# Real-Time Traffic over Wireless LAN ソリューション リファレンス ネットワーク設計ガイド

初版：2013 年 11 月 11 日


**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



Text Part Number: OL-29731-01-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。

# 目 次

# はじめに

ここでは、目的、対象読者、マニュアルの構成について説明します。



## 目的

『*Real-Time Traffic over Wireless LAN* ソリューション リファレンス ネットワーク設計ガイド』には、エンドポイントとクライアント間でのリアルタイム トラフィックの送受信、およびリアルタイム トラフィック アプリケーションやサービスの利用のための接続を提供するワイヤレス ソリューションの設計リファレンスが記載されています。リアルタイム トラフィック対応のエンドポイントをサポートし、リアルタイム トラフィック アプリケーションおよびサービスを可能にするワイヤレス ネットワークの導入は、Real-Time Traffic over WLAN（RToWLAN）の導入と呼ばれます。

リアルタイム トラフィックのエンドポイントおよびアプリケーションは、リアルタイム ネットワーク トラフィックを生成してネットワーク帯域を消費します。 このネットワーク トラフィックにはパケット化された音声およびビデオに加えて、ほぼ生成された直後に消費される他のトラフィックも含まれます。 リアルタイム ネットワーク トラフィックは、ほぼ直ぐに価値がなくなるため、再送信は行われず、遅延、遅延時間のゆらぎ（ジッタ）、またはパケット損失に対する許容度が制限されます。 送信側と受信側の間でリアルタイムトラフィックの配送において遅延やパケット損失がほぼないネットワークが必要となります。そうでない場合、再送信または遅延したトラフィックは、遠隔地の受信側で破棄される場合があります。

適切に計画された RToWLAN の導入設計では、高品質の音声およびビデオ通信が提供されるだけでなく、デスクトップ仮想化やプレゼンスなど、その他のリアルタイム トラフィック アプリケーションおよびサービスのための配信時間も十分に提供されます。 この設計ガイドでは、特定のハードウェアおよびソフトウェア要件よりも、RToWLAN 導入のソリューション レベルの計画や設計に関連した側面を中心に説明します。

この『*Real-Time Traffic over Wireless LAN* ソリューション リファレンス ネットワーク設計ガイド』は以前の『*Voice over Wireless LAN Design Guide*』に代わるものです。以前のガイドは、http://www.cisco.com/ から入手できます。

# 対象読者

このマニュアルは、リアルタイム トラフィック エンドポイントおよびクライアント対応の Cisco Unified Wireless LAN の導入のプランニングと設計を担当するシステム設計および導入技術者を対象としています。

# マニュアルの構成

次の表に、このマニュアルの各章を示します。

**表 *1*：マニュアルの概要**

| 章 | 説明 |
|---|---|
| はじめに, （? ページ） | 目的、対象読者、マニュアルの構成を説明します。 |
| Real-Time Traffic over WLAN の概要, （1 ページ） | RToWLAN ソリューションとそのソリューション アーキテクチャ、RToWLAN 導入の各種コンポーネントと考慮事項など、ワイヤレス、コラボレーション、エンドポイント、ネットワーク管理に関連する設計情報の概要を説明します。 |
| Real-Time Traffic over WLAN の無線周波数設計, （25 ページ） | RToWLAN 導入および無線周波数（RF）導入の問題に関する RF ネットワークの要件について概要を説明します。 |
| Real-Time Traffic over WLAN の QoS, （55 ページ） | Cisco Unified Wireless Network における WLAN QoS とその実装の概要を説明します。 |
| Real-Time Traffic over WLAN のセキュリティ, （91 ページ） | WLAN セキュリティの概要を説明します。 |
| Real-Time Traffic over WLAN のローミング, （105 ページ） | RToWLAN 導入の WLAN ローミングとその影響について概要を説明します。 |

第 1 章

# Real-Time Traffic over WLAN の概要

この章では、RToWLANを導入することのドライバと利点について説明した後、企業のソリューション リファレンス ネットワーク アーキテクチャについて図説します。 また、RToWLAN ソリューション導入のタッチ ポイントについて概要を説明します。RToWLAN ソリューションのアーキテクチャを簡単に概説し、以下の RToWLAN ソリューションの 3 つの主要コンポーネントについて示します。

- 企業の 802.11 WLAN ソリューション インフラストラクチャ
- 企業のコラボレーション ソリューション アプリケーションおよびサービス
- Real-Time Traffic over WLAN のエンドポイント

さらに、コンポーネントについて説明した後で、特に QoS、セキュリティ、ハイ アベイラビリティ、およびキャパシティ プランニングに焦点を当てて、単一サイトへの導入と分散した複数サイトへの導入の両者に共通する RToWLAN ソリューションを設計する場合の考慮事項について説明します。

# RToWLAN ソリューションのドライバと利点

今日の企業活動のスピードはこれまでになく速くなっています。 企業が成長し競争に勝って成功を収めていくためには、人員の合理化、コラボレーション、そしてタイムリーなビジネス プロセスが不可欠です。 企業データや通信インフラストラクチャのセキュリティを維持しながら、より多くの業務を実行できるように、企業ではモバイル ワーク スタイルの推進に力を入れています。 さらに、企業は、テクノロジーによってプロセスを簡素化するだけなく、ユーザの生産性を向上させてビジネス プロセスを加速する新しいテクノロジーを用いて、収益の増加とコスト削減も目指しています。

WLAN ネットワークを介して配信されるリアルタイム トラフィック アプリケーションおよびサービスでは、次のような利点が得られます。

- **企業内でモバイル セルラー デバイスが不要**：WLAN を介した音声およびビデオの IP 通話が企業の WLAN の全部または一部を通過することで、セルラー ネットワークへの直接コールよりもコストの節減になります。 従業員は、セルラー音声ネットワークを介した音声通話を数分間行う代わりに、キャンパス内の WLAN エンドポイントまたはクライアントを介して音声およびビデオ通話を行うことができます。
- **企業内のモバイル プロバイダー ネットワーク カバレッジに対する依存が軽減**：802.11 WLAN ネットワーク接続を利用した場合、十分な数のアクセス ポイントを導入することで、企業はネットワークのカバレッジとキャパシティを十分に提供できるようになり、同時に企業内のモバイル プロバイダー ネットワーク カバレッジに対する依存性を軽減および除去できます。
- **従業員所有の個人およびゲスト デバイスを有効活用**：スマートフォンやタブレットなどの個人用のモバイル デバイスの普及にともない、企業においてもこれらのデバイスの流入が増加しています。 このタイプの企業は、よく個人所有デバイスの持ち込み（BYOD）と呼ばれます。 BYOD ソリューションによる従業員所有のデバイスやゲスト デバイスの有効活用には、次のような効果があります。
  - 全体的な従業員満足度が増加します。
  - リアルタイム トラフィック コラボレーション アプリケーションおよびサービスに対応したデバイスを活用することで、生産性が向上します。
- **モバイル ワーカーのアベイラビリティおよび到達可能性の最大化**：企業コラボレーションに対応したモバイル デバイスを活用することで、企業内のあらゆる場所の従業員に接続できるようになる一方、モバイル デバイスのユーザ エクスペリエンスは従来型の企業内エンドポイントと遜色ありません。 この柔軟性は、いくつもの企業クライアントやデバイスを使用するユーザにスムーズなユーザ エクスペリエンスを提供します。
- **モバイル通信による固定網通信の代替（FMS）の導入環境で、高品質な音声通話およびビデオ通話とシームレスなモバイル ユーザ エクスペリエンスを提供**：企業 IP テレフォニー システムからデュアルモード モバイル スマートフォンおよびタブレットで企業の電話番号を使用できるようにするには、音声およびビデオ IP 通話を企業の WLAN ネットワークを介して送信する必要があります。 RToWLAN ネットワークは、ネットワークの帯域幅やスループット、優先度の高いキューイングまたは通信がリアルタイム トラフィックに対して最適となる

ように、調整されます。IPベースの音声通話やビデオ通話の場合、これは、パケット損失、ジッタ、遅延が最小化されることを意味し、高品質な音声およびビデオを提供できます。モバイルエンドポイントおよびクライアントでの企業の電話番号の使用には、次のような効果があります。

- 企業の IP 通話制御機能に統合できます。
- 企業ダイヤル プランが提供され、企業デバイス間でシームレスなユーザ エクスペリエンスが実現します。
- モバイル ワーカーに企業のデスクフォンが不要となります。

RToWLAN を導入すると、企業は次のような利点を得られます。

- モバイル プロバイダーの音声およびデータ サービスの支出が軽減します。
- 従業員の生産性、到達可能性、およびアベイラビリティが向上します。
- BYOD ソリューションによって低コストまたはコストゼロで、増加する個人モバイルデバイスを企業内でのコラボレーションや通信の手段として活用できます。
- 柔軟性とシームレスなユーザエクスペリエンスを提供することで、コラボレーションや他のビジネス アプリケーションまたはサービスを使用する従業員の満足度が向上します。

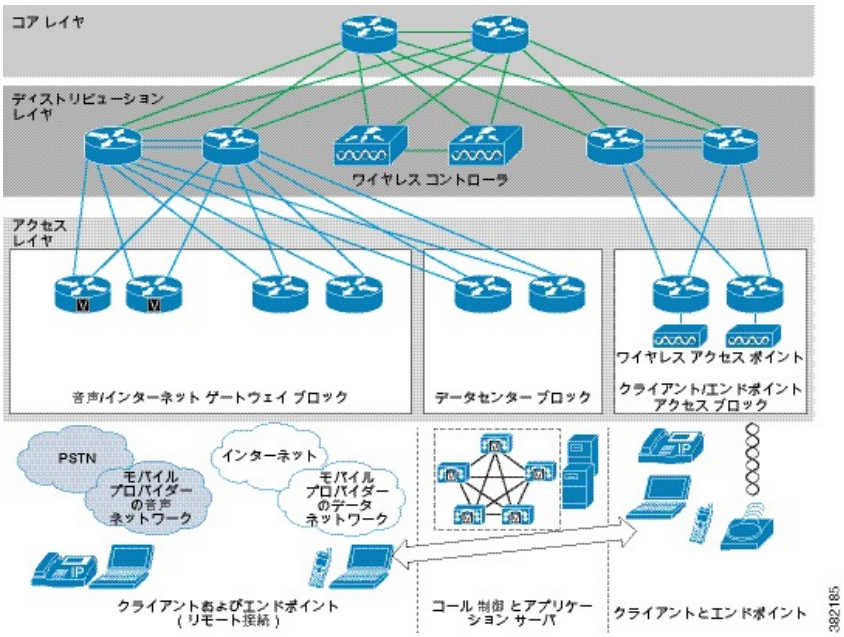
# RToWLAN ソリューション リファレンス ネットワーク設計アーキテクチャ

ここでは、ワイヤレス エンドポイントおよびクライアントに対するリアルタイム トラフィック アプリケーションおよびサービスを導入する際のネットワーク トポロジの例（図 1：Real-Time Traffic over WLAN ソリューション ネットワーク トポロジの概要, （4 ページ）を参照）について概説します。この RToWLAN ソリューションの設計例では、通常のレイヤ構成である、アクセス、ディストリビューション、およびコア キャンパス ネットワークを基本として使用しています。この設計には、以下のコンポーネントが追加として含まれます。

- リアルタイム トラフィックおよび他の IP ネットワーク トラフィックの伝送用のワイヤレス ネットワーク インフラストラクチャを提供する WLAN コントローラ（WLC）およびアクセス ポイント（AP）
- クライアントおよびモバイル エンドポイントのワイヤレス ネットワーク接続用にクライアントおよびエンドポイント アクセス ブロックに追加されたワイヤレス アクセス ポイント
- リアルタイム トラフィックを有効にする場合のコール制御や他のアプリケーション サーバを含むデータセンター ブロック

- PSTN へのアクセスと企業への双方向のアクセスを提供する音声およびインターネット ゲートウェイ ブロック

**図 *1*：*Real-Time Traffic over WLAN* ソリューション ネットワーク トポロジの概要**




すべての企業の RToWLAN 導入にとって重要な以下の 2 つのソリューション コンポーネント エリアに焦点をあてます。

- ディストリビューション、クライアント、エンドポイント アクセス ブロック内で有効な企業の 802.11 ワイヤレス インフラストラクチャ（上の図を参照）
- データセンター、音声、インターネット ゲートウェイ内で有効な企業のコラボレーション インフラストラクチャ（上の図を参照）

## 企業ワイヤレス LAN の概要

企業の 802.11 ワイヤレス LAN（WLAN）インフラストラクチャは RToWLAN ソリューション導入の基盤です。 ネットワーク接続がワイヤレス エンドポイントで利用でき、リアルタイム トラフィックに対して帯域幅とスループットが十分に提供されるように、企業ワイヤレス ネットワークを設計する必要があります。 また、導入が予想される RToWLAN エンドポイント デバイス数に対して十分なキャパシティの WLAN を設計する必要があります。 ハードウェアまたは IP 接続の障害によってWLANネットワークのアベイラビリティが完全に排除されないように、冗長性に優れた WLAN を設計することも必要です。

WLAN インフラストラクチャはネットワーク接続を提供するだけでなく、有線ネットワークを使用して、選択されたトラフィックに対してベスト エフォート処理よりも優れた認証と暗号化セキュリティ サービスおよび QoS を提供します。 この機能を配信するため、802.11 WLAN インフラストラクチャは、ワイヤレス LAN コントローラ（WLC）、ワイヤレス アクセス ポイント

（AP）、ワイヤレス LAN 管理アプリケーションなど、多くのコンポーネントとアプリケーションから構成されています。

### 企業コラボレーションの概要

コラボレーション システムは多数の機能およびサービスを有効にします。最も一般的で普及している機能は IP を介した音声およびビデオ通話ですが、 これらのコラボレーション システムは、会議、メッセージング、プレゼンス、情報およびドキュメント共有、Fixed Mobile Convergence、番号統合など、従来の IP テレフォニーを超える通信機能を提供できます。 これらの機能やサービスはセットで導入されることが多く、企業とその従業員に対して包括的なコラボレーション ソリューションを提供します。音声およびビデオエンドポイント、ゲートウェイ、ボイスメールおよびプレゼンスのアプリケーション サーバなど、コラボレーション システムはさまざまなコンポーネントとアプリケーションに依存しています。

# RToWLAN ソリューション アーキテクチャの概要

RToWLAN ソリューション導入の全体的なアーキテクチャ（図 2： RToWLAN ソリューション アーキテクチャの概要, （6 ページ） を参照）は、次の 3 つの主要コンポーネントから構成されます。

- **802.11 ワイヤレス LAN インフラストラクチャ**：ワイヤレス インフラストラクチャでは、エンドポイントやクライアントの接続用に 802.11 ワイヤレス LAN を有効にします。 このインフラストラクチャには、WLAN コントローラ、アクセス ポイント、管理アプリケーションが含まれます。
- **コラボレーション アプリケーションおよびサービス**：コラボレーション アプリケーションでは、音声通話やビデオ通話などのリアルタイム トラフィック サービスを有効にします。これらのアプリケーションおよびサービスには、PSTN ゲートウェイ、メディア リソース、ボイスメール、インスタント メッセージおよびプレゼンスが含まれます。
- **リアルタイム トラフィック対応 802.11 ワイヤレス エンドポイント**：ワイヤレス エンドポイントは、802.11 WLAN を介してリアルタイム トラフィックを消費および生成します。 これらのエンドポイントには、ワイヤレス対応デスクトップおよびモバイル ソフトウェア アプリケーション、クライアント、ワイヤレス IP フォン ハードウェアが含まれます。

RToWLAN アプリケーションを有効にしてリアルタイム サービスをワイヤレスで配信する場合は、これらのコンポーネントのすべてが必要となります。

図 *2*：***RToWLAN*** ソリューション アーキテクチャの概要

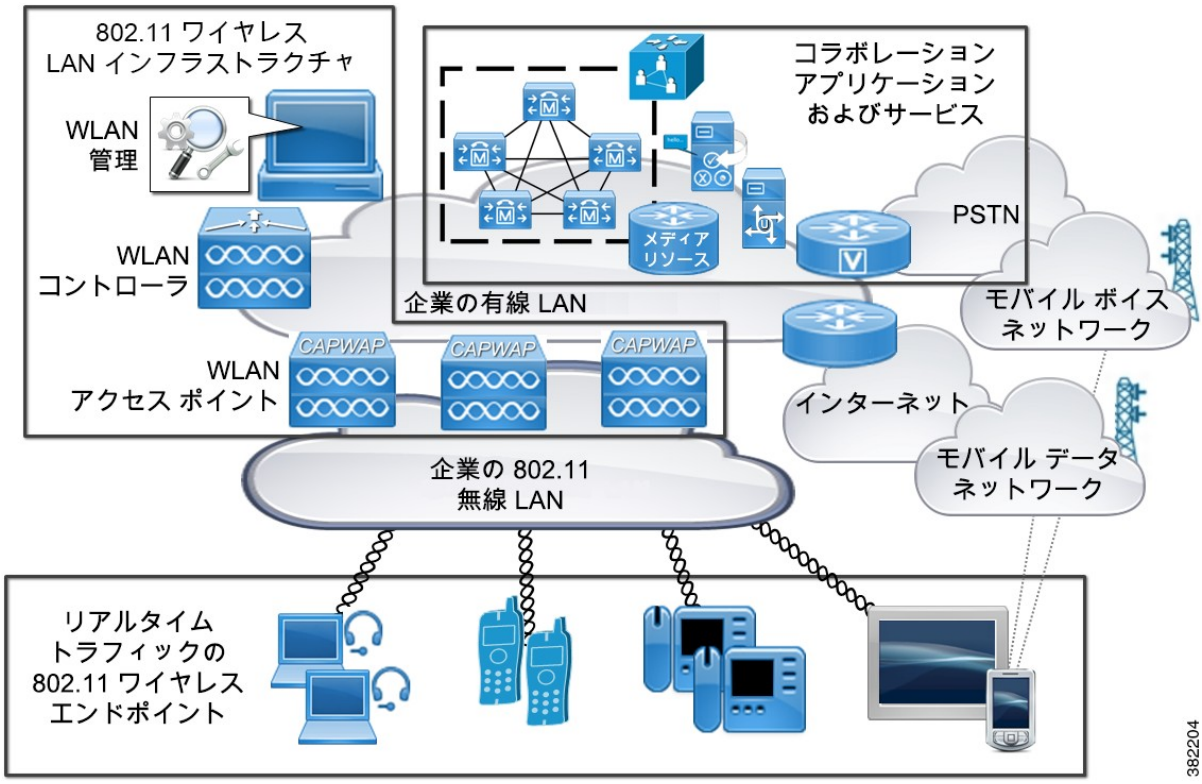



図 2： RToWLAN ソリューション アーキテクチャの概要, （6 ページ）を参照してください。この章の以降の内容には、通常の企業アプリケーションおよびサーバによって提供される基本的なネットワーク サービスに関する情報は記載されていません。 これらのネットワーク サービスの存在は前提とされており、RToWLAN に直接関連する事例を除いて、以下に関する考慮事項は説明されません。

- ネットワークベースのデバイスとユーザ認証および識別サービス。認証権限サーバ、二要素認証サプリカント、ディレクトリ サーバなどのアイデンティティ ストア、セキュリティ サービスを提供する他のアプリケーションまたはコンポーネントなど。
- ネットワーク タイムおよび IP アドレスの解決と割り当て。ネットワーク タイム サービス（NTP）、ドメイン ネーム サービス（DNS）、動的な IP アドレス割り当て（DHCP）など。
- ネットワーク ルーティング、パケット転送およびキューイング、QoS、アドミッション制御。

# 企業の 802.11 ワイヤレス LAN ソリューション インフラストラクチャ

企業の 802.11 ワイヤレス LAN（WLAN）ネットワークは RToWLAN ソリューションに不可欠です。これは、接続されたリアルタイム トラフィック対応のワイヤレスデバイスによって生成されるリアルタイム トラフィックを伝送するネットワークをワイヤレスインフラストラクチャが提供するからです。 次の表に、802.11 ワイヤレス ネットワーク インフラストラクチャのコンポーネントを示します。

**表 *2*：*802.11* ワイヤレス ネットワーク インフラストラクチャのコンポーネント**

| 802.11 ワイヤレス ネットワーク インフラストラクチャのコンポーネント | 説明 |
|---|---|
| ワイヤレス LAN アクセス ポイント | ワイヤレス LAN アクセス ポイントは、無線ネットワークからのワイヤレスデバイスへのアクセスを提供し、デバイスやクライアントが有線ネットワーク コンポーネントと通信できるようにします。アクセスポイントは、ワイヤレス デバイス ネットワーク接続を提供するだけでなく、有線ネットワークと無線ネットワーク間の境界ポイントとしても機能します。 ワイヤレス LAN コントローラは、登録されているアクセス ポイントを管理します。 |
| ワイヤレス LAN コントローラ | ワイヤレス LAN コントローラ（WLC）は、ワイヤレス ネットワークにおいて集中管理を行う役割を果たすネットワーク インフラストラクチャ デバイスです。 アクセス ポイントの設定および管理、無線周波数のモニタリング、クライアントのアソシエーションと認証を集中管理することで、WLC はワイヤレス LAN の導入を容易にします。 ワイヤレス アクセス ポイントを WLC に登録すると、ワイヤレス アクセス ポイントはすべての管理とクライアント トラフィックを WLC にトンネリングします。 また、WLC は、ネットワークのワイヤレス クライアントと有線部分の間でトラフィックの切り替えも行います。 |
| ワイヤレス管理 | ワイヤレス LAN 管理アプリケーションおよびサービスは、強固なワイヤレス ライフサイクル管理ツールを提供し、ネットワーク管理者がワイヤレス ネットワークで問題なく計画、導入、モニタ、トラブルシューティング、レポートを実行できるようにします。 |

企業WLANネットワークは、ユーザ、アプリケーション、エンドポイントのニーズを満たすように設計する必要があります。 WLAN カバレッジは、十分な Wi-Fi チャネルの帯域幅を提供し、高品質なアプリケーションパフォーマンスをサポートする必要があります。ユーザにとって十分な帯域幅の WLAN カバレッジエリアを設計するには、エンドポイントの Wi-Fi パフォーマンス機能を理解する必要があります。 ワイヤレス エンドポイントおよびモバイル クライアント デバイスはさまざまな機種を使用できますが、すべてのワイヤレス クライアントが同じ機能を備えているとは限りません。 WLANの導入を成功させるためには、詳細なワイヤレスインフラストラクチャのプランニングを行う必要があります。

ワイヤレスネットワークの導入を成功させるには、徹底的なワイヤレスサイト調査を実施して、導入環境全体で動作中のエンドポイントに必要な帯域幅とスループットを提供するように無線周波数の設定と設計を最適化する必要があります。 さらに、このサイト調査によって、干渉源の特定も容易となり、除去することができます。 サイト調査では、次の無線周波数設計の基本原則を確認するようにします。

- **隣接チャネル セルの分離**：同一のチャネルまたは隣接するチャネルにより干渉が発生する可能性があり、ネットワーク スループットが低下してパケット損失が増加するおそれがあります。 サイト調査を実施すると、隣接チャネル セルが適切に分離されていることを確認できます。
- **非隣接チャネル セルのオーバーラップ**：非隣接チャネルをオーバーラップさせて、ワイヤレス エンドポイントがアクセス ポイントとワイヤレス チャネル セル間でシームレスに移動またはローミングできるようにします。 サイト調査を実施すると、非隣接チャネル セルが十分にオーバーラップしていることを確認できます。
- **必要な全サービス エリアのチャネル セルのカバレッジ**：建物の吹き抜けや建物と建物の間、建物周囲でのワイヤレス ネットワーク カバレッジを想定する場合は、すべての必要な場所に適切なワイヤレス チャネル カバレッジを提供するよう、アクセス ポイントとアンテナが正しく配置されていることをサイト調査によって確認できます。
- **チャネル セル密度**：高品質なリアルタイム アプリケーションおよびサービスのパフォーマンスに対応するために、必要なエンドポイントの数がサポートされ、必要なネットワーク帯域幅とスループットが WLAN チャネルに提供されるよう、適切なチャネル セル密度が提供される必要があります。
- **ワイヤレス干渉の識別および軽減**：不適切な AP およびアンテナの配置、導入エリアの物理的な構造と特性、無線周波数設計の不備によって発生するワイヤレス干渉をサイト調査の間に特定する必要があります。 さらに、WLAN の導入を計画する場合は、コードレス電話、個人用ワイヤレス ネットワーク デバイス、硫黄プラズマ照明システム、電子レンジなどの干渉源や、変圧器、強力な電気モーター、冷蔵庫、エレベータおよびエレベータ機器、電磁波干渉（EMI）を発生する可能性のある他の電源デバイスなどの高出力電気デバイスをについて考慮する必要があります。 アクセス ポイントの位置およびアンテナの方向、無線周波数設定、AP 電力レベルを調整するか、これらの干渉源を削除または除去して、干渉を軽減する必要があります。

今日では、コントローラおよびアクセス ポイントは特定の使用目的や特定の規模に特化されています。 個人の住宅環境では、同じ WLAN チャネル無線周波数を同時に共有するモバイル クライアント デバイスの数は制限されています。 したがって、帯域幅は懸念事項ではありません。 た

だし、企業環境では、多数のデバイスが Wi-Fi チャネルに接続されています。 帯域幅が不十分な状態だと音声通話を聞き取れなかったり、ビデオ通話を視聴できなかったりする可能性があり、アプリケーションの障害が発生する場合もあります。

### 関連トピック

Real-Time Traffic over WLAN の無線周波数設計, （25 ページ）
シスコのワイヤレス製品
Enterprise Mobility Design Guide

# 企業のコラボレーションソリューションアプリケーションおよびサービス

企業に有線およびワイヤレス LAN を計画して導入した後は、そのインフラストラクチャの上に企業向けのコラボレーション アプリケーション、サービス、およびエンドポイントを導入する必要があります。 企業向けのコラボレーション導入は、必要なコンポーネント、アプリケーション、サービスを使用でき、インフラストラクチャが十分なキャパシティと信頼性を提供するように設計される必要があります。

コラボレーション システムによって、数多くの機能およびサービスが利用できるようになります。たとえば、音声通話やビデオ通話、ボイスメールおよびインスタントメッセージ（IM）、プレゼンスおよびアベイラビリティなどのメッセージング機能、さらに電話会議、保留音、番号統合などの各メディア リソースなどです。 これらの機能やサービスはセットで導入されることが多く、企業とその従業員に対して包括的なコラボレーション ソリューションを提供します。

コラボレーション システムの中核と考えられる企業のコール制御プラットフォームは、音声通話およびビデオ通話サービス（Cisco Unified Communications Manager など）を提供します。 また、コラボレーション システムは、以下のようないくつかのコンポーネントおよびアプリケーションに依存します。

- **ゲートウェイ**：PSTN への外部アクセスと、他のコール制御プラットフォーム、アプリケーション、デバイスへの内部アクセスを提供する、IP または TDM インターフェイスを持つプラットフォーム。
- **メディア リソース**：音声およびビデオ会議、保留音、トランスコーディングなどの補足的なサービスによりコール フローを強化するため、ネットワーク全体に配置されているハードウェアまたはソフトウェアベースのリソース。
- **コラボレーション アプリケーション**：従来の音声通話やビデオ通話を超える通信機能を提供するアプリケーション。 たとえば、ボイスメール、IM およびプレゼンス、電話会議、情報およびドキュメント共有、Fixed Mobile Convergence、番号統合などの機能です。

また、音声およびビデオエンドポイントはコラボレーションシステムの重要なコンポーネントです。 企業ユーザは、デスクフォン、ワイヤレス フォン、ソフトウェア クライアント、イマーシブ ビデオ システム、スマートフォンおよびタブレット用のモバイル クライアントなどのエンドポイントと通信してコラボレートします。

コラボレーション ハードウェア、アプリケーション、サービスを導入する場合や、リアルタイム トラフィック対応のワイヤレス エンドポイントを有効にする前に、必要なコラボレーションおよび通信アプリケーション/サービスの導入および設定を適切に行ってください。 次の要因について検討する必要があります。

- デバイス設定

  ロケーション、ユーザのアソシエーション、コール権限、ボタン レイアウト、他の機能設定など、コール制御システム内のデバイス設定を、正常に動作するように適切に設定する必要があります。

- ネットワーク サービス操作

  デバイスは、ネットワークに接続し、ネットワーク経由でコール制御システムから設定を取得または受信して、コラボレーション インフラストラクチャ コンポーネントに接続および通信できる必要があります。

- ダイヤル プラン

  IP アドレッシングと IP ルーティングが IP ネットワーキングの基本であるように、コール制御システムで設定される企業ダイヤル プランはコラボレーション システム オペレーションの基本です。 ユーザがコールを送受信できるようにするには、次のダイヤル プラン設定を適切に実装する必要があります。

  - デバイスへの電話番号のナンバリングまたは割り当て
  - ダイヤリング手順の有効化と制限クラスのデバイスへの適用
  - デバイスの設定に従った発着信番号の操作

- コンポーネント間の統合

  追加機能およびサービスを配信するために、コラボレーションと通信インフラストラクチャ コンポーネント間の統合を有効にして設定します。 たとえば、コール制御プラットフォームと PSTN ゲートウェイまたはボーダー コントローラ、ボイスメールと IM またはプレゼンス アプリケーション サーバ、電話番号またはコンタクト ソース プラットフォームなどの間の統合を実施して、PSTNアクセスやIMおよびプレゼンスなどの追加サービスを有効にする必要があります。

- セキュリティ

  セキュアな運用を行うため、企業のセキュリティ ポリシーに従ってセキュリティ機能を導入します。 とりわけ、音声またはビデオ メディアの暗号化やシグナリング、証明書ベースのトランク統合、ダイジェスト認証済みデバイスなどの機能を使用する計画がある場合は、適切な設定とインフラストラクチャ（認証局サーバなど）を導入する必要があります。

非ワイヤレスのリアルタイム トラフィックに対応したエンドポイントをまず使用して上記の考慮事項を確認し、必要な機能が適切に動作することを確認してから、RToWLAN ワイヤレス エンドポイントの導入を続行してください。

### 関連トピック

802.11 RToWLAN エンドポイント，（11 ページ）

シスコの音声製品
シスコのコラボレーション製品
シスコの企業コラボレーション導入設計

# 802.11 RToWLAN エンドポイント

企業の WLAN インフラストラクチャとコラボレーション アプリケーションおよびサービスを設計して実装した後は、この全体的なインフラストラクチャの上に RToWLAN 対応のデバイスとクライアントを導入する必要があります。

（注） WLAN インフラストラクチャの設計および実装フェーズの間（特にサイト調査中）に、RToWLAN エンドポイントの選定を検討します。 インフラストラクチャ上に導入する特定の RToWLAN エンドポイントについて検討せずに WLAN インフラストラクチャを設計すると、パケット損失、過剰遅延、音声およびビデオ品質の低下などの問題につながります。

RToWLAN エンドポイントは、次の 2 つのカテゴリに分類されます。

- ハードウェアベースのワイヤレス IP フォン
- ワイヤレス デバイスのソフトウェアベース クライアント

### ハードウェアベースのワイヤレス IP フォン

ハードウェアベースのワイヤレス IP フォンは、音声通話やビデオ通話機能に特化して設計された専用のワイヤレス IP 音声フォンおよびビデオ フォンです。

ハードウェアベースのワイヤレス IP フォンは、次の 2 つのサブカテゴリに分類されます。

- **デスクトップ WLAN フォン（または固定 WLAN フォン）**：IP デスク フォンはネットワークにワイヤレス接続しますが、壁面コンセントから電源が供給されるため、移動はできません （例：Cisco Desktop Collaboration Experience DX650）。
- **モバイル WLAN フォン**：ワイヤレス IP フォンはバッテリ電源式でネットワークにワイヤレス接続されます。アクティブなネットワーク接続を維持したまま企業内を移動することができます （例：Cisco Unified Wireless IP Phone 7925G）。

### ワイヤレス デバイスのソフトウェアベース クライアント

ワイヤレス デバイスのソフトウェアベース クライアントは多機能ワイヤレス デバイス上で実行され、さまざまな種類のトラフィックを生成して多様なオペレーションを実行できます。 多機能ワイヤレス デバイスはコラボレーション ソフトウェア アプリケーションを実行し、音声通話やビデオ通話に加えて他のコラボレーション機能も実行できます。

ワイヤレス デバイス上で実行されるソフトウェアベース クライアントは、次の 2 つのサブカテゴリに分類されます。

- デスクトップ コンピューティング プラットフォーム

これらのデバイスはネットワークにワイヤレス接続されますが、プラットフォームによって、移動できる場合やそうでない場合があります。 デスクトップ コンピュータが壁面コンセントからの電源供給に依存するのに対し、ラップトップ コンピュータはバッテリ電源式のため、ネットワークへのアクティブなワイヤレス接続を維持したまま周辺を移動させることができます。 これらのデバイスは通常、Microsoft Windows または Apple Mac オペレーティング システムを実行するため、コラボレーション ソフトウェア クライアントはこれらのオペレーティング システムをサポートする必要があります。

（例：Cisco Jabber for Windows）。

- モバイル コンピューティング プラットフォーム

  スマートフォンとタブレットは、この種類のデバイス例です。バッテリ電源式でワイヤレス接続される場合は、ネットワークへのアクティブな接続を維持したまま企業内を移動させることができます。 これらのデバイスは通常、Android または Apple iOS オペレーティング システムを実行するため、コラボレーション ソフトウェア クライアントはこれらのオペレーティング システムをサポートする必要があります。

  （例：Cisco Jabber for Android）。

### エンドポイントの選定と WLAN サイト調査

ユーザにとって十分な帯域幅の WLAN カバレッジ エリアを設計するには、エンドポイントの WLAN パフォーマンス機能を理解する必要があります。 ワイヤレス エンドポイントおよびモバイル クライアント デバイスはさまざまな機種を使用できますが、すべてのワイヤレス クライアントが同じ機能を備えているとは限りません。

サイト調査は、WLAN を導入する際の基本要件の 1 つであり、クライアント デバイスまたはエンドポイントの Wi-Fi 機能について必ず検討する必要があります。 ほとんどのスマートフォンおよびタブレットは 802.11 をサポートします。 ただし、一般にスマートフォンやタブレットは、ラップトップよりもアンテナとデータ レートの性能が劣ります。 また、それらのほとんどは企業 WLAN マーケット専用ではありません。 ほぼすべてのスマートフォンやタブレットは企業のセキュリティ ポリシーをサポートします。 ただし、その多くは、音声通話やビデオ通話の QoS および帯域幅制御用の 802.11e WMM などの Wi-Fi プロトコルおよび機能をサポートしません。 調査プロセスを開始する前に、これらの制限について検討してください。

一般的に、スマートフォンとタブレットは、アクセスポイント間のローミング ロジックに関しては、標準以下の性能しかありません。 一般消費者向けまたは非企業向け Wi-Fi エンドポイントのほとんどは、アクセスポイント間のローミング時にパフォーマンスが低下します。 クライアントのローミングは予測不可能な場合があり、企業向けのローミング ロジックを使用しないエンドポイントでは共通して、同じパスを繰り返し通過し、ミリ秒または秒単位の同じローミング時間を繰り返すことはありません。 非企業向け Wi-Fi エンドポイントでは、高密度な導入環境において、スループットがより高くなる可能性がある他のアクセス ポイントを使用することはせず、同じアクセスポイントを繰り返しローミングすることがよくあります。 調査プロセスの開始前に、施設で使用する予定のデバイスの機能をテストして理解しておくことが重要です。

Cisco WLAN コントローラは、非企業向けクライアントのローミングを支援するパラメータを提供します。 これらのパラメータには、最低受信信号強度表示（RSSI）、ヒステリシス（dB）、ミリワットあたりのスキャンしきい値（dBm）、および遷移時間が含まれます。 これらのパラメー

タの設定は、各モバイルクライアントの挙動が異なるため、さまざまなモバイルクライアントを使用してオンサイトでテストする必要があります。

### 関連トピック

企業のコラボレーション ソリューション アプリケーションおよびサービス, （9 ページ）
Real-Time Traffic over WLAN の無線周波数設計, （25 ページ）
Cisco IP Phone
Cisco Jabber

# RToWLAN ソリューション導入の考慮事項

ここでは、RToWLAN ソリューションを設計して実装する場合に検討する必要がある重要な事項について説明します。

### ハードウェアおよびソフトウェアの選択

RToWLAN ソリューションの導入でハードウェアおよびソフトウェアを選択する場合は、機能セット、サポートされる規格や機能、ハードウェアおよびソフトウェアの互換性について検討する必要があります。選択したワイヤレスおよびコラボレーションインフラストラクチャとそのインフラストラクチャに導入されるデバイスが必要な機能を確実に配信できることが重要となります。選定対象がワイヤレス LAN コントローラとアクセス ポイント、コラボレーションプラットフォームとアプリケーション、またはエンドポイント デバイスであるかどうかは関係ありません。

一般則として、高度なネットワーク機能やアプリケーション機能の豊富なセットをサポートすると同時に、多様なシステムとの相互運用性や互換性を確保できる、ワイヤレスおよびコラボレーションプロトコル規格に適合する認証済みの製品を選択する必要があります。たとえば、ワイヤレス インフラストラクチャ コンポーネントを選択する場合は、最低要件として、802.11 ワイヤレス規格（802.11a、802.11g、より新しい 802.11n および 802.11ac ワイヤレス アクセス規格、802.11e および 802.11r などの高度なワイヤレス規格）を完全にサポートしているかを検討します。 これらの規格をサポートすることで、遅延が最小限でベスト エフォート処理を備えた必要な帯域幅を音声およびビデオなどのリアルタイム トラフィックに提供できるようになります。

コラボレーションおよび通信インフラストラクチャを設計する場合は、RToWLAN 導入環境でモバイル ワーカーが必要とする適切な機能セットを提供するために、高度な機能（ロケーションおよびアベイラビリティ認識、Fixed Mobile Convergence、IP を介した音声およびビデオ、デュアルモード デバイス サポートなど）を提供するシステムが必要になります。

### WLAN を介した音声およびビデオ

RToWLAN ソリューションの導入を成功させるためには、適切に調整された QoS 対応のハイ アベイラビリティ WLAN ネットワークを計画して導入し、音声通話やビデオ通話とその他のリアルタイム トラフィック アプリケーションを有効にすることが非常に重要です。

802.11 RToWLAN エンドポイントは、重要なコール シグナリングと音声およびビデオのリアルタイム メディア トラフィックの両方を伝送するのに WLAN インフラストラクチャに依存しているため、データとリアルタイム メディア トラフィックの両方に最適化された WLAN ネットワークを導入する必要があります。 WLAN ネットワークの導入が適切でないと、多くの干渉が発生して

キャパシティが低下するため、RToWLAN アプリケーションおよびサービスのパフォーマンスが低下することにつながります。 音声通話やビデオ通話の事例では、コール品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする問題が発生する場合もあります。 アプリケーションのパフォーマンスが低下すると、コールの送受信や他のリアルタイム アプリケーションを使用するために WLAN 導入環境を使用できなくなります。

また、別の基本要件として、RToWLAN ソリューションの導入前、導入中、および導入後に WLAN 無線周波数（RF）のサイト調査を実施する必要があります。 これにより、RToWLAN アプリケーションおよびサービスをサポートするために、セル境界、構成および機能設定、キャパシティ、冗長性を最適化します。 サイト調査では、WLAN の RF 設計によって同一チャネル干渉が最小となっており、十分な無線信号レベルと非隣接チャネルのオーバーラップが提供されていることを確認する必要があります。これによって、RToWLAN エンドポイント デバイスが別のロケーションに移動したり、ローミングしたりする際に、十分なリアルタイム トラフィックのスループットと音声およびビデオ品質を維持できるようになります。

ワイヤレス インフラストラクチャが以下のコラボレーションおよびユニファイド コミュニケーション アプリケーションのネットワーク最小要件に準拠するように、適切なサイト調査と慎重なプランニングを行います。

- コラボレーションまたはその他の通信アプリケーション トラフィックの平均 IP パケット損失が 1 % 以下
- コラボレーションまたはその他の通信アプリケーション トラフィックの平均エンドツーエンド遅延変動またはジッタが 30 ミリ秒以下
- コラボレーションまたはその他の通信アプリケーション トラフィックの平均単方向パケット遅延が 150 ミリ秒以下

（注） 単方向の遅延が 150 ミリ秒を超える音声およびビデオ トラフィックを伝送しようとする RToWLAN ネットワークを実装すると、音声通話やビデオ通話の品質だけでなく、通話の確立やメディア カットスルー時間にも問題が発生します。 これらの問題は、通話を確立する際に各エンドポイントとコール制御プラットフォームの間でいくつかのコール シグナリング メッセージを交換する必要があるために発生します。

サイト調査と RToWLAN ネットワークの慎重なプランニングの実施によって、2.4 GHz の WLAN 帯域（802.11b/g/n）での導入を成功させることはできますが、RToWLAN エンドポイントの接続に対しては可能な場合 5 GHz の WLAN 帯域（802.11a/n/ac）を使用することを推奨します。 5 GHz の WLAN によって、2.4 GHz の WLAN よりも高密度なデバイスの導入が実現し、トラフィックのスループットをさらに最適化して干渉をより低減させることが可能です。 高密度、高スループット、低干渉は、音声通話やビデオ通話を含む RToWLAN アプリケーションおよびサービスの重要なネットワーク特性です。 加えて、Bluetooth ヘッドセットや他の Bluetooth 対応の周辺機器の普及によって、企業の 2.4 GHz WLAN への干渉を避けることは難しくなっています。 5 GHz の帯域を使用して RToWLAN を導入すれば、Bluetooth の干渉を懸念する必要がなくなります。

（注） デュアルバンド WLAN（2.4 GHz および 5 GHz の帯域の両方を使用する WLAN）では、RToWLAN エンドポイントが両方の帯域をサポートしている場合、同じ Service Set Identifier（SSID）を用いてデバイスが 802.11b/g/n と 802.11a/n の間でローミングすることが可能です。ただし、一部のデバイスでは、デュアルバンド WLAN によってリアルタイム トラフィック パスにギャップが発生する可能性があります。 これらのギャップを回避するには、リアルタイム トラフィック アプリケーションおよびサービスで 1 つの帯域だけを使用します。

### QoS

RToWLAN ソリューションの導入を成功させるために重要な 1 つのコンポーネントは、ネットワークおよびアプリケーション層で Quality of Service（QoS）を実装することです。 QoS では、ネットワークの通過時に、異なる種類のネットワーク トラフィックに対して帯域幅のうちの特定の量を割り当てたり、他のトラフィックよりも高い優先度を与えたりすることができます。 さまざまな方式を使用して、ネットワーク スループットの異なるレベルやトラフィック タイプに基づくアクセスを提供できます。

リアルタイム トラフィックでは、QoS 方式は次の 2 つのカテゴリに分類されます。

- パケット マーキング

  パケット マーキングは、パケットがトラフィック パスに沿ってネットワーク インターフェイスに入力および出力される際に、どのようにキューイングされるのかを決定します。 パケットマーキングに基づいて、特定の種類のトラフィックに対して多くの（または少ない）帯域幅を割り当てたり、または送信のスピードおよび頻度を変更することができます。一般に、リアルタイム メディア トラフィックはネットワークを通過するとき、ネットワーク パスに沿ったすべての送信キューで優先処理されます。 コールのセットアップやアプリケーション機能を補助するために使用されるリアルタイム シグナリング トラフィックは、このシグナリングや他のコントロール プレーン トラフィックの予測されるオーバーヘッドに基づいた専用の帯域幅を割り当てられます。 リアルタイム シグナリングと他の非メディア トラフィックは、優先トラフィック キューに割り当てる必要はありません。

- パケット キューイング

  パケット マーキングはアプリケーションまたはエンドポイント レベルで実行できる場合とそうでない場合がありますが、ほとんどの IP ネットワークでは、ネットワークを通過する際にトラフィック フローをマーキングまたは再マーキングすることができます。 ネットワークによるトラフィック フローのマーキングや再マーキングは、通常、IP ポート番号または IP アドレスに基づいています。 クライアント アプリケーションまたはデバイスは、特定のアプリケーション要件または標準のマーキング ガイドラインに基づいて、エンドポイント レベルでパケット マーキングを実行します（たとえば、音声メディアはレイヤ 2、802.11 WLAN、ユーザ優先度 6 としてマークされ、レイヤ 3 の IP パケット マーキングは、サービス クラス 5、DiffServ コード ポイント 0x46、または Per-Hop Behavior Expedited Forwarding となります）。

レイヤ 2（ユーザ優先度、つまり UP）での 802.11 WLAN パケット マーキングでは、さまざまな RToWLAN アプリケーションおよびエンドポイントの課題が生じます。 一部のアプリケーション

およびエンドポイントでは、標準ガイドラインに準拠したレイヤ 2 で RToWLAN トラフィック フローにマーキングする際に、多数のエンドポイントデバイス、特に多機能モバイルデバイスが、レイヤ 2 802.11 UP のマーキングをサポートしない場合があります。 エンドポイント デバイスが 802.11e および WMM に完全準拠し、オペレーティング システムがアプリケーションによるマーキングに従って UP 値をサポートしない限り、ワイヤレス ネットワークの RToWLAN トラフィック スループットを向上させるようにレイヤ 2 の QoS マーキングに依存することはできません。

レイヤ 3 のパケット マーキングは、RToWLAN アプリケーションおよびエンドポイントでさらに一般的です。 多数のアプリケーションとエンドポイントが、レイヤ 3 の RToWLAN トラフィック フローにマーキングします。 アプリケーションとエンドポイントが推奨ガイドラインに従ってトラフィックにマーキングする場合、既存の有線ネットワーク QoS ポリシーを変更する必要はありません。これは、リアルタイム トラフィックは自動的に標準 QoS ポリシー（ビデオおよびコントロールプレーン トラフィックに対する音声および専用帯域幅の優先処理）に基づいて適切に処理されるからです。

アプリケーションまたはエンドポイントによる正しいパケット マーキングは、重要である一方で、アプリケーションまたはエンドポイントによって正しいトラフィック タイプに適切なパケット マーキングが適用されていることも重要です。 RToWLAN エンドポイントで生成される一部のネットワーク トラフィックのパケット マーキングを信頼できない場合、管理者はすべてのトラフィックでネットワークベースのパケットの再マーキングを信頼するように決定できます。 この事例では、トラフィック タイプ（ポート番号またはプロトコル）と IP アドレスに基づく企業ポリシーに従ってすべてのトラフィックを再マーキングし、ネットワークの優先キューイングと専用帯域幅をトラフィック フローに適用します。一般則として、エンドポイントとそれらのデバイス上で実行しているアプリケーションを企業で完全に制御しているのでない限り、RToWLAN エンドポイントからのパケットマーキングを信頼すべきではありません。信頼できないデバイスやアプリケーションのパケットの再マーキングに加えて、管理者はネットワークベースのポリシングとレート制限を有効にし、信頼できないデバイスやアプリケーションがネットワーク帯域幅をあまり消費しないようにすることができます。

一部の導入環境では、RToWLAN エンドポイントが、RToWLAN アプリケーションおよびサービスを利用するために企業ネットワークに安全に接続されます。 これらの接続はインターネットを通過するため、IP パスにエンドツーエンドの QoS が存在しません。 すべてのパケット マーキングは無視されて、全トラフィックがベストエフォートとして処理されます。 これらのタイプの接続を介して RToWLAN アプリケーションのパフォーマンスを保証することはできません。

### セキュリティ

ワイヤレス エンドポイントを導入する場合は、ネットワークへのアクセス制御およびネットワーク トラフィック保護に使用されるセキュリティ メカニズムについて検討します。 ワイヤレス LAN インフラストラクチャおよび RToWLAN エンドポイントは、WPA、WPA2、EAP-FAST、PEAP など、広範囲の認証および暗号化プロトコルをサポートします。 一般に、ワイヤレス LAN を保護するために選択する認証および暗号化方式は、導入する WLAN インフラストラクチャと RToWLAN エンドポイントの両方によってサポートされる IT セキュリティ ポリシーと合わせる必要があります。

Proactive Key Caching（PKC）または Cisco Centralized Key Management（CCKM）などの高速キー再生成をサポートする認証および暗号化方式は、リアルタイム トラフィック ソリューションの導入にとって重要です。 これは、RToWLAN エンドポイントがネットワークのアクセス ポイントか

ら別のアクセスポイントにローミングする際、アクティブな音声通話やビデオ通話と他のRToWLANアプリケーションが接続と稼働状態を維持できるようにする必要があるからです。

その他にも、重要なセキュリティの考慮事項としてWLANネットワークへのシームレスな接続が挙げられます。 RToWLAN アプリケーションおよびサービスを最大限利用するために、エンドポイントはユーザの介入なしで WLAN ネットワークに自動接続する必要があります。 証明書ベースのID および認証は、ネットワーク接続におけるユーザの介入（最初のプロビジョニング後）を排除して認証遅延を最小化することで、優れたユーザエクスペリエンスを促進します。 ただし、企業のセキュリティ ポリシーが二要素認証やワンタイム パスワードを要求する導入環境では、ネットワーク接続にユーザの介入が必要です。 このような事例では、RToWLAN アプリケーションおよびサービスへのアクセスは遅延します。

### リモート セキュア接続

適切なセキュリティ インフラストラクチャと設定を用いると、802.11 RToWLAN エンドポイントは、パブリックまたはプライベート 802.11 WLAN ネットワークや Wi-Fi ホット スポットを使用して、リモート ロケーションから企業に接続できます。 これによって、リモート接続されたエンドポイントに RToWLAN アプリケーションおよびサービスを安全に配信できるようになりますが、これらのタイプのリモート接続を介して RToWLAN アプリケーションおよびサービスを配信するかどうかは検討する必要があります。

リモート セキュア接続を介して RToWLAN アプリケーションおよびサービスを有効にすると問題が多いのは、主に以下の 2 つの理由からです。

- 非企業の 802.11 WLAN

  カフェや空港で見られるホット スポットなどのパブリックおよびプライベート 802.11 WLAN ネットワークは、通常、リアルタイム トラフィック アプリケーションに最適化されておらず、エンタープライズクラスのセキュリティまたはパフォーマンスを配信しません。 非エンタープライズ クラスの 802.11 WLAN を介して、許容される RToWLAN ソリューションのパフォーマンス（音声およびビデオ品質、接続の信頼性など）を保証することはできません。

- インターネット トラバーサル

  リモート接続によってリアルタイム トラフィックが企業とエンドポイント間のインターネットを通過するため、音声およびビデオ品質などの RToWLAN アプリケーションのパフォーマンスは低下する場合があります。 インターネットを介した接続は保証されることはなく、常にベスト エフォートになります。 IP パスにエンドツーエンドの QoS は存在せず、すべてのパケット マーキングが無視されます。 全トラフィックはベスト エフォートとして処理されます。 このようなインターネットベースのネットワーク接続を介した場合、許容される RToWLAN ソリューションのパフォーマンスを保証することはできません。

### 関連トピック

Real-Time Traffic over WLAN の無線周波数設計, （25 ページ）
Real-Time Traffic over WLAN の QoS, （55 ページ）
Real-Time Traffic over WLAN のセキュリティ, （91 ページ）
Real-Time Traffic over WLAN のローミング, （105 ページ）

# RToWLAN ソリューションのハイ アベイラビリティ

ハイ アベイラビリティは、RToWLAN のプランニングや導入時に検討すべきもう一つの重要な事項です。 リアルタイム トラフィック アプリケーションおよびサービスの導入を成功させるための厳しいネットワークや無線周波数の設計要件とともに、WLAN インフラストラクチャおよびリアルタイム アプリケーション、サービス、エンドポイントの冗長性およびフェールオーバーについても検討する必要があります。

ハードウェアやサービスの障害が起こった場合でも、ネットワーク エッジからデータセンターを経由しすべてのロケーションに至るまでの、企業のネットワーク インフラストラクチャ内の IP パスを維持できるように、冗長性を備えた配置で有線ネットワーク インフラストラクチャを実装する必要があります。 冗長な物理ネットワーク接続と適切なネットワーク ルーティングおよびスイッチング設定により、コール制御プラットフォームや他のアプリケーション サーバなどの RToWLAN コンポーネントのハードウェア部分は、ネットワークのコンポーネントまたはネットワークの一部を使用できない場合でも、ネットワーク上で通信が可能となります。

アクセス ポイント、ワイヤレス LAN コントローラ、または認証システムに障害が発生するシナリオでも、エンドポイントのネットワーク接続の継続性を確保できるように、WLAN インフラストラクチャを障害復元力のある方法で導入する必要があります。 可用性の高いネットワーク接続を提供することで、隔離されたインフラストラクチャが停止した場合でも、リアルタイム アプリケーションおよびサービスは機能を継続することができます。

同様に、リアルタイム トラフィック アプリケーションおよびサービスと、そのサービスを提供するエンドポイントは、ハイ アベイラビリティである必要があります。 シスコのコール制御機能によって提供されるリアルタイムの音声およびビデオ サービスの場合、プライマリのコール制御プラットフォームに障害が発生した際に、他のプラットフォームまたはコンポーネントがこれらのサービスをエンドポイントやそのユーザに継続して提供できることが必須条件となります。 ネットワーク サービスの冗長性に加えて、エンドポイントとそれらで実行されるリアルタイム トラフィック アプリケーションは、自動的にバックアップ サービス ノードにフェールオーバーして動作を継続できる必要があります。

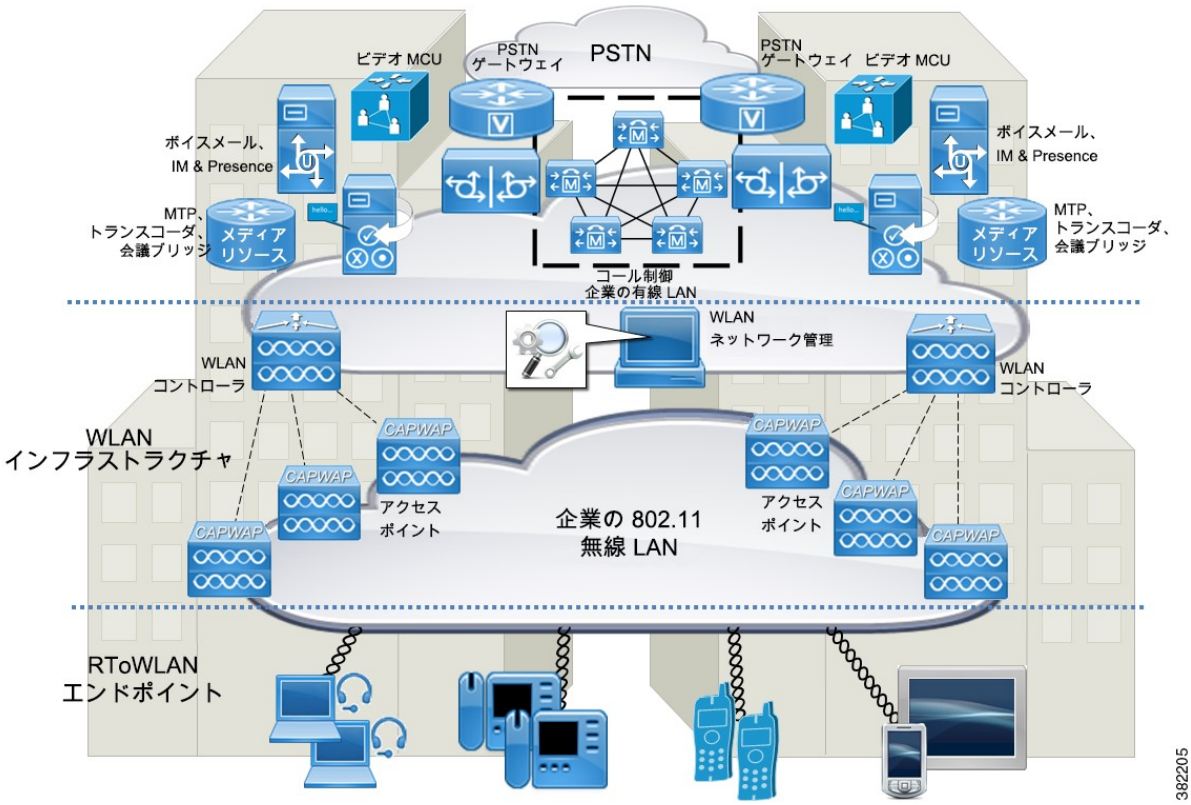
RToWLAN ソリューション導入におけるハイ アベイラビリティの考慮事項により、企業のネットワークまたは導入環境の物理的な特性が必要となる場合もあります。

### 単一サイトまたはキャンパスへの RToWLAN 導入

単一サイトまたはキャンパスへの導入では、単一のロケーション内、または非常に近距離にある一群のロケーション内で RToWLAN ソリューションの実装および運用を行います。 この導入で最初に考慮すべき事項は、ネットワーク接続と音声通話やビデオ通話などの RToWLAN サービスに障害復元力を提供することです。

図 3： RToWLAN の単一サイト導入, （19 ページ） に、RToWLAN ソリューション全体のハイ アベイラビリティを確保するために重要なコンポーネントやサービスの重複を利用している、単一サイトまたはキャンパスへの導入を示します。

**図 *3*： *RToWLAN* の単一サイト導入**




（注） 図には有線ネットワーク インフラストラクチャの冗長性が示されていませんが、それが存在することは前提である必要があります。

また、キャンパス ロケーションの 2 つの建物間に存在する分散データセンターも示しており、次の重要なコンポーネントやサービスがすべて冗長構成となっています。

- ワイヤレス ネットワーク コンポーネント：複数の WLAN コントローラとアクセス ポイント。

  冗長なワイヤレス ネットワーク インフラストラクチャ コンポーネントを導入して、RToWLAN エンドポイントのワイヤレス ネットワーク接続がハイ アベイラビリティになるようにします。 また、ロケーション内で固定されている場合と移動またはローミングする場合の両方で、ネットワークベースの RToWLAN アプリケーションおよびサービスにデバイスが継続的にアクセスできるようにします。

- コラボレーション コンポーネント：複数のコール制御プラットフォームまたはノード、メディア リソース（会議ブリッジ、メディア制御ユニットなど）、PSTN ゲートウェイまたはボーダー コントローラ、アプリケーション サーバ。

  冗長なコール制御プラットフォーム、メディア リソース、PSTN 接続、アプリケーション サーバを導入して、RToWLAN アプリケーションおよびサービスがハイ アベイラビリティになり、RToWLAN エンドポイントがこれらのアプリケーションおよびサービスを継続的に使用できるようにします。

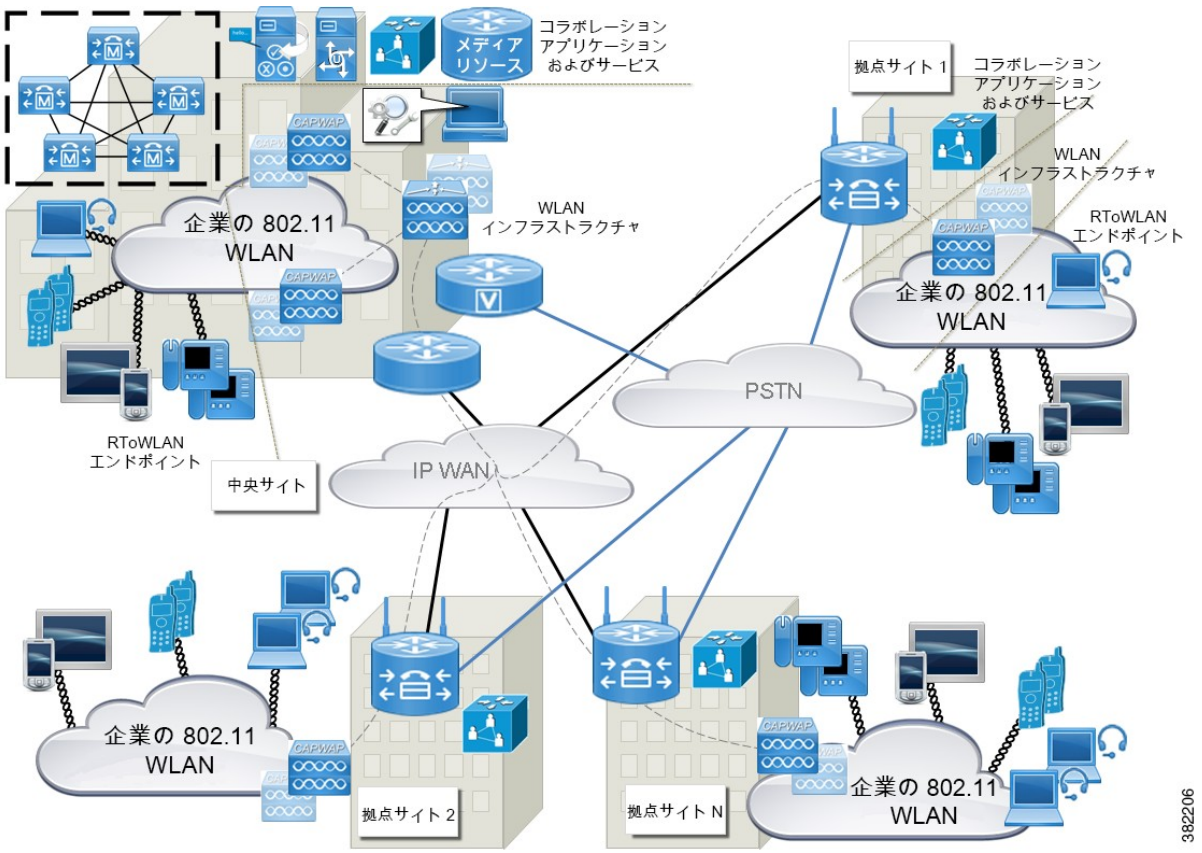
### RToWLAN の分散導入

分散導入では、複数のサイトやロケーションで RToWLAN ソリューションの実装および運用を行い、RToWLAN デバイスはネットワーク全体に分散します。 これらのタイプの導入では、ネットワーク接続と音声通話やビデオ通話などの RToWLAN サービスに障害復元力を提供することが、依然として最初に考慮すべき事項となります。 ただし、サイトの相互接続性に関しては、分散導入に特有な考慮事項があります。

図 4： RToWLAN の分散導入, （21 ページ） は分散導入を示しています。企業全体で永続的なネットワーク接続と RToWLAN アプリケーションおよびサービスへの永続的なアクセスを提供す

るために、重要なWLANおよびコラボレーション コンポーネントとサービスは、各サイトでローカルに冗長構成とする必要があります。

**図 *4*： *RToWLAN* の分散導入**




アクセス ポイント（AP）は、密度およびサイト調査の要件に基づいて、企業全体で冗長に導入されています。 ワイヤレス LAN コントローラ（WLC）の場合、次の 2 つのハイ アベイラビリティ導入オプションがあります。

- 中央サイトの WLC は、すべてのロケーションで AP の制御と管理を行い、集中的な管理および制御を提供します。

  拠点サイトと中央サイト間でIPネットワークの障害が発生した場合、拠点サイトのローカル AP がローカルの RToWLAN エンドポイント デバイスへのサービスの提供を継続し、中央サイトからクレデンシャルをキャッシュしてネットワーク接続と認証サービスを提供します。このタイプのハイ アベイラビリティ方式は、AP とワイヤレス デバイスの数が制限されたより小さな拠点サイトにとって最適に機能します。

- 各拠点サイトに導入されたローカル WLC は、ローカル サイトで AP の制御と管理を行います。

  拠点サイトと中央サイト間でIPネットワークで発生した場合は、すべてのWLANネットワーク サービスはローカルで提供を継続します。 また、このタイプの導入では集中型の認証サー

ビスを利用することも可能です。ローカル サイトの WLC が中央サイトからクレデンシャルをキャッシュし、IP ネットワークの停止中にローカル認証サービスを提供します。 このタイプのハイ アベイラビリティは、多数の AP とワイヤレス デバイスを使用するより大きな拠点サイトに適しています。 分散 WLC またはローカル WLC の場合においても、ほとんどの導入環境で、WLAN ネットワーク管理コンポーネントおよびアプリケーション全体は通常、中央集中的な構成を維持します（図 4： RToWLAN の分散導入, （21 ページ）を参照）。

（注） 拠点サイトのサイズがそれぞれ異なり、各ロケーションで必要なサービス レベルが異なるような導入環境では、ハイブリッド型の導入を行うことが可能です。一部のロケーションではワイヤレス AP の集中的な管理や制御を利用し、他のロケーションでは分散的な制御やローカル制御を利用します。

図 4： RToWLAN の分散導入, （21 ページ）に、両方の WLC ハイ アベイラビリティ導入オプションを示します。 中央サイトの WLC と、拠点サイトの AP を含むすべての AP との間に描かれたグレーの破線は、集中型の WLC 制御を表しています。 各拠点サイト ロケーションのルータは、ローカル WLC 機能（ワイヤレス アンテナによって示されています）を提供できます。

RToWLAN アプリケーションおよびサービスへの永続的なアクセスを提供するには、コラボレーション コール制御プラットフォームと他のコンポーネントも、各企業サイトで冗長構成にする必要があります。 図 4： RToWLAN の分散導入, （21 ページ）には、各拠点サイトの音声対応ルータとメディア制御ユニット（MCU）によって示されるように、コール制御、PSTN 接続、メディア リソースなど、重要なコラボレーション コンポーネントの冗長構成が示されています。 分散導入で WLC のハイ アベイラビリティを実現できるように、コラボレーション コール制御を中央サイト内で集中化するか、またはすべてのロケーションに分散することもできます。 図 4： RToWLAN の分散導入, （21 ページ）には、拠点サイトと中央サイト間で IP ネットワークの障害が発生した場合の、集中型のコール制御と、各拠点サイトで提供される分散型のバックアップ コール制御が示されています。

RToWLAN 導入と分散マルチサイト導入において重要となるもう 1 つの考慮事項は、RToWLAN デバイスのモビリティです。 マルチサイト導入では、ほとんどの RToWLAN エンドポイントのモバイル特性により、ロケーション間の移動は一般的です。 RToWLAN エンドポイントが企業サイト間を移動するときに、コラボレーション コール制御プラットフォームでそのロケーションを動的に追跡する必要があります。 デバイスの IP アドレスまたは他の識別情報に基づいて、コール制御アプリケーションがデバイスのロケーションを測定し、必要に応じて、コール ルーティング、PSTN 出力ポイント、コーデックおよびメディア リソースの選択を調整する必要があります。

RToWLAN の分散導入で重要となるもう 1 つの考慮事項は、コール アドミッション制御です。コールアドミッション制御は、コラボレーションコールの制御機能です。音声通話またはビデオ通話のトラフィックによって企業サイト間の帯域幅がオーバーサブスクライブされないようにします。 サイト間の接続で帯域幅のオーバーサブスクリプションが発生すると、音声およびビデオの品質低下、コールのセットアップの遅延、さらにはコールの切断の原因にもなります。 通常は速度が遅い企業サイト間のリンクで、利用できる帯域幅とスループットを制限すると、コール アドミッション制御では、品質の高い音声通話またはビデオ通話をセットアップして維持するために、IP パスで十分な帯域幅が利用できるようにします。 十分な帯域幅が利用できない場合、コール制御システムはコールのセットアップを拒否するか、ローカル サイトの PSTN 接続を使用して

コールを再ルーティングします。 コール アドミッション制御は、RToWLAN に固有のものではありませんが、分散マルチサイト コラボレーション導入における重要な考慮事項となります。

# RToWLAN ソリューションのキャパシティ プランニング

RToWLAN 導入の拡張性は、リアルタイム トラフィック アプリケーションおよびサービスを実装する場合、設計における主要な考慮事項となります。 ネットワークおよびコール処理に十分なキャパシティを提供できないと、エンドポイントによる関連付け、認証、登録、音声通話やビデオ通話の送受信、または他のコラボレーション アプリケーションの利用を妨げるようなサービスおよび機能の停止が発生する場合があります。

エンドポイントが WLAN にアクティブに接続して高品質な音声通話やビデオ通話を実現するには、WLAN インフラストラクチャは十分なクライアント接続と帯域幅のキャパシティを提供する必要があります。 とりわけ、WLAN チャネル セルあたりの音声またはビデオの同時双方向トラフィック ストリームの数は、キャパシティに関する重要な考慮事項であり、関連付けるエンドポイントの数とともに、導入されるデバイスの密度と潜在的なユーザ コールのレートを最終的に決定します。

WLAN インフラストラクチャのエンドポイントと帯域幅のキャパシティのほかに、コラボレーション システムの機能のキャパシティについても検討する必要があり、これによってリアルタイム トラフィック アプリケーションおよびサービスが有効になります。 シスコのコール制御機能では、各コール制御プラットフォームまたはノードに、決められたエンドポイントおよびコール ボリュームのキャパシティが存在します。 同様に、メディア リソース プラットフォームと MCU にも、決められたコールまたはセッションのキャパシティが存在します。 必要な数の RToWLAN エンドポイント ユーザにサービスを提供するには、適切な数のコール制御アプリケーション ノードを追加して、十分なエンドポイントとコール ボリュームのキャパシティを導入する必要があります。

第 2 章

# Real-Time Traffic over WLAN の無線周波数設計

この章では、RToWLAN 導入における無線周波数（RF）の計画および設計の全般的な考慮事項について説明します。 RF の計画および設計の考慮事項に影響を及ぼすそれ以外のポイントは、エンドポイントの機能、ローカルの条件、規制です。 この章では、一般的な導入シナリオについて説明し、RF に関連するプロセスと考慮事項を解説します。



## ハイ アベイラビリティ

ハイ アベイラビリティ（HA）は、RToWLAN を含むシステムの計画を検討する際の重要なポイントです。 RToWLAN導入では、有線ネットワークで使用する同じHA戦略をRToWLANソリューションの有線コンポーネントに適用することができます。 検討する必要がある RToWLAN のアベイラビリティに固有のポイントは、RF カバレッジの HA、つまり、単一の WLAN 無線に依存しない RF カバレッジを提供することです。 RF の HA を提供する主要なメカニズムは、セル境界のオーバーラップ です。

20 % のオーバーラップは、推奨信号レベルにおいて特定のアクセス ポイント（AP）セルの 80 % が他の AP によってもカバーされるということを意味します。そのセルの RToWLAN コールでそれ以外の 20 % の品質が低下しても、利用は可能です。 Cisco Unified Wireless Network のカバレッジ ホール アルゴリズムは、RF の HA のカバレッジを増幅します。WLAN クライアントで SNR（信号対雑音比）の値が悪化し、SNR の問題を修正するために AP の電力レベルが増大している状態を検出します。

（注） カバレッジ ホール アルゴリズムを使用した導入計画では、ホールを調整するため AP が電力レベルを増大させているかを考慮する必要があります。 そのため、AP の最大電力よりも低い可能性がある RToWLAN エンドポイントの最大電力を、AP の初期電力レベルを設定する際に考慮する必要があります。

**関連トピック**

カバレッジ ホール アルゴリズム, （27 ページ）

# キャパシティ プランニング

キャパシティ プランニングは、RToWLAN の計画におけるもう 1 つの重要なパラメータです。コール キャパシティは、エリアでサポートできる RToWLAN の同時コール数です。 このコール数は、RF 環境、RToWLAN エンドポイントの機能、WLAN システムの機能によって変化する場合があります。

特に、WLAN を介して送信されるメディアの一部がビデオの場合は、RToWLAN の設計で 5 GHz のスペクトル チャネルを使用することを強く推奨します。

次の表に、ベスト ケースのシナリオとして 3 つの例を示します。最適化された WLAN サービス（Cisco Unified Wireless Network など）を提供する WLAN をエンドポイントで使用する場合の、ビデオ通話に対するアクセス ポイントまたはチャネルあたりのおおよその最大キャパシティです。 これらの例では、802.11n WLAN 標準の 5 GHz チャネル（Bluetooth なし、チャネル ボンディングなし）を使用する RToWLAN について検討します。

**表 *3*：*WLAN* を介したビデオ通話のキャパシティ**

| 同時双方向ビデオ通話の推定最大数 | 解像度/ビット レート | WLAN 標準 | データ レート/MCS インデックス |
|---|---|---|---|
| 7 | H.264 720p/2500 Kbps | 802.11n | MCS 7（40 MHz チャネル） |
| 4 | H.264 720p/2500 Kbps | 802.11n | MCS 4（40 MHz チャネル） |
| 1 | H.264 720p/2500 Kbps | 802.11n | MCS 1（40 MHz チャネル） |
| 16 | H.264 360p/400 Kbps | 802.11n | MCS 7（40 MHz チャネル） |
| 12 | H.264 360p/400 Kbps | 802.11n | MCS 4（40 MHz チャネル） |

| 同時双方向ビデオ通話の推定最大数 | 解像度/ビット レート | WLAN 標準 | データ レート/MCS インデックス |
|---|---|---|---|
| 8 | H.264 360p/400 Kbps | 802.11n | MCS 1（40 MHz チャネル） |

5 GHzのスペクトルは低ノイズと低干渉が特長であるため、より高いキャリア周波数の実装では、キャパシティがより大きくなる可能性があります。5 GHzのスペクトルで利用できる追加の非オーバーラップ チャネルによって、特定エリアのコール キャパシティも向上します。 さらに、ビデオの 40 MHz チャネルはキャパシティを増やせるので、これを使用することを推奨します。 これらのおおよその最大数は、特定の環境ノイズ、カバレッジ、減衰、Bluetooth 使用率、チャネル使用率、該当エンドポイントがサポートする空間ストリームの数、セルにおけるクライアントの混在によって変化することも考慮してください。

次の表に、最適された WLAN サービスを提供する WLAN をエンドポイントで使用する場合の、音声通話に対するアクセス ポイントまたはチャネルあたりのおおよその最大キャパシティとして例を 2 つ示します。 これらの例では、802.11a WLAN 標準の 5 GHz チャネル（チャネル ボンディングなし）を使用する RToWLAN について検討します。

**表 *4*：*WLAN* を介した音声通話のキャパシティ**

| 同時双方向音声通話の推定最大数 | オーディオ コーデック/ビット レート | WLAN 標準 | データ レート |
|---|---|---|---|
| 20 | G.711-G.722/64 Kbps | 802.11a | 12 Mbps |
| 27 | G.711-G.722/64 Kbps | 802.11a | 24 Mbps 以上 |

（注） ここでは、AP 数ではなくチャネル キャパシティが制限要因となるため、上述のコール キャパシティは、非オーバーラップ チャネルあたりの値になります。 これらのコール キャパシティの最大数は、一般的なプランニングの目的に応じて決定されます。 導入時には実際のRToWLAN エンドポイントによって指定されるコール キャパシティを使用する必要があります。この値がそのエンドポイントでサポートされるキャパシティであるためです。 また、5 GHzの帯域を利用する場合は、40 MHzのチャネルを使用することを推奨します。 コール キャパシティのプランニングで正確な値を決定するための詳細については、エンドポイントのマニュアルを参照してください。

# カバレッジ ホール アルゴリズム

プランニングにおいてカバレッジホールアルゴリズムを使用する導入計画では、ホールを調整するためにAP が電力レベルを増大させるかどうかを考慮する必要があります。 そのため、AP の最

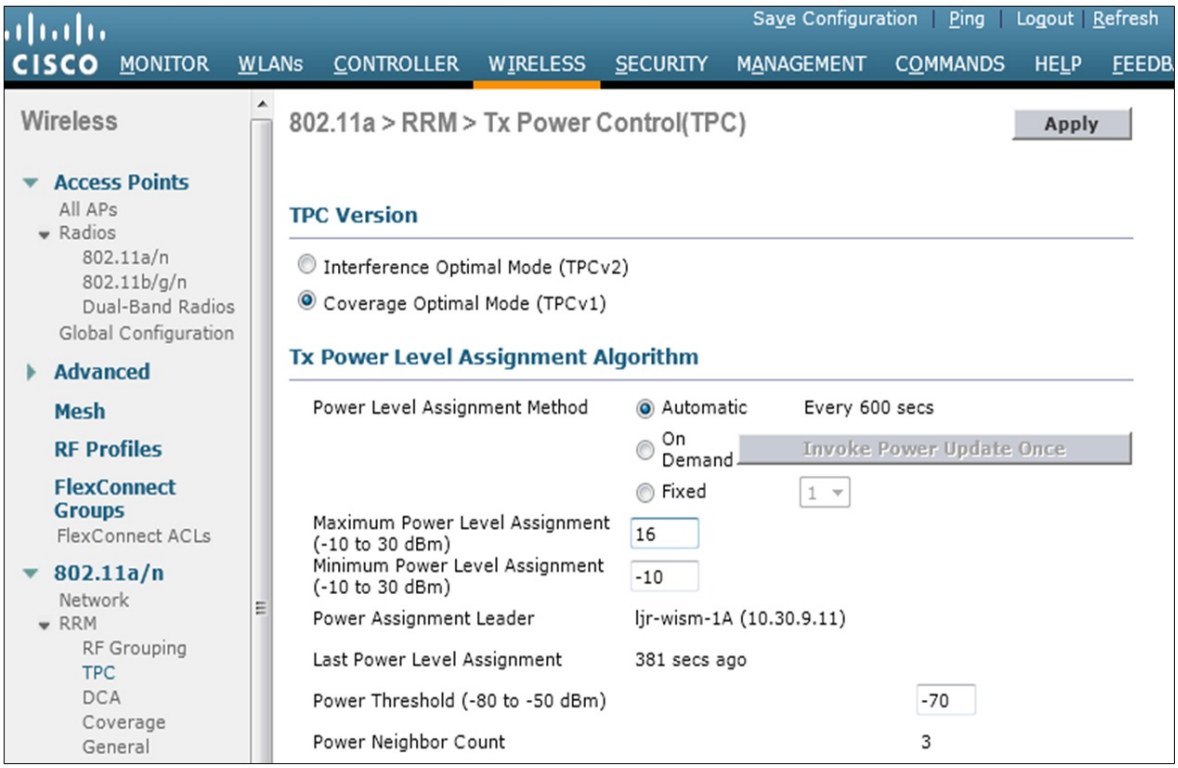
大電力よりも低い可能性がある RToWLAN エンドポイントの最大電力について、AP の初期電力レベルを設定する際に検討する必要があります。 たとえば、RToWLAN エンドポイントの最大電力レベルが 16 dBm、AP の初期電力レベルが 16 dBm である場合、RF ホールをカバーするために AP の電力レベルを上げても、そのホール内の RToWLAN クライアントの助けにはなりません。これは、RToWLAN では、これ以上電力レベルを上げて AP からの増大した電力を補うことはできないからです。 この例では、ホール カバレッジを有効にするため、AP の初期電力レベルを 13 dBm 以下にし、RF ホールをカバーするために AP および RToWLAN の両方で電力を上げる十分な余地を残しておく必要があります。

メディアリッチ アプリケーションとリアルタイム アプリケーションをサポートする設計目的で AP を配置する場合、AP 数が通常の密度から高密度へ相対的に変化します。 リモート管理モジュール（RMM）の電力レベル割り当てがレベル 3 および 4 である場合は中密度、電力レベル 5 ～ 8 の場合は高密度になります。 RMM により電力レベル 1 または 2 が割り当てられるような AP の配置の場合、そのカバレッジの密度は高いとは考えられません。 AP の電力レベルが 1 であると、ネットワークから切断された AP の周囲にある AP は電力を増大させることができません。また、オフラインになっている AP により作られたホールをカバーすることもできません。 周囲の AP の電力レベルが 2 である場合は、その周囲の AP の電力レベルが 1 まで増大します。

最小密度を形成することが設計の目的である場合は、設置される実際の AP とアンテナを用いて、調査プロセスと初期カバレッジ評価を実行する必要があります。 それから、RMM の最大送信電力（dBm 単位）を、最も弱いクライアントの最大送信電力に設定します。 AP の初期配置では、そのカバレッジエリアが最も弱いクライアントのカバレッジエリアより大きくならないようにする必要があります。 AP のカバレッジがクライアントのカバレッジに一致するように、RRM の dBm 値を最も弱いモバイル クライアントの dBm 送信電力と同一に設定します。

次の図に、Cisco WLAN の伝送パワー コントロール設定を示します。

**図 5**：カバレッジ ホール アルゴリズムの伝送パワー コントロール




802.11g、802.11a、802.11n、または 802.11ac を使用するすべてのクライアントは、クライアント リンクのダウンストリームと最大比合成（MRC）のアップストリームを活用します。これは、クライアントあたりの動的 Wi-Fi 信号の品質が向上し、AP 停止によるカバレッジ ホールが存在する場合に効果的である可能性があります。

# 設計上の考慮事項

ここでは、RToWLAN を使用するワイヤレス エンドポイントの RF カバレッジを設計する場合に検討する必要がある重要な要素について説明します。

### リッチ メディアの一般的な AP ガイドライン

リッチ メディアのパケット損失やジッタの要件と RToWLAN エンドポイント ユーザのモビリティ向上により、通常の WLAN データ導入環境以上の接続品質とカバレッジが要求されます。新しい世代の WLAN 機器やソフトウェアを利用すれば RToWLAN をさらに向上させることはできますが、RToWLAN の導入を成功に導く基盤としては、無線周波数の計画、設計、実装が大きな要素となります。RToWLAN の導入を成功させるには、WLAN の RF 環境を設計、計画、実装、運用、維持することが重要です。WLAN データ導入で使用されるプロセス、ガイド、ヒューリスティック、ツールは、RToWLAN 導入の成功には役立ちません。

最適な RToWLAN ネットワークの一般的な RToWLAN ガイドラインは、次のとおりです。

- セル オーバーラップは最低 20 %、医療機関などでの重要な通信ではオーバーラップは約 20 ～ 30 %、WLAN データ設計では AP セル オーバーラップは 5 ～ 10 % で可。
- -67 dBm のセル境界。

（注） RToWLAN の設計では 5 GHz のスペクトル チャネルを使用することを強く推奨します（特に、WLAN を介して送信されるメディアの一部がビデオの場合）。 可能であれば、20 MHz の代わりに 40 MHz チャネルを使用してください。

- 802.11n AP プラットフォームを使用する場合は、ClientLink/ビームフォーミングを使用して WLAN パフォーマンスを最適化します。
- 音声およびビデオ導入のパフォーマンスを最適化するために、12 Mbps 未満のデータ レートを無効にする必要があります（MCS 0 など）。

（注） RToWLAN エンドポイントの RF 特性はさまざまであり、WLAN の設計やキャパシティに大幅な影響を及ぼすことがあります。 ここに記載されている内容と一致しない RF 導入要件に従って RToWLAN エンドポイントの導入を計画する場合は、エンドポイントのガイドラインに従う必要があります。 エンドポイントの推奨事項はさまざまですが、ここに記載されている一般的な原則とポイントはセルのサイズが変わっても引き続き適用できます。

### 2.4 GHz のネットワーク設計

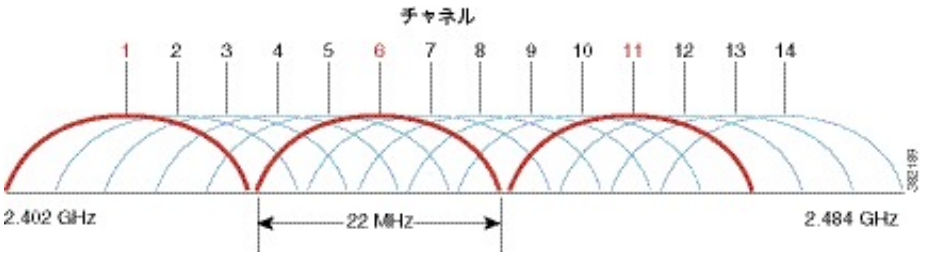
RToWLAN の設計では 5 GHz のスペクトル チャネルを使用することを推奨します。

IEEE 802.11b/g チャネル セットでは、合計で 14 チャネルを定義しています。 各チャネルの帯域幅は 22 MHz ですが、チャネルの間隔は 5 MHz のみです。 このことによりチャネルがオーバーラップし、隣接チャネルからの信号は互いに干渉することがあります。

14 チャネル DS システム（米国では 11 チャネルを使用可能）では、非オーバーラップ（非干渉）チャネルは 1、6、および 11 チャネルの 3 つのみです（それぞれの間隔は 25 MHz）。 このチャネル間隔により、マルチ AP 環境（オフィスやキャンパスなど）でのチャネルの使用や割り当てを

管理します。通常は、企業内にセルラー方式でAPが導入され、隣接APは非オーバーラップチャネルに割り当てられます。 2.4 GHz チャネルの割り当てを示す次の図を参照してください。

**図 *6*： *2.4GHz* チャネルの割り当て**




IEEE 802.11b は、1、2、5.5、11 Mbps のデータ レートを提供します。 IEEE 802.11g は、2.4 GHz の帯域で 6、9、12、18、24、36、48、54 Mbps のデータ レートを提供し、IEEE 802.11b とスペクトルは同じです。 IEEE 802.11g には IEEE 802.11b との下位互換性があります。単一の AP で IEEE 802.11b および IEEE 802.11g クライアントの両方に WLAN アクセスを提供します。

### 同一チャネル干渉の考慮事項

前述したように、米国の 2.4 GHz スペクトルの非オーバーラップ チャネルは 3 つのみです。 そのため、AP を導入しようとする場合に、同じチャネル上の AP がそのチャネル上の他の AP から信号を受信しないようにすることは困難です。 サポートするクライアント ビット レートとともに AP カバレッジ半径が変化し、この半径で作られる境界が AP 境界と見なされます。

実際には、AP はビット レート境界よりもはるかに大きい距離で AP 周囲の WLAN RF 環境に影響を及ぼすため、同一チャネル干渉は複雑になります。 これは、AP からの RF エネルギーの強さが、WLAN フレームに復調できるほどではありませんが、IEEE 802.11 無線の送信の遅延の原因となるには十分なためです。 RF 環境への AP の影響に加えて、AP にアソシエートしたクライアントは、AP セルにアソシエートした RF エネルギーの範囲をさらに拡張します。

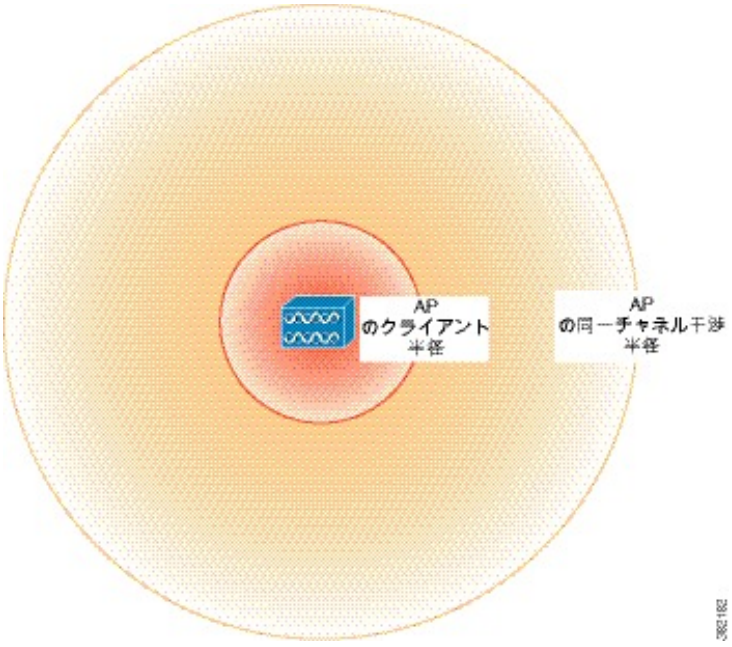
IEEE 802.11 の MAC は、キャリア検知多重アクセス/衝突回避（CSMA-CA）アルゴリズムであり、IEEE 802.11 フレームを送信しようとする前にキャリア検知が Clear Channel Assessment（CCA）を実行します。 CCA のメカニズムは、IEEE 802.11 の各物理層に対して指定されます。単純なそのままのエネルギー レベル、物理層コンバージェンス プロトコル（PLCP）ヘッダーの電力レベル、またはキャリア検知のいずれかによってトリガーされます。 IEEE 802.11 無線の CCA は使用されるビット レートとともに変化せず、一般に、ユーザが設定することはできません。

AP の WLAN の一部ではない IEEE 802.11 無線が AP の WLAN に及ぼす CCA 遅延の影響は、同一チャネル干渉と呼ばれます。 同一チャネル干渉はフレームの送信に遅延をもたらすため、RToWLAN コール中のジッタと遅延が増加します。 WLAN QoS は WLAN トラフィックを優先度付けしますが、これは CCA 後に発生するため、優先度付けによって CCA に起因するジッタと遅延を回避することはできません。

RToWLAN エンドポイントには、-67 dBm の電力レベル境界と、-86 dBm の隣接 AP チャネル間の間隔が必要です。 -67 dBm の要件により、パケット損失を最小化し、-86 dBm の要件により、隣接チャネル セル間の間隔を空けて同じチャネル上の他の AP セルによる同一チャネル干渉を最小化できます。

次の図に、オープン オフィス環境の標準的な RF 損失の式に基づいて、-67 dBm および -86 dBm の要件から作成される 2 つの境界の例を示します。

**図 7**：***AP*** **のビット レートと同一チャネル干渉の境界**



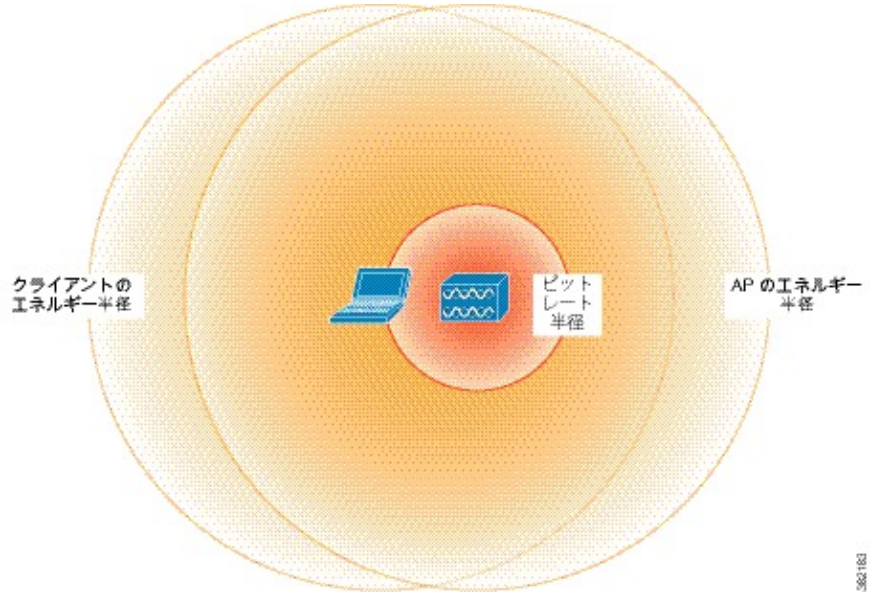

この RF 環境では、AP のクライアント半径は 43 フィートとなり、標準アンテナ ゲイン（2 dB）および 16 dBm の AP 出力電力（40 mW）を使用している場合、AP の同一チャネル干渉は 150 フィートとなります。 異なる RF 環境、AP 電力、アンテナによってクライアントと同一チャネル干渉の半径は異なりますが、ここに記載されている原理は引き続き適用できます。

（注） AP に対して選択する出力電力は、RToWLAN エンドポイントの機能や導入要件に合わせる必要があります。 たとえば、9971 のコラボレーション エンドポイントでは、802.11a を使用する場合 40 mW（16 dBm）の最大出力電力が必要です。 802.11a を使用する場合、9971 のコラボレーション エンドポイントの導入環境では、40 mW を超える AP 電力を使用する必要はありません。 AP の停止時に RToWLAN カバレッジを提供する Cisco Unified Wireless Network のホール カバレッジ メカニズムでは、AP が RF ホールをカバーでき、RToWLAN エンドポイントに対して適切な範囲で動作するように、AP のプランニングで使用する AP 電力を 40 mW 未満とする必要があります（9971 のコラボレーション エンドポイントを使用する場合など）。

より低い AP 送信電力を使用するもう一つの利点は、同一チャネル干渉の半径がそれに比例して減少することです。 上の例では、40 mW（16 dBm）の送信電力で、同一チャネル半径が 150 フィート、クライアント半径が 43 フィートとなります。 電力が 20 mW（13 dBm）まで減少すると、同一チャネル半径は 130 フィート、クライアント半径は 38 フィートまで減少し、さらに AP によって生成される同一チャネル干渉に比例して、同一チャネル干渉も減少します。

AP の RF 同一チャネル干渉半径と WLAN クライアントは、同一チャネルの干渉に影響を及ぼします。 次の図を参照してください。

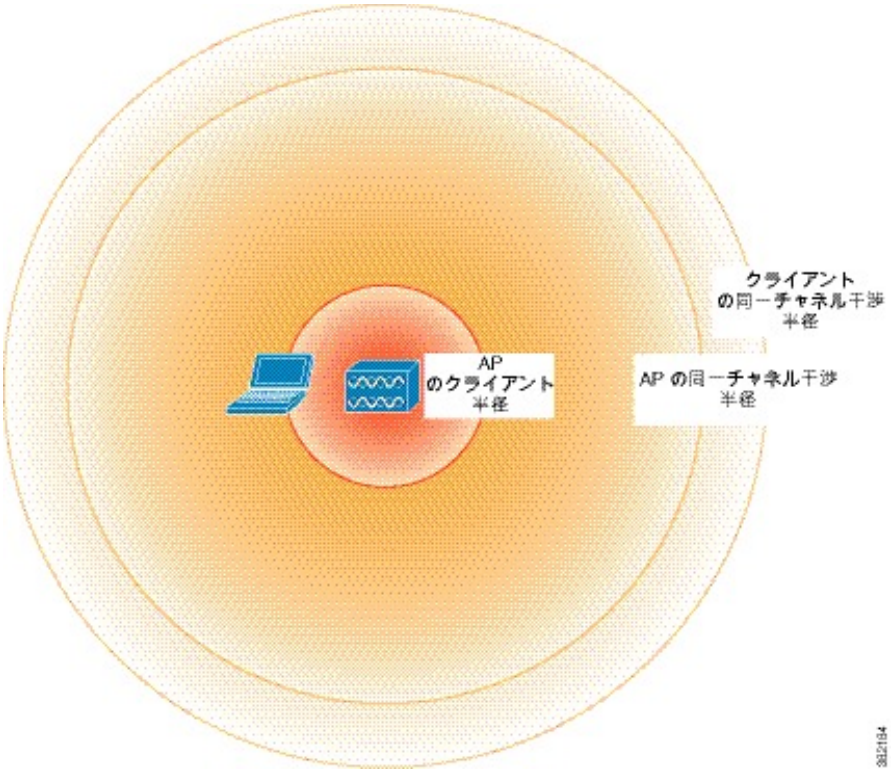
**図 *8*：単一クライアントの同一チャネル干渉半径**




次の図はクライアントの同一チャネル干渉を分かりやすく示しています。ビット レート半径の境界内の任意の場所に 1 つ以上のクライアントを配置することができます。 前述した計算による 43

フィートのビット レート半径と 150 フィートの AP の同一チャネル干渉半径では、新しいクライアントの同一チャネル干渉半径が 193 フィートになります。

**図 *9*：クライアント全体の同一チャネル干渉半径**




（注） WLAN クライアントは通常、AP と同じロケーションに存在せず、障害物によって信号が大きく減衰する可能性が高いため、193 フィートの半径はワースト ケースに近い状況を表しています。

### 同一チャネル干渉に対するビット レートの影響

この例における AP のクライアント半径では、RToWLAN エンドポイントの通常のビット レートは、ノイズに応じて約 24 Mbps 以上となります。 ビット レートを下げて AP のクライアント半径をさらに拡張することができます。 しかし、この方法は次の理由から推奨されません。

- ビット レートを下げると AP のクライアント半径は拡張されますが、クライアントの同一チャネル干渉半径も拡大し、RToWLAN コール キャパシティが AP 1 台分のみのエリアが増加します。 また、ビット レートを下げると、ビデオ通話の品質が低下します。
- ビット レートを下げると、全体のコール セル キャパシティが低下します。これは、低いビット レートのパケットは多くの時間を消費し、送信パケット数が減少するためです。

RToWLAN コールの品質はデータ レート変化の影響を受けます。 通常、データ レートを変化させると、以前に使用していたデータ レートでフレームを送信できなくなります。データ レートを変更するかどうかは、フレームの確認応答を受信することなく複数回フレームを送信した場合に決定されます。 これにより、RToWLAN コール中の遅延やジッタが増加します。

最初の送信を成功させるために、一部のクライアントではトラフィック ストリーム レート セット（TSRS）の IE を利用して、有効なデータ レートのサブセット（12 ～ 24 など）を使用することができます。

### 20 % のセル オーバーラップ

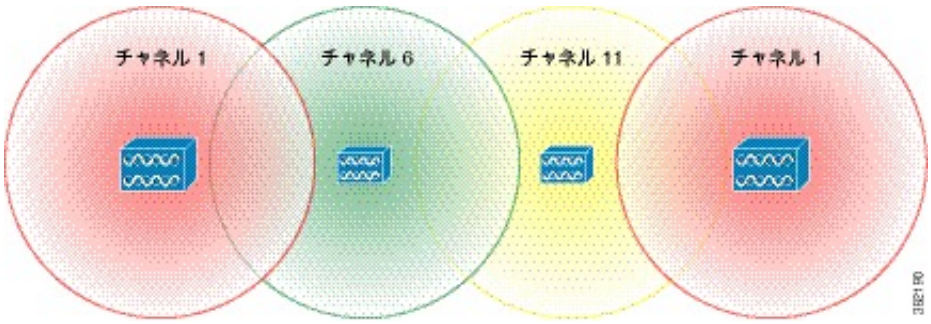
RToWLAN の導入では、最低 20% の AP セル オーバーラップを使用することを推奨します。 これにより、セル境界に近い場合、RToWLAN エンドポイントは代替 AP を検出して接続できるようになります。 特定の RToWLAN クライアントのセル境界でのデータ レートの変更と再送信の量を最小化することで、コールの中断は最小限に抑えながら RToWLAN クライアントの AP のアソシエーションを変更することもできます。

20 % のオーバーラップ要件は、セル境界によって示される 70 フィートの 2 倍の距離よりも AP を互いに近付けて配置することを意味します。 2 つの円のオーバーラップ エリアの半径は 1 になります。 d は各円の中心間の距離です。 20 % のエリアでは、標準半径が 1 の場合の d の値は 1.374、境界が 67 dBm の場合は AP 間が 59 フィートになります。

（注） その他のよく使用される距離の値は、10 %（1.611）、15 %（1.486）、25 %（1.269）、30 %（1.198）です。

次の図に、20 % の AP オーバーラップを示します。

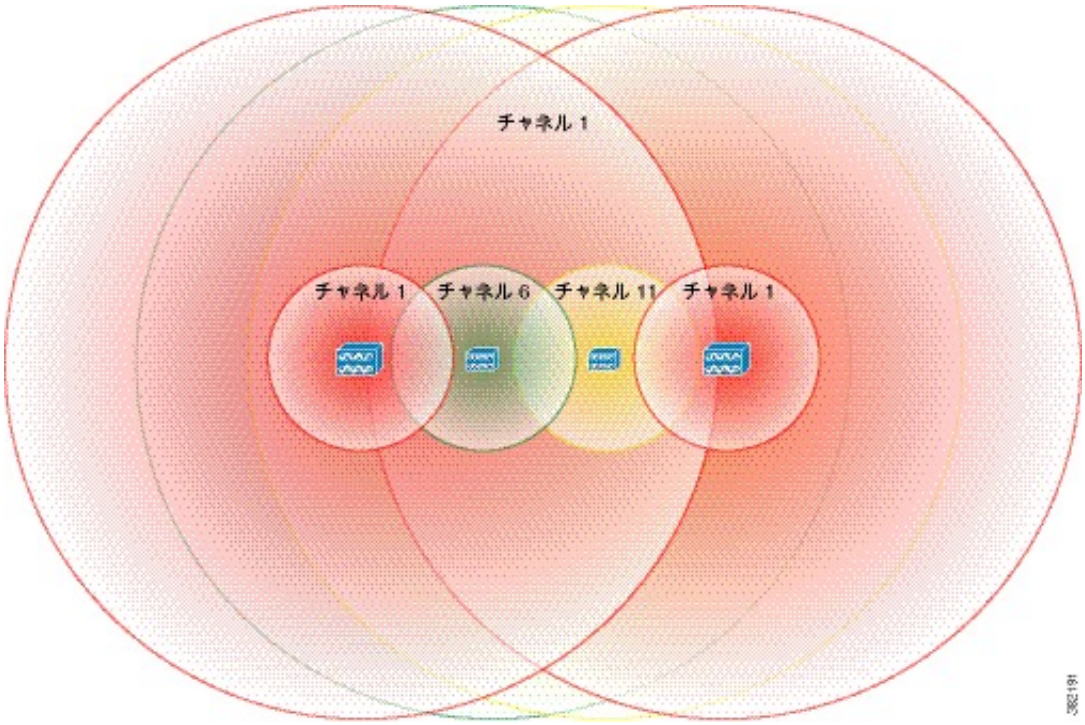
**図 *10* : *20 %* のオーバーラップの *AP***



### 同一チャネル干渉と 20 % の AP セル オーバーラップ

次の図に、20 % のオーバーラップの AP とその同一チャネル干渉の境界を示します。

**図 *11*：*20 %* のオーバーラップの *AP* とその同一チャネル干渉の境界**




チャネル 1 を使用する各 AP の同一チャネル干渉の境界は、同じチャネルを使用する AP とオーバーラップします。 このケースでは、RToWLAN の導入で同一チャネル干渉が発生しています。また、AP セル間の信頼性の高いローミングの要件である 20 % のオーバーラップの複合的な効果と、同一チャネル干渉による影響は、特定のエリアにおける RToWLAN チャネル セルのコール キャパシティに従って低下することにも注意する必要があります。

（注） 同一チャネル干渉を軽減するために、オーバーラップを減少させることは効果的ではありません。 オーバーラップを減少させるとローミング パフォーマンスが低下し、ユーザの満足度が低下します。 その一方で、コール キャパシティについては、計画および設計において対処することができます。

既存の WLAN データ導入環境（最初は初期低電力セル境界とより小さいオーバーラップを使用）を、RToWLAN 向けに推奨される電力境界とオーバーラップを満たすようにを変更した場合、時間的精度が要求されるアプリケーションでは問題が生じる可能性があります。 実際の影響はアプリケーションの実装に左右されるため、WLAN の変更によって影響を及ぼされる可能性があるアプリケーションを予測することは困難です。 一般に、キープアライブ タイムアウトを必要とするカスタム アプリケーションは影響を受けやすいため、タイマー調整が不要になるように新しい環境で検証を行う必要があります。

### 導入例

建物内の AP レイアウトは、建物の構造や形状と WLAN カバレッジの要件に左右されます。 実装に固有の変動要素によるさまざまな効果により、導入する必要がある AP 数に対して推奨される導入方法や、同一チャネル干渉の影響を決定するソリューションは 1 つに限定されません。 次の各項では、導入タイプを示す例を挙げて設計プロセスについて説明します。

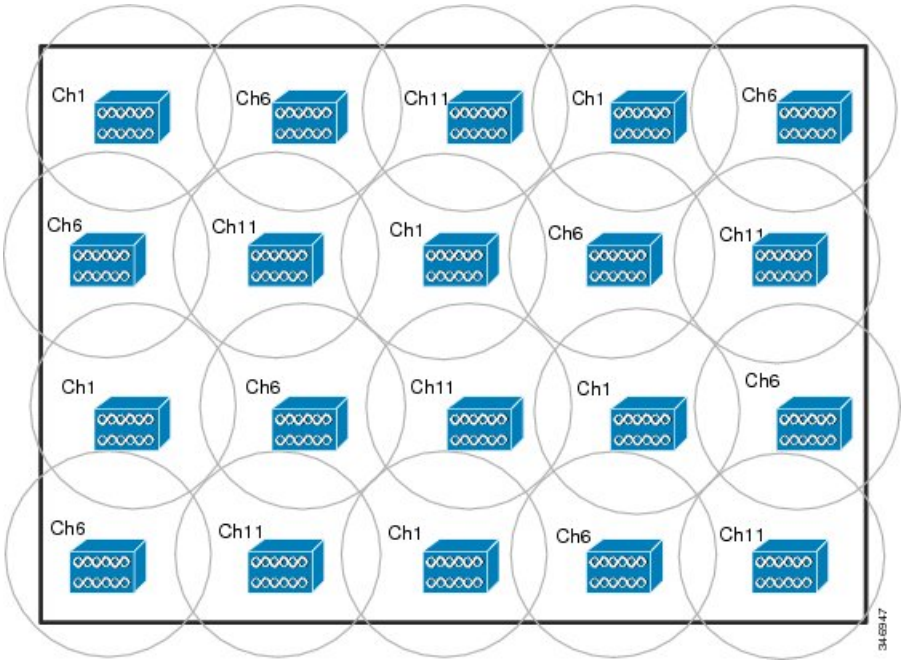
- シングルフロア ビルの導入例
- マルチフロア ビルの導入例

### シングルフロア ビルの導入例

20 個の AP と 15 個の AP を配置するシングルフロア導入の図は、建物が存在するロケーションを示しているわけではありません。 建物と建物の間にカバレッジが存在しない場合、建物の出口周辺にカバレッジが存在していることが重要です。

次の図は、寸法が 285 x 185 フィートである長方形の建物を示しています。この場合、カバレッジを完成させるために 20 個の AP が必要です。

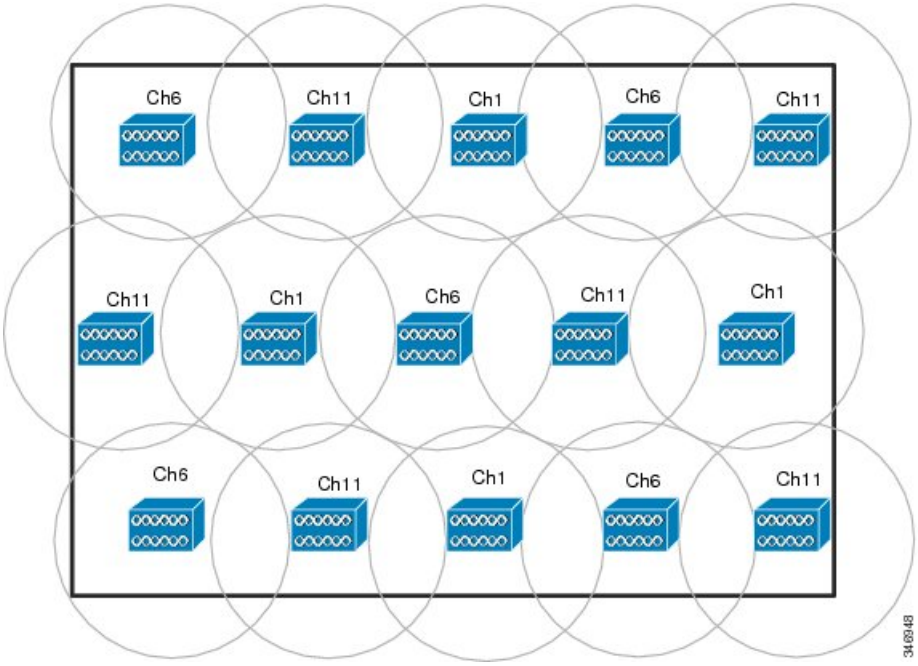
**図 *12*：*20* 個の *AP* を配置する *2.4 GHz* のシングル フロア導入**




AP 境界と計画が同じ WLAN データ導入環境では、使用できる AP は 15 個のみですが、次の図に示すように、カバレッジ ギャップは小さくなり、オーバーラップも減少します。 RToWLAN 導入

環境の 1 つの特徴は、ユーザの移動が多く、WLAN のデータ クライアントが発見できないカバレッジ ギャップが検出されることです。 そのため、AP を 20 個導入することを推奨します。

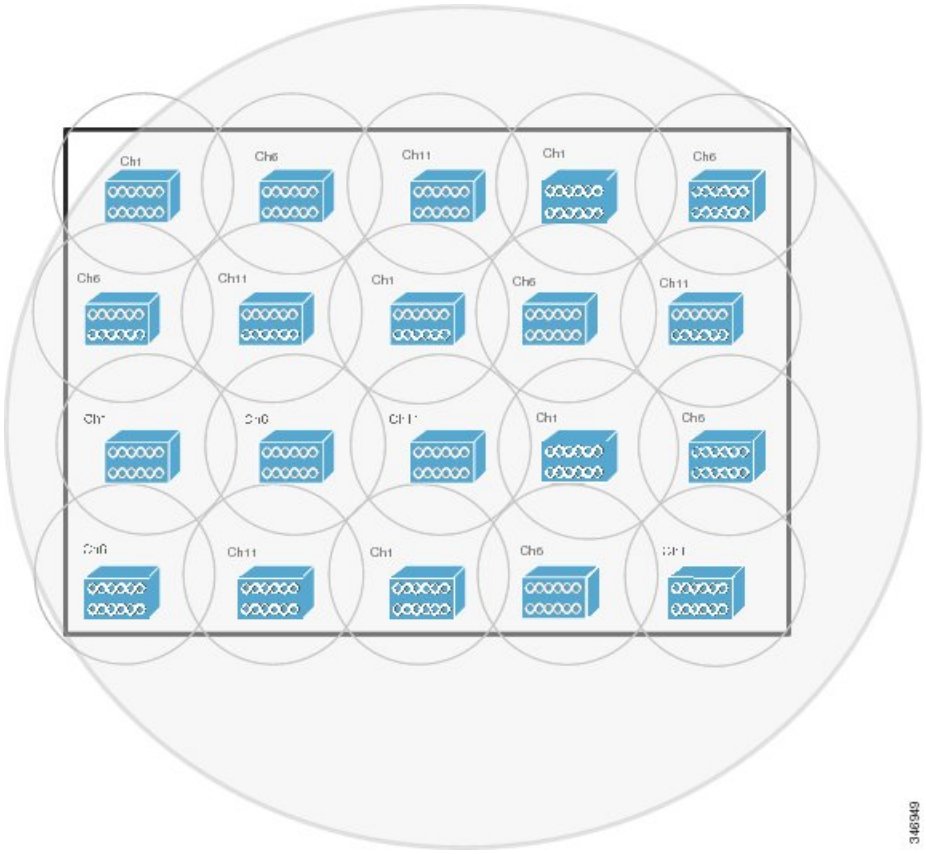
**図 *13*： *15* 個の *AP* を配置する *2.4 GHz* のシングル フロア導入**




次の図は、同一チャネル干渉の半径が建物全体に拡張された AP の例について、その同一チャネル干渉の半径を示しています。 ここでは、チャネル 1 を使用する AP 同士が、チャネル キャパシティを効果的に共有します。 チャネル 1 の 6 個の AP により、カバレッジは単一の AP に対して 6 倍に拡大されますが、同じ比率でキャパシティが増大するわけではなく、単一の AP と比較してキャパシティを大幅に増大させることはできません。 これは、他のチャネルの AP についても当てはまります。 同一チャネル干渉のため、フロアのコール キャパシティは、3 個の独立した AP のキャパシティを少し上回る程度で、20 個の AP のキャパシティには及びません。 これが、AP

あたりのコール数ではなく、チャネルあたりのコール数によって RToWLAN のコール キャパシティを解決する主な理由です。 チャネル キャパシティは制限要因です。

**図 *14*： *2.4 GHz* のシングルフロア同一チャネル干渉**




（注） セキュリティを考慮して、建物の外部でワイヤレス接続が必要なシナリオを除き、建物の物理境界の外側にセル半径を拡張しないことを推奨します。 たとえば、キャンパス導入では建物間にワイヤレス カバレッジが必要です。

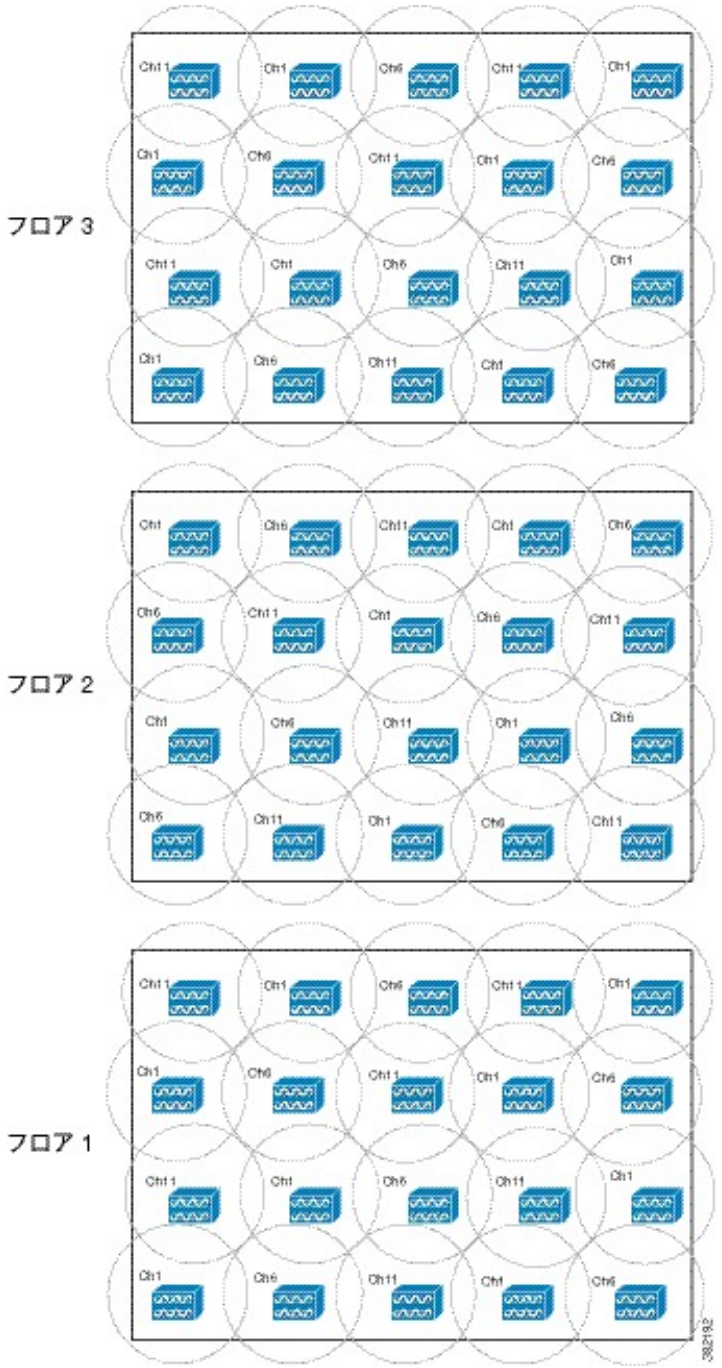
### マルチフロア ビルの導入例

（注） マルチフロア ビルの導入例では、マルチフロア チャネルの割り当ての概念とフロア間の同一チャネル干渉に限り説明します。 リアルタイム導入では、これらのチャネル実装例を使用しないことを推奨します。

マルチフロア ビルでは、RF エネルギーがフロア間を通過でき、RF プランニングの一部として、フロア間の同一チャネル干渉を最小化するために隣接フロア間でチャネルがずらして配置されま

す（次の図を参照）。 AP の同一チャネル干渉の半径を検討する場合、フロア間の信号パスが同じフロアのものと異なることに注意する必要があります（フロア間のパスには鉄筋コンクリートの塊がある場合が多いため）。 AP の同一チャネル干渉の半径を検討する場合は、このことを考慮する必要があります。

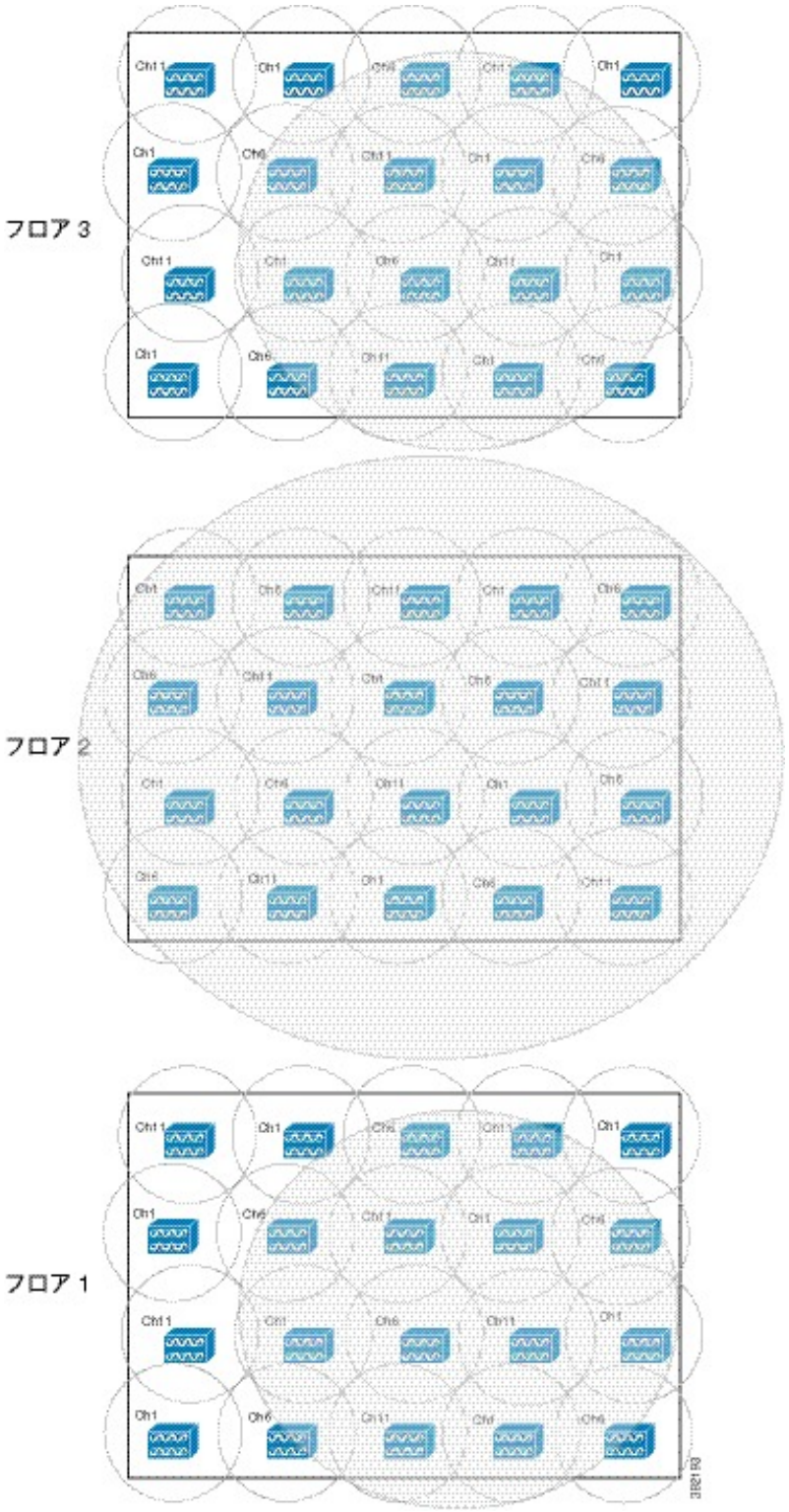
**図 *15*：*2.4 GHz* マルチフロア チャネルの割り当て**



次の図は、異なるフロア上の AP の同一チャネル干渉半径の例を示しています。フロア 2 はシングルフロアの例と同じレイアウトで、フロア 1 およびフロア 3 は上下のフロアにおける同一チャネル干渉を示しています。 ここでは、フロア間の同一チャネル干渉が引き続き重要となります。

3 つのフロア全体のキャパシティは、AP 6 個または 7 個分と同程度になると想定するのが妥当です（導入される AP 60 個分にはなりません）。

**図 *16*：同一チャネル干渉を示す *2.4 GHz* マルチフロア ビル**


フロア 3
フロア 2
フロア 1

### 位置情報サービスの設計の考慮事項

IEEE 802.11 位置情報サービスの信号レベル要件は RToWLAN に近いですが、AP の配置要件は異なります。 たとえば、図 12：20 個の AP を配置する 2.4 GHz のシングル フロア導入, （37 ページ）では、AP の配置が位置情報サービス（LBS）導入の要件を満たしています。 この環境の例では、建物の周辺や中心部に多数の AP が導入されています。 また、AP の追加セットが必要な場合があります。 LBS の AP 配置要件では、建物の形状やサイズによって、より多くの AP を追加する可能性があります。 LBS 用に AP を追加すると、追加された AP にアソシエートする IEEE 802.11 管理トラフィックが増加するので、同一チャネル干渉のレベルも上がります。 ただし、既存の同一チャネル干渉が存在する場合、その差は重要でなくなります。 RToWLAN の導入で重要な点は、AP を追加しても、同一チャネル干渉によって 2.4 GHz 帯域のキャパシティの増加にはつながらないということです。

### 自動 RF の重要性

2.4 GHz 帯域の同一チャネル干渉は RToWLAN チャネル セルのコール キャパシティに影響を及ぼすため、RToWLAN ネットワークの計画、設計、運用を行う際は、この制限について検討する必要があります。 この章で紹介するすべての例は、自動 RF が有効で、AP がチャネルを変更して干渉を最小化し、チャネル計画を最適化していることを前提としています。 この前提では、導入環境のコール キャパシティは、単一の AP のキャパシティの 3 倍程度になります。 自動 RF によって、2.4 GHz チャネルにおける同一チャネル干渉の影響に対処するためにできることは多くありません。これは、2.4 GHz 帯域の制限要因が 3 つの非オーバーラップ チャネルであるためです。 自動 RF は AP 電力レベルを調整し、電力レベルを下げることで同一チャネル干渉を軽減できます。しかし、この電力レベル調整では、RToWLAN 導入環境の信号レベル要件とカバレッジ要件に対してバランスを取る必要があります。 最も良い方法は、IEEE 802.11a 標準の 5 GHz 帯域を使用してキャパシティを拡大し、AP 導入の投資効果を高めることです。

### 5 GHz のネットワーク設計

ここでは、5 GHz の RToWLAN 導入に関する以下の考慮事項について説明します。

- IEEE 802.11a の物理層
- IEEE 802.11a のチャネル
- IEEE 802.11a の動作周波数とデータ レート
- IEEE 802.11a および RToWLAN の導入

### IEEE 802.11a の物理層

IEEE 802.11a 標準では、物理層（OSI モデル）の要件が定義されています。5 GHz の Unlicensed National Information Infrastructure（UNII）周波数帯域で動作し、データ レートは 6 Mbps ～ 54 Mbps の範囲であることが必要です。また、直交周波数分割多重方式（OFDM）が使用されるマルチキャリア システム（52 のサブキャリアを使用、2 位相偏移変調（BPSK）、4 位相偏移変調（QPSK）、直交振幅変調（QAM）、または 64 QAM で変調を行い異なるデータ レートを提供）です。 OFDM では、サブキャリア チャネルをオーバーラップできるため、スペクトル効率が高まります。 OFDM で使用する変調テクノロジーは、IEEE 802.11b で使用されるスペクトラム拡散技術よりも効率性に優れており、802.11g で使用されるものと同一です。

### IEEE 802.11a のチャネル

（注） お住まいの国または地域でサポートされるチャネルに関する最新情報については、国別の規制に関する情報を参照してください。また、すべてのクライアントがすべてのチャネルをサポートするわけではありません。

次の例は、米国版の IEEE 802.11a 標準です。5 GHz のライセンス不要帯域は、300 MHz のスペクトルをカバーし、23 チャネルをサポートします。 その結果、米国では 5 GHz 帯域は 3 つの帯域にまとめられています。

- 5.150 ～ 5.250 GHz（UNII-1）
- 5.250 ～ 5.350 GHz（UNII-2）
- 5.500 ～ 5.700 GHz（UNII-2 拡張）
- 5.725 ～ 5.875 GHz（UNII-3）

### IEEE 802.11a の動作周波数とデータ レート

IEEE 802.11a 標準は、5 GHz 無線帯域のライセンス不要部分で動作する場合に、電子レンジ、コードレス電話、Bluetooth などの 2.4 GHz 帯域で動作するデバイスからの干渉に強い特性を備えています。 IEEE 802.11a 標準は異なる周波数範囲で動作するため、既存の IEEE 802.11b または IEEE 802.11g に準拠するワイヤレス デバイスとの互換性はありません。 ただし、2.4 GHz と 5 GHz の機器は、干渉することなく同じ物理環境で動作できます。

IEEE 802.11a 標準では、特定の電力およびゲインで、6、9、12、18、24、36、48、54 Mbps のデータ レート（54 Mbps が最大データ レート）を使用できますが、一般に 2.4 GHz ネットワークに比べて範囲が狭くなります。 ただし、2.4 GHz 帯域では非オーバーラップ チャネルが 3 つであるのに比べて、最大 24 の非オーバーラップ周波数チャネルがあるため（地理的エリアに依存）、ネットワーク キャパシティが増加して拡張性が向上し、隣接セルからの干渉がないマイクロセルラ導入環境を作成できます。

IEEE 802.11a が動作する 5 GHz 帯域は、いくつかのサブ帯域に分けられます。 次の表に記載されている各 UNII 帯域は、当初は別の使用目的で提供されていましたが、現在ではすべて、該当する電力制限の屋内 IEEE 802.11a 導入環境で使用できます。 当初、FCC では、それぞれが 4 つのチャネルから構成される UNII-1、UNII-2、および UNII-3 帯域を定義しました。 各チャネルは 20 MHz の RF スペクトル帯域幅を使用して 20 MHz の間隔を空けているため、4 つの非オーバーラップ チャネルが提供されます。

表 *5* : *IEEE 802.11a* の動作周波数範囲

| 帯域 | チャネル ID | 中心周波数 |
|---|---|---|
| UNII-1 | 36 | 5180 |
| | 40 | 5200 |
| | 44 | 5200 |
| | 48 | 5240 |
| UNII-2 | 52 | 5260 |
| | 56 | 5280 |
| | 60 | 5300 |
| | 64 | 5320 |
| | 100 | 5500 |
| | 104 | 5520 |
| | 108 | 5540 |
| | 112 | 5560 |
| | 116 | 5580 |
| | 120 | 5600 |
| | 124 | 5620 |
| | 128 | 5640 |
| | 132 | 5660 |
| | 136 | 5680 |
| | 140 | 5700 |

| 帯域 | チャネル ID | 中心周波数 |
|---|---|---|
| UNII-3 | 149 | 5745 |
| | 153 | 5765 |
| | 157 | 5785 |
| | 161 | 5805 |
| | 165 | 5825 |

送信電力、アンテナゲイン、アンテナスタイル、使用率など、各UNII帯域の制限は異なります。

- UNII-1帯域は屋内動作用に設計されており、完全に固定されたアンテナを使用するデバイスが最初に必要となります。 この帯域（5.150 ～ 5.250 GHz）のチャネルは36、40、44、48です。
- UNII-2帯域は屋内または屋外動作用に設計されており、外部アンテナの使用が許可されています。 この帯域（5.250 ～ 5.350 GHz）のチャネルは52、56、60、64で、動的周波数選択（DFS）やトランスミッタ電力制御（TPC）が必要です。

  一部のクライアントは、5GHzチャネル、特に、UNII-2拡張チャネル（100～140）をサポートしません。お住まいの国でサポートされるチャネルに関する最新情報については、チャネル計画を完了する前に、国別の規制に関する情報を参照してください。また、すべての地域でチャネル120、124、および128がサポートされるとは限らないことに注意してください（例：米国およびヨーロッパ）。
- UNII-3帯域は、当初、外部アンテナを使用する屋外ブリッジ製品用でしたが、現在では屋内または屋外のIEEE 802.11a WLANに使用することも許可されています。 この帯域（5.725 ～ 5.825 GHz）のチャネルは149、153、157、161、165で、DFSおよびTPCは不要です。 すべてのクライアントがチャネル165をサポートするとは限らないことに注意してください。
- 新しい周波数範囲（5.470 ～ 5.725 GHz）のチャネルは100、104、108、112、116、120、124、128、132、136、140で、DFSおよびTPCが必要です。

特定の範囲の全チャネルを規制ドメインのすべてで使用できるとは限りません。 UNII-1、-2、および-3帯域の各種チャネル、および追加された新しい11チャネルについては、前述の表を参照してください。

（注） お住まいの国または地域でサポートされるチャネルに関する最新情報については、国別の規制に関する情報を参照してください。

### IEEE 802.11a および RToWLAN の導入

5 GHz 帯域には 24 もの非オーバーラップ チャネルが存在しますが、5 GHz スペクトルの下の 4 チャネルと上の 4 チャネルには DFS および TPC 要件がないため、これらのチャネルを RToWLAN のベースとして使用することを推奨します。 次に、DFS および TPC によって影響を受けない他のチャネルを確認し、それらのチャネルを 8 チャネルの RToWLAN ベースに追加します。 DFS および TPC のタイミング要件は、RToWLAN のコール品質に悪影響を及ぼす可能性があります。 RToWLAN の導入を計画しているロケーションのチャネルに DFS および TPC が影響を及ぼす可能性がある場合は、適切にチャネルを選択する必要があります。 そうでない場合は、特定のチャネルを個々に選択しても問題ありません。 選択するチャネルが WLAN クライアント（データおよび RToWLAN）でサポートされていることを確認してください。 8 つの非 DFS チャネルを使用するだけなら簡単ですが、追加チャネルを安全に導入するごとに、設計のキャパシティは増大します。

DFS および TPC チャネルを回避するだけでなく、各チャネルのサイドバンドからの干渉を防ぐために、AP チャネルのレイアウトで隣接チャネルを回避することを推奨します。 チャネル間隔とチャネル マスク特性により、IEEE 802.11a クライアントで生成されるサイドバンドが隣接チャネルに干渉する可能性があります。

このマニュアルで 5 GHz 実装の RToWLAN 向けとして使用する一般的な電力レベルと AP 間隔の推奨値は、2.4 GHz の実装と同じです。

- 電力レベル境界が ～ 67 dBm、隣接 AP チャネルの間隔が -86 dBm です。
- 5 GHz 帯域の導入環境では、最低でも 20 % の非隣接チャネル間のオーバーラップが推奨されます。
- デュアルバンドの導入環境やミッション クリティカルな環境では、30 % 以上のオーバーラップを使用することができます。

5 GHz 帯域の範囲は 2.4 GHz 帯域の範囲とは異なります。 ただし、5 GHz 帯域の例で述べたように、推奨される電力レベルと通常のアンテナを使用する場合に算出される距離は、2.4 GHz の例で使用される距離と似ています。 そのため、2.4 GHz および 5 GHz 帯域の両方で、同じ AP のロケーションとオーバーラップが使用されています。 2 つの導入間の主な差異は、非オーバーラップ チャネルの追加によって使用可能となる追加キャパシティです。 この違いは、RToWLAN の導入で 5 GHz 帯域を推奨する十分な理由となります。

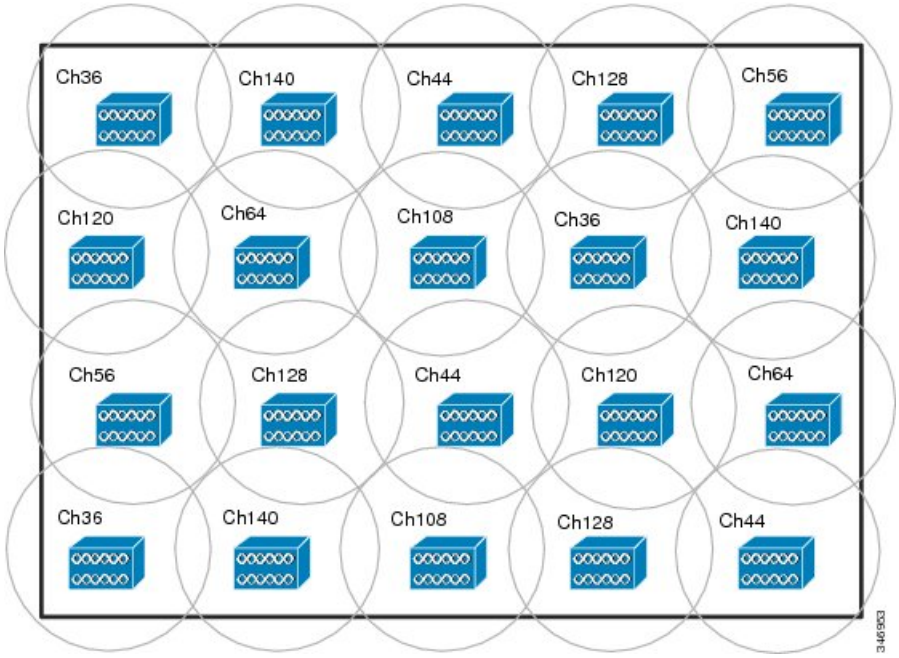
（注） ここで説明される TPC メカニズムは、自動 RF の一部である TPC アルゴリズムとは異なります。

### シングルフロア ビルの例

次の図は、8 つの異なるチャネルを使用する AP レイアウトを示しています。再利用されるチャネル間の距離を最大化するように設計されています。 ただし、ほとんどのケースで、使用可能なチャネル数をより多くすることが要件となります。 この例では、2.4 GHz および 5 GHz の AP クライアント半径と同一チャネル干渉の半径は同じなので、ここではマルチ フロアの例を繰り返しません。 2 つの帯域間の主な差異は、キャパシティの増大です。これは、5 GHz 帯域にアソシエー

トした追加チャネルによって使用可能になったものです。 5 GHz 帯域で使用できるチャネル数を増加させると、導入されるAPの数とシステムのキャパシティの相関を強くすることができます。

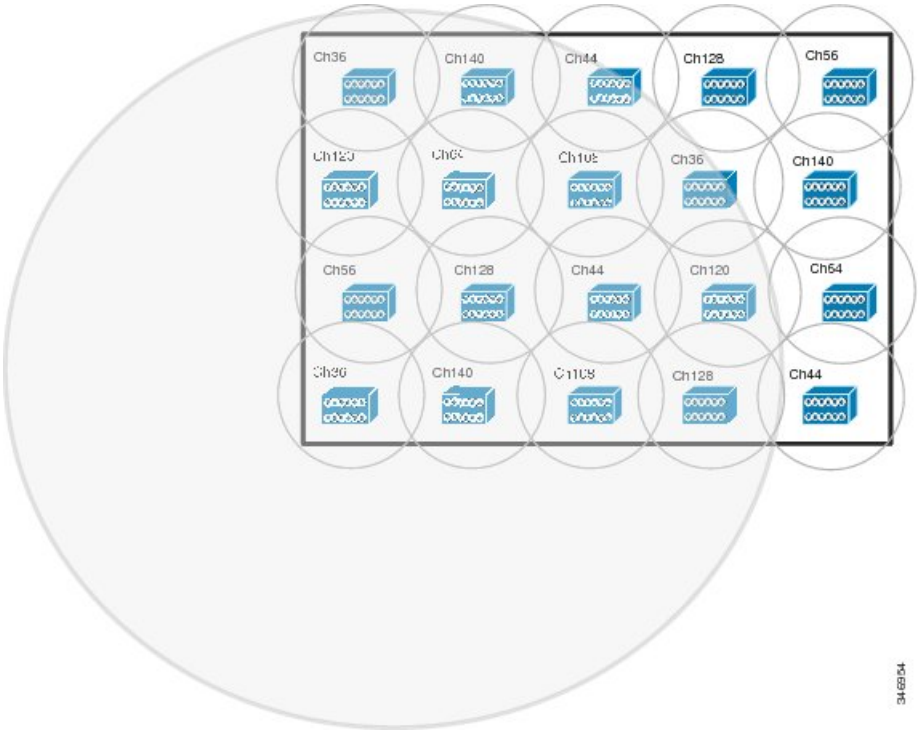
**図 *17* : *5 GHz* のシングルフロア レイアウト**




（注） 上の図で使用されているチャネルは、非オーバーラップ チャネルを説明するためだけに使用されており、特定の国または地域で推奨されるチャネル レイアウトではありません。

次の図では、先の図と同じ AP レイアウトの例が示されていますが、単一 AP の同一チャネル干渉の半径が組み合わされています。

**図 *18*：*5 GHz* のシングルフロア レイアウトと同一チャネル半径**




上の図は、同一チャネル半径が小さく、使用可能なチャネル数は多いが、フロアのコール キャパシティ全体の影響が大きくなっていることを示しています。 20 個の AP と 8 チャネルを使用している場合、フロア全体の同一チャネル干渉の量を計算することは困難です。 そのため、8 チャネルを使用できる場合のフロアの RToWLAN コール キャパシティは、単一 AP のコール キャパシティの 8 倍程度になります。

（注） 上の図で使用されているチャネルは、非オーバーラップ チャネルを説明するためだけに使用されており、特定の国または地域で推奨されるチャネル レイアウトではありません。

### プランニング ツール

Cisco Unified Wireless Network ワイヤレス制御システム（WCS）は、WLAN プランニング ツールを提供します。

この章に記載されている例では、簡易的な描画ツールを使用しており、WLAN のプランニングで検討する必要がある複雑な物理構造や建物のレイアウトは考慮されていません。 WLANのレイアウトを計画するには、WLAN プランニング ツールを使用することを推奨します。 プランニング中の小さなエラーをレイアウトの実装中に解決するには10倍のコストが必要ですが、運用中に解

決するには 100 倍のコストが必要となる可能性があります。 WLAN サイト計画を設計するためのプランニングとプランニング ツールへの投資には費用がかかりますが、それによって実装後には最大限の利点が得られるようになります。

### WLAN ネットワークを介したマルチキャスト

マルチキャスト用のワイヤレス LAN コントローラ（WLC）の設定オプションには、特定のマルチキャスト パケットのユニキャストへの変更（信頼性の高い WLAN プロトコル パケットの配信）、定義済みマルチキャスト グループの作成、およびアプリケーション ソースに基づくパケットの優先度付けが含まれます。 WLC の設定は、アクセス ポイント（AP）間または WLC 間のローミング時に、マルチキャスト グループのメンバーシップを維持する上で重要な役割を果たします。

WLAN を介したマルチキャストは Wi-Fi エンドポイントに配信の問題をもたらします。 これらの問題は、マルチキャストが有線ネットワークの帯域幅を温存する効果的な手段となる有線イーサネットでは顕著には見られず一般的な問題ではありません。 帯域幅の管理や信頼性の確保に WLC の設定オプションを使用していない場合、ワイヤレス上のマルチキャストは多くの場合、WLAN チャネルの利用可能な帯域幅を無駄にすることになります。 AP に転送されるマルチキャスト ストリームは AP の有効な無線すべてにより転送されるため、AP の 2.4 GHz および 5 GHz 無線の両方がマルチキャスト トラフィックを転送します。 デフォルトのパラメータを使用すると、マルチキャスト アプリケーションを使用してマルチキャスト トラフィックを受信する Wi-Fi エンドポイントが存在しない場合でも、WLAN を介してマルチキャスト トラフィックが転送されます。 Wi-Fi チャネル上の不要な未使用のマルチキャスト トラフィックは、AP、クライアント、および WLAN チャネルのパフォーマンスを低下させます。 また、ホットスタンバイ ルータ プロトコル（HSRP）、Protocol Independent Multicast（PIM）、Enhanced Interior Gateway Routing Protocol（EIGRP）、および Open Shortest Path First（OSPF）などのプロトコルにより生成されたマルチキャスト パケットを含む、任意のクライアント VLAN のローカル ソースからのマルチキャスト トラフィックが、WLAN 全体にフラッディングします。 このトラフィックはすべて、使用している最も低いブロードキャスト データ レートで、WLAN 上でスループットを低下させている可能性がある特定の AP にアソシエートしたクライアントにより送信されます。 イーサネット上のマルチキャスト トラフィックと同様に、Wi-Fi エンドポイントはマルチキャスト パケットの受領を確認しません。

マルチキャストのパフォーマンス機能を使用する前提条件は、WLC および AP 間のすべてのルータでマルチキャスト対応のネットワークを設定していることです。 管理者がマルチキャストを有効にし（マルチキャスト モードはデフォルトで無効）、CAPWAP マルチキャスト グループを設定すると、AP は、通常の join プロセス中（ブート時）にコントローラの CAPWAP マルチキャスト グループのアドレスをダウンロードします。 各 AP へマルチキャスト パケットを配信するために、CAPWAP マルチキャスト グループが効果的に使用されます。 これにより、ネットワーク内のルータが標準的なマルチキャスト テクノロジーを使用して、AP に対してマルチキャスト パケットを複製および配信できるようになります。 CAPWAP マルチキャスト グループでは、WLC がマルチキャスト ソースとなり、AP がマルチキャスト レシーバになります。

### 関連トピック

20 % のセル オーバーラップ計算
ワイヤレス ネットワークにおけるマルチキャスト導入の推奨事項

# 802.11n および 802.11ac プロトコル

このマニュアル、およびこの章で取り上げる設計パラメータは、新しい 802.11n および 802.11ac プロトコルに適用できます。 音声や他のジッタの影響にされやすいアプリケーションでは、これらのプロトコルとともに、-67 dBm のセル エッジを使用することを推奨します。 これらの新しいプロトコルではパケット速度が速くなりますが、WLAN使用量やアプリケーションリソースの需要が増加するため、セルのキャパシティ プランニングは依然として WLAN カバレッジ設計の重要な側面となります。

802.11n および 802.11ac プロトコルは、従来のプロトコルと同様、半二重無線プロトコルです。主な相違点は、データ パケットの送信に使用する周波数の大きさです。 オリジナルの 802.11 仕様（1997年）において、2.4 GHzのWLANチャネルが定義されました。 また、802.11a仕様（1999年）では 5 GHz のチャネルが定義されました。 802.11n の仕様は、2.4 GHz と 5 GHz の両方の帯域と互換性を維持します。 802.11n では、40 MHz の周波数でセル チャネルを作成するためにチャネル ボンディングを追加することで、高スループット（HT）の概念が追加されました。 また、802.11n では空間ストリームと各標準規格に準拠したビームフォーミングが導入されています。802.11ac の帯域幅のニーズを満たすには、2.4 GHz に割り当てられた周波数が十分ではないため、802.11ac はその仕様から 2.4 GHz を除外しています。 802.11n および 802.11ac では、2 つ以上の 20 MHz 802.11 チャネル ボンディングをサポートし、以前の 802.11 プロトコルよりも多くの帯域幅をクライアントまたはアクセス ポイントに提供します。

802.11n/802.11ac ボンディング チャネルは、80 MHz の AC Wave1 または 160 MHz の AC Wave2 にすることができる単一チャネルに、他の 802.11 Wi-Fi チャネルの周波数を追加することで作成される WLAN チャネルです。 新しい 5 GHz プロトコルの 802.11ac には 2 つのハードウェア リリースがあります。 第 1 世代の 802.11ac ハードウェアは WAVE 1 として知られており、 次にリリースされた 802.11ac ハードウェアは WAVE 2 として知られています。 802.11ac の仕様では、新しい物理（PHY）仕様が定義され、直交周波数分割多重方式（OFDM）の無線変調システムに基づく非常に高いスループット（VHT）が提供されます。 また、この仕様では空間ストリームの数が増加しており、マルチユーザ伝送向けに提供されます。 WAVE 2 では、2 つの 80 MHz チャネルのボンディングを提供し、160 MHz のチャネルとしています。 160 MHz のチャネルは、隣接チャネルまたは 2 つの 80+80 MHz 非隣接チャネルのいずれかとすることができます。

802.11ac では、マルチユーザの複数入力および複数出力（MIMO）（空間ストリームをサポートする複数クライアント）がサポートされるようになり、ユニークなデータ ストリームを同時に送受信できます。 これらの仕様強化により、アクセス ポイントのカバレッジ エリアのスループットと帯域幅が増大しています。 また、ビームフォーミングによって各クライアントのパフォーマンスのために AP 数が増加し、その AP の WLAN チャネルの帯域幅も増大しています。 さらに、クライアントの無線または AP の無線における MIMO アンテナ サポートにより、送受信の品質が向上します。これらのテクノロジーの向上によって、カバレッジエリアのキャパシティは増大しています。 1990 年代のレガシー テクノロジーと同様に、AP カバレッジは依然として Wi-Fi エンドポイントのアプリケーション パフォーマンスに関する重要な設計上の考慮事項です。

802.11ac の VHT PHY は、802.11n および 802.11a プロトコルと下位互換性を持っています。 そのため、802.11a レガシー クライアントは、そのクライアントでサポートされるデータ レートで、802.11ac APからのトラフィックのアソシエーション、認証を行い、通過させることが可能です。

現在の 802.11ac AP は、1.3 Gbps の送信データ レートを提供する 3 つの空間ストリームによる 4x4 MIMO テクノロジーをサポートします。

新しい VHT クライアント無線ハードウェアでのクライアント デバイス アプリケーションのパフォーマンスは、WLAN チャネルの現在の帯域幅に直接関連します。 これは、レガシー クライアントの条件でしたが、次世代の Wi-Fi プロトコルの条件にも当てはまります。 そのため、初期の WLAN セル設計で使用される同じ設計基準が依然として通用します。 一般に、WLAN アプリケーションは、有線アプリケーションと同じくらいの多くの帯域幅を必要とします。 特定のフロア スペースでより多くの帯域幅を実現するには、そのフロア スペースの WLAN チャネルの効率が優れている必要があります。 これには、クライアント無線と AP 無線の効率性を高める必要があります。また、その無線に割り当てられるデータ レートの設定を変更しなければならない場合もあります。 1997 年のデータ レートの 1 Mbps と 2 Mbps を削除することを強く推奨します。 該当する場合は、1999 年のデータ レートの 5.5 Mbps と 11 Mbps も削除することを推奨します。 必要に応じて、これらのデータ レートセットのいずれかを使用している場合、高密度のカバレッジ エリアでクライアント アプリケーションのパフォーマンスに影響が出る可能性が高くなります。このため、5 GHz を有効にすることを強く推奨します。

多様なサービスを提供できるWLANネットワークを難易度が高い環境へ導入することは、どのような組織にとっても成功へのハードルが高いプロジェクトとなり得ます。 このことを初めから正しく実行するためには、場合によっては獲得が困難な特別なスキルや知識が必要となります。 ワイヤレス導入の経験が豊富なネットワーク インテグレータとパートナーを組むと、非常に有益な場合があります。

この 802.11ac 仕様は、802.11ac モジュールが搭載された AP3600 と AP3700 でサポートされます。現在の無線テクノロジーでは 80 MHz の帯域チャネルがサポートされますが、マルチユーザ伝送や 160 MHz の帯域チャネルはサポートされません。

### 関連トピック

802.11ac をサポートする Cisco AP 向けデータ シート
802.11ac ホワイト ペーパー

第 3 章

# Real-Time Traffic over WLAN の QoS

この章では、Real-Time Traffic over WLAN の実装における Quality of Service（QoS）について説明します。 WLAN の QoS について全般的に説明します。QoS はセキュリティやセグメント化のコンポーネントの一部ですが、これらについては詳しく取り上げません。 Cisco Centralized WLAN アーキテクチャの機能に関する情報も記載されています。



## QoS アーキテクチャの概要

QoS とは、特定のネットワーク トラフィックに対して、さまざまなネットワーク テクノロジーを介してディファレンシエーテッド サービスを提供するネットワーク機能のことです。QoS テクノロジーは次の利点を提供します。

- キャンパス、WAN、およびサービス プロバイダ ネットワークで使用されるビジネス マルチメディアおよび音声アプリケーションに基盤を提供します。
- ネットワーク マネージャが、ネットワーク ユーザとのサービス レベル契約（SLA）を策定できます。
- ネットワーク リソースをより効率的に共有でき、ミッションクリティカルなアプリケーションの処理を効率化します。

- 時間的精度が要求されるマルチメディアおよび音声アプリケーションのトラフィックを管理して、ベスト エフォートのデータ トラフィックよりも高い優先度、広い帯域幅を割り当てて、トラフィックの遅延が少なくなるようにします。
- WLAN のアプリケーションの可視性および制御

QoS では、WLAN や WAN を含む LAN 全体で帯域幅をより効率的に管理できます。 QoS は、以下のことを通じてネットワーク サービスを向上させ、高い信頼性を提供します。

- 重要なユーザおよびアプリケーションの専用帯域幅のサポート
- ジッタおよび遅延の制御（リアルタイム トラフィックに必要）
- ネットワークの輻輳の管理と最小化
- トラフィック フローをスムーズにするネットワーク トラフィックのシェーピング
- ネットワーク トラフィックの優先度の設定

# Real-Time Traffic over WLAN における QoS の重要性

パケットの送受信に使用するWLANは、ライセンス不要であり、保護およびシールドされていません。 複数の仕様、プロトコル、およびデバイスが、WLAN によるライセンス不要でコスト ゼロのメディア（無線周波数）を活用します。 次の例について考えてみます。

ビジネス オフィスのタブレット ユーザが、文書を印刷するために Bluetooth を使用しています。 同じオフィスの別のラップトップ ユーザは、ビデオ会議とプレゼンテーションのために 2.4 GHz 周波数の Wi-Fi を使用しています。 また、ロビーにいる新規ゲスト ユーザは、Wi-Fi ネットワークのゲスト VLAN を介して電子メールをチェックするために、スマートフォンを使用しています。 Wi-Fi ネットワークでは 3 台のデバイスによって共有される 2.4 GHz 無線周波数を優先度付けし、ゲストのスマートフォンユーザおよびタブレットユーザよりも、リアルタイムのビデオ会議アプリケーションを優先させる必要があります。 さらに、Wi-Fi ネットワークで、タブレットの Bluetooth 伝送の干渉も解決する必要があります。

### WLAN のキューイングおよびスケジューリング メカニズム

802.11 WLAN はキューイングおよびスケジューリング メカニズムを備えており、それらは 4 つのアクセス カテゴリ（AC）に分けられます。 これら 4 つの Wi-Fi AC キューは、Wi-Fi チャネルに差別化されたアクセスを提供します。 また、4 つの Wi-Fi QoS カテゴリは 802.1P のアクセス カテゴリにも対応しています。 複数のレイヤ 3 プロトコルを伝送するように Wi-Fi は設計されているので、各実装では、通常、Wi-Fi 無線で送信されるパケットの IP ヘッダーの DiffServ コード ポイント（DSCP）の値を AC の 1 つにマッピングします。

音声パケットは、電話のコールに含まれる音声パケットの DSCP 値または IP QoS 値（音声アクセス カテゴリ）に応じて、WLAN に対して最も高い優先度でキューイングされます。 シスコのワイヤレス コントローラは、音声パケットを Platinum QoS プロファイルにもマッピングします。 音声通話またはビデオ通話からの音声およびビデオパケットは、データ パケットよりも速い速度かつ高い頻度で Wi-Fi チャネルへアクセスします。 Wi-Fi は共有メディアなので、電話のコールとデータ アプリケーション間でパケットの衝突が発生します。 Wi-Fi QoS は、リアルタイムの音声

およびビデオ トラフィックとデータ トラフィックの両方に対して、WLAN の Enhanced Distributed Coordination Function（EDCF; 拡張型分散コーディネーション機能）の設定値に基づき、バックオフとパケット再試行ロジックの優先度付けを行います。

Bluetooth（BT）無線と、ラップトップ、スマートフォン、タブレット、アクセス ポイントの Wi-Fi 無線は、すべて半二重です。 それぞれパケットを送出した後に、送出したパケットが適切に受信されたことを示す Acknowledge パケットを受け取れるように、パケット受信状態に移行します。 ここでは、Wi-Fi に関する 802.11e の仕様（2005 年）が、QoS のチャネルの優先度付けで重要な役割を果たします。 802.11 WLAN プロトコルには、基本となるメディア アクセス ロジックとして、キャリア検知多重アクセス/衝突回避（CSMA/CA）と呼ばれるプロセスが含まれています。 パケット送信前にキャリア（無線周波数）が存在しない場合、Wi-Fi ユニットは受信パケット モードで待機します。 そのため、BT 無線付近の Wi-Fi デバイスは、送信可能になるまで BT 無線の送信終了を待機します。 スマートフォンとイヤホンの間で使用される主要な BT データ レートは 2 Mbps です。 したがって、BT 無線から送信される 256 バイトの G.711 音声パケットでは、同じ 2.4 GHz 周波数の Wi-Fi デバイスで 1100 マイクロ秒以上の遅延が発生しますが、802.11n Wi-Fi の同じ G.711 音声パケットの送信には約 50 マイクロ秒しかかかりません。

Cisco CleanAir テクノロジーは、BT やその他の干渉が存在する一般的なエリアを定義して特定し、これらの回避を容易にします。 しかし、BT では、Wi-Fi が使用する 2.4 GHz 周波数の割り当て全体を使用します。 そのため、Wi-Fi チャネルで回避できないプロトコルであり、QoS メカニズムが BT の干渉を軽減するベスト ソリューションになります。

Wi-Fi QoS プロトコルは Wi-Fi マルチメディア（WMM）として知られています。 WMM は 802.11e 仕様のサブセットです。 802.11e 仕様は 2005 年に承認されましたが、その前から Wi-Fi Alliance と Microsoft によって広く使用されていました。 802.11e 仕様では、ハードウェアの変更なしに Wi-Fi QoS に対応するためには、デバイスで新しいドライバが必要でした。 QoS 機能がないレガシー デバイスでは、ファームウェアのメモリが制限されており、ハードウェアが特別に設計されます。

2005 年に認定された Wi-Fi QoS プロトコルによって、品質、範囲、速度の継続的な改善とともに、Wi-Fi チャネルの帯域幅のニーズが大幅に高まりました。 したがって、1、2、5.5 および 11 Mbps のレガシー データ レートに依存したサイトでは、正当な有効な理由があればこれらのレートを完全に無効化できるようになっています。

802.11 WLAN チャネルの帯域幅は、管理されたメディア リソースです。 Wi-Fi チャネルは、ファースト ホップのアップストリームとラスト ホップのダウンストリームです。 このメディアは無線周波数および非 Wi-Fi プロトコルに対してオープンであるため、メディア ホップが Wi-Fi デバイスで実行しているアプリケーションのパフォーマンスに影響を及ぼします。 Cisco Jabber などの音声およびビデオ アプリケーションを検討する際に、Wi-Fi チャネルは、コールの平均オピニオン評点（MOS）の値に悪影響を及ぼす可能性が最も高いメディアとなります。 したがって、ユーザの期待を満たすようにアプリケーションが実行されることを保証するため、帯域幅を管理する必要があります。

802.11b のデータ レートを削除することで、2.4 GHz の Wi-Fi チャネルの帯域幅を 2 倍にできます。 802.11b を必要とし、パフォーマンスに問題があるサイトでは、1、2 および 5.5 のデータ レートを無効にするかどうか検討する必要があります。 必要な 11 Mbps のデータ レートを使用することにより、特殊なアプリケーションのレガシー デバイスで必要とされるサポートをすべて提供します。 ビーム フォーミング テクノロジーを備えたシスコの AP は、直交周波数分割多重方式（OFDM）変調を使用して、クライアントのパフォーマンスと Wi-Fi チャネルの帯域幅をさらに

向上させています。 1999 年、802.11a 仕様の 5 GHz 帯域の Wi-Fi に OFDM 無線変調が導入されました。 2003 年に認定された 802.11g 仕様により、2.4 GHz に対して OFDM が導入されるようになりました。テクノロジーが導入されて使用されるようになってから 10 年を越える年月が経過し、2.4 GHz の OFDM 変調では、802.11b テクノロジーの下位互換性を維持するための高いコストは不要になっています。

QoS プロファイルとしても知られている次の 4 つの WMM QoS 優先度オプションが、Cisco Wireless LAN Controller の WLAN/SSID 設定で使用されます。

- Platinum
- Gold
- Silver
- Bronze

これらの WMM オプションは、AP およびワイヤレス LAN コントローラ間のアップストリームと、ワイヤレス コントローラから Wi-Fi エンドポイントまでのダウンストリームで、トラフィックの優先度制限を設定します。

たとえば、ベスト エフォートの WLAN/SSID 設定 Silver で DSCP 音声優先度を持つ音声パケットは、IP Control and Provisioning of Wireless Access Points（CAPWAP）のラッパー ヘッダーの DSCP 値がベスト エフォートとなります。 音声設定が Platinum で WLAN/SSID の DSCP 値がゼロのデータ パケットは、ベスト エフォートの優先度を維持し、一方で、同じ WLAN/SSID の音声パケットは、その音声優先度を維持します。

Cisco WLAN コントローラ（WLC）では、適切な DSCP 値がマーキングされていないビデオまたは音声パケットを、WLAN/SSID に設定された最高優先度にアップグレードするいくつかの方法を提供します。例えば、Windows コンピュータ上の Cisco Jabber のようなデスクトップクライアントに対してです。 ソフトウェア アプリケーションがオーディオおよびビデオ パケットを適切な DSCP 値でマーキングするようにコール制御サーバを設定できますが、Windows オペレーティング システムが QoS マーキングを実行できないデフォルトの設定である可能性があります。 そのため、ベスト エフォートの Wi-Fi メディア アクセスで AP にオーディオおよびビデオが送信されます。 ただし、AP からのアップストリームでは、ディープ パケット スヌーピングを使用してそれらのパケットを検査し、後続のパケット マーキングをアップグレードすることができます。

Cisco Enterprise Medianet 対応の Cisco Jabber アプリケーションは、メディアネット スイッチとのピア関係を利用できます。 メディアネット対応のクライアントアプリケーションは、以下の機能を通じて、ビデオおよびリッチ メディアに固有の課題を解決する組み込みのインテリジェンスな機能を提供します。

- ネットワークを介したビデオ パフォーマンスとエンドユーザの Quality of Experience（QoE）の拡張
- ビデオ エンドポイントのインストールと管理の簡素化
- 音声、データ、およびビデオ アプリケーションのより迅速なトラブルシューティング
- ビデオ、音声、およびデータがネットワークに及ぼす影響の評価機能

Wi-Fi クライアントからネットワークへのファースト ホップは、共有 Wi-Fi チャネルです。 クライアント デバイスからの Wi-Fi チャネルへのアクセスは、パフォーマンスに関するユーザの体感全体において最も影響があるポイントです。

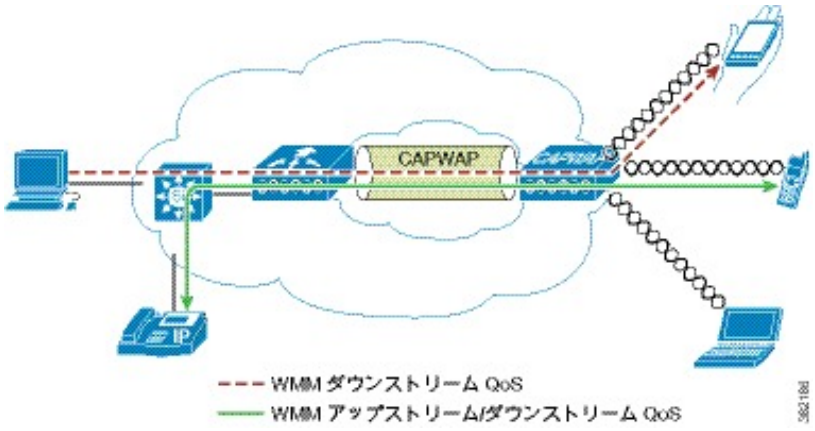
WLAN設定では、エンドポイントのWi-Fiクライアントから AP への（あるいはその逆の）パケットのマーキングに対して制御を行っていません。 アプリケーションの DSCP マーキング、オペレーティング システム、および WMM ドライバが、マーキング値と AC キューの制御を行っています。 そのため、最も重要なことは、ソース クライアントのこれらの 3 つの側面を管理することです。 エンドポイントの Wi-Fi クライアントで QoS の欠落によりファースト ホップで発生した遅延を、AP または AP からのアップストリームでディープ パケット インスペクションや再マーキング ロジックによって取り戻すことはできません。

# ワイヤレス QoS の導入スキーム

Cisco Unified Wireless 製品は、WMM（Wi-Fi Alliance 発行の IEEE 802.11e に基づいた QoS システム）、WMM Power Save、およびアドミッション制御をサポートしています。

次の図に、Cisco Unified Wireless テクノロジーの機能に基づくワイヤレス QoS の導入例を示します。

**図 *19*：*QoS* の導入例**




## QoS パラメータ

QoS は、通信の質およびサービスの可用性を反映した通信システムのパフォーマンスの基準として定義されています。 サービスの可用性は、QoS の重要な要素です。 QoS を正常に実装するには、ネットワーク インフラストラクチャがどのような状況下でも使用可能でなければなりません。 ネットワークの通信の質は、遅延、ジッタ、および損失で決まります。

表 *6*： *QoS* パラメータ

| 送信 | |
|---|---|
| **品質** | **説明** |
| 遅延 | 遅延は、パケットが送信エンドポイントから送信された後、受信エンドポイントに到達するまでの時間です。 この時間はエンドツーエンド遅延と呼ばれ、2 つの領域に分けられます。<br>• **固定ネットワーク遅延**：符号化および復号化の時間（音声およびビデオ）、および電気パルスまたは光パルスがメディアを通過して送信先へ届くまでの限られた時間が含まれます。<br>• **可変ネットワーク遅延**：伝送に必要な時間全体に影響を及ぼす可能性のある輻輳などのネットワークの状態を意味します。 |
| ジッタ | ジッタ（または遅延変動）は、パケット間のエンドツーエンド遅延の差です。 たとえば、あるパケットが発信エンドポイントから送信先エンドポイントまでネットワークを通過するのに 100 ms 必要であり、次のパケットは同じ伝送に 125 ms 必要である場合、ジッタは 25 ms となります。 |
| 損失 | 損失（またはパケット損失）は、送信されたパケットの合計数に対して正常に送受信されたパケットの比較測定です。 損失は、ドロップされたパケットの割合で表されます。 |

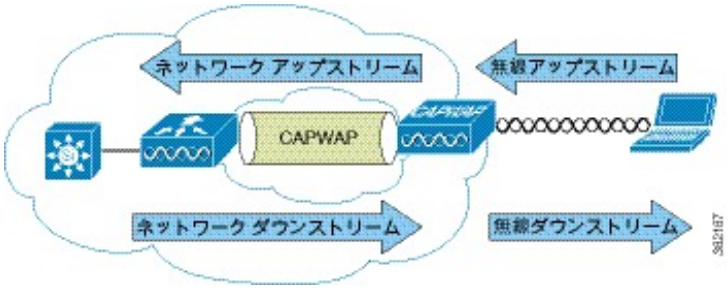
### アップストリーム QoS とダウンストリーム QoS

次の図は、無線アップストリームと無線ダウンストリームを定義し、次のものを示しています。

- **無線ダウンストリーム QoS**：AP から送出されて WLAN クライアントまで移動するトラフィック。 無線ダウンストリーム QoS は最も一般的な導入です。 無線クライアントのアップストリーム QoS は、クライアントの実装に依存しています。
- **無線アップストリーム QoS**：WLAN クライアントから送出されて AP まで移動するトラフィック。 WMM は、WMM をサポートする WLAN クライアントのアップストリーム QoS を提供します。
- **ネットワーク ダウンストリーム**：WLC から送出されて AP まで移動するトラフィック。 このポイントで QoS が適用され、AP へのトラフィックの優先度付けおよびレート制限を行うことができます。 イーサネット ダウンストリーム QoS の設定については、この章では取り上げません。

- **ネットワーク アップストリーム**：AP から送出されて WLC まで移動するトラフィック。 AP は、AP のトラフィック分類ルールに従って、AP からアップストリーム ネットワークへのトラフィックを分類します。

**図 *20*：アップストリーム *QoS* とダウンストリーム *QoS***




### QoS/WMM および Wi-Fi チャネル/ネットワークのパフォーマンス

負荷が軽いネットワークでは、QoS 機能のアプリケーションを検出できません。 ネットワークの負荷が増加するにつれて、アプリケーション パフォーマンスに QoS 機能が適用され始めます。 メディアの負荷が軽いときに遅延、ジッタ、および損失が測定される場合、システムで障害が発生している、ネットワーク設計が適切でない、またはアプリケーションの遅延、ジッタ、損失に関する要件がネットワークに適合していない、ということのいずれかを示しています。

QoS は、選択されたトラフィック タイプに対して遅延、ジッタ、損失を許容境界内に保持するように機能します。 AP から無線ダウンストリーム QoS のみが提供される場合、無線アップストリームのクライアント トラフィックはベストエフォートとして処理されます。 クライアントは、アップストリーム伝送において他のクライアントと競合し、AP からのベスト エフォート伝送とも競合します。 特定の負荷条件では、クライアントでアップストリームの輻輳が発生し、AP の QoS 機能にもかかわらず、QoS の影響を受けやすいアプリケーションのパフォーマンスは許容レベル以下となります。 アップストリームおよびダウンストリームの QoS は、AP および WLAN クライアントの両方で WMM を使用するか、WMM とクライアント独自の実装を使用することで、動作させることができます。

（注） WLAN クライアントの WMM へのサポートは、クライアント トラフィックが自動的に WMM の恩恵を得ているという意味ではありません。 WMM の利点を求めるアプリケーションが適切な優先度の分類をそのトラフィックに割り当て、オペレーティング システムはその分類を WLAN インターフェイスに渡す必要があります。 ワイヤレス音声ハンドセットなどの専用デバイスでは、その実装が設計の一部として統合されています。 ただし、パーソナル コンピュータなどの汎用プラットフォームに実装する場合に、良好な結果を得るためには、アプリケーション トラフィックの分類と OS サポートを最初に実装する必要があります。

# Wi-Fi マルチメディア

以前はワイヤレス マルチメディア拡張と呼ばれていた Wi-Fi マルチメディア（WMM）は、Wi-Fi における QoS を意味します。 QoS によって、Wi-Fi アクセス ポイントはトラフィックを優先度付けし、異なるアプリケーション間における共有ネットワーク リソースの割り当て方法を最適化できます。

ここでは、WMM 実装に関する次の 3 つの考慮事項について説明します。

- WMM アクセス
- WMM 分類
- WMM キュー

### WMM アクセス

WMM は、802.11e ドラフトの機能セットをサポートする Wi-Fi Alliance 認定です。 この認定はクライアントと AP の両方を対象にしており、WMM の動作を認定します。 WMM は主に 802.11e の拡張型分散コーディネーション機能（EDCF）コンポーネントの実装です。 新しく追加される Wi-Fi 認定では、802.11e の他のコンポーネントへの対応も予定されています。

### WMM 分類

WMM は、IEEE（現在は 802.1D 仕様の一部）によって開発された 802.1P 分類方式を使用します。

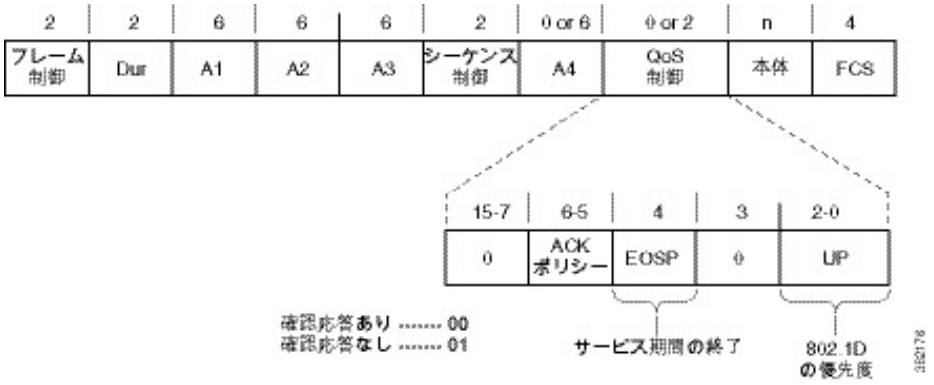
この分類方式には 8 つの優先度があり、WMM はそれらを 4 つのアクセス カテゴリ AC_BK、AC_BE、AC_VI、AC_VO にマッピングします。 これらのアクセス カテゴリは、次の表に示すように WMM デバイスで必要となる 4 つのキューにマッピングされます。

**表 *7*： *802.1P* および *WMM* 分類**

| 優先度 | 802.1P の優先度 | 802.1P での名称 | アクセスカテゴリ | WMM での名称 |
|---|---|---|---|---|
| 最低 | 1 | BK | AC_BK | バックグラウンド |
| | 2 | - | | |
| | 0 | BE | AC_BE | ベストエフォート |
| | 3 | EE | | |
| | 4 | CL | AC_VI | ビデオ |
| | 5 | VI | | |
| | 6 | VO | AC_VO | 音声 |
| 最高 | 7 | NC | | |

次の図に、WMM のデータ フレーム形式を示します。

**図 *21*：*WMM* のフレーム形式**



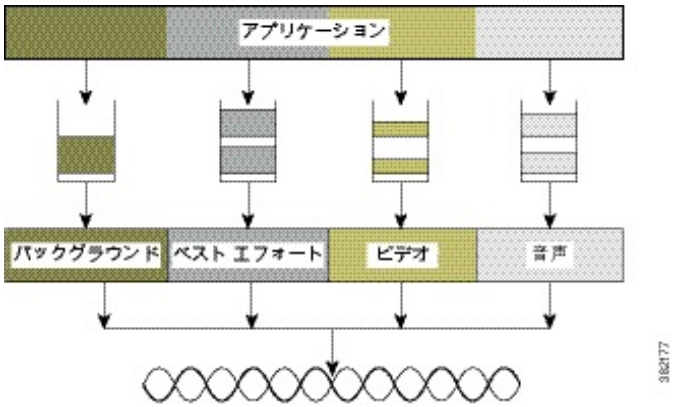

WMM が 8 つの 802.1P 分類を 4 つのアクセス カテゴリにマッピングしても、802.1D 分類はフレーム内に残したままで送信されます。

（注） IETF 推奨に基づき、シスコのネットワークで推奨および使用されている分類と WMM および IEEE 802.11e 分類は異なります。 分類の主な違いは、音声およびビデオ トラフィックがそれぞれ 5 および 4 に変更されたことです。 これにより、分類 6 をレイヤ 3 ネットワークの制御に使用できます。 両方の標準に準拠するため、Cisco Unified Wireless ソリューションはトラフィックがワイヤレスと有線の境界をまたぐ場合に、さまざまな分類標準の間で変換を実行します。

### WMM キュー

次の図に、WMM クライアントまたは AP で実行されるキューイングを示します。

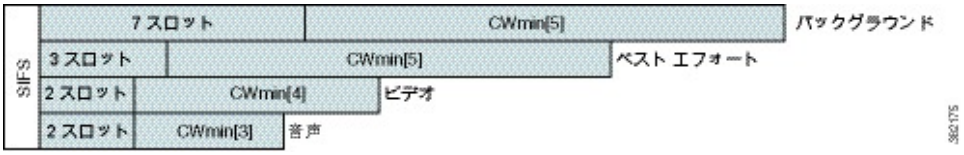
**図 *22*：*WMM* キュー**



アクセス カテゴリごとに 1 つずつ、4 つに分けられたキューが存在します。 これらの各キューはワイヤレス チャネルで競合します。EDCF で定義されるように、各キューで異なるフレーム間スペース、コンテンション ウィンドウ（CW）、最小コンテンション ウィンドウ（CWmin）、最大コンテンション ウィンドウ（CWmax）の値を使用します。 異なるアクセス カテゴリの複数のフレームが内部で競合した場合は、優先度の高いフレームが送信され、優先度の低いフレームは外部フレームと競合したときのように自身のバックオフパラメータをキューイング メカニズムに合わせて調整します。

次の図に、EDCF の背後にある原則を示します。ここでは、異なるフレーム間スペース、CWmin、CwMax の値がトラフィックの分類ごとに適用されます（明確にするため CwMax の説明は省略）。

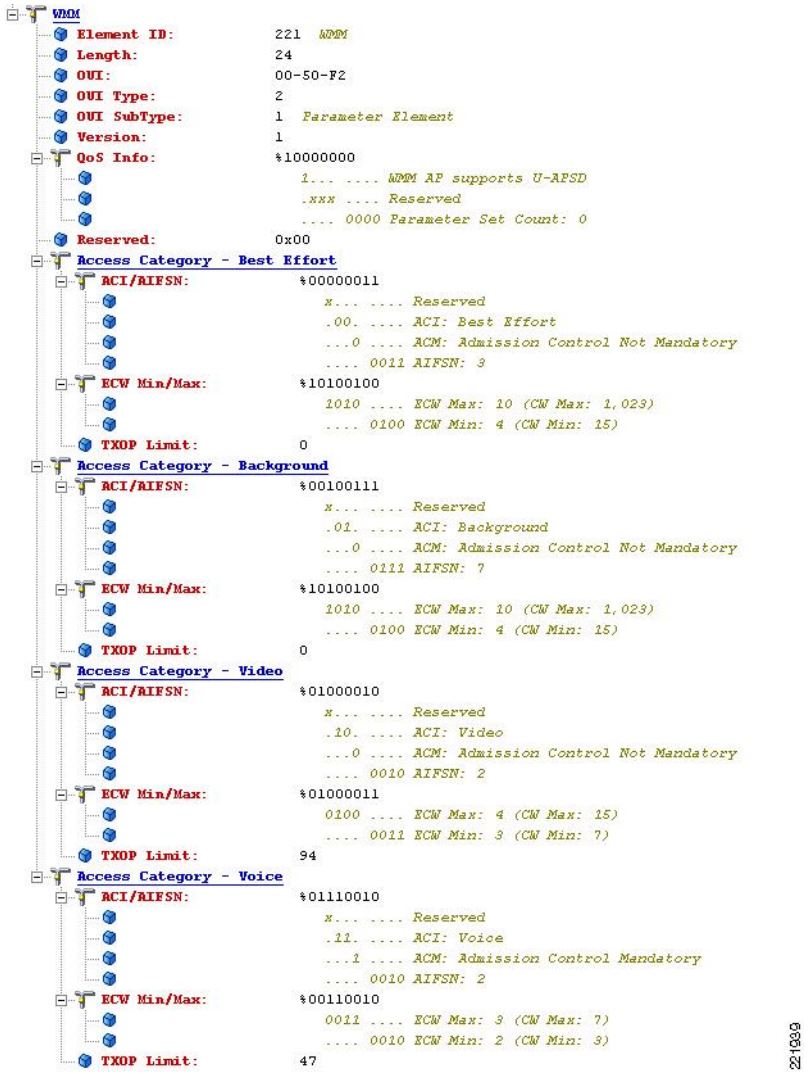
**図 *23*：アクセス カテゴリ（*AC*）のタイミング**




異なるトラフィック タイプはランダム バックオフのカウントダウンを実行する前に異なるインターフェイス スペースを待機でき、ランダム バックオフ数の生成に使用する CW 値もトラフィック分類に依存します。 たとえば、音声トラフィックの CWmin[3] は $2^3$-1 で、ベスト エフォート トラフィックの CWmin[5] は $2^5$-1 です。 優先度の高いトラフィックのフレーム間スペースは小さく、CWmin 値も低いため、ランダム バックオフも短くなります。一方、ベスト エフォート トラフィックのフレーム間スペースは長く、CWmin 値も大きいため、平均してランダム バックオフ番号も大きくなります。

次の図に、プローブ応答内の WMM 情報を示します。

**図 *24*：プローブ応答の *WMM* 要素情報**




クライアントの要素は、WMM AC 情報の有無だけでなく、アドミッション制御が必要な WMM カテゴリも定義します。 たとえば、上の図では音声 AC のアドミッション制御は [Mandatory] に設定されます。 この AC を使用するには、クライアントが要求を AP に送信し、その要求を受け付けさせることが必要です。

### Unscheduled Automatic Power-Save Delivery

Wi-Fi デバイスの WMM 機能である、Unscheduled Automatic Power Save Delivery（U-APSD）では、主な利点が 2 つあります。

- 音声クライアントは、AP における音声フレームの送受信を同期できます。これにより、クライアントは各音声フレーム タプルの送受信間に省電力モードに遷移できます。

U-APSD をサポートするアクセス カテゴリで WLAN クライアント フレームを伝送すると、AC の WLAN クライアントにキューイングされるデータ フレームを AP が送信します。U-APSD クライアントは、AP から End-of-Service Period（EOSP）ビットが設定されたフレームを受信するまで、AP をリッスンし続けます。 他にフレームがないことを示す EOSP ビットが設定されたフレームをクライアントが受信すると、クライアントは省電力モードに戻ります。 通常の Delivery Traffic Indication Map（DTIM）間隔によって制御される期間にビーコン方式をリッスンするよりも、このトリガー メカニズムではクライアントの電源をより効率的に使用できます。 これは、音声とビデオの遅延およびジッタの要件が、Voice and Video over IP（VVoIP）クライアントがコール中に省電力モードでないこと（通話時間が削減される）と、短い DTIM 間隔を使用すること（スタンバイ時間が削減される）のいずれかであるためです。

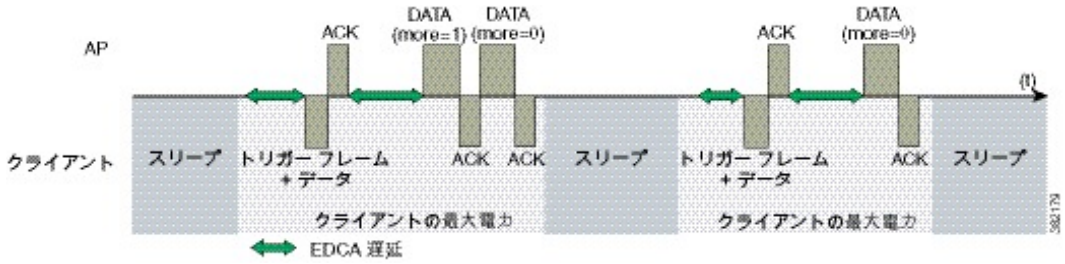
U-APSD では、DTIM 間隔を長く設定して使用し、コール品質に影響を与えることなくスタンバイ時間を最大化できます。 この機能は、アクセス カテゴリに依存することなく個別に使用できますが、AP における音声 AC だけは U-APSD を使用し、その他の AC は標準の省電力機能を使用します。

- コール キャパシティの向上

  AP からの伝送バッファ済みデータ フレームを WLAN クライアントからのトリガー データ フレームと結合することにより、AP からのフレームが一連のフレーム間スペースとランダム バックオフなしで送信されます。これにより、ネットワーク接続が減少します。

次の図に U-APSD を使用するトラフィック フローの例を示します。

**図 *25*：*U-APSD* のトラフィック フロー**

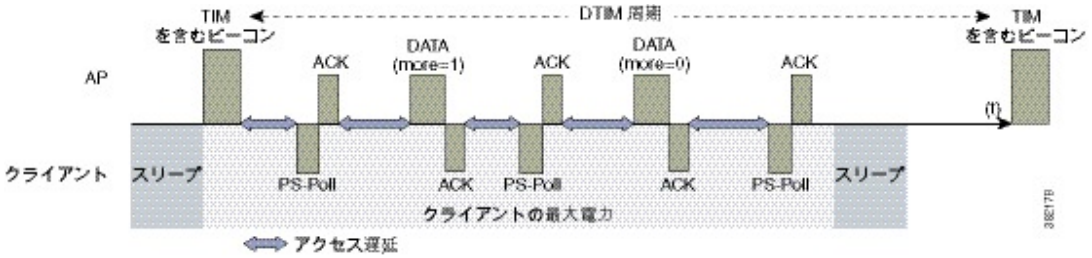



この例では、クライアントが AP に送信するトラフィックがトラフィック取得のトリガーになります。 AP はフレームを確認すると、データのキュー登録完了と待機をクライアントに知らせます。 次に、通常、最初のフレームだけ EDCF アクセス遅延のある Transmit Opportunity（TXOP）バーストのデータが AP からクライアントに送信されます。 そして、確認応答フレーム後の後続フレームがすべて直接送信されます。 Real-Time Traffic over WLAN の実装では、1 つのフレームだけが AP でキュー登録され、リアルタイム対応 WLAN クライアントは、AP からそのフレームを受信するとアイドル状態になります。

U-APSD アプローチでは以前の方式の欠点が改善されているため、効率性が向上しています。 音声およびビデオが対称型のクライアント トラフィックを使用して、ポーリングのタイミングが制御されます。 クライアントが 20 ミリ秒ごとにフレームを送信する場合は、20 ミリ秒の間隔ごとにフレームの受信を待機します。 これにより、n * 100 ミリ秒のジッタではなく、20 ミリ秒の最大ジッタになります。

次の図に、標準 802.11 の省電力配信プロセスにおけるフレーム交換の例を示します。

**図 *26*：標準のクライアント省電力**




省電力モードのクライアントは、まず AP ビーコンの Traffic Indicator Map（TIM）から、AP に待機中のデータがあることを検出します。 クライアントはデータを取得するために AP を省電力ポーリング（PS-Poll）する必要があります。 クライアントに送信されるデータに複数のフレームが必要な場合、AP は送信データ フレーム内でその旨を示します。 このプロセスでは、すべてのバッファ済みデータを取得するまで、クライアントが AP に PS-Poll を送信し続ける必要があります。

標準のクライアント省電力には 2 つの問題点があります。

- 分散制御機能（DCF）に関連付けられた標準のアクセス遅延が発生するため、PS-Poll と通常のデータ交換の効率が低下します。
- バッファ済みデータの取得は、ビーコン間隔の整数倍である DTIM に左右されます。 標準のビーコン間隔は 100 ミリ秒です。 これによって、音声通話やビデオ通話のジッタ レベルが許容されなくなり、音声およびビデオ対応ワイヤレス エンドポイントのハンドセットが、コール中に省電力モードからフル送受信の動作に切り替わります。

  標準のクライアント省電力モードでは、許容される音声およびビデオ品質が確保されますが、バッテリ寿命は短くなります。Cisco Unified Wireless IP Phone はPS-Poll 機能を提供してこの問題に対応します。この機能を使用して、電話はビーコン TIM を待たずに PS-Poll 要求を生成します。 これにより、デバイスはフレーム送信時にフレームをポーリングし、省電力モードに戻ることができます。この機能ではU-APSD と同程度の効率の向上は実現されませんが、U-APSD がなくてもWLAN における Cisco Unified Wireless IP Phone のバッテリ寿命は向上します。

### Traffic Specification のアドミッション制御

Traffic Specification（TSPEC）では、802.11e クライアントが自身のトラフィック要件を AP に通知できます。 802.11e のメディア アクセス コントロール（MAC）定義では、次の 2 つのメカニズムにより優先度付けされたアクセスが提供されます。どちらのメカニズムも Transmit Opportunity（TXOP）によって提供されます。

- 競合ベースの EDCF オプション
- 制御アクセス オプション

TSPEC 機能を使用してクライアントは自身のトラフィック特性を指定できます。この特性により、自動的に制御アクセス メカニズムが使用されます。 制御アクセス メカニズムでは、クライアントは TSPEC 要求に合わせるために特定の TXOP を付与できます。 ただし、リバース メカニ

ズムも使用可能になるので、EDCF におけるさまざまな AC の使用を制御するため、TSPEC 要求を使用できます。TSPEC メカニズムでは、クライアントは優先度タイプのトラフィックを送信する前に TSPEC 要求を送信する必要があります。

たとえば、音声 AC の使用が必須の WLAN クライアント デバイスでは、まず AC を使用する要求を作成する必要があります。 音声およびビデオ AC の使用は TSPEC 要求によって設定できますが、ベスト エフォートおよびバックグラウンド AC は TSPEC 要求なしで使用できます。

TSPEC 要求を満たすため、802.11e Hybrid Coordinated Channel Access（HCCA）ではなく EDCF AC を使用できます。これは、トラフィック パラメータはシンプルで、アプリケーション要件を満たす特定の TXOP を作成する代わりにキャパシティを割り当てて、要件を満たすようにすることができるためです。

### トラフィック ストリームの追加

トラフィック ストリームの追加（ADDTS）機能は WLAN クライアントが AP に対してどのようにアドミッション要求を実行するのかを制御します。 TSPEC 要求を AP に伝える場合は、次の 2 つの形式のアドミッション要求を使用できます。

- **ADDTS アクション フレーム**：音声通話やビデオ通話が AP にアソシエートしたクライアントによって開始または終了される場合に使用されます。 ADDTS には TSPEC が含まれており、トラフィック ストリーム レートセット（TSRS）情報要素（IE、Cisco Compatible Extension バージョン 4 クライアント）を含む場合もあります。
- **再アソシエーション メッセージ**：STA が他の AP にローミングしている場合に、再アソシエーション メッセージが 1 つの TSRS IE と 1 つ以上の TSPEC を含んでいると、再アソシエーション メッセージが使用されます。

ADDTS の TSPEC 要素はトラフィック要求を示しています。 データ レートおよびフレーム サイズに加えて、TSPEC 要素は AP にクライアント デバイスが使用する最小物理レートも通知します。 これは、ステーションが TSPEC における送受信で使用する時間を決定する際に役立ちます。そのため、AP は自身に TSPEC を満たすリソースがあるかどうか計算できるようになります。WLAN クライアント（VoIP ハンドセット）は、コールの開始やローミングの要求中に TSPEC アドミッション制御を使用します。 WLAN クライアントがローミングしている間、TSPEC 要求は再アソシエーション要求に追加されます。

### 関連トピック

Enterprise Mobility Design Guide

# クライアント接続のタイプ

次の図に、Cisco WLAN コントローラ（WLC）の [Monitor] > [Clients] ページを示します。このページには、クライアントが WLAN とのアソシエーションに使用する Wi-Fi プロトコルが表示されます。 この図では、プロトコルが 802.11bn であるため、クライアントは 2.4 GHz チャネルに接続されています。 また、クライアントを 802.11b、802.11g、802.11n にすることも可能です。 プ

ロトコルが 802.11an の場合、クライアントは 5 GHz チャネルに接続されます。 MAC アドレスのリンクをクリックすると、選択したクライアントの特性が表示されます。

**図 *27*：*WLAN* コントローラのクライアント**


次の図に、[Clients] > [Detail] ページを示します。このページには、WLC で使用できる詳細なクライアント情報が表示されます。 また、このページにはクライアントの接続ステータスに関する 3 つの重要なフィールドとその値が表示されます。

- [Current Tx-Rate-Set]：データ レートが示されます。ここでは m15 です。
- [RSSI]：-39 dBm の値は強い信号を意味します。

  リアルタイム トラフィック アプリケーションにおいて推奨される受信信号強度インジケータ（RSSI）は、セル エッジで -67 dBm の強さです。
- [QoS Level]：[Platinum] に設定すると、クライアントは最も高い WMM 優先度で送受信できます。

図 *28*：*WLAN* コントローラのクライアントの詳細ページ *1/2*

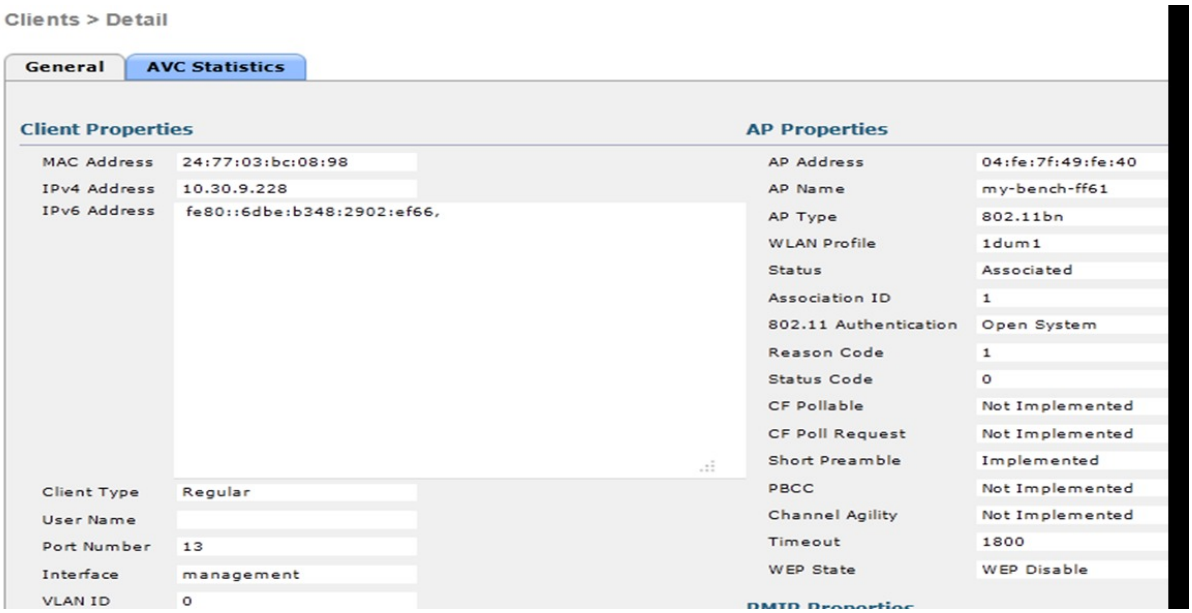
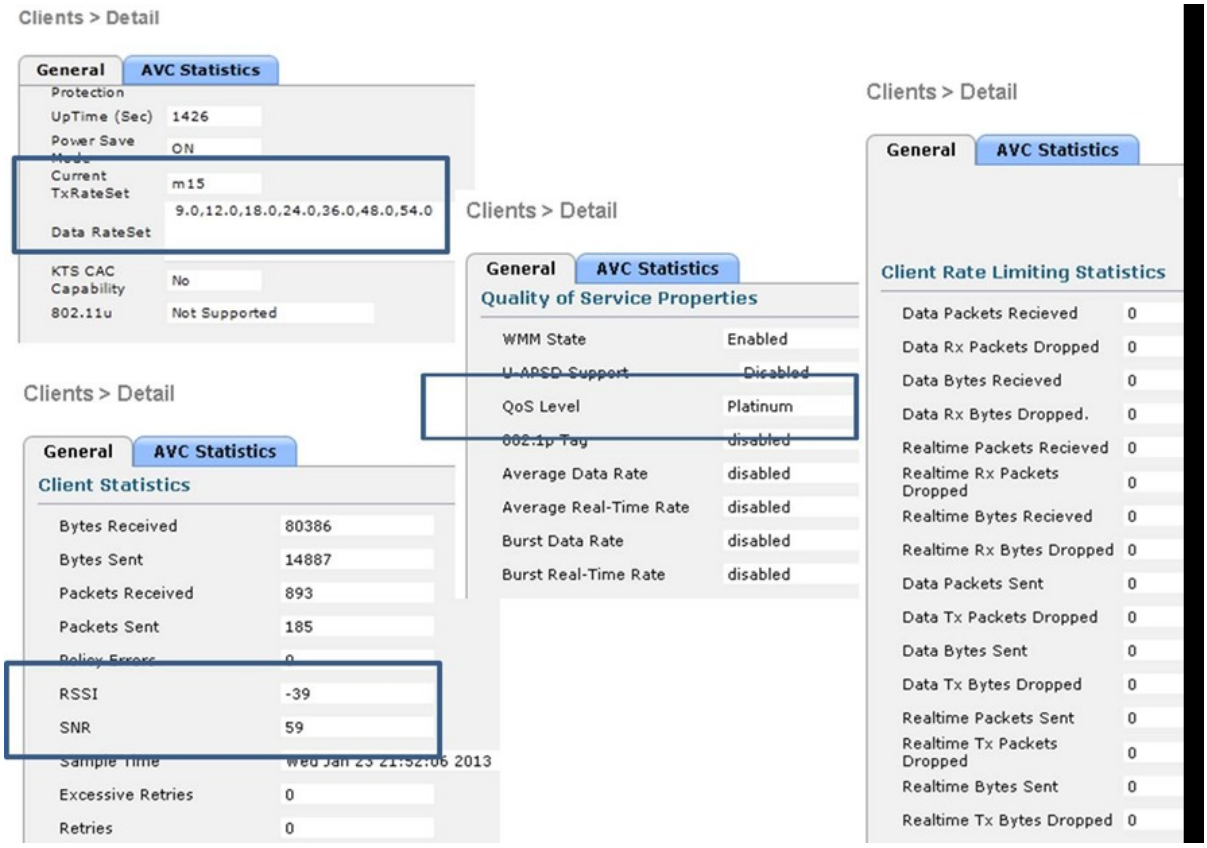


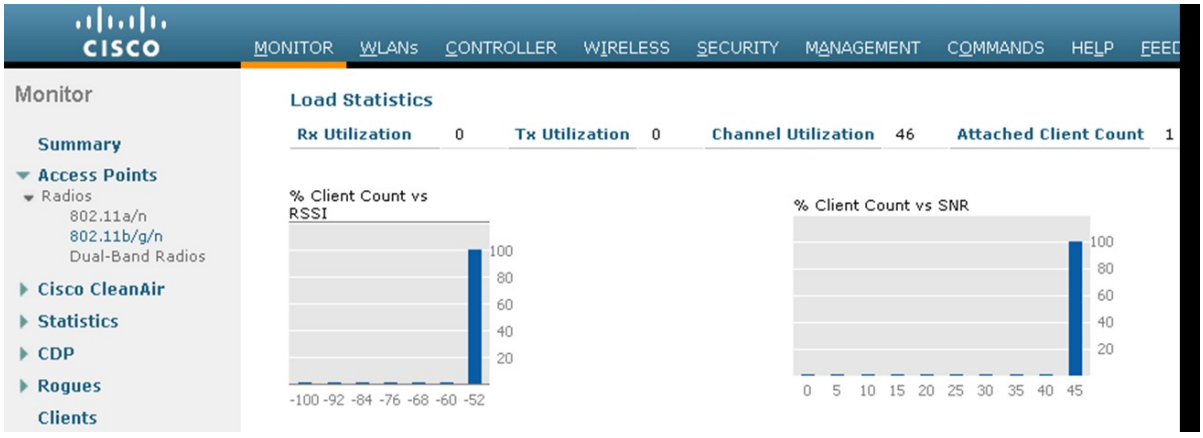
図 *29* : *WLAN* コントローラのクライアントの詳細ページ *2/2*




レート制限列の値は、このクライアントがレート制限プロファイルの一部でないことを示しています。

次の図に、クライアントにアソシエートした AP の負荷統計情報を示します。

図 *30* : *WLAN* コントローラのチャネル使用率



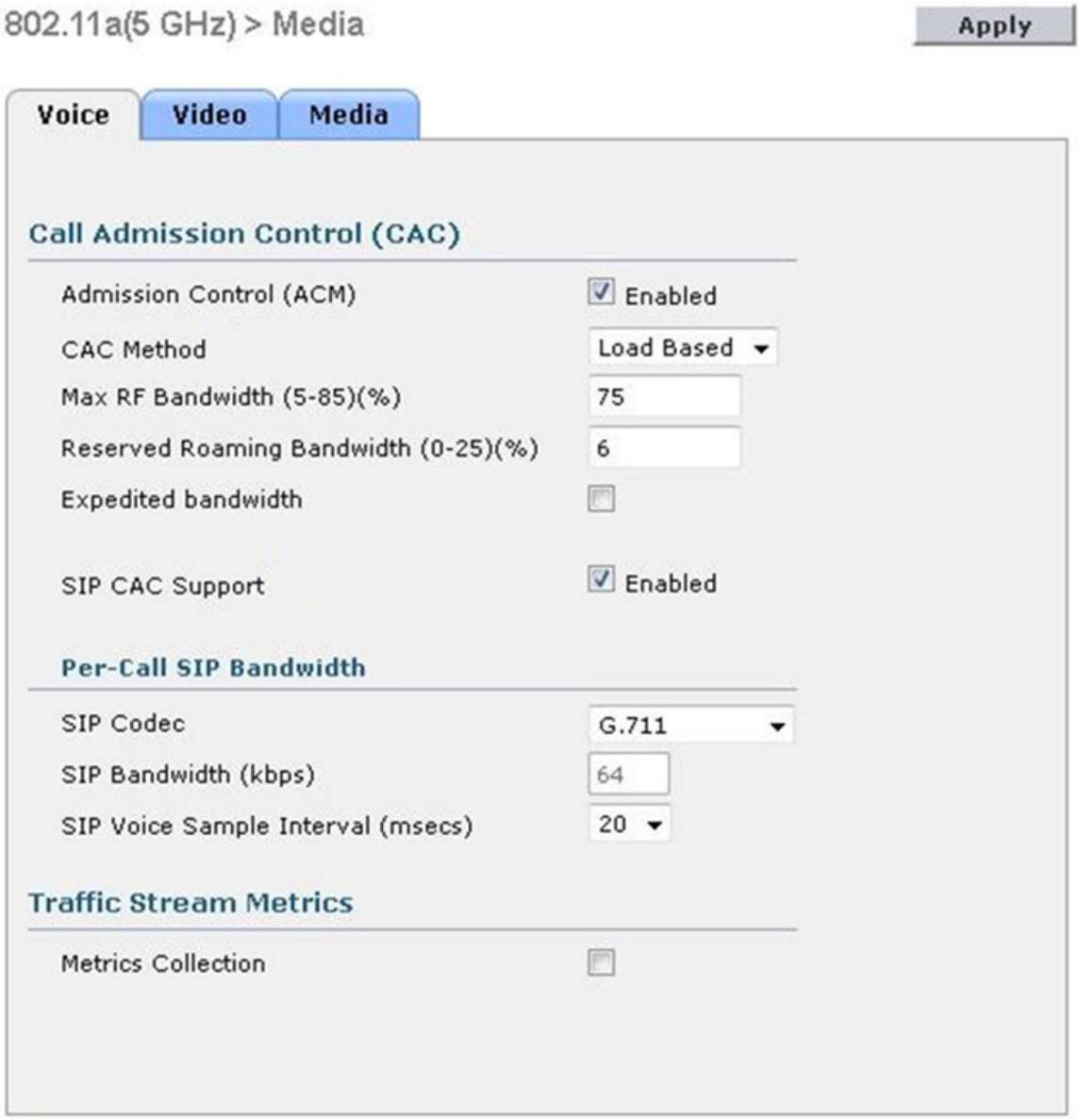

AP 無線は 802.11b/g/n で、AP およびクライアントのチャネル使用率は 46 % です。 互いに多くのパケットは送信していないので、クライアントと AP の使用率は両方とも 0 % です。 しかし、そ

の他の AP、その他のクライアント、干渉からのトラフィックにより、クライアントと AP が使用するチャネルは強いビジー状態になっています。

46 % のチャネル使用率は、チャネル使用率のワイヤレス パケット化された ALOHA 標準を上回っています。 チャネル使用率が 33 % に到達すると、ALOHA プロトコルは無線チャネルが制限に達したと定義します。つまり、チャネルがビジーになり、パケットは伝送されるまでオープンタイム スロットを待機する必要があります。 このチャネル使用率のレベルは、Wi-Fi 2.4 GHz チャネルでは珍しくありません。 このシナリオではチャネル帯域幅の管理に QoS を活用します。 これは、Wi-Fi コール アドミッション制御（CAC）の理由にもなります。 CAC は 802.11e 仕様の一部です。

次の図に、WLC CAC の設定ページを示します。

**図 *31*：*WLC* コール アドミッション制御の設定**




高品質なコールを維持して帯域幅を確保するには、ワイヤレス電話と他のデバイスのアドミッション制御必須（ACM）負荷ベース CAC が有効です。 負荷ベース CAC は、複数の AP 間で高レベルのチャネル再利用が見られる高密度導入において、最適な Wi-Fi 負荷を測定します。 シスコでは SIP CAC もサポートしています。 SIP CAC では、WLAN でメディア セッション スヌーピングが有効になっている必要があります。 CAC 方式が負荷ベースの場合、SIP CAC はチャネル負荷も使用します。 ほとんどのソフトフォンとスマートフォンはコール接続プロトコルに SIP を使用します。そのため、SIP CAC が重要になります。 新しい音声通話やビデオ通話が通過する帯域幅が不

十分なシナリオで、SIP CAC を有効にして TCP ベースの SIP クライアントを導入すると、WLAN ネットワークが SIP フレーム アップストリームおよびダウンストリームの転送を停止します。 クライアント コードの動作により、呼損になる可能性があります。 UDP ベースの SIP クライアントの SIP CAC である場合は、WLAN ネットワークが 486 Network Busy メッセージを送信します。 クライアント コードの動作に基づいて、クライアントは他の AP にローミングするかコール セットアップを終了します。 音声トラフィックの CAC 設定に加えて、ビデオおよびメディア トラフィック用のタブが用意されています。 これらには、CAC をビデオやメディアに拡張する設定オプションが含まれています。 これらのタブを活用すると、リアルタイムの音声およびビデオアプリケーションとメディア アプリケーション間で Wi-Fi チャネルの帯域幅をどのように分けるのか設定することができ、同様にデータ アプリケーションにどの程度の帯域幅を残すのか決定することができます。

SIP ベースの Cisco WLAN エンドポイントとモバイル クライアントを導入する場合は、TCP ベースの SIP と UDP ベースの SIP を使用するため、SIP CAC のサポートを無効にすることをお勧めします。

### 関連トピック

ALOHA モバイル ネットワーク プロトコル定義
WLC モデルに基づく CAC 設定の Cisco ワイヤレス LAN コントローラ設定

# WLAN インフラストラクチャの QoS 拡張機能

Cisco Centralized WLAN アーキテクチャには、WMM のサポートに加えて、複数の QoS 機能があります。 Cisco WLAN コントローラの QoS プロファイルは、QoS 拡張機能の実装における主要なメカニズムです。 次の 4 つの QoS プロファイルと、それに対応するトラフィック タイプがサポートされます。

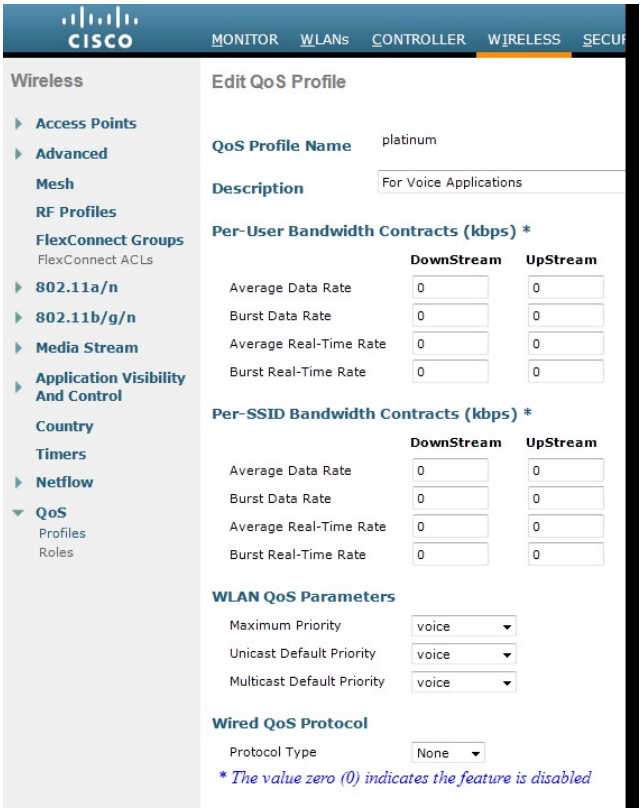
- Platinum：音声アプリケーション トラフィック
- Gold：ビデオ アプリケーション トラフィック
- Silver：ベスト エフォート トラフィック
- Bronze：バックグラウンド トラフィック

次の図に、Cisco WLAN コントローラで使用可能な 4 つの QoS プロファイルを示します。

図 *32* : ***WLAN*** コントローラの ***QoS*** プロファイル

帯域幅の契約、RF 使用制御、および許可された最大の IEEE 802.1P 分類をプロファイルごとに設定できます。

**図 *33* : *WLAN* コントローラの *QoS* プロファイルの編集**




[Per-User Bandwidth Contracts] 設定にデフォルト値を使用して、ディファレンシエーテッド サービスに IEEE 802.11 の WMM 機能を使用することをお勧めします。

特定のプロファイルを使用する WLAN に対しては、そのプロファイルの IEEE 802.1P 分類によって 2 つの重要な動作が制御されます。

- WLC から送信されるパケットに使用するサービス クラス（CoS）値を決定します。

  プロファイルに設定された CoS 値は、そのプロファイルを使用する WLAN のすべての CAPWAP パケットの CoS マーキングに使用されます。 そのため、Platinum QoS プロファイルを使用する WLAN の場合、IEEE 802.1P マークが 6 なら、コントローラの AP マネージャ インターフェイスから送信される CAPWAP パケットで CoS が 5 とマーキングされます。CoS は Cisco QoS ベースライン推奨事項に準拠するようにコントローラで調整されます。WLC へのネットワーク接続で DSCP ではなく CoS を信頼するようにネットワークが設定される場合は、CoS 値によって AP が受信する CAPWAP パケットの DSCP が決定され、さらに、この DSCP によって WLAN トラフィックの WMM 分類とキューイングが決定されます。これは、フレームの WLAN WMM の分類が、そのフレームを伝送する CAPWAP パケットの DSCP 値から算出されるためです。

- その WLAN に接続したクライアントが使用できる最大 CoS 値を決定します。

  IEEE 802.1P 分類によって、そのプロファイルを使用する WLAN で許可される最大 CoS 値が設定されます。

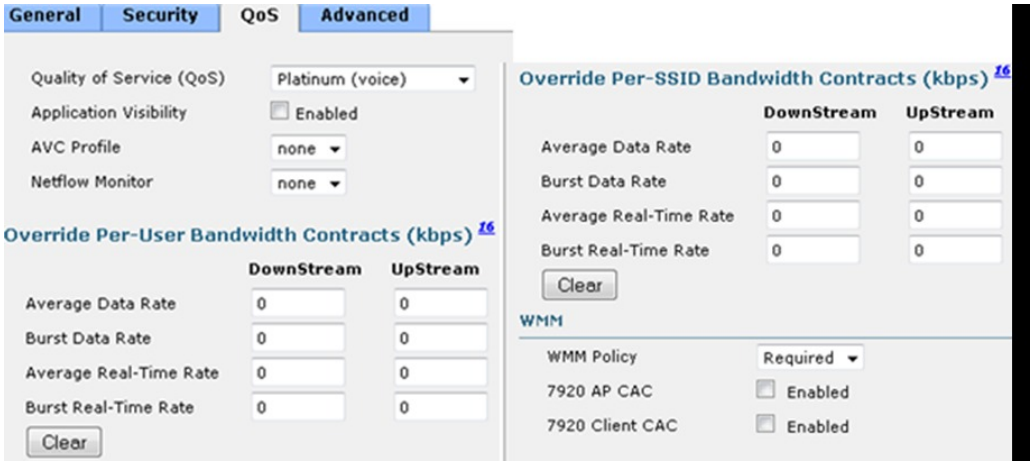
WMM 音声トラフィックは CoS 6 で AP に着信し、AP は CoS 6 に基づき、このトラフィックして自動的に CoS から DSCP へのマッピングを実行します。 WLC 設定の CoS 値が 6 より小さい値に設定されている場合は、この変更された値が AP の WLAN QoS プロファイルで使用され、使用する CoS マーキングの最大値と WMM AC が設定されます。

重要な点は、Unified Wireless Network では常に IEEE 802.11e 分類を考慮する必要があり、IEEE 分類と Cisco QoS ベースライン間の変換を Unified Wireless Network ソリューションで実行できるようにすることです。

[Per-User Bandwidth Contracts]、[Per-SSID Bandwidth Contracts]、および [WLAN QoS] パラメータの詳細については、WLC コードのリリースとモデルに対応した WLC 設定ガイドを参照してください。

次の図に示されるように、さまざまなデフォルト QoS プロファイルを使用して WLAN を設定できます。

**図 *34*：*WLAN* コントローラの *WLAN* デフォルト *QoS* プロファイルの設定**




各プロファイル（Platinum、Gold、Silver、Bronze）には、一般的な使用に対して注釈が付けられます。 さらに、認証、許可、およびアカウンティング（AAA）を使用して、ID に基づき QoS プロファイルをクライアントに割り当てることができます。 一般的な企業の場合は、ユーザごとの帯域幅の契約や Over-the-Air QoS などの WLAN 導入パラメータにデフォルト値を使用します。また、クライアントに最適な QoS を提供するには、WMM や有線 QoS のような標準の QoS ツールを使用する必要があります。

上の図に示されているように、QoS プロファイルに加えて WLAN ごとの WMM ポリシーも次のオプションで制御できます。

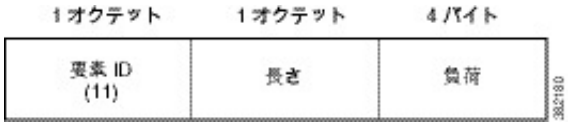
- [Disabled]：WLAN は WMM 機能をアドバタイズしません。または、WMM ネゴシエーションを許可しません。

- [Allowed]：WLAN は WMM クライアントと WMM 以外のクライアントを許可します。
- [Required]：WMM 対応クライアントのみを WLAN にアソシエートします。

### QoS Basic Service Set

次の図に Cisco AP で推奨される QoS Basic Service Set（QBSS）情報要素（IE）を示します。 **負荷** フィールドは AP で現在データ転送に使用されている使用可能な帯域幅の割り当てを示します。

**図 *35*： *QBSS* 情報要素**




使用中の QBSS は、WLAN 上の WMM とクライアントの設定に左右されます。 要件に基づき、次の 3 つの QBSS IE のタイプがサポートされます。

- 古い QBSS（ドラフト 6 [先行標準]）
- 新しい QBSS（ドラフト 13 IEEE 802.11e [標準]）
- 新しい分散型 CAC 負荷の IE（シスコの IE）

図 34：WLAN コントローラの WLAN デフォルト QoS プロファイルの設定, （77 ページ） に 7920 AP およびクライアント CAC、AP がビーコンに適切な QBSS 要素を含めるようにする WLAN コントローラ（WLC）の WLAN 設定のコンポーネントを示します。 Cisco Unified Wireless IP Phone のような QoS 要件のある WLAN クライアントは、これらの推奨 QoS パラメータを使用して、アソシエーションに最適な AP を決定します。

クライアントのコールアドミッション制御（CAC）の制限または AP CAC 制限を使用して、WLC は 7920 CAC サポートを提供します。 これらの機能は次のとおりです。

- **クライアント CAC 制限**：7920 クライアント CAC は古い QBSS 方式にマッピングされます。この方式は Clear Channel Assessment（CCA）ベースでなく、特定の AP における 802.11 トラフィックだけが計上されます。 クライアントは固定された CAC 制限を設定して、その制限に達すると発信コールを防ぐことができます。
- **AP CAC 制限**：7920 AP CAC は CCA ベースの新しい QBSS 方式にマッピングされ、その他の AP と同様に、ローカル AP の 802.11 トラフィックを含む RF チャネルのすべてのエネルギーが計上されます。また、802.11 以外のデバイス（電子レンジ、Bluetooth など）からのエネルギーも計上されます。 クライアントは固定された CAC 制限を設定して、その制限に達すると発信コールを防ぐことができます。

WMM、クライアント CAC 制限、AP CAC 制限のさまざまな組み合わせにより、次のように異なる QBSS IE が送信されます。

- WMM だけが有効な場合は、IE 番号 2（IEEE 802.11e 標準）の QBSS 負荷 IE がビーコン応答とプローブ応答で送信されます。

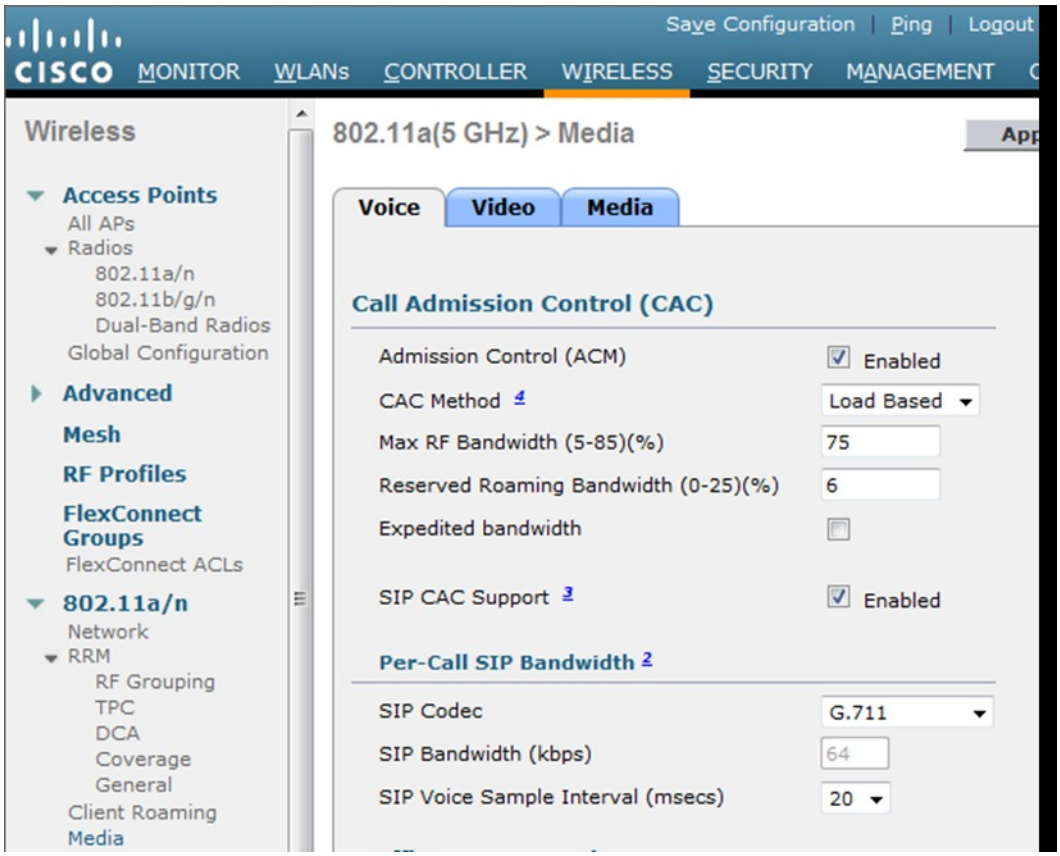
- 7920 クライアント CAC 制限をサポートする必要がある場合は、IE 番号 1（先行標準の QBSS IE）が bg 無線のビーコン応答とプローブ応答で送信されます。
- 7920 AP CAC 制限をサポートする必要がある場合は、番号 3 の QBSS IE が bg 無線のビーコン応答とプローブ応答で送信されます。

（注） さまざまな QBSS IE が同じ ID を使用するため、これら 3 つの QBSS は相互に排他的です。 たとえば、ビーコン応答とプローブ応答には QBSS IE を 1 つだけ含めることができます。

### アドミッション制御パラメータの設定

次の図に、コントローラにおける音声パラメータ設定の設定画面の例を示します。

**図 *36*：音声パラメータの設定**




SIP ベースの Cisco WLAN エンドポイントとモバイル クライアントを導入する場合は、TCP ベースの SIP と UDP ベースの SIP を使用するため、SIP CAC のサポートを無効にすることをお勧めします。

アドミッション制御パラメータは最大の RF 帯域幅で構成されます。この帯域幅では無線を使用でき、通常の ADDTS 要求により WLAN を介した音声通話やビデオ通話を開始させることができます。 予約ローミング帯域幅は、AP にローミングする通話中のコールがある RToWLAN クライアントに対して、アソシエーションまたは再アソシエーションの最中に ADDTS 要求へ応答するために予約するキャパシティです。

これらのパラメータに基づいてアドミッション制御を有効にするには、[Admission Control (ACM)] チェックボックスをオンにします。 これにより、AP のキャパシティに基づいてアドミッション制御が有効になりますが、エリア内の他の AP におけるチャネル負荷の影響の可能性は考慮されません。 このチャネル負荷をキャパシティに算入するには、[CAC Method] ドロップダウンで [Load Based] を選択し、[Admission Control (ACM)] チェック ボックスをオンにします。

次の図に、WCS で使用できる音声統計レポートの例を示します。このレポートには 1 つの AP の無線で確立されたコール数と、AP にローミングされたコール数が示されています。 このレポートや他の音声統計情報をスケジュールしたり、アドホック実行したりすることができます。また、これらはグラフィック表示されるか、データ ファイルとして書き込まれます。

**図 *37*：*WCS* からの音声統計情報**


（注） コール アドミッション制御は、音声およびビデオ QoS プロファイルのためにだけ実行されます。

### TSPEC アドミッション制御の影響

TSPECアドミッション制御の目的は、優先度の高いリソースを保護することです。 したがって、TSPEC アドミッション制御を使用していないクライアントが、そのトラフィックをブロックされることはなく、トラフィックの送信を試みると、そのトラフィックは再分類されます。クライア

ントが保護された AC で WMM に準拠したトラフィックを伝送している場合、これは必要ありません。

次の表では、トラフィック ストリームが確立されているかどうかに応じた、アドミッション制御を有効にした場合の分類への影響を説明します。

**表 *8*：アップストリーム トラフィック**

| | トラフィック ストリームが確立 | トラフィック ストリームなし |
|---|---|---|
| アドミッション制御なし | 動作に変化はなく、パケットはネットワークに送信されます。UP は max=WLAN QoS 設定に制限されます。 | 動作に変化はなく、パケットはネットワークに送信されます。UP は max=WLAN QoS 設定に制限されます。 |
| アドミッション制御 | 動作に変化はなく、パケットはネットワークに送信されます。UP は max=WLAN QoS 設定に制限されます。 | パケットは WMM クライアントのネットワークに送信される前に（CoS および DSCP 両方とも）BE に対して再マークされます。 WMM 以外のクライアントでは、パケットは WLAN QoS を使用して送信されます。 |

**表 *9*：ダウンストリーム トラフィック**

| | トラフィック ストリームが確立 | トラフィック ストリームなし |
|---|---|---|
| アドミッション制御なし | 変化なし | 変化なし |
| アドミッション制御 | 変化なし | パケットは WMM クライアントのネットワークに送信される前に（CoS および DSCP 両方とも）BE に対して再マークされます。 WMM 以外のクライアントでは、パケットは WLAN QoS を使用して送信されます。 |

# IEEE 802.11e、IEEE 802.1P、および DSCP マッピング

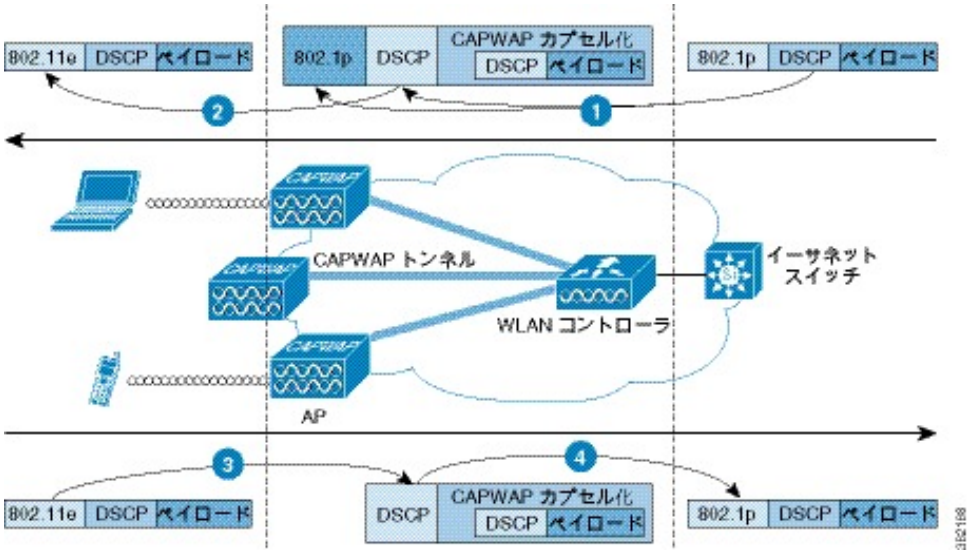
Unified Wireless Network 内の WLAN データは CAPWAP（IP UDP パケット）を介してトンネリングされます。 WLAN フレームに適用される QoS 分類を維持するためには、DSCP に対する分類と DSCP から CoS に対する分類のマッピング プロセスが必要です。

たとえば、WLAN クライアントが WMM 分類トラフィックを送信する場合は、IEEE 802.1P 分類をフレーム内に保持します。 AP はこの分類を、フレームを伝送する CAPWAP パケットの DSCP 値に変換する必要があります。これにより、WLC にパケットが到達すると適切な優先度で処理されるようになります。 AP に送信される CAPWAP パケットの場合も、同様のプロセスが WLAN コントローラ（WLC）で必要になります。

WMM 以外のクライアントからのトラフィックを分類するメカニズムも必要です。これにより、AP および WLC は WMM 以外のクライアントの CAPWAP パケットに適切な DSCP 分類を適用します。

次の図に、WMM クライアント、AP、WLC のトラフィック分類フローの例を、番号付きで示します。

**図 *38*：*WMM* と *IEEE 802.1P* との関係**




次に、トラフィック分類フローについて説明します。

1. 802.1P マーキングを持つフレームと IP DSCP マーキングを持つパケットが、WLC 有線インターフェイスに着信します。 パケットの IP DSCP は、WLC から送信される CAPWAP パケットの DSCP を決定します。
2. AP に着信する CAPWAP パケットの IP DSCP は 802.11e CoS マーキングに変換されます。
3. AP に着信するフレームの 802.11e CoS マーキングは CAPWAP DSCP 値に変換されます。この値は QoS プロファイルの最大値に制限されます。

4 WLC から送信されるパケットの DSCP は、WLAN クライアントから送信されたパケットの DSCP と同じです。 フレームの 802.1P 値は次の項目の影響を受けます。

- QoS 変換テーブル（表 10： アクセス ポイントの QoS 変換値, （84 ページ）を参照）
- WLAN の QoS プロファイル
- QoS プロファイル用に設定された有線 QoS プロトコル（図 33：WLAN コントローラの QoS プロファイルの編集, （76 ページ）を参照）

有線 QoS プロトコルが [None] に設定される場合、802.1p 値は設定されません。 ただし、プロトコルが 802.1p に設定される場合、使用される 802.1p は 802.1p テーブルの最大値が制限される変換テーブルの影響を受けます。

複数の分類メカニズムとクライアント機能には、複数の戦略が必要です。

- CAPWAP 制御フレームには優先度付けが必要で、CAPWAP 制御フレームは CS6 の DSCP 分類でマーキングされます。
- WMM を有効にしたクライアントには、対応する DSCP 分類にマッピングされたフレームの分類があります。対応する分類とは WLC に送信される CAPWAP パケットの DSCP 分類です。 このマッピングは QoS ベースラインへの準拠に必要な変更を除いて、IEEE CoS から DSCP へのマッピング標準に従っています。 この DSCP 値は、WLC で IEEE 802.1Q フレームの CoS 値に変換されます。このフレームは WLC インターフェイスから送信されます。
- WMM 以外のクライアントには、その WLAN のデフォルト QoS プロファイルに合わせて設定された CAPWAP トンネルの DSCP があります。 たとえば、ワイヤレス IP フォンをサポートする WLAN の QoS プロファイルが [Platinum] に設定されている場合、その AP WLAN からのデータ フレーム パケットは EF の DSCP 分類になります。
- WLC からの CAPWAP データ パケットは DSCP 分類になります。この分類は、WLC に送信される有線データ パケットの DSCP によって決定されます。 DSCP を WMM 分類に変換する AP テーブルは IEEE 80211.e 分類を決定します。この分類は AP から WMM クライアントにフレームを送信する際に使用されます。

（注） AP から WLAN クライアントへのトラフィックに使用される WMM 分類は、格納される IP パケットの DSCP 値でなく、CAPWAP パケットの DSCP 値に基づいています。 したがって、エンドツーエンドの QoS システムの整備が重要になります。

### QoS ベースラインの優先度のマッピング

CAPWAP AP と WLC は QoS ベースラインの変換を実行し、WMM 値が IEEE 値でなく、適切な QoS ベースライン DSCP 値にマッピングされるようにします。

表 *10*：アクセス ポイントの *QoS* 変換値

| トラフィック タイプ | IP DSCP | QoS プロファイル | 802.1p | IEEE 802.11e UP |
|---|---|---|---|---|
| ネットワーク間制御（CAPWAP 制御、802.11 管理） | 48（CS6） | Platinum | 6 | 7 |
| 音声 | 46（EF） | Platinum | 5 | 6 |
| インタラクティブ ビデオ | 34（AF41） | Gold | 4 | 5 |
| ミッション クリティカル | 26（AF31） | Gold | 3 | 4 |
| コール シグナリング | 24（CS3） | Gold | 3 | 4 |
| トランザクション | 18（AF21） | Silver | 2 | 3 |
| バルク データ | 10（AF11） | Bronze | 1 | 2 |
| ベストエフォート | 0（BE） | Silver | 0 | 0 |
| スカベンジャー | 2 | Bronze | 0 | 1 |

次の表に、AP（自律 AP など）が CoS 値を変換する場合の変換値を示します。

表 *11*：設定された優先度タイプによる *AP* の *WMM* パケットの再マーキング

| ダウンストリーム L2 パケットの再マーキング [1] | | | アップストリーム L2 パケットの再マーキング | | |
|---|---|---|---|---|---|
| 一般的なアプリケーション | CoS | WMM UP | 802.1d での名称 | WMM UP | CoS |
| ベスト エフォート データ | 0 | 0 | BE | 0 | 0 |
| 標準優先度のデータ | 1 | 2 | BK | 1 | 1 |

| ダウンストリーム L2 パケットの再マーキング [1] | | | アップストリーム L2 パケットの再マーキング | | |
|---|---|---|---|---|---|
| 一般的なアプリケーション | CoS | WMM UP | 802.1d での名称 | WMM UP | CoS |
| 高優先度のデータ | 2 | 3 | - | 2 | 1 |
| コール シグナリング | 3 | 4 | EE | 3 | 2 |
| ビデオ会議 | 4 | 5 | CL | 4 | 3 |
| 音声ベアラ | 5 | 6 | VI | 5 | 4 |
| 予約済み | 6 | 7 | VO | 6 | 5 |
| 予約済み | 7 | 7 | NC [2] | 7 | 7 |

[1] ダウンストリーム方向では、AP は有線インターフェイスで CoS マーキングを行い、示されている UP にマッピングします。アップストリーム方向では、AP は dot11 インターフェイスで受信した UP を付けて有線インターフェイスの CoS にマッピングします。この再マッピングを使用することで、最適な WMM AC と CoS の照合を実行できます。

[2] CoS=7にマッピングする必要がある唯一のネットワーク制御トラフィックとして、スパニングツリー トラフィックがあります。これは、ワークグループ ブリッジが導入されるとき、または複数の建物間で LAN 同士を接続する屋外型ブリッジが導入されるときに使用されます。 802.11 MAC 管理トラフィックが自律 AP 上で UP = 7 で伝送されても、AP の有線ポートにはブリッジされません。

### CAPWAP ベースの AP への QoS 機能の導入

QoS をワイヤレス AP に導入する場合は、次の点に注意してください。

- 有線 CAPWAP AP インターフェイスは、レイヤ 2 CoS（IEEE 802.1P）情報の読み込み/書き込みを実行します。 WLC と AP はレイヤ 3 分類（DSCP）情報によって WLAN クライアント トラフィック分類を通信します。 中間ルータはこの DSCP 値を変更できます。したがって、送信先で受信されたレイヤ 2 分類は CAPWAP トラフィックの送信元でマーキングされたレイヤ 2 分類を反映していません。
- AP では NULL VLAN ID が使用されなくなりました。 そのため、L2 CAPWAP は QoS を実質的にサポートしません。これは、AP が IEEE 802.1P/Q タグを送信せず、L2 CAPWAP にフォールバックする外部 DSCP がないためです。
- AP はフレームを再分類しません。CoS 値または WLAN プロファイルに基づいて優先度を決定します。
- AP は、無線出力ポートでのみ EDCF のようなキューイングを使用します。

- AP は、イーサネット出力ポートでのみファーストイン ファーストアウト（FIFO）キューイングを使用します。

### WAN QoS と FlexConnect

WLC に転送されるデータ トラフィックがある WLAN の場合、動作は FlexConnect 以外の AP（以前のハイブリッド リモート エッジ アクセス ポイントまたは H-REAP AP）と同じです。 WMM トラフィックがローカルにスイッチされた WLAN の場合、AP はアップストリーム トラフィックの 802.1Q VLAN タグに 802.1P 値をマーキングします。 これは、ネイティブ VLAN ではない、タグ付きの VLAN でのみ発生します。

ダウンストリーム トラフィックの場合、FlexConnect はイーサネット側から着信する 802.1Q タグを使用して、ローカルにスイッチされる VLAN の無線で WMM 値のキューイングとマーキングを行います。

アップストリームとダウンストリームの両方のパケットで WLAN QoS プロファイルが適用されます。 ダウンストリームでは、デフォルトの WLAN 値よりも高い IEEE 802.1P 値を受信すると、デフォルトの WLAN 値が使用されます。 アップストリームでは、クライアントがデフォルトの WLAN 値よりも高い WMM 値を送信すると、デフォルトの WLAN 値が使用されます。 WMM 以外のトラフィックでは、AP からのクライアント フレームに CoS マーキングは含まれません。

# ワイヤレス QoS 導入のガイドライン

有線ネットワークで QoS を導入するときに参考にするガイドラインは、ワイヤレス ネットワークで QoS を導入する場合でも使用できます。 QoS は追加の帯域幅は作成せず、その他のアプリケーションに割り当てられる帯域幅を優先度付けして最適化します。

ワイヤレス QoS の導入を成功させるには、ネットワークを通過するトラフィックのタイプとプロトコルを認識して、アプリケーション特有の遅延感度や帯域幅の要件を理解し、WLAN QoS を適切に設計および設定する必要があります。

### スループット

IEEE 802.11 QoS を導入する場合は、提供されるトラフィックを検討および理解することが重要です。 IEEE 802.11 スループットは提供されるトラフィックのフレーム サイズの影響を受けやすいため、ビット レートとフレーム サイズの両方について考慮する必要があります。

次の表に、フレーム サイズがスループットに及ぼす影響を示します。パケット サイズが小さくなるとスループットが低下します。

**表 *12*： フレーム サイズと比較したスループット**

| | 300 | 600 | 900 | 1200 | 1500 | フレーム サイズ（バイト） |
|---|---|---|---|---|---|---|
| 11g/a 6-54 Mbps | 11.4 | 19.2 | 24.6 | 28.4 | 31.4 | スループット（Mbps） |

| | 300 | 600 | 900 | 1200 | 1500 | フレーム サイズ（バイト） |
|---|---|---|---|---|---|---|
| 11b 1-11 Mbps | 2.2 | 3.6 | 4.7 | 5.4 | 6 | スループット（Mbps） |

たとえば、3 Mbps のレートでトラフィックを送信するアプリケーションが 11 Mbps の IEEE 802.11b ネットワークに導入され、300 バイトの平均フレーム サイズを使用する場合、アプリケーションがスループット要件を満たす AP の QoS 設定はありません。 これは、前述したスループットとフレーム サイズの組み合わせに必要なスループットを IEEE 802.11b がサポートできないためです。フレーム サイズが 1500 バイトの同じ送信トラフィック量では、スループットが向上します。

### QoS スイッチの設定

ここでは、次のワイヤレス インフラストラクチャ コンポーネントの有線 - 無線境界における、有線スイッチ ポートの設定について説明します。

- AP 有線スイッチの接続
- WLC 有線スイッチの接続

### AP 有線スイッチの接続

AP から送信されてスイッチを通過した CAPWAP パケットの DSCP をスイッチは信頼する必要があるため、AP スイッチの QoS 設定は比較的簡単です。 AP から送信された CAPWAP フレームにサービス クラス（CoS）マーキングはありません。

アクセス スイッチで IOS コマンド **mls qos trust dscp** を使用すると、WLC ポリシーで設定されるように AP の DSCP マーキングを信頼するようになります。 クライアント トラフィックに割り当てられる DSCP の最大値は、AP の WLAN に適用される QoS ポリシーに基づきます。

上記のコンフィギュレーション コマンドはパケット分類にのみ対応します。 ローカル QoS ポリシーに応じて、キューイング コマンドと他の QoS 関連の設定を追加できます。

### WLC 有線スイッチの接続

WLC 接続スイッチにおける QoS 分類は AP 接続スイッチよりも複雑です。これは、WLC から送信されるトラフィックの DSCP と CoS のどちらを信頼するのか決定する必要があるためです。QoS スイッチの設定を決定する場合は、次の事項が役立ちます。

- WLC から送信されるトラフィックには、アップストリーム（WLC またはネットワークが送信先）、またはダウンストリーム（AP および WLAN クライアントが送信先）のいずれかが考えられます。 ダウンストリーム トラフィックは CAPWAP カプセル化されており、AP および WLAN クライアントからのアップストリーム トラフィックは CAPWAP カプセル化されているか、WLC から送信されるカプセル化が解除された WLAN クライアント トラフィックのいずれかになります。

- WLC の QoS ポリシーは CAPWAP パケットの DSCP 値を制御します。 WLAN クライアントは DSCP 値を変更しません。この値は CAPWAP トンネル ヘッダーによってカプセル化された WLAN クライアント トラフィックに設定されます。
- WLC QoS ポリシーは、フレームのアップストリーム、ダウンストリーム、カプセル化、カプセル化解除にかかわらず、WLC から送信されるフレームの CoS 値を設定します。

IOS コマンド **mls qos trust cos** を使用すると、WLC の CoS 設定を信頼するようになります。 これにより、WLC 設定と追加ポリシーを WLC スイッチ接続で管理する代わりに、WLAN QoS を一元的に管理できます。 より精密な制御を望むユーザは、WLAN クライアントの VLAN に QoS 分類ポリシーを導入できます。

### ワイヤレス向けのアプリケーションの可視性およびコントロール（AVC）

シスコのワイヤレス AVC には、次の利点があります。

- アプリケーションレベルの最適化と制御により、すべてのワイヤレス ユーザの QoE が向上します。
- トラブルシューティング時間を短縮し、ネットワーク ダウンタイムを最短にする予防的なモニタリングと、エンドツーエンドのアプリケーションの可視性があります。
- アプリケーションの使用状況やパフォーマンスに関するより優れた可視性により、ネットワーク キャパシティの管理とプランニングを実行できます。
- Cisco Jabber の音声や IM セッションなど、ビジネスに不可欠なアプリケーションとサブフローの優先度付けを実行できます。

#### AVC の機能

ワイヤレス LAN コントローラの AVC には、他のシスコ製品の AVC に相当する機能があります。 AVC アプリケーション認識は WLAN/SSID まで設定可能です。 各 WLAN はさまざまな AVC パラメータをオプションで有効にできます。これにより、独自の WLAN を構成できます。 WLAN は、クライアントが認証およびアソシエーションに使用する SSID の名前を定義します。 また、同じ WLAN 設定で、Wi-Fi チャネルを介したパケット伝送における Wi-Fi QoS の最高レベルも定義されます。 AVC プロファイルによって再マーキングされたパケットには、WLAN 設定で定義された QoS 優先度を上回るものはありません。 たとえば、WLAN がゲスト ユーザ向けにベスト エフォートの QoS 優先度レベルで作成される場合などです。 AVC ポリシーがパケットをオーディオパケットと認識していても、音声およびビデオのパケットはベストエフォート優先度で伝送されます。 ゲスト SSID は、「FaceTime」コールをベスト エフォート優先度に制限するように設定できます。 また、同じゲスト SSID は、「You Tube」をブロックする AVC プロファイルを使用するように設定できます。これにより、同じ Wi-Fi チャネルを共有する他の SSID に、より多くの帯域幅が提供されます。

WLAN にアソシエートしている Wi-Fi クライアントの場合、ワイヤレス LAN コントローラの AVC はディープパケットインスペクションを介したアプリケーション認識を使用し、ワイヤレス LAN コントローラの AVC 設定ごとに個々のアプリケーションのパケット処理方法を決定します。 ワイヤレス LAN コントローラは、パケットをブロックする場合とパケットの QoS マーキングを変更する場合のコントロール ポイントです。 ユーザは、FaceTime アプリケーションが FaceTime コールを確立するサーバに接続しないようにブロックできます。 このブロックはワイヤレス LAN

コントローラで実行します。AVCプロファイルがアプリケーションをブロックする場合でも、クライアントデバイスはWLANにアソシエートしたままです。 FaceTimeアプリケーション パケットを再マーキングするAVCプロファイルが作成された場合、その再マーキングはワイヤレスLANコントローラで実行されます。 再マーキングは、アップストリームおよびダウンストリームの方向で実行されます。 アップストリーム トラフィック（APを通過するWi-Fiエンドポイントからワイヤレス LAN コントローラまでのトラフィック）の場合、ワイヤレス LAN コントローラから送信先のエンドポイントに転送されるパケットまで、パケットが再マーキングされます。AVCは発信元クライアントでのQoSパケット マーキングや、これらのパケットのマーキングを制御できません。これは、マーキングがAPからワイヤレスLANコントローラに転送されるためです。 ダウンストリーム トラフィック（ワイヤレス LAN コントローラにより AP を通過して Wi-Fi エンドポイントに転送されるエンドポイント パケット）の場合、パケットの再マーキングはワイヤレス LAN コントローラで実行されます。 AP は、FaceTime トラフィックに 802.11e/WMM QoS 優先度を付与して WLAN に転送します。この優先度は、AVC FaceTime プロファイルで割り当てられる DSCP 値を表しています。

CAPWAP は、AP およびワイヤレス LAN コントローラを接続するプロトコルです。 CAPWAP パケットは IP アプリケーション パケットをカプセル化します。 アップストリームをマーキングするCAPWAP QoSパケットは、エンドポイントアプリケーションパケットにおけるWi-Fiヘッダーの 802.11e/WMM QoS 値に基づきます。 一方、ダウンストリームをマーキングする CAPWAP QoS パケットは、WLAN設定に基づきます。 FaceTimeの例では、CAPWAPパケットにおけるヘッダーの DSCP 値は、FaceTime 向けの AVC プロファイルで設定された DSCP 値によって、ワイヤレス LAN コントローラで割り当てられます。 ユーザは、ワイヤレス LAN コントローラごとに AVC プロファイルを設定し、WLAN に割り当てることができます。

（注） ワイヤレスLANコントローラ バージョン7.4以降のAVC設定オプションは、ワイヤレスLANコントローラの設定ガイドでワイヤレスLANコントローラのリリース コードバージョン番号別に提供されています。 Cisco.com からワイヤレス LAN コントローラのリリース設定ガイドをダウンロードすることができます。 個別の WLC/AVC 設定ガイドは、ワイヤレス LAN コントローラのソフトウェア ページと同じシスコ製品ページで、ワイヤレス LAN コントローラのハードウェア タイプ別に公開されています。

### AVC のバージョン

AVC のワイヤレス LAN コントローラ バージョンは、ワイヤレス LAN コントローラの一部として実行されます。追加のライセンスは必要ありません。 ワイヤレス LAN コントローラの AVC は、Cisco ワイヤレス LAN コントローラ リリース 7.4 で使用できるようになりました。

ワイヤレスLANコントローラのAVCでサポートされるのは、Network Based Application Recognition（NBAR）プロトコル パックの FTP/TFTP ロードです。プロトコル パックのリリースは、ワイヤレス LAN コントローラのリリースに組み込まれている NBAR エンジンのバージョンと一致します。 たとえば、ワイヤレス LAN コントローラ リリース 7.5 は、NBAR エンジン バージョン 13 を使用します。 したがって、リリース 7.5 向けにリリースされたプロトコル パックは、pp-AIR-7.5-13-4.1.1.pack と同様の番号になります。

次のワイヤレス LAN コントローラ CLI コマンドを実行すると、プロトコル パックと AVC エンジンのバージョンを確認できます。

- **show avc protocol-pack version**
- **show avc engine version**

Cisco.com に掲載されているワイヤレス LAN コントローラのソフトウェア リリース バージョンと同じダウンロード ページから、AVC NBAR2 プロトコル パックをワイヤレス LAN コントローラのタイプ別にダウンロードできます。

### トラフィック シェーピング、Over-the-Air QoS、および WMM クライアント

トラフィック シェーピングと Over-the-Air QoS は WLAN WMM 機能が存在しない場合に便利なツールですが、直接 IEEE 802.11 トラフィックを優先度付けする場合には役立ちません。 WMM クライアントまたはワイヤレス ハンドセットをサポートする WLAN では、トラフィック シェーピングまたは Over-the-Air QoS を使用せずに、これらのクライアントの WLAN QoS メカニズムを使用する必要があります。

### 関連トピック

Enterprise QoS Solution Reference Network Design Guide
Cisco Solutions for Enterprise Medianet: Optimizing Networks for Video, Voice, and Data
Data Values for DiffServ Code Point and Type of Service Parameters
Cisco AVC テクノロジーおよび製品

第 4 章

# Real-Time Traffic over WLAN のセキュリティ

ワイヤレス LAN（WLAN）システムのセキュリティは、すべての WLAN 導入において常に重要な考慮事項になります。 暗号化によって拡張され、プライバシーを確保する認証、許可、およびアカウンティング（AAA）の原則に応じて WLAN アクセスの制御は異なります。 この章では、RToWLAN の導入における WLAN セキュリティの認証および暗号化に焦点を当てて説明します。

WLAN セキュリティの詳細については、『*Enterprise Mobility Design Guide*』（http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob73dg/emob73.html）を参照してください。



## Real-Time Traffic over WLAN のセキュリティの概要

802.11 ワイヤレス LAN は共有ネットワーク アクセス メディアであるため、WLAN インフラストラクチャの無線周波数（RF）範囲内のすべての WLAN デバイスから、WLAN トラフィックを確認できます。

WLAN の共有ネットワーク アクセスでは、次の課題が発生します。

- 不正なユーザまたはデバイスから WLAN のユーザおよびデバイスのプライバシーをどのように確保するか。

- WLAN の認証済みユーザとデバイスのプライバシーを確保する方法
- マルチキャストおよびブロードキャスト WLAN トラフィックのプライバシーを確保する方法
- WLAN のユーザとデバイスを区別する方法

WLANセキュリティの各世代は、これらの課題をそれぞれの方法で解決してきました。しかし、主要なメカニズムは、信頼できないメディアの通信を安全にするために使用される共通の戦略、つまり認証と暗号化に基づいています。

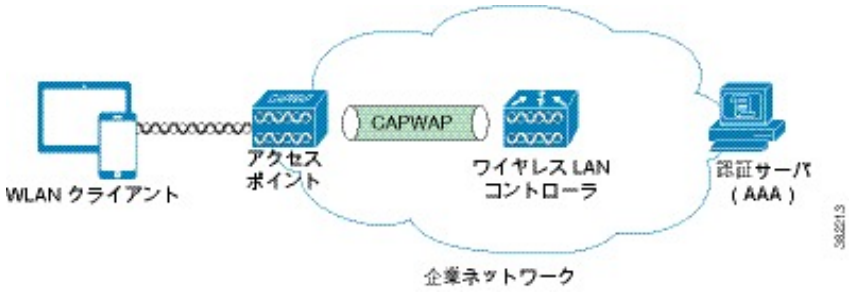
# 802.11 セキュリティ スキーム

リアルタイム トラフィック対応の WLAN を導入する場合に、実装できる 802.11 セキュリティ スキームがいくつかあります。ネットワーク管理者が使用するセキュリティ スキームの種類は、導入される WLAN ネットワーク インフラストラクチャと特定の RToWLAN クライアント デバイスによってサポートされる機能により異なります。

次の図に、WLAN セキュリティの基本コンポーネントを示します。ワイヤレス ネットワークを通過するセキュア ネットワーク接続と暗号化トラフィックの実装に必要なコンポーネントは、次のとおりです。

- ワイヤレス クライアント デバイス
- ワイヤレス アクセス ポイント（AP）
- ワイヤレス LAN コントローラ（WLC）
- 認証または AAA サーバ

**図 *39*：セキュアなワイヤレス *LAN* トポロジ**




RToWLAN 対応のクライアント デバイスと RToWLAN サービスを導入するベスト プラクティスとして、WLANで有効なセキュリティ メカニズムは、次の内容を実現するユーザおよびデバイス認証と、トラフィックの暗号化を実行できる必要があります。

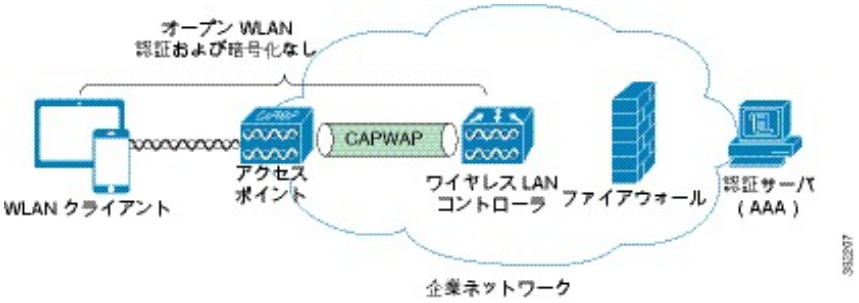
- 認証済みのユーザおよびユーザ デバイスだけにネットワークへのアクセス権が付与される
- 傍受および盗聴からリアルタイム トラフィック フローを保護する

### オープン セキュリティ スキーム

オープン セキュリティ スキームでは、WLAN に対するクライアント デバイス アクセスで暗号化と認証を行いません。

次の図に、オープン WLAN のセキュリティ トポロジを示します。

**図 *40*：オープン ワイヤレス *LAN* のセキュリティ トポロジ**




WLAN では、すべての 802.11 対応デバイスの接続がオープンです。 このセキュリティ スキームでは不正アクセスからネットワークを保護できず、傍受および盗聴からもユーザおよびクライアント トラフィックを保護しないため、企業の WLAN 導入には一般的に不適切と考えられています。 ただし、暗号化と認証を実行できなくても、基本的なインターネット接続を目的としたゲスト アクセスや、個人所有デバイスの持ち込み（BYOD）シナリオにおける個人用デバイスまたは社内用以外のデバイスの持ち込みなど、導入する目的によってはオープン WLAN のサービス セット ID（SSID）が役立ちます。

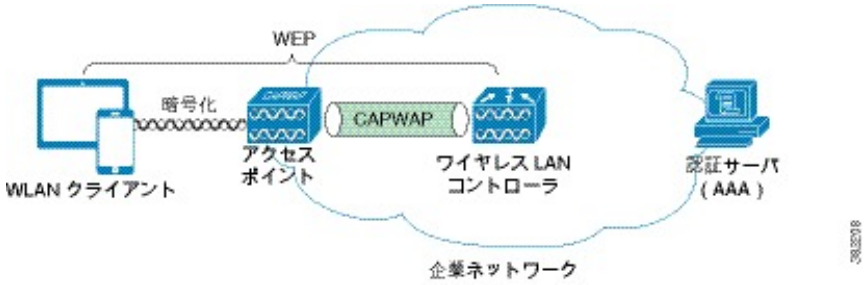
BYOD の導入の場合、セキュアな無線 SSID や企業のネットワークで接続に必要な拡張のネットワーク管理やセキュリティでの認証及び権限付与が必要となる前に、全てのユーザや端末が無線 LAN に接続できるオープン ネットワークを提供します。 これらのシナリオでオープン セキュリティ スキームを構築する場合、オープンな SSID の無線ネットワークから他のセキュアな企業ネットワークへ不正なアクセスを防止できるようネットワークを分離する必要があることに注意してください。

### Wired Equivalent Privacy

Wired Equivalent Privacy（WEP）セキュリティ スキームは、クライアント端末が WLAN に接続するためにユーザまたは端末を認証する場合、共有キーによる暗号化を最低限提供します。 次の図

に、WLAN クライアント デバイス - WLAN インフラストラクチャ AP および WLC 間における WEP 暗号化の WEP セキュリティ トポロジを示します。

**図 *41*： *WEP* ワイヤレス *LAN* のセキュリティ トポロジ**




オリジナルの 802.11 標準では、WEP 暗号化メカニズムが定義されていますが、認証メカニズムは定義されていません。 オリジナルの 802.11 標準で提供される認証レベルは、グループ内のすべてに同じ静的暗号キーを使用する必要があるグループ レベルのものでした。 また、このキーはユニキャスト、マルチキャスト、ブロードキャスト トラフィックの暗号化に使用されていました。 WLAN セキュリティ ソリューションがクライアント MAC アドレスを認証することで、このグループ認証はさらに拡張されています。 しかし、クライアント MAC アドレスを認証するこのソリューションでは、次の理由により、セキュリティの大幅な改善が実現していません。

- WEP キーがすべてのユーザで共有されることに変更はなく、ユーザ別のプライバシーは追加されていません。
- WEP キーの管理が困難です。WEP キーを 1 つでも変更する必要があると、すべてのデバイスを更新する必要があります。
- 802.11 MAC アドレスは暗号化されずに送信され、MAC アドレスはユーザではなく WLAN クライアント デバイスを識別するという認証の脆弱性が存在します。
- クライアント デバイスの MAC アドレスのデータベースを維持する必要があるため、大規模なユーザ グループにおける MAC アドレス認証の管理が困難です。

802.11 標準で実装された MAC アドレス認証あり/なしのオリジナル WEP 暗号化方式は、静的設定に基づいていました。 動的 WEP メカニズムの導入で静的な WEP キー実装が改善される一方で、WEP 暗号化メカニズムの問題が静的および動的 WEP の両方のセキュリティの脆弱性となる可能性があります。 WEP 暗号化メカニズムの問題自体は、クライアント トラフィックをモニタリングすることで WEP キーが導き出すことができるという事実に関連しています。

### Wi-Fi Protected Access

WEP の脆弱性とソリューションに対する需要により、Wi-Fi Alliance は 802.11i ワークグループを通して WLAN セキュリティの改善を実施しました。 これらの改善は Wi-Fi Protected Access（WPA）として定義されています。 Temporal Key Integrity Protocol（TKIP）を代わりに使用することで、WPA は WEP 暗号化の主な脆弱性を解決しました。 WPA と 802.11i 標準の関連セクションには多少の相違点がありますが、これらの相違点をユーザが意識することはありません。 WPA で使用される 802.11i 標準のセクションは、主に WEP との十分な下位互換性を維持して WLAN を保護す

るニーズを満たし、現在導入しているハードウェアを更新または置き換える必要がないようにします。 TKIP は WEP（RC4）の暗号化エンジンのコアを再利用するため、WPA はソフトウェアまたはファームウェアを更新することで、大半のシステムに実装できます。 WPA ではオリジナルの WEP 定義に存在しなかった認証メカニズムの不足も解決され、さらに WEP との組み合わせで使用される MAC アドレス認証の実装も可能です。

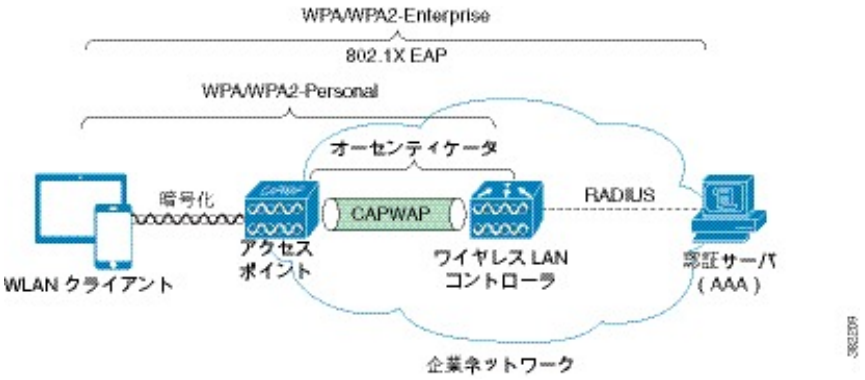
### Wi-Fi Protected Access 2

WPA で開発されたセキュリティ機能は、802.11i ワークグループの推奨事項に基づいています。802.11i ワークグループとは、802.11 標準で定義されていたオリジナルのセキュリティ機能に代わる機能を開発するためのグループです。 WPA で採用された 802.11i のセキュリティ変更が重要である一方、802.11i 標準の主要なコンポーネントは、暗号化における最新の業界標準となる暗号化メカニズム、Advanced Encryption Standard（AES）を WLAN セキュリティに使用しています。 AES カウンタ モード CBC-MAC の基本メカニズムは、WPA と WEP のメカニズムとは大きく異なり、通常はハードウェアの更新がサポートされる必要があります（AES カウンタ モードは暗号化メカニズムを、CBC-MAC はフレーム保護メカニズムを意味します）。 WPA2 では AES のサポートが可能です。 WPA2 における AES 暗号化のサポートに必要なハードウェア要件によると、WPA からの移行は、ほとんどの場合ハードウェアの更新または置換に依存します。 多くの場合、WLAN クライアントインフラストラクチャを更新するよりも、ネットワークインフラストラクチャを更新するほうが簡単です。また、WPA2 への完全移行は、WLAN クライアント インフラストラクチャの世代間の変更によっても異なります。 また、WPA から WPA2 に移行するかどうか検討する場合は、現在 WPA には既知の重大なセキュリティ問題が存在しないことを考慮してください。

### WPA と WPA2：Enterpris および Personal

次の図に、WPA と WPA2 が定義する 2 つの異なるセキュリティ スキーム（WPA/WPA2-Personal および WPA/WPA2-Enterprise）を示します。

図 *42*： *WPA /WPA2* ワイヤレス *LAN* のセキュリティ トポロジ




- **WPA/WPA2-Personal**

  WPA/WPA2-Personal は、WPA/WPA2-Enterprise と同じ暗号化ツールを使用しますが、WLAN クライアントの認証に共有キーを使用します。 WPA-Personal で使用される認証の共有キー メカニズムでは、ユーザ単位またはデバイス単位の認証は行われません。 したがって、対象の WLAN SSID の一部となっているすべてのデバイスと AP は、同じ共有キーを使用します。

一方、暗号化に使用されるキーは、初期の 4-Way Handshake におけるランダム化により、ユーザ単位およびセッション単位で固有ですが、認証に使用される共有キーはすべてにおいて共通です。 RToWLAN 導入における WPA/WPA2-Personal の主な利点は、AAA サーバを使用する必要がないことです。これは、規模のより小さい導入や、中央サイトまたは大規模な地域サイトから分かれた拠点サイトが 1 つ以上存在するマルチサイト導入に適用されます。

（注） WPA/WPA2-Personal セキュリティ スキームを採用する場合は、強固なキーを使用するように注意してください。これは、WPA/WPA2-Personal に対するディクショナリ攻撃を効果的に実行するツールが存在するためです。

- **WPA/WPA2-Enterprise**

  WPA/WPA2-Enterprise は、WPA/WPA2-Personal と同じベース WPA フレーム保護および暗号化機能を使用しますが、拡張認証プロトコル（EAP）ベースの認証を行う 802.1X をスキームに追加します。 EAP ベース認証を行う 802.1X では、AAA 認証サーバを使用する必要があります。

### WPA/WPA2-Enterprise と WPA/WPA2-Personal

通常、企業の RToWLAN 導入には、WPA/WPA2-Personal ではなく WPA/WPA2-Enterprise の使用が適しています。 WPA/WPA2-Personal は通常、ホーム ユーザまたは小規模オフィスの導入を対象にしています。 共有キー セキュリティ システムには、エンタープライズで通常必要とされる認証機能はありません。また、RToWLAN クライアント デバイスが紛失したり、盗難にあったり、通常のキー ローテーション制度の一部であったりする場合は、共有キーの更新時のオーバーヘッドが原因で動作上の問題が発生します。

共有キーはすべてのユーザとデバイスに使用されるため、キーのクラッキング、推測、盗難に成功した場合のメリットは非常に高くなります。 これは、RToWLAN の導入に WPA/WPA2-Personal を使用できないことを意味しているわけではありません。 AAA 認証サーバの企業セキュリティ要件と、RToWLAN ハンドセット要件や RToWLAN 導入の特性のバランスを取る必要があります。リアルタイム トラフィック サービスおよびアプリケーションでは一般的にハイ アベイラビリティが求められますが、集中認証システムに依存する拠点やリモート環境でハイ アベイラビリティを実現することは困難です。 集中認証に対する依存を排除するように、ワイヤレス LAN コントローラのローカル AAA 認証サーバまたは組み込み AAA サービスを使用して、認証データベースを拠点に分散させると、この問題を解決できます。または、WLAN システムに RToWLAN を導入して、WPA/WPA2-Personal を活用します。

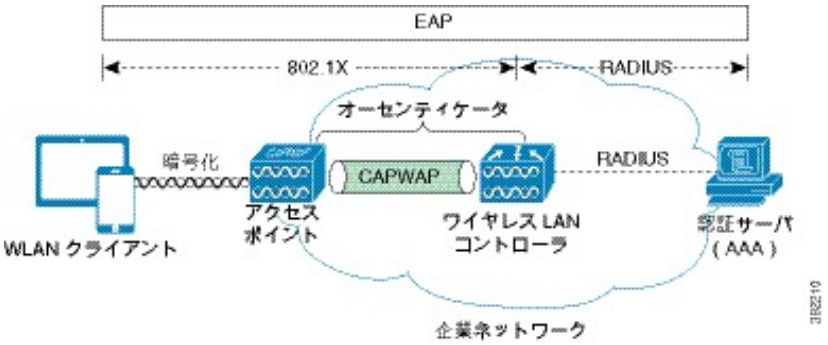
### 関連トピック

802.1X および拡張認証プロトコル, （97 ページ）
802.11 暗号化, （100 ページ）

# 802.1X および拡張認証プロトコル

企業レベルのWLANセキュリティを確保するため、802.1Xおよび拡張認証プロトコル（EAP）の認証メカニズムが実装されて、WLAN と WLAN クライアント デバイスの相互認証が実現されました。 次の図に、基本の 802.1X および EAP 認証のセキュア トポロジを示します。

**図 *43*： *802.1X* および *EAP* ワイヤレス *LAN* のセキュリティ トポロジ**




802.1X はポートベースのネットワーク アクセス コントロール向け IEEE 標準のことで、802.11i セキュリティ標準ワークグループで採用されました。 802.1X標準は、次のロジックを使用して802.11無線 LAN ネットワークに対する認証アクセスを実現します。

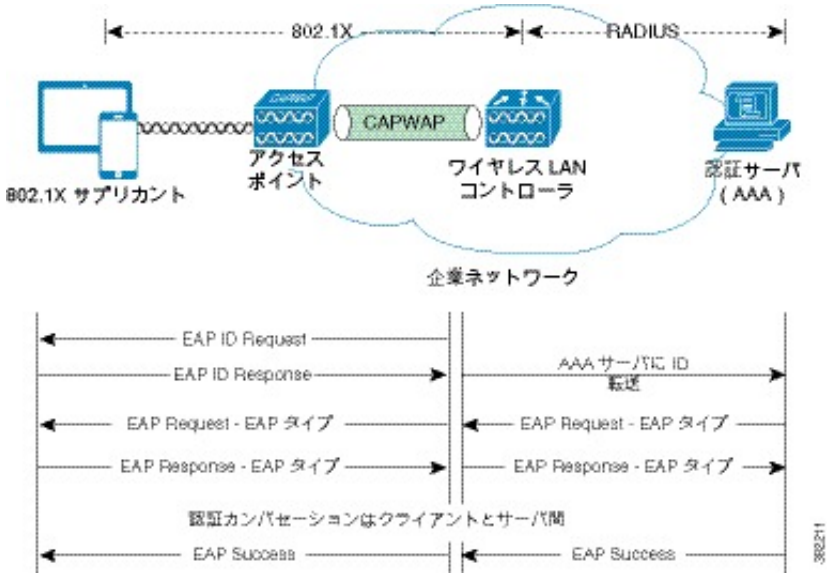
- 802.11 のアソシエーション プロセス中、AP で WLAN クライアント デバイスごとに仮想ポートが作成されます。
- 次に、AP はこの仮想ポートの 802.1X ベース トラフィック以外のすべてのデータ フレームをブロックします。
- EAP 認証パケットは 802.1X トラフィック フレームで伝送され、AP およびワイヤレス LAN コントローラによって AAA 認証サーバに渡されます。
- EAP 認証に正常に完了すると、認証サーバは EAP 成功のメッセージをワイヤレス LAN コントローラと AP に送信し、WLAN クライアント デバイスにそのメッセージが渡されます。
- 次に、AP は WLAN クライアント デバイスからの（音声およびビデオを含む）データ トラフィックを仮想ポートに経由させます。
- データ トラフィックが通過できるように仮想ポートを開く前に、クライアント デバイスと AP 間でデータ リンクの暗号化が確立されます。

認証プロセス中に固有のユーザ単位/セッション単位共有キーが派生され、このキーの一部がセッション単位暗号キーとして使用されます。

EAP認証プロセスでは多くのプロトコルがサポートされます。最終的に使用されるプロトコルは、WLAN クライアント デバイスのサプリカントや WLAN インフラストラクチャの機能によって異

なります。 使用される EAP タイプに関係なく、すべてのプロトコルは一般的に次の図の EAP フローの例で示されるように動作します。

図 *44* : ***EAP*** プロトコルのフロー




RFC 3748 で定義されているように、EAP では EAP 認証プロセスの過程で 4 つのタイプのパケットがサポートされます。

- **EAP Request（要求）**

  オーセンティケータ（上の図ではワイヤレス LAN コントローラと AP の組み合わせ）によって 802.1X サプリカント（上の図では WLAN クライアント デバイス）に送信された要求パケットです。 各 EAP 要求には、要求対象を示す特定のタイプがあります。 図の例では、最初の EAP 要求は WLAN クライアント デバイス ID を、次の EAP 要求は認証に使用される EAP タイプを対象にしています。 シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。

- **EAP Response（応答）**

  応答パケットは、WLAN クライアント デバイスによって AP およびワイヤレス LAN コントローラに送信され、開始された EAP 要求に一致するシーケンス番号を使用します。 ID またはタイプの応答の場合、ワイヤレス LAN コントローラによって応答は認証サーバに転送されます。

- **EAP Success（成功）**

  上の図に示されているように、認証カンバセーションで WLAN クライアント デバイスまたはユーザが適切なクレデンシャルを使用していると、AAA サーバはワイヤレス LAN コントローラに EAP 成功パケットを送信し、AP を経由して WLAN クライアント デバイスにもパケットが送信されます。

- **EAP Failure（失敗）**

適切なクレデンシャルが WLAN クライアント デバイスで使用されていない場合や、その他の障害が発生した場合、AAA サーバはワイヤレス LAN コントローラに EAP 障害パケットを送信します。コントローラは AP を経由してパケットを WLAN クライアント デバイスに送信し、結果として認証が失敗します。

# RToWLAN EAP の共通サプリカント タイプ

ここでは、RToWLAN EAP の次の共通サプリカント タイプについて説明します。

- EAP-FAST
- EAP-TLS
- PEAP

### EAP-FAST

EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）プロトコルは、802.11i 以前のシスコ独自の Lightweight EAP（LEAP）に代わるものです。 LEAP は特に、RToWLAN IP ハンドセットのような専用デバイスやアプリケーション特有の処理能力が限られている点を考慮して設計されました。 10 文字より少ない脆弱なパスワードが LEAP 認証トランザクションの分析によって生成されることがあるという LEAP のセキュリティ問題を念頭に置きながら、LEAP の「軽快な」特質も維持することも考慮して、EAP-FAST はこれらのセキュリティ問題に対応するため設計されました。

EAP-TLS で使用される TLS トンネルの設定にアソシエートする公開キー インフラストラクチャ（PKI）のオーバーヘッドを必要とせずに、EAP-Transport Layer Security（TLS）のようなトンネル認証プロトコルと同じトンネリング保護を実現するため、EAP-FAST は設計されています。 EAP-FAST は通常、クライアント デバイスと認証サーバ間のトンネル認証に Protected Access Credential（PAC）を使用します。 自動の PAC プロビジョニングを使用していても、PAC が傍受されるとそれを使用してユーザ クレデンシャルにアクセスします。 手動の PAC プロビジョニングの使用中やプロビジョニング中に認証サーバ証明書をオプションで使用すると、このような潜在的な脅威を軽減できます。

トンネル化プロトコルの EAP-FAST は、Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2（MSCHAPv2）や汎用トークン カード（GTC）などの複数の内部認証メカニズムをサポートしています。 サポートされる内部認証メカニズムは。RToWLAN クライアントの実装によって異なります。

### EAP-TLS

EAP-TLS プロトコルは、PKI を使用してトンネル認証保護を実現し、WLAN クライアント デバイスと WLAN ネットワーク インフラストラクチャの両方を認証します。 EAP-TLS は、ユーザとサーバの認証やダイナミック セッション キーの生成に証明書を使用します。 このため、クライアント証明書と認証サーバ証明書を両方ともインストールする必要があります。 EAP-TLS は高度なセキュリティを実現しますが、クライアント証明書の管理が必要となります。

### PEAP

Protected EAP（PEAP）は、WLAN クライアント デバイスと認証サーバによる認証交換の保護に TLS を使用します。 PEAP MSCHAPv2 の場合は、MSCHAPv2 を使用してトンネルを経由し、この認証交換をカプセル化します。 PEAP GTC では、トンネルを経由して汎用トークン カードを交換し、認証プロセスが保護されます。

# 802.11 暗号化

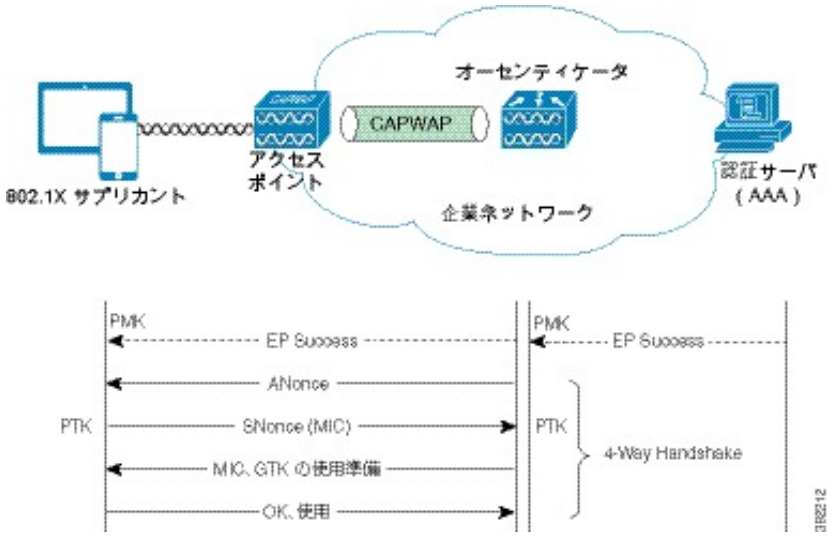
暗号化は 802.11 WLAN セキュリティの重要なコンポーネントであり、ローカル RF のブロードキャスト ネットワークに対してプライバシーを提供するために必要です。 WLAN クライアント デバイスとインフラストラクチャが許可する場合、RToWLAN 導入はネットワーク通信を保護する WPA または WPA2 セキュリティ メカニズムの一部として TKIP または AES 暗号化を活用します。これは、それらの高度なメカニズムが提供する優れたセキュリティ機能によるものです。 WPA および WPA2 セキュリティ メカニズムでは、暗号キーの派生メソッドにより WEP 暗号化が大幅に改善されます。

WPA および WPA2 の暗号キーは 4 方向暗号ハンドシェイクを使用して派生されます。WLAN クライアントと WLAN AP 間で共有されるキーは暗号化に直接使用されず、代わりに暗号キーを派生する 4 方向ハンドシェイクの基本として使用されます。 この 4 方向ハンドシェイクは、WPA/WPA2-Personal と WPA/WPA2-Enterprise の両方で使用されます。

EAP 認証中に相互で生成した Pair-wise Master Key（PMK）から、暗号化に使用されるキーが生成されます。 この PMK は EAP Success メッセージのオーセンティケータに送信されますが、サプリカントには転送されません。これは、サプリカントがコピーした PMK 自体で生成するためです。

次の図に、WPA/WPA2-Enterprise で使用される 4 方向ハンドシェイク メカニズムの基本を示します。

図 *45* : ***WPA/WPA-2 Enterprise*** におけるワイヤレス暗号キー生成用の *4* 方向ハンドシェイク



1. オーセンティケータは、オーセンティケータ ナンス（ANonce）が含まれている EAP over LAN（EAPOL）キー フレームを送信します。ANonce は、オーセンティケータによって生成されるランダムな番号です。（Nonce：Number used once）
   a. サプリカントはサプリカント ナンス（SNonce）を生成します。これは、サプリカントで生成されるランダムな番号です。
   b. サプリカントは、ANonce および SNonce から Pair-wise Temporal Key（PTK）を生成します。
2. サプリカントは、SNonce および Message Integrity Check（MIC）を含んだ EAPOL キー フレームを送信します。
3. オーセンティケータは ANonce と SNonce から PTK を生成し、EAPOL キー フレームの MIC を検証します。
4. 検証が成功すると、オーセンティケータは Group Temporal Key（GTK）を含んだ EAPOL キー フレーム、マルチキャスト、ブロードキャスト暗号キーを送信します。
5. このフレームの MIC を検証するときに、サプリカントは PTK と GTK を組み込みます。
6. サプリカントは EAPOL キー フレームを送信し、これらの一時キーが組み込まれたことを確認します。
7. このフレームの MIC を検証するときに、オーセンティケータはクライアントの PTK を組み込みます。

この時点で、サプリカントとオーセンティケータには両者に一致する PMK があり、両者が同じ PTK と GTK を共有していることを検証します。

上の図で示されているように、WPA/WPA2-Enterprise では、4 方向ハンドシェイクで暗号キーを生成するときに使用する共有キーが、802.1X EAP 認証プロセス中に生成されます。 この EAP 認証プロセスでは、WPA/WPA2-Personal には存在しない AAA 機能を使用できます。これにより、各ユーザまたはデバイス個別の認証、適用される認証 ID（許可）に基づくポリシー、認証 ID に基づく統計情報の収集（アカウンティング）が可能になります。

WPA/WPA2-Enterprise と WPA/WPA2-Personal の動作の違いは、4 方向ハンドシェイクが、WLAN クライアント デバイスのサプリカントと WLC で設定された共有キーを使用することです。WPA-Personal で使用される認証の共有キー メカニズムでは、ユーザ単位またはデバイス単位の認証は行われません。 したがって、対象の WLAN SSID の一部となっているすべてのデバイスと AP は、同じ共有キーを使用します。 一方、WPA/WPA2-Enterprise の場合と同様に、暗号化に使用されるキーはユーザ単位およびセッション単位で固有になります。これは、最初の 4 方向暗号化ハンドシェイク中に実行されるランダム化によるものです。

# キーのキャッシングと管理

RToWLAN クライアント デバイスにおいて、正常に WLAN ネットワークが認証されてトラフィック フローの暗号化メカニズムが確立されると、アソシエートした AP 経由でトラフィックを安全に送受信できるようになります。 しかし、RToWLAN デバイスが WLAN ネットワークの一部から別の場所に移動またはローミングした場合はどうなるでしょうか。また、WLAN で他の AP に

アソシエートする必要があるのでしょうか。 このような状況で、RToWLAN クライアント デバイスのユーザが音声通話中またはビデオ通話中である場合は、できるだけ早くクライアント デバイスを新しい AP にアソシエートすると同時に、実装されたセキュリティ認証と暗号化のメカニズムを維持することが重要になります。 迅速かつ簡単に再アソシエーションと再認証を行うには、認証および暗号キーを管理するか、場合によってはキャッシングする必要があります。

### 関連トピック

Real-Time Traffic over WLAN のローミング, （105 ページ）

# 802.11 の追加セキュリティ メカニズム

不正アクセスや支障を及ぼすネットワーク攻撃を防ぐため、RToWLAN のネットワーク管理者はセキュアなクライアント デバイスの WLAN へのアソシエイト、認証、トラフィック暗号化に加えて、802.11 WLAN の追加セキュリティ メカニズムについて考慮する必要があります。 たとえば、MAC フラッディング、中間者攻撃、DHCP スヌーピングまたはスターベーションなどの従来の有線ネットワーク攻撃ベクトルは、適切なネットワーク管理と有線およびワイヤレス LAN インフラストラクチャのセキュリティ機能によって軽減されます。 同様に、有線およびワイヤレス侵入の防止、検出、軽減は、RToWLAN の導入を成功させる重要なコンポーネントです。 特に、不正なアクセス ポイントとクライアントの検出と軽減または排除は、最小限の干渉で健全なワイヤレス LAN の無線周波数を維持するために不可欠です。 不正な AP とクライアントの検出をしないと、適切な無線周波数の設計が危険にさらされる場合があります。それにより、ワイヤレス ネットワークのスループットやキャパシティの低下、音声およびビデオ品質の低下、場合によっては、リアルタイム トラフィック アプリケーションおよびサービスの完全な障害が発生します。

### 関連トピック

Enterprise Mobility Design Guide

# RToWLAN 設計上の考慮事項

ネットワーク設計全般において重要となるのは、RToWLAN の導入でワイヤレス ネットワークを保護することです。 RToWLAN アプリケーションおよびサービスを実装する場合は、認証および暗号化方式の選択、拡張性、高可用性について考慮する必要があります。

### 認証および暗号化方式の選択

導入を成功させるには、RToWLAN アプリケーションおよびサービスで適切な 802.11 セキュリティ メカニズムを有効にすることが重要です。 セキュアな RToWLAN 導入を設計する場合の最も重要な考慮事項は、アクセス ポイント、ワイヤレス LAN コントローラ、WLAN クライアント デバイス自体などの WLAN インフラストラクチャ コンポーネントの機能です。 次の重要事項を考慮してください。

- 最も強固なセキュリティ メカニズムの実装を常に試みます。 802.1X EAP 認証、TKIP/AES 暗号化による WPA または WPA2-Enterprise セキュリティ方式は、WEP またはオープン認証よりも適切です。計画対象のクライアント デバイスやインフラストラクチャに使用される暗

号化方式は、より強力なセキュリティ方式のサポートに対応します。一方、インフラストラクチャまたは対象クライアントデバイスが、安全性がより高いメカニズムをサポートしない場合は、組織のセキュリティ ポリシーと機器の基準に基づいて、ネットワーク管理者はサポートできる最も安全なメカニズムを判断する必要があります。

- 個人所有デバイスの持ち込みがWLANインフラストラクチャを使用する可能性のあるBYODを実装する場合は、オープン認証および非暗号化接続を有効にしてこれらのデバイスを参加させるか、または単純にインターネットのみを利用可能なゲストアクセスを用意する必要があります。このような場合、（少なくとも初期の段階の）セキュリティで保護されないネットワーク アクセスは、高度なセキュア認証や暗号化方式と同じように重要となります。
- セキュリティ方式またはRToWLAN導入方式を選択する場合に重要なその他の考慮事項は、ネットワークの接続を完了するためにエンド ユーザの操作が必要かどうかです。 音声およびビデオ対応クライアントをユーザの操作なしで初期プロビジョニング後にバックグラウンドで企業ネットワークへ接続させることを、ネットワーク管理者はよく検討してください。これは、企業の音声やビデオのインフラなどで、リアルタイム トラフィック アプリケーションおよびサービスの最大使用率を保証します。 具体的には、証明書ベースの ID や EAP-TLS のような認証セキュリティ メカニズムを使用することで、ネットワーク接続と認証の遅延を最小化して高速な WLAN デバイス接続を保証し、優れたユーザ エクスペリエンスの促進に役立ちます。 RToWLAN クライアント デバイスに高速、安全、シームレスなネットワーク接続メカニズムを用意できないと、リアルタイム トラフィック アプリケーションおよびサービスの使用が制限されてしまう場合があります。これは、ユーザが認証プロセスの完了操作を遅れて実行するか、忘れてしまうためです。
- 最終的に、使用する暗号化方式および認証方式は、導入するクライアントデバイスやワイヤレス基盤、RToWLAN 導入の対象となる使用方法によって決定されます。

### 拡張性

一般的に、管理者はより強固なセキュリティ メカニズムを選択する一方で、導入されるユーザ数とデバイス数の観点から、セキュリティ ソリューションの拡張性についても考慮する必要があります。 大量のユーザとデバイスが導入されるシナリオでは、ワイヤレス クライアント デバイス ネットワーク接続の最も忙しい時間帯に、認証サーバまたはサービスが認証要求の負荷に対応できることが重要です。

たとえば、導入の規模によっては平日の始業時間において、所有する RToWLAN デバイスをワイヤレス ネットワークに接続しようとするユーザの数が、認証サーバの認証またはクレデンシャル データベースのストレージキャパシティを超える場合があります。これにより、少なくともいくつかのデバイスでは認証の失敗または遅延が発生して問題となります。 このような状況では、管理者は認証の履行と、クレデンシャル ストレージを複数の認証サーバに分散させることを検討してください。 RToWLAN の導入を成功させるため、予想される認証負荷に対応できる十分なキャパシティがあることを確認します。

### ハイ アベイラビリティ

その他に RToWLAN 導入の安全性確保において重要な点は、WLAN ネットワーク セキュリティ サービスに高い可用性があることを確認することです。 たとえば、RToWLAN クライアント デバイスのネットワーク接続を保護するために認証サーバが必要な場合、デバイスが接続を試みると

きに認証サーバが使用可能であり、デバイスを認証することが重要です。 ネットワークの問題により、認証サーバに障害が発生するか使用できない状況では、冗長認証サーバが使用可能であり、認証要求を処理できることが重要です。

高可用性な認証サービスやサーバの冗長性がないと、RToWLAN クライアント デバイスはサーバに障害が発生している間、WLANネットワークに接続できない可能性があります。 たとえば、複数のサイトで分散型ネットワークを導入しており、中央サイトにある集中認証サーバを経由して拠点サイトの認証サービスが提供されている状況で、拠点サイトと中央サイト間でネットワーク障害が発生すると、拠点サイトにあるクライアント デバイスはローカル サイトまたはローカル サイトからアクセスできる別のサイトで、冗長認証サービスが使用可能になるまで認証できなくなり、WLAN には接続できません。 可能な限り高可用性な認証サービスを含めて RToWLAN の導入を設計してください。

第 5 章

# Real-Time Traffic over WLAN のローミング

基本的なレベルでは、IEEE 802.11 企業ネットワークのローミングは、IEEE 802.11 クライアントが、アクセス ポイント（AP）のアソシエーションを AP から同じ WLAN 内の他の AP に変更する場合に発生します。 クライアントの機能により、同じ周波数帯域内または 2.4 GHz と 5 GHz の周波数帯域間における AP 間の同じ WLAN で、802.11 WLAN クライアントはローミングを実行します。 適切なインフラストラクチャ ネットワークが設計されている場合、同時セルラーおよび Wi-Fi 接続のあるスマートフォンとタブレットは、ネットワークに対してシームレスにローミングできます。 クライアントが、ある Service Set Identifier（SSID）の WLAN から別の SSID の WLAN にローミングする場合、そのローミングはシームレスに行われません。 Wi-Fi クライアント ロジックでは Wi-Fi WLAN 認証は一度につき 1 回だけ維持されます。

WLAN クライアントはソフトウェア機能のみに基づいてローミングするか、WLAN インフラストラクチャ AP によって提供される経由ローミング機能に基づきます。 クライアントで制御するローミングの場合は、クライアントがローミングの必要性を判断し、代替 AP の検出、評価、ローミングを実行します。 クライアント上のソフトウェアは現在の Wi-Fi 接続の品質を確認し、接続およびローミング ロジックを実行して代替 AP に参加し、より高品質な接続を確保します。

（注） WLAN 標準の本文（IEEE など）と業界団体（Wi-Fi Alliance）のいずれも、クライアントがローミングすべきタイミングや、クライアントにおけるローミング先代替 AP の決定方法を指定していません。 各ベンダーのローミング アルゴリズムには独自性があり、一般的に公開されません。

# 802.11r および 802.11k の IEEE 標準

現在、IEEE 802.11k および 802.11r は、WLAN 環境においてシームレスな Basic Service Set（BSS）の移行を可能にする重要な業界標準となっています。 802.11r および 802.11k 標準は、Wi-Fi 802.11r Fast Transition、セキュア認証、802.11k ネイバー リスト無線管理をサポートします。

リリース 7.4 以降を実行する Cisco Unified WLAN コントローラにおいて、Apple iOS 6 以降を実行するモバイル無線デバイスは、企業ローミングの 802.11k ネイバー リストを活用します。

次の手順では、Apple iPhone が 802.11k ネイバー リストを要求、受信、処理する方法について説明します。

1. AP にアソシエートしている iPhone が、同じ WLAN にある隣接する AP リストの要求を送信します。 要求は、アクション パケットと呼ばれる 802.11 管理フレームの形式になります。
2. 同じ WLAN にある隣接する AP の Wi-Fi チャネル番号が付いたリストを使用して、AP は応答します。 この応答フレームもアクション パケットです。
3. iPhone は応答フレームを受信し、今後のローミングで使用される AP を識別します。

802.11k 無線リソース管理（RRM）プロセスを使用することで、モバイル クライアント デバイスは効率的かつ高速にローミングを実行できます。 これは、いつでも使える状態でのローミングが一般的なエンタープライズ環境において、良好なコール品質を実現するための要件です。 スマートフォンのベンダーは 802.11r および 802.11k 標準を採用していることから、ベンダーのユーザはローミング中も良好なコール品質が得られて、より効率的なローミングを実行できます。

推奨される WLAN コントローラ（WLC）の 802.11k 設定では、ネイバー リスト応答パケット内の 2.4 GHz および 5 GHz 両方の AP チャネル番号を提供するように RRM を有効にします。 WLAN における音声通話やビデオ通話だけでなく、すべてのアプリケーションとデバイスに 5 GHz 帯域の Wi-Fi チャネルを使用することをお勧めします。

ネイバー リスト情報があるため、モバイル クライアント デバイスはローミングできる AP を検索するために、すべての 2.4 GHz および 5 GHz チャネルを確認する必要はなくなります。 これには次の利点があります。

- すべてのチャネルのチャネル使用率が減少します。これにより、すべてのチャネルの帯域幅が増加します。
- ローミング時間が短縮され、モバイル デバイスによる判断が改善されます。
- デバイスは各チャネルの無線設定を変更したり、各チャネルでプローブ要求を送信したりしないため、デバイスのバッテリ寿命が向上します。

デバイスは、チャネルで受信するすべてのプローブ応答フレームを処理する必要はありません。デバイスに必要なことは、802.11k ネイバー リスト応答フレームの AP リストにある AP に接続できることを検証するだけです。

### 高速ローミング

Apple iOS 6 以降を実行するデバイスで推奨されるエンタープライズ セキュリティ設定は、802.11r Fast Transition です。 IEEE 802.11r 仕様は 2008 年 7 月に承認され、2004 年 6 月の 802.11i 仕様に準拠しています。

802.11r では、クライアントと AP 間で交換されるパケット数が減少します。 クライアントは、実際にローミングする前に、ローミングする AP に対して事前認証を行います。 つまり、AP はクライアント認証クレデンシャルをキャッシュ化し、クライアントと AP 間で必要なパケットがより少なくなるため、ローミング自体は高速に実行されます。

802.11r では、次の標準ベース Fast Transition が導入されています。

- 再アソシエーションの前または最中に、クライアントはセキュリティおよびQoS状態をローミング先の AP に確立します。
  - **方法 1**：**Over-the-Air（クライアントからローミング先の AP まで）**：Wi-Fi チャネルでパケットを 4 つ交換します。
  - **方法 2**：**Over-the-DS（AP からのローミング）**： Wi-Fi チャネルでパケットを 2 つ交換し、イーサネット経由でパケットを 2 つ交換します。

次に、802.11r Fast Transition に影響する現在の注意事項と制限事項を示します。

- この機能はメッシュ AP ではサポートされません。
- FlexConnect モードの AP では、次の事項を考慮します。
  - 802.11r Fast Transition は、Cisco WLAN リリース 7.3 以降の中央およびローカルでスイッチされる WLAN でのみサポートされます。
  - この機能は、ローカル認証が有効な WLAN ではサポートされません。
- また、この機能は、Cisco 600 シリーズ OfficeExtend アクセス ポイントではサポートされません。
- 802.11r クライアントのアソシエーションは、スタンドアロン モードの AP ではサポートされません。
- 802.11r 高速ローミングは、スタンドアロン モードの AP ではサポートされません。
- 802.11r 高速ローミングは、ローカル認証と中央認証 WLAN の間ではサポートされません。
- クライアントがスタンドアロン モードで Over-the-DS 事前認証を使用していると、802.11r 高速ローミングはサポートされません。 Over-the-DS ローミングでは、有線インフラストラクチャでパケットが送信されます。
- スタンドアロン AP からクライアントへのサービスは、セッション タイマーの期限が切れるまでの間だけサポートされます。
- TSpec は 802.11r 高速ローミングではサポートされません。
- WLAN リンク遅延があると、高速ローミングも遅延します。 クライアントは、音声またはデータの最大遅延を検証する必要があります。

- WLAN コントローラ（WLC）は、Over-the-Air 方式と Over-the-DS 方式の両方のローミング中に、802.11r Fast Transition 認証要求を処理します。
  - 2 つの必須パケットが有線接続された AP で送信され、残り 2 つのパケットが WLAN で送信されるため、Over-the-DS が推奨されます。 DS オプションを選択しない場合は、4 つのパケットがすべて WLAN で送信されます。

### Fast Transition 用の推奨される WLAN コントローラ設定

WLAN ネットワークに 802.11r Fast Transition クライアントを追加するには、次の WLAN 推奨設定を使用します。

（注） これらの推奨事項は Apple とシスコの共同作業によるものです。

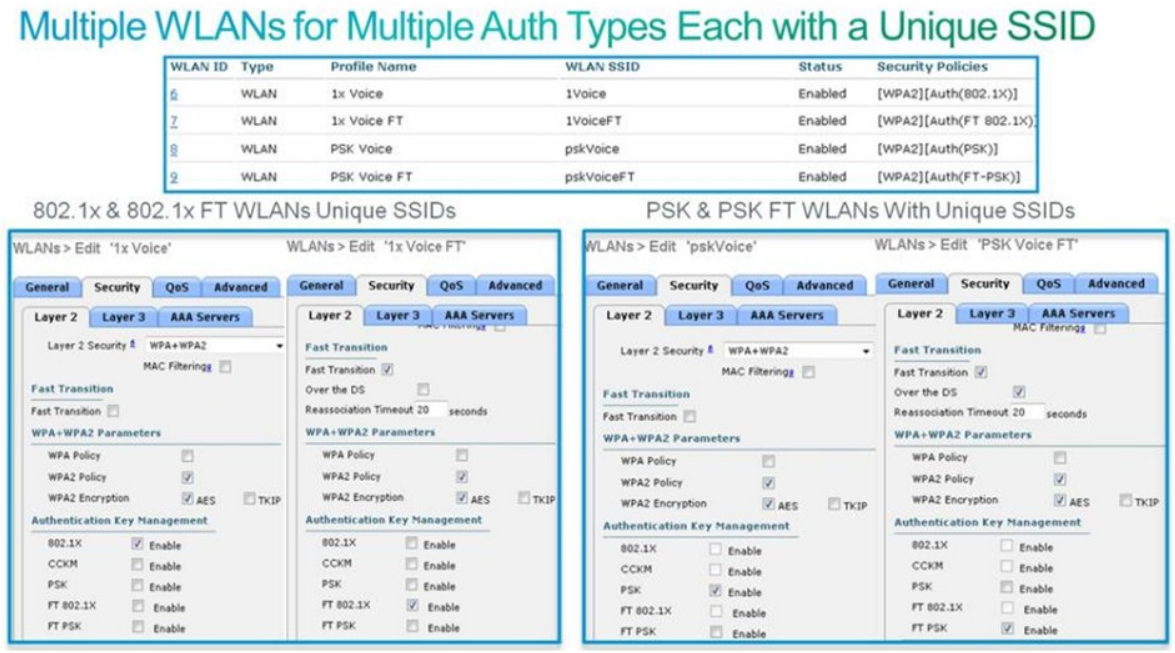
- Fast Transition 802.1x クライアント向けの追加の WLAN を設定します。
- Fast Transition PSK クライアント向けの追加の WLAN を設定します。
- レガシー クライアントには、個別の WLAN とサービス セット ID（SSID）を使用することをお勧めします。

Fast Transition 設定が行われた WLAN のアソシエーション応答パケットの追加情報を、古い無線ドライバは理解できないため、これらの推奨事項が用意されています。 802.11r 仕様が 2008 年に承認されましたが、すべてのクライアント無線ドライバが 802.11r に関連した管理パケットの変更点に対応するように更新されたわけではありません。 これは一部の Apple 社製品にも当てはまります。

（注） 802.11r 仕様では Wi-Fi パケット構造が変更されています。 レガシー クライアントが変更点に対応するようにプログラムされていない場合があり、802.11r が有効な WLAN へのアソシエーションは失敗します。 したがって、802.11r 対応デバイスには新しい WLAN を使用することをお勧めします。 iPad2 は、802.11r WLAN に参加できないデバイスの例です。

次の図に、さまざまな仕様をサポートするクライアントデバイスの種類に対応する、複数の WLAN および SSID がある WLAN インフラストラクチャを示します。

**図 *46*： 複数の *WLAN* および *SSID* の例**




コマンドライン インターフェイス（CLI）またはグラフィカル ユーザ インターフェイス（GUI）の Fast Transition 設定オプションについての情報は、WLC ファームウェアのインストール バージョンに対応した『*Cisco Wireless LAN Controller Configuration Guide*』（http://www.cisco.com/）を参照してください。

### 関連トピック

802.11k 仕様
802.11r の詳細情報
IEEE 802.11r 仕様

# クライアント ローミングの決定

現在の AP への接続が劣化すると、802.11 ワイヤレス クライアントはローミングの必要性を検出します。 クライアントは代替 AP の他の 802.11 チャネルをスキャンして再アソシエーションを行い、ローミング先 AP への認証を行うため、ローミングは必然的にクライアント トラフィックに影響を及ぼします。 ローミングを実行する前に、クライアントは次の内容を実施して、ローミングを必要とせずに現在の接続を向上させます。

- **データ リトライ**：IEEE 802.11 MAC は信頼できる転送を明記しています。 ワイヤレス クライアントと AP 間で送信されるすべてのユニキャスト フレームは、MAC 層で確認されます。

IEEE 802.11 標準は、確認応答が受信されなかったデータ フレーム伝送の再試行に使用されるプロトコルを明記しています。

- **データ レートシフト**：IEEE 802.11a、802.11b、802.11g はそれぞれ、さまざまなデータ レートをサポートしています。 指定された周波数帯域（たとえば、2.4 GHz または 5 GHz）でサポートされるデータ レートがプライム インフラストラクチャ（PI）または WLC で設定され、その周波数帯域を使用する AP に継承されます。 次に、指定された WLAN の各 AP がサポートされるデータ レートをビーコン内で示します。 クライアントまたは AP がワイヤレス接続の劣化を検出した場合は、より低いサポート伝送レートに変更できます。通常、低い伝送レートでは伝送の高い信頼性を確保できるためです。

ベンダーまたはドライバのバージョンごと（同じベンダーの異なるデバイス タイプごとの場合もある）にローミング アルゴリズムが異なっていても、次の共通の場面では通常、ローミングが発生します。

- **最大データ再試行回数の超過**：許容数を超えるデータの再試行が行われると、通常、ローミングがトリガーされます。
- **受信信号強度インジケータ（RSSI）の低下**：受信信号強度がしきい値より低下した場合、クライアントデバイスはローミングすることを決定できます。 このローミング トリガーがローミングを開始するのに、アクティブなクライアント トラフィックは必要ありません。
- **信号対雑音比（SNR）の低下**：受信信号強度とノイズ フロアの差がしきい値より低下すると、クライアントデバイスはローミングすることを決定できます。 このローミング トリガーがローミングを開始するのに、アクティブなクライアント トラフィックは必要ありません。
- **独自のロード バランシング スキーム**：一部のワイヤレスの実装には、クライアント トラフィックを複数の AP に均等に分散させることを促進するため、クライアントをローミングさせようとするスキームが存在します。 これは、WLAN インフラストラクチャの判断でローミングが開始され、ベンダー固有のプロトコルでクライアントと通信するケースの 1 つです。

### Cisco Compatible Extensions クライアント ローミングのトリガー

ワイヤレス LAN コントローラ（WLC）は、RF ローミング パラメータのデフォルト セットで設定されます。これらのパラメータは、クライアントがローミングするタイミングの決定に採用している RF しきい値の設定に使用されます。 デフォルト パラメータはカスタム セットを定義すると上書きできます。 IEEE 802.11 周波数帯域（2.4 GHz または 5 GHz）ごとに 1 つの Cisco Compatible Extensions（CCX）パラメータが WLC に定義されます。

Cisco Compatible Extensions バージョン 4 以降で実行される WLAN クライアントは、次のパラメータを使用できます（パラメータはCisco Compatible Extensions のチャネル スキャン，（113 ページ）に記載されている拡張ネイバー リスト機能によってクライアントに通信されます）。

- [Scan threshold]：クライアントが適切な AP にローミングする前まで許容される RSSI の最小値です。 RSSI が指定された値よりも低い場合、クライアントは指定遷移時間内により強い信号のある AP へローミングできる必要があります。 このパラメータはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供

します。 たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。

- [Transition time]：AP にアソシエートしたクライアントの RSSI がスキャンのしきい値より低下した場合に、ローミング先となる適切な隣接 AP を検出したり、ローミングを完了したりするためにクライアントで許容される最長の時間です。 スキャンのしきい値と遷移時間のパラメータは、クライアント ローミング パフォーマンスの最低レベルを保証します。 AP 間に特定の最小オーバーラップ間隔を確保することで、最良のクライアント速度とローミング ヒステリシス（ヒステリシスの定義は後続の内容を参照）を実現するだけでなく、これらのパラメータはローミングをサポートする WLAN ネットワークの設計に役立ちます。
- [Minimum RSSI] フィールド：AP にアソシエートするクライアントで必要な RSSI 最小値です。
- [Hysteresis]：クライアントが AP にローミングするときに必要な隣接する AP の信号強度を示す値です。 このパラメータは、クライアントが 2 つの AP 間のボーダーまたはボーダー付近に物理的に存在している場合に、AP間のローミングの量を減らすことを目的としています。
- [Call admission control （CAC）]：WLAN インフラストラクチャからコール アドミッション制御が拒否されると、クライアント デバイスはローミングを開始します。

（注） ワイヤレス クライアントが CCX 互換である場合でも、前述された CCX トリガーの代わりに 802.11k やベンダー固有のローミング アルゴリズムを引き続き使用することもできます。

# 新しいアクセス ポイントのローミングの選択

### チャネル スキャン

ワイヤレス クライアントは他の 802.11 チャネルをスキャンして、同じ WLAN または SSID で使用可能な AP を検索し、使用できる AP の情報を取得します。 ワイヤレス クライアントは、次の 2 つの方法で他の IEEE 802.11 チャネルをスキャンできます。

- **アクティブ スキャン**：クライアントが自身の 802.11 無線をスキャンされているチャネルに変更する場合、プローブ要求をブロードキャストする場合、および（一致する SSID の）チャネルの AP からプローブ応答（または定期ビーコン）の受信を待機する場合に、アクティブ スキャンが実行されます。 802.11 標準でクライアントの待機に必要な時間は指定されていませんが、10 ミリ秒が一般的です。 アクティブ スキャンで使用されるプローブ要求フレームには、次の 2 つの種類があります。
  - **ダイレクト プローブ**：クライアントは指定された送信先 SSID があるプローブ要求を送信します。一致する SSID の AP のみがプローブ応答を返します。
  - **ブロードキャスト プローブ**：クライアントはブロードキャスト SSID（実際は空の SSID）をプローブ要求で送信します。プローブ要求を受信したすべての AP は、サポートされる SSID ごとにプローブ応答を返します。

- **パッシブ スキャン**：クライアントが自身の 802.11 無線をスキャンされているチャネルに変更する場合と、そのチャネルの AP から定期的なビーコンを待機する場合に、パッシブ スキャンが実行されます。 デフォルトで、AP は 100 ミリ秒ごとにビーコンを送信します。

  パッシブ スキャンでは、定期ビーコン ブロードキャストの受信に 100 ミリ秒かかるため、大半のクライアントはアクティブ スキャンを使用します。

チャネル スキャン中は、クライアントはクライアント データ トラフィックの送受信ができません。 クライアントは次の方法を使用して、クライアント データ トラフィックに対する影響を最小化します。

- **バックグラウンド スキャン**：クライアントは、ローミングする前に使用可能なチャネルをスキャンします。 RF 環境と必要に応じてクライアントが高速にローミングできる使用可能な AP に関する情報を、スキャンにより取得します。 クライアントが活発にデータを伝送しない場合のみスキャンするか、一度に 1 つだけ代替チャネルを定期的にスキャンすることで、クライアント トラフィックへの影響を最小化できます。 単一チャネルのスキャンではデータ損失が最小になります。
- **オンローミング スキャン**：クライアントによってローミングの必要性が判断されると、オンローミング スキャンが実行されます。 ローミングの遅延とデータ トラフィックへの影響を最小化するために、各ベンダーまたはデバイスは独自のアルゴリズムを実装できます。 たとえば、非オーバーラップ チャネルのみをスキャンするクライアントが存在する場合があります。

### 通常のスキャン動作

大半のクライアントローミングアルゴリズムが独自のものでも、通常の動作を一般化することができます。通常のワイヤレスクライアントのローミング動作は、次のアクティビティで構成されています。

- **オンローミング スキャン**：クライアントがローミング時の最新の情報を保持できます。
- **アクティブ スキャン**：ローミング時の遅延が短いため、パッシブ スキャンよりもアクティブ スキャンをお勧めします。

WLANクライアントは、次の情報属性を使用して、ローミングアルゴリズムを動的に変更できます。

- クライアントのデータ型（コール中の音声通話など）
- ルーチンの定期バックグラウンド スキャン中に取得された、バックグラウンド スキャン情報

WLANクライアントが属性を使用してスキャンアルゴリズムを変更するその他の方法として、次のものが挙げられます。

- **チャネルのサブネットをスキャン**：たとえば、クライアントはバックグラウンドスキャンで取得した情報を使用し、付近の AP で使用されているチャネルを判断できます。

- **スキャンをすぐに終了**：たとえば、コール中の音声通話では、クライアントはすべてのチャネルの全 AP が検出されるまで待機せず、最初の許容される AP を使用できます。
- **スキャンタイマーの変更**：たとえば、コール中の音声通話では、クライアントはアクティブスキャンを使用して、プローブ応答の待機にかかる時間を最小化できます。

### Cisco Compatible Extensions のチャネル スキャン

WLAN クライアントは、AP にアソシエーション（または再アソシエーション）するタイミングを最終的に決定しますが、シスコの AP はクライアントに情報を提供して AP の選択を支援します。提供される情報は、ビーコンやプローブ応答のチャネル負荷などの情報か、隣接する AP のリストです。

WLC ソフトウェア リリース 4.0 以降は、次の Cisco Compatible Extensions レイヤ 2 クライアント ローミング機能拡張をサポートします。

- **AP 支援ローミング**：この機能により、クライアントはスキャン時間を短縮できます。 Cisco Compatible Extensions v2 クライアントは、AP にアソシエートするたびに前回の AP の特性をリストして、新しい AP へ情報パケットを送信します。 AP はこの情報を使用して前回の AP のリストを作成し、ローミング時間を短縮します。このリストは、アソシエーションの後で、すぐにクライアントへユニキャストで送信されます。 AP のリストにはチャネル、クライアントの現在の SSID をサポートしている隣接 AP の Basic Service Set Identifier（BSSID）、アソシエーション解除後の経過時間が含まれています。
- **拡張ネイバー リスト**：この機能は AP 支援ローミング機能 v2 の一部として送信される、ネイバー リストの Cisco Compatible Extension v4 拡張機能です。 これは、正常なアソシエーションまたは再アソシエーションの直後に、必ず AP からクライアントへ自動的に提供されます。 AP はネイバー リストが最新になるように定期的に確認を行うため、対応するクライアントに自動的な更新を送信することもできます。 拡張ネイバー リストには、Cisco Compatible Extensions クライアント ローミングのトリガー, （110 ページ）に記載された RF パラメータが AP ごとに含まれます。 また、AP タイミング パラメータの追加情報、クライアント サブネットの AP サポート情報、クライアントから AP に送信した最新の伝送強度と信号対雑音比（SNR）がリストの AP ごとに含まれています。
- **拡張ネイバー リスト要求（E2E）:**エンドツーエンド（E2E）仕様は、音声/ローミング能力の全体的向上のために新しいプロトコルとインターフェイスを定義する、シスコと Intel の共同プログラムです。 これは、Cisco Compatible Extensions 環境にある Intel クライアントにのみ適用されます。 これにより、Intel クライアントはいつでもネイバー リストを要求できるようになります。 要求が発生すると AP は要求を WLC に転送します。 WLC は要求を受信し、クライアントが関連付けられている AP に対するネイバーの現在の Cisco Compatible Extensions ローミング サブリストで応答します。

（注） 特定のクライアントが E2E をサポートするかどうか確認するには、WLC GUI の [Wireless] > [Clients] をクリックして目的のクライアントの [Detail] リンクをクリックします。 [Client Properties] の E2E [Version] フィールドも確認します。

- **ダイレクト ローミング要求**：この機能により、クライアントがアソシエートする AP とは異なる AP のクライアントに、WLC がより高品質のサービスを提供できる状況で、WLC はクライアントにダイレクト ローミング要求を送信できます。 この場合、WLC はクライアントが参加できる最適な AP リストをクライアントに送信します。 クライアントは、ダイレクトされたローミング要求に応答することも、無視することもできます。 Cisco Compatible Extensions 以外のクライアントと、Cisco Compatible Extensions バージョン 3 以降を実行するクライアントでは、どの操作も必要ありません。 この機能を使用するために設定する必要はありません。

WLC ソフトウェア リリース 4.0 は Cisco Compatible Extensions バージョン 1 ～ 4 をサポートします。 Cisco Compatible Extensions のサポートは、WLC のすべての WLAN で自動的に有効になり、無効にすることはできません。 WLC クライアント データベースにあるクライアントの Cisco Compatible Extensions バージョンを WLC は保存し、これらを使用して Cisco Compatible Extensions フレームを適切に生成および応答します。 ローミング機能拡張を使用するには、クライアントが Cisco Compatible Extensions バージョン 4（または AP 支援ローミング向けの Cisco Compatible Extensions バージョン 2）をサポートする必要があります。

多くのスマートフォン、タブレット、その他のモバイル デバイスは CCX に適応しないため、これらの CCX パラメータは使用しないでください。

### 潜在的なローミング ターゲットのリストの確認

ローミング対象になる可能性がある AP のリストをワイヤレス クライアントが受信すると、クライアントはそのクライアントに固有のアルゴリズムを使用して、ローミング対象にする指定された AP を選択します。 ローミング アルゴリズムでは、演算時に次の項目を考慮する必要があります。

- 受信信号強度インジケータ（RSSI）
- SNR
- AP のクライアント数
- AP で使用されている送受信帯域幅
- AP から送信されるビーコン応答とプローブ応答からの RF チャネル ロード情報

# 新しいアクセス ポイントへの再認証

ワイヤレス クライアントが WLAN に最初に参加する場合は、ネットワークへアクセスが許可される前に認証する必要があります。 ここでは、次の考慮事項とプロセスについて説明します。

- 認証タイプ
- ローミングにおける再認証

### 認証タイプ

WLAN のアクセスに次の認証方式を使用できます。

- **オープン認証**：認証は行われません。すべてのクライアントが WLAN へのアクセスを許可されます。
- **Wired Equivalent Privacy（WEP）共有キー（静的 WEP）**：静的 WEP では、送信元および受信先の両方が同じ事前プロビジョニング キーを持つ必要があります。これは、お互いから送信されるメッセージを復号化するためです。
- **Wi-Fi Protected Access（WPA）-Personal および WPA2-Personal**：共有キー（暗号キーではない）が WLAN および WLAN クライアントの両方で設定されます。このキーが WPA 4 方向ハンドシェイクで使用され、セッション単位の暗号キーが生成されます。
- **WPA-Enterprise または WPA2-Enterprise で使用される IEEE 802.1X/拡張認証プロトコル（EAP）認証**：導入要件に応じて、セキュアなワイヤレスの導入に、次の EAP 認証プロトコルのいずれかを使用できます。
  - Protected EAP（PEAP）
  - EAP-Transport Layer Security（EAP-TLS）
  - EAP-Flexible Authentication through Secure Tunneling（EAP-FAST）

  使用するプロトコルに関係なく、上記のすべてのプロトコルは現在、基盤となる転送に IEEE 802.1X、EAP、およびリモート認証ダイヤルイン ユーザ サービス（RADIUS）を使用しています。 WLAN クライアントの正常な認証に基づき、これらのプロトコルはネットワーク アクセスを許可し、重要なユーザによる WLAN ネットワークの認証を許可します。

IEEE 802.1X/EAP 認証の基本的な流れを図 44： EAP プロトコルのフロー，（98 ページ）に示します。 この図で、『認証カンバセーションはクライアントとサーバ間』と示されている部分は、クライアントと認証サーバ間の認証プロセスを表しています。 この認証では、WLC はクライアントと認証サーバ間で複数のパケットを伝送する必要があります。 認証フローのこの部分では、クライアントと認証サーバの両方で CPU 負荷の高い暗号化処理も必要です。 認証のこの部分では遅延がすぐに 1 秒を超えます。また、次に説明されている高速ローミング アルゴリズムの重要項目でもあります。

### ローミングにおける再認証

ここでは、異なる認証タイプのローミングについて説明します。

- オープン認証または静的 WEP によるローミング
- IEEE 802.1X または EAP 認証によるローミング
- 高速セキュア ローミング
- Proactive Key Caching（PKC）による高速ローミング

### オープン認証または静的 WEP によるローミング

クライアントがオープン認証（キーなし）または共有キーを使用してローミングする場合、認証で発生するローミング遅延はわずかです。 これは、クライアントと AAA サーバ間で追加のパケットを交換する必要がないためです。

### IEEE 802.1X または EAP 認証によるローミング

クライアントが動的 WEP の IEEE 802.1X、WPA-Enterprise、WPA2-Enterprise のいずれかを使用してローミングする場合、IEEE 802.1X 認証は通常、AAA/RADIUS サーバで実行される必要があります。 AAA/RADIUS サーバによる認証には 1 秒より長くかかる場合があります。 Video over IP または Voice over IP のような遅延に影響されやすいアプリケーションでは、遅延による 1 秒間の中断もローミングで許可されません。そのため、ローミング遅延の短縮に役立つ高速セキュア ローミング アルゴリズムが開発されました。

### 高速セキュア ローミング

高速ローミング アルゴリズムには、Cisco Centralized Key Management（CCKM）、Opportunistic Key Cache（OKC）、Proactive Key Caching（PKC）があります。 CCKM と PKC では、AAA/RADIUS サーバに対する IEEE 802.1X 全体または EAP の再認証を必要とせず、WLAN クライアントに新しい AP へのローミングを実行したり、クライアントと AP 間で新しいセッション キー、すなわち Pairwise Transient Key（PTK）の再確立を実行したりできます。

CCKM と PKC はともにレイヤ 2 ローミング アルゴリズムであるため、IP アドレス変更などのレイヤ 3 の問題は考慮されません。 Cisco Unified Wireless Network では、AP でなくクライアントへの WLC で開始される IP アドレスの割り当てをサブセットが担当します。 CCKM および PKC では、次の利点が得られます。

- 指定された SSID の多くの WLAN クライアントを同じレイヤ 2 サブネットにグループ化するために役立ちます。
- レイヤ 2 ドメインと高速セキュア ローミング ドメインのスコープを最大化します。

さらに、複数の WLC が導入され、同じモビリティグループの WLC で管理された AP 間では、同一または異なるサブネットにまたがるクライアントローミングがサポートされます。セッションがアクティブである限り、セッションはそのまま持続され、WLC 間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当ての IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。

### Cisco Centralized Key Management による高速セキュア ローミング

CCKM は、Cisco Compatible Extensions クライアントによってサポートされるシスコの標準であり、高速セキュア ローミングを実現します。

CCKM はクライアントでサポートされる必要があります。 Cisco Compatible Extensions では、高速セキュア ローミングを含む多くのクライアント機能をサポートする、クライアント側の仕様が提供されます。 次の表に、Cisco Compatible Extensions の各バージョンでサポートされる EAP タイプの概要を示します。

表 *13*： *Cisco Compatible Extensions EAP* のサポート

| Cisco Compatible Extensions バージョン | サポートされる EAP タイプ |
|---|---|
| Cisco Compatible Extensions バージョン 2 | Lightweight Extensible Authentication Protocol（LEAP）による CCKM |

| Cisco Compatible Extensions バージョン | サポートされる EAP タイプ |
|---|---|
| Cisco Compatible Extensions バージョン 3 | LEAP、EAP-FAST による CCKM |
| Cisco Compatible Extensions バージョン 4 | EAP、EAP-FAST、EAP-TLS、LEAP による CCKM |

CCKM は初期の WLAN クライアント認証時にキー階層を確立し、クライアントがローミングするときに、その階層を使用して新しいキーをすばやく確立します。 次の各項では、初期の確立フェーズとローミング フェーズについて説明します。

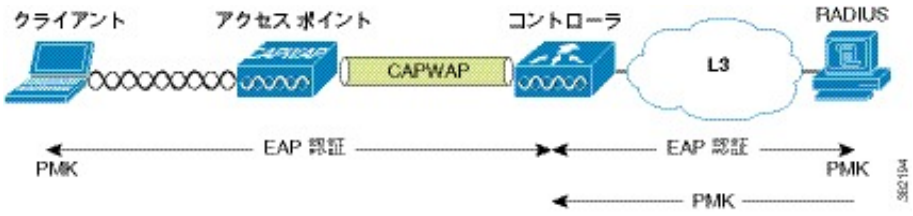
- CCKM ローミング - 初期のキー階層の確立
- CCKM ローミング - クライアント ローミング

### CCKM ローミング - 初期のキー階層の確立

図 47：CCKM の初期キー（1/4），（117 ページ）から図 50：CCKM の初期キー（4/4），（119 ページ）では、初期のキー階層の確立プロセスが示されています。 WPA-Enterprise および WPA2-Enterprise では、正常な EAP 認証の結果は Pairwise Master Key（PMK）です（図 44： EAP プロトコルのフロー，（98 ページ）を参照）。

次の図に、クライアントおよび AAA/RADIUS サーバにおける PMK の確立と、WLC に向けた PMK の一連の転送を示します。

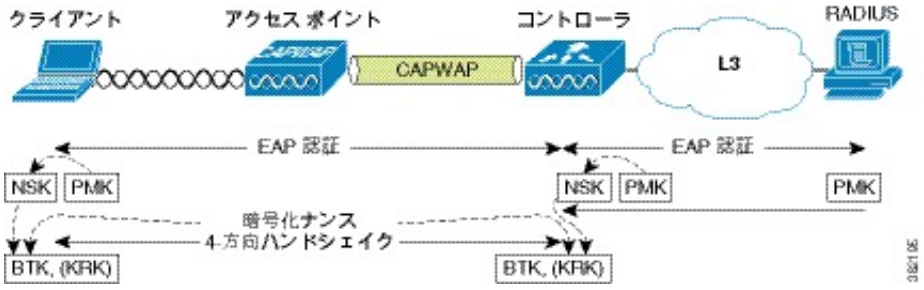
**図 *47*：*CCKM* の初期キー（*1/4*）**




WLC とクライアントは、どちらも PMK から Network Session Key（NSK）を派生させます。 NSK が確立されると、WPA 規定の 4 方向ハンドシェイクがクライアントと WLC 間で実行されます。

4 方向ハンドシェイクの最後に、Base Transient Key（BTK）と Key Request Key（KRK）が確立されます。 次の図を参照してください。

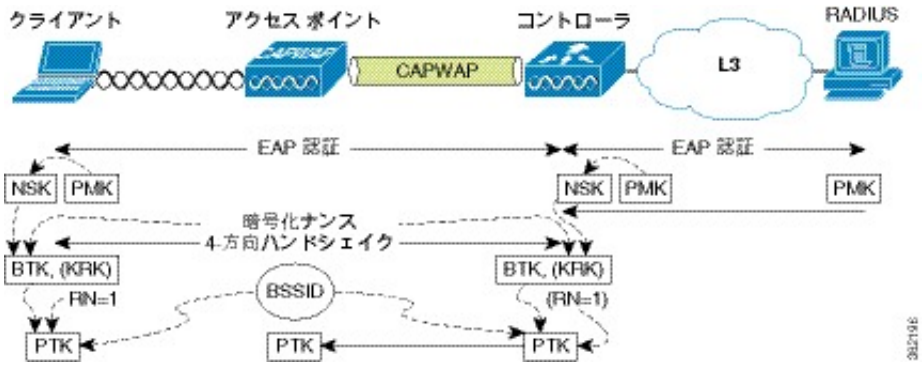
**図 *48*：*CCKM* の初期キー（*2/4*）**




WPA および WPA2 は、この時点において CCKM とほとんと違いはありません。 WPA/WPA2 は（NSK を派生させる代わりに）PMK を直接使用し、4 方向ハンドシェイクの後に Pairwise Transient Key（PTK）を確立して、WPA/WPA2 ユニキャスト キーの確立を終了します。

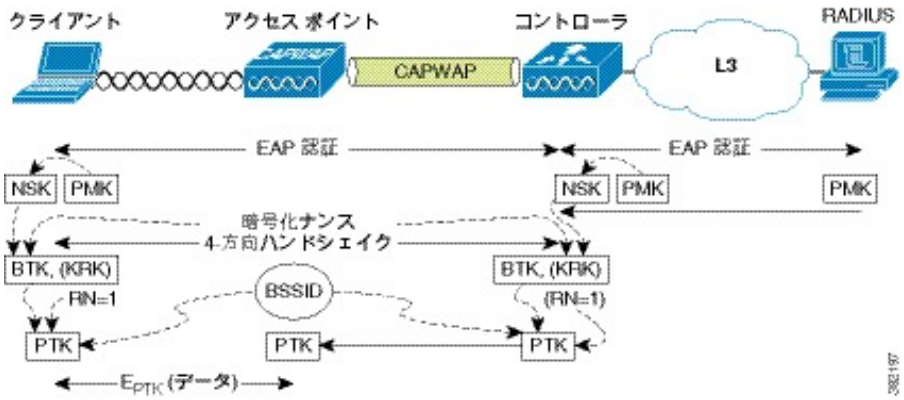
クライアントと WLC は、どちらも BTK、初期キー再生成番号（RN）= 1、BSSID をハッシュ化して PTK を派生させます。 次に、WLC は Control and Provisioning of Wireless Access Points（CAPWAP）トンネルの AP に PTK を転送します。 次の図を参照してください。

**図 *49*：*CCKM* の初期キー（*3/4*）**



クライアントと AP は PTK を使用して通信します。PTK は両者の間で送信されるデータを暗号化します。 次の図を参照してください。

図 *50* : *CCKM* の初期キー（*4/4*）

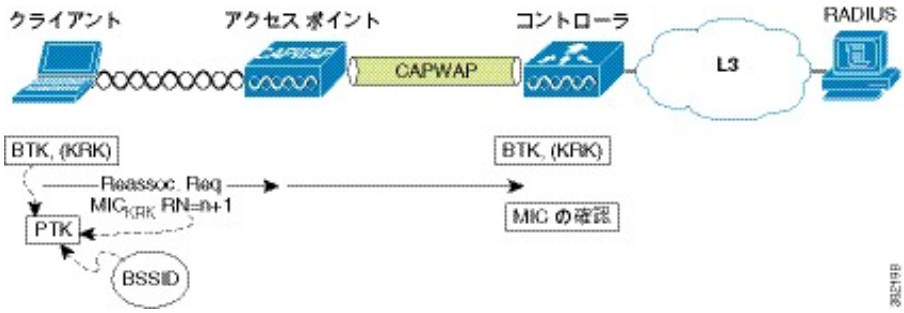



## CCKM ローミング - クライアント ローミング

CCKMは非常に高速なローミングの実現を目的としています。CCKMがないと、ローミング時に必ず WPA/WPA2 クライアントは WPA/WPA2 4 方向ハンドシェイクの前に、完全な EAP 認証をリモート AAA/RADIUS サーバに対して実行する必要があります。 このプロセスには 1 秒より長くかかる場合があります。 CCKM を使用すると、ローミング クライアントと WLC は事前に確立されたキー関連情報を使用して、PTK をすぐに確立できます（通常は n/10 ミリ秒以内）。

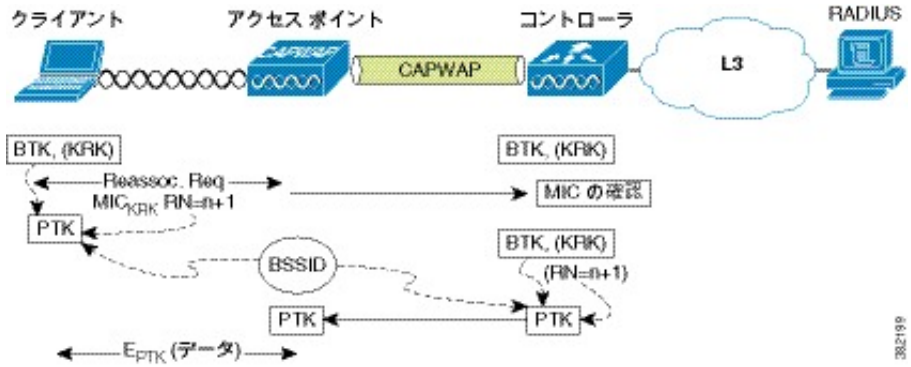
クライアントが新しい AP にローミングする場合、クライアントは次のキー再生成番号と一緒に再アソシエーション要求を送信します。 クライアントが再アソシエーション要求に追加する Message Integrity Check（MIC）によって、スプーフィングの再アソシエーション要求に対する保護が実現します（暗号入力として KRK を使用し、MIC が生成されます）。 AP によって再アソシエーション要求が WLC に転送され、MIC が検証されます。 次の図を参照してください。

図 *51* : *CCKM* のローミング キー（*1/2*）



WLC は次の PTK を計算して AP に転送します。 これで、クライアントと AP は新しい PTK を使用して通信できます。PTK は両者の間で送信されるデータを暗号化します。 次の図を参照してください。

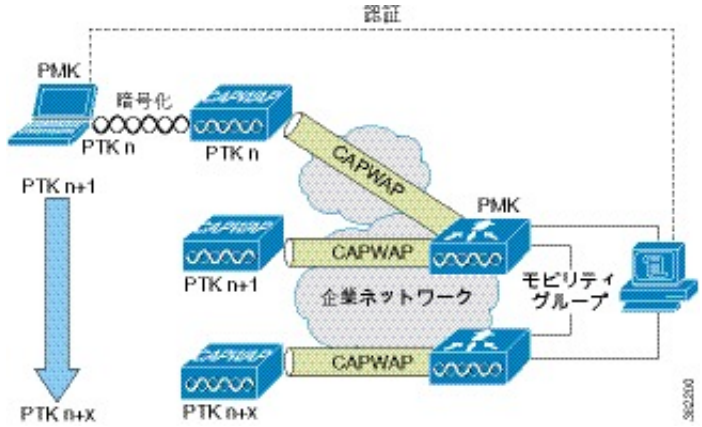
図 *52* : ***CCKM*** のローミング キー（*2/2*）




### Proactive Key Caching（PKC）による高速ローミング

PKC は IEEE 802.11i 拡張であり、WPA/WPA2 PMK の事前キャッシュを（クライアント ローミング イベントの前に）使用できます。この PMK は AP におけるクライアント IEEE 802.1 x/EAP 認証中に派生されます。 次の図を参照してください。

図 *53* : ***PKC*** ローミング




アソシエートしようとするクライアントが PMK を送信するときに、指定された WLAN クライアントの PMK がすでに AP に存在する場合は、IEEE 802.1X/EAP の完全認証は必要ありません。 代わりに、WLAN クライアントはシンプルに WPA 4 方向ハンドシェイク プロセスを使用し、AP との通信用に新しいセッション暗号キーを安全に派生させます。

（注） PKC は、IEEE 802.11i 拡張であるため WPA ではサポートされませんが、WPA2 ではサポートされます。

Cisco Unified Wireless の導入では、AP に対するキャッシュ済み PMK の配布は簡素化されます。PMK は WLC にキャッシングされ、クライアント ローミング イベントの前に、その WLC に接続するすべての AP と WLC のモビリティ グループに属する、全 WLC 間で使用できます。

### 802.11r Fast Transition ローミング

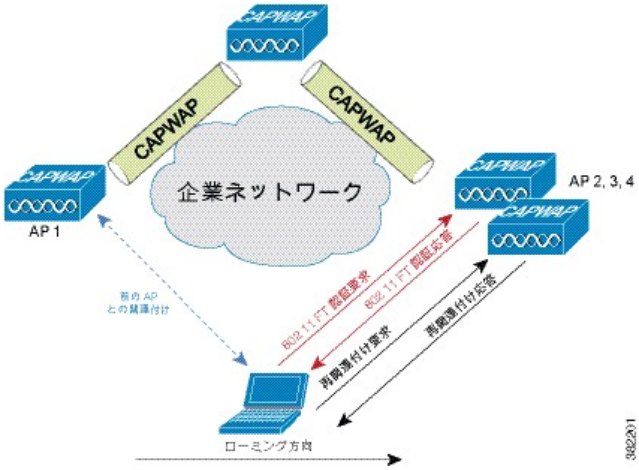
802.11r のセキュア ローミングはクライアント、AP、WLC のキャッシュにより、より少ないパケットの交換で実現されます。クライアントは、実際にローミング先 *AP* にローミングする前に、ローミング先 *AP* に事前認証を行います。そのため、AP とクライアント間で交換されるパケットがより少なくなり、実際のローミングは高速に実行されます。クライアントがローミング先 *AP* にアソシエートしているうちはパケットが交換されます。したがって、クライアントがローミング先 *AP* に再認証されるため、データ パケットの交換においてタイム ロスは発生しません。

次に、802.11r のローミング設定の 2 つのオプションについて説明します。

- Over-the-Air のみの Fast Transition（FT）ローミング
- インフラストラクチャの認証パケットによる FT ローミング

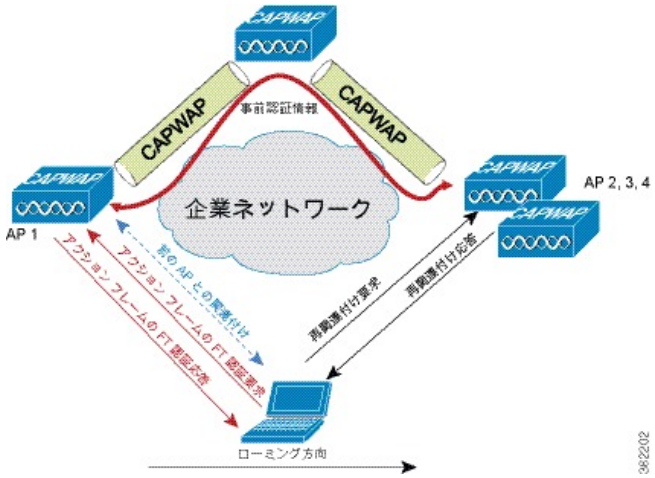
802.11r Fast Transition 認証要求および応答は、次の図に示されるように Wi-Fi チャネル上で処理できます。

図 *54*： *Wi-Fi* チャネルにおける *802.11r Fast Transition* ローミング



また、802.11r Fast Transition 認証要求および応答を有線ネットワークのサブネット上で処理することもできます。 次の図に表示されるように、これは分散システム（DS）におけるローミングとも呼ばれます。

図 *55*： 有線ネットワークのサブネットを借りる *802.11r Fast Transition* ローミング




**関連トピック**

Cisco Compatible Extensions
Enterprise Mobility Design Guide

# IP レイヤの設定

ある AP から別の AP にクライアントがローミングする場合、クライアントは新しい IP アドレスが必要か、古い IP アドレスを引き続き使用できるのかを判断する必要があります。 クライアントはローミング中に、次の動作を実行する必要があります。

- DHCP から有効な IP アドレスを取得
- IP 重複アドレス検出の有効化
- Mobile IP Signaling の有効化（必要な場合）
- バーチャルプライベートネットワーク（VPN）インターネットキー交換（IKE）シグナリング（必要な場合）

Cisco WLC の導入において、同じモビリティ グループでローミングする場合、クライアント IP アドレスは変更されません。 同じまたは異なるサブセットの同じモビリティ グループにある 1 つ以上の WLC で管理される AP 間でも、WLC の導入ではクライアント ローミングがサポートされます。 セッションがアクティブである限り、セッションはそのまま持続され、WLC 間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当ての IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。

シスコの高速セキュア ローミング プロトコル（CCKM または PKC）を使用せずにローミングするクライアントは、現在の IP アドレスを要求する DHCP 要求を送信します。 Cisco WLC 環境において、WLC インフラストラクチャはクライアントが同じサブネットに留まり、古い IP アドレスを引き続き使用できるようにします。 次に、クライアントは自身の IP アドレスに ping を実行して重複アドレス検出を試行し、使用中の同じ IP アドレスで応答する WLAN クライアントがないか確認します。 クライアントがモバイル IP または VPN を使用している場合は、IP アドレスが固有であることが確認された後にそれらのプロトコルを使用します。

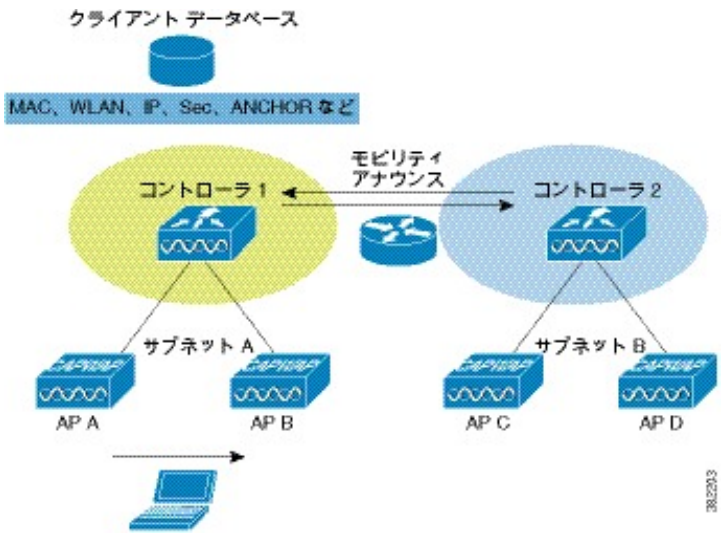
# クライアントローミングのインフラストラクチャへの影響

ワイヤレス クライアントが AP に認証およびアソシエートする場合、AP の WLC は自身のモビリティ データベースに対象クライアントのエントリを登録します。 このエントリにはクライアントの MAC アドレスおよび IP アドレス、セキュリティ コンテキスト、アソシエーション、QoS コンテキスト、WLAN、アソシエートした AP が含まれています。 WLC はこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。

ワイヤレス クライアントが自身のアソシエーションを AP から別の AP へ移動する場合は、WLC が新しくアソシエートした AP でクライアント データベースを更新します。 必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。

同一または異なるサブセットで同じモビリティ グループの WLC で管理される AP 間でも、複数の WLC の導入でクライアント ローミングがサポートされます。 セッションがアクティブである限り、セッションはそのまま持続され、WLC 間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当ての IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。 次の図に、このコンテキストのローミングを示します。

**図 *56*：*WLAN* インフラストラクチャのローミング**



### ローミング遅延の測定

ローミングは、次のコンポーネントに分割できます。

- クライアント ローミングの決定
- クライアントがローミングする新しい AP の選択
- 新しい AP への再認証
- IP レイヤの設定
- クライアント ローミングのインフラストラクチャへの影響

前述した各コンポーネントは、ローミングの遅延が発生する要因になります。 しかし、ローミング遅延の測定方法に業界で統一されたものはありません。 ローミング遅延の最も現実的な測定は、古い AP のローミング クライアントによって送信された最後のパケットから、新しい AP のローミング クライアントで受信された最初のパケットまでを対象にすることです。 これにより、前述したすべてのコンポーネントが測定され、次の表に示されているように双方向通信を確立させることができます。

**表 *14*：ローミング遅延の測定プロセスの概要**

| ローミング操作 | 測定ポイント | 説明 |
|---|---|---|
| 開始 | 古いAPのローミング クライアントによって送信された最後のパケット | ローミング遅延の測定を開始するときに、双方向通信の確立が継続していることを確認します。通常、クライアントがローミングを開始するとフレームは古いAPのローミング クライアントに引き続き転送されます。 |
| 終了 | 新しいAPのローミング クライアントが受信した最初のパケット | クライアントの新規ロケーションがネットワーク インフラストラクチャによって認識されていて、クライアントがパケットを送受信していることを確認し、双方向通信を保証します。 |

（注） 異なる WLAN 実装のローミング遅延を比較する場合は、どの場合でもローミング遅延の測定に同じ基準を使用するように留意します。

## クライアント ローミングのモニタリング

Cisco Compatible Extensions バージョン 4 のチャネル スキャン機能に加えて、Cisco Compatible Extensions バージョン 4 クライアントは、新しい AP にローミング理由を示すローミング理由レポートも送信します。 また、ネットワーク管理者はローミング履歴を作成およびモニタできるようになります。

次の表に示されている Cisco ワイヤレス LAN コントローラ コマンドライン インターフェイスのコマンドを使用して、Cisco Compatible Extensions レイヤ 2 クライアント ローミングの情報を確認します。

**表 *15*：*Cisco Compatible Extensions* レイヤ *2* クライアント ローミング**

| 目的 | 入力コマンド | 取得される情報 |
|---|---|---|
| 802.11a または 802.11b/g ネットワークのクライアント ローミング向けに設定された現在の RF パラメータを表示する | **show {802.11a \| 802.11bg} l2roam rf-params** | 802.11a または 802.11b/g ネットワークのクライアント ローミング向けに設定された現在の RF パラメータ |
| 特定の AP の Cisco Compatible Extensions レイヤ 2 クライアント ローミング統計情報を表示する | **show {802.11a \| 802.11bg} l2roam statistics ap_mac** | 次の情報を取得するには、このコマンドを使用します。<br>• 受信したローミング理由レポートの数<br>• 受信したネイバー リスト要求の数<br>• 送信したネイバー リスト レポートの数<br>• 送信したブロードキャスト ネイバー更新の数 |

| 目的 | 入力コマンド | 取得される情報 |
|---|---|---|
| 特定のクライアント ローミング履歴を表示する | **show client roam-history client_mac** | 次の情報を取得するには、このコマンドを使用します。<br>• レポートを受信した時刻<br>• 現在クライアントがアソシエートしている AP の MAC アドレス<br>• 以前クライアントがアソシエートしていた AP の MAC アドレス<br>• 以前クライアントがアソシエートしていた AP のチャネル<br>• 以前クライアントがアソシエートしていた AP の SSID<br>• 以前の AP からクライアントがアソシエート解除された時間<br>• クライアントがローミングした理由 |
| Cisco Compatible Extensions レイヤ 2 クライアント ローミングのデバッグ情報を取得する | **debug l2roam {detail \| error \| packet \| all} enable** | Cisco Compatible Extensions レイヤ 2 クライアント ローミングのデバッグ レポート |

### 802.11k 管理フレーム形式

次の図に、WildPackets スニファ トレースでキャプチャした復号化済みの 802.11k ネイバー リスト パケットを示します。 このパケットは Apple iPhone 5 がアソシエートした AP から送信されました。 iPhone は AP にネイバー要求フレームを送信し、 AP は現在隣接する AP のリストを使用して応答しました。 隣接する 3 つの AP の MAC アドレスとそれら AP の各 Wi-Fi チャネルが、802.11k ネイバー リスト応答フレームに組み込まれます。 この使用可能な情報により、802.11k モバイル クライアントは、すべての 5 GHz チャネルをスキャンしてローミング先候補の AP を検索する必要はありません。 一致するクレデンシャルがあり、クライアントのカバレッジ エリア内の AP に対して 802.11k クライアントのソフトウェアはローミングを実行きます。このエリアではバッテリ寿命が向上し、Wi-Fi チャネルの不必要な使用が減少し、コール処理を実行する Wi-Fi チャネルの電話は他より高い平均オピニオン評点（MOS）値の高品質なコールを維持します。 次の図に、

モバイル クライアントによって要求されたすべての要素情報を示します。 802.11k 仕様では、より多くの情報要素とさらなる詳細に対応します。

**図 *12*： *802.11k* ネイバーリストで復号化されたパケット**

```
Packet Info
  Packet Number:          10
  Flags:                  0x00000000
  Status:                 0x00000000
  Packet Length:          76
  Timestamp:              11:17:30.073269600 11/06/2012
  Data Rate:              18  9.0 Mbps
  Channel:                112  0MHz
  Signal Level:           17%
  Signal dBm:             -78
  Noise Level:            17%
  Noise dBm:              -95
802.11 MAC Header
  Version:                0  [0 Mask 0x03]
  Type:                   %00  Management  [0]
  Subtype:                %1101  Management Action  [0]
Frame Control Flags:      %00000000  [1]
                          0... .... Non-strict order
                          .0.. .... Non-Protected Frame
                          ..0. .... No More Data
                          ...0 .... Power Management - active mode
                          .... 0... This is not a Re-Transmission
                          .... .0.. Last or Unfragmented Frame
                          .... ..0. Not an Exit from the Distribution System
                          .... ...0 Not to the Distribution System
  Duration:               52  Microseconds  [2-3]
  Destination:            54:26:96:10:84:16  iPhone5 -1 8416  [0-5]
  Source:                 00:22:90:93:18:C4  Cisco:93:18:C4  [6-11]
  BSSID:                  00:22:90:93:18:C4  Cisco:93:18:C4  [12-17]
  Seq Number:             1397  [18-19 Mask 0xFFF0]
  Frag Number:            0  [18 Mask 0x0F]
802.11 Management - Action
  Category Code:          5  Radio Measurement  [20]
  Action Code:            5  Neighbor Report Response  [21]
  Dialog Token:           0x30  [22]
Neighbor Report
  Element ID:             52  Neighbor Report  [23]
  Length:                 13  [24]
  BSSID:                  00:21:1B:FC:41:C4  Cisco:FC:41:C4  [25-30]
  BSSID Information:      %11110111000000100000000000000000  [31-34]
                          ........ xxxxxx.. xxxxxxxx xxxxxxxx Reserved
                          ........ ......1. ........ ........ Immediate Block Ack Enabled
                          ........ .......0 ........ ........ Delayed Block Ack Disabled
                          1....... ........ ........ ........ Radio Measurement Enabled
                          .1...... ........ ........ ........ APSD Enabled
                          ..1..... ........ ........ ........ QoS/WMM is Enabled
                          ...1.... ........ ........ ........ Spectrum Management Enabled
                          ....0... ........ ........ ........ Key Scope is UnSet
                          .....1.. ........ ........ ........ Security is Set
                          ......11 ........ ........ ........ AP Reachability - Reachable

    Regulatory Class:     0  [35]
    Channel Number:       157  [36]
    PHY type:             7  [37]

  Neighbor Report
    Element ID:           52  Neighbor Report  [38]
    Length:               13  [39]
    BSSID:                04:FE:7F:48:DE:04  Cisco:48:DE:04  [40-45]
    BSSID Information:    %11110111000000100000000000000000  [46-49]
                          ........ xxxxxx.. xxxxxxxx xxxxxxxx Reserved
                          ........ ......1. ........ ........ Immediate Block Ack Enabled
                          ........ .......0 ........ ........ Delayed Block Ack Disabled
                          1....... ........ ........ ........ Radio Measurement Enabled
                          .1...... ........ ........ ........ APSD Enabled
                          ..1..... ........ ........ ........ QoS/WMM is Enabled
                          ...1.... ........ ........ ........ Spectrum Management Enabled
                          ....0... ........ ........ ........ Key Scope is UnSet
                          .....1.. ........ ........ ........ Security is Set
                          ......11 ........ ........ ........ AP Reachability - Reachable

    Regulatory Class:     0  [50]
    Channel Number:       108  [51]
    PHY type:             7  [52]

  Neighbor Report
    Element ID:           52  Neighbor Report  [53]
    Length:               13  [54]
    BSSID:                04:FE:7F:49:8B:E4  Cisco:49:8B:E4  [55-60]
    BSSID Information:    %11110111000000100000000000000000  [61-64]
                          ........ xxxxxx.. xxxxxxxx xxxxxxxx Reserved
                          ........ ......1. ........ ........ Immediate Block Ack Enabled
                          ........ .......0 ........ ........ Delayed Block Ack Disabled
                          1....... ........ ........ ........ Radio Measurement Enabled
                          .1...... ........ ........ ........ APSD Enabled
                          ..1..... ........ ........ ........ QoS/WMM is Enabled
                          ...1.... ........ ........ ........ Spectrum Management Enabled
                          ....0... ........ ........ ........ Key Scope is UnSet
                          .....1.. ........ ........ ........ Security is Set
                          ......11 ........ ........ ........ AP Reachability - Reachable

    Regulatory Class:     0  [65]
    Channel Number:       104  [66]
    PHY type:             7  [67]

FCS - Frame Check Sequence
  FCS:                    0xB2D77B10  [72-75]
```

347134

付 録 A

# 用語集



## 用語集

### A

| | |
|---|---|
| AAA | Authentication, Authorization, and Accounting（認証、許可、およびアカウンティング） |
| AC | Access Categories |
| ACM | Admission Control Mandatory |
| ADDTS | Add Traffic Stream |
| AES | Advanced Encryption Standard |
| ANonce | Authenticator Nonce |
| AP | Access Points |
| AVC | Application Visibility and Control（アプリケーションの可視性およびコントロール） |
| AVVID | Architecture for Voice, Video and Integrated Data |

### B

| | |
|---|---|
| BPSK | Binary Phase Shift Keying（2 位相偏移変調） |

| | |
|---|---|
| BSS | Basic Service Set |
| BSSID | Basic Service Set Identifier |
| BT | Bluetooth |
| BTK | Base Transient Key |
| BYOD | Bring Your Own Device（個人所有デバイスの持ち込み） |

## C

| | |
|---|---|
| CAC | Call Admission Control（コール アドミッション制御） |
| CAPWAP | Control and Provisioning of Wireless Access Points |
| CCA | Clear Channel Assessment |
| CCKM | Cisco Centralized Key Management |
| CCX | Cisco Compatible Extensions |
| CLI | Command Line Interface |
| CoS | Class of Service |
| CSMA-CA | Carrier Sense Multiple Access-Collision Avoidance（キャリア検知多重アクセス/衝突回避） |

## D

| | |
|---|---|
| dBm | Decibels per Milliwatt（デシベル/ミリワット） |
| DCF | Distributed Coordination Function（分散制御機能） |
| DFS | Dynamic Frequency Selection（動的周波数選択） |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Services |
| DS | Distributed System（分散システム） |
| DSCP | Differentiated Services Code Point |
| DTIM | Delivery Traffic Indication Map |

## E

| | |
|---|---|
| EAP | Extensible Authentication Protocol（拡張認証プロトコル） |
| EAP-FAST | EAP-Flexible Authentication via Secure Tunneling |
| EAP-TLS | EAP-Transport Layer Security |
| EAPOL | EAP over LAN |
| EDCF | Enhanced Distributed Coordination Function（拡張分散制御機能） |
| EF | Expedited Forwarding（緊急転送） |
| EMI | Electromagnetic interference（電磁波干渉） |
| EIGRP | Enterprise Interior Gateway Routing Protocol |
| EOSP | End-of-Service Period |

## F

| | |
|---|---|
| FMS | Fixed Mobile Substitution（モバイル通信による固定網通信の代替） |
| FT | Fast Transition |

## G

| | |
|---|---|
| GTC | Generic Token Card（汎用トークン カード） |
| GTK | Group Temporal Key |
| GUI | Graphical User Interface |

## H

| | |
|---|---|
| HA | High Availability（高可用性） |
| HCCA | Hybrid Coordinated Channel Access |
| H-REAP | Hybrid Remote Edge Access Point |

| | |
|---|---|
| HSRP | Hot Standby Router Protocol |
| HT | High Throughput |

## I

| | |
|---|---|
| IE | Information element（情報要素） |
| IKE | Internet Key Exchange |
| IM | Instant Messaging（インスタント メッセージ） |
| IP | Internet Protocol（インターネット プロトコル） |

## K

| | |
|---|---|
| KRK | Key Request Key |

## L

| | |
|---|---|
| LEAP | Lightweight EAP |
| LBS | Location-based Service（位置情報サービス） |

## M

| | |
|---|---|
| MAC | Media Access Control（メディア アクセス コントロール） |
| MCU | Media Control Unit（メディア制御ユニット） |
| MIC | Message Integrity Check |
| MIMO | Multiple Input - Multiple Output |
| MOS | Mean Opinion Score（平均オピニオン評点） |
| MRC | Maximum Ratio Combining（最大比合成） |
| MSCHAPv2 | Microsoft Challenge-Handshake Authentication Protocol Version 2（Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2） |

## N

| | |
|---|---|
| NBAR | Network Based Application Recognition |
| NSK | Network Session Key |
| NTP | Network Time Services |

## O

| | |
|---|---|
| OFDM | Orthogonal Frequency Division Multiplexing（直交周波数分割多重方式） |
| OKC | Opportunistic Key Cache |
| OSI | Open Systems Interconnection（オープン システム インターコネクション） |
| OSPF | Open Shortest Path First |

## P

| | |
|---|---|
| PAC | Protected Access Credential |
| PC | Personal Computer（パーソナル コンピュータ） |
| PEAP | Protected EAP |
| PHB | Per Hop Behavior |
| PIM | Protocol Independent Multicast |
| PKC | Proactive Key Caching |
| PKI | Public Key Infrastructure（公開キー インフラストラクチャ） |
| PLCP | Physical Layer Convergence Protocol |
| PMK | Pair-wise Master Key |
| PSTN | Public Switched Telephone Network（公衆電話交換網） |
| PTK | Pair-wise Temporal Key |

## Q

| | |
|---|---|
| QAM | Quadrature Amplitude Modulation（直交振幅変調） |
| QBSS | QoS Basic Service Set |
| QPSK | Quadrature Phase Shift Keying（4 位相偏移変調） |
| QoE | Quality of Experience |
| QoS | Quality of Service |

## R

| | |
|---|---|
| RADIUS | Remote Authentication Dial-in User Service（リモート認証ダイヤルイン ユーザ サービス） |
| RF | Radio Frequency（無線周波数） |
| RMM | Remote Management Module（リモート管理モジュール） |
| RRM | Radio Resource Management |
| RSSI | Received Signal Strength Indication（受信信号強度） |
| RToWLAN | Real-Time Traffic over Wireless LAN |

## S

| | |
|---|---|
| SIP | Session Initiation Protocol |
| SLA | Service-level Agreements（サービス レベル契約） |
| SNR | Signal-to-Noise Ratio（SN 比） |
| SNonce | Supplicant Nonce（サプリカント ナンス） |
| SSID | Service Set Identifier |

## T

| | |
|---|---|
| TDM | Time Division Multiplexing（時分割多重） |
| TIM | Traffic Indicator Map |

| | |
|---|---|
| TKIP | Temporal Key Integrity Protocol |
| TLS | Transport Layer Security |
| TPC | Transmitter Power Control（送信電力制御） |
| TSPEC | Traffic Specification |
| TSRS | Traffic Stream Rate Set |
| TXOP | Transmit Opportunity |

## U

| | |
|---|---|
| U-APSD | Unscheduled Automatic Power-Save Delivery |
| UDP | User Datagram Protocol |
| UNII | Unlicensed National Information Infrastructure |
| UP | User Priority（ユーザ優先度） |

## V

| | |
|---|---|
| VHT | Very High Throughput |
| VoWLAN | Voice over Wireless LAN |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network（バーチャル プライベート ネットワーク） |

## W

| | |
|---|---|
| WCS | Wireless Control System |
| WEP | Wired Equivalent Privacy |
| WLC | Wireless LAN Controller（ワイヤレス LAN コントローラ） |
| WLAN | Wireless LAN（ワイヤレス LAN） |
| WMM | Wi-Fi Multimedia Mode（Wi-Fi マルチメディア モード） |

| | |
|---|---|
| WPA | Wi-Fi Protected Access |
| WPA2 | Wi-Fi Protected Access 2 |

# 索 引

## 記号



## 数字



## A



## B



## C



## D



## E



## F



## K



## L



## M

## N



## P



## Q



## R



## S



## T



## U



## V



## W



## あ



## い



## お



## か



## き



## こ

## わ