CHAPTER 2

WAAS ネットワークの計画

広域アプリケーション サービス（WAAS）ネットワークをセットアップする前に、既存のネットワークから移行する場合に検討する必要がある一般的なガイドラインと制限事項があります。

（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」は、WAE アプライアンスおよび WAE ネットワーク モジュール（NME-WAE デバイス ファミリ）を示します。

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 ポイントに配備され、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、定義された処理地点でネットワークの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ています。

- **ハブ & スポークの構成 —** ハブ & スポーク構成では、ほとんどの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。WAAS 製品の詳細については、第 1 章「Cisco WAAS の概要」を参照してください。

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 RAM のサイズ）。拡張性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.2-19）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「WAAS ネットワーク システム パラメータのチェックリスト」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.2-29）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 アカウントの作成と管理」を参照してください。
   - WAE を論理グループにまとめる意味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.2-30）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.6-8）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.2-5）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、WAFS （広域ファイル サービス）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。
   - 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、WCCP バージョン 2 またはポリシーベース ルーティング（PBR）、WAFS 専用トラフィックには DFS または 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.2-20）を参照してください。

     （注） WCCP は、IPv4 ネットワークでのみ動作します。

   - 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 アクセス コントロール リスト（ACL）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 IP 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.2-27）を参照してください。

   - WAE で IP 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.2-27）を参照してください。

（注）　WAE で定義される IP 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。詳細については、「WAE 上の IP ACL とアプリケーション定義ポリシーの優先順位について」（p.8-3）を参照してください。

- 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.4-42）を参照してください。
- WAFS サービスを展開する計画の場合は、WAFS 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ために、透過的な代行受信方式または非透過的な代行受信方式（DFS または NetBIOS）のどちらを使用するかを決定します。詳細については、「CIFS クライアント要求の要求リダイレクション」（p.4-53）を参照してください。
- WAAS ネットワークで最適化する対象となる主要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を網羅しているかどうかを確認します。アプリケーションがこれらの定義済みのポリシーで網羅されていない場合は、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「デフォルト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 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.2-32）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、および希望する機能（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。

上記の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、展開する前に、ネットワークに WAAS デバイスを統合するために、ネットワークに関する情報を収集する必要があります。さらに、いくつかの細かい調整が必要になる場合があります。

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。

- 1 台または複数の Core WAE が、常駐ファイル サーバへのアクセスを提供するデータセンター（セントラル オフィス）。データセンターでは、単体の WAE を配置したり、高可用性や負荷分散のために 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、高可用性は、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、負荷分散は、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 を使用する場合のみサポートされます。
- ユーザが Edge WAE を使用して WAN 経由でファイル サーバーにアクセスできるブランチ オフィス。ブランチ オフィスでは、単体のエッジ デバイスとして WAE を配置したり、高可用性や負荷分散用に 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、高可用性は、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、負荷分散は、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 を使用する場合のみサポートされます。

協業ネットワークでは、（2 台の交差接続されたサーバで）反対方向にデータを共有するように構成されたネットワーク全体に、Core WAE と Edge WAE を配置します。

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、パケットが流れる両方の方向で行われます。レイヤ 3 ヘッダとレイヤ 4 ヘッダが維持されるので、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.2-26）を参照してください。

（注）　Core WAE と Edge WAE が相互に通信するには、ファイアウォールを開放する必要があります。WAFS を展開する予定の場合のみ、ポート 4050 を使用するようにファイアウォールを設定する必要があります。ただし、汎用 TCP 最適化を展開する予定の場合は、ポート 4050 を使用するようにファイアウォールを設定する必要はありません。

ここで説明する内容は、次のとおりです。

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 Core WAE 側と Edge WAE 側で準備を行う必要がある場合があります。

- Core WAE の統合（p.2-6）
- Edge WAE の統合（p.2-6）

（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。Edge WAE および Core WAE ネットワークで、別の Windows マシンがこ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。

Core WAE の統合

Core 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 Core WAE 側で Cisco WAAS を Windows 環境に正しく統合するには、Core 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。

Edge WAE の統合

Edge 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）
- DFS サイト名（該当する場合）

ネットワークの Edge 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 Edge 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、Edge 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。
- WAFS の非透過的な統合を使用する Active Directory （AD）環境では、Cisco WAFS のキャッシュに保存されるファイル サーバ名を手動で AD コンピュータ カタログに追加します。これらの名前（存在する場合、デフォルトのプレフィクスや拡張子やを含む）を追加すると、あとで

DFS のような AD サービスと統合できます。DFS を使用する場合は、現在の Edge WAE の位置を示す AD サイト名に注意し、Edge WAE 設定の CIFS セクションで更新します。この注意点は、WAFS の透過的な統合を使用する場合には適用されません。

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）
- Core 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 Core WAE 側と Edge WAE 側で次の作業を実行する必要があります。

- Core WAE と Edge 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。すなわち、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 Core WAE（プライマリ）と Edge 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 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。ほとんどの WAFS 通信は、ブランチ オフィスとセントラル オフィス間の組織内で行われます。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、TCP/IP ポート 4050 経由で行われます。

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 Edge WAE に接続し、Core 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、インライン モードが使用される場合、Edge WAE はポート 139 または 445 でクライアント接続を受信します。WCCP もインライン モードも有効でない場合は、Edge WAE は、ポート 139 でのみ接続を受信します。

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 Edge WAE に接続する場合、関連する Core 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、Core WAE は、ポート 139 の使用を試みます。

一部の組織は、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 を閉じます。組織がポート 139 をセキュリティの理由から閉じた場合、WAAS ネットワークがポート 139 を迂回するように設定できます。組織がこのような場合、WAAS ネットワークで WAFS サービスのみを展開する場合、ポート 139 を迂回し、代わりにポート 445 を使用するには、次の作業を実行する必要があります。

- 『*Cisco Wide Area Application Services Quick Configuration Guide*』の説明に従って、ルータと Edge 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 Edge WAE でインライン モードを使用することもできます。
- Edge WAE で WAAS Central Manager GUI または Device Manager GUI を使用して、ポート 445 を有効にし、ポート 139 を無効にします。集中管理された Edge WAE でこの作業を実行するには、WAAS Central Manager GUI を使用します（WAAS Central Manager GUI で Edge WAE の横にある **[Edit]** アイコンをクリックし、[Contents] ペインから **[File Servers] > [Edge Configuration]** を選択します）。WAAS Central Manager デバイスに登録されていない Edge WAE のためにこの作業を実行するには、WAE Device Manager GUI を使用します（WAE Device Manager GUI から **[WAFS Edge] > [Configuration]** を選択し、**[CIFS]** タブをクリックします）。

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 印刷サービスをセットアップした場合、プリント サーバはポート 50139 で動作します。WAAS 印刷サービスを構成する詳細については、第 13 章「WAAS 印刷サービスの設定および管理」を参照してください。

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。WAE が登録されたら、デバイスを承認し、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 で意図的に無効になっており、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。WAE の初期設定が完了したら、WAAS CLI を使用して、明示的に WAE を特定の WAAS Central Manager に登録するように構成します。

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** インターフェイス設定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** インターフェイス設定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送信する必要があります。RFC 2132 に対応する項 8.4 をここで引用します。

> 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エンコードする必要があります。ただし、次のような違いがあります。
>
> 1. 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。
> 2. 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。
> 3. 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みなされるために、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。FE-511、WAE-511、WAE-512、WAE-611、WAE-612、および WAE-7326 モデルの場合、最初のインターフェイスは、GigabitEthernet 1/0 です。NME-WAE デバイスでは、設定されたインターフェイスで自動登録が有効です。

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（「固定 IP アドレスの選択またはインターフェイス レベルの DHCP の使用」[p.2-10] を参照してください）。

次の例は、ギガビット イーサネット 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
```

固定 IP アドレスの選択またはインターフェイス レベルの 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
- Hostname
- 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

相互運用性に関する問題の特定と解決については、次の各項を参照してください。

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 シスコ製ルータにインストールされている FE-511 ファイル エンジン、WAE-511、WAE-512、WAE-611、WAE-612、および WAE-7326、または NME-WAE 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	Edge 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/2003
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。

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とファイル ブロック 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。

- 一貫性ポリシーと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
- ファイル ブロック ポリシーの **[Content]** タブ

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。

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。

- 名前に Unicode 文字を含むファイルには、複製ユーティリティを使用できません。
- ユーザ名には Unicode 文字を入れることができません。
- 一貫性やファイル複製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。

（注）　WAAS ソフトウェアは、Cisco IOSIP 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 リリース 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。ポリシー フィルタの次の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.2-13）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分類と異なり、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 ヘッダのみ）、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 インターフェースで、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つづけます。圧縮されたパケットは分類されないため、この状況により（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.2-26] 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周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.2-13）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（RSVP）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、監視、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 ソフトウェアの管理装置では、次の事項に注意してください。

- NetFlow はサポートされています。ただし、統計情報を収集する位置によっては、圧縮されていない値（最適化されていないトラフィックに関する統計情報）でなく、圧縮された値（最適化されたトラフィックに関する統計情報）が表示される場合があります。
- 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 サービス レベル契約（SLA）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。
- 侵入検知システム（IDS）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。
- アクセス コントロール リスト（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 IP 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.2-27）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。

- ネットワーク　アドレス変換（NAT）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、あまり使用されず、サポートされていません。

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、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、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。

WAAS と ACNS の連結

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、さらに WAAS を配備できます。
- ACNS がネットワークに展開されていないが、ビデオのような特定の 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 を通じて、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 Core WAE、Edge WAE、およびファイル エンジン（FE）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** グローバル設定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** 設定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 デバイス ファミリ）は、WAAS Central Manager モードで動作するように設定できません。

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、Edge WAE、または Core 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、高可用性、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）。ブランチ オフィスとデータセンター間のフローを最適化するために、ブランチ オフィスの WAE は Edge WAE として機能し、データセンターの WAE は Core WAE として機能します。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。
- **Edge WAE の台数 —** 各リモートのオフィスに、少なくとも 1 台の Edge 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 Edge WAE を配置すると、システム管理が簡単になります。状況によっては、DFS または WCCP バージョン 2 を使用して複数の Edge WAE をクラスタ構成にすると、フェールオーバー機能を提供できます。ユーザ数が多い場合は、WCCP バージョン 2 を推奨します。
- **Core WAE の台数 —** 組織に必要な冗長性のレベルに依存します。各組織に少なくとも 1 台の Core 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です。

（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。

- **Core 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 Core 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 Core WAE をネットワークに追加する必要があります。

  システム容量を超えてデータが消失することを防止するために、WAAS は 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、主に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

配備するハードウェア プラットフォームの決定

特定の Cisco ルータに接続している FE-511 ファイル エンジン、および WAE-511、WAE-512、WAE-611、WAE-612、および WAE-7326、または NME-WAE ネットワーク モジュールで稼働する WAAS ソフトウェア。専用のデバイスに WAAS Central Manager を展開する必要があります。

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 へリダイレクションできます。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 へリダイレクションされます。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 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。

次の各項で、トラフィック代行受信についてさらに説明します。

- インライン代行受信を使用する長所と短所（p.2-20）
- WCCP に基づくルーティングを使用する長所と短所（p.2-21）
- PBR を使用する長所と短所（p.2-22）
- WAAS トラフィック用の WCCP または PBR ルーティングの設定（p.2-22）

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 2 つのペアを含んでおり、ネットワーク トポロジが必要であれば、2 つのルータに接続できます。

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のみを受信し、ほかのすべての VLAN に対してトラフィックはブリッジングされ処理されないように、Cisco WAE Inline Network Adapter を設定できます。

Cisco WAE Inline Network Adapter が搭載された複数の WAE デバイスを連続的にクラスタ化して、スピルオーバー負荷分散や active-active フェールオーバーを提供できます。スピルオーバー負荷分散では、接続しきい値が 1 つの WAE に達したとき、別の WAE によって追加の接続が最適化されます。

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 Core WARE 上の Edge 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 アクセラレーションを実行した WCCP 代行受信または Cisco Application Control Engine（ACE）での負荷分散の使用を推奨します。

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.4-46）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トを確立し、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 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手段を提供します。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 Core WAE およびブランチ オフィスのルータと Edge 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 を起動し稼働させるために、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 を稼働させるために、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負荷分散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 の状態を監視します。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、Edge 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 Edge 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 Edge WAE と Core 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（負荷分散など）を構成することができます。詳細については、「WAE 用の

WCCP 設定の集中管理」（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.4-8）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（すなわち、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、どのようにネットワーク 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。

- 一般に、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 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 ソフトウェアが稼働する任意の 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 リリース 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、コストが等しいルート間の負荷分散をサポートしていません。そのため、PBR は、展開場所の拡張性を提供しません。
- PBR は、WCCP バージョン 2 より設定が難しいです。WAAS トラフィックに対する PBR の設定方法についての例は、「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.4-36）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ションされます。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ションします。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.2-26）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

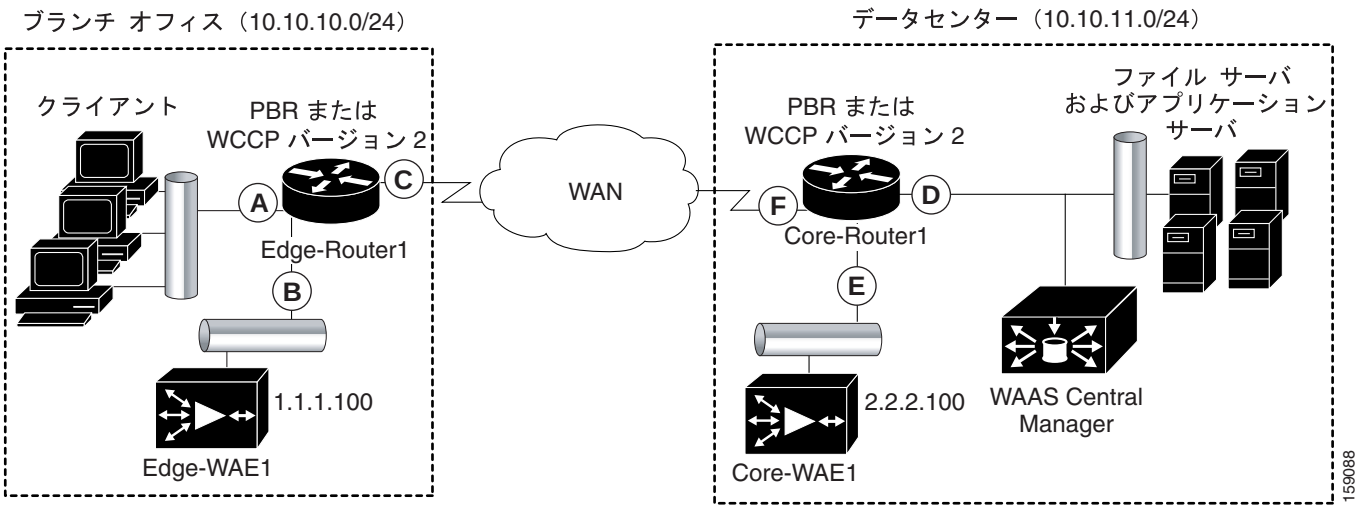

表 2-2 に、PBR または WCCP バージョン 2 を使用して、透過的にトラフィックを WAE へリダイレクトするために設定する必要があるルータ インターフェイスのまとめを示します。

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	
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-Router 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）

この透過的なトラフィックリダイレクション方式は、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.2-13）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 （Edge WAE）へリダイレクトすることができます。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（Core WAE）へリダイレクトすることができます。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.2-26）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; シスコ エクスプレス転送）、distributed Cisco Express Forwarding （dCEF; 分散 CEF）、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 は不要ですが、パフォーマンスを改善するために推奨します。WCCP は、CEF がルータで有効になっている場合、IP CEF を利用するように最適化されます。

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。

ここで説明する内容は、次のとおりです。

- 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.2-26）
- 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.2-26）

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

WAE が、指定した WCCP バージョン 2 ルータによって透過的にリダイレクトされる TCP トラフィック用の無差別 TCP デバイスとして機能するようにするには、WAE は WCCP バージョン 2 シリーズ 61 と 62 を使用します。WCCP シリーズ 61 と 62 は、WAE 上の正式名 tcp-promiscuous によって表され、Edge WAE の WAAS CLI の次のサンプル出力のように表示されます。

```
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
```

図 4-5 に示すように、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。

WAAS Central Manager GUI を使用して個々の WAE で CP 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 設定の集中管理」（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迂回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。

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.2-13）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。

ここで説明する内容は、次のとおりです。

- WAE 上の IP ACL（p.2-27）
- WAE 上の固定迂回リスト（p.2-28）

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 デバイスへのアクセスと WAAS デバイス経由のアクセスを制限する標準および拡張 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。IP ACL を使用すると、コーポレート ネットワークに損害を与えるハッカー、ワーム、およびウイルスの潜入を減らすことができます。たとえば、WAAS デバイスに着信 WCCP カプセル化トラフィック用の IP ACL を設定できます。

WAFS ソフトウェアは、さまざまなサービスを特定のインターフェイスに結合できる制御機能も提供しています。たとえば、IP ACL を使用して、WAE にファイル サービス用のパブリック インターフェイスを定義したり、SNMP のような管理サービス用のプライベート インターフェイスを定義したりできます。詳細については、第 8 章「WAAS デバイス用の IP アクセス コントロール リストの作成および管理」を参照してください。

（注）　WAE で定義される IP ACL は、WAE で定義されている WAAS アプリケーション定義より常に優先します。

WAE 上の固定迂回リスト

WAE では、IP ACL の定義に加えて、固定迂回リストも設定できます。固定迂回を使用すると、設定可能なクライアントとファイル サーバの集合間のトラフィックのフローが、WAE による処理を迂回できます。Edge WAE に固定迂回項目を設定すると、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 Edge WAE へリダイレクトすることなく、トラフィックを迂回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ファイル サーバ（または特定のクライアントからすべてのファイル サーバ）への接続を WAAS がキャッシングしないようにしたい場合、固定迂回を使用することができます。WAE または WAE のグループ用に固定迂回リストを集中的に設定する方法については、「WAE 用の固定迂回リストの設定」（p.4-34）を参照してください。

（注）　アクセス リストの方が効率的であるため、WAE 上の固定迂回リストを使用するより、WCCP 対応ルータ上のアクセス リストを使用することを推奨します。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。

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、監視、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、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用の次の認証、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。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.6-35）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 デバイス上の 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 を通じて 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 を通じて、Core WAE または Edge 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 サービスと要素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.7-8）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 Edge WAE と Core 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
  - WAFS コア クラスタ

  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
  - 加速
  - 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、グループに入れたい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詳細については、次を参照してください。第 3 章「デバイス グループとデバイス位置の使用」

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一部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。また、この手順は、WAFS 複製機能を使用して、WAE を設置した後で実行することもできます。次に、ブランチ オフィス ファイル サーバ共有をデータセンターに複製します。

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。それには、ブランチ オフィスの WAE が Edge WAE と Core WAE として機能し、その間の接続を確立する必要があります。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、次のように通常の作業シナリオを復元またはセットアップします。

- ブランチ オフィスのコア FE を撤去します。
- ブランチ オフィスのエッジとコアの接続を除去します。
- Edge FE プロセスを起動します。
- ブランチ オフィスのエッジとデータ - センタの Core FE の接続を設定します。
- 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。

- 事前配置と複製は、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。
- リソース認証情報（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 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、Edge WAE のキャッシュ サイズを超えてはなりません。