無線ネットワークの概要

無線通信の導入により、モバイル Wireless IP Phone は、社内の無線ローカル エリア ネットワーク（WLAN）内で音声通信を可能にします。無線音声通信を提供するために、Cisco Unified Wireless IP Phone 7920 は、無線アクセス ポイントと、Cisco Unified CallManager をはじめとする主要な Cisco IP テレフォニー コンポーネントを使用し、これらと相互対話します。

この章では、Cisco Unified Wireless IP Phone 7920 と WLAN 環境における Voice-over-IP（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。

無線 LAN について

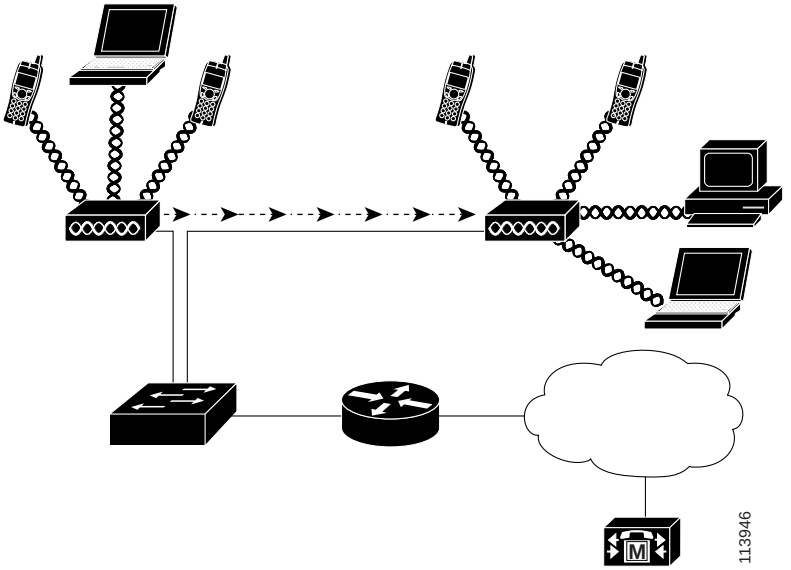
この項では、WLAN に関する次のトピックについて取り上げます。

従来の LAN では、電話機とコンピュータはケーブルを使用して導線上でメッセージとデータ パケットを伝送します。無線 LAN では、無線波を使用してメッセージとデータ パケットを伝送します。

WLAN には、無線信号を送受信するアクセス ポイント デバイスが必要です。Cisco Aironet アクセス ポイント（1200、1100、および 350 シリーズ モデルなど）は、WLAN 上の音声をサポートしています。図 2-1 は、ラップトップ コンピュータの無線データと Cisco Unified Wireless IP Phone 7920 モデルの Wireless IP テレフォニー（WIPT）を組み込んだ一般的な WLAN トポロジを示しています。

無線デバイスは、電源を入れるとすぐにアクセス ポイントを検索し、アクセス ポイントに関連付けられます。ユーザが社内の WLAN 環境内のあるロケーションから別のロケーションに移動すると、無線デバイスは 1 つのアクセス ポイントの範囲外に出て、別のアクセス ポイントの範囲内に移動します。アクセス ポイントでは、有線ネットワークを使用してデータと音声パケットをスイッチおよびルータに伝送します。音声パケットは Cisco Unified CallManager サーバに送信され、コール処理とルーティングが行われます。

図 2-1　Cisco Unified Wireless IP Phone 7920 を使用した無線 LAN



無線 LAN 通信の 802.11 規格

無線 LAN は、すべての Ethernet ベースの無線トラフィックの基準となる Institute of Electrical and Electronics Engineers（IEEE）802.11 規格に従う必要があります。802.11b 規格は、無線 LAN 通信の最も有力な規格で、一般に WiFi と呼ばれます。802.11b 規格では、データの送信と受信の両方で 1、2、5.5、および 11 Mbps の速度を提供する 2.4 GHz の無線周波数（RF）が指定されています。

2.4 GHz の RF 範囲は、ライセンスが不要なオープン周波数範囲です。この帯域では、コードレス電話や電子レンジなどの多くの機器が使用されるため、無線通信は干渉やノイズの影響を受けやすくなります。干渉によって信号が破壊されることはありませんが、伝送速度が低下し、11 Mbps の信号速度が常に 1 Mbps まで低下する可能性もあります。さらに、RF 干渉によって、無線ネットワーク上の音声品質が低下する可能性もあります。

このような干渉の防止に役立てるために、信号を周波数範囲または帯域幅に分散する Direct-sequence Spread Spectrum（DSSS; ダイレクト シーケンス スペクトラム拡散方式）のテクノロジーが開発されました。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。各デバイスは特殊なコードを持ち、これを使用してそれぞれのデータ パケットを識別し、その他のデータ パケットを無視します。シスコの無線製品は、WLAN 上で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。

無線ネットワークへの接続

無線ネットワークの重要なコンポーネントは、ネットワークに無線リンクまたは「ホット スポット」を提供するアクセス ポイントです。音声通信をサポートするアクセス ポイントでは、Cisco IOS バージョン 12.3(8)JA 以降が稼働することを必須としています。Cisco IOS には、音声トラフィックの管理機能を提供します。AP の詳細については、P.2-24 の「無線ネットワークとアクセス ポイントの設定」を参照してください。

各アクセス ポイントは、LAN 上に構成された Cisco Catalyst 4000 などのネットワーク レイヤ スイッチにケーブル接続されています。このスイッチにより、Wireless IP テレフォニー（WIPT）をサポートするゲートウェイや Cisco Unified CallManager サーバにアクセスできます。

アクセス ポイントは、2.4 GHz 周波数帯のチャンネルを使用して RF 信号を送受信します。2.4 GHz 周波数帯で無線通信に使用できるチャネル数は、規制区域によって決まっています。Cisco Aironet アクセス ポイントは、北米では 11 、欧州（ETSI）では 13 、日本では 14 の通信チャネルをサポートします。1 つのアクセス ポイントは、使用可能なチャネル範囲内の特定のチャネルでブロードキャストします。安定した無線環境を提供し、チャネルの干渉を減少させるために、各アクセス ポイントに重複しないチャネルを指定する必要があります。推奨されるチャネルは北米で 1、6、および 11 です。

アクセス ポイントには伝送範囲またはカバレッジ区域があり、その範囲は AP のアンテナのタイプと送信電力によって異なります。アクセス ポイントのカバレッジ範囲は、有効な等方性放射電力（EIRP）の出力、1、5、20、50、および 100mW に対して、500 ～ 1000 フィート（約 152 ～ 305 メートル）の間で変化します。有効なカバレッジを提供するために、アクセス ポイントでは範囲を約 20% 重複して、電話ユーザが 1 つのアクセス ポイントから別のアクセス ポイントに移動したときに接続が途切れることのないようにする必要があります。

無線ネットワーク デバイスでは、Service Set Identifier（SSID; サービス セット ID）が使用されます。SSID を使用すると、一定のアクセス ポイントのセットに関連付けることのできるユーザ デバイスのセットをグループ化できます。特定のアクセス ポイントを使用することのできる各無線デバイスには、そのアクセス ポイントと同じ SSID が設定されます。アクセス ポイントの設定の詳細については、『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。

音声通信の保護

範囲内にあるすべての WLAN デバイスは他の無線 LAN トラフィックをすべて受信できるため、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 Unified Wireless IP Phone 7920 と Cisco Aironet アクセス ポイントは包括的な Cisco SAFE セキュリティ アーキテクチャでサポートされています。

音声通信を保護するために、無線ネットワークでは認証方式と暗号化方式を使用します。Wired Equivalent Privacy（WEP）は、無線セキュリティに導入された最初の方式ですが、障害の発生しやすい方式です。セキュリティの問題と WEP の脆弱性を解決するために、WiFi Alliance は Wireless Protected Access（WPA; 無線保護アクセス）を定義しました。

Wi-Fi Protected Access は、規格準拠の相互運用可能なセキュリティ拡張です。このセキュリティ拡張により、現在および将来の無線 LAN システムに関するデータ保護およびアクセス制御のレベルが向上します。WPA は現在策定中の IEEE 802.11i 規格から派生したもので、この規格との上位互換性があります。WPA は、データ保護に Temporal Key Integrity Protocol（TKIP）を使用し、認証キー管理に 802.1X を使用します。

強化された暗号化アルゴリズムと認証、および迅速なキー更新により、WPA には WEP と比べて大幅に改良されたセキュリティが備わっています。中央集中型の Remote Authentication Dial-in User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）サーバを使用することにより、アクセス ポイントまたはネットワークのいずれかで、Wireless IP Phone などの無線クライアントを認証できます。

Cisco Wireless IP テレフォニー ソリューションは、これに加えて次のセキュリティ領域への対応を可能にします。

- Wired Equivalent Privacy（WEP）、Wireless Protected Access（WPA）、拡張認証プロトコル（EAP）、および Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）による暗号化と認証を使用して、不正ログインおよび障害のある通信を防止する無線ネットワーク セキュリティ。
- Cisco Unified Wireless IP Phone 7920 電話ロック パスワードを含む、ディレクトリおよびデータベースのパスワード保護。

関連項目

- Cisco Unified Wireless IP Phone で使用されるネットワーキング プロトコル（P.2-7）
- 無線ネットワークでのセキュリティの仕組み（P.2-16）

VoIP 無線ネットワークのコンポーネント

Cisco Unified Wireless IP Phone 7920 は、コールを正常に発信および受信するために、無線ローカル エリア ネットワーク（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、ネットワークのコンポーネントの概要について説明します。

Cisco Unified Wireless IP Phone で使用されるネットワーキング プロトコル

Cisco Unified IP Phone は、複数の業界規格と音声通信対応の Cisco ネットワーキング プロトコルをサポートします。表 2-1 は、Cisco Unified Wireless IP Phone 7920 がサポートするネットワーキング プロトコルの概要を説明したものです。

表 2-1　Cisco Unified Wireless IP Phone 7920 でサポートされるネットワーキング プロトコル

ネットワーキング プロトコル	目的	使用上の注意
Cisco Centralized Key Management（CCKM）	無線ネットワークでの高速認証に使用されるキー生成プロトコル。	Cisco Unified Wireless IP Phone 7920 は、アクセス ポイント間における高速でセキュアなローミングのために CCKM を使用します。

表 2-1　Cisco Unified Wireless IP Phone 7920 でサポートされるネットワーキング プロトコル（続き）

ネットワーキング プロトコル	目的	使用上の注意
Cisco Discovery Protocol（CDP; シスコ検出プロトコル）	すべてのシスコ製機器で実行されるデバイス検出プロトコル。 CDP を使用すると、デバイスは他のデバイスに存在を通知して、ネットワーク内の他のデバイスについての情報を受信することができます。	Cisco Unified Wireless IP Phon は、CDP を使用して、補助 VLAN ID、ポートごとの電力管理の詳細、サービス品質（QoS）の設定情報などの情報を Cisco Catalyst スイッチとの間で通信します。
Extensible Authentication Protocol（EAP; 拡張認証プロトコル）	クライアント（電話機）と RADIUS サーバ間の、独自のパスワードベース相互認証方式。	Cisco Unified Wireless IP Phone 7920 は、無線ネットワークでの認証に EAP を使用します。
Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）	クライアント（電話機）と EAP-FAST RADIUS サーバの間の Protected Access Credential（PAC）認証方式。	Cisco Unified Wireless IP Phone 7920 は、無線ネットワークでの認証に EAP-FAST を使用します。
Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）	ネットワーク デバイスに IP アドレスを動的に割り当てます。 DHCP を使用すると、IP Phone がネットワークに接続し、使用できるようになります。管理者が IP アドレスを割り当てたり、追加のネットワーク パラメータを設定したりする必要はありません。	DHCP はデフォルトで有効になっています。無効になっている場合は、各電話機で、IP アドレス、サブネット マスク、ゲートウェイ、および TFTP サーバを手動でローカルに設定する必要があります。 DHCP カスタム オプション 150 を使用します。この方式では、TFTP サーバの IP アドレスをオプション値として設定します。　サポートされるその他の DHCP 設定については、『*Cisco Unified CallManager システム ガイド*』を参照してください。

表 2-1　Cisco Unified Wireless IP Phone 7920 でサポートされるネットワーキング プロトコル（続き）

ネットワーキング プロトコル	目的	使用上の注意
インターネット プロトコル（IP）	ネットワーク全体において、パケットのアドレス指定を行って送信するメッセージング プロトコル。	IP を使用して通信するには、ネットワーク デバイスに、IP アドレス、サブネット、およびゲートウェイが割り当てられている必要があります。 Cisco Unified IP Phone で DHCP を使用している場合、IP アドレス、サブネット、およびゲートウェイの ID は自動的に割り当てられます。DHCP を使用していない場合は、各電話機にこれらのプロパティを手動でローカルに割り当てる必要があります。
Light Extensible Authentication Protocol（LEAP）	クライアント（電話機）と RADIUS サーバ間の、独自のパスワードベース相互認証方式。	Cisco Unified Wireless IP Phone 7920 は、無線ネットワークでの認証に LEAP を使用します。
Real-Time Control Protocol（RTCP）	RTP プロトコルと使用し、データ ネットワーク上で双方向の音声やビデオなどのリアルタイム データを転送します。	Cisco Unified IP Phone では、RTCP プロトコルを使用して、データの配信状況および最低限の制御と識別機能をモニタリングします。
Real-Time Transport（RTP; リアルタイム転送）	データ ネットワークで双方向の音声およびビデオなどのリアルタイム データを転送するための規格。	Cisco Unified IP Phone は、RTP プロトコルを使用して、他の電話機およびゲートウェイとの間でリアルタイム音声トラフィックを送受信します。
Skinny Client Control Protocol（SCCP）	シスコ独自のメッセージを使用して、IP デバイスと Cisco Unified CallManager との間で通信します。	Cisco Unified IP Phone では、VoIP コールシグナリングおよびメッセージ受信インジケータ（MWI）などの拡張機能に SCCP プロトコルを使用します。
Temporal Key Integrity Protocol（TKIP）と Message Integrity Check（MIC; メッセージ完全性チェック）の連携	無線 LAN を介して送信される暗号化データの暗号化およびデータ整合性のプロトコル。	Cisco Unified Wireless IP Phone 7920 では、TKIP/MIC アルゴリズムを使用して、音声通信の整合性を保護および持続します。

表 2-1　Cisco Unified Wireless IP Phone 7920 でサポートされるネットワーキング プロトコル（続き）

ネットワーキング プロトコル	目的	使用上の注意
Transmission Control Protocol（TCP; 伝送制御プロトコル）	コネクション型の転送プロトコル。	Cisco Unified IP Phone では、TCP を使用して Cisco Unified CallManager に接続し、XML サービスにアクセスします。
Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）	ネットワークでのファイル転送方式。 Cisco Unified IP Phone では、TFTP を使用して、電話機のタイプに固有の設定ファイルを取得できます。	ネットワーク内には、DHCP サーバから自動的に識別される TFTP サーバが必要です。ネットワーク内で複数の TFTP サーバが稼働している場合には、各電話機に TFTP サーバを手動で割り当てる必要があります。
User Datagram Protocol（UDP; ユーザ データグラム プロトコル）	データ パケットを配信するためのコネクションレス型のメッセージング プロトコル。	Cisco Unified IP Phone は、UDP メッセージを受信して処理します。RTP 音声トラフィックは UDP で実行されます。
Wi-Fi（802.11b）	無線による Ethernet トラフィックの伝送方法を定義したオープンな規格で、一般に Wi-Fi と呼ばれます。この規格では、無線 LAN 通信の無線周波数（RF）とデータ速度を定義しています。	Cisco Unified Wireless IP Phone 7920 は、2.4 ～ 2.497 GHz の RF で、1、2、5.5、および 11Mbps のデータ レートが動的に変化する 802.11b 標準を使用しています。
Wired Equivalent Privacy（WEP）	電話機とアクセス ポイントに格納されている暗号化キーを使用するデータの暗号化のための無線セキュリティ プロトコル。	Cisco Unified Wireless IP Phone 7920 は、ネットワークのセキュリティ設定に応じて、静的 WEP キーまたは動的 WEP キーのいずれかを使用できます。
Wireless Protected Access（WPA; 無線保護アクセス）	強化された認証、暗号化キー管理と必須暗号化、およびメッセージ整合性方式を提供します。	Cisco Unified Wireless IP Phone 7920 は、TKIP および MIC（メッセージ完全性チェック）を使用する暗号化を含め、WPA と WPA 事前共有キー認証の両方をサポートします。

関連項目

- 電話機の起動プロセスについて（P.2-28）
- VoIP 無線ネットワークのコンポーネント（P.2-7）

- DHCP 設定の変更（P.5-5）
- TFTP オプションの設定（P.5-10）

Cisco Aironet アクセス ポイントとの相互対話

無線音声デバイスは、無線データ デバイスと同じアクセス ポイントを使用します。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。Web ページを検索中のパケット損失によりページの表示が遅くなり、エンド ユーザに影響を与える場合があります。ただし、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場合があります。

無線音声のユーザはモバイルで、コールに接続しながら構内やフロア間を移動できます。これに対して、データ ユーザは PC を別の場所に移動する場合がありますが、その場合は新しい場所で接続し直します。音声セッション継続の管理中にローミングが可能であることは、無線音声の 1 つの利点です。そのため、RF カバレッジには、データでは通常カバーされない、吹き抜け、エレベータ、会議室の外にある人気のない場所、通路などの区域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、無線音声に適した値を決定するサイト調査を実施する必要があります。この調査結果から、音声対応 WLAN の設計とレイアウトのための情報が得られます。たとえば、電力レベル、チャネルの割り当て、およびアクセス ポイントの位置などです。サイト調査の詳細については、『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。

無線音声を導入し、使用できるようにした後は、引き続き設置後にサイト調査を実施して、アクセス ポイントの場所とその構成が無線音声ユーザのニーズを継続して満たしているかどうかを検証します。新規ユーザ グループの追加、機器の追加の設置、または大量のインベントリのスタックを行うと、無線環境が変わります。このような場合には、アクセス ポイントのカバレッジが、それまで同様に最適な音声通信にとって十分であるかを検証する必要があります。詳細については、P.6-9 の「サイト調査の確認の実行」を参照してください。

アクセス ポイントへの関連付け

Cisco Unified Wireless IP Phone 7920 は、起動時に無線を使用して、認識できる Service Set Identifiers（SSID; サービス セット ID）と暗号化タイプを持つアクセス ポイントをスキャンします。電話機は適格なアクセス ポイント ターゲットのリストを構築および保守し、次の 2 つの変数を使用して、関連付けに最適なアクセス ポイントを決定します。

- Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）: 電話機は、この値を使用して、RF カバレッジ区域内で使用可能なアクセス ポイントの信号強度を判別します。電話機は最も高い RSSI 値を持つアクセス ポイントに関連付けしようとします。
- QoS Basis Service Set（QBSS）: アクセス ポイントでは、このビーコン情報要素（IE）を使用して、アクセス ポイントのチャネル利用率を Cisco Unified Wireless IP Phone に送信します。電話機は QBSS 値を使用して、そのアクセス ポイントでそれ以上のトラフィックを効果的に処理できる状況かどうかを判別します。

Cisco Unified Wireless IP Phone は、最高の RSSI 値と最低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アクセス ポイントに関連付けられます。

関連項目

- 無線ネットワークでのローミング（P.2-12）
- 音声通信の保護（P.2-5）
- 無線ネットワークとアクセス ポイントの設定（P.2-24）

無線ネットワークでのローミング

Cisco Unified Wireless IP Phone ユーザは、電話機で会話しながら 1 つの場所から別の場所に移動できます。広範囲のカバレッジを持つ携帯電話とは異なり、Cisco Unified Wireless IP Phone のカバレッジ区域は狭いため、電話ユーザはアクセス ポイント間を頻繁に移動する必要があります。Wireless IP Phone を使用したローミングの制限の一部を理解するために、次の例で WLAN におけるローミングについて説明します。

- コール前のローミング：Cisco Unified Wireless IP Phone 7920 のユーザがオフィスで電話機の電源を入れると、電話機が近くのアクセス ポイントに関連付けられます。ユーザは、建物を離れて別の建物に移動し、そこでコールを発信します。電話機は、新しい場所からコールを発信するために、別のアクセス ポイントに関連付けられます。関連付けられたアクセス ポイントが同じレイヤ 2 VLAN 内にある場合は、電話機の IP アドレスは変わりません。ただし、ローミングしている電話機がレイヤ 3 境界を越え、DHCP が有効である場合は、電話機は自分自身がそれまでと同じサブネット内に存在しないと認識します。電話機は、ネットワークに接続してコールを発信する前に、新しい IP アドレスを要求します。

（注） 現在のネットワークを離れ、同じ ネットワークに戻る場合は、電話機がネットワークに再接続されるのを待つか、［オウトウ / ソウシン］キーを押してすぐに再接続します。

- コール中のローミング：Cisco Unified Wireless IP Phone 7920 ユーザはコール中で、1 つの建物から別の建物に移動します。電話機が別のアクセス ポイントの範囲内に移動するとローミング イベントが発生し、電話機は認証され新しいアクセス ポイントに関連付けられます。現在のアクセス ポイントは、ユーザが介入することなく、継続的な音声接続の管理中に新しいアクセス ポイントにコールを渡します。アクセス ポイントが同じレイヤ 2 サブネットに属している限り、Cisco Unified Wireless IP Phone は同じ IP アドレスを維持したままコールが続きます。Cisco Unified Wireless IP Phone は、アクセス ポイント間をローミングするときに、新しいアクセス ポイントそれぞれで再認証されます。認証の詳細については、P.2-16 の「無線ネットワークでのセキュリティの仕組み」を参照してください。

  Cisco Unified Wireless IP Phone ユーザが、IP サブネット A をカバーするアクセス ポイントから IP サブネット B をカバーするアクセス ポイントに移動すると、電話機には移動後のサブネットで有効な IP アドレスまたはゲートウェイがなくなり、コールは接続解除されます。

  Cisco Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール（WLSM）のリリースに伴い、Cisco Unified Wireless IP Phone 7920 は現在、レイヤ 3 のローミングをサポートします。Cisco WLSM の詳細については、次の URL で入手できる製品マニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/wlsm_1_1/index.htm

- 高速セキュア ローミング：Cisco Centralized Key Management（CCKM）は、関連付けし直す間に遅延することなく、認証されたクライアント デバイスを 1 つのアクセス ポイントから別のアクセス ポイントに安全にローミングできるようにします。CCKM プロトコルのサポートにより、Cisco Unified Wireless IP Phone 7920 では、1 つのアクセス ポイントから別のアクセス ポイントへの引き渡しの交渉が容易になります。ローミング プロセス中、電話機は近くのアクセス ポイントをスキャンして、最良の状態でサービスを提供できるアクセス ポイントを判別し、再度新しいアクセス ポイントと関連付けします。WPA や EAP などのより強力な認証方式を実装している場合は、交換する情報量が増えてローミング時の遅延の原因となります。CCKM の詳細については、次の URL で入手できる『*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

  この問題を解決するため、CCKM（Cisco Centralized Key Management）プロトコルでは、無線ドメイン サーバ（WDS）上でセッション クレデンシャルのキャッシュを提供します。電話機が 1 つのアクセス ポイントから次のアクセス ポイントにローミングするたびに、使用するアクセス ポイントに対して WDS に格納されているマスター キーを提供することにより、CCKM は交換するメッセージ数をローミング中に圧縮します。再度の関連付けによる交換は 2 つのメッセージに削減するため、ローミング時間も短くなります。

関連項目

- 無線ネットワークでの音声品質（P.2-14）
- Cisco Aironet アクセス ポイントとの相互対話（P.2-11）
- 無線ネットワークとアクセス ポイントの設定（P.2-24）

無線ネットワークでの音声品質

無線 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、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影響を与えることはありませんが、音声コールには重大な影響を及ぼします。音声トラフィックが、遅延やジッタの少ない、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、サービス品質（QoS）を使用して、音声とデータに個別の仮想 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。WLAN での音声接続をサポートするネットワーク スイッチとアクセス ポイントに、次の VLAN を構成する必要があります。

- 音声 VLAN：Wireless IP Phone との間で送受信される音声トラフィック
- ネイティブ VLAN：無線 PC 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）

（注） ネイティブ VLAN は VLAN 1 にしないでください。VLAN 1 は通常、すべてのネットワーク デバイスのデフォルト ネイティブ VLAN になっています。

音声 VLAN とデータ VLAN には個別の SSID を割り当てます。WLAN では、別の管理 VLAN を構成することもできますが、SSID を管理 VLAN に関連付けないようにしてください。

電話機を音声 VLAN に分離し、音声パケットにより高い CoS を割り当てることで、音声トラフィックがデータ トラフィックよりも優先度の高い処理を確実に受けるようにできます。結果として、遅延や損失パケットが少ない状態でトラフィックを管理できます。

詳細については、『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guide_book09186a00802a029a.html

関連項目

- 無線ネットワークでのセキュリティの仕組み（P.2-16）
- Cisco Unified CallManager との相互対話（P.2-21）
- 無線ネットワークとアクセス ポイントの設定（P.2-24）

無線ネットワークでのセキュリティの仕組み

無線デバイスがネットワーク上で通信するには、認証方式を使用してアクセス ポイントまたはネットワークの認証を受ける必要があります。Cisco Unified Wireless IP Phone 7920 は、WLAN において次の認証方式を使用できます。

- オープン認証：オープン　システムでは、任意の無線デバイスが認証を要求できます。要求を受けたアクセス ポイントは、任意のリクエスタまたはユーザのリスト上のリクエスタだけに認証を与える場合があります。無線デバイスとアクセス ポイント間の通信は暗号化されない可能性もあります。暗号化される場合は、デバイスは WEP キーを使用してセキュリティを提供できます。WEP を使用するデバイスは、WEP を使用しているアクセス ポイントでの認証のみを試みます。
- 共有キー認証：共有キー認証では、アクセス ポイントは、アクセス ポイント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 テキストの文字列を送信します。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、アクセス ポイントに返します。チャンレンジ テキストが正しく暗号化されている場合、アクセス ポイントは要求側のデバイスに認証を許可します。WEP キーがアクセス ポイント上の WEP キーと一致する場合に限り、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監視できるため、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。暗号化されているチャレンジ テキストと暗号化されていないチャレンジ テキストを比較することにより、侵入者は WEP キーを計算できます。
- WPA 事前共有キー（PSK）認証：アクセス ポイントと電話機は、同じ認証キーで設定されます。事前共有キー（またはパスワード フレーズ）は、各電話機とアクセス ポイントの間で交換される一意のペアワイズ キーの作成に使用されます。パスワード フレーズは、64 文字の 16 進数の文字列、または 8 ～ 63 文字の ASCII パスワードで設定できます。事前共有キーのパスワードは電話機に保存されるため、電話機を紛失したり盗まれたりすると、障害が発生する可能性があります。
- EAP　認証：セキュリティを最大限にするには、クライアント　デバイスは、Cisco Access Control Server（ACS）などの Remote Authentication Dial-in User Service（RADIUS）サーバを使用して、ネットワークで認証を行うことができます。

EAP は、EAP 準拠 RADIUS サーバを必要とする専用の認証プロトコルです。EAP を使用すると、無線デバイスは、中央集中型の RADIUS サーバのユーザ データベースを介してユーザ名とパスワードを使用することにより、相互に認証し合うことができます。

Cisco Unified Wireless IP Phone が 1 つのアクセス ポイントから別のアクセス ポイントにローミングする場合は、ローミング先のアクセス ポイントでも EAP 認証が要求されます。ボイス ストリームは、中央集中型の RADIUS サーバを介して次のアクセス ポイントで EAP 認証が完了するまでは流れません。

アクセス ポイントと RADIUS サーバ間の遅延時間を減らすため、RADIUS サーバの配置を慎重に検討してください。ローカル RADIUS サーバでのローミング時の遅延は、リモート RADIUS サーバの場合より短くなります。小規模なリモート オフィスでは、Cisco アクセス ポイントで RADIUS サーバを使用し、50 ユーザまでを認証できます。

EAP-FAST は、Transport Level Security（TLS）トンネル内の EAP トランザクションを暗号化するクライアント サーバのセキュリティ アーキテクチャです。トンネルは、Protected Access Credential（PAC）に基づいて確立されます。この認証方式には、EAP 認証と同じ制限事項は適用されません。

TLS トンネルは、EAP-FAST が無線ネットワークの認証方式として使用されている場合に使用されます。TLS トンネルでは、クライアントと RADIUS サーバ間の認証で Protected Access Credential（PAC）を使用します。RADIUS サーバはクライアントに権限 ID（AID）を送信し、受け取ったクライアントは適切な PAC を選択します。PAC-Opaque が RADIUS サーバに返され、サーバはマスター キーを使用して PAC-Opaque を暗号化します。これで両方のエンド ポイントが PAC キーを持つことになり、TLS トンネルが作成されます。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、最初に 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、RADIUS サーバとの認証でおよそ 20 秒間のダウンタイムが発生します。
セキュリティ ポリシーの要件に応じ、Cisco Centralized Key Management（CCKM）を使用して、無線ドメイン サーバ（WDS）レベルで認証を実行できます。これにより、新しい PAC を取得しなくてもローミングが可能になります。ただし、電話機が CCKM なしで Cisco ACS と直接通信する場合は、新しい PAC の取得が必要になり、20 秒間のダウンタイムが発生します。

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。

- WiFi Protected Access（WPA）：RADIUS サーバにある情報を使用して、認証に一意のペアワイズ キーを生成します。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 はアクセス ポイントおよび電話機に格納された WPA 事前共有キーより高いセキュリティを提供します。
- Cisco Centralized Key Management（CCKM）：RADIUS サーバと無線ドメイン サーバ（WDS）にある情報を使用して、キーを管理し認証します。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 および CCKM では、暗号化キーは電話機に入力されませんが、アクセス ポイント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。

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 Unified Wireless IP Phone 7920 では、暗号化方式として Wired Equivalent Privacy（WEP）と Temporal Key Integrity Protocol（TKIP）をサポートします。暗号化にいずれかのしくみを使用すると、アクセス ポイントと Cisco Unified Wireless IP Phone の間で、シグナリング（SCCP）パケットと音声（RTP）パケットの両方が暗号化されます。

- WEP：無線ネットワークで 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、アクセス ポイントで認証が行われます。正常に接続させるには、電話機に設定された WEP キーとアクセス ポイントで設定された WEP キーが一致する必要があります。Cisco Unified Wireless IP Phone 7920 は、40 ビット暗号化または 128 ビット暗号化を使用し、電話機およびアクセス ポイントで静的なままの WEP キーをサポートします。

  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アクセス ポイントに渡します。そのため、次の WEP キーを各認証で変更できます。
- Temporal Key Integrity Protocol（TKIP）：WPA および CCKM は、WEP に対するいくつかの改良点を持つ 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。

（注）　WPA および WPA 事前共有キーは TKIP 暗号化でのみ使用できるのに対し、CCKM は TKIP または WEP 暗号化のどちらでも使用できます。

（注）　Cisco Unified Wireless IP Phone 7920 は、CMIC による Cisco Key Integrity Protocol（CKIP）をサポートしません。

認証方式と暗号化方式の選択

認証方式と暗号化方式は、無線 LAN 内で設定されます。VLAN は、ネットワーク内およびアクセス ポイント上で設定され、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。無線クライアント デバイスが正常に認証されるには、アクセス ポイントおよび Cisco Unified Wireless IP Phone などのクライアント デバイスに、認証および暗号化方式の要件を満たす同じ SSID を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、オプションで暗号化に静的 WEP を使用したり、強化されたセキュリティを使用したりすることができます。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 Unified Wireless IP Phone 7920 に Authenticated Key Management（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 を持つアクセス ポイントで設定できます。Cisco Unified Wireless IP Phone 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アクセス ポイントを選択します。AKM では、WPA 事前共有キー、WPA、または CCKM を使用して認証できます。

電話機で AKM を設定すると、WPA 事前共有キーの使用時にアクセス ポイントは暗号化キーを提供したり、WEP の使用時に電話機で暗号化キーを設定したりすることができます。

（注）　WPA 事前共有キーを使用する場合は、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。

AKM を使用する場合の暗号化オプションには、WPA 事前共有キー、WPA 認証での TKIP、CCKM 認証での TKIP や WEP などがあります。

認証方式と暗号化方式の詳細、およびそれらの設定方法については、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/en/US/products/hw/wireless/ps4570/products_installation_and_configuration_guides_list.html

表 2-2 に、Cisco Unified Wireless IP Phone 7920 でサポートされる Cisco Aironet アクセス ポイント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、クセス ポイントの設定に対応する電話機のネットワーク設定のオプションを示します。

表 2-2　認証方式と暗号化方式

アクセス ポイントの設定		Cisco Unified Wireless IP Phone 7920	
認証	**暗号化**	**認証**	**暗号化**
オープン	静的 WEP	オープン（オプション）	なしまたは静的 WEP
共有キー	静的 WEP（必須）	共有キー	静的 WEP（必須）
ネットワーク EAP	WEP	EAP	WEP（必須）
ネットワーク EAP	TKIP または WEP（CCKM では WDS が必要）	AKM と CCKM	TKIP または WEP
ネットワーク EAP	TKIP と WPA	AKM と WPA	TKIP
オープン	TKIP と WPA または WPA 事前共有キー	AKM と WPA 事前共有キー	TKIP

関連項目

- Cisco Unified CallManager との相互対話（P.2-21）
- VoIP 無線ネットワークのコンポーネント（P.2-7）
- 無線ネットワークとアクセス ポイントの設定（P.2-24）

Cisco Unified CallManager との相互対話

Cisco Unified CallManager は、Cisco Unified Wireless IP Phone 7920 のコールを処理および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 CallManager は、IP テレフォニー システム（電話機、アクセス ゲートウェイ）のコンポーネントやリソース（電話会議やルート プランなどの機能）を管理します。無線音声の導入には、Cisco Unified CallManager Release 3.3(3) SR1 以降を使用する必要があります。

Cisco Unified CallManager で電話機を認識させるには、電話機を Cisco Unified CallManager に登録し、データベース内で設定する必要があります。Cisco Unified CallManager での電話機の設定については、P.1-9 の「Cisco Unified CallManager での Cisco Unified IP Phones の設定」を参照してください。

Cisco Unified CallManager を構成して IP Phone 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 CallManager アドミニストレーション ガイド*』および『*Cisco Unified CallManager システム ガイド*』を参照してください。

関連項目

- Cisco Unified CallManager での Cisco Unified Wireless IP Phone の設定（P.7-2）
- 電話機の設定ファイルとプロファイル ファイル（P.2-21）

電話機の設定ファイルとプロファイル ファイル

電話機の設定ファイルは、Cisco Unified CallManager に接続するためのパラメータを定義し、TFTP サーバに保存されます。一般に、Cisco Unified CallManager Administration で電話機のリセットが必要な変更を行うと、電話機の設定ファイルも自動的に変更されます。

設定ファイルには、電話機の正しいイメージ ロードについての情報も含まれます。このイメージ ロードが現在電話機にロードされているイメージと異なる場合、電話機は TFTP サーバに接続して新しいイメージ ファイルを要求します。

電話機は最初に、設定ファイル SEP*xxxxxxxxxxxx*.cnf.xml を要求します。*xx* は、それぞれ、電話機の MAC アドレスの各整数を小文字 2 桁の 16 進数で表記したものです。このファイルが見つからない場合、電話機は設定ファイル XMLDefault.cnf.xml を要求します。

*.cnf.xml ファイルを取得すると、電話機はその電話機に固有のプロファイル ファイルを要求します。このプロファイル ファイルが見つからない場合、電話機は適切な共通プロファイル ファイルを要求します。

プロファイル ファイルのいずれかが見つかった場合も、見つからなかった場合も、電話機は起動プロセスを続行します。

関連項目

- 電話機の起動プロセスについて（P.2-28）

DHCP サーバとの相互対話

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）は、ネットワーク管理者が、ネットワーク内のインターネット プロトコル（IP）アドレスの割り当てを管理および自動化するための通信プロトコルです。ネットワークに IP デバイスを追加したときには、一意の IP アドレスを割り当てる必要があります。DHCP を使用しない場合は、各デバイスで IP アドレスを手動入力する必要があります。DHCP では、IP アドレスは動的に割り当てられ、デバイスで不要になった IP アドレスは再利用されます。

ネットワークで DHCP が有効な場合、Cisco Unified Wireless IP Phone 7920 は DHCP サーバの DHCP スコープの設定を使用して、電話プロビジョニング起動プロセスを実行します。DHCP サーバの設定値は、Cisco Unified CallManager ネットワーク内で設定する必要があります。

DHCP スコープには、次の設定があります。

- TFTP サーバ
- DNS サーバの IP アドレス（ホスト名を使用しない場合はオプション）
- サブネット マスク、IP アドレス、およびゲートウェイのプールおよび範囲

TFTP サーバの DHCP 設定の優先順位は、表 2-3 に示すとおり、Cisco Unified Wireless IP Phone 7920 に固有のものです。

表 2-3　DHCP 設定の優先順位

優先順位	DHCP の設定
第 1 位	DHCP オプション 150
第 2 位	DHCP オプション 66
第 3 位	SIADDR
第 4 位	ciscoCM1

DHCP が無効な場合、Cisco Unified Wireless IP Phone 7920 は、次のネットワーク設定を使用して電話プロビジョニング起動プロセスを実行します。これらの静的パラメータは、Cisco Unified Wireless IP Phone 7920 ごとに設定する必要があります。

- プライマリ TFTP サーバ IP
- プライマリ DNS サーバ IP
- セカンダリ DNS サーバ IP
- IP アドレス
- サブネット マスク IP
- プライマリ ゲートウェイ IP

無線ネットワークとアクセス ポイントの設定

ここでは、音声パフォーマンスの最適化に必要とされる主要なアクセス ポイント（AP）の設定オプションを示します。Cisco Aironet アクセス ポイントなどのアクセス ポイントを設置するときのすべての設定手順またはオプションを示すものではありません。アクセス ポイントの設定の詳細については、ご使用のモデルに対応した『*Cisco Aironet アクセス ポイント インストレーション コンフィギュレーション ガイド*』またはアクセス ポイントのマニュアルを参照してください。

無線音声 LAN を設定する場合は、アクセス ポイント を使用して Cisco IOS バージョン 12.3(8) JA 以降を実行してください。

（注） パフォーマンスを最適化するには、Cisco IOS バージョン 12.3(8) JA を使用します。

Cisco Unified Wireless IP Phone 7920 は、Cisco IOS を自律モードで実行可能な Cisco Aironet アクセス ポイント（AP）と、Lightweight Access Point Protocol（LWAPP）を使用してライトウェイト モードで動作し、無線 LAN コントローラを使用する AP をサポートします。表 2-4 に、サポートされる AP モデルと WLAN におけるそれぞれの動作モードを示します。」

表 2-4　サポートされるアクセス ポイントとモード

アクセス ポイント モデル	自律モード	ライトウェイト モード
Cisco Aironet 350 シリーズ AP	あり	なし
Cisco Aironet 1100 シリーズ AP	あり	なし
Cisco Aironet 1130 シリーズ AP	あり	なし
Cisco Aironet 1200 シリーズ AP	あり	あり
Cisco Aironet 1240 シリーズ AP	あり	あり
Cisco Aironet 1300 シリーズ AP	あり	なし
Cisco 1000 シリーズ Lightweight AP	なし	あり

サードパーティ ベンダー製の Wi-Fi 準拠 AP は、Cisco Unified Wireless IP Phone 7920 で機能しても、Dynamic Transmit Power Control（DTPC）、ARP キャッシング、LEAP/EAP-FAST、または QBSS などの主要な機能をサポートしない場合があります。

Cisco Aironet アクセス ポイントの設定

表 2-5 で、Cisco Aironet アクセス ポイントの多くの設定作業について説明し、参考資料を示します。

表 2-5　Cisco Aironet アクセス ポイントの設定作業

アクティビティ	説明	参考資料
Cisco IOS バージョンが推奨バージョンであることの確認	System Software の下で、Cisco IOS バージョン 12.3(8)JA 以降であることを確認します。	『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。 Cisco Aironet アクセス ポイントとの相互対話（P.2-11）
音声用 VLAN の設定	音声トラフィックを分離し QoS を有効にするには、アクセス ポイントとネットワーク　スイッチに独立した音声 VLAN が必要です。	『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。 無線ネットワークでの音声品質（P.2-14）
各 VLAN の Service Set Identifier（SSID; サービス セット ID）の設定	相互通信する無線デバイスのセットを識別子です。複数のアクセス ポイントが同じ SSID を使用して、無線電話機のグループをサポートできます。	『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。 Cisco Aironet アクセス ポイントとの相互対話（P.2-11）

表 2-5　Cisco Aironet アクセス ポイントの設定作業（続き）

アクティビティ	説明	参考資料
VLAN の QoS の設定	音声 VLAN の QoS ポリシーを作成し、より高い CoS を音声トラフィックに割り当てます。 Wireless IP Phone の QoS 要素を有効にして、チャネル利用率（QBSS）の情報を電話機に提供します。	『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。 無線ネットワークでの音声品質（P.2-14）
ARP キャッシングの有効化	このオプションを有効にすると、双方向オーディオが保証されます。デフォルトでは、アクセス ポイントの ARP キャッシングは無効です。	『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。
無線（802.11b）設定値の設定	Data Rate：特殊なデバイス要件がない限り、11 Mbps のみ使用可能です。 Client Transmit Power：サイト調査の後、適切な所要電力を決定し、特定の Client Transmit Power 設定値を設定します。Cisco Unified Wireless IP Phone 7920 では、アクセス ポイントと同じ設定を使用します。 **（注）** Max に設定すると、アクセス ポイントは Client Transmit Power 設定を通知しません。	『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。
音声 VLAN セキュリティの設定	音声 VLAN に対応する SSID に、次の認証オプションおよび暗号化オプションを使用します。 • オープン • 共有キー • EAP • AKM	『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。 認証方式と暗号化方式の選択（P.2-19）

Cisco 1000 シリーズ Lightweight（Airespace）アクセス ポイントの設定

Airespace アクセス ポイントを使用する場合は、EAP セッションのタイムアウトを、2 秒から最低でも 20 秒に伸ばす必要があります。

ステップ 1　Airespace コントローラへの SSH または Telnet。

ステップ 2　`config advanced eap request-timeout 20` と入力します。

ステップ 3　`save config` と入力します。

ステップ 4　`y` と入力して確定します。

関連項目

- ネットワーク要件（P.3-2）
- Cisco Unified CallManager での Cisco Unified IP Phones の設定（P.1-9）
- Cisco Unified Wireless IP Phone 7920 の設置（P.3-11）

電話機の起動プロセスについて

無線 VoIP ネットワークに接続すると、Cisco Unified Wireless IP Phone 7920 は、表 2-6 に示す標準の起動プロセスを順番に実行します。ネットワーク設定によっては、ご使用の Cisco Unified Wireless IP Phone で、表のすべての手順を実行しない場合もあります。

表 2-6　Cisco Unified IP Phone 起動プロセス

手順	説明	関連項目
1. 電話機の電源をオン	Cisco Unified Wireless IP Phone 7920 は、不揮発性フラッシュ メモリを搭載し、そのメモリにファームウェア イメージとユーザ定義のプリファレンスが格納されています。起動時にブートストラップ ローダが実行され、フラッシュ メモリに保存された電話イメージがロードされます。このイメージを使用して、電話機のソフトウェアとハードウェアが初期化されます。	Cisco Unified IP Phone のへの電源の供給（P.3-11） 起動と接続の問題の解決（P.10-2）
2. アクセス ポイントのスキャン	Cisco Unified Wireless IP Phone 7920 は、無線で RF カバレッジ区域をスキャンします。電話機は、そのネットワーク プロファイルをスキャンし、SSID と認証タイプが一致するアクセス ポイントを探索します。電話機は、RSSI が最も高くチャネル利用率（QBSS）が最も低い、ネットワーク プロファイルと一致するアクセス ポイントに関連付けられます。	Cisco Aironet アクセス ポイントとの相互対話（P.2-11） 起動と接続の問題の解決（P.10-2）

表 2-6　Cisco Unified IP Phone 起動プロセス（続き）

手順	説明	関連項目
3. アクセス ポイントでの認証	Cisco Unified Wireless IP Phone 7920 が認証プロセスを開始します。 • **オープン**に設定されている場合は、任意のデバイスがアクセス ポイントの認証を行うことができます。セキュリティを高めるために、オプションで静的 WEP 暗号化を使用できます。 • **共有キー**に設定されている場合、電話機は WEP キーを使用してチャレンジ テキストを暗号化します。ネットワーク アクセスが可能になる前に、チャレンジ テキストの暗号化に WEP キーが使用されたことをアクセス ポイントで検証する必要があります。 • **EAP** に設定されている場合は、ネットワーク アクセスが可能になる前に、RADIUS サーバによって EAP ユーザ名とパスワードが認証されます。 • **AKM** に設定されている場合、電話機は、次のキー管理オプションのいずれかが有効になっているアクセス ポイントを検索します。 – WPA または CCKM：電話機は RADIUS サーバで認証されます。 – WPA-PSK：電話機は、事前共有キーパスワードを使用して、アクセス ポイントで認証されます。	無線ネットワークでのセキュリティの仕組み（P.2-16）

表 2-6　Cisco Unified IP Phone 起動プロセス（続き）

手順	説明	関連項目
4. IP ネットワークの設定	Cisco Unified Wireless IP Phone が DHCP を使用して IP アドレスを取得する場合、電話機は DHCP サーバに照会して IP アドレスを取得します。ネットワークで DHCP を使用しない場合は、各電話機にローカルで固定 IP アドレスを割り当てる必要があります。 IP アドレスの割り当てに加え、DHCP サーバは Cisco Unified Wireless IP Phone を TFTP サーバに誘導します。電話機に静的に定義された IP アドレスがある場合は、TFTP サーバの IP アドレスを電話機でローカルに設定する必要があります。その後、電話機は TFTP サーバに直接接続します。	• DHCP 設定の変更（P.5-5） • スタティック設定の設定（P.5-7） • 起動と接続の問題の解決（P.10-2）
5. ロード ID のダウンロード	Cisco Unified Wireless IP Phone は、正しいファームウェアがインストールされていること、または新しいファームウェアがダウンロード可能かどうかを検査します。 Cisco Unified CallManager は、.cnf 形式または cnf.xml 形式の設定ファイルを使用して、デバイスにロード ID を通知します。.xml 形式の設定ファイルを使用するデバイスは、ロード ID を設定ファイル内で受け取ります。	• 電話機の設定ファイルとプロファイル ファイル（P.2-21）
6. 設定ファイルのダウンロード	TFTP サーバには、設定ファイルとプロファイル ファイルがあります。設定ファイルには、Cisco Unified CallManager に接続するためのパラメータと、電話機で実行するイメージ ロードについての情報が含まれます。プロファイル ファイルには、電話機とネットワークの設定について、さまざまなパラメータと値が含まれます。	• TFTP オプションの設定（P.5-10） • 電話機の設定ファイルとプロファイル ファイル（P.2-21） • 起動と接続の問題の解決（P.10-2）

表 2-6　Cisco Unified IP Phone 起動プロセス（続き）

手順	説明	関連項目
7. Cisco Unified CallManager への接続	設定ファイルは、Cisco Unified IP Phone と Cisco Unified CallManager が通信する方法を定義しています。TFTP サーバからファイルを取得した後、リストで電話機は優先順位が最も高い Cisco Unified CallManager に TCP 接続を試みます。	• Cisco Unified CallManager との相互対話（P.2-21） • 起動と接続の問題の解決（P.10-2）
8. Cisco Unified CallManager への登録	電話機がデータベースに手動で追加された場合、Cisco Unified CallManager はその電話機を識別して登録します。電話機がデータベースに手動で追加されたのではなく、Cisco Unified CallManager で自動登録が有効になっている場合、その電話機は、Cisco Unified CallManager データベースに自分自身を自動登録しようとします。	• Cisco Unified CallManager での Cisco Unified IP Phones の設定（P.1-9） • Cisco Unified CallManager へのユーザの追加（P.7-18）

関連項目

- Cisco Unified CallManager での Cisco Unified Wireless IP Phone の設定（P.7-2）
- 電話機の設定ファイルとプロファイル ファイル（P.2-21）