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 および WAVE アプライアンス、WAAS を実行する SM-SRE モジュール、および vWAAS インスタンスを示します。

この章の内容は、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。
- 従来の WAAS 導入モデルを使用するか、AppNav 導入モデルを使用するかを決定します。AppNav の詳細については、第 4 章「AppNav の設定」を参照してください。
- 各場所に必要な WAAS デバイスの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、さまざまなハード ディスク モデルや RAM 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 7 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 デバイスの追加管理アカウントを作成する必要があるかどうかを判断します。詳細については、第 8 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 を論理グループにグループ化する必要があるかどうかを判断します。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。デフォルトでは、Telnet が使用されますが、展開によっては SSH が推奨される場合もあります。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.7-7）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、「サイトおよび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）。
- 展開する WAAS サービスを決定します。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.10-3）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（AppNav、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）など）。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 WCCP 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 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.2-25）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.2-25）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.5-42）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「定義済み最適化ポリシー」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。

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。

サイトおよび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 サーバおよびアプリケーション 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 経由でファイルおよびアプリケーション 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。これらの同じ場所に配置した WAE は、反対方向でデータを共有するように設定されます（相互にリンクされた 2 台のサーバ）。

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.2-24）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。

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。

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、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。

- 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 CIFS 関連ポート

ここでは、クライアント、CIFS トラフィックを加速化している WAE、および CIFS ファイル サーバ間で使用されている CIFS 関連ポートについて説明します。CIFS 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 139 およびポート 445

WAAS ネットワークに CIFS アクセラレーション サービスを展開した場合、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 CIFS サービス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 または Cisco インターフェイス モジュール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。

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.6-31）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。

広帯域幅 WAN のブランチ オフィスのパフォーマンスの調整

WAAS は CIFS を含めたさまざまなプロトコル用に、レイヤ 4 TCP 最適化とレイヤ 7 アプリケーション アクセラレータを組み合わせます。広帯域幅 WAN（たとえば、50 Mbps を超える）のブランチ オフィスの場合、ネイティブ遅延が少ない（たとえば、20 ms RTT 未満）と、ユーザ セッション数とデータ パターンに応じて、レイヤ 4 の最適化だけが最適なレベルのパフォーマンスを実現できることがあります。このような場合は、実稼働環境の負荷でエンドユーザの応答時間を測定し、アプリケーション アクセラレータの適切な動作状態およびサイジングを決定することを推奨します。

自動登録と WAE について

自動登録は自動的にプライマリ ネットワークを設定し、WAAS Central Manager デバイスに WAE を登録します。起動時に、プライマリ インターフェイスに既存のネットワーク設定がない WAAS デバイス（WAAS Central Manager 自体を除く）は、自動的に WAAS Central Manager デバイスを検出し、登録できます。WAAS デバイスのプライマリ インターフェイスのネットワーク設定を手動で設定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 を使用してデバイスの他のインターフェイスと設定の構成をリモートで実行します。

『*Cisco Wide Area Application Services Quick Configuration Guide*』に示す構成例では、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てインターフェイス設定を手動で構成するときには、自動登録機能は WAE で無効になっています。

自動登録は、Dynamic Host Configuration Protocol（DHCP）の形式を使用します。自動登録が機能するためには、基本設定で構成された DHCP サーバが必要です。

（注） WAE は、DHCP DISCOVER メッセージのオプション 60 のベンダー クラス ID として「CISCOCDN」を送信し、WAE のデバイス グループへの分割を容易にします。

自動登録 DHCP では、次のオプションが DHCP サーバの要求に存在している必要があります。

- サブネット マスク（オプション 1）
- ルータ（デフォルト ゲートウェイ）（オプション 3）
- ドメイン名（オプション 15）
- ドメイン ネーム サーバ（オプション 6）

また、DHCP の要求に WAE ホスト名（オプション 12）が含まれている場合がありますが、必須ではありません。ホスト名のオプションが指定されていない場合、WAE ホスト名は NO-HOSTNAME-*a-b-c-d* に自動的に設定されます。ここで、*a.b.c.d* は、DHCP サーバによって WAE に割り当てられている IP アドレスです。

ドメイン ネーム 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 ネーム サーバ オプションは、すべての既存のネーム 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。

WAE が DHCP からネットワーク設定を行った後は、Central Manager に登録できるように Central Manager ホスト名を知っている必要があります。Central Manager のホスト名を取得するために、WAE は設定された DNS サーバに問い合わせます。自動登録が機能するために、DNS SRV（サービス ロケーション）レコードを設定して、DNS サーバを Central Manager のホスト名で設定する必要があります。このレコードは設定が容易で、通常の DNS 動作に影響しません。DNS SRV レコードは次のように設定する必要があります。

- サービスを _waascms に指定
- プロトコルを _tcp に指定
- このサービスを提供するホストは、Central Manager の完全修飾ドメイン名（FQDN）に指定

Windows Server 2008 に SRV レコードを作成するには、DNS マネージャを開き、[Forward Lookup Zones] に移動して正しい DNS ゾーンを選択します。ゾーンを右クリックし、[Other New Records] を選択して、[Service Location (SRV)] を選択します。

DNS 要求が失敗するか、ドメインが設定されていない場合、WAE は ciscowaas.local ドメインに SRV レコードの代替 DNS クエリーを試行します。この代替要求も失敗すると、WAE は Central Manager に登録できません。ただし、ネットワーク設定は維持され、CLI から追加設定を行うために Telnet で接続することができます。

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。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、自動登録がデフォルトで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。自動登録を無効にするときに、インターフェイスの動的に設定された IP アドレスを固定 IP アドレスとして維持する場合は、このコマンドで **preserve-ip** オプションを使用します。このオプションは、IP アドレスが削除されたために WAE がネットワーク接続を失うことを防ぎます。

（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 が自動登録で使用するインターフェイス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インターフェイス レベルの DHCP の使用」（P.2-9）を参照）。

次に、インターフェイス GigabitEthernet 1/0 で自動登録を無効にする例を示します。

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

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 auto-register
```

スタティック 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。組織でコンピュータ ユーザにネットワークへの接続を設定するには、IP アドレスを各デバイスに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 DHCP 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。設定する項目は次のとおりです。

- インターフェイスの IP アドレスとサブネット マスク
- 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

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。次の項目について説明します。

相互運用性とサポート

ここでは、次の内容について説明します。

WAAS ソフトウェアでサポートされるハードウェア、CIFS クライアントおよび Web ブラウザのリストについては、『*Release Note for Cisco Wide Area Application Services*』を参照してください。

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。

（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。最終的にパケットが正しく色づけされます。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、Frame Relay QoS、および Layer 2（VLAN）QoS をサポートしません。

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.2-11）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 設定ではこれらのパケットが C1 に属しているとマーキングされています。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限り、NBAR はパケット内で分類の検索を続行します。圧縮されたパケットは分類されないため、パケット インスペクションを実行する 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.2-24）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 インスペクションを停止します。ただし、他のフロー（たとえば、Citrix）の場合、フロー内で分類が動的に変更される可能性があるため、NBAR は継続的にパケットを検索します。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） この動的な分類サポートでは、「WAAS による Cisco IOS QoS 分類機能のサポート」（P.2-11）で指定されている DSCP/ToS 設定のマーキングのサポート、ポーリングを使用した動的な変更の追跡が必要です。

NBAR-WAAS 準拠を確実にするために、いくつかのルータ設定に従う必要があり、次のルータ設定に従っていることを確認する必要があります。

- 分類が適切な DSCP マーキングに基づいていることを確認します。
- 一般的なルータ（ルータで設定される IP アクセス リスト）がエントリのパケットですでにマーキングされている DSCP/TOS 設定をスクラビングせず、NBAR はマーキングされたパケットをマーキング解除しません。

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 ソフトウェアと MPLS RSVP メッセージとの間に相互作用がないため、RSVP 機能がサポートされます。

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検出するため、この機能は NBAR サポートと緊密に関連しています。ただし、Cisco IOS AutoQoS 機能は厳密には発信機能であり（たとえば、インターフェイスの着信側では有効にできません）、発信インターフェイスで NBAR を有効にすることはサポートされないため、この状況によって潜在的な問題が発生する可能性があります。

この潜在的な問題を回避するには、次のインターフェイスで AutoQoS 機能の trust オプションを有効にして、マーキングされた値に基づいて分類やキューイングが実行されるようにします（この解決策を使用して、NBAR が発信インターフェイスで有効にならないようにします）。

- 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 は隣接デバイスで設定し、NetFlow が WAAS デバイスに関連して設定される場所に従って、フローレコード情報をエクスポートすることができます。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 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。
- 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.2-25）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.6-31）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 mode：WAAS Central Manager が使用するモード。
- WAAS アプリケーション アクセラレータ モード：トラフィックの最適化および高速化のために WAAS アクセラレータ（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）が使用するモード。
- WAAS AppNav コントローラ モード：アプリケーション アクセラレータ モードで動作している他の WAAS デバイスへのトラフィックを代行受信および分散する AppNav コントローラ（ANC）として動作している WAAS デバイスのモード。

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。

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)# 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]yes
Shutting down all services, will timeout in 15 minutes.
reload in progress ..
```

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 モジュールは、NME-WAE または SM-SRE ファミリのデバイスでは、WAAS Central Manager モードで稼働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。

デバイス モードの変更

すでに Central Manager に登録されているデバイスのデバイス モードを変更する場合は、最初にデバイスを Central Manager から登録解除してデバイスモードを変更し、デバイスをリロードし、CMS サービスを再度有効にする必要があります。

次に、デバイス モードを application-accelerator から appnav-controller に変更する手順を説明します。

ステップ 1　Central Manager からデバイスを登録解除します。

```
wae# cms deregister
Deregistering WAE device from Central Manager will result in loss of data on encrypted
file systems, imported certificate/private keys for SSL service and cifs/wafs preposition
credentials. If secure store is initialized and open, clear secure store and wait for one
datafeed poll rate to retain cifs/wafs preposition credentails.
Do you really want to continue (yes|no) [no]?yes
Disabling management service.
management services stopped
Sending de-registration request to CM
SSMGR RETURNING: 7 (Success)
Removing cms database tables.
Re-initializing SSL managed store and restarting SSL accelerator.Deregistration complete.
Save current cli configuration using 'copy running-config startup-config' command because
CMS service has been disabled.
```

ステップ 2　デバイス モードを appnav-controller に変更します。

```
wae# configure
wae(config)# device mode appnav-controller
The new configuration will take effect after reload.
```

ステップ 3　設定を保存してリロードします。

```
wae(config)# exit
wae# copy run start
wae# reload
Proceed with reload?[confirm]yes
Proceed with clean WCCP shutdown?[confirm]yes

WCCP clean shutdown initiated
Waiting for shutdown ok (1 seconds) . Press ^C to skip waiting
WCCP clean shutdown wait time expired
Shutting down all services, will timeout in 15 minutes.
```

```
reload in progress ..
```

ステップ 4　リブート終了後に WAE にログインします。

```
AppNav Controller


wae login: admin
Password:
System Initialization Finished.
wae#
```

ステップ 5　CMS サービスを再度有効にします。

```
wae# config
wae(config)# cms enable
Registering WAAS AppNav Controller...
Sending  device registration request to Central Manager with address 10.43.65.50
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in WAAS Central Manager UI.
management services enabled
```

ステップ 6　設定を保存します。

```
wae(config)# exit
wae# copy run start
```

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キャパシティ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：トラフィック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 WAE の数：リモート オフィスごとに 1 つ以上のブランチ 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 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 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。
- ANC の数：AppNav 導入モデルを使用している場合、1 つ以上の ANC が必要です。

組織に必要な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：システムの固定キャパシティと動的キャパシティに依存します。
  - 固定キャパシティ：キャパシティ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。
  - 動的キャパシティ：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） 動的キャパシティは、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。

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 または Cisco インターフェイス モジュール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。

AppNav 導入では、データセンター内の AppNav コントローラは、WCCP、PBR、またはインライン モードを介して、代行受信したトラフィックを受信し、トラフィックを最適化する WAAS ノードに配信します。AppNav 導入の詳細については、第 4 章「AppNav の設定」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。

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 5 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では、Cisco WAE Inline Network Adapter、Cisco インターフェイス モジュール または Cisco AppNav コントローラ インターフェイス モジュール がインストールされた WAE アプライアンスを使用する必要があります。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は必要ないため、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。

インライン アダプタまたはモジュールには、それぞれがインライン グループ インターフェイスまたはブリッジ グループ インターフェイスにグループ化された、1 つ以上の LAN/WAN イーサネット ポートのペアが含まれています。インライン アダプタまたはモジュールにポートの複数のペアがある場合、ネットワーク トポロジで必要であれば複数のルータに接続できます。

インライン グループ インターフェイスまたはブリッジ グループ インターフェイスは、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。

（注） AppNav コントローラ インターフェイス モジュールは、障害が発生した場合でもトラフィック フローを継続する自動バイパス モードをサポートしていません。ハイアベイラビリティを実現するためには、2 台以上の AppNav コントローラ インターフェイス モジュールを AppNav クラスタに導入する必要があります。AppNav ソリューションでのインライン モードの使用の詳細については、第 4 章「AppNav の設定」を参照してください。

特定の 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、インラインまたはブリッジのグループ インターフェイスを設定できます。

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、インライン モードで WAE デバイス（AppNav コントローラを除く）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、ハードウェアで加速された WCCP 代行受信または Cisco Application Control Engine（ACE）でのロード バランシングおよび WAAS AppNav 導入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、「インライン モード代行受信の使用」（P.5-45）を参照してください。

次の 3 つの要素を使用すると、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。

- 次の特定の WAE モデルでは、インライン インターフェイスの複数のペアを使用できます。
  - WAVE-294/594/694/7541/7571/8541 モデルは、設置された 1 つの Cisco インターフェイス モジュールをサポートし、8 つのインライン グループの最大 16 のインライン ポートを構成できます。また、設置された 1 つの AppNav コントローラ インターフェイス モジュールをサポートし、5 つのブリッジ グループに最大 12 のインライン ポートを設定できます。
  - WAE-674/7341/7371 モデルは、4 インライン グループの合計 8 つのポートを提供するデュアル インライン Cisco WAE Inline Network Adapter をサポートします。

- ハイアベイラビリティをサポートするための 2 つの WAE（AppNav コントローラを除く）のシリアル インライン クラスタリング。
- 代行受信されるトラフィックや通過するトラフィックを制御する、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.5-30）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 または ANC、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 を設定するよりもはるかに簡単です。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。

WCCP バージョン 2 プロトコルには、たとえば、複数のデバイス間の自動フェールオーバーやロードバランシングなど、便利な機能が組み込まれています。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 または ANC の状態をモニタします。WAE がダウンした場合、ルータは WAE へのパケットのリダイレクトを停止します。WCCP バージョン 2 を使用した場合、ブランチ WAE は WAAS サービスのシングル ポイント障害となりません。また、ルータまたは ANC は、複数のブランチ オフィスの WAE の間でトラフィックをロード バランスできます。

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。

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 上での WCCP の設定」（P.5-12）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、「ルータでの高度な WCCP 機能の設定」（P.5-7）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。ルートは、明示的な許可または拒否の条件が含まれる基準アクセス リストをマッピングします。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を定義します（たとえば、パケットをローカル WAE であるネクスト ホップに送信する）。

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 よりも高いパフォーマンスを実現します。
- 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、Cisco IOS ソフトウェアの適切なバージョンを実行している Cisco IOS 対応のルータまたはスイッチで実装できます。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欠点は、次のとおりです。

- PBR は、等コスト ルート間のロード バランシングをサポートしない。このため、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 よりも設定が難しい。WAAS トラフィックのための PBR の設定方法の例は、「ポリシー ベース ルーティング代行受信の使用」（P.5-36）を参照してください。

WAAS トラフィックの WCCP または PBR ルーティングの設定

WAAS の主要な機能は WAN トラフィックを加速することです。一般に、WAAS は、TCP トラフィックを加速します。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。アプリケーション固有およびネットワーク固有のインテリジェンスを持つ WAE が、WAN の両側に配置されます。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、トラフィックを透過的に代行受信してローカル WAE に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.2-24）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

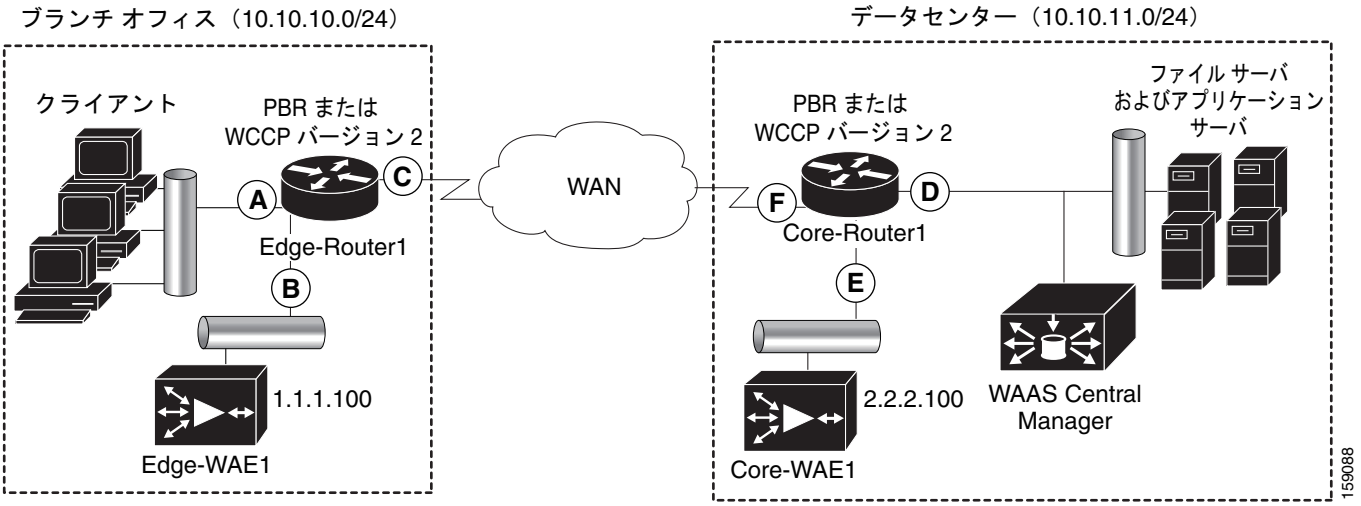

表 2-1 に、PBR または WCCP バージョン 2 を使用して、透過的にトラフィックを WAE へリダイレクトするために設定する必要があるルータ インターフェイスの概要を示します。

表 2-1　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 interface	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）。

表 2-1　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 interface	説明
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、近端のルータだけではなく、遠端のルータでもトラフィックが代行受信されてリダイレクトされる必要があります。これによって、トンネルベース モードでは 2 つのインターセプト ポイントであるのに対して、4 つのインターセプト ポイントが必要となります。

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（デフォルトでは、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、またはその他）で TCP 無差別を設定する場合、個別にサービス 61 および 62 を定義して設定する必要があります。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。サービス ID は設定可能で、デフォルトは 61 と 62 です。

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。デフォルトとは異なる ID を設定した場合は、ルータで使用されるサービス ID が WAE の ID と一致している必要があります。

デフォルトでは、TCP 無差別モード サービスに IP プロトコル 6 が指定されます。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.2-24）を参照してください。

可能な場合、ブランチ ソフトウェア ルータの着信インターフェイスでパケット リダイレクションを設定します。着信トラフィックはシスコ エクスプレス フォワーディング（CEF）、分散型シスコ エクスプレス フォワーディング（dCEF）、Fast Forwarding、または Process Forwarding 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。インターフェイス上で **ip wccp redirect exclude in** を設定してから、**ip wccp redirect in** コマンドを設定すると、**exclude in** コマンドは上書きされます。**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.2-24）
- 「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.2-24）

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、デフォルトでは WAE で WCCP バージョン 2 サービス 61 および 62 を使用します。ただし、サービス ID は設定可能です。WCCP サービスは、WAE CLI では標準名の tcp-promiscuous で、WAAS Central Manager GUI では TCP Promiscuous という名前で表現されます。（図 5-3 を参照）。

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 の基本的な WCCP 設定を変更する手順については、「WAE 上での WCCP の設定」（P.5-12）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、「WCCP 代行受信接続の出力方式の設定」（P.5-32）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。

ルータとローカル WAE の間の無限のルーティング ループを回避するには、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）またはルータの LAN ポートからサブインターフェイス（異なる仮想サブインターフェイス）を介して 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。また、この方法では WAE の既存のネットワークへの統合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.5-10）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 9 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.5-30）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、次の認証、許可、アカウンティング（AAA）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.7-32）を参照してください。

WAAS の管理者アカウント

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。

- ロールベースのアカウント：ユーザに WAAS Central Manager GUI、WAAS Central Manager CLI、WAE Device Manager GUI へのアクセスを許可します。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.8-6）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、容易に共通の品質と機能を共有できる WAE の集合であるデバイスの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。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）　AllWAASGroup と AllWAASExpressGroup はデフォルトのデバイス グループで、自動的にすべての WAAS および WAAS Express デバイスが含まれます。これらのグループ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デバイス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。

デフォルトで、WAAS Central Manager を使用すると、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、CIFS 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 アクセラレータによる CIFS 環境でのみ動作します（SMB アクセラレータではサポートされていません）。
- 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 つのオプションから選択できます。
  - 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。