するには、**clear statistics all** EXEC コマンドを入力します。

クライアント WAE 上の LDAP サーバ署名の無効化

WAE 上の LDAP サーバ署名を無効にするには、次の手順に従ってください。

ステップ 1　Windows ドメインから WAE の登録を解除します。

```
WAE# windows-domain diagnostics net "ads leave -U Administrator"
```

ステップ 2　ユーザ ログイン認証を無効にします。

```
WAE# configure
WAE(config)# no authentication login windows-domain enable primary
```

ステップ 3　WAE で LDAP サーバ署名を無効にします。

```
WAE(config)# no smb-conf section "global" name "ldap ssl" value "start_tls"
```

WAAS デバイス用の管理ログイン認証および許可方式の有効化

この項では、WAAS デバイスまたはデバイス グループ用のさまざまな管理ログイン認証および許可方式（認証設定）を一元的に有効にする方法について説明します。

注意　ローカル認証および許可を無効にする前に、RADIUS、TACACS+、または Windows ドメイン認証が設定され、正常に動作していることを確認します。ローカル認証が無効で、RADIUS、TACACS+、または Windows ドメイン認証が正しく設定されていない場合、もしくは RADIUS、TACACS+、または Windows ドメイン サーバがオンラインでない場合は、WAAS デバイスにログインできないことがあります。

デフォルトで、WAAS デバイスは、ローカル データベースを使用して、管理ログイン要求を認証し、アクセス権を許可します。WAAS デバイスは、すべての認証データベースが無効であるかどうかを確認し、そうである場合は、システムをデフォルトの状態に設定します。このデフォルトの状態の詳細については、「管理ログインの認証および許可のデフォルト設定」（P.6-4）を参照してください。

（注）　これらの設定を構成し、送信する前に、WAAS デバイス（またはデバイス グループ）用の TACACS+、RADIUS、または Windows サーバ設定を構成する必要があります。WAAS デバイスまたはデバイス グループでこれらのサーバ設定を構成する方法については、「TACACS+ サーバ認証設定について」（P.6-15）、「RADIUS サーバ認証設定の構成」（P.6-12）、および「Windows ドメイン サーバ認証設定の構成」（P.6-17）を参照してください。

デフォルトでは、WAAS デバイスは、何らかの理由でプライマリ方式の管理ログイン認証が失敗した場合に、セカンダリ方式の管理ログイン認証にフェールオーバーします。WAAS Central Manager GUI を使用して、このデフォルトのログイン認証フェールオーバー方式を変更します。

- WAAS デバイスのデフォルト値を変更するために、[My WAN] > [Manage Devices] を選択します。デフォルトのログイン認証フェールオーバー方式を変更する WAAS デバイスの名前の横にある [Edit] アイコンをクリックし、ナビゲーション ペインで [Configure] > [Security] > [AAA] > [Authentication Methods] を選択します。表示されるウィンドウで [Failover to next available authentication method] チェックボックスを選択し、[Submit] をクリックします。
- デバイス グループのデフォルト値を変更するために、[My WAN] > [Manage Device Groups] を選択します。デフォルトのログイン認証フェールオーバー方式を変更するデバイス グループの名前の横にある [Edit] アイコンをクリックし、ナビゲーション ペインで [Configure] > [Security] > [AAA] > [Authentication Methods] を選択します。表示されるウィンドウで [Failover to next available authentication method] チェックボックスを選択し、[Submit] をクリックします。

[failover to next available authentication method] オプションを有効にすると、WAAS デバイス（またはデバイス グループ内のデバイス）は、認証が何らかの別の理由で失敗した場合ではなく、管理ログイン認証サーバに到達できない場合にだけ、次の認証方式を照会します。

複数の TACACS+ サーバまたは RADIUS サーバを設定できる場合は、まずプライマリ サーバで認証が試みられます。プライマリ サーバに到達できなければ、TACACS+ ファームまたは RADIUS ファーム内のその他のサーバでの認証試行が順に行われていきます。サーバに到達不能という以外の何らかの理由で認証に失敗した場合は、ファーム内の他のサーバでの認証試行は行われません。このプロセスは、[Failover to next available authentication method] チェックボックスの設定に関係なく適用されます。

（注）　ログイン認証フェールオーバー機能を使用するには、TACACS+、RADIUS、または Windows ドメインをプライマリ認証方式として、ローカルをセカンダリ ログイン認証方式として設定する必要があります。

[failover to next available authentication method] オプションが *enabled*（有効）の場合は、次のガイドラインに従ってください。

- WAAS デバイスに設定できるログイン認証方式は 2 つ（プライマリおよびセカンダリ方式）だけです。

- WAAS デバイス（またはデバイス グループ内のデバイス）は、指定した認証サーバが到達不能な場合にだけ、プライマリ認証方式からセカンダリ認証方式へフェールオーバーします。
- 認証と許可（設定）の両方のセカンダリ方式として、ローカル データベース方式を設定します。

たとえば、[failover to next available authentication method] オプションが有効で、RADIUS がプライマリ ログイン認証方式、ローカルがセカンダリ ログイン認証方式として設定されている場合は、次のように処理されます。

1. WAAS デバイス（またはデバイス グループ内のデバイス）は、管理ログイン要求を受信すると、外部の RADIUS 認証サーバを照会します。
2. 次のどちらかが実行されます。
   a. RADIUS サーバが到達可能である場合、WAAS デバイス（またはデバイス グループ内のデバイス）は、この RADIUS データベースを使用して管理者を認証します。
   b. RADIUS サーバが到達不能な場合、WAAS デバイスはセカンダリ認証方式を使用して（つまり、ローカル認証データベースを照会して）、管理者の認証を試みます。

（注） ローカル データベースは、この RADIUS サーバが使用できない場合にだけ、認証のためにアクセスされます。それ以外の場合（たとえば、RADIUS サーバでの認証に失敗した場合）は、認証のためにローカル データベースはアクセスされません。

逆に、[failover to next available authentication method] オプションが *disabled*（無効）の場合は、WAAS デバイス（またはデバイス グループ内のデバイス）は、プライマリ認証データベースで認証に失敗した理由に関係なく、セカンダリ認証データベースにアクセスします。

すべての認証データベースの使用が有効になっている場合は、フェールオーバーの理由に基づき、選択された優先順位で、すべてのデータベースが照会されます。フェールオーバーの理由が指定されていない場合は、すべてのデータベースがその優先順位で照会されます。たとえば、最初にプライマリ認証データベースが照会され、次にセカンダリ認証データベースが照会され、最後に第 3 のデータベースが照会されます。

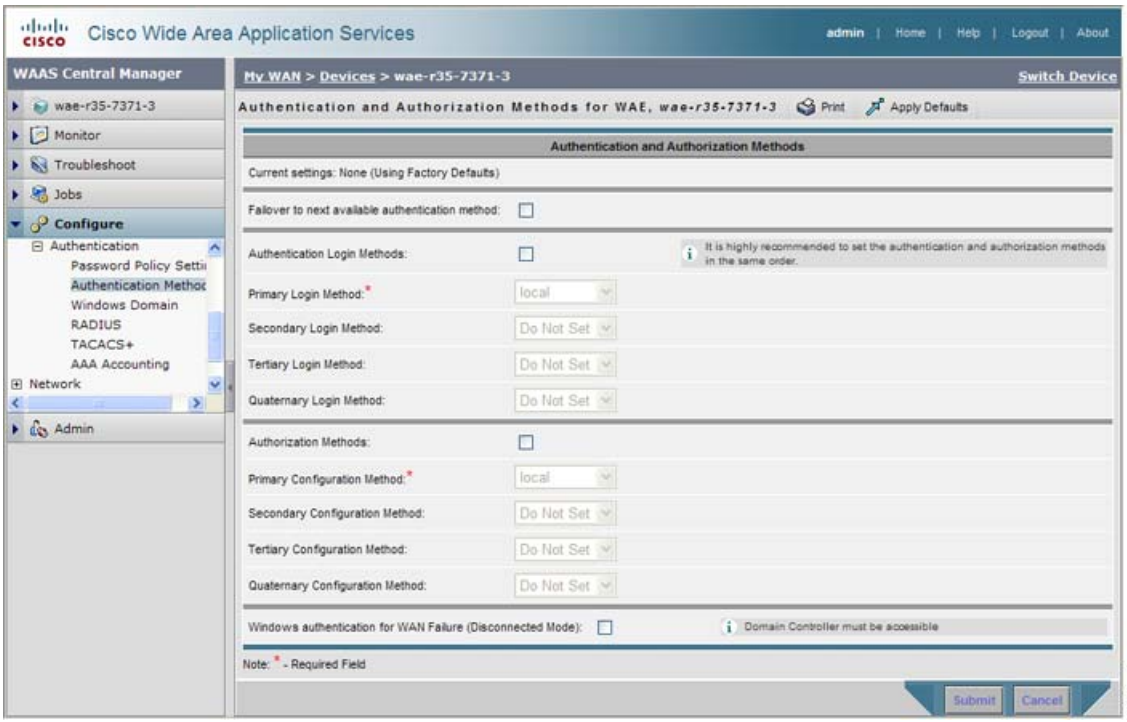
WAAS デバイスまたはデバイス グループ用のログイン認証および許可方式を指定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [Authentication Methods] を選択します。[Authentication and Authorization Methods] ウィンドウが表示されます（図 6-7 を参照）。

図 6-7　[Authentication and Authorization Methods] ウィンドウ



ステップ 4　[Failover to next available authentication method] チェックボックスを選択して、1 次認証サーバに到達できない場合にだけ 2 次認証データベースを照会します。このチェックボックスが選択解除されている場合は、何らかの理由でプライマリ認証方式が失敗すると、他の認証方式が試行されます。

この機能を使用するには、TACACS+、RADIUS、または Windows ドメインをプライマリ認証方式として、ローカルをセカンダリ ログイン認証方式として設定する必要があります。認証と許可（設定）の両方の 2 次方式として、必ず、ローカル方式を設定してください。

ステップ 5　[Authentication Login Methods] チェックボックスを選択して、ローカル、TACACS+、RADIUS、または Windows データベースを使用して認証特権を有効にします。

ステップ 6　選択したデバイスまたはデバイス グループが使用するログイン認証方式の順序を指定します。

a. [Primary Login Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [WINDOWS] を選択します。このオプションは、選択したデバイス（またはデバイス グループ）が、管理ログイン認証に使用する必要がある最初の方式を指定します。

b. [Secondary Login Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [Windows] を選択します。このオプションは、最初の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理ログイン認証に使用する必要がある方式を指定します。

c. [Tertiary Login Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [Windows] を選択します。このオプションは、最初の方式と第 2 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理ログイン認証に使用する必要がある方式を指定します。

d. [Quaternary Login Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [Windows] を選択します。このオプションは、最初の方式、第 2 の方式、および第 3 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理ログイン認証に使用する必要がある方式を指定します。

（注）　ログイン認証方式と許可方式の優先順位リストの最後の方式として、ローカル方式を指定することを強く推奨します。この方法に従うことで、指定した外部のサードパーティ サーバ（TACACS+、RADIUS、または Windows ドメイン サーバ）に到達可能できない場合でも、WAAS 管理者は、ローカル認証方式と許可方式を使用して WAAS デバイスにログインできます。

ステップ 7　[Authentication Methods] チェックボックスを選択して、ローカル、TACACS+、RADIUS、または Windows データベースを使用して認証特権を有効にします。

（注）　許可特権は、コンソールと Telnet の接続試行、安全な FTP（SFTP）セッション、およびセキュア シェル（SSH、バージョン 1 およびバージョン 2）セッションに適用されます。

ステップ 8　選択したデバイス（またはデバイス グループ）が使用する必要があるログイン許可（設定）方式の順序を指定します。

（注）　管理ログインの認証方式と許可方式を同じ順序で設定することを強く推奨します。たとえば、管理ログイン認証と許可の両方の 1 次ログイン方式として RADIUS を使用し、2 次ログイン方式として TACACS+ を使用し、第 3 の方式として Windows を使用し、第 4 の方式としてローカル方式を使用するように、WAAS デバイスを設定します。

a. [Primary Configuration Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [WINDOWS] を選択します。このオプションは、選択したデバイス（またはデバイス グループ）が、管理特権を決定するために使用する必要がある最初の方式を指定します。

（注）　（ステップ 4 で）[Failover to next available authentication method] チェックボックスを選択した場合は、必ず、[Primary Configuration Method] ドロップダウン リストから [TACACS+] または [RADIUS] を選択して、1 次許可（設定）方式として TACACS+ または RADIUS 方式を設定してください。

b. [Secondary Configuration Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [WINDOWS] を選択します。このオプションは、最初の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理特権を決定するために使用する必要がある方式を指定します。

（注）　（ステップ 4 で）[Failover to next available authentication method] チェックボックスを選択した場合は、必ず、[Secondary Configuration Method] ドロップダウン リストから [local] を選択して、2 次許可（設定）方式として ローカル方式を設定してください。

c. [Tertiary Configuration Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [WINDOWS] を選択します。このオプションは、最初の方式と第 2 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理特権を決定するために使用する必要がある方式を指定します。

d. [Quaternary Configuration Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [WINDOWS] を選択します。このオプションは、最初の方式、第 2 の方式、および第 3 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理特権を決定するために使用する必要がある方式を指定します。

ステップ 9　[Windows authentication for WAN Failure (Disconnected Mode)] チェックボックスを選択して、切断モードでの内容要求認証を有効にします。切断モードは、WAFS レガシー モードを使用している場合にだけ使用できます。

この機能を有効にすると、Windows ドメイン サーバは、切断モードで内容要求を認証します。デフォルトでは、この機能は、WAE で無効になっています。

この機能を有効にする場合は、WAE 用の自動アカウント パスワード変更を無効にすることを推奨します。詳細については、「Edge WAE 用の自動マシン アカウント パスワード変更の無効化」（P.6-23）を参照してください。

（注）　切断モードに対する Windows 認証は、「Windows ドメイン サーバ認証設定の構成」（P.6-17）の説明に従って、NTLM を [Windows Domain setting] ウィンドウで共有認証方式として選択した場合にだけ動作します。

ステップ 10　[Submit] をクリックして、設定を保存します。

（注）　Windows の認証または許可方式を有効にしていた場合は、Central Manager が WAE に問い合わせて、それが Windows ドメインに登録されていることを確認します。これには、[Submit] をクリックした後、最大で 1 分間かかる場合があります。このプロセスについて確認を求めるメッセージが表示され、[OK] をクリックしなければ先に進みません。デバイス グループの設定を行っている場合は、Central Manager が個々の WAE に問い合わせることはなく、各 WAE が正常に登録されていることを管理者が確認する必要があります。システムの動作は不明である（WAE が登録されていない場合）ことを知らせるメッセージが表示され、[OK] をクリックしなければ先に進みません。

（注）　Windows 認証方式を有効にした場合は、アクティブになるまで約 15 秒かかります。Windows 認証ステータスの確認や、Windows 認証が必要な操作を実行するまでに、少なくとも 15 秒待ってください。

CLI からログイン認証および許可方式を設定するには、**authentication** グローバル コンフィギュレーション コマンドを使用できます。デバイスに対して Windows ドメイン認証および許可方式を有効にする前に、デバイスを Windows ドメイン コントローラで登録する必要があります。

AAA コマンド許可の設定

コマンド許可は、外部 AAA サーバを通じて、CLI ユーザによって実行された各コマンドの許可を行います。CLI ユーザによって実行されたコマンドはすべて、許可されなければ実行されません。RADIUS ユーザ、Windows ドメイン ユーザ、およびローカル ユーザは、影響を受けません。

（注）　CLI インターフェイスを通じて実行されたコマンドだけが、コマンド許可の対象となります。

コマンド許可が有効になっている場合、許可されたコマンドが引数なしで実行されるようにするには、TACACS+ サーバ上で "permit null" を指定する必要があります。

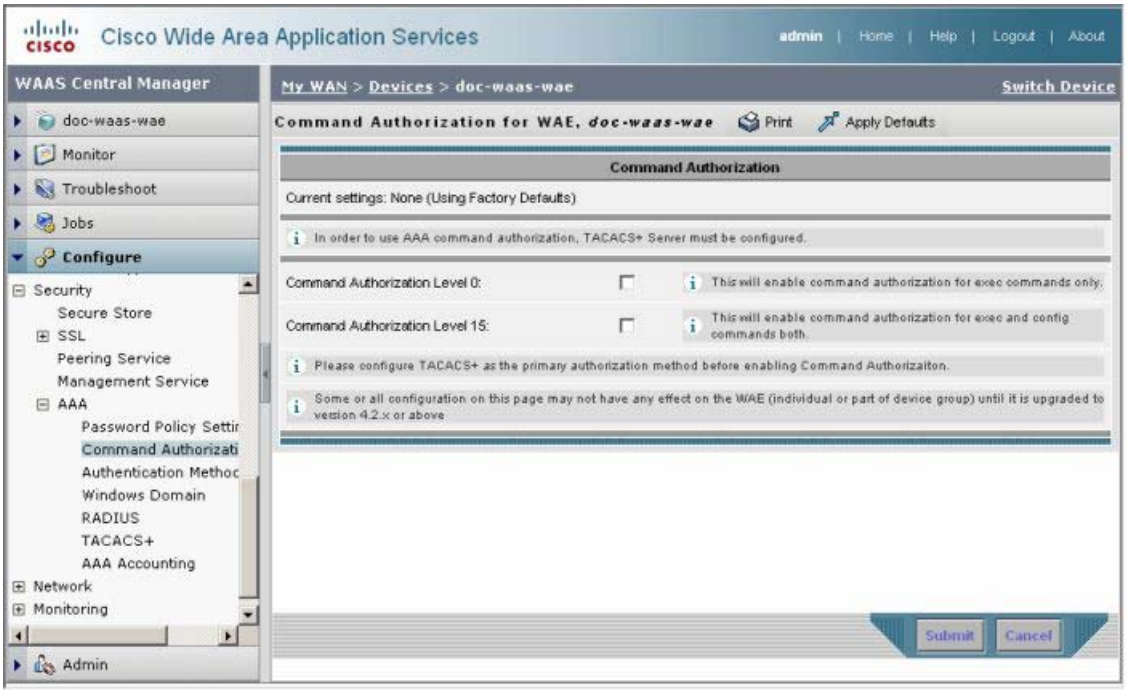
WAAS デバイスまたはデバイス グループのコマンド許可を設定するには、次の手順を実行します。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [Command Authorization] を選択します。[Command Authorization] ウィンドウが表示されます（図 6-8 を参照）。

図 6-8　[Command Authorization] 設定ウィンドウ



ステップ 4　必要なレベルの [Command Authorization Level] チェックボックスをオンにします。

- レベル 0：ユーザのレベル（通常ユーザかスーパー ユーザか）に関係なく、EXEC コマンドだけが実行される前に TACACS+ サーバによって許可されます。グローバル コンフィギュレーション コマンドは許可されません。
- レベル 15：ユーザのレベル（通常ユーザかスーパー ユーザか）に関係なく、EXEC コマンドとグローバル コンフィギュレーション レベルのコマンドの両方が、実行される前に TACACS+ サーバによって許可されます。

（注）　コマンド許可を設定するには、その前に TACACS+ サーバを設定しておく必要があります。

ステップ 5　[Submit] をクリックして、設定を保存します。

WAAS デバイス用の AAA アカウンティングの設定

アカウンティングは、すべてのユーザの操作と操作が行われた日時を追跡します。監査証跡または接続時間やリソース使用量（転送バイト数）の課金に使用できます。デフォルトで、アカウンティングは無効になっています。

WAAS アカウンティング機能は、TACACS+ サーバ ログ機能を使用します。アカウンティング情報は、TACACS+ サーバだけに送信されます。コンソールや他のデバイスには送信されません。WAAS デバイスの syslog ファイルは、アカウンティング イベントをローカルに記録します。syslog に保存されるイベントの形式は、アカウンティング メッセージの形式と異なります。

TACACS+ プロトコルを使用すると、WAAS デバイスと中央サーバの間で、AAA 情報を効率的に通信できます。TACACS+ プロトコルは、TCP を使用して、クライアントとサーバの間に信頼できる接続を確立します。WAAS デバイスは、認証および許可要求とアカウンティング情報を TACACS+サーバへ送信します。

（注） WAAS デバイス用の AAA アカウンティング設定を構成する前に、WAAS デバイス用の TACACS+ サーバ設定を構成する必要があります（「TACACS+ サーバ認証設定について」（P.6-15）を参照）。

（注） デバイスに対して AAA アカウンティングを有効にする場合は、コマンド処理中の遅延を回避するために TACACS+ サーバへのアクセスを許可する IP ACL 条件を最初のエントリ位置に作成することを強く推奨します。IP ACL については、第 8 章「WAAS デバイス用の IP ACL の作成および管理」を参照してください。

WAAS デバイスまたはデバイス グループ用の AAA アカウンティング設定を一元的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [AAA] > [AAA Accounting] を選択します。[AAA Accounting Settings] ウィンドウが表示されます

ステップ 4　[System Events] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）がリロードなどのユーザに関連しないシステム レベル イベントをいつ追跡するかを指定し、イベント用のアカウンティングをアクティブにするキーワードを選択します。

ステップ 5　[Exec Shell and Login/Logout Events] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）が EXEC シェルとユーザ ログインおよびログアウトに関するイベントをいつ追跡するかを指定し、EXEC モード プロセス用のアカウンティングをアクティブにするキーワードを選択します。レポートには、ユーザ名、日付、開始時刻と終了時刻、および WAAS デバイスの IP アドレスが記載されます。

ステップ 6　[Normal User Commands] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）が通常のユーザ特権レベル（特権レベル 0）ですべてのコマンドをいつ追跡するかを指定し、superuser でない管理（通常のユーザ）レベルですべてのコマンドのアカウンティングをアクティブにするキーワードを選択します。

ステップ 7　[Administrative User Commands] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）が superuser 特権レベル（特権レベル 15）ですべてのコマンドをいつ追跡するかを指定し、superuser 管理ユーザ レベルですべてのコマンドのアカウンティングをアクティブにするキーワードを選択します。

注意　**wait-start** オプションを使用する前に、WAAS デバイスが TACACS+ サーバで設定され、正常にサーバにアクセスできることを確認してください。WAAS デバイスは、設定されている TACACS+ サーバにアクセスできない場合に、応答しなくなることがあります。

表 6-2 で、イベントの種類のオプションについて説明します。

表 6-2　AAA アカウンティング用のイベントの種類

GUI パラメータ	機能
イベントの種類のオプション	
stop-only	WAAS デバイスは、指定されたアクティビティまたはイベントの終了時に、停止レコード アカウンティング通知を TACACS+ アカウンティング サーバへ送信します。
start-stop	WAAS デバイスは、イベントの開始時に開始レコード アカウンティング通知、イベントの終了時に停止レコード アカウンティング通知を TACACS+ アカウンティング サーバへ送信します。 開始アカウンティング レコードは、バックグラウンドで送信されます。開始アカウンティング レコードが TACACS+ アカウンティング サーバによって受信応答されたかどうかに関係なく、要求されたユーザ サービスが開始します。
wait-start	WAAS デバイスは、開始アカウンティング レコードと停止開始アカウンティング レコードの両方を TACACS+ アカウンティング サーバへ送信します。ただし、要求されたユーザ サービスは、開始アカウンティング レコードが受信応答されるまで開始しません。停止アカウンティング レコードも送信されます。
Do Not Set	指定したイベント用のアカウンティングが無効になります。

ステップ 8　[Submit] をクリックして、設定を保存します。

CLI から AAA アカウンティング設定を構成するには、**aaa accounting** グローバル コンフィギュレーション コマンドを使用できます。

監査証跡ログの表示

WAAS Central Manager デバイスは、システムでのユーザの操作をログに記録します。ログに記録される唯一の操作は、WAAS ネットワークを変更する操作です。WAAS システムでユーザの操作の記録を表示する詳細については、「監査証跡ログの表示」（P.16-63）を参照してください。

CHAPTER 7

管理者ユーザ アカウントおよびグループの作成と管理

この章では、Wide Area Application Service（WAAS）Central Manager GUI からユーザ アカウントおよびグループを作成する方法について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

管理者ユーザ アカウントの概要

WAAS システムでは、WAAS Central Manager GUI や WAAS CLI にアクセスするために使用できる管理者アカウントがすでに作成されています。このアカウントのユーザ名は *admin*、パスワードは *default* です。このアカウントのパスワードを変更するには、WAAS Central Manager GUI を使用します。

追加の管理者ユーザ アカウントを作成する場合は、2 種類のアカウントの説明について表 7-1 を参照してください。

表 7-1　アカウントの種類の説明

アカウントの種類	説明
ロールに基づくアカウント	特定の WAAS サービスを管理し、設定するアカウントを作成できます。たとえば、アプリケーション アクセラレーションの設定を特定の管理者に委譲したい場合があります。この場合、[Acceleration] ページだけにアクセスできるロールに基づくアカウントを作成できます。 あるいは、WAAS Central Manager GUI の代わりに WAE Device Manager だけにアクセスできるロールに基づくアカウントを作成できます。また、ローカル ユーザ アカウントでもあるロールに基づくアカウントを作成できます。 ロールに基づくアカウントは、WAAS Central Manager GUI の [Admin] ドロワーから作成します。
ローカル アカウント	ユーザは、CLI から WAE デバイスにアクセスでき、オプションで Print Services Administration GUI と WAE Device Manager GUI にアクセスできます。この種類のアカウントを持つユーザは、WAAS Central Manager にログインできますが、アクセス権は GUI 機能にアクセスできないデフォルトのアカウントに初期設定されます。 CLI だけから WAE デバイスまたは WAE Device Manager GUI にアクセスする必要がある管理者がいる場合は、ローカル アカウントを作成することを推奨します。 ローカル アカウントは、ロールに基づくアカウントと同じように作成しますが、アカウントを作成するときに [Local User] チェックボックスを選択します。

ユーザ アカウントの作成と管理

ここでは、次の内容について説明します。

アカウントの作成の概要

表 7-2 に、ロールに基づく新しい管理者アカウントを作成するために完了する必要がある手順の概要を示します。

表 7-2　ロールに基づく管理者アカウントを作成するためのチェックリスト

作業	追加情報と手順
1. 新しいアカウントを作成する。	システムに、特定のユーザ名、パスワード、および特権レベルを持つアカウントを作成します。詳細については、「新しいアカウントの作成」（P.7-4）を参照してください。
2. 新しいアカウントのロールを作成する。	アカウントが WAAS ネットワークで設定できるサービスを指定するロールを作成します。詳細については、「新しいロールの作成」（P.7-11）を参照してください。外部認証サーバを使用している場合、ユーザにロールを自動的に割り当てる一致ユーザ グループを定義できます。

表 7-2　ロールに基づく管理者アカウントを作成するためのチェックリスト （続き）

作業	追加情報と手順
3. 新しいアカウントにロールを割り当てる。	新しいアカウントに新しいロールを割り当てます。詳細については、「ユーザ アカウントへのロールの割り当て」（P.7-13）を参照してください。外部認証サーバを使用している場合、ユーザにロールを自動的に割り当てる一致ユーザ グループを定義できます。
4. ドメインを作成する。	新しいアカウントが管理できる WAE またはデバイス グループを指定するドメインを作成します。詳細については、「新しいドメインの作成」（P.7-15）を参照してください。
5. ドメインにエンティティを追加する。	ドメインに 1 つまたは複数の WAE またはデバイス グループを追加します。詳細については、「エンティティのドメインへの追加」（P.7-15）を参照してください。
6. ユーザ アカウントにドメインを割り当てる。	新しいユーザ アカウントにドメインを割り当てます。詳細については、「ユーザ アカウントへのドメインの割り当て」（P.7-16）を参照してください。外部認証サーバを使用している場合、ユーザにドメインを自動的に割り当てる一致ユーザ グループを定義できます。

アカウントの操作

ユーザ アカウントを作成するときは、ユーザ名、アカウントを所有する個人の氏名、連絡先情報、職位、部門のような、ユーザに関する情報を入力します。すべてのユーザ アカウント情報は、WAAS Central Manager の内部のデータベースに保存されます。

次に、各ユーザ アカウントにロールを割り当てることができます。*ロール*は、ユーザがアクセスできる WAAS Central Manager GUI の設定ページとユーザが設定または変更する権限を持つサービスを定義します。WAAS Central Manager は、admin と print という 2 つの定義済みのロールを提供します。admin ロールは、すべてのサービスにアクセスできます。print ロールは、すべての印刷関連ページにアクセスできます。*ドメイン*は、ユーザがアクセスして設定または変更できるネットワーク内のエンティティを定義します。ユーザ アカウントには、ロールおよびドメインを割り当てることも、割り当てないこともできます。

ユーザ アカウントに加え、TACACS+ または Windows ドメイン サーバ（RADIUS サーバではなく）でユーザの外部認証を使用している場合は、ユーザ グループを作成できます。外部認証サーバで定義されたユーザ グループと一致するユーザ グループ名を作成することにより、WAAS は外部認証サーバで定義されているとおりに、グループのメンバシップに基づいて、ユーザにロールおよびドメインをダイナミックに割り当てることができます。各ユーザに個別にロールまたはドメインを定義する必要はありません。

（注）　TACACS+ サーバでユーザの外部認証を使用する場合、ユーザ名を数字から始めたり、数字だけで構成したりすることはできません。そのようなユーザ名を使用すると、ログインに失敗します。

WAAS Central Manager には、あらかじめ 2 つのデフォルトのユーザ アカウントが設定されています。最初のアカウント、*admin* アカウントは、システムのすべてのサービスとすべてのエンティティにアクセスできる管理者ロールに割り当てられます。このアカウントはシステムから削除できませんが、変更することはできます。このアカウントのユーザ名とロールは変更できません。admin ロールを割り当てられたアカウントだけが、他の admin レベルのアカウントを作成できます。

設定済みの 2 番めのユーザ アカウントは、*default* アカウントです。認証されても、まだ WAAS Central Manager に登録されていないユーザ アカウントは、default アカウントに割り当てられているアクセス権（ロール）を取得します。このアカウントは管理者が設定できますが、削除したり、ユーザ名を変更したりすることはできません。当初、default アカウントは、ロールが定義されていないため、GUI 機能にアクセスできません。ただし、WAAS Central Manager GUI にはログインできます。

ここでは、次の内容について説明します。

新しいアカウントの作成

アカウントをセットアップする最初の手順では、ユーザ名を指定し、ローカル CLI アカウントを同時に作成するかどうかを選択して、アカウントを作成します。アカウントを作成したら、アカウントが管理し、設定できる WAAS サービスとデバイスを決定するロールをアカウントに割り当てることができます。

表 7-3 に、アカウントをセットアップするときにローカル CLI ユーザを作成することの結果について説明します。

表 7-3　ローカル ユーザを作成することによる結果

処理	結果
ローカル ユーザの作成	• アカウントを使用して、WAAS CLI、WAAS Central Manager GUI（デフォルトのロールで）、および WAE Device Manager（オプションを選択した場合）にアクセスできます。 • ユーザは自身のパスワードを変更でき、パスワードの変更はスタンバイ WAAS Central Manager に伝達されます。 • アカウントは WAAS Central Manager データベースに保存され、スタンバイ WAAS Central Manager に伝達されます。
ローカル ユーザの非作成	• プライマリおよびスタンバイ WAAS Central Manager 管理データベースに、ユーザ アカウントが作成されます。 • CLI にはユーザ アカウントが作成されません。ユーザは、CLI にアクセスするために別のアカウントを使用する必要があります。 • 外部認証サーバが設定されている場合、新しいアカウントを使用して WAAS Central Manager GUI にログインできます。ユーザには、デフォルト ユーザ用に定義されているロールが割り当てられます（当初はロールなし）。 • ローカル ユーザは、[Admin] > [AAA] セクションにアクセスできるロールを持っている場合だけ、WAAS Central Manager GUI を使用して自身のパスワードを変更できます。

（注） ユーザ アカウントが CLI だけから作成された場合、初めて WAAS Central Manager GUI にログインすると、Centralized Management System（CMS）が、デフォルトの許可とアクセス制御を持つユーザ アカウント（ユーザ名は CLI で設定されたユーザ名）を自動的に作成します。CLI から作成されたア

カウントは、当初、WAAS Central Manager GUI のどの設定ページにもアクセスできません。CLI から作成されたアカウントに WAAS Central Manager GUI から設定作業を実行する必要があるロールを割り当てるには、admin アカウントを使用する必要があります。

新しいアカウントを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users] を選択します。

[User Accounts] ウィンドウに、システム上のすべてのユーザ アカウントが表示されます。

ステップ 2　[Create New User Accounts] アイコンをクリックします。

[Creating New User Account] ウィンドウが表示されます。

（注）　このウィンドウには、管理者レベルの特権を持つユーザだけがアクセスできます。

ステップ 3　[Username] フィールドに、ユーザ アカウント名を入力します。

ユーザ名は大文字と小文字が区別され、英字、数字、ピリオド、ハイフン、およびアンダースコア以外の文字は使用できません。

ステップ 4　ユーザが WAE Device Manager GUI にアクセスできるようにするには、次の手順に従ってください。

a.　[WAE Device Manager User] チェックボックスを選択します。

b.　[Device Manager Access] ドロップダウン リストから、このアカウントが Device Manager GUI にアクセスするためのオプションを選択します。

- [Read Only]：このユーザに許可するアクセスを Device Manager GUI への読み取り専用に制限します。
- [Read Write]：このユーザに Device Manager GUI への読み取り / 書き込みアクセスを許可します。

ステップ 5　ローカル CLI ユーザ アカウントを作成するには、次の手順に従ってください。

a.　[Local User] チェックボックスを選択します。ローカル CLI ユーザを作成する利点については、表 7-3（P.7-4）を参照してください。すべての WAE デバイスにローカル ユーザが作成されます。

（注）　外部認証サーバに定義済みで、WAAS デバイスへのアクセスが許可されているユーザ名と同じユーザ名のローカル ユーザは作成しないでください。

b.　[Password] フィールドにローカル ユーザ アカウントのパスワードを入力し、[Confirm password] フィールドに同じパスワードを再入力します。パスワードは大文字と小文字の区別をし、長さは 1 ～ 31 字である必要があります。‘ “ | （一重引用符、二重引用符、パイプ）の文字、または制御文字を含めることはできません。

c.　[CLI Privilege Level] ドロップダウン リストから、ローカル ユーザ アカウント用のオプションを選択します。

- [0]（通常のユーザ）：このユーザが使用できる CLI コマンドをユーザ レベルの EXEC コマンドだけに制限します。これは、デフォルトの値です。
- [15]（スーパー ユーザ）：このユーザに特権 EXEC レベルの CLI コマンドの使用を許可します。このレベルのコマンドは、admin ロールの Central Manager GUI ユーザが実行できる機能と似ています。

（注）　システム動作を設定、表示、およびテストするには、WAAS の CLI EXEC モードを使用します。このモードは、ユーザと特権の 2 つのアクセス レベルに分かれています。「通常」の特権を持つローカル ユーザは、ユーザ レベルの EXEC CLI モードだけにアクセスできます。「スーパーユーザ」特権を持つローカル ユーザは、特権 EXEC モードと他のすべてのモード（たとえば、コンフィギュレーション モードとインターフェイス モード）にアクセスして、任意の管理作業を実行できます。ユーザ レベルおよび特権 EXEC モードと CLI コマンドの詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

ステップ 6　[Print Admin] チェックボックスを選択して、このアカウントを使用して WAAS Central Manager 上の中央レポジトリにドライバをアップロードし、Print Services Administration GUI にアクセスします。

詳細については、「ドライバ リポジトリとしての WAAS Central Manager の設定」（P.13-17）および「Print Services Administration GUI の使用方法」（P.13-28）を参照してください。

print admin アカウントについては、次の事項に注意してください。

- この [Print Admin] チェックボックスは、[Local User] チェックボックスを選択しないと有効になりません。
- アカウントを使用してリポジトリにドライバをアップロードするには、print admin アカウントに特権レベル 15（特権ユーザ）が必要です。print admin アカウントの特権レベルが 0 の場合、Print Services Administration GUI にアクセスするためだけに使用できます。
- print admin アカウントは、print または admin ロールが割り当てられていない場合、WAAS Central Manager の印刷関連ページにアクセスできません。
- print admin アカウントにドメインを割り当てる必要があります。ユーザがアクセスする必要のあるすべての WAE を割り当てたドメインに所属させる必要があります。
- 外部認証ユーザには、print ロールを割り当てることができません。

ステップ 7　（任意）[User Information] フィールドの該当するフィールドにユーザに関する情報（氏名、電話番号、E メール アドレス、職位、および部門）を入力します。

ステップ 8　（任意）[Comments] フィールドに、このアカウントに関する任意の追加情報を入力します。

ステップ 9　[Submit] をクリックします。

[Changes Submitted] メッセージが、ウィンドウの一番下に表示されます。

ステップ 10　この新しいアカウントにロール（「ロールの操作」（P.7-10）を参照）、およびドメイン（「ドメインの操作」（P.7-14）を参照）を割り当てます。

ユーザ アカウントの変更と削除

（注）　CLI からユーザ アカウントを変更しても、Centralized Management System（CMS）データベースはアップデートされず、変更は Central Manager GUI に反映されません。

既存のユーザ アカウントを変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users] を選択します。

[User Accounts] ウィンドウが表示されます。

ステップ 2　変更するユーザ アカウントの横にある [Edit] アイコンをクリックします。

[Modifying User Account] が表示されます。次のように、ユーザ アカウントを削除または編集できます。

（注）　このウィンドウには、管理者レベルの特権を持つユーザだけがアクセスできます。

- ユーザ アカウントを削除するには、タスクバーの [Delete] アイコンをクリックし、[OK] をクリックして削除を確認します。

  ローカル ユーザ アカウントが WAAS Central Manager GUI を使用して作成された場合、対応するユーザ アカウントが CLI から削除され、すべてのスタンバイ WAAS Central Manager からも削除されます。

  （注）　CLI からユーザ アカウントを削除しても、CMS データベース内の対応するユーザ アカウントは*無効になりません*。そのため、ユーザ アカウントは、CMS データベースにアクティブ状態で残ります。WAAS Central Manager GUI で作成したユーザ アカウントは、常に WAAS Central Manager GUI から削除する必要があります。

- ユーザ アカウントを編集するには、ユーザ名とアカウント情報に必要な変更を行い、[Submit] をクリックします。

自身のアカウントのパスワードの変更

WAAS Central Manager GUI にログインしている場合は、次の要件が満たされていれば、自分のアカウント パスワードを変更できます。

- アカウントとパスワードが、CLI でなく、WAAS Central Manager GUI で作成された。
- パスワード ウィンドウにアクセスできる。

（注）　ローカル CLI ユーザ パスワードは、CLI から変更しないでください。CLI からローカル CLI ユーザ パスワードを変更しても、管理データベースはアップデートされず、スタンバイ WAAS Central Manager に伝達されません。したがって、管理データベース内のパスワードは、CLI で設定した新パスワードと一致しません。

（注）　WAAS Central Manager GUI からパスワードを初期設定することには、プライマリとスタンバイの両方の WAAS Central Manager が同期し、GUI ユーザがパスワードを変更するために CLI にアクセスする必要がないという利点があります。

自身のアカウント用のパスワードを変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [Password] を選択します。

[Changing Password for User Account] ウィンドウが表示されます。

ステップ 2　[New Password] フィールドに、変更したパスワードを入力します。パスワードは大文字と小文字の区別をし、長さは 1 ～ 31 字である必要があります。‘ “ | （一重引用符、二重引用符、パイプ）の文字、または制御文字を含めることはできません。

ステップ 3　[Confirm New Password] フィールドに、確認のためにパスワードを再入力します。

ステップ 4　[Submit] をクリックします。

パスワードが変更されたことを確認する「Changes Submitted」メッセージが、ウィンドウの一番下に表示されます。

WAAS Central Manager GUI を使用してアカウントのパスワードを変更すると、Central Manager が管理するすべての WAE デバイスのパスワードが変更されます。

別のアカウントのパスワードの変更

admin 特権を持つアカウントを使用して WAAS Central Manager GUI にログインすると、他のアカウントのパスワードを変更できます。

（注）　CLI からユーザ パスワードを変更すると、パスワードの変更はローカル デバイスだけに適用され、Central Manager GUI には反映されません。また、他のデバイスにも伝達されません。

別のアカウント用のパスワードを変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users] を選択します。

ロールに基づくユーザ アカウントのリストが表示されます。

ステップ 2　新しいパスワードが必要なアカウントの横にある [Edit] アイコンをクリックします。[Modifying User Account] が表示されます。

ステップ 3　[Password] フィールドに、変更したパスワードを入力します。パスワードは大文字と小文字の区別をし、長さは 1 ～ 31 字である必要があります。‘ “ | （一重引用符、二重引用符、パイプ）の文字、または制御文字を含めることはできません。

ステップ 4　[Confirm Password] フィールドに、確認のためにパスワードを再入力します。

ステップ 5　[Submit] をクリックします。

パスワードが変更されたことを確認する「Changes Submitted」メッセージが、ウィンドウの一番下に表示されます。

ユーザ アカウントの表示

すべてのユーザ アカウントを表示するには、WAAS Central Manager GUI から [Admin] > [AAA] > [Users] を選択します。[User Accounts] ウィンドウに、管理データベース内のすべてのユーザ アカウントが表示されます。「新しいアカウントの作成」（P.7-4）の説明に従って、このウィンドウから新しいアカウントを作成することもできます。

特定のデバイスのユーザ アカウントを表示するには、[My WAN] > [Manage Devices] を選択し、ユーザを表示するデバイスの横にある [Edit] アイコンをクリックします。次に、デバイスがアプリケーション アクセラレータであるか、Central Manager であるかによって、[Device Users] または [CM Users] をクリックします。[Users for device] ウィンドウに、そのデバイスに定義されているすべてのユーザ アカウントが表示されます。

そのデバイスでユーザ アカウントがロックされている場合は、このウィンドウからロックを解除できます。アカウントの横にあるチェックボックスを選択して、[Unlock] ボタンをクリックします。

アカウントの詳細を表示するには、そのアカウントの横にある [View] アイコンをクリックします。

ユーザ アカウントのロック解除

ユーザ アカウントがロックされると、そのユーザは、管理者がアカウントのロックを解除するまで、WAAS サービスにログインできません。ユーザが 3 回連続してログイン試行に失敗すると、ユーザ アカウントがロックされます。

アカウントのロックを解除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、[Admin] > [AAA] > [Users] を選択します。

[User Accounts listing] ウィンドウが表示され、各ユーザ アカウントのステータスが示されます。

（注）　このウィンドウには、管理者レベルの特権を持つユーザだけがアクセスできます。

ステップ 2　変更するユーザ アカウントの横にある [Edit] アイコンをクリックします。

[Modifying User Account] ウィンドウが表示され、このアカウントがロックされたデバイスのリストが示されます。

ステップ 3　アカウントのロックを解除するデバイスを選択します。

デバイス ユーザのリストが表示されます。

ステップ 4　ロック解除するユーザを選択し、[unlock] ボタンをクリックします。

パスワードの操作

WAAS システムには、*標準*と*強力*の 2 つのレベルのパスワード ポリシーがあります。デフォルトでは、標準パスワード ポリシーが有効になっています。

パスワード ポリシーを変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　パスワード ポリシーを作成するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　WAAS Central Manager GUI のナビゲーション ペインで、[Configure > [Security] > [AAA] > [Password Policy Settings] を選択します。

ステップ 4　[Enforce stringent password] チェックボックスを選択して、強力パスワード ポリシーを有効化します。

ステップ 5　[Maximum login retries] フィールドに、ユーザがロックされずに行うことができるログイン試行の最大回数を入力します。ロックされたユーザは、管理者がクリアするまでロックされたままとなります。アカウントのロックをクリアするには、「ユーザ アカウントのロック解除」（P.7-9）を参照してください。

ステップ 6　[Submit] をクリックして、変更を保存します。

CLI からパスワード ポリシーを設定するには、**authentication strict-password-policy** グローバル コンフィギュレーション コマンドを使用します。

標準のパスワード ポリシーが有効な場合、ユーザ パスワードは次の要件を満たしている必要があります。

- パスワードの長さは、1 ～ 31 文字までです。
- パスワードには、大文字と小文字（A ～ Z および a ～ z）および数字（0 ～ 9）を使用できます。
- パスワードには、‘ “ | （一重引用符、二重引用符、パイプ）の文字、または制御文字は使用できません。

強力なパスワード ポリシーが有効な場合、ユーザ パスワードは次の要件を満たしている必要があります。

- パスワードの長さは、8 ～ 31 文字までです。
- パスワードには、大文字と小文字の両方（A ～ Z および a ～ z）、数字（0 ～ 9）、および ~`!@#$%^&*()_+-=[]\{};:,</> を含む特殊文字を使用できます。
- パスワードには、‘ “ | （一重引用符、二重引用符、パイプ）の文字、または制御文字は使用できません。
- パスワードをすべて同じ文字にすることはできません（たとえば、**99999**）。
- パスワードを連続した文字にすることはできません（たとえば、**12345**）。
- パスワードをユーザ名と同じにすることはできません。
- 新しいパスワードは、それ以前の 12 個のパスワードとは異なっている必要があります。ユーザ パスワードの有効期限は 90 日間です。
- パスワードにディクショナリ用語を使用することはできません。

ユーザ アカウントは、設定されている回数だけログイン試行に失敗するとロックされます（デフォルトは 3 回）。管理者がクリアしない限り、ユーザはロックされたままです。アカウントのロックをクリアするには、「ユーザ アカウントのロック解除」（P.7-9）を参照してください。

ロールの操作

WAAS Central Manager GUI を使用すると、各管理者が特定の WAAS サービスの設定と管理に集中できるように、WAAS システム管理者のロールを作成できます。たとえば、管理者にアプリケーション ポリシーの作成と変更を許可し、他のシステム変更を許可しないロールを設定できます。

ロールとは、有効にされた 1 組のサービスと見なすことができます。ロールを作成するときにサービスを選択することになるため、ロールが担当するサービスについて明確に把握する必要があります。ロールを作成したら、この章で後述する説明に従って、既存のアカウントにロールを割り当てることができます。

ロールにより、有効化されている各サービスに読み取りと書き込み、または読み取り専用アクセス権が与えられます。

各ユーザ アカウントまたはグループには、0 を含む任意の数のロールを割り当てることができます。ロールは、継承されず、組み込まれません。WAAS Central Manager は、admin と print という 2 つの定義済みのロールを提供します。CLI ユーザが持つ特権レベル 15 と同様に、admin ロールはすべてのサービスへのアクセス権を持ちます。admin ロールがないと、ユーザはすべての管理タスクを実行できません。print ロールは、WAAS Central Manager のすべての印刷関連ページにアクセスできます。

（注）　ユーザに admin ロールを割り当てても、ユーザ特権レベルは 15 に変更されません。管理タスクを実行するには、ユーザの特権レベルも 15 にする必要があります。

ユーザに admin ロールを割り当てると、すべての Device Manager GUI ページに対する読み取り / 書き込み権限が付与されます。

WAAS は外部 TACACS+ または Windows ドメイン認証サーバで定義されているとおりに、グループのメンバシップに基づいて、ユーザにロールをダイナミックに割り当てることができます。この機能を使用するには、外部認証サーバで定義されたユーザ グループに一致する WAAS Central Manager 上のユーザ グループ名を定義し、これらのユーザ グループにロールを割り当てる必要があります。ユーザ グループの詳細については、「ユーザ グループの操作」（P.7-18）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。

新しいロールの作成

新しいロールを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] >[Roles] を選択します。

[Roles listing] ウィンドウが表示されます。

ステップ 2　タスクバーの [Create New Role] アイコンをクリックします。

[Creating New Role] ウィンドウが表示されます

ステップ 3　[Name] フィールドに、ロールの名前を入力します。

名前には、英字、数字、ピリオド、ハイフン、アンダースコア、およびスペース以外の文字は使用できません。

ステップ 4　このロールに管理させたいサービスの横にあるチェックボックスを選択します。

このウィンドウのチェックボックスには、3 つのステートがあります。ボックスにチェックがある場合、ユーザはこのサービスに対する読み取りと書き込みアクセス権があるという意味です。チェックボックスを再度クリックすると、インジケータはチェックボックスを部分的に塗りつぶした四角に変わります。このインジケータは、ユーザがこのサービスに対して読み取り専用アクセス権を持つという意味です。空の四角は、そのサービスにアクセスできないことを示します。

カテゴリの下にサービスのリストを展開するには、フォルダをクリックし、このロールのために有効にするサービスの横にあるチェックボックスを選択します。カテゴリのすべてのサービスを同時に選択するには、それらのサービスの最上位フォルダの横にあるチェックボックスを選択します。

表 7-4 に、ロールのために有効にできるサービスを示します。

表 7-4　WAAS サービスの説明

サービス	説明
[Devices]	このロールは、WAAS Central Manager GUI の [My WAN] ドロワーの設定を構成および管理できます。[My WAN] ドロワー全体を有効にしたくない場合は、このロールに管理させたいサブページを選択します。
[Monitor]	このロールは、WAAS Central Manager GUI の [Monitor] ドロワーの設定を構成および管理できます。[Monitor] ドロワー全体を有効にしたくない場合は、このロールに管理させたいサブページを選択します。
[Report]	このロールは、WAAS Central Manager GUI の [Report] ドロワーの設定を構成および管理できます。[Report] ドロワー全体を有効にしたくない場合は、このロールに管理させたいサブページを選択します。

表 7-4　WAAS サービスの説明 （続き）

サービス	説明
[Jobs]	このロールは、WAAS Central Manager GUI の [Jobs] ドロワーの設定を構成および管理できます。[Jobs] ドロワー全体を有効にしたくない場合は、このロールに管理させたいサブページを選択します。
[Configure]	このロールは、WAAS Central Manager GUI の [Configure] ドロワーの設定を構成および管理できます。[Configure] ドロワー全体を有効にしたくない場合は、このロールに管理させたいサブページを選択します。
[Admin]	このロールは、WAAS Central Manager GUI の [Admin] ドロワーの項目にアクセスできます。[Admin] ドロワー全体を有効にしたくない場合は、このロールに管理させたいサブページを選択します。
[All WAEs]	このロールは、WAAS ネットワーク内のすべての WAE にアクセスできます。このサービスを有効にしない場合、ユーザ アカウントは、アカウントに割り当てられたドメインに関連する WAE だけにアクセスできます。 このサービスを選択すると、ロールに基づくアカウントを設定するときに次の作業を省略できます。 • ネットワーク内のすべての WAE を含むドメインの作成および保守 • すべての WAE を含むドメインのアカウントへの割り当て
[All Device Groups]	このロールは、WAAS ネットワーク内のすべてのデバイス グループにアクセスできます。このサービスを有効にしない場合、ユーザ アカウントは、アカウントに割り当てられたドメインに関連するデバイス グループだけにアクセスできます。 このサービスを選択すると、ロールに基づくアカウントを設定するときに次の作業を省略できます。 • ネットワーク内のすべてのデバイス グループを含むドメインの作成および保守 • すべてのデバイス グループを含むドメインのアカウントへの割り当て
[Monitoring API]	このロールは、HTTPS 要求による API のモニタリングにアクセスできます。詳細については、『*Cisco Wide Area Application Services API Reference*』を参照してください。
[System Status]	このロールは、デバイスのアラーム ウィンドウ [My WAN] >[Alerts] にアクセスできます。 デバイス アラームの詳細については、第 16 章「WAAS ネットワークのモニタリングおよびトラブルシューティング」を参照してください。

ステップ 5　（任意）[Comments] フィールドに、このロールに関するコメントを入力します。

ステップ 6　[Submit] をクリックして、設定を保存します。

（注）　[Configure] > [File Services] > [Baseline Group]、[Configure] > [Acceleration] > [Baseline Group]、または [Configure] > [Platform] > [Baseline Group] の各ページへのアクセス権を持つロールを作成する場合、必要なすべての設定ページにアクセスできるよう、そのロールの [All Device Groups] サービスも有効にする必要があります。または、ベースライン グループに属するすべてのデバイスを含むドメインに、このロールのユーザを割り当てることもできます。

ユーザ アカウントへのロールの割り当て

作成したロールは、アカウント（ユーザ グループ）に割り当てる必要があります。アカウントを作成しても、アカウントにロールを割り当てない場合、このアカウントは、WAAS Central Manager GUI にログインできますが、データは表示されず、設定ページを使用できません。

（注）　デフォルトで、admin ユーザ アカウントには、システム内のすべてのエンティティにアクセスできるロールが割り当てられます。このユーザ アカウント用のロールは変更できません。

1 つまたは複数のロールをユーザ アカウント グループに割り当てるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users]（または [Admin] > [AAA] > [User Groups]）を選択します。

[User Accounts]（または [User Groups]）ウィンドウが表示され、設定されているすべてのユーザ アカウントが表示されます。

ステップ 2　ロールを割り当てるユーザ アカウントまたはグループの横にある [Edit] アイコンをクリックします。

[Modifying User Account]（または [Modifying User Group]）ウィンドウが表示されます。

ステップ 3　[Role Management] タブをクリックします。

[Role Management] ウィンドウが表示され、設定されているすべてのロール名が表示されます。

ステップ 4　選択したユーザ アカウントまたはグループに割り当てたいロール名の横に表示される [Assign] アイコン（青色の十字）をクリックします。

ステップ 5　すでに割り当てられているロールの割り当てを解除するロール名の横にある [Unassign]（緑色のチェック マーク）をクリックします。

（注）　タスクバーの [Assign all Roles] アイコンをクリックして、現在のウィンドウ内のすべてのロールをユーザ アカウントまたはグループに割り当てます。あるいは、[Remove all Roles] アイコンをクリックして、ユーザ アカウントまたはグループに関連付けられたすべてのロールの割り当てを解除します。

ステップ 6　[Submit] をクリックします。

割り当てられたロールの横に緑色のチェック マークが表示され、割り当てられていないロールの横に青色の十字マークが表示されます。このユーザ アカウントまたはグループに割り当てられたロールは、[Modifying User Account]（または [Modifying User Group]）ウィンドウの [Roles] セクションに表示されます。

ロールの変更と削除

（注）　デフォルトで、admin ユーザ アカウントは、すべてのサービスにアクセスでき、変更できません。

ロールを変更または削除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] >[Roles] を選択します。

[Roles] ウィンドウが表示されます。

ステップ 2　変更または削除するロールの名前の横にある [Edit] アイコンをクリックします。

[Modifying Role] ウィンドウが表示されます。次のように、ロールを変更できます。

- このロールを削除するには、タスクバーの [Delete] アイコンをクリックします。
- このロールを編集するには、フィールドで必要な変更を行い、[Submit] をクリックします。
- このロール用のサービスを有効にするには、必要なサービスの横にあるチェックボックスを選択します。すでに選択されているサービスを無効にするには、無効にするサービスの横にあるチェックボックスの選択を解除します。あるカテゴリのすべてのサービスを同時に選択するには、最上位サービスの横にあるチェックボックスを選択します。

ロールの設定の表示

特定のユーザ アカウントまたはグループにロールを割り当てる前に、ロール設定を表示したい場合があります。

ロール設定を表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users]（または [Admin] > [AAA] > [User Groups]）を選択します。

[User Accounts]（または [User Groups]）ウィンドウが表示され、設定されているすべてのユーザ アカウントまたはグループが表示されます。

ステップ 2　表示するユーザ アカウントまたはグループの横にある [Edit] アイコンをクリックします。

[Modifying User Account]（または [Modifying User Group]）ウィンドウが表示されます。

ステップ 3　[Role Management] タブをクリックします。

[Role Management] ウィンドウが表示されます。

ステップ 4　表示するロールの横にある [View] アイコンをクリックします。

[Viewing Role] ウィンドウが表示され、ロール名、このロールに関するコメント、およびこのロール用に有効になっているサービスが表示されます。

ステップ 5　設定の表示が完了したら、[Close] をクリックします。

ドメインの操作

*ドメイン*は、WAAS ネットワークを構成するデバイス グループまたは WAE の集合です。ロールは、ユーザが WAAS ネットワークで管理できるサービスを定義します。これに対し、ドメインは、ユーザがアクセスできるデバイス グループ、WAE、またはファイル サーバのダイナミック共有を定義します。

ドメインを作成するとき、ドメインに関連付けられるエンティティ タイプを選択します。エンティティ タイプには、WAE、デバイス グループ、またはなし（サーバ ダイナミック共有用）があります。ファイル サーバのダイナミック共有の場合、ダイナミック共有は、「ダイナミック共有の作成」（P.11-21）の説明に従ってダイナミック共有設定で割り当てられます。

WAAS は外部 TACACS+ または Windows ドメイン認証サーバで定義されているとおりに、グループのメンバシップに基づいて、ユーザにドメインをダイナミックに割り当てることができます。この機能を使用するには、外部認証サーバで定義されたユーザ グループに一致する WAAS Central Manager 上のユーザ グループ名を定義し、これらのユーザ グループにドメインを割り当てる必要があります。ユーザ グループの詳細については、「ユーザ グループの操作」（P.7-18）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。

新しいドメインの作成

新しいドメインを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] >[Domains] を選択します。

[Domains listing] ウィンドウが表示されます。

ステップ 2　タスクバーの [Create New Domain] アイコンをクリックします。

[Creating New Domain] ウィンドウが表示されます

ステップ 3　[Name] フィールドに、ドメインの名前を入力します。

ステップ 4　[Entity Type] ドロップダウン リストから、ドメインに割り当てたいエンティティ タイプを選択します。エンティティの選択肢は、[WAE]、[Device Groups]、および [None] です。このドメインが、ファイル サーバのダイナミック共有に使用されている場合、[None] を選択します。

ステップ 5　（任意）[Comments] フィールドに、このドメインに関するコメントを入力します。

ステップ 6　[Submit] をクリックします。

選択したエンティティ タイプがまだドメインに割り当てられていない場合、エンティティ タイプが割り当てられていないことを示すメッセージが表示されます。

ステップ 7　後続のセクション、「エンティティのドメインへの追加」の説明に従って、このドメインにエンティティを割り当てます。[Entity Type] に [None] を選択した場合は、ドメインにエンティティを割り当てないでください。「ダイナミック共有の作成」（P.11-21）に説明されているように、エンティティはダイナミック共有設定で使用されます。

エンティティのドメインへの追加

ドメインを作成したら、ドメインにエンティティを割り当てる必要があります。エンティティは、WAE の集合またはデバイス グループの集合です。ファイル サーバのダイナミック共有で使用されるドメインには、エンティティを割り当てる必要はありません。この場合のエンティティ タイプは [None] です。

ドメインにエンティティを追加するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] >[Domains] を選択します。

ステップ 2　変更するドメインの横にある [Edit] アイコンをクリックします。

ステップ 3　[Entity Management] タブをクリックします。

現在のドメインの [*Entity_name* Assignments for Domain] ウィンドウが表示されます。

リスト内の項目の表示はフィルタできます。フィルタにより、設定した基準に一致するリスト内の項目を見つけることができます。

次のように、ドメインにエンティティを追加し、ドメインからエンティティを削除できます。

- 現在のドメインにエンティティを追加するには、追加するエンティティの横にある [Assign] アイコン（青色の十字マーク）をクリックします。設定を確定すると、選択したエンティティの横に緑色のチェック マークが表示されます。

  あるいは、選択したドメインにすべてのエンティティを追加するには、タスクバーの [Assign all] アイコンをクリックします。

- 現在のドメインからエンティティを削除するには、ドメインから削除するエンティティの名前の横にある [Unassign] アイコン（緑色のチェック マーク）をクリックします。設定を確定すると、割り当てを解除したエンティティの横に青色の十字マークが表示されます。

  あるいは、ドメインからすべてのエンティティを削除するには、タスクバーの [Remove all] アイコンをクリックします。

ステップ 4　[Submit] をクリックします。

ドメインに割り当てたエンティティの横に緑色のチェック マークが表示されます。

ステップ 5　後続のセクションの説明に従って、アカウントにドメインを割り当てます。

ユーザ アカウントへのドメインの割り当て

ドメインをアカウントまたはグループに割り当てると、アカウントまたはグループが管理できるエンティティ（デバイスまたはデバイス グループ）、またはファイル サーバ ダイナミック共有を指定することになります。

（注）　アカウントまたはグループに割り当てたロールで、[ALL WAEs]、または [ALL Device Groups] のサービスが有効になっている場合は、ドメインをアカウントまたはグループに割り当てる必要がありません。アカウントまたはグループは、自動的に WAAS システム内のすべての WAE、デバイス グループ、またはその両方にアクセスできます。詳細については、表 7-4（P.7-11）を参照してください。

ユーザ アカウントまたはグループにドメインを割り当てるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users]（または [Admin] > [AAA] > [User Groups]）を選択します。

[User Accounts]（または [User Groups]）ウィンドウが表示され、設定されているすべてのユーザ アカウントまたはグループが表示されます。

ステップ 2　ドメインを割り当てるユーザ アカウントまたはグループの横にある [Edit] アイコンをクリックします。

[Modifying User Account]（または [Modifying User Group]）ウィンドウが表示されます。

ステップ 3　[Domain Management] タブをクリックします。

[Domain Management] ウィンドウが表示され、設定されたすべてのドメインおよびそのエンティティ タイプが表示されます。

ステップ 4　選択したユーザ アカウントまたはグループに割り当てたいドメイン名の横に表示される [Assign] アイコン（青色の十字マーク）をクリックします。

ユーザ アカウントまたはグループに関連付けられたドメインの割り当てを解除するには、ドメイン名の横にある Unassign（緑色のチェック マーク）をクリックします。

（注）　現在のウィンドウ内のすべてのドメインをユーザ アカウントまたはグループに割り当てるには、タスクバーの [Assign all Domains] アイコンをクリックします。あるいは、ユーザ アカウントまたはグループに関連付けられたすべてのドメインの割り当てを解除するには、[Remove all Domains] アイコンをクリックします。

ステップ 5　[Submit] をクリックします。

割り当てられたドメインの横に緑色のチェック マークが表示され、割り当てられていないドメインの横に青色の十字マークが表示されます。このユーザ アカウントまたはグループに割り当てられたドメインは、[Modifying User Account]（または [Modifying User Group]）ウィンドウの [Domains] セクションに表示されます。

ドメインの変更と削除

既存のドメインを変更または削除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] >[Domains] を選択します。

[Domains] ウィンドウが表示されます。

ステップ 2　変更するドメインの横にある [Edit] アイコンをクリックします。

[Modifying Domain] ウィンドウが表示されます。次のように、ドメインを変更できます。

- ドメインを削除するには、タスクバーの [Delete] アイコンをクリックし、[OK] をクリックして削除を確認します。
- ドメインを変更するには、フィールドで必要な変更を行い、[Submit] をクリックします。

ドメインの表示

特定のユーザ アカウントまたはグループのドメイン設定を表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users]（または [Admin] > [AAA] > [User Groups]）を選択します。

[User Accounts]（または [User Groups]）ウィンドウが表示され、設定されているすべてのユーザ アカウントまたはグループが表示されます。

ステップ 2　ドメイン設定を表示するユーザ アカウントまたはグループの横にある [Edit] アイコンをクリックします。

[Modifying User Account]（または [Modifying User Group]）ウィンドウが表示されます。

ステップ 3　[Domain Management] タブをクリックします。

[Domain Management] ウィンドウが表示されます。

ステップ 4　ドメイン名の横にある [View] アイコン（虫眼鏡）をクリックして、ドメインに関する詳細を表示します。

[Viewing Domain] ウィンドウが表示され、ドメイン名、エンティティ タイプ、このドメインに関するコメント、およびこのドメインに割り当てられたエンティティが表示されます。

ステップ 5　設定の表示が完了したら、[Close] をクリックします。

ユーザ グループの操作

TACACS+ または Windows ドメイン サーバ（RADIUS サーバではなく）でユーザの外部認証を使用している場合は、ユーザ グループを作成する必要があります。外部認証サーバで定義されたユーザ グループと一致するユーザ グループ名を作成することにより、WAAS は外部認証サーバで定義されているとおりに、グループのメンバシップに基づいて、ユーザにロールおよびドメインをダイナミックに割り当てることができます。ロールまたはドメインを各ユーザ別に定義する必要はなく、ユーザ グループにロールまたはドメインを定義すると、ユーザが属するグループに定義されたロールおよびドメインがユーザに割り当てられます。

（注）　外部ユーザ グループに基づいてロールおよびドメインをダイナミックに割り当てるには、シェルのカスタム属性をサポートする TACACS+ サーバが必要です。たとえば、これらの属性は Cisco ACS 4.x でサポートされていますが、5.0 ではサポートされていません。

WAAS は、外部認証サーバから各ユーザのグループ メンバシップ情報を読み取ります。

ここでは、次の内容について説明します。

- 「新しいユーザ グループの作成」（P.7-18）
- 「ユーザ グループへのロールの割り当て」（P.7-19）
- 「ユーザ グループへのドメインの割り当て」（P.7-19）
- 「ユーザ グループの変更と削除」（P.7-20）
- 「ユーザ グループの表示」（P.7-21）

新しいユーザ グループの作成

新しいユーザ グループを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [User Groups] を選択します。

[User Groups] リスト ウィンドウが表示されます

ステップ 2　タスクバーの [Create New User Groups] アイコンをクリックします。

[Creating New User Group] ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、ユーザ グループの名前を入力します。

この名前が、使用している外部認証サーバで定義されたユーザ グループの名前に一致していることを確認します。名前の一致は、大文字と小文字を区別します。

（注）　ユーザ グループ名に # + " < > , （カンマ）を含めることはできません。ユーザ グループ名を数字、ピリオド（.）、またはスペースだけで構成することはできません。ピリオド、アスタリスク（*）、またはスペースが先頭にある場合は削除されます。

ステップ 4　（任意）[Comments] フィールドに、このユーザに関するコメントを入力します。

ステップ 5　[Submit] をクリックします。

ステップ 6　次のセクションの説明に従って、このユーザ グループにロールまたはドメインを割り当てます。

ユーザ グループへのロールの割り当て

作成されたユーザ グループには、ロールを割り当てる必要があります。ユーザ グループを作成しても、グループにロールを割り当てない場合、このグループは、WAAS Central Manager GUI にログインできますが、データは表示されず、設定ページを使用できません。

1 つまたは複数のロールをユーザ グループに割り当てるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] >[User Groups] を選択します。

[User Groups] ウィンドウが表示され、設定されているすべてのユーザ グループが表示されます。

ステップ 2　ロールを割り当てたいユーザ グループの横にある [Edit] アイコンをクリックします。

[Modifying User Group] ウィンドウが表示されます。

ステップ 3　[Role Management] タブをクリックします。

[Role Management for User Group] ウィンドウが表示され、設定されているすべてのロール名が表示されます。

ステップ 4　選択したユーザ グループに割り当てるロール名の横に表示される [Assign] アイコン（青色の十字マーク）をクリックします。

ステップ 5　すでに割り当てられているユーザ グループのロールの割り当てを解除するロール名の横にある [Unassign]（緑色のチェック マーク）をクリックします。

（注）　タスクバーの [Assign all Roles] アイコンをクリックして、現在のウィンドウ内のすべてのロールをユーザ グループに割り当てます。あるいは、[Remove all Roles] アイコンをクリックして、ユーザ グループに関連付けられたすべてのロールの割り当てを解除します。

ステップ 6　[Submit] をクリックします。

割り当てられたロールの横に緑色のチェック マークが表示され、割り当てられていないロールの横に青色の十字マークが表示されます。このユーザ グループに割り当てられたロールは、[Modifying User Group] ウィンドウの [Roles] セクションに表示されます。

ユーザ グループへのドメインの割り当て

ユーザ グループにドメインを割り当てると、ユーザ グループのメンバーであるユーザが管理できるエンティティ（デバイスまたはデバイス グループ）を指定することになります。

（注）　ユーザ グループに割り当てたロールで [All WAE]、または [All Device Groups] のサービスが有効になっている場合は、ドメインをユーザ グループに割り当てる必要がありません。このグループのユーザは、自動的に WAAS システム内のすべての WAE、デバイス グループ、またはその両方にアクセスできます。詳細については、表 7-4（P.7-11）を参照してください。

ユーザ グループにドメインを割り当てるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [User Groups] を選択します。

[User Groups] ウィンドウが表示され、設定されているすべてのユーザ グループが表示されます。

ステップ 2　ドメインを割り当てるユーザ グループの横にある [Edit] アイコンをクリックします。

[Modifying User Group] ウィンドウが表示されます。

ステップ 3　[Domain Management] タブを選択します。

[Domain Management for User Group] ウィンドウが表示され、設定されたすべてのドメインおよびそのエンティティ タイプが表示されます。

ステップ 4　選択したユーザ グループに割り当てるドメイン名の横に表示される [Assign] アイコン（青色の十字マーク）をクリックします。

ユーザ グループに関連付けられたドメインの割り当てを解除するには、ドメイン名の横にある Unassign（緑色のチェック マーク）をクリックします。

（注）　現在のウィンドウ内のすべてのドメインをユーザ グループに割り当てるには、タスクバーの [Assign all Domains] アイコンをクリックします。あるいは、ユーザ グループに関連付けられたすべてのドメインの割り当てを解除するには、[Remove all Domains] アイコンをクリックします。

ステップ 5　[Submit] をクリックします。

割り当てられたドメインの横に緑色のチェック マークが表示され、割り当てられていないドメインの横に青色の十字マークが表示されます。ユーザ グループに割り当てられたドメインは、[Modifying User Group] ウィンドウの [Domains] セクションに表示されます。

ユーザ グループの変更と削除

既存のユーザ グループを変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] >[User Groups] を選択します。

[User Groups] ウィンドウが表示されます。

ステップ 2　変更するユーザ グループの横にある [Edit] アイコンをクリックします。

[Modifying User Group] ウィンドウが表示されます。次のように、ユーザ グループを削除または編集できます。

（注）　このウィンドウには、管理者レベルの特権を持つユーザだけがアクセスできます。

- ユーザ グループを削除するには、タスクバーの [Delete] アイコンをクリックし、[OK] をクリックして削除を確認します。
- ユーザ グループを編集するには、名前とコメント情報に必要な変更を行い、[Submit] をクリックします。

- ユーザ グループに割り当てられた [Roles] を変更するには、[Role Management] タブをクリックして、ロールに必要な変更を行い、[Submit] をクリックします。
- ユーザ グループに割り当てられた [Domains] を変更するには、[Domain Management] タブをクリックして、ロールに必要な変更を行い、[Submit] をクリックします。

ユーザ グループの表示

すべてのユーザ グループを表示するには、WAAS Central Manager GUI から [Admin] > [AAA] > [User Groups] を選択します。[User Groups] ウィンドウに、管理データベース内のすべてのユーザ アカウントが表示されます。「新しいユーザ グループの作成」（P.7-18）の説明に従って、このウィンドウからグループを作成することもできます。

CHAPTER 8

WAAS デバイス用の IP ACL の作成および管理

この章では、Wide Area Application Service（WAAS）の Central Manager GUI を使用して、WAAS デバイス用の IP Access Control List（ACL; アクセス コントロール リスト）を集中的に作成し、管理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。

（注） IP ACL 設定の表示、編集、または作成を行うには、admin 特権を持つアカウントを使用して WAAS Central Manager GUI にログインする必要があります。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

WAAS デバイス用の IP ACL について

集中管理される WAAS ネットワーク環境では、管理者がさまざまなデバイスやサービスへの不正アクセスを防止できる必要があります。IP ACL は、WAAS デバイス宛ての IP パケットを許可または拒否できるようにして、パケットを選別できます。

WAAS ソフトウェアは、WAAS デバイスへのアクセスを制限できる標準および拡張 ACL をサポートしています。WAAS ソフトウェアは、次の種類の ACL を使用できます。

- インターフェイス ACL：組み込みのポート チャネル、およびスタンバイ インターフェイス、およびCisco WAE Inline Network Adapter InlineGroup インターフェイスに対して適用されます。この種類の ACL は、管理トラフィック（Telnet、SSH、および Central Manager GUI）の制御を目的としています。インターフェイス ACL を適用するには、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用します。

- 代行受信 ACL：すべてのインターフェイスに適用されます。このタイプの ACL は、どのトラフィックが代行受信されるかを定義します。この ACL で許可されるトラフィックは代行受信され、この ACL で拒否されるトラフィックは WAE を通過します。代行受信 ACL を適用するには、**interception access-list** グローバル コンフィギュレーション コマンドを使用します。代行受信 ACL の使用方法の詳細については、「代行受信アクセス コントロール リストの設定」（P.4-29）を参照してください。
- Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）ACL：着信 WCCP リダイレクト トラフィックに適用され、外部サーバと外部クライアント間のアクセスを制御します。WAE は、ファイアウォールと同様に機能します。WCCP ACL を適用するには、**wccp access-list** グローバル コンフィギュレーション コマンドを使用します。
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）ACL：SNMP エージェントに適用され、SNMP MIB または SNMP 統計情報をポーリングする外部 SNMP サーバによって SNMP エージェントへのアクセスを制御します。SNMP ACL を適用するには、**snmp-server access-list** グローバル コンフィギュレーション コマンドを使用します。
- トランザクション ログ フロー ACL：トランザクション ログ機能に適用され、トランザクションのログへの記録を制限します。トランザクション ログ ACL を適用するには、**transaction-logs flow access-list** グローバル コンフィギュレーション コマンドを使用します。

次の例は、WAAS デバイスが存在する環境で、インターフェイス ACL を使用する方法を示しています。

- WAAS デバイスは、顧客の施設に常駐し、サービス プロバイダーによって管理され、サービス プロバイダーはその管理のためだけにデバイスの安全性を確保する必要があります。
- WAAS デバイスは、企業内の任意の場所に配置されます。ルータおよびスイッチと同様に、管理者は、Telnet、SSH、および WAAS Central Manager GUI から IT ソース サブネットへのアクセスを制限する必要があります。

ACL を使用するには、最初に ACL を設定し、次に WAAS デバイス上の特定のサービスやインターフェイスに ACL を適用する必要があります。次に、さまざまな企業展開にインターフェイス ACL を使用する方法の例を示します。

- 外部インターフェイスを要塞化したアプリケーション層プロキシ ファイアウォールには、公開されるポートがありません。「要塞化」とは、主にセキュリティの理由から、インターフェイスがアクセスに使用できるポートを慎重に制限することです。インターフェイスは外部に存在するため、さまざまな攻撃の可能性があります。WAAS デバイスの外部アドレスはインターネットからグローバルにアクセスでき、内部アドレスはプライベートです。内部インターフェイスには、Telnet、SSH、および GUI アクセスを制限する ACL があります。
- WCCP を使用している WAE は、インターネット ルータから独立したサブネットに配置されます。WAE とルータの両方に IP ACL が必要です。ルータ上の IP アクセス リストは、最高の優先順位を持ち、WAE に定義された IP ACL より優先します。

（注）　WAAS CLI の代わりに WAAS Central Manager GUI を使用して、ACL を集中的に設定し、WAAS デバイスに適用することを強く推奨します。詳細については、「WAAS デバイス用の IP ACL の作成と管理」（P.8-2）を参照してください。

WAAS デバイス用の IP ACL の作成と管理

この項では、WAAS Central Manager GUI を使用して、WAAS デバイス用の IP ACL を作成し、管理するためのガイドラインと例を提供します。

IP ACL を作成するときは、次の重要事項に注意する必要があります。

- IP ACL 名はデバイス内で一意でなければなりません。

- IP ACL 名は 30 文字以内に制限され、余白や特殊文字を使用できません。
- 1 台の WAAS Central Manager デバイスで、最大 50 個の IP ACL とデバイス当たり合計 500 個の条件を管理できます。
- IP ACL 名が数値の場合、1 ～ 99 は標準の IP ACL を表し、100 ～ 199 は拡張 IP ACL を表します。数字で始まる IP ACL 名には、数字以外の文字を使用できません。
- WAAS Central Manager GUI を使用すると、標準の IP ACL を SNMP と WCCP に関連付けることができます。ACL に関連付けられたこのようなアプリケーションにアクセスしようとするデバイスは、アクセスを許可されるために信頼されるデバイスのリストに含まれる必要があります。
- すでに設定されている任意の標準 IP ACL を SNMP と WCCP に関連付けることができます。ただし、拡張 IP ACL は、WCCP アプリケーションだけに関連付けることができます。
- すべての条件とネットワーク インターフェイスやアプリケーションとの関連付けを含む IP ACL を削除できます。あるいは、IP ACL 条件だけ削除できます。すべての条件を削除すると、必要に応じ、IP ACL の種類を変更できます。IP ACL 項目はその後も IP ACL リストに現れますが、実質的には存在しません。
- WAAS によって使用される任意の種類の ACL に対して空の ACL を指定すると、すべてのトラフィックが許可されます。

WAAS Central Manager GUI を使用して、1 台の WAE 用の IP ACL を作成し、変更する方法と、IP ACL をアプリケーションに関連付け、WAE 上のインターフェイスに適用するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　IP ACL を作成するデバイス（たとえば、bd-s14 という名前のデータセンターの WAE）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [TCP/IP Settings] > [IP ACL] を選択します。

[IP ACL] ウィンドウが表示されます。デフォルトでは、WAE 用の IP ACL は、定義されていません。[IP ACL] ウィンドウで、現在、WAE 用の IP ACL が設定されていないかどうかを確認します。

ステップ 4　タスクバーで、[Create a new IP ACL] アイコンをクリックします。

[Creating New IP ACL] ウィンドウが表示されます。次のようにフィールドに入力します。

- [Name] フィールドで、IP ACL の命名規則に従って名前（たとえば、test1）を入力します。

  デフォルトで、この新しい IP ACL は、標準 ACL として作成されます。

  （注）　IP ACL 名は、デバイス内で一意であり、30 文字以内でなければならず、余白や特殊文字を使用できません。

- このデフォルト設定を変更して、この新しい ACL を拡張 ACL として作成する場合は、[ACL Type] ドロップダウン リストから [Extended] を選択します。

ステップ 5　[Submit] をクリックして、test1 という名前の IP ACL を保存します。条件が定義されていない IP ACL は、個々のデバイスに表示されません。

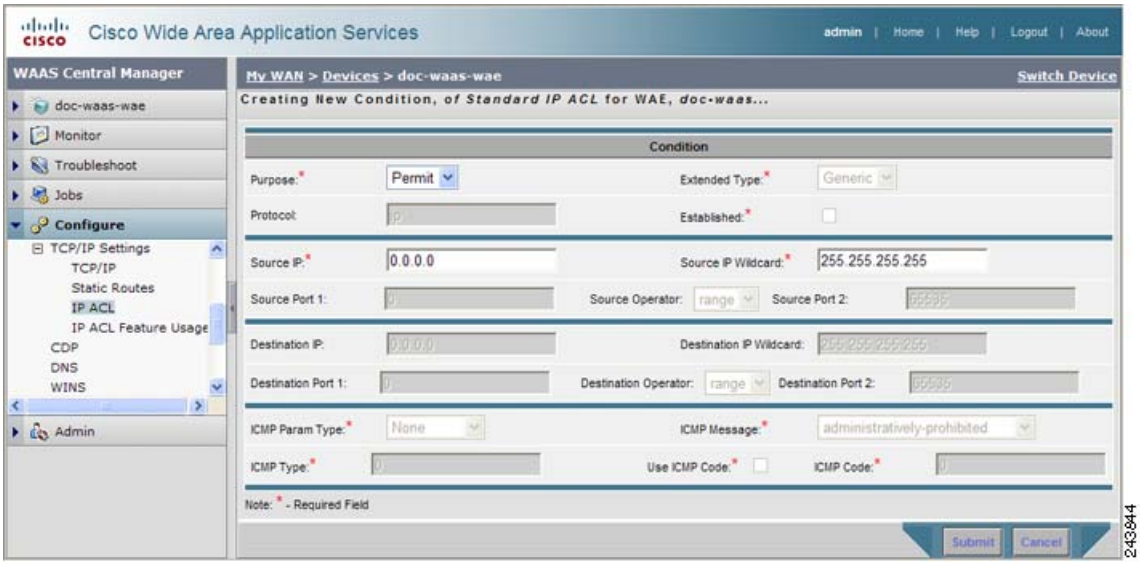
ステップ 6　作成した test1 という名前の標準 IP ACL に条件を追加します。

a.　タスクバーで、[Create New Condition] アイコンをクリックします。

[Creating New Condition] ウィンドウが表示されます（図 8-1 を参照）。

（注）　IP ACL の条件を作成するために使用できるフィールドの数は、作成した IP ACL の種類（標準または拡張）によって異なります。

図 8-1　[Extended IP ACL] ウィンドウでの新しい状態の作成



b. 次のように、作成している IP ACL の種類に有効になっているプロパティの値を入力します。

- 標準 IP ACL 用の条件を設定するには、ステップ 7 へ進みます。
- 拡張 IP ACL 用の条件を設定するには、ステップ 8 へ進みます。

ステップ 7　標準 IP ACL 用の条件を設定します。

a. ドロップダウン リストから、目的（[Permit] または [Deny]）を選択します。

b. [Source IP] フィールドで、送信元の IP アドレスを入力します。

c. [Source IP Wildcard] フィールドで、送信元の IP アドレスのワイルドカードを入力します。

d. [Submit] をクリックして、条件を保存します。

[Modifying IP ACL] ウィンドウが再表示され、条件と設定されたパラメータが表形式で表示されます。

e. IP ACL に別の条件を追加するには、上記の手順を繰り返します。

f. [Modifying IP ACL] ウィンドウから条件のリストの順序を変更するには、[Move] 列の上向き矢印または下向き矢印を使用するか、列見出しをクリックして、任意の設定済みパラメータで並べ替えます。

（注）　WAAS Central Manager GUI に表示される条件の順序は、IP ACL がデバイスに適用される順序になります。

g. IP ACL への条件の追加が完了し、すべての項目と条件の表示順序に満足したら、[Modifying IP ACL] ウィンドウの [Submit] をクリックして、デバイス データベースに IP ACL を確定します。

[Modifying IP ACL] ウィンドウの右下部に緑色の「Change submitted」インジケータが表示され、IP ACL がデバイス データベースに送信中であることを示します。表 8-1 で、標準 IP ACL のフィールドについて説明します。

表 8-1　標準 IP ACL の条件

フィールド	デフォルト値	説明
[Purpose]*[1]	[Permit]	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
[Source IP]*	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
[Source IP Wildcard]*	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。

1. * = 必須フィールド

ステップ 8　拡張 IP ACL 用の条件を設定します。

a. ドロップダウン リストから、目的（[Permit] または [Deny]）を選択します。

b. [Extended Type] ドロップダウン リストから、[Generic]、[TCP]、[UDP]、または [ICMP] を選択します（表 8-2 を参照）。

表 8-2　拡張 IP ACL の条件

フィールド	デフォルト値	説明
[Purpose]*[1]	[Permit]	パケットを許可するか拒否するかを指定します。[Permit] または [Deny] を選択します。
[Extended Type]*	[Generic]	条件に適用するインターネット プロトコルを指定します。 選択すると、[GUI] ウィンドウがリフレッシュされ、該当するフィールド オプションが有効になります。オプションは、[generic]、[TCP]、[UDP]、または [ICMP] です。

1. * = 必須フィールド

拡張 IP ACL の種類を選択すると、選択した種類によって GUI でさまざまなオプションが使用できるようになります。

c. 選択した種類に有効になったフィールドで、データを入力します（詳細については、表 8-4 ～ 表 8-7 を参照してください）。

d. [Submit] をクリックして、条件を保存します。

[Modifying IP ACL] ウィンドウが再表示され、条件と設定されたパラメータが表形式で表示されます。

e. IP ACL に別の条件を追加するには、上記の手順を繰り返します。

f. [Modifying IP ACL] ウィンドウから条件のリストの順序を変更するには、[Move] 列の上向き矢印または下向き矢印を使用するか、列見出しをクリックして、任意の設定済みパラメータで並べ替えます。

（注） WAAS Central Manager GUI に表示される条件の順序は、IP ACL がデバイスに適用される順序になります。

g. IP ACL への条件の追加が完了し、すべての項目と条件の表示順序に満足したら、[Modifying IP ACL] ウィンドウの [Submit] をクリックして、デバイス データベースに IP ACL を確定します。

[Modifying IP ACL] ウィンドウの右下部に緑色の「Change submitted」インジケータが表示され、IP ACL がデバイス データベースに送信中であることを示します。

ステップ 9　IP ACL から個々の状態を変更または削除します。

a. 変更する IP ACL の名前の横にある [Edit] アイコンをクリックします。[Modifying IP ACL] ウィンドウが表示され、現在、IP ACL に適用されているすべての条件が表示されます。

b. 変更または削除する条件の横にある [Edit Condition] アイコンをクリックします。[Modifying Condition] ウィンドウが表示されます。

c. 条件を変更するには、必要に応じて使用できるフィールドを変更します。

d. 条件を削除するには、タスクバーの [Trash]（[Delete IP ACL Condition]）アイコンをクリックします。

e. 条件のリストの順序を変更するには、[Move] 列の上向き矢印または下向き矢印を使用し、[Submit] をクリックします。

ステップ 10　標準 IP ACL を SNMP または WCCP に関連付けます。

a. 標準 IP ACL を SNMP または WCCP に関連付けるデバイスの名前の横にある [Edit] アイコンをクリックします。

b. ナビゲーション ペインで、[Configure] > [Network] > [TCP/IP Settings] > [IP ACL Feature Usage] を選択します。[IP ACL Feature Settings] ウィンドウが表示されます。

c. ドロップダウン リストから、SNMP または WCCP 用の IP ACL の名前を選択します（詳細については、表 8-3 を参照してください）。IP ACL をアプリケーションに関連付けない場合は、[Do Not Set] を選択します。

表 8-3　IP ACL Feature Settings（IP ACL 機能設定）

WAAS Central Manager GUI パラメータ	機能
[SNMP]	標準 IP ACL を SNMP に関連付けます。このオプションは、WAE または WAAS Central Manager デバイスとして動作している WAAS デバイス用にサポートされています。
[WCCP]	任意の IP ACL を WCCP バージョン 2 に関連付けます。このオプションは、WAE として動作している WAAS デバイスだけでサポートされています。WAAS Central Manager デバイスとして動作している WAAS デバイスではサポートされていません。WCCP は、WAE だけでサポートされています。WAAS Central Manager デバイスではサポートされていません。

d. [Submit] をクリックして、設定を保存します。

ステップ 11　IP ACL をインターフェイスに適用します。

a. IP ACL を WAE 上のインターフェイスに適用するデバイスの名前の横にある [Edit] アイコンをクリックします。

b. ナビゲーション ペインで、[Configure] > [Network] > [Network Interfaces] を選択します。

デバイス用の [Network Interfaces] ウィンドウが表示されます。このウィンドウは、そのデバイスで使用できるすべてのインターフェイスを表示します。

（注）　[Port Type] 列には、EtherChannel 設定を示すポートチャネル インターフェイスが含まれる場合があります。WAAS ソフトウェア用の EtherChannel では、最大 4 個の同じ速度のネットワーク インターフェイスを 1 つの仮想インターフェイスにグループ化することができます。

c. IP ACL を適用するインターフェイスの名前の横にある [Edit] アイコンをクリックします。[Modifying Network Interface] ウィンドウが表示されます。

d. ウィンドウの下部へスクロールします。[Inbound ACL] ドロップダウン リストから、IP ACL の名前を選択します。

e. [Outbound ACL] ドロップダウン リストから、ACL の名前を選択します。

WAAS Central Manager GUI から変更できるネットワーク インターフェイス プロパティはインバウンド IP ACL とアウトバウンド IP ACL だけです。他のすべてのプロパティの値はデバイス データベースから入力され、WAAS Central Manager GUI では読み取り専用です。

ステップ 12　[Submit] をクリックして、設定を保存します。

ステップ 13　代行受信されるトラフィックの定義に IP ACL を使用する方法については、「代行受信アクセス コントロール リストの設定」（P.4-29）を参照してください。

ステップ 14　（任意）IP ACL を削除します。

a. 削除する IP ACL を持つデバイスの名前の横にある [Edit] アイコンをクリックします。

b. ナビゲーション ペインで、[Configure] > [Network] > [TCP/IP Settings] > [IP ACL] を選択します。

c. 削除する IP ACL の名前（たとえば、test1）の横にある [Edit] アイコンをクリックします。

[Modifying IP ACL] ウィンドウが表示されます。IP ACL 用の条件を作成した場合は、2 つの削除オプションがあります。

- [Delete ACL]：すべての条件とネットワーク インターフェイスやアプリケーションとの関連付けを含む IP ACL を削除します。
- [Delete All Conditions]：すべての条件を削除しますが、IP ACL 名は保持されます。

d. IP ACL 全体を削除するには、タスクバーの大型 [Trash]（[Delete ACL]）アイコンをクリックします。処理を確認するプロンプトが表示されます。[OK] をクリックします。記録が削除されます。

e. 条件だけを削除するには、タスクバーの小型 [Delete All Conditions Trash/List] アイコンをクリックします。処理を確認するプロンプトが表示されたら、[OK] をクリックします。ウィンドウがリフレッシュされ、条件が削除され、[ACL Type] フィールドが使用できるようになります。

CLI から IP ACL を定義するには、**ip access-list** グローバル コンフィギュレーション コマンドを使用でき、WAAS デバイス上のインターフェイスに IP ACL を適用するには、**ipaccess-group** インターフェイス コンフィギュレーション コマンドを使用できます。SNMP 用の IP ACL の使用を設定するには、**snmp-server access-list** グローバル コンフィギュレーション コマンドを使用できます。WAE が受信する着信 WCCP リダイレクト トラフィックに適用する IP ACL を指定するには、**wccp access-list** グローバル コンフィギュレーション コマンドを使用できます。代行受信 ACL を設定するには、**interception access-list** グローバル コンフィギュレーション コマンドを使用します。

拡張 IP ACL 条件のリスト

拡張 IP ACL 用の条件を定義するときは、（「WAAS デバイス用の IP ACL の作成と管理」（P.8-2）のステップ 8 の説明に従って）条件に適用するインターネット プロトコルを指定できます。

拡張 IP ACL 条件のリストは、次のとおりです。

- Generic（表 8-4 を参照）
- TCP（表 8-5 を参照）
- UDP（表 8-6 を参照）
- ICMP（表 8-7 を参照）

表 8-4　拡張 IP ACL の Generic 条件

フィールド	デフォルト値	説明
[Purpose]*[1]	[Permit]	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
[Extended Type]*	[Generic]	任意のインターネット プロトコルと一致します。
[Protocol]	[ip]	インターネット プロトコル（[gre]、[icmp]、[ip]、[tcp]、または [udp]）。任意のインターネット プロトコルと一致するには、キーワード **ip** を使用します。
[Source IP]*	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
[Source IP Wildcard]*	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
[Destination IP]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
[Destination IP Wildcard]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。

1. * = 必須フィールド

表 8-5　拡張 IP ACL の TCP 条件

フィールド	デフォルト値	説明
[Purpose]*[1]	[Permit]	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
[Extended Type]*	[TCP]	TCP インターネット プロトコルと一致します。
[Established]	未選択（false）	選択すると、TCP データグラムに Acknowledgment（ACK; 確認応答）または RST ビットが設定され、確立した接続を示す場合、ACL 条件との照合が行われます。接続を形成するために使用される初期の TCP データグラムは照合されません。

表 8-5　拡張 IP ACL の TCP 条件 （続き）

フィールド	デフォルト値	説明
[Source IP]*	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
[Source IP Wildcard]*	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
[Source Port 1]	0	TCP ポートの 10 進番号または名前。有効なポート番号は、0 ～ 65535 です。有効な TCP ポート名は、ftp、ftp-data、https、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、rtsp、ssh、telnet、および www です。
[Source Operator]	[range]	送信元ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
[Source Port 2]	65535	TCP ポートの 10 進番号または名前。[Source Port1] を参照してください。
[Destination IP]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
[Destination IP Wildcard]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
[Destination Port 1]	0	TCP ポートの 10 進番号または名前。有効なポート番号は、0 ～ 65535 です。有効な TCP ポート名は、ftp、ftp-data、https、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、rtsp、ssh、telnet、および www です。
[Destination Operator]	[range]	送信先ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
[Destination Port 2]	65535	TCP ポートの 10 進番号または名前。[Destination Port 1] を参照してください。

1. * = 必須フィールド

表 8-6　拡張 IP ACL の UDP 条件

フィールド	デフォルト値	説明
[Purpose]*[1]	[Permit]	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
[Extended Type]*	[UDP]	UDP インターネット プロトコルと一致します。
[Established]	—	UDP には使用できません。
[Source IP]*	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号

表 8-6　拡張 IP ACL の UDP 条件 （続き）

フィールド	デフォルト値	説明
[Source IP Wildcard]*	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
[Source Port 1]	0	UDP ポートの 10 進番号または名前。有効なポート番号は、0 ～ 65535 です。有効な UDP ポート名は、bootpc、bootps、domain、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、ntp、snmp、snmptrap、tacacs、tftp、および wccp です。
[Source Operator]	[range]	送信元ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
[Source Port 2]	65535	UDP ポートの 10 進番号または名前。[Source Port1] を参照してください。
[Destination IP]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
[Destination IP Wildcard]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
[Destination Port 1]	0	UDP ポートの 10 進番号または名前。有効なポート番号は、0 ～ 65535 です。有効な UDP ポート名は、bootpc、bootps、domain、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、ntp、snmp、snmptrap、tacacs、tftp、および wccp です。
[Destination Operator]	[range]	送信先ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
[Destination Port 2]	65535	UDP ポートの 10 進番号または名前。[Destination Port 1] を参照してください。

1. * = 必須フィールド

表 8-7　拡張 IP ACL の ICMP 条件

フィールド	デフォルト値	説明
[Purpose]*[1]	[Permit]	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
[Extended Type]*	[ICMP]	ICMP インターネット プロトコルと一致します。
[Source IP]*	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号

表 8-7　拡張 IP ACL の ICMP 条件 （続き）

フィールド	デフォルト値	説明
[Source IP Wildcard]*	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
[Destination IP]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
[Destination IP Wildcard]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
[ICMP Param Type]*	[None]	[None]、[Type/Code]、または [Msg] の中から選択します。 [None] : [ICMP Type]、[Code]、および [Message] フィールドを無効にします。 [Type/Code] : ICMP メッセージの種類とコードで ICMP メッセージを選別できます。また、ICMP メッセージ コード番号を設定する機能を有効にできます。 [Msg] : キーワードを使用して、種類とコードの組み合せを指定できます。[ICMP message] ドロップダウン リストをアクティブにします。[ICMP Type] フィールドを無効にします。
[ICMP Message]*	[administratively-prohibited]	ドロップダウン リストから選択したキーワードを使用して、ICMP の種類とコードの組み合せを指定できます。
[ICMP Type]*	0	0 ～ 255 の数字。このフィールドは、[Type/Code] を選択すると有効になります。
[Use ICMP Code]*	未選択	選択すると、[ICMP Code] フィールドが有効になります。
[ICMP Code]*	0	0 ～ 255 の数字。特定の種類の ICMP メッセージを ICMP メッセージ コードでさらに選別できるメッセージ コード オプション

1. * = 必須フィールド

CHAPTER 9

その他のシステム設定の構成

この章では、Wide Area Application Service（WAAS）デバイスの基本設定を実行したあと、システム クロックの設定、デフォルトのシステム設定の変更、アラーム過負荷検出の有効化などのその他のシステム タスクを実行する方法について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

デバイス プロパティの変更

WAAS Central Manager GUI を使用すると、次のように WAE デバイスのプロパティを変更できます。

- デバイス名を変更する
- デバイスに新しい位置を割り当てる
- デバイスに管理トラフィックで使用される IP アドレスを割り当てる
- デバイスをアクティブまたは非アクティブにする

また、WAAS Central Manager GUI を使用して、デバイスのステータスがオンライン、保留状態、または非アクティブのいずれであるかを決定できます。

GUI では WAAS Central Manager デバイスの名前の変更しか実行できません。

デバイスのプロパティを変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　変更するデバイスの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[*Device Name*] > [Activation] を選択します。

選択したデバイスのプロパティを編集するためのフィールドがある [Device Activation] ウィンドウが表示されます。

WAAS Central Manager デバイスの場合、このウィンドウで変更できるフィールドは、デバイスの名前と NetBIOS 名だけです。さらに、デバイスの IP アドレスと役割が表示されます。

ステップ 4　[General Configuration] 見出しの下で、次のデバイス プロパティを設定または変更します。

- デバイスのホスト名を変更するには、[Name] フィールドに新しい名前を入力します。この名前は、次の規則に従う必要があります。
  - 名前には英数字とハイフン（-）だけを使用する。
  - 最初と最後の文字は、英数字である。
  - 長さは 30 文字以内。
  - 大文字と小文字を区別しない。
  - 次の文字は違反と見なされ、デバイス名に使用できない。
    @、#、$、%、^、&、*、()、|、\”” /<>
- デバイスをアクティブまたは非アクティブにするには、[Activate] チェックボックスを選択または選択解除します。このボックスを選択すると、デバイスは WAAS Central Manager GUI による集中管理用にアクティブになります。

  また、タスクバーの [Deactivate] アイコンをクリックして、デバイスを非アクティブにすることもできます。デバイスを非アクティブにすると、ハードウェアの障害時に、そのすべての設定を失うことなく、デバイスを交換できます。
- デバイスの NetBIOS 名を変更するには、提供されるフィールドにデバイスの新しい NetBIOS 名を入力します。

（注）　WAE が非トランスペアレント モードで動作していて、プリント サービスが有効である場合、[Name] フィールドに入力するデバイスの NetBIOS 名およびホスト名には同一の名前を設定する必要があります。

ステップ 5　[Locality] 見出しの下で、[Location] ドロップダウン リストから新しい位置を選択して、位置を設定または変更します。このデバイス用の新しい位置を作成するには、「位置の作成」（P.3-14）を参照してください。

ステップ 6　[NAT Configuration] 見出しの下で、次のフィールドを使用して NAT 設定を構成します。

- [Use WAE’s primary IP Address] チェックボックスを選択して、WAAS Central Manager がデバイスのプライマリ インターフェイスに設定されている IP アドレスを使用して、NAT ファイアウォールの背後にある WAAS ネットワークでデバイスと通信できるようにします。
- WAAS Central Manager が明示的に設定された IP アドレスを使用して、NAT ファイアウォールの背後にある WAAS ネットワークでデバイスと通信できるようにするには、[Management IP] フィールドにデバイスの IP アドレスを入力します。WAE のプライマリ インターフェイスがインライン グループ インターフェイスに設定されていて、管理トラフィックが個別の IP アドレス（同

じインライン グループ インターフェイスのセカンダリ IP アドレスまたは組み込みインターフェイスのセカンダリ IP アドレス）に設定されているシナリオでも、このアドレスを入力する必要があります。

- [Port] フィールドで、管理 IP アドレス用のポート番号を入力します。

（注）　WAAS Central Manager は、プライマリ IP アドレスを使用してデバイスにアクセスできない場合、管理 IP アドレスを使用して通信を試みます。

ステップ 7　[Comments] フィールドに、このデバイスに表示するコメントを入力します。

ステップ 8　[Submit] をクリックします。

ソフトウェア ライセンスの管理

WAAS ソフトウェア バージョン 4.1.1 では、特定の WAAS 最適化機能およびアクセラレーション機能を有効にするソフトウェア ライセンスが導入されました。ソフトウェア ライセンスは、有効にする機能が動作する前に、インストールおよび設定される必要があります。

表 9-1 に、購入できるソフトウェア ライセンスおよび各ライセンスにより有効にされる機能を示します。

表 9-1　WAAS ソフトウェア ライセンス

ライセンス	説明
Transport	基本的な DRE、TFO、および LZ の最適化を有効にします。Enterprise ライセンスが設定されている場合は、設定できません。
Enterprise	EPM、HTTP、MAPI、NFS、SSL、CIFS（WAFS）、Window Print のアプリケーション アクセラレータ、WAAS Central Manager、および基本的な DRE、TFO、LZ 最適化を有効にします。Transport ライセンスが設定されている場合は、設定できません。
Video	ビデオ アプリケーション アクセラレータを有効にします。最初に Enterprise ライセンスを設定する必要があります。
Virtual-Blade	仮想化機能を有効にします。最初に Enterprise ライセンスを設定する必要があります。

ライセンスは、デバイス グループではなく個々の WAE デバイス上でインストールおよび管理されます。すべてのライセンスがすべてのデバイスでサポートされるわけではありません。

WAAS Central Manager から WAE にライセンスを追加するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　変更する WAE デバイスの横にある [Edit] アイコンをクリックします（Central Manager 上のライセンスを管理するには CLI を使用する必要があるため、Central Manager デバイスを選択しないでください）。

ステップ 3　ナビゲーション ペインで、[Admin] > [License Management] を選択します。

ステップ 4　追加する各ライセンスの横にあるチェックボックスを選択します。

ステップ 5　[Submit] をクリックします。

CLI からライセンスを追加するには、**license add** EXEC コマンドを使用します。

CLI からライセンスを削除するには、**clear license** EXEC コマンドを使用します。

CLI からすべてのライセンスのステータスを表示するには、**show license** EXEC コマンドを使用します。

新しい WAAS デバイスを最初に設定する場合、セットアップ ユーティリティでもライセンスを設定します。

Inetd RCP および FTP サービスの有効化

Remote Copy Protocol（RCP; リモート コピー プロトコル）を使用すると、リモート ホストとスイッチの間で設定ファイルをダウンロード、アップロード、およびコピーできます。コネクションレス型プロトコルの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用する TFTP とは異なり、RCP はコネクション型の TCP を使用します。Inetd（インターネット デーモン）は、特定のポートに対する接続要求またはメッセージを聴取し、サーバ プログラムを起動して、それらのポートに関連付けられたサービスを実行します。RCP は、デバイス間でファイルをコピーします。

RCP は、UNIX ユーザがリモート UNIX システムでシェル コマンドを実行できる UNIX rshell サービスのサブセットです。RCP は、UNIX の組み込みサービスです。このサービスは、伝送プロトコルとして TCP を使用し、TCP ポート 514 で要求を聴取します。RCP サービスは、WAAS ソフトウェアを使用する WAAS デバイスで有効にできます。

WAAS デバイスで RCP および FTP サービスを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　RCP サービスを有効にするデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network] > [Network Services] を選択します。[Network Services] ウィンドウが表示されます。

ステップ 4　[Enable Rcp Service] チェックボックスを選択して、Inetd RCP サービスを有効にします。このオプションはデフォルトで無効になっています。

（注）　Inetd デーモンは、FTP、RCP、および TFTP サービスを聴取します。Inetd が RCP 要求を聴取するには、RCP サービス用に明示的に有効にする必要があります。

ステップ 5　[Enable FTP Service] チェックボックスを選択して、Inetd FTP サービスを有効にします。このオプションはデフォルトで無効になっています。

ステップ 6　[Submit] をクリックして、変更を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

日時設定の構成

このセクションでは、WAAS ネットワーク デバイス用の日時設定を構成する方法について説明します。内容は、次のとおりです。

NTP 設定の構成

WAAS Central Manager GUI を使用すると、ネットワーク上の Network Time Protocol（NTP; ネットワーク タイム プロトコル）ホストを使用して日時設定を構成できます。NTP を使用すると、WAAS ネットワーク内の異なる地域にあるデバイスの日時設定を同期化できます。これは正しいシステム動作とモニタリングのために重要です。各 WAAS デバイスで、必ずクロックの同期を維持するように NTP サーバを設定してください。

NTP 設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　設定するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーションペインで、[Configure] > [Data/Time] > [NTP] を選択します。[NTP Settings] ウィンドウが表示されます。

ステップ 4　[Enable] チェックボックスを選択して、NTP 設定を有効にします。このオプションはデフォルトで無効になっています。

ステップ 5　[NTP Server] フィールドに、ホスト名または IP アドレスを入力します。

ステップ 6　[Submit] をクリックします。

（注）　予期しない時間変更は、予期しないシステム動作の原因となる場合があります。NTP サーバの設定後またはシステム クロックの変更後に、システムをリロードすることを推奨します。

時間帯設定の構成

ネットワーク上に時刻サービスを提供する外部ソース（NTP サーバなど）がある場合は、システム クロックを手動で設定する必要はありません。手動でクロックを設定するときは、現地時間を入力します。

（注）　システムには 2 個のクロックがあります。ソフトウェア クロックとハードウェア クロックです。ソフトウェアは、ソフトウェア クロックを使用します。ハードウェア クロックは、ソフトウェア クロックを初期化するために、起動時にだけ使用されます。

デバイスまたはデバイス グループで時間帯を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　時間帯を設定するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Data/Time] > [Time Zone] を選択します。[Time Zone Settings] ウィンドウが表示されます。

ステップ 4　標準時間帯を設定するには、次の手順に従ってください。

a. [Time Zone Settings] セクションで、[Standard Time Zone] オプション ボタンをクリックします。夏時間を設定していない UTC（オフセット =0）がデフォルトです。標準時間帯を設定すると、システムは自動的に UTC オフセットを調整するので、UTC オフセットを指定する必要はありません。

時間帯の標準的な表記法は、*Location/Area* 形式を使用します。ただし、*Location* は世界の大陸または地域、*Area* はその地域内の時間帯領域です。

b. ドロップダウン リストから、時間帯の地域を選択します（このリストの略号については、表 9-2 を参照してください）。

ウィンドウがリフレッシュされ、2 番めのドロップダウン リストに、選択した地域のすべての領域の時間帯が表示されます。

c. 時間帯の領域を選択します。UTC オフセットは自動的に標準時間帯に設定されます。

夏時間が組み込まれている標準時間帯もあります（米国の大半の時間帯が該当）。これらの地域では、夏時間のあいだは UTC オフセットが自動的に変更されます。設定可能な標準時間帯およびその UTC オフセットのリストについては、表 9-3 を参照してください。

ステップ 5　デバイスでカスタマイズされた時間帯を設定するには、次の手順に従ってください。

a. [Time Zone Settings] セクションで、[Customized Time Zone] オプション ボタンをクリックします。

b. [Customized Time Zone] フィールドで、時間帯の名前を指定します。時間帯項目は大文字と小文字を区別し、スペースを含めて最大 40 文字を使用できます。標準時間帯の名前を指定すると、[Submit] をクリックしたときにエラー メッセージが表示されます。

c. UTC オフセットについて、最初のドロップダウン リストから [+] または [-] 記号を選択して、設定された時間帯が UTC より進んでいるか、遅れているかを指定します。また、カスタマイズされた時間帯の UTC オフセット時間（0 ～ 23）と分（0 ～ 59）を選択します。UTC オフセットの範囲は、-23:59 から 23:59 です。デフォルトは 0:0 です。

ステップ 6　カスタマイズされた夏時間を設定するには、[Customized Summer Time Savings] セクションで次の手順に従ってください。

（注）　カスタマイズされた夏時間は、標準時間帯とカスタマイズされた時間帯の両方に指定できます。

a. 対夏時間を設定するには、[Absolute Dates] オプション ボタンをクリックします。

夏時間の開始日付と終了日付は、絶対日付または反復日付で設定できます。絶対日付設定は一度だけ適用され、毎年設定する必要があります。反復日付は、複数年にわたって繰り返し適用されます。

b. [Start Date] フィールドと [End Date] フィールドで、夏時間を開始し、終了する必要がある月（January ～ December）、日（1 ～ 31）、および年（1993 ～ 2032）を mm/dd/yyyy 形式で指定します。終了日付が常に開始日付よりあとにあることを確認します。

あるいは、[Start Date] フィールドと [End Date] フィールドの横にある [Calendar] アイコンをクリックして、[Date Time Picker] ポップアップ ウィンドウを表示します。デフォルトで、現在の日付が黄色で表示されます。必要に応じて、[Date Time Picker] ポップアップ ウィンドウで左矢印または右矢印を使用して、前の年または次の年を選択します。ドロップダウン リストから月を選択します。月の日をクリックします。選択した日付が青色で表示されます。[Apply] をクリックします。あるいは、[Set Today] をクリックして、現在の日付へ戻ります。選択した日付は、[Start Date] フィールドと [End Date] フィールドに表示されます。

c. 反復夏時間を設定するには、[Recurring Dates] オプション ボタンをクリックします。

d. [Start Day] ドロップダウン リストから、開始する曜日（[Monday] ～ [Sunday]）を選択します。

e. [Start Week] ドロップダウン リストから、開始する週を設定するオプション（[first]、[2nd]、[3rd]、または [last]）を選択します。たとえば、[first] を選択すると、夏時間を月の最初の週に開始し、[last] を選択すると、夏時間を月の最後の週に開始するように設定できます。

f. [Start Month] ドロップダウン リストから、開始する月（[January] ～ [December]）を選択します。

g. [End Day] ドロップダウン リストから、終了する曜日（[Monday] ～ [Sunday]）を選択します。

h. [End Week] ドロップダウン リストから、終了する週を設定するオプション（[first]、[2nd]、[3rd]、または [last]）を選択します。たとえば、[first] を選択すると、夏時間を月の最初の週に終了し、[last] を選択すると、夏時間を月の最後の週に終了するように設定できます。

i. [Start Month] ドロップダウン リストから、終了する月（[January] ～ [December]）を選択します。

ステップ 7　[Start Time] ドロップダウン リストから、夏時間を開始する時（0 ～ 23）と分（0 ～ 59）を選択します。[End Time] ドロップダウン リストから、夏時間を終了する時（0 ～ 23）と分（0 ～ 59）を選択します。

夏時間の [Start Time] フィールドと [End Time] フィールドは、夏時間を反映するためにクロックを変更する時刻です。デフォルトで、開始時刻と終了時刻の両方が 00:00 に設定されます。

ステップ 8　[Offset] フィールドで、UTC からのオフセット（0 ～ 1439 分）を指定します（表 9-3 を参照）。

夏時間のオフセットは、システム クロックを指定した開始時刻より進め、終了時刻より遅らせる時間（分）を指定します。

ステップ 9　対応する時間帯に夏時間を指定しないようにするには、[No Customized Summer Time Configured] オプション ボタンをクリックします。

ステップ 10　[Submit] をクリックして、設定を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

表 9-2　時間帯地域の略号

時間帯	時間帯名
CET	中央ヨーロッパ標準時
CST6CDT	中部夏時間
EET	東ヨーロッパ標準時
EST	東部標準時
EST5EDT	東部夏時間
GB	英国

表 9-2　時間帯地域の略号 （続き）

時間帯	時間帯名
GB-Eire	英国 / アイルランド
GMT	グリニッジ標準時
HST	ハワイ標準時
MET	中央ヨーロッパ標準時
MST	山岳部標準時
MST7MDT	山岳部夏時間
NZ	ニュージーランド
NZ-CHAT	ニュージーランド、チャタム諸島
PRC	中国
PST8PDT	太平洋夏時間
ROC	台湾
ROK	韓国
UCT	世界標準時
UTC	世界標準時
WET	西ヨーロッパ標準時
W-SU	中央ヨーロッパ標準時

表 9-3　時間帯、UTC からのオフセット

時間帯	UTC からのオフセット（時間）
Africa/Algiers	+1
Africa/Cairo	+2
Africa/Casablanca	0
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Nairobi	+3
America/Buenos_Aires	-3
America/Caracas	-4
America/Mexico_City	-6
America/Lima	-5
America/Santiago	-4
Atlantic/Azores	-1
Atlantic/Cape_Verde	-1
Asia/Almaty	+6
Asia/Baghdad	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2

表 9-3　時間帯、UTC からのオフセット （続き）

時間帯	UTC からのオフセット（時間）
Asia/Kabul	+4.30
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	-4
Canada/Newfoundland	-3.30
Canada/Saskatchewan	-6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2
Europe/London	0
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	-12
Pacific/Samoa	-11
US/Alaska	-9
US/Central	-6
US/Eastern	-5

表 9-3　時間帯、UTC からのオフセット （続き）

時間帯	UTC からのオフセット（時間）
US/East–Indiana	-5
US/Hawaii	-10
US/Mountain	-7
US/Pacific	-8

UTC は、かつての Greenwich Mean Time（GMT; グリニッジ標準時）です。表に示すオフセット時間（UTC との相対時間）は、実質的に冬時間のものです。夏時間中は、オフセットが表の値と異なる場合があり、システム クロックによって計算され、それに応じて表示されます。

セキュア ストア設定の構成

セキュア ストア暗号化は、WAAS システムのためのより強力な暗号化とキー管理を実現します。WAAS Central Manager と WAE デバイスは、パスワードの処理、暗号キーの管理、およびデータの暗号化にセキュア ストア暗号化を使用します。

ここでは、次の内容について説明します。

セキュア ストアの概要

Central Manager または WAE デバイスでセキュア ストア暗号化を有効にすると、WAAS は強力な暗号化アルゴリズムとキー管理ポリシーを使用して、システム上の特定のデータを保護します。このデータには、WAAS システム内でアプリケーションが使用する暗号キー、CIFS パスワード、ユーザ ログイン パスワード、証明書キー ファイルおよびが含まれます。

セキュア ストア暗号化を有効にするには、Central Manager でパスワードを入力する必要があります。このパスワードは、安全規格に従い *キー暗号キー*を生成するために使用されます。WAAS システムは、キー暗号キーを使用して、Central Manager または WAE デバイス上で生成された他のキーを暗号化し保存します。これらのその他のキーは、ディスクの暗号化や SSL アクセラレーション、または CIFS アクセラレータのクレデンシャル、WAFS コア パスワード、ユーザ パスワードの暗号化と保存などの WAAS 機能で使用されます。

セキュア ストアが Central Manager で有効な場合、データは、SHA1 ハッシュと AES 256 ビット アルゴリズムを使用して、入力されたパスワードから生成された 256 ビット キー暗号キーを使用して暗号化されます。セキュア ストアが WAE デバイスで有効な場合、データは、SecureRandom（暗号として強力な疑似乱数ジェネレータ）を使用して生成された 256 ビット キー暗号キーを使用して暗号化されます。

セキュア ストアを実装するには、システムが次の要件を満たしている必要があります。

- Central Manager がネットワークで使用できるように設定されている必要があります。
- WAE デバイスが、Central Manager に登録されている必要があります。
- WAE デバイスが Central Manager とオンラインになっている（アクティブ接続を確立している）必要があります。この要件は、セキュア ストアが WAE デバイスで有効な場合にのみ適用されます。
- すべての Central Manager と WAE デバイスで、WAAS ソフトウェア バージョン 4.0.19 以上を実行している必要があります。

強力なストア暗号化を実装するには、次の手順に従ってください。

ステップ 1　プライマリ Central Manager で強力なストレージ暗号化を有効にします（「Central Manager でのセキュア ストア暗号化の有効化」を参照）。

ステップ 2　スタンバイ Central Manager で強力なストレージ暗号化を有効にします（「スタンバイ Central Manager でのセキュア ストア暗号化の有効化」を参照）。

ステップ 3　WAE デバイスまたは WAE デバイス グループで強力なストレージ暗号化を有効にします（「WAE デバイスでのセキュア ストア暗号化の有効化」を参照。セキュア ストアは、Central Manager で有効にしてから、WAE デバイスで有効にする必要があります）。

セキュア ストアは、Central Manager と WAE デバイスで独立して有効にすることができます。暗号化されたデータの完全な保護を保証するには、セキュア ストアを Central Manager と WAE デバイスの両方で有効にします。最初に、Central Manager 上でセキュア ストアを有効にする必要があります。

（注）　Central Manager をリブートした場合、セキュア ストア暗号化を手動で再有効化する必要があります。リモート WAE デバイスのディスク暗号化機能および CIFS 事前配置機能は、Central Manager でセキュア ストア パスワードを入力して、セキュア ストア暗号化を再度有効化するまで動作しません。

セキュア ストアが有効な場合、次のシステムの特性に影響します。

- Central Manager データベースに保存されたパスワードは、強力な暗号化技術を使用して暗号化されます。
- CIFS 事前配置クレデンシャルは、Central Manager と WAE デバイスの強力な暗号キーを使用して暗号化されます。
- 証明書キー ファイルは、Central Manager の強力な暗号キーを使用して暗号化されます。
- プライマリ Central Manager が失敗すると、セキュア ストア キー管理はスタンバイ Central Manager によって処理されます（スタンバイ Central Manager では、セキュア ストア モードを手動で有効にする必要があります）。
- バックアップ スクリプトは、バックアップの実行時に、デバイスのセキュア ストア モード ステータスをバックアップします。バックアップは、Central Manager 上でのみサポートされています。

- 復元スクリプトは、バックアップ ファイルのセキュア ストア モードが有効であるかどうかを確認します。バックアップ ファイルがセキュア ストア モードである場合は、デバイスを確認し復元するために、パス フレーズを入力する必要があります。復元は、Central Manager 上でのみサポートされています。
- WAE デバイスでセキュア ストアを有効にすると、システムは Central Manager からの新しい暗号キーを初期化し取得します。WAE は、このキーを使用して、ディスク上の CIFS 事前配置クレデンシャルや情報などのデータを暗号化します（ディスク暗号化も有効な場合）。
- セキュア ストアを有効にしたあとで WAE をリブートすると、WAE は Central Manager からキーを自動的に取得します。これにより、WAAS 永続ストレージに保存されているデータにアクセスできるようになります。キーの取得に失敗した場合は、クリティカル アラームが発生し、セキュア ストアを手動で再オープンする必要があります。更新に CIFS 事前配置、ダイナミック共有、またはユーザ設定が含まれる場合、セキュア ストアが再オープンされるまで、WAE は Central Manager からの設定更新を拒否します。また、WAE から Central Manager に送信される更新には、事前配置設定は含まれません。
- セキュア ストアがアクティブな場合、セキュア ストア モードをサポートしていない旧バージョンの WAAS ソフトウェアにはダウングレードできません。旧バージョンの WAAS ソフトウェアをインストールする前に、セキュア ストア モードを無効にする必要があります。
- セキュア ストアは特定のシステム情報を暗号化しますが、ハード ドライブ上のデータは暗号化しません。データ ディスクを保護するには、別途、ディスク暗号化を有効にする必要があります（「ディスクの暗号化の有効化」（P.15-29）を参照）。

Central Manager でのセキュア ストア暗号化の有効化

Central Manager でセキュア ストア暗号化を有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、[Admin] > [Secure Store] を選択します。[Configure CM Secure Store] ウィンドウが表示されます。

ステップ 2　[Enter passphrase] および [Confirm passphrase] フィールドにパスワードを入力します。

パスワードは、次の規則に従う必要があります。

- 長さは 8 ～ 64 字
- 許可される文字セット（[A-Za-z0-9~%'!#$^&*()|;:,\"<>/]*）だけを使用
- 数字を少なくとも 1 文字含める
- 大文字と小文字を少なくとも 1 文字ずつ含める

ステップ 3　[Initialize] ボタンをクリックします。

セキュア ストアが初期化され、オープンされます。データはパスワードから派生したキーを使用して暗号化されます。

CLI からセキュア ストアを有効にするには、**cms secure-store init** EXEC コマンドを使用します。

（注）　Central Manager をリブートした場合は常に、セキュア ストアを手動で再オープンする必要があります。リモート WAE デバイスのディスク暗号化機能および CIFS 事前配置機能は、Central Manager でセキュア ストア パスワードを入力して、セキュア ストアを再オープンするまで動作しません。[Open

Secure Store] セクションを使用する必要がある場合を除き、上記と同じ設定画面を使用します。セキュア ストアはすでに初期化されているので、[Initialize Secure Store] セクションは表示されません。あるいは、**cms secure-store open** EXEC コマンドを使用することもできます。

（注）　プライマリ Central Manager のセキュア ストアを有効にした場合は、同様にスタンバイ Central Manager のセキュア ストアも有効にする必要があります（「スタンバイ Central Manager でのセキュア ストア暗号化の有効化」（P.9-13）を参照）。

セキュア ストア暗号化のステータスをチェックするには、**show cms secure-store** コマンドを入力します。

スタンバイ Central Manager でのセキュア ストア暗号化の有効化

（注）　スタンバイ Central Manager では、暗号キー管理のサポートは限定されています。プライマリ Central Manager が失敗した場合、スタンバイ Central Manager は WAE デバイスに対して暗号キーの取得を可能にするだけで、新しい暗号キーの初期化は行いません。プライマリ Central Manager が使用不能な場合は、WAE デバイスのディスク暗号化またはセキュア ストアは有効にしないでください。

スタンバイ Central Manager でセキュア ストア暗号化を有効にするには、最初にプライマリ Central Manager でセキュア ストアを有効にしてから、CLI を使用して、スタンバイ Central Manager 上で **cms secure-store open** EXEC モード コマンドを実行します。

ステップ 1　プライマリ Central Manager でセキュア ストア暗号化を有効にします（「Central Manager でのセキュア ストア暗号化の有効化」（P.9-12）を参照）。

ステップ 2　スタンバイ Central Manager がプライマリ Central Manager からデータを複製するまで待ちます。

レプリケーション（複製）は、60 秒以内（デフォルト）に、またはシステムの設定に従って実行されます。

ステップ 3　スタンバイ Central Manager で **cms secure-store open** コマンドを入力して、セキュア ストア暗号化をアクティブにします。

スタンバイ Central Manager が、「please enter pass phrase」メッセージで応答します。

ステップ 4　パスワードを入力し、Enter を押します。

スタンバイ Central Manager が、セキュア ストア暗号化を使用してデータを暗号化します。

（注）　システム上のスタンバイ Central Manager ごとにステップ 3 ～ 4 を繰り返します。

セキュア ストア暗号化のステータスをチェックするには、**show cms secure-store** コマンドを入力します。

WAE デバイスでのセキュア ストア暗号化の有効化

WAE デバイスでセキュア ストア暗号化を有効にするには、次の手順に従ってください。

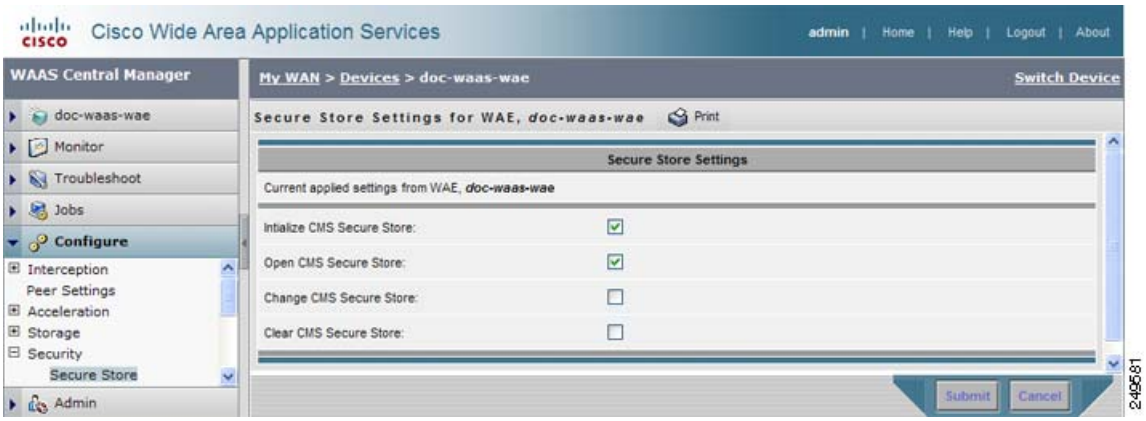
ステップ 1　WAAS Central Manager GUI から、[Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　セキュア ストアを有効にするデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

（注）　セキュア ストア ステータスは、デバイス グループ内のすべての WAE デバイスで同一である必要があります。グループ内のすべての WAE デバイスのセキュア ストアを有効にするか、すべての WAE デバイスのセキュア ストアを無効にする必要があります。WAE デバイスをデバイス グループに追加する前に、その WAE デバイスのセキュア ストア ステータスが他の WAE デバイスのステータスと一致するように設定する必要があります（「デバイス グループの操作」（P.3-2）を参照）。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [Secure Store] を選択します。図 9-1 に示すように、[Secure Store Settings] ウィンドウが表示されます。

図 9-1　[Secure Store Settings] ウィンドウの例



ステップ 4　[Initialize CMS Secure Store] ボックスを選択します（[Open CMS Secure Store] ボックスは自動的に選択されています）。

ステップ 5　[Submit] をクリックして、セキュア ストア暗号化をアクティブにします。

新しい暗号キーが Central Manager で初期化され、WAE はセキュア ストア暗号化を使用してデータを暗号化します。

CLI からセキュア ストアを有効にするには、**cms secure-store init** EXEC コマンドを使用します。

（注）　**cms secure-store** コマンドを実行する前に、WAE 上でデータ入力ポール レート間隔（デフォルトは 5 分）以内にその他の CLI 設定変更を行った場合、これらの先行する設定変更は失われるため、再度実行する必要があります。

（注）　デバイス グループのセキュア ストアを有効または無効にしても、変更内容はすべての WAE デバイスに同時に反映されません。WAE デバイスを表示した際には、Central Manager が各 WAE デバイスのステータスを更新するまで十分な時間を確保してください。

セキュア ストア暗号キーおよびパスワードの変更

セキュア ストア暗号化パスワードは、Central Manager が暗号化されたデータ用の暗号キーを生成するために使用されます。

Central Manager でパスワードを変更し新しい暗号キーを生成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、[Admin] > [Secure Store] を選択します。

ステップ 2　[Current passphrase] フィールドに、現在のパスワードを入力します。

ステップ 3　[Enter new passphrase] フィールドに、新しいパスワードを入力します。

パスワードは、次の規則に従う必要があります。

- 長さは 8 ～ 64 字
- 許可される文字セット（[A-Za-z0-9~%'!#$^&*()|;:,\"<>/]*）だけを使用
- 数字を少なくとも 1 文字含める
- 大文字と小文字を少なくとも 1 文字ずつ含める

ステップ 4　[Confirm passphrase] フィールドに、もう一度新しいパスワードを入力します。

ステップ 5　[Change] ボタンをクリックします。

WAAS デバイスは、新しいパスワードから派生した新しい暗号キーを使用して、保存されているデータを暗号化し直します。

CLI から Central Manager のパスワードを変更し新しい暗号キーを生成するには、**cms secure-store change** EXEC コマンドを使用します。

WAE デバイスの新しい暗号キーを生成するには、WAAS Central Manager GUI を使用して、次の手順に従います。

ステップ 1　WAAS Central Manager GUI から、[Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　新しい暗号キーを生成するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [Secure Store] を選択します。

ステップ 4　[Change CMS Secure Store] チェックボックスを選択し、[Submit] をクリックします。

Central Manager 内で新しい暗号キーが生成されます。Central Manager が、WAE 内の暗号キーを新しいキーで置き換えます。WAE は、新しい暗号キーを使用して保存されているデータを暗号化し直します。

CLI からセキュア ストア暗号キーを設定するには、**cms secure-store change** EXEC コマンドを使用します。

Central Manager でのセキュア ストア暗号化のリセット

Central Manager をリロードし、セキュア ストア パスワードを忘れたためにセキュア ストアをオープンできない場合は、**cms secure-store reset** コマンドを使用します。このコマンドにより、すべての暗号化されたデータ、証明書ファイルとキー ファイル、およびキー マネージャのキーが削除されます。セキュア ストアは初期化されていない状態のままになります。

Central Manager でセキュア ストア暗号化をリセットするには、次の手順に従ってください。

ステップ 1　プライマリ Central Manager で **cms secure-store reset** コマンドを入力します。

ステップ 2　スタンバイ Central Manager がプライマリ Central Manager からデータを複製するまで待ちます。

レプリケーション（複製）は、60 秒以内（デフォルト）に、またはシステムの設定に従って実行されます。

ステップ 3　セキュア ストアが初期化され、オープンされた状態の場合は、スタンバイ Central Manager で **cms secure-store reset** コマンドを入力します。

ステップ 4　プライマリ Central Manager から、すべてのユーザ アカウント パスワード、CIFS クレデンシャル、CIFS レガシー モードのコア パスワードをリセットします。

ユーザ パスワードをリセットする方法については、「別のアカウントのパスワードの変更」（P.7-8）を参照してください。CIFS レガシー モードのコア クラスタ パスワードをリセットする方法については、「コア クラスタの設定」（P.11-11）を参照してください。ダイナミック共有パスワードをリセットする方法については、「ダイナミック共有の作成」（P.11-21）を参照してください。事前配置パスワードをリセットする方法については、「事前配置ディレクティブの作成」（P.11-26）を参照してください。

ステップ 5　「Central Manager でのセキュア ストア暗号化の有効化」（P.9-12）の説明に従って、プライマリ Central Manager でセキュア ストアを初期化し、オープンします。

ステップ 6　スタンバイ Central Manager のセキュア ストアが初期化されており、オープンされていない場合は、プライマリ Central Manager からスタンバイ Central Manager にデータが複製されるまで待ってから、**cms secure-store open** コマンドを使用して、スタンバイ Central Manager でセキュア ストアをオープンします。

ステップ 7　Central Manager に登録されている各 WAE で、次の手順を実行します。

a.　セキュア ストアが初期化され、オープンされている場合は、Central Manager から、セキュア ストアをクリアします（「WAE デバイスでのセキュア ストア暗号化の無効化」（P.9-17）を参照）。または、CLI から、**cms secure-store clear** EXEC コマンドを入力します。

b.　Central Manager から、セキュア ストアを初期化します（「WAE デバイスでのセキュア ストア暗号化の有効化」（P.9-13）を参照）。または、CLI から、**cms secure-store init** EXEC コマンドを入力します（この手順はステップ 7a を実行した場合にだけ必要です）。

c.　**crypto pki managed-store initialize** コマンドを入力し、SSL アクセラレータを再起動します。

d.　ディスク暗号化が有効になっている場合は、Central Manager から、ディスク暗号化を無効にします（「ディスクの暗号化の有効化」（P.15-29）を参照）。または、CLI から、**no disk encrypt enable** グローバル コンフィギュレーション コマンドを入力します。

e.　ステップ 7d の前にディスク暗号化が有効になっている場合は、デバイスをリロードします。リロード後、ディスク暗号化を再度有効にし、デバイスをもう一度リロードします。

（注）　ステップ 7 を実行する前に WAE がリロードされた場合、ディスク暗号化、SSL アクセラレーション、およびセキュア ストアは正しく機能しなくなります。このような場合は、WAE を工場出荷時のデフォルト設定に戻す必要があります。

ステップ 8　プライマリ Central Manager から、WAE で設定されているすべての高速化およびピアリング サービス用に、すべての証明書およびキー ファイルを再インポートします。

WAE デバイスでのセキュア ストア暗号化の無効化

WAE デバイスでセキュア ストア暗号化を無効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、[Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　セキュア ストアを無効にするデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [Secure Store] を選択します。図 9-1 に示すように、[Secure Store Settings] ウィンドウが表示されます。

ステップ 4　[Clear CMS Secure Store] チェックボックスを選択し、[Submit] をクリックすると、セキュア ストア暗号化は無効になり、標準の暗号化に戻ります。

また、**cms secure-store clear** コマンドを入力しても、セキュア ストア暗号化を無効にし、標準の暗号化に戻すことができます。

CLI から WAE または Central Manager のセキュア ストアを無効にするには、**cms secure-store clear** EXEC コマンドを使用します。

（注）　プライマリ Central Manager のセキュア ストアを無効にした場合は、同様にスタンバイ Central Manager のセキュア ストアも無効にする必要があります。

デフォルトのシステム設定プロパティの変更

WAAS ソフトウェアではすでにシステム プロパティが設定済みですが、システムのデフォルト動作を変更するために変更できます。これらのプロパティを変更するには、WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [System Properties] を選択します。

表 9-4 で、変更できるシステム設定プロパティについて説明します。

表 9-4　システム設定プロパティの説明

システム プロパティ	説明
cdm.remoteuser.deletionDaysLimit	外部ユーザが最後にログインしてから、WAAS Central Manager データベースから削除されるまでの最大日数。たとえば、cdm.remoteuser.deletionDaysLimit が 5 に設定されている場合、最後のログイン時と現在の時間の差が 5 日を超えると、この外部ユーザはデータベースから削除されます。デフォルトは、1 日です。外部ユーザとは、WAAS Central Manager ではなく、外部 AAA サーバで定義されるユーザです。
cdm.session.timeout	WAAS Central Manager GUI セッションのタイムアウト（分）。デフォルトは、10 分です。セッションがこの長さの時間アイドル状態である場合、ユーザは自動的にログアウトされます。
DeviceGroup.overlap	デバイスが複数のデバイス グループに属することが可能かどうかを示すステータス。デフォルトは true です（デバイスは複数のデバイス グループに属することができます）。

表 9-4　システム設定プロパティの説明 （続き）

システム プロパティ	説明
System.datafeed.pollRate	WAAS デバイスと WAAS Central Manager 間のポール レート（秒）。デフォルトは、300 秒です。
System.device.recovery.key	デバイス ID の復旧キー。このプロパティを使用すると、WAAS ネットワーク内の別のノードでデバイスを交換できます。
System.guiServer.fqdn	Device Manager GUI を起動するために使用する方式（IP アドレスまたは FQDN）。
System.healthmonitor.collectRate	CMS デバイスの状態（またはステータス）をモニタするための収集と送信の速度（秒）。速度を 0 に設定すると、状態のモニタは無効になります。デフォルトは、120 秒です。
System.lcm.enable	ローカルと中央の管理機能（有効または無効）。このプロパティを使用すると、ローカル デバイスの CLI または WAAS Central Manager GUI を使用して構成した設定を WAAS ネットワーク設定データの一環として保存できます。デフォルトは true です。このプロパティが false（無効）に設定されている場合、ローカル デバイスで実行された設定変更は Central Manager に伝達されず、Central Manager で実行された設定がローカル デバイスの設定を上書きします。
System.monitoring.collectRate	WAE がモニタリング レポートを収集し、WAAS Central Manager へ送信する速度（秒）。デフォルトは 300 秒（5 分）です。この間隔を減らすと、WAAS Central Manager デバイスのパフォーマンスに影響します。
System.monitoring.dailyConsolidationHour	WAAS Central Manager が 1 時間ごとおよび 1 日ごとにモニタリング レコードを集計する時刻。デフォルトは 1（午前 1 時）です。
System.monitoring.enable	WAE 統計情報のモニタリング（有効または無効）。デフォルトは true です。
System.monitoring.maxDevicePerLocation	位置レベル レポートでモニタリング対象としてサポートされるデバイスの最大数。デフォルト値は 25 です。
System.monitoring.maxReports	カスタム レポートごとに保存する、成功または失敗したレポート インスタンスの最大数。デフォルトは、10 個のレポート インスタンスです。

表 9-4　システム設定プロパティの説明 （続き）

システム プロパティ	説明
System.monitoring.monthlyConsolidationFrequency	WAAS Central Manager が日単位のモニタリング レポートを月次レポートに集計する回数（日単位）。この設定を 1 に設定すると、WAAS Central Manager は、毎日集計を実行する必要があるかどうかを検査し、集計に十分なデータがある場合のみ集計を実行します。デフォルトは、14 日です。 毎月のデータ レコードを作成すると、対応する毎日のレコードはデータベースから削除されます。集計は、少なくとも 2 か月分のデータと集計周期日数分のデータが存在する場合のみ実行されます。そのため、WAAS Central Manager は、常に先月の毎日のデータ レコードを保持し、先週のデータを 1 日単位で表示できます。 たとえば、データ収集が 2006 年 2 月 2 日に開始し、System.monitoring.monthlyConsolidationFrequency が 14 に設定されている場合、WAAS Central Manager は、2 月 16 日、3 月 2 日、3 月 16 日、および 3 月 30 日に過去 2 か月分のデータがあるかどうかを検査します。これらの日には十分なデータが存在しないため、集計は実行されません。 ただし、4 月 13 日には、2 か月分のデータが存在します。WAAS Central Manager は、2 月のデータを集計し、2 月の毎日のデータ レコードを削除します。
System.monitoring.recordLimitDays	システムに保持するモニタリング データの最大日数。デフォルトは、1825 日です。
System.monitoring.timeFrameSettings	すべてのチャートを示すのに使用されるデフォルトの期間。ユーザが保存するデータは変更されません。デフォルトは、Last Hour です。
System.print.driverFtpTimeout	FTP でプリンタ ドライバ ファイルが転送されるのを待つ最大秒数。範囲は、10 ～ 1800 秒です。デフォルトは、600 秒です。
System.registration.autoActivation	Central Manager に登録されている WAE デバイスを自動的にアクティブにする自動アクティベーション機能のステータス。デフォルトは、true です（デバイスは自動的に登録されます）。
System.rpc.timeout.syncGuiOperation	Central Manager の WAE 接続との GUI 同期操作のタイムアウト（秒）。デフォルトは、50 秒です。
System.security.maxSimultaneousLogins	ユーザに許可される WAAS Central Manager の最大同時セッション数。同時セッションを無制限に許可する場合は 0（ゼロ、デフォルト）を指定します。セッションを終了するには、Central Manager からログオフする必要があります。ユーザがログオフせずにブラウザを閉じた場合、セッションは 120 分後にタイムアウトするまで閉じられません（タイムアウトは設定できません）。許可される並列セッションの数を超えた場合も、タイムアウトになるまで Central Manager GUI に再びアクセスできません。この設定は CLI から Central Manager デバイスへのアクセスには影響を及ぼしません。
System.security.webApplicationFilter	JavaScript、SQL、または制限された特殊文字の入力を拒否する Web アプリケーション フィルタのステータス。デフォルトは、false です。

表 9-4　システム設定プロパティの説明 （続き）

システム プロパティ	説明
System.standby.replication.maxCount	スタンバイ Central Manager に複製される統計データ レコードの最大数（1,000 単位）。範囲は、10 ～ 300 です。デフォルトは、200（200,000 レコード）です。この数字を増やすことは推奨できません。
System.standby.replicationTimeout	スタンバイ Central Manager への複製を待つ最大秒数。範囲は、300 ～ 3600 秒です。デフォルトは、900 秒です。このタイムアウトを減らすことは推奨できません。

システム プロパティの値を表示または変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [System Properties] を選択します。[Config Properties] ウィンドウが表示されます。

ステップ 2　変更するシステム プロパティの横にある [Edit] アイコンをクリックします。[Modifying Config Property] ウィンドウが表示されます。

ステップ 3　変更するシステム プロパティに応じて、ドロップダウン リストから、新しい値を入力するか、新しいパラメータを選択します。

ステップ 4　[Submit] をクリックして、設定を保存します。

Web アプリケーション フィルタの設定

Web アプリケーション フィルタは、WAAS Central Manager GUI を Cross-Site Scripting（XSS; クロスサイト スクリプティング）攻撃から保護するセキュリティ機能です。XSS のセキュリティ問題は、ユーザから発信されるデータを、アプリケーションが最初に内容を検査または符号化せずに Web ブラウザに送信した場合に発生する可能性があります。これにより、悪意のある スクリプトがクライアントのブラウザで実行され、データベースの整合性が損なわれる可能性があります。

このセキュリティ機能により、WAAS ユーザが送信するすべてのアプリケーション パラメータは、HTML ページに読み込まれる前に検査および/または符号化されることが確認されます。

ここでは、次の内容について説明します。

- 「Web アプリケーション フィルタの有効化」（P.9-20）
- 「セキュリティ検査」（P.9-21）

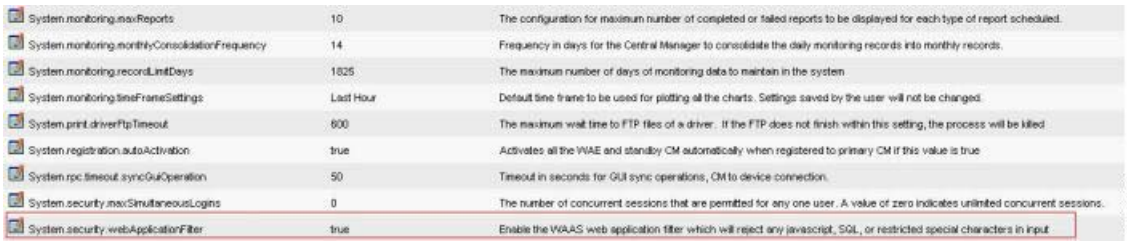
Web アプリケーション フィルタの有効化

Web アプリケーション フィルタを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI から、[Configure] > [System Properties] を選択します。[Config Properties] ウィンドウが表示されます（図 9-2 を参照）。

（注）　CLI を使用してこの機能を有効にすることはできません。この機能はデフォルトで無効になっています。

図 9-2　[Config Properties]



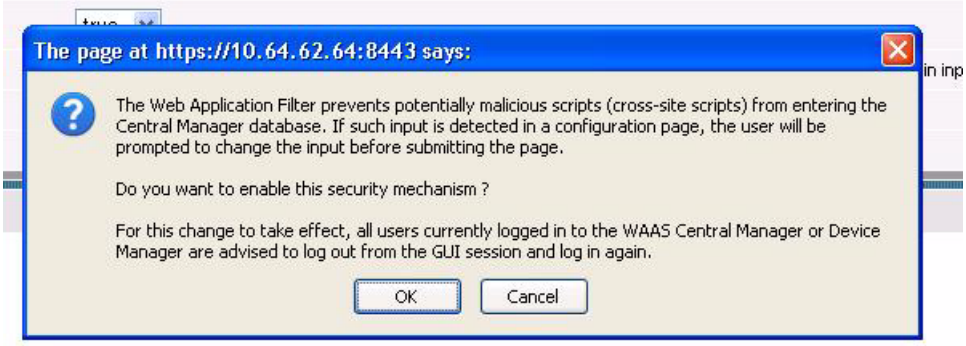
ステップ 2　system.security.webApplicationFilter 項目の横にある [Edit] アイコンをクリックします。

[Modifying Config Property] ウィンドウが表示されます。

ステップ 3　[Value] ドロップダウン リストから [true] を選択して、この機能を有効にします。

Central Manager または Device Manager ユーザに対し、この機能を有効にしたあと、ログアウトしてから再度ログインすることを勧める警告メッセージが表示されます（図 9-3 を参照）。

図 9-3　[Modifying Config Property]



ステップ 4　[OK] をクリックし、[Submit] をクリックします。

ステップ 5　ログアウトしてから再度ログインします。

セキュリティ検査

Web アプリケーション フィルタ機能では、入力検査とサニタイズという 2 つの方法を使用してセキュリティを検証します。入力検査では、データを受け入れる前にすべての入力データを検査します。サニタイズは、データ内にすでに存在する悪意のある設定やスクリプトが実行されることを防止します。

ここでは、次の内容について説明します。

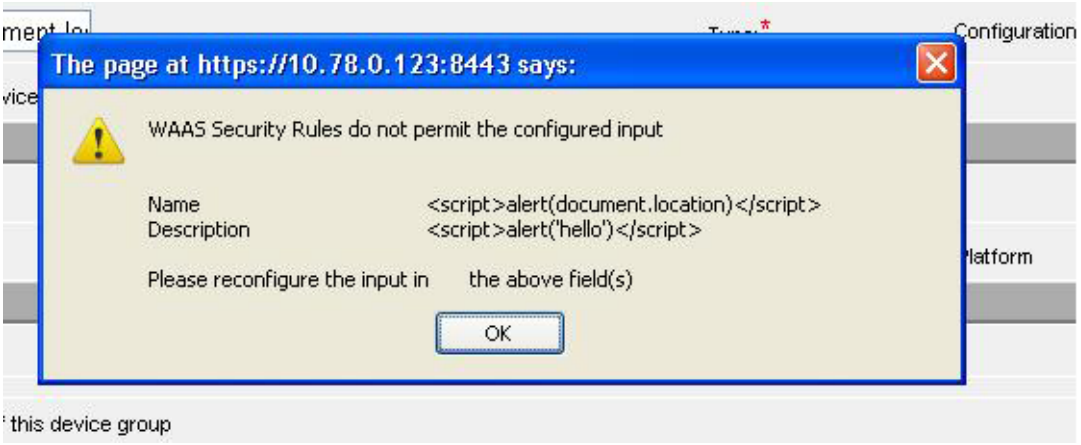
- 「入力検査」（P.9-21）
- 「サニタイズ」（P.9-22）

入力検査

入力検査は、Central Manager および Device Manager データベースに入力されるすべてのデータをスキャンするもので、admin ユーザだけが設定できます。

Central Manager GUI を使用して送信されたデータに XSS の疑いがある場合はすべてブロックされます。入力がブロックされると、警告が表示されます（図 9-4 を参照）。

図 9-4　　警告



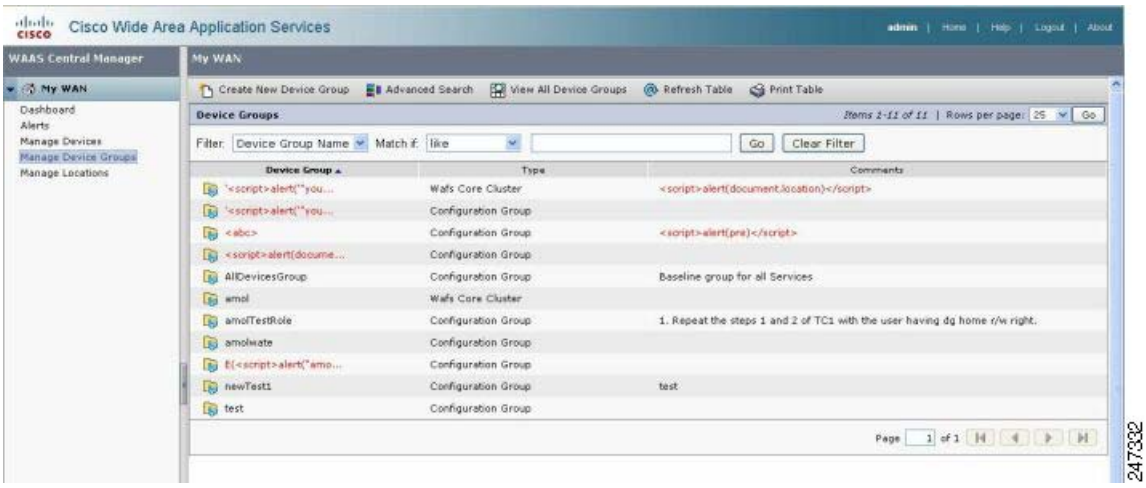
入力データは次の XSS フィルタ ルールと照合されます。

- セミコロン（;）が含まれる場合、入力は拒否されます。
- 山カッコ（<>）で囲まれている場合、入力は拒否されます。
- 上記のタグ（&#60、&#62、%3c、%3e）の生成に間接的に使用される可能性がある場合、入力は拒否されます。

サニタイズ

サニタイザは、データベースに対して XSS 攻撃があったときに、悪意のある設定やスクリプトがブラウザで実行されるのを防止します。ユーザはサニタイズを設定することはできません（図 9-5 を参照）。

図 9-5　　XSS 設定データ



Central Manager から送信された設定データに XSS の疑いがある場合は、[My WAN] > [Manage Device Groups] > [Device Groups] ページに赤色で表示されます。

オフライン WAAS デバイスの高速検出の設定

オフライン デバイスの高速検出を有効にすると、オフライン WAAS デバイスを高速に検出できます。WAAS デバイスは、2 回以上のポーリング期間にわたって getUpdate（get configuration poll）要求で WAAS Central Manager にアクセスできない場合、オフラインとして宣言されます（この機能の詳細については、「オフライン デバイスの高速検出について」（P.9-23）を参照してください）。

オフライン WAAS デバイスの高速検出を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Fast Device Offline Detection] を選択します。[Configure Fast Offline Detection] ウィンドウが表示されます。

（注）　オフライン デバイス高速検出機能は、WAAS Central Manager がデバイスから最初の UDP ハートビート パケットと getUpdate 要求を受信するときだけ有効です。

ステップ 2　[Enable] チェックボックスを選択して、WAAS Central Manager がデバイスのオフライン ステータスを高速検出できるようにします。

ステップ 3　[Heartbeat Rate (Seconds)] フィールドで、デバイスが UDP ハートビート パケットを WAAS Central Manager へ送信する必要がある頻度を指定します。デフォルトは、30 秒です。

ステップ 4　[Heartbeat Fail Count] フィールドで、デバイスがオフラインと宣言される前にデバイスから WAAS Central Manager への送信中に削除できる UDP ハートビート パケットの個数を指定します。デフォルトは、1 です。

ステップ 5　[Heartbeat UDP Port] フィールドで、デバイスが UDP ハートビート パケットをプライマリ WAAS Central Manager へ送信するために使用するポート番号を指定します。デフォルトは、ポート 2000 です。

[Maximum Offline Detection Time] フィールドに、失敗したハートビート カウントとハートビート速度の積が表示されます。

最大オフライン検出時間 = 失敗したハートビート カウント×ハートビート速度

オフライン デバイスの高速検出機能を有効にしていない場合、WAAS Central Manager は、デバイスがオフラインと宣言される前に、デバイスが getUpdate 要求でアクセスされるまで 2 回以上のポーリング期間を待ちます。ただし、オフライン デバイスの高速検出機能を有効にすると、WAAS Central Manager は、[Maximum Offline Detection Time] フィールドに表示される値を超えるまで待ちます。

WAAS Central Manager がデバイスから Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を受信すると、2 ×（ハートビート速度）×（失敗したハートビート カウント）の期間の後で、WAAS Central Manager GUI にデバイスがオフラインとして表示されます。

ステップ 6　[Submit] をクリックします。

オフライン デバイスの高速検出について

WAAS デバイスと WAAS Central Manager の通信に UDP を使用すると、オフラインになったデバイスをより高速に検出できます。UDP ハートビート パケットは、指定した間隔で WAAS ネットワーク内の各デバイスからプライマリ WAAS Central Manager へ送信されます。プライマリ WAAS Central

Manager は、各デバイスから UDP ハートビート パケットを受信した最後の時刻を追跡します。WAAS Central Manager は、指定した個数の UDP パケットを受信しない場合、応答しないデバイスのステータスをオフラインとして表示します。UDP ハートビートは getUpdate 要求より必要な処理量が少ないため、より頻繁に送信でき、WAAS Central Manager はより高速にオフライン デバイスを検出できます。

この機能を有効または無効にする、2 個の UDP パケット間の間隔を指定する、および失敗したハートビート カウントを設定することができます。ハートビート パケット速度は、2 個の UDP パケットの間隔として定義されます。WAAS Central Manager GUI は、指定したハートビート パケット速度と失敗したハートビート カウントの値を使用して、ハートビート速度と失敗したハートビート カウントの積としてオフライン検出時間を表示します。オフライン デバイスの高速検出を有効にすると、WAAS Central Manager は、UDP をサポートしていないネットワーク セグメントに存在するデバイスを検出し、getUpdate（get configuration poll）要求を使用してオフライン デバイスを検出します。

デフォルトで、オフライン デバイスの高速検出機能は無効になっています。

アラーム過負荷検出の設定

WAAS デバイスは、Node Health Manager からの着信アラーム レートを追跡できます。着信アラーム レートが High Water Mark（HWM; 最高水準点）を超えると、WAAS デバイスはアラーム過負荷状態になります。この状況は、複数のアプリケーションがエラー条件を報告するために同時にアラームを上げると発生します。WAAS デバイスがアラーム過負荷状態になると、次の状況が発生します。

- それ以降のアラーム発信およびクリア動作に関する SNMP トラップは、一時停止されます。raise alarm-overload アラームと clear alarm-overload アラームに対応するトラップが送信されます。ただし、raise alarm-overload アラームが発信されてから clear alarm-overload アラームが発信されるまでの間に行われたアラーム動作に関するトラップは一時停止されます。
- アラーム過負荷発信およびクリア通知は、ブロックされません。アラーム過負荷状態は、SNMP と Configuration Management System（CMS; 構成管理システム）に伝達されます。ただし、アラーム過負荷状態では、SNMP と CMS に個々のアラームは通知されません。情報は、CLI を使用しないと入手できません。
- アラーム レートが Low Water Mark（LWM; 最低水準点）を下回るレベルまで減少するまで、WAAS デバイスはアラーム過負荷状態のままです。
- 着信アラーム レートが LWM より下がると、WAAS デバイスはアラーム過負荷状態から出て、アラーム カウントを SNMP と CMS に報告し始めます。

WAAS デバイスがアラーム過負荷状態にある場合、Node Health Manager は、WAAS デバイスで上げられるアラームを記録し、着信アラーム レートを追跡し続けます。WAAS デバイスで上げられるアラームは、『*Cisco Wide Area Application Services Command Reference*』に説明されている **show alarm** CLI コマンドを使用して表示できます。

WAAS デバイス（またはデバイス グループ）用のアラーム過負荷検出を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices]（または [Device Groups]）ウィンドウが表示されます。

ステップ 2　アラーム過負荷検出を設定するデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーションペインで、[Configure] > [Monitoring] > [Alarm Overload Detection] を選択します。[Alarm Overload Detection Settings] ウィンドウが表示されます。

ステップ 4　複数のアプリケーションがエラー条件を報告したときに、WAAS デバイス（またはデバイス グループ）がアラーム発信とクリア動作を一時停止するように設定しない場合は、[Enable Alarm Overload Detection] チェックボックスの選択を解除します。デフォルトで、このチェックボックスは選択されています。

ステップ 5　[Alarm Overload Low Water Mark (Clear)] フィールドで、それより下がると WAAS デバイスがアラーム過負荷状態から出る 1 秒あたりの着信アラーム数を入力します。

最低水準点とは、アラームを再起動する前にアラームの数が下がる必要がある最低水準です。デフォルト値は 1 です。最低水準点は、最高水準点値未満でなければなりません。

ステップ 6　[Alarm Overload High Water Mark (Raise)] フィールドで、それを超えると WAAS デバイスがアラーム過負荷状態に入る 1 秒あたりの着信アラーム数を入力します。デフォルト値は 10 です。

ステップ 7　[Submit] をクリックして、設定を保存します。

CLI からアラーム過負荷検出を設定するには、**alarm overload-detect** グローバル コンフィギュレーション コマンドを使用します。

E メール通知サーバの設定

レポートを定期的に生成するようスケジュールし、レポートが生成されたときに、レポートへのリンクを 1 人または複数の受信者に E メール送信することが可能です（詳細は、「レポートの管理」（P.16-48）を参照）。

E メール通知を有効化するには、次の手順に従って WAAS Central Manager に E メール サーバ 設定を構成する必要があります。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　E メール サーバ設定を構成する WAAS Central Manager デバイスの横にある [Edit] アイコンをクリックします。

（注）　SMTP メール サーバだけがサポートされています。他の種類のメール サーバを設定した場合、E メール通知は失敗します。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [Email Notification Server] を選択します。[Configure Email Server Details] ウィンドウが表示されます

ステップ 4　[Mail Server Hostname] フィールドに、E メール送信に使用される SMTP E メール サーバのホスト名を入力します。

ステップ 5　[Mail Server Port] フィールドに、ポート番号を入力します。デフォルトは、ポート 25 です。

ステップ 6　[Server Username] フィールドに、有効な E メール アカウントのユーザ名を入力します。

ステップ 7　[Server Password] フィールドに、E メール アカウントのパスワードを入力します。

ステップ 8　[From Address] フィールドに、E メール通知の送信者として表示される E メール アドレスを入力します。

ステップ 9　[Submit] をクリックします。

CHAPTER 10

WAE Device Manager GUI の使用方法

この章では、Wide Area Application Services（WAAS）Central Manager GUI とは異なるインターフェイスである WAE Device Manager GUI を使用する方法について説明します。WAE Device Manager は、ネットワーク内の個々の WAE デバイスを制御し、モニタできる Web ベースの管理インターフェイスです。WAAS Central Manager デバイスには、WAE Device Manager インターフェイスがありません。多くの場合、WAE Device Manager と WAAS Central Manager GUI の両方に同じデバイス設定が存在します。そのため、できるだけ WAAS Central Manager GUI からデバイス設定を構成することを推奨します。

WAE Device Manager でデバイス設定を変更すると、変更は WAAS Central Manager に伝搬され、そのデバイスのグループ設定を上書きします。あとで WAE Device Manager から構成した設定をグループ設定で上書きしたい場合は、WAAS Central Manager GUI のグループ上書き機能を使用できます。詳細については、「グループ設定の変更」（P.3-8）を参照してください。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

WAE Device Manager の起動

各 WAAS デバイスは、WAE Device Manager の Web ベースのインターフェイスを使用して個別に管理します。WAE Device Manager は、Internet Explorer を使用して、WAAS ネットワークの任意の場所からリモートで起動できます。

WAE Device Manager を起動するには、次のいずれかの方法を使用します。

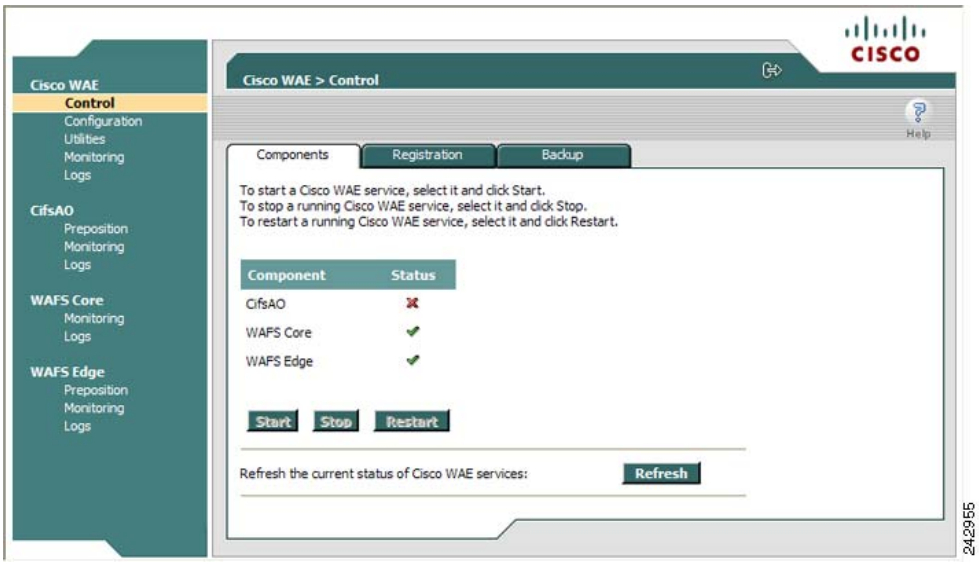
- https://*Device_IP_Address*:8443/mgr にアクセスします。

  WAE Device Manager の [Login] ウィンドウが表示されます。提供されたフィールドにユーザ名とパスワードを入力し、[Login] をクリックします。デフォルトのユーザ名は admin、パスワードは default です。

- WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択し、管理したいデバイスの横にある [Edit] アイコンをクリックし、ウィンドウの一番下にある [Device GUI] ボタンをクリックします。

WAE Device Manager インターフェイスが表示されます（図 10-1 を参照）。

図 10-1　WAE Device Manager インターフェイス



WAE Device Manager の概要

WAE Device Manager は、2 つのセクションに分かれています。左側の領域には、ナビゲーション領域が表示されます。右側の領域には、ナビゲーション領域から選択したオプションに関する情報が表示されます。

ナビゲーション領域を使用すると、さまざまな WAE コンポーネント用の管理画面をナビゲートできます。ナビゲーション領域には、次のオプションがあります。

- [Cisco WAE]：WAE コンポーネントの起動と停止、WAE の登録と登録解除、設定ファイルのバックアップと復元、およびさまざまな WAE ユーティリティの使用が可能です。詳細については、「Cisco WAE の管理」（P.10-4）を参照してください。

- [CifsAO]：事前配置作業のモニタ、WAFS デバイス統計情報の表示、およびログの表示が可能です。詳細については、「CIFS アクセラレータ デバイスの管理」（P.10-19）を参照してください。

  CifsAO オプションは、この WAAS デバイスで透過的 CIFS アクセラレータが有効となっている場合にだけ表示されます。詳細については、「グローバル最適化機能の有効化と無効化」（P.12-2）を参照してください。

- [WAFS Core]：WAFS Core 統計情報のモニタおよびログ情報の表示が可能です。詳細については、「WAFS Core デバイスの管理」（P.10-22）を参照してください。

  [WAFS Core] オプションは、この WAAS デバイスがレガシー WAFS モードでコア デバイスとして設定されている場合にだけ表示されます。詳細については、第 11 章「WAFS の設定」を参照してください。

- [WAFS Edge]：事前配置作業のモニタ、WAFS Edge 統計情報のモニタ、およびログ情報の表示が可能です。詳細については、「WAFS Edge デバイスの管理」（P.10-23）を参照してください。

  [WAFS Edge] オプションは、この WAAS デバイスがレガシー WAFS モードでエッジ デバイスとして設定されている場合にだけ表示されます。詳細については、第 11 章「WAFS の設定」を参照してください。

ナビゲーション領域のオプションには、選択すると表示領域に追加タブを表示するサブオプションがあります。表示領域の必須フィールドには、アスタリスク（*）が付いています。必須フィールドに値を入力せずに [Save] をクリックすると、エラー メッセージが表示されます。エラーが発生したウィンドウへ戻るには、[Back] リンクをクリックします。

表に表示された情報は、列見出しをクリックして並び替えることができます。もう一度見出しをクリックすると、情報が逆の順序で並べ替えられます。

WAE Device Manager 内をナビゲートするとき、現在の位置が常に表示領域の一番上に表示されます。

WAE Device Manager からログアウトするには、表示領域の右上部にある  アイコンをクリックします。

（注）　WAE Device Manager を使用するには、ブラウザで JavaScript、クッキー、およびポップアップ ウィンドウを有効にする必要があります。

WAE 管理作業のフロー

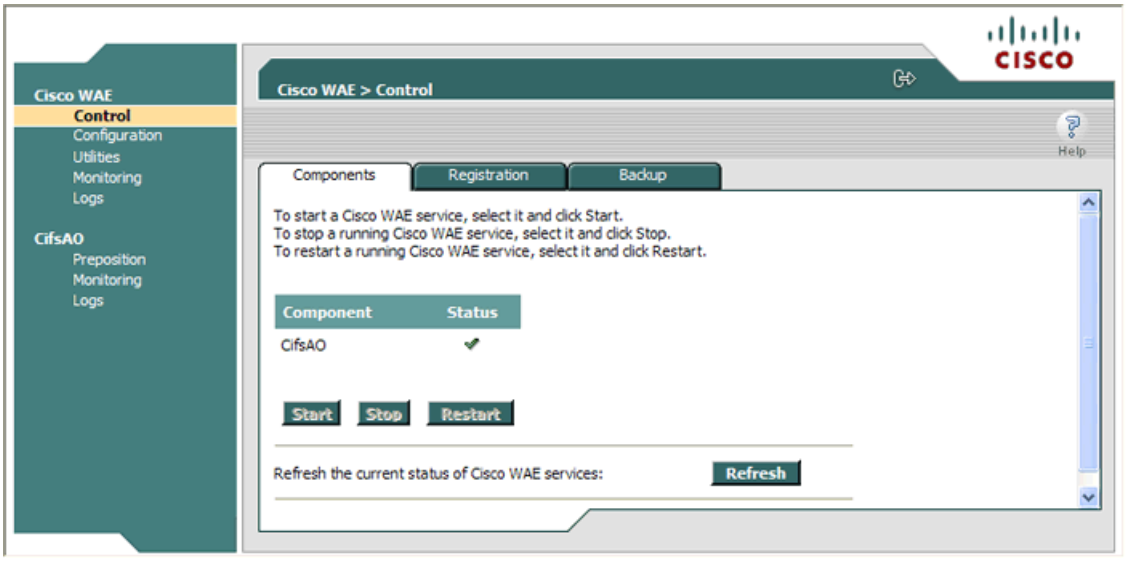
（『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って）WAE を配置し、登録したあとで、WAE Device Manager を使用して次の処理を実行します。

- 「コンポーネントの起動と停止」（P.10-5）の説明に従って、コンポーネントを起動し、停止します。
- 「WAE の登録と登録解除」（P.10-6）の説明に従って、WAE を登録し、登録を解除します。
- 「設定ファイルのバックアップ」（P.10-7）の説明に従って、設定ファイルをバックアップし、復元します。
- 「Windows 認証の設定」（P.10-10）の説明に従って、Windows 認証を設定します。
- 「通知設定の定義」（P.10-15）の説明に従って、コンポーネント固有の通知受信者を定義します。
- 「[Utilities] オプション」（P.10-17）の説明に従って、WAE メンテナンス ユーティリティを実行します。
- 「[Preposition] オプション」（P.10-20）の説明に従って、WAFS デバイスで実行した事前配置作業の詳細、現在の状態、および履歴を表示します。
- 「WAE のモニタリング」（P.10-23）の説明に従って、SNMP が生成する情報と各 WAE コンポーネントに関するグラフを表示します。
- 「WAE ログの表示」（P.10-32）の説明に従って、各 WAE コンポーネントに関するログを表示します。

Cisco WAE の管理

ナビゲーション領域の Cisco WAE メニュー項目を使用して、WAE コンポーネントのステータスの表示や WAE 上のコンポーネントの起動と停止などの基本的な操作を実行します。図 10-2 に、[Cisco WAE Control] ウィンドウを示します。

図 10-2　[Cisco WAE Control] ウィンドウ



[Cisco WAE] メニュー項目には、次のオプションがあります。

- [Control]：「[Control] オプション」（P.10-4）の説明に従って、WAE とそのコンポーネントを制御できます。
- [Configuration]：「[Configuration] オプション」（P.10-8）の説明に従って、基本的な設定作業を実行できます。
- [Utilities]：「[Utilities] オプション」（P.10-17）の説明に従って、WAE でさまざまなメンテナンス ユーティリティを実行できます。
- [Monitoring]：「WAE のモニタリング」（P.10-23）の説明に従って、WAE の CPU およびディスク使用率に関する表とグラフを表示できます。
- [Logs]：「WAE ログの表示」（P.10-32）の説明に従って、さまざまな WAE サブシステムに関するイベント ログを表示できます。

[Control] オプション

[Control] オプションは、次のタブを表示します。

- [Components]：各 WAE コンポーネントの動作ステータスを表示できます。任意のコンポーネントを起動、停止、および再起動できます。詳細については、「コンポーネントの起動と停止」（P.10-5）を参照してください。
- [Registration]：WAAS Central Manager で WAE を登録したり、WAE の登録を解除したりできます。詳細については、「WAE の登録と登録解除」（P.10-6）を参照してください。

- [Backup]：WAE 設定ファイルをダウンロードして保存し、必要に応じてこれらのファイルを WAE に復元できます。詳細については、「設定ファイルのバックアップ」（P.10-7）および「設定ファイルの復元」（P.10-7）を参照してください。

コンポーネントの起動と停止

[Components] タブを使用すると、どのコンポーネントが動作していて、どのコンポーネントが動作していないかを表示し、コンポーネントを起動、停止、および再起動できます。

このタブから [Refresh] をクリックすると、各コンポーネントのステータスをアップデートし、WAE Device Manager インターフェイスをアップデートして、WAAS Central Manager GUI からデバイスに行った最近の変更を反映できます。たとえば WAE Device Manager にログインするとき、デバイスを透過的 CIFS アクセラレータに設定すると、[Refresh] をクリックするか、再び WAE Device Manager にログインするまで、この変更は反映されません。

（注）　コンポーネントが動作していない場合、そのほとんどの設定をオフラインで実行できます。ただし、コンポーネントに行った設定変更は、再起動するまで反映されません。

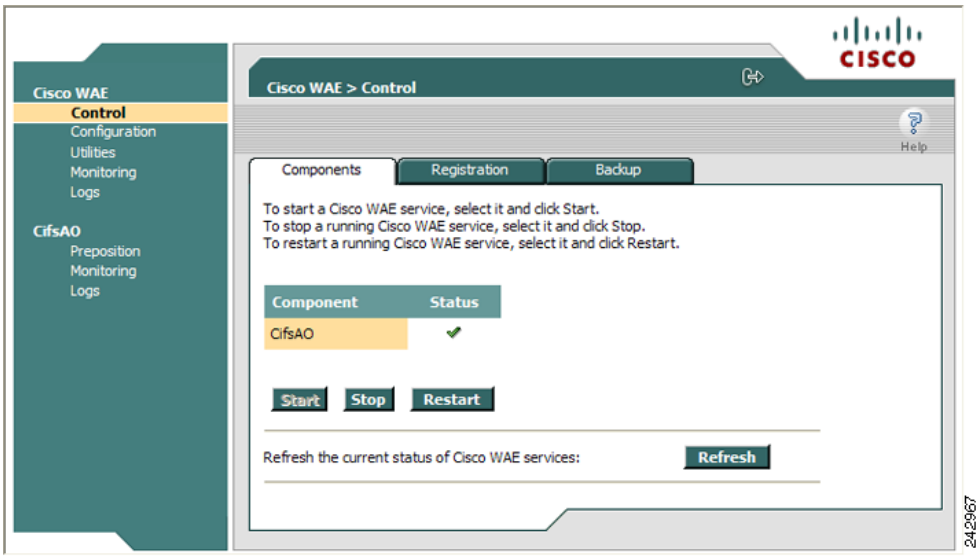
（注）　デバイスが WAAS Central Manager に登録されていない場合は、コンポーネントを起動または停止しないでください。

コンポーネントを起動および停止するには、次の手順に従ってください。

ステップ 1　[Cisco WAE Control] ウィンドウの [Components] タブで、アクティブにしたいコンポーネントを選択し、[Start] をクリックします。

数秒後に図 10-3 に示されたように、選択したコンポーネントの横に、そのステータスが動作中であることを示す緑色のチェックマーク ✔ が表示されます。

図 10-3　[Components] タブ：コンポーネントの起動



- コンポーネントを停止するには、リストからコンポーネントを選択し、[Stop] をクリックします。

数秒後に、選択したコンポーネントの横に、動作していないことを示す赤色の ✖ が表示されます。

- WAE コンポーネントを再起動するには、リストからコンポーネントを選択し、[Restart] をクリックします。
- WAE コンポーネントの現在の状態を表示するには、[Refresh] をクリックします。

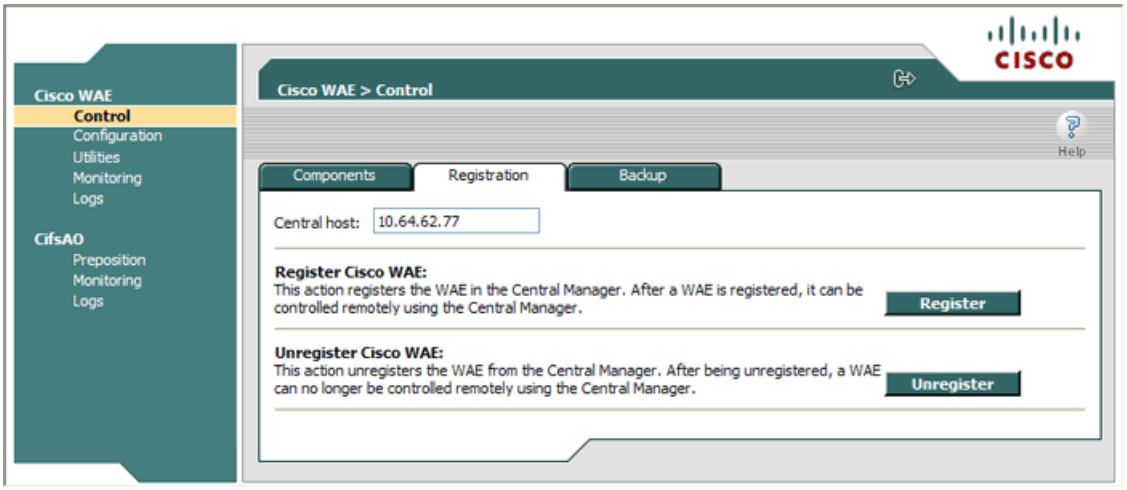
WAE の登録と登録解除

[Registration] タブを使用すると、指定した WAAS Central Manager に WAE を登録したり、WAE の登録を解除したりできます。WAE を登録すると、WAAS Central Manager GUI から WAE を表示し、管理できます。

WAE を登録するには、次の手順に従ってください。

ステップ 1　[Cisco WAE Control] ウィンドウで、[Registration] タブをクリックします（図 10-4 を参照）。

図 10-4　[Cisco WAE Control]：[Registration] タブ



ステップ 2　[Central Host] フィールドで、WAAS Central Manager のアドレスが表示されることを確認します。このフィールドにアドレスが表示されない場合、WAE は Central Manager に登録されていません。

ステップ 3　[Register] をクリックして、WAE を登録します。

「Registration will update the WAE properties in the WAAS Central Manager.Are you sure?」というメッセージが表示されます。[OK] をクリックします。成功すると、「Appliance registered successfully」メッセージが表示されます。

ステップ 4　[Unregister] をクリックして、Cisco WAE の登録を解除します。

成功すると、「Appliance unregistered successfully」メッセージが表示されます。

（注）　WAE の登録を解除すると、WAAS Central Manager GUI で WAE に対して定義されているすべてのポリシーが削除されます。

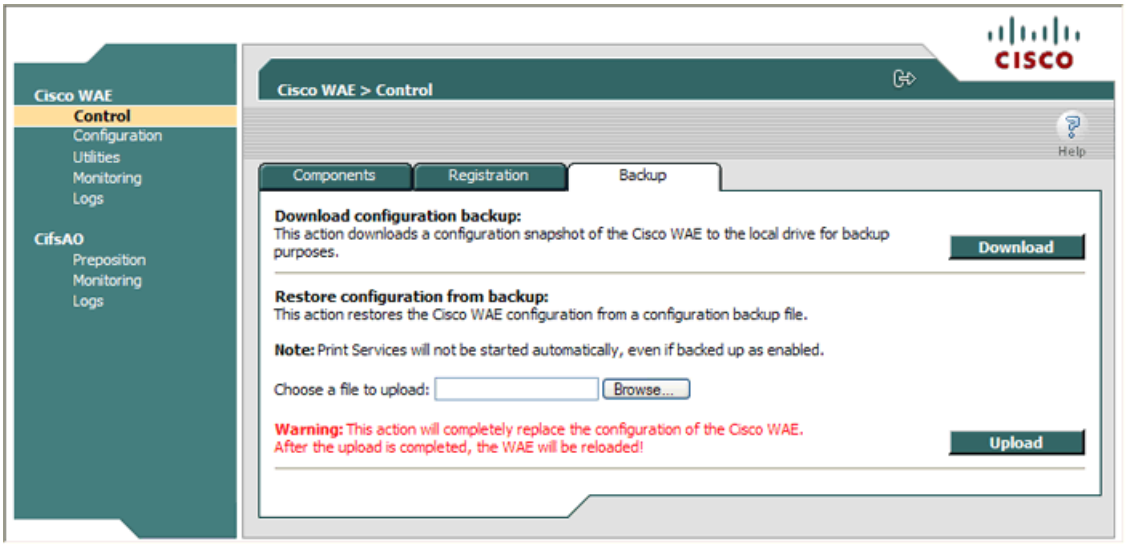
設定ファイルのバックアップ

[Backup] タブを使用すると、WAE の設定ファイルをバックアップおよび復元できます。

WAE 設定をバックアップするには、次の手順に従ってください。

ステップ 1　[Cisco WAE Control] ウィンドウで、[Backup] タブをクリックします（図 10-5 を参照）。

図 10-5　[Cisco WAE Control] : [Backup] タブ



ステップ 2　[Download configuration backup] 領域で、[Download] をクリックします。

ステップ 3　[File Download] ウィンドウで、[Save] をクリックします。

ステップ 4　[Save As] ウィンドウで、ファイルを保存したい位置まで移動します。また、ファイル名を変更することもできます。

ステップ 5　[Save] をクリックします。

WAE 設定ファイルが、選択した送信先フォルダへダウンロードされ、1 つの圧縮ファイルで保存されます。

バックアップからファイルを復元する方法については、「設定ファイルの復元」（P.10-7）を参照してください。

設定ファイルの復元

[Backup] タブを使用すると、WAE の設定ファイルを復元できます。設定を復元すると、WAE はバックアップを実行する前の状態へ戻ります。

設定ファイルを復元するには、次の手順に従ってください。

ステップ 1　[Restore configuration from backup] 領域から、[Browse] をクリックして、復元したいバックアップファイルの位置までナビゲートします。

ステップ 2　[Upload] をクリックして、選択した設定ファイルを復元します。

（注）　アップロードが完了すると、WAE がリロードされます。

[Configuration] オプション

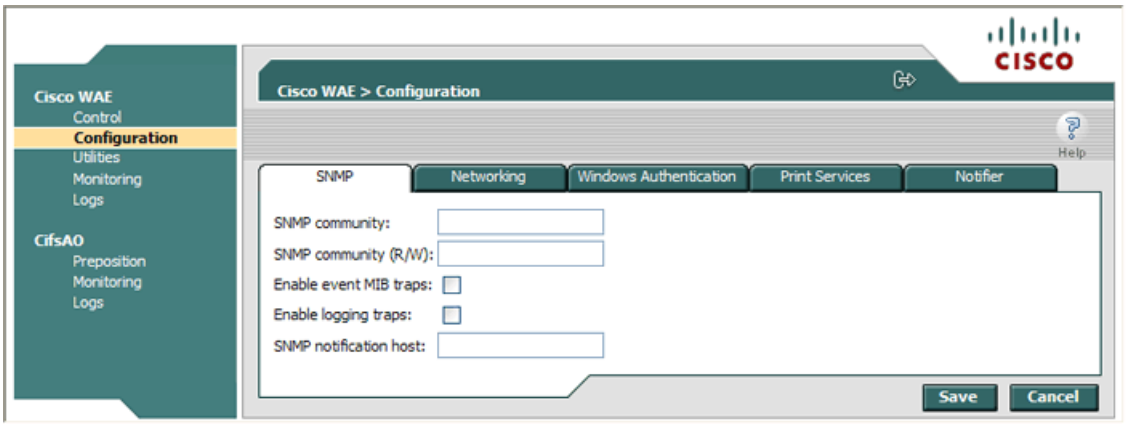
[Cisco WAE] メニュー項目の [Configuration] オプションは、次のタブを表示します。

- [SNMP]：WAE でイベント MIB とロギング トラップを有効にできます。詳細については、「SNMP 設定の構成」（P.10-8）を参照してください。
- [Networking]：デバイスの初期設定時に定義された WAE 設定（『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照）を表示できます。詳細については、「ネットワーク設定の表示」（P.10-9）を参照してください。
- [Windows Authentication]：Windows 認証でデバイス ログイン、切断モード、および CLI 設定を有効にするために WAE で必要な設定を定義できます。詳細については、「Windows 認証の設定」（P.10-10）を参照してください。
- [Print Services]：印刷サービスを設定できます。印刷サービスの設定の詳細については、第 13 章「WAAS レガシー印刷サービスの設定および管理」を参照してください。
- [Notifier]：WAE によりアラートが生成されたときに通知を送信する電子メール アドレスを定義できます。詳細については、「通知設定の定義」（P.10-15）を参照してください。

SNMP 設定の構成

[SNMP] タブを使用すると、Cisco WAE で SNMP 設定を構成できます。SNMP 設定を構成するには、[Configuration] ウィンドウの [SNMP] タブをクリックします。[SNMP] タブが表示されます（図 10-6 を参照）。

図 10-6　[WAE Configuration]：[SNMP] タブ



このタブでは、次の設定を構成できます。

- [SNMP community]：WAE の SNMP エージェントにアクセスするときに認証用のパスワードとして使用する、読み取りアクセス用の SNMP コミュニティ ストリングを設定します。

- [SNMP community (R/W)] : WAE の SNMP エージェントにアクセスするときに認証用のパスワードとして使用する、読み取りまたは書き込みアクセス用の SNMP コミュニティ ストリングを設定します。
- [Enable event MIB traps] : WAE は、[SNMP notification host] フィールドに指定された SNMP ホストにイベント MIB トラップを送信できます。
- [Enable logging traps] : デバイスのロギング トラップを有効にします。
- [SNMP notification host] : WAE が MIB およびロギング トラップをホストへ送信できるように、SNMP ホストの IP アドレスまたはホスト名を入力します。

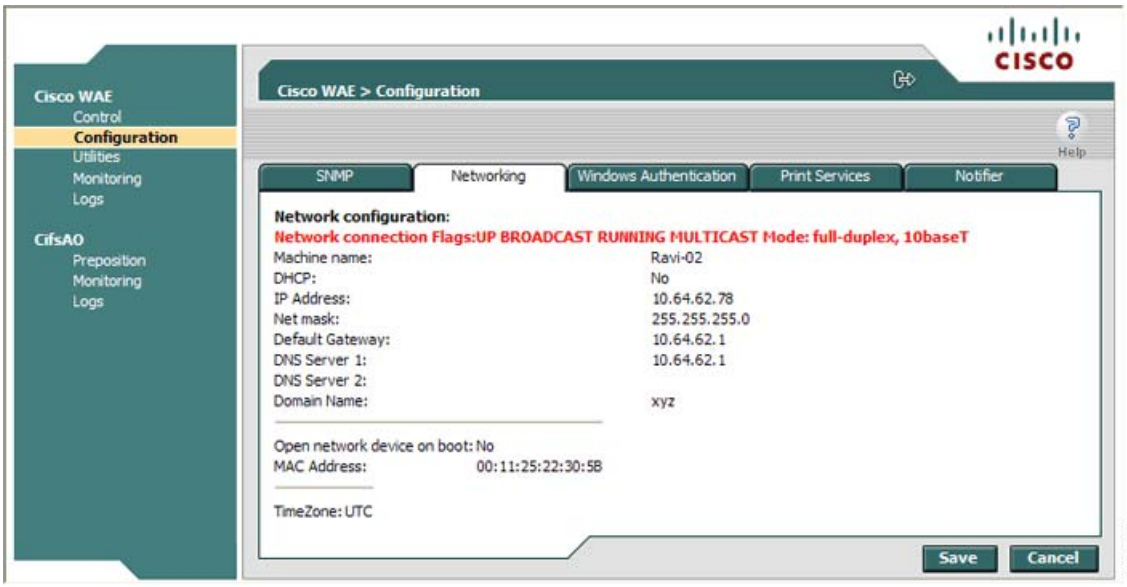
このページで変更を行ったあとで [Save] をクリックするか、[Cancel] をクリックして変更を取り消します。

ネットワーク設定の表示

[Networking] タブ（図 10-7 を参照）を使用すると、WAE と LAN 間の接続パラメータを表示できます。

WAE 接続設定を表示するには、[Configuration] ウィンドウの [Networking] タブをクリックします。

図 10-7　[Cisco WAE Configuration] : [Networking] タブ



[Networking] タブには、次の情報が含まれます。

- ネットワーク接続フラグ：ネットワーク ステータス フラグ
- モード：デュプレクスおよび接続速度
- [Machine name] : WAE のホスト名
- [DHCP] : ネットワークで DHCP サーバが使用できるかどうか
- [IP Address]
- [Net mask]
- [Default Gateway]
- [DNS Server 1]

- [DNS Server 2]
- [Domain Name]
- [MAC Address]
- [Time Zone]

Windows 認証の設定

WAAS Central Manager GUI と WAE Device Manager は、Pluggable Authentication Module（PAM; プラグイン可能な認証モジュール）を使用してユーザ ログインを認証します。WAAS Central Manager GUI で定義した管理ユーザは、WAE Device Manager へ配信されます。管理ユーザ認証は、WAAS Central Manager GUI または WAE Device Manager へのログイン時にだけ実行されます。各 WAE にはデフォルトの GUI および CLI ユーザがあり、そのユーザ名は admin、パスワードは default です。このユーザ アカウントは削除できませんが、パスワードは変更できます。

（注）　CLI ユーザ アカウント情報と管理 GUI 設定が一致しない場合は、設定配信時に管理 GUI 設定が一致しないすべての CLI ユーザ アカウント情報を更新します。CLI ユーザ アカウント設定を構成すると、ユーザにこの動作を通知する警告が CLI ユーザに表示されます。

ここでは、次の内容について説明します。

ローカル データベースを使用したログイン認証および許可について

ローカル ユーザ認証および許可は、ローカルで設定されたユーザ名とパスワードを使用して、管理ユーザ ログインの試行を認証します。ログインとパスワードは、各 WAE に対してローカルです。

デフォルトで、ローカル ユーザ ログイン認証が、プライマリ認証方式として有効になります。ローカル ユーザ ログイン認証は、他の 1 つまたは複数の管理ログイン認証方式を有効にした後でだけ無効にできます。ただし、ローカル ユーザ ログイン認証を無効にすると、その他のすべての管理ログイン認証方式が無効になった場合に、ローカル ユーザ ログイン認証は自動的に再度有効になります。

Windows ドメイン認証は、別のユーザ ログイン認証方式です。コンソール、Telnet、FTP、SSH、または HTTP（WAFS Central Manager および WAE Device Manager のインターフェイス）を使用して、Windows ドメイン ユーザを認証できます。

サポートされている認証方式

WAE で Windows 認証を有効にすると、ドメイン コントローラに登録するときのユーザ、WAE、およびサービスの認証プロセスの安全性を強化する追加設定を構成できます。

WAFS は、WAE で次の Windows 認証方式をサポートしています。

- NTLMv2 認証：ほとんどの Windows オペレーティング システムに組み込まれている Windows 認証プロトコル
- Kerberos：秘密キー暗号方式を使用し、Windows 2003 Server に組み込まれている Windows 認証プロトコル

（注）　Windows ドメイン認証は、WAAS デバイスに Windows ドメイン サーバが設定されていない限り、実行されません。デバイスが正しく登録されていない場合、認証と許可は実行されません。WAAS は、Windows Server 2000 または Windows Server 2003 だけで稼動している Windows ドメイン コントローラによる認証をサポートします。

NTLM 認証を使用している場合は、Windows 2000 よりも前のオペレーティング システムをサポートするオプションを使用して Windows ドメイン サーバをインストールする必要があります（Windows サーバの dcpromo ウィザードの [installation Permissions] 画面で、[Permissions compatible with pre-Windows 2000 server operating systems.] を選択します）。

LDAP サーバ署名

Lightweight Directory Access Protocol（LDAP）サーバ署名は、Microsoft Windows Server のネットワーク セキュリティ設定の設定オプションです。このオプションは、WAE などの LDAP クライアントの署名要件を制御します。LDAP 署名は、LDAP パケットがネットワークの途中で改変されていないことを確認し、パッケージ データが既知の送信元から送信されたことを保証するために使用されます。

WAAS ソフトウェアでは、ドメイン セキュリティ ポリシー用の LDAP サーバ署名要求オプションが「Require signing（署名が必要）」に設定されている場合に、Windows 2003 ドメインでの印刷サービスとログイン認証の両方がサポートされます。LDAP サーバ署名機能により、WAE はドメインに参加してユーザを安全に認証できます。

（注）　LDAP 署名を要求するように Windows ドメイン コントローラを設定するときは、CLI から **smb-conf section "global" name "ldap ssl" value "start_tls"** グローバル コンフィギュレーション コマンドを使用して、WAE 上の LDAP サーバ署名も設定する必要があります。このオプションは、WAE Device Manager インターフェイスを使用して有効にできません。**smb-conf** コマンドを使用する方法については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

Windows 認証の設定

[Windows Authentication] タブを使用すると、WAE 上のセキュリティ設定を構成できます。

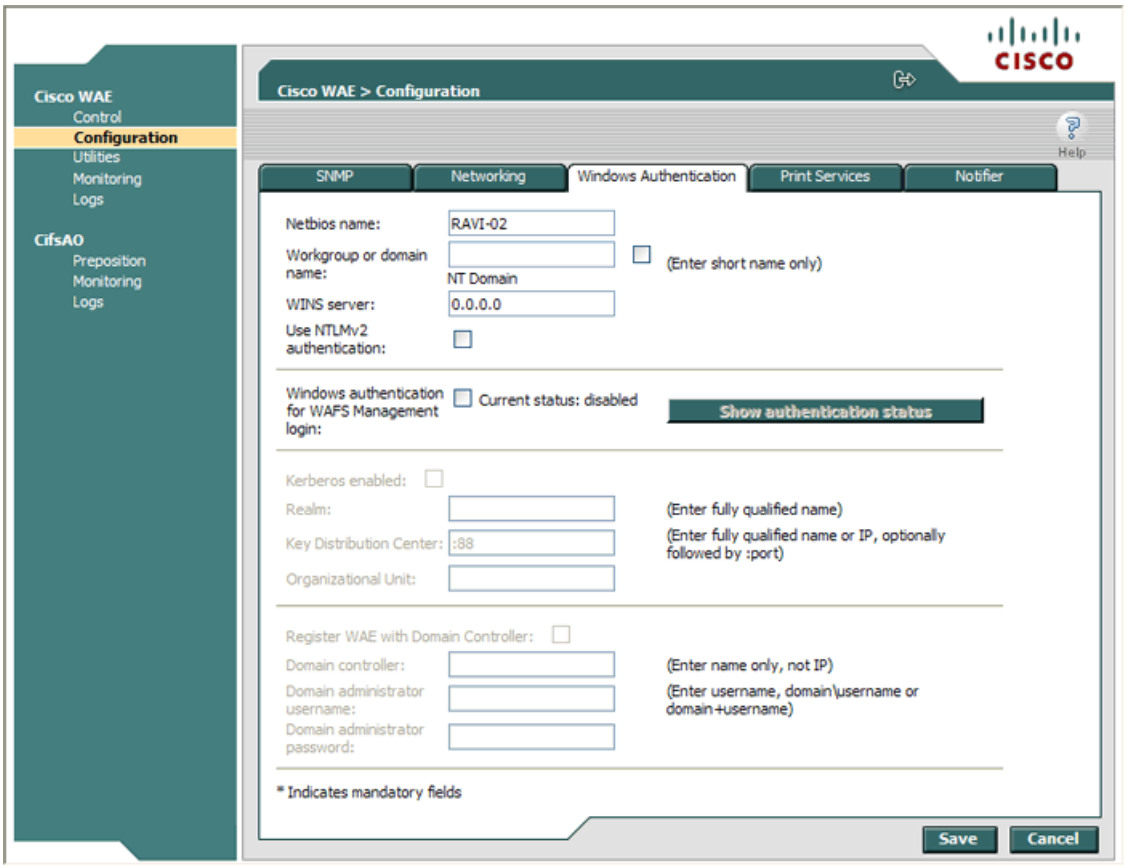
Windows 認証を設定するには、次の手順に従ってください。

ステップ 1　WAE Device Manager にログインします。

ステップ 2　[Configuration] ウィンドウで、[Windows Authentication] タブをクリックします。

[Window Authentication] ウィンドウが表示されます（図 10-8 を参照）。

図 10-8　[Cisco WAE Configuration]：[Windows Authentication] タブ



ステップ 3　NetBIOS 名を入力します。

NetBIOS 名は 15 文字以内であり、特殊文字を使用できません。

（注）　デフォルトで、[NetBIOS name] フィールドには自動的にファイル エンジンのホスト名が入力されます。このホスト名が変化しても、NetBIOS フィールドは自動的に新しい名前にアップデートされません。

ステップ 4　ワークグループまたはドメイン名を短縮名形式で入力し、ワークグループまたはドメインが Windows NT 4 ドメインである場合は、[NT Domain] チェックボックスを選択します。

たとえば、ドメイン名が cisco.com の場合、短縮形は cisco です。ワークグループまたはドメインが Windows 2000 または Windows 2003 ドメインの場合は、[NT Domain] チェックボックスを*選択しない*でください。

[NT Domain] チェックボックスを選択すると、ドメイン名と短縮名形式にピリオド（.）を使用できますが、NT ドメインの完全修飾名を入力しないように注意してください。

ステップ 5　使用している Windows Internet Naming Service（WINS）サーバの IP アドレスまたはホスト名を入力します。

ステップ 6　[Use NTLMv2 authentication] チェックボックスを選択して、NTLMv2 認証を有効にします。

（注）　すべてのクライアントのセキュリティ ポリシーが「Send NTLMv2 responses only/Refuse LM and NTLM」に設定されている場合にだけNTLMv2 サポートを有効にしてください。クライアントで NTLM v2 が必要ない場合に NTLM v2 を使用すると、認証に失敗することがあります。

ステップ 7　[Windows authentication for WAFS Management login] チェックボックスを選択し、Windows ドメインを使用して、WAFS への Telnet、FTP、コンソール、SSH、およびユーザ インターフェイス（WAAS Central Manager GUI および WAE Device Manager）ログインを認証します。

WAAS Central Manager GUI を使用してユーザを追加するときは、ログイン パスワードが WAE に保存されているローカル ユーザとしてユーザを設定することができます。ローカル ユーザは WAE によって認証されますが、ローカルでないユーザは一般に Windows ドメイン認証を使用して確認されます。

ステップ 8　Kerberos 認証を使用している場合は、[Kerberos enabled] チェックボックスを選択し、次の情報を指定します。

- Kerberos 領域の完全修飾名。すべての Windows 2000 ドメインは Kerberos 領域ですが、領域名は常にドメイン名をすべて大文字にしたバージョンです。
- Key Distribution Center（KDC; キー発行局）の完全修飾名または IP アドレス。また、「*ip address*」または「*name:port number*」という形式でポート番号を指定することもできます。たとえば、「10.10.10.2:88」のようになります。
- 組織単位。

ステップ 7 で説明した 1 つ以上のボックスを選択しないと、Kerberos 認証を有効にできません。Kerberos の有効後に、WAE のクロックとドメイン コントローラのクロックの差が 5 分以内であることを確認します。そうでない場合は、ドメイン コントローラは、認証に Kerberos を使用しません。

Windows 2000（SP4 搭載）または Windows 2003（SP1 搭載）ドメイン コントローラを使用している場合は、Kerberos 認証を有効にする必要があります。

ステップ 9　LDAP サーバ署名を要求するようにドメイン コントローラを設定した場合は、WAAS CLI で **smb-conf section global name "ldap ssl" value "start_tls"** グローバル コンフィギュレーション コマンドを使用して、WAE 上の LDAP サーバ署名を有効にする必要があります。**smb-conf** コマンドを使用する方法については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

ステップ 10　[Register WAE with Domain Controller] チェックボックスを選択します。

（注）　Kerberos を有効または無効にするときは、WAE をドメイン コントローラに登録し、Windows 認証を有効にするか、NetBIOS 名、ワークグループ、または Kerberos 領域を変更する必要があります。

チェックボックスの下に、一連のフィールドが表示されます。これらのフィールドに次の情報を入力します。

- ドメイン コントローラ（IP アドレスでなく、名前を入力します）

  Kerberos が無効になっている場合にだけ、ドメイン コントローラの NetBIOS 名を入力できます。Kerberos が有効になっている場合は、ドメイン コントローラの完全修飾ドメイン名を入力できます。
- ドメイン管理者ユーザ名（ユーザ名、ドメイン¥ユーザ名、またはドメイン＋ユーザ名を入力します）
- ドメイン管理者パスワード

ステップ 11　[Save] をクリックします。

Windows 認証設定が保存され、WAE がドメイン コントローラに登録されます。

ステップ 12　Windows 認証が正しく動作していることを確認します。「Windows 認証ステータスの確認」（P.10-14）を参照してください。

Windows 認証ステータスの確認

Windows 認証を有効にしたら、Windows 認証ステータスを確認し、認証問題の解決に有用な組み込みテストの結果を表示できます。

「Windows 認証の設定」（P.10-11）で説明されている設定を正しく行わないと、Windows 認証問題が発生することがあります。また、ドメイン コントローラの設定が変わった場合も、問題が発生することがあります。

[Authentication Details] ウィンドウは、次の情報を表示します。

- winbind 認証テストのリスト
- 各テストの結果
- 合格または不合格の表示
- テスト不合格の理由を調べるのに役に立つトラブルシューティングのヒント

Windows 認証ステータスを確認するには、次の手順に従ってください。

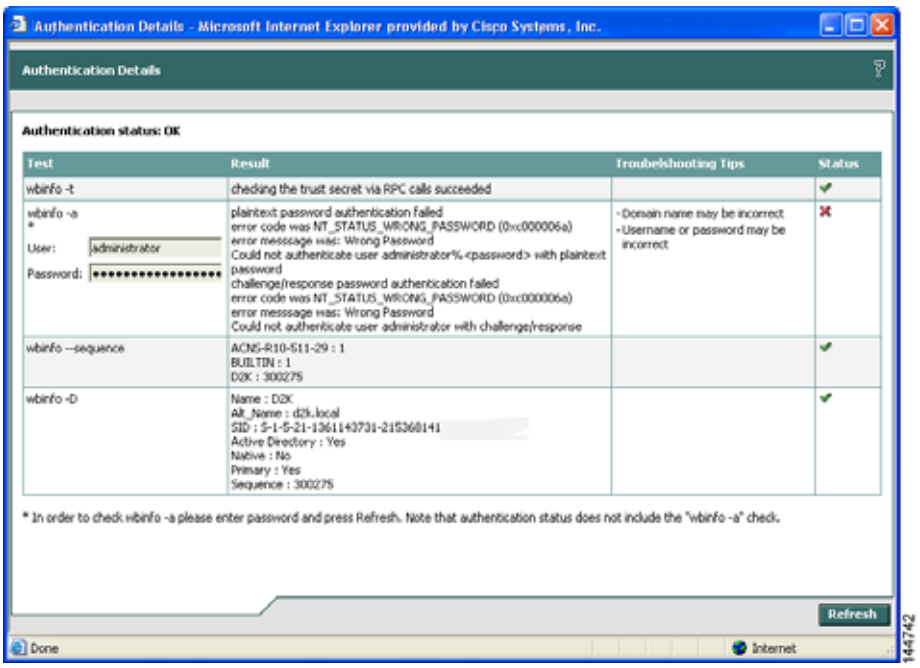
ステップ 1　[Windows Authentication] タブで、[Show authentication status] をクリックします。

認証ステータスが表示されるまでに時間がかかり、認証ステータスを取得するときに WAE のパフォーマンスが低下する場合があることを説明するメッセージが表示されます。

ステップ 2　メッセージ ダイアログボックスで、[OK] をクリックして続行するか、[Cancel] をクリックして認証詳細の表示を取り消します。

[OK] をクリックすると、[Authentication Details] ウィンドウが表示されます（図 10-9 を参照）。

図 10-9　[Authentication Details] ウィンドウ



ステップ 3　ウィンドウの一番上にある [Authentication status] フィールドを確認します。

[status] フィールドに「OK」が表示されている場合、Windows 認証は正しく機能しています。このフィールドに「Not OK」が表示されている場合は、次の手順に進みます。

ステップ 4　各テストのステータスを表示し、提供されるトラブルシューティングのヒントを使用して問題を解決します。

表 10-1 で、これらのテストについて説明します。

表 10-1　認証テストの説明

テスト	説明
wbinfo -t	Samba サーバが Windows ドメインに追加されるときに作成されるワークステーション信用アカウントが動作していることを確認します。
wbinfo -a	指定したユーザ名とパスワードに基づいてドメイン クレデンシャルをテストします。このテストを実行するには、適切なユーザ名とパスワードを入力し、[Refresh] をクリックします。テスト結果が表示されるのを待ちます。
wbinfo -D	ドメインに関する Samba からの情報を表示します。
wbinfo --sequence	すべての既知のドメインのシーケンス番号を表示します。
Time skew	WAE と KDC サーバ間の時間オフセットを表示します。時間オフセットは 5 分以内でなければなりません。そうでない場合、Windows KDC サーバは、認証に Kerberos を使用しません。WAAS CLI を使用して、WAE 上の時間を設定できます。 このテストは、Kerberos 認証が有効になっている場合にだけ実行されます。

ステップ 5　[Refresh] をクリックして、すべてのテストが正常に完了することを確認します。

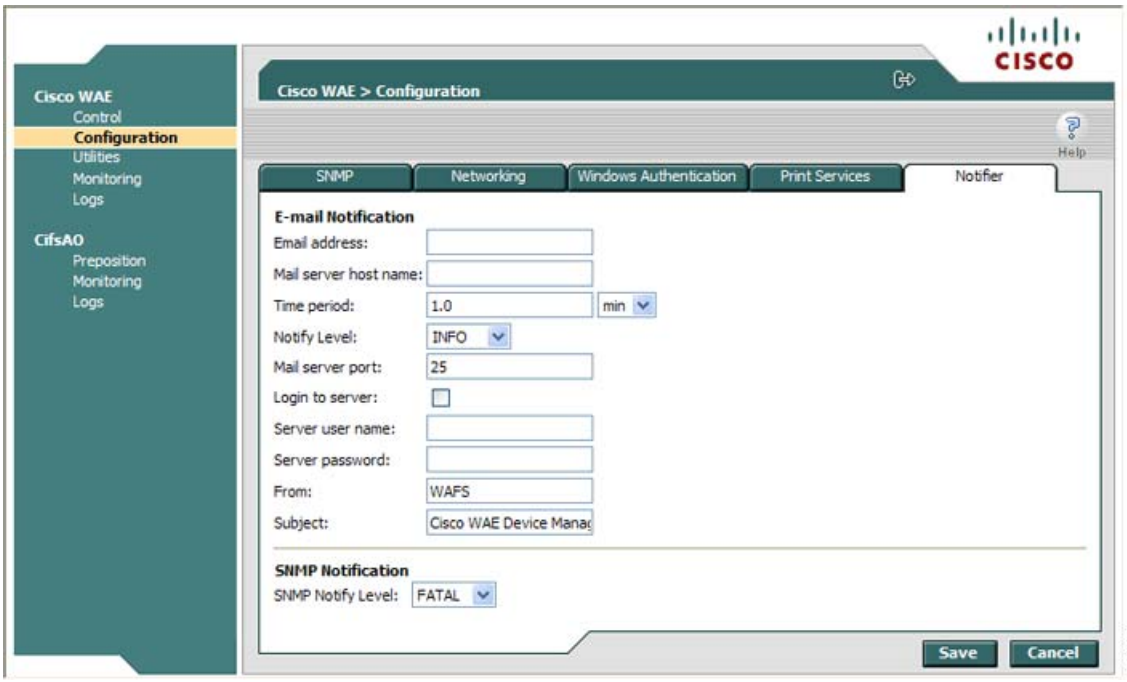
通知設定の定義

[Notifier] タブを使用すると、WAE がアラートを生成したときに通知を送信する電子メール アドレスを定義できます。

通知設定を定義するには、次の手順に従ってください。

ステップ 1　[Configuration] ウィンドウで、[Notifier] タブをクリックします（図 10-10 を参照）。

図 10-10　[Notifier] タブ



ステップ 2　[Email address] フィールドに、この WAE に関する通知を送信するアドレスを入力します。

ステップ 3　[Mail server host name] フィールドに、メール サーバ ホストの名前を入力します。

ステップ 4　[Time period] フィールドに、電子メールを送信するまでに通知を収集する時間を入力し、ドロップダウン リストから関連する時間単位（[min] または [sec]）を選択します。

ステップ 5　[Notify Level] ドロップダウン リストから、通知を生成するための最小イベント重大度を選択します。

ステップ 6　[Mail server port] フィールドに、メール サーバに接続するためのポート番号を入力します。

ステップ 7　通知を送信するために WAE がメール サーバにログインする必要がある場合は、[Login to server] チェックボックスを選択します。このオプションを選択すると、追加フィールドが有効になります。

ステップ 8　[Server username] フィールドに、メール サーバにアクセスするためのユーザ名を入力します。

ステップ 9　[Server password] フィールドに、メール サーバにアクセスするためのパスワードを入力します。

ステップ 10　[From] フィールドに、各電子メール通知の [From] フィールドに表示する文面を入力します。

ステップ 11　[Subject] フィールドに、各通知の標題として表示する文面を入力します。

ステップ 12　[SNMP Notify Level] ドロップダウン リストから、SNMP 通知を生成するための最小イベント重大度を選択します。

ステップ 13　[Save] をクリックします。

[Utilities] オプション

[Utilities] オプションは、次のタブを表示します。

- [Support]：サポート目的で WAE データを外部の場所にダンプできます。詳細については、「サポート ユーティリティの実行」（P.10-17）を参照してください。
- [WAFS Cache Cleanup]：WAFS キャッシュからすべてのファイルを削除できます。詳細については、「Cache Cleanup ユーティリティの実行」（P.10-18）を参照してください。
- [File Server Rename]：WAFS キャッシュ内のファイル サーバの名前を変更できます。詳細については、「File Server Rename ユーティリティの実行」（P.10-19）を参照してください。

サポート ユーティリティの実行

[Support] タブには、デバイスで実行されている WAAS ソフトウェア バージョンおよびビルド番号を含む WAE に関する製品情報が表示されます。

また、[Support] タブでは、さまざまなコンポーネントの設定ログ ファイルなど、WAE とその動作の現在の状態のスナップショットを提供するシステム レポートをダウンロードできます。サポートが必要な場合、このレポートをシスコ テクニカル サポート（TAC）へ送信できます。

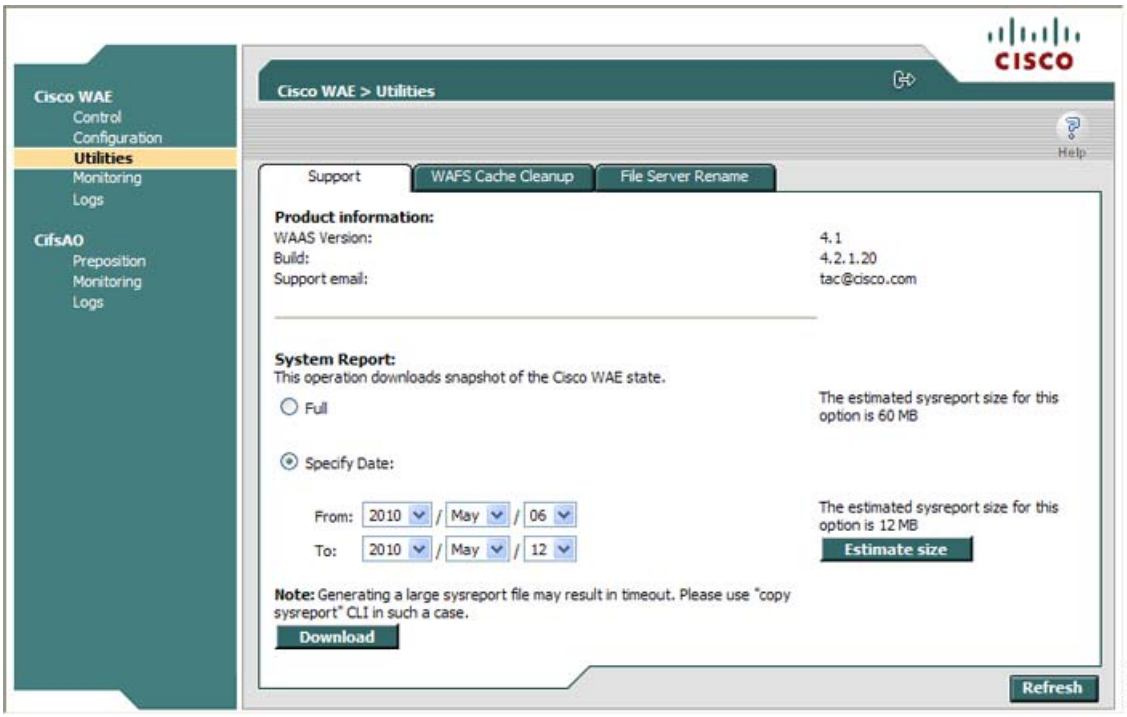
（注）　システム レポート全体をダウンロードすると、WAE のパフォーマンスに影響する場合があります。そのため、ピーク時間を避けてシステム レポートをダウンロードするか、レポートの日付範囲を制限することを推奨します。

システム レポートをダウンロードするには、次の手順に従ってください。

ステップ 1　[Utilities] ウィンドウで、[Support] タブをクリックします。

[Support] ウィンドウが表示されます（図 10-11 を参照）。

図 10-11　[Utilities]：[Support] タブ



ステップ 2　[System Report] 領域で、次のオプション ボタンのいずれかを選択します。

- [Full]：システム レポート全体をダウンロードします。
- [Specify Date]：指定した日付範囲のレポートをダウンロードします（デフォルト値は過去 7 日間）。

ステップ 3　[Estimate size] をクリックして、レポートのサイズを表示します。

レポートの実際のサイズが見積りと異なる場合があります。見積りサイズが大きい場合は、日付範囲を狭くするか、レポートを分断して、WAE の負荷を最小限に抑えることができます。

ステップ 4　[Download] をクリックします。

レポートをダウンロードすると、デバイス上のすべてのサービスのパフォーマンスに影響する場合があることを知らせるメッセージが表示されます。

ステップ 5　[OK] をクリックして、収集プロセスを開始します。

ステップ 6　[File Download] ウィンドウで、[Save] をクリックします。

ステップ 7　[Save As] ウィンドウで、ファイルを保存したい位置まで移動します（ファイル名を変更することもできます）。[Save] をクリックします。ファイルが tar gzip 形式で保存されます。

Cache Cleanup ユーティリティの実行

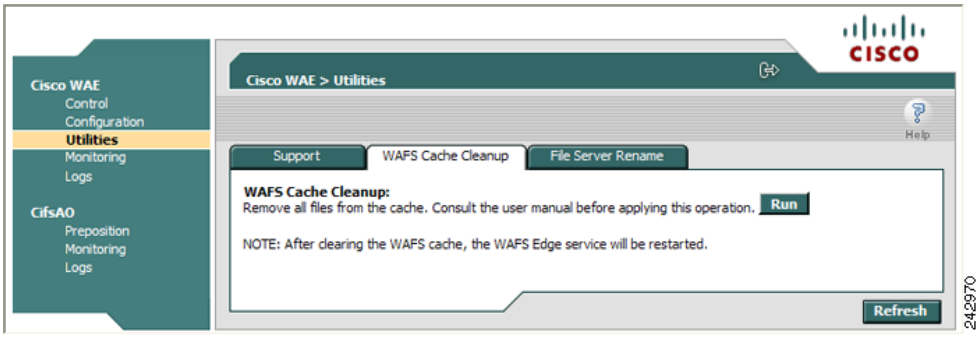
[WAFS Cache Cleanup] タブを使用すると、WAFS デバイス キャッシュからすべてのファイルを削除できます。

Cache Cleanup ユーティリティを実行するには、次の手順に従ってください。

ステップ 1　[Utilities] ウィンドウで、[WAFS Cache Cleanup] タブをクリックします。

[WAFS Cache Cleanup] ウィンドウが表示されます（図 10-12 を参照）。

図 10-12　[Utilities]：[WAFS Cache Cleanup] タブ



ステップ 2　[Run] をクリックして、キャッシュ内容を消去します。

File Server Rename ユーティリティの実行

[File Server Rename] タブを使用すると、WAAS デバイスで特定のファイル サーバ名のすべてのリソース用のリソース位置を変更できます。この機能により、WAFS キャッシュ内のファイルのファイル サーバ名が変更されます。

File Server Rename ユーティリティを実行するには、次の手順に従ってください。

ステップ 1　WAFS Edge コンポーネントが動作している場合は、「コンポーネントの起動と停止」（P.10-5）の説明に従って停止させてください。

ステップ 2　[Utilities] ウィンドウで、[File Server Rename] タブをクリックします。

ステップ 3　[Current File Server name] フィールドに、現在の名前を入力します。

ステップ 4　[New File Server name] フィールドに新しい名前を入力し、[Run] をクリックして新しい名前を有効にします。

（注）　別の既存のキャッシュされたファイル サーバの名前を [New File Server name] フィールドに指定しないでください。既存の名前を新しい名前として指定すると、このファイル サーバのキャッシュされた内容が、名前を変更するファイル サーバのキャッシュされた内容で上書きされます。

CIFS アクセラレータ デバイスの管理

ナビゲーション領域で [CifsAO] オプションを使用すると、事前配置作業のモニタ、WAFS デバイス統計情報の表示、およびログの表示が可能になります。[CifsAO] オプションは、透過的 CIFS アクセラレータ モードを使用している場合にだけ表示されます。

[CifsAO] オプションには、次のメニュー項目があります。

- [Preposition]：WAAS Central Manager GUI で作成した事前配置ポリシーの進行状況をモニタできます。さらに、オプションで事前配置作業を停止できます。詳細については、「[Preposition] オプション」（P.10-20）を参照してください。
- [Monitoring]：「Cisco WAE コンポーネントのモニタリング」（P.10-25）の説明に従って、表とグラフに WAFS デバイス統計情報を表示できます。
- [Logs]：CIFS アクセラレータに関連するイベント ログを表示できます。詳細については、「Cisco WAE ログの表示」（P.10-34）を参照してください。

[Preposition] オプション

[Preposition] オプションを使用すると、WAAS Central Manager GUI で作成された事前配置ポリシーの詳細と現在の状態を表示できます。これらのポリシーは、事前に設定したスケジュールに従って、どのファイルを事前に WAAS デバイス キャッシュに配置するかを定義します。事前配置を使用すると、システム管理者は、ピーク時間外に、頻繁にアクセスされる大型のファイルを戦略的にネットワーク エッジに配置できるため、効率が上がり、エンド ユーザがそれらのファイルに初めてアクセスする場合でも迅速にアクセスできるようになります。

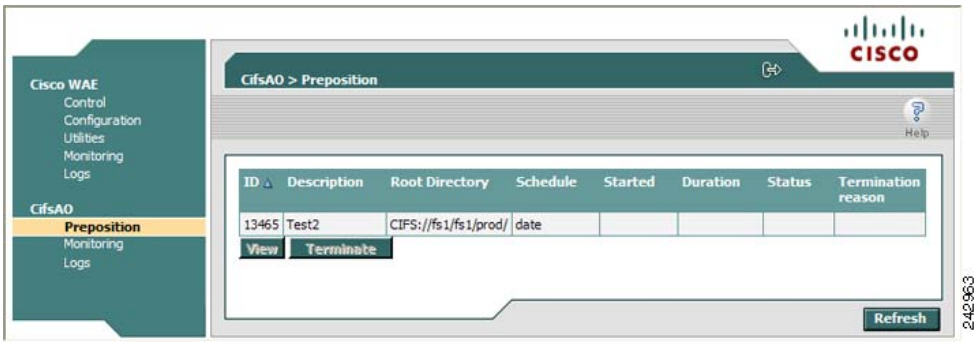
事前配置するファイルを含むルート ディレクトリ、各ポリシーのスケジュール、各ポリシーの最新の作業のステータスなどの情報を表示できます。また、各ポリシーの詳細な作業履歴を表示し、進行中の任意の作業を手動で停止できます。

このデバイス用の事前配置ポリシーを表示するには、次の手順に従ってください。

ステップ 1　ナビゲーション領域で、[Preposition] をクリックします。

[CifsAO] > [Preposition] ウィンドウが表示されます（図 10-13 を参照）。

図 10-13　[CifsAO] > [Preposition] ウィンドウ



[Preposition] ウィンドウには、この WAFS Edge デバイスに割り当てられているすべての事前配置ポリシーが表示された表が含まれています。各ポリシーについて、次の情報が表示されます。

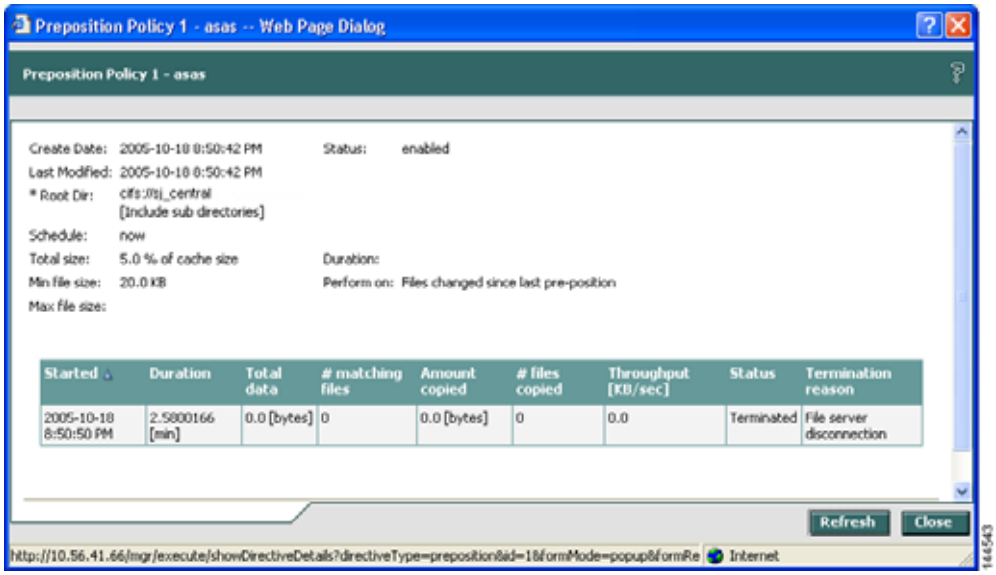
- [ID]：選択したポリシーの ID 番号。
- [Description]：ポリシーに割り当てられている説明的な名前。
- [Root Directory]：事前に配置する内容の元のディレクトリ。
- [Schedule]：ポリシーに定義されたスケジュール。
- [Started]：システムでこのポリシーが最後に呼び出された日時。
- [Duration]：最後の作業の経過時間。

- [Status]：リフレッシュ ボタンがクリックされるたびにアップデートされるポリシーの現在の状態。ポリシーで定義されている作業が現在実行されている場合、そのステータスは In Progress になります。進行中の事前配置作業を停止することができます。
- [Termination reason]：ポリシーが停止した理由。

ステップ 2　詳細な作業履歴（選択したポリシーの反復）を表示するには、表からポリシーを選択し、[View] をクリックします。

[Preposition Task Details] ウィンドウが表示されます（図 10-14 を参照）。

図 10-14　[Preposition Task Details] ウィンドウ



[Preposition Policy] ウィンドウの上部には、選択したポリシーに関する次の詳細が表示されます。

- [Create Date]：ポリシーが作成された日時。
- [Last Modified]：ポリシーが最後に変更された日付。
- [Total size]：事前に配置するファイルの合計サイズに設定された制限値（存在する場合）。
- [Min file size]：ポリシーの影響を受けるルート ディレクトリ（および事前配置ポリシーに含まれるサブディレクトリ）内のファイルの最小サイズ。
- [Max file size]：ポリシーの影響を受けるルート ディレクトリ（および事前配置ポリシーに含まれるサブディレクトリ）内のファイルの最大サイズ。
- [Perform on]：選択した位置から事前に配置するファイル（最後の事前配置後に変更されたファイル、定義された時間内に変更されたファイル、またはすべてのファイル）。

[Preposition Policy] ウィンドウの下部には、選択したポリシーで実行された最新の作業（最大で最後の 10 反復）が表示された、次の情報を含む表が含まれています。

- [Total data]：ポリシーにより転送されるデータの合計量。
- [# matching files]：ポリシーの定義済みフィルタと一致するファイルの数。
- [Amount copied]：ポリシーの最後の実行でコピーされたデータの合計量（ポリシーが現在処理中である場合や、処理に設定された時間制約などのためにポリシーが完了しなかった場合、この量は、[Total data] フィールドに表示される量より少ない場合があります）。
- [# files copied]：ポリシーの最後の実行でコピーされたファイルの数。

- [Throughput]：ポリシーで達成されたスループット（Kbps 単位）。
- [Termination reason]：ポリシーが停止した理由（重要な場合）。ポリシーは、時間的、空間的制約で停止したり、管理者が手動で停止する場合があります。

ステップ 3　[Close] をクリックして、[Policies] ウィンドウへ戻ります。

（注）　[Policies] ウィンドウに表示される情報をアップデートするには、[Refresh] をクリックします。

事前配置作業の停止

進行中の事前配置作業を任意の時点で停止することができます。事前配置作業を停止しても、作業を生成した事前配置ポリシーは削除されません。システムは、次のスケジュール時間になると、ポリシーに記述された作業を実行します。

（注）　デバイスが WAAS Central Manager に登録されていない場合は、事前配置作業を停止しないでください。

事前配置作業を停止するには、次の手順に従ってください。

ステップ 1　[Policies] ウィンドウで、ステータスが In Progress のポリシーを選択し、[Terminate] をクリックします。確認メッセージが表示されます。

ステップ 2　[Yes] をクリックして作業を停止します。[View] をクリックして [Preposition Policy] ウィンドウを表示すると、作業履歴を表示する表に、最後の作業が管理者によって停止されたことを示すメッセージが含まれます。

WAFS Core デバイスの管理

ナビゲーション領域の [WAFS Core] オプションを使用すると、WAFS Core 統計情報のモニタおよびログ情報の表示が可能になります。[WAFS Core] オプションは、WAFS レガシー モードを使用している場合にだけ表示されます。

（注）　レガシー モード WAFS は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー モード WAFS を有効にすると、Central Manager 上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー WAFS の何らかの設定値を設定しようとした場合に警告されます。レガシー WAFS をお使いの場合は、透過的 CIFS アクセラレータに移行してください。

[WAFS Core] オプションには、次のメニュー項目があります。

- [Monitoring]：「Cisco WAE コンポーネントのモニタリング」（P.10-25）の説明に従って、表とグラフに WAFS Core 統計情報を表示できます。
- [Logs]：WAFS Core に関連するイベント ログを表示できます。詳細については、「Cisco WAE ログの表示」（P.10-34）を参照してください。

WAFS Edge デバイスの管理

ナビゲーション領域の [WAFS Edge] メニュー項目により、事前配置作業のモニタ、WAFS Edge 統計情報のモニタ、およびログ情報の表示が可能です。[WAFS Edge] オプションは、WAFS レガシー モードを使用している場合にだけ表示されます。

（注）　レガシー モード WAFS は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー モード WAFS を有効にすると、Central Manager 上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー WAFS の何らかの設定値を設定しようとした場合に警告されます。レガシー WAFS をお使いの場合は、透過的 CIFS アクセラレータに移行してください。

[WAFS Edge] オプションには、次のメニュー項目があります。

- [Preposition] : WAAS Central Manager GUI で作成した事前配置ポリシーの進行状況をモニタできます。さらに、オプションで事前配置作業を停止できます。詳細については、「[Preposition] オプション」（P.10-20）を参照してください。WAFS レガシー モードと透過的 CIFS アクセラレータ モードの事前配置動作は同じです。
- [Monitoring] :「Cisco WAE コンポーネントのモニタリング」（P.10-25）の説明に従って、表とグラフに WAFS Edge デバイス統計情報を表示できます。
- [Logs] : WAFS Edge デバイスに関連するイベント ログを表示できます。詳細については、「Cisco WAE ログの表示」（P.10-34）を参照してください。

WAE のモニタリング

Cisco WAE、WAFS Core、WAFS Edge、および 透過的 CIFS アクセラレータ コンポーネントで使用できる [Monitoring] オプションを使用すると、WAE の現在の状態を示す詳細な表を表示できます。また、選択したコンポーネントに関する履歴データを表示するグラフも提供されます。これらのグラフを使用すると、日、週、月、または年間の WAE 統計情報を追跡できます。

（注）　WAE 統計情報とグラフは、フリーウェアの MRTG ユーティリティによって生成されます。詳細については、http://people.ee.ethz.ch/~oetiker/webtools/mrtg/ を参照してください。

表 10-2 に示すように、モニタリング オプションは WAE コンポーネントごとに異なります。

表 10-2　コンポーネント別のモニタリング オプション

コンポーネント	モニタされる統計情報
Cisco WAE	CPU とディスク ドライブの使用率
透過的 CIFS アクセラレータ	CIFS トラフィックおよびキャッシュ
WAFS Core	接続
WAFS Edge	接続、CIFS トラフィック、および キャッシュ

ここでは、次の内容について説明します。

グラフのモニタリング

WAAS ソフトウェアは、モニタ統計ごとに 4 つの履歴グラフを生成します。各グラフは、次のように、選択したデータの異なる時間範囲を表します。

- [Daily]：過去 24 時間のデータを表示します。各データ点は、平均 5 分を表します。
- [Weekly]：過去 7 日間のデータを表示します。各データ点は、平均 30 分を表します。
- [Monthly]：過去 5 週間のデータを表示します。各データ点は、平均 2 時間を表します。
- [Yearly]：過去 12 か月のデータを表示します。各データ点は、平均 1 日を表します。

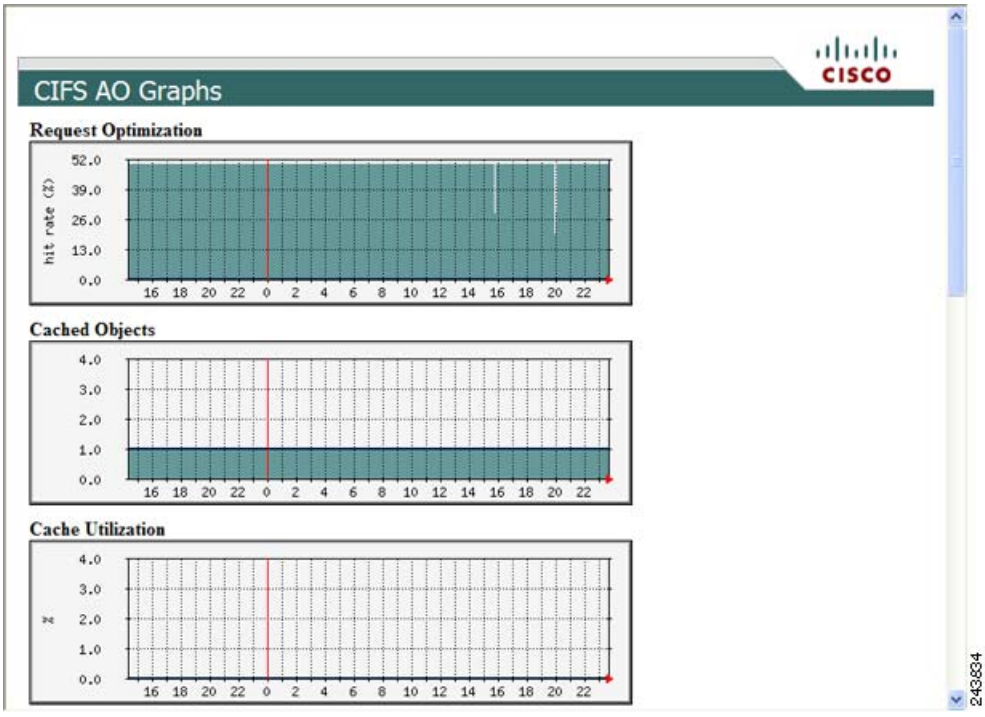
これらのグラフの下に、それぞれの時間範囲での最大値とモニタされる統計値の現在の値も表示されます。

表示オプション

コンポーネントに使用できるすべてのモニタ対象統計情報に関する日別グラフの索引ウィンドウを表示したり、特定の統計情報（キャッシュ使用率など）に関する 4 つの履歴グラフを同時に表示したりできます。

図 10-15 に、ユーザが索引グラフを表示することを選択したときの画面の例を示します。

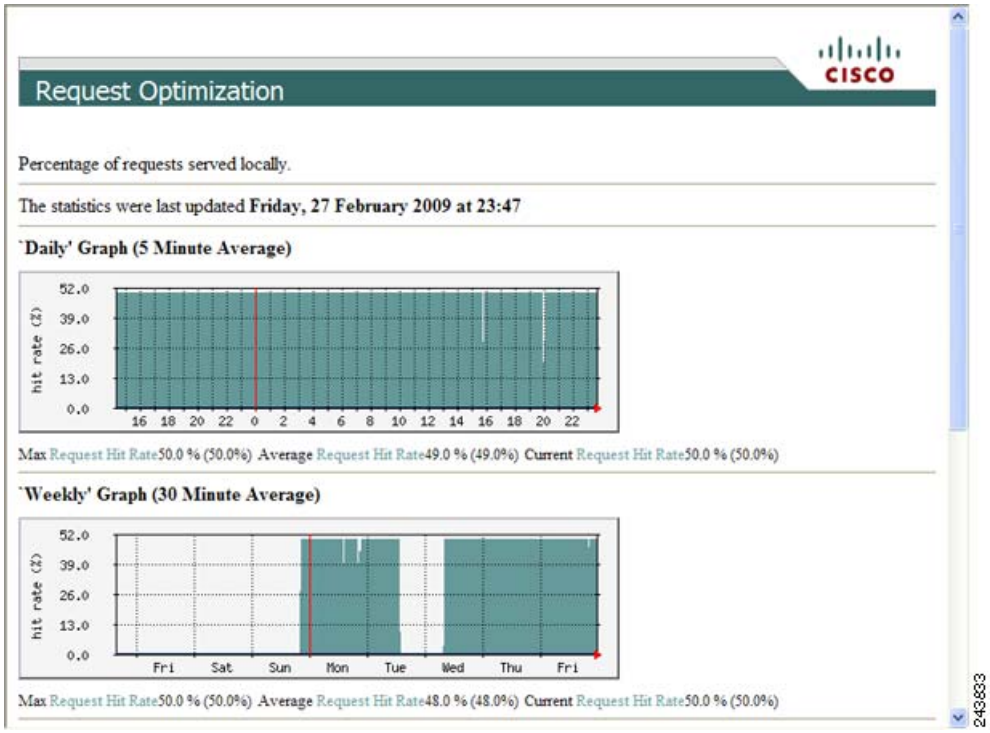
図 10-15　索引グラフ画面の例



ヒント　索引ウィンドウの各グラフは、リンクとして機能します。グラフをクリックすると、選択した統計情報に関する 4 つの履歴グラフすべてが表示されます。たとえば、索引グラフ ウィンドウで [Request Optimization] グラフをクリックすると、日、週、月、および年間の Request Optimization 履歴グラフが表示されます。ブラウザで [Back] ボタンをクリックすると、索引グラフへ戻ります。

図 10-16 に、ユーザが特定の統計情報に関する履歴グラフを表示することを選択したときの画面の例を示します。

図 10-16　履歴グラフ ウィンドウの例



（注）　ブラウザの [印刷] コマンドを使用すると、グラフを印刷できます。

Cisco WAE コンポーネントのモニタリング

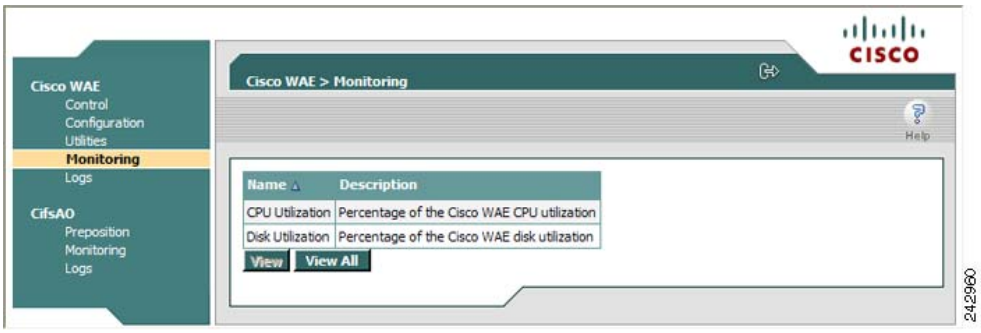
Cisco WAE コンポーネント用の [Monitoring] オプションは、WAE でモニタされる統計情報の表を表示します。この表から、WAE の Central Processing Unit（CPU; 中央処理装置）の使用率とディスク ドライブの使用率を示す履歴グラフを表示できます。

CPU 使用率は、CPU が使用する帯域幅と使用できる合計帯域幅の比率です。数値は、% で表示されます。ディスク ドライブの使用率は、すべてのディスク ドライブで使用されているディスク容量と使用できる合計ディスク容量の比率です。この数値も、% で表示されます。

WAE コンポーネントをモニタするには、次の手順に従ってください。

ステップ 1　ナビゲーション領域で、[Cisco WAE] メニュー項目の下にある [Monitoring] をクリックします。[Cisco WAE Monitoring] ウィンドウが表示されます（図 10-17 を参照）。

図 10-17　[Cisco WAE Monitoring] ウィンドウ



ステップ 2　次のいずれかを実行します。

- 表示したい統計情報を（その行をクリックして）選択し、[View] をクリックして、その統計情報に関する履歴グラフを含むポップアップ ウィンドウを表示します。
- [View All] をクリックして、WAE コンポーネントの両方の統計情報に関する日別グラフを含む索引ウィンドウを表示します。

WAFS Core のモニタリング

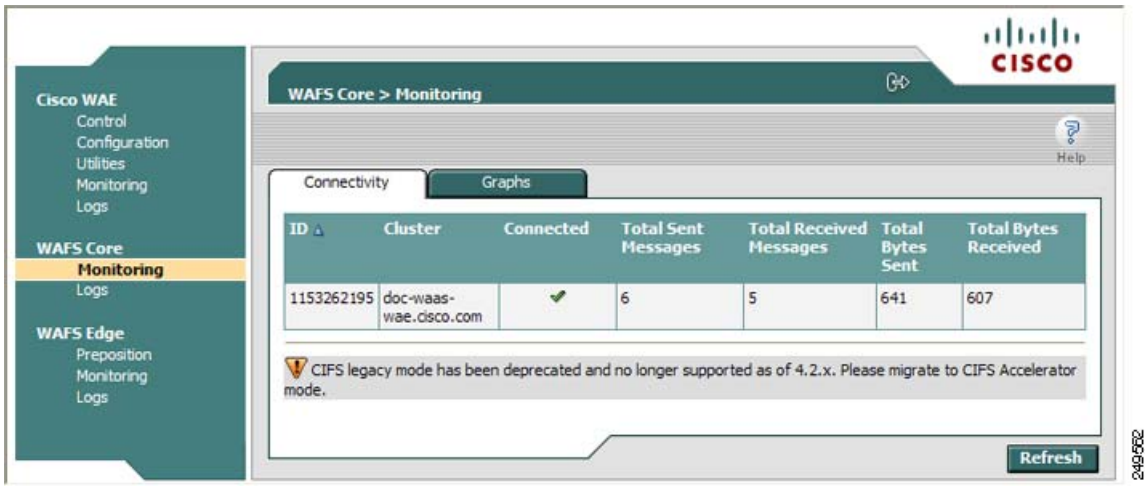
[WAFS Core] メニュー項目の [Monitoring] オプションは、次の 2 つのタブを表示します。

- [Connectivity]：WAFS Core に関する接続統計情報の表を表示します。この表は、デフォルトで表示されます。
- [Graphs]：WAFS Core で利用できるグラフのリストを表示します。

WAFS Core コンポーネントをモニタするには、次の手順に従ってください。

ステップ 1　ナビゲーション領域で、[WAFS Core] コンポーネントの下にある [Monitoring] をクリックします。[WAFS Core Monitoring] ウィンドウに、[Connectivity] タブが表示されます（図 10-18 を参照）。

図 10-18　[WAFS Core Monitoring]：[Connectivity] タブ

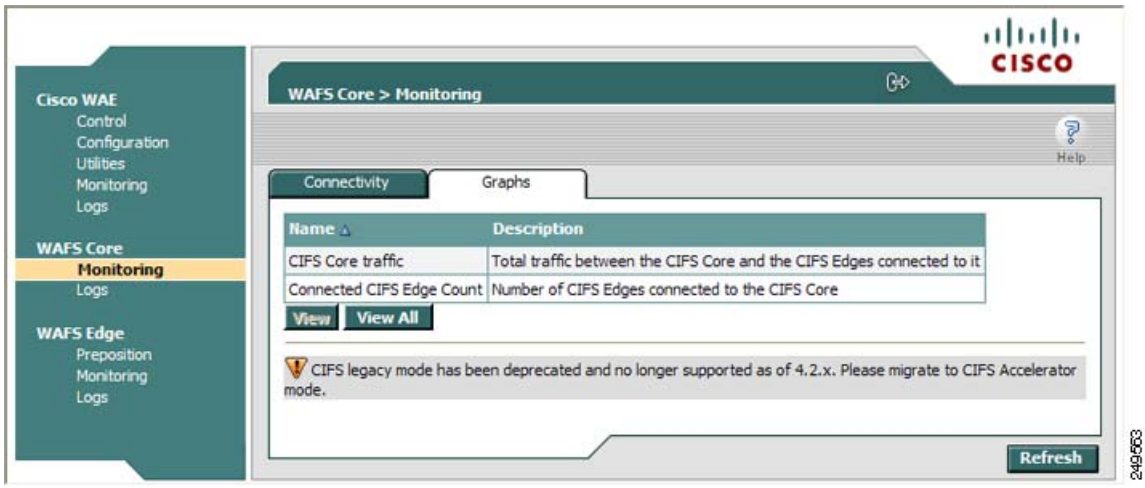


[Connectivity] タブは、WAFS Core に関する次のデータを含む表を表示します。

- [ID]：WAFS Core の英数字のシステム ID。
- [Cluster]：この WAFS Core が所属するコア クラスタの名前（存在する場合）。
- [Connected]：WAFS Core が、現在 WAFS Edge デバイスに接続されている（✔）か、WAFS Edge デバイスから切断されている（✘）かを示します。
- [Total Sent Messages]：アクティブ化されてからこの WAFS Core から送信されたメッセージの総数。
- [Total Received Messages]：アクティブ化されてからこの WAFS Core で受信されたメッセージの総数。
- [Total Bytes Sent]：アクティブ化されてからこの WAFS Core から送信されたバイトの総数。
- [Total Bytes Received]：アクティブ化されてからこの WAFS Core で受信されたバイトの総数。

ステップ 2　[Graphs] タブをクリックします（図 10-19 を参照）。

図 10-19　[WAFS Core Monitoring]：[Graphs] タブ



WAFS Core コンポーネントには、次の履歴グラフが使用できます。

- [Connected WAFS Edge counts] : 選択した WAFS Core に現在接続されている WAFS Edge デバイスの台数。このグラフは、WAFS Edge デバイスの切断を検出するために有用です。
- [WAFS Core traffic] : WAFS Core と WAFS Core に接続されている各 WAFS Edge デバイス間のトラフィックの総量（キロビット単位）。緑色の折れ線は、送信したトラフィックを表します。青色の折れ線は、受信したトラフィックを表します。

ステップ 3　次のいずれかを実行します。

- 表示したい統計情報を（その行をクリックして）選択し、[View] をクリックして、その統計情報に関する履歴グラフを含むポップアップ ウィンドウを表示します。
- [View All] をクリックして、WAFS Core コンポーネントの両方の統計情報に関する日別グラフを含む索引ウィンドウを表示します。

透過的 CIFS アクセラレータまたは WAFS Edge デバイスのモニタリング

透過的 CIFS アクセラレータ デバイスと WAFS Edge デバイスのモニタリングはほとんど同じです。ただし、透過的 CIFS アクセラレータでは接続をモニタしません。

[Monitoring] オプションは、次のタブを表示します。

- [Connectivity] : WAFS Edge デバイスに関する接続統計情報の表を表示します。透過的 CIFS アクセラレータ モードを使用している場合、このタブは表示されません。
- [CIFS] : CIFS プロトコルと選択されたデバイスのステータスに関するデータを表示します。
- [Cache] : デバイス キャッシュに関するデータを表示します。
- [Graphs] : デバイスで利用できるグラフのリストを表示します。

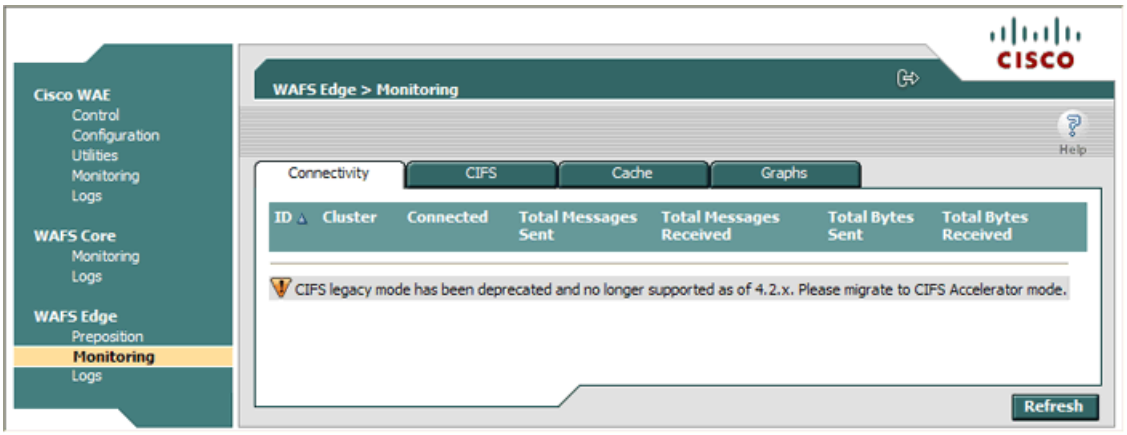
（注）　[CIFS] タブと [Cache] タブに表示される SNMP パラメータは、特殊な MIB ファイルに含まれます。

透過的 CIFS アクセラレータまたは WAFS Edge デバイスをモニタするには、次の手順に従ってください。

ステップ 1　ナビゲーション領域で、[CifsAO] または [WAFS Edge] メニューの下にある [Monitoring] をクリックします。

[Monitoring] ウィンドウが表示されます（図 10-20 を参照）。透過的 CIFS アクセラレータ モードを使用している場合は、[Connectivity] タブは使用されず、最初に [CIFS] タブが表示されます。ステップ 2 に進みます。

図 10-20　[WAFS Edge Monitoring]：[Connectivity] タブ



[Connectivity] タブは、WAFS Edge デバイスに関する次のデータを含む表を表示します。

- [ID]：WAFS Edge デバイスの英数字のシステム ID。
- [Cluster]：この WAFS Edge デバイスが接続されているコア クラスタの名前（存在する場合）。
- [Connected]：WAFS Edge デバイスが、現在 WAFS Core に接続されている（✔）か、WAFS Core から切断されている（✘）かを示します。
- [Total Messages Sent]：アクティブ化されてからこの WAFS Edge デバイスから送信されたメッセージの総数。
- [Total Messages Received]：アクティブ化されてからこの WAFS Edge デバイスで受信されたメッセージの総数。
- [Total Bytes Sent]：アクティブ化されてからこの WAFS Edge デバイスから送信されたバイトの総数。
- [Total Bytes Received]：アクティブ化されてからこの WAFS Edge デバイスで受信されたバイトの総数。

ステップ 2　[CIFS] タブをクリックします。

[CIFS] タブは、次の CIFS 関連情報を表示します。

- [Total Time Saved]：CIFS アクセラレーションによって節約された時間の合計。
- [Total KBytes read]：クライアントが CIFS プロトコルを使用してこのデバイスから読み取ったキロバイト総数（キャッシュ経由とリモートの両方）。
- [Total KBytes written]：クライアントが CIFS プロトコルを使用してこのデバイスに書き込んだキロバイト総数。
- [Remote requests count]：WAN 経由でリモート転送されたクライアント CIFS 要求の総数。この統計情報の名前は、履歴グラフを表示するために使用できるリンクです（最初に [Graphs] タブに移動する必要はありません）。これらのグラフには、ローカル要求も表示されます。
- [Local requests count]：このデバイスによりローカルで処理されたクライアント CIFS 要求の総数。この統計情報の名前は、履歴グラフを表示するために使用できるリンクです（最初に [Graphs] タブに移動する必要はありません）。これらのグラフには、リモート要求も表示されます。
- [Total remote time]：このデバイスが WAN 経由でリモート送信されたすべてのクライアント CIFS 要求を処理するのにかかった合計時間（ミリ秒単位）。
- [Total local time]：このデバイスがローカルに処理されたすべてのクライアント CIFS 要求を処理するのにかかった合計時間（ミリ秒単位）。

- [Connected sessions count]：このデバイスに接続されている CIFS セッションの総数。この統計情報の名前は、日、週、月、および年間のグラフを表示するために使用できるリンクです（最初に [Graphs] タブへ進む必要がありません）。
- [Open files count]：このデバイスで開いている CIFS セッションの総数。この統計情報の名前は、日、週、月、および年間のグラフを表示するために使用できるリンクです（最初に [Graphs] タブへ進む必要がありません）。
- [CIFS Command Statistics]：CIFS コマンドの統計情報の表。要求の総数、リモート要求数、非同期要求数、ローカルに処理された各要求をこのデバイスで処理した平均時間（ミリ秒単位）、WAN 経由でリモート送信された各要求をこのデバイスで処理した平均時間（ミリ秒単位）を、コマンドタイプごとに表で示します。

  CIFS 統計情報をリセットするには、表の下の [Reset CIFS Statistics] ボタンをクリックします。

ステップ 3　[Cache] タブをクリックします。

[Cache] タブは、次の情報を表示します。

- [Maximum cache disk size]：WAFS デバイス キャッシュに割り当てられた最大ディスク容量（GB 単位）。
- [Current cache disk usage]：WAFS デバイス キャッシュで現在使用されているディスク容量（KB 単位）。この統計情報の名前は、履歴グラフを表示するために使用できるリンクです（最初に [Graphs] タブに移動する必要はありません）。
- [Maximum cache resources]：WAFS デバイス キャッシュで許可されるリソース（ファイルとディレクトリ）の最大数。
- [Current cache resources]：WAFS デバイス キャッシュに現在含まれているリソースの数。この統計情報の名前は、履歴グラフを表示するために使用できるリンクです（最初に [Graphs] タブに移動する必要はありません）。
- [Evicted resources count]：デバイスが起動してからキャッシュから除去されたリソースの数。
- [Last eviction time]：キャッシュから最後に除去された日時。
- [Cache size high watermark]：WAFS デバイスでリソースの除去を開始するディスク使用率（%）。
- [Cache size low watermark]：WAFS デバイスでリソースの除去を停止するディスク使用率（%）。
- [Cache resources high watermark]：WAFS デバイスでリソースの除去を開始する合計キャッシュ リソースの比率（%）。
- [Cache resources low watermark]：WAFS デバイスでリソースの除去を停止する合計キャッシュ リソースの比率（%）。
- [Last evicted resource age]：最後に除去されたリソースが WAFS デバイス キャッシュに存在した時間。
- [Last evicted resource access time]：最後に除去されたリソースが最後にアクセスされた日時。

ステップ 4　[Graphs] タブをクリックします（図 10-21 を参照）。

図 10-21　[WAFS Edge Monitoring] : [Graphs] タブ

デバイスには、次の履歴グラフを使用できます。

- [CIFS Edge - CIFS Core traffic] : WAFS Edge デバイスとそれに接続している各 WAFS Core 間のトラフィックの総量（KB 単位）。緑色の折れ線は、送信したトラフィックを表します。青色の折れ線は、受信したトラフィックを表します。この項目は、WAFS レガシー モードを使用している場合にだけ表示されます。
- [CIFS Edge - Client Average Throughput] : WAFS Edge デバイスと WAFS Edge デバイスがサービスを提供するクライアント間のトラフィックの総量と合計稼動時間（アイドル時間を含む）の比率。KB/ 秒で表示されます。この項目は、WAFS レガシー モードを使用している場合にだけ表示されます。
- [Cache Disk Capacity] : WAFS デバイス キャッシュで使用されるディスク容量（MB 単位）。
- [Cache Utilization] : 定義された制限値に基づいてキャッシュで使用されるディスク容量の比率（%）とリソースの比率（%）。
- [Cached Objects] : キャッシュに含まれるオブジェクト（ファイルとディレクトリ）の総数。
- [Client Average Throughput] : WAFS Edge デバイスと WAFS Edge デバイスがサービスを提供するクライアント間のトラフィックの総量と合計稼動時間（アイドル時間を含む）の比率。KB/ 秒で表示されます。この項目は、CIFS 透過的アクセラレータ モードを使用している場合にだけ表示されます。
- [Connected CIFS Core count] : 選択した WAFS Edge デバイスに接続されている WAFS Core の数。この項目は、WAFS レガシー モードを使用している場合にだけ表示されます。

（注）　WAFS Edge デバイスは、アベイラビリティを改善するために複数の WAFS Core に接続できます。

- [Connection Statistics] : デバイスで加速された CIFS セッションの数。

- [File Optimization]：開いている CIFS ファイルの総数。
- [Request Optimization]：（ユーザが要求した内容のファイル サーバへ WAN 経由でリモート送信されるユーザ要求と異なり）キャッシュが応答したユーザ要求の比率（%）。
- [Requests Count]：ローカルで処理された要求（キャッシュが応答したクライアント要求）の平均比率とリモートで処理された要求（リモート ファイル サーバが応答したクライアント要求）の平均比率。要求カウントは、1 秒あたりの要求数で表示されます。

ステップ 5　次のいずれかを実行します。

- 表からグラフを選択し、[View] をクリックして、選択した統計情報に関する 4 つの履歴グラフを表示するポップアップ ウィンドウを表示します。
- [View All] をクリックして、WAFS Edge デバイスに関する日別グラフを含む索引ウィンドウを表示します。

WAE ログの表示

Cisco WAE、CifsAO、WAFS Core、および WAFS Edge コンポーネントがログに記録したイベント情報を表示できます。使用できるイベント情報は、表示しているコンポーネントによって変化します。

ここでは、次の内容について説明します。

- 「WAE ログ」（P.10-32）
- 「Cisco WAE ログの表示」（P.10-34）

WAE ログ

次の項の説明に従って、各ログ ファイルに表示する内容を設定し、ファイルにログをローカルに保存できます。

- 「表示基準の設定」（P.10-32）
- 「ログ項目の表示」（P.10-33）
- 「ログ ファイル情報の保存」（P.10-33）

表示基準の設定

図 10-22 に示すように、すべての WAE ログに表示したいデータの基準を設定できます。

図 10-22　WAE ログ データの基準

ログ情報を表示する基準を設定するには、次の手順に従ってください。

ステップ 1　[From] ドロップダウン リストから、開始日付（年、月、および日）と時刻（24 時間形式の時間と分）を選択します。

ステップ 2　[To] ドロップダウン リストから、終了日付（年、月、および日）と時刻（24 時間形式の時間と分）を選択します。

ステップ 3　（任意）[Log Level] ドロップダウン リストから、イベントの最小重大度を選択します。

最小重大度を選択すると、指定した重大度より大きいすべてのイベントが表示されます。デフォルトは [All] です。

ステップ 4　（任意）[Lines] ドロップダウン リストから、ログの 1 ページに表示するイベントの数（1 行当たり）を選択します。

デフォルトは、100 イベントです。

ステップ 5　（任意）ログをさらに選別するためのフィルタ文字列を入力します。

ステップ 6　[Update] をクリックします。

ログ項目の表示

各ログ項目には、イベントの発生日時、イベントの重大度、およびログ メッセージを含む説明が含まれます。ログ メッセージの形式は、イベントの種類によって変化します。

イベントの重大度は、イベントの深刻さを示します。6 つの選択肢が定義され、次の情報を提供します。

- [All]：すべての重大度レベルのイベントを表示します。
- [Debug]：デバッグ用に指定されたイベントと一致するイベントが発生したことを示します。
- [Info]：コンポーネントの正しい動作に関するイベントが発生したことを示します。この種類のイベントには、処置は不要です。
- [Warning]：コンポーネントで軽度の問題が発生したことを示します。コンポーネントは、自動的に回復可能です。
- [Error]：コンポーネントの正しい動作に影響する問題が発生したことを示します。処置が必要になる可能性があります。
- [Fatal]：コンポーネントの動作が停止するような深刻な問題がコンポーネントで発生したことを示します。処置が必要です。

ログ ファイル情報の保存

ログをテキスト ファイルとして保存し、ローカル ドライブへダウンロードすることができます。

ログをテキスト ファイルとして保存するには、次の手順に従ってください。

ステップ 1　[From] ドロップダウン リストと [To] ドロップダウン リストを使用して、保存したい期間を設定します（「表示基準の設定」（P.10-32）を参照）。

ステップ 2　表示したいイベントの重大度を設定します。

詳細については、「表示基準の設定」（P.10-32）を参照してください。

ステップ 3　[Update] をクリックします。

ステップ 4　[Download] をクリックします。

[File Download] ウィンドウが表示されます。

ステップ 5　[File Download] ウィンドウの [Save] をクリックします。

ステップ 6　ログ ファイルを保存したいディレクトリを指定します。

ステップ 7　[OK] をクリックします。

Cisco WAE ログの表示

各 WAE コンポーネントは、それ自身のログ ファイルを生成します。

Cisco WAE コンポーネントは、次のログを生成します。

- Manager ログ：設定の変更、WAE の登録、他の WAE コンポーネントの起動または停止の通知などの WAE Device Manager と WAAS Central Manager GUI コンポーネントに関連するイベントを表示します。
- WAFS Watchdog ログ：WAE 内の他のアプリケーション ファイルをモニタし、必要に応じて再起動する、ウォッチドッグ ユーティリティに関連するイベントを表示します。

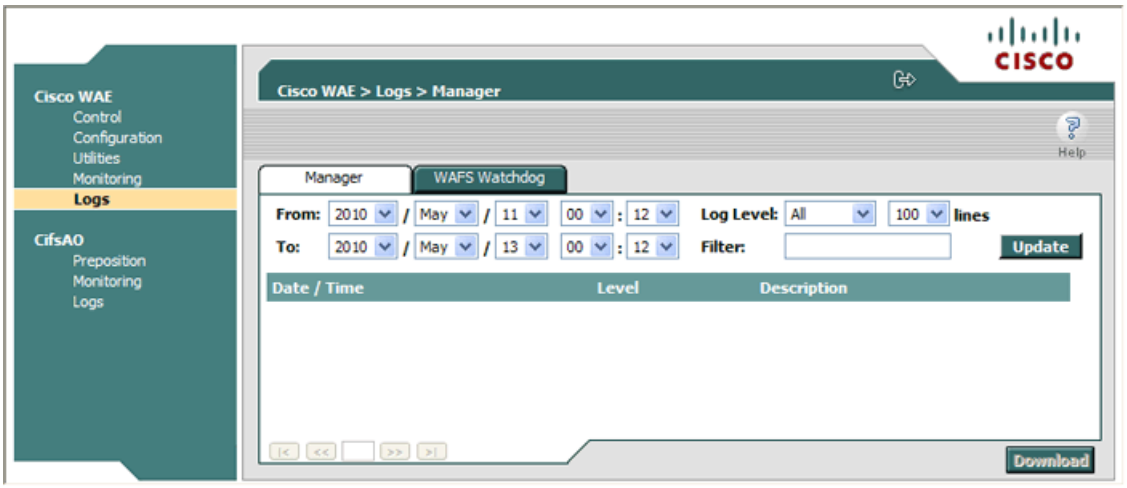
WAFS Core は、WAFS Core の動作に関連するすべてのイベントを表示する 1 つのログを生成します。また、WAFS Edge デバイスは、WAFS Edge の動作に関連するすべてのイベントを表示する 1 つのログを生成します。透過的 CIFS アクセラレータ モードを使用している場合、CIFS アクセラレータは CIFS アクセラレータの動作に関連するすべてのイベントを表示する 1 つのログを生成します。

Cisco WAE、CIFS アクセラレータ、WAFS Core、または WAFS Edge ログを表示するには、次の手順に従ってください。

ステップ 1　ナビゲーション領域で、Cisco WAE、WAFS Core、WAFS Edge、または CifsAO コンポーネントの下にある [Logs] オプションをクリックします。

図 10-23 に、Cisco WAE コンポーネント用の [Logs] ウィンドウを示します。

図 10-23　Cisco WAE コンポーネントの [Logs] ウィンドウ



ステップ 2　Cisco WAE を選択した場合は、[Manager] または [WAFS Watchdog] タブをクリックし、表示したいログを選択します。

ステップ 3　[From]、[To]、[Level]、および [Lines] ドロップダウン リストを使用して、表示基準を設定します（「表示基準の設定」（P.10-32）を参照）。

ステップ 4　（任意）[Filter] テキスト ボックスに関連する自由文面を入力して、特定の語や句を含むイベントだけが表示されるように、ログのフィルタを設定します。

ステップ 5　[Update] をクリックします。選択した基準に従って、[Logs] ウィンドウがリフレッシュされます。

（注）　イベントの数がウィンドウ当たりに選択した行数を超えると、各ログ ウィンドウの一番下にナビゲーション矢印（ |< << 1 >> >| ）が表示されます。

PART 3

WAAS サービスの設定

CHAPTER 11

WAFS の設定

この章では、ブランチ オフィスのユーザが集中管理されたデータセンターに保存されているデータに、より効率的にアクセスできる Wide Area File Services（WAFS; 広域ファイル サービス）を設定する方法について説明します。WAFS 機能は、ブランチ オフィスのユーザ付近の Edge WAE でデータをキャッシュして、WAN の遅延と帯域幅制限を解決します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

ファイル サービスについて

今日、企業は、国内と海外のさまざまな地域にリモート オフィスを構えています。一般に、これらのリモート オフィスには、ローカル ユーザに必要なデータを保存し、管理するために、独自のファイル サーバがあります。

このような運用には、各リモート オフィスでファイル サーバを購入し、管理し、アップグレードするためにコストがかかるという問題があります。これらのファイル サーバを保守するために、特にサーバの障害に備えてデータを保護するために、膨大なリソースと人員を配置する必要があります。リモート オフィスは、必要なレベルのデータ保証を実現するために、リモート サイトでデータをバックアップし、一般に遠隔の安全な場所まで輸送するための専任のリソースを割り当てる必要があります。このシナリオにリモート オフィスの数（数十、数百、数千など）を掛けると、このような企業データ管理の方法では、コストが急激に増加し、重大なデータのリスクが大幅に増えることがわかります。

このシナリオの論理的な解決策は、データを正しく管理するために必要な設備、訓練を受けた人員、およびストレージ容量が存在する中央の位置へ企業のすべての重要なデータを移動する方法です。データセンターがバックアップや他のストレージ管理設備を提供することで、企業は、社員の生産性とストレージの使用率を改善し、データ保証とセキュリティを強化することができます。

企業のデータセンターとリモート オフィス間の WAN は、帯域幅の制限と大きな遅延により、信頼性が低く、低速になる傾向があります。さらに、WAN には、データセンター ソリューションの実装に対する他の阻害要因があります。

その 1 つは、WAN 経由で動作するファイル サーバ プロトコルです。Windows 用のファイル サーバ プロトコルである Common Internet File System（CIFS; 共通インターネット ファイル システム）は、LAN 経由で動作するように設計されています。ファイル操作のたびに、クライアントとファイル サーバの間で、複数のプロトコル メッセージが交換されます。この状況は、LAN では意識されませんが、WAN 経由の場合はただちに大きな遅延になります。また、このような大きな遅延により、ファイル サーバ プロトコル自体が停止する場合があります。

ファイル サーバ プロトコルが WAN 経由で正しく機能する場合でも、各トランザクションの間に長い遅延が存在します。通常、これらの遅延により、ワード プロセシング プログラム、イメージ編集プログラム、および設計ツールのようなユーザ アプリケーションがタイムアウトし、正常に動作しなくなる場合があります。

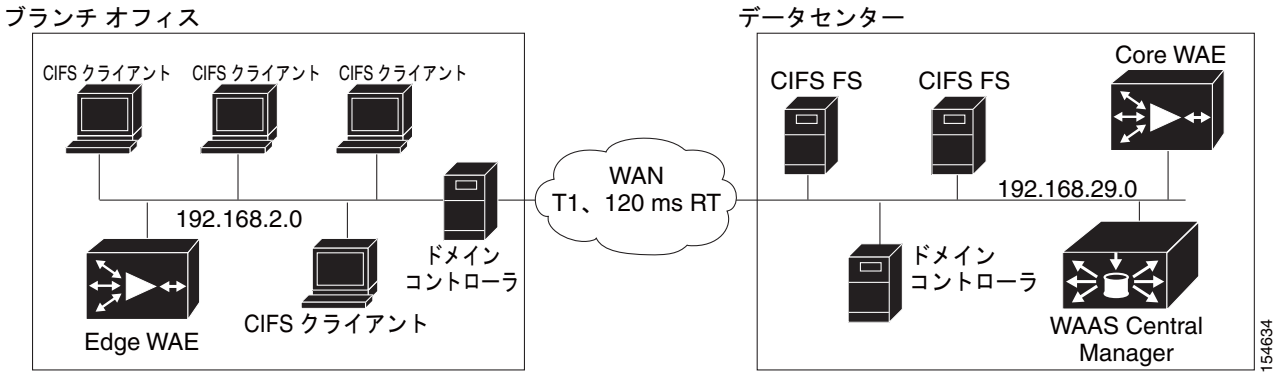
信頼性の低い WAN、ファイル システム プロトコルの互換性、およびユーザ アプリケーションの互換性のような問題は、ユーザ エクスペリエンスに影響し、生産性が低下する使いにくい作業環境の原因になります。

Wide Area Application Service（WAAS）ファイル サービス機能は、ブランチ オフィスのユーザ付近の Edge WAE でデータをキャッシュして、WAN の遅延と帯域幅制限を解決します。このデータ キャッシング方式により、ブランチ オフィスのユーザは、WAN 経由で LAN に似た速度で集中管理されたデータにアクセスできます。ソリューションは、いくつかの重要な概念に基づいています。

- できる限り WAN を使用しない：WAAS は、WAN を横断する必要がある操作の数を最小限に抑えることで、実質的にユーザが WAN から受ける多くの障害をなくします。
- WAN を最適利用する：ファイル サービス機能は、システムが WAN を最適利用できる高度なキャッシング、圧縮、およびネットワーク最適化テクノロジーを使用します。
- ファイル システム プロトコルの意味を維持する：WAAS ソフトウェアは、WAN 経由で独自のプロトコルを使用しますが、標準のファイル システム プロトコル コマンドの意味を完全に維持します。そのため、実質的にネットワーク内のデータの正確性と一貫性が維持されます。
- ソリューションをユーザに透過的にする：最善のソリューションは、エンドユーザの操作を中断せず、ユーザが業務方法を変更する必要がないソリューションです。WAAS ファイル サービス ソリューションは、サーバ側とクライアント側のいずれにもソフトウェアをインストールする必要がなく、ユーザが新しいことを学習する必要もありません。ユーザは、仕事の進め方を変更せずに、安全なデータセンターがあることによるすべての利点を活用できます。

WAAS ファイル サービス機能を使用すると、企業は、データを正しく管理するために必要な設備、IT スタッフ、およびストレージ デバイスを提供するデータセンターにファイル サーバを集約できます。図 11-1 に、WASS ファイル サービスを設定したあとの典型的な構成シナリオを示します。

図 11-1　WAAS ファイル サービス ソリューション



ファイル サービス機能の概要

この項では、WAAS ファイル サービス機能の概要を説明します。内容は次のとおりです。

- 「自動ディスカバリ」（P.11-4）
- 「事前配置」（P.11-4）
- 「データ一貫性」（P.11-5）
- 「データ並列性」（P.11-6）
- 「Microsoft 製品との相互運用性」（P.11-7）

WAAS バージョン 4.1.1 以降には、相互に排他的な次の 2 つの WAFS モードが含まれています。

- 透過的 CIFS アクセラレータ モード：このモードは、WAAS バージョン 4.1.1 で導入されました。この新しいトランスペアレント モードでは、コア、エッジ、接続設定は必要ありません。このモードは自動ディスカバリに依存し、設定する必要はなく、CIFS トラフィックを透過的に加速します。切断モードはサポートされていません。使いやすさという点から、このモードを推奨します。
- レガシー モード：すべての WAAS バージョンで提供されるこのモードは、Core クラスタ、Edge ファイル サービス、および Core デバイスと Edge デバイス間の接続を設定する必要があります。複数の WAAS 4.0.x デバイスを相互運用する必要がある場合、または切断モードでの動作が必須である場合は、このモードを使用します。

  このモードにもファイル サーバを自動的に検出する機能が含まれますが、制限があります。詳細については、「レガシー モードによる自動ディスカバリ」（P.11-4）を参照してください。

（注）　レガシー モード WAFS は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー モード WAFS を有効にすると、Central Manager 上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー WAFS の何らかの設定値を設定しようとした場合に警告されます。レガシー WAFS をお使いの場合は、透過的 CIFS アクセラレータに移行してください。

WAE デバイスまたはグループで透過的 CIFS アクセラレータが有効である場合、システムはすべての既存の Core または Edge の設定、および Core と Edge の設定ウィンドウを無効にします。さらに、デバイスは Core クラスタに属することができません。CIFS アクセラレータ モードでは、各要求の方向に応じて、WAE デバイスが同時に Edge および Core として動作します。手動の設定は不要です。

（注）　WAFS アクセラレーションは、接続の各端のピア WAE が同じ WAFS モード（透過的 CIFS アクセラレータまたはレガシー）を使用している場合に限り動作します。

自動ディスカバリ

自動ディスカバリ機能により、個々のファイル サーバを WAAS Central Manager に登録しなくても WAFS を有効にすることができます。自動ディスカバリ機能により、WAAS は、トランスペアレント モードの CIFS 要求を受信すると、自動的に新しいファイル サーバを検出し、そのファイル サーバに接続しようとします。

レガシー モードによる自動ディスカバリ

レガシー動作モードにも、いくつか制限を伴いますが、ファイル サーバの自動ディスカバリ機能があります。レガシー モードを使用している場合、自動ディスカバリ機能は、デフォルトでは、未登録のファイル サーバへの CIFS 要求に対して動作します。

ファイル サーバへのパスが複数ある場合、WAAS は最も遅延の小さいパスを選択します。Core WAE と検出されたサーバの間の遅延が 25 ミリ秒を超える場合、サーバは遠すぎると判断され、接続は最適化されません。さらに、Edge WAE とサーバの間の遅延が 2 ミリ秒未満の場合、サーバはローカルと判断され、接続は最適化されません。

（注）　WAFS レガシー モードを使用し、ファイル サーバを登録せずに自動ディスカバリ機能に依存している場合、事前配置、ダイナミック共有、および切断モードといった WAFS 機能を使用できません。さらに、ファイル サーバにデジタル署名が必要な場合、WAFS はそのデータをキャッシュできません。

新しいファイル サーバは、この自動ディスカバリのモードによりポリシー エンジンのダイナミック マップに追加されるので、**show policy-engine application dynamic** EXEC コマンドを使用して、これらのファイル サーバを確認することができます。ファイル サーバは、最後の接続が閉じてから 3 分間ダイナミック マップに残っています。

事前配置

事前配置機能を使用すると、システム管理者は、頻繁に使用するファイルを中央のストレージから選択した Edge WAE のキャッシュに事前に「配置」できます。これにより、ユーザは最初からファイルに高速アクセスでき、使用可能な帯域幅の使用効率が上昇します。WAAS Central Manager GUI から、事前配置ディレクティブを作成します。

エンド ユーザが Edge WAE キャッシュにないファイルを開こうとすると、Edge WAE は、ファイルが保存されているファイル サーバから WAN 経由でファイルを取得します。事前配置は、管理者が、定義済みのスケジュールに従って、頻繁にアクセスされる大型ファイルをファイル サーバから選択した Edge WAE キャッシュへ保存できる機能です。事前配置を適切に行うことで、管理者は、ユーザがこれらのファイルに初めてアクセスするときでも、キャッシュ レベルのパフォーマンスを利用可能にすることができます。事前配置は、ネットワークがアイドル状態にあるときに（夜間など）重い内容を転送し、日中は他のアプリケーションに帯域幅を解放して、WAN 帯域の使用率を改善します。

WAAS Central Manager GUI を使用すると、管理者は、（それぞれのスケジュールが設定された）相互に重なる複数の事前配置ポリシー、対象 Edge WAE のリスト、および定義された時間とサイズの制約を作成できます。

（注）　事前配置には、複数のルートを設定する機能も含まれます。「新しい事前配置ディレクティブの作成」（P.11-27）を参照してください。

データー貫性

WAAS ソフトウェアは、相互に関係のある 2 つの機能を使用して、システム全体のデータ整合性を保証します。その 1 つは、データの最新性を管理する *一貫性* です。もう 1 つは、複数のクライアントによるデータ アクセスを制御する *並列性* です。

複数の位置で複数のコピーを維持すると、そのうちのいくつかのファイルが変更される可能性が増し、他のファイルとの一貫性が失われます。一貫性の意味は、最新性（コピーが最新であるかどうか）と元のファイル サーバと交換されるアップデートの伝搬の保証のために使用されます。

WAAS ソフトウェアは、組み込み一貫性ポリシーに次の一貫性の意味を適用します。

- サイト内での厳格な CIFS 動作：同じキャッシュのユーザは、常に標準の厳格な CIFS 一貫性の意味が保証されます。
- CIFS を開くときのキャッシュ検証：CIFS では、ファイルを開く操作は、ファイル サーバへパススルーされます。一貫性を守るため、WAAS ソフトウェアは、ファイルを開くたびにファイルの最新性を検証し、ファイル サーバのファイルが更新されている場合、キャッシュされたファイルを無効にします。

  WAAS ソフトウェアは、キャッシュ内のファイルのタイム スタンプとファイル サーバ上のファイルのタイム スタンプを比較して、データを検証します。タイム スタンプが同一の場合、Edge WAE 上のキャッシュされたコピーは有効と見なされ、ユーザは Edge WAE キャッシュからファイルを開くことを許可されます。

  タイム スタンプが異なる場合、Edge WAE は、キャッシュからファイルを削除し、ファイル サーバに最新のコピーを要求します。
- キャッシュの予防的アップデート：WAAS ソフトウェアは、Edge WAE でキャッシュされているデータの最新性を維持するために、CIFS 環境での変更通知の使用をサポートしています。

  クライアントがディレクトリまたはファイルを変更すると、Edge WAE は、ファイル サーバへ変更通知を送信します。次に、ファイル サーバは、変更されたディレクトリとファイルのリストを含む変更通知をすべての Edge WAE へ送信します。変更通知を受信すると、各 Edge WAE は、キャッシュ内の通知にリストされているディレクトリとファイルを無効にし、最新バージョンでキャッシュをアップデートします。

  たとえば、ユーザが既存の Word 文書を編集し、Edge WAE キャッシュに変更を保存すると、Edge WAE は、ファイルが変更されたことを知らせる変更通知をファイル サーバへ送信します。次に、Edge WAE は、変更されたセクションをファイル サーバへ送信し、ファイル サーバは予防的に変更通知をネットワーク内の他の Edge WAE へ送信します。次に、これらの Edge WAE は、すべてのアクセス ポイント全体でファイルが一貫するようにキャッシュをアップデートします。

  このプロセスは、ディレクトリの名前を変更する、新しいサブディレクトリを追加する、ファイルの名前を変更する、またはキャッシュされたディレクトリに新しいファイルを作成するときにも適用されます。
- CIFS を閉じるときのフラッシュ：CIFS では、ファイルを閉じる操作は、すべての書き込みバッファをファイル サーバにフラッシュし、すべてのアップデートがファイル サーバに伝達されたあとでは、閉じる要求だけが許可されます。一貫性の観点から、ファイルを開くときの有効性とファ

イルを閉じるときのフラッシュとの組み合せにより、OS を介してハードウェアにアクセスするアプリケーション（Microsoft Office など）がセッションとして動作することが保証されます。WAAS ネットワークでは、開く、ロック、編集、ロック解除、および閉じるコマンドが正しく動作することが保証されます。

- 経過時間に基づくディレクトリの検査（CIFS）: ディレクトリは、設定済みの経過時間に関連付けられています。経過時間が経過すると、Edge WAE キャッシュはディレクトリを再検査します。

  ユーザが初めてディレクトリの内容を表示しようとすると、Edge WAE は、ファイル サーバがユーザとグループのアクセス権を含むディレクトリの Access Control List（ACL; アクセス コントロール リスト）を使用して、許可検査を実行できるようにします。Edge WAE は、ユーザがどのディレクトリにアクセスし、ファイル サーバがそのアクセスを許可したかどうかをモニタします。ユーザが短時間（経過時間）の間に同じディレクトリにアクセスしようとした場合、Edge WAE ファイル サーバにアクセスせず、代わりにキャッシュされたアクセス権を使用してユーザにアクセスを提供するかどうかを決定します。経過時間が経過すると、Edge WAE はファイル サーバにアクセスして、キャッシュされたユーザのアクセス権をリフレッシュします。

  この許可プロセスは、ユーザがファイル サーバでアクセスする許可を持っていないキャッシュ内のディレクトリやファイルにアクセスすることを防止します。

データ並列性

並列性制御は、複数のユーザがキャッシュされた同じデータに読み取り、書き込み、またはその両方のアクセスを行うときに重要です。並列性制御は、ファイル システム ロックを確立および削除して、このアクセスを同期化します。このファイル ロック機能は、データ整合性を保証し、次の利点があります。

- クライアントは、リモート ファイル サーバからデータを取得しなくてもよいように、積極的にファイル データをキャッシュできます。
- 既存の CIFS クライアント実装で動作する多くのアプリケーションのパフォーマンスを改善します。
- 一度に 1 人のユーザだけがファイルのセクションを変更できるので、データ整合性が維持されます。

WAAS ソフトウェアは、ネットワーク帯域幅を使用して WAN 経由でファイル サーバでデータの読み取りや書き込みを実行する代わりに、ローカル キャッシュで安全にデータの読み取りや書き込みを実行できるように、ユーザがファイルをロックできる CIFS oplock 機能をサポートしています。oplock を使用すると、ユーザは、他のユーザがファイルにアクセスしていないことがわかっているため、キャッシュされたデータが古くなることなく、事前に先行読み出しデータをキャッシュできます。また、ユーザは、ローカル キャッシュにデータを書き込むことができ、ファイルを閉じるまで、または別のユーザが同じファイルを開くように要求するまで、ファイル サーバをアップデートする必要がありません。

oplock は、ファイルだけに適用されます。ファイル サーバは、ディレクトリと名前付きパイプに oplock 要求を許可しません。

ファイル ロック プロセス

ユーザがファイルを開くと、ロック要求がファイル サーバへ送信されます。Edge WAE は、ユーザからファイル サーバへのすべてのロック要求とファイル サーバからユーザへのすべての応答を代行受信し、転送します。他のユーザがファイルにロックを設定していない場合、ファイル サーバは、ユーザが安全にファイルをキャッシュできるように排他ロック要求を許可します。

別のユーザが同じファイルを開くように要求すると、次の処理が実行されます。

1. ファイル サーバは、最初のユーザが取得した排他的ファイル ロックを取り消します。
2. 最初のユーザは、次の処理を実行します。

- キャッシュに保存されたファイルの変更をファイル サーバにフラッシュします。この処理により、ファイルを開く 2 番めのユーザがファイル サーバから最新の情報を受信することが保証されます。
- 別のユーザがファイルを開いたためにそのデータの最新性が保証されないため、ファイル用の先行読み出しバッファを削除します。

3. ファイル サーバは、2 番めのユーザにファイルを開くことを許可します。

Microsoft 製品との相互運用性

WAAS ファイル サービス機能は、次の Microsoft CIFS 機能と相互運用できます。

- ユーザ認証と許可用の Active Directory
- Microsoft CIFS のオフライン フォルダ
- Microsoft DFS インフラストラクチャ
- 「共有フォルダ用の Windows シャドウ コピー」（P.11-7）の説明に従う共有フォルダ用の Windows シャドウ コピー

共有フォルダ用の Windows シャドウ コピー

WAAS ファイル サービスは、Windows Server 2003/2008 オペレーティング システムの一部である共有フォルダ用のシャドウ コピー機能をサポートしています。この機能は、Microsoft Volume Shadow Copy Service を使用して、ユーザが前バージョンのフォルダやファイルを簡単に表示できるように、ファイル システムのスナップショットを作成します。

WAAS 環境では、ユーザは、ネイティブ Windows 環境と同様に、Edge WAE からフォルダまたはファイルを右クリックし、[Properties] > [Previous Version] を選択して、シャドウ コピーを表示します。

機能の制限事項を含む共有フォルダ用のシャドウ コピーの詳細については、Microsoft Windows Server 2003/2008 の資料を参照してください。

ユーザは、Edge WAE 上のシャドウ コピー フォルダにアクセスするとき、ファイル サーバ上のネイティブ環境と同じ作業を実行できます。これらの作業は、次のとおりです。

- シャドウ コピー フォルダの参照
- シャドウ コピー フォルダの内容のコピーまたは復元
- シャドウ コピー フォルダ内のファイルの表示およびコピー

共有フォルダ機能用のシャドウ コピーは、次の作業をサポートしていません。

- シャドウ コピー ディレクトリの名前の変更または削除
- シャドウ コピー ディレクトリ内のファイルの名前の変更、作成、または削除

サポートされるサーバおよびクライアント

WAAS は、次のファイル サーバで共有フォルダ用のシャドウ コピーをサポートしています。

- Windows Server 2008 および Windows Server 2008 R2
- Windows Server 2003（SP1 付き、SP1 なし）
- NetApp Data ONTap バージョン 6.5.2、6.5.4、7.0、および 7.3.3
- EMC Celerra バージョン 5.3、5.4、および 5.6

WAAS は、次のクライアント用の共有フォルダ用のシャドウ コピーをサポートしています。

- Windows 7
- Windows Vista
- Windows XP Professional
- Windows 2000（SP3 以降）
- Windows 2003

（注）　Windows 2000 および Windows XP（SP2 なし）クライアントでは、共有フォルダ用のシャドウ コピーをサポートするために、前バージョンのクライアントをインストールする必要があります。

ファイル サービスの準備

WAE でファイル サービスを有効にする前に、必ず、次の作業を完了してください。

- 同一の設定で複数のデバイスを設定する場合は、ファイル サービスを有効にするすべてのエッジ デバイスを含むデバイス グループを作成したことを確認します。デバイス グループを作成する方法については、第 3 章「デバイス グループとデバイス位置の使用」を参照してください。
- ファイル サービスを有効にするエッジ デバイスを識別します。エッジ デバイスは、ローカル ファイル サーバを他のエッジ デバイスへエクスポートする場合、コア デバイスとしても機能できます。
- エクスポートするファイル サーバを識別し、表 11-1 を参照して、これらのファイル サーバが WAAS ソフトウェアによって動作できることを確認します。これ以外のファイル サーバは WAAS によって動作する可能性はありますが、表に示されたファイル サーバだけがテスト済みです。ファイル サーバは、opportunistic locking（oplocks）および CIFS 通知をサポートしている必要があります。

（注）　WAAS ファイル サービス機能では、FAT32 ファイル システムを使用するファイル サーバはサポートされません。ポリシー エンジン規則を使用して、FAT32 ファイル システムを使用するすべてのファイル サーバを CIFS 最適化から除外できます。

表 11-1　テスト済みのファイル サーバ

ベンダー	製品	バージョン
Dell	PowerVault	715N
Network Appliance	FAS3140	ONTAP 7.3.3
	FAS940	ONTAP 7.0.1R.1
	FAS270	ONTAP 7.0.1R.1
	FAS250	ONTAP 7.0.1R.1
	F760	6.5.2R1P16
	F85	6.4.5
EMC	Celerra NS702	5.4.17.5
	Celerra NS702	5.4.14-3
	Celerra NS700	5.6.42-5
	Celerra NS501	5.3.12-3
Microsoft	Windows NT 4.0	
	Windows Server 2000	サービス パックなし、SP1、SP3、および SP4
	Windows Server 2003	サービス パックなし、SP1、SP2、および R2
	Windows Server 2008[1]	SP1 および R2
Novell[2]	6.5	SP-3
RedHat	Samba	3.0.1.4a

1. Vista クライアントの場合、WAAS は SMB1 プロトコルを透過的に使用します。
2. WAAS は、NCP、eDirectory/NDS、および iPrint 用の CIFS 最適化、サーバ統合、および汎用のネットワーク加速のために、Novell6.5 をサポートしています。Novell ファイル サーバが NFAP オプションを使用する場合、WAAS は、WAAS CIFS アダプタを使用して、プロトコル層とトランスポート層で Novell トラフィックを最適化できます。NFAP は、Novell の NCP（Novell Core Protocol）のほかに CIFS プロトコルを使用する Novell のネイティブ ファイル アクセス パックです。

（注）　ファイル サーバでのオペレーティング システムとファイル システムの組み合わせによっては、サーバが異なる SMB コマンドに対して異なるタイムスタンプ精度で応答する可能性があります。このような状況では、CIFS アプリケーション アクセラレータがデータの一貫性を維持するためキャッシュされたファイルを一致しないタイムスタンプで使用することを回避した場合、最大限の CIFS 最適化性能を得られない可能性があります。

NME-WAE でのファイル サービスの使用

Cisco アクセス ルータに搭載したネットワーク モジュールで WAAS を稼動している場合は、ファイル サービスをサポートするために特定のメモリ要件があります。NME-WAE では、ファイル サービスをサポートするため次のメモリ量が搭載されている必要があります。

- 透過的 CIFS アクセラレータ モード：1GB RAM
- レガシー モード、Edge ファイル サービス：1GB RAM
- レガシー モード、Core（または Edge および Core の両方）ファイル サービス：2GB RAM

デバイスに十分なメモリがないときにファイル サービスを有効にしようとすると、WAAS Central Manager はエラー メッセージを表示します。

[Device Dashboard] ウィンドウで、デバイスのメモリ量を確認できます。詳細については、「[Device Dashboard] ウィンドウ」（P.16-9）を参照してください。

ファイル サービスの設定

WAAS バージョン 4.1.1 以降では、設定方法が異なる、相互に排他的な 2 つの WAFS モードをサポートしています。

- 透過的 CIFS アクセラレータ モード：このモードでは、コア、エッジ、または接続の設定が不要です。このモードは自動ディスカバリに依存し、設定する必要はなく、CIFS トラフィックを透過的に加速します。使いやすさという点から、このモードを推奨します。

  表 11-2 に、透過的 CIFS アクセラレータ モードを設定するために完了する必要がある手順の概要を示します。このモードを使用することにより、この章にあるほとんどの設定手順を省略できます。

- レガシー モード：このモードでは、Core クラスタ、Edge ファイル サービス、および Core デバイスと Edge デバイス間の接続を設定する必要があります。複数の WAAS 4.0.x デバイスを相互運用する必要がある場合、または切断モードでの動作が必須である場合は、このモードを使用します。

動作中の WAAS デバイスでこの 2 種類の WAFS モードを切り替えるには、「ファイル サービス モードの切り替え」（P.11-37）を参照してください。

（注）　レガシー モード WAFS は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー モード WAFS を有効にすると、Central Manager 上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー WAFS の何らかの設定値を設定しようとした場合に警告されます。レガシー WAFS をお使いの場合は、透過的 CIFS アクセラレータに移行してください。

表 11-3 に、ファイル サービスを設定するために完了する必要がある手順の概要を提供します。

表 11-2　透過的モードのファイル サービスを設定するためのチェックリスト

作業	追加情報と手順
1. ファイル サービスを準備する。	WAAS デバイスでファイル サービスを有効にし、設定する前に、完了する必要がある作業を提供します。詳細については、「ファイル サービスの準備」（P.11-8）を参照してください。
2. CIFS アクセラレーションを有効化する。	透過的 CIFS アクセラレータを有効化します。詳細については、「グローバル最適化機能の有効化と無効化」（P.12-2）を参照してください。
3. （任意）ダイナミック共有を識別する。	エクスポートされたファイル サーバで、ダイナミック共有を識別します。ファイル サーバにダイナミック共有がない場合は、この手順を省略できます。 詳細については、「ダイナミック共有の作成」（P.11-21）を参照してください。
4. （任意）事前配置ディレクティブを作成する。	エクスポートされたファイル サーバから Edge WAE キャッシュへどのファイルを予防的にコピーするかを定義します。詳細については、「事前配置ディレクティブの作成」（P.11-26）を参照してください。

表 11-3　レガシー モードのファイル サービスを設定するためのチェックリスト

作業	追加情報と手順
1. ファイル サービスを準備する。	WAAS デバイスでファイル サービスを有効にし、設定する前に、完了する必要がある作業を提供します。詳細については、「ファイル サービスの準備」（P.11-8）を参照してください。
2. WAFS コア クラスタを設定する。	WAFS コア クラスタは、エクスポートされたファイル サーバから Edge WAE のキャッシュへデータをコピーする必要があります。詳細については、「コア クラスタの設定」（P.11-11）を参照してください。
3. エッジ デバイスを設定する。	デフォルトで、ファイル サービスは、WAAS デバイスで有効になっていません。エッジ デバイスでファイル サービスを有効にし、開始するには、「エッジ デバイスの設定」（P.11-14）を参照してください。
4. （任意）ファイルサーバを WAAS Central Manager に登録する。	どのファイル サーバをエクスポートするかを WAAS システムに指定します。また、この手順は、コア クラスタと登録したファイル サーバ間のリンクを作成します。詳細については、「Edge WAE キャッシュへエクスポートするためのファイル サーバの設定」（P.11-17）を参照してください。自動ディスカバリを使用している場合、この手順はオプションです。
5. （任意）ダイナミック共有を識別する。	エクスポートされたファイル サーバで、ダイナミック共有を識別します。ファイル サーバにダイナミック共有がない場合は、この手順を省略できます。 詳細については、「ダイナミック共有の作成」（P.11-21）を参照してください。
6. コア クラスタとエッジ デバイス間の接続を作成する。	コア クラスタが Edge WAE キャッシュへデータをコピーできるようにします。詳細については、「コア クラスタと Edge WAE 間の接続の作成」（P.11-23）を参照してください。
7. （任意）事前配置ディレクティブを作成する。	エクスポートされたファイル サーバから Edge WAE キャッシュへどのファイルを予防的にコピーするかを定義します。詳細については、「事前配置ディレクティブの作成」（P.11-26）を参照してください。

コア クラスタの設定

レガシー モードでファイル サービスを設定する最初の手順では、デバイスでコア サービスを有効にし、デバイスをコア クラスタに割り当てます。コア クラスタには、エクスポートされたファイル サーバ（または複数のファイル サーバ）から Edge WAE のキャッシュへデータをコピーする役割があります。後続の各セクションで、クラスタがどのファイル サーバをエクスポートし、どのエッジ デバイスをキャッシュされたデータで満たすかがわかるように、エッジ デバイスとファイル サーバ（任意）をこのコア クラスタに割り当てます。

ステップ 1 ～ 7 で、コア サーバ サービスを有効にし、デバイスをコア クラスタに割り当てます。ステップ 8 ～ 12 で、新しいコア クラスタを設定します。この手順の最後の手順で、デバイスが Core WAE として機能するために必要なデバイスをリロードする方法について説明します。

WAFS コア クラスタを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

[Devices] ウィンドウに、WAAS システムに作成されているデバイスのリストが表示されます。

ステップ 2　新しいコア クラスタに含めるデバイスの横にある [Edit] ボタンをクリックします。

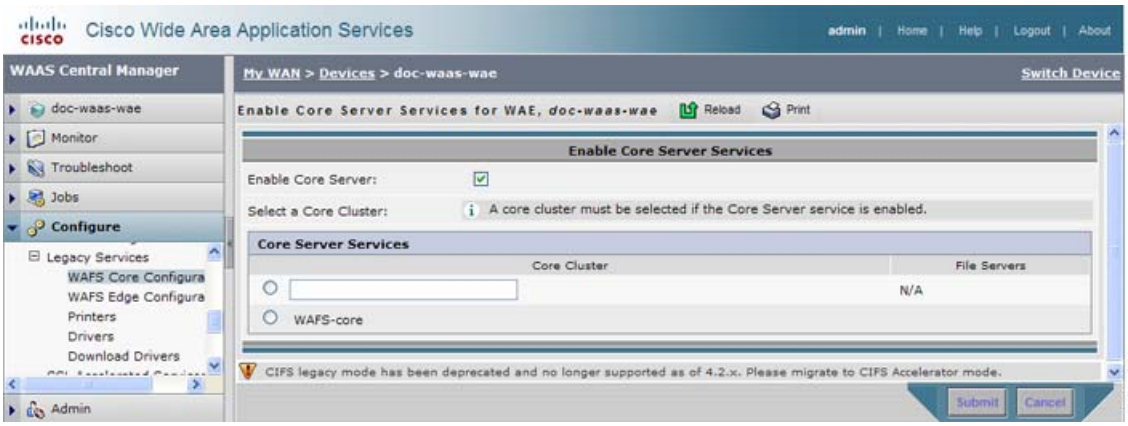
[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Service] > [WAFS Core Configuration] を選択します。

[Enable Core Server Services] ウィンドウが表示されます（図 11-2 を参照）。

（注）　CIFS アクセラレータが有効な場合は、コア サーバを設定できません。

図 11-2　　コア サーバ サービスの有効化



ステップ 4　[Enable Core Server] チェックボックスを選択します。

ステップ 5　コア クラスタの横にあるオプション ボタンを選択して、このデバイスをそのコア クラスタに割り当てます。既存のコア クラスタがない場合は、このデバイス用の新しいレガシー WAFS コア クラスタを作成する必要があります。「新しいデバイス グループの作成」（P.3-3）を参照してください。

ステップ 6　[Submit] をクリックします。

デバイスがコア サーバとして機能するために、手動でデバイスをリブートする必要があることを知らせるポップアップ メッセージが表示されます。

ステップ 7　ポップアップ メッセージを読んだら、[OK] をクリックします。

デバイスでコア サーバ サービスが有効になり、デバイスが指定したコア クラスタに参加します。この手順の最後で、コア サービスをアクティブにするために必要なデバイスをリブートする方法について説明します。

ポップアップ メッセージで [Cancel] をクリックすると、[Enable Core Server window] ウィンドウへ戻り、変更は送信されません。

ファイル サーバを明示的に登録する代わりに自動ディスカバリ機能に依存していて、オプションの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）を設定する必要がない場合、ステップ 14 に進みます。

ステップ 8　WAAS Central Manager GUI の右上部にある [Home] リンクをクリックして、グローバル コンテキストに戻り、ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。

ステップ 9　新しいコア クラスタの横にある [Edit] アイコンをクリックします。

ステップ 10　ナビゲーション ペインで、[Cluster Name] > [Core Server Settings] を選択します。[Configure Core Server Settings] ウィンドウが表示されます（図 11-3 を参照）。

図 11-3　コア クラスタの設定例

ステップ 11　[File Server access username]、[File Server access password]、および [Confirm password] の各フィールドに、このコア クラスタの一部として設定されるすべての CIFS ファイル サーバに対して使用されるアクセス情報を入力します。事前配置については、入力したアクセス クレデンシャルによって事前配置されるルート ディレクトリおよびその親ディレクトリへの読み取りアクセスが許可される必要があります。

ファイル サーバを明示的に登録する代わりに自動ディスカバリ機能に依存している場合、これらのフィールドは必要ありません。

「Edge WAE キャッシュへエクスポートするためのファイル サーバの設定」（P.11-17）で、このコア クラスタがどのファイル サーバにエクスポートするかを指定します。

ステップ 12　（任意）次のように、優先順位の高いメッセージ用の DSCP 値を設定します。

a.　[Set DSCP value for high priority messages] チェックボックスを選択します。

b.　次のいずれかのオプションを選択します。

- [Match Edge]：このコア クラスタに接続している Edge WAE の DSCP 値と照合します。この照合は、「コア クラスタと Edge WAE 間の接続の作成」（P.11-23）の説明に従ってエッジ デバイスとコア デバイス間の接続を作成するときに実行されます。
- [DSCP Value]：このコア クラスタ用の DSCP 値を指定できます。

  ドロップダウン リストから値を選択し、サポートされている値の説明について表 11-4（P.11-16）を参照します。ドロップダウン リストから [Please Make a Choice] を選択する場合は、対応するフィールドに 0 ～ 63 の値を入力します。

DSCP は、ネットワーク トラフィックに異なるレベルのサービスを割り当てることができる IP パケットのフィールドです。ネットワーク上の各パケットに（表 11-4 に示す）DSCP コードを付け、対応するサービスのレベルを関連付けて、サービスのレベルを割り当てます。DSCP は、IP precedence フィールドと Type of Service（ToS; タイプ オブ サービス）フィールドの組み合せです。詳細については、RFC 2474 を参照してください。

システムのパフォーマンスを改善するために、WAFS 制御トラフィック用の DSCP 値を設定することを推奨します。それには、QoS マーキングを実施するようにルータを設定する必要があります。

ステップ 13　[Submit] をクリックします。

ステップ 14　タスクバーの [Reload WAE] アイコンをクリックするか、次の手順を実行して、デバイスをリロードします。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

b. コア サービスを有効にしたデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

c. タスクバーの [Reload WAE] アイコンをクリックします。デバイスがリブートし、デバイスでコア サービスがアクティブになります。

エッジ デバイスの設定

コア クラスタを作成し、設定したら、次の手順で（レガシー モードの場合）、キャッシュにエクスポートされたファイル サーバ データを含むエッジ デバイスを設定します。

デバイスまたはデバイス グループでエッジ サーバを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

（注）　ネットワークで Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）が有効になっている場合は、エッジ デバイス グループでファイル サービスを有効にすることを推奨します。WCCP が無効になっている場合は、名前の競合を防止するために、個々のエッジ デバイスでファイル サービスを有効にする必要があります。

ステップ 2　ファイル サービスを有効にするデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

選択したオプションに応じて、[Device Dashboard] ウィンドウまたは [Modifying Device Group] ウィンドウが表示されます。

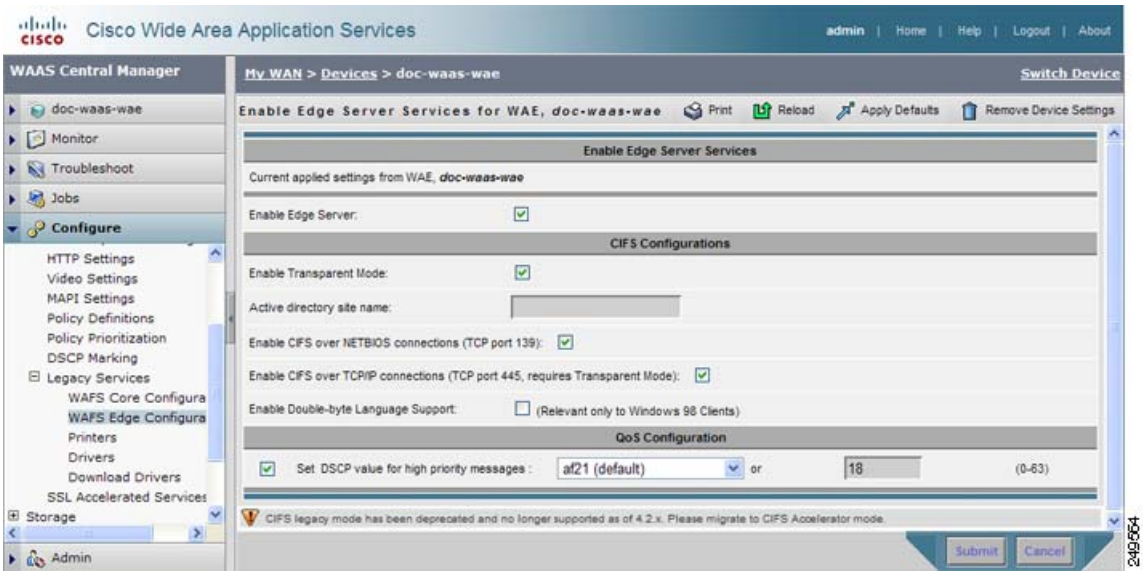
WAAS Central Manager デバイスでは、エッジ サービスを有効にできません。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Service] > [WAFS Edge Configuration] を選択します。

[Enable Edge Server Services] ウィンドウが表示されます（図 11-4 を参照）。

（注）　CIFS アクセラレータが有効な場合は、エッジ サーバ サービスを設定できません。

図 11-4　エッジ デバイス上のファイル サービスの有効化



ステップ 4　[Enable Edge Server] チェックボックスを選択します。

ウィンドウの他のフィールドが有効になります。

ステップ 5　ネットワークで WCCP または PBR が有効になっている場合、またはインライン モードを使用している場合は、[Enable Transparent Mode] チェックボックスを選択します。

トランスペアレント モードが有効になっているかどうかに基づいて、ポート 139 と 445 を有効にするためのオプションが自動的にアップデートされます。

トランスペアレント モードを有効にすると、TCP ポート 139 とポート 445 を有効にするためのオプションが自動的に選択されます。トランスペアレント モードを無効にすると（[Enable Transparent Mode] を選択しないと）、TCP ポート 139 を有効にするオプションは選択され、ポート 445 はトランスペアレント モードだけで使用されるため、TCP ポート 445 を有効にするオプションは選択されません。

ステップ 6　提供されるフィールドに、Active Directory サイトの名前を入力します。

ステップ 7　次のオプションを選択して（少なくとも 1 つは選択する必要がある）、Edge WAE で関連するポートを有効にします。

- [Enable CIFS over NETBIOS connections (tcp port 139)] : クライアントと Edge WAE 間およびコア クラスタとファイル サーバ間でポート 139 が開いている場合、このオプションを選択します。

  セキュリティ上の理由から、ネットワークでポート 139 が開いていない場合は、このオプションの選択を解除し、次の作業を実行します。

  - ルータ と Edge WAE で WCCP を有効にするか、または Edge WAE でインライン モードを有効にします。詳細については、第 4 章「トラフィック代行受信の設定」を参照してください。
  - [Enable CIFS Over TCP/IP Connections] チェックボックスを選択して、Edge WAE 上のポート 445 を有効にします。
- [Enable CIFS over TCP/IP connections (tcp port 445, requires Transparent Mode)] : ネットワークでポート 445 が開いている場合は、このオプションを選択します。

  ネットワークでポート 445 が閉じている場合は、Edge WAE がこのポートで接続を確立しようと試みないようにこのオプションの選択を解除し、[Enable CIFS over NETBIOS connections] チェックボックスを選択します。

  ポート 445 を無効にすると、すべてのクライアントが Edge WAE のポート 139 に直接接続し、コア クラスタはファイル サーバのポート 139 に接続します。

（注）　ポート 139 とポート 445 上の接続を有効または無効にしても、既存のクライアントは Edge WAE との接続を失いません。

ステップ 8　日本語のような 2 バイト言語をサポートする必要がある Windows 98 クライアントがある場合は、[Enable Double-byte Language Support] チェックボックスを選択します。

次の状況では、このオプションを選択しないでください。

- 環境に Windows 98 クライアントが存在しない。
- 環境に Windows 98 クライアントが存在するが、1 バイト言語をサポートするだけでよい。

このオプションの設定に関係なく、英語は常にサポートされています。

ステップ 9　（任意）次の手順に従って、優先順位の高いメッセージ用の DSCP 値を設定します。

a. [Set DSCP value for high priority messages] チェックボックスを選択します。

b. ドロップダウン リストから値を選択します。サポートされている値の説明については、表 11-4 を参照してください。

ドロップダウン リストから [Please Make a Choice] を選択する場合は、対応するフィールドに 0 ～ 63 の値を入力します。

DSCP は、ネットワーク トラフィックに異なるレベルのサービスを割り当てることができる IP パケットのフィールドです。ネットワーク上の各パケットには DSCP コード（表 11-4 に示す）が付き、対応するサービスのレベルが割り当てられます。DSCP は、IP precedence フィールドと Type of Service（ToS; タイプ オブ サービス）フィールドの組み合せです。詳細については、RFC 2474 を参照してください。

システムのパフォーマンスを改善するために、WAFS 制御トラフィック用の DSCP 値を設定することを推奨します。それには、QoS マーキングを実施するようにルータを設定する必要があります。

表 11-4　DSCP コード

DSCP コード	説明
af11	AF11 dscp（001010）でパケットを設定します。
af12	AF11 dscp（001100）でパケットを設定します。
af13	AF13 dscp（001110）でパケットを設定します。
af21	AF21 dscp（010010）でパケットを設定します。
af22	AF22 dscp（010100）でパケットを設定します。
af23	AF23 dscp（010110）でパケットを設定します。
af31	AF31 dscp（011010）でパケットを設定します。
af32	AF32 dscp（011100）でパケットを設定します。
af33	AF33 dscp（011110）でパケットを設定します。
af41	AF41 dscp（100010）でパケットを設定します。
af42	AF42 dscp（100100）でパケットを設定します。
af43	AF43 dscp（100110）でパケットを設定します。
cs1	CS1（優先順位 1）dscp（001000）でパケットを設定します。
cs2	CS2（優先順位 2）dscp（010000）でパケットを設定します。
cs3	CS3（優先順位 3）dscp（011000）でパケットを設定します。

表 11-4　DSCP コード （続き）

DSCP コード	説明
cs4	CS4（優先順位 4）dscp（100000）でパケットを設定します。
cs5	CS5（優先順位 5）dscp（101000）でパケットを設定します。
cs6	CS6（優先順位 6）dscp（110000）でパケットを設定します。
cs7	CS7（優先順位 7）dscp（111000）でパケットを設定します。
default	デフォルトの dscp（000000）でパケットを設定します。
ef	EF dscp（101110）でパケットを設定します。

ステップ 10　[Submit] をクリックします。デバイスがエッジ サーバとして機能するために、手動でデバイスをリブートする必要があることを知らせるポップアップ メッセージが表示されます。

ステップ 11　ポップアップ メッセージを読んだら、[OK] をクリックします。デバイスでエッジ サーバ サービスが有効になります。

ポップアップ メッセージで [Cancel] をクリックすると、[Edge Configuration] ウィンドウへ戻り、変更は送信されません。

ステップ 12　タスクバーの [Reload WAE] アイコンをクリックするか、次の手順を実行して、デバイスをリロードします。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

b. エッジ サービスを有効にしたデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

c. タスクバーの [Reload WAE] または [Reboot All Devices] アイコンをクリックします。デバイスがリブートし、デバイスでエッジ サービスがアクティブになります。

Edge WAE キャッシュへエクスポートするためのファイル サーバの設定

レガシー モードの場合は、コア クラスタと Edge WAE でファイル サービスを有効にしたら、オプションで WAAS Central Manager GUI を使用して、エクスポートするファイル サーバを設定できます。ネットワークに WAAS ネットワークに定義する必要がある多くのファイル サーバが存在する（たとえば 10 台以上）場合は、プロセスを高速化するために、Comma-Separated Values（CSV; カンマ区切り形式）ファイルを作成し、インポートできます。

ファイル サーバを設定せずにレガシー モードを使用する場合は、レガシー モードの自動ディスカバリ機能を依存することにより、ユーザがファイル サーバにアクセスしたときに WAFS が自動的にファイルサーバを検出できます。ファイル サーバを明示的に登録しない場合は、この項を省略できます。

このセクションには、WAAS Central Manager GUI でファイル サーバを設定するための次の項目があります。

- 「WAAS Central Manager を使用したファイル サーバの登録」（P.11-18）
- 「CSV ファイルを使用したファイル サーバ定義のインポート」（P.11-18）

- 「登録したファイル サーバへのコア クラスタの割り当て」（P.11-20）
- 「ダイナミック共有の作成」（P.11-21）

WAAS Central Manager を使用したファイル サーバの登録

WAAS Central Manager にファイル サーバを登録するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [File Servers] を選択します。[File Servers] ウィンドウが表示されます。

このウィンドウから、次の作業を実行できます。

- ファイル サーバの横にある [Edit] アイコンをクリックして、既存ファイルサーバの設定を編集します。次に、ファイル サーバ設定を削除したり、任意のファイル サーバ設定を変更できます。
- タスク バーの [Import from CSV] アイコンをクリックし、CSV ファイルから複数のファイル サーバ定義をインポートします（「CSV ファイルを使用したファイル サーバ定義のインポート」（P.11-18）を参照）。
- 次の手順の説明に従って、エクスポートする新しいファイル サーバを識別します。

ステップ 2　タスクバーの [Create New File Server] アイコンをクリックして、エクスポートする新しいファイル サーバを識別します。[Registering New File Server] ウィンドウが表示されます

ステップ 3　[File Server Name] フィールドに、エクスポートするファイル サーバのホスト名を入力します。サーバの NetBIOS 名、DNS 名、または IP アドレスを入力できます。

（注）　同じファイル サーバを複数回登録することはできません。

ステップ 4　[Allow Access on WAN Failure] チェックボックスを選択して、CIFS クライアントが WAN 障害時にこの Edge WAE にキャッシュされたデータに読み取り専用でアクセスできるようにします。

このオプションを有効にすると、WAN 障害が発生した場合に、CIFS クライアントは、キャッシュされるディレクトリ構造を参照し、キャッシュされたファイル全体を読み取ることができます。その間、認証と許可は維持されます。

詳細については、「WAN 障害に対する WAAS ネットワークの準備」（P.11-35）を参照してください。

ステップ 5　[Submit] をクリックします。

ファイル サーバが WAAS システムに登録され、ナビゲーション ペインが追加オプションでリフレッシュされます。

ステップ 6　「登録したファイル サーバへのコア クラスタの割り当て」（P.11-20）に進み、登録したファイル サーバにコア クラスタを割り当てます。

CSV ファイルを使用したファイル サーバ定義のインポート

ネットワークに WAAS ネットワークに定義する必要がある多くのファイル サーバが存在する（たとえば 10 台以上）場合は、プロセスを高速化するために、CSV ファイルを作成し、インポートできます。Excel または別の表計算アプリケーションを使用して、CSV ファイルを作成できます。

ここでは、次の内容について説明します。

- 「CSV ファイルの作成要件」（P.11-19）
- 「CSV ファイルに関する留意事項」（P.11-19）

- 「CSV ファイルのインポート」（P.11-20）

CSV ファイルの作成要件

表 11-5 に、CSV ファイルの要件を示します。

表 11-5　CSV ファイルの要件

列見出し	構文 / 意味	説明
Name	ファイル サーバの名前を指定します。[Registering New File Server] ウィンドウの [File Server Name] フィールドに対応しています。	必須。 「WAAS Central Manager を使用したファイル サーバの登録」のステップ 3 と同じ制約。
AllowDisconnected	[Registering New File Server] ウィンドウの [Allow access on WAN Failure] チェックボックスに対応しています。適用する場合は「true」に、適用しない場合は「false」に設定します。	任意。 指定しないと、「false」になります。
Cluster	ファイル サーバを割り当てる既存のコア クラスタの名前を指定します。	任意。 指定しないと、ファイル サーバはコア クラスタに割り当てられません。 クラスタ名が複数回ファイル サーバに割り当てられている場合、エラー報告されません。

CSV ファイルに関する留意事項

CSV ファイルを作成するときは、次の点に注意してください。

- 最初の行には、指定する列見出しを列挙する必要があります。
- 少なくとも、ファイルには「Name」列が必要です（他の列は任意です）。
- 列見出しは大文字と小文字を区別せず、任意の順序で指定できます。
- ファイル サーバを複数のコア クラスタに割り当てるには、複数の「Cluster」列を指定できます。データ行に複数のクラスタを指定する場合は、カラム見出し行に複数の「Cluster」列が必要です。
- 行を指定するときは、各列に値を入れる必要はありません。ただし、正しい数の列を指定する必要があります。つまり、列の数は、見出し行に定義されるオブジェクトの数と対応する必要があります。次の例は、有効な CSV ファイル エントリを示しています（コア クラスタ c-1、c-2、および c-5 が存在すると仮定しています）。カンマが連続する位置は、デフォルト値が使用されることを示します。

  例：

  ```
  name,allowdisconnected,cluster,cluster
  s71,TRUE,c-1,
  s72,,c-2,c-5
  ```

CSV ファイルのインポート

CSV ファイルを作成したら、WAAS Central Manager GUI を使用してファイルをインポートします。

CSV ファイルをインポートするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [File Servers] を選択します。

ステップ 2　タスク バーの [Import from CSV] アイコン（  ）をクリックします。

[Importing File Server Definitions] ウィンドウが表示されます。

ステップ 3　[Browse] をクリックします。

[Choose File] ウィンドウが表示されます。

ステップ 4　インポートする CSV ファイルまでナビゲートし、選択し、[Open] をクリックします。[Path to File Server Definitions] フィールドに、パスとファイル サーバ名が表示されます。

ステップ 5　[Importing File Server Definitions] ウィンドウで、[Submit] をクリックします。

CSV ファイルがインポートされ、「successfully imported」メッセージが表示されます。

WAAS Central Manager は、次の事項を確認します。

- ファイル見出しが正しい。
- 各行にファイル サーバ名がある。
- ファイルに少なくとも 1 台のファイル サーバが指定されている。
- すべての行に正しい数の列があり、各行の構文が正しい。

ファイルが上記の条件に適合しない場合、WAAS Central Manager にエラー メッセージが表示され、ファイル サーバはインポートされません。エラー メッセージは、最大 10 行のエラーの説明を提供できます。ただし、エラーが見出しやファイルの読み取り不能に関係している場合、それ以上のチェックは行われません。

登録したファイル サーバへのコア クラスタの割り当て

ファイルサーバを WAAS Central Manager に登録したら、少なくとも 1 つのコア クラスタをファイル サーバに割り当てる必要があります。コア クラスタには、Edge WAE のキャッシュへファイル サーバをエクスポートする役割があります。ファイル サーバを明示的に登録する代わりに自動ディスカバリ機能に依存している場合は、この手順を行う必要はありません。

登録したファイル サーバにコア クラスタを割り当てるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [File Servers] を選択します。

[File Servers] ウィンドウが表示されます。

ステップ 2　コア クラスタに割り当てるファイル サーバの横にある [Edit] アイコンをクリックします。

ステップ 3　[Core Cluster] タブをクリックします [Core Cluster Assignments] ウィンドウが表示されます。

[Core Cluster Assignments] ウィンドウは、WAAS ネットワークに設定されているデバイス グループを表示します。デフォルトで、10 のデバイス グループが表示されます。

ステップ 4　次のいずれかを実行して、コア クラスタをファイル サーバに割り当てます。

- タスクバーの  をクリックして、使用できるすべてのコア クラスタをファイル サーバに割り当てます。
- ファイル サーバに割り当てる各コア クラスタの横にある  をクリックします。選択すると、アイコンは  に変化します。

（注）　ファイル サーバには、コア クラスタだけを割り当てることができます。ファイル サーバには、（ で識別される）通常のデバイス グループを割り当てることができません。

ステップ 5　選択した WAFS コア クラスタ用の [Resolve File Server Name] アイコン（  ）をクリックします。このアイコンは [Type] 列の横にあり、ファイル サーバ用に入力した名前が IP アドレスに解決ができることを確認します。

このアイコンは、WAFS コア クラスタだけに使用できます。ファイル サーバ名を解決できない場合、[Comments] 列にエラー メッセージが表示されます。その場合は、ファイル サーバの正しい名前を入力したことを確認します。

ステップ 6　[Submit] をクリックします。

選択したコア クラスタの横にあるアイコンが  に変化します。

ステップ 7　（任意）追加したファイル サーバにダイナミック共有が含まれる場合は、「ダイナミック共有の作成」（P.11-21）を参照してください。

ファイル サーバにダイナミック共有が含まれるときは、WAAS Central Manager GUI でダイナミック共有を指定する必要があります。

ダイナミック共有の作成

多くのファイル サーバが、複数ユーザがユーザのクレデンシャルに基づいて自動的に別のディレクトリにマップされる同じ共有にアクセスできるダイナミック共有を使用します。一般に、ダイナミック共有は、ファイル サーバでユーザ ホーム ディレクトリを設定するために使用されます。たとえば、ファイル サーバでダイナミック共有として Home という名前のディレクトリを設定できます。この共有にアクセスする各ユーザは、自動的にそれぞれの個人用ディレクトリへリダイレクトされます。

ファイル サーバにダイナミック共有が含まれる場合は、このセクションの説明に従って、そのダイナミック共有を WAAS Central Manager に登録する必要があります。

WAAS Central Manager でダイナミック共有を指定すると、各ユーザが共有を異なるビューで表示できるようになります。Windows Server で設定した場合には、アクセス ベースの列挙操作が可能になります。

（注）　WAAS Central Manager でのダイナミック共有の設定により、CLI を使用して WAE デバイスで直接設定されたダイナミック共有設定が上書きされます。

ダイナミック共有を追加する前に、次の制限事項に注意してください。

- 各ダイナミック共有は、ファイル サーバで一意でなければなりません。
- 事前配置ディレクティブを持つダイナミック共有は、追加できません。ダイナミック共有を追加する前に、事前配置ポリシーを削除する必要があります。

- WAAS Central Manager GUI を使用すると、ダイナミック共有として任意のディレクトリを定義できます。ただし、ファイル サーバでダイナミック共有としてディレクトリを設定しないと、すべてのユーザが同じディレクトリから同じ内容を読み取り、または書き込みを行います。クレデンシャルに基づいて異なるディレクトリへリダイレクトされません。
- レガシー モードを使用している場合、同じファイル サーバ名および同じ共有名を持つ 2 つの異なるダイナミック共有を追加できますが、それぞれを別のコア クラスタに関連付ける必要があります。共有ごとに異なる ID を持ちます。
- レガシー モードを使用している場合、ダイナミック共有は、明示的に登録されたファイル サーバにのみ追加できます。透過的 CIFS アクセラレータ モードを使用している場合に限り、ダイナミック共有は自動検出されたファイル サーバでサポートされます。

ダイナミック共有を追加するには、次の手順に従ってください。

ステップ 1　ダイナミック共有を追加する前に、次の点を確認してください（レガシー モードを使用している場合のみ）。

- ダイナミック共有が、すでに CIFS ファイル サーバに設定されている。
- WAAS Central Manager GUI でファイル サーバを設定した。ファイル サーバを識別する方法の詳細については、「Edge WAE キャッシュへエクスポートするためのファイル サーバの設定」（P.11-17）を参照してください。

ステップ 2　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File Services] >[Dynamic Shares] を選択します。

ダイナミック共有のリストが表示されます。[Dynamic Shares] ウィンドウに設定されているすべてのダイナミック共有が示されます。このウィンドウから、次の作業を実行できます。

- 共有の横にある [Edit] アイコンをクリックして、既存のダイナミック共有の設定を編集します。ダイナミック共有を削除したり、任意のダイナミック共有設定を変更できます。
- 次の手順の説明に従って、新しいダイナミック共有定義を追加します。

ステップ 3　タスクバーの [Create New Dynamic Share] アイコンをクリックして、新しいダイナミック共有を追加します。[Creating a new Dynamic Share] ウィンドウが表示されます

ステップ 4　[Name] フィールドに、ダイナミック共有の名前を入力します。

ダイナミック共有名では、/、\、:、*、?、"、<、>、| は使用できません。
レガシー モードでは、英字、数字、アンダースコア（_）、およびハイフン（-）だけを使用できます。

ステップ 5　[Assigned Domain] ドロップダウン リストから、ダイナミック共有に割り当てる WAAS ドメインを選択します。このドメインにも割り当てられているユーザだけが、ダイナミック共有へのアクセス権を持ちます。

この種類の WAAS ドメインはエンティティを使用しません（ドメインを定義するとき、[Entity Type] で [None] を選択します）。ドメインの詳細については、「ドメインの操作」（P.7-14）を参照してください。

ステップ 6　（任意）レガシー モードを使用している場合、[CIFS - Use WAFS transport mode] チェックボックスを選択します。

このチェックボックスを選択した場合、透過的 CIFS アクセラレータ モードにだけ該当するフィールドがあるため、このウィンドウ内の特定のフィールドは表示されません。

ステップ 7　[File Server] フィールドで、ダイナミック共有を持つファイル サーバの名前を入力します。

[CIFS - Use WAFS transport mode] チェックボックスを選択した場合、テキスト フィールドは表示されません。その代わり、ドロップダウン リストには登録したファイル サーバが表示されます。ファイル サーバを登録する方法の詳細については、「WAAS Central Manager を使用したファイル サーバの登録」（P.11-18）を参照してください（透過的 CIFS モードでは、ファイル サーバの登録は必要ありません）。

ステップ 8　[User Name]、[Password]、および [Confirm Password] の各フィールドでは、ファイル サーバのユーザ名およびパスワードのクレデンシャルを入力します。ユーザ名が Windows ドメイン内に存在する場合、domain¥username のように [User name] フィールドの一部としてドメイン名を指定します（[CIFS - Use WAFS transport mode] チェックボックスを選択した場合、これらのフィールドは表示されません）。

これらのクレデンシャルは、[Browse] ボタンをクリックしたときにファイル サーバにアクセスするためだけに使用されます。

ステップ 9　[Share Name] フィールドで次のいずれかの作業を実行して、ダイナミック共有の位置を指定します。

- ファイル サーバでダイナミック共有の名前を入力します。共有名では、/、\、:、*、?、"、<、>、| は使用できません。
- [Share Name] フィールドの横にある [Browse] をクリックして、正しいルート ディレクトリまでナビゲートします。

（注）　レガシー モードで [Browse] ボタンを表示するには、ファイル サーバがコア クラスタに割り当てられ、クラスタに少なくとも 1 つの Core WAE が含まれる必要があります。この 2 つの条件に適合しない場合、レガシー モードで [Browse] ボタンは表示されません。透過的 CIFS アクセラレータ モードでは、WAAS Central Manager に登録済みで、有効な CIFS アクセラレータが搭載された WAE デバイスが 1 つ以上存在している場合のみ、[Browse] ボタンが表示されます。

ステップ 10　共有のステータスが enabled（有効）に設定されていることを確認します。ステータスを disabled（無効）に変更すると、共有は WAAS 環境でのダイナミック共有として設定されません。

ステップ 11　[Submit] をクリックします。

これで、指定したディレクトリは、Edge WAE キャッシュ上のダイナミック共有として機能します。

コア クラスタと Edge WAE 間の接続の作成

WAAS システムにファイル サーバを登録したら、コア クラスタと Edge WAE 間の接続を作成する必要があります（レガシー モードの場合）。この接続により、コア クラスタは、Edge WAE 上のキャッシュにファイルをコピーできます。

複数のコア クラスタと Edge WAE を含む接続を定義する前に、コア クラスタと Edge WAE の各リンクが、割り当て帯域幅や往復遅延のような同じ接続パラメータと同じエイリアス方式を持っていることを確認してください。このようになっていない場合は、リンクごとに個別の接続を定義する必要があります。

コア クラスタと 1 台または複数の Edge WAE 間の接続を作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] >[Connectivity] を選択します。

[Connectivity] ウィンドウが表示されます。

このウィンドウから、次の作業を実行できます。

- 接続の横にある [Edit] アイコンをクリックして、既存の接続の設定を編集します。接続を削除したり、任意の接続設定を変更できます。
- 次の手順の説明に従って、新しい接続を追加します。

ステップ 2　タスクバーの [Create New Connection] アイコンをクリックして、新しい接続を追加します。

[Creating a New Connection] ウィンドウが表示されます

ステップ 3　接続の名前を入力します。

ステップ 4　この接続に含めるコア クラスタの横にあるオプション ボタンを選択します。

ステップ 5　[Submit] をクリックします。

この接続用にファイル サーバをエクスポートしない場合は、エッジ デバイスやグループをこの接続に割り当てる前に、[File Server Settings] ウィンドウで各ファイル サーバの選択を解除する必要があることを知らせるメッセージが表示されます。

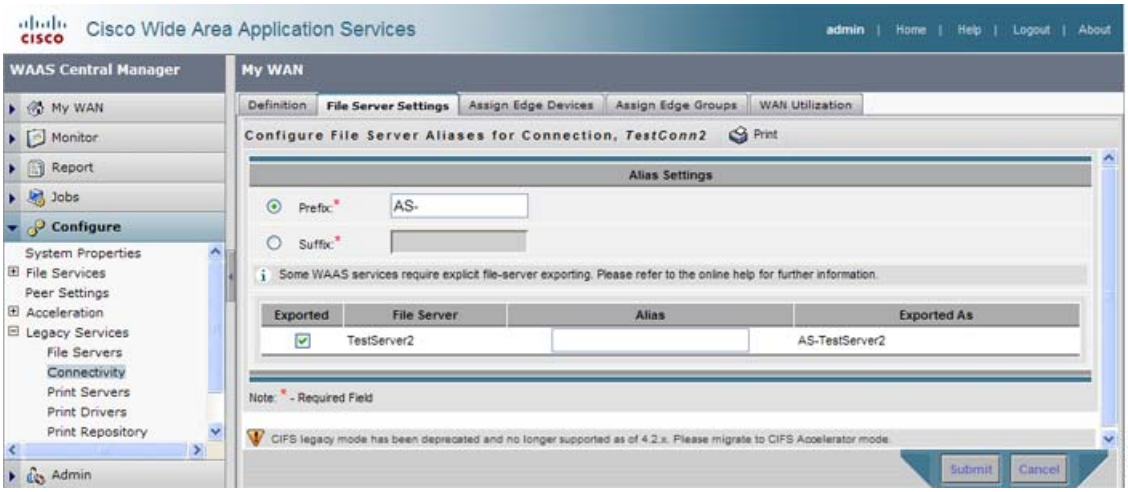
ステップ 6　メッセージを読んだら、[OK] をクリックします。

ファイル サーバを明示的に登録する代わりに自動ディスカバリ機能に依存している場合、ファイル サーバを設定する必要がないので、ステップ 12 に進みます。

ステップ 7　[File Server Settings] タブをクリックします。

[Configure File Server Aliases] ウィンドウが表示されます（図 11-5 を参照）。

図 11-5　ファイル サーバのエイリアスの設定



このウィンドウを使用すると、各ファイル サーバの命名方法を定義できます。元のファイル サーバ名、ファイル サーバ名 + プレフィクスまたは拡張子、または独自方式のエイリアスを使用できます。たとえば、プレフィクスとして **as-** を指定し、ファイル サーバの名前が **win3srv** の場合、このファイル サーバはユーザに **as-win3svr** として表示されます。

また、このウィンドウで、コア クラスタにエクスポートさせたいファイル サーバを選択できます。

ステップ 8　次のいずれかのオプションを選択して、プレフィクスまたは拡張子の値を指定します。

- [Prefix]：エクスポートされたファイル サーバのエイリアスの先頭に、入力したプレフィクスを追加します。
- [Suffix]：エクスポートされたファイル サーバのエイリアスの末尾に、入力した拡張子を追加します。

デフォルトで、WAAS は、ファイル サーバのエイリアスの先頭に AS- というプレフィクスを追加します。ブランクのプレフィクスや拡張子は、入力できません。ステップ 10 の説明に従ってエイリアスを指定すると、プレフィクスと拡張子の設定が上書きされます。

ステップ 9　この接続でエクスポートする各ファイル サーバの横にあるチェックボックスを選択します（少なくとも 1 つを選択する必要があります）。デフォルトで、すべてのファイル サーバが選択されます。

（注）　このウィンドウのファイル サーバが表示されない場合は、「登録したファイル サーバへのコア クラスタの割り当て」（P.11-20）の説明のように、このコア クラスタがファイル サーバに割り当てられていないことになります。先に進む前に、該当するセクションの手順を完了する必要があります。

ステップ 10　（任意）[Alias] 列に、選択したファイル サーバのエイリアスを入力します。

エイリアスには最大 15 文字の自由な名前を使用できますが、エイリアスはステップ 8 で定義したプレフィクスと拡張子のデフォルト設定を上書きします。

ステップ 11　[Submit] をクリックします。

[Exported As] 列に、エクスポートされた各ファイル サーバの名前が、エンド ユーザに表示されるように表示されます。

ステップ 12　次のいずれかのタブを実行します。

- [Assign Edge Devices]：個々のエッジ デバイスをこの接続に割り当てます。
- [Assign Edge Groups]：エッジ デバイス グループをこの接続に割り当てます。

選択したオプションに応じて、[Edge Device Assignments] ウィンドウまたは [Edge Group Assignments] ウィンドウが表示されます。

いずれのビューでも、割り当てウィンドウでは、リスト内の項目のビューをフィルタできます。フィルタにより、設定した基準に一致するリスト内の項目を見つけることができます。

ステップ 13　次のいずれかを実行して、この接続に入れるエッジ デバイスを選択します。

- タスクバーの をクリックして、使用できるすべてのエッジ デバイスまたはグループをこの接続に割り当てます。
- この接続に割り当てたい各エッジ デバイスまたはデバイス グループの横にある をクリックします。選択すると、アイコンは に変化します。

（注）　エッジ サービスが有効になっているエッジ デバイスまたはデバイス グループだけを割り当てることができます。通常のコア クラスタやオフライン デバイス（ で識別される）は、接続に割り当てることができません。エッジ サービスを有効にする方法については、「エッジ デバイスの設定」（P.11-14）を参照してください。

ステップ 14　[Submit] をクリックします。

選択した各エッジ デバイスまたはデバイス グループの横にあるアイコンが に変化します。

ステップ 15　（任意）この接続用の WAN 使用率設定を設定するには、次の作業を実行します。

a.　[WAN Utilization] タブをクリックします。[WAN Utilization] ウィンドウが表示されます。

b.　Edge WAE と Core WAE 間の WAFS トラフィックで使用される帯域幅を制御する次の WAN 使用率設定を定義します。

- [Maximum allocated bandwidth]：接続に割り当てる最大帯域幅（キロビット / 秒）を入力します。この値は、この接続での WAE 間の物理 WAN リンクの最大帯域幅以下でなければなりません。デフォルト設定は、1544 KB/ 秒です。WAFS は、帯域幅の使用をこの設定値の 1.5 倍に制限します。
- [Minimum roundtrip delay]：リンクがアイドル状態のときに、1 ビットが、ある WAE と相手側の間の往復にかかる時間（ミリ秒）を入力します。デフォルト設定は、80 ミリ秒です。

（注）　あとでこの接続用の WAN 使用率設定を変更する場合は、新しい値を有効にするために、Edge WAE を再起動する必要があります。

ステップ 16　[Submit] をクリックします。

事前配置ディレクティブの作成

事前配置ディレクティブを使用すると、どのファイルを CIFS ファイル サーバから選択した Edge WAE のキャッシュへ事前にコピーする必要があるかを決定できます。事前配置を使用すると、WAN のアイドル時間を利用して、頻繁にアクセスされるファイルを選択した WAE へ転送できます。そのため、ユーザは、これらのファイルに初めてアクセスするときでも、キャッシュ レベルのパフォーマンスを利用できます。

レガシー モードの場合、事前配置ディレクティブは明示的に登録されたファイル サーバにのみ追加できます。事前配置は、透過的 CIFS アクセラレータ モードの場合に限り自動検出されたファイル サーバでサポートされます。

事前配置ディレクティブを定義するときは、ファイル サーバからの内容を事前に配置する Edge WAE を選択し、事前に配置するファイル サーバ上のルート ディレクトリを指定します。当初、事前配置ディレクティブは、未スケジュール状態にあります。また、内容を事前に配置する日時と周期を決定するスケジュールを作成する必要があります。内容を定期的に事前配置できるため、作業の反復ごとに指定したすべてのファイルをコピーするか、指定した周期の間に変更されたファイルだけをコピーするかを指定できます。

さらに、事前配置作業が WAN 帯域幅や Edge WAE キャッシュ空間を過剰に使用しないように、時間とサイズの制限を指定できます。これらの制限を使用して、ネットワーク効率を最適化し、この機能の誤用を防止することを強く推奨します。

事前配置ディレクティブがアクティブになる時刻になると、Edge WAE で事前配置作業が開始します。WAAS Central Manager GUI で、処理中および処理後に各事前配置作業をモニタできます。必要に応じて、アクティブな事前配置作業を停止することもできます。

事前配置では、ファイル サーバにアクセスするために必要なユーザ名およびパスワードを指定する必要があります。透過的 CIFS アクセラレータ モードでは、これらの項目は、次の手順に従って [Creating New Preposition Directive] ウィンドウで直接指定できます。レガシー モードでのユーザ名およびパスワードの指定の詳細については、「コア クラスタの設定」（P.11-11）のステップ 11 を参照してください。

（注）　事前配置の更新情報が Central Manager に送信されたときに、いずれかの事前配置ファイルサーバのクレデンシャルを復号化できない場合、以降のすべての事前配置の更新情報は WAE から Central Manager に送信されません。復号化の失敗を示すエラーメッセージが、errorlog/cms_log.current に記録されます。事前配置クレデンシャルを再設定する必要があります。

事前配置には、複数のルートを設定する機能も含まれます。「新しい事前配置ディレクティブの作成」（P.11-27）を参照してください。

透過的 CIFS アクセラレータ モードで事前配置を使用する場合、ブランチ オフィス の WAE とデータセンター WAE の両方が必要です（他の高速トラフィックでも同様です）。次のネットワーク エンティティ間の接続を確認します。

- クライアントとブランチ オフィスの WAE
- ブランチ オフィスの WAE とデータセンターの WAE
- ブランチ オフィスの WAE とファイル サーバ
- データセンターの WAE とファイル サーバ

事前配置トラフィックをブロックする可能性のあるすべての ACL を変更する必要があります。

（注） レガシー モードで事前配置ディレクティブを定義するために必要な接続が存在しない場合、警告メッセージが表示されます。

（注） 事前配置ディレクティブは、CLI を使用して作成し、管理できますが、Central Manager GUI を使用することを推奨します。Central Manager では、WAE のグループの事前配置を管理できるからです。GUI 設定と CLI 設定の両方を使用すると、1 つのデバイスへの変更が他のデバイスに影響する可能性があるので、予測できない結果になることがあります。

次の項目で、事前配置ディレクティブを作成する方法について説明します。

- 「新しい事前配置ディレクティブの作成」（P.11-27）
- 「事前配置ディレクティブへのデバイスの割り当て」（P.11-32）
- 「新しい事前配置スケジュールの作成」（P.11-33）

新しい事前配置ディレクティブの作成

事前配置ディレクティブを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File Services] >[Preposition] を選択します。

[Preposition Directives] ウィンドウが表示されます。このウィンドウは、システムに存在する事前配置ディレクティブに関する次の情報を表示します。

- [Preposition Directive]：事前配置ディレクティブの名前。
- [Type]：事前配置ディレクティブがすべてのファイルに影響する（Full）か、最後の事前配置作業の後で変更されたファイルだけに影響する（Differential）か。
  - Full の場合、作業のフィルタと一致するすべてのファイルおよびファイル サーバで検出されたすべてのファイルが Edge に送信され、キャッシュと比較されます。
  - Differential の場合、最後に正しく事前配置された後に変更されたファイルだけが Edge キャッシュに送信されます。最後に正しく事前配置された時刻は Edge デバイスから取得されるので、Edge デバイスのクロックとファイル サーバのクロックが同期していることを確認してください。最初は常に完全スキャンされます。事前配置作業を変更すると、最後に正しくスキャンされた時刻がリセットされます。
  - Since の場合、指定された期間内で変更されたファイルだけが Edge キャッシュに送信されます。

- [Status]：事前配置ディレクティブが有効であるか、無効であるか。
- [File Server]：エクスポートされたファイル サーバの名前。

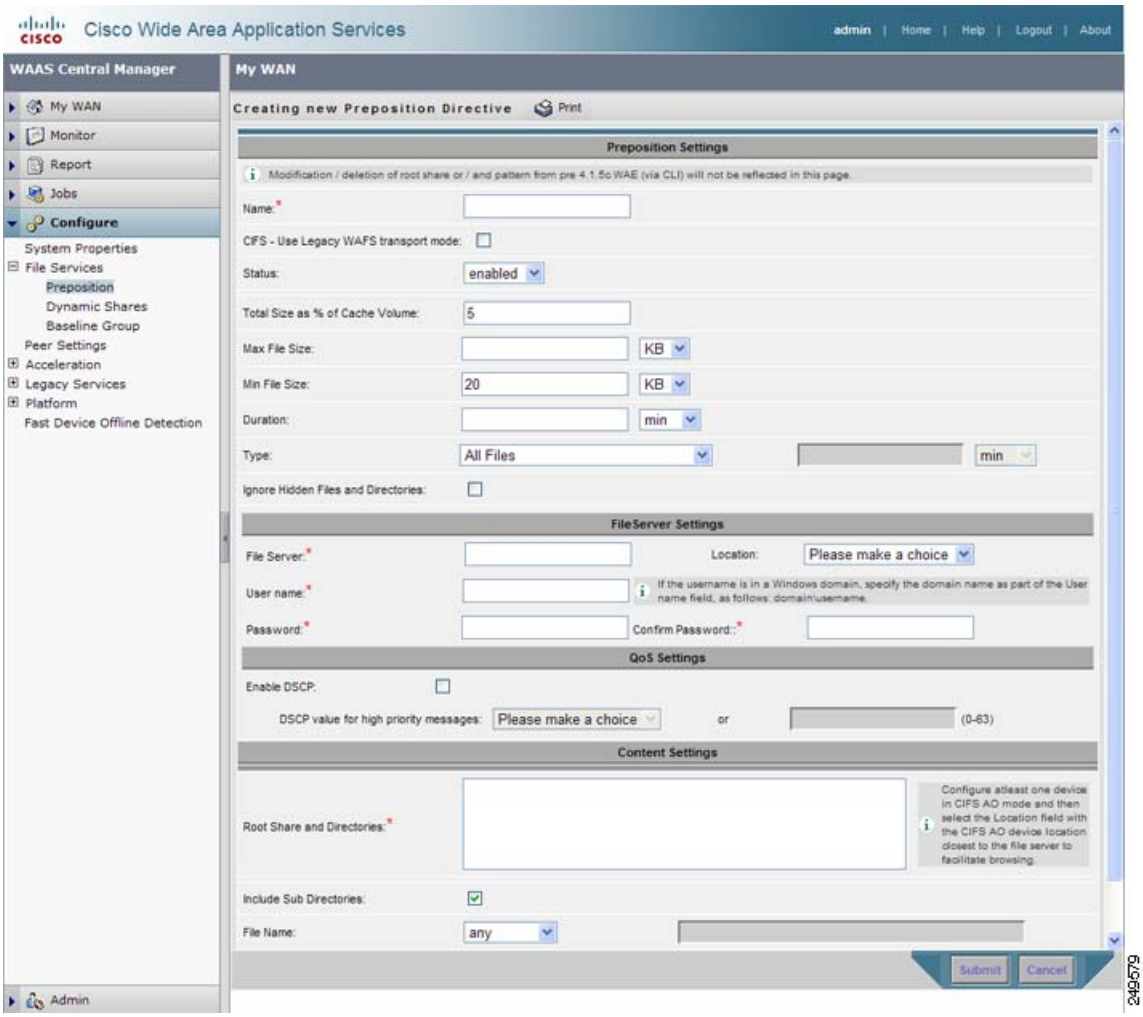
[Preposition Directive] ウィンドウから、次の作業を実行できます。

- ディレクティブの横にある [Edit] アイコンをクリックして、既存の事前配置ディレクティブの設定を編集します。次に、事前配置ディレクティブを削除したり、任意の設定を変更できます。
- 次の手順の説明に従って、新しい事前配置ディレクティブを追加します。

ステップ 2　新しい事前配置ディレクティブを作成するには、新規作成事前配置ディレクティブ タスクバーの [Create New Preposition Directive] アイコンをクリックします。

[Creating New Preposition Directive] ウィンドウが表示されます（図 11-6 を参照）。

図 11-6　新しい事前配置ディレクティブの作成



ステップ 3　ディレクティブの名前を入力します。名前では、二重引用符（"）を使用できません。

ステップ 4　（任意）レガシー モードを使用している場合、[CIFS - Use Legacy WAFS transport mode] チェックボックスを選択します。

このチェックボックスを選択した場合、透過的 CIFS アクセラレータ モードにだけ該当するフィールドがあるため、このウィンドウ内の特定のフィールドは表示されません。

ステップ 5　[Status] ドロップダウン リストから、[enabled] または [disabled] を選択します。無効にしたディレクティブは、有効になりません。

ステップ 6　（任意）[File Server] ドロップダウン リストで、エクスポートするファイル サーバの名前を選択します。ファイル サーバを登録する方法の詳細については、「WAAS Central Manager を使用したファイル サーバの登録」（P.11-18）を参照してください。透過的 CIFS モードでは、ファイル サーバの登録は必要ありません（[CIFS - Use Legacy WAFS transport mode] チェックボックスを選択した場合、[File Server] フィールドは表示されません）。

ステップ 7　（任意）提供されるフィールドを使用して、時間とサイズの制限を定義します。

表 11-6 で、時間とサイズを制限するフィールドについて説明します。

表 11-6　事前配置の時間とサイズの制限

フィールド	説明
[Total Size as % of Cache Volume]	ファイルを事前配置する Edge WAE キャッシュ全体が消費できる比率（%）。たとえば、この事前配置ディレクティブの使用量を WAE キャッシュの 30% に制限するには、このフィールドに 30 と入力します。デフォルト値は 5% です。 事前配置で定義したキャッシュの比率により、キャッシュに保存されているサイズにかかわらず 1 回の作業で事前配置できる最大サイズが定義されます。 キャッシュが満杯の場合は、理由を問わず、オンデマンド キャッシングのような事前配置が行われます。つまり除去プロセスが開始され、ファイルは、最後のアクセス時刻が古い順にキャッシュから削除されます。
[Max File Size]	エクスポートできる最大ファイル サイズ。この値を超えるファイルは、WAE キャッシュへエクスポートされません。
[Min File Size]	エクスポートできる最小ファイル サイズ。この値より小さいファイルは、WAE キャッシュへエクスポートされません。通常の WAAS を通じて WAN 経由で迅速に取得できるため、20 KB 未満のファイルを事前に配置することは効率的でありません。 デフォルト値は 20KB です。

表 11-6　事前配置の時間とサイズの制限 （続き）

フィールド	説明
[Duration]	WAAS がファイル サーバをエクスポートする最大時間。WAAS がファイル サーバをエクスポートするのにこの時間を超えると、すべてのファイルが Edge WAE キャッシュへコピーされる前に、WAAS はエクスポート プロセスを停止します。 事前配置作業が予定時刻に開始されない場合（たとえば Edge と Core が接続されていない場合）、この時間中は開始が試行されます。 このフィールドに値を指定しないと、WAAS は、必要な時間をかけてこのファイル サーバをエクスポートします。
[Type]	スキャン プロセスの時間フィルタ。[Type] ドロップダウン リストから、次のいずれかのオプションを選択します。 • [All Files] : すべてのファイルを Edge WAE キャッシュへエクスポートします。これは、デフォルトの設定です。 • [Files changed since last preposition] : 最後の事前配置以後に変更されたファイルだけを Edge WAE キャッシュへエクスポートします。この遅延フィルタは、2 回目以降の作業に適用されます。 このオプションを指定すると、新しいディレクトリが最後の修正時刻が変更されずに事前配置済みのディレクトリに移動された場合、次の事前配置セッションではこの新しいディレクトリは事前配置されません。 • [Files changed since last] : 指定した時間内に変更されたファイルだけをエクスポートします。過去 2 時間にファイル サーバで行われたファイル アップデートをエクスポートする場合は、提供されるフィールドに **2** を入力し、ドロップダウン リストから [hour] を選択します。

（注） 事前配置作業中にいずれかの制限値を超えると、作業が停止し、メッセージが管理者ログへ送信されます。残っているファイルは、次回の作業中にエクスポートされます。その前にユーザが残っているファイルの 1 つを要求すると、通常のように WAAS ソフトウェアを通じて WAN 経由で取得されます。

ステップ 8　（任意）ファイル サーバに表示されないディレクトリを事前配置しない場合は、[Ignore Hidden Directories] チェックボックスをオンにします。デフォルトでは、このチェックボックスは選択されていません。このチェックボックスが未選択のままであれば、表示されないディレクトリは事前配置されます。

（注） レガシー モードを使用していて、ファイル サーバを明示的に登録する代わりに自動ディスカバリ機能を使用している場合、レガシー モードの自動検出されたファイル サーバでは事前配置がサポートされていないため、このチェックボックスは適用されません。

ステップ 9　[File Server] フィールドで、エクスポートするファイル サーバの名前を入力します。名前では、二重引用符（"）またはフォワード スラッシュ（/）を使用しないでください。

[CIFS - Use Legacy WAFS transport mode] チェックボックスを選択した場合、[File Server Setting] エリアは表示されません）。その代わり、ドロップダウン リストには登録したファイル サーバが表示されます（ステップ 6 を参照）。

ステップ 10　[Location] ドロップダウン リストから、ファイル サーバにブラウジング サービスを提供するデバイスの位置を選択します。最高のブラウジング パフォーマンスを得るため、ファイル サーバに近接する位置を指定します。位置を定義する詳細については、「デバイス位置の操作」（P.3-14）を参照してください（[CIFS - Use Legacy WAFS transport mode] チェックボックスを選択した場合、[Location] は表示されません）。

ステップ 11　[User Name]、[Password]、および [Confirm Password] の各フィールドでは、ファイル サーバのユーザ名およびパスワードのクレデンシャルを入力します。ユーザ名が Windows ドメイン内に存在する場合、domain¥username のように [User name] フィールドの一部としてドメイン名を指定します（[CIFS - Use Legacy WAFS transport mode] チェックボックスを選択した場合、これらのフィールドは表示されません）。

入力したアクセス クレデンシャルによって事前配置のルート ディレクトリおよびその親ディレクトリへの読み取りアクセスが許可される必要があります。

ステップ 12　（任意）事前配置トラフィックに DSCP マーキング値を指定する場合は、[DSCP value for high priority messages] チェックボックスを選択します。ドロップダウン リストから DSCP 値を選択するか、テキスト フィールドに 0 ～ 63 の値を入力します。サポートされている値の説明については、表 11-4（P.11-16）を参照してください（[CIFS - Use Legacy WAFS transport mode] チェックボックスを選択した場合、DSCP 設定は表示されません）。

DSCP は、ネットワーク トラフィックに異なるレベルのサービスを割り当てることができる IP パケットのフィールドです。ネットワーク上の各パケットに DSCP コードを付け、対応するサービスのレベルを関連付けて、サービスのレベルを割り当てます。DSCP は、IP precedence フィールドと Type of Service（ToS; タイプ オブ サービス）フィールドの組み合せです。詳細については、RFC 2474 を参照してください。

ステップ 13　[Root Share and Directory] フィールドに、エクスポートするファイル サーバ上のディレクトリを入力します。次の任意の方法を使用して、ディレクトリを識別します。

- *protocol*://*server*/*share* または *server*¥*share* の形式で、1 つまたは複数のディレクトリ パスを手動で入力します。たとえば、cifs://win12srv/home または win12srv¥home です。複数のディレクトリを複数の行で入力することもできます。その場合は、それぞれの行にそれぞれのフル ディレクトリ パスを入力します。ルート ディレクトリ（/）は、共有ルートとして指定できません。

  複数ルートの共有を定義する場合は、単一のルート設定を行う一連の事前配置をルートごとに反復します。

- [Browse] ボタンをクリックして、ファイル サーバ上のディレクトリを参照します。ディレクトリの中に移動するには、ディレクトリ名の左にあるファイル フォルダ アイコンをクリックします。エクスポートするディレクトリの横にあるチェックボックスをオンにし、[Select Directory] ボタンをクリックします。ウィンドウが表示され、複数のディレクトリが選択できます。

  レガシー モードでは、[Browse] ボタンは、[Configure Core Server Settings] ウィンドウで [File Server access username] および [File Server access password] フィールドを設定した場合にだけ表示されます（図 11-3 を参照）。透過的 CIFS モードでは、[Location] ドロップダウン リストからファイル サーバに最も近接する CIFS アクセラレータの位置を選択した場合に、ブラウズ機能が最高の動作を行います。位置を選択しない場合、CIFS アクセラレータが有効であるすべてのデバイスにブラウズ要求が送信され、要求がタイムアウトとなる可能性があります。

- [Include Sub Directories] チェックボックスを選択して、指定したルート ディレクトリの下にあるすべてのサブディレクトリを含めます。このオプションを指定しない場合は、指定したルート ディレクトリのフィールドだけが事前配置され、表示中にサブディレクトリを指定できません。

- [File Name] ドロップダウン リストからパターン演算子を選択し、隣接するテキスト ボックスにパターンを記述する文面を入力して、特定のファイルの種類までポリシー定義を絞り込みます。たとえば、**ends with .doc** と入力します。スペースまたは次の特殊文字は使用しないでください。
  | : > < " ?* / \

ステップ 14　[Submit] をクリックします。

ディレクティブがシステムに保存され、ナビゲーション ペインに追加オプションが表示されます。

事前配置ディレクティブへのデバイスの割り当て

事前配置ディレクティブを作成したら、Edge WAE またはデバイス グループをディレクティブに割り当てる必要があります。この作業は、どの Edge WAE が事前配置内容をキャッシュに保存するかを決定します。

（注）　事前配置には、複数のルートを設定する機能も含まれます。「新しい事前配置ディレクティブの作成」（P.11-27）を参照してください。

Edge WAE またはデバイス グループを事前配置ディレクティブに割り当てるには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File Services] >[Preposition] を選択します。

[Preposition Directives] ウィンドウが表示され、システムに存在する事前配置ディレクティブが表示されます。

ステップ 2　Edge WAE またはデバイス グループに割り当てたい事前配置ディレクティブの横にある [Edit] アイコンをクリックします。

ステップ 3　ウィンドウの一番上にある次のタブのうち、いずれかをクリックします。

- [Assign Edge Devices]：このディレクティブに割り当てる 1 つまたは複数の Edge WAE を選択できます。
- [Assign Edge Groups]：このディレクティブに割り当てるデバイス グループを選択できます。

選択したオプションに応じて、[Edge Device Assignments] ウィンドウまたは [Device Groups Assignments] ウィンドウが表示されます。

いずれのビューでも、割り当てウィンドウでは、リスト内の項目のビューをフィルタできます。フィルタにより、設定した基準に一致するリスト内の項目を見つけることができます。

ステップ 4　次のいずれかを実行して、この事前配置ディレクティブに割り当てる Edge WAE またはデバイス グループを選択します。

- タスクバーの をクリックして、使用できるすべての Edge WAE またはデバイス グループをこのディレクティブに割り当てます。
- このディレクティブに割り当てる各 Edge WAE またはデバイス グループの横にある をクリックします。選択すると、アイコンは に変化します。

（注）　デバイスまたはデバイス グループはオフラインである（✖で識別される）場合、そのデバイスまたはグループをこのディレクティブに割り当てることができません。デバイス グループに割り当てられた事前配置ディレクティブは、その割り当てられたデバイス グループ内の接続先 Edge デバイスにだけ適用されます。

CIFS アクセラレータ モードの事前配置ディレクティブをデバイス グループに割り当てた場合、ディレクティブは、割り当てられたデバイス グループで CIFS アクセラレーションが有効化されているデバイスにだけ適用されます。同様に、レガシー モードの事前配置ディレクティブをデバイス グループに割り当てた場合、ディレクティブは、割り当てられたデバイス グループでレガシー モードが有効化されているデバイスにだけ適用されます。

ステップ 5　[Submit] をクリックします。

選択した各エッジ デバイスまたはデバイス グループの横にあるアイコンが ✔ に変化します。

（注）　WAE で CIFS アクセラレータが無効になっている場合、WAE が割り当てられている事前配置ディレクティブから削除されます。また、事前配置ディレクティブは、設定を実行しているデバイスから削除されます。

新しい事前配置スケジュールの作成

事前配置ディレクティブを作成し、WAE をディレクティブに割り当てたら、いつ何回事前配置を実行するかを決定するスケジュールを作成することを推奨します。

たとえば、営業時間内のトラフィック量を最小限に抑えるために、事前配置スケジュールを夜間に設定する場合があります。あるいは、エクスポートされるデータがよく変更される場合、事前配置スケジュールを反復実行に設定する場合があります。これにより、このディレクティブに割り当てられた WAE のキャッシュに、最新のファイル アップデートが存在することを保証できます。

Edge WAE の事前配置作業を異なる時間帯で同時に開始するスケジュールの場合、Edge WAE の作業は Core WAE の時間帯に基づいて開始されます。Edge WAE と Core WAE のクロックが同期していない場合、作業は予定通りに開始されません。

事前配置スケジュールを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File Services] >[Preposition] を選択します。

[Preposition Directives] ウィンドウが表示され、システムに存在する事前配置ディレクティブが表示されます。

ステップ 2　スケジュールを作成する事前配置ディレクティブの横にある [Edit] アイコンをクリックします。

ステップ 3　ウィンドウの一番上にある [Schedule] タブをクリックします。

[Creating New Preposition Schedule] ウィンドウが表示されます。デフォルトでは、スケジュールは設定されていません。

ステップ 4　次のいずれかのスケジュール オプションを選択します。

- [Not Scheduled]：この時点で事前配置はスケジューリングされていません。
- [Now]：このスケジュールを送信してから数分以内に事前配置を実行します。

事前配置ディレクティブを変更して [Submit] ボタンをクリックするたびに、[Now] スケジュールが開始されます。リロードされたエッジ デバイスがオンラインに復帰した場合も、すぐに [Now] スケジュールが開始されます。

- [Daily]：毎日の指定した時刻に事前配置を実行します。
- [Date]：指定した日時に事前配置を実行します。
- [Weekly]：選択した曜日の指定した時刻に事前配置を実行します。
- [Monthly Days]：毎月、選択した日の指定した時刻に事前配置を実行します。
- [Monthly Weekdays]：毎月、選択した曜日の指定した時刻に事前配置を実行します。たとえば、毎月の第 2 火曜日に事前配置を実行するスケジュールを作成できます。

ステップ 5　事前配置作業の開始時刻を指定します。

時刻は 24 時間形式で表し、00:00 は深夜の 0 時を表します。時刻は、データを事前配置する Edge WAE の現地時間を指します。異なる時間帯に複数の Edge WAE がある場合は、時刻は Core WAE の現地時間を指します。

（注）　[Now] オプションでは、開始時刻を指定できません。

ステップ 6　[Submit] をクリックします。

スケジュールが保存されたことを確認する「Changes Submitted」メッセージが、ウィンドウの一番下に表示されます。

ステップ 7　事前配置ステータスを確認して、事前配置ディレクティブが正常に完了したことを確認します。詳細については、「事前配置ステータスの確認」（P.11-34）を参照してください。

ファイル サービスの管理

この項の次の項目で、ファイル サーバを管理する方法について説明します。

事前配置ステータスの確認

1 つまたは複数の事前配置ディレクティブを作成したら、すべての事前配置作業のステータスを確認して、正常に完了したことを確認できます。作業が正常に完了しない場合は、事前に配置された一部のファイルが Edge WAE キャッシュへ正常にコピーされていない場合があります。

事前配置作業のステータスを確認するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File Services] >[Preposition] を選択します。

[Preposition Directives] ウィンドウが表示され、システムに存在する事前配置ディレクティブが表示されます。

ステップ 2　ステータスを確認する事前配置ディレクティブの横にある [Edit] アイコンをクリックします。

ステップ 3　ウィンドウの一番上にある [Preposition Status] タブをクリックします。[Preposition Status] ウィンドウが表示されます。

このページは、次の情報を表示します。

- [WAE]：事前配置されるファイルをキャッシュに受信する各 Edge WAE の名前。
- [Start Time]：事前配置作業が開始した日時。
- [Duration]：事前配置作業が完了するまでにかかった時間。
- [Amount Copied]：WAE キャッシュへコピーされたデータ量（バイト単位）。
- [Status]：事前配置作業が正常に完了したかどうか。
- [Reason]：事前配置作業が失敗した理由。

ステップ 4　[Status] 列に [Completed] が表示されることを確認します。

この列に失敗が表示される場合は、[Reason] 列を参照して事前配置作業が失敗した理由を確認します。問題を解決したら、事前配置作業を今すぐ再実行するようにスケジュールを設定するか、スケジュール済みの開始時刻まで待ち、あとでステータスを確認できます。

事前配置作業の開始と停止

Device Manager GUI から、事前配置作業を開始または停止できます。詳細については、「[Preposition] オプション」（P.10-20）を参照してください。

WAN 障害に対する WAAS ネットワークの準備

Edge WAE をコア クラスタにリンクする接続ディレクティブを設定するときは、WAN 障害によってコア クラスタとの接続が切断された場合に切断モードで動作するように Edge WAE を設定するオプションがあります。

（注）　切断モードは、ファイル サービスの透過的 CIFS アクセラレータ モードを使用している場合は使用できません。

ここでは、次の内容について説明します。

切断モードについて

切断モードを使用すると、WAN 障害が発生した場合でも、CIFS クライアントは、キャッシュ ディレクトリを参照し、Edge WAE 上のキャッシュされているファイル全体を読み取ることができます。WAN 障害時には Edge WAE がキャッシュされたデータをファイル サーバと比較できないため、CIFS クライアントは、キャッシュされたデータに読み取り専用アクセスしか行うことができません。

Edge WAE とコア クラスタ間の WAN 接続が復元すると、Edge WAE は自動的に通常の接続モードに戻ります。

Edge WAE は、コア クラスタとの接続を失うと、切断モードに切り替わります。これを「WAN 障害」と呼びます。

（注）　ファイル サーバが故障しても、（Edge WAE がコア クラスタとの接続を維持している場合）切断モードには切り替わりません。

Edge WAE は、1 つの接続が切断モードで動作し、別の接続が通常の接続モードで動作することができます。たとえば、Edge WAE 用に 1 つのディレクティブ リンクがコア クラスタ A に接続し、他のディレクティブ リンクがコア クラスタ B に接続する 2 つの接続ディレクティブを作成すると、WAN 障害によってコア クラスタとのリンクが切断された場合、Edge WAE はその接続を切断モードに切り替えます。Edge WAE のコア クラスタ B との通信は、通常の接続モードのまま残ります。

切断モードは、明示的に登録されたファイル サーバでのみ動作します。切断モードは、自動検出されたファイル サーバではサポートされていません。

DNS とドメイン コントローラの要件

切断モードでは、ブランチ オフィスのローカル ドメイン コントローラが、CIFS クライアントを認証する必要があります。切断モードで動作する Edge WAE は、Kerberos を除くすべての認証方式をサポートします。

DNS だけの環境では、ブランチ オフィスにローカル DNS サーバも必要です。DNS の代わりに WINS を使用する場合は、ブランチ オフィスにローカル WINS サーバが必要です。

キャッシュされたファイルへの切断モード アクセスを有効にするには、（WAN 障害時に Windows 認証を実行するために）Active Directory ドメインまたは Windows NT ドメインに Edge WAE を追加する必要があります。

（注）　デフォルトで、Windows ドメイン コントローラは、認証プロセスの一環として自動マシン アカウント パスワード変更を実行します。Edge WAE 用のマシン アカウント パスワードは 7 日周期で Edge WAE とドメイン コントローラの間で自動的にネゴシエートされ、変更されます。ただし、認証サービスが停止している場合、このプロセスは実行されず、Edge WAE 用のマシン アカウント パスワードは失効します。この状況を回避するために、Edge WAE 用の自動マシン アカウント パスワード変更を無効にすることを推奨します。詳細については、「Edge WAE 用の自動マシン アカウント パスワード変更の無効化」（P.6-23）を参照してください。

（注）　一般に、WINS 登録のタイムアウトは 3 日です。その結果、WCCP が切断モードで有効になっている場合、元のファイル サーバの WINS 登録がタイムアウトし、クライアントで名前解決問題が発生する場合があります。

切断モードでのデータ アベイラビリティ

Edge WAE が切断モードにある場合、CIFS クライアントは、Edge WAE で完全にキャッシュされているファイルに読み取り専用でアクセスできます。CIFS クライアントは、部分的にキャッシュされたファイルやキャッシュされていないファイルのディレクトリ構造を表示できますが、これらのファイルを開くことができません。

ディレクトリは、その ACL がキャッシュされている場合のみ、切断モードで使用できます。つまり、アクセスされたことがなく、キャッシュされていない共有は、表示されません。

切断モードでファイルが使用できることを保証する最善の方法は、Edge WAE キャッシュにファイルのコピーを予防的に配置する事前配置ディレクティブを設定することです。詳細については、「新しい事前配置ディレクティブの作成」（P.11-27）を参照してください。

切断モードの設定

ファイル サーバを WAAS Central Manager に登録するとき、切断モードで動作するように Edge WAE を設定できます。詳細については、「WAAS Central Manager を使用したファイル サーバの登録」（P.11-18）を参照してください。

また、Active Directory ドメインまたは Windows NT ドメインに Edge WAE を追加する必要があります。詳細については、「WAAS デバイス上の Windows ドメイン サーバ設定の構成」（P.6-18）を参照してください。[Show Authentication Status] ボタンをクリックして、WAE が正常にドメインに追加されたことを確認します。認証ステータスが OK でない場合でも、**wbinfo -t** コマンドが正常に動作（RPC 経由の信用が正常終了）するかぎり、WAE は読み取り専用切断モード用の認証を提供します。

コア クラスタのメンバーの表示

（注）　ファイル サービスの透過的 CIFS アクセラレータ モードを使用している場合、このモードにコア クラスタは存在しないため、この機能は使用できません。

コア クラスタ デバイス グループのメンバーである Core WAE を表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。[Device Groups] ウィンドウが表示されます。

ステップ 2　それに属するメンバーを表示する WAFS コア クラスタ デバイス グループの横にある [Edit] アイコンをクリックします。[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Members] を選択します。選択したデバイス グループに属するデバイスのリストが表示されます。

ファイル サービス モードの切り替え

WAAS バージョン 4.1.1 以降では、設定方法が異なる相互に排他的な 2 つの WAFS モード（透過的 CIFS アクセラレータ モードとレガシー モード）をサポートしています。この項では、WAAS デバイスでのモードの切り替え方法について説明します。また、次の内容についても説明します。

- 「レガシー モードから透過的 CIFS アクセラレータ モードへの変更」（P.11-38）

- 「透過的 CIFS アクセラレータ モードからレガシーモードへの変更」（P.11-40）

レガシー モードから透過的 CIFS アクセラレータ モードへの移行の詳細については、『*Cisco Wide Area Application Services Software 4.1 Common Internet File System Migration*』を参照してください。

（注） レガシー モード WAFS は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー モード WAFS を有効にすると、Central Manager 上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー WAFS の何らかの設定値を設定しようとした場合に警告されます。レガシー WAFS をお使いの場合は、透過的 CIFS アクセラレータに移行してください。

レガシー モードから透過的 CIFS アクセラレータ モードへの変更

現在 WAAS デバイスがレガシー モードを使用しており、透過的 CIFS アクセラレータ モードに変更する場合、次の手順を実行します。

ステップ 1　既存の事前配置ディレクティブが存在する場合、次の手順で事前配置ディレクティブを編集して、割り当てられているエッジ デバイスを削除します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File Services] >[Preposition] を選択します。[Preposition Directives] ウィンドウが表示されます。

b. 編集する事前配置ディレクティブの横にある [Edit] アイコンをクリックします。

c. [Assign Edge Devices] タブをクリックして、割り当てられているエッジ デバイスを表示します。

d. [Remove all Edge Devices] アイコンをクリックして、すべてのエッジ デバイスを削除します。

e. [Assign Edge Groups] タブをクリックして、割り当てられているエッジ デバイス グループを表示します。

f. [Remove all Edge Groups] アイコンをクリックして、すべてのエッジ デバイス グループを削除します。

ステップ 2　既存の事前配置ディレクティブが存在する場合、この事前配置ディレクティブを編集して、透過的 CIFS アクセラレータ モードに変更します。

a. [CIFS - Use WAFS transport mode] チェックボックスの選択を解除し、[File Server] フィールドにファイル サーバ名を入力します（事前配置ディレクティブの編集の詳細については、「新しい事前配置ディレクティブの作成」（P.11-27）を参照してください）。

b. [Location] ドロップダウン リストから、ファイル サーバにブラウジング サービスを提供するデバイスの位置を選択します。最高のブラウジング パフォーマンスを得るため、ファイル サーバに近接する位置を指定します。位置を定義する方法の詳細については、「デバイス位置の操作」（P.3-14）を参照してください。

c. [User Name]、[Password]、および [Confirm] の各フィールドでは、ファイル サーバのユーザ名およびパスワードのクレデンシャルを入力します。ユーザ名が Windows ドメイン内に存在する場合、domain¥username のように [User name] フィールドの一部としてドメイン名を指定します。入力したアクセス クレデンシャルによって事前配置のルート ディレクトリおよびその親ディレクトリへの読み取りアクセスが許可される必要があります。

d. [Submit] をクリックします。

ステップ 3　既存の定義されているダイナミック共有が存在する場合、このダイナミック共有を編集して、透過的 CIFS アクセラレータ モードに変更します（ダイナミック共有の編集の詳細については、「ダイナミック共有の作成」（P.11-21）を参照してください）。

a. [CIFS - Use WAFS transport mode] チェックボックスの選択を解除し、[File Server] フィールドにファイル サーバ名を入力します。

b. [User Name]、[Password]、および [Confirm] の各フィールドでは、ファイル サーバのユーザ名およびパスワードのクレデンシャルを入力します。ユーザ名が Windows ドメイン内に存在する場合、domain¥username のように [User name] フィールドの一部としてドメイン名を指定します。これらのクレデンシャルは、[Browse] ボタンをクリックしたときにファイル サーバにアクセスするためだけに使用されます。

c. [Submit] をクリックします。

ステップ 4　コア クラスタと Edge WAE 間で定義されている接続ディレクティブを削除します（詳細については、「コア クラスタと Edge WAE 間の接続の作成」（P.11-23）を参照してください）。

a. WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] >[Connectivity] を選択します。

b. 各接続ディレクティブの横にある [Edit] アイコンをクリックしてから、タスクバーの [Delete Connectivity Directive] アイコンをクリックします。確認ダイアログで [OK] をクリックします。

ステップ 5　「エッジ デバイスの設定」（P.11-14）および「コア クラスタの設定」（P.11-11）の説明に従って、デバイスでエッジ サーバ サービスとコア サーバ サービスを無効にします。[Enable Edge Server] チェックボックスおよび [Enable Core Server] チェックボックスの選択を解除する必要があります。

ステップ 6　次の手順で、透過的 CIFS アクセラレータを有効にします。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

b. グローバル最適化機能を変更するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[Configure] > [Acceleration] > [Enabled Features] を選択します（「グローバル最適化機能の有効化と無効化」（P.12-2）を参照）。

d. [CIFS Accelerator] をクリックします。

e. [Submit] をクリックします。

ステップ 7　デバイスを再ロードし、再起動するまで待機します。

ステップ 8　「事前配置ディレクティブへのデバイスの割り当て」（P.11-32）の説明に従って、エッジ デバイスを既存の事前配置ディレクティブまたは新しい事前配置ディレクティブに割り当てます。

（注）　CLI を使用してファイル サービス モードを切り替える場合、Central Manager GUI に「Roles changed, reload required」という適切ではないアラームが表示されることがあります。このアラームが表示されないようにするには、データ フィードのポール サイクル（約 10 分間）を 2 回分待機し、CLI でスイッチ モードを切り替えてからデバイスを再ロードします。

透過的 CIFS アクセラレータ モードからレガシーモードへの変更

現在 WAAS デバイスが透過的 CIFS アクセラレータ モードを使用しており、レガシー モードに変更する場合、次の手順を実行します。

ステップ 1　「WAAS Central Manager を使用したファイル サーバの登録」（P.11-18）の説明に従って、ファイル サーバを定義します。

ステップ 2　既存の事前配置ディレクティブが存在する場合、次の手順で事前配置ディレクティブを編集して、割り当てられているエッジ デバイスを削除します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [File Services] >[Preposition] を選択します。[Preposition Directives] ウィンドウが表示されます。

b. 編集する事前配置ディレクティブの横にある [Edit] アイコンをクリックします。

c. [Assign Edge Devices] タブをクリックして、割り当てられているエッジ デバイスを表示します。

d. [Remove all Edge Devices] アイコンをクリックして、すべてのエッジ デバイスを削除します。

e. [Assign Edge Groups] タブをクリックして、割り当てられているエッジ デバイス グループを表示します。

f. [Remove all Edge Groups] アイコンをクリックして、すべてのエッジ デバイス グループを削除します。

ステップ 3　既存の事前配置ディレクティブが存在する場合、[CIFS - Use WAFS transport mode] チェックボックスを選択し、[File Server] ドロップダウン リストでファイル サーバを選択してこのディレクティブを編集し、モードをレガシー モードに変更します。[Submit] をクリックします。事前配置ディレクティブの編集の詳細については、「新しい事前配置ディレクティブの作成」（P.11-27）を参照してください。

ステップ 4　既存の定義済みのダイナミック共有が存在する場合、[CIFS - Use WAFS transport mode] チェックボックスを選択し、[File Server] ドロップダウン リストでファイル サーバを選択してこのダイナミック共有を編集し、モードをレガシー モードに変更します。[Submit] をクリックします。ダイナミック共有の編集の詳細については、「ダイナミック共有の作成」（P.11-21）を参照してください。

ステップ 5　次の手順で、透過的 CIFS アクセラレータを無効化します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

b. グローバル最適化機能を変更するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[Configure] > [Acceleration] > [Enabled Features] を選択します（「グローバル最適化機能の有効化と無効化」（P.12-2）を参照）。

d. [CIFS Accelerator] の選択を解除します。

e. [Submit] をクリックします。

ステップ 6　「エッジ デバイスの設定」（P.11-14）の説明に従ってデバイスでエッジ サーバ サービスを有効化します。デバイスがコア デバイスとして使用されている場合は、「コア クラスタの設定」（P.11-11）の説明に従ってデバイスでコア サーバ サービスを有効化します。

ステップ 7　デバイスを再ロードし、再起動するまで待機します。

ステップ 8　「登録したファイル サーバへのコア クラスタの割り当て」（P.11-20）の説明に従って、登録した各ファイル サーバにコア クラスタを割り当てます。この手順は、コア クラスタを作成済みであることを前提にしています。

ステップ 9　「コア クラスタと Edge WAE 間の接続の作成」（P.11-23）の説明に従って、エッジ デバイスとコア デバイスとの間の接続を作成します。

ステップ 10　「事前配置ディレクティブへのデバイスの割り当て」（P.11-32）の説明に従って、エッジ デバイスを事前配置ディレクティブに割り当てます。

CHAPTER 12

アプリケーション アクセラレーションの設定

この章では、Wide Area Application Service（WAAS）システムで、WAN 経由で加速化されるアプリケーション トラフィックの種類を決定するアプリケーション ポリシーを設定する方法について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

アプリケーション アクセラレーションについて

WAAS ソフトウェアには、WAAS システムが最適化し、加速化するアプリケーション トラフィックの種類を決定する、150 を超える定義済みのアプリケーション ポリシーが組み込まれています。これらの定義済みポリシーは、ネットワークで最も一般的な種類のアプリケーション トラフィックを網羅しています。定義済みポリシーのリストについては、付録 A「定義済みのアプリケーション ポリシー」を参照してください。

各アプリケーション ポリシーには、次の要素があります。

- アプリケーション定義：アプリケーション名、トラフィックに適用される Differentiated Services Code Point（DSCP; DiffServ コード ポイント）マーキング値、および WAAS Central Manager がこのアプリケーション用の統計情報を収集するかどうかなど、特定のアプリケーションに関する一般情報を識別します。
- 分類子：特定の種類のトラフィックを識別する一致条件を含んでいます。たとえば、デフォルトの HTTP 分類子は、ポート 80、8080、8000、8001、および 3128 へ進むすべてのトラフィックと一致します。最大 512 の分類子と 1024 の一致条件を作成できます。

- ポリシー：アプリケーション定義と分類子を 1 つのポリシーにまとめます。また、このポリシーは、WAAS デバイスが定義されたトラフィックに適用する最適化とアクセラレーション機能を決定します（存在する場合）。最大 512 のポリシーを作成できます。また、ポリシーにはトラフィックに適用され、アプリケーション レベルまたはグローバル レベルで設定された DSCP 値を上書きする DSCP マーキング値も含まれます。

WAAS Central Manager GUI を使用すると、定義済みポリシーを変更し、他のアプリケーション用の追加ポリシーを作成できます。アプリケーション ポリシーを作成する方法については、「新しいトラフィック アプリケーション ポリシーの作成」（P.12-29）を参照してください。レポートの表示、ポリシーの復元、アプリケーションのモニタリング、およびその他の機能については、「アプリケーション アクセラレーションの管理」（P.12-37）を参照してください。

（注）　WAAS Central Manager で設定されたすべてのアプリケーション定義は、デバイス グループ メンバシップ設定を無視して、WAAS Central Manager に登録されているすべての WAAS デバイスにグローバルに適用されます。

グローバル最適化機能の有効化と無効化

グローバル最適化機能は、デバイスまたはデバイス グループで、TFO 最適化、Data Redundancy Elimination（DRE; データ冗長性除去）、および永続的圧縮を有効にするかどうかを決定します。デフォルトで、これらの機能は、すべて有効です。これらの機能の 1 つを無効にすると、デバイスは、それが代行受信するトラフィックに完全な WAAS 最適化手法を適用できなくなります。

さらに、グローバル最適化機能には、EPM、CIFS、HTTP MAPI、NFS、SSL、およびビデオの各アプリケーション アクセラレータが含まれます。デフォルトで、すべてのアプリケーション アクセラレータは有効です。アプリケーション アクセラレータには、動作するための特定のライセンスも必要です。ライセンスのインストールの詳細については、「ソフトウェア ライセンスの管理」（P.9-3）を参照してください。

すべてのアプリケーション アクセラレータが動作するには、WAN リンクのどちらか一方の側にあるピア WAE の両方でアクセラレータを有効化する必要があります。

グローバル最適化機能を有効または無効にするには、次の手順に従ってください。

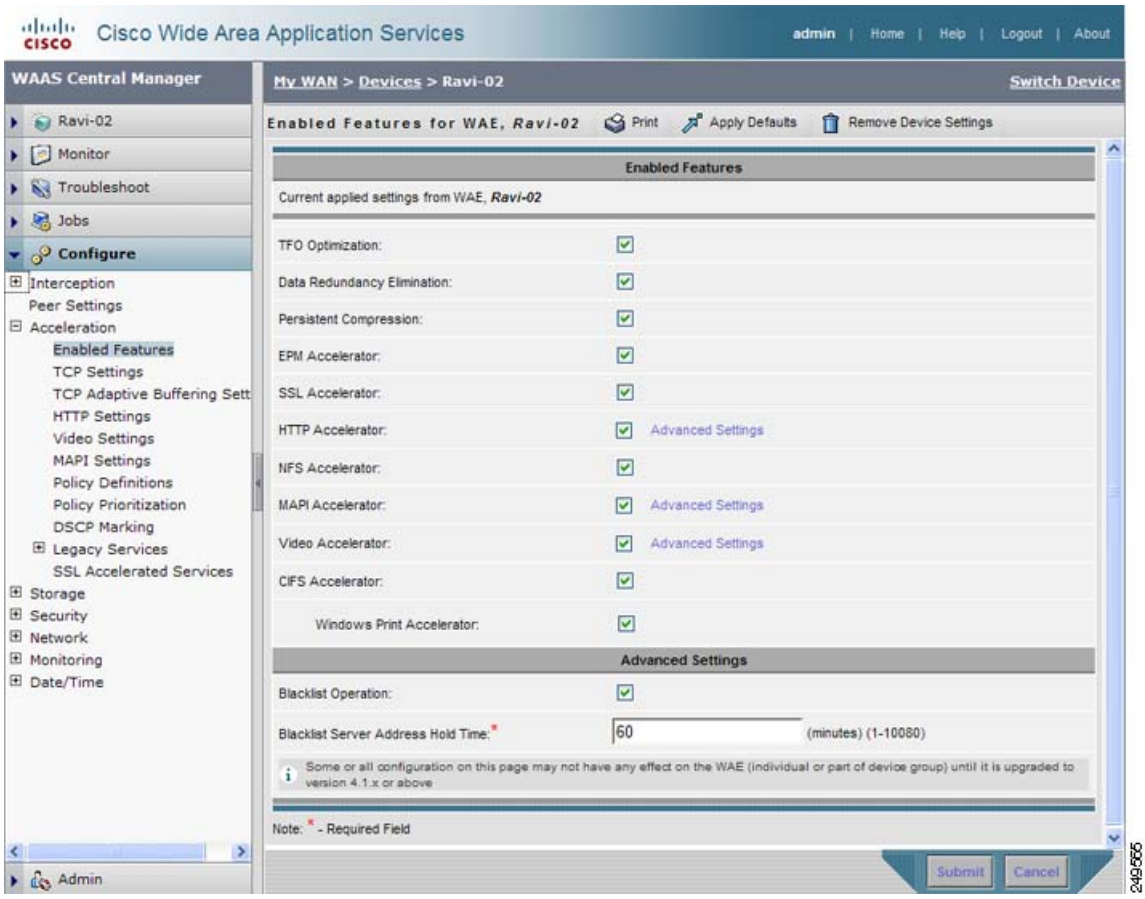
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　グローバル最適化機能を変更するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Enabled Features] を選択します。

[Enabled Features] ウィンドウが表示されます（図 12-1 を参照）。

図 12-1　　グローバル最適化機能の変更



ステップ 4　有効にする最適化機能を選択し、無効にする機能の選択を解除します。各最適化機能の詳細な説明については、「Cisco WAAS の主なサービス」（P.1-4）を参照してください。

ステップ 5　[HTTP Accelerator] チェックボックスを選択した場合、[HTTP Acceleration Configuration] ウィンドウへのショートカットとして [Advanced Settings] リンクをクリックできます。詳細については「HTTP アクセラレーションの設定」（P.12-5）を参照してください。

ステップ 6　[Video Accelerator] チェックボックスを選択した場合、[Video Acceleration Configuration] ウィンドウへのショートカットとして [Advanced Settings] リンクをクリックできます。詳細については、「ビデオ アクセラレーションの設定」（P.12-9）を参照してください。

ステップ 7　[MAPI Accelerator] チェックボックスを選択した場合、[MAPI Acceleration Configuration] ウィンドウへのショートカットとして [Advanced Settings] リンクをクリックできます。詳細については、「MAPI アクセラレーションの設定」（P.12-8）を参照してください。

ステップ 8　[CIFS Accelerator] チェックボックスを選択した場合は、次のオプションがあります。

- Window Print Accelerator：クライアントと Windows プリント サーバ間のプリント トラフィックを加速するには、このボックスを選択します。CIFS アクセラレータが有効である場合、このアクセラレータはデフォルトで有効です。

（注）　WAFS レガシー モードから CIFS アクセラレータに変更する場合、CIFS アクセラレータを有効化する前に WAFS レガシー モードを無効にする必要があります。WAFS レガシー モードを無効にするには、Data Center および Branch ファイル サービスを無効にする必要があります。WAFS の設定情報については、第 11 章「WAFS の設定」を参照してください。

（注）　クライアントのプリント サービスの使用に影響を及ぼす可能性があるため、クライアント セッション中には Windows プリント アクセラレーションを無効にしないでください。Windows プリント アクセラレーションを無効にする必要がある場合は、クライアント セッションを切断し、その後再度確立してください。

ステップ 9　[Advanced Settings] の領域では、[Blacklist Operation] 機能を無効にする場合、この機能の選択を解除します。この機能により、WAE は、オプションのある TCP 設定パケットがブロックされるか、または WAE デバイスに戻らない状況に対し、よりよい対処を行うことができます。この動作は、オプションのある TCP 設定パケットをブロックするネットワーク デバイス（ファイアウォールなど）および非対称ルートにより発生する可能性があります。WAE はオプションのある TCP パケットを受信できない元のサーバ（ファイアウォールの後ろにあるサーバなど）を追跡できるので、オプションのある TCP パケットをこれらのブラックリスト サーバに送信しないことを学習します。WAAS は、オプションのある TCP パケットが削除される状況においても、ブランチ WAE とデータセンター WAE 間のトラフィックを加速化できます。この機能を有効にしておくことを推奨します。

ステップ 10　60 分のデフォルトのブラックリスト サーバ アドレス保持時間を変更する場合は、[Blacklist Server Address Hold Time] フィールドに、新しい時間（分）を入力します。有効な範囲は、1 ～ 10080 分（1 週間）です。

サーバ IP アドレスがブラックリストに追加されると、そのアドレスは設定された保持時間の間ブラックリストに残ります。その後の接続の試みでは、サーバが TCP オプションを受信できるかどうかを WAE が再決定できるように、再び TCP オプションが含まれるようになります。ネットワーク パケットの損失により、サーバが誤ってブラックリストに載せられる可能性があるため、TCP オプションの送信を定期的に再試行することは有用です。

[Blacklist Server Address Hold Time] フィールドを変更することにより、ブラックリスト時間を短くしたり長くしたりできます。

ステップ 11　[Submit] をクリックします。

変更がデバイスまたはデバイス グループに保存されます。

CLI から、TFO 最適化、DRE、および永続的圧縮を設定するには、**tfo optimize** グローバル コンフィギュレーション コマンドを使用します。

CLI から EPM アクセラレーションを設定するには、**accelerator epm** グローバル コンフィギュレーション コマンドを使用します。

CLI から HTTP アクセラレーションを設定するには、**accelerator http** グローバル コンフィギュレーション コマンドを使用します。

CLI から NFS アクセラレーションを設定するには、**accelerator nfs** グローバル コンフィギュレーション コマンドを使用します。

CLI から MAPI アクセラレーションを設定するには、**accelerator mapi** グローバル コンフィギュレーション コマンドを使用します。

CLI からビデオ アクセラレーションを設定するには、**accelerator video** グローバル コンフィギュレーション コマンドを使用します。

CLI から SSL アクセラレーションを設定するには、**accelerator ssl** グローバル コンフィギュレーション コマンドを使用します。

CLI から CIFS アクセラレーションを設定するには、**accelerator cifs**、および **accelerator cifs preposition** グローバル コンフィギュレーション コマンドを使用します。

CLI から Windows プリント アクセラレーションを設定するには、**accelerator windows-print** グローバル コンフィギュレーション コマンドを使用します。

CLI から ブラックリスト動作機能を設定するには、**tfo auto-discovery** グローバル コンフィギュレーション コマンドを使用します。

CLI からアプリケーション アクセラレータのステータスと統計情報を表示するには、**show accelerator** および **show statistics accelerator** EXEC コマンドを使用します。Windows プリント アクセラレータの統計情報を表示するには、**show statistics windows-print requests** EXEC コマンドを使用します。

各アプリケーション アクセラレータを使用する詳細については、次の項を参照してください。

- 「HTTP アクセラレーションの設定」（P.12-5）
- 「MAPI アクセラレーションの設定」（P.12-8）
- 「ビデオ アクセラレーションの設定」（P.12-9）
- 「SSL アクセラレーションの設定」（P.12-11）
- CIFS の場合：第 11 章「WAFS の設定」

HTTP アクセラレーションの設定

HTTP アプリケーション アクセラレータは、HTTP トラフィックを加速します。HTTPS を使用する SSL トラフィックは、SSL アクセラレータに渡されます。

デフォルトの Web アプリケーション ポリシーでは、トラフィックを HTTP アクセラレータに送信することが定義されています。Web アプリケーション ポリシーは、HTTP 分類子を使用し、ポート 80、8080、8000、8001、および 3128 上のトラフィックと一致します。他のポート上でも HTTP トラフィックが存在すると予測される場合は、HTTP 分類子にそのポートを追加します。

HTTP アクセラレータを有効化するには、[Enabled Features] ウィンドウで、[HTTP Accelerator] チェックボックスを選択します（図 12-1 を参照）。

HTTP アクセラレーション設定を構成するには、次の手順に従ってください。

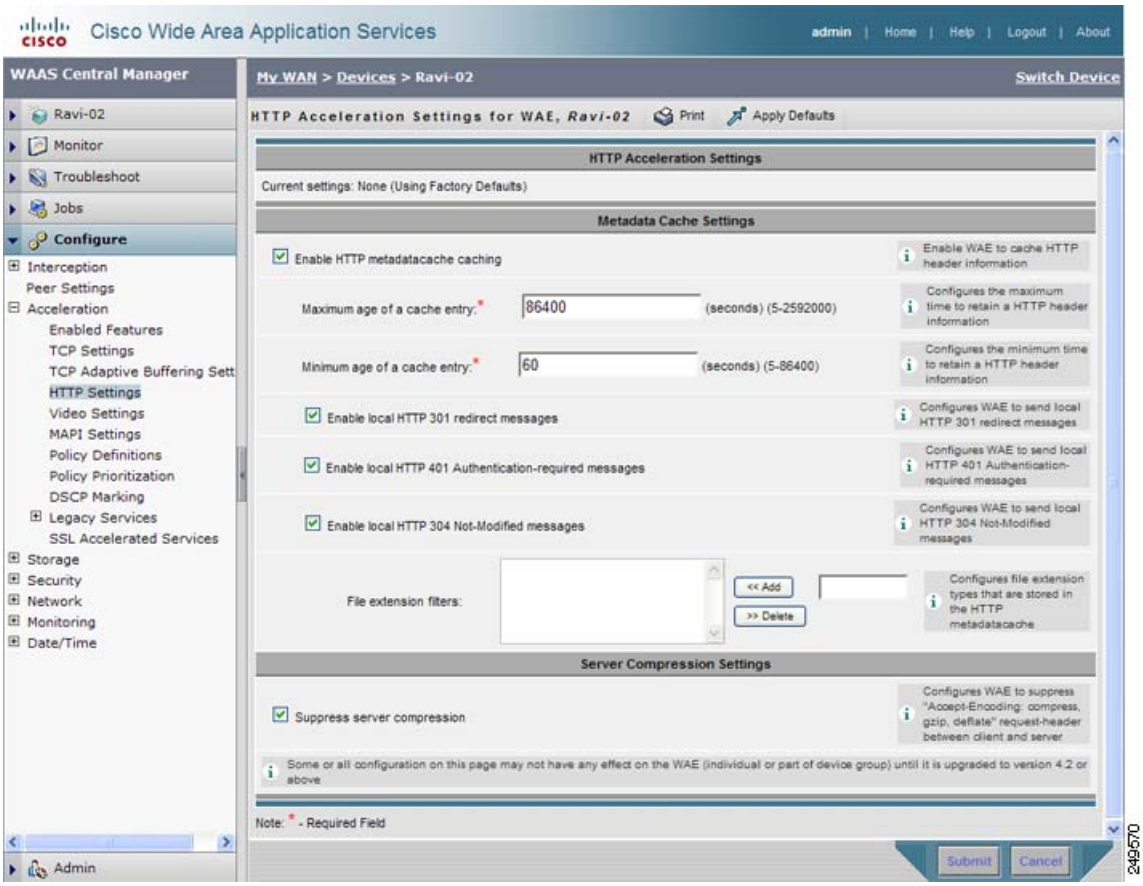
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　HTTP アクセラレーション設定を変更するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [HTTP Settings] を選択します。

[HTTP Acceleration Settings] ウィンドウが表示されます（図 12-2 を参照）。

図 12-2　HTTP アクセラレーション設定の変更



ステップ 4　[Enable HTTP metadatacache caching] チェックボックスを選択して、WAE による HTTP ヘッダー（メタデータ）情報のキャッシングを有効にします。デフォルト設定では、無効になっています。

[Metadata Cache Settings] 内のその他の設定を有効にするには、このチェックボックスをオンにする必要があります。このチェックボックスがオンになっていない場合は、ヘッダーのキャッシングは一切行われません。

HTTP メタデータのキャッシングの詳細については、「HTTP メタデータ キャッシングについて」（P.12-7）を参照してください。

ステップ 5　[Maximum age of a cache entry] フィールドに、HTTP ヘッダー情報をキャッシュ内に保持する最大秒数を入力します。デフォルトは 86400 秒（24 時間）です。指定できる期間は、5 ～ 2592000 秒（30 日間）です。

ステップ 6　[Minimum age of a cache entry] フィールドに、HTTP ヘッダー情報をキャッシュ内に保持する最小秒数を入力します。デフォルトは、60 秒です。指定できる範囲は、5 ～ 86400 秒（24 時間）です。

ステップ 7　[Enable local HTTP 301 redirect messages] チェックボックスを選択して、WAE による HTTP 301 メッセージのキャッシングとローカルでのサービスを有効にします。デフォルト設定では、有効になっています。

ステップ 8　[Enable local HTTP 401 Authentication-required messages] チェックボックスを選択して、WAE による HTTP 401 メッセージのキャッシングとローカルでのサービスを有効にします。デフォルト設定では、有効になっています。

ステップ 9　[Enable local HTTP 304 Not-Modified messages] チェックボックスを選択して、WAE による HTTP 200 および 304 メッセージのキャッシングと、HTTP 304 メッセージのローカルでのサービスを有効にします。デフォルト設定では、有効になっています。

ステップ 10　特定のファイル名拡張子をメタデータ キャッシングの適用先として設定するには、そのファイル名拡張子を右端の [File extension filters] フィールドに入力します。複数の拡張子を指定する場合はカンマで区切ります（例 : jpeg, gif, png）。ファイル名拡張子の先頭につくドットは含めません。[<< Add] ボタンをクリックして、入力したファイル名拡張子を、左側に表示されているアクティブなリストに追加します。最大 20 個のファイル名拡張子を入力できます。

リストから拡張子を削除するには、アクティブなリスト内でそれを選択してから [>> Delete] ボタンをクリックします。

デフォルトでは、ファイル名拡張子のフィルタは 1 つも定義されていないため、メタデータのキャッシングはすべての種類のファイルに適用されます。

ステップ 11　[Suppress server compression] チェックボックスを選択して、WAE にクライアントとサーバの間でのサーバ圧縮を停止させる設定を行います。デフォルト設定では、無効になっています。

このチェックボックスをオンにすることにより、WAE に HTTP 要求ヘッダーから Accept-Encoding 値を削除するように指示して、Web サーバがクライアントに送信する HTTP データを圧縮しないようにできます。これにより、WAE はその独自の圧縮を HTTP データに適用できるようになります。通常は、ほとんどのファイルについて、Web サーバが行うよりもはるかに圧縮率が高くなります。ほとんど変化のない一部のファイル タイプ（.css ファイルや .js ファイルなど）については、この設定は無視され、Web サーバによる圧縮が許可されます。

ステップ 12　[Submit] をクリックします。

変更がデバイスまたはデバイス グループに保存されます。

CLI から HTTP アクセラレーションを設定するには、**accelerator http** グローバル コンフィギュレーション コマンドを使用します。

メタデータ キャッシュ内の内容を表示するには、**show cache http-metadatacache** EXEC コマンドを使用します。

メタデータ キャッシュをクリアするには、**clear cache http-metadatacache** EXEC コマンドを使用します。

HTTP メタデータ キャッシングについて

メタデータ キャッシング機能は、ブランチ オフィスの WAE の HTTP アクセラレータが特定のサーバ応答をキャッシングし、クライアントに対してローカルに応答できるようにします。次のサーバ応答メッセージがキャッシングされます。

- HTTP 200 OK（If-None-Match 要求および If-Modified-Since 要求に適用される）
- HTTP 301 リダイレクト
- HTTP 304 未変更（If-None-Match 要求および If-Modified-Since 要求に適用される）
- HTTP 401 認証が必要

次の場合には、メタデータ キャッシングは適用されません。

- RFC 標準に準拠していない要求と応答
- 255 文字を超える URL
- cookie ヘッダーを持つ 301 および 401 応答

- HEAD 方式が使用されている
- パイプライン化されたトランザクション

（注）　メタデータ キャッシング機能は、WAAS バージョン 4.2.1 で導入されましたが、バージョン 4.2.1 が必要になるのはブランチ オフィスの WAE でだけです。この機能は、もっと低いバージョンのデータ センター WAE 上の HTTP アクセラレータとも相互運用性があります。

MAPI アクセラレーションの設定

MAPI アプリケーション アクセラレータは、Messaging Application Programming Interface（MAPI）プロトコルを使用する Microsoft Outlook Exchange トラフィックを加速させます。Microsoft Outlook 2000 ～ 2007 のクライアントがサポート対象です。クライアントは、キャッシュ モードまたは非キャッシュ モードのいずれかの Outlook で設定できます。いずれのモードも加速化されます。

メッセージ認証（署名）を使用するセキュア接続または暗号化は、加速化されません。また、MAPI over HTTP は加速化されません。

（注）　Microsoft Outlook 2007 では、デフォルトで暗号化が有効です。MAPI アプリケーション アクセラレータを利用するには、暗号化を無効にする必要があります。

MAPI アプリケーション アクセラレータが動作するには、EPM アプリケーション アクセラレータを有効にする必要があります。EPM は、デフォルトで有効です。さらに、システムでは、タイプ EPM のアプリケーション ポリシーを定義し、MAPI UUID を指定して、MAPI の [Accelerate] 設定を行う必要があります。このポリシー（E メールとメッセージング アプリケーション用の MAPI）は、デフォルトで定義されます。

MAPI など、EPM トラフィックでは通常定義済みのポートを使用しません。Outlook の管理者が、スタティック ポートを使用するため、非標準的な方法で Outlook を設定している場合、Outlook に設定済みのスタティック ポートに一致する分類子により MAPI トラフィックを加速化させるという新しい基本アプリケーション ポリシーを作成する必要があります。

（注）　WAE が接続により過負荷状態になると、MAPI アプリケーション アクセラレータは、内部的に予約されている接続リソースを使用して MAPI 接続の高速化を続けます。予約されていたリソースも使い果たすと、接続リソースに空きができるまで、新しい MAPI 接続はパススルーされます。

MAPI アクセラレータを有効化するには、[Enabled Features] ウィンドウで、[MAPI Accelerator] チェックボックスを選択します（図 12-1 を参照）。

MAPI アクセラレーション設定を構成するには、次の手順に従ってください。

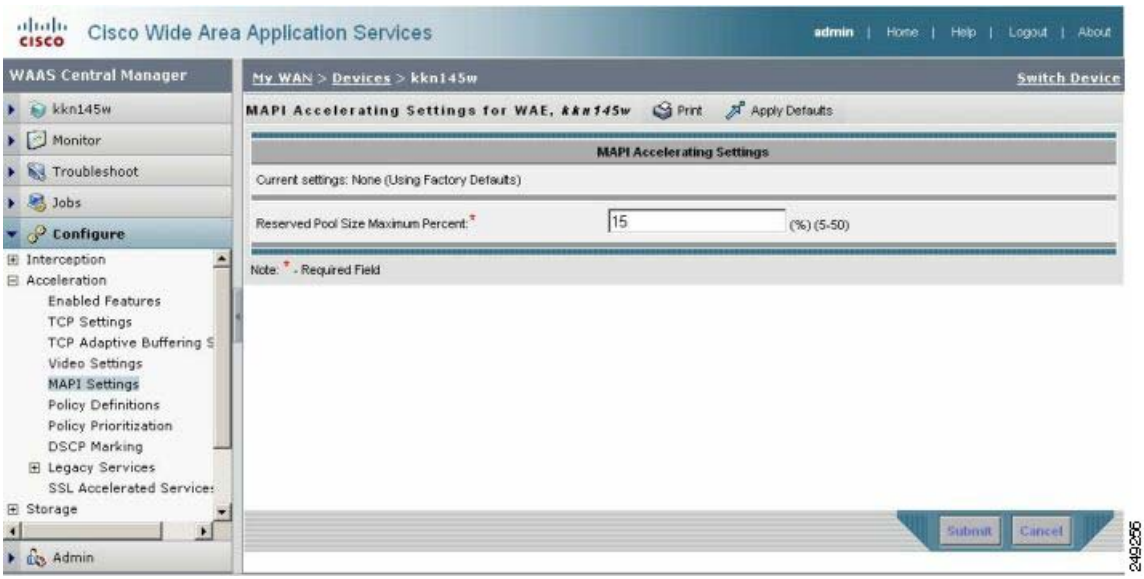
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　MAPI アクセラレーション設定を変更するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [MAPI Settings] を選択します。

[MAPI Acceleration Settings] ウィンドウが表示されます（図 12-3 を参照）。

図 12-3　　MAPI アクセラレーション設定の変更



ステップ 4　[Reserved Pool Size Maximum Percent] フィールドに、TFO の過負荷時の MAPI 最適化のために予約される最大接続数を制限する、最大接続割合を入力します。プラットフォームの TFO 接続制限に対する割合で指定します。有効な割合の範囲は、5 ～ 50% です。デフォルトは 15% です。この場合、MAPI アクセラレータで最適化されるクライアントとサーバの間の Association Group（AG）ごとに約 0.5 の接続が予約されます。

クライアントは、接続するサーバごとに少なくとも 1 つの AG を維持し、AG あたり約 3 つの接続が平均で使用されます。AG あたりの平均接続数がそれよりも多い、または TFO の過負荷が頻繁に発生する配置では、予約されるプール サイズの最大割合により大きい値を指定することを推奨します。

予約された接続は、デバイスが TFO の過負荷状態でないときは使用されません。予約された接続は、AG が終了すると解放されます。

ステップ 5　[Submit] をクリックします。変更がデバイスまたはデバイス グループに保存されます。

ビデオ アクセラレーションの設定

ビデオ アプリケーション アクセラレータは、RTSP over TCP を使用する Windows Media ライブ ビデオ ブロードキャストを加速化させます。ビデオ アクセラレータは、自動的に、WAN からの 1 つのソース ビデオ ストリームを複数のストリームに分割し、LAN 上の複数のクライアントに供給します。

ビデオ アクセラレータは、自動的に、UDP ストリームを要求しているクライアントがプロトコル ロールオーバーを行って、TCP を使用できるようにします（クライアントとサーバの両方で TCP が可能な場合）。

ストリーミング アプリケーション ポリシーのデフォルトの RTSP 分類子は、ビデオ アクセラレータにトラフィックを送信するように定義されています。

デフォルトでは、ビデオ アクセラレータは加速されていないビデオ トラフィックをすべて送信して、ネゴシエーション済みの標準 TCP 最適化ポリシーにより処理されるようにします（ビデオ アクセラレータがこのようなトラフィックをドロップするよう明示的に設定されていない場合）。すべての加速されていないビデオ トラフィック、または過負荷状態が原因で加速されていないトラフィックだけをドロップするように選択できます。

ビデオ アクセラレータを有効化するには、[Enabled Features] ウィンドウで、[Video Accelerator] チェックボックスを選択します（図 12-1 を参照）。

ビデオ アクセラレーション設定を構成するには、次の手順に従ってください。

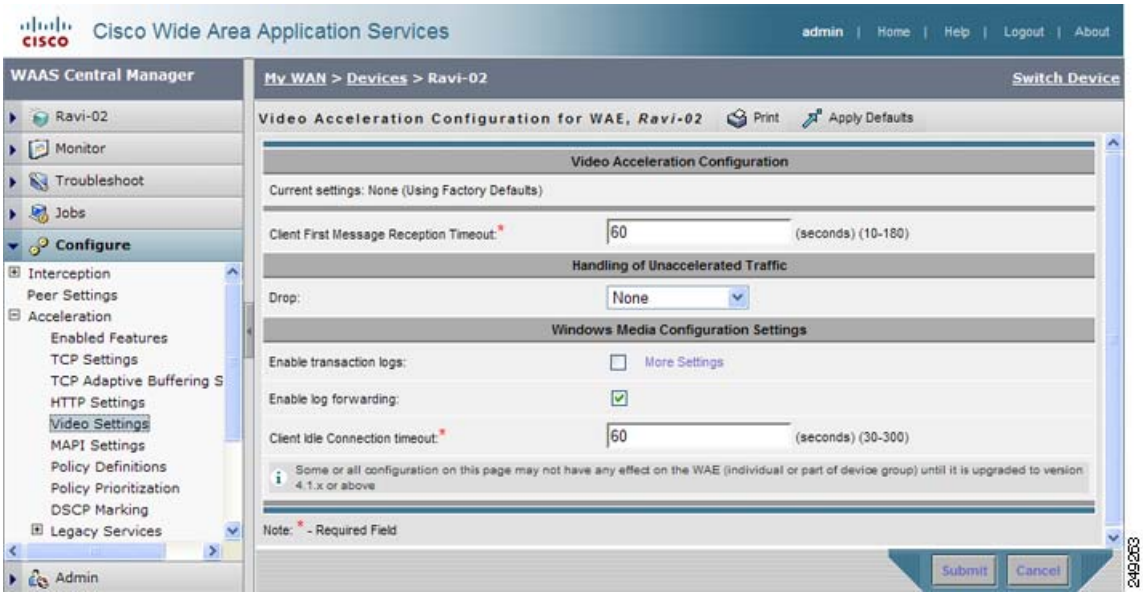
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　ビデオ アクセラレーション設定を変更するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Video Settings] を選択します。

[Video Acceleration Configuration] ウィンドウが表示されます（図 12-4 を参照）。

図 12-4　ビデオ アクセラレーション設定の変更



ステップ 4　[Client First Message Reception Timeout] フィールドでは、ビデオ アクセラレータで接続が受け入れられてから接続のタイムアウトが発生するまで、クライアントからの最初のメッセージおよびサーバからの最初の応答を待機する時間（秒）を入力します。有効範囲は、10 ～ 180 秒です。デフォルトは、60 です。

ステップ 5　ドロップダウン リストで、加速されていないビデオ トラフィックのドロップ方法を次の中から選択します。

- [All]：サポート対象外の伝送や形式、あるいは過負荷が原因で加速されないすべてのビデオ トラフィックをドロップします。すべての Windows Media ビデオオンデマンド トラフィックおよびすべての非 Windows Media RTSP トラフィックはドロップされます。
- [Overload Only]：アクセラレータの過負荷だけが原因で加速されないすべてのビデオ トラフィックをドロップします。
- [None]：加速されていないビデオ 接続をネゴシエーション済みの TCP 最適化ポリシーで処理します（トラフィックはドロップされません）。

（注）　有効なライセンスがない場合や特定のエラー状態など、一部の条件下ではビデオ アクセラレータがポリシー エンジンに登録されません。加速されていないすべてのビデオ トラフィックをドロップするようにビデオ アクセラレータを設定すると、ポリシー エンジンはすべてのビデオ トラフィックをドロップします（ビデオ アクセラレータがポリシー エンジンに正しく登録されていれば加速されるようなトラフィックであっても同様です）。

ステップ 6　[Enable transaction logs] チェックボックスを選択して、トランザクション ログ機能を有効にします。この機能により、大量のログ データが生成されます。デフォルトで、このボックスは選択されていません。[More Settings] リンクをクリックして、[Windows Media Transaction Log Settings] 設定ページに移動します。

ステップ 7　[Enable log forwarding] チェックボックスを選択して、Windows Media ログのアップストリーム Windows Media Server への転送を有効にします。デフォルトで、このボックスは選択されています。

ステップ 8　[Client Idle Connection timeout] フィールドでは、最初のクライアント要求の後、接続のタイムアウトが発生するまで、クライアント接続がアイドル状態のまま待機する最大時間（秒）を入力します。有効範囲は、30 ～ 300 秒です。デフォルトは、60 です。

ステップ 9　[Submit] をクリックします。

変更がデバイスまたはデバイス グループに保存されます。

CLI からビデオ アクセラレーションを設定するには、**accelerator video** グローバル コンフィギュレーション コマンドを使用します。

SSL アクセラレーションの設定

SSL アプリケーション アクセラレータでは、Secure Sockets Layer（SSL）暗号化接続上のトラフィックが最適化されます。SSL アクセラレーションを有効にすると、WAAS ソフトウェア DRE 最適化は SSL 暗号化トラフィックに対してあまり効果はありません。SSL アプリケーション アクセラレーションにより、WAAS は、接続のセキュリティを保ったまま、復号化および最適化の適用が可能になります。

（注）　SSL アクセラレータは、一番最初のバイトから SSL/TLS ハンドシェイクを開始しないプロトコルの最適化は行いません。唯一の例外は、プロキシを通過する HTTPS です（HTTP アクセラレータが SSL/TLS の開始を検出し、その接続を最適化されるように SSL アクセラレータに引き渡します）。

SSL アプリケーション アクセラレータは、SSL Version 3（SSLv3）および Transport Layer Security Version 1（TLSv1）プロトコルをサポートしています。TLSv1.1 および TLSv1.2 プロトコルはサポートされていません。

表 12-1 に、SSL を設定し、有効にするために完了しなければならない手順の概要を示します。

表 12-1　SSL アクセラレーションを設定するためのチェックリスト

作業	追加情報と手順
1. SSL アクセラレーションの設定を準備します。	SSL アクセラレーションを WAAS デバイス上で設定する前に収集する必要のある情報を特定します。詳細については、「SSL アクセラレーションを使用するための準備」（P.12-12）を参照してください。

表 12-1　SSL アクセラレーションを設定するためのチェックリスト （続き）

作業	追加情報と手順
2. セキュア ストア、Enterprise ライセンス、および SSL アクセラレーションを有効にします。	Central Manager セキュア ストアの設定方法、Enterprise ライセンスの有効化方法、および SSL アクセラレーションの有効化方法について説明します。セキュア ストア モードは、SSL 暗号化証明書およびキーを安全に扱うために必要です。詳細については、「セキュア ストア、Enterprise ライセンス、および SSL アクセラレーションの有効化」（P.12-13）を参照してください。
3. SSL アプリケーション最適化を有効にします。	SSL アクセラレーション機能の有効化方法について説明します。詳細については、「グローバル最適化機能の有効化と無効化」（P.12-2）を参照してください。
4. SSL アクセラレーション設定を構成します。	（任意）SSL アクセラレーションの基本設定の構成方法について説明します。詳細については、「SSL グローバル設定の構成」（P.12-14）を参照してください。
5. 暗号リストを作成し、管理します。	（任意）WAAS デバイスで使用される暗号アルゴリズムの選択方法と設定方法について説明します。詳細については、「暗号リストの操作」（P.12-18）を参照してください。
6. CA 証明書を設定します。	（任意）Certificate Authority（CA; 認証局）証明書の選択方法、インポート方法、および管理方法について説明します。詳細については、「認証局の操作」（P.12-20）を参照してください。
7. SSL マネジメント サービスを設定します。	（任意）Central Manager と WAE デバイスの間で使用される SSL 接続を設定する方法について説明します。詳細については、「SSL マネジメント サービスの設定」（P.12-22）を参照してください。
8. SSL ピアリング サービスを設定します。	（任意）最適化された SSL トラフィックを伝送するために、ピア WAE デバイス間で使用される SSL 接続を設定する方法について説明します。詳細については、「SSL ピアリング サービスの設定」（P.12-24）を参照してください。
9. SSL アクセラレーション サービスを設定し、有効にします。	SSL アプリケーション最適化機能によって加速されるサービスの追加方法、設定方法、および有効化方法について説明します。詳細については、「SSL アクセラレーション サービスの使用」（P.12-25）を参照してください。

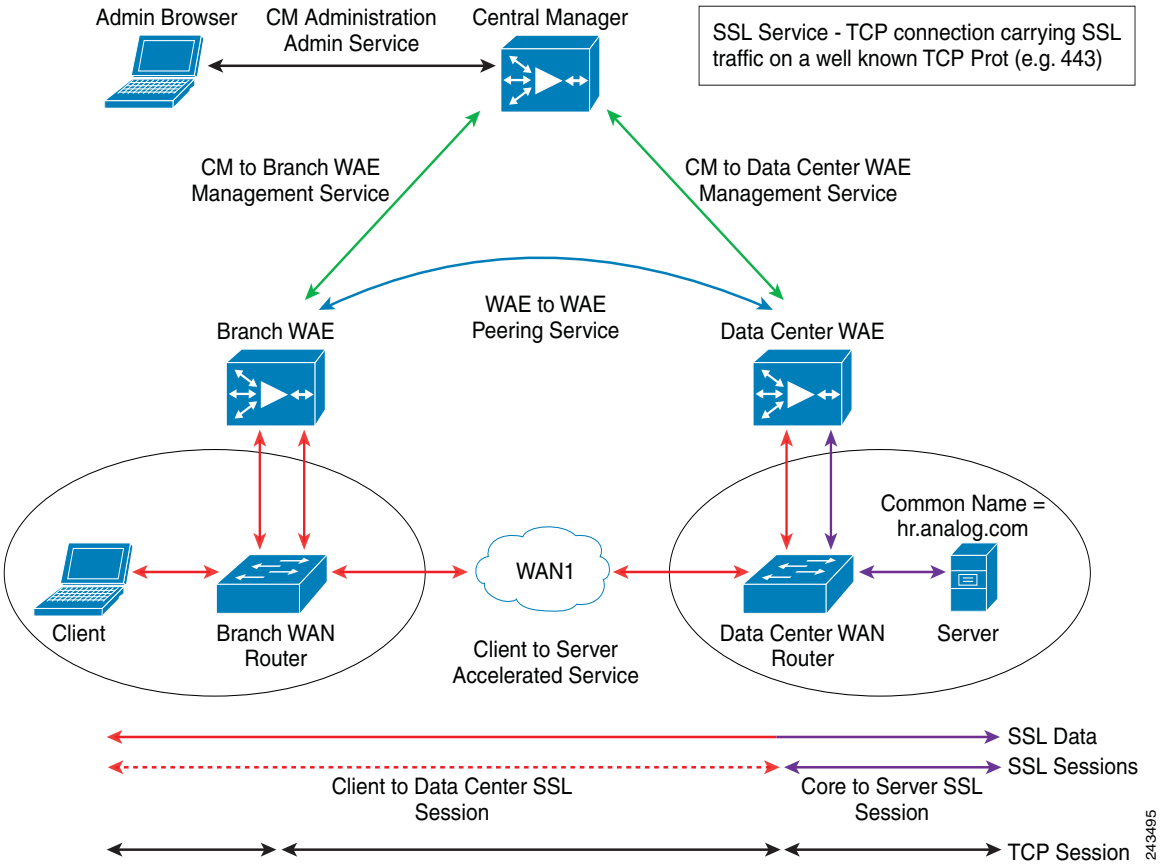
SSL アクセラレーションを使用するための準備

SSL アクセラレーションを設定する前に、次の情報を確認する必要があります。

- SSL トラフィックに対して加速化されるサービス
- サーバの IP アドレスとポート情報
- Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）証明書と秘密キー情報（証明書共通名と認証局署名情報を含む）
- サポートされる暗号スイート
- サポートされる SSL バージョン

図 12-5 に、WAAS ソフトウェアが SSL アプリケーション最適化を処理する方法を示します。

図 12-5　SSL アクセラレーションのブロック図



SSL アクセラレーションを設定する場合は、SSL アクセラレーション サービスをサーバ側（データセンター）の WAE デバイス上で設定する必要があります。クライアント側（ブランチ オフィス）の WAE では、セキュア ストアを初期化してそのロックを解除するか開く必要がありますが、SSL アクセラレーション サービスを設定する必要はありません。一方、SSL アクセラレータは、SSL アクセラレーション サービスが動作するために、データセンター WAE とブランチ WAE の両方で有効にする必要があります。WAAS Central Manager は、SSL マネジメント サービスを提供し、暗号化証明書とキーを保持します。

セキュア ストア、Enterprise ライセンス、および SSL アクセラレーションの有効化

SSL アクセラレーションを WAAS システム上で使用するには、次の手順を実行しておく必要があります。

ステップ 1　Central Manager でセキュア ストア暗号化を有効にします。

セキュア ストア暗号化を有効にするには、「セキュア ストア設定の構成」（P.9-10）を参照してください。

ステップ 2　Enterprise ライセンスを有効にします。

Enterprise ライセンスを有効にするには、「ソフトウェア ライセンスの管理」（P.9-3）を参照してください。

ステップ 3　SSL アクセラレーションをデバイス上で有効にします。

SSL アクセラレーション機能を有効にするには、「グローバル最適化機能の有効化と無効化」（P.12-2）を参照してください。

（注）　SSL アクセラレータがすでに稼動しているときに、新しい WAE を Central Manager に登録した場合は、データフィード ポーリングが 2 サイクル実行されてから、設定変更を行う必要があります。そうしなければ、変更は無効になる可能性があります。

SSL グローバル設定の構成

基本的な SSL アクセラレーション設定を構成するには、次の手順に従ってください。

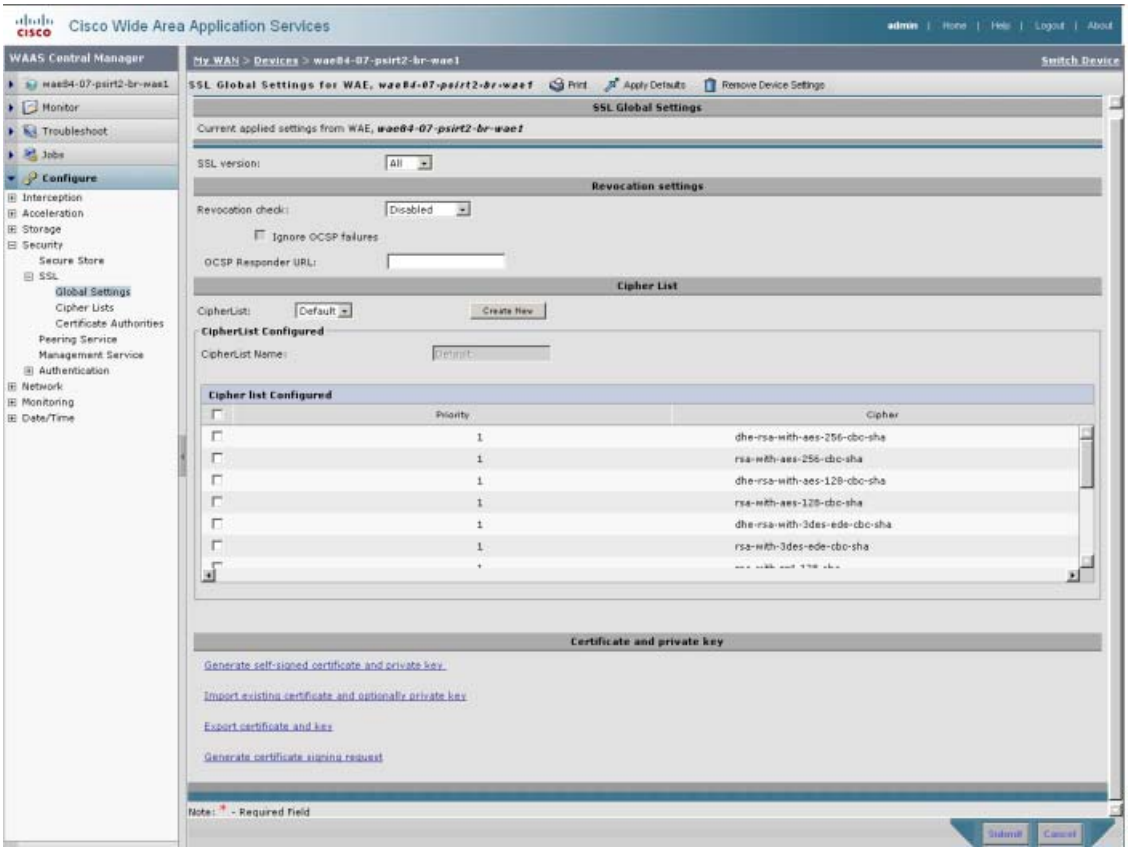
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　SSL アクセラレーションを設定したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [SSL] > [Global Settings] を選択します。

[SSL Global Settings] ウィンドウが表示されます（図 12-6 を参照）。

図 12-6　SSL グローバル設定



ステップ 4　特定のデバイス グループの SSL 設定を使用するようにデバイスを設定するには、SSL グローバル設定ツールバーにある [Select a Device Group] ドロップダウン リストからデバイス グループを選択します。デバイスには、独自の SSL 設定、またはデバイス グループの SSL 設定を使用できます。ただし、複数のデバイス グループの SSL 設定を使用するように、デバイスを設定することはできません。

ステップ 5　[SSL version] フィールドで、使用する SSL プロトコルの種類を選択します。SSL バージョン 3 プロトコルの場合は [SSL3] を選択し、Transport Layer Security バージョン 1 プロトコルの場合は [TLS1] を選択し、SSL3 プロトコルと TLS1 SSL プロトコルの両方を許可する場合は [All] を選択します。

ステップ 6　（任意）証明書失効の Online Certificate Status Protocol（OCSP）パラメータを設定します。

a. [OCSP Revocation check] ドロップダウン リストで、OCSP 失効チェック方法を選択します。

[ocsp-url] を選択すると、SSL アクセラレータは、[OCSP Responder URL] フィールドに指定された OCSP レスポンダを使用して証明書の失効ステータスをチェックします。[ocsp-cert-url] を選択すると、証明書を署名した認証局証明書に指定されている OCSP レスポンダ URL を使用します。

b. [Ignore OCSP failures] チェックボックスが選択されている場合、SSL アクセラレータは、OCSP レスポンダから明確な応答を得ていなくても、OCSP 失効チェックを成功として処理します。

ステップ 7　[Cipher List] フィールドで、SSL アクセラレーションに使用される暗号スイートのリストを選択します。詳細については、「暗号リストの操作」（P.12-18）を参照してください。

ステップ 8　証明書 / キー ペアの方法を選択します（図 12-7 を参照）。

図 12-7　　サービス証明書と秘密キーの設定

- WAAS デバイスで SSL に自己署名証明書 / キー ペアを使用するには、[Generate Self-signed Certificate Key] をクリックします。
- 既存の証明書 / キー ペアをアップロードまたは張り付けるには、[Import Existing Certificate Key] をクリックします。
- 現在の証明書 / キー ペアをエクスポートするには、[Export Certificate Key] をクリックします。
- 既存の証明書 / キー ペアを更新または置き換えるには、[Generate Certificate Signing Request] をクリックします。Certificate Signing Request（CSR; 証明書署名要求）は、新しい証明書を生成するために認証局で使用されます。

  インポートまたはエクスポートするファイルは、PKCS12 形式と PEM 形式のいずれかである必要があります。

サービス証明書と秘密キーの設定手順については、「サービス証明書と秘密キーの設定」（P.12-16）を参照してください。

ステップ 9　[Submit] をクリックします。

サービス証明書と秘密キーの設定

サービス証明書と秘密キーを設定するには、次の手順に従ってください。

ステップ 1　自己署名証明書と秘密キーを生成するには（図 12-8 を参照）、次の手順に従ってください。

図 12-8　　自己署名証明書と秘密キー

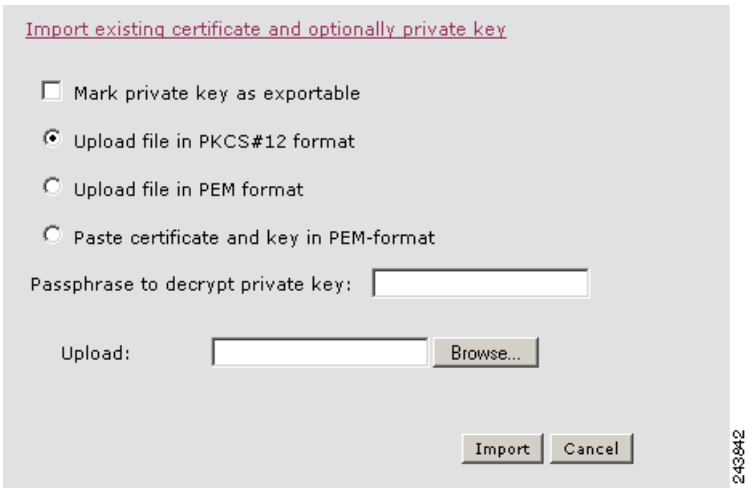
a. この証明書 / キーを後で WAAS Central Manager およびデバイス CLI からエクスポートする場合は、[Mark private key as exportable] チェックボックスを選択します。

b. 証明書と秘密キーのフィールドに必要事項を入力します。

ステップ 2　既存の証明書または証明書チェーン、および（必要に応じて）秘密キーをインポートするには（図 12-9 を参照）、次の手順に従ってください。

（注）　WAAS SSL 機能は、RSA の署名 / 暗号化アルゴリズムとキーだけをサポートします。

図 12-9　既存の証明書または証明書チェーンのインポート



a. この証明書/キーを後で WAAS Central Manager およびデバイス CLI からエクスポートする場合は、[Mark private key as exportable] チェックボックスを選択します。

b. 既存の証明書または証明書チェーン、および秘密キーをインポートするには、次のいずれかを実行します。

- 証明書とキーを PKCS#12 形式で（または Microsoft PFX 形式として）アップロードする。
- 証明書と秘密キーを PEM 形式でアップロードする。
- 証明書と秘密キーの PEM の内容を貼り付ける。

証明書と秘密キーがすでに設定されている場合は、証明書だけアップデートできます。この場合、Central Manager では、インポートされた証明書と現在の秘密キーを使用して、証明書と秘密キーのペアが構築されます。この機能は、既存の自己署名証明書を認証局によって署名されたものにアップデートする場合や、期限の切れる証明書をアップデートするために使用できます。

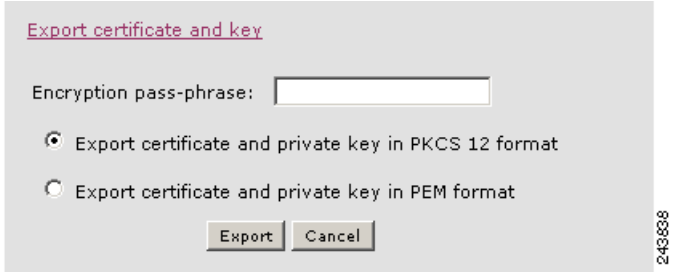
Central Manager では、証明書チェーンをインポートできます。このチェーンは、最初にエンド証明書が指定され、その後にエンド証明書または中間 CA 証明書を署名する中間 CA 証明書のチェーンが続き、最後はルート CA で終わる必要があります。

Central Manager では、このチェーンが検証され、CA 証明書の使用期限が切れているか、チェーン内の署名順序が論理的でない場合、そのチェーンは拒否されます。

c. 秘密キーを復号化するパスフレーズを入力します。秘密キーが暗号化されていない場合は、該当するフィールドを空のままにします。

ステップ 3　設定された証明書と秘密キーをエクスポートするには（図 12-10 を参照）、次の手順に従ってください。

図 12-10　証明書とキーのエクスポート



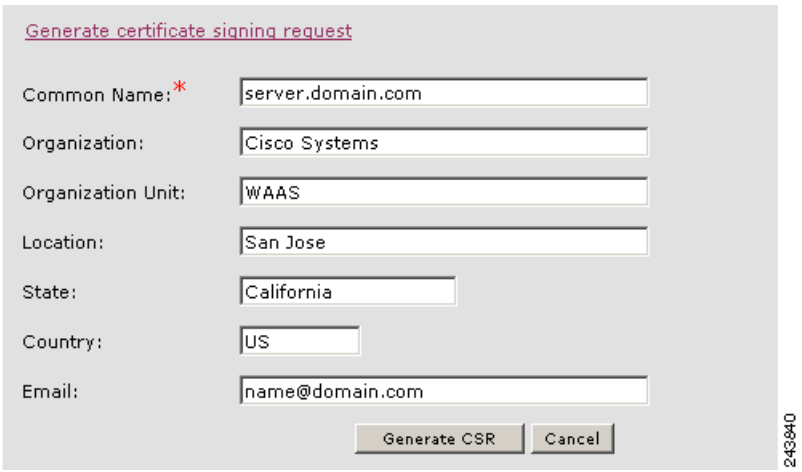
a. 暗号化パスフレーズを入力します。

b. 現在の証明書および秘密キーを PKCS#12 形式または PEM 形式でエクスポートします。PEM 形式の場合、証明書と秘密キーの両方が 1 つの PEM ファイルに含められます。

（注） 生成またはインポート時にエクスポート不可能と指定した証明書と秘密キーは、Central Manager でエクスポートできません。

ステップ 4　現在の証明書と秘密キーから証明書署名要求を生成するには（図 12-11 を参照）、次の手順に従ってください。

図 12-11　証明書署名要求の生成



現在の証明書を、認証局によって署名されたものにアップデートするには、次の手順を実行します。

a. PKCS#10 証明書署名要求を生成します。

b. 生成された証明書署名要求を、証明書の生成と署名を行う認証局に送信します。

c. 認証局から受信した証明書を、[Importing existing certificate and optionally private key] オプションを使用してインポートします。

（注） 生成された証明書要求のキーのサイズは、現在の証明書のキーのサイズと同じです。

暗号リストの操作

暗号リストは、SSL アクセラレーション設定に割り当て可能な暗号スイートの集合です。暗号スイートは、キー交換アルゴリズム、暗号化アルゴリズム、および Secure Hash Algorithm を含む SSL 暗号化方式です。

暗号リストを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　暗号リストを設定したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [SSL] > [Cipher Lists] を選択します。

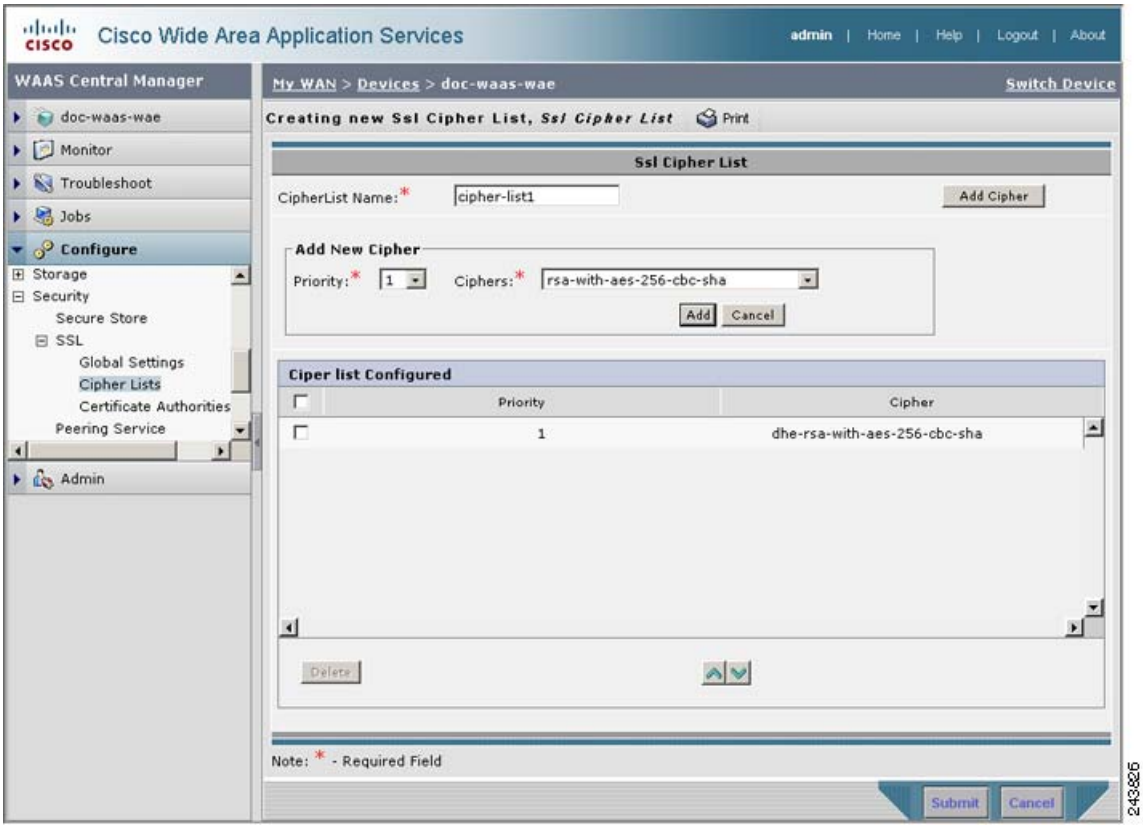
[SSL Cipher Lists] ウィンドウが表示されます（図 12-12 を参照）。

図 12-12　SSL 暗号リストの表示

ステップ 4　[Create] をクリックして、新しい暗号リストを追加します。

[Creating New SSL Cipher List] ウィンドウが表示されます（図 12-13 を参照）。

図 12-13　SSL 暗号リストの作成



ステップ 5　[Cipher List Name] フィールドに暗号リストの名前を入力します。

ステップ 6　[Add Cipher] をクリックして、暗号スイートを暗号リストに追加します。

ステップ 7　追加する暗号スイートを [Ciphers] フィールドで選択します。

（注）　Microsoft IIS サーバに対して SSL 接続を確立する場合は、DHE ベースの暗号スイートを選択してはなりません。

ステップ 8　選択した暗号スイートの優先順位を [Priority] フィールドで選択します。

（注）　SSL ピアリング サービスが設定されている場合は、コア デバイス上の暗号リストに関連付けられた優先順位が、エッジ デバイス上の暗号リストに関連付けられた優先順位よりも優先されます。

ステップ 9　[Add] をクリックして、選択した暗号スイートを暗号リストに加えます。あるいは、[Cancel] をクリックして、暗号リストを元の状態のままにします。

ステップ 10　ステップ 6 からステップ 9 を繰り返して、必要なだけ暗号スイートを暗号リストに追加します。

ステップ 11　（任意）暗号スイートの優先順位を変更するには、暗号スイートのチェックボックスを選択し、暗号リストの下にある上向き矢印または下向き矢印のボタンを使用して優先順位を設定します。

（注）　アクセラレーション サービスに暗号リストが適用される場合、ここで割り当てた暗号リストの優先順位は、クライアントで指定された暗号の順序で上書きされます。この暗号リストで割り当てた優先順位は、暗号リストが SSL ピアリング サービスとマネジメント サービスに適用される場合に限り有効です。

ステップ 12　（任意）暗号リストから暗号スイートを削除するには、暗号スイートのチェックボックスを選択し、[Delete] をクリックします。

ステップ 13　暗号リストの設定が完了したら、[Submit] をクリックします。

認証局の操作

WAAS SSL アクセラレーション機能では、システムで使用される Certificate Authority（CA; 認証局）証明書を設定できます。WAAS に含まれる多くの既知の CA 証明書のいずれかを使用するか、独自の CA 証明書をインポートできます。

CA 証明書を管理するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　CA 証明書を管理したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [SSL] > [Certificate Authorities] を選択します。

[SSL CA Certificate List] ウィンドウが表示されます（図 12-14 を参照）。

図 12-14　SSL CA 証明書リストの表示

ステップ 4　WAAS に含まれるプリロードされた CA 証明書のいずれかを、次の手順に従って追加します。

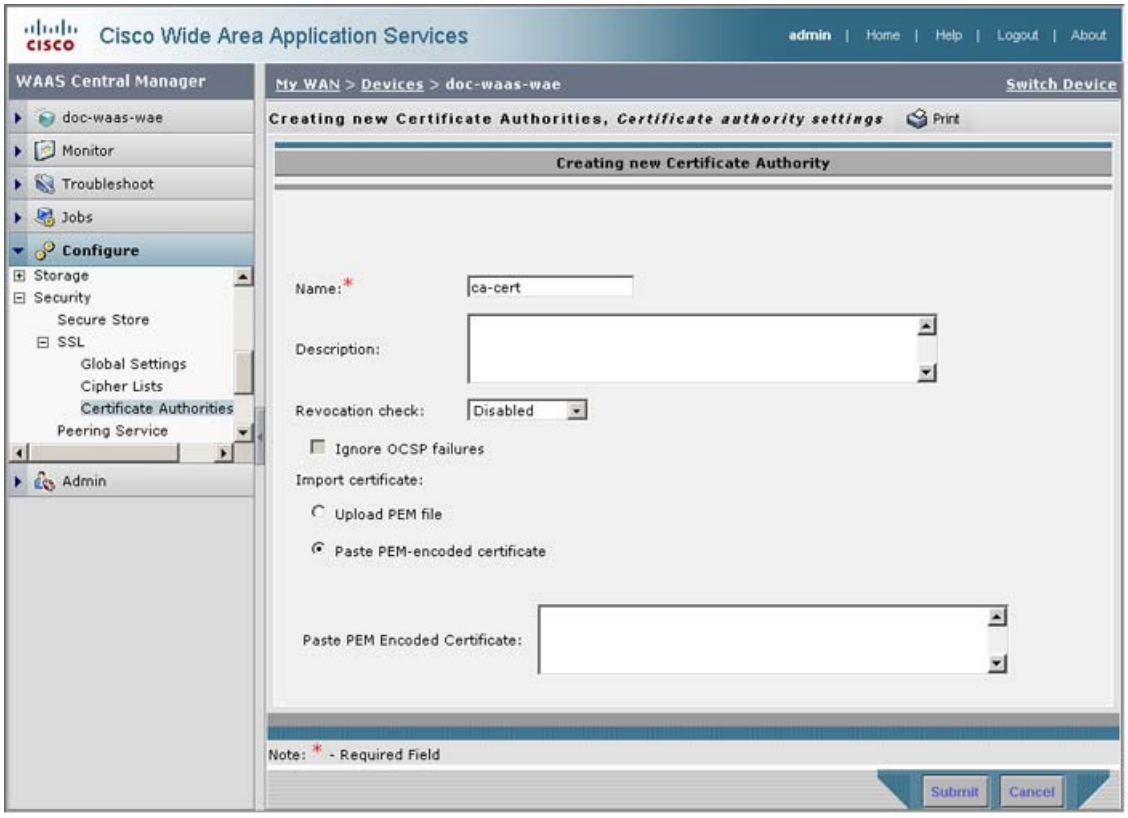
a. [Well-known CAs] をクリックします。

b. 追加する既存の CA 証明書を選択し、[Import] をクリックします。選択した CA 証明書は、[SSL CA Certificate List] に表示されているリストに追加されます。

ステップ 5　独自の CA 証明書を次の手順に従って追加します。

a. [Create] をクリックします。[Creating New CA Certificate] ウィンドウが表示されます（図 12-15 を参照）。

図 12-15　新しい CA 証明書の作成



b. 証明書の名前を [Certificate Name] フィールドに入力します。

c. （任意）CA 証明書の説明を [Description] フィールドに入力します。

d. [Revocation check] ドロップダウン リストで [disabled] を選択して、この CA によって署名された証明書の OCSP 失効チェックを無効にします。[Ignore OCSP failures] チェックボックスを選択して、OCSP 失効チェックが失敗しても失効チェックは成功したとマーク付けされるようにします。

e. [Upload PEM File] または [Paste PEM Encoded Certificate] を選択して、証明書情報を追加します。

ファイルをアップロードする場合は、ファイルを Privacy Enhanced Mail（PEM; プライバシー強化メール）形式にする必要があります。使用するファイルの位置を指定し、[Upload] をクリックします。

CA 証明書情報を貼り付ける場合は、PEM 形式の証明書のテキストを [Paste PEM Encoded certificate] フィールドに貼り付けます。

f. [Submit] をクリックして、変更を保存します。

ステップ 6　（任意）リストから認証局を削除するには、認証局を選択した後、ツールバーにある [Delete] アイコンをクリックします。

ステップ 7　CA 証明書リストの設定が完了したら、[Submit] をクリックします。

SSL マネジメント サービスの設定

SSL マネジメント サービスは、Central Manager と WAE デバイスの間の安全な通信に影響を与える SSL 設定パラメータです（図 12-5（P.12-13）を参照）。使用される証明書/キー ペアは、WAAS デバイスごとに固有です。そのため、SSL マネジメント サービスは、個々のデバイスに対してだけ設定でき、デバイス グループには設定できません。

SSL マネジメント サービスを設定するには、次の手順に従ってください。

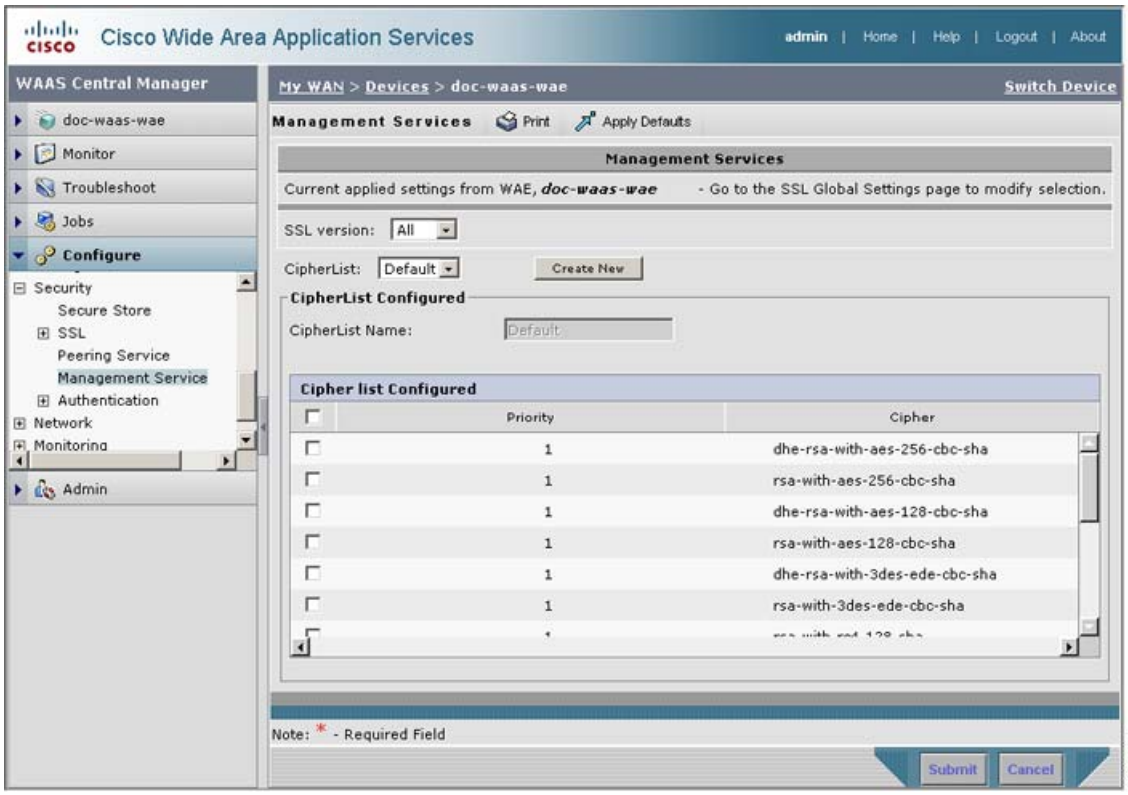
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　SSL マネジメント サービスを設定したいデバイスの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [Management Service] を選択します。

[Management Services] ウィンドウが表示されます（図 12-16 を参照）。

図 12-16　SSL マネジメント サービスの設定



ステップ 4　[SSL version] フィールドで、使用する SSL プロトコルの種類を選択します。SSL バージョン 3 プロトコルの場合は [SSL3] を選択し、Transport Layer Security バージョン 1 プロトコルの場合は [TLS1] を選択し、SSL3 プロトコルと TLS1 SSL プロトコルの両方を使用する場合は [All] を選択します。

（注）　WAAS Central Manager に設定されたマネジメント サービスの SSL バージョンと暗号の設定は、WAAS Central Manager とユーザのブラウザの間の SSL 接続にも適用されます。

プライマリおよびスタンバイの Central Manager は、マネジメント サービスのバージョンや暗号リストを共有する必要があります。マネジメント サービスのバージョンおよび暗号リストの設定を変更すると、プライマリ Central Manager とスタンバイ Central Manager と WAE デバイスの間の接続が失われる可能性があります。

表 12-2 に、Internet Explorer と Mozilla Firefox でサポートされる暗号リストを示します。

表 12-2　Internet Explorer と Mozilla Firefox でサポートされる暗号リスト

暗号	Internet Explorer	Firefox
dhe-rsa-with-aes-256-cbc-sha	IE7/Vista でサポート	サポート
rsa-with-aes-256-cbc-sha	IE7/Vista でサポート	サポート
dhe-rsa-with-aes-128-cbc-sha	IE7/Vista でサポート	サポート
rsa-with-aes-128-cbc-sha	IE7/Vista でサポート	サポート
dhe-rsa-with-3des-ede-cbc-sha	デフォルトでは使用不可	サポート

表 12-2　Internet Explorer と Mozilla Firefox でサポートされる暗号リスト （続き）

暗号	Internet Explorer	Firefox
rsa-with-3des-ede-cbc-sha	デフォルトでは使用不可	サポート
rsa-with-rc4-128-sha	サポート	サポート
rsa-with-rc4-128-md5	サポート	サポート
dhe-rsa-with-des-cbc-sha	未サポート	デフォルトでは使用不可
rsa-export1024-with-rc4-56-sha	サポート	デフォルトでは使用不可
rsa-export1024-with-des-cbc-sha	サポート	デフォルトでは使用不可
dhe-rsa-export-with-des40-cbc-sha	未サポート	未サポート
rsa-export-with-des40-cbc-sha	未サポート	未サポート
rsa-export-with-rc4-40-md5	サポート	サポート

（注）　Mozilla Firefox と Internet Explorer の両方で SSLv3 プロトコルと TLSv1 プロトコルがサポートされています。ただし、TLSv1 は、デフォルトでは使用できない場合があります。その場合は、ブラウザで TLSv1 を有効にする必要があります。

ブラウザでサポートされていない暗号またはプロトコルを設定すると、ブラウザと Central Manager の間の接続が失われます。この問題が発生した場合は、CLI から Central Manager マネジメント サービスの SSL 設定をデフォルトに設定して、接続を復元します。

Internet Explorer など、一部のブラウザは、Central Manager 上での SSL バージョンと暗号の設定変更に対して正しく対処しません。そのため、変更を送信した後にエラー ページがブラウザに表示されることがあります。この問題が発生した場合は、ページをリロードします。

ステップ 5　Cipher List ペインで、SSL アクセラレーションに使用される暗号スイートのリストを選択します。詳細については、「暗号リストの操作」（P.12-18）を参照してください。

SSL ピアリング サービスの設定

SSL ピアリング サービス設定パラメータは、SSL 接続を最適化すると同時に、WAE デバイス間に SSL アクセラレータによって確立される安全な通信を制御します（図 12-5（P.12-13）を参照）。ピアリング サービス証明書と秘密キーは、WAAS デバイスごとに固有です。そのため、個々のデバイスに対してだけ設定でき、デバイス グループには設定できません。

SSL ピアリング サービスを設定するには、次の手順に従ってください。

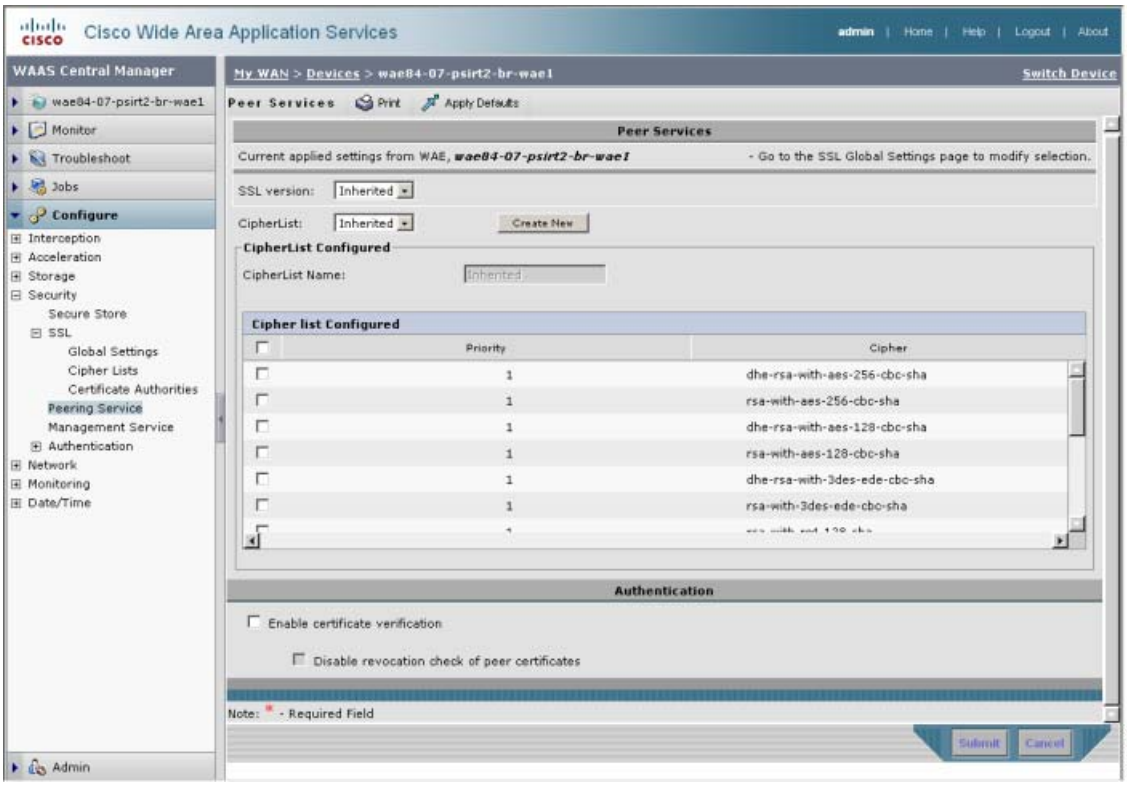
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　SSL ピアリング サービスを設定したいデバイスの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Security] > [Peering Service] を選択します。

[Peering Service] ウィンドウが表示されます（図 12-17 を参照）。

図 12-17　SSL ピアリング サービスの設定



ステップ 4　[SSL Version] フィールドで、使用する SSL プロトコルの種類を選択するか、[Inherited] を選択してグローバル SSL 設定に設定されている SSL プロトコルを使用します。SSL バージョン 3 プロトコルの場合は [SSL3] を選択し、Transport Layer Security バージョン 1 プロトコルの場合は [TLS1] を選択し、SSL3 プロトコルと TLS1 SSL プロトコルの両方を使用する場合は [All] を選択します。

ステップ 5　ピア証明書の検証を有効にするには、[Enable Certificate Verification] チェックボックスを選択します。証明書の検証を有効にすると、自己署名証明書を使用する WAAS デバイスは、相互にピア接続を確立することができなくなり、結果として、SSL トラフィックを加速できなくなります。

ステップ 6　[Disable revocation check for this service] チェックボックスを選択して、OCSP 証明書失効チェックを無効にします。

ステップ 7　[Cipher List] ペインで、WAE デバイス ピア間の SSL アクセラレーションに使用される暗号スイートのリストを選択するか、[Inherited] を選択して SSL グローバル設定に設定されている暗号リストを使用します。詳細については、「暗号リストの操作」（P.12-18）を参照してください。

ステップ 8　[Submit] をクリックします。

SSL アクセラレーション サービスの使用

WAAS システム上で SSL アクセラレーションを有効にし、その設定を完了したら、SSL パス上で加速されるサービスを少なくとも 1 つ定義する必要があります。SSL アクセラレーション サービスを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

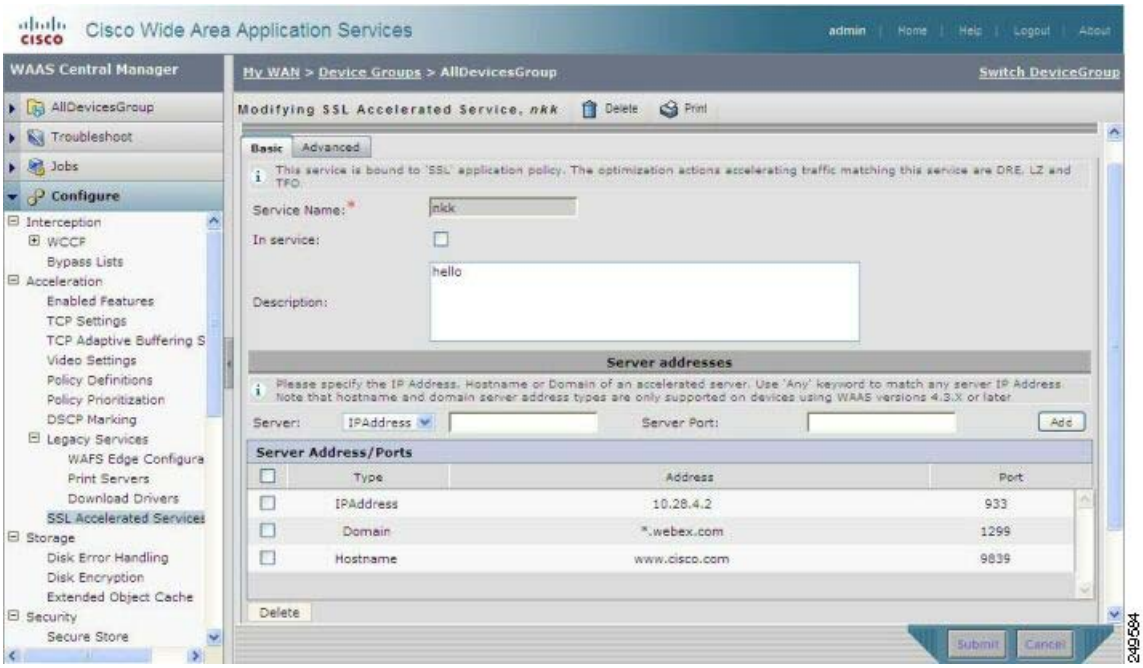
ステップ 2　アクセラレーション サービスを定義するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [SSL Accelerated Services] を選択します。

ステップ 4　アクセラレーション サービスを削除するには、そのサービスを選択し、[Delete] をクリックします。

ステップ 5　[Create] をクリックして、アクセラレーション サービスを新しく定義します。最大 128 のアクセラレーション サービスが可能です。[Basic SSL Accelerated Services Configuration] ウィンドウが表示されます（図 12-18 を参照）。

図 12-18　SSL アクセラレーション サービスの設定：基本



ステップ 6　サービスの名前を [Service Name] フィールドに入力します。

ステップ 7　このアクセラレーション サービスを有効にするには、[In service] チェックボックスを選択します。

ステップ 8　（任意）サービスの説明を [Description] フィールドに入力します。

ステップ 9　[Server] ドロップダウン リストから、[IP Address, Hostname]、または [Domain] を SSL サービスのエンドポイント タイプとして選択します。加速化されるサーバのサーバ IP アドレス、ホスト名、またはドメインを入力します。キーワード **Any** を使用して、任意のサーバ IP アドレスを指定します。最大 32 個の IP アドレス、32 個のホスト名、および 32 個のドメインが指定できます。

（注）　ホスト名とドメイン サーバ アドレスのタイプは、WAAS ソフトウェアのバージョン 4.2.x 以上を使用している場合にだけサポートされます。サーバ IP アドレス キーワードの **Any** がサポートされるのは、WAAS ソフトウェアのバージョン 4.2.x 以上を使用している場合だけです。

ステップ 10　アクセラレーションが適用されるサービスと関連付けられるポートを入力します。[Add] をクリックして、各アドレスを追加します。サーバのホスト名を指定した場合、そのホスト名は Central Manager によって IP アドレスに解決されてから、[Server IP/Ports] テーブルに追加されます。

ステップ 11　リストから IP アドレスを削除するには、[Delete] をクリックします。

ステップ 12　証明書とキー ペアの方法を選択します（図 12-19 を参照）。

図 12-19　　サービス証明書と秘密キーの設定

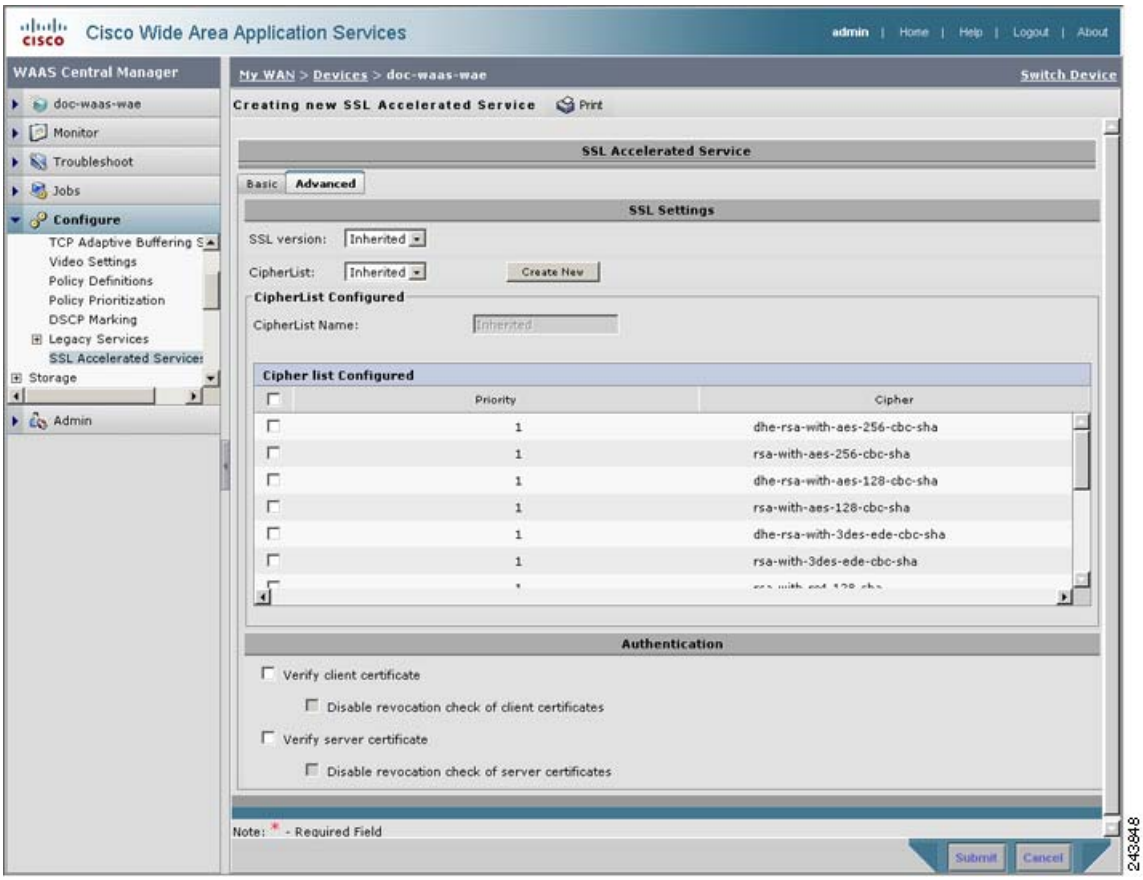
- WAAS デバイスで SSL に自己署名証明書 / キー ペアを使用するには、[Generate Self-signed Certificate Key] をクリックします。
- 既存の証明書 / キー ペアをアップロードまたは張り付けるには、[Import Existing Certificate Key] をクリックします。
- 現在の証明書 / キー ペアをエクスポートするには、[Export Certificate Key] をクリックします。
- 既存の証明書 / キー ペアを更新または置き換えるには、[Generate Certificate Signing Request] をクリックします。Certificate Signing Request（CSR; 証明書署名要求）は、新しい証明書を生成するために認証局で使用されます。

  インポートまたはエクスポートするファイルは、PKCS12 形式と PEM 形式のいずれかである必要があります。

サービス証明書と秘密キーの設定手順については、「サービス証明書と秘密キーの設定」（P.12-16）を参照してください。

ステップ 13　[Advanced Settings] タブをクリックして、サービスの SSL パラメータを設定します。[Advanced SSL Accelerated Services Configuration] ウィンドウが表示されます（図 12-20 を参照）。

図 12-20　SSL アクセラレーション サービスの設定：詳細



ステップ 14　（任意）[SSL version] フィールドで、使用する SSL プロトコルの種類を選択するか、[Inherited] を選択してグローバル SSL 設定に設定されている SSL プロトコルを使用します。SSL バージョン 3 プロトコルの場合は [SSL3] を選択し、Transport Layer Security バージョン 1 プロトコルの場合は [TLS1] を選択し、SSL3 プロトコルと TLS1 SSL プロトコルの両方を使用する場合は [All] を選択します。

ステップ 15　（任意）[Cipher List] フィールドで、WAE デバイス ピア間の SSL アクセラレーションに使用される暗号スイートのリストを選択するか、[Inherited] を選択して SSL グローバル設定に設定されている暗号リストを使用します。詳細については、「暗号リストの操作」（P.12-18）を参照してください。

ステップ 16　（任意）証明書失効の Online Certificate Status Protocol（OCSP）パラメータを設定します。

a.　クライアント証明書チェックの検証を有効にするには、[Verify client certificate] チェックボックスを選択します。

b.　[Disable revocation check for this service] チェックボックスを選択して、OCSP クライアント証明書失効チェックを無効にします。

c.　サーバ証明書チェックの検証を有効にするには、[Verify server certificate] チェックボックスを選択します。

d.　[Disable revocation check for this service] チェックボックスを選択して、OCSP サーバ証明書失効チェックを無効にします。

（注）　サーバとクライアントのデバイスが自己署名証明書を使用する場合、証明書の検証が有効になっていると、WAAS デバイスで SSL トラフィックを加速できなくなります。

ステップ 17　SSL アクセラレーション サービスの設定が完了したら、[Submit] をクリックします。

新しいトラフィック アプリケーション ポリシーの作成

表 12-3 に、新しいトラフィック アプリケーション ポリシーを作成するために完了する必要がある手順の概要を示します。

表 12-3　新しいアプリケーション ポリシーを作成するためのチェックリスト

作業	追加情報と手順
1. アプリケーション ポリシーを作成するための準備をする。	WAAS デバイスに新しいアプリケーション ポリシーを作成する前に完了する必要がある作業を行います。詳細については、「アプリケーション ポリシーを作成するための準備」（P.12-29）を参照してください。
2. アプリケーション定義を作成する。	アプリケーション名や WAAS Central Manager がこのアプリケーション用の統計情報を収集するかという、最適化するアプリケーションに関する一般情報を識別します。またこの手順では、デバイスまたはデバイス グループにアプリケーション定義を割り当てることができます。詳細については、「アプリケーション定義の作成」（P.12-30）を参照してください。
3. アプリケーション ポリシーを作成する。	WAAS デバイスまたはデバイス グループが特定のアプリケーション トラフィックに対して実行する処理の種類を決定します。この手順では、次の処理を実行する必要があります。 • WAAS デバイスが特定の種類のトラフィックを識別できるアプリケーション分類子を作成します。たとえば、特定の IP アドレスへ進むすべてのトラフィックと一致する条件を作成できます。 • WAAS デバイスまたはデバイス グループが定義されたトラフィックに対して実行する処理の種類を指定します。たとえば、WAAS が、特定のアプリケーション用のすべてのトラフィックに TFO および LZ 圧縮を適用するように指定できます。 詳細については、「アプリケーション ポリシーの作成」（P.12-31）を参照してください。

アプリケーション ポリシーを作成するための準備

新しいアプリケーション ポリシーを作成する前に、次の準備作業を完了します。

- WAAS システム上のアプリケーション ポリシーのリストを参照し、これらのポリシーが定義する種類のトラフィックをまだ網羅していないことを確認します。WAAS システムに組み込まれている定義済みポリシーのリストを表示するには、付録 A「定義済みのアプリケーション ポリシー」を参照してください。
- 新しいアプリケーション トラフィック用の一致条件を識別します。たとえば、アプリケーションが特定の送信先または送信元ポートを使用する場合は、そのポート番号を使用して一致条件を作成できます。また、送信元または送信先 IP アドレスを一致条件に使用することもできます。
- 新しいアプリケーション ポリシーが必要なデバイスまたはデバイス グループを識別します。複数の WAAS デバイス全体でポリシーが一貫するように、デバイス グループに関するアプリケーション ポリシーを作成することを推奨します。

アプリケーション定義の作成

アプリケーション ポリシーを作成する最初の手順では、アプリケーション名や WAAS Central Manager がアプリケーション用の統計情報を収集するかというアプリケーションに関する一般情報を識別するアプリケーション定義を設定します。アプリケーション定義を作成したら、デバイスまたはデバイス グループに割り当てます。WAAS システムには、最大 255 のアプリケーション定義を作成できます。

新しいアプリケーション定義を作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Acceleration] > [Applications] を選択します。

[Applications] ウィンドウが表示され、WAAS システム上のすべてのアプリケーションのリストが表示されます。このウィンドウから、次の作業を実行できます。

- 定義を変更または削除するアプリケーションの横にある [Edit] アイコンをクリックします。
- WAAS システムがアプリケーション用の統計情報を収集するか決定します。アプリケーション用の統計情報が収集される場合、[Monitor Enabled] 列に [Yes] が表示されます。
- 次の手順の説明に従って、新しいアプリケーション グループを作成します。

タスクバーの [Create New Application] アイコンをクリックします。[Creating Application] ウィンドウが表示されます。

ステップ 2　このアプリケーションの名前を入力します。

名前にはスペースや特殊文字は使用できません。

ステップ 3　[Enable Statistics] チェックボックスを選択して、WAAS Central Manager がこのアプリケーションに関するデータを収集できるようにします。このアプリケーション用のデータ収集を無効にするには、このボックスの選択を解除します。

WAAS Central Manager GUI は、最大 20 のアプリケーション用の統計情報を表示でき、21 番めのアプリケーション用の統計情報を有効にしようとすると、エラー メッセージが表示されます。ただし、WAAS CLI を使用すると、特定の WAAS デバイスにポリシーが存在するすべてのアプリケーション用の統計情報を表示できます。詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

アプリケーション用の統計情報を収集しているときに統計情報の収集を無効にすることにし、あとで統計情報の収集を再有効化する場合、履歴データは保持されますが、統計情報の収集が無効になっていた間のデータは欠落します。ただし、統計情報を収集しているアプリケーションを削除し、その後にアプリケーションを再作成する場合は、アプリケーション用の履歴データが失われます。アプリケーションを再作成したあとのデータだけが表示されます。

（注）　WAAS Central Manager は、アプリケーション ポリシー全体の作成が完了するまで、このアプリケーション用のデータ収集を開始しません。

ステップ 4　（任意）[Comments] フィールドに、説明を入力します。

入力した説明は、[Applications] ウィンドウに表示されます。

ステップ 5　[Submit] をクリックします。

アプリケーション定義が保存され、ナビゲーション ペインにデバイスまたはデバイス グループにアプリケーションを割り当てることができるオプションが表示されます。

ステップ 6　ナビゲーション ペインで、次のいずれかのオプションをクリックします。

- [Assign Device Groups] : 1 つまたは複数のデバイス グループにアプリケーションを割り当てます。
- [Assign Devices] : 1 つまたは複数の WAAS デバイスにアプリケーションを割り当てます。

選択したオプションによって、[Device Groups Assignments] ウィンドウまたは [WAE Assignments] ウィンドウが表示されます。

いずれのビューでも、割り当てウィンドウでは、リスト内の項目のビューをフィルタできます。フィルタにより、設定した基準に一致するリスト内の項目を見つけることができます。

ステップ 7　このアプリケーションに割り当てるデバイスまたはデバイス グループを選択します。デバイスを選択するには、次のいずれかの手順を使用します。

- タスクバーの をクリックして、使用できるすべての WAAS デバイスまたはデバイス グループを割り当てます。
- 割り当てる各 WAAS デバイスまたはデバイス グループの横にある をクリックします。選択すると、アイコンは に変化します。デバイスまたはデバイス グループの割り当てを解除するには、もう一度アイコンをクリックします。

ステップ 8　[Submit] をクリックします。

選択したデバイスの横にあるアイコンが に変化し、アプリケーションが正常にデバイスに割り当てられたことを示します。

アプリケーション ポリシーの作成

アプリケーション定義を作成したら、指定したトラフィックに WAAS デバイスが実行する処理を決定するアプリケーション ポリシーを作成する必要があります。たとえば、WAAS デバイスが特定のポートまたは特定の IP アドレスに到達するすべてのアプリケーション トラフィックに TCP 最適化および圧縮を適用するアプリケーション ポリシーを作成できます。WAAS システムには、最大 512 のアプリケーション ポリシーを作成できます。

トラフィック一致規則は、アプリケーション分類子に含まれます。一致条件と呼ぶこれらの規則は、TCP ヘッダーのレイヤ 2 およびレイヤ 4 の情報を使用してトラフィックを識別します。

アプリケーション ポリシーを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

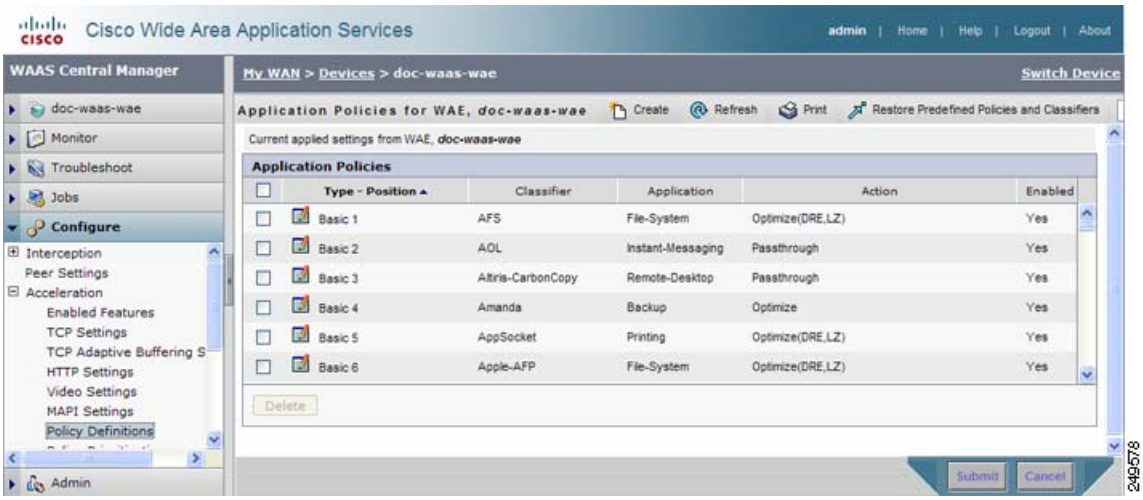
ステップ 2　アプリケーション ポリシーを作成するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウまたは [Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Policy Definitions] を選択します。

[Application Policies] ウィンドウが表示されます（図 12-21 を参照）。

図 12-21　[Application Policies] ウィンドウ



このウィンドウは、選択したデバイスまたはデバイス グループに存在するすべてのアプリケーション ポリシーに関する情報を表示します。ポリシーの種類（Basic、WAFS transport、Port Mapper、または Other）とその種類の中でのポリシーの位置を表示します。位置は、WAAS がアプリケーション トラフィックを処理する方法を決定するときにポリシーを参照する順序を決定します。ポリシーの位置を変更するには、「アプリケーション ポリシーの位置の変更」（P.12-40）を参照してください。また、このウィンドウは、分類子、アプリケーション定義、および各ポリシーに割り当てられている処理を表示します。

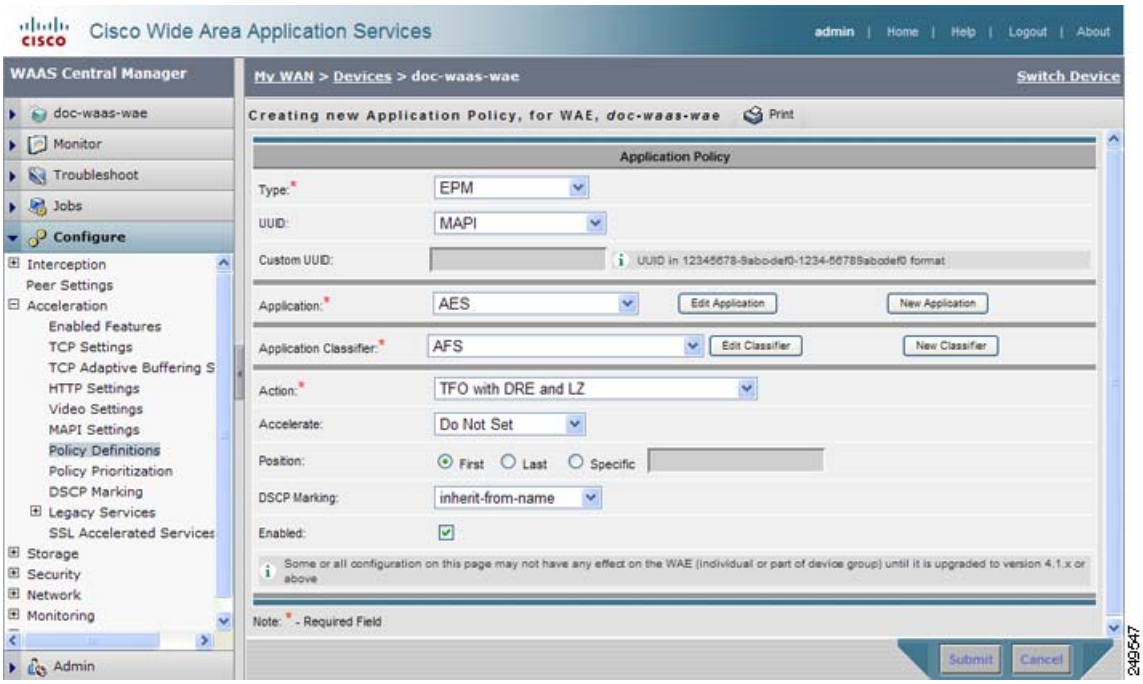
[Application Policies] ウィンドウから、次の作業を実行できます。

- 削除する 1 つまたは複数のアプリケーション ポリシーの横にチェックを付けてから、[Delete] ボタンをクリックして、チェックのついたポリシーを削除します。
- そのポリシーを変更または削除するアプリケーション ポリシーの横にある [Edit] アイコンをクリックします。
- 定義済みポリシーと分類子を復元します。詳細については、「アプリケーション ポリシーと分類子の復元」（P.12-38）を参照してください。
- 次の手順の説明に従って、アプリケーション ポリシーを作成します。

ステップ 4　タスクバーの [Create New Policy] アイコンをクリックして、新しいアプリケーション ポリシーを作成します。

[Creating New Application Policy] ウィンドウが表示されます（図 12-22 を参照）。

図 12-22　　アプリケーション ポリシーの作成



ステップ 5　[Type] ドロップダウン リストから、アプリケーション ポリシーの種類を選択します。

表 12-4 で、アプリケーション ポリシーの種類について説明します。

表 12-4　　アプリケーション ポリシーの種類

オプション	説明
[Basic]	標準的な種類のアプリケーション ポリシー。他の種類に該当しない場合、このオプションを選択します。
[WAFS Transport]	Wide Area File Services（WAFS; 広域ファイル サービス）を有効にすると、ブランチ WAE とデータセンター WAE の間を流れるすべての CIFS トラフィックが最適化されます。ブランチ WAE とデータセンター WAE の間を流れる CIFS トラフィックについて（パススルーのような）別の処理を指定するには、[WAFS Transport] オプションを選択します。 ファイル サービスを有効にする方法については、第 11 章「WAFS の設定」を参照してください。
[EPM]	EPM に基づくアプリケーション用のポリシーの種類。EndPoint Mapper（EPM; エンドポイント マッパー）は、特定のアプリケーションにダイナミックにサーバ ポートを割り当てるサービスです。常に同じポートを使用するほとんどのアプリケーションと異なり、EPM サービスに依存するアプリケーションは、要求ごとに異なるポートを割り当てることができます。 EPM アプリケーションは固定ポートを使用しないため、アプリケーション トラフィックを WAAS システムに識別するために、アプリケーションの UUID を指定する必要があります。 [EPM] オプションを選択すると、設定済みの EPM アプリケーションを選択したり、カスタム アプリケーション用の UUID を入力できるように、UUID フィールドが有効になります。

ステップ 6　ポリシーの種類に EPM を選択した場合は、[UUID] ドロップダウン リストから次のいずれかの EPM アプリケーションを選択します。

- [MAPI]：MAPI アプリケーションに関連付けられた定義済みの UUID（a4f1db00-ca47-1067-b31f-00dd010662da）を使用します。
- [MS-SQL-RPC]：SQL Session Manager アプリケーションに関連付けられた定義済みの UUID（3f99b900-4d87-101b-99b7-aa0004007f07）を使用します。
- [MS-AD-Replication]：Active Directory アプリケーションに関連付けられた定義済みの UUID（e3514235-4b06-11d1-ab04-00c04fc2dcd2）を使用します。
- [MS-FRS]：ファイル複製サービスに関連付けられた定義済みの UUID（f5cc59b4-4264-101a-8c59-08002b2f8426）を使用します。
- [Custom]：[Custom] フィールドに、カスタム EPM アプリケーション用の UUID を入力できます。

ステップ 7　次のいずれかを実行して、このポリシーに関連付けるアプリケーションを指定します。

- [Application] ドロップダウン リストから、「アプリケーション定義の作成」（P.12-30）で作成したような既存のアプリケーションを選択します。このリストは、WAAS システム上のすべての事前定義されたアプリケーションと新しいアプリケーションを表示します。

  既存のアプリケーションを変更するには、ドロップダウン リストからアプリケーションを選択し、[Edit Application] をクリックします。次に、アプリケーションの名前を変更する、説明を追加または削除する、およびアプリケーション用の統計情報の収集を有効または無効にすることができます。必要な変更を行ったら、[Submit] をクリックして変更を保存し、[Application Policies] ウィンドウへ戻ります。

- アプリケーションを作成するには、[New Application] をクリックします。アプリケーション名の指定、統計情報の収集の有効化、および DSCP マーキング値の指定が可能です。DSCP マーキングに関して、グローバルなデフォルト値の使用を選択するか（「デフォルトの DSCP マーキング値の定義」（P.12-39）を参照）、またはいずれかの他の定義済みの値を選択できます。サポート対象の DSCP マーキング値の説明については、表 11-4（P.11-16）を参照してください。表 11-4 に示されている値に加えて、copy を選択して、着信パケットからの DSCP 値をコピーし、発信パケットで使用することもできます。アプリケーション詳細を指定したら、[Submit] をクリックして新しいアプリケーションを保存し、[Application Policies] ウィンドウへ戻ります。新しいアプリケーションは、自動的にこのデバイスまたはデバイス グループに割り当てられます。

ステップ 8　[Application Classifier] ドロップダウン リストから分類子を選択して、このポリシー用の既存の分類子を選択します。

既存の分類子を変更するには、ドロップダウン リストから分類子を選択し、[Edit Classifier] をクリックします。次に、分類子の名前を変更する、説明を追加または削除する、新しい一致条件を作成する、または既存の一致条件を編集することができます。必要な変更を行ったら、[Submit] をクリックして変更を保存し、[Application Policies] ウィンドウへ戻ります。

ステップ 9　このポリシー用の新しい分類子を作成するには、[New Classifier] をクリックします。

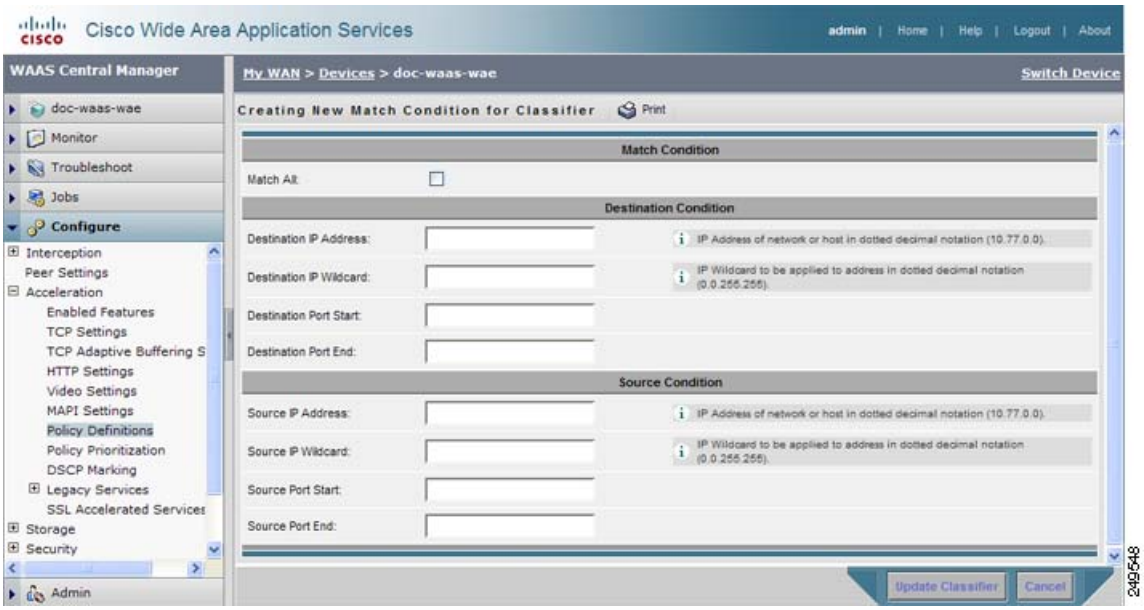
新しい分類子を作成できるように、[Creating New Application Classifier] ウィンドウが表示されます。次の手順を実行して、新しい分類子を作成します。

a.　このアプリケーション分類子の名前を入力します。名前にはスペースや特殊文字は使用できません。

b.　（任意）図 12-21（P.12-32）に示す [Application Policies] ウィンドウに表示する説明を入力します。

c.　[Configure Match Conditions] セクションで、[Create New Match Condition] アイコンをクリックします（このページから移動するかどうかを確認するダイアログボックスが表示された場合は、[OK] をクリックします）。[Creating New Match Condition] ウィンドウが表示されます（図 12-23 を参照）。

図 12-23　新しい一致条件の作成



d. すべてのトラフィックと一致する条件を作成するには、[Match All] チェックボックスを選択します。[Match All] チェックボックスを選択すると、ウィンドウの他のすべてのフィールドが自動的に無効になります。

e. 送信先または送信元の条件フィールドに値を入力して、特定の種類のトラフィック用の条件を作成します。

たとえば、IP アドレス 10.10.10.2 へ進むすべてのトラフィックと一致するようにするには、[Destination IP Address] フィールドにその IP アドレスを入力します。

（注）　IP アドレス範囲を指定するには、送信先または送信元の [IP Wildcard] フィールドにワイルドカード サブネット マスクを入力します。

f. [Update Classifier] をクリックします。[Creating New Application Classifier] ウィンドウへ戻ります。このウィンドウの一番下に、新しい一致条件が表示されます。

g. [Submit] をクリックします。[Creating New Application Policy] ウィンドウへ戻ります。

ステップ 10　[Action] ドロップダウン リストから、定義されたトラフィックに WAAS デバイスが実行する必要がある処理を選択します。表 12-5 で、各処理について説明します。

表 12-5　処理の説明

処理	説明
Passthrough	TFO、DRE、または圧縮を使用して、WAAS デバイスが、このポリシーに定義されたアプリケーション トラフィックを最適化することを防止します。このポリシーに一致するトラフィックでも、[Accelerate] ドロップダウン リストからアクセラレータを選択すると、加速化することができます。
TFO Only	一致するトラフィックにさまざまな Transport Flow Optimization（TFO; 転送フローの最適化）方式を適用します。TFO 方式には、BIC-TCP、ウィンドウ サイズの最大化と縮尺、および選択的受信確認があります。TFO 機能の詳細な説明については、「TFO の最適化」（P.1-4）を参照してください。
TFO with Data Redundancy Elimination	一致するトラフィックに TFO と Data Redundancy Elimination（DRE; データ冗長性除去）の両方を適用します。DRE は、WAN 経由で短縮されたデータ ストリームを送信する前に、冗長的な情報を削除します。DRE は、大型データ ストリーム（数十から数百バイト以上）で動作します。
TFO with LZ Compression	一致するトラフィックに TFO と LZ 圧縮アルゴリズムの両方を適用します。LZ 圧縮は DRE と同様に動作しますが、異なる圧縮アルゴリズムを使用してより小型のデータ ストリームを圧縮し、限られた圧縮履歴を維持します。
DRE および LZ での TFO	一致するトラフィックに TFO、DRE、および LZ 圧縮を適用します。

ステップ 11　[Accelerate] ドロップダウン リストから、定義されたトラフィックに WAAS デバイスが実行する必要がある次の追加アクセラレーション処理のいずれか 1 つを選択します。

- [Do Not Set]：追加アクセラレーションを行いません。
- [MS Port Mapper]：Microsoft Endpoint Port Mapper（EPM）を使用して加速化します。
- [CIFS]：CIFS Accelerator を使用して加速化します。
- [HTTP]：HTTP Accelerator を使用して加速化します。
- [NFS]：NFS Accelerator を使用して加速化します。
- [MAPI]：MAPI Accelerator を使用して加速化します。
- [VIDEO]：VIDEO Accelerator を使用して加速化します。

ステップ 12　該当する [Position] オプション ボタンをクリックして、次の中からこのアプリケーション ポリシーの位置を選択します。

- [First]：このポリシーを位置リストの先頭に配置します。WAAS デバイスは、トラフィックを分類するとき、リストの第 2 位ポリシーへ移動する前に、このポリシーを最初に使用します。すでに先頭位置にポリシーがある場合、そのポリシーはリストの第 2 位に下がります。
- [Last]：このポリシーを位置リストの末尾に配置します。WAAS デバイスは、トラフィックを分類するとき、このポリシーを最後に使用します。すでに末尾位置にポリシーがある場合、そのポリシーはリストの最後から第 2 位になります。

  デバイスがリスト内のどのポリシーとも一致しない場合、WAAS デバイスはトラフィックを最適化せずに通過させます。
- [Specific]：このポリシー用の特定の位置を入力できます。指定した位置にすでにポリシーがある場合、そのポリシーはリスト内で 1 つ下がります。

ステップ 13　（任意）[DSCP Marking] ドロップダウン リストから値を選択します。サポートされている値の説明については、表 11-4（P.11-16）を参照してください。表 11-4 に示されている値に加えて、copy を選択して、着信パケットからの DSCP 値をコピーし、発信パケットで使用することもできます。ドロップダウン リストから [inherit-from-name] を選択した場合、アプリケーション レベルまたはグローバル レベルで定義された DSCP 値が使用されます。

DSCP は、ネットワーク トラフィックに異なるレベルのサービスを割り当てることができる IP パケットのフィールドです。ネットワーク上の各パケットに DSCP コードを付け、対応するサービスのレベルを関連付けて、サービスのレベルを割り当てます。DSCP は、IP precedence フィールドと Type of Service（ToS; タイプ オブ サービス）フィールドの組み合せです。詳細については、RFC 2474 を参照してください。

DSCP マーキングは、パススルー トラフィックに適用されません。

アプリケーション レベルで設定された DSCP 値は、アプリケーションに関するすべての分類子に適用されます。ポリシーで設定された DSCP 値は、アプリケーション レベルまたはグローバル レベルで設定された DSCP 値を上書きします。

ステップ 14　[Enabled] チェックボックスを選択して、このポリシーをアクティブにします。このポリシーを無効にするには、このボックスの選択を解除します。

ステップ 15　[Submit] をクリックします。

[Application Policies] ウィンドウに新しいポリシーが表示されます（図 12-21（P.12-32）を参照）。

アプリケーション アクセラレーションの管理

ここでは、次の内容について説明します。

アプリケーションのリストの表示

WAE デバイスまたはデバイス グループに存在するアプリケーションのリストを表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　アプリケーションを表示するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Policy Definitions] を選択します。[Application Policies] ウィンドウが表示されます。

ステップ 4　[Application] 列見出しをクリックして、特定のアプリケーションを見つけやすくするためにアプリケーション名で列を並べ替えます。

ポリシー レポートの表示

各 WAE デバイスにまたはデバイス グループに存在するポリシーのレポートを表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Acceleration] > [Policies] を選択します。

ポリシー レポートが表示されます。ポリシー レポートは、各デバイスまたはデバイス グループとデバイスまたはデバイス グループ上のアクティブなポリシーの数を表示します。

ステップ 2　デバイスまたはグループの横にある [Edit] アイコンをクリックして、そこに定義されているアプリケーション ポリシーを表示します。

分類子レポートの表示

各 WAE デバイスまたはデバイス グループに存在する分類子のレポートを表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Acceleration] > [Classifiers] を選択します。

分類子レポートが表示されます。分類子レポートは、定義されている各分類子とそれが設定されているデバイスの数を表示します。

ステップ 2　分類子の横にある [View] アイコンをクリックして、分類子が設定されているデバイスおよびデバイス グループのレポートを表示します。

ステップ 3　デバイスまたはグループの横にある [Edit] アイコンをクリックして、そこに定義されているアプリケーション ポリシーを表示します。

アプリケーション ポリシーと分類子の復元

WAAS システムでは、WAAS システムに組み込まれていた定義済みポリシーと分類子を復元できます。定義済みポリシーのリストについては、付録 A「定義済みのアプリケーション ポリシー」を参照してください。

定義済みポリシーに、WAAS デバイスがアプリケーション トラフィックを処理する方法に対してマイナスに影響するような変更を加えた場合、定義済みポリシー設定を復元することによって、その変更を上書きできます。

定義済みポリシーと分類子を復元するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　ポリシーを復元するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Policy Definitions] を選択します。

[Application Policies] ウィンドウが表示されます。

ステップ 4　[Restore Predefined Policies and Classifiers] タスクバー アイコンをクリックして、WAAS ソフトウェアに組み込まれていた 150 個を超えるポリシーと分類子を復元します。システム上で作成した新しいポリシーはすべて削除されます。定義済みポリシーが変更されていた場合、これらの変更は失われ、元の設定が復元されます。

アプリケーションのモニタリング

アプリケーション ポリシーを作成したら、WAAS システムが期待通りにアプリケーション トラフィックを処理していることを確認するために、関連付けられたアプリケーションをモニタする必要があります。アプリケーションをモニタするには、「アプリケーション定義の作成」（P.12-30）の説明に従って、そのアプリケーションの統計情報収集が有効になっている必要があります。

トラフィック最適化レポートを使用して、特定のアプリケーションをモニタできます。詳細については、「最適化概要レポート」（P.16-39）を参照してください。

デフォルトの DSCP マーキング値の定義

アプリケーション定義およびアプリケーション ポリシーで定義されたポリシーに従って、WAAS ソフトウェアでは処理するパケット上に DSCP 値を設定できます。

DSCP 値は、ネットワーク トラフィックに異なるレベルのサービスを割り当てることができる IP パケットのフィールドです。ネットワーク上の各パケットに DSCP コードを付け、対応するサービスのレベルを関連付けて、サービスのレベルを割り当てます。DSCP マーキングにより、接続用のパケットが WAAS に対して外部的に処理される方法が決定されます。DSCP は、IP precedence フィールドと Type of Service（ToS; タイプ オブ サービス）フィールドの組み合せです。詳細については、RFC 2474 を参照してください。DSCP 値は、事前に定義されているため、変更できません。

この属性は、次のレベルで定義できます。

- グローバル：DSCP 値にグローバルなデフォルトを設定できます。より低いレベルの値が定義されていない場合、この値がトラフィックに適用されます。
- アプリケーション：アプリケーション定義内の DSCP 値を、グローバルなアプリケーション定義レベルではなく、デバイスまたはデバイス グループ レベルで定義できます。この値は、特定のデバイスまたはデバイス グループ上のアプリケーションに関連付けられたすべてのトラフィックに適用され、グローバルなデフォルトを上書きします。
- ポリシー：アプリケーション ポリシー内の DSCP 値を定義できます。この値は、ポリシー内に定義された分類子と一致するトラフィックにだけ適用され、アプリケーションまたはグローバルの DSCP 値を上書きします。

ここでは、次の内容について説明します。

- 「デフォルトの DSCP マーキング値の定義」（P.12-40）

デフォルトの DSCP マーキング値の定義

グローバルなデフォルトの DSCP マーキング値を定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　デフォルトの DSCP マーキング値を定義するデバイスまたはグループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [DSCP Marking] を選択します。[Global DSCP Settings] ウィンドウが表示されます。

ステップ 4　[Global Default DSCP Marking] ドロップダウン リストから値を選択し、サポートされている値の説明について表 11-4（P.11-16）を参照します。表 11-4 に示された値に加えて、デフォルト設定は copy で、着信パケットからの DSCP 値をコピーし、発信パケットで使用します。

ステップ 5　[Submit] をクリックして、設定を保存します。

アプリケーション ポリシーの位置の変更

各アプリケーション ポリシーには、WAAS デバイスがトラフィックを分類するときにポリシーを参照する順序を決定する位置が割り当てられています。たとえば、WAAS デバイスは、トラフィックを代行受信するとき、トラフィックとアプリケーションを対応付けるために、リストの最初のポリシーを参照します。最初のポリシーに一致するものがない場合、WAAS デバイスはリスト内の次のポリシーへ移動します。

新しいポリシーに位置を割り当てる方法については、「アプリケーション ポリシーの作成」（P.12-31）を参照してください。

トラフィックを最適化せずにパススルーするポリシーの位置に注意する必要があります。これらのポリシーをリストの一番上に配置すると、リストの下の方にある最適化ポリシーが無効になるからです。たとえば、IP アドレス 10.10.10.2 へ進むトラフィックと一致する 2 つのアプリケーション ポリシーがあり、最初のポリシーがこのトラフィックを最適化し、最初のポリシーより高い位置にある別のポリシーがこのトラフィックをパススルーさせる場合、10.10.10.2 へ進むすべてのトラフィックが最適化されずに WAAS システムを通過します。そのため、ポリシーの一致条件が重ならないことを確認し、作成したアプリケーションをモニタして、WAAS がトラフィックを期待通りに処理していることを確認する必要があります。アプリケーションをモニタする方法については、第 16 章「WAAS ネットワークのモニタリングおよびトラブルシューティング」を参照してください。

アプリケーション ポリシーの位置を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　変更するアプリケーション ポリシーを含むデバイスまたはグループの横にある [Edit] アイコンをクリックします。

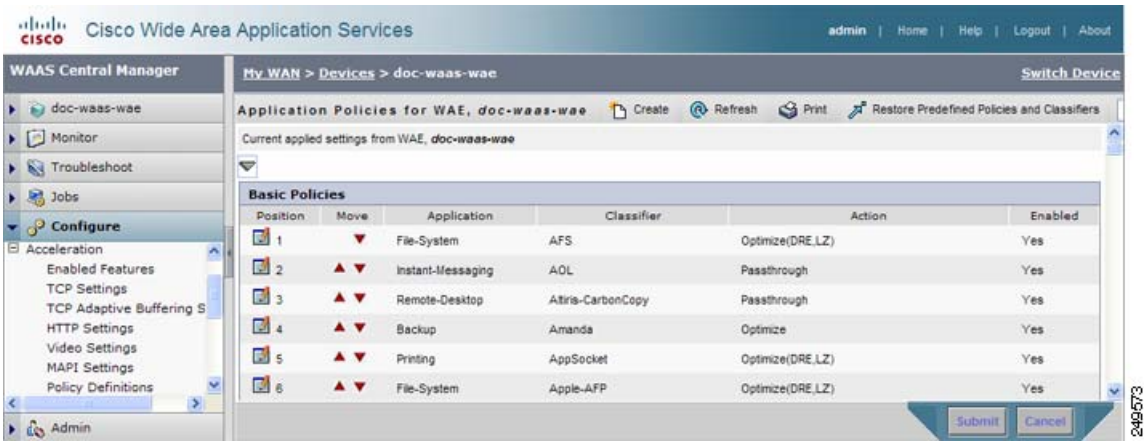
ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Policy Prioritization] を選択します。

ステップ 4　[Application Policies] ウィンドウが表示されます。このウィンドウでは、ポリシーが、Basic、Other、Port Mapper、および WAFS のカテゴリに分類されています。

ステップ 5　適切なカテゴリの横にある矢印をクリックして、そのカテゴリのアプリケーションのリストを表示します（図 12-24 を参照）。

ほとんどの場合、位置を変更するアプリケーションは、Basic Policies カテゴリにあります。このカテゴリには、WAAS システムに組み込まれているほとんどの事前定義されたアプリケーションが含まれるためです。これらの定義済みポリシーのリストについては、付録 A「定義済みのアプリケーション ポリシー」を参照してください。

図 12-24　　アプリケーション ポリシーの位置の変更



ステップ 6　ポリシー カテゴリの横にある矢印をクリックして、そのカテゴリのアプリケーションのリストを表示します。

ステップ 7　ポリシーの横にある上下の矢印（ ▲ ▼ ）を使用して、リストでのそのポリシーの位置を上下に移動します。

ステップ 8　ポリシーが必要でないと判断した場合は、次の手順に従ってポリシーを削除します。

a. 削除するポリシーの横にある [Edit] アイコンをクリックします。

[Modifying Application Policy] ウィンドウが表示されます。

b. タスクバーの [Delete] アイコンをクリックします。

アクセラレーション TCP 設定の変更

WAAS システムは、WAE デバイスのハードウェア プラットフォームに基づいて、自動的に加速 TCP 設定を構成するため、ほとんどの場合、アクセラレーション TCP 設定を変更する必要はありません。WAAS は、次の状況で自動的に設定を構成します。

- ネットワークに最初に WAE デバイスを設置したとき。
- デバイスで **restore factory-default** コマンドを入力したとき。このコマンドの詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

WAAS システムでは、接続ごとに、クライアントまたはサーバのアドバタイズされた Maximum Segment Size（MSS; 最大セグメント サイズ）と一致するように、MSS が自動調整されます。WAAS システムでは、クライアントまたはサーバによってアドバタイズされた MSS 値と 1432 のいずれか小さい方が使用されます。

ネットワークに高い BDP リンクがある場合、WAE デバイス用に自動的に設定されるデフォルトのバッファ設定を調整する必要がある場合があります。詳細については、「高い BDP リンク用の TCP バッファの計算」（P.12-43）を参照してください。

WAE デバイスで、デフォルトの TCP 適応バッファリング設定を調整する場合、「TCP 適応バッファリング設定の変更」（P.12-44）を参照してください。

アクセラレーション TCP 設定を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　アクセラレーション TCP 設定を変更するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [TCP Settings] を選択します。[Acceleration TCP Settings] ウィンドウが表示されます。

ステップ 4　[Send TCP Keepalive] チェックボックスを選択した状態のままにします。

[Send TCP Keepalive] チェックボックスを選択すると、この WAE デバイスまたはグループは、TCP キープアライブ交換から応答を受信しない場合に、そのピア デバイスとの TCP 接続を切断できます。この場合、2 台のピア WAE デバイスは、TCP 接続経由で TCP キープアライブを交換し、特定の期間にわたってキープアライブの応答を受信しない場合、TCP 接続を切断します。キープアライブ オプションを有効にすると、WAN ネットワークでの短い中断によって、ピア WAE デバイス間の TCP 接続が切断されます。

[Send TCP Keepalive] チェックボックスを選択しないと、TCP キープアライブは送信されず、明示的に切断しないかぎり、接続は維持されます。デフォルトで、この設定は有効になっています。

ステップ 5　必要に応じて、TCP アクセラレーション設定を変更します。これらの設定の説明については、表 12-6を参照してください。

高い BDP 回線用にこれらの設定を計算する方法については、「高い BDP リンク用の TCP バッファの計算」（P.12-43）を参照してください。

表 12-6　TCP 設定

TCP 設定	説明
Optimized Side	
Maximum Segment Size	この WAAS デバイスと最適化された接続に参加する他の WAAS デバイス間で許可された最大パケット サイズ。デフォルトは、1432 バイトです。
Send Buffer Size	この WAAS デバイスから、最適化された接続に参加する他の WAAS デバイスへ送信される TCP パケットに許可される TCP 送信バッファ サイズ（キロバイト）。デフォルトは、32 KB です。
Receive Buffer Size	最適化された接続に参加する他の WAAS デバイスからの着信 TCP パケットに許可される TCP 受信バッファ サイズ（キロバイト）。デフォルトは、32 KB です。
Original Side	
Maximum Segment Size	元のクライアントまたはサーバと、この WAAS デバイス間で許可される最大パケット サイズ。デフォルトは、1432 バイトです。
Send Buffer Size	この WAAS デバイスから元のクライアントまたはサーバへ送信される TCP パケットに許可される TCP 送信バッファ サイズ（キロバイト）。デフォルトは、32 KB です。
Receive Buffer Size	元のクライアントまたはサーバからの着信 TCP パケットに許可される TCP 受信バッファ サイズ（キロバイト）。デフォルトは、32 KB です。

ステップ 6　高い Bandwidth Delay Product（BDP; 帯域遅延積）リンク経由で WAE を配置している場合は、[Set High BDP recommended values] ボタンをクリックすると、送信バッファおよび受信バッファに推奨サイズを設定できます。高い BDP リンク用の TCP バッファを計算する方法の詳細については、「高い BDP リンク用の TCP バッファの計算」（P.12-43）を参照してください。

ステップ 7　[Submit] をクリックします。

CLI から TCP キープアライブを設定するには、**tfo tcp keepalive** グローバル コンフィギュレーション コマンドを使用します。

CLI から TCP アクセラレーション設定を構成するには、**tfo tcp optimized-mss**、**tfo tcp optimized-receive-buffer**、**tfo tcp optimized-send-buffer**、**tfo tcp original-mss**、**tfo tcp original-receive-buffer**、および **tfo tcp original-send-buffer** グローバル コンフィギュレーション コマンドを使用します。

TCP バッファ サイズを表示するには、**show tfo tcp** EXEC コマンドを使用します。

高い BDP リンク用の TCP バッファの計算

WAAS ソフトウェアは、帯域幅、遅延、およびパケット損失のような複数のリンク特性を含む、さまざまなネットワーク環境で展開できます。すべての WAAS デバイスは、次の値までの最大帯域遅延積（BDP）を持つネットワークに対応できるように設定されています。

- WAE-511/512：デフォルト BDP は 32 KB
- WAE-611/612：デフォルト BDP は 512 KB
- WAE-674：デフォルト BDP は 2,048 KB
- WAE-7326：デフォルト BDP は 2,048 KB
- WAE-7341：デフォルト BDP は 2,048 KB
- WAE-7371：デフォルト BDP は 2,048 KB
- WAVE-274：デフォルト BDP は 2,048 KB
- WAVE-474：デフォルト BDP は 2,048 KB
- WAVE-574：デフォルト BDP は 2,048 KB

ネットワークがより高い帯域幅を提供したり、高い遅延が含まれる場合は、次の計算式を使用して実際のリンク BDP を計算します。

BDP [キロバイト] = (リンク帯域幅 [キロバイト/秒] × ラウンドトリップ遅延 [秒])

WAE が最適化しているトラフィックに対するリンクが複数のリンク 1 ～ N である場合、最大 BDP は次のように計算する必要があります。

MaxBDP = Max (BDP(link 1),..,BDP(link N))

計算した MaxBDP が WAE モデルのデフォルト BDP より大きい場合は、計算した MaxBDP に対応できるようにアクセラレーション TCP 設定を変更する必要があります。

Max BDP のサイズが計算できたら、[Acceleration TCP Settings] ウィンドウで、最適化された接続のための [Send Buffer Size] と [Receive Buffer Size] に Max BDP の 2 倍以上の値を入力します。

（注）　これらの手動で設定されたバッファ サイズは、TCP 適応バッファリングが無効な場合にだけ適用されます。TCP 適応バッファリングは通常有効であるため、バッファ サイズは WAAS システムにより直接変更されます。TCP 適応バッファリングの詳細については、「TCP 適応バッファリング設定の変更」（P.12-44）を参照してください。

TCP 適応バッファリング設定の変更

WAAS システムは、ネットワーク帯域および各接続で発生する遅延に基づいて TCP 適応バッファリング設定を自動的に構成するため、ほとんどの場合、アクセラレーション TCP 適応バッファリング設定を変更する必要がありません。適応バッファリングにより、WAAS ソフトウェアは送受信されるバッファ サイズを直接変更して、パフォーマンスを向上させ、使用可能なネットワーク帯域をより効果的に利用できるようになります。

アクセラレーション TCP 適応バッファリング設定を変更するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　TCP 適応バッファリング設定を構成するデバイス名（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [TCP Adaptive Buffering Settings] を選択します。[TCP Adaptive Buffering Settings] ウィンドウが表示されます。

ステップ 4　TCP 適応バッファリングを有効化するには、[Enable] チェックボックスを選択します。デフォルトは有効です。

ステップ 5　[Send Buffer Size and Receive Buffer Size] フィールドに、送受信されるバッファの最大サイズ（キロバイト）を入力します。

ステップ 6　[Submit] をクリックします。

CLI から TCP 適応バッファリング設定を構成するには、**tfo tcp adaptive-buffer-sizing** グローバル コンフィギュレーション コマンドを使用します。

```
WAE(config)# tfo tcp adaptive-buffer-sizing receive-buffer-max 8192
```

CLI から TCP 適応バッファリング設定を無効にするには、**no tfo tcp adaptive-buffer-sizing enable** グローバル コンフィギュレーション コマンドを使用します。

デフォルトの設定済みの適応バッファリング サイズを表示するには、**show tfo tcp** EXEC コマンドを使用します。

CHAPTER 13

WAAS レガシー印刷サービスの設定および管理

この章では、WAE をブランチ オフィスのプリント サーバとして使用できる Wide Area Application Service（WAAS）レガシー印刷サービス機能を設定し、管理する方法について説明します。

他のプリンタ サービス オプションの詳細については、「WAAS 印刷サービス」（P.1-8）を参照してください。

（注） レガシー印刷サービスの機能は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー印刷サービスを有効にすると、デバイス上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー印刷サービスの何らかの設定値を設定しようとした場合に警告されます。レガシー印刷サービスをお使いの場合は、Windows プリント アクセラレータに移行してください。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

WAAS 印刷サービスについて

WAAS ソフトウェアには、ブランチ オフィスの WAE をプリント サーバに変換できる印刷サービスが含まれています。この機能により、ブランチ オフィスに別のプリント サーバを設置する必要がなくなります。WAAS 印刷サービスは、Windows クライアントで使用でき、IP に基づく任意のネットワーク プリンタで動作します。

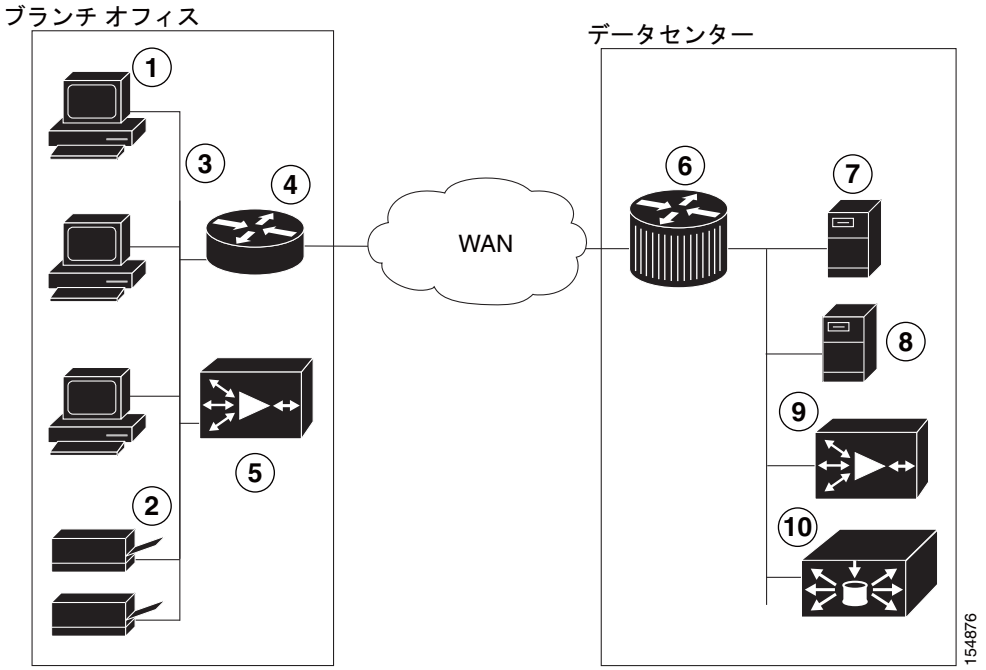
WAAS Central Manager GUI を使用すると、デバイスまたはデバイス グループ単位で、特定の WAAS プリント サーバに印刷ドライバを配信できます。また、WAAS Central Manager GUI から開くことができる Print Services Administration GUI から、印刷キューを管理し、プリント ジョブのステータスをモニタできます。

ここでは、次の内容について説明します。

ブランチ オフィスの印刷トポロジ

ブランチ オフィスの典型的なプリント サーバ トポロジでは、多数のクライアント デスクトップが、複数のプリンタの代わりに 1 台のプリント サーバを使用しています。WAAS レガシー印刷サービス ソリューションによって、ブランチ オフィスの WAE 上で WAAS ソフトウェアと一緒にプリント サーバをホストできます。図 13-1 に、ブランチ オフィスとデータセンターの WAAS 印刷サービス トポロジを示します。

図 13-1　ブランチ オフィスの WAAS 印刷サービス トポロジ



1	ブランチ オフィスの CIFS クライアント	**6**	データセンターの Cisco ルータ
2	ブランチ オフィスのネットワーク接続されたプリンタ	**7**	データセンターのファイル サーバ
3	ブランチ オフィスのローカル LAN	**8**	データセンターのバックアップ ファイル サーバ
4	ブランチ オフィスの Cisco ルータ	**9**	データセンターの WAE
5	ブランチ オフィスの WAE（WAAS プリント サーバ）	**10**	データセンターの WAAS Central Manager

この構成では、ブランチ オフィスの WAE が、ブランチ オフィスのクライアントにローカル印刷サービスを提供します。Microsoft クライアントは、現在 Microsoft プリント サーバを使用しているように、WAAS プリント サーバを使用します。

- クライアントは、Windows ウィザードを使用して、ローカル コンピュータに印刷キューを追加または削除できます。
- クライアントは、WAAS プリント サーバにプリント ジョブをスプールできます。
- WAAS プリント サーバは、印刷機能についてプリンタと通信します。

WAAS 印刷サービス

ブランチ オフィスの WAE 上の WAAS 印刷サービス ソリューションには、2 つの主要コンポーネントがあります。

- Samba：WAAS は、Samba を使用して、Microsoft クライアントが、印刷キューの追加と削除、ドライバの追加と削除、印刷キューの参照、および WAAS プリント サーバへのジョブのスプールを実行できるようにします。
- Common Unix Printing System（CUPS）：WAAS は、CUPS を使用して、印刷キューを管理し、Microsoft クライアントのスプール済みプリント ジョブを TCP/IP を使用して適切なプリンタへ送信します。

この項では、WAAS 印刷サービスについて説明します。内容は、次のとおりです。

印刷ドライバのサポートと相互運用性

WAAS WAE には、オープン ソースの Samba および CUPS テクノロジーの統合に基づくプリント サーバが含まれます。テスト プロセスの間、高性能の用紙処理などの複雑な機能を持つ特定の印刷ドライバが、ポイント印刷機能について WAAS と互換性がないことを判別します。特に、一部のプリンタ メーカーのソリューションに含まれる Fiery Driver は、Samba と互換性がありません。他の Multi Function Printer（MFP; 多機能プリンタ）でも、Samba と使用するときには機能に制限があり、WAAS ではサポートされません。

印刷ドライバが WAAS と互換性があるかどうかを判別するには、Add Printer Wizard を使用して WAE でドライバの追加プロセスを実行します。印刷キューを作成したあとに使用可能なすべてのクライアントの印刷機能を比較すると同時に、Microsoft Windows プリント サーバへの類似のインストールとも比較します。機能面で明らかな矛盾がある場合、印刷ドライバが WAAS プリント サーバのポイント印刷機能で使用できないことを意味します。回避策としては、各クライアント デスクトップ上に、CD または他のソースからのインストールが必要になります。

Windows XP Pro/Windows 2003 Server 環境で WAAS 印刷サービスを使用する場合、自動ドライバ ダウンロード機能が正常に動作するためには、WAE を Active Directory に登録する必要があります。これは、未登録のデバイスからホストがドライバをダウンロードできないというドメイン メンバーのデフォルト コンピュータ ポリシーによるものです。この問題が発生したとき、ユーザには次のようなメッセージが表示されます。「A policy is in effect on your computer which prevents you from connecting to this print queue. Please contact your system administrator.」

さらに、次の事項に注意してください。

- 印刷は、ブランチ オフィスの WAE が動作しているときだけ可能です。
- WAAS 印刷ソリューションでは、認証を行いません。どのユーザも WAAS プリント サーバにアクセス可能で、プリント ジョブを送信できます。
- WAAS では、IP ベースのネットワーク プリンタだけをサポートします。WAAS プリント サーバに直接接続しているプリンタが、HP や Linksys から入手できるパラレル、シリアル、または USB IP アダプタを使用することを推奨します。
- WAAS は、Raw Queue をサポートしています。したがって、ファイルの印刷形態への変換はすべて、ベンダー提供のプリンタ ドライバを使用してクライアント マシンで実行され、プリント サーバは Win2003 型の印刷キュー管理を実行します。
- WAAS は 32 ビット ドライバをサポートしています。WAAS ソフトウェアが使用する Samba バージョンは、64 ビット印刷ドライバをサポートしていません。

プリンタ クラスタ処理

プリンタ クラスタ処理を使用すると、管理者は、複数のプリンタをグループ化して、フェールオーバーとロード バランシング機能を提供できます。プリンタ クラスタにはプリンタを何台でも入れることができますが、最大で 12 台のプリンタを入れることを推奨します。同じモデルと機能を持つプリンタだけをグループ化する必要があります。クラスタ内のプリンタは、相互に近接する必要があります。すべてのプリンタ（プリンタ クラスタを含む）において、デフォルトのスプール スペースは 1 GB です。

プリンタ クラスタは、WAAS プリント サーバを使用する Microsoft クライアントでは 1 つの印刷キューとして表示されます。WAAS プリント サーバは、クラスタ内のデフォルト プリンタの選択をサポートしていません。プリンタ クラスタ内のプリンタへプリント ジョブを送信すると、プリント ジョブは自動的に WAAS プリント サーバが転送し、最初に使用できるプリンタへ送信します。

印刷サービスのユーザ

WAAS 印刷サービス環境には、次の種類のユーザが存在します。

- 管理ユーザ：プリンタ情報とプリンタ クラスタのメンバシップを追加および変更できるユーザ。
- プリント ユーザ：プリンタからジョブを印刷できるが、プリンタ設定の追加や変更は実行できないユーザ。プリント ユーザは、自身のプリント ジョブを削除および一時停止できます。

（注）　ジョブの所有者は、ジョブがスプール中であっても、Microsoft クライアントと Print Services Administration GUI で自身のジョブを管理できます。

機能のサポート

各種印刷サービス機能は、Samba、CUPS、WAAS ソフトウェアなどのさまざまなソフトウェア コンポーネントによって処理されます。表 13-1 に、特定の印刷サービス機能について、それらを提供するツールを示します。

表 13-1　WAAS 印刷サービス機能のサポート

機能	機能を提供するソフトウェア
プリンタの追加、変更、または削除	CUPS
プリンタ クラスタ（CUPS ではクラスと呼ばれる）の追加、変更、または削除	CUPS

表 13-1　WAAS 印刷サービス機能のサポート （続き）

機能	機能を提供するソフトウェア
プリント ジョブの表示と制御	CUPS、Windows プリンタ キュー コンソール
個々のプリンタのステータスのモニタ	CUPS
WAAS プリント サーバに接続しているプリンタのリスト、特定のプリンタに関連するドライブ、および配信されたすべてのドライバのリストの表示	WAAS Central Manager GUI
診断とトラブルシューティング	CUPS と Samba は、それぞれの診断を実行します。WAAS Central Manager GUI は、ドライバ配信に関係するエラー メッセージを表示します。
プリント サーバからのクライアント プリンタ ドライバのインストール	Samba[1]
プリント サーバへの印刷ドライバの配信	WAAS Central Manager GUI
Samba と Windows Active Directory を使用したプリンタのアベイラビリティの通知	Samba
ログのエクスポート	CLI を使用した手動の FTP
管理者（Admin）認証	WAAS Central Manager
安全な管理	WAAS ソフトウェア

1. WAAS ソフトウェアが使用する Samba バージョンは、64 ビット印刷ドライバをサポートしていません。

印刷サービスの計画

この項では、印刷サービスを設定する前に収集する必要がある情報について説明します。WAAS 印刷サービスを初めて設定しているか、Microsoft 印刷サービスから移行しているかに関係なく、この項で概要を説明する情報が必要です。印刷サービスを計画するときは、次の手順を使用すると、設定エラーを防止できます。

1. プリンタのネットワーク機能とドライバ サポートを計画します。

   この情報には、プリンタの種類（PostScript、PCL、その他）、プリンタ ネットワーク プロトコル、およびポート（LPD、IPP、LPQ、LPR およびポート）、およびフェールオーバー用にプリンタをクラスタ化する必要があるかどうかが含まれます。ドライバ情報を取得するには、ポイントして印刷機能をサポートするために WAAS プリント サーバにインストールするプリンタ ドライバを含む CD またはサーバを見つけます。

2. 印刷キュー設定を計画します。

   この情報には、プリント サーバ用に作成する印刷キューの名前と種類およびプリント サーバがプリンタのネットワーク機能やポートと通信する方法が含まれます。

次の各項で、印刷サービスの計画に関する詳細な情報を提供します。

- 「印刷管理ユーザの識別」（P.13-6）
- 「プリンタ情報の取得」（P.13-6）
- 「計画用のワークシート」（P.13-6）

印刷管理ユーザの識別

すべてのブランチ オフィスのクライアントが WAAS プリント サーバ上の印刷サービスを使用できますが、管理ユーザだけが印刷キューの管理のようなプリンタ管理作業を実行できます。これらの管理ユーザは、ブランチ オフィスの WAE と WAAS Central Manager デバイスに作成された admin アカウントを持つ必要があります。

印刷管理者権限を持つ必要があるユーザを識別します。WAAS プリント サーバと WAAS Central Manager デバイスでこれらのユーザを作成する必要があります。

（注）　プリンタにアクセスできる admin ユーザの数を制限することを推奨します。各 admin ユーザがプリンタのプロパティにアクセスすると、プリンタ オブジェクトが更新されるので、すべてのクライアントが次のセッションでプリンタ オブジェクトのコピーを更新しなければならなくなります。admin ユーザが定期的にプリンタにアクセスすると、遅延とトラフィックが増加する場合があります。

プリンタ情報の取得

印刷サービスを設定する前に、ネットワーク上の各プリンタに関する次の情報を取得すると便利です。

- プリンタの種類
- プリンタのプロトコル
- 印刷キューの数と名前
- プリンタの接続（直接ネットワークまたはプリント サーバ ゲートウェイ デバイスを使用）
- プリンタ ドライバ

  ドライバは、ベンダーが提供する CD-ROM に入っている場合があります。一般に使用されるドライバは、Windows オペレーティング システムにも組み込まれています。これらの共通ドライバにアクセスするには、Windows システムでプリンタの追加ウィザードを開きます。

計画用のワークシート

計画用のワークシートとして表 13-2、表 13-3、および表 13-4 を使用すると、WAAS 印刷サービスを正しく設定できます。

表 13-2　セキュリティ モデルとディレクトリ サービス

説明	値
プリント サーバ IP	
WINS サーバ IP	
プリント サーバの NetBIOS 名（任意）[1]	
プリント サーバ管理ワークステーションのユーザ名	

1. プリント サーバ用の NetBIOS 名が未指定の場合は、代わりにホスト名が使用されます。ホスト名が 15 文字より長い場合は、15 文字で切り捨てられます。

表 13-3　ネットワーク機能とドライバ サポート

説明	値
プリンタの種類（PostScript、PCL、その他）	
プリンタ ネットワーク プロトコル（LPD、IPP、LPQ、LPR）	
プリンタ ポート	
プリンタ クラスタ	
ドライバ ファイルの位置と名前	

表 13-4　印刷キューの設定

説明	値
印刷キューの名前	
印刷キューの種類	

印刷サービスの設定

この項では、WAAS ネットワークで印刷サービスを設定する方法について説明します。

設定用のチェックリスト

（注）　レガシー印刷サービスの機能は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー印刷サービスを有効にすると、デバイス上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー印刷サービスの何らかの設定値を設定しようとした場合に警告されます。レガシー印刷サービスをお使いの場合は、Windows プリント アクセラレータに移行してください。

表 13-5 に、WAAS ネットワークで印刷サービスを設定するために完了する必要がある設定手順を示します。

表 13-5　WAAS 印刷サービスを設定するためのチェックリスト

作業	追加情報と手順
1. 「計画」の項の情報を確認します。	WAAS ネットワークで印刷サービスを設定する前に、「印刷サービスの計画」（P.13-5）を参照してください。
2. WAE デバイスと WAAS Central Manager デバイスを印刷サービス用に準備します。	WAAS システムを印刷サービス用に準備するには、WAE デバイスと WAAS Central Manager デバイス用の WINS サーバ名と NetBIOS 名を指定する必要があります。さらに、WAE デバイス上で、CIFS アクセラレータか、レガシー WAFS エッジ サービスを有効にする必要もあります。詳細については、「WAE デバイスと Central Manager の印刷サービス用の準備」（P.13-8）を参照してください。

表 13-5　WAAS 印刷サービスを設定するためのチェックリスト （続き）

作業	追加情報と手順
3. WAE デバイスと WAAS Central Manager デバイスに、print admin 特権を持つアカウントを作成します。	Print Services Administration GUI を使用して印刷サービスを設定し、WAAS Central Manager デバイスの中央レポジトリにドライバを組み込むには、これらの各デバイスに print admin 特権を持つアカウントを作成する必要があります。詳細については、「print admin 特権を持つアカウントの作成」（P.13-10）を参照してください。
4. 印刷サービスを有効にします。	デフォルトで、WAAS 印刷サービス機能は、すべての WAAS デバイスで無効になっています。印刷サービスを有効にするには、「印刷サービスの有効化」（P.13-11）を参照してください。
5. WAAS プリント サーバにプリンタを追加します。	新しい WAAS プリント サーバにプリンタを追加するには、「WAAS プリント サーバへのプリンタの追加」（P.13-12）を参照してください。
6. プリント クラスタを作成します（任意）。	印刷サービスにフェールオーバー機能を提供するには、複数のプリンタをプリント クラスタにまとめることができます。詳細については、「プリンタ クラスタの追加」（P.13-15）を参照してください。
7. 中央のドライバ リポジトリとして WAAS Central Manager を設定します。	WAAS を使用すると、中央ドライバ リポジトリとして設定されている場合、WAAS Central Manager からすべての印刷ドライバを集中管理できます。詳細については、「ドライバ リポジトリとしての WAAS Central Manager の設定」（P.13-17）を参照してください。
8. WAAS プリント サーバへドライバを配信します。	ドライバ リポジトリとして WAAS Central Manager を設定し、ドライバをリポジトリに組み込んだら、WAAS ネットワーク内のすべてのプリント サーバへドライバを配信できます。詳細については、「WAAS プリント サーバへのドライバの配信」（P.13-20）を参照してください。
9. 印刷ドライバをプリンタに関連付けます。	WAAS プリント サーバへドライバを配信したら、WAAS プリント サーバ上の正しいプリンタにドライバを関連付ける必要があります。詳細については、「プリンタへのドライバの関連付け」（P.13-23）を参照してください。
10. WAAS プリント サーバ上の各印刷ドライバを初期化します。	印刷問題を防止するには、ブランチ オフィスのクライアントにインストールし、使用する前に、各印刷ドライバを初期化する必要があります。詳細については、「印刷ドライバの初期化」（P.13-23）を参照してください。
11. ブランチ オフィスのクライアントにプリンタを追加します。	印刷サービスを正しく設定したら、ブランチ オフィスのクライアントは、Microsoft プリンタの追加ウィザードを使用してプリンタを追加する必要があります。詳細については、「ブランチ オフィスのクライアントへの WAAS プリント サーバの追加」（P.13-24）を参照してください。

WAE デバイスと Central Manager の印刷サービス用の準備

印刷サービスを有効にする前に、WINS サーバ名と NetBIOS 名を指定して、WAE デバイスと Central Manager を準備する必要があります。さらに、WAE デバイス上で、CIFS アクセラレータか、レガシー WAFS エッジ サービスを有効にする必要もあります。これらの設定は、WAE デバイスと Central Manager を最初に設定したときにすでに設定されている場合があります。

（注）　WINS を使用しない場合でも、プリンタを手動で Active Directory に追加することにより、レガシー プリント サービスを導入できます。これにより、そのプリンタは、ネットワーク ブラウザから見えなくなってからも、プリント サーバと同じサブネット内に配置されている Windows クライアントが存在しなければ、クライアントから検出することが可能になります。

WAE デバイスと Central Manager を印刷サービス用に準備するには、次の手順に従ってください。

ステップ 1　（任意）WAE デバイスの NetBIOS 名を指定します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

b. 印刷サービスを有効にしたい WAE デバイスの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[*Device Name*] > [Activation] を選択します。[Device Activation] ウィンドウが表示されます。

d. [NetBIOS Name] フィールドに、WAE デバイスの NetBIOS 名を入力します。

（注） WAE が非トランスペアレント モードで動作している場合、[Name] フィールドに入力するデバイスの NetBIOS 名およびホスト名には同一の名前を設定する必要があります。

e. [Submit] をクリックして、変更を保存します。

この WAE デバイスで印刷サービスを有効にすると、デバイスのプリント サーバ名として NetBIOS 名が使用されます。NetBIOS 名を指定しない場合、代わりにデバイスのホスト名が使用されます。デバイスのホスト名は、「デバイス プロパティの変更」（P.9-1）の説明に従って [Activation] ページで指定します。

CLI を使用して NetBIOS 名を指定するには、**windows-domain netbios-name** グローバル コンフィギュレーション コマンドを使用します。

ステップ 2　WAAS Central Manager デバイスの NetBIOS 名を指定します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

b. WAAS Central Manager デバイスの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[*Device Name*] > [Activation] を選択します。[Device Activation] ウィンドウが表示されます。

d. [NetBIOS Name] フィールドに、WAAS Central Manager の NetBIOS 名を入力します。

e. [Submit] をクリックして、変更を保存します。

ステップ 3　WAE デバイスの WINS サーバ名を指定します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

b. 印刷サービスを有効にしたい WAE デバイスの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[Configure] > [Network] > [WINS] を選択します。

d. [WINS Server] フィールドに、WINS サーバの名前を入力します。

e. [Submit] をクリックして、変更を保存します。

CLI を使用して NetBIOS 名を指定するには、**windows-domain wins-server** グローバル コンフィギュレーション コマンドを使用します。

WINS を使用していない場合は、手動でプリンタを Active Directory に追加します。

ステップ 4　WAAS Central Manager の WINS サーバ名を指定します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

b. WAAS Central Manager デバイスの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[Configure] > [Network] > [WINS] を選択します。

d. [WINS Server] フィールドに、WINS サーバの名前を入力します。

e. [Submit] をクリックして、変更を保存します。

ステップ 5　CIFS アクセラレータを WAE デバイス上で有効にします（有効にしない場合は、ステップ 6 に進みます）。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

b. 印刷サービスを有効にしたい WAE デバイスの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[Configure] > [Acceleration] > [Enabled Features] を選択します。

d. [CIFS Accelerator] チェックボックスを選択します。

e. [Submit] をクリックして、変更を保存します。

ステップ 6　レガシー WAFS エッジ サービスを WAE デバイス上で有効にします（有効にしない場合は、ステップ 5 を実行します）。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

b. 印刷サービスを有効にしたい WAE デバイスの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Services] > [Edge Configuration] を選択します。

d. [Enable Edge Server] チェックボックスを選択します。CIFS および QoS 設定が有効になります。これらの設定を構成する方法については、「エッジ デバイスの設定」（P.11-14）を参照してください。

e. [Submit] をクリックして、変更を保存します。

（注）　エッジ サービスを有効にしたら、デバイスをリブートまたは再ロードする必要があります。

print admin 特権を持つアカウントの作成

Print Services Administration GUI を使用して印刷サービスを設定するには、WAAS Central Manager デバイスに print admin 特権を持つアカウントを作成する必要があります。また、このアカウントを使用すると、中央レポジトリへドライバをアップロードできます。

また、print admin 特権を持つユーザ アカウントにはドメインを割り当てる必要があります。ドメインは、ユーザがアクセス可能なデバイス グループまたは WAE を定義します。ユーザがアクセスする必要のあるすべての WAE を割り当てたドメインに所属させる必要があります。

WAAS Central Manager デバイスに print admin 特権を持つアカウントを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [AAA] > [Users] を選択します。[User Accounts] ウィンドウに、システム上のすべてのユーザ アカウントが表示されます。

ステップ 2　[Create New User Accounts] アイコンをクリックします。[Creating New User Account] ウィンドウが表示されます。

ステップ 3　[Username] フィールドに、ユーザ アカウント名を入力します。ユーザ名は、大文字と小文字を区別し、特殊文字を使用できます。

ステップ 4　[Local User] チェックボックスを選択します。

ステップ 5　[Password] フィールドにローカル ユーザ アカウントのパスワードを入力し、[Confirm password] フィールドに同じパスワードを再入力します。パスワードは、大文字と小文字を区別します。

ステップ 6　[CLI Privilege Level] ドロップダウン リストから、**0（通常のユーザ）**または **15（スーパーユーザ）**を選択します。

ステップ 7　[Print Admin] チェックボックスを選択します。

ステップ 8　（任意）[User Information and Comments] セクションにあるフィールドに入力します。

ステップ 9　[Submit] をクリックして、変更を保存します。

次に、print 役割をアカウントに割り当てる必要があります。

ステップ 10　[Role Management] タブをクリックします。

[Role Management for User Account] ウィンドウが表示され、設定されているすべての役割名が表示されます。

ステップ 11　print 役割の横に表示される [Assign] アイコン（青色の十字）をクリックします。

ステップ 12　[Submit] をクリックします。

次に、ドメインをアカウントに割り当てる必要があります。

ステップ 13　[Domain Management] タブをクリックします。

[Domain Management for User Account] ウィンドウが表示され、設定されているすべてのドメイン名が表示されます。

ステップ 14　アカウントに割り当てたいドメインの横に表示される [Assign] アイコン（青色の十字）をクリックします。ユーザがアクセスする必要のあるすべての WAE を割り当てたドメインに所属させる必要があります。

ステップ 15　[Submit] をクリックします。

WAAS Central Manager デバイスにアカウントを作成する方法については、「新しいアカウントの作成」（P.7-4）を参照してください。

CLI から print admin 特権（特権レベル 15）を持つアカウントを作成するには、**username** グローバル コンフィギュレーション コマンドを使用できます。

印刷サービスの有効化

WAE 上の印刷サービスを有効にするには、WAE Device Manager GUI を使用する必要があります。

（注）　レガシー印刷サービスの機能は、WAAS バージョン 4.2.1 での使用は推奨されません。まだ機能はしますが、サポート対象から外されており、将来のバージョンでは削除される予定です。レガシー印刷サービスを有効にすると、デバイス上でアラームが発生し、すべての Central Manager GUI ページおよび CLI で、レガシー印刷サービスの何らかの設定値を設定しようとした場合に警告されます。レガシー印刷サービスをお使いの場合は、Windows プリント アクセラレータに移行してください。

任意の WAE 上の印刷サービスを有効にできますが、WAAS Central Manager 上の印刷サービスは有効にできません。印刷サービスを有効にすると、ブランチ オフィスの WAE が WAAS プリント サーバになり、匿名 FTP ユーザ アカウントがデバイスに作成されます。この FTP アカウントは、WAAS Central Manager 上の印刷ドライバにアクセスするために使用されます。

ブランチ オフィスの WAE で印刷サービスを有効にするには、次の手順に従ってください。

ステップ 1　次の URL にアクセスして、WAE Device Manager GUI にログインします。

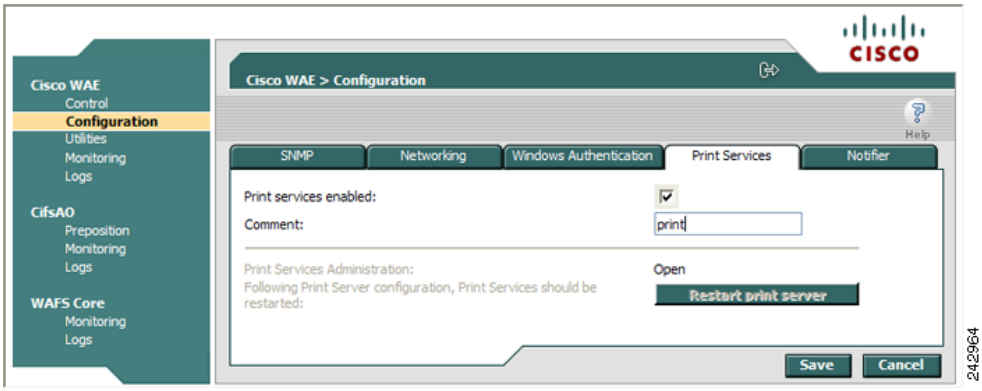
https://*wae-ip-address*:8443/mgr

wae-ip-address は、印刷サービスを有効にしたいブランチ オフィスの WAE の IP アドレスです。

ステップ 2　[Cisco WAE] メニューから [Configuration] を選択し、[Print Services] タブをクリックします。

[Print Services] ウィンドウが表示されます（図 13-2 を参照）。

図 13-2　[Print Services] ウィンドウ



ステップ 3　[Print services enabled] チェックボックスを選択して、印刷サービスを有効にします。

ステップ 4　（任意）[Comment] フィールドに説明を入力します。

この説明は、ユーザが Windows エクスプローラでブラウズするときに、プリント サーバの横に表示されます。

ステップ 5　[Save] をクリックして、印刷サービスを再起動します。

再起動すると、Print Services Administration GUI の [Open] リンクが有効になります。デバイスで印刷サービスが有効になると、デバイスは WAAS プリント サーバになります。

（注）　CLI を通じて変更を行い、プリント サーバを再起動する必要があるときは、[Restart Print Server] ボタンを使用します。

CLI から印刷サービスを有効にするには、**print-services enable** グローバル コンフィギュレーション コマンドを使用できます。

WAAS プリント サーバへのプリンタの追加

印刷サービスを有効にしたら、1 台または複数のプリンタを新しい WAAS プリント サーバに追加する必要があります。プリンタを追加すると、Windows 印刷クライアントが WAAS プリント サーバへジョブをスプールするために使用する印刷キューも追加されます。

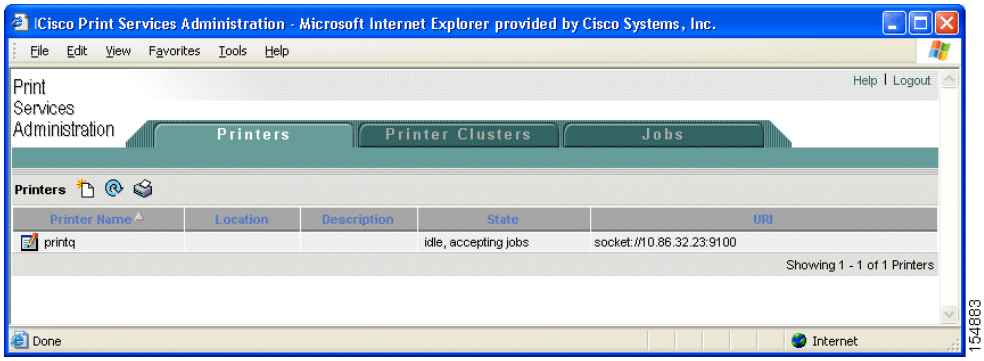
WAAS プリント サーバにプリンタを追加するには、次の手順に従ってください。

ステップ 1　次のいずれかを実行して、Print Services Administration GUI を開きます。

- WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [Print Servers] を選択し、クラスタに追加するプリント サーバの名前の横の [Edit] アイコンをクリックしてから、タスクバーの [CUPS] アイコンをクリックします。
- WAE Device Manager GUI で、[Cisco WAE] メニューから [Configuration] を選択し、[Print Services] タブをクリックし、[Open] リンクをクリックします。

Print Services Administration GUI が表示されます（図 13-3 を参照）。

図 13-3　Print Services Administration GUI

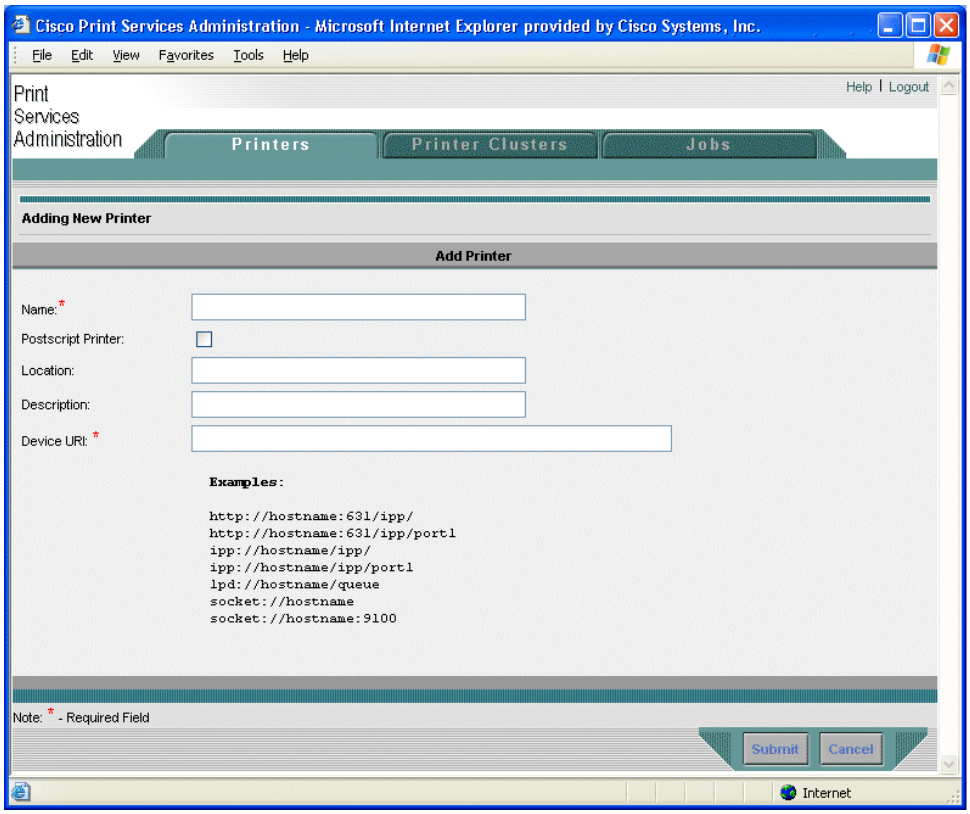


ステップ 2　[Add Printer] アイコンをクリックします。ユーザ名とパスワードを入力するプロンプトが表示されます。

ステップ 3　この WAE デバイスに作成した print admin アカウント用のユーザ名とパスワードを入力し、[OK] をクリックします。

[Add Printer] ウィンドウが表示されます（図 13-4 を参照）。このアカウントを作成する方法については、「新しいアカウントの作成」（P.7-4）を参照してください。

図 13-4　WAAS プリント サーバへのプリンタの追加



ステップ 4　提供されるフィールドに次の情報を入力します。

- [Printer name]（必須）：プリンタのユーザ定義の名前（最大 127 文字）。英字、数字、およびアンダースコアだけを使用できます。スペースは使用できず、名前はシステム全体で固有でなければなりません。たとえば、異なるプリンタに同じ名前を使用できません。同じ名前を持つプリンタが存在する場合は、新しい設定が古い設定を更新します。同じ名前を持つプリンタ クラスタが存在する場合は、エラーが表示されます。
- [Postscript printer]：このチェックボックスを使用すると、プリンタが PostScript 対応かどうかを指定できます（デフォルトは PostScript 非対応です）。PostScript プリンタには、generic.ppd が使用されます。PostScript 非対応プリンタの場合、PPD が raw に設定されます。PostScript プリンタ設定は、テスト ページと見出しページの印刷をサポートしています。このチェックボックスは、新しいプリンタを追加するときだけ表示されます。プリンタを変更している場合、このチェックボックスは表示されません。
- [Location]：プリンタのユーザ指定位置（最大 127 文字）。
- [Description]：プリンタのユーザ指定の説明（最大 127 文字）。
- [Device URI]（必須）：デバイス URI は、次の形式のプリンタのアドレスです。

  protocol://server:port/queue

  最大 1024 文字まで使用できます。許可されるプロトコルは、lpd、socket、ipp、および http だけです。プロトコルの妥当性検査は実行されますが、それ以上の URI 文字列検査は実行されません。正しく入力するためのヒントとして、URI の例のリストが表示されます。特定のプリンタの情報（プリンタ ポート、プロトコル）は、プリンタ メーカーのマニュアル、プリンタのテスト ページ、またはプリンタの前面パネルから取得できます。

（注）　プロトコル、ポート、またはキューを正しくを指定しないと、ページが正しく印刷されません。

ステップ 5　[Submit] をクリックして、変更を保存します。

新しい印刷キューは、1 分以内にクライアントに表示されます。

ステップ 6　プロセスを繰り返して、WAAS プリント サーバに他のプリンタを追加します。

プリンタを追加したあと、そのプリンタを Windows Active Directory に追加する必要があります。Active Directory にプリンタを追加するには、次の手順に従ってください。

ステップ 1　Windows ドメイン コントローラで、[Active Directory Users and Computers] を開きます。

ステップ 2　プリンタを公開したいコンテナ オブジェクト フォルダを右クリックし、[New] をクリックしてから [Printer] をクリックします。

[New Object-Printer] ダイアログボックスが表示されます。

ステップ 3　テキスト ボックスにプリンタへのパス（¥¥printserver¥printername など）をタイプし、[OK] をクリックします。

プリンタ クラスタの追加

プリンタ クラスタ処理を使用すると、複数のプリンタをグループ化できます。このクラスタ化により、フェールオーバーとロード バランシング機能が提供されます。プリンタ クラスタには、最大 12 台のプリンタを入れることができます。同じモデルと機能を持つプリンタだけをグループ化する必要があります。クラスタ内のプリンタは、相互に近接する必要があります。

プリンタ クラスタは、WAAS プリント サーバを使用する Microsoft クライアントでは 1 つの印刷キューとして表示されます。WAAS プリント サーバは、クラスタ内のデフォルト プリンタの選択をサポートしていません。プリンタ クラスタ内のプリンタへプリント ジョブを送信すると、プリント ジョブは自動的に WAAS プリント サーバが転送し、最初に使用できるプリンタへ送信します。

すべてのプリンタ（プリンタ クラスタを含む）において、デフォルトのスプール スペースは 1 GB です。

プリント クラスタを追加するには、次の手順に従ってください。

ステップ 1　次のいずれかを実行して、Print Services Administration GUI を開きます。

- WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [Print Servers] を選択し、クラスタに追加するプリント サーバの名前の横の [Edit] アイコンをクリックしてから、タスクバーの [CUPS] アイコンをクリックします。
- WAE Device Manager GUI で、[Cisco WAE] メニューから [Configuration] を選択し、[Print Services] タブをクリックし、[Open] リンクをクリックします。

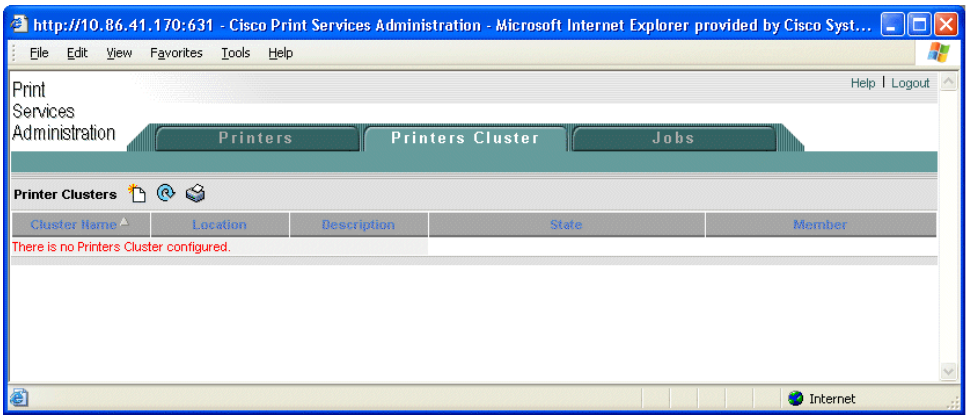
Print Services Administration GUI が表示されます。

ステップ 2　[Printer Cluster] タブをクリックします

まだ Print Services Administration GUI にログインしていない場合は、print admin アカウントのユーザ名とパスワードを入力するプロンプトが表示されます。この情報を入力し、[OK] をクリックします。

[Printer Clusters] ウィンドウが表示されます（図 13-5 を参照）。

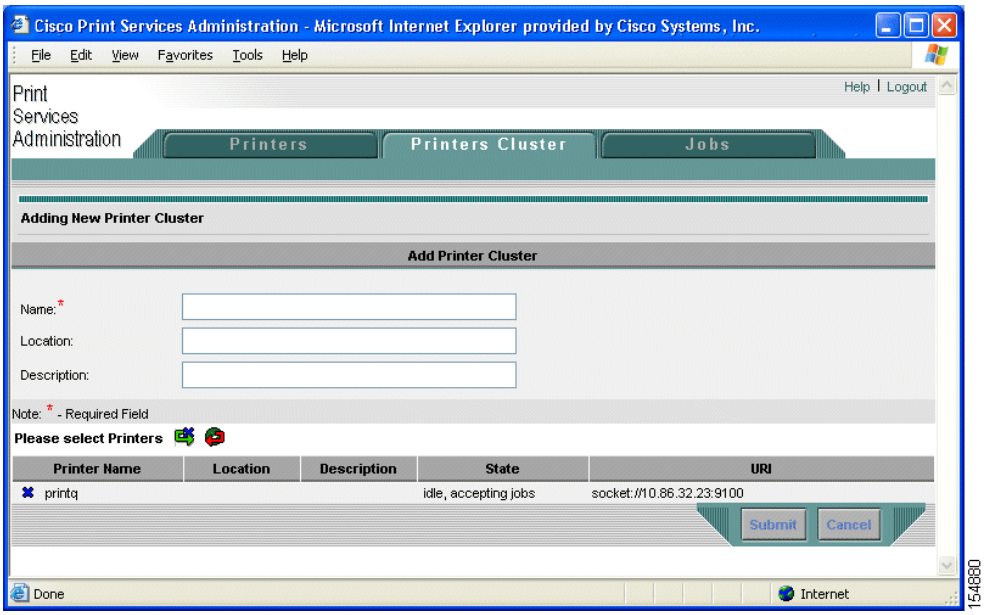
図 13-5　[Print Services Administration] ウィンドウ：[Printer Clusters] タブ



ステップ 3　タスクバーの [Add Printer Cluster] アイコンをクリックします。

[Add Printer Cluster] ウィンドウが表示されます（図 13-6 を参照）。

図 13-6　プリンタ クラスタの新規追加



ステップ 4　プリンタ クラスタの名前を入力します。

プリンタ クラスタ名には、英字、数字、およびアンダースコアを入れることができます（スペースは使用できません）。名前は 127 文字以内であり、システム全体で固有でなければなりません。たとえば、異なるプリンタ クラスタに同じ名前を使用できません。同じ名前を持つプリンタ クラスタが存在する場合は、新しい設定が古い設定を更新します。同じ名前を持つプリンタが存在する場合は、エラーが表示されます。

ステップ 5　プリント クラスタの位置を入力します（任意）。

位置の名前は、127 文字以内です。

ステップ 6　プリンタ クラスタの説明を入力します（任意）。

この説明は、127 文字以内です。

ステップ 7　次のいずれかを実行して、この新しいクラスタに参加させたいプリンタを選択します。

-  をクリックして、使用できるすべてのプリンタを選択します。
- クラスタに参加させたい各プリンタの横にある  をクリックします。

ステップ 8　[Submit] をクリックします。

設定が保存されます。

新しい印刷キューは、1 分以内にクライアントに表示されます。

ドライバ リポジトリとしての WAAS Central Manager の設定

WAAS プリント サーバへ配信したいすべてのドライバを保存する印刷ドライバ リポジトリとして、WAAS Central Manager を設定できます。この項のステップ 1 ～ 4 でドライバ リポジトリとして WAAS Central Manager を設定する方法について説明し、ステップ 5 ～ 10 で Windows プリンタ ドライバ追加ウィザードを使用して、中央レポジトリにドライバを追加する方法について説明します。

ドライバ リポジトリとして WAAS Central Manager を設定しないと、印刷ドライバを集中的に WAAS プリント サーバへ配信できません。この場合、各 WAAS プリント サーバに手動でドライバをインストールする必要があります。個々のプリント サーバにドライバをインストールする方法については、「個々の WAAS プリント サーバへの印刷ドライバのインストール」（P.13-19）を参照してください。

複数の WAAS プリント サーバがある場合は、ドライバ リポジトリとして WAAS Central Manager を設定することを推奨します。

印刷ドライバ リポジトリとして WAAS Central Manager を設定するには、次の手順に従ってください。

ステップ 1　「print admin 特権を持つアカウントの作成」（P.13-10）で作成した print admin アカウントを使用して、WAAS Central Manager GUI にログインします。

ステップ 2　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [Print Repository] を選択します。

[Print Driver Repository Settings] ウィンドウが表示されます

ステップ 3　[Enable Central Manager as Driver Repository] チェックボックスを選択します。

ステップ 4　[Submit] をクリックして、変更を保存します。

ステップ 5　Windows クライアントにログインし、次のコマンドを入力して、新しい中央レポジトリにドライバを追加します。

net use ¥¥*CM_netbios_name*¥print$ * /USER:*username*

CM_netbios_name 値は、WAAS Central Manager デバイスの NetBIOS 名です。*username* は、ステップ 1 で作成したユーザ名です。

PCL ドライバの代わりに、高速にロードされる PostScript（PS）印刷ドライバを使用することを推奨します。

ステップ 6　Windows クライアントから、[Run] ウィンドウに次のコマンドを入力します。

¥¥*CM_netbios_name*

CM_netbios_name 値は、WAAS Central Manager デバイスの NetBIOS 名です。

Central Manager のドライバ リポジトリが表示されます。

ステップ 7　[Printers] アイコンをダブルクリックします。

[Printers on Device] ウィンドウが表示されます。

ステップ 8　[Printers on Device] ウィンドウから、[File] > [Server Properties] を選択します。

[Print Server Properties] ウィンドウが表示されます。

ステップ 9　[Drivers] タブを選択し、[Add...] をクリックします。

プリンタ ドライバの追加ウィザードが開きます。

（注）　ドライバを追加するために十分な印刷共有空間がない場合、Windows と互換性がないためにドライバをインストールできなかった、またはコンピュータ ハードウェアやネットワーク接続問題に関係する障害のために Windows がすべてのデータを保存できなかったことを示す Windows エラー メッセージが表示されます。このようなメッセージが表示される場合は、使用されなくなったドライバを削除してから、手順を繰り返して新しいドライバを追加します。

ステップ 10　ウィザードに従って、WAAS Central Manager 上のリポジトリに必要なドライバを追加します。

（注）　リポジトリにドライバを追加するときに発生するエラー条件を防止するには、[Print Server Properties] ウィンドウの [Drivers] タブの [Update] または [Replace] ボタンを*クリックしないでください。*

ステップ 11　ウィザードが完了したら、WAAS Central Manager GUI で [Configure] > [Legacy Services] > [Print Drivers] を選択することにより、ドライバがリポジトリに正常に追加されたことを確認します。

ドライバのリストが表示されるまでに、最大 5 分かかる場合があります。追加したドライバがこのリストに表示されることを確認します。「デフォルトのシステム設定プロパティの変更」（P.9-17）に説明されている [System.datafeed.pollRate] フィールドを調整して、リストが更新される時間の長さを設定できます。

（注）　ディスク容量の不足によりドライバをインストールできないことを示すエラー メッセージが表示される場合は、リポジトリから未使用のドライバを削除してディスク容量を解放し、手順を繰り返してドライバを追加する必要があります。Windows 95、98、NT、および 2000 は、ドライバのインストール中に追加の保存ディレクトリを作成するため、これらのオペレーティング システムには印刷ドライバをインストールするために約 2 倍のディスク容量が必要です（インストールする各ドライバの 2 倍以上のディスク容量を解放する必要があります）。さらに、Windows 95、98、および NT オペレーティング システムでは、次の手順に従って Windows が削除しなかった一時的な印刷ドライバ ディレクトリを削除して、ディスク容量を解放できます（Windows 2000 および XP は、これらの一時的なディレクトリを自動的に削除します）。

一時的な印刷ドライバ ディレクトリを削除するには、次の手順を実行します。

a.　WAAS Central Manager 上の CLI から、**cd** コマンドを使用して、一時的な印刷ドライバ ディレクトリが存在するディレクトリに変更します。次に例を示します。

cd spool/samba/printers/W32X86

b.　**ls** コマンドを使用して、ディレクトリの内容を表示します。

c.　「__SKIP__xxx」というディレクトリを見つけて、一時的な印刷ドライバ ディレクトリを識別します。

d.　**rmdir** コマンドを使用して、一時的な印刷ドライバ ディレクトリを削除します。

個々の WAAS プリント サーバへの印刷ドライバのインストール

WAAS Central Manager をドライバ リポジトリとして設定して集中的にドライバを配信したくない場合は、Windows のドライバの追加ウィザードを使用して、必要なドライバを個々の WAAS プリント サーバにインストールできます。

WAAS プリント サーバにプリンタ ドライバをインストールするには、次の手順に従ってください。

ステップ 1　Windows クライアントにログインし、次のコマンドを入力します。

net use ¥¥*WAE_netbios_name*¥print$ * /USER:*username*

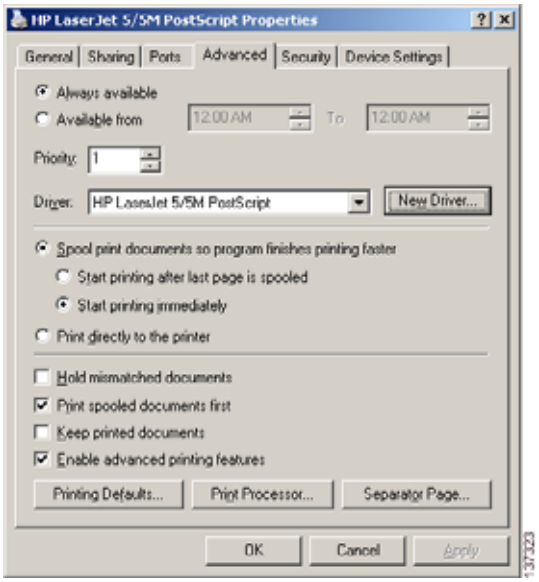
WAE_netbios_name 値は、WAAS プリント サーバの NetBIOS です。*username* は、「print admin 特権を持つアカウントの作成」（P.13-10）で指定したユーザ名です。

ステップ 2　Windows Network Neighborhood を使用してプリント サーバ共有を検索し、それをクリックします。あるいは、Windows システムで [Run] ウィンドウを開いて、¥¥*wae_netbios_name* と入力できます。

ステップ 3　[Printers] フォルダを開いて、WAAS Print Server に設定されたプリンタを表示します。

ステップ 4　ドライバをアップロードしたいプリンタを選択して右クリックし、[Properties] を選択します（図 13-7 を参照）。

図 13-7　プリンタ情報シートの例



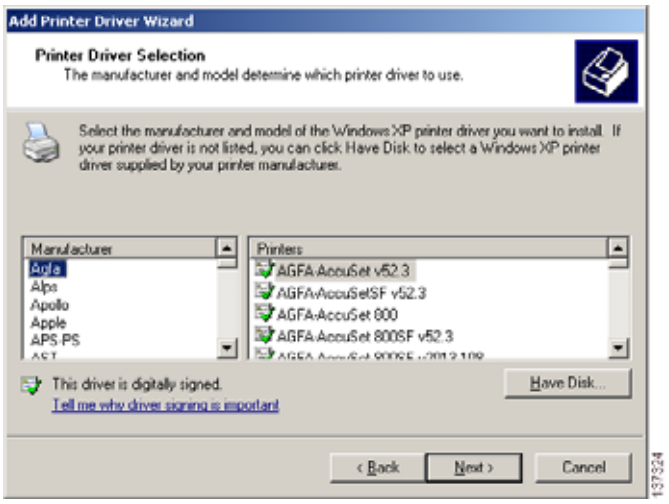
ステップ 5　CD-ROM またはサーバでプリンタ ドライバを見つけます。

ステップ 6　[New Driver] ボタンをクリックして、ドライバの追加ウィザードを開始します。

ステップ 7　[Next] をクリックします。

[Printer Driver Selection] ウィンドウが表示されます（図 13-8 を参照）。

図 13-8　ドライバ選択 ウィンドウ



ステップ 8　[Printer Driver Selection] ウィンドウに必要なドライバが表示されない場合は、[Have Disk] をクリックし、CD-ROM またはサーバでのプリンタ ドライバの位置を参照します。

ステップ 9　[OK] をクリックして、ドライバのインストールを完了します。

これでドライバが WAAS プリント サーバへアップロードされたので、任意のユーザが印刷するときにクライアント マシンへドライバをダウンロードできます。

ステップ 10　「印刷ドライバの初期化」（P.13-23）の説明に従って、ドライバを初期化します。

WAAS プリント サーバへのドライバの配信

ドライバ リポジトリとして WAAS Central Manager を設定し、中央レポジトリにドライバをインストールしたら、WAAS プリント サーバへドライバを配信できます。

次のいずれかの方式を使用して、WAAS プリント サーバへドライバを配信できます。

- ドライバを選択し、ドライバを配信したいプリント サーバを選択します。複数の WAAS プリント サーバまたはデバイス グループへ 1 つのドライバを配信するには、この方法を推奨します。「単一のドライバの複数デバイスまたは複数グループへの配信」（P.13-21）を参照してください。
- プリント サーバまたはデバイス グループを選択し、選択したデバイスにインストールする必要があるドライバを選択します。1 つのプリント サーバまたはデバイス グループへ複数のドライバを配信するには、この方法を使用することを推奨します。「1 つのデバイスまたはグループへの複数のドライバの配信」（P.13-21）を参照してください。

1 つまたは複数の WAAS プリント サーバへ印刷ドライバを配信したあと、「印刷ドライバの配信の確認」（P.13-22）の説明に従って、印刷ドライバの配信を確認できます。

（注）　印刷サービスが有効になっていない WAE へ印刷ドライバを配信しようとしても、ドライバはその WAE へ配信されません。

単一のドライバの複数デバイスまたは複数グループへの配信

複数のデバイスまたはグループへ 1 つのドライバを配信するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [Print Drivers] を選択します。[Drivers in the Repository] ウィンドウが表示されます。

ステップ 2　配信するドライバの横にある [Edit] アイコンをクリックします。ドライバのホーム ウィンドウが表示されます。

このウィンドウから、次の作業を実行できます。

- 下記の手順の説明に従って、プリント サーバへドライバを配信する。
- タスクバーの [Trash] アイコンをクリックして、リポジトリからドライバを削除する。
- ドライバに関する詳細を表示する。

ステップ 3　このドライバを配信するには、ナビゲーション ペインで次のいずれかのオプションをクリックします。

- [Distribute to Print Server]：個々の WAAS プリント サーバへドライバを配信します。
- [Distribute to Device Group]：同じデバイス グループに属する WAAS プリント サーバのグループへドライバを配信します。

選択したオプションに応じて、[Print Server assignments] ウィンドウまたは [Device Group assignments] ウィンドウが表示されます。

ステップ 4　WAAS 印刷ドライバを配信したいデバイスを選択します。

デバイスを選択するには、次のいずれかの手順を使用します。

- タスクバーの  をクリックして、使用できるすべてのプリント サーバまたはデバイス グループへドライバを配信します。
- 各プリント サーバまたはデバイス グループの横にある  をクリックして、これらの特定のデバイスへドライバを配信します。選択すると、アイコンは  に変化します。

ステップ 5　[Submit] をクリックします。

選択したデバイスの横にあるアイコンが  に変化し、指定したデバイスへドライバが配信されます。

ステップ 6　印刷ドライバが正常に配信されたことを確認します（「印刷ドライバの配信の確認」（P.13-22）を参照してください）。

1 つのデバイスまたはグループへの複数のドライバの配信

1 つのデバイスまたはグループへ複数のドライバを配信するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　印刷ドライバを配信したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウまたは [Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Services] > [Download Drivers] を選択します。

[Drivers in the Repository] ウィンドウが表示されます。

ステップ 4　次のいずれかを実行して、配信するドライバを選択します。

- タスクバーの をクリックして、リスト内のすべてのドライバを選択します。
- 配信する各ドライバの横にある をクリックします。選択すると、アイコンは に変化します。

ステップ 5　[Submit] をクリックします。

選択したドライバの横にあるアイコンが に変化し、選択したデバイスまたはデバイス グループが指定したドライバをダウンロードします。

ステップ 6　印刷ドライバが正常に配信されたことを確認します（「印刷ドライバの配信の確認」（P.13-22）を参照してください）。

印刷ドライバの配信の確認

1 つまたは複数の WAAS プリント サーバへ印刷ドライバを配信したら、WAAS Central Manager GUI を使用して、配信エラーをチェックし、必要ならドライバを再配信できます。

印刷ドライバが WAAS プリント サーバへ正しく配信されたことを確認するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [Print Servers] を選択します。

[Print Servers] テーブルが表示されます。このテーブルの [Driver Distribution Status] 領域に、成功および失敗したドライバ配信の数が表示されます。また、このテーブルには、プリント サーバがダウンロード処理中のドライバの数も表示されます。

ステップ 2　[Print Server Errors] 列と [Failed] 列でエラーの数を確認します。

これらの列は、WAAS プリント サーバで報告されたエラーの数を表示します。[Failed] 列はドライバ配信エラーの数を示し、[Print Server Errors] 列はプリント サーバでのシステム エラーの数を表示します。

ステップ 3　[Print Server Errors] 列または [Failed] 列に 0 以外の値（たとえば、1、2 または 3）が表示される場合は、次の手順を実行します。

a. 列の数値をクリックします。エラーのリストが表示されます。

b. エラー情報を使用して、プリント サーバまたはドライバ配信問題を解決します。

c. [Retry Downloading Failed Drivers] アイコンをクリックして失敗した印刷ドライバを再配信し、前の手順を繰り返してエラーをチェックします。

WAAS Central Manager GUI の次のページのタスクバーに、[Retry Downloading Failed Drivers] アイコンが表示されます。

- [My WAN] > [Manage Devices] に進み、該当するプリント サーバの横にある [Edit] アイコンをクリックし、ナビゲーション ペインの [Configure] > [Acceleration] > [Legacy Services] > [Drivers] を選択します。
- [My WAN] > [Manage Device Groups] に進み、該当するデバイス グループの [Edit] アイコンをクリックし、ナビゲーション ペインの [Configure] > [Acceleration] > [Legacy Services] > [Download Drivers] を選択します。

ステップ 4　WAAS プリント サーバ用の [Print Server Errors] 列と [Failed] 列に 0（配信エラーなし）が表示される場合は、次の手順を実行します。

a. 印刷ドライバを配信したプリント サーバの 1 つの横にある [Edit] アイコンをクリックします。

b. ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Services] > [Print Services] > [Drivers] を選択します。

このデバイスにインストールされているドライバのリストが表示されます。

c. 配信したドライバの [Download Status] 列に [Completed] が表示されることを確認します。

リストに印刷ドライバが表示されない場合は、最大 10 分待ち、ページを更新します。新しく配信したドライバがリストに [Completed] と表示されるまでに、最大 10 分かかる場合があります。

プリンタへのドライバの関連付け

WAAS プリント サーバへドライバを配信したら、「WAAS プリント サーバへのプリンタの追加」（P.13-12）で追加したプリンタにドライバを関連付ける必要があります。

配信したドライバをプリンタに関連付けるには、次の手順に従ってください。

ステップ 1　Windows クライアントにログインします。

ステップ 2　次のコマンドを実行して、print admin 特権レベルを設定します。

net use ¥¥*WAE_netbios_name*¥print$ * /USER:*username*

WAE_netbios_name は、「WAAS プリント サーバへのプリンタの追加」（P.13-12）で追加したプリンタを含む WAAS プリント サーバの NetBIOS 名です。*username* は、「print admin 特権を持つアカウントの作成」（P.13-10）で指定したユーザ名です。

ステップ 3　Windows クライアントから、[Run] ウィンドウに次のコマンドを入力します。

¥¥*wae_netbios_name*

[printer share] ウィンドウが表示されます。

ステップ 4　プリンタ アイコンをダブルクリックして、プリンタのリストを表示します。

ステップ 5　「WAAS プリント サーバへのプリンタの追加」（P.13-12）で追加したプリンタを右クリックし、[Properties] を選択します。

ステップ 6　[Advanced] タブをクリックし、[Driver] ドロップダウン リストから適切なドライバを選択します。

ステップ 7　[Apply] をクリックして変更を保存し、[OK] をクリックしてウィンドウを閉じます。

印刷ドライバの初期化

クライアントに印刷ドライバをインストールする前に、ブランチ オフィスのクライアントが正常にドライバをインストールし、Microsoft Word や PowerPoint のようなアプリケーションから印刷できるように、ドライバを初期化する必要があります。一般に、初期化されていないドライバは正常にインストールされず、クライアントがそのドライバを使用して Microsoft Word や PowerPoint から印刷しようとするとエラーになります。

WAAS プリント サーバは Windows ドライバ コードをローカルに実行して自動的にドライバを初期化できないため、手動でドライバを初期化する必要があります。

手動で印刷ドライバを初期化するには、次の手順に従ってください。

ステップ 1　Windows クライアントから、管理ユーザとして WAAS プリント サーバにログインします。

ステップ 2　WAAS プリント サーバで、Printers and Faxes フォルダを開きます。

ステップ 3　共有プリンタを選択します。

ステップ 4　プリンタを右クリックし、[Properties] を選択します。

ステップ 5　[General] タブから、[Printing Preferences] を選択します。

ステップ 6　ページの向きを [Portrait] から [Landscape] へ変更し、[Apply] をクリックし、[OK] をクリックします。

ステップ 7　ページの向きを [Landscape] から [Portrait] へ戻し、[Apply] をクリックし、[OK] をクリックします。

ページの向きを変更することで、設定が正しく適用されることを確認します。

ステップ 8　（任意）今後クライアントにドライバをインストールするときに適用したい印刷デフォルト値を設定します。

ドライバの初期化が完了したら、続ける前に次の手順に従ってください。

ステップ 1　Samba プリント サーバ上でドライバがインストールされたことを確認し、サポートされないプリンタ機能を理解するため、印刷ドライバごとに print_diff ユーティリティを実行します。このユーティリティの詳細については、『*Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*』の「Print_Diff Utility」を参照してください。

ステップ 2　Samba と Windows 印刷ドライバの間のプロパティの違いを解決するため、印刷ドライバごとに print_fix ユーティリティを実行します。このユーティリティの詳細については、『*Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*』の「Print_Fix Utility」を参照してください。

ステップ 3　print_fix ユーティリティがドライバ プロパティを更新したあとプロパティを確認するには、印刷ドライバごとに print_diff ユーティリティを再び実行します。

ブランチ オフィスのクライアントへの WAAS プリント サーバの追加

WAAS プリント サーバを使用して印刷し、すでに印刷キューを作成した Windows クライアントは、Microsoft プリンタの追加ウィザードを実行する必要があります。

Windows クライアントにプリンタを追加するには、次の手順に従ってください。

ステップ 1　Windows クライアントの [Start] メニューから、[Printers and Faxes] を選択します。

ステップ 2　[Add a Printer] をクリックします。

プリンタの追加ウィザードが開きます。

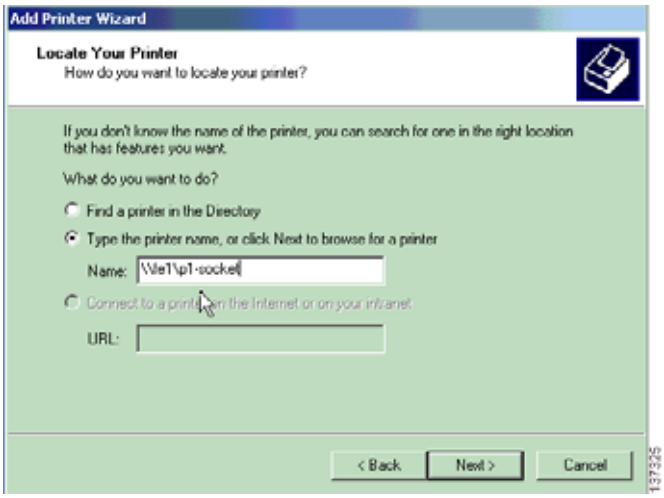
ステップ 3　[Next] をクリックします。

ステップ 4　オプション ボタンをクリックしてネットワーク プリンタを選択します。

ステップ 5　[Next] をクリックします。

[Locating Your Printer] ウィンドウが表示されます（図 13-9 を参照）。

図 13-9　[Locating Your Printer] ウィンドウ



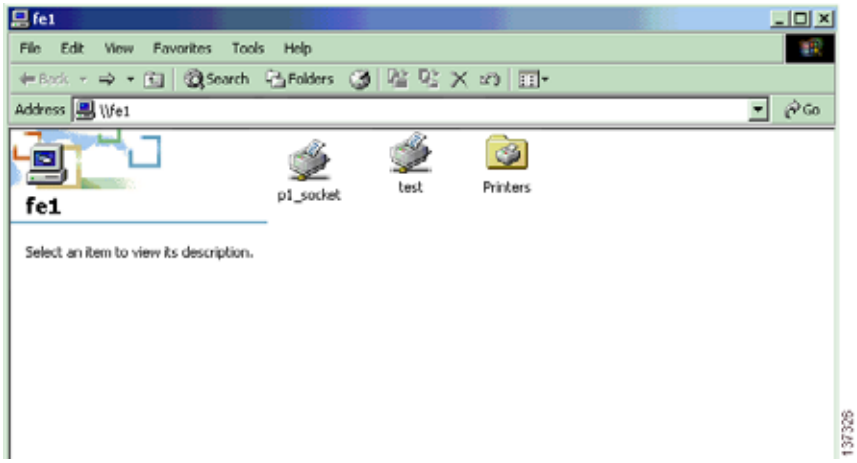
ステップ 6　次のいずれかの方法を使用してプリンタを選択し、[Next] をクリックします。

- プリンタ名を入力します。
- Active Directory で WAAS プリント サーバを検索します（プリンタが公開されている場合）。
- ドメインを参照して WAAS プリント サーバを見つけます。

（注） Windows がプリンタの追加ウィザードで WAAS 印刷キューを参照するとき、相互運用性問題が発生する場合があります。そのような場合は、明示的にプリンタ名を入力する必要があります。

プリンタのリストにプリンタが表示されます（図 13-10 を参照）。

図 13-10　正常なプリンタの追加



プリンタが正常に追加されると、印刷を開始できます。

印刷サービスの管理

ここでは、次の内容について説明します。

プリント サーバ詳細の表示

印刷サービスを設定すると、WAAS Central Manager GUI を使用して、ネットワークにインストールされている印刷ドライバと WAAS プリント サーバの詳細を表示できます。

表 13-6 で、WAAS Central Manager GUI から印刷ドライバとプリント サーバの詳細を表示する方法について説明します。

表 13-6　WAAS Central Manager GUI からのプリント サーバ詳細の表示

表示対象	作業手順
WAAS Central Manager のリポジトリに存在するすべてのドライバ	[Configure] > [Legacy Services] > [Print Drivers]
ドライバに関する詳細情報	[Configure] > [Legacy Services] > [Print Drivers] の後、ドライバをクリック。
特定の WAAS にインストールされているドライバ	[Configure] > [Legacy Services] > [Print Servers] の後、次の手順を実行。 1. WAAS プリント サーバを選択します。 2. [Driver] タブをクリックします。 この WAAS プリント サーバへ配信されるすべてのドライバのリストが表示されます。ドライバを配信する方法については、「WAAS プリント サーバへのドライバの配信」（P.13-20）を参照してください。
WAAS プリント サーバに関連付けられたプリンタ	[Configure] > [Legacy Services] > [Print Servers] の後、次の手順を実行。 1. WAAS プリント サーバを選択します。 2. [Printer] タブをクリックします（デフォルトでは表示）。 または、[My WAN] > [Manage Devices] へ進み、次の手順を実行します。 1. 印刷キューを表示したい WAAS プリント サーバを選択します。 2. ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Services] > [Printers] を選択します。
ネットワーク内の WAAS プリント サーバのリスト	[Configure] > [Legacy Services] > [Print Servers]

表 13-6　WAAS Central Manager GUI からのプリント サーバ詳細の表示 （続き）

表示対象	作業手順
特定のデバイス グループ内の WAAS プリント サーバのリスト	[My WAN] > [Manage Device Groups] を選択し、次の手順を実行します。 1. 表示したいプリント サーバを含むデバイス グループの横にある [Edit] アイコンをクリックします。 2. ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Services] > [Print Servers] を選択します。 選択したデバイス グループに関連付けられたプリント サーバのリストが表示されます。
ドライバ配信エラー	[Configure] > [Legacy Services] > [Print Servers] の後、[Failed] 列内の数値をクリック。
プリント サーバ エラー	[Configure] > [Legacy Services] > [Print] の後、[Print Server Errors] 列内の数値をクリック。
WAAS プリント サーバのステータス	[Configure] > [Legacy Services] > [Print Servers] の後、次の手順を実行。 1. [Time Stamp] 列を表示し、時刻が 5 分以上前でないことを確認します。各 WAAS プリント サーバは、System.monitoring.collectRate フィールドに指定した周期で、WAAS Central Manager へステータス レポートを送信します（「デフォルトのシステム設定プロパティの変更」（P.9-17）に説明されています）。WAAS プリント サーバがこのレポートを時間通りに送信できない場合、おそらくサーバが停止しています。 2. WAAS プリント サーバが過去 5 分以内にステータス レポートを送信していない場合は、次のようにします。 a. [Admin] > [Logs] > [System Messages] へ進みます。 b. メッセージ ログを検索して、WAAS プリント サーバが正しく動作していない理由を確認します。[Node Name] 列を使用すると、特定の WAAS プリント サーバに関する情報を迅速に見つけることができます。 （注）　ログ ファイルが最大サイズの 1 MB に達すると、CUPS ログ ファイルが切り替わります。

総合設定の構成

総合設定を使用すると、WAAS プリント サーバが、それが属するデバイス グループへ配信されたドライバを自動的にダウンロードするように設定できます。たとえば、WAAS プリント サーバがデバイス グループ DG1 に属し、総合設定が有効に設定されている場合、プリント サーバは、DG1 デバイス グループへ配信した任意のドライバを自動的にダウンロードします。ただし、同じプリント サーバで総合設定が無効に設定されている場合、プリント サーバは、DG1 デバイス グループへ配信したドライバをダウンロードしません。

WAAS Central Manager は、すでに WAE デバイスに存在するドライバを再配信しません。たとえば、WAAS プリント サーバが 2 つのデバイス グループ（DG1 と DG2）に属し、総合設定が有効に設定されている場合、プリント サーバは、両方のデバイス グループへ配信されているドライバの 1 つのインスタンスだけをダウンロードします。

WAAS プリント サーバをデバイス グループに追加すると、プリント サーバ用の総合設定が有効になり、デバイス グループに属するドライバが自動的にプリント サーバへ配信されます。総合設定が有効になっているときにデバイス グループからプリント サーバを削除すると、どのプリンタもドライバを使用していない場合、デバイス グループに割り当てられているすべてのドライバがプリント サーバから削除されます。

WAAS プリント サーバに総合設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

[Devices] ウィンドウが表示されます。

ステップ 2　総合設定を構成したい WAAS プリント サーバの横にある [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Acceleration] > [Legacy Services] > [Drivers] を選択します。

WAAS プリント サーバにインストールされているドライバのリストが表示されます。

ステップ 4　リストの一番上の [Yes] オプション ボタンをクリックして総合設定を有効にするか、[No] をクリックして総合設定を無効にします。

確認ダイアログボックスが表示されます。

ステップ 5　[OK] をクリックします。

総合設定を有効にすると、WAAS プリント サーバは、そのデバイス グループへ配信されているすべてのドライバのダウンロードを開始します。

Print Services Administration GUI の使用方法

Print Services Administration GUI を使用すると、特定の WAAS プリント サーバ用のさまざまな作業を実行できます。Print Services Administration GUI は、WAAS Central Manager GUI または WAE Manager GUI からアクセスできます。

（注）　Print Services Administration GUI にアクセスすると、プリンタの追加のような任意の作業を実行するときに、print admin アカウントのユーザ名とパスワードを入力するプロンプトが表示されます。WAE デバイス上の print admin アカウントを作成する方法については、「新しいアカウントの作成」（P.7-4）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。

Print Services Administration GUI の起動

Print Services Administration GUI は、WAE Device Manager GUI または WAAS Central Manager GUI から開くことができます。

WAE Device Manager GUI から Print Services Administration GUI を開くには、次の手順に従ってください。

ステップ 1　WAE Device Manager GUI から、[Cisco WAE] > [Configuration] を選択します。

ステップ 2　[Print Services] タブをクリックし、[Open] リンクをクリックします。Print Services Administration GUI が表示されます。

WAAS Central Manager GUI から Print Services Administration GUI を開くには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [Legacy Services] > [Print Servers] を選択します。

ネットワークにインストールされている WAAS プリント サーバのリストが表示されます。

ステップ 2　管理したい WAAS プリント サーバの横にある [Edit] アイコンをクリックします。

ステップ 3　ツールバーの [CUPS] アイコンをクリックします。

Print Services Administration GUI が表示されます。

プリンタの追加

WAAS プリント サーバにプリンタを追加する方法については、「WAAS プリント サーバへのプリンタの追加」（P.13-12）を参照してください。

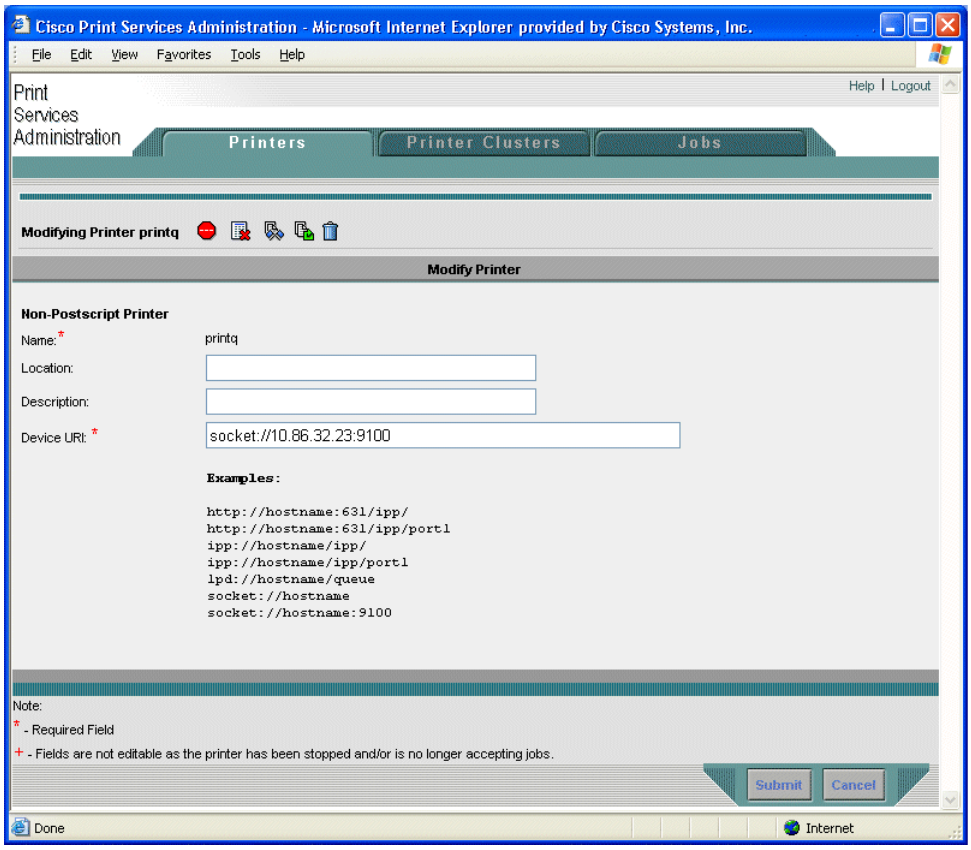
プリンタ設定の変更

既存のプリンタの設定を変更するには、次の手順に従ってください。

ステップ 1　Print Services Administration GUI の [Printers] タブから、変更するプリンタを選択します。

[Modifying Printer] ウィンドウが表示されます（図 13-11 を参照）。

図 13-11　プリンタ設定の変更



このウィンドウを使用して、位置、説明、およびデバイス URI 設定を変更します。[Name] フィールドは変更できません。また、対応するアイコンをクリックして、次の作業を実行できます。

- [Print a test page]（PostScript プリンタ専用）：テスト ページがプリンタへ送信されます。
- [Configure printer]（PostScript プリンタ専用）：開始および終了見出しページ オプションを設定できる [Configure Printer] ウィンドウが表示されます。詳細については、「印刷見出しの有効化」（P.13-31）を参照してください。
- [Stop/Start the printer]：プリンタを開始および停止できます。プリンタを停止する前に、確認を求める警告メッセージが表示されます。
- [Accept/Reject Jobs]：このプリンタへジョブを送信できるかどうかを決定できます。
- [Show Completed Jobs]：このプリンタ用に完了したジョブだけを表示する [Job Listing] ページを表示します。詳細については、「プリント ジョブの表示」（P.13-32）を参照してください。
- [Show Active Jobs]：このプリンタ用のアクティブなジョブだけを表示する [Job Listing] ページを表示します。詳細については、「プリント ジョブの表示」（P.13-32）を参照してください。
- [Delete this printer configuration]：このプリンタを削除できます。プリンタがプリンタ クラスタに属する場合、プリンタを削除すると、プリンタがクラスタから削除されます。プリンタがクラスタ内の唯一のプリンタである場合は、クラスタ自体が削除されます。

ステップ 2　次の設定のいずれかを変更します。

- [Location]：プリンタのユーザ指定位置（最大 127 文字）。
- [Description]：プリンタのユーザ指定の説明（最大 127 文字）。

- [Device URI]（必須）：デバイス URI は、次の形式のプリンタのアドレスです。

  protocol://server:port/queue

  最大 1024 文字まで使用できます。許可されるプロトコルは、lpd、socket、ipp、および http だけです。プロトコルの妥当性検査は実行されますが、それ以上の URI 文字列検査は実行されません。正しく入力するためのヒントとして、URI の例のリストが表示されます。特定のプリンタの情報（プリンタ ポート、プロトコル）は、プリンタ メーカーのマニュアル、プリンタのテスト ページ、またはプリンタの前面パネルから取得できます。

（注）　これらのフィールドは、プリンタが動作している場合に限り設定できます。プリンタが停止しているか、ジョブを拒否している場合、フィールドは読み取り専用になり、プリンタ ステータスを示すメッセージが表示されます。

ステップ 3　[Submit] をクリックして、変更を保存します。

印刷キューの変更は、1 分以内にクライアントに表示されます。

印刷見出しの有効化

各プリント ジョブ用の開始または終了見出しを有効にするには、次の手順に従ってください。

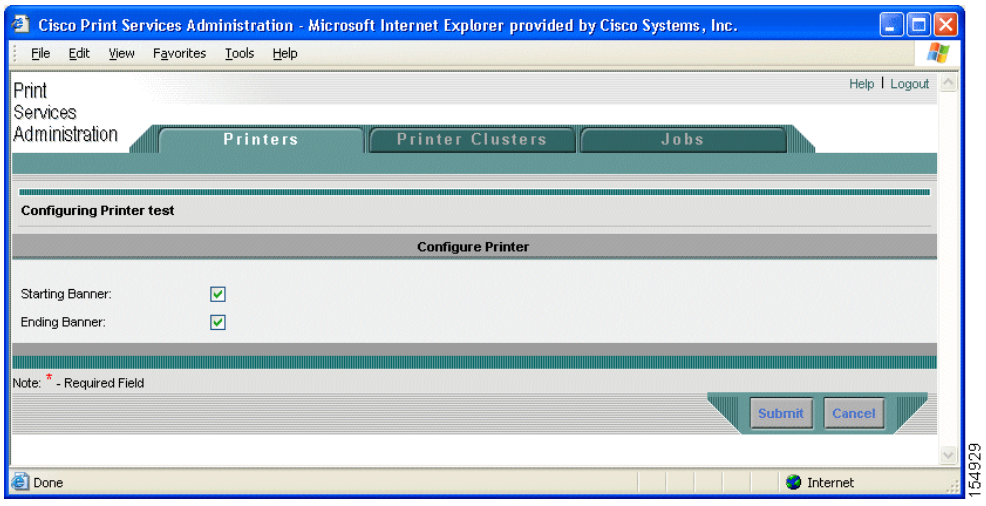
ステップ 1　Print Services Administration GUI の [Printers] タブから、変更するプリンタを選択します。

[Modifying Printer] ウィンドウが表示されます（図 13-11（P.13-30）を参照）。

ステップ 2　ツールバーの [Configure] ボタン（  ）をクリックします。

[Configuring Printer] ウィンドウが表示されます（図 13-12 を参照）。

図 13-12　開始および終了印刷見出しの設定



ステップ 3　有効にしたい見出しオプションの横にあるチェックボックスを選択します。

- [Starting Banner]：各ジョブ用の開始見出しの印刷を有効にします。
- [Ending Banner]：各ジョブ用の終了見出しの印刷を有効にします。

開始および終了見出しは、同じ情報を印刷します。これらのオプションを使用すると、ページ上の見出しの位置を選択できます。

ステップ 4　[Submit] をクリックします。

（注）　誤って PostScript 非対応プリンタを PostScript プリンタとして指定し、バナー ページを有効化した場合、プリンタは、「%!PS-Adobe-3.0. %%」のような文字を印刷してから、多数のブランク ページを印刷します。このメッセージは、プリンタ設定が正しくないことを示しています。有効なテスト ページと見出しページを印刷するには、プリンタの PostScript 機能を正しく指定する必要があります。

プリント クラスタの設定

プリント クラスタを設定する方法については、「プリンタ クラスタの追加」（P.13-15）を参照してください。

プリント ジョブの表示

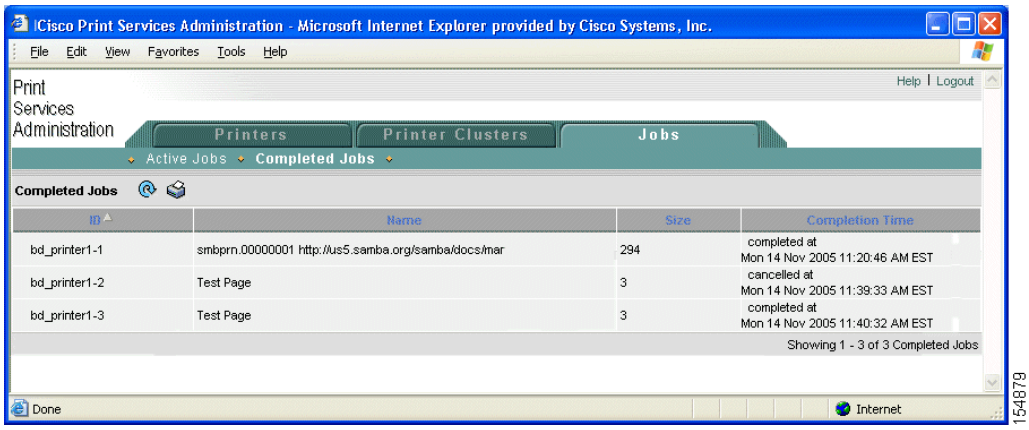
Print Services Administration GUI の [Jobs] タブを使用して、完了したジョブとアクティブなジョブのリストを表示します。

ページは、次のジョブ詳細を表示します。

- [ID]：プリンタ名とシーケンス番号を連結して生成されます。
- [Name]：印刷するために選択したジョブの名前。
- [Size]：ジョブのサイズ。
- [Status]：報告されたジョブのステータス。[Active Job Listing] ページだけで使用できます。
- [Completion Time]：報告されたジョブの完了日時。[Completed Job Listing] ウィンドウだけで使用できます。

[Completed Job Listing] ウィンドウ（図 13-13 を参照）は、まだスプール領域（/local/local1/spool/cups）にあるジョブだけを表示します。スプール領域は、最後に完了した 500 ジョブを保持し、サイズは 1GB に制限されています。完了ジョブ数の制限に達すると、完了した最新のジョブを保存するために最も古いジョブが削除されます。スプール領域からジョブを削除すると、[Completed Job Listing] ウィンドウに表示されなくなります。

図 13-13　[Completed Job Listing] ウィンドウ

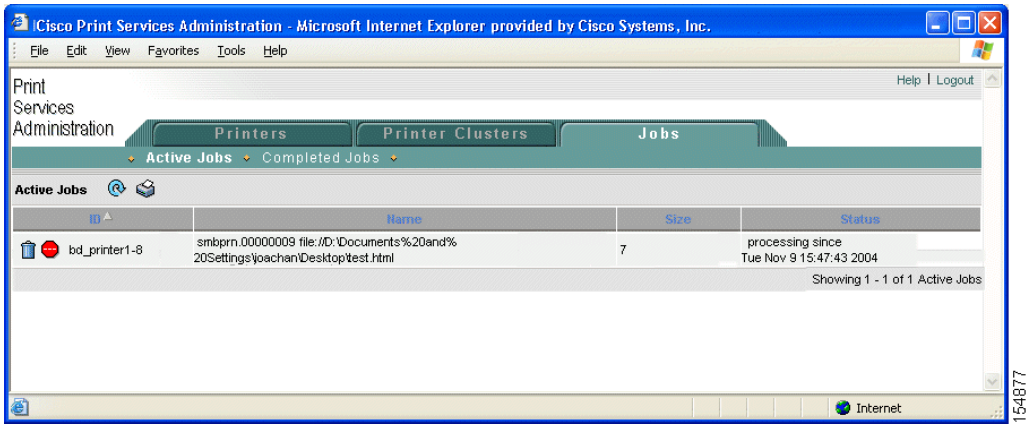


[Active Job Listing] ウィンドウ（図 13-14 を参照）では、ジョブの横にある対応するアイコンをクリックして次の作業を実行することもできます。

- [Stop Job]：選択したジョブを停止します。
- [Delete Job]：選択したジョブを削除します。

[Active Job Listing] ウィンドウは、完了していないまたは取り消されていないすべてのプリント ジョブを表示します。

図 13-14　[Active Job Listing] ウィンドウ：ジョブの停止と削除が可能



プリント サーバ ページ ログの表示

WAAS プリント サーバ ページ ログは /local/local1/logs/cups_access_log に保存されています。cups_access_log ファイルは、プリンタに送信される各ページを示します。行ごとに次の情報が含まれます。

printer user job-id date-time page-number num-copies job-billing hostname

次に、ログ エントリの例を示します。

DeskJet root 2 [20/May/2008:19:21:05 +0000] 1 0 acme-123 localhost

フィールドの説明は次のとおりです。

- *printer* フィールドには、ページを印刷したプリンタの名前が含まれます。ジョブをプリンタ クラスに送信する場合、このフィールドにはジョブを割り当てたプリンタの名前が含まれます。
- *user* フィールドには、印刷のためこのファイルを送信したユーザ（IPP requesting-user-name 属性）の名前が含まれます。
- *job-id* フィールドには、印刷中のページの番号が含まれます。CUPS サーバが開始すると、ジョブ番号は 1 にリセットされます。したがって、この番号が一意である必要はありません。
- *date-time* フィールドには、ページが印刷を開始した日時が含まれます。このフィールドの形式は、access_log ファイルの *date-time* フィールドと同じです。
- *page-number* および *num-pages* フィールドには、ページ番号とそのページを印刷したコピーの数が含まれます。コピーできないプリンタの場合、*num-pages* フィールドは常に 1 になります。
- *job-billing* フィールドには、IPP create-job または print-job 要求で提供された job-billing 属性のコピーが含まれます。何も提供されなかった場合は「-」になります。
- *hostname* フィールドには、印刷ジョブを送信したホスト（IPP job-originating-host-name 属性）の名前が含まれます。

印刷サービスのトラブルシューティング

トラブルシューティング問題は、次のカテゴリに分けて説明します。

- 「一般的な既知の問題」（P.13-34）
- 「ログインとアクセスの問題」（P.13-35）
- 「印刷問題の防止」（P.13-35）
- 「WAAS Central Manager と WAAS CLI 間の通信について」（P.13-36）

『*Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*』も参照してください。このマニュアルでは、多くの共通の Samba 印刷ドライバのインストールの問題に対する、印刷ユーティリティ ツールを使用したトラブルシューティングと解決の方法を説明しています。

一般的な既知の問題

WAAS 印刷サービスに関する一般的な既知の問題は、次のとおりです。

- Linksys デバイスは、IPP 1.1 印刷をサポートしていません。LPD プロトコルだけを使用してください。
- Linksys URI は、Linksys ユーザ ガイドに指定されているように、P1/2/3 の代わりに L1/2/3 を使用する必要があります。
- Windows クライアントで、Windows Print Queue ステータスが正しく更新されない場合があります。その場合は、F5 を押して手動で更新してください。
- Print Services Administration GUI でプリンタを追加すると、プリンタが Windows クライアント システムに表示されるまでに最大 1 分かかる場合があります。
- プリンタ ステータスとエラー メッセージが、印刷クライアントに表示されない場合があります。
- サポートされているプリンタは、IP ベースのネットワーク プリンタだけです。直接接続プリンタがある場合は、パラレル / シリアル /USB IP アダプタを使用してください。
- 中央レポジトリにドライバをロードするときに「Access is denied」エラーが表示される場合は、ドライバ ファイルが読み取り専用でなく、読み取り / 書き込みになっていることを確認してください。

- TDB ファイルが壊れていると、印刷問題が発生する場合があります。これらのファイルを検査するには、**windows-domain diagnostics** CLI コマンドを使用してください。このコマンドの詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

ログインとアクセスの問題

WAAS 印刷サービスを使用するとき、次のログインとアクセスの問題が発生する場合があります。

- 認証情報は、**syslog.txt** ファイルに入っています。**smb-conf** 詳細 コンフィギュレーション コマンドを使用して関連する smb.conf ディレクティブを追加すると、このファイルでログ レベルを上げることができます。詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。
- Windows から WAAS プリント サーバにアクセスできない場合は、Windows からログアウトし、次のコマンドを入力する必要があります。

  net use ¥¥*WAE_netbios_name*¥print$ * /USER:*username*

  WAE_netbios_name 値は、WAAS Central Manager デバイスの NetBIOS 名です。*username* は、「print admin 特権を持つアカウントの作成」（P.13-10）で指定したユーザ名です。
- admin ユーザがプリンタにドライバを追加できない場合、ユーザは Windows からログアウトし、次のコマンドを入力する必要があります。

  net use ¥¥*WAE_name*¥print$ * /USER:*username*

  WAE_name は、WAAS Central Manager デバイスのホスト名または IP アドレスです。*username* は、「個々の WAAS プリント サーバへの印刷ドライバのインストール」（P.13-19）で作成したアカウントの名前です。
- ユーザ名の問題を防止するには、次のガイドラインに従ってください。
  - WAAS Central Manager は、大文字と小文字を区別しないで固有のユーザ名を検査します（たとえば、「user1」と「User1」は同じであり、両方を追加することはできません）。
  - ユーザを作成するための CLI コマンドは大文字と小文字を区別するので、CLI を使用すると、user1 と User1 の両方を追加できます。

印刷問題の防止

WAAS 印刷サービスを使用するときに印刷問題を防止するには、次のガイドラインに従ってください。

- クラスタを使用するときは、常にクラスタ設定ウィンドウを使用し、クラスタ メンバーを個別に設定しないでください。メンバーがただ 1 つのクラスタでも、この処理により、動作が不安定になる場合があります。
- プリンタ クラスタには、同じ機能を持つプリンタを入れる必要があります。正しく設定しないと、印刷エラーになる場合があります。プリンタを削除すると、関連するクラスタからもそのプリンタが削除されます。
- 印刷テスト ページと見出しページは、PostScript プリンタだけでサポートされています。PostScript 非対応プリンタでは、正しく印刷されません。
- ポイント印刷が動作しない場合は、「WAAS プリント サーバへのドライバの配信」（P.13-20）の説明に従って、ドライバが正しく WAAS プリント サーバへ配信されていることを確認してください。
- ジョブは、最初から再度印刷されます。設定変更のために WAAS 印刷サービスが再起動すると、印刷中のジョブは再度印刷されます。

- ジョブが印刷されない場合は、次の手順を実行します。
  - プリンタが動作していることを確認します。
  - URI が正しく設定されていることを確認します。
  - プリンタが停止していない、または WAAS 印刷サービス設定でジョブが拒否されていないことを確認します。
  - CIFS アクセラレータとレガシー WAFS エッジ サービスのいずれかがプリント サーバ上で有効化され、稼動中であることを確認します。
  - **smbd** プロセスと **cupsd** プロセスの両方が動作していることを確認します。
  - スプール ディレクトリが一杯になっていないことを確認します。
  - プリンタ ドライバが正しく配信されていることを確認します。詳細については、「印刷ドライバの初期化」（P.13-23）を参照してください。
- WAAS プリント サーバの NetBIOS 名の変更を最小限に抑えます。NetBIOS 名を変更する必要がある場合は、WAAS Central Manager GUI または **windows-domain** CLI コマンドを使用します。
- PostScript ジョブが PostScript 非対応プリンタへ送信されると、「%!PS-Adobe-3.0...」メッセージが印刷されます。これを解決するには、プリンタを PostScript 非対応に設定するか、プリント ジョブを PostScript プリンタへ送信します。
- ブランチ内のプリンタで拡張機能用のチェックボックスを選択できない場合は、「Enable advanced printing features」が、クライアント プリンタ ドライバが Enhanced Metafile Spooling（EMF）を使用してプリント サーバと通信できるようにしている場合があります。

  WAAS プリント サーバは印刷形態に変換しないため、WAAS 印刷サービスは、EMF でなく、RAW スプールだけをサポートしています。クライアントは、プリント ジョブを印刷形態に変換し、プリンタがそのジョブを受信しているかのように、RAW 形式でジョブを送信します。

（注） RAW スプールのためにプリンタ機能は失われません。ただし、WAAS プリント サーバによる印刷形態への変換機能だけが失われます。RAW スプールでは、プリント サーバでなく、クライアントが、印刷形態への変換を実行します。

WAAS Central Manager と WAAS CLI 間の通信について

WAAS Central Manager または WAAS CLI を使用して印刷サービスを設定できるため、これらのツール間の次の通信に注意する必要があります。

（注） CUPS を再起動すると、一時的にプリント ジョブが中断されることがあります。

- 印刷サービスが動作していない場合、WAAS Central Manager GUI では、Print Services Administration GUI 用の [Open] リンクが無効になっています。WAAS Central Manager をロードしてから CLI で **no print-services enable** グローバル コンフィギュレーション コマンドを入力して印刷サービスを停止すると、印刷サービスにアクセスするときに「The page cannot be displayed」メッセージが表示されます。
- WAAS Central Manager GUI または CLI から設定を変更した場合は、Samba および CUPS ソフトウェアを再起動する必要があります。再起動時には、プリント サービスのアベイラビリティと動作が一時的に中断されます。設定に変更を加える前に、ユーザによる確認が必要です。

印刷サービス CLI コマンドの詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

CHAPTER 14

仮想ブレードの設定

この章では、WAE または WAVE デバイスに配置されたコンピュータ エミュレータである仮想ブレードを設定する方法について説明します。仮想ブレードを使用すると、WAE ハードウェアにインストールする追加のオペレーティング システムが使用するための WAE システム リソースを割り当てることができます。仮想ブレードが提供する隔離した環境で、サードパーティ アプリケーションをホスティングできます。たとえば、WAE デバイスに仮想ブレードを設定して、Windows の印刷およびドメイン検索サービスを実行できます。

仮想ブレードへの Windows のインストールと設定の詳細については、『*Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*』を参照してください。

仮想ブレードは、WAE および WAVE デバイスの特定のモデルだけでサポートされます。サポートされない WAE と WAVE デバイスでは、仮想ブレード設定画面は機能しません。

（注） この章では、ネットワークに存在する WAAS Central Manager、Wide Area Application Engine（WAE）、および Wide Area Virtualization Engine（WAVE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は WAE および WAVE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

仮想ブレードについて

WAAS 仮想ブレードは、WAE または WAVE デバイス内のコンピュータ エミュレータとして機能します。仮想ブレードにゲスト オペレーティング システムとアプリケーションをインストールして Wide Area Application Service（WAAS）システムと連動し、ネットワークのユーザに追加のサービスを提供できます。

（注）　WAAS 仮想ブレードは、Windows Server 2003 または Window Server 2008 オペレーティング システム、Active Directory、印刷サービス、DHCP、および DNS サービスだけをサポートします。他のオペレーティング システムとアプリケーションは仮想ブレードで動作しますが、WAAS 仮想ブレードは他のオペレーティング システムとアプリケーションをサポートしません。

仮想ブレードごとに、仮想化された CPU、メモリ、ファームウェア、ディスク ドライブ、CD ドライブ、およびネットワーク インターフェイス カードを装備しています。仮想ホスト ブリッジは、仮想ブレード、WAE デバイス、残りの WAAS ネットワークの間の通信を制御します。

（注）　WAE または WAVE デバイスに仮想ブレードを設定する場合、システム リソースが仮想ブレード用に予約されます。仮想ブレードがアクティブでない場合、これらのリソースは WAAS システムでは使用できません。これは、WAAS システムのパフォーマンスに影響を与えます。

ゲスト オペレーティング システムを観察および管理できるよう、各仮想ブレードには、VNC クライアントを使用した仮想ブレード コンソールへの接続を可能にする Virtual Network Computing（VNC; 仮想ネットワーク コンピューティング）サーバが含まれています。VNC クライアントには、仮想ブレード コンソールの IP アドレスが必要になります。これは、コロンの後に仮想ブレード番号が指定された WAAS デバイスの IP アドレスです（例：10.10.10.40:1）。

（注）　VNC クライアントでは、仮想ブレードに接続するポートを判断するために、仮想ブレード番号に 5900 が追加されます。たとえば、仮想ブレード 1 の場合、ポート 5901 となります。ポート番号を指定するもう 1 つの方法として、IP アドレスの後にスペースを入れ、続けて実際のポート番号を指定します。たとえば、10.10.10.40 5901 となります。

仮想ブレードを使用すると、次の操作を実行できます。

- 仮想ブレード環境のシステム特性の設定
- オペレーティング システムおよびアプリケーションのインストール
- 仮想ブレードの間でのネットワーク フローの設定
- 仮想ブレードの開始および停止

表 14-1 に、WAE で 1 つまたは複数の仮想ブレードをセットアップし、有効にするのに必要な手順の概要を示します。

表 14-1　仮想ブレード設定の概要

手順	説明
1. 仮想ブレードを使用して WAE を準備する。	WAE-674（必ずしも他のプラットフォームとは限りません）で仮想ブレード機能を有効にします。「仮想ブレードを使用するための準備」（P.14-3）を参照してください。
2. 仮想ブレード システム パラメータを設定する。	仮想ブレードにシステム リソースとインターフェイスをセットアップします。「仮想ブレードの設定」（P.14-4）を参照してください。
3. WAE で仮想ブレードを開始する。	仮想ブレードの実行を開始します。「仮想ブレードの有効化と無効化」（P.14-9）を参照してください。
4. ファイルを仮想ブレードに転送する。	仮想ブレードで使用するファイルを WAE ハードドライブにコピーします。「仮想ブレードへのディスク イメージのコピー」（P.14-11）および「仮想ブレードのバックアップと復元」（P.14-12）を参照してください。

仮想ブレードを使用するための準備

（注）　この手順は、WAE-674 デバイスだけに適用されます。仮想ブレードは、WAVE プラットフォームで常に有効になります。WAVE デバイスで仮想ブレードを無効にすることはできません。

WAE-674 で仮想ブレードを設定し、有効にする前に、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　設定する WAE デバイスの横にある [Edit] アイコンをクリックします。

（注）　仮想ブレードは、Central Manager デバイスではなく、アプリケーション アクセラレータ WAE だけで有効にできます。

（注）　個別の WAAS デバイスだけで仮想ブレードを設定できます。デバイス グループに仮想ブレードを設定することはできません。

ステップ 3　ナビゲーション ペインで、[Admin] > [Virtualization] > [General Settings] を選択します。[General Settings] ウィンドウが表示されます。

ステップ 4　[Enable Virtualization] を選択して、仮想化を有効にします。

（注）　仮想化が有効な場合、リカバリ CD を使用して WAAS を再インストールするだけで無効化できます。

ステップ 5　[Submit] をクリックします。

一般的な設定を変更することを確認するプロンプトが表示されます。表示されたら WAE を再起動します。再起動後、WAE にはディスク パーティションと仮想ブレードの使用向けに予約された他のリソースがあります。

（注）　リカバリ CD から WAE を復元しない限り、この変更を取り消すことはできません。

（注）　WAE デバイスに仮想ブレードを設定する場合、システム リソースが仮想ブレード用に予約されます。仮想ブレードがアクティブでない場合、これらのリソースは WAAS システムでは使用できません。これは、WAAS システムのパフォーマンスに影響を与えます。

ステップ 6　[OK] をクリックします。WAE が再起動します。

ステップ 7　仮想ブレードで実行するオペレーティング システムのディスクまたはイメージを検索します。CD-ROM を利用できること、またはディスク イメージを WAE ハード ドライブにコピーしていることを確認します（「仮想ブレードへのディスク イメージのコピー」（P.14-11）を参照）。

WAAS CLI で仮想化を有効にするには、**virtual-blade** グローバル コンフィギュレーション コマンドを使用します。

仮想ブレードの設定

ここでは、新しい仮想ブレードを設定する、または既存のブレードを編集する方法について説明します。仮想ブレード番号、説明、起動方式、ディスクの割り当て、CPU リスト、他のパラメータなどのリソースを設定できます。仮想ブレードを初めて設定した後は、変更可能なリソース パラメータだけがメモリとブリッジド インターフェイスであることに注意してください。仮想ブレード上のこれらのパラメータを変更するには、まず仮想ブレードを停止し、変更を行ってから仮想ブレードを開始します。

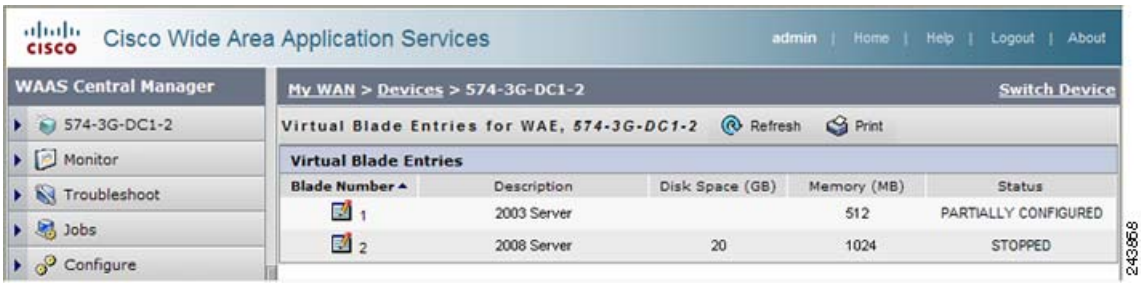
WAE または WAVE デバイスで仮想ブレードを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　設定する WAE デバイスの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Admin] > [Virtualization] > [Virtual Blades] を選択します。[Virtual Blade Entries] ウィンドウが表示されます（図 14-1 を参照）。

図 14-1　[Virtual Blade Entries List] ウィンドウ

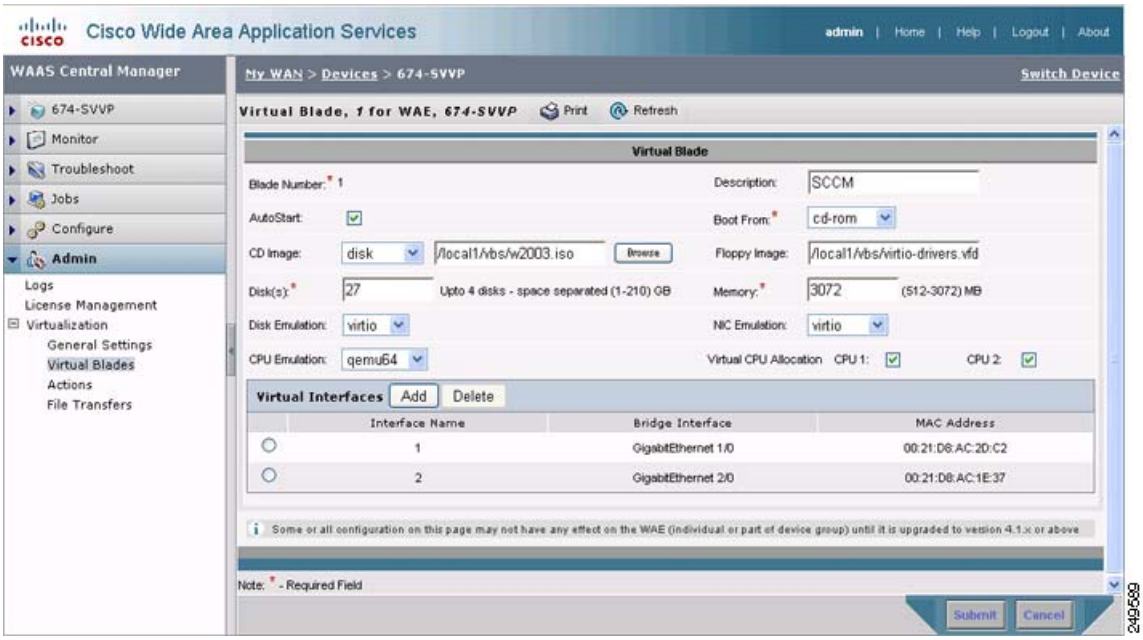


既存の仮想ブレードが [Virtual Blade Entries] リストに表示されます。

（注）　WAAS バージョン 4.1.1 で稼動する仮想ブレードのステータスは取得できないので、ステータスの列には [NOT AVAILABLE] と表示されます。ステータスを取得するには、[Virtual Blade Actions] ウィンドウ（図 14-4）を参照してください。

ステップ 4　設定する仮想ブレードの横にある [Edit] アイコンをクリックし、[Create] ボタンをクリックして、新しい仮想ブレードを作成します。[Virtual Blade] 設定ウィンドウが表示されます（図 14-2 を参照）。

図 14-2　[Virtual Blade] 設定ウィンドウ



ステップ 5　オペレーティング システムとアプリケーションを実行するよう、必要に応じて仮想ブレード システムを設定します。

a. 新しい仮想ブレードを作成する場合、[Blade Number] フィールドに作成する仮想ブレードの番号を入力します。

設定できる仮想ブレードの数は、使用している WAAS アプライアンスのモデルと、そのアプライアンスに搭載されているメモリの量によって異なります。

b. （任意）[Description] フィールドに、仮想ブレードの簡単な説明を入力します。

c. （任意）[Autostart] チェックボックスを選択して、WAE の起動時に自動的に起動するよう仮想ブレードを設定します。

d. 次のように、[Boot From] リストを使用して、起動元の仮想ブレードの送信元を選択します。

- 物理 CD または CD イメージ（/local1/vbs ディレクトリに保存されている .iso イメージ ファイル）から仮想ブレードを起動するには、[cd-rom]（デフォルト）を選択します。ゲスト OS のインストーラ CD から起動するには、ゲスト OS をインストールする前にこの選択を行います。
- WAE ハード ドライブにインストールされたゲスト OS から仮想ブレードを起動するには、[disk] を選択します。インストールしたゲスト OS から起動するには、ゲスト OS をインストールした後にこの選択を行います。

- 仮想ブレードを起動する [network] をネットワーク場所から選択します（お使いのネットワーク上で PXE が有効であることが必要）。同じソフトウェアのバージョンを多数の仮想ブレードにインストールする場合、または集中管理型ネットワークで OS 全体を保存および管理した状態で各仮想ブレードを起動する場合に、この選択を行います。

ネットワークを起動してゲスト OS をインストールする場合、以降の起動でディスクから起動する仮想ブレードを設定できます。これを行うには、仮想ブレードが実行されている状態で、**boot from** パラメータを変更します。

e. CD イメージ リストを使用して、CD イメージの場所を指定します。[Boot From] リストの [cd-rom] を指定した場合、[CD Image] の設定が必要となり、その設定によってブート イメージの場所が設定されます。[Boot From] リストの [disk] または [network] を指定した場合、[CD Image] の設定は任意となり、ゲスト OS で使用可能な CD-ROM イメージの場所が設定されます（ただし起動には使用されません）。[CD Image] は、次のように選択できます。

- [cd-rom] を選択して、WAE CD-ROM ドライブの物理 CD から CD イメージを読み込みます。
- [disk] を選択して、WAE ハード ドライブの ISO ファイルから CD イメージを読み込みます。[disk] を選択した場合は、[Browse] ボタンをクリックして、/local1/vbs ディレクトリから ISO ファイルを選択します。/local1/vbs ディレクトリにファイルが存在する場合に限り、[Browse] ボタンが表示されます。ISO ファイルを /local1/vbs ディレクトリにコピーする必要がある場合は、「仮想ブレードへのディスク イメージのコピー」（P.14-11）を参照してください。

[Virtual Blade Actions] ページで [Eject CD-ROM] をクリックし、続けて [Use CD-ROM] をクリックするか、ISO ディスク イメージを指定して [Set Image] をクリックすると、動作中に CD イメージを変更できます。

f. 仮想ブレード上の仮想フロッピー ディスク用にリソースを予約する場合、[Floppy Image] フィールドにフロッピー ディスク イメージのパス名を入力します。パスは必ず、/local1/vbs/*filename* とします。

g. [Disk Space] フィールドに、仮想ブレードに割り当てる仮想ハード ディスクのサイズをギガバイト単位で入力します。

図 14-2 のとおり、4 つのハード ディスク サイズをスペースで区切ることによって、仮想ブレードに最大 4 つの仮想ハード ディスクを設定できます。IDE ディスク エミュレーションを使用している場合、3 つめのディスクのサイズに 0 を指定する必要があります。これは、この IDE バスの位置が CD-ROM に使用されるためです。

注意 WAE デバイスに複数の仮想ディスクを設定している場合は、この Central Manager ウィンドウから、WAAS バージョン 4.1.1 を実行している WAE デバイスの仮想ブレードを管理しないでください。この Central Manager ウィンドウを使用して、すでに複数の仮想ハード ディスクが設定されており、WAAS バージョン 4.1.1 を実行している WAE デバイスの仮想ブレード設定の一部を変更すると、Central Manager によって最初のディスク以降のすべてのディスクのディスク設定が削除され、その他の仮想ディスクが消去されます。

WAAS バージョン 4.1.1 を実行している WAE デバイスについては、Central Manager から複数の仮想ハード ディスクを設定できません。代わりに、WAE の CLI から **disk** 仮想ブレード コンフィギュレーション コマンドを使用します。

h. [Memory] フィールドでは、仮想ブレードで使用可能な WAE メモリの量をメガバイト単位で割り当てます。

仮想ブレードに割り当てることができるメモリの量は、WAE または WAVE アプライアンスのメモリの量と、他の仮想ブレードに割り当てられているメモリの量によって異なります。1 つの仮想ブレードに割り当てることができる最小限のメモリは、512 MB です。

i. [Disk Emulation] リストでは、仮想ブレードが使用するディスク エミュレーションのタイプを選択します。[IDE] を選択します。

[IDE] は、IDE（ATA）タイプのディスク エミュレータを指定します。[virtio] は、仮想マシン用に最適化された汎用ディスク コントローラ エミュレータを指定します。

（注） virtio エミュレータを選択した場合、システムに paravirtualization（PV; 準仮想化）ドライバがインストールされている必要があり、この設定を検証する必要があります。ディスク エミュレーション向け virtio は試験用のみで提供されるため、サポートされる機能ではありません。

j. [NIC Emulation] リストでは、仮想ブレードが使用する NIC エミュレーションのタイプを選択します。[rtl8139]、[E1000]、または [virtio] を選択します。

[rtl8139] は Realtek ネットワーク カード エミュレータを指定し、[E1000] は Intel PRO/1000 ネットワーク カード エミュレータを指定し、[virtio] は仮想マシン用に最適化された汎用の NIC エミュレータを指定します。virtio エミュレータを選択した場合、システムに準仮想化（PV）ドライバをインストールする必要があります（「準仮想化ドライバのインストール」（P.14-9）を参照）。

k. [CPU Emulation] リストでは、仮想ブレードが使用する CPU エミュレーションのタイプを選択します。[qemu64]（64 ビット プロセッサ エミュレータの場合）または qemu32（32 ビット プロセッサ エミュレータの場合）を選択します。

l. [Virtual CPU Allocation] フィールドで、仮想ブレードに割り当てる各 CPU を選択します。

単一の CPU を選択すると、その CPU だけが使用されます。CPU リストに 2 つのエントリが含まれている場合、この 2 つの CPU が SMP モードで使用されます。2 つ以上の CPU の場合、奇数番号の仮想ブレードが CPU 1 を使用し、偶数番号の仮想ブレードが CPU 2 を使用します。

CPU は任意の組み合わせを設定できますが、仮想ブレードを有効にして SMP モードで 2 つ以上のコアを使用するようにすると、同じコアを使用する別の仮想ブレードを妨害する可能性があります。この場合、警告が表示されます。

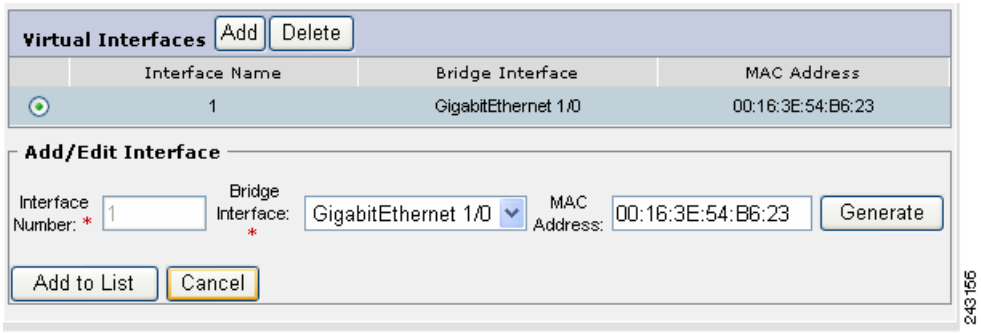
（注） 実行中の仮想ブレードは CPU 間で移動できますが、CPU を追加または削除するには仮想ブレードを停止する必要があります。

仮想ブレードで使用可能な数は、デバイスによって異なります。CPU を 2 つ備えたデバイスでは、1 つの CPU は常に WAAS ソフトウェア用に予約されています。CPU を 4 つ備えたデバイスでは、2 つの CPU は常に WAAS ソフトウェア用に予約されています。仮想ブレードを起動しない場合、すべての CPU が WAAS ソフトウェア用に使用されます。

ステップ 6　次のように実行して、仮想ブレードと WAE 上の物理インターフェイスの間で使用するインターフェイス ブリッジを設定します。

a. [Virtual Interfaces] ペインで、[Add] をクリックします。[Virtual Interface Add] ペインが表示されます（図 14-3 を参照）。

図 14-3　[Virtual Interface Add] 表示ペイン



b. [Interface Number] フィールドに、ブリッジングする仮想ブレード インターフェイスを入力します。有効な値は 1 または 2 です。

c. [Bridge Interface] リストでは、仮想ブレード インターフェイスのブリッジング先である物理 WAE インターフェイスを選択します。[GigabitEthernet] または [PortChannel] のいずれかを選択します。

d. [MAC Address] フィールドに、ブリッジド インターフェイスの MAC アドレスを入力するか、[Generate] をクリックして WAAS に MAC アドレスを生成させます。

e. [Add to List] をクリックして、仮想ブレード インターフェイスを仮想ブレード インターフェイス リストに追加します。

（注）　仮想ブレード コンソールにアクセスするには、ポート番号として指定された（コロンで区切られた）仮想ブレード番号のあるブリッジ インターフェイスの IP アドレスを使用します。たとえば、インターフェイス GigabitEthernet 1/0 をブリッジングし、その IP アドレスが 10.10.10.20 である場合、**10.10.10.20:1** を使用して、仮想ブレード 1 コンソールを取得します。

ステップ 7　ディスプレイ上のオプション ボタンをクリックして、仮想インターフェイスを選択します。

ステップ 8　[Submit] をクリックします。

WAAS CLI で仮想ブレードを設定するには、次のコマンドを使用します。

- **virtual-blade**（仮想ブレード コンフィギュレーション モードを開始します）
- **(config-vb) autostart**（autostart を有効にします）
- **(config-vb) boot**（起動デバイスを設定します）
- **(config-vb) cpu-list**（CPU リストを設定します）
- **(config-vb) description**（仮想ブレードの説明を入力します）
- **(config-vb) device**（CPU、NIC、およびディスク エミュレータを定義します）
- **(config-vb) disk**（仮想ブレード用にディスク スペースを割り当てます）
- **(config-vb) interface**（仮想ブレード インターフェイスを WAE のインターフェイスにブリッジングします）
- **(config-vb) memory**（仮想ブレード用にシステム メモリを割り当てます）
- **(config-vb) vnc**（仮想ブレードで、デフォルトで有効になっている VNC サーバを無効にします）

準仮想化ドライバのインストール

準仮想化ドライバをインストールするには、次の手順を実行します。

ステップ 1　準仮想化ドライバ ファイル（virtio-drivers.iso）を次の Cisco Software Center のサイトからダウンロードします。

http://www.cisco.com/public/sw-center/index.shtml

VirtIO ネットワーク ドライバは次の Windows オペレーティング システムで使用できます。

- Windows 2003 32 ビットおよび 64 ビット
- Windows Server 2008 32 ビットおよび 64 ビット
- Windows Server 2008 R2 64 ビット

ステップ 2　次のコマンドを使用して、virtio-drivers.iso をお使いの WAAS デバイスの /vbs ディレクトリへコピーします。

```
wae# copy ftp disk ip_address source_dir virtio-drivers.iso vbs/virtio-drivers.iso
```

上記で、*ip_address* および *source_dir* は、FTP サーバの IP アドレスと送信元ディレクトリです。

ステップ 3　次のコマンドを使用して、virtio-drivers.iso ファイルを仮想ブレードにロードします。

```
wae# virtual-blade 1 cd disk vbs/virtio-drivers.iso
```

ステップ 4　インストール用に次のドライバ方式のいずれかを選択します。

- 2008 または 2008 R2 64 ビット用にドライバをインストールするには、Windows コマンド シェルから次のコマンドを実行します。

  ```
  c:￥pnputil -i -a d:￥inf￥amd64￥Win2008￥netkvm.inf
  ```

- 2008 32 ビット用にドライバをインストールするには、Windows コマンド シェルから次のコマンドを実行します。

  ```
  c:￥pnputil -i -a d:￥inf￥i386￥Win2008￥netkvm.inf
  ```

- Windows 2003 用にドライバをインストールするには、Windows エクスプローラを開いて、次のいずれかのディレクトリへ移動します。
  - d:￥inf￥i386￥Win2003
  - d:￥inf￥amd64￥Win2003

  次に、netkvm.inf を右クリックして、ポップアップ コンテキスト メニューで [Install] を選択します。

仮想ブレードの有効化と無効化

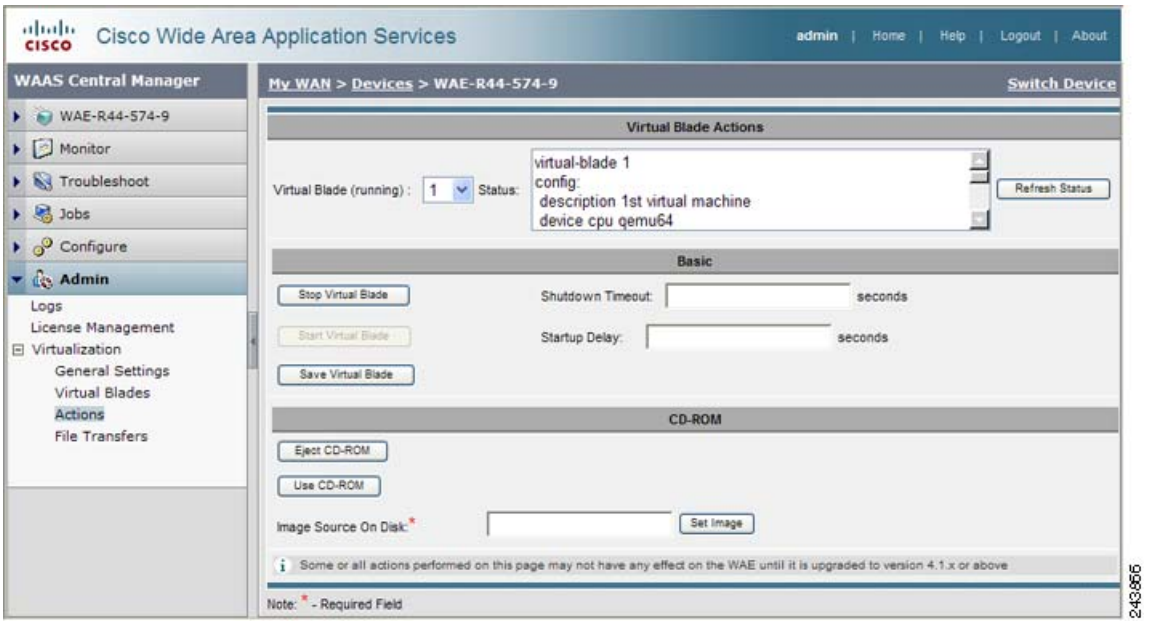
WAE で仮想ブレードを有効または無効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　設定する WAE デバイスの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Admin] > [Virtualization] > [Actions] を選択します。[Virtual Blade Actions] ウィンドウが表示されます（図 14-4 を参照）。

図 14-4　[Virtual Blade Actions] ウィンドウ



ステップ 4　[Virtual Blade] リストでは、有効または無効にする仮想ブレードを選択します。仮想ブレードのステータスが [Status] フィールドに表示されます。

[Virtual Blade] リストのデフォルトの選択は [All] です。[All] が選択されている場合、[Status] フィールドではすべての仮想ブレードの現在のステータスが表示されます。

ステップ 5　[Start Virtual Blade] をクリックして、選択した仮想ブレードを有効にします。

- （任意）[Startup Delay] フィールドに起動遅延を秒単位で入力します。

  起動遅延を使用すると、仮想ブレードが起動する前に VNC セッションをコンソールに接続できます。したがって、初回の起動を確認できます。

ステップ 6　[Stop Virtual Blade] をクリックして、選択した仮想ブレードを無効にします。

- （任意）[Stop Virtual Blade] ボタンをクリックした後に仮想ブレードをシャットダウンする時間を仮想ブレード オペレーティング システムに提供するには、[Shutdown Timeout] フィールドに値を秒単位で入力します。

  シャットダウン タイムアウトにより、オペレーティング システムが正常にシャットダウンできる遅延時間を提供します。オペレーティング システムにより、仮想ブレードがこの時間までにシャットダウンされなかった場合、WAAS はシャットダウンをキャンセルします。

  シャットダウン タイムアウトを 0 に設定すると、WAAS によりただちに強制シャットダウンが実行されます。強制シャットダウンは、実際のコンピュータの電源コードを引き抜くことに相当します。

  仮想ブレードで稼動するオープン プログラムのデータを失わないようにするには、オペレーティング システムにシャットダウンを実行させるのが安全です。

ステップ 7　変更した後は、[Refresh Status] をクリックして、仮想ブレードのステータスを更新します。

仮想ブレードの動作中は、[Eject CD-ROM] をクリックし、続けて [Use CD-ROM] をクリックするか（物理 CD の場合）、ISO ディスク イメージを指定して [Set Image] をクリックすることにより、CD イメージを変更できます。

（注）　仮想ブレードのオペレーティング システムはシャットダウンされず、WAAS デバイスをリブートすると再開されます。WAE または WAVE デバイスをリブートすると、WAAS ソフトウェアによって仮想ブレードが現在の状態で保存され、リブートが完了するとその状態に復元されます。

WAAS CLI で仮想ブレードを有効にするには、**virtual-blade** *n* **start** EXEC コマンドを使用します。仮想ブレードを無効にするには、**virtual-blade** *n* **stop** EXEC コマンドを使用します。

CD または仮想 CD イメージをイジェクトするには、**virtual-blade** *n* **cd eject** EXEC コマンドを使用します。

CD-ROM ドライブに挿入されている新しい CD を使用するには、**virtual-blade** *n* **cd cd-rom** EXEC コマンドを使用します。

WAE /local1/vbs ディレクトリから新しい CD ISO イメージを使用するには、**virtual-blade** *n* **cd disk** *pathname* EXEC コマンドを使用します。

仮想ブレードへのディスク イメージのコピー

WAAS デバイス ハード ドライブに保存されているディスク イメージから起動する場合、ディレクトリ /local1/vbs の下の仮想ブレード ステージング領域にそのイメージ ファイルをコピーする必要があります。

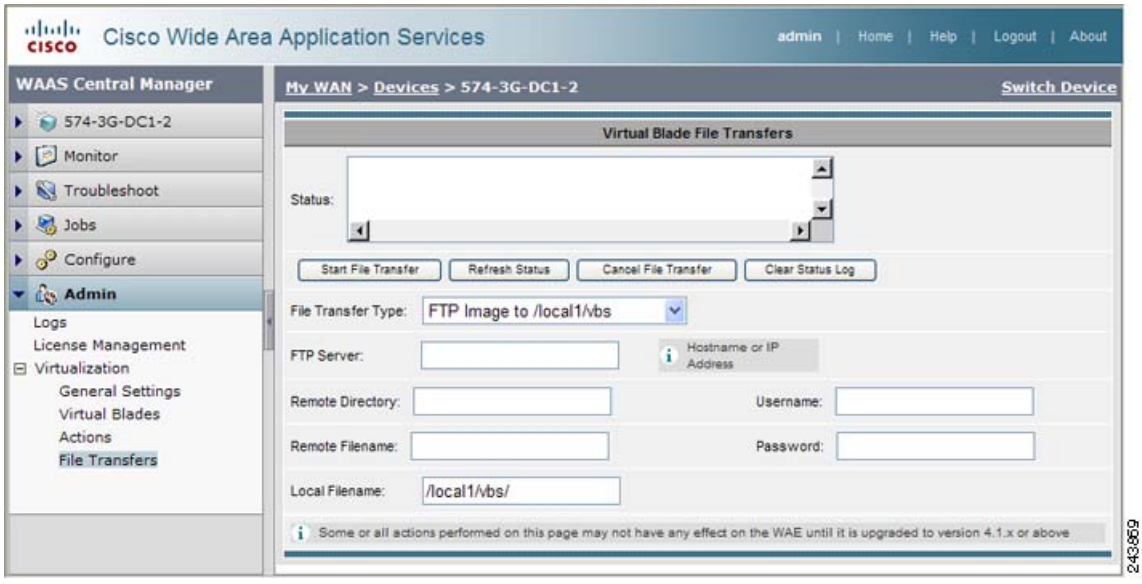
ディスク イメージ ファイルを WAE の /local1/vbs ディレクトリにコピーするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　設定する WAE デバイスの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Admin] > [Virtualization] > [File Transfers] を選択します。[Virtual Blade File Transfers] ウィンドウが表示されます（図 14-5 を参照）。

図 14-5　[Virtual Blade File Transfers] ウィンドウ



ステップ 4　[File Transfer Type] リストで、[FTP Image to /local1/vbs]（デフォルト）を選択します。

ステップ 5　[FTP Server] フィールドに、ディスク イメージが存在する FTP サーバの IP アドレスまたはホスト名を入力します。

ステップ 6　[Remote Directory] フィールドに、ディスク イメージが存在する FTP サーバ上のディレクトリへのパスを入力します。

ステップ 7　[Remote Filename] フィールドに、ディスク イメージのファイル名を入力します。

ステップ 8　[Username] フィールドと [Password] フィールドに、FTP サーバに有効なユーザ名とパスワードを入力します。

ステップ 9　[Local Filename] フィールドに、WAE デバイス上でディスク イメージの保存場所となるパスとファイル名を入力します。ディレクトリ パスは必ず、/local1/vbs/ とします。

ステップ 10　[Start File Transfer] をクリックして、ファイル転送を開始します。

ファイル転送ステータス情報が [Status] フィールドに表示されます。ステータス情報を更新するには、[Refresh Status] をクリックします。

ファイル転送をキャンセルするには、[Cancel File Transfer] をクリックします。

ステータス情報フィールドをクリアするには、[Clear Status Log] をクリックします。

仮想ブレード ディスクのバックアップや復元も、このウィンドウから実行できます。詳細については、「仮想ブレードのバックアップと復元」（P.14-12）を参照してください。

CLI を使用して、オペレーティング システム ISO イメージを仮想ブレードのディレクトリにコピーするには、**copy ftp disk** EXEC コマンドを使用します。たとえば、次のコマンドでは、ブート イメージ winserver.iso が FTP サーバ 10.10.10.200 の WAAS ディレクトリから WAE デバイスの仮想ブレード ディレクトリ（/local1/vbs/）にコピーされます。

```
wae# copy ftp disk 10.10.10.200 WAAS winserver.iso /local1/vbs/winserver.iso
```

仮想ブレードのバックアップと復元

仮想ブレードのディスク イメージのバックアップと復元を行うことができます。ディスク イメージは、仮想ブレード上で稼動する、ブート可能なオペレーティング システムおよびアプリケーションです。たとえば、仮想ブレードには印刷サービスを実行する Windows Server 2003 のディスク イメージがあります。

（注）　WAAS 仮想ブレードは、Windows Server 2003 または Window Server 2008 オペレーティング システム、Active Directory、印刷サービス、DHCP、および DNS サービスだけをサポートします。他のオペレーティング システムとアプリケーションは仮想ブレードで動作しますが、WAAS 仮想ブレードは他のオペレーティング システムとアプリケーションをサポートしません。

仮想ブレード ディスク イメージを FTP サーバにバックアップするには、次の手順に従ってください。

ステップ 1　バックアップする仮想ブレードを停止します。WAAS Central Manager から仮想ブレードを停止するには、「仮想ブレードの有効化と無効化」（P.14-9）で説明した手順を使用します。

ステップ 2　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 3　設定する WAE デバイスの横にある [Edit] アイコンをクリックします。

ステップ 4　ナビゲーション ペインで、[Admin] > [Virtualization] > [File Transfers] を選択します。[Virtual Blade File Transfers] ウィンドウが表示されます（図 14-5 を参照）。

ステップ 5　[File Transfer Type] リストから [Backup Virtual Blade to FTP] を選択します。

ステップ 6　[FTP Server] フィールドに、仮想ブレード ディスク イメージのバックアップを保存する FTP サーバの IP アドレスまたはホスト名を入力します。

ステップ 7　[Remote Directory] フィールドに、ディスク イメージをコピーする FTP サーバ上のディレクトリへのパスを入力します。

ステップ 8　[Remote Filename] フィールドに、ディスク イメージのファイル名を入力します。

ステップ 9　[Username] フィールドと [Password] フィールドに、FTP サーバに有効なユーザ名とパスワードを入力します。

ステップ 10　[Virtual Blade No.] フィールドに、バックアップする仮想ブレードの数を入力します。

ステップ 11　[Disk No.] フィールドに、バックアップする仮想ブレード ディスクの数を入力します。Microsoft Windows Server を実行する仮想ブレードをバックアップする場合は、常に **1** を入力します。

ステップ 12　[Start File Transfer] をクリックして、ファイル転送を開始します。

以前にバックアップした仮想ブレード ディスク イメージを復元する手順は上記と同様ですが、[File Transfer Type] リストでは [Restore Virtual Blade from FTP] を選択します。

WAE に仮想ブレードがすでに設定されている場合は、仮想ブレード ディスク イメージを復元する前にその仮想ブレードの設定を削除する必要があります。

（注）　仮想ブレード ディスク イメージを復元する前に仮想ブレードの設定を削除した場合は、復元操作の後に仮想ブレードを再設定する必要があります。復元操作によって設定されるディスク サイズを除き、すべての仮想ブレード システム パラメータを設定します。

ファイル転送ステータス情報が [Status] フィールドに表示されます。ステータス情報を更新するには、[Refresh Status] をクリックします。

ファイル転送をキャンセルするには、[Cancel File Transfer] をクリックします。

ステータス情報フィールドをクリアするには、[Clear Status Log] をクリックします。

CLI を使用して WAE 上の仮想ブレードのディスク イメージを FTP サーバにバックアップするには、**copy virtual-blade** EXEC コマンドを使用します。たとえば、次のコマンドは、ファイル file.img を仮想ブレード 1 のディスク 1 から FTP サーバ 10.75.16.234 に転送します。

```
wae# copy virtual-blade 1 disk 1 ftp 10.75.16.234 / file.img
```

ディスク イメージを WAE の仮想ブレードに復元するには、**copy ftp virtual-blade** EXEC コマンドを使用します。たとえば、次のコマンドは、ファイル file.img を FTP サーバ 10.75.16.234 から仮想ブレード 1 のディスク 1 に転送します。

```
wae# copy ftp virtual-blade 1 disk 1 10.75.16.234 / file.img
```

PART 4

WAAS ネットワークの保守、モニタリング、およびトラブルシューティング

CHAPTER 15

WAAS システムの保守

この章では、WAAS システムを保守するために実行する必要がある場合の作業について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

WAAS ソフトウェアのアップグレード

表 15-1 で、WAAS ソフトウェアを最新バージョンにアップグレードするために必要な手順の概要を説明します。

WAAS ネットワーク内のすべてのデバイスで、同じバージョンの WAAS ソフトウェアが稼動している必要があります。一部の WAAS デバイスで異なるバージョンのソフトウェアが稼動している場合、WAAS Central Manager は、最も高いバージョンである必要があります。これは、WAAS バージョン 4.0.x（WAAS Central Manager の最も低いバージョン）からの変更です。バージョンの相互運用性の制限の詳細については、『*Release Note for Cisco Wide Area Application Services*』を参照してください。

WAAS Central Manager（バージョン 4.2.1）は、より高いバージョン レベルの登録済み WAE デバイスを検出すると、マイナー アラームを生成して通知します。さらに、WAE デバイスが [device listing] ページに赤で表示されます。

WAAS Central Manager バージョン 4.2.1 は、バージョン 4.0.19 以降が稼動する WAE デバイスを管理します。一部の WAAS Central Manager ページ（新機能付き）は、4.2.1 より低いバージョンが稼動する WAAS デバイスには適用されません。ページなどの設定を変更すると、設定は保存されますが、デバイスをバージョン 4.2.1 にアップグレードするまで有効になりません。

（注）　WAAS バージョン 4.2.1 は、WAAS デバイスが 4.0.19 より低いソフトウェア バージョンを実行している、混在バージョン WAAS ネットワークでの実行はサポートしません。バージョン 4.0.17 以前を実行している WAAS デバイスがある場合、まずこれらをバージョン 4.0.19（または以降の 4.0.x バージョン）にアップグレードしてから、バージョン 4.2.1 をインストールする必要があります。最初にすべての WAE をバージョン 4.0.19（または以降の 4.0.x バージョン）にアップグレードしてから、すべての WAAS Central Managers をバージョン 4.0.19（または以降の 4.0.x バージョン）にアップグレードします。WAAS Central Manager からバージョン 4.2.1 へのアップグレードを開始します。

一部の旧リリースから特定のリリースへのアップグレードだけがでサポートされています。目的のリリースへのアップグレードがサポートされていないリリースを稼動している WAAS デバイスでは、このデバイスをサポートされている中間のリリースにアップグレードしてから、最終的な目的のリリースにアップグレードします。アップグレードがサポートされているバージョンの詳細については、『*Release Note for Cisco Wide Area Application Services*』でアップグレードするソフトウェアのバージョンを参照してください。

表 15-1　WAAS ソフトウェアをアップグレードするためのチェックリスト

作業	追加情報と手順
1. WAAS ネットワークで動作している現在のソフトウェア バージョンを決定する。	Cisco.com にアクセスしたときに新しいバージョンをダウンロードする必要があるかどうかを知るために、現在使用しているソフトウェア バージョンを確認します。 詳細については、「現在のソフトウェア バージョンの決定」（P.15-3）を参照してください。
2. Cisco.com から新しい WAAS ソフトウェア バージョンを取得する。	Cisco.com にアクセスして新しいソフトウェア バージョンをダウンロードし、ローカル FTP サーバまたは HTTP サーバにこのファイルを配置します。 詳細については、「Cisco.com からの最新のソフトウェア バージョンの入手」（P.15-3）を参照してください。
3. WAAS Central Manager で新しいソフトウェア バージョンを登録する。	WAAS Central Manager がファイルにアクセスできるように、新しいソフトウェアファイルの URL を登録します。 詳細については、「WAAS Central Manager GUI でのソフトウェア ファイルの位置の指定」（P.15-4）を参照してください。
4. WAAS Central Manager をアップグレードする。	プライマリおよびスタンバイ WAAS Central Manager をアップグレードします。 詳細については、「WAAS Central Manager のアップグレード」（P.15-6）を参照してください。
5. デバイス グループを使用して WAAS デバイスをアップグレードする。	WAAS Central Manager をアップグレードしたら、デバイス グループに属するすべての WAAS デバイスをアップグレードします。 詳細については、「デバイス グループを使用した複数のデバイスのアップグレード」（P.15-9）を参照してください。
6. ソフトウェア バージョン ファイルを削除する。	WAAS ネットワークを完全にアップグレードしたあと、必要な場合はソフトウェア ファイルを削除できます。 詳細については、「ソフトウェア ファイルの削除」（P.15-9）を参照してください。

WAAS ソフトウェアをバージョン 4.2.1 から低いバージョンにダウングレードまたはロール バックする場合、最初に WAE デバイスを、次にスタンバイ Central Manager（該当する場合）を、最後にプライマリ Central Manager をダウングレードまたはロールバックします。ダウングレードの詳細については、『*Release Note for Cisco Wide Area Application Services*』でお使いのソフトウェア バージョンを参照してください。

現在のソフトウェア バージョンの決定

特定のデバイスで動作している現在のソフトウェア バージョンを表示するには、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウは、表示される各デバイス用のソフトウェア バージョンを表示します。

また、[Devices] ウィンドウで、デバイスの名前の横にある [Edit] アイコンをクリックすることもできます。[Device Dashboard] ウィンドウが表示され、そのデバイスのソフトウェア バージョンが表示されます。

（注） ソフトウェア バージョンは、ソフトウェア アップグレードが正常に完了するまで、アップグレードされません。ソフトウェアアップグレードの進行中に表示されるバージョン番号は、基本バージョンであり、アップグレードされるバージョン番号ではありません。

あるいは、特定のデバイス用のナビゲーション ペインで、[Troubleshoot] > [CLI Commands] > [Show Commands] を選択します。[version] を選択し、[Submit] をクリックします。2 番めのポップアップ ウィンドウが表示され、**show version** コマンドの CLI 出力が表示されます。

Cisco.com からの最新のソフトウェア バージョンの入手

Cisco.com から最新の WAAS ソフトウェア バージョンを入手するには、次の手順に従ってください。

ステップ 1　好みのブラウザを起動し、次のサイトを開きます。

http://www.cisco.com/cisco/web/download/index.html

ステップ 2　[Application Networking Services] 製品カテゴリをクリックします。

ステップ 3　プロンプトが表示されたら、指定されたユーザ名とパスワードを使用して Cisco.com にログインします。[Download Software] ウィンドウが表示され、使用可能なソフトウェア製品が表示されます。

ステップ 4　[Wide Area Application Software] フォルダをクリックして展開します。

ステップ 5　[Cisco Wide Area Application Services (WAAS) Software] ページを選択します。

ステップ 6　ダウンロードする WAAS ソフトウェア バージョンへのリンクを選択します。ページの右側に、[Software Download] ペインが表示されます。

ステップ 7　ダウンロードするファイルの横にある [Download Now] ボタンをクリックします。または、複数のファイルを一度にダウンロードする場合は、[Add to cart] ボタンをクリックしてから、[Download Cart] リンクをクリックしてカートを表示します。

アップグレードするデバイスのソフトウェア イメージとして正しいタイプ（Universal（WAAS-4.2.*x*.*x*-K9.bin）または Accelerator only（WAAS-4.2.*x*.*x*-K9.AA.bin））を必ず指定してください。

[Download Cart] が表示されます。

ステップ 8　[Proceed With Download] ボタンをクリックしてファイルをダウンロードします。

- Cisco.com から初めてソフトウェアをダウンロードする場合は、[Encryption Software Export Distribution Authorization] フォームが表示されます。
  - フォームに入力し、[Submit] をクリックします。Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy が表示されます。
  - ポリシーを読み、[Accept] をクリックします。Cisco End User Software License Agreement が表示されます。
- すでに [Encryption Software Export Distribution Authorization] フォームに記入し、Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy を読んで承諾した場合、これらのフォームは表示されません。その代わりに、[Proceed With Download] ボタンをクリックすると、Cisco End User Software License Agreement が表示されます。

ステップ 9　Cisco End User Software License Agreement を読み、[Agree] ボタンをクリックします。[Download option] ウィンドウが表示されます。

ステップ 10　[Download Manager Option] リンク（Java を使用）または [Non Java Download Option] リンクを選択します。

- [Download Manager Option] を選択した場合、Java ウィンドウが表示されます。初めて Download Manager を使用するときには、セキュリティ警告を表示するポップアップ ウィンドウが表示されます。[Run] ボタンをクリックして、Download Manager をインストールしてください。[Select Location] ポップアップ ウィンドウで、ダウンロード場所を選択し、[Open] をクリックします。ダウンロードが開始されます。[Download Manager] ウィンドウのコントロールを使用してダウンロードの一時停止、再開、またはキャンセルを実行できます。
- [Non Java Download Option] を選択した場合、ファイルをダウンロードするためのリンクが含まれたポップアップ ウィンドウが表示されます。ソフトウェア ファイル リンクを右クリックしてソフトウェアをダウンロードし、[Save Link As] または [Save Link Target As] オプションを使用して、FTP サーバまたは HTTP サーバにファイルを保存します。

ステップ 11　次の項の説明に従って、WAAS Central Manager GUI でソフトウェア ファイルの位置を登録します。

WAAS Central Manager GUI でのソフトウェア ファイルの位置の指定

WAAS ソフトウェアをアップグレードするには、最初に WAAS Central Manager GUI で WAAS ソフトウェア ファイルの位置を指定し、ソフトウェア ファイル設定を構成する必要があります。WAAS Central Manager GUI のソフトウェア ファイル設定フォームは、ソフトウェア ファイル（.bin）を定義し、これを使用して、ソフトウェア ファイルを入手する方法、デバイスに事前配置するか、直接ダウンロードするかどうかを指定できます。

WAAS ソフトウェアには次に示すとおり 2 つのタイプがあります。

- Universal : Central Manager および Application Accelerator 機能が含まれます。このタイプのソフトウェア ファイルを使用して、Central Manager または Application Accelerator デバイスをアップグレードできます。
- Accelerator only : Application Accelerator 機能のみが含まれます。このタイプのソフトウェア ファイルを使用して、Application Accelerator デバイスのみをアップグレードできます。Application Accelerator を Central Manager に変更する場合は、Universal ソフトウェア ファイルをインストールし、デバイスを再ロードし、デバイス モードを central-manager に変更した後、改めてデバイスを再ロードすることが必要です。また、Accelerator only イメージには kdump 分析機能は含まれません。

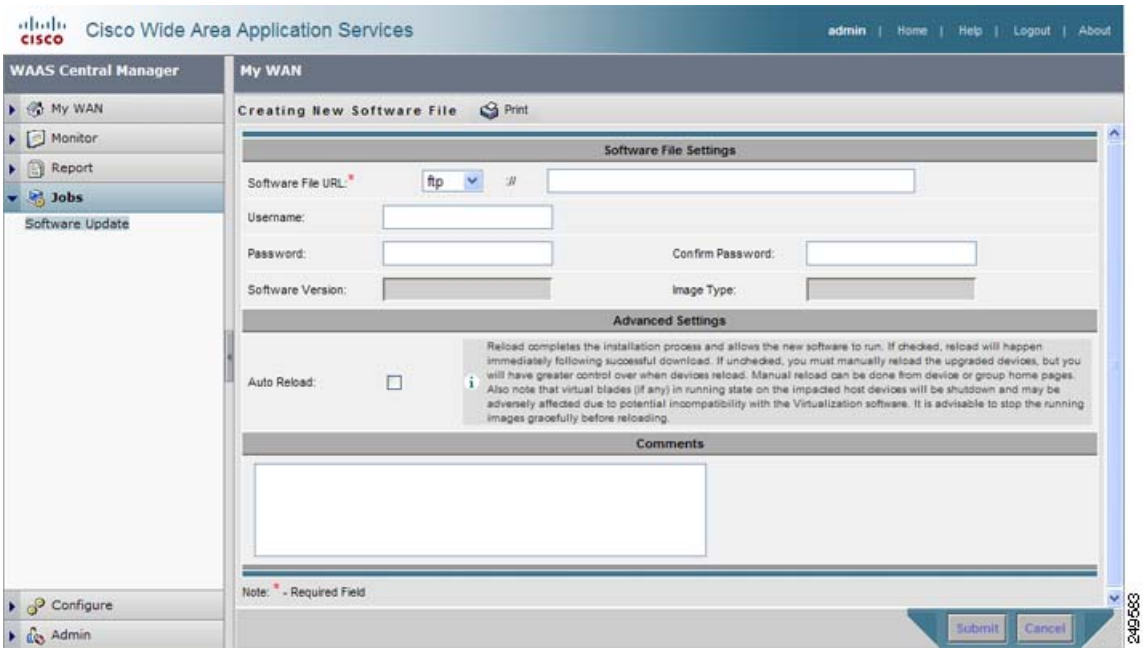
ソフトウェア ファイル設定フォームを構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Jobs] > [Software Update] を選択します。

ステップ 2　タスクバーの [Create New Software File] アイコンをクリックします。

[Creating New Software File] ウィンドウが表示されます（図 15-1 を参照）。

図 15-1　[Creating New Software File] ウィンドウ



ステップ 3　次のように、[Software File URL] フィールドで、新しい WAAS ソフトウェア ファイルの位置を指定します。

a.　ドロップダウン リストから、プロトコル（[http] または [ftp]）を選択します。

b.　Cisco.com からダウンロードした .bin ソフトウェア ファイルの URL を入力します。たとえば、有効な URL は次のようになります。

http://internal.mysite.com/waas/*WAAS-4.x.x.x-K9*.bin

この場合、WAAS-4.x.x-K9 は、ソフトウェア アップグレード ファイルの名前です（通常、ファイル名にはバージョン番号が含まれます）。

URL が、アップグレード対象のデバイスの正しいタイプのソフトウェア イメージ（Universal または Accelerator only）を示していることを確認します。

ステップ 4　サーバがユーザ ログイン認証を要求する場合は、[Username] フィールドにユーザ名を入力し、[Password] フィールドにログイン パスワードを入力します。[Confirm Password] フィールドに、同じパスワードを入力します。

[Software Version] および [Image Type] フィールドは編集できません。ユーザが設定を送信し、イメージが検証された後、これらのフィールドには自動的に値が入力されます。

ステップ 5　[Advanced Settings] セクションで [Auto Reload] チェックボックスを選択して、ソフトウェアをアップグレードしたときにデバイスを自動的に再ロードするようにします。このボックスを選択しない場合は、ソフトウェアをアップグレードしたあとで、アップグレード プロセスを完了するためにデバイスを手動で再ロードする必要があります。

（注） デバイスの再ロード時に、デバイス上で実行されている仮想ブレードがシャットダウンされ、Virtualization ソフトウェアと互換性がないために悪影響を受ける可能性があります。したがって、再ロードする前にイメージの実行を正常に終了する必要があります。

ステップ 6　（任意）表示されるフィールドに、コメントを入力します。

ステップ 7　[Submit] をクリックします。

ソフトウェア イメージ ファイルが検証され、[Software Version] および [Image Type] フィールドには、イメージ ファイルから抽出された適切な情報が入力されます。

注意 ブラウザが WAAS Central Manager GUI 用のユーザ名とパスワードを保存するように設定されている場合、ブラウザは、[Creating New Software File] ウィンドウのユーザ名フィールドとパスワード フィールドにユーザ名とパスワードを自動入力します。[Submit] をクリックする前に、これらのフィールドをクリアする必要があります。

これで、使用するソフトウェア ファイルが、WAAS Central Manager に登録されます。ソフトウェアのアップグレードまたはダウングレードを実行するときは、登録した URL が [Update Software] ウィンドウで使用できる選択肢の 1 つになります。

CLI からデバイスを再ロードするには、**reload** EXEC コマンドを使用します。

（注） 登録済みソフトウェア ファイルのリストを表示している際に、ソフトウェア ファイルの [Image Type] カラムに [Unknown] と表示される場合は、このソフトウェア ファイルがバージョン 4.2.1 以前の WAAS で追加されたことを示します。このような不明なソフトウェア ファイルを使用する場合は、再送信する必要があります。ファイルの横にある [Edit] アイコンをクリックして [Modifying Software File] ウィンドウを開き、[Submit] ボタンをクリックしてファイルを再送信します。

WAAS Central Manager のアップグレード

WAAS ネットワークのソフトウェアをアップグレードするときは、WAE デバイスをアップグレードする前に WAAS Central Manager から開始します。

（注） WAAS バージョン 4.0.x の場合、WAAS Central Manager の前に WAE デバイスをアップグレードします

プライマリおよびスタンバイ WAAS Central Manager デバイスは、同じバージョンの WAAS ソフトウェアを使用する必要があります。同じではない場合、スタンバイ WAAS Central Manager はこれを検出し、プライマリ WAAS Central Manager から受信する設定更新を処理しません。スタンバイ WAAS Central Manager が異なるバージョン レベルであることがわかると、プライマリ WAAS Central Manager（バージョン 4.2.1）はスタンバイ WAAS Central Manager を [device listing] ページに赤で表示します。

プライマリ WAAS Central Manager を使用してソフトウェア アップグレードを実行する場合は、最初にスタンバイ WAAS Central Manager をアップグレードし、次にプライマリ WAAS Central Manager をアップグレードする必要があります。また、ソフトウェアをアップグレードする前に、プライマリ WAAS Central Manager 用のデータベース バックアップを作成し、データベース バックアップ ファイルを安全な場所にコピーすることを推奨します。

WAAS Central Manager デバイスには、このアップグレード手順を使用します。また、このアップグレード手順を使用して、WAAS Central Manager のあとに一度に 1 台ずつ WAAS デバイスをアップグレードすることもできます。

1 台のデバイスでソフトウェアを別の WAAS ソフトウェア リリースへアップグレードするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　アップグレードする Central Manager デバイスの [Edit] アイコンをクリックします。

[Device Dashboard] ウィンドウが表示されます。

ステップ 3　アップグレードする予定のバージョンが、デバイスで動作していないことを確認します。

ステップ 4　[Jobs] > [Update Software] ボタンをクリックします。

[Software Update] ウィンドウが表示されます。

ステップ 5　ファイル名の横にあるオプション ボタンをクリックして、[Software Files] リストからソフトウェア ファイル URL を選択します。

Central Manager デバイスをアップグレードしているので、リストには Universal のイメージ タイプのソフトウェア ファイルだけが表示されます。使用可能なイメージがない場合は、「WAAS Central Manager GUI でのソフトウェア ファイルの位置の指定」（P.15-4）の手順に従って、ソフトウェア ファイルを作成する必要があります。

ステップ 6　[Submit] をクリックし、[OK] をクリックして決定を確認します。

[Devices]：一覧ウィンドウが再表示されます。このウィンドウから、アップグレードの進行状況をモニタできます。

[Software Version] 列に、ソフトウェア アップグレードのステータス メッセージが表示されます。これらの中間メッセージは、WAAS デバイスのシステム ログにも書き込まれます。アップグレード ステータス メッセージの説明については、表 15-2 を参照してください。

ステップ 7　プライマリ WAAS Central Manager をアップグレードするのに Internet Explorer ブラウザを使用する場合、キャッシュをクリアしてからブラウザを閉じ、WAAS Central Manager へのブラウザ セッションを再起動します。

ブラウザのキャッシュは、Internet Explorer の [Tools] > [Internet Options] > [General] タブでクリアできます。

（注）　WAAS Central Manager GUI を正常に機能させるには、Internet Explorer でキャッシュをクリアしてから、WAAS Central Manager へのブラウザ セッションを再起動します。

（[Creating New Software File] ウィンドウで [Auto Reload] を選択すると）アップグレード手順が完了したときに WAAS Central Manager がリブートし、一時的にデバイスおよびグラフィカル ユーザ インターフェイスにアクセスできなくなる場合があります。

表 15-2　アップグレード ステータス メッセージ

アップグレード ステータス メッセージ	条件
「Pending」	要求が WAAS Central Manager からデバイスへまだ送信されていない、あるいはデバイスが要求の受信を肯定応答していません。
「Downloading」	ソフトウェア ファイルをダウンロードする方法を決定中です。
「Proceeding with Download」	ソフトウェア ファイルをダウンロードする方法が直接ダウンロードに決定されます。ソフトウェア ファイルの直接ダウンロード要求を処理します。
「Download in Progress (Completed ...)」	ソフトウェア ファイルの直接ダウンロードを処理しています。「Completed」は、処理されたメガバイト数を示します。
「Download Successful」	ソフトウェア ファイルの直接ダウンロードが正常終了しました。
「Download Failed」	ソフトウェア ファイルの直接ダウンロードを処理できません。トラブルシューティングが必要です。デバイスのシステム メッセージ ログを参照してください。一度に複数のデバイスをアップグレードしている場合、ソフトウェア ファイルをホスティングしているサーバが要求で負荷がかかりすぎると、ダウンロードでエラーが発生する可能性があります。[Retry] リンクが表示されたら、このリンクをクリックしてアップグレードを再試行します。
「Proceeding with Flash Write」	ソフトウェア ファイルをデバイスのフラッシュ メモリに書き込む要求が出されました。
「Flash Write in Progress (Completed ...)」	デバイスのフラッシュ メモリへの書き込みを処理しています。「Completed」は、処理されたメガバイト数を示します。
「Flash Write Successful」	ソフトウェアのフラッシュ書き込みが正常終了しました。
「Reloading」	ソフトウェア アップグレードを完了するために、デバイスを再ロードする要求が出されました。デバイスが数分間オフラインになる場合があります。
「Reload Needed」	デバイスを再ロードする要求が出されていません。ソフトウェア アップグレードを完了するために、手動でデバイスを再ロードする必要があります。
「Cancelled」	ソフトウェア アップグレード要求が中止された、または前のソフトウェア アップグレード要求が CLI から取り消されました。
「Update Failed」	ソフトウェア アップグレードを完了できませんでした。トラブルシューティングが必要です。デバイスのシステム メッセージ ログを参照してください。一度に複数のデバイスをアップグレードしている場合、ソフトウェア ファイルをホスティングしているサーバが要求で負荷がかかりすぎると、アップグレードでエラーが発生する可能性があります。[Retry] リンクが表示されたら、このリンクをクリックしてアップグレードを再試行します。

デバイス グループを使用した複数のデバイスのアップグレード

（注）　この手順は、WAE デバイス専用です。WAAS Central Manager デバイスは、デバイス グループを使用してアップグレードできません。

複数のデバイスで最新の WAAS ソフトウェア リリースにアップグレードするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Device Groups] を選択します。

[Device Groups] 一覧ウィンドウが表示され、WAAS ネットワーク内のすべてのデバイス グループが表示されます。

ステップ 2　アップグレードするデバイス グループの横にある [Edit] アイコンをクリックします。

[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Jobs] > [Software Update] を選択します。

[Software Update for Device Group] ウィンドウが表示されます

ステップ 4　ファイル名の横にあるオプション ボタンをクリックして、[Software File URL] リストからソフトウェア ファイル URL を選択します。使用可能なイメージがない場合は、「WAAS Central Manager GUI でのソフトウェア ファイルの位置の指定」（P.15-4）の手順に従って、ソフトウェア ファイルを作成する必要があります。

アップデートするデバイスが多数あり、同じサイズのソフトウェア ファイルを使用してネットワーク帯域幅を保存したい場合は、イメージ タイプが Accelerator only（Universal イメージよりサイズが小さい）のソフトウェア ファイルを指定します。後で、Accelerator only デバイスから Central Manager に変更する場合は、Universal ソフトウェア ファイルをインストールし、デバイスを再ロードし、デバイス モードを central-manager に変更した後、改めてデバイスを再ロードすることが必要です。

ステップ 5　[Submit] をクリックします。

アップグレードの進行状況を表示するには、[Devices] ウィンドウ（[My WAN] > [Manage Devices]）へ進み、[Software Version] 列でソフトウェア アップグレード ステータス メッセージを表示します。これらの中間メッセージは、WAAS デバイスのシステム ログにも書き込まれます。アップグレード ステータス メッセージの説明については、表 15-2 を参照してください。

ソフトウェア ファイルの削除

WAAS デバイスを正常にアップグレードすると、WAAS システムからソフトウェア ファイルを削除できます。

（注）　システムをダウングレードする必要がある場合に備えて、ソフトウェアを削除する前に数日待つことを推奨します。

WAAS ソフトウェア ファイルを削除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Jobs] > [Software Update] を選択します。

ステップ 2　削除するソフトウェア ファイルの横にある [Edit] アイコンをクリックします。[Modifying Software File] ウィンドウが表示されます。

ステップ 3　タスクバーの [Trash] アイコンをクリックします。

ソフトウェア ファイルを削除するかどうかを確認するプロンプトが表示されます。

ステップ 4　[OK] をクリックします。

選択したソフトウェア ファイルが WAAS ネットワークから削除された [Software Files] 一覧ウィンドウへ戻ります。

WAAS システムのバックアップと復元

ここでは、次の内容について説明します。

WAAS Central Manager データベースのバックアップと復元

WAAS Central Manager デバイスは、WAAS ネットワーク全体のデバイス設定情報を Centralized Management System（CMS）データベースに保存します。システムの信頼性を向上するために、手動で CMS データベースの内容をバックアップできます。

CMS データベース バックアップは、WAAS Central Manager が他の WAAS デバイスと通信するために使用するアーカイブ データベース ダンプ、WAAS Central Manager 登録情報、およびデバイス情報を含む独自の形式にあります。CMS データベース バックアップ ファイルは、プライマリおよびスタンバイ WAAS Central Manager デバイス間で交換できません。そのため、プライマリ WAAS Central Manager からのバックアップ ファイルを使用して、スタンバイ WAAS Central Manager を復元することはできません。

WAAS Central Manager 用の CMS データベースをバックアップするには、**cms database backup** EXEC コマンドを使用します。データベースをバックアップするには、バックアップ ファイルを保存したいリモート サーバの位置、パスワード、およびユーザ ID を指定する必要があります。

（注）　CMS データベースのバックアップでは、印刷ドライバをバックアップしません。Central Manager データベースのバックアップを行う場合、WAAS 印刷サービスを使用しているならば印刷ドライバを再インストールする必要があります。

CMS データベースをバックアップし、復元するには、次の手順に従ってください。

ステップ 1　次の例に示すように、WAAS Central Manager GUI デバイスで、**cms database backup** コマンドを使用して、CMS データベースをファイルにバックアップします。

```
CDM# cms database backup
creating backup file with label 'backup'
backup file local1/cms-db-7-22-2008-17-36_4.1.3.0.1.dump is ready. use 'copy' commands to
move the backup file to a remote host.
```

（注）　バックアップ ファイルには、cms-db-*date-timestamp_version*.dump という形式の名前が自動的に設定されます。たとえば、cms-db-7-22-2008-17-36_4.1.3.0.1.dump です。なお、タイムスタンプは、24 時間形式（HH:MM）で秒は表示されません。

ステップ 2　**copy disk ftp** コマンドを使用して、リモート サーバにファイルを保存します。

次の例に示すように、このコマンドは、ローカル ディスクからリモート FTP サーバへファイルをコピーします。

```
CDM# cd /local1
CDM# copy disk ftp 10.86.32.82 /incoming cms-db-7-22-2008-17-36_4.1.3.0.1.dump
cms-db-7-22-2008-17-36_4.1.3.0.1.dump

Enter username for remote ftp server:ftp
Enter password for remote ftp server:*******
Initiating FTP upload...
Sending:USER ftp
10.86.32.82 FTP server (Version wu-2.6.1-18) ready.
Password required for ftp.
Sending:PASS *******
User ftp logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (10,86,32,82,112,221)
Sending:CWD /incoming
CWD command successful.
Sending PASV
Entering Passive Mode (10,86,32,82,203,135)
Sending:STOR cms-db-7-22-2008-17-36_4.1.3.0.1.dump
Opening BINARY mode data connection for cms-db-7-22-2008-17-36_4.1.3.0.1.dump.
Transfer complete.
Sent 18155 bytes
```

ステップ 3　次のように CMS データベースを復元します。

a. CMS サービスを無効にします。

```
CDM# no cms enable
```

（注）　CMS サービスを停止すると、WAAS Central Manager GUI が無効になります。CMS サービスが無効になると、現在この GUI にログインしているすべてのユーザが自動的にログアウトされます。

b. 既存の CMS データベースを削除します。

```
CDM# cms database delete
```

c. バックアップ ファイルから、CMS データベースの内容を復元します。

```
CDM# cms database restore cms-db-7-22-2008-17-36_4.1.3.0.1.dump
```

（注）　復元後、バックアップの作成以降に Central Manager に登録された WAE は、Central Manager から切断されます。バックアップ ファイルには、これらの WAE に関する情報がないからです。これらの WAE をオンラインにするには、Central Manager でこれらの WAE の登録を取り消してから、再び登録します。切断された各 WAE で、次のコマンドを使用します。

```
WAE# cms deregister force
WAE# configure
WAE(config)# cms enable
```

d. Central Manager で CMS サービスを有効にします。

```
CDM# cms enable
```

WAE デバイスのバックアップと復元

システム障害の発生に備えて、各 WAAS デバイスのデータベースを定期的にバックアップしてください。

（注）　この項で説明するバックアップと復元方式は、WAAS Central Manager として設定されていない WAE デバイスだけに適用されます。WAAS Central Manager デバイスをバックアップする方法については、「WAAS Central Manager データベースのバックアップと復元」（P.15-10）を参照してください。

次のいずれかの方法を使用して、個々の WAE デバイスのデータベースをバックアップし、復元できます。

- WAE Device Manager：WAE Device Manager を使用してデバイスのデータベースをバックアップし、復元する方法については、「設定ファイルのバックアップ」（P.10-7）を参照してください。
- CLI：次のコマンドを使用して、デバイスのデータベースをバックアップし、復元できます。
  - **wafs backup-config**：ファイル サーバ、プリンタ、およびユーザ用の設定を含むレガシー WAFS システム設定全体をファイルに保存します。このコマンドを使用したあとで、WAE を再び登録することを強く推奨します。
  - **wafs restore-config**：指定したバックアップ ファイルに基づいて設定を復元します。このコマンドは、自動的にリロード機能を実行します。
  - **copy running-config**：現在動作しているネットワーク設定を起動時設定に保存します。

さらに、任意の時点に、ディスクとフラッシュ メモリからユーザデータを削除し、アプライアンスにキャッシュされているすべての既存ファイルを削除して、WAE を出荷時のデフォルト設定に復元できます。ネットワーク設定値などの基本構成情報は維持できます。リブート後には、Telnet および Secure Shell（SSH; セキュア シェル）を介してアプライアンスにアクセスできます。

（注）　ソフトウェア アップグレードが適用されている場合、復元プロセスは、工場出荷時のデフォルト設定ではなく、現在インストールされているバージョンのデフォルト設定へ戻します。

CLI から WAE を工場出荷時のデフォルト設定または現在の設定のデフォルトに戻すには、**restore factory-default** [**preserve basic-config]** EXEC コマンドを使用します。

CLI コマンドの詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

Cisco WAAS ソフトウェア リカバリ CD の使用

ソフトウェア リカバリ CD-ROM は、WAE ハードウェア デバイスに同梱されています。ここでは、インストールされているソフトウェアに障害が発生した場合に、ソフトウェア リカバリ CD-ROM を使用して、システム ソフトウェアを再インストールする手順について説明します。

注意　ソフトウェア リカバリ CD を受け取ったあとでソフトウェアをアップグレードした場合は、CD-ROM ソフトウェア イメージを使用すると、システムがダウングレードされる場合があります。

WAAS ソフトウェアには、3 つの基本コンポーネントがあります。

- ディスクに基づくソフトウェア
- フラッシュに基づくソフトウェア
- ハードウェア プラットフォーム クッキー（フラッシュ メモリに保存）

WAAS ソフトウェアが正しく動作するには、このすべてのコンポーネントが正しくインストールされている必要があります。

ソフトウェアは、シスコシステムズが提供する 2 種類のソフトウェア イメージに含まれています。

- ディスクとフラッシュ メモリ コンポーネントを含む .bin イメージ（Universal バージョンの WAAS ソフトウェア）
- フラッシュ メモリ コンポーネントのみを含む .sysimg イメージ

  対応するディスクに基づくソフトウェアがない、WAAS フラッシュ メモリに基づくソフトウェアだけを含むインストールは、限られたモードで起動し、動作するため、完全なインストールを完了する前にさらにディスクを設定できます。

  復旧用の .sysimg コンポーネントが提供されているため、ディスクの内容を変更しないでフラッシュ メモリだけを修復できます。

（注）　使用されるシステム イメージは、デバイスによって異なります。WAVE-274/474/574 および WAE-674/7341/7371 デバイス（64 ビット プラットフォーム）では、WAAS-4.x.x.x-K9.x86_64.sysimg という名前のシステム イメージが使用されます。その他すべてのデバイスでは、WAAS-4.x.x.x-K9.sysimg という名前のシステム イメージが使用されます。

これらのオプションは、ソフトウェア リカバリ CD-ROM のインストーラ メニューで使用できます。

- オプション 1：[Configure Network]：.bin イメージが CD-ROM でなく、ネットワークに存在する場合（古い CD-ROM を使用して新しいソフトウェアをインストールする場合など）は、このオプションを選択して .bin イメージをインストールする前にネットワークを設定する必要があります。

  このオプションは、ネットワークから .sysimg ファイルをインストールする場合、自動的に実行されます。

- オプション 2 : [Manufacture Flash] : このオプションは、フラッシュ メモリを検査し、有効でない場合、シスコの標準レイアウトになるように自動的にフラッシュ メモリを再フォーマットします。再フォーマットが必要な場合、新しいクッキーが自動的にインストールされます。

  このオプションは、.bin または .sysimg のインストールの一環として自動的に実行されます。

- オプション 3 : [Install Flash Cookie] : このオプションは、ハードウェア プラットフォーム固有のクッキーを生成し、フラッシュ メモリにインストールします。このオプションを使用する必要があるのは、マザーボードの交換やシステム間のフラッシュ メモリ カードの移動のようなハードウェア コンポーネントに変更があった場合のみです。

  このオプションは、必要な場合、フラッシュ製造工程で .bin または .sysimg のインストールの一環として自動的に実行されます。

- オプション 4 : [Install Flash Image from Network] およびオプション 5 : [Install Flash Image from CD-ROM] : これらのオプションにより、フラッシュ メモリ .sysimg だけをインストールでき、ディスク内容は変更されません。新しいシャーシにお客様の古いディスクを搭載するときなどに使用できます。

  これらのオプションは、自動的にフラッシュ検査を実行し、必要な場合はハードウェア クッキーをインストールします。ネットワークからインストールするときは、まだ実行していない場合にネットワークを設定するためのプロンプトが表示されます。

- オプション 6 : [Install Flash Image from Disk] : このオプションは、将来の拡張用の予備で、使用できません。

- オプション 7 : [Recreate RAID device] : このオプションは WAE-7341、WAE-7371、および WAE-674 デバイスに限り表示され、RAID アレイを再作成します。

- オプション 8 : [Wipe Out Disks and Install .bin Image] : このオプションは、WAAS ソフトウェアをインストールするために望ましい手順を提供します。

注意　オプション 8 は、デバイス内のすべてのディスク ドライブから内容を消去します。

  このオプションは、次の手順を実行します。

  a. フラッシュ メモリのフォーマットが、シスコ仕様に適合していることを確認します。適合している場合は、ステップ b へ進みます。適合していない場合、システムは、フラッシュ メモリを再フォーマットして Cisco ファイル システムをインストールし、ハードウェア プラットフォーム固有のクッキーを生成しインストールします。

  b. すべてのドライブからデータを消去します。

  c. ディスクにデフォルトの Cisco ファイル システム レイアウトを再作成します。

  d. .bin イメージからフラッシュ メモリ コンポーネントをインストールします。

  e. .bin イメージからディスク コンポーネントをインストールします。

- オプション 9 : [Exit (Eject and reboot)] : このオプションは、CD-ROM を取り出し、デバイスをリブートします（WAE-7341、WAE-7371、および WAE-674 デバイスを除いたすべての WAE デバイスの場合、このオプションはオプション 8 になります）。

ソフトウェア リカバリ CD-ROM を使用して WAE アプライアンスにシステム ソフトウェアを再インストールするには、次の手順に従います。

ステップ 1　アップグレードする WAE アプライアンスにシリアル コンソールを接続し、コンソールを次の手順に使用します。

ステップ 2　WAE デバイスの CD ドライブに、WAAS 4.1.x CD-ROM を挿入します。

ステップ 3　WAE をリブートします。WAE が起動すると、次のメニューが表示されます。

```
Installer Main Menu:
  1. Configure Network
  2. Manufacture flash
  3. Install flash cookie
  4. Install flash image from network
  5. Install flash image from cdrom
  6. Install flash image from disk
  7. Recreate RAID device (WAE-674/7341/7371 only)
  8. Wipe out disks and install .bin image
  9. Exit (Eject and reboot)
Choice [0]:
```

オプション 7 は WAE-7341、WAE-7371、および WAE-674 デバイスに限り表示されます。

ステップ 4　オプション 2 を選び、フラッシュ メモリを準備します。

この手順では、デバイスのクッキーを準備し、WAAS ソフトウェアにより使用されていたネットワーク設定も取得します。このネットワーク設定はフラッシュ メモリに保存され、WAAS ソフトウェアがインストール後に起動するときに、ネットワークを設定するために使用されます。

ステップ 5　オプション 3 を選び、前の手順で準備したフラッシュ クッキーをインストールします。

ステップ 6　オプション 5 を選び、CD-ROM からフラッシュ イメージをインストールします。

ステップ 7　（任意）WAE-7341、WAE-7371、または WAE-674 デバイスで動作している場合、オプション 7 を選択して RAID アレイを再作成します。

ステップ 8　オプション 8 を選択し、ディスクを拭いてバイナリ イメージをインストールします。

この手順では、ディスクを消去することによりディスクを準備します。WAAS 4.1.x イメージがインストールされます。

ステップ 9　オプション（WAE モデルに応じて 8 または 9）を選択し、WAE をリブートします。

WAE のリブート後、WAAS 4.1.x ソフトウェアが動作します。WAE には最小限のネットワーク設定があり、さらに設定するために、端末コンソール経由で WAE にアクセスできます。

Cisco アクセス ルータにインストールされた NME-WAE ネットワーク モジュールにシステム ソフトウェアを再インストールするには、次の手順に従います。

ステップ 1　NME-WAE モジュールがインストールされた Cisco ルータにログインし、NME-WAE モジュールをリロードします。

```
router-2851> enable
router-2851# service-module integrated-Service-Engine 1/0 reload
```

ステップ 2　すぐにモジュールのセッションを開きます。

```
router-2851# service-module integrated-Service-Engine 1/0 session
```

ステップ 3　モジュールのリロード中、起動フェーズ 3 では次のオプションが表示されます。指示に従って、*** を入力します。

```
[BOOT-PHASE3]: enter `***' for rescue image: ***
```

ステップ 4　復旧用イメージ ダイアログが表示されます。次の例は、復旧用イメージ ダイアログの使用方法を示しています（ユーザ入力は太字フォントで表記されています）。

```
This is the rescue image.  The purpose of this software is to let
you install a new system image onto your system's boot flash
device.  This software has been invoked either manually
```

```
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.

To download an image from network, this software will request
the following information from you:
    - which network interface to use
    - IP address and netmask for the selected interface
    - default gateway IP address
    - FTP server IP address
    - username and password on FTP server
    - path to system image on server

Please enter an interface from the following list:
   0: GigabitEthernet 1/0
   1: GigabitEthernet 2/0
enter choice: 0
Using interface GigabitEthernet 1/0

Please enter the local IP address to use for this interface:
[Enter IP Address]: 10.1.13.2

Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.240

Please enter the IP address for the default gateway:
[Enter Gateway IP Address]: 10.1.13.1

Please enter the IP address for the FTP server where you wish
to obtain the new system image:
[Enter Server IP Address]: 10.107.193.240

Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: username

Please enter the password for username 'username' on FTP server:

Please enter the directory containing the image file on the FTP server:
[Enter Directory on server (e.g. /)]: /

Please enter the file name of the system image file on the FTP server:
[Enter Filename on server]: WAAS-4.1.7.10-K9.sysimg


Here is the configuration you have entered:

Current config:
          IP Address: 10.1.13.2
             Netmask: 255.255.255.240
     Gateway Address: 10.1.13.1
      Server Address: 10.107.193.240
            Username: username
            Password: *********
     Image directory: /
      Image filename: WAAS-4.1.7.10-K9.sysimg

Attempting download...
Downloaded 15821824 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
.......................................................................... done.
```

```
Finished writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system.
```

ステップ 5　モジュールのリブート後、HTTP サーバから .bin イメージをインストールします。

```
NM-WAE-1# copy http install 10.77.156.3 /waas WAAS-4.1.1-k9.bin
```

ステップ 6　モジュールをリロードします。

```
NM-WAE-1# reload
```

モジュールのリブート後、WAAS 4.1.x ソフトウェアが動作します。

RAID ペアの正常な再ビルドの確認

WAE デバイスをリブートする前に、すべての RAID ペアが再ビルドされたことを確認する必要があります。デバイスの再ビルド中にリブートすると、ファイル システムが損傷するおそれがあります。

レガシー WAFS コア サービスまたはエッジ サービスを有効にするか、**restore factory-default** コマンドを使用するか、ハード ディスク ドライブを交換または追加するか、ディスク パーティションを削除するか、またはブートしたリカバリ CD-ROM から WAAS を再インストールするかしたあとの、次のリブート時に RAID ペアが再ビルドされます。

ドライブのステータスを表示して、RAID ペアが「NORMAL OPERATION」または「REBUILDING」ステータスであるかどうかをチェックするには、**show disk details** EXEC コマンドを使用します。RAID が再ビルド中であることが表示された場合は、その再ビルド プロセスが完了するまで待つ必要があります。この再ビルド プロセスには数時間かかることがあります。

デバイスのリブート前に RAID ペアの再ビルド プロセスの完了を待たないと、問題を示す次の現象が発生することがあります。

- Central Manager GUI でデバイスがオフラインになっている。
- CMS をロードできない。
- ファイル システムが読み取り専用であるというエラー メッセージが表示される。
- syslog に、「Aborting journal on device md2」、「Journal commit I/O error」、「Journal has aborted」、「ext3_readdir: bad entry in directory」などのエラーが含まれている。
- ディスク操作または操作不能に関連するその他の異常な動作

このような現象のいずれかが発生した場合、WAE デバイスをリブートし、RAID の再ビルドが完了するまで待ちます。

システム ソフトウェアの復旧

WAAS デバイスには、フラッシュ メモリ内のイメージが壊れた場合に呼び出される復旧用システム イメージが常駐しています。システム イメージをフラッシュ メモリに書き込む際に停電が発生するとシステム イメージが壊れる場合があります。復旧用イメージは、デバイスのメイン メモリへシステム イメージをダウンロードし、フラッシュ メモリに書き込むことができます。

（注）　使用されるシステム イメージは、デバイスによって異なります。WAVE-274/474/574 および WAE-674/7341/7371 デバイス（64 ビット プラットフォーム）では、WAAS-4.x.x.x-K9.x86_64.sysimg という名前のシステム イメージが使用されます。その他すべてのデバイスでは、WAAS-4.x.x.x-K9.sysimg という名前のシステム イメージが使用されます。

復旧用イメージを使用して新しいシステム イメージをインストールするには、次の手順に従ってください。

ステップ 1　FTP サーバを実行しているホストへシステム イメージ ファイル（*.sysimg）をダウンロードします。

ステップ 2　デバイスとのコンソール接続を確立し、ターミナル セッションを開きます。

ステップ 3　電源スイッチを切り替えて、デバイスをリブートします。

復旧用イメージ ダイアログが表示されます。次の例は、復旧用イメージ ダイアログの使用方法を示しています（ユーザ入力は太字フォントで表記されています）。

```
This is the rescue image. The purpose of this software is to let
you download and install a new system image onto your system's
boot flash device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.

To download an image, this software will request the following
information from you:
    - which network interface to use
    - IP address and netmask for the selected interface
    - default gateway IP address
    - server IP address
    - which protocol to use to connect to server
    - username/password (if applicable)
    - path to system image on server

Please enter an interface from the following list:
    0: FastEthernet 0/0
    1: FastEthernet 0/1
    0
Using interface FastEthernet 0/0

Please enter the local IP address to use for this interface:
[Enter IP Address]: 172.16.22.22

Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.224

Please enter the IP address for the default gateway:
[Enter Gateway IP Address]: 172.16.22.1

Please enter the IP address for the FTP server where you wish
to obtain the new system image:
[Enter Server IP Address]: 172.16.10.10

Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: anonymous

Please enter the password for username 'anonymous' on FTP server (an email address):

Please enter the directory containing the image file on the FTP server:
[Enter Directory on server (e.g. /)]: /
```

```
Please enter the file name of the system image file on the FTP server:
[Enter Filename on server]: WAAS-4.1.7.10-K9.sysimg

Here is the configuration you have entered:
Current config:
          IP Address: 172.16.22.22
             Netmask: 255.255.255.224
     Gateway Address: 172.16.22.1
      Server Address: 172.16.10.10
            Username: anonymous
            Password:
     Image directory: /
      Image filename: WAAS-4.1.7.10-K9.sysimg

Attempting download...
Downloaded 10711040 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
.....................................................................................Finished
writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system.
Initializing memory. Please wait.
```

ステップ 4　ユーザ名 **admin** としてデバイスにログインします。**show version** コマンドを入力して、正しいバージョンが動作していることを確認します。

```
Username: admin
Password:

Console> enable
Console# show version
Wide Area Application Services (WAAS)
Copyright (c) 1999-2008 by Cisco Systems, Inc.
Wide Area Application Services Release 4.1.1
Version: ce507-5.2.0

Compiled 02:34:38 May 8 2008 by (cisco)
Compile Time Options: PP SS



System was restarted on Thu June 22 16:03:51 2008.
The system has been up for 4 weeks, 1 day, 6 hours, 7 minutes, 23 seconds.
```

紛失した管理者パスワードの復旧

管理者パスワードを忘れたり、紛失したり、設定が間違っている場合は、デバイス上のパスワードをリセットする必要があります。

（注）　失われた管理者パスワードは復元できません。この手順の説明に従って、新しいパスワードにリセットする必要があります。

パスワードをリセットするには、次の手順に従ってください。

ステップ 1　デバイスとのコンソール接続を確立し、ターミナル セッションを開きます。

ステップ 2　デバイスをリブートします。

デバイスがリブートしているときに、次のプロンプトが表示されたら、Enter を押します。

```
Cisco WAAS boot:hit RETURN to set boot flags:0009
```

ステップ 3　起動フラグを入力するプロンプトが表示されたら、**0x8000** を入力します。

```
Available boot flags (enter the sum of the desired flags):
0x4000 - bypass nvram config
0x8000 - disable login security

[CE boot - enter bootflags]:0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]:yes

[Display output omitted]
Setting the configuration flags to 0x8000 lets you into the system, bypassing all
security. Setting the configuration flags field to 0x4000 lets you bypass the NVRAM
configuration.
```

ステップ 4　デバイスが起動手順を完了すると、CLI にアクセスするためのユーザ名を入力するプロンプトが表示されます。デフォルトの管理者ユーザ名（**admin**）を入力します。

```
Cisco WAE Console

Username: admin
```

ステップ 5　CLI プロンプトが表示されたら、グローバル コンフィギュレーション モードで **username password** コマンドを使用して、ユーザ用のパスワードを設定します。

```
WAE# configure
WAE(config)# username admin password 0 password
```

パスワードには、平文パスワードまたは暗号化されたパスワードを指定できます。

（注）　ユーザ ID（UID）は設定しないでください。

ステップ 6　設定の変更を保存します。

```
WAE(config)# exit
WAE# write memory
```

ステップ 7　（任意）デバイスをリブートします。

```
WAE# reload
```

リブートはオプションです。ただし、起動フラグがリセットされ、以後のコンソール管理者ログインがパスワード検査を迂回しないことを確認する場合はリブートします。

（注）　WAAS ソフトウェアでは、リブートするたびに起動フラグが 0x0 にリセットされます。

ディスクに基づくソフトウェアの欠落からの復旧

この項では、次のタイプのディスク ドライブの問題から復元する方法について説明します。

- WAAS デバイスが、ディスク障害時に交換する必要がある 1 台のディスク ドライブを搭載している。
- WAAS デバイスが 2 台のディスク ドライブを搭載し、両方ドライブ（diks00 および disk01）で意図的にディスク パーティションを削除した。

  一般に複数のディスク ドライブを搭載するシステムは、重要なシステム パーティション上の RAID 1 で保護されているため、ドライブを交換するとき、この項の手順に従う必要はありません。

この条件から復旧するには、次の手順に従ってください。

ステップ 1　次の手順を完了して、デバイスを非アクティブにします。

a. WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] に進みます。

b. 非アクティブにするデバイスの横にある [Edit] アイコンをクリックします。

c. ナビゲーション ペインで、[*Device Name*] > [Activation] を選択します。[Device Activation] ウィンドウが表示されます。

d. [Activate] チェックボックスの選択を解除し、[Submit] をクリックします。

デバイスが非アクティブになります。

ステップ 2　デバイスの電源を切り、故障したハード ドライブを交換します。

ステップ 3　デバイスの電源を入れます。

ステップ 4　WAAS ソフトウェアをインストールします。詳細については『*Cisco Wide Area Application Services Quick Configuration Guide*』を参照してください。

ステップ 5　CMS ID 復旧手順を使用して、デバイス CMS ID を復旧し、このデバイスを WAAS Central Manager 上の既存のデバイス レコードに関連付けます。詳細については、「WAAS デバイス登録情報の復旧」（P.15-21）を参照してください。

WAAS デバイス登録情報の復旧

デバイス登録情報は、デバイスと WAAS Central Manager の両方に保存されます。ハードウェア障害のためにデバイスの登録 ID が失われたり、デバイスを交換する必要がある場合、WAAS ネットワーク管理者は、CLI コマンドを発行して失った情報を復旧し、新しいデバイスを追加するときは、故障したデバイスの ID を仮定できます。

失った登録情報を復旧する、または同じ登録情報を持つ新しいデバイスで故障したデバイスを交換するには、次の手順に従ってください。

ステップ 1　次の手順を完了して、故障したデバイスに「Inactive」および「Replaceable」というマークを付けます。

a. WAAS GUI から、[My WAN] > [Manage Devices] を選択します。

b. 非アクティブにするデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

c. ナビゲーション ペインで、[*Device Name*] > [Activation] を選択します。

d. [Activate] チェックボックスの選択を解除します。ウィンドウが更新され、デバイスに交換可能マークを付けるためのチェックボックスが表示されます。

e. [Replaceable] チェックボックスを選択し、[Submit] をクリックします。

（注） このチェックボックスは、デバイスが非アクティブであるときだけ、GUI に表示されます。

ステップ 2　次のように、システム デバイス復旧キーを設定します。

a. WAAS Central Manager GUI ナビゲーション ペインで、[Configure] > [System Properties] を選択します。

b. System.device.recovery.key プロパティの横にある [Edit] アイコンをクリックします。[Modifying Config Property] ウィンドウが表示されます。

c. [Value] フィールドにパスワードを入力し、[Submit] をクリックします。デフォルトのパスワードは、**default** です。

ステップ 3　新しいデバイス用の基本的なネットワーク設定を構成します。

ステップ 4　デバイス CLI との Telnet セッションを開き、**cms recover identity** *keyword* EXEC コマンドを入力します。*keyword* は、WAAS Central Manager GUI で設定したデバイス復旧キーです。

WAAS Central Manager は、WAAS デバイスから復旧要求を受信すると、次の基準に適合するデバイス レコードをデータベースで検索します。

- レコードが非アクティブかつ交換可能である。
- レコードが復旧要求に指定されたホスト名またはプライマリ IP アドレスを持っている。

復旧要求とデバイス レコードが一致する場合、WAAS Central Manager は、既存のレコードを更新し、要求するデバイスへ登録応答を送信します。他のデバイスが同じ ID を仮定することがないように、交換可能状態がクリアされます。WAAS デバイスは、復旧された登録情報を受信すると、登録情報をファイルに書き込み、そのデータベース表を初期化し、起動します。

ステップ 5　デバイスをアクティブにします。

a. WAAS GUI から、[My WAN] > [Manage Devices] を選択します。

b. アクティブにする WAAS デバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

c. ナビゲーション ペインで、[*Device Name*] > [Activation] を選択します。WAAS デバイスのステータスがオンラインになります。

d. [Activate] チェックボックスを選択し、[Submit] をクリックします。

RAID 1 システムのディスク保守の実行

WAAS は、障害の発生したディスクの交換およびスケジュール設定されたディスクの保守のいずれに対しても、ホットスワップ機能をサポートします。ディスクに障害が発生すると、WAAS は自動的にディスクの障害を検出し、ディスクは不良としてマークが付けられ、RAID 1 ボリュームから削除されます。ディスク保守のスケジュールを設定するには、手動でディスクをシャットダウンする必要があります。

ディスクを WAE から物理的に取り外す前に、ディスクのシャットダウンが完了するのを待つ必要があります。RAID 削除プロセスが完了すると、WAAS はディスク障害アラームおよびトラップを生成します。さらに、syslog ERROR メッセージが記録されます。

（注）　RAID アレイの再ビルド プロセス中に削除イベント（ディスク障害またはソフトウェアのシャットダウンなど）が発生した場合、RAID 削除プロセスの完了に最長 1 分かかることがあります。このプロセスの所要時間は、ディスクのサイズによって異なります。

RAID 再ビルド プロセス中に WAAS ソフトウェアにより障害発生ディスクが削除された場合、RAID 再ビルドの障害アラームが生成されます。RAID 再ビルド プロセス中にディスクを管理上のシャットダウンにする場合、RAID 再ビルドの中断アラームが生成されます。

交換ディスクを取り付けると、WAAS ソフトウェアは交換ディスクを検出し、ディスクの互換性チェックを実行します。さらに、パーティションを作成してディスクを初期化し、そのディスクをソフトウェア RAID に追加して、RAID 再ビルド プロセスを開始します。

新しく挿入したディスクの ID が、同じ物理スロットでそれまでに不良のマークが付けられたディスクの ID と同じ場合、ディスクはマウントされず、交換後チェック、初期化、RAID の再ビルドは行なわれません。

新しく取り付けたディスクは、以前のディスクと同じタイプで、次の互換性要件を満たしている必要があります。

- 交換ディスクが RAID ペアの disk00、disk02、または disk04 用の場合、交換ディスクはアレイで動作中のディスクと同じサイズである必要があります。
- 交換ディスクが RAID ペアの disk01、disk03、または disk05 用の場合、交換ディスクはアレイで動作中のディスクと同じまたはそれ以上の RAID 容量である必要があります。

ホットスワップ プロセスの一部である互換性チェックでは、容量互換性がチェックされます。互換性がないとアラームが生成され、ホットスワップ プロセスが中断されます。

表 15-3 に、WAE-612 のドライブ タイプの互換性を示します。すべてのドライブが同じタイプである必要があります。

表 15-3　WAE-612 ドライブタイプの互換性のマトリクス

ドライブ タイプ	SAS[1]	SATA2[2]
SAS	Ok	なし
SATA2	なし	Ok

1. Serial Attached SCSI
2. Serial Advanced Technology Attachment 2

ディスク保守を実行するには、次の手順に従ってください。

ステップ 1　ディスクを手動でシャットダウンします。

a. グローバル コンフィギュレーション モードを開始してから、**disk disk-name** *diskxx* **shutdown** コマンドを入力します。

```
WAE# configure
WAE(config)# disk disk-name diskxx shutdown
```

b. ディスクのシャットダウンが完了するのを待ってから、ディスクを WAE から物理的に取り外します。RAID 削除プロセスが完了すると、WAAS はディスク障害アラームおよびトラップを生成します。さらに、syslog ERROR メッセージが記録されます。

（注）　ディスクを削除するためにシステムの電源を切る必要はないので、**disk error-handling reload** オプションが有効になっている場合は無効にすることを推奨します。

ステップ 2　交換ディスクを WAE のスロットに挿入します。交換ディスクの ID は、交換前のディスクとは異なっている必要があります。

ステップ 3　**no disk disk-name** *diskxx* **shutdown** グローバル コンフィギュレーション コマンドを入力して、ディスクを再び有効にします。

RAID 5 システムのディスク交換

RAID 5 論理ドライブを使用するシステムの物理ディスク ドライブを取り外して交換するには、次の手順に従ってください。

ステップ 1　WAE の WAAS CLI の EXEC モードで **disk disk-name** *diskxx* **replace** コマンドを入力します。

ステップ 2　EXEC モードで *show disks details* コマンドを入力して、ディスク ドライブ **diskxx** が Defunct 状態になっていることを確認します。RAID 論理ドライブは、この時点で Critical 状態になっています。

ステップ 3　ドライブのハンドルを開く位置（ドライブに対して垂直）に動かします。

ステップ 4　ホットスワップ ドライブ アセンブリをベイから引き出します。

ステップ 5　1 分間待ってから、交換ドライブ アセンブリをベイのガイド レールに合わせ、ドライブ アセンブリが止まるまでベイにスライドさせて、新しいドライブを同じスロットに挿入します。ドライブがベイに正しく装着されていることを確認します。

ステップ 6　ドライブ ハンドルを閉じます。

ステップ 7　ハード ディスク ドライブのステータス LED をチェックし、ハード ディスク ドライブが正常に動作していることを確認します。オレンジのハード ディスク ドライブのステータス LED が点灯している場合、そのドライブは故障しているので、交換する必要があります。グリーンのハード ディスク ドライブのアクティビティ LED が点滅している場合、そのドライブがアクセスされていることを示します。

ステップ 8　1 分間待ってから、EXEC モードで **show disks details** コマンドを使用して、交換したディスク ドライブが Rebuilding 状態になっていることを確認します。

（注）　ServeRAID コントローラは、論理 RAID ドライブの一部であるドライブの取り外しと再挿入を検出すると、自動的に再ビルド操作を開始します。

ステップ 9　再ビルド操作が完了するまで待ちます。EXEC モードで **show disks details** コマンドを使用すれば、再ビルド操作が完了したかどうかをチェックできます。再ビルド操作が完了すると、物理ドライブの状態は Online、RAID 論理ドライブの状態は Okay になっています。

300 GB SAS ドライブの場合、再ビルドが完了するのに最長で 5 時間かかることがあります。

複数のディスクで障害が発生し、RAID 5 論理ステータスが Offline の場合、次のステップに従って RAID 5 アレイを再作成する必要があります。

ステップ 1　クローバル コンフィギュレーション モードを開始してから、**disk logical shutdown** コマンドを入力して RAID 5 アレイを無効にします。

ステップ 2　EXEC モードで **write** コマンドを入力し、NVRAM に実行コンフィギュレーションを保存します。

ステップ 3　EXEC モードで **reload** コマンドを入力し、システムをリロードします。

ステップ 4　システムがリブートされたら、EXEC モードで **show disks details** コマンドを入力し、システム コンフィギュレーションをチェックします。この時点で、ディスクはマウントされておらず、論理 RAID ドライブは Shutdown 状態になっています。

ステップ 5　EXEC モードで **disk recreate-raid** コマンドを入力して、RAID 5 アレイを再作成します。

ステップ 6　このコマンドが正常に実行されたら、グローバル コンフィギュレーション モードで **no disk logical shutdown** コマンドを入力して、論理ディスクのシャットダウン設定を無効にします。

ステップ 7　EXEC モードで **write** コマンドを入力し、NVRAM に設定を保存します。

ステップ 8　EXEC モードで **reload** コマンドを入力し、システムをリロードします。

ステップ 9　システムがリブートされたら、EXEC モードで **show disks details** コマンドを入力し、システム コンフィギュレーションをチェックします。この時点でディスクはマウントされて、論理 RAID ドライブは Shutdown 状態ではなくなっています。

ステップ 10　再ビルド操作が完了するまで待ちます。EXEC モードで **show disks details** コマンドを使用すれば、再ビルド操作が完了したかどうかをチェックできます。再ビルド操作が完了すると、物理ドライブの状態は Online、RAID 論理ドライブの状態は Okay になっています。

RAID 5 アレイの再ビルドが完了するには数時間かかります。

複数のディスクまたは RAID コントローラで障害が発生し、ドライブが交換されて RAID ディスクが再ビルドされた後でも、論理ディスクがエラー状態のままであることがあります。ディスクを再有効化するには、**no disk logical shutdown force** コマンドを使用してから WAE をリロードします。

Central Manager の役割の設定

WAAS ソフトウェアは、スタンバイ WAAS Central Manager を実装しています。このプロセスにより、別の WAAS Central Manager デバイスで WAAS ネットワーク設定のコピーを維持できます。プライマリ WAAS Central Manager に障害が発生した場合、スタンバイはプライマリを交換するために使用できます。

相互運用性については、スタンバイ WAAS Central Manager を使用する場合、WAAS Central Manager の完全な設定を維持するために、プライマリ WAAS Central Manager と同じソフトウェア バージョンである必要があります。バージョンが異なると、スタンバイ WAAS Central Manager はこの状態を検出し、問題が解決されるまで、プライマリ WAAS Central Manager から受信する設定の更新を処理しません。

（注）　プライマリ Central Manager とスタンバイ Central Manager は、ポート 8443 で通信します。ネットワークでプライマリ Central Manager とスタンバイ Central Manager との間にファイアウォールが存在する場合、ポート 8443 上のトラフィックを許可するようにファイアウォールを設定して、Central Manager 同士が通信を行い、同期を維持できるようにします。

（注）　スタンバイ Central Manager を設定する前に、WAAS 印刷サービスを使用しているならば印刷ドライバを手動でインストールする必要があります。印刷ドライバは、プライマリ Central Manager データベースからスタンバイ デバイスに自動的に複製されません。

ここでは、次の内容について説明します。

WAE のスタンバイ Central Manager への変換

この項では、アプリケーション アクセラレータとして動作している WAE をスタンバイ Central Manager に変換する方法について説明します。

WAAS ソフトウェアには次に示すとおり 2 つのタイプがあります。

- Universal：Central Manager および Application Accelerator 機能が含まれます。
- Accelerator only：Application Accelerator 機能のみが含まれます。Application Accelerator を Central Manager に変更する場合は、Universal ソフトウェア ファイルを使用する必要があります。

WAE が Accelerator only イメージを使用して動作している場合、WAE Central Manager に変換するには、まず Universal ソフトウェア ファイルを使用して WAE をアップデートし、デバイスを再ロードし、デバイス モードを central-manager に変更した後、改めてデバイスを再ロードすることが必要です。WAE のアップデートの詳細については、「WAAS ソフトウェアのアップグレード」（P.15-1）を参照してください。

show version EXEC コマンドを使用して、WAE が Accelerator only イメージを実行しているかどうかチェックできます。Accelerator only イメージを実行している場合は、「(WAAS-ACCELERATOR-K9)」と出力されます。また、WAE が Accelerator only イメージを実行している場合、**show running-config** EXEC コマンドを使用した場合も同様の出力となります。

Universal イメージを使用して WAE をスタンバイ Central Manager に変換するには、次の手順に従ってください。

ステップ 1　**cms** コマンドを使用して、Central Manager からこの WAE の登録を取り消します。

```
WAE# cms deregister force
```

これにより、その他すべての Central Manager との以前の関連付けがすべて消去されます。

ステップ 2　**device** コマンドを使用して、デバイス モードを Central Manager として設定します。

```
WAE# configure
WAE(config)# device mode central manager
```

変更内容を適用するには、デバイスをリロードする必要があります。

ステップ 3　**central-manager** コマンドを使用して、Central Manager の役割をスタンバイとして設定します。

```
WAE(config)# central-manager role standby
```

ステップ 4　**central-manager** コマンドを使用して、プライマリ Central Manager のアドレスを設定します。

```
WAE(config)# central-manager address cm-primary-address
```

ステップ 5　**cms** コマンドを使用して CMS サービスを有効にします。

```
WAE(config)# cms enable
```

プライマリ Central Manager のスタンバイ Central Manager への変換

プライマリ Central Manager をスタンバイ Central Manager に変換するには、次の手順を実行します。

ステップ 1　**cms** コマンドを使用して、Central Manager の登録を取り消します。

```
WAE# cms deregister
```

これにより、その他すべての Central Manager との以前の関連付けがすべて消去されます。

ステップ 2　**central-manager** コマンドを使用して、Central Manager の役割をスタンバイとして設定します。

```
WAE# configure
WAE(config)# central-manager role standby
```

ステップ 3　**central-manager** コマンドを使用して、プライマリ Central Manager のアドレスを設定します。

```
WAE(config)# central-manager address cm-primary-address
```

ステップ 4　**cms** コマンドを使用して CMS サービスを有効にします。

```
WAE(config)# cms enable
```

スタンバイ Central Manager のプライマリ Central Manager への変換

プライマリ WAAS Central Manager が動作不能になった場合、ウォーム スタンバイ Central Manager の 1 つをプライマリ Central Manager にするように手動で再設定できます。次のように、グローバル設定 **central-manager role primary** コマンドを使用して新しい役割を設定します。

```
WAE# configure
WAE(config)# central-manager role primary
```

このコマンドにより、役割がスタンバイからプライマリに変更され、マネジメント サービスが再起動して、この変更を認識します。

プライマリ Central Manager がまだオンラインでアクティブなときにウォーム スタンバイ Central Manager をプライマリに切り替えると、両方の Central Manager が互いに検出し合うことにより自動的に停止し、管理サービスを無効にします。Central Manager は停止に切り替わり、自動的にフラッシュ メモリに保存されます。

停止した WAAS Central Manager をオンライン状態に戻すには、どちらの Central Manager をプライマリ デバイスにし、どちらをスタンバイ デバイスにするかを決定します。プライマリ デバイスで、次の CLI コマンドを実行します。

```
WAE# configure
WAE(config)# central-manager role primary
WAE(config)# cms enable
```

スタンバイ デバイスで、次の CLI コマンドを実行します。

```
WAE# configure
WAE(config)# central-manager role standby
WAE(config)# central-manager address cm-primary-address
WAE(config)# cms enable
```

Central Manager の役割を切り替える場合、次の「両方の Central Manager の役割の切り替え」（P.15-28）を参照してください。

両方の Central Manager の役割の切り替え

注意　WAAS Central Manager をプライマリからスタンバイに切り替えると、Central Manager での設定が消去されます。Central Manager は、スタンバイになったあと、現在ではプライマリであるいずれかの Central Manager からの設定情報を複製し始めます。スタンバイおよびプライマリ ユニットが役割を切り替える前に同期しない場合、重要な設定情報が失われる可能性があります。

Central Manager の役割を切り替える前に、次の手順に従います。

ステップ 1　Central Manager デバイスで、同じバージョンの WAAS ソフトウェアが動作していることを確認します。

ステップ 2　両方の WAAS Central Manager で同じ Coordinated Universal Time（UTC; 協定世界時）が設定されるように、両方のデバイスで物理クロックを同期化します。

ステップ 3　次の項目の状態を確認することにより、スタンバイがプライマリと同期していることを確認します。

a. デバイスのオンライン状態を確認します。

元のスタンバイ Central Manager と現在アクティブなすべてのデバイスは、Central Manager GUI でオンラインとして表示されています。この手順では、ほかのすべてのデバイスが両方の Central Manager を認識するようにします。

b. プライマリ WAAS Central Manager からの最近の更新の状態を確認します。

show cms info EXEC コマンドを使用して、最後の更新の時間を確認します。最新の状態では、[Time of last config-sync] フィールドの値は 1 ～ 5 分である必要があります。スタンバイ WAAS Central Manager がプライマリ WAAS Central Manager の設定を完全に複製したことを確認します。

更新時間が最新でない場合、接続の問題があるかどうか、またはプライマリ WAAS Central Manager がダウンしているかどうかを確認します。必要に応じて問題を解決し、最後の更新時間が示すように、設定が複製されるまで待ちます。

ステップ 4　次の順番で役割を切り替えます。

a. 元のプライマリ モードをスタンバイ モードに切り替えます。

```
WAE1# configure
WAE1(config)# central-manager role standby
WAE(config)# cms enable
```

b. 元のスタンバイ モードをプライマリ モードに切り替えます。

```
WAE2# configure
WAE2(config)# central-manager role primary
WAE(config)# cms enable
```

役割変更を設定すると、CMS サービスが自動的に再起動します。

ディスクの暗号化の有効化

ディスクの暗号化は、展開された WAAS システムを通って流れる機密情報および WAAS 永続ストレージに保存される機密情報を安全に保護する必要性に対応しています。ディスクの暗号化機能には、WAE ディスク上での実際のデータ暗号化と、暗号キーの保管および管理という 2 つの面があります。

ディスクの暗号化を有効にすると、WAAS 永続ストレージの全データが暗号化されます。暗号化データのロックを解除する暗号キーは、Central Manager に保管され、キー管理は Central Manager で行われます。ディスクの暗号化を設定したあとで WAE をリブートすると、WAE は Central Manager からキーを自動的に取得します。これにより、WAAS 永続ストレージに保存されているデータにアクセスできるようになります。

（注）　リブート時に WAE が WAAS Central Manager に到達できない場合、暗号化パーティションのマウント以外のことをすべて行います。この状態では、すべてのトラフィックはパススルーとして処理されます。WAAS Central Manager との通信が復元する（および暗号キーを取得する）と、暗号化パーティションがマウントされます。キャッシュの内容は失われません。

ディスク暗号化の要件は次のとおりです。

- Central Manager がネットワークで使用できるように設定されている必要があります。
- WAE デバイスが、Central Manager に登録されている必要があります。
- WAE デバイスが Central Manager とオンラインになっている（アクティブ接続を確立している）必要があります。この要件は、ディスクの暗号化を有効にする場合にだけ適用されます。
- ディスクの暗号化設定を有効にするには、WAE をリブートする必要があります。

  WAE をリブートしたあと、新しいキーを使用して暗号化パーティションが作成され、既存のデータはパーティションから削除されます。

暗号化の有効化または無効化に関係なく、ディスクの暗号化設定に変更があると、ディスクのキャッシュがクリアされます。この機能は、万一 WAE が盗難に遭った場合に、顧客の機密情報が暗号解除されたりアクセスされたりしないように保護します。

ディスクの暗号化を有効にしてから、この機能をサポートしていないソフトウェア バージョンにダウングレードした場合、データ パーティションを使用できません。そのような場合は、ダウングレードしたあとにディスク パーティションを削除する必要があります。

Central Manager GUI からディスクの暗号化を有効および無効にするには、[My WAN] > [Manage Devices] を選択してからデバイスを選択し、[Configure] > [Storage] > [Disk Encryption] を選択します。ディスクの暗号化を有効にするには、[Enable] チェックボックスを選択して、[Submit] をクリックします。デフォルトで、このボックスは選択されていません。ディスクの暗号化を無効にするには、[Enable] チェックボックスの選択を解除し、[Submit] をクリックします。

WAE CLI からディスクの暗号化を有効および無効にするには、**disk encrypt** グローバル コンフィギュレーション コマンドを使用します。

ディスクの暗号化を有効または無効にすると、ファイル システムはその後の最初のリブートの間に再度初期化されます。ディスク パーティションのサイズにより、再初期化には 10 分から数時間かかります。この間、WAE にはアクセス可能ですが、サービスの提供はありません。

Central Manager の IP アドレスを変更したり、Central Manager を再配置したり、Central Manager を元の Central Manager からすべての情報をコピーしていない別の Central Manager に置き換えたりしてから、ディスクの暗号化が有効になったときに WAE をリロードした場合、WAE ファイル システムは再初期化プロセスを完了したり、Central Manager から暗号キーを取得したりすることができません。

WAE が暗号キーの取得に失敗した場合、CLI から **no disk encrypt enable** グローバル コンフィギュレーション コマンドを使用してディスクの暗号化を無効にして、WAE をリロードします。ディスクの暗号化を有効にし WAE をリロードする前に、Central Manager との接続を確認します。このプロセスにより、ディスク キャッシュがクリアされます。

（注） スタンバイ Central Manager が データフィード ポーリング レート時間の少なくとも 2 倍の間（約 10 分）稼動中で、プライマリ Central Manager から管理アップデートを受信した場合、アップデートには暗号キーの最新バージョンが含まれます。この状態でのスタンバイへのフェールオーバーは、WAE に対して透過的に発生します。データフィード ポーリング レートは、設定変更のため WAE が Central Manager をポーリングする間隔を定義します。デフォルトでは、この間隔は 300 秒です。

暗号化ステータスの詳細を表示するには、**show disks details** EXEC コマンドを使用します。ファイルシステムの初期化の間、**show disks details** では、「`System initialization is not finished, please wait...`」というメッセージが表示されます。Central Manager GUI の [Device Dashboard] ウィンドウでもディスクの暗号化ステータス（有効か無効か）を表示できます。

ディスク エラー処理方法の設定

（注） ディスク エラーの処理の設定および有効化は、ディスクのホットスワップをサポートするデバイスには必要なくなりました。WAAS 4.0.13 以降では、ソフトウェアが自動的にクリティカル エラーのあるディスクをサービスから削除します。

WAAS Central Manager を使用すると、4.1.1 以前のソフトウェア バージョンを実行する WAAS デバイスについてディスク エラーの処理方法を設定し、ディスク デバイス エラー処理しきい値を定義できます。

不良ディスク ドライブがクリティカル ディスク ドライブで、自動リロード機能が有効の場合、WAAS ソフトウェアは、そのディスク ドライブに「不良」マークを付け、WAAS デバイスが自動的にリロードされます。WAAS デバイスがリロードされると、syslog メッセージと SNMP トラップが生成されます。

（注） 自動リロード機能は自動的に有効になり、WAAS バージョン 4.1.3 以降を実行するデバイスでは設定できません。

WAAS Central Manager GUI を使用してディスク エラー処理方法を設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　ディスク エラー処理方法を設定するデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Storage] > [Disk Error Handling] を選択します。

[Disk Error Handling Settings] ウィンドウが表示されます。

ステップ 4　[Enable] チェックボックスを選択して設定ウィンドウを有効にし、必要に応じて次のオプションを選択します。

- [Enable Disk Error Handling Reload] : ファイル システム（sysfs）（disk00）に問題がある場合、デバイスはディスクを再ロードします。このオプションは、デバイス グループおよびバージョン 4.1.1 以前の WAAS デバイスに限り表示され、デフォルトでは無効です。バージョン 4.1.1 よりも後の WAAS には適用されません。
- [Enable Disk Error Handling Remap] : デバイスは、自動的にディスク エラーを再マップします。このオプションは、デフォルトで有効になっています。
- [Enable Disk Error Handling Threshold] : ディスクに不良マークが付く前にディスク エラーの上限数を指定します。[Threshold] フィールドに、0 ～ 100 の値を入力する必要があります。デフォルトのしきい値は 10 です。このオプションは、デフォルトで無効です。このオプションは、デバイス グループおよびバージョン 4.1.1 以前の WAAS デバイスに限り表示されます。バージョン 4.1.1 よりも後の WAAS には適用されません。

ステップ 5　[Submit] をクリックして、設定を保存します。

拡張オブジェクト キャッシュの有効化

WAAS Central Manager により、CIFS オブジェクト キャッシング向けの追加のディスク スペースを設定できます。ディスク キャッシングは、境界にあるコンテンツを処理する目的で DRE および CIFS に使用されます。拡張オブジェクト キャッシュ機能により、CIFS および Virtual Blade Services が使用するディスク ストレージ容量を選択できます。

この機能がサポートされるのは、WAE-674-4G および WAE-674-8G モデルだけで、デバイス グループ内の他のモデルには影響を与えません。

（注）　拡張オブジェクト キャッシュが有効で、デバイスを 4.2.1 以前のバージョンにダウングレードした場合、CIFS キャッシュ データ、DRE キャッシュ データ、および仮想ブレード データはすべて失われます。

WAAS Central Manager GUI を使用して拡張オブジェクト キャッシュを有効化するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　拡張オブジェクト キャッシュを有効にしたいデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Storage] > [Extended Object Cache] を選択します。

[Extended Disk Space Settings] ウィンドウが表示されます。

ステップ 4　[Enable] チェックボックスを選択して、拡張オブジェクト キャッシュ サービスを有効にします。サイズ調整の詳細については、表 15-4 および表 15-5 を参照してください。

（注）　30 GB を超える vbspace を備えた WAE-674-4G または WAE-674-8G モデルで拡張オブジェクト キャッシュを有効にした場合、デバイスは上書きモードになります。上書きモードでは、デバイス ページ（またはデバイス グループ ページ）に DG の強制設定ボタンが表示されます。

30 GB を超える vbspace を使用して仮想ブレードを有効にした場合は、拡張オブジェクト キャッシュを有効にする前に、まず仮想ブレードを終了して、設定を削除する必要があります。これを実行しなければ、vbspace のサイズは 30 GB まで減少します。

ステップ 5　[Submit] をクリックして、設定を保存します。

WAE-674 プラットフォームのディスク キャッシュ サイズは、有効になっている機能によって変わります。

表 15-4 に、WAE-674-4G プラットフォームのディスク キャッシュ サイズを示します。

表 15-4　WAE-674-4G プラットフォームのディスク キャッシュ サイズ

	拡張オブジェクト キャッシュが無効の場合		拡張オブジェクト キャッシュが有効の場合	
ディスク パーティション	仮想ブレードが無効	仮想ブレードが有効	仮想ブレードが無効	仮想ブレードが有効
DRE キャッシュ	120 GB	120 GB	120 GB	120 GB
CIFS オブジェクト キャッシュ	95 GB	95 GB	340 GB	300 GB
仮想ブレード	--	120 GB	--	30 GB

表 15-5 に、WAE-674-8G プラットフォームのディスク キャッシュ サイズを示します。

表 15-5　WAE-674-8G プラットフォームのディスク キャッシュ サイズ

	拡張オブジェクト キャッシュが無効の場合		拡張オブジェクト キャッシュが有効の場合	
ディスク パーティション	仮想ブレードが無効	仮想ブレードが有効	仮想ブレードが無効	仮想ブレードが有効
DRE キャッシュ	320 GB	150 GB	150 GB	150 GB
CIFS オブジェクト キャッシュ	95 GB	95 GB	310 GB	275 GB
仮想ブレード	--	200 GB	--	30 GB

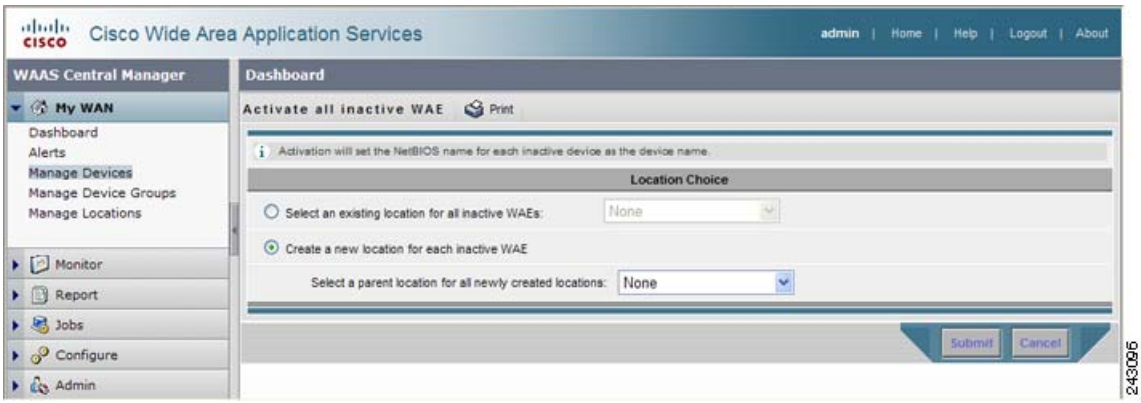
すべての非アクティブ WAAS デバイスのアクティブ化

ネットワーク内のすべての非アクティブ WAAS デバイスをアクティブにするには、次の手順を実行します。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] 一覧ウィンドウが表示されます。

ステップ 2　タスクバーの [Activate all inactive WAEs] アイコンをクリックします。[Activate All Inactive WAEs] ウィンドウが表示されます（図 15-2 を参照）。

図 15-2　非アクティブ デバイスのアクティブ化



ステップ 3　[Select an existing location for all inactive WAEs] オプション ボタンをクリックしてすべての非アクティブ WAAS デバイス用の既存の位置を選択し、ドロップダウン リストから位置を選択します。

あるいは、[Create a new location for each inactive WAE] オプション ボタンをクリックして、各非アクティブ デバイス用の新しい位置を作成することもできます。[Select a parent location for all newly created locations] ドロップダウン リストから位置を選択して、新しく作成したすべての位置の親位置を指定します。

ステップ 4　[Submit] をクリックします。非アクティブ WAE が再度アクティブ化され、指定した位置に配置されます。

デバイスまたはデバイス グループのリブート

WAAS Central Manager GUI を使用して、デバイスまたはデバイス グループをリモートにリブートできます。

個々のデバイスをリブートするには、次の手順に従ってください。

ステップ 1　WAAS GUI から、[My WAN] > [Manage Devices] を選択します。

ステップ 2　リブートするデバイスの名前の横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Reload WAE] アイコンをクリックします。処理を確認するプロンプトが表示されます。

ステップ 4　[OK] をクリックして、デバイスのリブートを確認します。

CLI からデバイスをリブートするには、**reload** EXEC コマンドを使用します。

セキュア ストアを有効にした WAAS Central Manager をリブートする場合、**cms secure-store open** EXEC コマンドを使用してリブートしたあとでセキュア ストアを再オープンする必要があります。

デバイス グループ全体をリブートするには、次の手順を実行します。

ステップ 1　WAAS GUI から、[My WAN] > [Manage Device Groups] を選択します。

ステップ 2　リブートするデバイス グループの名前の横にある [Edit] アイコンをクリックします。[Modifying Device Group] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Reboot All Devices in Device Group] アイコンをクリックします。処理を確認するプロンプトが表示されます。

ステップ 4　[OK] をクリックして、デバイス グループのリブートを確認します。

制御されたシャットダウンの実行

制御されたシャットダウンとは、デバイスの電源を切ることなく（ファンは継続して稼動し、電源 LED も点灯したままの状態で）、WAAS デバイス を正常にシャットダウンするプロセスを指してします。制御されたシャットダウンを行うと、すべてのアプリケーション アクティビティとオペレーティング システムがアプライアンス上で適切に停止されますが、電源は投入されたままです。制御されたシャットダウンは、アプライアンスにサービスを提供している場合のダウンタイムを最小限に抑える上で役立ちます。

注意　制御されたシャットダウンが実行されなかった場合は、WAAS ファイル システムが破損する可能性があります。また、アプライアンスが適切にシャットダウンされなかった場合は、リブートするのにかなりの時間がかかります。

shutdown EXEC コマンドを使用して、CLI から制御されたシャットダウンを実行できます。詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

Cisco アクセス ルータに搭載されたネットワーク モジュールで WAAS が稼動している場合は、ルータ CLI から **service-module integrated-service-engine** *slot/unit* **shutdown** EXEC コマンドを使用して、制御されたシャットダウンを実行します。詳細については、『Configuring Cisco WAAS Network Modules for Cisco Access Routers』を参照してください。

CHAPTER 16

WAAS ネットワークのモニタリングおよびトラブルシューティング

この章では、WAAS システムの問題を特定し、解決するために使用できる WAAS Central Manager GUI のモニタリングとトラブルシューティング ツールについて説明します。

（注）

この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

[System Dashboard] ウィンドウからのシステム情報の表示

WAAS Central Manager GUI では、[System Dashboard] ウィンドウで WAAS ネットワークに関する一般情報および詳細情報を表示できます。ここでは、[System Dashboard] ウィンドウについて説明します。内容は次のとおりです。

図 16-1 に、[System Dashboard] ウィンドウを示します。

図 16-1　[System Dashboard] ウィンドウ

[System Dashboard] ウィンドウのチャートに表示される情報は、2 回のポーリング周期の最後の WAE デバイスの状態を表す WAAS ネットワークのスナップショットに基づいています。WAAS Central Manager GUI で、ポール間の周期を設定できます（[Configure] > [System Properties] > [System.monitoring.collectRate]）。デフォルトのポーリング速度は、300 秒（5 分）です。アラームはリアルタイムで提供され、ポーリング速度には依存しません。

グラフおよびチャートのモニタリング

デフォルトの [System Dashboard] ウィンドウには、WAAS システムが処理するアプリケーション トラフィックに関する複数のグラフィック表示を示す 4 つのタブが含まれます。

- [Traffic] タブには次のグラフィック表示が含まれます。
  - [Traffic Summary] チャート: 過去 1 時間の WAAS ネットワークでトラフィック比率が最も高いアプリケーションを示します。
  - [Original Traffic over Time] グラフ: 過去 1 時間のオリジナル トラフィックおよびパススルー トラフィックの量を示します。

  - [Traffic Volume and Reduction] グラフ：過去 1 時間のオリジナル トラフィックと最適化されたトラフィックの量、およびトラフィック減少の比率を表示します。
  - [Optimized Traffic over Time] グラフ：過去 1 時間の最適化されたトラフィックおよびパススルー トラフィックの量を示します（このグラフは最小化されています）。
- [Optimization] タブには、次のグラフィックが表示されます。このタブは、デフォルト タブです。
  - [Compression Summary] チャート：過去 1 時間の WAAS ネットワークでトラフィック低下率が最も高い上位 10 のアプリケーションを示します。比率（%）計算には、パススルー トラフィックが含まれていません。
  - [Bandwidth Optimization] チャート：WAAS 最適化の結果、増加した WAN リンクの実効帯域幅容量を示します。値は、実際の値の倍数です。
  - [Traffic Volume and Reduction] チャート：過去 1 時間のオリジナル トラフィックと最適化されたトラフィックの量、およびトラフィック低下率を示します。
- [Acceleration] タブには次のグラフィック表示が含まれます。
  - [HTTP: Estimated Time Savings] グラフ：HTTP アクセラレータによって過去 1 時間の HTTP トラフィックで短縮された応答時間の概算を示します。
  - [MAPI: Estimated Time Savings] グラフ：MAPI アクセラレータによって過去 1 時間の MAPI トラフィックで短縮された応答時間の概算を示します。
  - [NFS: Estimated Time Savings] グラフ：NFS アクセラレータによって過去 1 時間の NFS トラフィックで短縮された応答時間の概算を示します。
- [Platform] タブには次のグラフィック表示が含まれます。
  - [Managed Devices Information]：ネットワーク内の WAAS デバイスの総数を示します。この数はオンライン、オフライン、非アクティブ、および保留状態を示します。また、ネットワークで展開されている異なる重大度およびソフトウェア バージョンの数についても示します。

チャートおよびグラフの数字は、少数第 1 位が四捨五入されて KB、MB、または GB で示されています。表では、少数第 4 位が四捨五入されています。CSV ファイルにエクスポートされるデータ値はバイト単位なので、四捨五入されません。

システム ダッシュボードに表示されるグラフィック表示とテーブルをカスタマイズできます。詳細については、「ダッシュボードまたはレポートのカスタマイズ」（P.16-10）を参照してください。個々のチャートについては、「チャートの説明」（P.16-14）で詳しく説明します。

システム ダッシュボード、関連するグラフおよびチャートに表示される大半のデバイス情報、統計情報、アラーム情報も、API をモニタすることによりプログラムで使用できます。詳細については、『*Cisco Wide Area Application Services API Reference*』を参照してください。

（注）　統計情報に一貫性および信頼性を持たせるために、各 WAE デバイス上のクロックをプライマリ WAAS Central Manager とセカンダリ WAAS Central Manager クロックの 5 分以内に同期させる必要があります。NTP サーバを使用してすべての WAAS デバイスの同期を維持する方法については、「NTP 設定の構成」（P.9-5）を参照してください。さらに、Central Manager が WAE から統計情報の更新を受信する際のネットワーク遅延が 5 分を超える場合、統計情報の集約が予定通り機能しないことがあります。

アラーム パネル

[System Dashboard] ウィンドウのアラーム パネルには、着信アラームのほぼリアルタイムのビューが表示されます。パネルは 2 分ごとに更新され、システム アラーム データベースへの更新が反映されます。

アラーム パネルには、[Active Alarms] および [Acknowledged Alarms] の 2 つのタブがあります。[Active Alarms] タブには、すべての着信アラームのダイナミック ビューが表示されます。アラームの確認応答を行えば、アクティブ表示からアラームを削除できます。確認応答したアラームは、[Acknowledged Alarms] ビューに移動されます。確認応答を行ったアラームを選択し、いつでも [Active] ビューに戻すことができます。

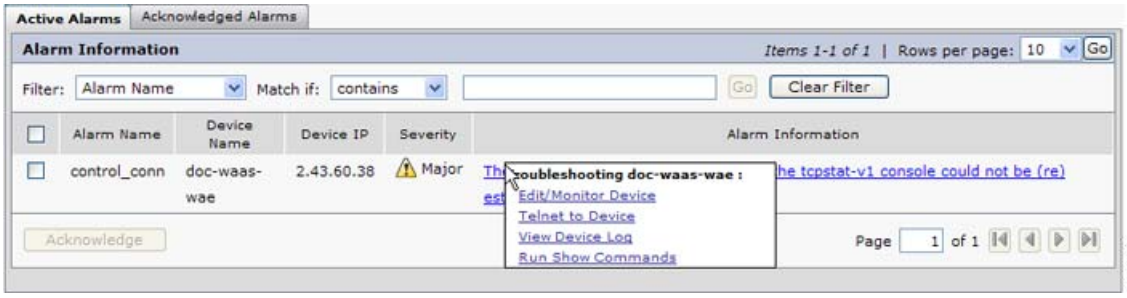
アラーム パネルで確認応答できるのはアクティブ アラームだけです。保留中、オフライン、非アクティブのアラームは、アラーム パネルで確認応答できません。

いずれかのビューの場合、アラーム パネルではリストにあるアラームのビューもフィルタできます。フィルタにより、設定した基準に一致するリスト内のアラームを見つけることができます。

[Alarm Information] 列の項目にマウスを合わせると、状況依存ポップアップ メニューが表示されます。ポップアップ メニューには、WAAS Central Manager GUI のトラブルシューティング ウィンドウとモニタリング ウィンドウへのリンクが表示されます。これらのリンクの詳細については、「アラートを使用したデバイスのトラブルシューティング」（P.16-6）を参照してください。

図 16-2 に、[System Dashboard] ウィンドウのアラーム パネルを示します。

図 16-2　[System Dashboard] ウィンドウのアラーム パネル



アクティブ アラームを確認応答して、[Active Alarms] セクションから別個の [Acknowledged Alarms] セクションに移動するには、次の手順を実行します。

ステップ 1　[System Dashboard] ウィンドウのアラーム パネルで、確認応答するアラームの名前の横にあるチェックボックスを選択します。

ステップ 2　[Acknowledge] ボタンをクリックします。

アラームに関するコメントを入力できるダイアログ ボックスがポップアップで表示されます。

ステップ 3　コメントを入力し、[OK] をクリックします。または、[Cancel] をクリックして、確認応答アクションを完了せずに [Active Alarm] パネルに戻ります。

コメントで、アラームを発生させた特定の問題の原因と解決方法に関する情報を共有できます。コメント フィールドには、最大 512 文字を入力できます。このフィールドでは、アルファベット、数字、特殊文字を組み合わせて使用できます。

アラームは [Acknowledged Alarms] タブに移動されます。

[System Dashboard] ウィンドウのアラーム パネルに表示されたアラームをフィルタおよびソートするには、次の手順に従ってください。

ステップ 1　[Filter] ドロップダウン リストから、次のいずれかのフィルタ オプションを選択します。

- [Alarm Name]

- [Device Name]
- [Device IP]
- [Severity]
- [Alarm Information]

ステップ 2　[Match if] ドロップダウン リストから、次のいずれかの一致条件を選択します。

- [contains]
- [starts with]
- [ends with]
- [is exactly]
- [not exactly]
- [not contain]
- [clear]

ステップ 3　テキスト入力フィールドに一致文字列を入力します。このフィールドには、特殊文字を含む英数字のテキストを入力できます。

ステップ 4　[Go] をクリックします。

ステップ 5　アラーム エントリをソートするには、列のヘッダーをクリックします。

エントリは、アルファベット順（ASCII 順）にソートされます。ソート順（昇順または降順）は、列のヘッダーにある矢印で示されます。上矢印は昇順を示します。

ステップ 6　フィルタをクリアするには、[Clear] をクリックします。

デバイス アラーム

デバイス アラームは、デバイス オブジェクトに関連付けられており、WAAS デバイスで動作するアプリケーションとサービスについて表示します。デバイス アラームは、報告するアプリケーションまたはサービスによって定義されます。また、デバイス アラームに、デバイスと WAAS Central Manager GUI との間で報告されている問題を反映させることもできます。表 16-1 で、表示可能なさまざまなデバイス アラームについて説明します。

表 16-1　問題報告用のデバイス アラーム

アラーム	アラーム重大度	デバイス ステータス	説明
[Device is offline]	クリティカル	オフライン	デバイスは WAAS Central Manager と通信できませんでした。
[Device is pending]	メジャー	保留	デバイス ステータスを決定できません。
[Device is inactive]	マイナー	非アクティブ	デバイスは、まだ WAAS Central Manager によってアクティブにされたり、受け付けられたりしていません。
[Device has lower software version]	マイナー	オンライン	デバイスは、ソフトウェア バージョンが WAAS Central Manager より古いため、一部の機能をサポートしません。

アラートを使用したデバイスのトラブルシューティング

WAAS Central Manager GUI では、[Troubleshooting Devices] ウィンドウでデバイスごとにアラームを表示し、デバイスをトラブルシューティングできます。

[Troubleshooting Devices] ウィンドウからデバイスのトラブルシューティングを実行するには、次の手順に従ってください。

ステップ 1　[WAAS Central Manager GUI navigation] ペインから、次のいずれかの方法で [Troubleshooting Devices] ウィンドウを起動します。

- [My WAN] > [Alerts] を選択して、すべてのデバイスでアラームを表示する。
- [My WAN] > [Manage Devices] を選択し、[Device Status] 列のデバイス アラーム ライト バーをクリックして 1 つのデバイス上のアラームを表示する。

[Troubleshooting Devices] ウィンドウは、[WAAS Central Manager] ウィンドウに、または別のポップアップ ウィンドウとして表示されます（図 16-3 を参照）。

図 16-3　[Troubleshooting Devices] ウィンドウ

ステップ 2　[Alarm Information] 列で、[Troubleshooting tools contextual] メニューが表示されるまで、アラーム メッセージの上にマウスを重ねます。ポップアップ メニューには、WAAS Central Manager GUI のトラブルシューティング ウィンドウとモニタリング ウィンドウへのリンクが表示されます。

ステップ 3　使用するトラブルシューティング ツールを選択し、リンクをクリックすると WAAS Central Manager GUI 内の適切なウィンドウに移動できます。表 16-2 で、デバイス アラームで使用可能なツールについて説明します。

表 16-2　デバイス アラーム用のトラブルシューティング ツール

項目	ナビゲーション	説明
ソフトウェアのアップデート	デバイスの [Jobs] > [Software Update] を選択します。	このデバイスの [Software Update] ウィンドウを表示します。デバイス ソフトウェア バージョンが Central Manager より低い場合のみ、表示されます。
デバイスの編集 / モニタ	[Device Dashboard]	設定用の [Device Dashboard] ウィンドウを表示します。

表 16-2　デバイス アラーム用のトラブルシューティング ツール （続き）

項目	ナビゲーション	説明
デバイスに対する Telnet	[Telnet] ウィンドウを開きます。	デバイス IP アドレスを使用して Telnet セッションを開始します。
デバイス ログの表示	デバイスの [Admin] > [Logs] を選択します。	このデバイス用にフィルタされたシステム メッセージ ログを表示します。
show コマンドの実行	デバイスの [Troubleshoot] > [CLI Commands] > [Show Commands] を選択します。	デバイスの **show** コマンド ツールを表示します。詳細については、「WAAS Central Manager GUI からの show コマンドと clear コマンドの使用」（P.16-66）を参照してください。

デバイス情報の表示

WAAS Central Manager GUI を使用すると、次の 2 つのウィンドウから、デバイスに関する基本情報および詳細情報を表示できます。

- 「[Devices] ウィンドウ」：デバイス ステータスやデバイスにインストールされている現在のソフトウェア バージョンのような各デバイスに関する基本的な情報とともに、WAAS ネットワーク内のすべてのデバイスのリストを表示します。
- 「[Device Dashboard] ウィンドウ」：インストールされているソフトウェア バージョンや、デバイスがオンラインであるかオフラインであるかなど、特定のデバイスに関する詳細な情報を表示します。

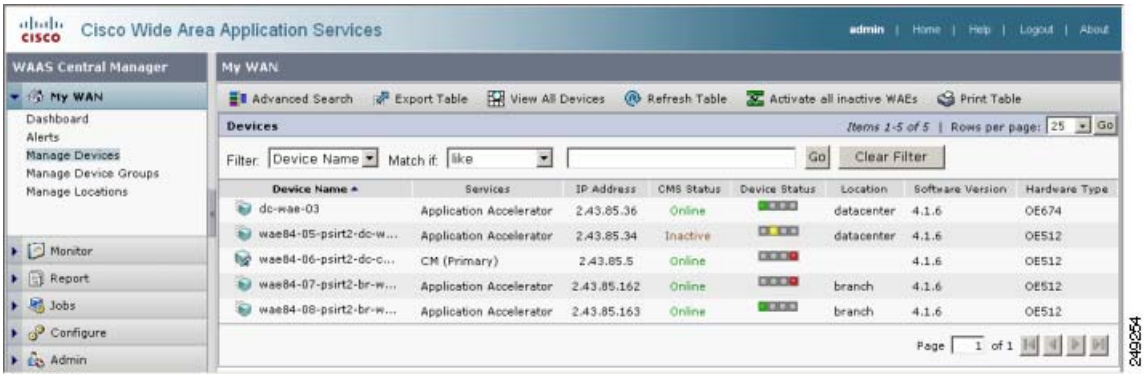
次の各項で、各ウィンドウについて説明します。

[Devices] ウィンドウ

[Devices] ウィンドウは、WAAS Central Manager に登録しているすべての WAAS デバイスを表示します。このリストを表示するには、WAAS Central Manager GUI で [My WAN] > [Manage Devices] を選択します。

図 16-4 に、[Devices] ウィンドウの例を示します。

図 16-4　[Devices] ウィンドウ



このウィンドウは、各デバイスに関する次の情報を表示します。

- デバイスで有効になっているサービス。これらのサービスの説明については、表 16-3 を参照してください。
- デバイスの IP アドレス。
- CMS ステータス（[Online]、[Offline]、[Pending]、または [Inactive]）。ステータスの詳細については、「デバイス アラーム」（P.16-5）を参照してください。
- デバイス ステータス。システム ステータスの報告メカニズムは、4 つのアラーム ライトを使用して、解決する必要がある問題を識別します。各ライトは、次のように異なるアラーム レベルを表します。
  - 緑色：アラームなし（システムは正常な状態）
  - 黄色：マイナー アラーム
  - オレンジ：メジャー アラーム
  - 赤：クリティカル アラーム

  アラーム ライト バーにマウスを合わせると、ポップアップ メッセージにアラーム数の詳細が表示されます。アラーム ライト バーをクリックして、デバイスをトラブルシューティングします。詳細については、「アラートを使用したデバイスのトラブルシューティング」（P.16-6）を参照してください。
- デバイスに関連付けられた位置。位置の詳細については、第 3 章「デバイス グループとデバイス位置の使用」を参照してください。特定の位置内にあるすべてのデバイスのデータを集計したレポートを表示できます（「位置レベル レポート」（P.16-36）を参照）。
- デバイスにインストールされ、動作しているソフトウェアのバージョン。
- デバイスのハードウェア タイプ。OE574 などのタイプが表示された場合、数字はモデル番号を示しています。この場合は、WAVE-574 です。NME-WAE は、NME-WAE モジュールを指し、SM-WAE は SM-SRE モジュールを指します。

WAAS Central Manager より高いソフトウェア バージョン レベルである WAE デバイスを赤で示します。また、スタンバイ WAAS Central Manager のバージョン レベルがプライマリ WAAS Central Manager と異なる場合、スタンバイ WAAS Central Manager を赤で示します。

リスト内のデバイスのビューは、リストの上にある [Filter] フィールドおよび [Match if] を使用してフィルタリングできます。テキスト フィールドにフィルタ文字列を入力し、[Go] ボタンをクリックしてフィルタを適用します。フィルタ設定が、リストの下に表示されます。フィルタをクリアしてすべてのデバイスを表示するには、[Clear Filter] ボタンをクリックします。フィルタにより、設定した基準に一致するリスト内のデバイスを見つけることができます。

表 16-3　サービスの説明

サービス	説明
[CM (Primary)]	デバイスは、プライマリ WAAS Central Manager として有効になっています。プライマリおよびスタンバイ Central Manager デバイスの詳細については、「スタンバイ Central Manager のプライマリ Central Manager への変換」（P.15-27）を参照してください。
[CM (Standby)]	デバイスは、スタンバイ WAAS Central Manager として有効になっています。プライマリおよびスタンバイ Central Manager デバイスの詳細については、「スタンバイ Central Manager のプライマリ Central Manager への変換」（P.15-27）を参照してください。
[Application Accelerator]	デバイスはアプリケーション アクセラレータとして有効になっています。

表 16-3　サービスの説明 （続き）

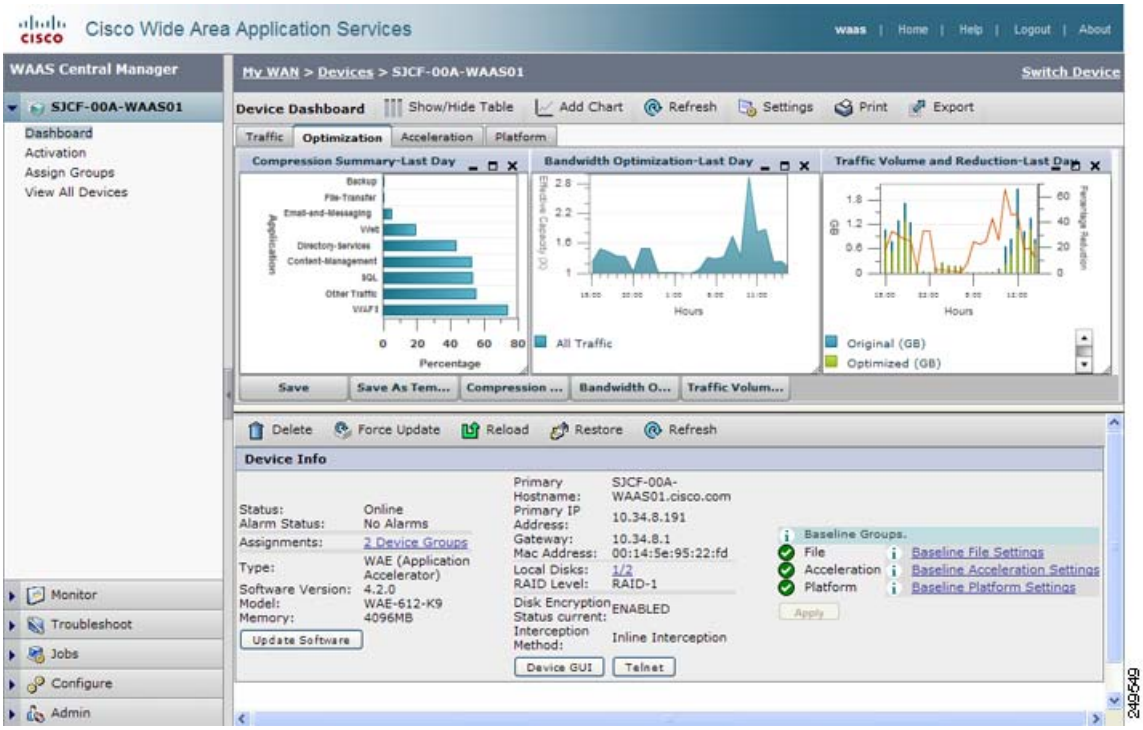
サービス	説明
[Replication Accelerator]	デバイスはレプリケーション アクセラレータとして有効になっています (4.0.19 以降の 4.0.x デバイスでのみサポートされます)。
[Edge]	デバイスはレガシー WAFS エッジ サービスが有効になっており、リモート ファイル サーバに保存されているデータを高速化できます。WAFS を有効にする方法については、第 11 章「WAFS の設定」を参照してください。
[Core]	デバイスはレガシー WAFS コア サービスが有効になっており、リモート ファイル サーバに保存されているデータを高速化できます。WAFS を有効にする方法については、第 11 章「WAFS の設定」を参照してください。
[Print]	デバイスはレガシー印刷サービスが有効になっているので、ブランチ オフィス クライアント用のプリント サーバとして機能できます。プリンタ サーバを設定する方法については、第 13 章「WAAS レガシー印刷サービスの設定および管理」を参照してください。

[Device Dashboard] ウィンドウ

[Device Dashboard] ウィンドウは、デバイス モデル、IP アドレス、代行受信方法、デバイス特有のチャートなど、WAAS デバイスに関する詳細な情報を表示します（図 16-5 を参照）。

[Device Dashboard] ウィンドウにアクセスするには、[My WAN] > [Manage Devices] へ進み、表示するデバイスの横にある [Edit] アイコンをクリックします。

図 16-5　[Device Dashboard] ウィンドウ



[Device Dashboard] ウィンドウから、次の作業を実行できます。

- 選択した WAE デバイスが処理するアプリケーション トラフィックに関するチャートとグラフを表示する（WAAS Central Manager デバイスが選択されていない場合、チャートまたはグラフは表示されません）。
- ウィンドウの一番上にあるチャート パネルに表示されたチャートをカスタマイズする。詳細については、「ダッシューボードまたはレポートのカスタマイズ」（P.16-10）を参照してください。個々のチャートについては、「チャートの説明」（P.16-14）で詳しく説明します。
- デバイスがオンラインかどうか、デバイスの IP アドレスとホスト名、デバイスで動作しているソフトウェア バージョン、およびデバイスが搭載しているメモリの量といった基本詳細を表示する。
- デバイスが属するデバイス グループを表示する。デバイス グループの詳細については、第 3 章「デバイス グループとデバイス位置の使用」を参照してください。
- デバイスで定義されているユーザを表示し、ロックされているすべてのユーザのロックを解除する。詳細については、「デバイス ユーザの表示とロックの解除」（P.16-10）を参照してください。
- [Update Software] をクリックして、デバイス上のソフトウェアを更新する。詳細については、第 15 章「WAAS システムの保守」を参照してください。
- [Device GUI] をクリックして、WAE Device Manager を開く。この GUI を使用してデバイスを管理する方法については、第 10 章「WAE Device Manager GUI の使用方法」を参照してください。
- [Telnet] をクリックして、デバイスとの Telnet セッションを確立し、CLI コマンドを発行する。
- デバイスをベースライン グループに割り当てる、または、割り当てを解除する。詳細については、第 3 章「デバイス グループとデバイス位置の使用」を参照してください。

デバイス ユーザの表示とロックの解除

デバイスで定義されているユーザを表示するには、[My WAN] > [Manage Devices] に進み、表示するデバイスの横にある [Edit] アイコンをクリックします。次にナビゲーション ペインで、[Device Users] を選択します（Central Manager デバイスで、[CM Users] を選択します）。

ユーザのリストが表で表示されます。この表には、ユーザ名、ログインの失敗回数、ログインの失敗回数の上限、および最後にログインを失敗した時刻が表示されます。ユーザに関する詳細を表示するには、該当するユーザの横にある [View] アイコンをクリックします。

失敗ログインの試行回数の上限に達したためにユーザがロックされた場合、ユーザ名の横にあるボックスを選択し、表の下の [Unlock] ボタンをクリックすることによってユーザのロックを解除できます。

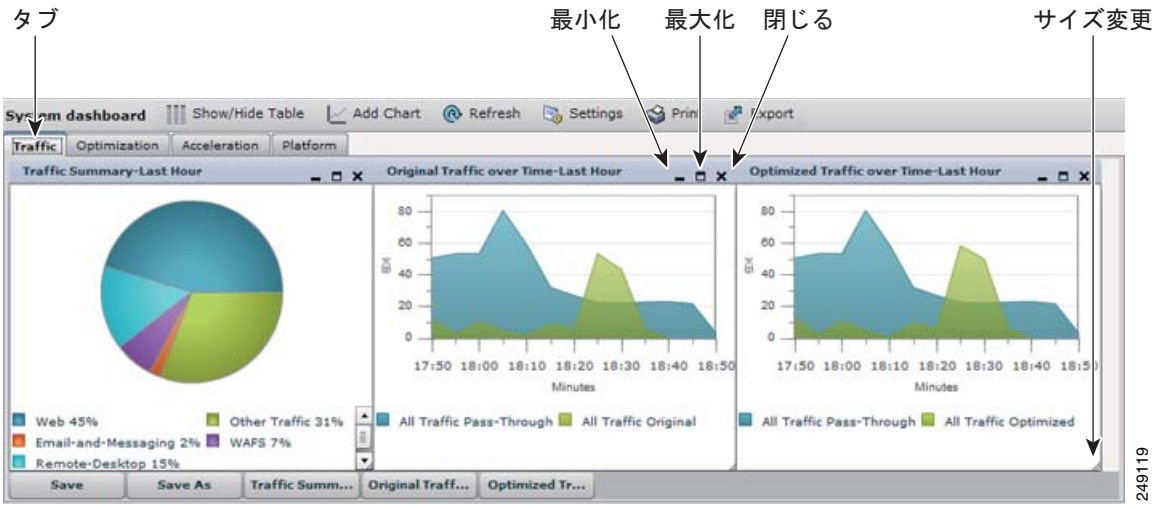
ダッシューボードまたはレポートのカスタマイズ

システムおよびデバイス ダッシュボードとレポートをカスタマイズできます。ダッシュボードとレポートは同じ方法で動作します。カスタム レポート作成の詳細については、「レポートの管理」（P.16-48）を参照してください。

ウィンドウの右上にあるチャート パネル（図 16-6 を参照）にタブがある場合、別のタブをクリックすれば別のチャートのグループを表示できます。

個別のチャート ペインの一番上にある [minimize]、[maximize]、および [close] の各ボタンを使用して、チャートの最小化や最大化を行ったり、チャートを閉じることができます。チャートを最大化している場合、[middle] ボタンは、チャートを小さなサイズで保存する [restore] ボタンに変更されます。タイトル バーをクリックして [chart] ペインを移動できます。[chart] ペインの右下にある [resize control] をクリックおよびドラッグしてチャートのサイズを変更できます。

図 16-6　チャート パネル



ダッシュボードの一番上にあるアイコンを使用すると、次を実行できます。

- [Show/Hide Table]：ウィンドウの下部にある表パネルを表示または非表示にします。システム ダッシュボードの場合、これは [Alarms] 表です。デバイス ダッシュボードの場合、[Device Information] 表です。[Dashboard] 表は固定で、変更することはできません。別の表をカスタム レポートに含めることができます。
- [Add Chart]：グラフ形式のチャートをチャート パネルに追加します。最大で 6 つのチャートを表示できます。チャートの追加の詳細については、「チャートの追加」（P.16-12）を参照してください。個々のチャートについては、「チャートの説明」（P.16-14）で詳しく説明します。
- [Refresh]：新しい情報でチャートを更新します。
- [Settings]：各チャートに表示されるデータ用に、期間と含まれるアプリケーションを設定します。これらの設定の詳細については、「チャートの設定」（P.16-12）を参照してください。
- [Print]：チャートおよび表のデータなどが出力されるレポートを印刷します。
- [Export]：チャートの統計情報データを CSV ファイルにエクスポートします。チャートの統計データは、少数第 1 位が四捨五入されて KB、MB、または GB で示されています。エクスポートされるデータは、正確なバイト値です。

チャート パネルの下のボタンを使用すると、次の作業を実行できます。

- [Save]：現在の設定でダッシュボードまたはレポートを保存します。次に表示するときに、これらの設定で表示されます。
- [Save As Template]：レポートを現在の設定で、新しい名前で保存します。ポップアップ ウィンドウにレポート名と、そのレポートに関する任意のメモを入力できます。入力できる文字は、数字、文字、スペース、ピリオド、ハイフン、およびアンダースコアです。レポートは、[Report] > [Manage Reports] ウィンドウで表示できます。
- [Chart Names]：名前の付いたチャートを表示または非表示にします。

チャートの追加

ダッシュボードまたはレポートにチャートを追加するには、次の手順に従ってください。

ステップ 1　ダッシュボードまたはレポートのチャート パネルで、タスクバーの [Add Chart] アイコンをクリックします。図 16-7 に示すように、[Add Chart] ウィンドウが表示されます。

図 16-7　　チャートの追加

ステップ 2　カテゴリの横にあるプラス記号をクリックして、チャート カテゴリを拡張します。

ステップ 3　表示する各チャートの横にあるボックスを選択します。個々のチャートについては、「チャートの説明」（P.16-14）で詳しく説明します。

レポートには最大 6 つのチャートを出力できます。

ステップ 4　[Add] をクリックします。

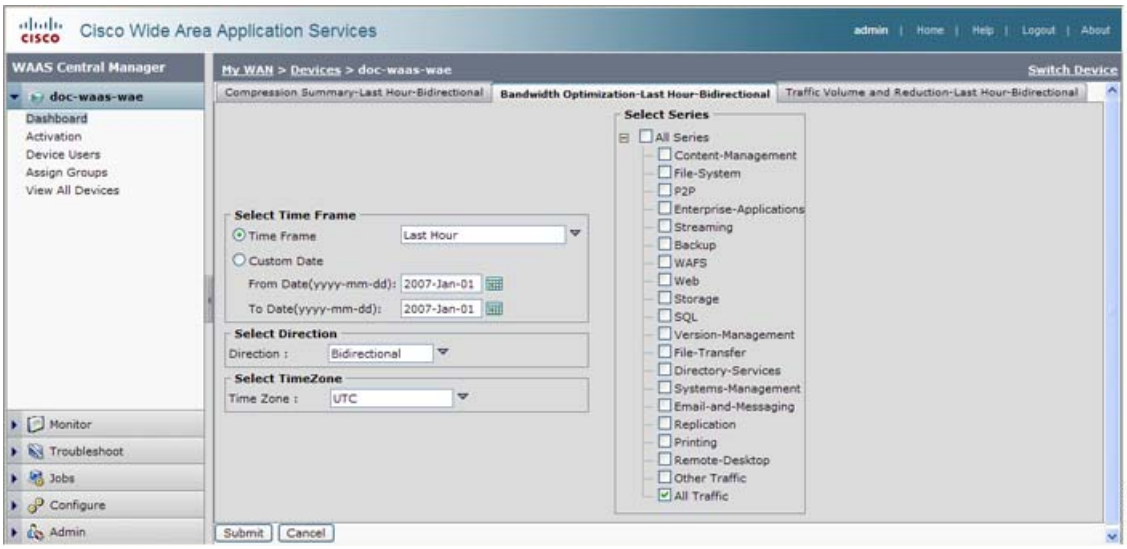
ダッシュボードまたはレポートからチャートを削除する場合は、そのチャートの [Close] ボタンをクリックし、レポートを保存します。

チャートの設定

チャートで示すデータを設定するには、次の手順に従ってください。

ステップ 1　ダッシュボードまたはレポートのチャート パネルで、タスクバーの [Settings] アイコンをクリックします。図 16-8 に示すように、[Settings] ウィンドウが表示されます。

図 16-8　　チャートの設定



ステップ 2　変更するチャートに対応するタブをクリックします。

ステップ 3　[Select Time Frame] 領域で、チャートの期間を選択します。適切なオプション ボタンをクリックして、次のいずれかのオプションを選択します。

- [Time Frame]：次のドロップダウン リストからいずれかの時間を選択します。
  - [Last Hour]：過去 1 時間のデータを 5 分周期（デフォルト）で表示します。「デフォルトのシステム設定プロパティの変更」（P.9-17）に説明されている System.monitoring.collectRate 設定を使用して、この周期を変更できます。
  - [Last Day]：過去 1 日のデータを（1 時間周期で）表示します。
  - [Last Week]：過去 1 週間のデータを（1 日周期で）表示します。
  - [Last Month]：過去 1 か月のデータを（1 日周期で）表示します。
- [Custom Date]：[From Date] フィールドに開始日付を入力し、[To Date] に終了日付を入力します。[calendar] アイコンをクリックして、ポップアップ カレンダーから日付を選択します。

（注）　現在の日付から 2 か月前の日付を越える範囲のカスタム日付が設定されているチャートを作成する場合、最新の 2 か月のデータが毎日のデータと共にプロットされ、以前のすべてのデータは、集約された毎月のデータと共にプロットされます。この動作により、最新の 2 か月のトラフィックが大幅に減少したように見えることがあります。これは、毎日のトラフィックの合計が、毎月のトラフィックの合計よりもかなり少ないためですが、これは通常です。

ステップ 4　[Direction] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [Bidirectional]：この WAAS デバイスを通じて LAN から WAN へ流れるトラフィックと WAN から LAN へ流れるトラフィックを含みます。
- [Inbound]：この WAAS デバイスを通じて WAN からクライアントへ流れるトラフィックを含みます。
- [Outbound]：この WAAS デバイスを通じてクライアントから WAN へ流れるトラフィックを含みます。

[Select Direction] 領域は、特定のデバイス レベル チャートを設定する場合に限り表示されます。

ステップ 5　[Time Zone] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [UTC]：レポートの時間帯を UTC に設定します。
- [CM Local Time]：レポートの時間帯を WAAS Central Manager の時間帯に設定します（デフォルト）。
- [**WAE** Local Time]：レポートの時間帯を WAE デバイスの時間帯に設定します。このオプションは、デバイス レベル チャートを設定する場合のみ表示されます。

ステップ 6　[Select Series] 領域では、プラス記号をクリックすると [All Series] リストを拡張します。チャートのデータに含める統計情報の対象とするアプリケーションの横に、チェック マークを付けます。このオプション領域は特定のチャート タイプにのみ適用されます。すべてのアプリケーションを含めるには、[All Traffic]（デフォルト）を選択します。

（注）　3 つを超えるアプリケーションを選択すると、面グラフ（比較）が読みやすい折れ線グラフに変換されます。これは、ユーザが選択可能なアプリケーションのチャートだけに適用されます。

ステップ 7　[Submit] をクリックします。

チャートの説明

この項では、選択してダッシュボードまたはレポートに含めることができるチャートについて説明します。次のカテゴリのチャートを使用できます。

- 「トラフィック分析に関するチャート」（P.16-14）
- 「最適化に関するチャート」（P.16-15）
- 「アクセラレーションに関するチャート」（P.16-18）
- 「プラットフォームに関するチャート」（P.16-34）

すべてのチャートは、チャートの設定が別の時間帯を使用するようにカスタマイズされていない限り、Central Manager のローカルの時間帯を使用してプロットされます。

トラフィック分析に関するチャート

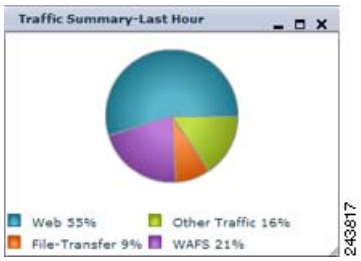
この項では、次のチャートについて説明します。

- 「[Traffic Summary]」（P.16-14）
- 「[Original Traffic Over Time]」（P.16-15）

[Traffic Summary]

[Traffic Summary] チャート（図 16-9 を参照）は最大比率のトラフィックを持つ上位 6 つのアプリケーションを示します。円グラフの各セクションは、ネットワークまたはデバイスでの合計トラフィックの比率（%）としてアプリケーションを表示します。分類されず、モニタされず、合計トラフィッが 2% 未満であるアプリケーションはともに [Other Traffic] という名前の 7 つめのカテゴリにグループ化されます。

図 16-9　[Traffic Summary] チャート



計算式：

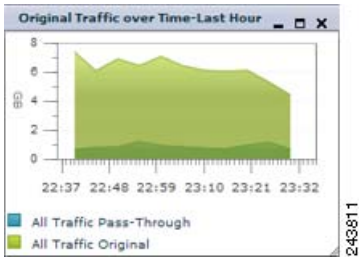
(アプリケーション トラフィック / 合計トラフィック) × 100

アプリケーション トラフィックとは、アプリケーションのオリジナル トラフィック（パススルー トラフィックを除くオリジナル + パススルー）です。

[Original Traffic Over Time]

[Original Traffic over Time] チャート（図 16-10 を参照）は、オリジナル トラフィックおよびパススルー トラフィックの量を示します。含めるアプリケーションを選択できます。デフォルトはすべてのトラフィックです。デフォルトでは、表示領域のチャートは面グラフです。3 を超えるアプリケーションを選択すると、折れ線グラフが使用されて読みやすくなります。

図 16-10　[Original Traffic Over Time] チャート



最適化に関するチャート

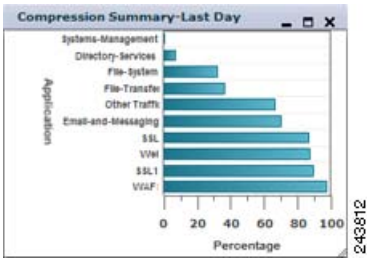
この項では、次のチャートについて説明します。

- 「[Compression Summary]」（P.16-16）
- 「[Compression Over Time]」（P.16-16）
- 「[Compression by Application Over Time]」（P.16-16）
- 「[Optimized Traffic Over Time]」（P.16-17）
- 「[Traffic Volume and Reduction]」（P.16-17）
- 「[Bandwidth Optimization]」（P.16-18）

[Compression Summary]

[Compression Summary] チャート（図 16-11 を参照）は、トラフィック量が多い上位 10 のアプリケーションについて、トラフィック低下率（パススルー トラフィックを除く）を棒グラフで示します。

図 16-11　[Compression Summary] チャート



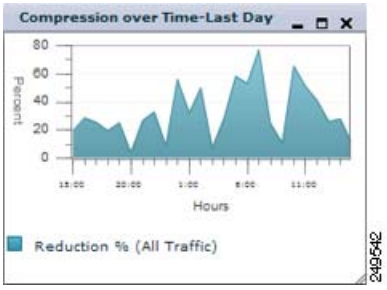
計算式：

パススルーを除く低下率（%）＝（パススルーを除くオリジナル – 最適化）/（パススルーを除くオリジナル）

[Compression Over Time]

[Compression over Time] チャート（図 16-12 を参照）は、WAAS 最適化手法を使用して軽減された合計トラフィックの比率（%）をグラフで示します。このチャートのデータには、パススルー トラフィックは含まれていません。

図 16-12　[Compression Over Time] チャート



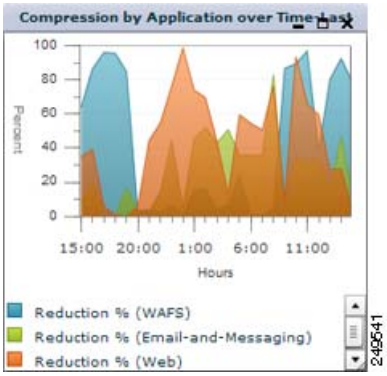
計算式：

低下率（%）＝（パススルーを除くオリジナル – 最適化）/（パススルーを除くオリジナル）

[Compression by Application Over Time]

[Compression by Application over Time] チャート（図 16-13 を参照）は、WAAS 最適化手法を使用して WAE デバイスで軽減された合計トラフィックの比率（%）をグラフで示します。このチャートのデータには、パススルー トラフィックは含まれていません。含めるアプリケーションを選択できます。デフォルトはすべてのトラフィックです。デフォルトでは、「[Compression Over Time]」チャートと同じ情報を示します。デフォルトでは、表示領域のチャートは面グラフです。3 を超えるアプリケーションを選択すると、折れ線グラフが使用されて読みやすくなります。

図 16-13　[Compression By Application Over Time] チャート



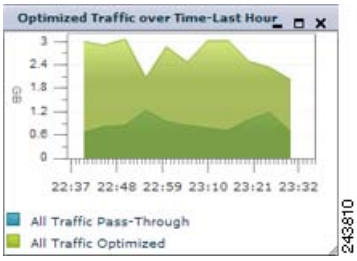
計算式：

低下率（%）＝ (パススルーを除くオリジナル – 最適化) / (パススルーを除くオリジナル)

[Optimized Traffic Over Time]

[Optimized Traffic over Time] チャート（図 16-14 を参照）は、WAE デバイスで最適化されたトラフィックおよびパススルー トラフィックの量をグラフで示します。左側に表示されるトラフィックの単位（バイト、KB、MB、または GB）は範囲によって異なります。デフォルトでは、表示領域のチャートは面グラフです。3 を超えるアプリケーションを選択すると、折れ線グラフが使用されて読みやすくなります。

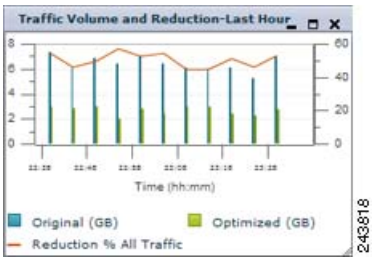
図 16-14　[Optimized Traffic Over Time] チャート



[Traffic Volume and Reduction]

[Traffic Volume and Reduction] チャート（図 16-15 を参照）は、オリジナルのトラフィックおよび最適化されたトラフィックの量と、トラフィック低下率（パススルー トラフィックを除く）を棒グラフで示します。左側に表示されるトラフィックの単位（バイト、KB、MB、または GB）は範囲によって異なります。トラフィック低下率の単位は、チャートの右側に表示されます。

図 16-15　[Traffic Volume and Reduction] チャート



計算式：

パススルーを除く低下率（%）= (パススルーを除くオリジナル – 最適化) / (パススルーを除くオリジナル)

[Bandwidth Optimization]

[Bandwidth Optimization] チャート（図 16-16 を参照）は、WAAS 最適化の結果、増加した WAN リンクの実効帯域幅容量を示します。値は 1X（倍）と 100X の間です。含めるアプリケーションを選択できます。デフォルトはすべてのトラフィックです。デフォルトでは、表示領域のチャートは面グラフです。3 を超えるアプリケーションを選択すると、折れ線グラフが使用されて読みやすくなります。

図 16-16　[Bandwidth Optimization] チャート

計算式：

実効 WAN 容量 = 1 / (1 - パススルーを除く低下率（%）)

パススルーを除く低下率（%）= (パススルーを除くオリジナル – 最適化) / (パススルーを除くオリジナル)

アクセラレーションに関するチャート

この項では、次のチャートについて説明します。

- 「HTTP」（P.16-19）
- 「CIFS」（P.16-21）
- 「MAPI」（P.16-25）
- 「NFS」（P.16-28）
- 「ビデオ」（P.16-31）
- 「SSL」（P.16-33）

HTTP

この項では、次のチャートについて説明します。

[HTTP: Estimated Time Savings]

[HTTP Estimated Time Savings] チャート（図 16-17 を参照）は、高速接続の再利用およびメタデータのキャッシングにより HTTP アクセラレータが短縮する応答時間の概算（%）をグラフで示します。

図 16-17　[HTTP: Estimated Time Savings] チャート

[HTTP: Connection Details]

[HTTP Connection Details] チャート（図 16-18 を参照）は、HTTP セッション接続統計情報を示します。この情報は、処理された接続の合計数と高速化されない（バイパスされた）接続の数を示します。表示領域のチャートは面グラフです。処理された接続の合計数が青で示され、緑で示されるバイパスされた接続数の下に表示されます。

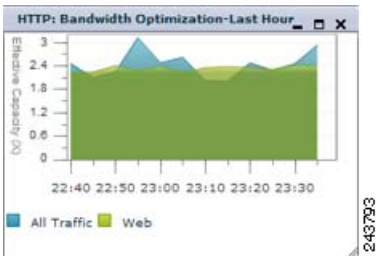
図 16-18　[HTTP Connection Details] チャート

[HTTP: Bandwidth Optimization]

[HTTP Bandwidth Optimization] チャート（図 16-19 を参照）は、HTTP アクセラレーションの結果の WAN リンクの実効帯域幅容量を元になる容量の乗数として示します。表示領域のチャートは面グラフです。全トラフィックのデータは青で示され、緑で示される Web（HTTP）トラフィックの下に表示されます。

チャートにデータが表示されない場合、この種類のトラフィックを含むアプリケーション定義のモニタリングが無効になっている可能性があります。Web アプリケーションのモニタリングが有効になっていることを確認してください。

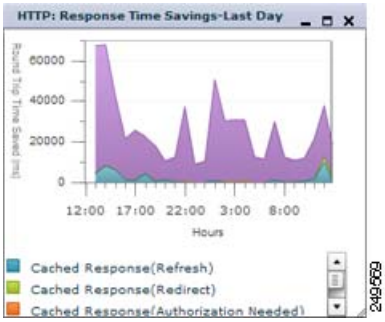
図 16-19　[HTTP Bandwidth Optimization] チャート



[HTTP: Response Time Savings]

[HTTP: Response Time Savings] チャート（図 16-20 を参照）は、メタデータのキャッシングおよび高速接続再利用の最適化により HTTP アクセラレータが短縮するラウンド トリップ応答時間をグラフで示します。これらは、異なる色で表示されます。表示領域のチャートは、積み上げ面グラフです。左側にある時間単位（ミリ秒、秒、または分）は、範囲によって決まります。

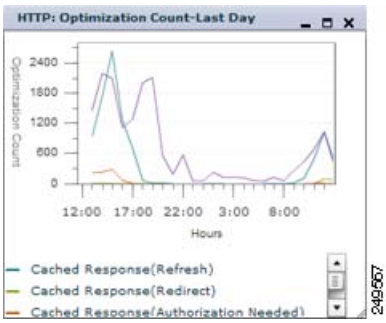
図 16-20　[HTTP Response Time Savings Chart]



[HTTP: Optimization Count]

[HTTP: Optimization Count] チャート（図 16-21 を参照）は、HTTP アクセラレータにより実行されたさまざまな種類の最適化の数をグラフで示します。これらは、異なる色で表示されます。このチャートに含まれる最適化は、高速接続の再利用とメタデータのキャッシングです。

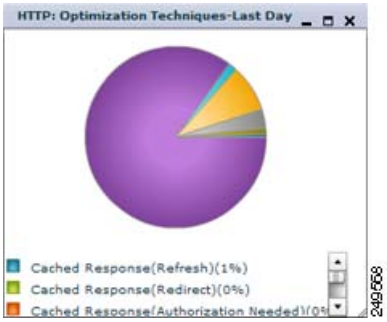
図 16-21　[HTTP: Optimization Count] チャート



[HTTP: Optimization Techniques]

[HTTP: Optimization Techniques] 円グラフ（図 16-22 を参照）は、HTTP アクセラレータにより実行されたさまざまな種類の最適化を示します。このチャートに含まれる最適化は、高速接続の再利用、メタデータのキャッシング、サーバ圧縮の停止、および DRE ヒントです。

図 16-22　[HTTP: Optimization Techniques] チャート



CIFS

この項では、次のチャートについて説明します。

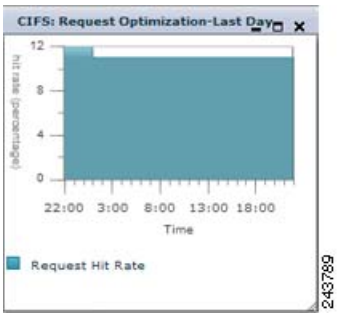
- 「[CIFS: Request Optimization]」（P.16-21）
- 「[CIFS: Cached Objects]」（P.16-22）
- 「[CIFS: Cache Utilization]」（P.16-22）
- 「[CIFS: Connection Statistics]」（P.16-23）
- 「[CIFS: File Optimization]」（P.16-23）
- 「[CIFS: Client Average Throughput]」（P.16-23）
- 「[CIFS: Connected CIFS Core Count]」（P.16-24）
- 「[CIFS: CIFS Edge-CIFS Core Traffic]」（P.16-24）
- 「[CIFS: Connected CIFS Edge Count]」（P.16-25）
- 「[CIFS: CIFS Core Traffic]」（P.16-25）

すべての CIFS に関するチャートは、デバイス レベルに限り使用可能です。使用可能な具体的なチャートは、透過的 CIFS アクセラレータ モード、WAFS レガシー モード（Edge デバイスとして）、WAFS レガシー モード（Core デバイスとして）など、デバイスのモードによって異なります。

[CIFS: Request Optimization]

[CIFS Request Optimization] チャート（図 16-23 を参照）は、CIFS キャッシュからローカルに処理された要求の比率（%）を示します。このチャートは、透過的 CIFS アクセラレータ モードまたは WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

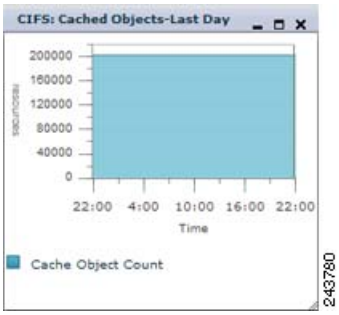
図 16-23　[CIFS Request Optimization] チャート



[CIFS: Cached Objects]

[CIFS Cached Objects] チャート（図 16-24 を参照）は、CIFS キャッシュ内のオブジェクトの数を示します。このチャートは、透過的 CIFS アクセラレータ モードまたは WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

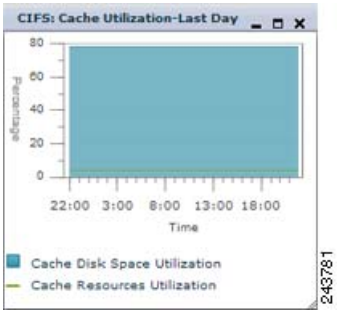
図 16-24　[CIFS Cached Objects] チャート



[CIFS: Cache Utilization]

[CIFS Cache Utilization] チャート（図 16-25 を参照）は、CIFS キャッシュの使用率を示します。このチャートは、透過的 CIFS アクセラレータ モードまたは WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

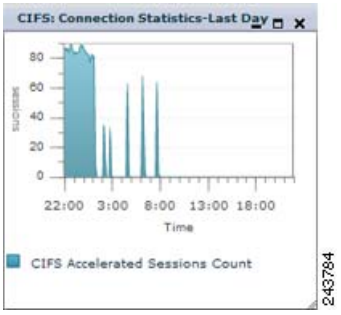
図 16-25　[CIFS Cache Utilization] チャート



[CIFS: Connection Statistics]

[CIFS Connection Statistics] チャート（図 16-26 を参照）は、加速化された CIFS セッション数を示します。このチャートは、透過的 CIFS アクセラレータ モードまたは WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

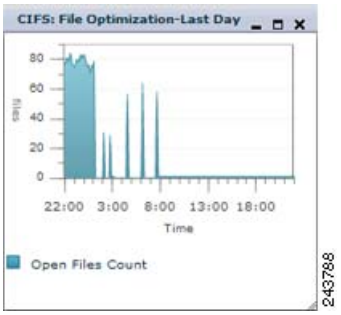
図 16-26　[CIFS Connection Statistics] チャート



[CIFS: File Optimization]

[CIFS File Optimization] チャート（図 16-27 を参照）は、開いている CIFS ファイルの数を示します。このチャートは、透過的 CIFS アクセラレータ モードまたは WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

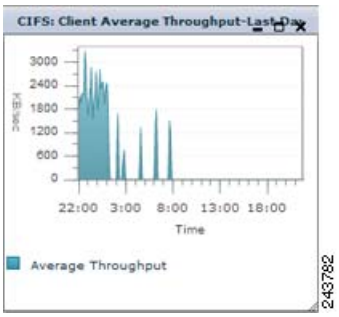
図 16-27　[CIFS File Optimization] チャート



[CIFS: Client Average Throughput]

[CIFS Client Average Throughput] チャート（図 16-28 を参照）は、WAAS デバイスとそのクライアントとの間の平均スループット（KB/秒）を示します。このチャートは、透過的 CIFS アクセラレータ モードまたは WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

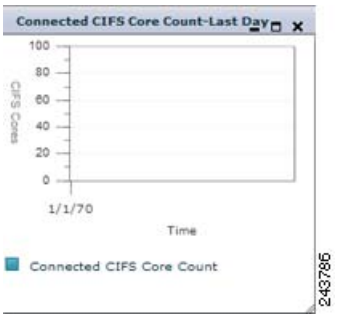
図 16-28　[CIFS Client Average Throughput] チャート



[CIFS: Connected CIFS Core Count]

[CIFS Connected CIFS Core Count] チャート（図 16-29 を参照）は、接続されている CIFS Core デバイスの数を示します。このチャートは、WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

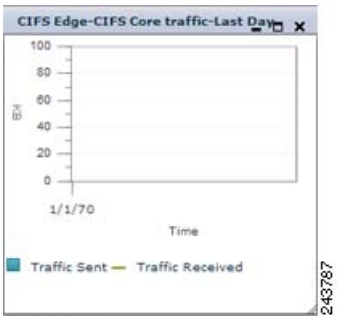
図 16-29　[CIFS Connected CIFS Core Count] チャート



[CIFS: CIFS Edge-CIFS Core Traffic]

[CIFS Edge-CIFS Core Traffic] チャート（図 16-30 を参照）は、Edge デバイスとこの Edge デバイスに接続されている CIFS Core デバイスとの間のトラフィック量を示します。このチャートは、WAFS レガシー モードで Edge デバイスとして動作するデバイスだけで使用できます。

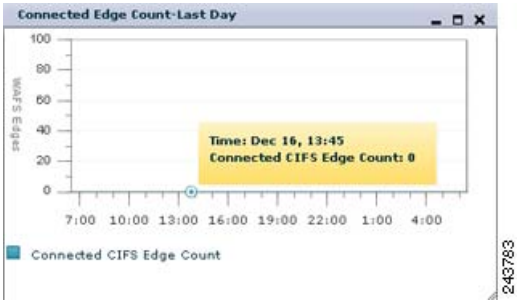
図 16-30　[CIFS Edge-CIFS Core Traffic] チャート



[CIFS: Connected CIFS Edge Count]

[CIFS Connected CIFS Edge Count] チャート（図 16-31 を参照）は、接続されている CIFS Edge デバイスの数を示します。このチャートは、WAFS レガシー モードで Core デバイスとして動作するデバイスだけで使用できます。

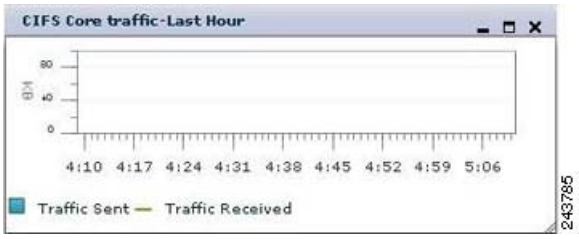
図 16-31　[CIFS Connected CIFS Edge Count] チャート



[CIFS: CIFS Core Traffic]

[CIFS Core Traffic] チャート（図 16-32 を参照）は、Core デバイスとこの Core デバイスに接続されている CIFS Edge デバイスとの間のトラフィック量を示します。このチャートは、WAFS レガシー モードで Core デバイスとして動作するデバイスだけで使用できます。

図 16-32　[CIFS Core Traffic] チャート



MAPI

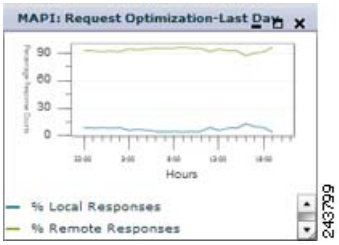
この項では、次のチャートについて説明します。

- 「[MAPI: Request Optimization]」（P.16-26）
- 「[MAPI: Response Time Optimization]」（P.16-26）
- 「[MAPI: Versions Detected]」（P.16-26）
- 「[MAPI: Estimated Time Savings]」（P.16-26）
- 「[MAPI: Connection Details]」（P.16-27）
- 「[MAPI: Acceleration Bypass Reason]」（P.16-27）
- 「[MAPI: Bandwidth Optimization]」（P.16-28）

[MAPI: Request Optimization]

[MAPI Request Optimization] チャート（図 16-33 を参照）は、ローカルおよびリモートの MAPI コマンドの応答の比率（%）を示します。ローカル応答とは、ピア WAE からの応答を待たずにクライアントに送信される応答です。リモート応答は、リモート サーバから受信します。

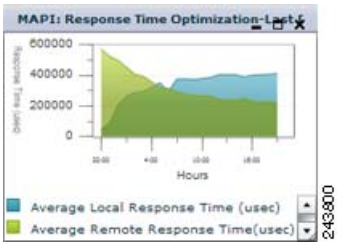
図 16-33　[MAPI Request Optimization] チャート



[MAPI: Response Time Optimization]

[MAPI: Response Time Optimization] チャート（図 16-34 を参照）は、ローカル MAPI 応答とリモート NFS 応答に使用される平均時間を比較します。左側にある時間単位（マイクロ秒、ミリ秒、秒、または分）は、範囲によって決まります。

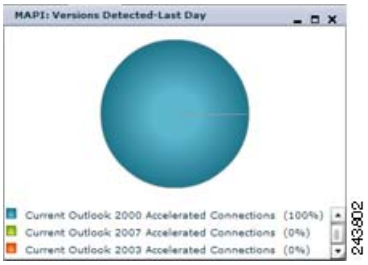
図 16-34　[MAPI Response Time Optimization] チャート



[MAPI: Versions Detected]

[MAPI Versions Detected] 円グラフ（図 16-35 を参照）は、異なるバージョン（2000、2003、2007）の Microsoft Outlook クライアントから検出された接続の数を示します。

図 16-35　[MAPI Versions Detected] チャート



[MAPI: Estimated Time Savings]

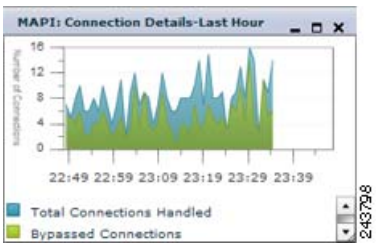
[MAPI Estimated Time Savings] チャート（図 16-36 を参照）は、MAPI アクセラレータが短縮する応答時間の概算（%）をグラフで示します。

図 16-36　[MAPI Estimated Time Savings] チャート

[MAPI: Connection Details]

[MAPI Connection Details] チャート（図 16-37 を参照）は、MAPI セッション接続統計情報を示します。この情報は、処理された接続の合計数および高速化されない（バイパスされた）接続の数を示します。表示領域のチャートは面グラフです。処理された接続の合計数が青で示され、緑で示されるバイパスされた接続数の下に表示されます。

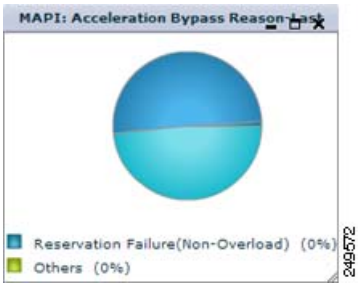
図 16-37　[MAPI Connection Details] チャート



[MAPI: Acceleration Bypass Reason]

[MAPI: Acceleration Bypass Reason] 円グラフ（図 16-38 を参照）は、MAPI トラフィックが高速化されない理由（予約の失敗（過負荷ではない理由で）、予約の失敗（過負荷）、MAPI 要求の署名、RPC パケットの不正な形式、ピアからのハンドオーバー要求、サポートされていないサーバ バージョン、ユーザが拒否リストに入っている、サポートされていないクライアント バージョン、セキュア接続（暗号化された）、サポートされていない DCERPC プロトコル バージョン、追跡されていない関連付けグループ、およびその他）を示します。

図 16-38　[MAPI Acceleration Bypass Reason] チャート

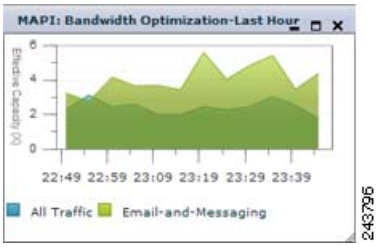


[MAPI: Bandwidth Optimization]

[MAPI Bandwidth Optimization] チャート（図 16-39 を参照）は、MAPI アクセラレーションの結果の WAN リンクの実効帯域幅容量を元になる容量の乗数として示します。表示領域のチャートは面グラフです。全トラフィックのデータは青で示され、緑で示される電子メールおよびメッセージング（MAPI）トラフィックの下に表示されます。

チャートにデータが表示されない場合、この種類のトラフィックを含むアプリケーション定義のモニタリングが無効になっている可能性があります。電子メールおよびメッセージング アプリケーションのモニタリングが有効になっていることを確認してください。

図 16-39　[MAPI Bandwidth Optimization] チャート



NFS

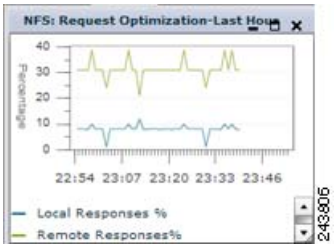
この項では、次のチャートについて説明します。

- 「[NFS: Request Optimization]」（P.16-28）
- 「[NFS: Response Time Optimization]」（P.16-29）
- 「[NFS: Versions Detected]」（P.16-29）
- 「[NFS: Estimated Time Savings]」（P.16-29）
- 「[NFS: Connection Details]」（P.16-30）
- 「[NFS: Acceleration Bypass Reason]」（P.16-30）
- 「[NFS: Bandwidth Optimization]」（P.16-30）

[NFS: Request Optimization]

[NFS Request Optimization] チャート（図 16-40 を参照）は、ローカルおよびリモートの NFS コマンドの応答の比率（%）を示します。ローカル応答とは、ピア WAE からの応答を待たずにクライアントに送信される応答です。リモート応答は、リモート サーバから受信します。

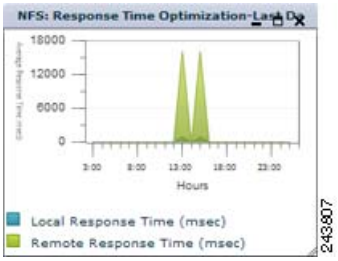
図 16-40　[NFS Request Optimization] チャート



[NFS: Response Time Optimization]

[NFS: Response Time Optimization] チャート（図 16-41 を参照）は、ローカル NFS 応答とリモート NFS 応答に使用される平均時間を比較します。左側にある時間単位（ミリ秒、秒、または分）は、範囲によって決まります。

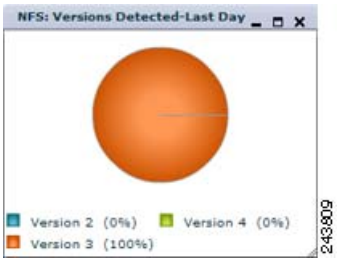
図 16-41　[NFS Response Time Optimization] チャート



[NFS: Versions Detected]

[NFS Versions Detected] 円グラフ（図 16-42 を参照）は、各 NFS バージョン（2、3、および 4）について検出された NFS メッセージの数を示します。NFS アクセラレータは NFS バージョン 3 トラフィックで動作するので、最良の結果を得るには、この種のトラフィックを検出します。

図 16-42　[NFS Versions Detected] チャート



[NFS: Estimated Time Savings]

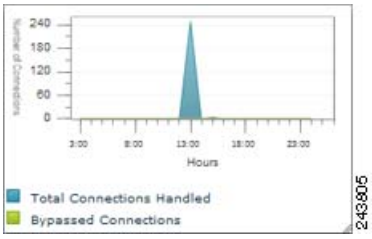
[NFS Estimated Time Savings] チャート（図 16-43 を参照）は、NFS アクセラレータが短縮する応答時間の概算（%）をグラフで示します。

図 16-43　[NFS Estimated Time Savings] チャート

[NFS: Connection Details]

[NFS Connection Details] チャート（図 16-44 を参照）は、NFS セッション接続統計情報を示します。この情報は、処理された接続の合計数と高速化されない（バイパスされた）接続の数を示します。表示領域のチャートは面グラフです。処理された接続の合計数が青で示され、緑で示されるバイパスされた接続数の下に表示されます。

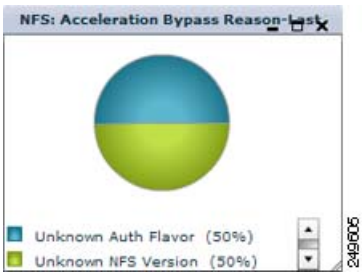
図 16-44　[NFS Connection Details] チャート



[NFS: Acceleration Bypass Reason]

[NFS Acceleration Bypass Reason] 円グラフ（図 16-45 を参照）は、NFS トラフィックが高速化されない理由（不明な認証の種類または不明な NFS バージョン）を示します。

図 16-45　[NFS Acceleration Bypass Reason] チャート

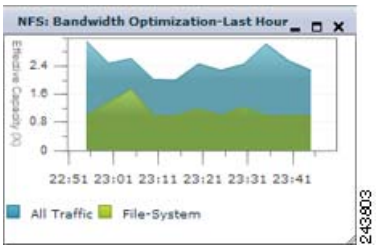


[NFS: Bandwidth Optimization]

[NFS Bandwidth Optimization] チャート（図 16-46 を参照）は、NFS アクセラレーションの結果の WAN リンクの実効帯域幅容量を元になる容量の乗数として示します。表示領域のチャートは面グラフです。全トラフィックのデータは青で示され、緑で示されるファイル システム（NFS）トラフィックの下に表示されます。

チャートにデータが表示されない場合、この種類のトラフィックを含むアプリケーション定義のモニタリングが無効になっている可能性があります。ファイル システム アプリケーションのモニタリングが有効になっていることを確認してください。

図 16-46　[NFS Bandwidth Optimization] チャート



ビデオ

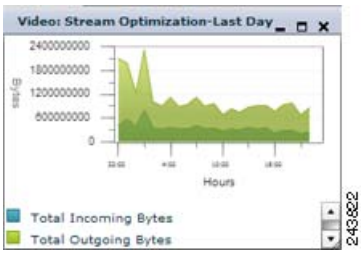
この項では、次のチャートについて説明します。

- 「[Video: Stream Optimization]」（P.16-31）
- 「[Video: Connection Details]」（P.16-31）
- 「[Video: Acceleration Bypass Reason]」（P.16-32）
- 「[Video: Bandwidth Optimization]」（P.16-32）

[Video: Stream Optimization]

[Video Stream Optimization] チャート（図 16-47 を参照）は、着信トラフィックの量と発信トラフィックの量を比較します。表示領域のチャートは面グラフです。着信の合計バイト数が青で示され、緑で示される発信の合計バイト数の下に表示されます。左側に表示されるトラフィックの単位（バイト、KB、MB、または GB）は範囲によって異なります。

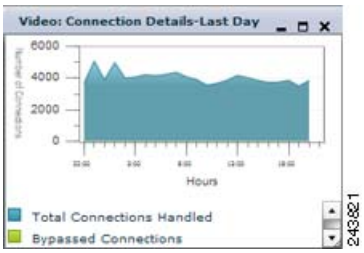
図 16-47　[Video Stream Optimization] チャート



[Video: Connection Details]

[Video Connection Details] チャート（図 16-48 を参照）は、ビデオ セッション接続統計情報を示します。この情報は、処理された接続の合計数および高速化されない（バイパスされた）接続の数を示します。表示領域のチャートは面グラフです。処理された接続の合計数が青で示され、緑で示されるバイパスされた接続数の下に表示されます。

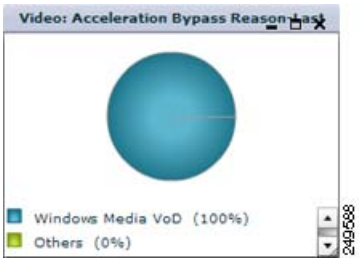
図 16-48　[Video Connection Details] チャート



[Video: Acceleration Bypass Reason]

[Video Acceleration Bypass Reason] 円グラフ（図 16-49 を参照）は、ビデオ トラフィックが高速化されない理由（Windows Media VOD、集約ビットレートの過負荷、他の理由、ストリーム ビットレートの過負荷、セッション カウントの過負荷、またはサポートされない伝送タイプ（つまり、サポートされない転送、サポートされないプレーヤー、またはサポートされないプロトコル））を示します。

図 16-49　[Video Acceleration Bypass Reason] チャート

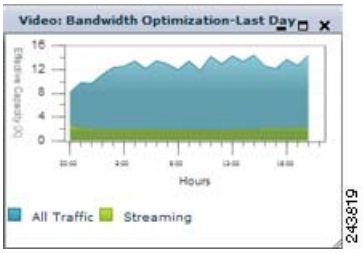


[Video: Bandwidth Optimization]

[Video: Bandwidth Optimization] チャート（図 16-50 を参照）は、ビデオ アクセラレーションの結果の WAN リンクの実効帯域幅容量を元になる容量の乗数として示します。表示領域のチャートは面グラフです。全トラフィックのデータは青で示され、緑で示されるストリーミング ビデオ トラフィックの下に表示されます。

チャートにデータが表示されない場合、この種類のトラフィックを含むアプリケーション定義のモニタリングが無効になっている可能性があります。ストリーミング アプリケーションのモニタリングが有効になっていることを確認してください。

図 16-50　[Video Bandwidth Optimization] チャート



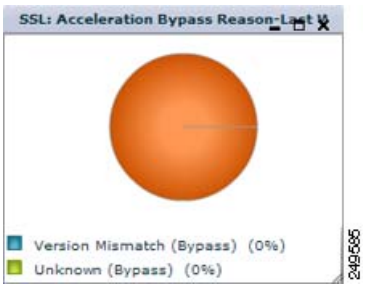
SSL

この項では、次のチャートについて説明します。

[SSL: Acceleration Bypass Reason]

[SSL Acceleration Bypass Reason] 円グラフ（図 16-51 を参照）は、SSL トラフィックが高速化されない理由（バージョンの不一致、不明、ドメインの不一致、暗号の不一致、取り消しエラー、証明書の認証エラー、他のエラー、および SSL 以外のトラフィック）を示します。

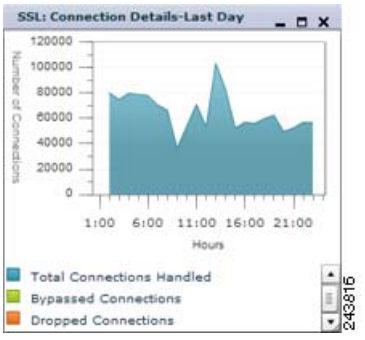
図 16-51　[SSL Acceleration Bypass Reason] チャート



[SSL: Connection Details]

[SSL Connection Details] チャート（図 16-52 を参照）は、SSL セッション接続統計情報を示します。この情報は、処理された接続の合計数、高速化されない（バイパスされた）接続の数、およびドロップされた接続の数を示します。表示領域のチャートは面グラフです。処理された接続の合計数は青で示され、緑で示されるバイパスされた接続の数の下に表示されます。バイパスされた接続の数は、オレンジで示されるドロップされた接続の数の下に表示されます。

図 16-52　[SSL Connection Details] チャート

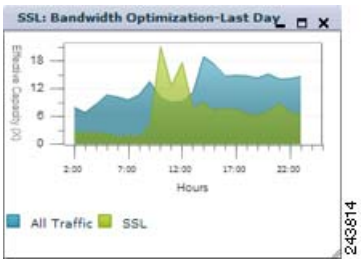


[SSL: Bandwidth Optimization]

[SSL Bandwidth Optimization] チャート（図 16-53 を参照）は、SSL アクセラレーションの結果の WAN リンクの実効帯域幅容量を元になる容量の乗数として示します。表示領域のチャートは面グラフです。全トラフィックのデータは青で示され、緑で示される SSL トラフィックの下に表示されます。

チャートにデータが表示されない場合、この種類のトラフィックを含むアプリケーション定義のモニタリングが無効になっている可能性があります。SSL アプリケーションのモニタリングが有効になっていることを確認してください。

図 16-53　[SSL Bandwidth Optimization] チャート



プラットフォームに関するチャート

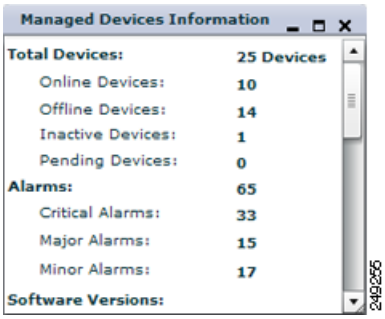
この項では、次のチャートについて説明します。

- 「[Managed Devices Information]」（P.16-34）
- 「[CPU Utilization]」（P.16-34）

[Managed Devices Information]

[Managed Devices Information] チャート（図 16-54 を参照）は、WAAS Central Manager が管理するデバイスの数、デバイス ステータス、アラームの数、およびソフトウェア バージョンに関する情報を示します。このチャートに表示されるデータをカスタマイズしたり、エクスポートしたりすることはできません。印刷は可能です。このチャートは、システム ダッシュボードの [Platform] タブにしか追加できません。

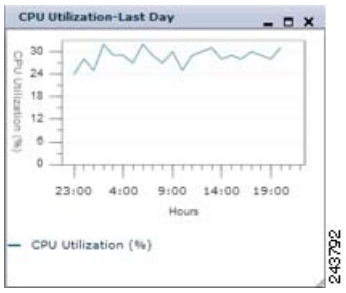
図 16-54　[Managed Devices Information] チャート



[CPU Utilization]

[CPU Utilization] チャート（図 16-55 を参照）は、デバイスの CPU 使用率を示します。このチャートは、特定の WAAS デバイスを選択した場合に限り使用できます。このチャートは、[Report] > [Manage Reports] > [CPU Usage] レポート ページで追加できる唯一のチャートです。

図 16-55　[CPU Utilization] チャート



定義済みのレポートを使用した WAAS のモニタ

WAAS Central Manager には、システム動作をモニタするために使用できる多くの定義済みのレポートがあります。これらのレポートは、ナビゲーション ペインの [Monitor] ドロワーにあります。レポートは、ウィンドウの下部に表示される統計情報の表および特定のチャートとグラフの組み合わせで構成されます。

「レポートの表示と編集」（P.16-50）の説明に従って、[Report] ドロワーの [Manage Report] 機能で編集することで、これらの定義済みレポートをカスタマイズできます。

次の定義済みレポートは、WAAS システム レベル、位置レベル、および WAE デバイス レベルで使用できます。

- 最適化
  - 「トラフィック概要レポート」（P.16-36）
  - 「最適化概要レポート」（P.16-39）
  - 「最適化の詳細レポート」（P.16-39）
- アクセラレーション
  - 「HTTP アクセラレーション レポート」（P.16-40）
  - 「ビデオ アクセラレーション レポート」（P.16-41）
  - 「SSL アクセラレーション レポート」（P.16-42）
  - 「MAPI アクセラレーション レポート」（P.16-42）
  - 「NFS アクセラレーション レポート」（P.16-43）

次の定義済みレポートは、WAAS システム レベルおよび WAE デバイス レベルでだけ使用できます。

- 「トポロジ レポート」（P.16-44）

次の定義済みレポートは、WAE デバイス レベルだけで使用できます。

- 最適化
  - 「接続統計情報レポート」（P.16-45）
- アクセラレーション
  - 「CIFS アクセラレーション レポート」（P.16-47）
- プラットフォーム
  - 「CPU 統計情報レポート」（P.16-47）
  - 「ディスク レポート」（P.16-48）

（注）　1,000 以上の WAE が存在する WAAS ネットワークでは、表の列をクリックしてシステム レベルのレポートの表を再ソートすると、表を再表示するまでに最大 90 秒の遅延が発生する可能性があります。タスクバーの [Print] アイコンをクリックした場合にも、PDF レポートが表示されるまでに同様の遅延が発生することがあります。

位置レベル レポート

位置レベル レポートでは、特定の位置内にあるすべての WAE からのデータが集計されます。位置の詳細については、「デバイス位置の操作」（P.3-14）を参照してください。

位置レベル レポートを表示するには、次の手順を実行します。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Locations] を選択します。

ステップ 2　レポートを表示する位置の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Monitor] を選択し、[Optimization] メニューまたは [Acceleration] メニューからレポートを選択します。

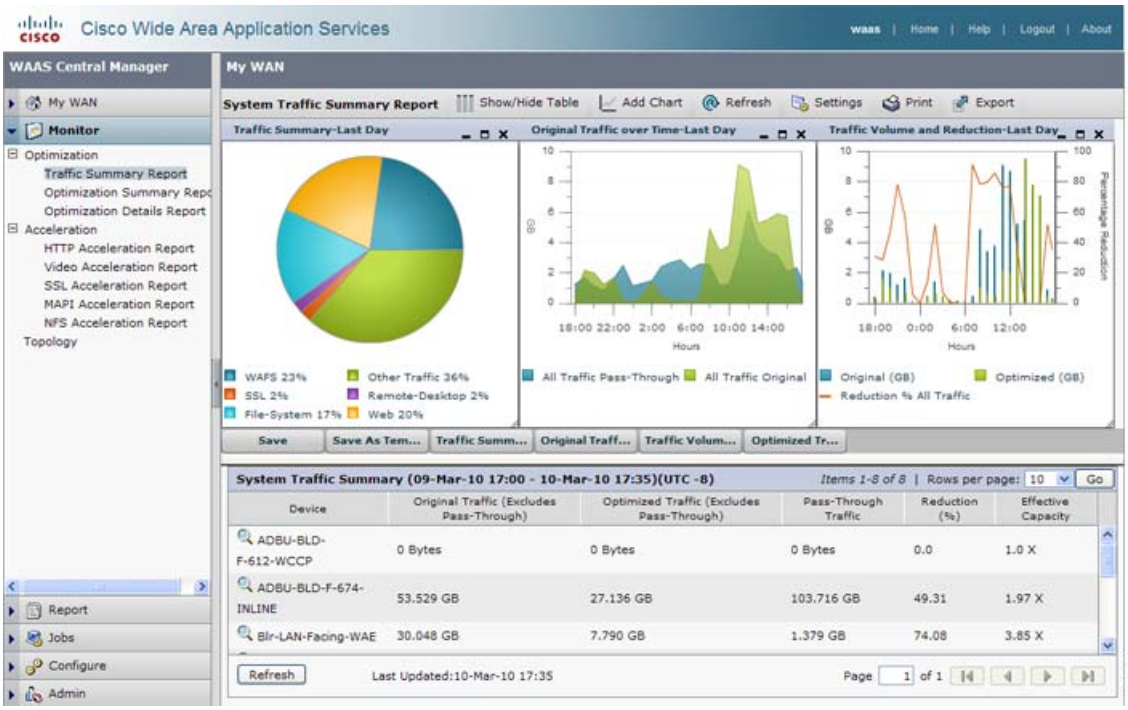
レポートをスケジューリングする場合は、任意の数の位置を選択することも可能で、レポートには選択したすべての位置内のすべてのデバイスのデータが含まれます。詳細については「レポートのスケジューリング」（P.16-51）を参照してください。

位置レベル レポートでサポートされるデバイスの最大数は、デフォルトで 25 です。この数は、System.monitoring.maxDevicePerLocation システム プロパティによって最大 250 にまで変更可能です。詳細については「デフォルトのシステム設定プロパティの変更」（P.9-17）を参照してください。

トラフィック概要レポート

トラフィック概要レポート（図 16-56 を参照）は、全トラフィックの概要を示します。

図 16-56　トラフィック概要レポート



次のチャートが含まれます。

- 「[Traffic Summary]」（P.16-14）
- 「[Original Traffic Over Time]」（P.16-15）
- 「[Traffic Volume and Reduction]」（P.16-17）
- 「[Optimized Traffic Over Time]」（P.16-17）（このチャートは最小化されています）

[Traffic Summary] 表は、チャートの下に表示されます。システム レベルおよび位置レベルでは、表の各行はこの Central Manager に登録されているか、またはこの位置内にある各デバイスの合計トラフィック情報を示します。デバイス レベルでは、表の各行が、デバイスで定義された各アプリケーションの合計トラフィック情報を示します。データについては、表 16-4 を参照してください。

任意の列見出しをクリックすると、表がソートされ、その列のデータ順に並べ替えられます。表がその列でソートされていることを示すために、見出しの下に小さい三角形のコントロールが現れます。この三角形をクリックすると、列のソート順が反転します。

一部の値では、システム レベルとデバイス レベルで異なる計算式が使用されます。これらの計算式は、表に記載されています。表で使用される用語は、次のように定義されています。

- オリジナルの着信：LAN（クライアント）から WAE に入るトラフィック。このトラフィックは、ピア WAE に向けて WAN で送信される前に最適化される必要があります。
- オリジナルの発信：ピア WAE から WAN で受信した後で、LAN（クライアント）に向けて WAE から出るトラフィック。
- 最適化された着信：WAN から WAE に入るトラフィック。このトラフィックは、クライアントに向けて LAN で送信される前に処理（最適化戻し）を行われる必要があります。
- 最適化された発信：最適化された後で、WAN およびピア WAE に向けて WAE から出るトラフィック。
- パススルー：WAE を通過し、最適化されていないトラフィック。

システム レベル、位置レベル、およびデバイス グループ レベルの統計情報を取得するには、全デバイスのオリジナルの着信、オリジナルの発信、最適化された着信、最適化された発信、パススルー クライアント、およびパススルー サーバのバイトを合計する必要があります。低下率（%）（パススルーを含む）、低下率（%）（パススルーを除く）、および実効容量の値は、すべてのデバイスのこれらの足された値を使用して計算されます。

表 16-4　[Traffic Summary] 表

表の列	説明と値の計算に使用される計算式
[Device]	デバイス名（システム レベルおよび位置レベルでしか表示されません）。
[Application]	アプリケーション名（デバイス レベルだけで表示されます）。
[Original Traffic (Excludes Pass-Through)]	パススルー トラフィックを除くオリジナル トラフィックの量を報告します。 システム：(オリジナルの発信 + オリジナルの着信)/2 デバイス/デバイス グループ：オリジナルの着信 + オリジナルの発信
[Optimized Traffic (Excludes Pass-Through)]	パススルー トラフィックを除く最適化されたトラフィックの量を報告します。 システム：(最適化された着信 + 最適化された発信)/2 デバイス/デバイス グループ：最適化された発信 + 最適化された着信
[Pass-Through Traffic]	パススルー トラフィックの量を報告します。 システム：(パススルー クライアント + パススルー サーバ)/2 デバイス/デバイス グループ：パススルー クライアント + パススルー サーバ 列見出しに表示されたアスタリスク（*）は、この表にデータが含まれるデバイスが他のデバイスでシリアル ピアとして設定されており、その 2 つのピア デバイス間では最適化が無効になっていることを示します。そのピアから送られるデバイス パススルー トラフィックが原因で、パススルー トラフィックの量が予想される量より多く表示されている可能性があります（詳細については、「インライン WAE のクラスタリング」（P.4-51）を参照してください）。[1]
[Reduction (%)]	節約されたバイトの比率を報告します。最適化されたトラフィックだけが対象です。 (パススルーを除くオリジナル – (最適化)) × 100 / (パススルーを除くオリジナル)
[Effective Capacity]	最適化の結果の WAN リンクの実効帯域幅容量を報告します。値は、元の容量の乗数です。最適化されたトラフィックだけが対象です。 1/(1 – パススルーを除く低下率（%）)

1. [Pass-Through Traffic] 列の数は、この特定の WAE（位置レポートの場合、その位置内のすべてのデバイス）を通過したトラフィックの量を示します。デバイスがシリアル インライン クラスタの一部である場合（つまり、別のデバイスで非最適化ピアとして設定されている場合）、あるデバイスでパススルーとして示されるトラフィックは、シリアル クラスタ内の別のデバイスによって最適化されている可能性があります。クラスタ内のいずれのデバイスによっても最適化されない、つまり、クラスタ全体を通過するトラフィックの量を把握することは役立ちます。

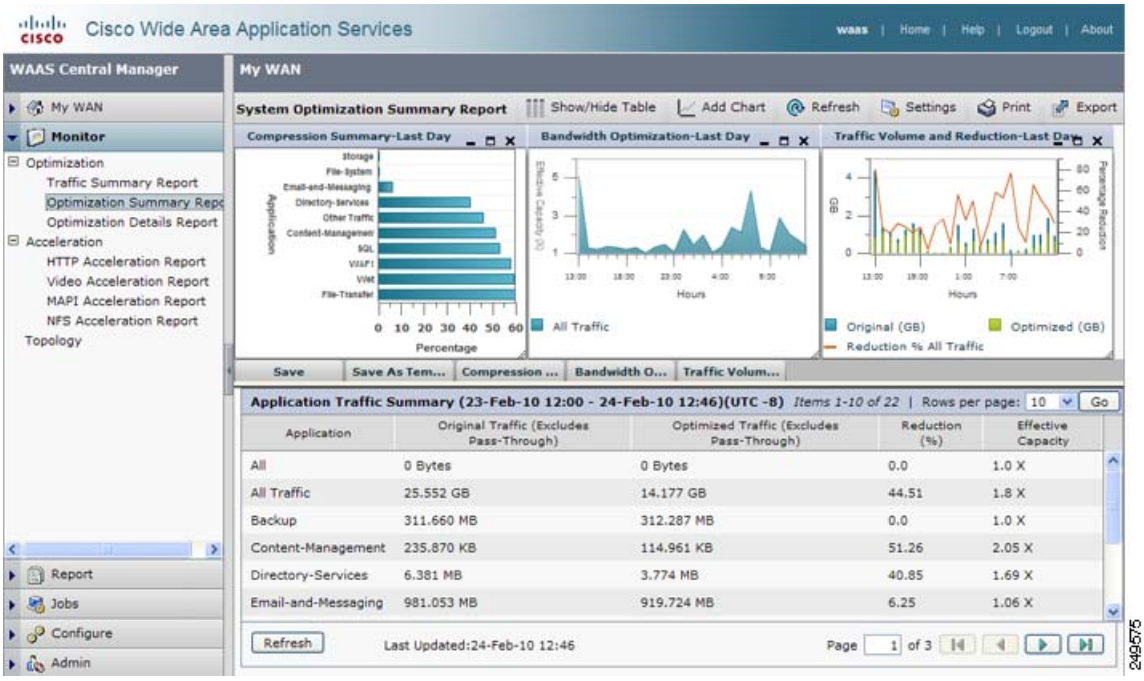
   LAN に近いデバイスが過負荷になっていない場合、このデバイスのパススルーの数字は、パススルー トラフィック全体を正確に示しています。しかし、このデバイスが過負荷になると、クラスタ内の 2 つめのデバイスが、1 つめのデバイスが通過させたトラフィックの最適化を開始します。この点は、考慮する必要があります。この場合、このクラスタのパススルー全体の数字は、次のように算出できます。この計算は、1 つめのデバイスが過去に過負荷になり、その後解消した場合にも実行する必要があります。

   たとえば、W1 と W2 がシリアル クラスタの一部であり、W1 が LAN に向いており（クラスタがブランチの場合はクライアントに近く、クラスタがデータセンターの場合はサーバに近い）、W2 は WAN に向いているとします。W1 または W2 のいずれによっても最適化されずにクラスタを通過するトラフィックの量は、(W1 パススルー トラフィック) – (W2 オリジナル トラフィック) という計算式で算出できます。

最適化概要レポート

最適化概要レポート（図 16-57 を参照）は、最適化の概要を示します。

図 16-57　　最適化概要レポート



次のチャートが含まれます。

- 「[Compression Summary]」（P.16-16）
- 「[Bandwidth Optimization]」（P.16-18）
- 「[Traffic Volume and Reduction]」（P.16-17）

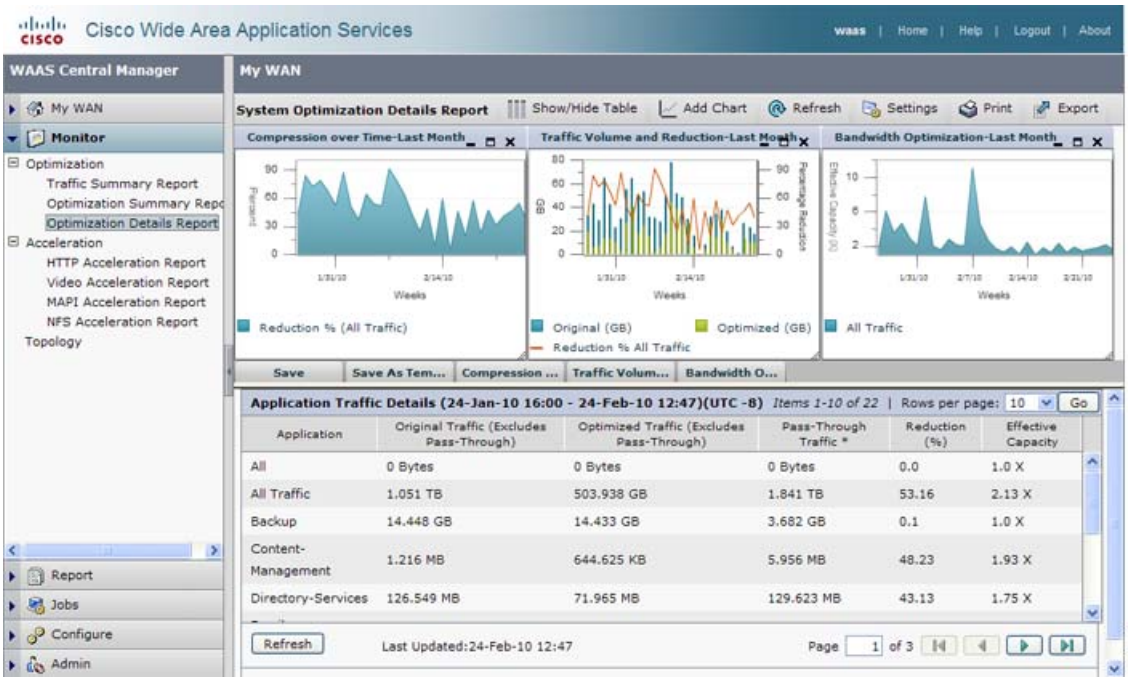
[Application Traffic Summary] 表は、チャートの下に表示されます。表の各行は、各アプリケーションの合計トラフィック情報を示します。列の説明および値の計算に使用される計算式は、表 16-4 に記載されています。次の列しか含まれません。

- [Application]
- [Original Traffic (Excludes Pass-Through)]
- [Optimized Traffic (Excludes Pass-Through)]
- [Reduction (%)]（これにはパススルー トラフィックは含まれません）
- [Effective Capacity]（これにはパススルー トラフィックは含まれません）

最適化の詳細レポート

[Optimization Details] レポート（図 16-58 を参照）には、最適化の詳細が表示されます。

図 16-58　[Optimization Details] レポート



次のチャートが含まれます。

- 「[Compression Over Time]」（P.16-16）
- 「[Traffic Volume and Reduction]」（P.16-17）
- 「[Bandwidth Optimization]」（P.16-18）

[Application Traffic Details] 表が、チャートの下に表示されます。表の各行は、各アプリケーションの合計トラフィック情報を示します。列の説明および値の計算に使用される計算式は、表 16-4 に記載されています。次の列しか含まれません。

- [Application]
- [Original Traffic (Excludes Pass-Through)]
- [Optimized Traffic (Excludes Pass-Through)]
- [Pass-Through Traffic]
- [Reduction (%)]（これにはパススルー トラフィックは含まれません）
- [Effective Capacity]（これにはパススルー トラフィックは含まれません）

HTTP アクセラレーション レポート

HTTP アクセラレーション レポート は、HTTP アクセラレーションの統計情報を示します。

2 つのタブには、次のチャートが含まれます。

- [Summary] タブ：
  - 「[HTTP: Estimated Time Savings]」（P.16-19）
  - 「[HTTP: Bandwidth Optimization]」（P.16-19）

- 「[HTTP: Connection Details]」（P.16-19）

- [Details] タブ：
  - 「[HTTP: Response Time Savings]」（P.16-20）
  - 「[HTTP: Optimization Count]」（P.16-20）
  - 「[HTTP: Optimization Techniques]」（P.16-21）

[HTTP Acceleration Statistics] 表は、チャートの下に表示されます。表の各行は、この Central Manager に登録されている各デバイスの統計情報を表示します。データについては、表 16-5 を参照してください。

表 16-5　[HTTP Acceleration Statistics] 表

表の列	説明と値の計算に使用される計算式
[Device]	デバイス名
[New Connections Handled]	この期間に処理された HTTP 接続の数を報告します。
[Active Connections]	HTTP アクセラレータで現在処理されている接続の数を報告します。
[New Bypassed Connections]	最初に HTTP アクセラレータで受信され、汎用アクセラレータにプッシュされた接続の数を報告します。
[Total Time Saved]	HTTP 最適化により短縮された時間を報告します。
[Total Round-Trip Time]	すべての接続の合計ラウンド トリップ時間とリモートで提供されるメタデータ キャッシュ失敗の時間を足した値を報告します。
[% Time Saved]	すべての集約サンプルについて短縮された接続時間の比率（%）を報告します。 短縮された合計時間 / (短縮された合計時間 + 全ての接続の合計ラウンド トリップ時間 + リモートで提供されるすべてのメタデータ キャッシュ失敗の合計時間)

ビデオ アクセラレーション レポート

ビデオ アクセラレーション レポートは、ビデオ アクセラレーションの統計情報を示します。

2 つのタブには、次のチャートが含まれます。

- [Summary] タブ：
  - 「[Video: Stream Optimization]」（P.16-31）
  - 「[Video: Bandwidth Optimization]」（P.16-32）
  - 「[Video: Connection Details]」（P.16-31）

- [Details] タブ：
  - 「[Video: Acceleration Bypass Reason]」（P.16-32）

[Video Acceleration Statistics] 表は、チャートの下に表示されます。表の各行は、この Central Manager に登録されている各デバイスの統計情報を表示します。データについては、表 16-6 を参照してください。

表 16-6　[Video Acceleration Statistics] 表

表の列	説明
[Device]	デバイス名
[New Connections Handled]	この期間に処理されたビデオ接続の数を報告します。
[Active Connections]	ビデオ アクセラレータで現在処理されている接続の数を報告します。
[New Bypassed Connections]	最初にビデオ アクセラレータで受信され、汎用アクセラレータにプッシュされた接続の数を報告します。

SSL アクセラレーション レポート

SSL アクセラレーション レポートは、SSL アクセラレーションの統計情報を示します。

次のチャートが含まれます。

- 「[SSL: Bandwidth Optimization]」（P.16-33）
- 「[SSL: Connection Details]」（P.16-33）
- 「[SSL: Acceleration Bypass Reason]」（P.16-33）

[SSL Acceleration Statistics] 表は、チャートの下に表示されます。表の各行は、この Central Manager に登録されている各デバイスの統計情報を表示します。データについては、表 16-7 を参照してください。

表 16-7　[SSL Acceleration Statistics] 表

表の列	説明
[Device]	デバイス名
[Handled Connections]	この期間に処理された SSL 接続の数を報告します。
[Active Connections]	SSL アクセラレータで現在処理されている接続の数を報告します。
[Dropped Connections]	SSL アクセラレータでドロップされた接続の数を報告します。
[Bypassed Connections]	最初に SSL アクセラレータで受信され、汎用アクセラレータにプッシュされた接続の数を報告します。

MAPI アクセラレーション レポート

MAPI アクセラレーション レポートは、MAPI アクセラレーションの統計情報を示します。

2 つのタブには、次のチャートが含まれます。

- [Summary] タブ：
  - 「[MAPI: Estimated Time Savings]」（P.16-26）
  - 「[MAPI: Bandwidth Optimization]」（P.16-28）
  - 「[MAPI: Connection Details]」（P.16-27）
- [Details] タブ：
  - 「[MAPI: Request Optimization]」（P.16-26）
  - 「[MAPI: Response Time Optimization]」（P.16-26）
  - 「[MAPI: Versions Detected]」（P.16-26）

– 「[MAPI: Acceleration Bypass Reason]」（P.16-27）

[MAPI Acceleration Statistics] 表は、チャートの下に表示されます。表の各行は、この Central Manager に登録されている各デバイスの統計情報を表示します。データについては、表 16-8 を参照してください。

表 16-8　[MAPI Acceleration Statistics] 表

表の列	説明と値の計算に使用される計算式
[Device]	デバイス名
[New Connections Handled]	この期間に処理された MAPI 接続の数を報告します。
[Active Connections]	MAPI アクセラレータで現在処理されている接続の数を報告します。
[New Bypassed Connections]	最初に MAPI アクセラレータで受信され、汎用アクセラレータにプッシュされた接続の数を報告します。
[New Local Request Count]	WAE でローカル処理されたクライアント要求の数を報告します。
[Avg. Local Response Time]	ローカル応答に費やされた平均時間（マイクロ秒単位）を報告します。
[New Remote Request Count]	WAN 経由でリモート処理されたクライアント要求の数を報告します。
[Avg. Remote Response Time]	リモート応答に費やされた平均時間（マイクロ秒単位）を報告します。
[% Time Saved]	すべての集約サンプルについて短縮された接続時間の比率（%）を報告します。 (Down – Up) × 100 / (Down) If(Down != 0) ここでは次のとおりです。 Down = (新規のローカル要求数 + 新規のリモート要求数) × 平均ローカル応答時間 Up = ((新規のローカル要求数 × 平均ローカル応答時間) + (新規のリモート要求数 × 平均リモート応答時間))

NFS アクセラレーション レポート

NFS アクセラレーション レポートは、NFS アクセラレーションの統計情報を示します。

2 つのタブには、次のチャートが含まれます。

- [Summary] タブ：
  - 「[NFS: Estimated Time Savings]」（P.16-29）
  - 「[NFS: Bandwidth Optimization]」（P.16-30）
  - 「[NFS: Connection Details]」（P.16-30）
- [Details] タブ：
  - 「[NFS: Request Optimization]」（P.16-28）
  - 「[NFS: Response Time Optimization]」（P.16-29）
  - 「[NFS: Versions Detected]」（P.16-29）
  - 「[NFS: Acceleration Bypass Reason]」（P.16-30）

[NFS Acceleration Statistics] 表は、チャートの下に表示されます。表の各行は、この Central Manager に登録されている各デバイスの統計情報を表示します。データについては、表 16-9 を参照してください。

表 16-9　[NFS Acceleration Statistics] 表

表の列	説明と値の計算に使用される計算式
[Device]	デバイス名
[New Connections Handled]	この期間に処理された NFS 接続の数を報告します。
[Active Connections]	NFS アクセラレータで現在処理されている接続の数を報告します。
[New Bypassed Connections]	最初に NFS アクセラレータで受信され、汎用アクセラレータにプッシュされた接続の数を報告します。
[New Local Request Count]	WAE でローカル処理されたクライアント要求の数を報告します。
[Avg. Local Response Time]	ローカル応答に費やされた平均時間（ミリ秒単位）を報告します。
[New Remote Request Count]	WAN 経由でリモート処理されたクライアント要求の数を報告します。
[Avg. Remote Response Time]	リモート応答に費やされた平均時間（ミリ秒単位）を報告します。
[% Time Saved]	すべての集約サンプルについて短縮された接続時間の比率（%）を報告します。 (Down – Up) × 100 / (Down) If(Down != 0) ここでは次のとおりです。 Down = (新規のローカル要求数 + 新規のリモート要求数) × 平均ローカル応答時間 Up = ((新規のローカル要求数 × 平均ローカル応答時間) + (新規のリモート要求数 × 平均リモート応答時間))

トポロジ レポート

システム レベルのトポロジ レポートは、WAE デバイス間のすべての接続をチャートで示します。

トポロジ マップは、青色の正方形を使用してデバイス間の接続を表示します。グリッドの右側にある凡例を使用して、デバイス名とグリッドの一番上に表示される番号を関連付けます。ウィンドウの一番上にあるドロップダウン リストを使用して、次の作業を実行します。

- デバイス間の代わりにさまざまな位置間の接続を表示する。
- デバイス名の代わりに接続の数でグリッドを並べ替える。

WAE の横にある [View] アイコンをクリックして、特定の WAE 用のピア デバイスのリストを表示します。[TFO Peer List] ウィンドウが表示されます。このウィンドウは、デバイス レベルのトポロジ レポートと同じです。

デバイス レベルのトポロジ レポートでは、特定の WAE に接続されているすべてのピア デバイスが一覧表示され、WAAS ネットワーク内のデバイス同士の関係を確認できます。[TFO Peer List] ウィンドウは、この WAE との最適化された接続に含まれる各ピア デバイスに関する情報を表示します。システム レベルのトポロジ レポートに移動するには、タスクバーで [Topology] アイコンをクリックします。

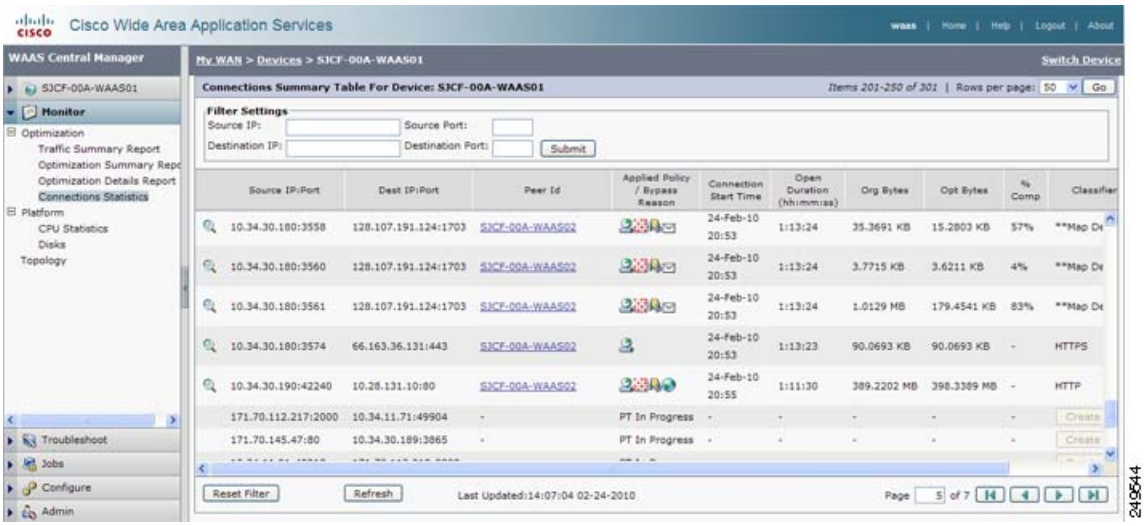
WAAS Central Manager にピア デバイスが登録されていない場合、名前には「Unknown, this peer is not being managed by CM」と表示され、IP アドレスには「Unknown」と表示されます。

（注）　WAAS Central Manager デバイスはトラフィックを最適化するためにどの WAE とも組まないため、WAAS Central Manager デバイスにはピア デバイスがありません。そのため、WAAS Central Manager デバイスでは、トポロジ機能を使用できません。

接続統計情報レポート

接続統計情報レポートには、デバイス接続概要の表が示されます。このレポートは、デバイス レベルだけで使用できます。この表には、デバイスで処理されたすべての TCP 接続が表示され、**show statistics connection** EXEC モード コマンドに相当します（図 16-59 を参照）。

図 16-59　　デバイスの接続概要表



このウィンドウは、各接続に関する次の情報を表示します。

- 送信元 IP アドレスおよびポート
- 宛先 IP アドレスおよびポート
- [Peer ID]：ピア デバイスのホスト名
- [Applied Policy/Bypass Reason]：適用された最適化ポリシー（TFO、DRE、LZ など）とアプリケーション アクセラレータをそれぞれアイコンで示します（アイコンにマウス ポインタを合わせると、その意味が表示されます）。接続が最適化されていない場合は、バイパスの理由が示されます。
- [Connection Start Time]：接続が開始された日付と時刻
- [Open Duration]：接続を開いていた時間数、分数、秒数
- 元のバイト総数
- 最適化したバイト総数
- 圧縮率
- [Classifier Name]：接続の分類子がない場合、この列には [Create New] ボタンが表示されています。このボタンをクリックすると、表の下に分類子の設定フォームが表示されます。このフォームで、送信元 IP アドレスと宛先 IP アドレス、および接続のポートに一致する分類子を作成できます。[Classifier Name] フィールドに名前を入力し、[Match All] チェックボックスを選択してすべてのトラフィックを一致させるか、[Source IP]、[Source Port]、[Destination IP]、および [Destination Port] の各ドロップダウンリストで該当項目を選択します。次に [Create Classifier] ボタンをクリックして、分類子を作成します。

（注）　WAE がデバイス グループからポリシーを継承している場合は、ユーザが誤ってデバイス グループ ポリシーを上書きするのを防ぐために、[Create New] ボタンは表示されません。分類子を作成するには、まずデバイス グループのポリシー ページを上書きしてから、[Connection Statistics] レポートに戻ってくる必要があります。

接続概要表のデータは、最初にウィンドウを表示したときにデバイスから取得されます。

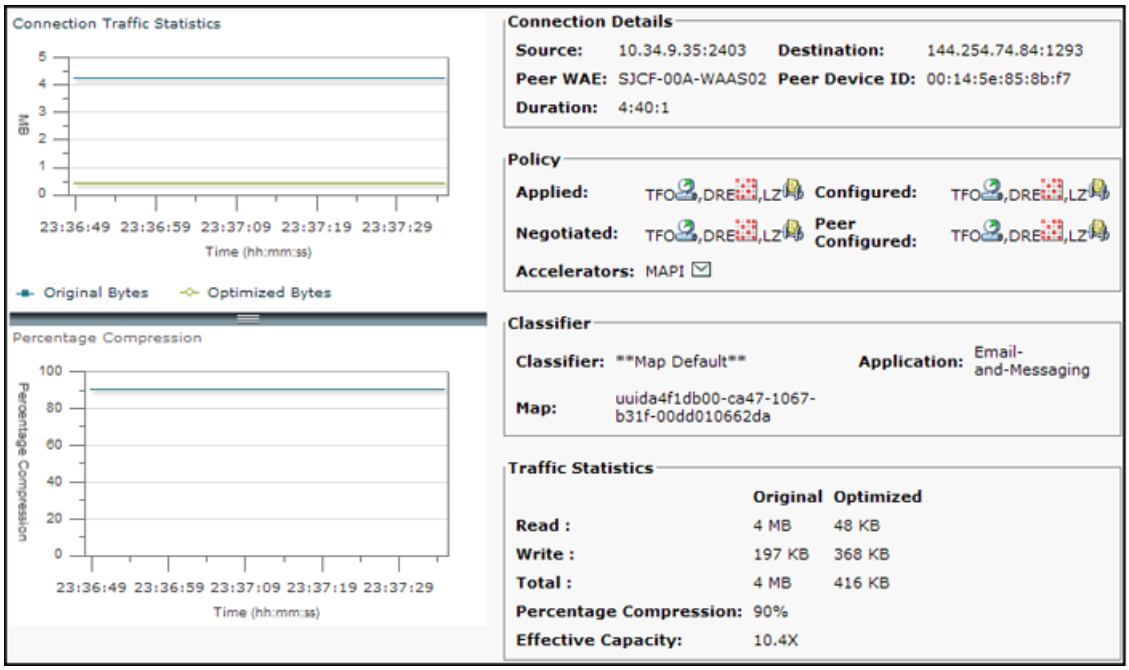
接続概要表のデータを更新するには、ウィンドウ下部の [Refresh] ボタンをクリックします。

[Connections Summary Table for Device] ウィンドウでは、次の作業を実行できます。

- フィルタ設定を適用し、選択した基準に基づいて特定の接続を表示する。
- 接続の詳細を表示する。
- [Reset Filter] ボタンをクリックして、フィルタ オプションをリセットし、表を更新する。

接続の詳細を表示するには、概要表の接続エントリの横にある [Details] アイコンをクリックします。[Connection Details] ウィンドウが表示されます。このウィンドウには、接続アドレス、ポート情報、ポリシー情報、およびトラフィック統計情報が表示されます。[Connection Details] ウィンドウには、リアルタイムのトラフィック統計情報をプロットするグラフも表示され、2 秒ごとに更新されます（図 16-60 を参照）。

図 16-60　　接続の詳細



（注）　[Percentage Compression] の値が負の場合、[Percentage Compression] と [Effective Capacity] の値は表示されません。

CIFS アクセラレーション レポート

CIFS アクセラレーション レポートは、CIFS アクセラレーション統計情報を示します。このレポートは、デバイス レベルだけで使用できます。CIFS アクセラレータ モード（透過的 CIFS アクセラレータ、レガシー CIFS Edge、またはレガシー CIFS Core）に応じて、異なるチャートを使用できます。

透過的 CIFS アクセラレータ デバイスでは、2 つのタブに次のチャートが含まれます。

- [Summary] タブ：
  - 「[CIFS: Connection Statistics]」（P.16-23）
  - 「[CIFS: File Optimization]」（P.16-23）
  - 「[CIFS: Request Optimization]」（P.16-21）
  - 「[CIFS: Cache Utilization]」（P.16-22）
- [Details] タブ：
  - 「[CIFS: Cached Objects]」（P.16-22）
  - 「[CIFS: Client Average Throughput]」（P.16-23）

レガシー CIFS Edge デバイスでは、2 つのタブに次のチャートが含まれます。

- [Summary] タブ：
  - 「[CIFS: Connection Statistics]」（P.16-23）
  - 「[CIFS: File Optimization]」（P.16-23）
  - 「[CIFS: Request Optimization]」（P.16-21）
  - 「[CIFS: Cache Utilization]」（P.16-22）
- [Details] タブ：
  - 「[CIFS: Cached Objects]」（P.16-22）
  - 「[CIFS: Connected CIFS Core Count]」（P.16-24）
  - 「[CIFS: CIFS Edge-CIFS Core Traffic]」（P.16-24）
  - 「[CIFS: Client Average Throughput]」（P.16-23）

レガシー CIFS Core デバイスでは、次のチャートが含まれます。

- [Summary] タブ：
  - 「[CIFS: Connected CIFS Edge Count]」（P.16-25）
  - 「[CIFS: CIFS Core Traffic]」（P.16-25）

（注）　タスクバーの [Print] アイコンを使用して CIFS アクセラレーション レポートを PDF ファイルに出力する場合、すべての CIFS チャートでは、設定したチャートの時間帯設定にかかわらず、WAE の現地時間（[CE Local Time] 設定）で時間が表示されます。

CPU 統計情報レポート

CPU 統計情報レポートは、「[CPU Utilization]」チャートを示します。

レポートの期間を変更するには、[Settings] をクリックします。

ディスク レポート

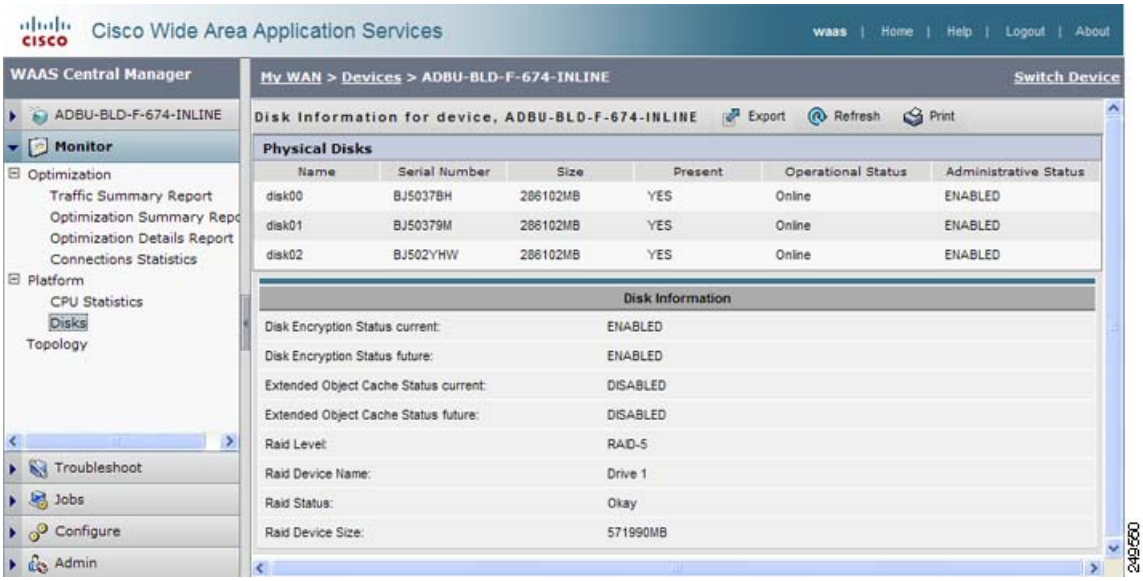
ディスク レポートには、物理ディスクおよび論理ディスクの情報が示されます（図 16-61 を参照）。

レポート ウィンドウには、各ディスクに関する次の情報が表示されます。

- ディスク名、シリアル番号、ディスク サイズを含む物理ディスク情報
- 現在のステータス [Present] フィールドでは、ディスクが存在する場合は [Yes]、ディスクが管理目的でシャットダウンされている場合は [Not Applicable] が表示されます。
- 操作ステータス（NORMAL、REBUILD、BAD、UNKNOWN、または Online）
- 管理ステータス（ENABLED または DISABLED）[Administrative Status] フィールドに [DISABLED] が表示されている場合、[Present] フィールドには [Not Applicable] が表示されます。
- 現在および今後のディスク暗号化ステータス
- 現在および今後の拡張オブジェクト キャッシュ ステータス
- RAID レベル。RAID 5 デバイスの場合、[Disk Information] ウィンドウには RAID デバイス名、RAID ステータス、および RAID デバイス サイズが表示されます。
- エラー情報（エラーが検出された場合）

タスクバーの [Export Table] アイコンをクリックすると、このウィンドウからすべてのディスク情報の詳細を Excel シートに保存できます。

図 16-61　[Disk Information for Device] ウィンドウ



レポートの管理

WAAS Central Manager を使用すると、定義済みレポートを編集し、カスタム レポートを作成できます。さらに、日別、週別、月別などの定期的なレポートを生成するようスケジューリングすることもできます。スケジューリングされたレポートを生成する場合、レポートへのリンクは電子メールで送信され、受信者に通知されます。

ここでは、次の内容について説明します。

カスタム レポートの作成

レポートは、チャート パネルの 1 つまたは複数のチャート（ウィンドウの上部）と、表パネルの表（ウィンドウの下部）で構成されます。システムおよびデバイス ダッシュボードの表示は、定義済みレポートや、[Monitor] ドロワーで使用可能な他のレポートの例です。

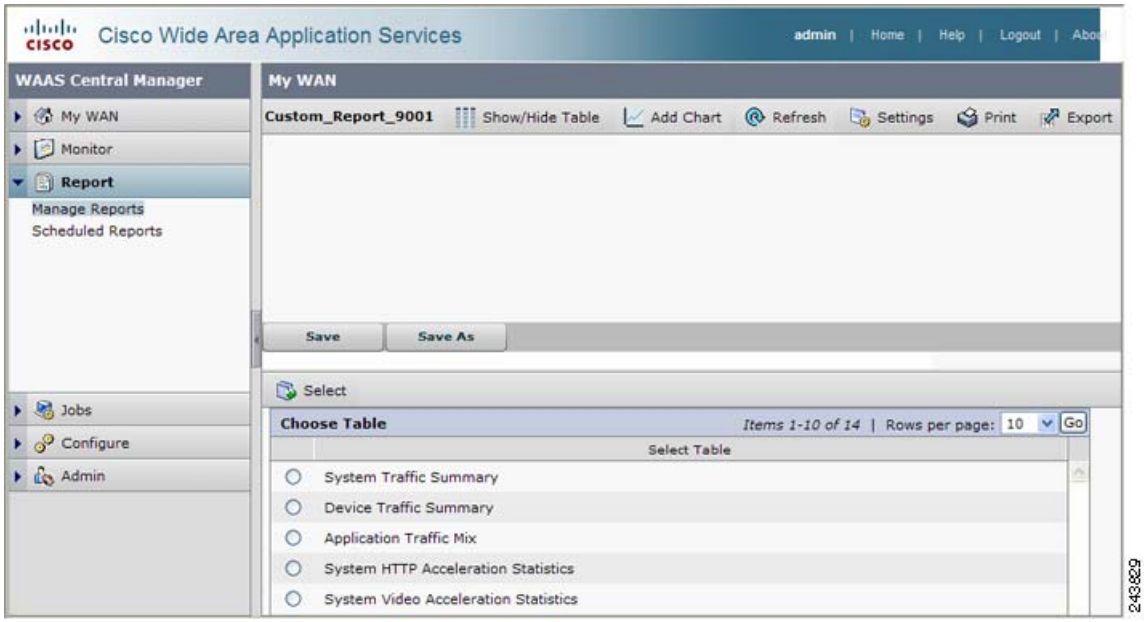
レポートは、デバイス レベルではなく、システム レベルに限り作成できます。

カスタム レポートを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Report] > [Manage Reports] を選択します。

ステップ 2　タスクバーの [Create New Report] アイコンをクリックします。図 16-62 に示すように、[Custom Report] ウィンドウが表示されます。

図 16-62　　レポートの作成



ステップ 3　[Choose Table] 領域の表の横にあるオプション ボタンをクリックしてから [Choose Table] 領域の上にある [Select] ボタンをクリックして、レポートの下部表パネル内に表示する表を選択します。

ステップ 4　1 つまたは複数のチャートを追加してレポートのチャート パネルの上部に表示されるようにするには、タスクバーの [Add Chart] アイコンをクリックします。図 16-7 に示すように、[Add Chart] ウィンドウが表示されます。

ステップ 5　カテゴリの横にあるプラス記号をクリックして、チャート カテゴリを拡張します。

ステップ 6　表示する各チャートの横にあるボックスを選択します。チャートの説明については、「チャートの説明」（P.16-14）を参照してください。

レポートには最大 6 つのチャートを出力できます。

ステップ 7　[Add] をクリックします。

ステップ 8　タスクバーの [Settings] アイコンをクリックして、チャートの設定をカスタマイズします。詳細については、「チャートの設定」（P.16-12）を参照してください。

ステップ 9　チャート パネルの下の [Save As] ボタンをクリックして、レポートを新しい名前で保存します。[Save As] ポップアップ ウィンドウが表示されます。

（[Save] ボタンを使用すると、レポートは Custom_Report_9001 などのデフォルト名で保存されます）

ステップ 10　レポート名とレポートに関する注を入力します。

レポート名には、文字、数字、ピリオド、ハイフン、アンダースコア、スペースしか使用できません。

ステップ 11　[Submit] をクリックします。

ダッシュボードまたはレポートからチャートを削除する場合は、そのチャートの [Close] ボタンをクリックし、レポートを保存します。

チャート パネルの上のタスクバー アイコンと、チャート パネルの下のボタンはすべて、「ダッシュボードまたはレポートのカスタマイズ」（P.16-10）で説明されているように動作します。

レポートの表示と編集

レポートを表示または編集するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Report] > [Manage Reports] を選択します。

ステップ 2　表示または編集するレポートの横にあるボックスを選択します。

検索しているレポートが見つからない場合、[Reports] 表の別のページに移動する必要があります。

ステップ 3　レポートを削除するには、タスクバーの [Delete] アイコンをクリックします。

ステップ 4　レポートを表示または編集するには、タスクバーの [Edit] アイコンをクリックします。レポートが表示されます。

または、レポートを表示するショートカットとして、レポートの横にある虫眼鏡アイコンをクリックします。

ステップ 5　レポート内のチャートを変更する場合、「カスタム レポートの作成」（P.16-49）で示すように標準の編集方式を使用します。

ステップ 6　[Save] または [Save As] をクリックしてレポートを保存します。

レポート名には、文字、数字、ピリオド、ハイフン、アンダースコア、スペースしか使用できません。

レポートを編集する場合、表パネルに表示されている表は変更できません。表を変更する場合、新しいレポートを作成する必要があります。

レポートを表示する場合、表パネルの下の [Refresh] ボタンをクリックして、表のデータを更新します。

admin ユーザは、すべてのユーザが作成したレポートの表示、編集、および削除を実行できます。定義済みのレポートの表示および編集も実行できます。admin 以外のユーザは、自身が作成したレポートの表示、編集、および削除を実行できます。定義済みのレポートの表示および編集も実行できます。

レポートのスケジューリング

レポートを 1 回、または日別、週別、月別など定期的に生成するようスケジューリングできます。スケジューリングされたレポートが生成されると、レポートの PDF コピーを電子メールで送信できます。

レポートをスケジューリングするには、次の手順に従ってください。

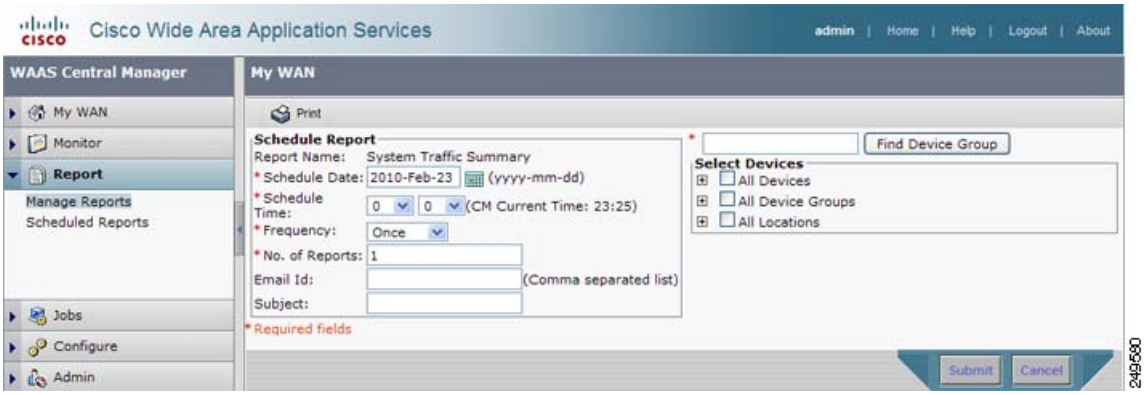
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Report] > [Manage Reports] を選択します。

ステップ 2　スケジューリングするレポートの横にあるボックスを選択します。

検索しているレポートが見つからない場合、[Reports] 表の別のページに移動する必要があります。

ステップ 3　タスクバーの [Schedule] アイコンをクリックします。図 16-63 に示すように、[scheduling] ウィンドウが表示されます。

図 16-63　　レポートのスケジューリング



ステップ 4　[Schedule Date] フィールドでは、スケジュール日付を YYYY-MM-DD 形式で入力する、または [calendar] アイコンをクリックして、日付を選択する [calendar] ポップアップ ウィンドウを表示します。

ステップ 5　[Schedule Time] フィールドでは、ドロップダウン リストから時間と分を選択します。時間は WAAS Central Manager の現地時間を示します。

ステップ 6　[Frequency] ドロップダウン リストでは、レポートの頻度を示す [Once]、[Daily]、[Weekly]、または [Monthly] を選択します。

ステップ 7　[No. of Reports] フィールドに、繰り返し発生するレポートを生成する回数を入力します。指定された回数レポートを生成したら、レポートは生成されません。

ステップ 8　[Email Id] フィールドには、レポートの受信者の電子メール アドレスをカンマで区切って入力します。

ステップ 9　[Subject] フィールドには、電子メールのメッセージの件名を入力します。

ステップ 10　[Select Devices] 領域では、レポートの統計情報に含めるデバイスを選択します。対象とする各デバイス、位置、またはデバイス グループの横にあるボックスを選択します。個々のデバイスは、[All Devices] リストにしかリストされません。

長いリストでデバイス グループを検索する（強調表示する）には、リストの上のフィールドにデバイス グループ名を入力し、[Find Device Group] をクリックします。検索は大文字と小文字を区別します。

ステップ 11　[Submit] をクリックします。

ステップ 12　レポートを生成したときに電子メール通知を行うため、電子メール サーバを設定します。詳細については、「E メール通知サーバの設定」（P.9-25）を参照してください。

（注）　1,000 以上の WAE が存在する WAAS ネットワークでは、スケジューリングされたレポートの生成に最大 4 分かかる場合があります。同時に複数のレポートをスケジューリングする場合、レポート数およびデバイス数に応じて、レポートの生成に最大 20 分の遅延が発生します。

スケジューリングされたレポートの管理

スケジューリングされたレポートを表示または削除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Report] > [Scheduled Reports] を選択します。[Scheduled Reports] ウィンドウで、スケジューリングされたレポートが表示されます。

ステップ 2　（任意）レポートを表示するときは、スケジュール行のプラス記号をクリックします。行が拡張してスケジュールのレポート インスタンスを表示します。各インスタンスに、レポート名、選択されているデバイス、選択されているデバイス グループ、選択されている位置、スケジュールされた時刻、完了時刻、頻度、ステータス、保留になって残されているレポートの数（繰り返し発生するレポートの場合）、およびスケジュールされたレポートのユーザ（この最後の列は管理者ユーザにしか表示されません）が示されます。

表示するレポート インスタンスの横にあるボックスを選択して、タスクバーの [View Completed Report] アイコンをクリックする、または [status] 列の [Completed] リンクをクリックします。完了したレポートのみを表示できます。レポート インスタンスに [Not Started or In Progress] がある場合、それが完了するまで待ってからレポートを表示する必要があります。

（注）　スケジューリングされたレポートの完了した各インスタンスでは、[Frequency] 列に [Once] と表示され、[Completed Time] にはレポートの生成日時が表示されます。これらのインスタンスは、レポートの表示可能インスタンスであり、インスタンスごとに 1 つです。（スケジュール期間に応じて）[Frequency] に [Daily]、[Weekly]、または [Monthly] が表示され、[Completed Time] が表示されないインスタンスも 1 つあります。このインスタンスは表示可能ではなく、スケジューリングされているレポート オブジェクトを示します。

ステップ 3　（任意）レポートを削除する場合、削除する 1 つまたは複数のレポート インスタンスの横にあるボックスを選択し、タスクバーの [Delete Selected Reports] アイコンをクリックします。インスタンスのグループの上にあるスケジュール名ではなく、レポート インスタンスを選択する必要があります。すべてのレポート インスタンスを削除すると、スケジュールも削除されます。

WAAS は最後に完了した、または失敗した 10 のレポート インスタンスをカスタム レポートごとに保存します。この数は、System.monitoring.maxReports システム プロパティによって設定可能です。このプロパティの変更の詳細については、「デフォルトのシステム設定プロパティの変更」（P.9-17）を参照してください。

admin ユーザは、すべてのユーザによってスケジューリングされたレポートおよびレポート作成者の名前を表示できます。admin 以外のユーザは、自身がスケジューリングしたレポートだけを表示できます。

定義済みレポートに対する変更は、個々のユーザごとに保存されます。つまり、あるユーザがスケジューリングされた定義済みレポートを変更しても、このユーザだけに変更が表示されます。他のユーザ（admin ユーザを含む）は、デフォルト設定のレポートが表示されます。

フロー モニタリングの設定

フロー モニタリング アプリケーションは、アプリケーションの傾向の調査、ネットワーク計画、ベンダー展開による影響の調査で使用されるトラフィック データを収集します。ここでは、WAE でのフロー モニタリング機能の設定方法について、次のトピックに分けて説明します。

- 「フロー モニタリングのアラーム」
- 「フロー モニタリングの NetQoS の使用例」

NetQoS のモニタリング アプリケーションが WAAS ソフトウェアと相互動作して、フロー モニタリングを提供できます。このアプリケーションを WAAS ソフトウェアと統合するには、WAE デバイスに NetQoS FlowAgent モジュールを設定します。WAE での NetQoS FlowAgent モジュールは、パケットフローの重要なメトリックを収集します。このメトリックはその後、ネットワークを介して NetQoS SuperAgent に送信されます。このモニタリング エージェントはデータを分析し、レポートを生成します。この機能が動作するには、NetQoS FlowAgent での追加の設定が必要です（「フロー モニタリングの NetQoS の使用例」（P.16-55）を参照）。

モニタリング エージェントは、コンソール（またはホスト）とコレクタの 2 つのモジュールから構成されています。WAE は、この 2 つのモニタリング エージェント モジュールに対して 2 種類の接続を開始します。つまり、コンソールへの一時接続と、コレクタへの固定接続です。WAE CLI または Central Manager GUI のいずれかで **flow monitor tcpstat-v1 host** コンフィギュレーション モード コマンドを使用して、WAE でのコンソール IP アドレスを設定します。この一時接続は、コントロール コネクションと呼ばれます。コントロール コネクションは TCP ポート 7878 を使用します。その目的は、WAE の割り当て先のコレクタの IP アドレスとポート番号を取得することです。また、WAE は、コントロール コネクションでモニタされるサーバに関する設定情報を取得します。WAE は、コントローラの IP アドレスとポート番号を取得すると、コレクタへの固定接続を開きます。モニタされているサーバの収集された要約データは、固定接続を介して送信されます。

コンソール（またはホスト）モジュールとコレクタ モジュールは、1 つのデバイス上に配置することも、別個のデバイス上に配置することもできます。これらの接続は、互いに独立しています。片方の接続に障害が発生しても、もう一方の接続の障害発生原因とはならず、その逆も同様です。

この接続の状態とさまざまな操作統計情報を表示するには、**show statistics flow monitor tcpstat-v1** EXEC モード コマンドを使用します。接続エラーおよびデータ転送エラーが、WAE および Central Manager GUI でアラームをトリガーします（「フロー モニタリングのアラーム」（P.16-54）を参照）。デバッグ情報を表示するには、**debug flow monitor tcpstat-v1** EXEC モード コマンドを使用します。

Central Manager GUI を使用して WAE でフロー モニタリングを設定するには、次の手順に従います。

ステップ 1　複数デバイスでフロー モニタリングを設定するために新しいデバイス グループを作成します。デバイス グループを作成するには、[My WAN] > [Manage Device Groups] > [Create New Device Group] を選択します。

a. デバイス グループを作成するとき、[Automatically assign all newly activated devices to this group] チェックボックスを選択してこのオプションを有効にします。

b. 既存の WAE デバイスを、この新しいデバイス グループに追加します。

ステップ 2　[Device Group listing] ウィンドウで、設定するフロー モニタリング設定デバイス グループの名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Network Monitoring] > [Flow Monitor] を選択します。[Flow Monitor Settings for Device Group] ウィンドウが表示されます

ステップ 4　[Enable] チェックボックスを選択します。

ステップ 5　[tcpstat-v1 Host] フィールドに、モニタリング エージェント コンソールの IP アドレスを入力します。

この設定により、WAE は、コレクタ デバイスの IP アドレスの取得を目的としてコンソールへの一時接続（コントロール コネクション）を確立できます。コンソール デバイスからコレクタの IP アドレス情報を設定する必要があります（NetQoS フロー モニタリング アプリケーション ソフトウェアの設定マニュアルを参照）。

ステップ 6　[Submit] をクリックし、設定をこのデバイス グループのデバイスに適用します。

CLI を使用して WAE でフロー モニタリングを設定するには、次の手順に従います。

ステップ 1　WAE にモニタリング エージェント コンソールの IP アドレスを登録します。

```
WAE(config)# flow monitor tcpstat-v1 host 10.1.2.3
```

この設定により、WAE は、コレクタ デバイスの IP アドレスの取得を目的としてコンソール（またはホスト）への一時接続（コントロール コネクション）を確立できます。コンソール デバイスからコレクタの IP アドレス情報を設定する必要があります（NetQoS フロー モニタリング アプリケーション ソフトウェアの設定マニュアルを参照）。

ステップ 2　WAE アプライアンスのフロー モニタリングを有効にします。

```
WAE(config)# flow monitor tcpstat-v1 enable
```

ステップ 3　**show running-config** EXEC コマンドを使用して、設定をチェックします。

フロー モニタリングのアラーム

表 16-10 では、フロー モニタリングでエラーが発生したときに出される 4 つの異なるアラームを説明しています。

表 16-10　フロー モニタリングのアラーム

名前	重大度	説明
CONTROL_CONN	メジャー	コントロール コネクションに問題があることを示します。
COLLECTOR_CONN	メジャー	コレクタ接続に問題があることを示します。

表 16-10　フロー モニタリングのアラーム （続き）

名前	重大度	説明
SUMMARY_COLLECTION	マイナー	パケット要約情報の収集に問題があることを示します。 バッファ キュー制限に達したか、メモリを割り当てられないなどの TFO エラーにより、要約パケットはドロップされます。 また、要約パケットの収集は、使用可能な WAN 帯域幅に依存しています。
DATA_UPDATE	マイナー	WAE が更新をコレクタ エージェントに送信できない問題があることを示します。

フロー モニタリングの NetQoS の使用例

NetQoS を WAAS ソフトウェアに統合するには、WAE デバイスで NetQoS FlowAgent を実行します。FlowAgent は、NetQoS が開発したソフトウェア モジュールで、WAE 装置にあります。FlowAgent はパケット フローに関するメトリックを収集します。このメトリックはその後、ネットワークを介して NetQoS SuperAgent に送信されます。SuperAgent は、ラウンドトリップ回数、サーバ応答回数、データ転送回数を測定し、データを分析してレポートを生成します。

（注）　NetQoS SuperAgent とともにフロー モニタリングを使用する場合、WAE でのフロー モニタリングでは最適化されたトラフィックのみが取り込まれます。

NetQoS でフロー モニタリングを設定するには、次の手順に従います。

ステップ 1　WAE CLI または Central Manager GUI で、WAE 装置の [tcpstat-v1 Host] フィールドに SuperAgent Master Console IP アドレスを入力します。

デバイス グループを使用して複数の装置を設定する場合、デバイス リストにあるすべての装置に設定が伝播されるまで待ちます。

ステップ 2　NetQoS SuperAgent コンソールで WAE を SuperAgent Aggregator（WAAS 用語ではコレクタ）に割り当て、NetQoS Networks、Servers、および Applications の各エンティティを設定します。

（注）　NetQoS SuperAgent Master Console の使用と NetQoS SuperAgent エンティティの設定についての詳細は、Web サイト（http://support.ca.com）を参照してください。

システム ログ機能の設定

システム ログ ファイル（Syslog）の特定のパラメータを設定するには、WAAS システム ログ機能を使用します。このファイルには、認証項目、特権レベル設定、および管理詳細が含まれています。システム ログ ファイルは、システム ファイル システム（SYSFS）パーティションに ¥local1¥syslog.txt として配置されます。

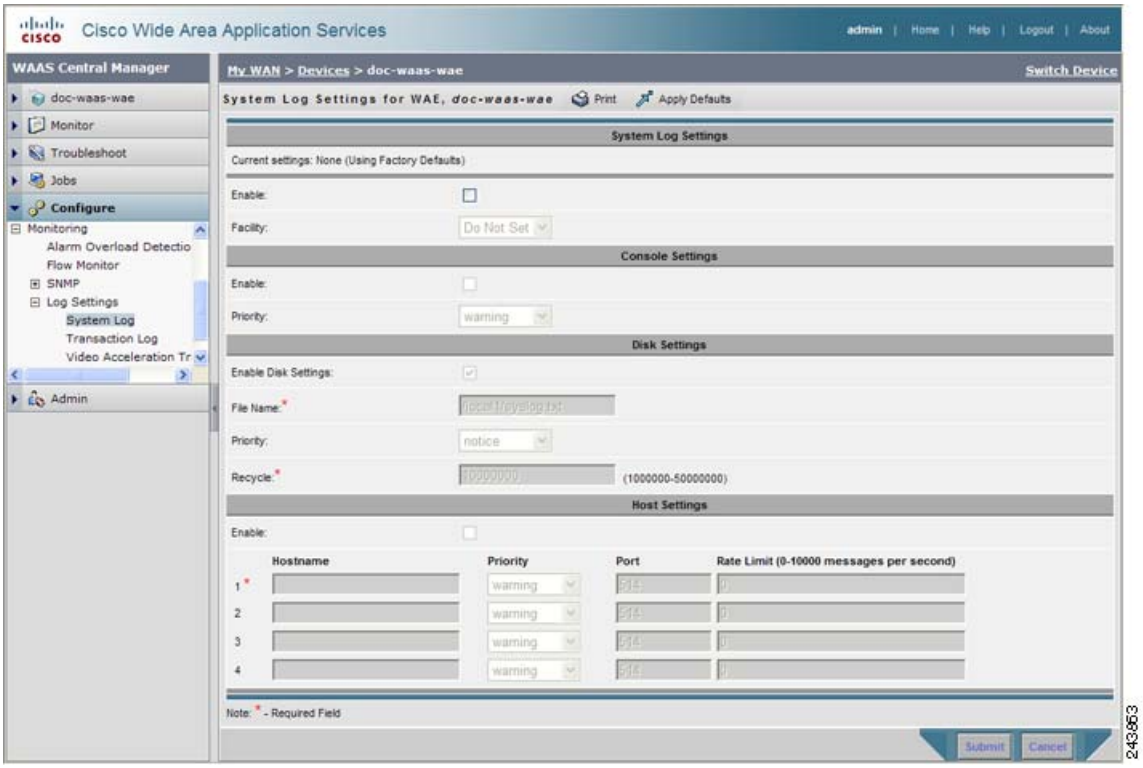
システム ログ機能を有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　システム ログ機能を有効にするデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [Log Settings] > [System Log] を選択します。[System Log Settings] ウィンドウが表示されます（図 16-64 を参照）。

図 16-64　[System Log Settings] ウィンドウ



ステップ 4　[System Log Settings] セクションで、[Enable] チェックボックスを選択してシステム ログ機能を有効にします。このオプションはデフォルトで無効になっています。

ステップ 5　[Facility] ドロップダウン リストから、適切な機能を選択します。

ステップ 6　コンソールに送信するシステム ログ ファイルを有効にします。

a.　[Console Settings] セクションで、[Enable] チェックボックスを選択します。

b.　[Priority] ドロップダウン リストから、指定したリモート Syslog ホストへ送信する必要があるメッセージの重大度を選択します。デフォルトの優先順位コードは、「warning」（レベル 4）です。各 Syslog ホストは、異なるレベルのイベント メッセージを受信できます（優先順位レベルのリストについては、表 16-11（P.16-58）を参照してください）。

ステップ 7　ディスクに送信する Syslog ファイルを有効にします。

a.　[Disk Settings] セクションで、[Enable Disk Settings] チェックボックスを選択します。

b.　[File Name] フィールドに、Syslog ファイルがディスクに保存されるパスとファイル名を入力します。

c. [Priority] ドロップダウン リストから、指定したリモート Syslog ホストへ送信する必要があるメッセージの重大度を選択します。デフォルトの優先順位コードは、「warning」（レベル 4）です。各 Syslog ホストは、異なるレベルのイベント メッセージを受信できます（優先順位レベルのリストについては、表 16-11（P.16-58）を参照してください）。

d. [Recycle] フィールドで、ディスクに保存されるときに再利用できる Syslog ファイルのサイズをバイト単位で指定します。ファイル サイズのデフォルト値は 10000000 です。

現在のログ ファイルのサイズが再利用サイズを超えると、ログ ファイルが切り替わります（ログ ファイル用のデフォルトの再利用サイズは、10,000,000 バイトです）。ログ ファイルは最大 5 回切り替わり、切り替えのたびに元のログと同じディレクトリにある *log_file_name.[1 ～ 5]* として保存されます。

切り替えるログ ファイルは、[File Name] フィールドで設定します（または **logging disk filename** コマンドを使用します）。

ステップ 8　ホストに送信する Syslog ファイルを有効にします。

a. [Host Settings] セクションで、[Enable] チェックボックスを選択します。Syslog メッセージを送信できる最大 4 つのホストを設定できます。詳細については「システム ログ機能用の複数のホスト」（P.16-58）を参照してください。

b. [Hostname] フィールドに、リモート Syslog ホストのホスト名または IP アドレスを入力します。[Hostname] フィールド 2 ～ 4 に最大 3 つのリモート Syslog ホストを指定します。ホストへのシステム ログを有効にしている場合は、1 つまたは複数のホスト名を指定する必要があります。

c. [Priority] ドロップダウン リストから、指定したリモート Syslog ホストへ送信する必要があるメッセージの重大度を選択します。デフォルトの優先順位コードは、「warning」（レベル 4）です。各 Syslog ホストは、異なるレベルのイベント メッセージを受信できます（優先順位レベルのリストについては、表 16-11 を参照してください）。

d. [Port] フィールドで、WAAS デバイスがメッセージを送信する必要があるリモート ホストの送信先ポートを指定します。デフォルトのポート番号は 514 です。

e. [Rate Limit] フィールドで、リモート Syslog ホストへ送信できる 1 秒あたりのメッセージ数を指定します。帯域幅とその他のリソースの消費量を制限するために、リモート Syslog ホストへのメッセージにレート リミットを設けることができます。この制限を越えると、指定されたリモート Syslog ホストはメッセージをドロップします。デフォルトのレート リミットはありません。デフォルトでは、すべての Syslog メッセージがすべての設定済みの Syslog ホストに送信されます。

ステップ 9　[Submit] をクリックします。

CLI からシステム ログ機能を設定するには、**logging** グローバル コンフィギュレーション コマンドを使用できます。

ここでは、次の内容について説明します。

- 「優先順位」（P.16-57）
- 「システム ログ機能用の複数のホスト」（P.16-58）

優先順位

表 16-11 に、対応するイベントを Syslog メッセージの受信者へ送信するときのさまざまな優先順位の詳細を示します。

表 16-11　システム ログ機能の優先順位と説明

優先順位コード	状態	説明
0	Emergency	システムを使用できません。
1	Alert	すぐに措置が必要です。
2	Critical	重大な状態です。
3	Error	エラーの状態です。
4	Warning	警告の状態です。
5	Notice	正常ですが注意すべき状態です。
6	Information	情報メッセージです。
7	Debug	デバッグ メッセージです。

システム ログ機能用の複数のホスト

各 Syslog ホストは、異なる優先順位の Syslog メッセージを受信できます。WAAS デバイスがさまざまなレベルの Syslog メッセージを 4 台の外部 Syslog ホストへ送信できるように、異なる Syslog メッセージ優先順位コードを持つ異なる Syslog ホストを設定できます。たとえば、優先順位コードが「error」（レベル 3）のメッセージを IP アドレスが 10.10.10.1 のリモート Syslog ホストへ送信し、優先順位コードが「warning」（レベル 4）のメッセージを IP アドレスが 10.10.10.2 のリモート Syslog ホストへ送信するように、WAAS デバイスを設定できます。

Syslog ホストとは別の Syslog ホストとの冗長性またはフェールオーバーを実現する場合は、WAAS デバイスに複数の Syslog ホストを設定し、設定した各 Syslog ホストに同じ優先順位コードを割り当てる必要があります（たとえば、Syslog ホスト 1、Syslog ホスト 2、および Syslog ホスト 3 に「critical」（レベル 2）優先順位コードを割り当てます）。

また、最大 4 台の Syslog ホストを設定できるだけでなく、複数のホスト用に次の項目を設定することもできます。

- Syslog メッセージをログ ホストへ送信するための WAAS デバイス上のデフォルトのポート番号 514 以外のポート番号。
- Syslog メッセージが使用する帯域幅の量を制御するために、リモート Syslog サーバへ送信されるメッセージ速度（1 秒あたりのメッセージ数）を制限する Syslog メッセージ用のレート リミット。

トランザクション ログ機能の設定

ここでは、次の内容について説明します。

トランザクション ログ機能の有効化

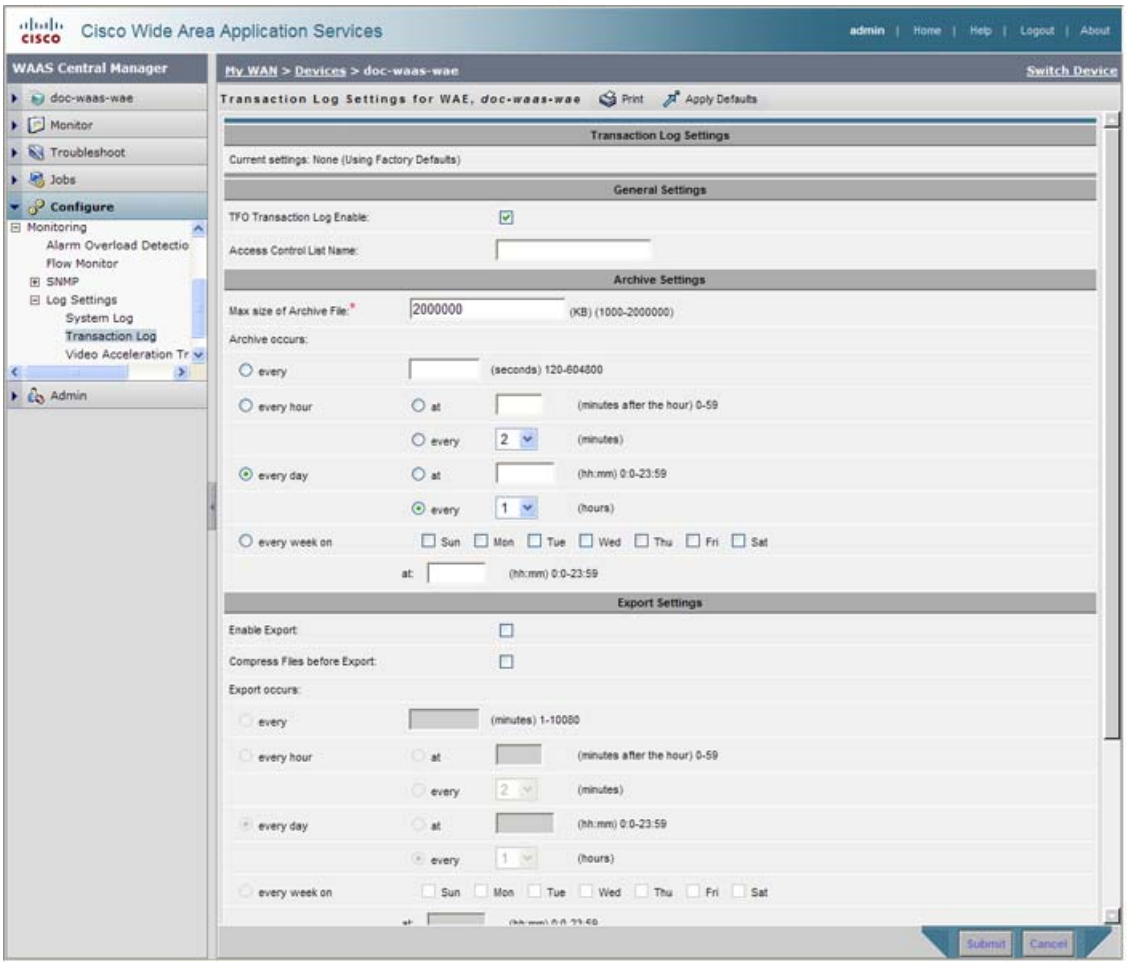
TFO フローおよびビデオ ストリームのトランザクション ログ機能を有効するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　システム ログ機能を有効にするデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウまたは [Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [Log Settings] > [Transaction Log]（TFO トランザクション ロギングの場合）、または [Configure] > [Monitoring] > [Log Settings] > [Video Acceleration Transaction Log]（ビデオ トランザクション ロギングの場合）を選択します。[Transaction Log Settings] ウィンドウが表示されます（図 16-65 を参照）。[Video Transaction Log Settings] ウィンドウは同じに見えますが、一番上に [General Settings] 領域がありません。

図 16-65　[Transaction Log Settings] ウィンドウ



ステップ 4　[General Settings] 見出しで、[TFO Transaction Log Enable] チェックボックスを選択してトランザクション ログ機能を有効にします。ビデオ トランザクション ログ機能の場合、このチェックボックスは表示されません。

ウィンドウのフィールドがアクティブになります。

ステップ 5　[Access Control List Name] フィールドには、トランザクション ログ機能を制限するために使用する アクセス コントロール リストの名前を任意で入力します。ACL を指定すると、アクセス リストで定義されたホストからのトランザクションのみが記録されます。ビデオ トランザクション ログ機能の場合、このフィールドは表示されません。

ip access-list グローバル コンフィギュレーション コマンドを使用して、アクセス リストを定義します。

ステップ 6　[Archive Settings] 見出しで、次のフィールドの値を指定します。

- [Max Size of Archive File]：ローカル ディスクに維持するアーカイブ ファイルの最大サイズ（キロバイト単位）。この値は、ローカル ディスクに維持するアーカイブ ファイルの最大サイズです。範囲は、1000 ～ 2000000 です。デフォルトは、2000000 です。
- [Archive Occurs Every (interval)]：作業ログ データをアーカイブ ログに移動し、クリアする周期。

ステップ 7　[Export Settings] セクションで、トランザクション ログ ファイルを FTP サーバへエクスポートするフィールドを設定します。

表 16-12 で、[Export Settings] セクションのフィールドについて説明します。

表 16-12　Export Settings

フィールド	機能
[Enable Export]	トランザクション ログを FTP サーバへエクスポートできます。
[Compress Files before Export]	アーカイブされたログ ファイルを外部 FTP サーバへエクスポートする前に圧縮できます。
[Export occurs every (interval)]	データを FTP サーバへ移動して、作業ログをクリアする必要がある周期です。
[Export Server]	FTP エクスポート機能は、最大 4 台のサーバをサポートできます。各サーバは、そのサーバに有効なユーザ名、パスワード、およびディレクトリで設定する必要があります。 • [Export Server]：FTP サーバの IP アドレスまたはホスト名。 • [Name]：FTP サーバにアクセスするために使用するアカウントのユーザ ID。 • [Password][Confirm Password]：[Name] フィールドに指定した FTP ユーザ アカウントのパスワード。[Password] フィールドと [Confirm password] フィールドの両方に、このパスワードを入力する必要があります。 • [Directory]：FTP サーバでトランザクション ログを保持する作業ディレクトリの名前。[Name] フィールドに指定したユーザは、このディレクトリへの書き込みアクセス権が必要です。 • [SFTP]：指定した FTP サーバが安全な FTP サーバである場合は、[SFTP] チェックボックスを選択します。

ステップ 8　[Submit] をクリックします。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] をクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合にだけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合にだけ表示されます。

CLI からトランザクション ログを有効にし、設定するには、**transaction-logs** グローバル コンフィギュレーション コマンドを使用できます。

トランザクション ログ

TFO トランザクション ログは、ディレクトリ /local1/logs/tfo のローカル ディスクに維持されます。ビデオ（Windows メディア）ログはディレクトリ /local1/logs/wmt/wms-90 に維持されます。

トランザクション ログ機能を有効にするときは、データをアーカイブ ログへ移動して作業ログをアーカイブする必要がある周期を指定できます。アーカイブ ログ ファイルは、ディレクトリ /local1/logs/ のローカル ディスクにあります。

複数のアーカイブ ファイルが保存されるため、ファイルがアーカイブされるとき、ファイル名にタイム スタンプが含まれます。ファイルは FTP/SFTP サーバへエクスポートできるため、ファイル名にはこの WAAS デバイスの IP アドレスも含まれます。

TFO トランザクションのため、アーカイブ ファイル名では次の形式を使用します。

tfo_IPADDRESS_YYYYMMDD_HHMMSS.txt

Windows メディア トランザクションのため、アーカイブ ファイル名では次の形式を使用します。

wms_90_IPADDRESS_YYYYMMDD_HHMMSS.txt

トランザクション ログの形式については、付録 B「トランザクション ログ形式」に記載されています。

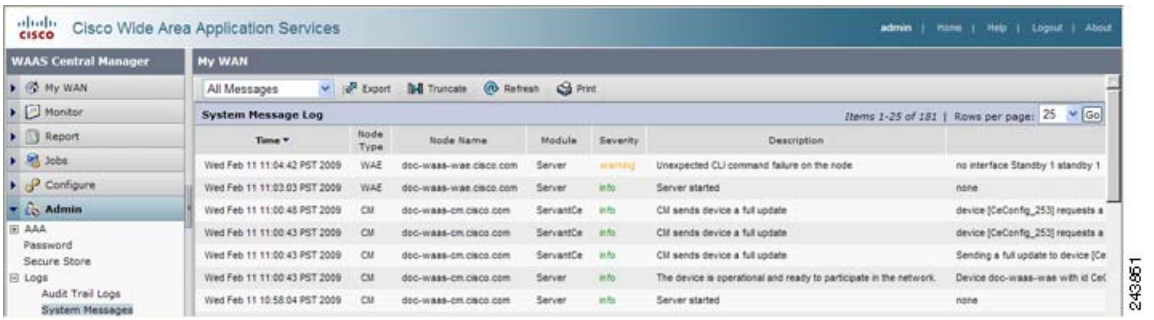
システム メッセージ ログの表示

WAAS Central Manager GUI のシステム メッセージ ログ機能を使用すると、WAAS ネットワークで発生したイベントに関する情報を表示できます。WAAS Central Manager は、「warning」またはそれ以上の重大度レベルの、登録されたデバイスからのメッセージを記録します。

WAAS ネットワーク用のログ情報を表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [Logs] > [System Messages] を選択します。[System Message Log] ウィンドウが表示されます（図 16-66 を参照）。

図 16-66　[System Message Log]



ステップ 2　[System Message Log] ドロップダウン リストから、次の中から表示するメッセージの種類を 1 つ選択します。

- All
- CLI
- Critical
- Database

ステップ 3　（任意）ノードの種類、ノード名、モジュール、またはメッセージ文のいずれかの列見出しをクリックして、メッセージを並べ替えます。デフォルトでは、メッセージは時間順に表示されます。

（注）　ノードで使用可能な名前がない場合、名前は「Unavailable」と表示されます。ノードが削除されていたり、WAAS ソフトウェアに再登録されていたりした場合に、このように表示されることがあります。

ステップ 4　（任意）次の手順を完了して、多くのメッセージが表に表示されないように、メッセージ ログを切り捨てます。

a.　タスクバーの [Truncate] アイコンをクリックします。[Truncate System Message Log] ウィンドウが表示されます。

b.　次のいずれかのオプションを選択します。

- [Size Truncation]：ログ内のメッセージを指定した件数に制限します。ログは、先入れ先出し方式を使用して、ログが指定した件数に達すると古いメッセージを削除します。
- [Date Truncation]：ログ内のメッセージを指定した日数に制限します。
- [Message Truncation]：指定したパターンと一致するメッセージをログから削除します。

c.　制限パラメータを指定したら、[Submit] をクリックします。

ステップ 5　多くのイベント メッセージがある場合は、関心がある操作を表示するために複数のページを表示する必要がある場合があります。進む（>>）および戻る（<<）ボタンをクリックしてページ間を移動します。あるいは、特定のページ番号のリンクをクリックして、そのページへ進みます。

監査証跡ログの表示

WAAS Central Manager は、システムでのユーザの操作をログに記録します。ログに記録される唯一の操作は、WAAS ネットワークを変更する操作です。この機能は、作業の日時と処理内容を記述して、ユーザ操作のアカウンタビリティを提供します。ログに記録される操作は、次のとおりです。

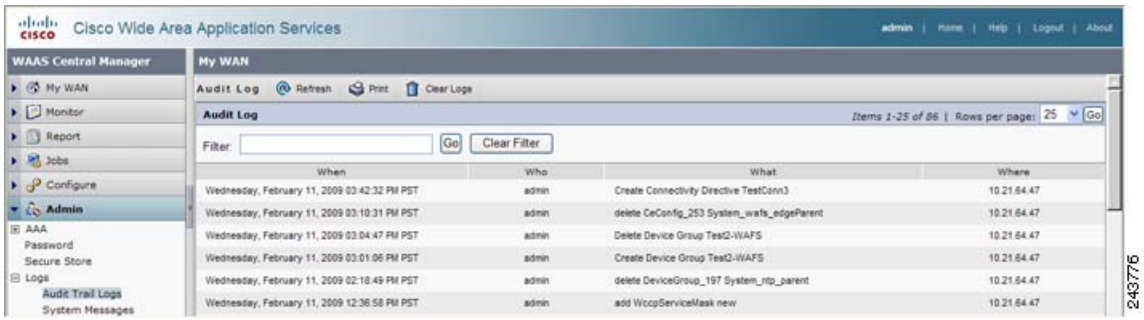
- WAAS ネットワーク エンティティの作成
- WAAS ネットワーク エンティティの変更と削除
- システム設定
- 監査証跡ログのクリア

監査証跡ログを表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[Admin] > [Logs] > [Audit Trail Logs] を選択します。

[Audit Log] ウィンドウが表示されます（図 16-67 を参照）。WAAS Central Manager のログに記録されるすべてのトランザクションは、日時、ユーザ、ログに記録された実際のトランザクション、および使用されたマシンの IP アドレス別に表示されます。

図 16-67　[Audit Log] ウィンドウ



ステップ 2　[Rows] ドロップダウン リストから数値を選択して、表示する行数を決定します。

デバイス ログの表示

WAAS ネットワーク内の特定のデバイスで発生したイベントに関する情報を表示するには、WAAS Central Manager GUI で使用できるシステム メッセージ ログ機能を使用できます。

WAAS ネットワークで発生したイベントを表示するには、「システム メッセージ ログの表示」（P.16-61）を参照してください。

WAAS デバイス用のログ情報を表示するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　システム メッセージ ログ詳細を表示するデバイスの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Admin] > [Logs] を選択します。[System Message Log for Device] ウィンドウが表示されます。

ステップ 4　[System Message Log] ドロップダウン リストから、表示するメッセージの種類を選択します。

システム ログ内の次のようなメッセージを表示できます。

- All（デフォルト）
- CLI
- Critical
- Database

ステップ 5　列見出しをクリックして、ノードの種類、ノード名、またはモジュールのいずれかによってメッセージを時間順に並べ替えます。デフォルトでは、メッセージは時間順に表示されます。

ノードが削除されたり WAAS ソフトウェアに再度登録されていたりして、ノードの名前が使用できない場合、名前は「Unavailable」と表示されます。

ステップ 6　多くのイベント メッセージがある場合は、進む（>>）および戻る（<<）ボタンを使用してページ間を移動する必要がある場合があります。あるいは、特定のページ番号のリンクをクリックして、そのページへ進みます。

カーネル デバッガの有効化

WAAS Central Manager GUI を使用すると、カーネル デバッガ（kdb）へのアクセスを有効または無効にできます。有効にすると、カーネル デバッガは、カーネル問題が発生したときに自動的にアクティブになります。

カーネル デバッガを有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　デバッグするデバイス（またはデバイス グループ）の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Troubleshoot] > [Kernel Debugger] を選択します。[Kernel Debugger] ウィンドウが表示されます。

ステップ 4　[Enable] チェックボックスを選択してカーネル デバッガを有効にし、[Submit] をクリックします。このオプションはデフォルトで無効になっています。

診断テストを使用したトラブルシューティング

次の項で説明するように、WAAS にはさまざまなトラブルシューティング ツールがあります。

- 「GUI を使用したトラブルシューティング」（P.16-65）
- 「CLI を使用したトラブルシューティング」（P.16-65）

GUI を使用したトラブルシューティング

WAAS Central Manager には、トラブルシューティングおよび診断レポート機能があります。

診断テストを実行するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。

ステップ 2　診断テストを実行するデバイス（またはデバイス グループ）の名前の横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Troubleshoot] > [Diagnostics Tests] を選択します。[Diagnostic Tool] ウィンドウが表示されます。

ステップ 4　実行する各診断テストの横にあるチェックボックスを選択する、またはすべてのテストを実行するチェックボックスを選択します。次のテストが使用できます。

- [Device Operation]：デバイス ステータス、コアダンプ ファイルの存在、または重大度がメジャーかクリティカルのアラームをチェックします。
- [Basic Configuration]：デバイスの基本的なネットワーク設定をチェックします。
- [Basic Connectivity]：デバイスと設定済み外部デバイス（DNS、認証、NTP サーバなど）との接続をチェックします。
- [Physical Interface]：デバイスの物理インターフェイスの設定および動作をチェックします。
- [Configuration Security]：悪意の可能性のある（XSS）エントリの実行設定をチェックします。
- [Traffic Optimization]：TFO の設定および動作をチェックします。
- [WCCP configuration and operation]：WCCP トラフィック代行受信の設定および動作をチェックします。
- [Inline configuration and operation]：インライン グループ インターフェイスの設定および動作をチェックします。
- [WAFS configuration and operation]：WAFS サービスの設定および動作をチェックします。

ステップ 5　[Run] をクリックします。

ステップ 6　ウィンドウの下部にテスト結果を表示します。結果をすべて表示するには、ウィンドウをスクロールする必要があります。

失敗したテストの場合、エラー メッセージは問題について説明し、推奨するソリューションを提供します。

同じ診断テストを実行し、タスクバーの [Refresh] アイコンをクリックして結果を更新できます。

結果を印刷するには、タスクバーの [Print] アイコンをクリックします。

CLI を使用したトラブルシューティング

test EXEC コマンドを使用して、診断テストおよび接続テストを実行できます。

ネットワークレベルのツールを使用して、パケットがネットワークを経由している途中で、そのパケットを代行受信し分析できます。これらのツールの 2 つが TCPdump と Tethereal であり、**tcpdump** および **tethereal** EXEC コマンドを使用して、CLI からアクセスできます。

WAAS デバイスは、複数のデバッグ モードをサポートしています。各モードは、**debug** EXEC コマンドを使用して切り替えることができます。これらのモードでは、設定エラーからプリント スプーラの問題に至るまでさまざまな問題をトラブルシューティングできます。**debug** コマンドは、Cisco TAC の指示があった場合に限り使用することを推奨します。

debug コマンドに関連した出力は、/local1/syslog.txt の Syslog ファイルか、またはファイル /local1/errorlog/*module_name*-errorlog.current のモジュールに関連したデバッグ ログに書き込まれます。

アプリケーション アクセラレータの **debug accelerator** *name module* コマンドに関連した出力は、ファイル *name*ao-errorlog.current に書き込まれます。*name* はアクセラレータ名です。アクセラレータ情報マネージャ デバッグ出力はファイル aoim-errorlog.current に書き込まれます。

モジュールに関連したデバッグ ログ ファイルは、現在のファイルが最大サイズに達したらバックアップ ファイルに切り替わります。バックアップ ファイルには *name*-errorlog#の名前が付いています。# はバックアップ ファイル番号です。

debug コマンドの場合、システム ログを有効にする必要があります。ログを有効にするコマンドは **logging disk enable** グローバル コンフィギュレーション コマンドです。これは、デフォルトで有効です。

debug コマンド モジュールがデバッグ出力の Syslog を使用する場合、**logging disk priority debug** グローバル コンフィギュレーション コマンドを設定する必要があります（デフォルトは **logging disk priority notice** です）。

debug コマンド モジュールが出力のデバッグ ログを使用する場合、次のようなデバッグ ログ出力の 4 つの異なるレベルの優先順位設定に基づいて出力をフィルタリングできます。

- クリティカルなデバッグ メッセージだけでフィルタリングするには、**logging disk priority critical** グローバル コンフィギュレーション コマンドを使用します。
- クリティカルおよびエラー レベルのデバッグ メッセージでフィルタリングするには、**logging disk priority error** グローバル コンフィギュレーション コマンドを使用します。
- クリティカル、エラー、およびトレース レベルのデバッグ メッセージでフィルタリングするには、**logging disk priority debug** グローバル コンフィギュレーション コマンドを使用します。
- すべてのデバッグ ログ メッセージ（クリティカル、エラー、トレース、および詳細なメッセージを含む）を検出するには、**logging disk priority detail** グローバル コンフィギュレーション コマンドを使用します。

優先順位の設定に関係なく、LOG_ERROR 以上のプライオリティの Syslog メッセージは、モジュールに関連したデバッグ ログに自動的に書き込まれます。

これらの CLI コマンドの詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

WAAS Central Manager GUI からの show コマンドと clear コマンドの使用

WAAS Central Manager GUI の **show** コマンド ツールと **clear** コマンド ツールを使用するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します。

ステップ 2　**show** または **clear** コマンドを発行するデバイスの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Troubleshoot] > [CLI Commands] を選択し、[Show Commands] または [Clear Commands] をクリックします。

ステップ 4　ドロップダウン リストから、**show** コマンドまたは **clear** コマンドを選択します。

ステップ 5　コマンドの引数を入力します（存在する場合のみ）。

ステップ 6　[Submit] をクリックして、コマンド出力を表示します。

ウィンドウが表示され、そのデバイス用のコマンド出力が表示されます。

また、CLI から、**show** EXEC コマンドを使用することもできます。詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。

CHAPTER 17

SNMP モニタリングの設定

この章では、SNMP トラップ、受信者、コミュニティ ストリングおよびグループの関連性、ユーザ セキュリティ モデル グループ、ユーザ アクセス権を設定する方法について説明します。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

この章の構成は、次のとおりです。

SNMP について

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）は、SNMP エージェントを介して Wide Area Application Service（WAAS）デバイスを外部モニタできる、相互運用可能な標準ベースのプロトコルです。

SNMP によって管理されるネットワークは、次のプライマリ コンポーネントから構成されます。

- 管理対象デバイス：SNMP エージェントを持つネットワーク ノードで、管理対象ネットワークに常駐します。管理対象デバイスには、ルータ、アクセス サーバ、スイッチ、ブリッジ、ハブ、コンピュータ ホスト、プリンタなどがあります。WAAS ソフトウェアを実行する各 WAAS デバイスは、SNMP エージェントを持っています。
- SNMP エージェント：管理対象デバイスに常駐するソフトウェア モジュールです。エージェントは、管理情報のうちローカルに関する知識を保持し、その情報を SNMP と互換可能な形式に変換します。SNMP エージェントは、Management Information Base（MIB; 管理情報ベース）からデータを収集します。MIB は、デバイス パラメータとネットワーク データに関する情報のリポジトリです。また、エージェントは、トラップ、つまり特定イベントの通知を管理システムに送信することもできます。
- 管理ステーション：SNMP ホストと呼ぶこともあります。管理ステーションは、SNMP を使用して SNMP エージェントに SNMP Get 要求を送信して、WAAS デバイスから情報を取得します。次に、管理対象デバイスは、管理情報を収集して保存し、SNMP を使用してこの情報を管理ステーションに提供します。

事前に、SNMP 管理アプリケーションが管理ステーションで展開されていないと、この SNMP 情報にはアクセスできません。この SNMP 管理ステーションは、SNMP を使用して SNMP Get 要求をデバイス エージェントに送信して WAAS デバイスから情報を取得するため、SNMP ホストと呼ばれています。

ここでは、次の内容について説明します。

SNMP 通信プロセス

SNMP 管理ステーションと WAAS デバイスに存在する SNMP エージェントは、SNMP を使用して、次のように通信します。

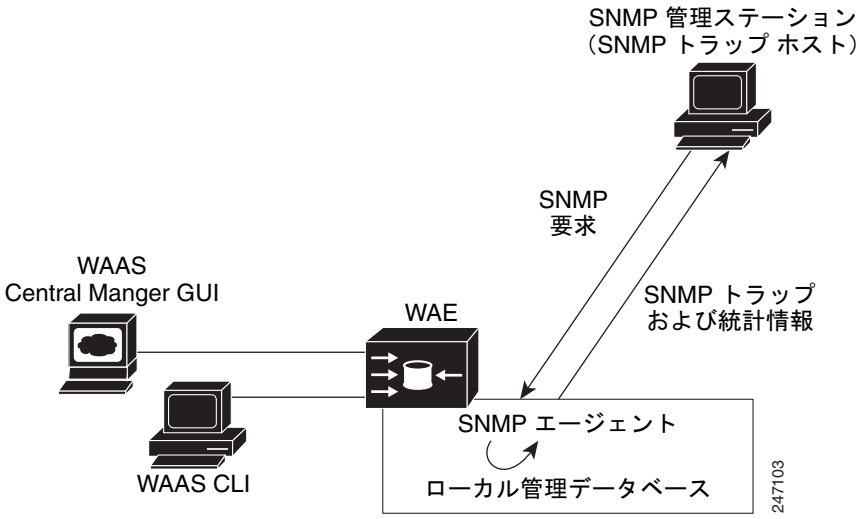
1. SNMP 管理ステーション（SNMP ホスト）は、SNMP を使用して WAAS デバイスに情報を要求します。
2. これらの SNMP 要求を受信すると、WAAS デバイス上の SNMP エージェントは、個々のデバイスに関する情報を保持しているテーブルにアクセスします。このテーブル、またはデータベースが、MIB と呼ばれます。

（注）　WAAS デバイス上の SNMP エージェントは、異常な状況でだけ SNMP ホストとの通信を開始します。つまり、ホストに送信する必要のあるトラップがある場合にホストとの通信を開始します。この項目の詳細については、「SNMP トラップの有効化」（P.17-9）を参照してください。

3. エージェントは、MIB 内で指定された情報を見つけると、SNMP を使用して、その情報を SNMP 管理ステーションに送信します。

図 17-1 に、個々の WAAS デバイス用のこれらの SNMP 操作を示します。

図 17-1　WAAS ネットワーク内の SNMP コンポーネント



サポートされている SNMP バージョン

WAAS ソフトウェアは、次の SNMP のバージョンをサポートします。

- バージョン 1（SNMPv1）：SNMP の初期の実装です。機能の完全な説明については、RFC 1157 を参照してください。
- バージョン 2（SNMPv2c）：SNMP の 2 番めのリリースで、RFC 1902 に規定されています。データ タイプ、カウンタ サイズ、およびプロトコル動作に追加があります。
- バージョン 3（SNMPv3）：最新バージョンの SNMP で、RFC 2271 ～ RFC 2275 に規定されています。

WAAS ソフトウェアを実行する各シスコ デバイスは、SNMP プロトコルを使用してデバイス設定と操作に関する情報を交換するために必要なソフトウェアを搭載しています。

SNMP セキュリティ モデルおよびセキュリティ レベル

SNMPv1 および SNMPv2c には、SNMP パケット トラフィックの機密性を保持するためのセキュリティ（つまり、認証またはプライバシー）機能がありません。その結果、ワイヤ上のパケットが検出され、SNMP コミュニティ ストリングが見破られてしまうことがあります。

SNMPv1 および SNMPv2c のセキュリティ上の欠点を解決するために、SNMPv3 では、ネットワークを経由するパケットを認証および暗号化することで、WAAS デバイスへの安全なアクセスを実現しています。WAAS ソフトウェアの SNMP エージェントは、SNMPv3 はもちろん、SNMPv1 と SNMPv2c もサポートします。

SNMPv3 で提供されるセキュリティ機能は、次のとおりです。

- メッセージの完全性：伝送中にパケットが一切妨害されていないことを保証します。
- 認証：有効な送信元からのメッセージであるかどうかを判別します。
- 暗号化：不正な送信元によってパケットが認識されてしまうのを防ぐため、パケットの内容をスクランブルします。

SNMPv3 は、セキュリティ モデルだけでなく、セキュリティ レベルも備えています。セキュリティ モデルは、ユーザと、ユーザが所属するグループに対して設定される認証プロセスです。セキュリティ レベルは、セキュリティ モデルの中で許容されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットの処理時に使用されるセキュリティ プロセスが決まります。使用可能なセキュリティ モデルは、SNMPv1、SNMPv2c、および SNMPv3 の 3 つです。

表 17-1 は、セキュリティ モデルとセキュリティ レベルの組み合わせをまとめたものです。

表 17-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	プロセス
v1	noAuthNoPriv	コミュニティ ストリング	なし	ユーザ認証の照合にコミュニティ ストリングを使用します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	ユーザ認証の照合にコミュニティ ストリングを使用します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ認証の照合にユーザ名を使用します。
v3	AuthNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	なし	Hash-Based Message Authentication Code（HMAC）-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。
v3	AuthPriv	MD5 または SHA	あり	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。Cipher Block Chaining（CBC; 暗号ブロック連鎖）-Data Encryption Standard 56-bit（DES-56; データ暗号規格 56 ビット）に基づく、DES-56 暗号化（パケット認証）を提供します。

SNMPv3 エージェントは、次のモードで使用できます。

- noAuthNoPriv モード（パケットに対してオンになっているセキュリティ メカニズムはありません）
- AuthNoPriv モード（プライバシー アルゴリズム（DES-56）を使用して暗号化する必要がない、パケット用）
- AuthPriv モード（暗号化する必要があるパケット用。プライバシーを保持するには、パケットに対して認証を実行する必要があります）

SNMPv3 を使用すれば、ユーザは、データが改ざんされるおそれを抱くことなく、SNMP エージェントから管理情報を安全に収集できます。また、Content Engine の設定を変更する SNMP set パケットなどの機密情報は、ワイヤ上で内容が露呈するのを防ぐために、暗号化できます。グループベースの管理モデルでは、さまざまなユーザが異なるアクセス特権で同じ SNMP エージェントにアクセスできます。

サポートされる MIB

この項では、WAAS がサポートしている シスコ固有の MIB について説明します。MIB は、アルファベット順に掲載されています。サポートされている シスコ固有の MIB は、次のとおりです。

- 「ACTONA-ACTASTOR-MIB」
- 「CISCO-CDP-MIB」
- 「CISCO-CONFIG-MAN-MIB」
- 「CISCO-CONTENT-ENGINE-MIB」
- 「CISCO-ENTITY-ASSET-MIB」

- 「CISCO-SMI」
- 「ENTITY-MIB」
- 「EVENT-MIB」
- 「HOST-RESOURCES-MIB」
- 「MIB-II」
- 「SNMP-COMMUNITY-MIB」
- 「SNMP-FRAMEWORK-MIB」
- 「SNMP-NOTIFICATION-MIB」
- 「SNMP-TARGET-MIB」
- 「SNMP-USM-MIB」
- 「SNMPv2-MIB」
- 「SNMP-VACM-MIB」

ACTONA-ACTASTOR-MIB

この MIB は、CIFS 透過的アクセラレータの統計情報と、WAAS 内のレガシー モードの WAFS コンポーネントの統計情報およびログ トラップを提供します。

CISCO-CDP-MIB

この MIB は、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 リピータの場合、この値はポートで一意の値になり、リピータがサポートしているどの ifIndex 値よりも大きくなります。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、これらの値が RFC 1516 のグループ番号とポート番号の値に対応します。

CISCO-CONFIG-MAN-MIB

この MIB は、さまざまな位置に存在する設定データのモデルを表します。

- running：動作中のシステムで使用中
- terminal：端末として接続されているハードウェアに保存
- local：NVRAM またはフラッシュ メモリにローカルに保存
- remote：ネットワーク上のサーバに保存

この MIB は、特に設定に関係する操作だけを含みますが、一般的なファイル保存と転送には一部のシステム機能を使用できます。

CISCO-CONTENT-ENGINE-MIB

これは、米国シスコシステムズ社の Cisco WAE デバイス用の MIB モジュールです。この MIB の次のオブジェクトがサポートされています。

- cceAlarmCriticalCount
- cceAlarmMajorCount
- cceAlarmMinorCount
- cceAlarmHistTable

CISCO-ENTITY-ASSET-MIB

この MIB は、ENTITY-MIB（RFC 2037）entPhysicalTable の資産情報項目をモニタします。この MIB は、MIBentPhysicalTable に表示される関連するエンティティの注文可能製品番号、シリアル番号、ハードウェア リビジョン、製造番号およびリビジョン、ファームウェア ID およびリビジョン（存在する場合）およびソフトウェア ID およびリビジョン（存在する場合）を表示します。

このデータが使用できないエンティティは、この MIB に表示されません。この MIB の表はほとんど埋まっていないので、特定の時点で特定のエンティティに一部の変数が存在しない場合があります。たとえば、電源が入っていないモジュールを示す行は、ソフトウェア ID（ceAssetSoftwareID）とリビジョン（ceAssetSoftwareRevision）に値がない場合があります。同様に、電源モジュールは、表にファームウェアやソフトウェア情報が表示されません。

データに他の項目が埋め込まれている場合がありますが（シリアル番号の中の製造日付など）、すべてのデータ項目を 1 つの単位と見なします。項目を分解したり、項目を構文解析しないでください。文字列の等価および非等価演算だけを使用してください。

CISCO-SMI

これは、Cisco Enterprise Structure of Management Information の MIB モジュールです。この MID でクエリーするものはありません。これは、Cisco MIB の構造を表します。

ENTITY-MIB

これは、1 つの SNMP エージェントがサポートする複数の論理エンティティを表すための MIB モジュールです。この MIB は、RFC 2737 で文章化されています。この MIB の次のグループがサポートされています。

- entityPhysicalGroup
- entityLogicalGroup

entConfigChange 通知がサポートされています。

EVENT-MIB

この MIB は、ネットワーク管理目的でイベント トリガーと処理を定義します。この MIB は、RFC 2981 として文章化されています。

HOST-RESOURCES-MIB

この MIB は、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している他の同様なコンピュータと通信する任意のコンピュータを示します。HOST-RESOURCES-MIB は、通信サービスが主な機能であるデバイス（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わけではありません。この MIB は、すべてのインターネット ホスト（たとえば、パーソナル コンピュータや UNIX が稼動するシステム）に共通の属性を提供します。この MIB の次のオブジェクトはサポートされていません。

- HrPrinterEntry
- hrSWOSIndex
- hrSWInstalledGroup

MIB-II

MIB-II は、インターネット標準 MIB です。MIB-II は、RFC 1213 に規定され、TCP/IP に基づくインターネットのネットワーク管理プロトコル用です。この MIB は、ダウンロード サイトの v1 ディレクトリにある RFC1213-MIB ファイル内にあります（他の MIB は v2 ディレクトリ内）。この MIB の次のオブジェクトはサポートされていません。

- ifInUcastPkts
- ifInUnknownProtos
- ifOutUcastPkts
- ifOutNUcastPkts
- ipRouteAge
- TcpConnEntry group
- egpInMsgs
- egpInErrors
- egpOutMsgs
- egpOutErrors
- EgpNeighEntry group
- egpAs

SNMP-COMMUNITY-MIB

この MIB は、RFC 2576 で文章化されています。

SNMP-FRAMEWORK-MIB

この MIB は、RFC 2571 で文章化されています。

SNMP-NOTIFICATION-MIB

この MIB は、RFC 3413 で文章化されています。

SNMP-TARGET-MIB

この MIB は、RFC 3413 で文章化されています。

SNMP-USM-MIB

この MIB は、RFC 2574 で文章化されています。

SNMPv2-MIB

この MIB は、RFC 1907 で文章化されています。WAAS では、この MIB の次の通知がサポートされています。

- coldStart
- linkUp
- linkDown
- authenticationFailure

SNMP-VACM-MIB

この MIB は、RFC 2575 で文章化されています。

MIB ファイルのダウンロード

WAAS ソフトウェアが稼動しているデバイスでサポートされるほとんどの MIB について、MIB ファイルを次の Cisco FTP サイトからダウンロードできます。

ftp://ftp.cisco.com/pub/mibs/v2

RFC1213-MIB ファイル（MIB-II の場合）は、次の Cisco FTP サイトからダウンロードできます。

ftp://ftp.cisco.com/pub/mibs/v1

各 MIB に定義されている MIB オブジェクトは、上記 FTP サイトの MIB ファイルに、一目でわかる形で記述されています。

WAAS デバイス上の SNMP エージェントの有効化

デフォルトでは、WAAS デバイス上の SNMP エージェントが無効になっており、SNMP コミュニティ ストリングは定義されていません。SNMP コミュニティ ストリングは、WAAS デバイス上の SNMP エージェントへアクセスするときに、認証用のパスワードとして使用されます。認証されるには、WAAS デバイスに送信された SNMP メッセージの Community Name フィールドが、WAAS デバイスに定義された SNMP コミュニティ ストリングに一致している必要があります。

デバイスに SNMP コミュニティ ストリングを定義すると、WAAS デバイス上の SNMP エージェントが有効になります。WAAS Central Manager GUI を使用すると、デバイスまたはデバイス グループに SNMP コミュニティ ストリングを定義できます。

SNMP 要求に SNMPv3 プロトコルが使用されている場合は、次のステップで、SNMP ユーザ アカウントを定義します。このアカウントは、SNMP を使用して WAAS デバイスにアクセスするために使用できます。WAAS デバイスで SNMPv3 ユーザ アカウントを作成する方法の詳細については、「SNMP ユーザの作成」（P.17-19）を参照してください。

SNMP を設定するためのチェックリスト

表 17-2 で、WAAS デバイスまたはデバイス グループで SNMP モニタリングを有効にするためのプロセスについて説明します。

表 17-2　SNMP を設定するためのチェックリスト

作業	追加情報と手順
1. SNMP モニタリングの準備をする。	詳細については、「SNMP モニタリングの準備」（P.17-9）を参照してください。
2. 有効にしたい SNMP トラップを選択する。	WAAS Central Manager は、WAAS デバイスまたはデバイス グループで有効にできるさまざまなトラップを提供しています。 詳細については、「SNMP トラップの有効化」（P.17-9）を参照してください。追加のトラップを定義するには、「SNMP トラップの定義」（P.17-12）を参照してください。

表 17-2　SNMP を設定するためのチェックリスト （続き）

作業	追加情報と手順
3. SNMP トラップを受信する SNMP ホストを指定する。	WAAS デバイスまたはデバイス グループがトラップを送信する必要がある SNMP ホストを指定します。異なる WAAS デバイスが異なるホストへトラップを送信できるように、複数のホストを指定できます。 詳細については、「SNMP ホストの指定」（P.17-14）を参照してください。
4. SNMP コミュニティ ストリングを指定する。	外部ユーザが MIB の読み取りまたは書き込みを実行できるように、SNMP コミュニティ ストリングを指定します。 詳細については、「SNMP コミュニティ ストリングの指定」（P.17-15）を参照してください。
5. SNMP ビューを設定する。	SNMP グループを特定のビューに制限するには、グループに表示したい MIB サブツリーを指定するビューを作成する必要があります。 詳細については、「SNMP ビューの作成」（P.17-16）を参照してください。
6. SNMP グループを作成する。	任意の SNMP ユーザを作成する、またはグループが特定の MIB サブツリーを表示するように制限したい場合は、SNMP グループを設定する必要があります。 詳細については、「SNMP グループの作成」（P.17-17）を参照してください。
7. SNMP ユーザを作成する。	SNMP 要求に SNMPv3 プロトコルが使用されている場合は、SNMP を使用して WAAS デバイスにアクセスするために、少なくとも 1 つの SNMPv3 ユーザ アカウントを WAAS デバイスに定義する必要があります。 詳細については、「SNMP ユーザの作成」（P.17-19）を参照してください。
8. SNMP 連絡先設定を構成する。	詳細については、「SNMP 連絡先設定の構成」（P.17-20）を参照してください。

SNMP モニタリングの準備

WAAS ネットワークを SNMP モニタリング用に設定する前に、次の準備作業を完了します。

- WAAS デバイスが SNMP トラップを送信するために使用する SNMP ホスト（管理ステーション）を設定します。
- すべての WAAS デバイスがトラップを同じホストへ送信するか、異なるホストへ送信するかを決定します。各 SNMP ホストの IP アドレスまたはホスト名を書き留めます。
- SNMP エージェントにアクセスするために使用するコミュニティ ストリングを入手します。
- グループ別にビューを制限できるように SNMP グループを作成するかどうかを決定します。
- 必要な追加の SNMP トラップを決定します。
- WAAS ネットワーク内のデバイス間でクロックを同期することが重要です。各 WAAS デバイス上で、クロックを同期するために Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバが設定されていることを確認します。

SNMP トラップの有効化

WAAS デバイスが SNMP トラップを送信できるようにするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。選択に応じて、[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP トラップを設定したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[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 17-2 を参照）。表 17-3 で、このウィンドウのフィールドについて説明します。

図 17-2　[SNMP General Settings] ウィンドウ

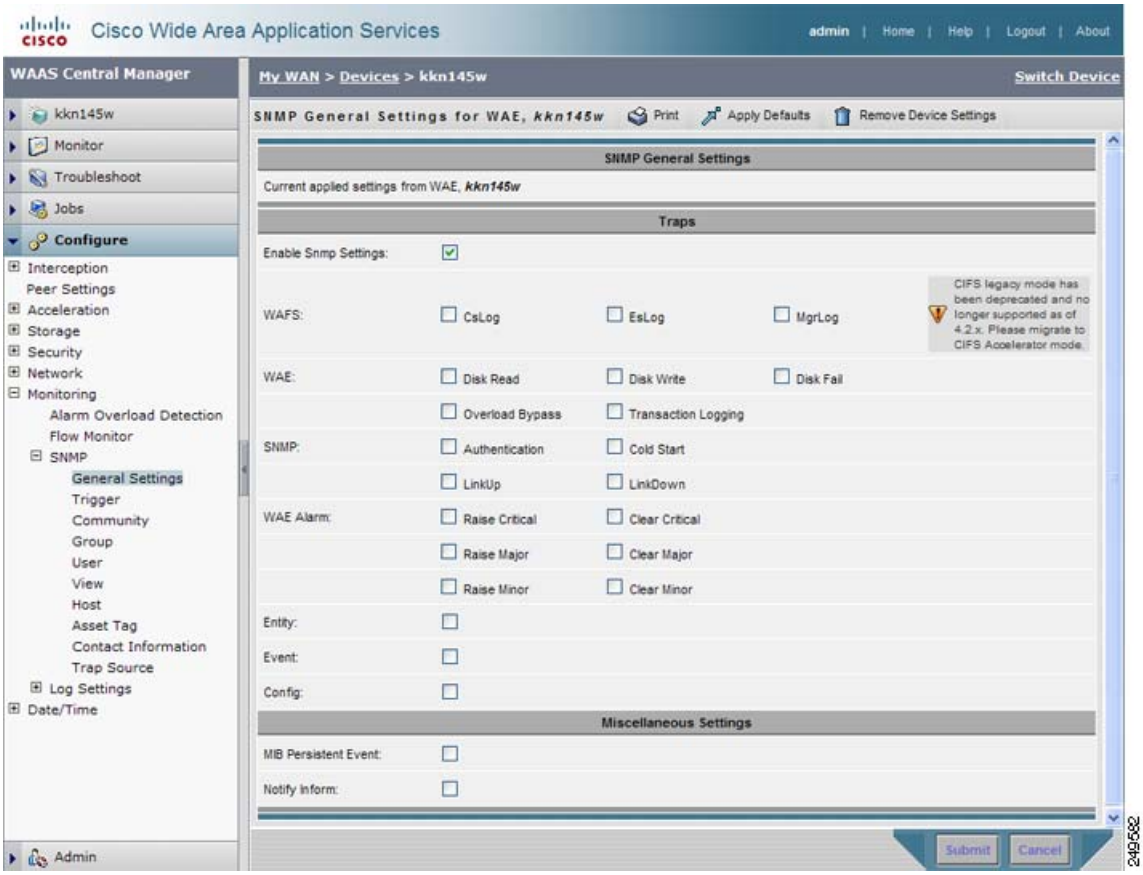


表 17-3　SNMP 一般設定

GUI パラメータ	機能
[Traps]	
[Enable Snmp Settings]	SNMP トラップを有効にします。

表 17-3　SNMP 一般設定 （続き）

GUI パラメータ	機能
[WAFS]	SNMP WAFS トラップを有効にします。 • [CsLog] : WAFS レガシー モード コア サーバ エラー ログ トラップを有効にします。 • [EsLog] : WAFS レガシー モード エッジ サーバ エラー ログ トラップを有効にします。 • [MgrLog] : WAAS Central Manager エラー ログ トラップを有効にします。
[WAE]	SNMP WAE トラップを有効にします。 • [Disk Read] : ディスク読み取りエラー トラップを有効にします。 • [Disk Write] : ディスク書き込みエラー トラップを有効にします。 • [Disk Fail] : ディスク障害エラー トラップを有効にします。 • [Overload Bypass] : WCCP 過負荷迂回エラー トラップを有効にします。 • [Transaction Logging] : トランザクション ログ書き込みエラー トラップを有効にします。
[SNMP]	SNMP 固有トラップを有効にします。 • [Authentication] : 認証トラップを有効にします。 • [Cold Start] : コールド スタート トラップを有効にします。 • [LinkUp] : リンク アップ トラップ。 • [LinkDown] : リンク ダウン トラップ。
[WAE Alarm]	SNMP アラーム トラップを有効にします。 • [Raise Critical] : クリティカル アラーム設定トラップを有効にします。 • [Clear Critical] : クリティカル アラーム消去トラップを有効にします。 • [Raise Major] : メジャー アラーム設定トラップを有効にします。 • [Clear Major] : メジャー アラーム消去トラップを有効にします。 • [Raise Minor] : マイナー アラーム設定トラップを有効にします。 • [Clear Minor] : マイナー アラーム消去トラップを有効にします。
[Entity]	SNMP エンティティ トラップを有効にします。
[Event]	イベント MIB を有効にします。
[Config]	CiscoConfigManEvent エラー トラップを有効にします。

表 17-3　SNMP 一般設定 （続き）

GUI パラメータ	機能
[Miscellaneous Settings]	
[MIB Persistent Event]	SNMP Event MIB の永続性を有効にします（このチェックボックスは、選択されているデバイスが Central Manager の場合には表示されません）。
[Notify Inform]	SNMP notify inform 要求を有効にします。inform 要求は、トラップより信頼性に優れていますが、ルータとネットワークのリソース使用量が増えます。 受信者がトラップを受信したときに受信確認を送信しないため、トラップの信頼性は低くなります。送信側は、トラップが受信されたかどうかを決定できません。ただし、inform 要求を受信する SNMP マネージャは、SNMP 応答でメッセージの受信を確認します。送信側が応答を受信しない場合、inform 要求を再び送信できます。したがって、inform 要求が意図した送信先に到達する可能性が高くなります。

ステップ 4　SNMP トラップを有効にするには、該当するチェックボックスを選択します。

ステップ 5　[Submit] をクリックします。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、現在の設定の横に、「Click Submit to Save」メッセージが赤い色で表示されます。また、[Reset] をクリックすると、すでに設定したウィンドウ設定に戻すことができます。[Reset] ボタンは、デフォルトまたはデバイス グループ設定を適用して現在のデバイス設定を変更し、まだ設定を送信していない場合だけ表示されます。

CLI から SNMP トラップを有効にするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用できます。

特別な設定に関連した他の MIB オブジェクトの追加 SNMP トラップを定義するには、「SNMP トラップの定義」（P.17-12）を参照してください。

SNMP トラップの定義

特別な設定に関連した他の MIB オブジェクトの追加 SNMP トラップを定義するには、次の手順に従って追加の SNMP トリガーを作成してください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。選択に応じて、[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP トラップを定義したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [Trigger] を選択します。[SNMP Trigger List Entries] ウィンドウが表示されます。このウィンドウの列は、表 17-4 で示すパラメータと同じです。

ステップ 4　タスクバーで、[Create New SNMP Trigger List Entry] アイコンをクリックします。[Creating New SNMP Trigger] ウィンドウが表示されます。表 17-4 に、このウィンドウ内のフィールドについて説明します。

表 17-4　新しい SNMP トリガー設定の作成

GUI パラメータ	機能
[MIB Name]	モニタするオブジェクトの MIB 変数名
[Wild Card]	（任意）[MIB Name] 値がワイルドカードの場合、このチェックボックスを選択します。SNMP トリガーを編集するときは、このチェックボックスは無効になります。
[Frequency]	トリガー サンプルの間で待機する秒数（60 ～ 600）
[Test]	SNMP トラップを開始するのに使用するテスト。次のいずれかのテストを選択します。 • [absent]：最後のサンプリングで存在した指定の MIB オブジェクトが、現在のサンプリングでは存在しない。 • [equal]：指定された MIB オブジェクトの値が指定されたしきい値と等しい。 • [falling]：指定された MIB オブジェクトの値が、指定されたしきい値より低くなった。この状態に対してトラップを生成したあとに同じ状態が発生しても、サンプリングした MIB オブジェクトの値がしきい値を超え、再び下限しきい値より低くなるまで、別のトラップは生成されません。 • [greater-than]：指定された MIB オブジェクトの値が、指定されたしきい値より高い。 • [less-than]：指定された MIB オブジェクトの値が、指定されたしきい値より低い。 • [on-change]：最後のサンプリング以降、指定された MIB オブジェクトの値が変更された。 • [present]：以前のサンプリングでは存在しなかった指定の MIB オブジェクトが、現在のサンプリングで存在する。 • [rising]：指定された MIB オブジェクトの値が、指定されたしきい値を超えた。この状態に対してトラップを生成したあとに同じ状態が発生しても、サンプリングした MIB オブジェクトの値がしきい値より低くなり、再び上昇しきい値を超えるまで、別のトラップは生成されません。
[Sample Type]	（任意）サンプル タイプ。次のとおりです。 • [absolute]：0 ～ 2147483647 の範囲内の固定整数値に対して、テストが評価されます。 • [delta]：現在のサンプリングと以前のサンプリングの間における MIB オブジェクトの値の変動に対して、テストが評価さされます。
[Threshold Value]	MIB オブジェクトのしきい値。[Test] ドロップダウン リストで [absent]、[on-change]、または [present] が選択されると、このフィールドは使用されません。
[MIB Var1] [MIB Var2] [MIB Var3]	（任意）通知に追加する最大 3 つの代替 MIB 変数の名前。これらの名前の検証はサポートされないので、必ず正しい名前を入力してください。
[Comments]	トラップの説明

ステップ 5　上記のフィールドには、MIB 名、周期、テスト、サンプル タイプ、しきい値、および説明を入力します。

ステップ 6　[Submit] をクリックします。

新しい SNMP トリガーが [SNMP Trigger List] ウィンドウに表示されます。

[SNMP Trigger List Entries] ウィンドウの MIB 名の横にある [Edit] アイコンをクリックすると、SNMP トリガーを編集できます。

MIB 名の横にある Edit アイコンをクリックしてから、[Delete] タスクバー アイコンをクリックすると、SNMP トリガーを削除できます。

（注）　デフォルト SNMP トリガのいずれかを削除した場合、それはリロード後に復元されます。

CLI から SNMP トラップを定義するには、**snmp trigger** EXEC コマンドを使用できます。

SNMP トリガーの集約

個々の WAE デバイスは、カスタム SNMP トリガーを定義できます。また、他のカスタム SNMP トリガーが定義されているデバイス グループに所属することもできます。

[SNMP Trigger List Entries] ウィンドウ内の [Aggregate Settings] オプション ボタンは、個々のデバイスでの SNMP トリガーの集約方法を次のように制御します。

- デバイスの設定にそのデバイスとそれが所属するデバイス グループに定義されたすべてのカスタム SNMP トリガーを使用する場合は、[Yes] を選択します。
- デバイス自身に定義されたカスタム SNMP トリガーだけに制限する場合は、[No] を選択します。

設定を変更すると次のメッセージが表示されます。「This option will take effect immediately and will affect the device configuration. Do you wish to continue?」。[OK] をクリックして続行します。

SNMP ホストの指定

ホストは、作成順に表示されます。作成できる SNMP ホストの最大数は 4 です。

SNMP ホストを指定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP ホストを定義したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウまたは [Modifying Device Groups] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [Host] を選択します。[SNMP Hosts] ウィンドウが表示されます。

ステップ 4　タスクバーで、[Create New SNMP Host] アイコンをクリックします。[Creating New SNMP Host] ウィンドウが表示されます。表 17-5 に、このウィンドウ内のフィールドについて説明します。

表 17-5　SNMP ホスト設定

GUI パラメータ	機能
[Trap Host]	WAE から SNMP トラップ メッセージで送信される SNMP トラップ ホストのホスト名または IP アドレス。これは必須フィールドです。
[Community/User]	WAE から SNMP トラップ メッセージで送信される SNMP コミュニティまたはユーザの名前（最大 64 文字）。これは必須フィールドです。
[Authentication]	SNMP トラップ動作の受信者へ通知を送信するために使用するセキュリティ モデル。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [No-auth]：セキュリティ メカニズムなしで通知を送信します。 • [v2c]：バージョン 2c セキュリティを使用して通知を送信します。 • [v3-auth]：SNMP バージョン 3 AuthNoPriv を使用して通知を送信します。 • [v3-noauth]：SNMP バージョン 3 NoAuthNoPriv を使用して通知を送信します。 • [v3-priv]：SNMP バージョン 3 AuthPriv を使用して通知を送信します。
[Retry]	inform 要求に許される再試行回数（1 ～ 10）。デフォルトは、2 回です。
[Timeout]	inform 要求のタイムアウト（1 ～ 1000 秒）。デフォルトは 15 秒です。

ステップ 5　SNMP トラップ ホストのホスト名または IP アドレス、SNMP コミュニティまたはユーザ名、通知を送信するためのセキュリティ モデル、および inform 要求の再試行回数とタイムアウトを入力します。

ステップ 6　[Submit] をクリックします。

CLI から SNMP ホストを指定するには、**snmp-server host** グローバル コンフィギュレーション コマンドを使用できます。

SNMP コミュニティ ストリングの指定

SNMP コミュニティ ストリングは、WAAS デバイスに存在する SNMP エージェントにアクセスするために使用するパスワードです。コミュニティ ストリングは、group と read-write の 2 種類あります。コミュニティ ストリングは、SNMP メッセージのセキュリティを強化します。

コミュニティ ストリングは、作成順に表示されます。作成できる SNMP コミュニティの最大数は 10 です。デフォルトでは、SNMP エージェントは無効で、コミュニティ ストリングは設定されていません。コミュニティ ストリングを設定すると、デフォルトですべてのエージェントへの読み取り専用アクセスが許可されます。

SNMP エージェントを有効にし、SNMP エージェントにアクセスできるコミュニティ ストリングを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP コミュニティ設定を構成したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [Community] を選択します。[SNMP Community Strings] ウィンドウが表示されます。

ステップ 4　タスクバーで、[Create New SNMP Community String] アイコンをクリックします。[Creating New SNMP Community String] ウィンドウが表示されます。表 17-6 に、このウィンドウ内のフィールドについて説明します。

表 17-6　SNMP コミュニティ設定

GUI パラメータ	機能
[Community]	WAE の SNMP エージェントにアクセスするときに認証用のパスワードとして使用するコミュニティ ストリング。認証されるには、WAE に送信された SNMP メッセージの「Community Name」フィールドが、ここで定義した SNMP コミュニティ ストリングに一致している必要があります。コミュニティ ストリングを入力すると、WAE 上の SNMP エージェントが有効になります。このフィールドには、最大 64 文字を入力できます。 これは必須フィールドです。
[Group name/rw]	コミュニティ ストリングが属するグループ。[Read/Write] オプションを使用すると、このコミュニティ ストリングに read または write グループを関連付けることができます。[Read/Write] オプションは、MIB サブツリーの一部へのアクセスだけを許可します。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [None]：コミュニティ ストリングに関連付けるグループ名を指定したくない場合は、このオプションを選択します。このオプションを選択すると、[Group Name] フィールドは無効のままになります。 • [Group]：グループ名を指定したい場合は、このオプションを選択します。 • [Read/Write]：コミュニティ ストリングに関連付けられたグループへの読み取り / 書き込みアクセスを許可したい場合は、このオプションを選択します。このオプションを選択すると、[Group Name] フィールドは無効のままになります。 これは必須フィールドです。
[Group Name]	コミュニティ ストリングが属するグループの名前。このフィールドには、最大 64 文字を入力できます。このフィールドは、前のフィールドで [Group] オプションを選択した場合にだけ使用できます。

ステップ 5　適切なフィールドに、コミュニティ ストリングを入力し、グループへの読み取り / 書き込みアクセスを許可するかどうかを選択し、グループ名を入力します。

ステップ 6　[Submit] をクリックします。

CLI からコミュニティ ストリングを設定するには、**snmp-server community** グローバル コンフィギュレーション コマンドを使用できます。

SNMP ビューの作成

ユーザのグループを特定の MIB ツリーを表示するだけに制限するには、WAAS Central Manager GUI を使用して SNMP ビューを作成する必要があります。ビューを作成したら、後続の項の説明に従って、このグループに属する SNMP グループと SNMP ユーザを作成する必要があります。

ビューは、作成順に表示されます。作成できるビューの最大数は 10 です。

バージョン 2 SNMP（SNMPv2）MIB ビューを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMPv2 ビューを作成したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [View] を選択します。[SNMP Views] ウィンドウが表示されます。

ステップ 4　タスクバーで、[Create New View] アイコンをクリックします。[Creating New SNMP View] ウィンドウが表示されます。表 17-7 に、このウィンドウ内のフィールドについて説明します。

表 17-7　SNMPv2 ビュー設定

GUI パラメータ	機能
[Name]	このビュー サブツリーのファミリ名を表す文字列（最大 64 文字）。ファミリ名は、ENTITY-MIB のような有効な MIB 名である必要があります。これは必須フィールドです。
[Family]	MIB のサブツリーを識別するオブジェクト ID（最大 64 文字）。これは必須フィールドです。
[View Type]	ビューから MIB ファミリを包含するか、除外するかを決定するビュー オプション。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [Included] : MIB ファミリをビューに入れます。 • [Excluded] : MIB ファミリをビューから除外します。

ステップ 5　適切なフィールドに、ビュー名、ファミリ名、およびビューの種類を入力します。

ステップ 6　[Submit] をクリックします。

ステップ 7　あとの項の説明に従って、このビューに割り当てる SNMP グループを作成します。

CLI から SNMP ビューを作成するには、**snmp-server view** グローバル コンフィギュレーション コマンドを使用できます。

SNMP グループの作成

任意の SNMP ユーザを作成する、またはユーザのグループが特定の MIB サブツリーを表示するように制限したい場合は、SNMP グループを設定する必要があります。

グループは、作成順に表示されます。作成できる SNMP グループの最大数は 10 です。

ユーザ セキュリティ モデル グループを定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP グループを作成したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウまたは [Modifying Device Group] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [Group] を選択します。[SNMP Group Strings for WAE] ウィンドウが表示されます。

ステップ 4　タスクバーで、[Create New SNMP Group String] アイコンをクリックします。[Creating New SNMP Group String for WAE] ウィンドウが表示されます。表 17-8 に、このウィンドウ内のフィールドについて説明します。

表 17-8　SNMP グループ設定

GUI パラメータ	機能
[Name]	SNMP グループの名前。最大 64 文字を入力できます。これは必須フィールドです。
[Sec Model]	グループ用のセキュリティ モデル。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [v1]：バージョン 1 セキュリティ モデル（SNMP バージョン 1 [noAuthNoPriv]） • [v2c]：バージョン 2c セキュリティ モデル（SNMP バージョン 2 [noAuthNoPriv]） • [v3-auth]：ユーザ セキュリティ レベル SNMP バージョン 3 AuthNoPriv • [v3-noauth]：ユーザ セキュリティ レベル SNMP バージョン 3 noAuthNoPriv • [v3-priv]：ユーザ セキュリティ レベル SNMP バージョン 3 AuthPriv **（注）** SNMPv1 または SNMPv2c セキュリティ モデルに従って定義されたグループは、SNMP ユーザには関連付けないでください。それらは、コミュニティ ストリングだけに関連付ける必要があります。
[Read View]	エージェントの内容を表示できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。グループのユーザに読み取りアクセスを提供するには、ビューを指定する必要があります。 SNMP ビューを作成する方法については、「SNMP ビューの作成」（P.17-16）を参照してください。
[Write View]	データを入力し、エージェントの内容を設定できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。 SNMP ビューを作成する方法については、「SNMP ビューの作成」（P.17-16）を参照してください。
[Notify View]	notify、inform、または trap を指定できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。 SNMP ビューを作成する方法については、「SNMP ビューの作成」（P.17-16）を参照してください。

ステップ 5　適切なフィールドに、SNMP グループ設定名、セキュリティ モデル、および読み取り、書き込み、および通知ビューの名前を入力します。

ステップ 6　[Submit] をクリックします。

ステップ 7　あとの項の説明に従って、この新しいグループに属する SNMP ユーザを作成します。

CLI から SNMP グループを作成するには、**snmp-server group** グローバル コンフィギュレーション コマンドを使用できます。

SNMP ユーザの作成

ユーザは、作成順に表示されます。作成できるユーザの最大数は 10 です。

SNMP エンジンにアクセスできるユーザを定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP ユーザを作成したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [User] を選択します。デバイスまたはデバイス グループ用の SNMP ユーザのリストが表示されます。

ステップ 4　タスクバーで、[Create New SNMP User] アイコンをクリックします。[Creating New SNMP User] ウィンドウが表示されます。表 17-9 に、このウィンドウ内のフィールドについて説明します。

表 17-9　SNMP ユーザ設定

GUI パラメータ	機能
[Name]	デバイスまたはデバイス グループにアクセスできるユーザの名前を表す文字列（最大 32 文字）。これは必須フィールドです。
[Group]	ユーザが属するグループの名前（最大 64 文字）。これは必須フィールドです。
[Remote SNMP ID]	リモート SNMP エンティティのグローバルに一意名識別子（10 ～ 64 文字）。SNMPv3 メッセージを WAE へ送信するには、WAE にリモート SNMP ID を持つ少なくとも 1 人のユーザを設定する必要があります。SNMP ID は、オクテット文字列形式で入力する必要があります。このフィールドに入力できるのは、16 進数文字とコロン（:）だけです。入力した文字列に何らかの色がついた場合、それはページの送信後に削除されます。
[Authentication Algorithm]	送信中の SNMP パケットの完全性を保証する認証アルゴリズム。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [No-auth]：SNMP パケット用にセキュリティ メカニズムをオンにする必要がありません。 • [MD5]：ハッシュに基づくメッセージ認証コード MD5（HMAC-MD5）アルゴリズムに基づく認証を提供します。 • [SHA]：ハッシュに基づくメッセージ認証コード安全なハッシュ（HMAC-SHA）アルゴリズムに基づく認証を提供します。
[Authentication Password]	ユーザ認証（HMAC-MD5 または HMAC-SHA）パスワードを設定する文字列（最大 256 文字）。表示制限を超える場合、文字数が表示領域に合わせて調整されます。 認証アルゴリズム用に [no-auth] オプションを選択した場合、このフィールドはオプションです。そうでない場合は、このフィールドに値を入力する必要があります。
[Confirmation Password]	確認用の認証パスワード。再入力するパスワードは、前のフィールドに入力したパスワードと同じである必要があります。

表 17-9　SNMP ユーザ設定 （続き）

GUI パラメータ	機能
[Private Password]	SNMP エージェントが SNMP ホストからパケットを受信できるようにする認証（HMAC-MD5 または HMAC-SHA）パラメータを設定する文字列（最大 256 文字）。表示制限を超える場合、文字数が表示領域に合わせて調整されます。
[Confirmation Password]	確認用のプライベート パスワード。再入力するパスワードは、前のフィールドに入力したパスワードと同じである必要があります。

ステップ 5　適切なフィールドに、ユーザ名、ユーザが属するグループ、ユーザが属するリモート エンティティのエンジン ID、SNMP トラフィックの改ざんから保護するために使用する認証アルゴリズム、ユーザ認証パラメータ、およびパケット用の認証パラメータを入力します。

ステップ 6　[Submit] をクリックします。

CLI から SNMP ユーザを作成するには、**snmp-server user** グローバル コンフィギュレーション コマンドを使用できます。

SNMP 資産タグ設定の構成

CISCO-ENTITY-ASSET-MIB に値を作成する SNMP 資産タグ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP 資産タグを定義したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウまたは [Modifying Device Groups] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [Asset Tag] を選択します。[SNMP Asset Tag Settings] ウィンドウが表示されます。

ステップ 4　[Asset Tag Name] フィールドに、資産タグの名前を入力します。

ステップ 5　[Submit] をクリックします。

CLI から SNMP 資産タグ設定を構成するには、**asset tag** グローバル コンフィギュレーション コマンドを使用できます。

SNMP 連絡先設定の構成

SNMP 連絡先設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices]（または [Manage Device Groups]）を選択します。[Devices] または [Device Groups] ウィンドウが表示されます。

ステップ 2　SNMP 連絡先を設定したいデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウまたは [Modifying Device Groups] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [Contact Information] を選択します。[SNMP Contact Settings] ウィンドウが表示されます。

ステップ 4　提供されるフィールドに、連絡先の氏名と住所を入力します。

ステップ 5　[Submit] をクリックします。

CLI から SNMP 連絡先設定を構成するには、**snmp-server contact** グローバル コンフィギュレーション コマンドを使用できます。

SNMP トラップ ソース設定値の設定

SNMP トラップの送信元になるソース インターフェイスを設定するには、次の手順を実行します。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインで、[My WAN] > [Manage Devices] を選択します [Devices] ウィンドウが表示されます（この設定は、デバイス グループではサポートされていません）。

ステップ 2　SNMP トラップ ソースを設定するデバイスまたはデバイス グループの横にある [Edit] アイコンをクリックします。[Device Dashboard] ウィンドウまたは [Modifying Device Groups] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、[Configure] > [Monitoring] > [SNMP] > [Trap Source] を選択します。[SNMP Trap Source Settings] ウィンドウが表示されます。

ステップ 4　[Trap Source] ドロップダウン リストから、トラップ ソースとして使用されるインターフェイスを選択します。使用可能なギガビット イーサネット、スタンバイ、およびポート チャネル インターフェイスから、IP アドレスを持つものだけがリストに表示されます。

（注）　トラップ ソースとして割り当てられたインターフェイスは、トラップ ソースとしての割り当てを解除するまでは削除できません。

ステップ 5　[Submit] をクリックします。

CLI から SNMP トラップ ソースの設定値を設定するには、**snmp-server trap-source** グローバル コンフィギュレーション コマンドを使用できます。

APPENDIX A

定義済みのアプリケーション ポリシー

Wide Area Application Service（WAAS）ソフトウェアには、WAAS システムがネットワーク上の最も一般的なトラフィックを分類し、最適化できる 150 以上の定義済みのアプリケーション ポリシーが組み込まれています。

表 A-1 に、WAAS がシステムに組み込まれているポリシーに基づいて最適化またはパススルーする定義済みのアプリケーションおよび分類子を示します。

アプリケーション ポリシーを作成する前に、定義済みのポリシーを参照し、必要に応じて変更することを推奨します。一般に、新しいポリシーを作成するより、既存のポリシーを変更する方が簡単です。

表 A-1 を参照するときは、次の情報に注意してください。

- 表内の小見出しはアプリケーション名を表し、これらの小見出しの下に、対応する分類子が掲載されています。たとえば、「認証」はアプリケーションの種類、「Kerberos」はそのアプリケーション用の分類子です。
- アプリケーションの横に「*モニタ対象*」と表記されている場合、アプリケーションは WAAS Central Manager のモニタ対象になります。ただし、一度に 20 のアプリケーションの統計情報しか表示できません。モニタされていないアプリケーションの統計情報を表示するには、次のいずれかの方法を使用します。
  - WAAS CLI を使用します。WAAS デバイス上のすべてのアプリケーション用の統計情報を表示できます。詳細については、『*Cisco Wide Area Application Services Command Reference*』を参照してください。
  - WAAS Central Manager GUI が、希望するアプリケーション用の統計情報を表示するように、アプリケーション設定を変更します。詳細については、第 12 章「アプリケーション アクセラレーションの設定」を参照してください。

WAAS ソフトウェアは、トラフィックの種類に応じて、次の最適化技術を使用します。

- TFO（転送フローの最適化）：ネットワーク経由のすべての TCP トラフィックを最適化する自動的なウィンドウの拡大縮尺、バッファ機能の強化、選択的受信確認などの最適化技術の集合。
- RE（冗長性の除去）：WAN 経由でデータ ストリームを送信する前に冗長な情報を削除して送信データのサイズを減らす圧縮技術。RE は、LZ 圧縮よりはるかに大きなストリームを処理し、より大きな圧縮履歴を維持します。
- LZ（圧縮）：RE と比較してより小さいデータ ストリームを処理し、制限された圧縮履歴を維持するもう 1 つの圧縮技術。
- アプリケーション アクセラレータ：CIFS、EPM、HTTP、MAPI、NFS、SSL、ストリーミング ビデオなどの種類のトラフィックのための、個別アプリケーション アクセラレータの集合。

表 A-1　定義済みトラフィック ポリシー

分類子	WAAS の処理	送信先ポート
認証		
Kerberos	Passthrough	88、2053、754、888、543、464、544、749
SASL	Passthrough	3659
TACACS	Passthrough	49
バックアップ *（モニタ対象）*		
Amanda	TFO	10080
BackupExpress	TFO	6123
CommVault	TFO	8400 ～ 8403
Connected-DataProtector	TFO	16384
IBM-TSM	LZ+TFO+DRE	1500 ～ 1502
Legato-NetWorker	TFO	7937、7938、7939
Legato-RepliStor	TFO	7144、7145
Veritas-BackupExec	TFO	6101、6102、6106、3527、1125
Veritas-NetBackup	TFO	13720、13721、13782、13785
CAD		
PDMWorks	LZ+TFO+DRE	30000、40000
コール管理		
Cisco-CallManager	Passthrough	2443、2748
SIP-secure	Passthrough	5061
VoIP-Control	Passthrough	1300、2428、2000 ～ 2002、1718 ～ 1720、5060、11000 ～ 11999
会議機能		
CU-SeeMe	Passthrough	7640、7642、7648、7649
ezMeeting	Passthrough	10101 ～ 10103、26260 ～ 26261
Intel-Proshare	Passthrough	5713 ～ 5717
MS-NetMeeting	Passthrough	522、1503、1731
VocalTec	Passthrough	1490、6670、25793、22555
コンソール		
SSL-Shell	Passthrough	614
Telnet	Passthrough	23、107、513
Telnets	Passthrough	992
Unix-Remote-Execution	Passthrough	514、512
コンテンツ管理 *（モニタ対象）*		
Documentum	LZ+TFO+DRE	1489
Filenet	LZ+TFO+DRE	32768 ～ 32774
ProjectWise-FileTransfer	LZ+TFO+DRE	5800
ディレクトリサービス *（モニタ対象）*		

表 A-1　定義済みトラフィック ポリシー （続き）

分類子	WAAS の処理	送信先ポート
LDAP	LZ+TFO+DRE	389、8404
LDAP-Global-Catalog	LZ+TFO+DRE	3268
LDAP-Global-Catalog-Secure	Passthrough	3269
LDAP-secure	Passthrough	636
電子メールとメッセージング *（モニタ対象）*		
HP-OpenMail	LZ+TFO+DRE	5755、5757、5766、5767、5768、5729
Internet-Mail	LZ+TFO+DRE	25、110、143、220
Internet-Mail-secure	TFO	995、993、465
Lotus-Notes	LZ+TFO+DRE	1352
MAPI[1]	LZ+TFO+DRE+ MAPI アクセラレータ	UUID:a4f1db00-ca47-1067-b31f-00dd010662da
MDaemon	LZ+TFO+DRE	3000、3001
NNTP	LZ+TFO+DRE	119
NNTP-secure	TFO	563
Novell-Groupwise	LZ+TFO+DRE	1677、1099、9850、7205、3800、7100、7180、7101、7181、2800
PCMail-Server	LZ+TFO+DRE	158
QMTP	LZ+TFO+DRE	209
X400	LZ+TFO+DRE	102
企業アプリケーション *（モニタ対象）*		
SAP	LZ+TFO+DRE	3200 ～ 3219、3221 ～ 3224、3226 ～ 3267、3270 ～ 3282、3284 ～ 3305、3307 ～ 3388、3390 ～ 3399、3600 ～ 3659、3662 ～ 3699
Siebel	LZ+TFO+DRE	8448、2320、2321
ファイルシステム *（モニタ対象）*		
AFS	LZ+TFO+DRE	7000 ～ 7009
Apple-AFP	LZ+TFO+DRE	548
NFS	LZ+TFO+DRE+ NFS アクセラレータ	2049
Novell-NetWare	LZ+TFO+DRE	524
Sun-RPC	Passthrough	111
ファイル転送 *（モニタ対象）*		
BFTP	LZ+TFO+DRE	152
FTP-Control[2]	Passthrough	21
FTP-Data[2]	LZ+TFO+DRE	src20
FTPS[2]	TFO	990
FTP-Control[2]	Passthrough	src989

表 A-1　定義済みトラフィック ポリシー （続き）

分類子	WAAS の処理	送信先ポート
Simple-FTP	LZ+TFO+DRE	115
TFTP	LZ+TFO+DRE	69
TFTPS	TFO	3713
インスタント メッセージング		
AOL	Passthrough	5190 ～ 5193
Apple-iChat	Passthrough	5297、5298
IRC	Passthrough	531、6660 ～ 6669
Jabber	Passthrough	5222、5269
Lotus-Sametime-Connect	Passthrough	1533
MS-Chat	Passthrough	6665、6667
MSN-Messenger	Passthrough	1863、6891 ～ 6900
Yahoo-Messenger	Passthrough	5000、5001、5050、5100
ネーム サービス		
DNS	Passthrough	53
iSNS	Passthrough	3205
Service-Location	Passthrough	427
WINS	Passthrough	42、137、1512
その他 *（モニタ対象）*		
Basic-TCP-services	Passthrough	1 ～ 19
BGP	LZ+TFO+DRE	179
MS-EndPointMapper	EPM アクセラレータ	135
MS-Message-Queuing	LZ+TFO+DRE	1801、2101、2103、2105
NTP	Passthrough	123
Other-Secure	Passthrough	261、448、684、695、994、2252、2478、2479、2482、2484、2679、2762、2998、3077、3078、3183、3191、3220、3410、3424、3471、3496、3509、3529、3539、3660、3661、3747、3864、3885、3896、3897、3995、4031、5007、5989、5990、7674、9802、12109
SOAP	LZ+TFO+DRE	7627
Symantec-AntiVirus	LZ+TFO+DRE	2847、2848、2967、2968、38037、38292
P2P *（モニタ対象）*		
BitTorrent	Passthrough	6881 ～ 6889、6969
eDonkey	Passthrough	4661、4662
Gnutella	Passthrough	6346 ～ 6349、6355、5634
Grouper	Passthrough	8038
HotLine	Passthrough	5500 ～ 5503
Kazaa	Passthrough	1214

表 A-1　定義済みトラフィック ポリシー （続き）

分類子	WAAS の処理	送信先ポート
Laplink-ShareDirect	Passthrough	2705
Napster	Passthrough	8875、7777、6700、6666、6677、6688
Qnext	Passthrough	44、5555
SoulSeek	Passthrough	2234、5534
WASTE	Passthrough	1337
WinMX	Passthrough	6699
印刷 *（モニタ対象）*		
AppSocket	LZ+TFO+DRE	9100
IPP	LZ+TFO+DRE	631
SUN-Xprint	LZ+TFO+DRE	8100
Unix-Printing	LZ+TFO+DRE	515、170
リモートデスクトップ *（モニタ対象）*		
Altiris-CarbonCopy	Passthrough	1680
Apple-NetAssistant	Passthrough	3283
Citrix-ICA	LZ+TFO+DRE	1494、2598
ControlIT	TFO	799
Danware-NetOp	TFO	6502
Laplink-Host	TFO	1547
Laplink-PCSync	TFO	8444
Laplink-PCSync-secure	TFO	8443
MS-Terminal-Services	TFO	3389
Netopia-Timbuktu	TFO	407、1417 ～ 1420
PCAnywhere	TFO	73、5631、5632、65301
RAdmin	TFO	4899
Remote-Anything	TFO	3999、4000
Vmware-VMConsole	TFO	902
VNC	TFO	5801 ～ 5809、6900 ～ 6909
XWindows	TFO	6000 ～ 6063
レプリケーション *（モニタ対象）*		
Double-Take	LZ+TFO+DRE	1100、1105
EMC-Celerra-Replicator	LZ+TFO+DRE	8888
MS-AD-Replication[1]	LZ+TFO+DRE+ EPM アクセラレータ	UUID:e3514235-4b06-11d1-ab04-00c04fc2 dcd2
MS-Content-Replication-Service	TFO	560、507
MS-FRS[1]	LZ+TFO+DRE+ EPM アクセラレータ	UUID:f5cc59b4-4264-101a-8c59-08002b2f 8426
Netapp-SnapMirror	LZ+TFO+DRE	10565 ～ 10569

表 A-1　定義済みトラフィック ポリシー （続き）

分類子	WAAS の処理	送信先ポート
Remote-Replication-Agent	TFO	5678
Rsync	TFO	873
SQL *（モニタ対象）*		
Borland-Interbase	LZ+TFO+DRE	3050
IBM-DB2	LZ+TFO+DRE	523
InterSystems-Cache	LZ+TFO+DRE	1972
MS-SQL	LZ+TFO+DRE	1433
MS-SQL-RPC[1]	LZ+TFO+DRE+ EPM アクセラレータ	UUID:3f99b900-4d87-101b-99b7-aa0004007f07
MySQL	LZ+TFO+DRE	3306
Oracle	LZ+TFO+DRE	66、1525、1521
Pervasive-SQL	LZ+TFO+DRE	1583
PostgreSQL	LZ+TFO+DRE	5432
Scalable-SQL	LZ+TFO+DRE	3352
SQL-Service	LZ+TFO+DRE	156
Sybase-SQL	LZ+TFO+DRE	1498、2638、2439、3968
UniSQL	LZ+TFO+DRE	1978、1979
SSL *（モニタ対象）*		
HTTPS	TFO	443
SSH		
SSH	TFO	22
ストレージ *（モニタ対象）*		
EMC-SRDFA-IP	LZ+TFO+DRE	1748
FCIP	LZ+TFO+DRE	3225
iFCP	LZ+TFO+DRE	3420
iSCSI	LZ+TFO+DRE	3260
ストリーミング *（モニタ対象）*		
Liquid-Audio	LZ+TFO+DRE	18888
MS-NetShow	LZ+TFO+DRE	1755
RTSP	LZ+TFO+DRE+ ビデオ アクセラレータ	554、8554
VDOLive	LZ+TFO+DRE	7000
システム管理 *（モニタ対象）*		
BMC-Patrol	Passthrough	6161、6162、8160、8161、6767、6768、10128
HP-OpenView	Passthrough	7426 ～ 7431、7501、7510
HP-Radia	LZ+TFO+DRE	3460、3461、3464、3466

表 A-1　定義済みトラフィック ポリシー （続き）

分類子	WAAS の処理	送信先ポート
IBM-NetView	Passthrough	729 ～ 731
IBM-Tivoli	LZ+TFO+DRE	94、627、1965、1580、1581
LANDesk	LZ+TFO+DRE	9535、9593 ～ 9595
NetIQ	Passthrough	2220、2735、10113 ～ 10116
Netopia-netOctopus	Passthrough	1917、1921
Novell-ZenWorks	LZ+TFO+DRE	1761 ～ 1763、517、2544、8039、2037
WAAS-FlowMonitor	TFO	7878
WBEM	Passthrough	5987、5988
バージョン管理 *（モニタ対象）*		
Clearcase	LZ+TFO+DRE	371
CVS	LZ+TFO+DRE	2401
VPN		
L2TP	TFO	1701
OpenVPN	TFO	1194
PPTP	TFO	1723
WAFS *（モニタ対象）*		
CIFS	LZ+TFO+DRE+ CIFS アクセラレータまたは WAFS レガシー アクセラレーション	139、445
Web *（モニタ対象）*		
HTTP	LZ+TFO+DRE+ HTTP アクセラレータ	80、8080、8000、8001、3128

1. これらの分類子は、WAAS の EPM サービスを使用してトラフィックを加速します。EPM に基づくアプリケーションには定義済みのポートがないため、アプリケーションの UUID を使用してトラフィックを識別する必要があります。
2. これらの分類子は、送信先ポートの代わりに送信元ポートを識別します。

APPENDIX B

トランザクション ログ形式

トランザクション ログ機能をして、Wide Area Application Service（WAAS）デバイスの個々の TCP トランザクションをログに記録できます。トランザクション ログ機能の設定については、「トランザクション ログ機能の設定」（P.16-58）を参照してください。

TFO トランザクション ログは、ディレクトリ /local1/logs/tfo のローカル ディスクに維持されます。

次のように、異なるテンプレートを持つ複数の種類のトランザクション ログ メッセージが存在します。

- 最適化されたフロー開始メッセージ：

  Time_Stamp、Conn_ID、Src_IP、Src_Port、Dst_IP、Dst_Port、OT、Log_type、Conn_type、Peer_ID、App_map_name、App_name、App_classifier_name、Flag_directed_mode、TFO_cfgd_policy、TFO_drvd_policy、TFO_peer_policy、TFO_neg_policy、TFO_applied_policy、TFO_reject_reason、AO_cfgd_policy、AO_drvd_policy、AO_neg_policy、AO_reject_reason、SSL_reject_reason、DSCP、Link_rtt

- 最適化されたフロー終了メッセージ：

  Time_Stamp、Conn_ID、Src_IP、Src_Port、Dst_IP、Dst_Port、OT、Log_type、Conn_type、AO_neg_policy、Original_bytes_read、Original_bytes_written、Optimized_bytes_read、Optimized_bytes_written

- パススルー フロー メッセージ：

  Time_Stamp、Src_IP、Src_Port、Dst_IP、Dst_Port、BP、Bypass_Reason、TFO_cfgd_policy、TFO_drvd_policy、TFO_peer_policy、TFO_reject_reason、AO_cfgd_policy、AO_drvd_policy、AO_reject_reason

- 最適化されたフロー TFO 終了メッセージ：

  Time_Stamp、Conn_ID、Src_IP、Src_Port、Dst_IP、Dst_Port、SODRE、END、Original_bytes_read、Original_bytes_written、Optimized_bytes_read、Optimized_bytes_written、Conn_close_state

- システム リスタート メッセージ：

  Time_Stamp :0 :0 :0 :0 :0 :RESTART

表 B-1 で、トランザクション ログ メッセージにあるフィールドについて説明します。

表 B-1　　トランザクション ログ フィールドの説明

フィールド	説明
Time_Stamp	ログ メッセージがいつ生成されたのかを示すタイム スタンプ。
Conn_ID	接続の一意な ID。
Src_IP、Src_Port	接続元 IP アドレスとポート番号。

表 B-1　トランザクション ログ フィールドの説明 （続き）

フィールド	説明
Dst_IP、Dst_Port	接続先 IP アドレスとポート番号。
OT	最適化された接続を示します。
BP	パススルー接続を示します。
SODRE	TFO によって生成されたログ メッセージを示します。
Log_type	START または END はフローの開始または終了を示します。
Conn_type	接続の種類： INTERNAL CLIENT：WAE からローカルで開始された接続 EXTERNAL CLIENT：WAE がブランチ デバイスとして動作する接続 INTERNAL SERVER：WAE でローカルで終了した接続 EXTERNAL SERVER：WAE がデータ センター デバイスとして動作する接続
Peer_ID	ピア WAE のデバイス ID。
App_map_name	マップの名前。
App_classifier_name	分類子の名前。
App_name	アプリケーションの名前。
Flag_directed_mode	T（true）は Directed モード接続を示し、F（false）はそれ以外の接続を示します。
TFO_cfgd_policy	ローカル デバイス上の TFO により設定されたポリシー。
TFO_drvd_policy	設定された条件とダイナミック条件に基づく、ローカル デバイス上の TFO により派生されたポリシー。このポリシーは、ピア WAE とネゴシエートするために使用されます。
TFO_peer_policy	ローカル デバイスに送信された、ピア上の TFO により派生されたポリシー。
TFO_neg_policy	TFO によりネゴシエートされたポリシー。このポリシーは、派生されたポリシーとピア ポリシー間で最も一般的でないポリシーです。
TFO_applied_policy	接続に適用される最後のポリシー。接続の確立後に、接続のデータに基づいて接続に対してポリシーの変更が行われ、その結果、適用されたポリシーがネゴシエートされたポリシーと異なる場合があります。
TFO_reject_reason	拒否された接続の理由を示します。「None」は拒否理由が設定されていないことを示します。
AO_cfgd_policy	ローカル デバイスで設定されたアプリケーション アクセラレータ。これは、対応するポリシーで設定されたアクセラレータから派生されます。
AO_drvd_policy	ローカル デバイス上の、アプリケーション アクセラレータにより派生されたポリシー。
AO_neg_policy	アプリケーション アクセラレータによりネゴシエートされたポリシー。このポリシーは、派生されたポリシーとピア ポリシー間で最も一般的でないポリシーです。
AO_reject_reason	接続がアプリケーション アクセラレータにより拒否された理由を示します。「None」は拒否理由が設定されていないことを示します。
SSL_reject_reason	接続が SSL アクセラレータにより拒否された理由を示します。「None」は拒否理由が設定されていないことを示します。
DSCP	送信接続で設定された DiffServ コード ポイント値。
Link_rtt	リンクのラウンドトリップ時間（ミリ秒単位）。

表 B-1　トランザクション ログ フィールドの説明 （続き）

フィールド	説明
Original_bytes_read	元の側の接続で読み取られたバイト数。
Original_bytes_written	元の側の接続で書き込まれたバイト数。
Optimized_bytes_read	最適化された側の接続で読み取られたバイト数。
Optimized_bytes_written	最適化された側の接続で書き込まれたバイト数。
RESTART	WAE が再ロードされ、トランザクション ログ プロセスが開始されたことを示します。

トランザクション ログ メッセージの一部の例を次に示します。

両側で完全に最適化（SSL 拒否あり）

```
Fri Jan 30 03:15:41 2009 :43 :2.57.223.130 :4808 :2.57.223.2 :443 :OT :START :EXTERNAL CLIENT
:00.14.5e.95.4c.85 :basic :SSL :HTTPS :F :(TFO) (TFO) (TFO) (TFO) (TFO) :<None> :(None) (None) (None) :<None>
:<Keepalive Timeout>  :0 :0
Fri Jan 30 03:15:41 2009 :43 :2.57.223.130 :4808 :2.57.223.2 :443 :SODRE :END :0 :0 :0 :0 :0
Fri Jan 30 03:15:41 2009 :43 :2.57.223.130 :4808 :2.57.223.2 :443 :OT :END :EXTERNAL CLIENT :(None) :284 :806
:806 :28
```

両側で完全に最適化

```
Mon Feb  2 14:31:21 2009 :16 :2.75.52.131 :4374 :2.75.52.3 :80 :OT :START :EXTERNAL CLIENT :00.14.5e.83.8c.cf
:basic :Web :HTTP :F :(DRE,LZ,TFO) (DRE,LZ,TFO) (DRE,LZ,TFO) (DRE,LZ,TFO) (DRE,LZ,TFO) :<None> :(HTTP) (HTTP)
(HTTP) :<None> :<None>  :0 :0
Mon Feb  2 14:31:26 2009 :16 :2.75.52.131 :4374 :2.75.52.3 :80 :SODRE :END :370 :173 :299 :429 :0
Mon Feb  2 14:31:26 2009 :16 :2.75.52.131 :4374 :2.75.52.3 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :299
:429
```

DRE だけが有効な状態で最適化

```
Mon Feb  2 14:48:31 2009 :27 :2.75.52.131 :4389 :2.75.52.2 :80 :OT :START :EXTERNAL CLIENT :00.14.5e.83.8c.cf
:basic :Web :HTTP :F :(DRE,TFO) (DRE,TFO) (DRE,LZ,TFO) (DRE,TFO) (DRE,TFO) :<None> :(HTTP) (HTTP) (HTTP)
:<None> :<None>  :0 :0
Mon Feb  2 14:48:36 2009 :27 :2.75.52.131 :4389 :2.75.52.2 :80 :SODRE :END :246 :468 :636 :405 :0
Mon Feb  2 14:48:36 2009 :27 :2.75.52.131 :4389 :2.75.52.2 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :636
:405
```

LZ だけが有効な状態で最適化

```
Mon Feb  2 14:39:12 2009 :20 :2.75.52.131 :4379 :2.75.52.3 :80 :OT :START :EXTERNAL CLIENT :00.14.5e.83.8c.cf
:basic :Web :HTTP :F :(LZ,TFO) (LZ,TFO) (DRE,LZ,TFO) (LZ,TFO) (LZ,TFO) :<None> :(HTTP) (HTTP) (HTTP) :<None>
:<None>  :0 :0
Mon Feb  2 14:39:17 2009 :20 :2.75.52.131 :4379 :2.75.52.3 :80 :SODRE :END :370 :173 :219 :295 :0
Mon Feb  2 14:39:17 2009 :20 :2.75.52.131 :4379 :2.75.52.3 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :219
:295
```

DRE と LZ の両方が無効な状態で最適化

```
Mon Feb  2 14:49:36 2009 :28 :2.75.52.131 :4390 :2.75.52.2 :80 :OT :START :EXTERNAL CLIENT :00.14.5e.83.8c.cf
:basic :Web :HTTP :F :(TFO) (TFO) (DRE,LZ,TFO) (TFO) (TFO) :<None> :(HTTP) (HTTP) (HTTP) :<None> :<None>  :0
:0
Mon Feb  2 14:49:41 2009 :28 :2.75.52.131 :4390 :2.75.52.2 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :468
:246
```

パススルー接続

```
Thu Jul 24 03:09:34 2008 :2.75.52.130 :40027 :2.75.52.2 :80 :BP :GLB_CFG :(DRE,LZ,TFO) (None) (None) :<Global
Config> :(HTTP) (None) :<Global Config>
```

System Restart

```
Sun Oct 25 17:46:32 2009 :0 :0 : 0 :0 :0 :RESTART
```

INDEX

数字

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W

あ

い

う

え

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ふ

へ

ほ

む

め

も

ゆ

わ