VoIP ワイヤレス ネットワーク

この章では、ワイヤレス対応 Cisco Desktop Collaboration Experience DX600 シリーズの電話機と、ワイヤレス ローカル エリア ネットワーク（WLAN）環境における VoIP ネットワークのその他の主要コンポーネントとの相互対話の概要について説明します。

（注） ワイヤレス Cisco Desktop Collaboration Experience DX600 シリーズの電話機の導入および設定方法については、『*Cisco Desktop Collaboration Experience DX650 Wireless LAN Deployment Guide*』を参照してください。

この章の内容は、次のとおりです。

- ワイヤレス LAN（Wireless LAN），1 ページ
- WLAN の規格とテクノロジー，3 ページ
- Bluetooth ワイヤレス テクノロジー，11 ページ
- VoIP ワイヤレス ネットワークのコンポーネント，12 ページ
- WLAN 内の音声通信のセキュリティ，17 ページ
- VoIP WLAN 導入，25 ページ
- ワイヤレス LAN の設定，27 ページ

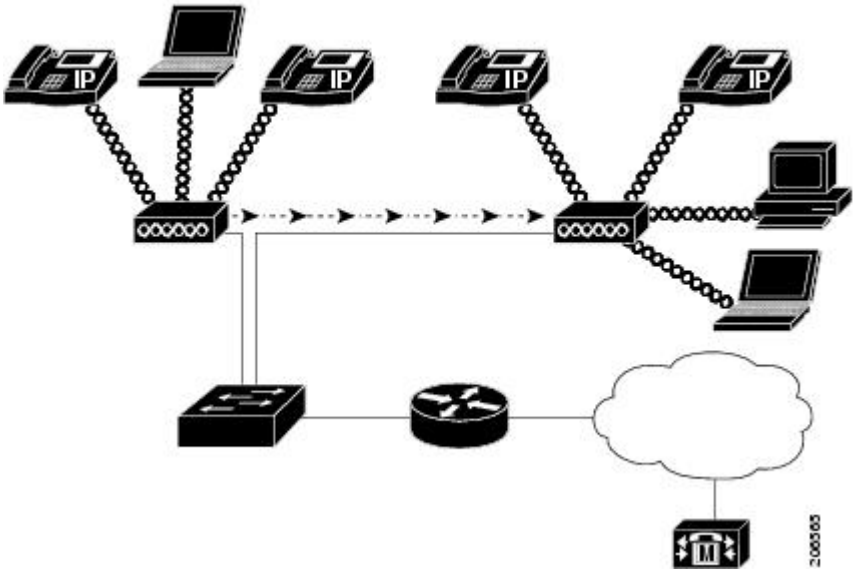
ワイヤレス LAN（Wireless LAN）

ワイヤレス通信の導入により、Cisco Desktop Collaboration Experience DX650 などのワイヤレス対応 Cisco Desktop Collaboration Experience DX600 シリーズの電話機を使用すると、社内の WLAN での音声通信が可能になります。 Cisco Desktop Collaboration Experience DX600 は、ワイヤレス音声通信を提供するために、ワイヤレス アクセス ポイント（AP）や、Cisco Unified CM の管理 などの主要な Cisco IP テレフォニー コンポーネントに依存していて、これらを使用して相互に対話します。 Cisco アクセス ポイントは、スタンドアロン モードまたは統合モードのいずれでも動作します。 統合モードでは、Cisco Unified Wireless LAN Controller が必要です。

Cisco Desktop Collaboration Experience DX650 には Wi-Fi 機能があり、802.11a、802.11b、802.11g、および 802.11n Wi-Fi を使用できます。

次の図に、ワイヤレス IP テレフォニーのワイヤレス音声伝送を可能にする典型的な WLAN トポロジを示します。

図 1：*Cisco Desktop Collaboration Experience での WLAN*



Cisco Desktop Collaboration Experience は、電源が投入されると、電話機のワイヤレス アクセスがオンに設定されている場合、AP を検索し、AP に関連付けされます。 記憶されているネットワークが圏外の場合は、ブロードキャストされているネットワークを選択するか、手動でネットワークを追加することができます。

AP は、有線ネットワークへの接続を使用して、スイッチとルータとの間でデータ パケットおよび音声パケットを送受信します。 音声シグナリングは、Cisco Unified Communications Manager サーバに送信され、呼処理とルーティングが行われます

AP は、ネットワークにワイヤレス リンクまたは「ホット スポット」を提供するため、WLAN の重要なコンポーネントとなっています。 音声通信をサポートする AP は Cisco IOS Release 12.4(21a)JY 以降を使用する必要があります。 Cisco IOS ソフトウェアには、音声トラフィックを管理する機能があります。 アクセス ポイントの詳細については、『DX600 Series Wireless LAN Deployment Guide』を参照してください。

一部の WLAN では、各 AP が、LAN 上に構成された Cisco Catalyst 3750 などのイーサネット スイッチに有線接続されています。 このスイッチにより、ワイヤレス IP テレフォニーをサポートするゲートウェイや Cisco Unified Communications Manager サーバにアクセスできます。

一部のネットワークには、ワイヤレス コンポーネントをサポートする有線コンポーネントが含まれます。 そのような有線コンポーネントには、ワイヤレス機能を有効にする特別なモジュールを装備したスイッチ、ルータ、ブリッジなどがあります。

Cisco Unified Wireless Network の詳細については、http://www.cisco.com/en/US/products/hw/wireless/index.htmlを参照してください。

WLAN の規格とテクノロジー

ここでは、WLAN 規格とテクノロジーについて説明します。

WLAN 通信の 802.11 規格

ワイヤレス LAN は、すべてのイーサネットベースのワイヤレス トラフィックの基準となるプロトコルを定義する電気電子学会（IEEE）802.11 規格に従う必要があります。 Cisco Desktop Collaboration Experience DX600 シリーズは、次の規格をサポートしています。

- 802.11a：5 GHz 周波数帯を使用して OFDM テクノロジーを使用することで、より多くのチャネルを提供し、データ レートを向上させます。 Dynamic Frequency Selection（DFS）および伝送パワー制御（TPC）は、この規格をサポートしています。
- 802.11b：低データ レート（1、2、5.5、11 Mbps）でデータの送信と受信の両方で 2.4 GHz の無線周波数（RF）を指定します。
- 802.11d：アクセス ポイントが、現在サポートされている無線チャネルおよび送信電力レベルを通知できるようにします。 802.11d が有効なクライアントは、その情報を使用して使用するチャネルと電力を決定します。 Cisco Desktop Collaboration Experience DX600シリーズ デバイスは、指定の国で法的に許可されたチャネルを判別するためにワールドモード（802.11d）が必要です。 サポートされているチャネルについては、次の表を参照してください。 Cisco IOS アクセス ポイントまたは Cisco Unified Wireless LAN Controller で 802.11d が適切に設定されていることを確認してください。 詳細については、ワールド モード（802.11d）, （5 ページ）および『*Cisco Desktop Collaboration Experience DX600 Wireless LAN Deployment Guide*』を参照してください。
- 802.11e：無線 LAN アプリケーションの一連の Quality of Service（QoS）拡張を定義します。
- 802.11g：802.11b と同じ免許不要の 2.4 GHz 周波数帯を使用します。ただし、直交周波数分割多重方式（OFDM）テクノロジーを使用することで、データ レートを高め、より高いパフォーマンスを提供します。 OFDM は、RF を使用して信号を伝送するための物理層の符号化テクノロジーです。
- 802.11h：5 GHz スペクトラムと伝送電力管理を提供します。 802.11a メディア アクセス コントロール（MAC）に、DFS と TPC を提供します。
- 802.11i：無線ネットワークにセキュリティ メカニズムを指定します。
- 802.11n：2.4 GHz または 5 GHz の無線周波数をデータの送信と受信に使用し、Multiple-Input Multiple-Output（MIMO）テクノロジー、チャネル ボンディング、およびペイロードの最適化を使用してデータ転送を強化します。

（注） Cisco Desktop Collaboration Experience DX600 シリーズ デバイスは 1 つのアンテナがあり、Single Input Single Output（SISO）システムを使用し、MCS 0〜7 データ レートのみサポートします（20 MHz で 72 Mbps および 40 MHz で 150 Mbps）。 より高いデータ レートを利用可能な MIMO テクノロジーを使用している 802.11n クライアントが存在する場合は、オプションとして MCS 8 〜 MCS 15 を有効にすることができます

次の表に、Cisco Desktop Collaboration Experience DX600 シリーズ デバイスでサポートされるチャネルを示しています。

部品番号	帯域範囲	使用可能なチャネル	5 GHz チャネル セット
	2.412 〜 2.484 GHz 5.180 〜 5.240 GHz 5.260 〜 5.320 GHz 5. 500 〜 5.700 GHz 5.745 〜 5.805 GHz	13（日本では 14） 4 4 11 4	UNII-2 UNII-2 UNII-2 拡張 UNII-3

（注） 802.11j（チャネル 34、38、42、46）およびチャネル 165 はサポートされていません。

表 *1*：*Cisco Desktop Collaboration Experience DX600* シリーズのサポートされているチャネル

部品番号	帯域範囲	使用可能なチャネル	チャネル セット
-	2.412〜2.472 GHz	13	1 〜 13
	5.180〜5.240 GHz	4	36、40、44、48
	5.260〜5.320 GHz	4	52、56、60、64
	5. 500〜5.700 GHz	11	100 〜 140
	5.745〜5.825 GHz	5	149、153、157、161、165

（注） 802.11j（チャネル 34、38、42、46）はサポートされていません。

ワールド モード（802.11d）

Cisco Desktop Collaboration Experience DX600 シリーズ デバイスをワールド モードで使用する場合、ワールドモード（802.11d）を有効にする必要があります。 Cisco Desktop Collaboration Experience DX600シリーズは、802.11dを使用して、使用するチャネルおよび伝送パワーを決定し、関連付けされたアクセス ポイントからクライアント設定を継承します。

（注） 周波数が 2.4 GHz で現在のアクセス ポイントがチャネル 1 ～ 11 で送信中である場合必ずしもワールド モード（802.11d）を有効にする必要はありません。

すべての国でこれらの周波数はサポートされているため、ワールドモード（802.11d）をサポートしているかどうかに関係なくこれらのチャネルのスキャンを試行できます。 2.4 GHz をサポートしている国については、次の『*Cisco Desktop Collaboration Experience DX650 Wireless LAN Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps12956/products_implementation_design_guides_list.html

アクセス ポイントが設置されている国に応じて、ワールド モード（802.11d）を有効にします。ワールド モードは、Cisco Unified Wireless LAN Controller に対して自動的に有効になります。

Cisco Autonomous Access Point の場合は、次のコマンドを使用してワールド モードを有効にする必要があります。

- **Interface dot11radio X**
- **world-mode dot11d country US both**

Cisco Desktop Collaboration Experience DX600 シリーズデバイスは、802.11d を使用して、使用するチャネルおよび伝送パワー レベルを決定し、関連付けされたアクセスポイントからクライアント設定を継承します。 Cisco Desktop Collaboration Experience をワールド モードで使用するには、アクセス ポイントのワールド モード（802.11d）を有効にします。

サポートされる国

Cisco Desktop Collaboration Experience DX600 シリーズ デバイスは次の国をサポートしています。

アルゼンチン（AR）	インド（IN）	ポーランド（PL）
オーストラリア（AU）	インドネシア（ID）	ポルトガル（PT）
オーストリア（AT）	アイルランド（IE）	プエルトリコ（PR）

ベルギー（BE）	イスラエル（IL）	ルーマニア（RO）
ブラジル（BR）	イタリア（IT）	ロシア連邦（RU）
ブルガリア（BG）	日本（JP）	サウジアラビア（SA）
カナダ（CA）	韓国（KR/KP）	シンガポール（SG）
チリ（CL）	ラトビア（LV）	スロバキア（SK）
コロンビア（CO）	リヒテンシュタイン（LI）	スロベニア（SI）
コスタリカ（CR）	リトアニア（LT）	南アフリカ（ZA）
キプロス（CY）	ルクセンブルク（LU）	スペイン（ES）
チェコ共和国（CZ）	マレーシア（MY）	スウェーデン（SE）
デンマーク（DK）	マルタ（MT）	スイス（CH）
エストニア（EE）	メキシコ（MX）	台湾（TW）
フィンランド（FI）	モナコ（MC）	タイ（TH）
フランス（FR）	オランダ（NL）	トルコ（TR）
ドイツ（DE）	ニュージーランド（NZ）	ウクライナ（UA）
ジブラルタル（GI）	ノルウェー（NO）	アラブ首長国連邦（AE）
ギリシャ（GR）	オマーン（OM）	イギリス（GB）
香港（HK）	パナマ（PA）	アメリカ合衆国（US）
ハンガリー（HU）	ペルー（PE）	ベネズエラ（VE）
アイスランド（IS）	フィリピン（PH）	ベトナム（VN）

無線周波数範囲

WLAN 通信では、次の無線周波数（RF）範囲が使用されます。

- 2.4 GHz：2.4 GHz を使用する多くのデバイスは、潜在的に 802.11b/g 接続と干渉を起こすおそれがあります。 干渉によってサービス拒否（DoS）シナリオが発生する可能性があり、正常な 802.11 伝送を妨害するおそれがあります。
- 5 GHz：この範囲は、Unlicensed National Information Infrastructure（UNII）周波数帯と呼ばれる複数の帯域に分割され、各帯域には4つのチャネルがあります。 重複しないチャネル、お

よび 2.4 GHz よりも多くのチャネルを提供するため、各チャネルに 20 MHz ずつ割り当てられます。

802.11 のデータ レート、送信電力、範囲、およびデシベル許容値

次の表に、801.11 規格別の送信（Tx）電力キャパシティ、データ レート、範囲（フィート単位とメートル単位）、および受信機によって許容されるデシベル値を示します。

表 *2* : 規格別の *Tx Power*、範囲、およびデシベル値

Standard	最大 Tx Power（注 1 を参照）	データ レート（注2を参照）	範囲	受信感度
802.11a				
	16 dBm	6 Mbps	604 フィート（184 m）	-91 dBm
		9 Mbps	604 フィート（184 m）	-90 dBm
		12 Mbps	551 フィート（168 m）	-88 dBm
		18 Mbps	545 フィート（166 m）	-86 dBm
		24 Mbps	512 フィート（156 m）	-82 dBm
		36 Mbps	420 フィート（128 m）	-80 dBm
		48 Mbps	322 フィート（98 m）	-77 dBm
		54 Mbps	289 フィート（88 m）	-75 dBm
802.11g				

Standard	最大 Tx Power（注 1 を参照）	データ レート（注2を参照）	範囲	受信感度
	16 dBm	6 Mbps	709 フィート（216 m）	-91 dBm
		9 Mbps	650 フィート（198 m）	-90 dBm
		12 Mbps	623 フィート（190 m）	-87 dBm
		18 Mbps	623 フィート（190 m）	-86 dBm
		24 Mbps	623 フィート（190 m）	-82 dBm
		36 Mbps	495 フィート（151 m）	-80 dBm
		48 Mbps	413 フィート（126 m）	-77 dBm
		54 Mbps	394 フィート（120 m）	-76 dBm
802.11b				
	17 dBm	1 Mbps	1,010 フィート（308 m）	-96 dBm
		2 Mbps	951 フィート（290 m）	-85 dBm
		5.5 Mbps	919 フィート（280 m）	-90 dBm
		11 Mbps	902 フィート（275 m）	-87 dBm

（注）

1. AP クライアントの設定が有効である場合、AP との関連付けを行うときに動的に調整します。
2. AP の通知するレートが使用されます。 データ レート制限機能が Cisco Unified Communications Manager の管理ページの電話機の設定で有効になっている場合は、Traffic Stream Rate Set IE（CCX V4）が使用されます。

サポートされているデータ レート、WLAN の Tx Power および受信機の感度の詳細については、『*Cisco Desktop Collaboration Experience DX650 Wireless LAN Deployment Guide*』を参照してください。

ワイヤレス変調テクノロジー

ワイヤレス通信では、シグナリングに次の変調テクノロジーが使用されます。

ダイレクト シーケンス スペクトラム拡散方式（DSSS）

信号を周波数範囲または帯域幅に分散することで、干渉を防止しています。 DSSS テクノロジーは、データの塊を複数の周波数上に多重化し、複数のデバイスが干渉を受けずに通信できるようにします。 各デバイスは、そのデバイスのデータ パケットを識別する特殊なコードを持ち、その他のデータ パケットはすべて無視されます。 Cisco ワイヤレス 802.11b/g 製品は、WLAN 上の複数のデバイスをサポートするために DSSS テクノロジーを使用しています。

直交周波数分割多重方式（OFDM）

RF を使用して信号を伝送します。 OFDM は、物理層の符号化テクノロジーで、1 つの高速データ キャリアを複数のより低速なキャリアに分割し、RF スペクトラムを経由してそれらを並行して伝送します。 802.11g および 802.11a で使用した場合、OFDM は最大 54 Mbps のデータ レートをサポートします。

次の表に、データ レート、チャネル数、および変調テクノロジーを規格別に比較したものを示します。

表 *3*：*IEEE* 規格別のデータ レート、チャネル数、および変調テクノロジー

項目	802.11b	802.11g	802.11a	802.11n
データ レート	1、2、5.5、11 Mbps	6、9、12、18、24、36、48、54 Mbps	6、9、12、18、24、36、48、54 Mbps	• 20 MHz チャネル: 7～72 Mbps • 40 MHz チャネル: 15～150 Mbps
重複しないチャネル	3（日本では 4 チャネルを使用）	3	最大 23	13 または 24
ワイヤレス変調	DSSS	OFDM	OFDM	OFDM

AP、チャネル、規制区域の関係

AP は、2.4 GHz または 5 GHz の周波数帯域のチャネルを使用して、RF 信号を送受信します。 安定したワイヤレス環境を提供し、チャネルの干渉を減少させるために、各 AP に重複しないチャネルを指定する必要があります。 北米の 802.11b および 802.11g 用に推奨されているチャネルは、1、6、11 です。

（注） コントローラベース以外のワイヤレス ネットワークでは、各 AP にチャネルを静的に設定することをお勧めします。 断続的に干渉が発生する場合、一部のチャネルはそのエリアでの途絶を防止するため、静的な設定が必要になることがあります。 ワイヤレス ネットワークでコントローラが使用されている場合、音声の途絶を最小限に抑える Auto-RF 機能を使用してください。

AP、チャネル、および規制区域の関係の詳細については、『*Cisco Desktop Collaboration Experience DX650 Wireless LAN Deployment Guide*』の「Designing the Wireless LAN for Voice」の章を参照してください。

関連トピック

VoIP WLAN 導入, （25 ページ）

WLAN とローミング

Cisco Desktop Collaboration Experience DX650 は、集中化されたキー管理プロトコルである Cisco Centralized Key Management（CCKM）をサポートしていて、またワイヤレス ドメイン サーバ（WDS）のセッション クレデンシャルのキャッシュを提供します。 AP は、高速ローミングが機能するために WDS に登録する必要があります。 CCKM は、Cisco Unified Wireless LAN Controller 単独でもサポートされています。

Cisco Desktop Collaboration Experience DX650 は、802.1X+WEP または WPA（TKIP）を使用した CCKM だけをサポートしています。 CCKM は、WPA2 または WPA（AES）をサポートしません。 CCKM の詳細については、次の Web サイトにある『*Cisco Fast Secure Roaming Application Note*』を参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

関連トピック

ワイヤレス ネットワークでの音声 QoS, （13 ページ）
VoIP WLAN 導入, （25 ページ）

Bluetooth ワイヤレス テクノロジー

Bluetooth では、30 フィート（10 m）以内の範囲の低帯域幅でワイヤレス接続を行えます。 最大のパフォーマンスが得られるのは、1 ～ 2 m（3 ～ 6 フィート）の範囲内です。 Bluetooth ワイヤレス テクノロジーは、2.4 GHz 帯域で動作します。これは 802.11b/g 帯域と同じです。 これは干渉が発生する可能性があります。 次のことを推奨します。

- 5 GHz 帯域で動作する 802.11a を使用する。
- 他の 802.11b/g デバイス、Bluetooth デバイス、電子レンジ、大型の金属製品との間隔をあけます。

Cisco Desktop Collaboration Experience DX650 上で Bluetooth を設定する方法の詳細については、Bluetooth 設定メニュー を参照してください。 Cisco Desktop Collaboration Experience DX650 での Bluetooth ヘッドセットの使用に関する詳細については、ハンズフリー プロファイル と、『Cisco Desktop Collaboration Experience DX600 Series Wireless LAN Deployment Guide』の「*Bluetooth Configuration*」の項を参照してください。

関連トピック

Bluetooth ワイヤレス ヘッドセット

VoIP ワイヤレス ネットワークのコンポーネント

Cisco Desktop Collaboration Experience DX650 は、コールを正常に発信および受信するために、WLAN の複数のネットワーク コンポーネントと相互対話する必要があります。 次の各トピックでは、ネットワーク コンポーネントについて説明します。

- Cisco Unified Wireless AP の対話, （12 ページ）
- ワイヤレス ネットワークでの音声 QoS, （13 ページ）
- Cisco Unified Communications Manager の連携, （16 ページ）

Cisco Unified Wireless AP の対話

Cisco Desktop Collaboration Experience DX600 シリーズ デバイスはワイヤレス データ デバイスと同じ AP を使用します。 ただし、WLAN の音声トラフィックには、データ トラフィック専用の WLAN とは異なる機器の設定とレイアウトが必要です。 データ伝送では、音声伝送よりも高いレベルの RF ノイズ、パケット損失、およびチャネル コンテンションに耐えることができます。 音声伝送時のパケット損失では、不安定な音声や途切れた音声によって結果的に通話が聞き取れなくなる可能性があります。 パケット エラーにより、ビデオにブロック ノイズが発生したり、ビデオがフリーズしたりすることもあります。

Cisco Desktop Collaboration Experience DX650 はデスクトップ電話機であるため（携帯電話ではないため）、ローカル環境の変化により、電話機でアクセス ポイント間のローミングが発生して、音声およびビデオ パフォーマンスに影響が出る可能性があります。 これとは対照的に、データ ユーザは一箇所に留まって、ときどき別の場所に移動します。 コールを保持しながらローミングが可能であることは、ワイヤレス音声の 1 つの利点です。そのため、RF カバレッジには、吹き抜け、エレベータ、会議室の外にある人気のない場所、通路などを含める必要があります。

優れた音声品質と最適な RF 信号カバレッジを確保するために、サイトの調査を実行する必要があります。 サイトの調査により、ワイヤレス音声に適した設定が決定されます。またサイトの調査は、AP の位置、電力レベル、チャネル割り当てなど、WLAN の設計とレイアウトに役立ちます。

ワイヤレス音声を導入し、使用できるようにした後も、引き続き設置後のサイトの調査を実施する必要があります。 新規ユーザ グループの追加、機器の追加設置、または大量のインベントリのスタックを行うと、ワイヤレス環境が変化します。 設置後の調査で、AP のカバレッジがそれまでと同様に最適な音声通信にとって十分であるかを検証します。

（注） ローミング中にはパケット損失が発生します。しかし、セキュリティ モードおよび高速ローミングの存在により、伝送中のパケット損失数が決まります。 Cisco Centralized Key Management（CCKM）を実装して、高速ローミングを有効にすることを推奨します。

ワイヤレス ネットワークにおける音声 QoS の詳細については、『*Cisco Desktop Collaboration Experience DX650 Wireless LAN Deployment Guide*』を参照してください。

アクセス ポイント アソシエーション

Cisco Desktop Collaboration Experience DX650 は、起動時に、認識できる SSID と暗号タイプを持つ AP をスキャンします。 この電話機は、適格な AP のリストを構築および保守し、次の変数を使用して最適な AP を決定します。

- 受信信号強度インジケータ（RSSI）：RF カバレッジ区域内で使用可能な AP の信号強度。 電話機は、最も高い RSSI 値を持つ AP と関連付けを持とうとします。
- トラフィック仕様（TSpec）：コール制限および WLAN ロード バランシングの計算。 各音声ストリームの TSpec 値を使用して、ファーストカム、ファーストサーブド方式に基づいて、音声デバイスに帯域幅を割り当てることができます。

Cisco Desktop Collaboration Experience DX650 は、最大の RSSI 値と最少のチャネル利用率の値（QBSS）を持ち、SSID と暗号化タイプが一致する AP に関連付けられます。 音声トラフィックが適切に処理されるように、AP に正しい QoS を設定する必要があります。

関連トピック

ワイヤレス ネットワークでの音声 QoS, （13 ページ）
WLAN 内の音声通信のセキュリティ, （17 ページ）
VoIP WLAN 導入, （25 ページ）

ワイヤレス ネットワークでの音声 QoS

ワイヤレス LAN の音声トラフィックは、データ トラフィックの場合と同様に、遅延、ジッター、およびパケット損失の影響を受けます。 これらの問題は、データのエンドユーザには影響しませんが、音声コールに重大な影響を及ぼすことがあります。 音声トラフィックが、遅延やジッターの少ない、適時の信頼できる処理を確実に受けられるようにするには、Quality of Service（QoS）を使用して、音声とデータを個別の仮想 LAN（VLAN）を使用する必要があります。 音声トラフィックを別の VLAN に分離することにより、QoS を使用して、音声パケットがネットワーク上を移動するときに優先度の高い処理を提供することができます。 また、データ トラフィックの場合は、通常すべてのネットワーク デバイスが使用するデフォルト ネイティブ VLAN ではなく、個別の VLAN を使用してください。

WLAN での音声接続をサポートするネットワーク スイッチと AP に、次の VLAN を構成する必要があります。

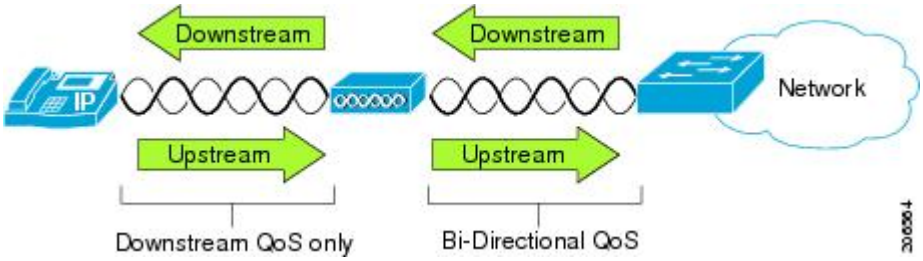
- Voice/Video VLAN：Cisco Desktop Collaboration Experience の間で送受信される音声トラフィック
- データ VLAN：その他のワイヤレス デバイスとの間で送受信されるデータ トラフィック
- ネイティブ VLAN：AP 管理

ボイス VLAN とデータ VLAN には個別の SSID を割り当てます。 WLAN で別の管理 VLAN を構成する場合は、SSID を管理 VLAN に関連付けしないでください。

電話機をボイス VLAN に分離し、より高い QoS を音声パケットに割り当てることで、音声トラフィックがデータ トラフィックよりもプライオリティの高い処理を確実に受けるようにできます。その結果、パケットの遅延や損失パケットを低下させることができます。

専用帯域幅を持つ有線ネットワークとは異なり、ワイヤレス LAN では、QoA の実装時にトラフィックの方向を考慮します。次の図に示すように、トラフィックはAPによってアップストリームまたはダウンストリームに分類されます。

図 *2*：ワイヤレス ネットワークでの音声トラフィック



Cisco IOS release 12.2(11)JA 以降、Cisco Aironet AP は Enhanced Distributed Coordination Function（EDCF）と呼ばれるコンテンションベースのチャネル アクセス メカニズムをサポートしています。 EDCF タイプの QoS には、ダウンストリーム（802.11b/g クライアント方向）QoS 用に最大 8 つのキューがあります。 キューは次のオプションに基づいて割り当てることができます。

- パケットの QoS または DiffServ コード ポイント（DSCP）設定
- レイヤ 2 またはレイヤ 3 アクセス リスト
- 特定のトラフィックの VLAN
- デバイスの動的登録

AP で最大 8 つのキューを設定できますが、可能な限り高い音声 QoS を保障するため、音声トラフィックに使用するキューは 2 つだけに留める必要があります。 音声（RTP）トラフィックとシグナリング（SIP）トラフィックを最高プライオリティ キューに入れ、データ トラフィックをベストエフォート キューに入れます。 802.11b/g EDCF では音声トラフィックがデータ トラフィックから保護される保証はありませんが、このキューイング モデルを使用することで、統計的に最高の結果が得られます。

各キューは次のとおりです。

- ベスト エフォート（BE）：0、3
- バックグラウンド（BK）：1、2
- ビデオ（VI）：4、5
- ビデオ（VO）：6、7

（注） Cisco Desktop Collaboration Experience は、SIP シグナリング パケットに DSCP 値 24（CS3）をマークし、RTP パケットに DSCP 値 46（EF）をマークします。

（注） コール制御（SIP）は、UP4（VI）として送信されます。 アドミッション制御必須（ACM）がビデオに対して無効になっている場合（Traffic Specification（TSpec）無効）、ビデオは UP5（VI）として送信されます。 ACM が音声に対して無効になっている場合（TSpec 無効）、音声は UP6（VO）として送信されます。

次の表に、音声、ビデオ、およびコール制御（SIP）のトラフィックを優先する AP 上の QoS プロファイルを示します。

表 4：*QoS* プロファイルとインターフェイス設定

トラフィックのタイプ	DSCP	802.1p	WMM UP	ポート範囲
音声	EF（46）	5	6	UDP 16384 ～ 32677
インタラクティブ ビデオ	AF41（34）	4	5	UDP 16384 ～ 32677
呼制御	CS3（24）	3	4	TCP/UDP 5060 ～ 5061

非決定性環境での音声伝送の信頼性を改善するため、Cisco Desktop Collaboration Experience は IEEE 802.11e 業界規格をサポートし、Wi-Fi Multimedia（WMM）に対応しています。 WMM は、音声、ビデオ、ベストエフォート データ、およびその他のトラフィックの差別化サービスを可能にします。 ただし、これらの差別化サービスが音声パケットに十分な QoS を提供するために、一度に 1 つのチャネルで一定量の音声帯域幅だけが使用可能または許可されています。 ネットワークが予約済み帯域幅で処理可能なボイスコールが「N」個で、音声トラフィックの量がこの制限を超えた（N+1 個のコール）場合、すべてのコールの品質が低下します。

VoIP の安定性とローミングの問題に対処するには、初期コールアドミッション制御（CAC）方式が必要です。 CAC は、アクティブな音声コールが AP に設定された制限を超過しないように保証することで、ネットワークが過負荷の場合でも QoS を維持します。 Cisco Desktop Collaboration Experience は、レイヤ 2 TSpec アドミッション コントロールとレイヤ 3 Cisco Unified Communications Manager アドミッション コントロール（RSVP）を統合できます。 ネットワークが輻輳している間、発信側と着信側は、ファースト ビジー インジケータを受け取ります。 システムは、AP がフル キャパシティの場合でも、ワイヤレス電話クライアントが隣接 AP へローミングできる程度の帯域幅の予約を維持します。 音声帯域幅制限に達した後、次のコールは、チャネル上の既存のコールの品質に影響を与えずに、隣接 AP に負荷分散されます。

良好な音声品質を維持するために、接続されたイーサネット スイッチに QoS を実装することを推奨します。 Cisco Desktop Collaboration Experience が設定した COS および DSCP 値は、変更する必要はありません。

（注） Cisco Desktop Collaboration Experience はビデオ CAC をサポートしていませんが、WLAN の音声 CAC はサポートしています。

VoIP コール品質の問題に対処するには、初期コール アドミッション制御（CAC）方式が必要です。 WLAN 上で SIP CAC が有効になっている場合、アクティブなボイスコールの数が AP に設定された制限を超過しないように保証することで、ネットワークが過負荷の場合でも QoS が維持されます。 ネットワークが輻輳している間、システムは AP が「フル キャパシティ」の場合でも、ワイヤレス電話クライアントが隣接 AP へローミングできる程度の帯域幅の予約を維持します。音声帯域幅制限に達した後、次のコールは、チャネル上の既存のコールの品質に影響を与えずに、隣接 AP に負荷分散されます。

（注） Cisco Desktop Collaboration Experience は SIP 通信には TCP を使用し、Cisco Unified Communications Manager AP がフル キャパシティの場合 での登録が失われる可能性があります。 CAC によって承認されていないクライアントから送受信サれるフレームはドロップされるため、登録解除の原因となることがあります。 そのため、SIP CAC を無効にすることを推奨します。

良好な音声品質を維持するためには、接続されたイーサネット スイッチに QoS を実装することを推奨します。 Cisco Desktop Collaboration Experience が設定したサービス クラス（CoS）および DSCP 値は、変更する必要はありません。

（注） ビデオ フレームの最適な伝送を行うために、DSCP、COS、および WMM UP マーキングが正しく表示されます。 Cisco Desktop Collaboration Experience では音声とビデオの CAC がサポートされていないため、SOP CAC を実装することを推奨します。

関連トピック

認証方式, （17 ページ）
Cisco Unified Communications Manager の連携, （16 ページ）
VoIP WLAN 導入, （25 ページ）

Cisco Unified Communications Manager の連携

Cisco Unified Communications Manager は、ワイヤレス IP Phone のコールを処理しルーティングするネットワーク内のコール制御コンポーネントです。 Cisco Unified Communications Manager は、電話会議やルート プランなどの機能で使用する IP テレフォニー システムのコンポーネント（電話機、アクセス ゲートウェイ、およびリソース）を管理します。 ワイヤレス LAN に Cisco Desktop Collaboration Experience を導入する場合、Cisco Unified Communications Manager Release 7.1(3) 以降および SIP を使用する必要があります。

Cisco Unified Communications Manager から Cisco Desktop Collaboration Experience が認識されるようになるには、その電話機が Cisco Unified Communications Manager に登録され、データベース内で設定される必要があります。

Cisco Unified Communications Manager を構成して、Cisco Desktop Collaboration Experience デバイスおよびIPデバイスとともに使用する方法の詳細については、『*Cisco Unified Communications Manager Administration Guide*』、『*Cisco Unified Communications Manager System Guide*』および『*Cisco Desktop Collaboration Experience DX600 Series Wireless LAN Deployment Guide*』を参照してください。

関連トピック

Cisco Unified Communications Manager での Cisco Desktop Collaboration Experience のセットアップ

WLAN 内の音声通信のセキュリティ

通信圏内にあるすべての WLAN デバイスは他の WLAN トラフィックをすべて受信できるため、WLAN内の音声通信の保護は重要です。 音声トラフィックが侵入者によって操作または傍受されることのないように、Cisco SAFE セキュリティ アーキテクチャは Cisco Desktop Collaboration Experience と Cisco Aironet AP をサポートしています。 ネットワーク内のセキュリティの詳細については、http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html を参照してください。

認証方式

Cisco Wireless IP テレフォニー ソリューションは、次の Cisco Desktop Collaboration Experience がサポートする認証方式を使用して、不正ログインおよび改ざんされた通信を防ぐワイヤレス ネットワーク セキュリティを提供します。

- オープン認証：オープン システムでは、任意のワイヤレスデバイスが認証を要求できます。 要求を受けた AP は、任意のリクエスタまたはユーザのリスト上にあるリクエスタだけに認証を与える場合があります。 ワイヤレス デバイスと AP との間の通信は暗号化されない可能性もあります。暗号化される場合、デバイスは有線と同等のプライバシー（WEP）キーを使用してセキュリティを提供できます。 WEP を使用しているデバイスは、WEP を使用している AP での認証だけを試みます。
- 共有キー認証：AP は、AP との通信を試みるすべてのデバイスに対して、暗号化されていないチャレンジテキストのストリングを送信します。 認証を要求しているデバイスは、事前に設定された WEP キーを使用してチャレンジ テキストを暗号化し、AP に返します。 チャレンジテキストが正しく暗号化されている場合、AP は要求側のデバイスの認証を許可します。 デバイスの WEP キーが AP 上の WEP キーと一致する場合にだけ、デバイスは認証を受けることができます。

  共有キー認証は、他のユーザがチャレンジをモニタできるため、WEPによるオープン認証よりも安全性が低くなる可能性があります。 暗号化されていないチャレンジ テキスト ストリ

ングと暗号化されているチャレンジ テキスト ストリングを比較することにより、侵入者は WEP キーを計算できます。

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）認証：このクライアント サーバのセキュリティ アーキテクチャは、AP と、Cisco Access Control Server（ACS）などの RADIUS サーバとの間の Transport Level Security（TLS）トンネル内の EAP トランザクションを暗号化します。

  TLS トンネルでは、クライアント（電話機）と RADIUS サーバの間の認証に Protected Access Credential（PAC）が使用されます。 サーバは Authority ID（AID）をクライアント（電話機）に送信します。それを受けてクライアントは適切な PAC を選択します。 クライアント（電話機）は PAC-Opaque を RADIUS サーバに返します。 サーバは、そのマスターキーで PAC を復号します。 これで両方のエンドポイントに同じ PAC キーが含まれ、TLS トンネルが構築されます。 EAP-FAST では、自動 PAC プロビジョニングがサポートされていますが、RADIUS サーバ上で有効にする必要があります。

  （注） Cisco ACS での PAC の有効期限は、デフォルトで 1 週間です。 電話機に期限切れの PAC が存在する場合、電話機が新しい PAC を取得するまでの間は、RADIUS サーバでの認証に比較的長い時間がかかります。 PAC プロビジョニングの遅延を回避するには、ACS サーバまたは RADIUS サーバで PAC の有効期間を 90 日以上に設定します。

- Light Extensible Authentication Protocol（LEAP）：クライアント（電話機）と RADIUS サーバ間の、シスコ独自のパスワードベースの相互認証方式です。 Cisco Desktop Collaboration Experience は、ワイヤレス ネットワークでの認証に LEAP を使用できます。
- Auto（AKM）：AP、WPA-PSK、WPA が示す設定情報から自動的に 802.11 認証メカニズムを選択します。
- Wi-Fi Protected Access（WPA）
- Wi-Fi Protected Access 2（WPA2）
- Wi-Fi Protected Access-Pre-Shared Key（WPA-PSK）
- Wi-Fi Protected Access 2-Pre-Shared Key（WPA2-PSK）
- Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling（EAP-FAST）
- Protected Extensible Authentication Protocol（PEAP）

  （注） EAP-FAST と PEAP は、802.1X EAP 選択経由で WPA/WPA2 を選択する際の 802.x オプションです。

- Extensible Authentication Protocol – Transport Layer Security（EAP-TLS）

- Protected Extensible Authentication Protocol EAP-Generic Token Card（PEAP-GTC）と Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol Version 2（PEAP-MSCHAPV2）
- Cisco Centralized Key Management（CCKM）

（注） CCKM は、WPA/WPA2 と組み合わせてオプションで使用できます。

- Wired Equivalent Protocol（WEP）
- オープン（Open）

認証方法についての詳細については、『*Cisco Desktop Collaboration Experience DX600 Series Wireless LAN Deployment Guide*』の「Wireless Security」を参照してください。

Cisco Secure Access Control Server 証明書のセットアップ

Cisco Secure Access Control Server (ACS) は、認証情報の保護と検証を保障するために EAP-TLS と PEAP 認証プロトコルとデジタル証明書を使用する認証サーバです。 各 EAP 認証方式では、証明書が適切にインストールおよび設定されている必要があります。

ACS 証明書は、次の図に示す ACS 証明書のセットアップ ページで設定します。

図 *3*：*ACS* 証明書のセットアップ

EAP-TLS の設定

サーバ証明書のインストールは、次のガイドラインに従う必要があります。

1 インストールは ACS 証明書設定ページを使用して実行されます。

2 証明書には通常、秘密キー パスワードを持つ server.pem および server_privatekey.crt の 2 つのファイルが含まれます。

3 ルート認証局（CA）は、[ACS 認証局設定（ACS Certification Authority Setup）] ページを使用して設定する必要があります。

4 ルート CA は [証明書信頼リストの編集（Edit Certificate Trust List）] 設定ページで、信頼できる CA である必要があります。

5 中間 CA を使用してサーバ証明書を作成している場合は、ルート CA はルート CA とサーバ証明書間のチェーンですべての CA に対して設定する必要があります。 これは、中間 CA を使用して作成されたユーザ証明書にも適用されます。 次は、中間 CA の使用例です。

   a Wi-Fi ルート CA が、ルート CA。

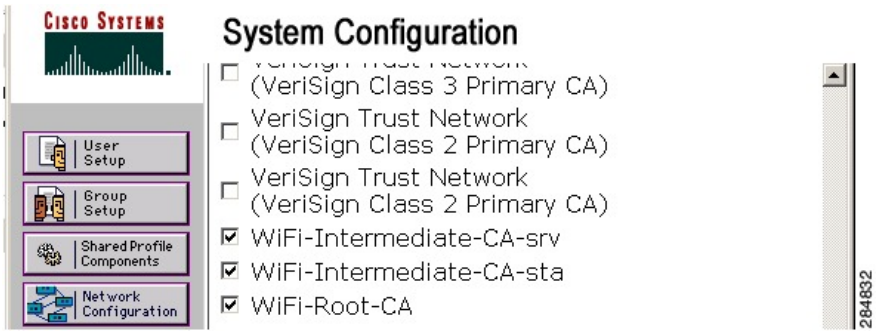
   b Wi-Fi-Intermediate-CA-srv が、ACS にインストールするサーバ証明書に署名した中間 CA（Wi-Fi ルート CA によって署名されている）。

   c Wi-Fi-Intermediate-CA-sta が、ACS にインストールするユーザ証明書に署名した CA 証明書。

6 証明書設定に加えて、ユーザ証明書の一般名に一致するユーザ アカウントを作成する必要があります。

7 証明書チェーン内のすべての CA 証明書は、次の図のようにインストールされ、信頼されている必要があります。

図 *4*：インストールおよび信頼済み *CA* 証明書

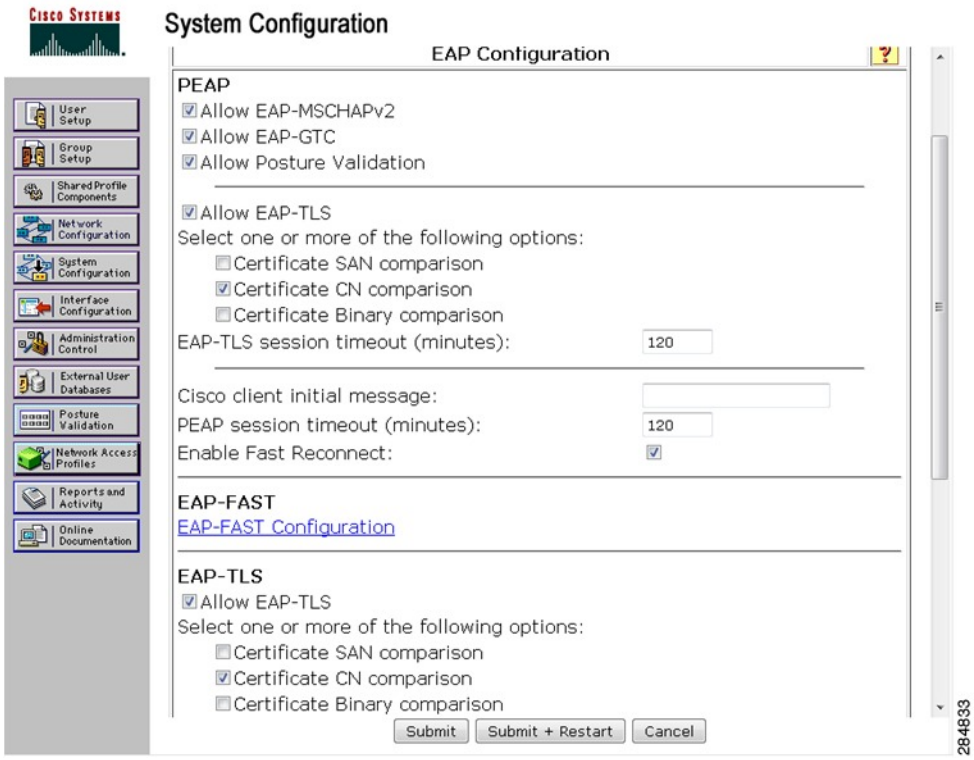


PEAP-GTC および PEAP-MSCHAPV2 の設定

証明書チェーン内のすべての CA 証明書がインストールされ、信頼されている必要があります。AD と同じユーザ ID を持つユーザ アカウントを作成する必要があります。

次の図は、[システム設定（System Configuration）] > [グローバル認証設定（Global Authentication Setup）] での EAP-TLS、PEAP-GTC および PEAP-MSCHAPV2 設定の例を示しています。

図 5：***EAP-TLS***、***PEAP-GTC*** および ***PEAP-MSCHAPV2*** のセットアップ



認証キー管理

次の認証方式では、RADIUS サーバを使用して認証キーを管理します。

- WPA/WPA2: 一意の認証キーを生成するために RADIUS サーバの情報を使用します。 これらのキーは、中央集中型の RADIUS サーバで生成されるため、WPA/WPA2 は、AP および電話機に格納されている WPA 事前共有キーよりも高いセキュリティを提供します。
- Cisco Centralized Key Management（CCKM）：RADIUS サーバとワイヤレス ドメイン サーバ（WDS）の情報を使用して、キーの管理および認証をします。 WDS は、高速でセキュアな再認証用に、CCKM 対応クライアントデバイスのセキュリティクレデンシャルのキャッシュを作成します。

WPA/WPA2 および CCKM では、暗号化キーは電話機に入力されず、AP と電話機の間で自動的に生成されます。 ただし認証で使用する EAP ユーザ名とパスワードは、各電話機に入力する必要があります。

（注） WPA（TKIP）および 802.1x（WEP）のみ CCKM をサポートします。

暗号化方式

音声トラフィックの安全性を確保するため、Cisco Desktop Collaboration Experience では、暗号化方式として WEP、TKIP、および Advanced Encryption Standards（AES）をサポートします。 暗号化にこれらのメカニズムを使用すると、AP と Cisco Desktop Collaboration Experience との間で、シグナリング Skinny Client Control Protocol（SCCP）パケットと音声リアルタイム トランスポート プロトコル（RTP）パケットの両方が暗号化されます。

WEP

ワイヤレス ネットワークで WEP を使用すると、オープン認証または共有キー認証を使用することにより、AP で認証が行われます。 正常に接続させるには、電話機で設定された WEP キーと AP で設定された WEP キーが一致する必要があります。 Cisco Desktop Collaboration Experience DX600 シリーズの電話機は、40 ビット暗号化または 128 ビット暗号化を使用し、電話機および AP で静的なままの WEP キーをサポートしています。

EAP と CCKM の認証では、暗号化に WEP キーを使用できます。 RADIUS サーバは WEP キーを管理し、すべての音声パケットの暗号化を認証した後で一意のキーを AP に渡します。そのため、次の WEP キーを各認証で変更できます。

TKIP

WPA と CCKM は、WEP にいくつかの改良が加えられた TKIP 暗号化を使用します。 TKIP は、パケットごとのキーの暗号化、および暗号化が強化されたより長い初期ベクトル（IV）を提供します。 さらに、メッセージ完全性チェック（MIC）は、暗号化されたパケットが変更されていないことを確認します。 TKIP は、侵入者が WEP を使用して WEP キーを解読する可能性を排除します。

AES

WPA2 認証に使用される暗号化方式。 この暗号化の国内規格は、暗号化と復号化に同じキーを持つ対称型アルゴリズムを使用します。 AES は、128 ビットサイズの暗号ブロック連鎖（CBC）暗号化を使用し、最小のキー サイズとして 128、192、および 256 ビットのキーをサポートします。 Cisco Desktop Collaboration Experience DX600 シリーズの電話機は 256 ビットのキー サイズをサポートします。

（注） Cisco Desktop Collaboration Experience は、CMIC による Cisco Key Integrity Protocol（CKIP）をサポートしません。

暗号化方式の詳細については、『*Cisco Desktop Collaboration Experience DX600 Series Wireless LAN Deployment Guide*』の「Wireless Security」を参照してください。

AP 認証および暗号化のオプション

認証方式と暗号化方式は、ワイヤレス LAN 内で設定されます。 VLAN は、ネットワーク内および AP 上で設定され、認証と暗号化の異なる組み合わせを指定します。 SSID は、VLAN と VLAN の特定の認証および暗号化方式に関連付けられます。 ワイヤレス クライアント デバイスを正常に認証するには、認証および暗号化方式で使用する SSID と同じ SSID を AP と Cisco Desktop Collaboration Experience に設定する必要があります。

一部の認証方式では、特定のタイプの暗号化が必要です。 オープン認証では、セキュリティを高めるために、暗号化で静的WEPを使用できます。 ただし、共有キー認証を使用している場合は、暗号化に静的 WEP を設定し、電話機で WEP キーを設定する必要があります。

Cisco Desktop Collaboration Experience に認証キー管理（AKM）を使用する場合は、認証と暗号化の方式に対する複数の選択肢を、異なる SSID を持つ AP で設定できます。 電話機は、認証を試みるときに、電話機でサポートする認証および暗号化方式を通知する AP で設定できます。 Auto（AKM）モードでは、WPA、WPA2、WPA 事前共有キー、または CCKM を使用して認証できます。

（注）

- WPA 事前共有キーまたは WPA2 事前共有キーを使用する場合、その事前共有キーを電話機で静的に設定する必要があります。 これらのキーは、APに存在するキーと一致している必要があります。
- Auto（AKM）モードを使用している場合、WPA、WPA2、WPA 事前共有キー、WPA2 事前共有キー、または CCKM の暗号化オプションは自動的に設定されます。
- AKM モードでは、電話機が WPA、WPA2、または CCKM キー管理を使用するように設定されている場合、または 802.1X が使用されている場合、電話機は LEAP を使用して認証されます。
- Cisco Desktop Collaboration Experience は、自動 EAP ネゴシエーションをサポートしていません。EAP-FAST モードを使用するには、EAP-FAST モードを指定する必要があります。

次の表に、Cisco Desktop Collaboration Experience がサポートしている、Cisco Aironet AP で設定される認証方式と暗号化方式のリストを示します。 表には、AP の設定に対応する電話機のネットワーク設定オプションを示します。

表 *5*：認証方式と暗号化方式

Cisco AP の設定			**Cisco Desktop Collaboration Experience の設定**
認証	キー管理	共通の暗号化	認証
オープン（Open）		なし	オープン（Open）

Cisco AP の設定			Cisco Desktop Collaboration Experience の設定
オープン（静的 WEP）（Open (Static WEP)）		WEP	オープン+WEP（Open+WEP）
共有キー（静的 WEP）（Shared key (Static WEP)）		WEP	共有+WEP（Shared+WEP）
LEAP 802.1X	オプションの CCKM	WEP	LEAP または自動（AKM）（Auto (AKM)）
LEAP WPA	WPA（オプションで CCKM を使用）	TKIP	LEAP または自動（AKM）（Auto (AKM)）
LEAP WPA2	WPA2	AES	LEAP または自動（AKM）（Auto (AKM)）
EAP-FAST 802.1X	オプションの CCKM	WEP	EAP-FAST
WPA を使用した EAP-FAST	WPA オプションの CCKM	TKIP	EAP-FAST
WPA2 を使用した EAP-FAST	WPA2	AES	EAP-FAST
WPA-PSK	WPA-PSK	TKIP	自動（AKM）（Auto (AKM)）
WPA2-PSK	WAP2-PSK	AES	自動（AKM）（Auto (AKM)）

シスコの WLAN セキュリティの詳細については、http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html を参照してください。

認証方式と暗号化方式を AP に設定する方法の詳細については、次の URL で入手可能なご使用のモデルおよびリリースの『*Cisco Aironet Configuration Guide*』を参照してください。

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

関連トピック

Cisco Unified Wireless AP の対話, （12 ページ）
認証方式, （17 ページ）
暗号化方式, （22 ページ）

Cisco Unified Communications Manager の連携, （16 ページ）
VoIP ワイヤレス ネットワークのコンポーネント, （12 ページ）
VoIP WLAN 導入, （25 ページ）

VoIP WLAN 導入

この項では、WLAN に Cisco Desktop Collaboration Experience デバイスを導入する際の設定ガイドラインについて説明します。

サポートされるアクセス ポイント

Cisco Desktop Collaboration Experience は、Cisco 自律ソリューションおよび統合ソリューションの両方でサポートされています。 最低バージョンと推奨バージョンは次のとおりです。

- Cisco IOS アクセス ポイント（Autonomous）
  - 最低 = 12.3(8)JEA2 以降
  - 推奨 = 12.4(10b)JA3 以降（Cisco Aironet シリーズ 1100、1140、1200、または 1230 には適用されません）。
- Cisco Unified Wireless LAN Controller
  - 最小 = 5.1.163.0 以降
  - 推奨 = 5.2.193.0 以降

- Cisco IOS アクセス ポイント（Autonomous）
  - 最低 = 12.4(21a)JY
  - 推奨 = 12.4(25d)JA 以降
- Cisco Unified Wireless LAN Controller
  - 最低 = 6.0.202.0
  - 推奨 = 7.0.116.0 以降

サポートされている AP およびモード

次の表では、各 Cisco アクセス ポイントでサポートされるモードを示します。

表 *6*：サポートされている *AP* およびモード

AP モデル	802.11b	802.11g	802.11a	自律モード	統合モード
Cisco Aironet 500 シリーズ	Yes	Yes	No	Yes	Yes
Cisco Aironet 1100 シリーズ	Yes	Yes	No	Yes	Yes
Cisco Aironet 1130 AG シリーズ	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1140 シリーズ	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1200 シリーズ	Yes	Yes	オプション	Yes	Yes
Cisco Aironet 1230 AG シリーズ	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1240 AG シリーズ	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1250 シリーズ	Yes	Yes	Yes	Yes	Yes
Cisco Aironet 1300 シリーズ	Yes	Yes	No	Yes	Yes

（注） Cisco Desktop Collaboration Experience は、屋外 MESH テクノロジー（Cisco Aironet 1500 シリーズ）を介した Voice over the Wireless LAN（VoWLAN）をサポートしていません。

相互運用性のテストを行っていないため、サードパーティ ベンダー製のアクセス ポイントはサポートされていません。ただし、そのアクセスポイントが主要な機能をサポートしていて規格に準拠している場合、Cisco Desktop Collaboration Experience は対応します。

サードパーティ ベンダー製の Wi-Fi 準拠 AP は、Cisco Desktop Collaboration Experience で機能しても、Wi-Fi Multimedia（WMM）、Unscheduled Auto Power Save Delivery（U-APSD）、トラフィック仕様（TSPEC）、QoS Basic Service Set（QBSS）、ダイナミック伝送パワー コントロール（DTPC）、またはプロキシ ARP などの主要な機能をサポートしない場合もあります。

サポートされるアンテナ

一部の Cisco アクセス ポイントでは、外部アンテナが必要であるか、使用可能です。 サポートされているアンテナのリストと、その取り付け方法については、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

（注） 全方位アンテナを搭載しているため、Cisco Aironet シリーズ 1130 および 1140 アクセス ポイントは天井に取り付ける必要があります。

サポートされているアンテナの一覧については、『*Cisco Desktop Collaboration Experience DX600 Series Wireless LAN Deployment Guide*』の「Supported Antennas」の章を参照してください。

ワイヤレス LAN の設定

ワイヤレス LAN が導入されている場所の Wi-Fi カバレッジがビデオ パケットおよび音声パケットの送信に最適であることを確認します。

音声およびビデオの Wi-Fi 接続が Cisco Desktop Collaboration Experience で有効になっている場合は、アプリケーション メニュー内の WLAN サイン イン アプリケーションを使用して Wi-Fi ネットワークを認証します。

アプリケーションを有効にするには、[アプリケーション（Applications）] > [管理者設定（Administrator Settings）] > [ネットワークのセットアップ（Network Setup）] > [WLAN のセットアップ（WLAN Setup）] > [WLAN サイン イン アクセス（WLAN Sign in Access）] に移動して、WLAN ネットワークを有効にします。

ユーザ名またはパスワードを変更するには、[アプリケーション（Applications）] > [管理者設定（Administrator Settings）] に移動します。

設定情報の詳細については、次の URL の『 *Cisco Desktop Collaboration Experience DX600 Series Wireless LAN Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps12956/products_implementation_design_guides_list.html

『*Cisco Desktop Collaboration Experience DX600 Series Wireless LAN Deployment Guide*』には、次の設定情報が含まれています。

- ワイヤレス ネットワークの設定
- Cisco Unified CM の管理 でのワイヤレス ネットワークの設定
- Cisco Desktop Collaboration Experience でのワイヤレスネットワークの設定

Cisco Desktop Collaboration Experience が WLAN に接続できるようになるには、適切な WLAN 設定で Cisco Desktop Collaboration Experience のネットワーク プロファイルを設定する必要があります。Cisco Desktop Collaboration Experience 上の [ネットワークのセットアップ（Network Setup）] メニューを使用して [WLAN のセットアップ（WLAN Setup）] サブメニューにアクセスし、WLAN 設定をセットアップすることができます。 手順については、[ワイヤレスとネットワークの設定（Wireless & network settings）] メニューを参照してください。

Cisco Unified Communications Manager Administration でのワイヤレス LAN のセットアップ

Cisco Unified CM の管理 で、ワイヤレス Cisco Desktop Collaboration Experience の「Wi-Fi」というパラメータを有効にする必要があります。 Cisco Unified Communications Manager Administration にある次のいずれかの場所で、このパラメータを有効にすることができます。

- 特定の電話機でワイヤレス LAN を有効にするには、特定の電話機の [プロダクト固有の設定（Product Specific Configuration Layout）] セクション（[デバイス（Device）] > [電話機（Phone）]）で Wi-Fi パラメータの有効設定を選択し、[共通設定の上書き（Override Common Settings）] チェックボックスをオンにしておきます。
- 電話機のグループに対してワイヤレス LAN を有効にするには、[共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウ（[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]）で Wi-Fi パラメータの有効設定を選択し、[共通設定の上書き（Override Common Settings）] チェックボックスをオンにした後、その共通の電話プロファイルを使用して（[デバイス（Device）] > [電話機（Phone）]）電話機を関連付けます。
- ネットワーク内にあるすべての WLAN 対応電話機に対してワイヤレス LAN を有効にするには、[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ（[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]）で Wi-Fi パラメータの有効設定を選択し、[共通設定の上書き（Override Common Settings）] チェックボックスをオンにします。

（注） Cisco Unified Communications Manager Administration の [電話の設定（Phone Configuration）] ウィンドウ（[デバイス（Device）] > [電話機（Phone）]）で、MAC アドレスの設定時に、有線の MAC アドレスを使用します。 Cisco Unified Communications Manager の登録にはワイヤレス MAC アドレスは使用しません。

Cisco Unified IP Phone のワイヤレス LAN のセットアップ

電話機が WLAN に接続できるようになる前に、適切な WLAN 設定で電話機のネットワーク プロファイルを設定する必要があります。 電話機の [ネットワークのセットアップ（Network Setup）] メニューを使用して [WLAN のセットアップ（WLAN Setup）] サブメニューにアクセスし、WLAN 設定をセットアップすることができます。

関連トピック

ワイヤレス LAN の設定, （27 ページ）