Cisco Unified IP Phone

Cisco Unified IP Phone 7906G および 7911G は、インターネット プロトコル（IP）ネットワークでの音声通信を実現します。 標準のデジタル ビジネス電話機とほぼ同様に機能し、電話コールの発受信に加えて、ミュート、保留、転送、スピード ダイヤルなどの機能を使用できます。 この電話機は、ネットワークに接続されているため、さらに生産性向上機能が用意されています。 これらの機能には、ネットワーク情報、XML アプリケーション、およびカスタム機能へのアクセスがあります。

Cisco Unified IP Phone は、他のネットワーク デバイスと同様に設定および管理する必要があります。 これらの電話機は、G.711a、G.711u、G.722、G.729a、G.729ab、および iLBC をエンコードし、G.711a、G.711u、G.722、および iLBC をデコードします。 これらの電話機は、圧縮解除されたワイドバンド（16 ビット、16 kHz）オーディオもサポートします。

注意 セル方式の電話、携帯電話、GSM 電話、または双方向ラジオを Cisco Unified IP Phone のすぐ近くで使用すると、相互干渉が発生することがあります。 詳細については、干渉デバイスの製造元の資料を参照してください。

この章は、次の項で構成されています。

- Cisco Unified IP Phone 7906G および 7911G，1 ページ
- ネットワーク プロトコル，3 ページ
- Cisco Unified IP Phone 7906 および 7911 のサポートされる機能，10 ページ
- Cisco Unified IP Phone のセキュリティ機能，12 ページ
- 電話機の消費電力，25 ページ
- Cisco Unified IP Phone の導入，26 ページ

Cisco Unified IP Phone 7906G および 7911G

Cisco Unified IP Phone 7906G および 7911G は、パーティションで区切られた作業スペース、教室、工場の作業場、倉庫、ロビーや、電話がユーザの一連の通信デバイスの補完となっているか、ほ

とんど使用されない場所で使用するために設計されたベーシックな IP Phone です。
Cisco Unified IP Phones 7906G および 7911G では次のことを実現します。

- 動的なソフトキー、アイコン、およびスクロール可能なディレクトリを使用したグラフ画面を提供することで、主要なビジネス機能セットへのアクセスを簡便化
- 1 つの電話番号で最大 6 つのコールをサポート
- シスコ インライン パワーまたは IEEE 802.3af Power over Ethernet の両方のインライン パワーをサポート
- 次を含む拡張セキュリティ機能をサポート
  - 製造元および現場でインストール可能な証明書
  - セキュアなメディアおよびシグナリング
  - 認証された設定
- 拡張コール機能に加えて、音声およびテキスト XML アプリケーションをサポート
- PC の接続、ロケーションごとに 1 つのケーブル プルの利点の維持（Cisco Unified IP Phone 7911G のみに適用）に使用する統合 10/100 メガビット イーサネット スイッチの搭載

ボタンとハードウェア

次の図と表を使用して、電話機でボタンとハードウェアを識別できます。

	項目	説明
1	電話スクリーン	電話メニューおよびコールアクティビティ（発信者 ID、通話時間、コールの状態など）を表示します。

	項目	説明
2	Cisco Unified IP Phone シリーズ	Cisco Unified IP Phone のモデル シリーズを示します。
3	ソフトキー ボタン	電話スクリーンに表示されているソフトキーのオプションをそれぞれアクティブにします。
4	ナビゲーション ボタン	メニュー項目のスクロールや項目の強調表示に使用します。 電話機がオンフックの場合、ユーザのスピードダイヤルを表示します。
5	アプリケーション メニュー ボタン	表示されるアプリケーション メニューにより、ボイスメッセージシステム、履歴とディレクトリ、各種設定、サービス、およびヘルプにアクセスできます。
6	保留ボタン	アクティブなコールの保留、保留にしたコールの復帰、アクティブなコールと保留にしたコールの切り替えを行います。
7	キーパッド	電話番号のダイヤル、文字の入力、およびメニュー項目の選択に使用します。
8	音量ボタン	ハンドセット、ヘッドセット、スピーカー、および呼出音の音量を制御します。
9	ライト ストリップを備えたハンドセット	ハンドセットのライトストリップは、着信コールまたは新しいボイス メッセージがあることを示します。
10	フットスタンド	デスクやテーブルの上で、電話機の角度を使いやすいように調整できます。

ネットワーク プロトコル

Cisco Unified IP Phones は、音声通信に必須の複数の業界標準ネットワーク プロトコルとシスコネットワーク プロトコルをサポートしています。 次の表に、Cisco Unified IP Phone 7906G および 7911G でサポートされているネットワーク プロトコルの概要を示します。

表 *1*：***Cisco Unified IP Phone*** でサポートされるネットワーク プロトコル

ネットワーク プロトコル	目的	使用方法
ブートストラッププロトコル（BootP）	BootP は、起動情報（自身の IP アドレスなど）を Cisco Unified IP Phone などのネットワーク デバイスが検出できるようにするものです。	BootP を使用して IP アドレスを Cisco Unified IP Phone に割り当てている場合、電話機のネットワーク構成の設定値として [BOOTP サーバ（BOOTP Server）] オプションが [はい（Yes）] と表示されます。
Cisco Discovery Protocol（CDP）	CDP は、シスコの製造するすべての装置で動作するデバイス検出プロトコルです。 デバイスは、CDP を使用して自身の存在をネットワーク内の他のデバイスにアドバタイズし、ネットワーク内の他のデバイスの情報を受信します。	Cisco Unified IP Phone では、補助 VLAN ID、ポートごとの電源管理の詳細情報、Quality of Service（QoS）設定情報などの情報を、CDP を使用して Cisco Catalyst スイッチとやり取りしています。
Cisco Peer-to-Peer Distribution Protocol（CPPDP）	CPPDP は、デバイスのピアツーピア階層を形成するために使用するシスコ独自のプロトコルです。 CPPDP は、ファームウェアや他のファイルをピア デバイスからネイバー デバイスにコピーするためにも使用します。	CPPDP は、ピア ファームウェア共有機能で使用されます。
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）	DHCP は、IP アドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。 DHCP を使用すると、IP Phone をネットワークに接続すれば、その電話機が機能するようになります。IP アドレスを手動で割り当てたり、ネットワーク パラメータを別途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。 無効にした場合は、個々の電話機がある場所で、IP アドレス、サブネット マスク、ゲートウェイ、および TFTP サーバを手動で設定する必要があります。 シスコでは、DHCP のカスタム オプション 150 を使用することを推奨します。 この方法では、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。 DHCP 設定の詳細については、『*Cisco Unified Communications Manager System Guide*』の「Dynamic Host Configuration Protocol」および「Cisco TFTP」の章を参照してください。

ネットワーク プロトコル	目的	使用方法
Hypertext Transfer Protocol（HTTP）	HTTP は、インターネットやワールドワイド ウェブ経由で情報やドキュメントを転送するための標準的な手段です。	Cisco Unified IP Phone では、XML サービスおよびトラブルシューティングに HTTP を使用します。
Hypertext Transfer Protocol Secure（HTTPS）	Hypertext Transfer Protocol Secure（HTTPS）は、サーバの暗号化とセキュアな ID を確保できるように、ハイパーテキスト転送プロトコルと SSL/TLS プロトコルを組み合わせたものです。	HTTP と HTTPS の両方をサポートする Web アプリケーションには 2 つの URL が設定されています。 HTTPS をサポートする Cisco Unified IP Phone は、HTTPS URL を選択します。
IEEE 802.1X	IEEE 802.1X 標準は、クライアントサーバアクセス コントロールと認証プロトコルを定義します。これにより、未承認のクライアントが一般にアクセス可能なポートから LAN に接続するのを制限します。 クライアントが認証されるまでは、802.1X アクセス コントロールによって、ポートを経由する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。 トラフィックは通常、認証が成功した後にポートを経由して移動できます。	Cisco Unified IP Phone は、EAP-FAST、EAP-TLS、および EAP-MD5 の認証方式をサポートすることで、IEEE 802.1X 標準を実装します。 802.1X 認証が有効になっている場合、PC ポートとボイス VLAN を無効にする必要があります。 詳細については、802.1X 認証, （22 ページ）を参照してください。

ネットワーク プロトコル	目的	使用方法
インターネットプロトコル（IP）	IP は、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。	IP を使用して通信するには、ネットワーク デバイスに対して、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。 IP アドレス、サブネット、およびゲートウェイの識別情報は、Dynamic Host Configuration Protocol（DHCP）を通じて Cisco Unified IP Phone を使用する場合は、自動的に割り当てられます。 DHCP を使用しない場合は、これらのプロパティを手動で割り当てる必要があります。 Cisco Unified IP Phone は、IPv4 アドレスと IPv6 アドレスの両方をサポートしています。 IP アドレッシング モード（IPv4 のみ、IPv6 のみ、および IPv4 と IPv6 の両方）を Cisco Unified CM の管理で設定します。 詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』の「Internet Protocol Version 6 (IPv6)」を参照してください。
Link Layer Discovery Protocol（LLDP）	LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコ デバイスとサードパーティ製デバイスでサポートされています。	Cisco Unified IP Phone は、PC ポートで LLDP をサポートします。

ネットワーク プロトコル	目的	使用方法
Link Layer Discovery Protocol-Media Endpoint Devices（LLDP-MED）	LLDP-MED は、音声製品用に開発された、LLDP 標準の拡張です。	Cisco Unified IP Phone は、次のような情報をやり取りするために、SW ポートで LLDP-MED をサポートします。 • ボイス VLAN の設定 • デバイスの検出 • 電源管理 • インベントリ管理 LLDP-MED サポートの詳細については、次の Web サイトで『*LLDP-MED and Cisco Discovery Protocol*』ホワイト ペーパーを参照してください。 http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
リアルタイム転送プロトコル（RTP）	RTP は、データ ネットワークを通じて、インタラクティブな音声やビデオなどのリアルタイム データを転送するための標準プロトコルです。	Cisco Unified IP Phone では、RTP プロトコルを使用して、リアルタイム音声トラフィックを他の電話機やゲートウェイとやり取りします。
Real-Time Control Protocol（RTCP; リアルタイム制御プロトコル）	RTCP は RTP と連携して、RTP ストリーム上で QoS データ（ジッター、遅延、ラウンドトリップ遅延など）を伝送します。	RTCP はデフォルトで無効になっています。 Cisco Unified Communications Manager を使用して電話機ごとに有効にできます。 詳細については、ネットワークの設定メニューを参照してください。
セキュア リアルタイム転送プロトコル（SRTP）	RTP に加えて、SRTP を使用できます。 SRTP では、データ転送時にメディア ストリームが暗号化されるため、セキュリティが強化されます。	SRTP が機能するには、コールされる電話機でも SRTP をサポートしている必要があります。サポートしていないと、これらの電話機はセキュアなメディア ストリームを復号化できません。

ネットワーク プロトコル	目的	使用方法
Session Initiation Protocol（SIP）	SIP は、IP を介したマルチメディア会議のための Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）標準です。 SIP は、アプリケーション層の ASCII ベースの制御プロトコルであり（RFC 3261 で規定）、2 つ以上のエンドポイント間でコールを確立、維持、および終了するために使用できます。	SIP はシグナリングとセッション管理の機能をパケットテレフォニーネットワークの内部で処理するように設計されています。 シグナリングによって、ネットワーク境界を越えてコール情報を伝送することが可能になります。 セッション管理とは、エンドツーエンドコールの属性を制御する機能を提供することです。 Cisco Unified IP Phone は、SIP または Skinny Client Control Protocol（SCCP）のいずれかを使用するように設定できます。 電話機が IPv6 アドレス モードで動作している場合、Cisco Unified IP Phone は SIP プロトコルをサポートしません。
Skinny Client Control Protocol（SCCP）	SCCP は、コール制御サーバとエンドポイント クライアント（IP Phone など）の間で通信を行うためのメッセージング セットを含んでいます。 SCCP は、シスコ独自のものです。	Cisco Unified IP Phone は、コール制御に SCCP を使用します。 Cisco Unified IP Phone は、SCCP または Session Initiation Protocol（SIP）のどちらかを使用するように設定できます。
セッション記述プロトコル（SDP）	SDP は SIP プロトコルの一部であり、2 つのエンドポイント間で接続が確立されている間に、どのパラメータが使用可能かを特定します。 会議は、会議に参加するすべてのエンドポイントでサポートされている SDP 機能だけを使用して確立されます。	コーデック タイプ、DTMF 検出、コンフォート ノイズなどの SDP 機能は、通常は運用中の Cisco Unified Communications Manager またはメディア ゲートウェイでグローバルに設定されています。 SIP エンドポイントの中には、これらのパラメータをエンドポイント上で設定できるものがあります。
伝送制御プロトコル（TCP）	TCP は、コネクション型の転送プロトコルです。	Cisco Unified IP Phone では、Cisco Unified Communications Manager への接続、および XML サービスへのアクセスに TCP を使用します。

ネットワーク プロトコル	目的	使用方法
トランスポート レイヤ セキュリティ（TLS）	TLS は、通信のセキュリティ保護と認証に使用される標準プロトコルです。	セキュリティが実装されると、Cisco Unified IP Phone では、Cisco Unified Communications Manager に安全に登録するときに TLS プロトコルが使用されます。 詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
トリビアルファイル転送プロトコル（TFTP）	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 TFTP は、電話機固有の設定ファイルを取得するために Cisco Unified IP Phone で使用されます。	TFTP では、ネットワーク内に TFTP サーバが必要です。このサーバは、DHCP サーバで自動的に識別できます。ネットワークで複数の TFTP サーバが動作している場合は、個々の電話機がある場所で各 TFTP サーバを手動で割り当てる必要があります。 詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco TFTP」を参照してください。
ユーザデータグラムプロトコル（UDP）	UDP は、データ パケットを配信するためのコネクションレス型メッセージング プロトコルです。	Cisco Unified IP Phone は UDP メッセージを受信し、処理します。

関連トピック

- Cisco Unified Communications 製品の連携
- 電話機の起動プロセス
- ネットワークの設定メニュー

Cisco Unified IP Phone での IPv6 サポート

Cisco Unified IP Phone はインターネット プロトコルを使用して、ネットワークで音声通信を提供します。 インターネット プロトコル バージョン 4（IPv4）は、32 ビット アドレスを使用するため、インターネットに接続するすべてのデバイスの一意の IP アドレスの要求増加に対応できません。 したがって、インターネット プロトコル バージョン 6（IPv6）が、現在のインターネット プロトコルの更新バージョンとなります。 IPv6 は 128 ビット アドレスを使用し、エンドツーエンド セキュリティ機能、拡張 Quality Of Service（QoS）、および使用可能な IP アドレス数の増加に対応します。

Cisco Unified IP Phone は IPv4 だけのアドレッシング モード、IPv6 だけのアドレッシング モード、IPv4/IPv6 デュアル スタック アドレッシング モードをサポートします。 IPv4 で、192.240.22.5 など、ドット付き 10 進表記で電話機の IP アドレスの各オクテットを入力できます。 IPv6 で 2005:db8:0:1:ef8:9876:ba72:dc9a など、各オクテットをコロンで区切り、16 進表記で IP アドレスの各オクテットを入力できます。 IPv6 アドレスを表示する場合、電話機は最初のゼロを省略して削除します。

Cisco Unified IP Phone は、IPv4 アドレスと IPv6 アドレスの両方を透過的にサポートするため、ユーザは慣れた電話機のすべてのコールを処理できます。 Skinny Call Control Protocol（SCCP）を使用する Cisco Unified IP Phone は、IPv6 をサポートします。 SIP を使用する Cisco Unified IP Phone は、IPv6 をサポートしません。

Cisco Unified IP Phone は、URL に IPv6 アドレスを含む URL に対応していません。 これは、認証 URL でクレデンシャルを検証するために電話機が HTTP プロトコルを使用する必要のあるサービス、ディレクトリ、メッセージ、ヘルプ、制限された Web サービスを含むすべての IP Phone サービス URL に影響します。 Cisco Unified IP Phone サービスを Cisco Unified IP Phone 用に設定する場合、IPv4 アドレスのある電話機サービスをサポートする電話機とサーバを設定する必要があります。

SIP を実行している電話機の IP アドレッシング モードとして IPv6 のみを設定している場合、Cisco TFTP サービスは IP アドレッシング モード設定を上書きし、設定ファイルで IPv4 のみを使用します。

Cisco Unified Communications ネットワークでの IPv6 の導入の詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』の「Internet Protocol Version 6 (IPv6)」の章、および http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/ipv6srnd.html で入手できる『*Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*』を参照してください。

Cisco Unified IP Phone 7906 および 7911 のサポートされる機能

Cisco Unified IP Phone 7906G および 7911G は、従来のアナログ電話機とほぼ同様に機能し、電話コールを発信および受信できます。 各 Cisco Unified IP Phone は、従来のテレフォニー機能に加えて、電話機をネットワーク デバイスとして管理およびモニタする機能も備えています。

機能の概要

Cisco Unified IP Phone は、コール転送や転送、リダイヤル、スピード ダイヤル、会議コール、ボイス メッセージング システムへのアクセスなど、主要なビジネス機能を提供します。 Cisco Unified IP Phone では、さらにその他の各種の機能も提供します。

Cisco Unified IP Phone は、Cisco Unified Communications Manager および IP ネットワークの他の部分にアクセスできるように設定する必要があります。 DHCP がネットワークで使用されている場

合は、電話機上で設定する設定値が少なくなります。 電話機では、IP アドレス、TFTP サーバ、およびサブネット情報の手動設定を行うことができます。

Cisco Unified IP Phone は、IP ネットワーク上の他のサービスやデバイスと連携することで、高度な機能を提供できます。 たとえば、Cisco Unified Communications Manager を社内の Lightweight Directory Access Protocol 3（LDAP3）標準ディレクトリと統合すると、ユーザが同僚の連絡先情報を IP Phone で直接検索できるようになります。 XML を使用すると、天気予報、株価情報、商品相場などの Web ベースの情報にユーザがアクセスできるようになります。

さらに、Cisco Unified IP Phone はネットワーク デバイスであるため、詳細なステータス情報を IP Phone から直接取得することができます。 この情報は、ユーザが Cisco Unified IP Phone を使用しているときに生じた問題をトラブルシューティングするのに役立ちます。

関連トピック

- サービスのセットアップ
- 社内ディレクトリとパーソナル ディレクトリのセットアップ
- モデル情報、ステータス、および統計
- Cisco Unified IP Phone の設定
- 機能、テンプレート、サービス、およびユーザ
- トラブルシューティングとメンテナンス

テレフォニー機能の管理

Cisco Unified IP Phone に関する設定の一部は、Cisco Unified Communications Manager の管理アプリケーションから変更できます。 この Web ベースのアプリケーションを使用して、電話機登録基準とコーリング サーチスペースのセットアップ、社内ディレクトリとサービスの設定、電話ボタンテンプレートの修正、その他のタスクを行うことができます。 詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

Cisco Unified Communications Manager の管理アプリケーションの詳細については、『*Cisco Unified Communications Manager System Guide*』など、Cisco Unified Communications Manager のマニュアルを参照してください。 また、このアプリケーションで参照できる状況依存ヘルプも参考情報として利用できます。

Cisco Unified Communications Manager のマニュアルには、次の Web サイトでアクセスできます。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Business Edition 5000 のマニュアルには、次の Web サイトでアクセスできます。

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

関連トピック

- Cisco Unified IP Phone で使用可能なテレフォニー機能

Cisco Unified IP Phone のネットワーク パラメータ

DHCP、TFTP、IP の設定値などのパラメータは、電話機で設定できます。 また、コールに関する統計情報や、ファームウェアのバージョンも電話機で取得できます。

関連トピック

Cisco Unified IP Phone の設定
モデル情報、ステータス、および統計

エンド ユーザへの情報

システム管理者は、多くの場合、ネットワーク内や社内の Cisco Unified IP Phone ユーザの主な情報源になります。 機能や手順について確実に最新の情報を伝えるために、Cisco Unified IP Phone のマニュアルをよく読んでおいてください。 Cisco Unified IP Phone の Web サイトに必ずアクセスしてください。

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

このサイトから、ウォレット カードを含む各種ユーザ ガイドを表示および注文できます。

マニュアルの提供に加えて、利用可能な Cisco Unified IP Phone の機能（自社固有の機能やご使用のネットワーク固有の機能も含む）、およびそれらの機能の利用方法とカスタマイズ方法（可能な場合）をユーザに知らせることも重要です。

関連トピック

社内のサポート Web サイト

Cisco Unified IP Phone のセキュリティ機能

Cisco Unified Communications Manager システムでセキュリティを実装すると、電話機や Cisco Unified Communications Manager サーバの ID 盗用を防止できます。 また、データ、コール シグナリング、およびメディア ストリームの改ざんも防止できます。

これらの脅威を軽減するため、Cisco Unified Communications ネットワークは、電話機とサーバ間で認証および暗号化された通信ストリームを確立および保持し、電話機に転送する前のファイルにデジタル署名し、Cisco Unified IP Phone 間のメディア ストリームおよびコール シグナリングを暗号化します。

Cisco Unified CM の管理でセキュリティ関連の設定値を設定した場合は、電話機の設定ファイルに機密情報が含まれます。 設定ファイルのプライバシーを確保するには、そのファイルを暗号化用に設定する必要があります。 詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Configuring Encrypted Phone Configuration Files」を参照してください。

次の表に、このマニュアルおよびその他のドキュメントでのセキュリティに関する追加情報の参照先を示します。

表 *2*：***Cisco Unified IP Phone*** セキュリティのトピック

トピック	参照先
Cisco Unified Communications Manager および Cisco Unified IP Phone に関するセットアップ情報、設定情報、およびトラブルシューティング情報を含む、セキュリティの詳細な説明	『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。
Cisco Unified IP Phone でサポートされるセキュリティ機能	サポート対象のセキュリティ機能, （15 ページ）を参照してください。
セキュリティ機能に関する制約	セキュリティ上の制約事項, （25 ページ）を参照してください。
セキュリティが実装されているコールの識別	認証、暗号化、および保護されている電話コール, （18 ページ）を参照してください。
トランスポート層セキュリティ（TLS）接続	• ネットワーク プロトコル, （3 ページ）を参照してください。 • 電話機設定ファイルを参照してください。
Cisco Unified IP Phone の 802.1X 認証	次の項を参照してください。 • 802.1X 認証, （22 ページ）。 • [セキュリティ設定（Security Configuration）] メニュー。 • [802.1X 認証（802.1X Authentication）] および [802.1X 認証ステータス（802.1X Authentication Status）]。 • Cisco Unified IP Phone のセキュリティの問題。
セキュリティと電話機の起動プロセス	電話機の起動プロセスを参照してください。
セキュリティと電話機の設定ファイル	電話機設定ファイルを参照してください。
セキュリティが実装されているときの電話機での [TFTP サーバ 1（TFTP Server 1）] または [TFTP サーバ 2（TFTP Server 2）] オプションの変更	ネットワークの設定メニューを参照してください。

トピック	参照先
電話機の [デバイス設定（Device Configuration）] メニューにある Communications Manager 1 ～ Communications Manager 5 の各オプションのセキュリティ アイコンの確認	Unified CM の設定メニューを参照してください。
電話機の [デバイス設定（Device Configuration）] メニューからアクセスする [セキュリティ設定（Security Configuration）] メニューの項目	[セキュリティ設定（Security Configuration）] メニューを参照してください。
電話機の [設定（Settings）] メニューからアクセスする [セキュリティ設定（Security Configuration）] メニューの項目	[セキュリティ設定（Security Configuration）] メニューを参照してください。
Certificate Trust List（CTL）ファイルと Identity Trust List（ITL）ファイルのロック解除	CTL ファイルと ITL ファイルのロック解除を参照してください。
電話機の Web ページへのアクセスの無効化	Web ページへのアクセスの制御を参照してください。
電話機からの CTL ファイルと ITL ファイルの削除	Cisco Unified IP Phone のリセットまたは復元を参照してください。
電話機のリセットまたは復元	Cisco Unified IP Phone のリセットまたは復元を参照してください。
エクステンション モビリティ HTTPS のサポート	ネットワーク プロトコル, （3 ページ）を参照してください。
Cisco Unified IP Phone の 802.1X 認証	次の項を参照してください。 • 802.1X 認証, （22 ページ）。 • [802.1X 認証（802.1X Authentication）] および [802.1X 認証ステータス（802.1X Authentication Status）]。 • Cisco Unified IP Phone のセキュリティの問題。 • [信頼リスト（Trust List）] メニュー。

サポート対象のセキュリティ機能

ここでは、電話機がサポートするセキュリティ機能の概要を示します。 これらの機能と、Cisco Unified Communications Manager および Cisco Unified IP Phone のセキュリティの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

電話機の現在のセキュリティ設定については、[セキュリティ設定（Security Configuration）] メニュー（アプリケーション メニューを押し、[設定（Settings）] > [セキュリティ設定（Security Configuration）] または [設定（Settings）] > [デバイス設定（Device Configuration）] > [セキュリティ設定（Security Configuration）] を選択します）を確認します。

（注） ほとんどのセキュリティ機能は、電話機に CTL と ITL ファイルのいずれかまたは両方がインストールされている場合にだけ使用できます。 CTL ファイルおよび ITL ファイルの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

表 *3*：セキュリティ機能の概要

機能	説明
イメージ認証	ファームウェアイメージが電話機にロードされる前に、署名付きバイナリ ファイル（拡張子 .sbn）を使用して、ファームウェア イメージに対する改ざんを防止します。 イメージが改ざんされると、電話機は認証プロセスに失敗し、新しいイメージを拒否します。
802.1X 認証	Cisco Unified IP Phone は 802.1X 認証を使用して、ネットワークへのアクセスの要求およびネットワーク アクセスができます。詳細については、802.1X 認証, （22 ページ）を参照してください。
カスタマーサイト証明書のインストール	各 Cisco Unified IP Phone は、デバイス認証に一意の証明書を必要とします。 電話機には製造元でインストールされる証明書（MIC）が含まれますが、追加のセキュリティについては、Cisco Unified CM の管理で、Certificate Authority Proxy Function（CAPF）を使用して証明書をインストールするように指定できます。 あるいは、電話機の [セキュリティ設定（Security Configuration）] メニューからローカルで有効な証明書（LSC）をインストールできます。 詳細については、Cisco Unified IP Phone のセキュリティを参照してください。

機能	説明
デバイス認証	Cisco Unified Communications Manager サーバと電話機との間で、一方のエンティティが他方のエンティティの証明書を受け入れるときに行われます。 電話機と Cisco Unified Communications Manager との間でセキュアな接続を確立するかどうかを判別し、必要に応じてトランスポート層セキュリティ（TLS）プロトコルを使用してエンティティ間にセキュアなシグナリング パスを作成します。 Cisco Unified Communications Manager で電話機を認証できない限り、Cisco Unified Communications Manager ではそれらの電話機は認証モードまたは暗号化モードで登録されません。
ファイルの認証	電話機がダウンロードするデジタル署名ファイルを検証します。 ファイルの作成後、ファイルの改ざんが発生しないように、電話機でシグニチャを検証します。 認証できないファイルは、電話機のフラッシュ メモリに書き込まれません。 電話機はこのようなファイルを拒否し、処理を続行しません。
シグナリング認証	TLS プロトコルを使用して、シグナリング パケットが転送中に改ざんされていないことを検証します。
製造元でインストールされる証明書	Cisco Unified IP Phone 7906G および 7911G にはそれぞれ、固有の MIC が内蔵されており、デバイス認証に使用されます。 MIC は、個々の電話機を識別するために長期的に割り当てられた証明であり、Cisco Unified Communications Manager はこれを使用して電話機を認証します。
セキュアな SRST リファレンス	セキュリティのために SRST リファレンスを設定し、Cisco Unified Communications Manager 管理ページで依存デバイスをリセットした後、TFTP サーバは SRST 証明書を電話機の cnf.xml ファイルに追加して、ファイルを電話機に送ります。 その後、セキュアな電話機は TLS 接続を使用して、SRST 対応ルータと相互に対話します。
メディアの暗号化	SRTP を使用して、サポートされるデバイス間のメディア ストリームがセキュアであることを証明し、意図したデバイスのみがデータを受け取り、読み取れるようにします。 デバイスのメディア マスターのキーペアの作成、デバイスへのキーの配布、キーが転送される間のキーの配布のセキュリティの確保などが含まれます。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバ間で送信されるすべての SCCP と SIP シグナリング メッセージを暗号化します。

機能	説明
CAPF（Certificate Authority Proxy Function）	電話機に非常に高い処理負荷がかかる、証明書生成手順の一部を実装します。また、キーの生成および証明書のインストールのために電話機と対話します。 電話機の代わりに、お客様指定の認証局に証明書を要求するよう CAPF を設定できます。または、ローカルで証明書を生成するように CAPF を設定することもできます。
電話機の Web サーバ機能の無効化（オプション）	電話機の多様な操作統計情報を表示する、電話機の Web ページへのアクセスを禁止できます。
電話機のセキュリティの強化	Cisco Unified CM の管理から制御する追加セキュリティ オプションです。次のオプションがあります。 • PC ポートを無効にする（7911G のみに適用） • Gratuitous Address Resolution Protocol（GARP）を無効にする • PC ボイス VLAN アクセスを無効にする（7911G のみに適用） • [設定（Setting）] メニューへのアクセスを無効にする、または、[ユーザ設定（User Preferences）] メニューへのアクセスと音量変更の保存だけを許可する制限付きアクセスを提供する • 電話機の Web ページへのアクセスを無効にする （注） [PC ポートを無効にする（PC Port Disabled）]、[GARP を使う（GARP Enabled）]、および [ボイス VLAN を使う（Voice VLAN enabled）] の現在の設定値を表示するには、電話機の [セキュリティ設定（Security Configuration）] メニューを調べます。

関連トピック

認証、暗号化、および保護されている電話コール, （18 ページ）
802.1X 認証, （22 ページ）
セキュリティ上の制約事項, （25 ページ）
デバイス設定メニュー

セキュリティ プロファイル

Cisco Unified Communications Manager 5.0 以降をサポートするすべての Cisco Unified IP Phone は、電話機が非セキュア、認証済み、または暗号化済みのいずれであるかを定義するセキュリティ プロファイルを使用します。セキュリティプロファイルの設定方法、および電話機へのプロファイルの適用方法については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

電話機に設定されているセキュリティ モードを確認するには、[セキュリティ設定（Security Configuration）] メニューの [セキュリティ モード（Security Mode）] の設定を表示します。

関連トピック

認証、暗号化、および保護されている電話コール, （18 ページ）
セキュリティ上の制約事項, （25 ページ）
[セキュリティ設定（Security Configuration）] メニュー

認証、暗号化、および保護されている電話コール

電話機にセキュリティが実装されている場合、認証および暗号化されたコールは、電話機の LCD スクリーンに表示されるアイコンで識別できます。 コールの開始時にセキュリティ トーンが再生される場合は、接続された電話がセキュアで保護されているかどうかも判断できます。

コールが認証された場合、そのコールの確立に関与したすべてのデバイスは信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されます。 コールは、セットアップ時にエンドツーエンドで認証されます。 電話機の LCD スクリーン内の通話時間タイマーの右にあるコール進捗アイコンが次のアイコンに変わります。

コールが暗号化された場合、そのコールの確立に関与したすべてのデバイスは信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されます。 さらに、コールのシグナリングとメディアストリームが暗号化されます。暗号化されたコールはコールの整合性とプライバシーを提供することで、高レベルのセキュリティを提供します。 処理中のコールが暗号化されているときは、電話機のLCDスクリーンのコール時間タイマーの右側にあるコール進捗アイコンが、次のアイコンに変化します。

（注） コールが PSTN などの非 IP コール レッグを経由してルーティングされる場合、コールが IP ネットワーク内で暗号化されており、鍵のアイコンが関連付けられていても、そのコールはセキュアではないことがあります。

保護コールの開始時にセキュリティ トーンが再生され、接続先の電話機も暗号化された音声および場合によってはビデオを送受信していることを示します。 保護されていない電話機にコールが接続されると、セキュリティ トーンは再生されません。

（注） 保護されたコールは、2台の電話機間の接続に対してのみサポートされます。 保護コールを設定すると、一部の機能（会議コール、共有回線、エクステンション モビリティ、回線をまたいで参加）は使用できません。 保護されたコールは認証されません。

関連トピック

Cisco Unified IP Phone のセキュリティ機能, （12 ページ）
802.1X 認証, （22 ページ）
セキュリティ上の制約事項, （25 ページ）

セキュアな会議コールの特定

セキュアな会議コールを開始し、参加者のセキュリティ レベルをモニタすることができます。 セキュアな会議コールは、次のプロセスに従って確立されます。

1. ユーザがセキュアな電話機から会議を開始します（暗号化された、または認証済みのセキュリティ モード）。
2. Cisco Unified Communications Manager が、コールにセキュアな会議ブリッジを割り当てます。
3. 参加者が追加されると、Cisco Unified Communications Manager は各電話機のセキュリティ モード（暗号化されているか、認証済み）を検証し、会議のセキュリティ レベルを維持します。
4. 電話機に会議コールのセキュリティ レベルが表示されます。 セキュアな電話会議では、電話機画面の [会議（Conference）] の右に（暗号化された）アイコンまたは（認証済み）アイコンが表示されます。 アイコンが表示される場合は、会議がセキュアではありません。

（注） 参加者の電話機のセキュリティ モードおよびセキュアな会議ブリッジの可用性によっては、会議コールのセキュリティ レベルに影響する連携動作と制限事項があります。 このような連携動作については、コール セキュリティの連携動作と制限事項, （20 ページ）を参照してください。

保護されたコールの識別

ユーザの電話機と相手側の電話機が保護されたコール用に設定されている場合、保護されたコールが確立されます。 相手側の電話機は、同じ Cisco IP ネットワーク内にあっても、Cisco IP ネットワーク以外のネットワークにあってもかまいません。 保護されたコールは、2 台の電話機の間

でのみ確立できます。 会議コールや、複数回線を使用するその他のコールはサポートされません。

保護されたコールの確立は、次のようなプロセスになります。

1. ユーザが保護された電話機（保護されたセキュリティ モード）からコールを開始します。
2. 電話機の画面に アイコン（暗号化済み）が表示されます。 このアイコンは、電話機がセキュアな（暗号化された）コール用に設定されていることを示しますが、接続先の電話機も保護されていることを意味するわけではありません。
3. 保護された他の電話機にコールが接続されると、セキュリティ トーンが再生され、通話の両側が暗号化および保護されていることを示します。 保護されていない電話機にコールが接続されると、セキュア トーンは再生されません。

（注） 保護されたコールは 2 台の電話機間の通話に対してサポートされます。 保護されたコールが設定されていると、会議、共有回線、Cisco Extension Mobility、回線をまたいで参加など一部の機能を使用できません。

コール セキュリティの連携動作と制限事項

Cisco Unified Communications Manager は、会議の確立時に電話機のセキュリティ ステータスを確認し、会議のセキュリティ表示を変更するか、またはコールの確立をブロックしてシステムの整合性とセキュリティを維持します。 次の表は、割り込み機能の使用時にコールのセキュリティ レベルに適用される変更内容を示しています。

表 *4*：割り込み使用時のコール セキュリティの連携動作

発信側電話機のセキュリティレベル	コールのセキュリティレベル	動作結果
非セキュア	暗号化されたコール	コールは割り込みを受け、非セキュア コールとして識別されます。
セキュア（暗号化済み）	認証済みコール	コールは割り込みを受け、認証されたコールとして識別されます。
セキュア（認証済み）	暗号化されたコール	コールは割り込みを受け、認証されたコールとして識別されます。
非セキュア	認証済みコール	コールは割り込みを受け、非セキュア コールとして識別されます。

次の表は、発信側（会議開催者）の電話機のセキュリティ レベル、参加者のセキュリティ レベル、およびセキュアな会議ブリッジの可用性に応じて会議のセキュリティ レベルに適用される変更内容を示しています。

表 *5*：会議コールのセキュリティの制限事項

発信側電話機のセキュリティレベル	使用する機能	参加者のセキュリティレベル	動作結果
非セキュア	会議	暗号化済みまたは認証済み	非セキュアな会議ブリッジ 非セキュアな会議
セキュア（暗号化済みまたは認証済み）	会議	少なくとも 1 台のメンバーが非セキュア。	セキュアな会議ブリッジ 非セキュアな会議
セキュア（暗号化済み）	会議	すべての参加者が暗号化済み	セキュアな会議ブリッジ セキュアな暗号化レベルの会議
セキュア（認証済み）	会議	すべての参加者が暗号化済みまたは認証済み。	セキュアな会議ブリッジ 認証済みレベルのセキュアな会議
非セキュア	会議	暗号化済みまたは認証済み	セキュアな会議ブリッジのみが利用可能で、使用されている 非セキュアな会議
セキュア（暗号化済みまたは認証済み）	会議	暗号化済みまたは認証済み	非セキュアな会議ブリッジのみが利用可能で、使用されている 非セキュアな会議
セキュア（暗号化済みまたは認証済み）	会議	セキュアまたは暗号化済み	会議はセキュアに保たれる 参加者の 1 人がコールを保留音（MoH）で保留しようとすると、MOH が再生されない。
セキュア（暗号化済み）	参加	暗号化済みまたは認証済み	セキュアな会議ブリッジ 会議はセキュアな状態を維持する（暗号化されているか、認証済み）

発信側電話機のセキュリティレベル	使用する機能	参加者のセキュリティレベル	動作結果
非セキュア	cBarge	すべての参加者が暗号化済み	セキュアな会議ブリッジ 会議が非セキュアに変更される
非セキュア	ミートミー	最小限のセキュリティレベルが暗号化	発信側は「セキュリティレベルを満たしていません。コールは拒否されました（Does not meet Security Level, call rejected）」というメッセージを受け取る。
セキュア（暗号化済み）	ミートミー	最小セキュリティ レベルは、認証済み	セキュアな会議ブリッジ 会議は、暗号化済みおよび認証済みのコールを受け入れる。
セキュア（暗号化済み）	ミートミー	最小限のセキュリティレベルは非セキュア	セキュアな会議ブリッジだけが使用可能になり、使用される。 会議はすべてのコールを受け入れる。

802.1X 認証

ここでは、Cisco Unified IP Phone での 802.1X のサポートについて説明します。

概要

Cisco Unified IP Phone と Cisco Catalyst スイッチは、従来から Cisco Discovery Protocol（CDP）を使用して相互を識別し、VLAN 割り当てやインライン パワー要件などのパラメータを特定していました。 CDP は、ローカルに接続されたワークステーションを識別しません。 Cisco Unified IP Phone は、EAPOL パススルー メカニズムを備えています。 このメカニズムにより、Cisco Unified IP Phone に接続されているワークステーションは、EAPOL メッセージを LAN スイッチの 802.1X オーセンティケータに渡すことができます。 パススルー メカニズムにより、IP Phone は、ネットワークにアクセスする前にデータ エンドポイントを認証する LAN スイッチとして動作しなくなります。

Cisco Unified IP Phone は、プロキシ EAPOL ログオフ メカニズムも備えています。 ローカルに接続された PC が IP Phone から切断されても、LAN スイッチと IP Phone 間のリンクは維持されるの

で、LAN スイッチは物理リンクの障害を認識しません。 ネットワークの完全性が脅かされるのを避けるため、IP 電話はダウンストリーム PC の代わりに EAPOL ログオフ メッセージをスイッチに送ります。 これは、LAN スイッチにダウンストリーム PC の認証エントリをクリアさせます。

Cisco Unified IP Phone には、802.1X サプリカントも含まれています。 このサプリカントを使用して、ネットワーク管理者は IP 電話と LAN スイッチ ポートの接続を制御できます。 電話機の 802.1X サプリカントの現行リリースでは、ネットワーク認証に EAP-FAST、EAP-TLS、および EAP-MD5 オプションを使用します。

必要なネットワーク コンポーネント

Cisco Unified IP Phone での 802.1X 認証のサポートには、次のようなコンポーネントが必要です。

- Cisco Unified IP Phone：電話機は 802.1X サプリカントとして機能します。 これはネットワークへのアクセス要求を開始します。
- Cisco Secure Access Control Server（ACS）（またはその他のサードパーティ製認証サーバ）：認証サーバと電話機の両方に、電話機の認証に使用される共有秘密が設定されている必要があります。
- Cisco Catalyst スイッチ（またはその他のサードパーティ製スイッチ）：スイッチはオーセンティケータとして機能し、電話機と認証サーバ間でメッセージを渡すことができるよう、802.1X をサポートしている必要があります。 やり取りが完了した後、スイッチはネットワークへの電話機のアクセスを許可または拒否します。

ベスト プラクティス：要件と推奨事項

- 802.1X の有効化：802.1X 標準を Cisco Unified IP Phone の認証に使用する場合、電話機で有効にする前に他のコンポーネントを正しく設定していることを確認してください。
- PC ポートの設定：802.1X 標準は VLAN の使用を考慮しないため、各スイッチ ポートにデバイスを 1 つだけ認証することを推奨します。 ただし、一部のスイッチ（Cisco Catalyst スイッチなど）はマルチドメイン認証をサポートしています。 スイッチ設定によって PC を電話機の PC ポートに接続できるかどうかが決まります。
  - 有効：複数ドメインの認証をサポートするスイッチを使用している場合、PC ポートを有効化し、そのポートに PC を接続できます。 この場合、スイッチと接続先 PC 間の認証情報の交換をモニタするために、Cisco Unified IP Phone はプロキシ EAPOL ログオフをサポートします。 Cisco Catalyst スイッチでの IEEE 802.1X サポートの詳細については、次の URL にある Cisco Catalyst スイッチのコンフィギュレーション ガイドを参照してください。

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - 無効：スイッチが同一ポート上の複数の 802.1X 対応デバイスをサポートしていない場合、802.1X 認証を有効化するときに PC ポートを無効にする必要があります。 PC ポートを無効化せずに PC を接続しようとすると、スイッチは電話機および PC へのネットワーク アクセスを拒否します。

- ボイス VLAN の設定：802.1X 標準では VLAN が考慮されないため、ボイス VLAN の設定はスイッチのサポートに基づいて行う必要があります。
  - 有効：複数ドメインの認証をサポートするスイッチを使用している場合は、ボイスVLANを引き続き使用できます。
  - 無効：スイッチがマルチドメイン認証をサポートしていない場合は、ボイス VLAN を無効にし、ネイティブ VLAN へのポートの割り当てを検討します。
- MD5 共有秘密の入力：電話機で 802.1X 認証を無効にするか、工場出荷時の状態にリセットすると、以前に設定された MD5 共有秘密は削除されます。

関連トピック

[セキュリティ設定（Security Configuration）] メニュー

[802.1X 認証（802.1X Authentication）] および [802.1X 認証ステータス（802.1X Authentication Status）]

UCR 2008

SCCP を使用する IP Phone は、次の機能を提供することで、Unified Capabilities Requirements（UCR）2008 をサポートします。

- 連邦情報処理標準（FIPS）104-2 のサポート：FIPS 104-2 をサポートするには、次のことが電話機に必要となります。
  - 適切な暗号化アルゴリズムを確実に使用できるように、Power On Self Testing（POST）を使用する。 電話機のファームウェアに適切なモジュールがないと、電話機は起動に失敗します。
  - すべてのインターネット通信に HTTPS を使用する。
  - 電話機への Web アクセスを無効にする。
  - CUCM を FIPS に準拠するようにセットアップする（802.1x EAP-MD5 を無効にするなど）。
- TVS IPv6：IPv6 アドレスが使用可能な場合、信頼検証サービス（TVS）サーバの IPv6 アドレスが電話機に表示されます。
- 80 ビット SRTCP タギング：電話機は、32 ビットと 80 ビット両方の SRTCP パケット ヘッダーをシームレスに処理します。

これらの機能の一部では、Cisco Unified Communications Manager で特定のパラメータを設定する必要があります。

次の表に、このマニュアルおよびその他のドキュメントでの UCR 2008 に関する追加情報の参照先を示します。

表 *6*：*Cisco Unified IP Phone UCR 2008* のトピック

トピック	参照先
Cisco Unified Communications Manager および Cisco Unified IP Phone に関するセットアップ情報、設定情報、およびトラブルシューティング情報を含む、セキュリティの詳細な説明	『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。
UCR 2008 パラメータのセットアップ	UCR 2008 のセットアップを参照してください。
POST 問題のトラブルシューティング	Cisco Unified IP Phone で「セキュリティ エラー（Security Error）」メッセージが表示されるを参照してください。

セキュリティ上の制約事項

電話機に暗号化が設定されていない場合、その電話機を使用して暗号化されたコールに割り込むことはできません。 この場合、割り込みに失敗すると、割り込みの開始側の電話機でリオーダートーン（速いビジー音）が聞こえます。

発信側の電話機に暗号化が設定されている場合、割り込みの発信側は、暗号化された電話機から認証されたコールまたは非セキュア コールに対して割り込みを実行できます。 割り込みが発生すると、Cisco Unified Communications Manager はそのコールをセキュアでないコールに分類します。

割り込みの開始側の電話機に暗号化が設定されている場合、割り込みの開始側は暗号化されたコールに割り込むことができ、電話機はそのコールが暗号化されていることを示します。

割り込みに使用される電話機が非セキュアの場合でも、ユーザは認証されたコールに対して割り込みを実行できます。 発信側の電話機がセキュリティをサポートしていない場合でも、認証アイコンはコール内の認証されたデバイスに引き続き表示されます。

電話機の消費電力

Cisco Unified IP Phone 7900 シリーズは、Cisco EnergyWise をサポートします。 EnergyWise は Power Save Plus とも呼ばれます。 ネットワークに EnergyWise コントローラが含まれている場合、それらの電話機をスケジュールに従ってスリープ状態（電源オフ）にしたり、復帰（電源オン）させたりして、電力消費を削減できます。 電話機の電源は、電源アダプタではなくスイッチの Power over Ethernet（PoE）ポートを使用して投入する必要があります。

EnergyWise は、電話機ごとに有効または無効に設定します。 また、エンタープライズ電話および共通電話の設定で EnergyWise パラメータを設定することもできます。 EnergyWise を有効にした場合は、他のパラメータと一緒にスリープと復帰の時刻を設定します。 これらのパラメータは、電話機設定 XML ファイルの一部として電話機へ送信されます。

スイッチの管理者は、予定の時刻よりも前に電話機を復帰させることができます。 スイッチからの電話機の電源投入の詳細については、スイッチのマニュアルを参照してください。

Cisco Unified IP Phone の導入

新しいUnified Communicationsシステムを導入するときは、システム管理者とネットワーク管理者がいくつかの初期設定作業を実施して、ネットワークをUnified Communicationsサービス用に準備する必要があります。 完全なCisco Unified Communicationsネットワークのセットアップと設定のための情報とチェックリストについては、『*Cisco Unified Communications Manager System Guide*』の「System Configuration Overview」を参照してください。

Unified Communications システムをセットアップし、システム全体にわたる機能を Cisco Unified Communications Manager で設定した後に、IP Phone をシステムに追加できます。

Cisco Unified Communications Manager での Cisco Unified IP Phone のセットアップ

電話機を Cisco Unified Communications Manager データベースに追加するには、次の方法を利用できます。

- 自動登録
- Cisco Unified CM の管理
- 一括管理ツール（BAT）
- BAT と Tool for Auto-Registered Phones Support（TAPS）

Cisco Unified Communications Manager で電話機を設定する方法の詳細については、次の資料を参照してください。

- 『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phone」の章
- 『*Cisco Unified Communications Manager Administration Guide*』の「Configuring Cisco Unified IP Phone Configuration」の章
- 『*Cisco Unified Communications Manager Administration Guide*』の「Autoregistration」の章
- 『*Cisco Unified Communications Manager Bulk Administration Guide*』

詳細については、Cisco Unified Communications Manager 電話機の追加方法を参照してください。

Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G のセットアップ

次の手順では、Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G の設定タスクの概要およびチェックリストを示します。 この手順では、推奨する順序で作

業を示して、電話機を設定するプロセスを解説しています。 一部のタスクは、システムおよびユーザのニーズによっては省略できます。 手順および内容の詳細については、手順に示した資料を参照してください。

手順

ステップ 1 電話機について、次の情報を収集します。

- 電話機のモデル
- MAC アドレス
- 電話機の設置場所
- 電話機のユーザの名前または ID
- デバイス プール
- コーリング サーチ スペースおよびロケーションの情報（使用する場合）
- 回線の数、関連付けられた電話番号（DN）、および電話機に割り当てるパーティション
- 電話機に関連付ける Cisco Unified Communications Manager ユーザ
- 電話ボタン テンプレート、ソフトキー テンプレート、電話機能、IP Phone サービス、または電話アプリケーションに影響する、電話機の使用状況情報

この情報では、電話機をセットアップするための設定要件のリストを示します。また、個々の電話機を設定する前に実施する必要のある、電話ボタンテンプレートやソフトキーテンプレートなどの前提的な設定作業を特定します。

詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phone」の章、および Cisco Unified IP Phone で使用可能なテレフォニー機能を参照してください。

ステップ 2 必要に応じて電話ボタンテンプレートをカスタマイズします。 これによりプライバシー機能が追加され、ユーザのニーズに対応できます。
詳細については、『Cisco Unified Communications Manager Administration Guide』の「Phone Button Template Configuration」の章、および電話ボタン テンプレートを参照してください。

ステップ 3 [電話の設定（Phone Configuration）] ウィンドウの次の必須フィールドに値を入力して、電話機を追加および設定します。

- 電話のタイプ（Phone Type）
- MAC アドレス（MAC Address）
- デバイス プール（Device Pool）
- ボタン テンプレート（Button Template）
- プロダクト固有の設定（Product Specific Configuration）
- ソフトキー テンプレート（Softkey Template）（カスタマイズしている場合）

デバイスを、デフォルト設定値を使用して Cisco Unified Communications Manager データベースに追加します。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Configuration」の章を参照してください。

[プロダクト固有の設定（Product Specific Configuration）] フィールドについては、[電話の設定（Phone Configuration）] ウィンドウで [?] ボタンのヘルプを参照してください。

（注） Cisco Unified Communications Manager データベースに電話機とユーザの両方を同時に追加する場合は、『*Cisco Unified Communications Manager Administration Guide*』の「User/Phone Configurations」を参照してください。

ステップ 4 [電話番号の設定（Directory Number Configuration）] ウィンドウの次の必須フィールドに値を入力して、電話機に電話番号を追加し、設定します。

- ディレクトリ番号（Directory Number）
- 複数コールとコール待機（Multiple Calls and Call Waiting）
- コール転送とコール ピックアップ（Call Forwarding and Pickup）（使用している場合）
- ボイス メッセージング（Voice Messaging）（使用している場合）

プライマリとセカンダリの電話番号、および電話番号に関連付ける機能を電話機に追加します。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Directory Number Configuration」の章、および Cisco Unified IP Phone で使用可能なテレフォニー機能を参照してください。

ステップ 5 ソフトキー テンプレートをカスタマイズします（任意）。
ユーザの電話機に表示されるソフトキー機能を追加、削除、または順序変更して、機能の利用ニーズに対応します。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Softkey Template Configuration」の章、およびソフトキー テンプレートを参照してください。

ステップ 6 スピード ダイヤル ボタンを設定し、スピード ダイヤル番号を割り当てます（任意）。 スピード ダイヤル番号を追加します。

（注） ユーザは、Cisco Unified Communications Manager ユーザ オプションを使用することで、スピード ダイヤルの設定値を電話機上で変更できます。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Configuration」の章の「Configuring Speed-Dial Buttons」の項を参照してください。

ステップ 7 Cisco Unified IP Phone サービスを設定し、サービスを割り当てます（任意）。 IP Phone サービスを提供します。

（注） ユーザは、Cisco Unified Communications Manager ユーザ オプションで、使用している電話機のサービスを追加または変更できます。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Services Configuration」の章、およびサービスのセットアップを参照してください。

ステップ 8 サービスを電話ボタンに割り当てます（任意）。 ボタンを 1 回押すだけで IP Phone サービスまたは URL にアクセスできるようにします。
『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Configuration」の章の「Adding a Cisco Unified IP Phone Service to a Phone Button」の項を参照してください。

ステップ 9 必須フィールドを設定して、ユーザ情報を追加します（任意）。

- 名前（姓）
- ユーザ ID
- パスワード（ユーザ オプション Web ページ）
- PIN（エクステンション モビリティで使用）

Cisco Unified Communications Manager のグローバル ディレクトリにユーザ情報を追加します。

（注） [社内ディレクトリ（Corporate Directory）] でユーザを検索するには、ユーザを Cisco Unified Communications Manager に追加する必要があります。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「End User Configuration」の章、および Cisco Unified Communications Manager ユーザの追加を参照してください。

（注） ユーザに関する情報を保存するために会社が Lightweight Directory Access Protocol（LDAP）ディレクトリを使用している場合、既存の LDAP ディレクトリを使用するために Cisco Unified Communications をインストールして設定できます。社内ディレクトリとパーソナル ディレクトリのセットアップを参照してください。

（注） Cisco Unified Communications Manager データベースに電話機とユーザの両方を同時に追加する場合は、『*Cisco Unified Communications Manager Administration Guide*』の「User/Phone Configurations」の章を参照してください。

ステップ 10 ユーザをユーザ グループに追加します。
ユーザ グループ内のすべてのユーザに適用される、共通のロールと権限のリストをユーザに割り当てます。 管理者は、ユーザ グループ、ロール、および権限を管理することによって、システム ユーザのアクセス レベル（つまり、セキュリティのレベル）を制御できます。 たとえば、ユーザをシスコの標準 CCM エンド ユーザ グループに追加する必要があります。こうすると、ユーザが Cisco Unified Communications Manager ユーザ オプションにアクセスできるようになります。

詳細については、『Cisco Unified Communications Manager Administration Guide』の「User Group Configuration」の章の「Adding Users to a User Group」の項を参照してください。

ステップ 11 ユーザを電話機に割り当てます（任意）。
ユーザが、コール転送やスピード ダイヤルの追加などの電話機能やサービスを設定できるようにします。

（注） 電話機の中には、会議室にある電話機など、ユーザが関連付けられないものもあります。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「End User Configuration」の章の「Associating Devices to a User」の項を参照してください。

Cisco Unified IP Phone の設置

電話機を Cisco Unified Communications Manager データベースに追加したら、次は電話機を設置します。 電話機は希望の場所に設置できます。または、設置の実行に必要な情報を電話機のユーザに提供できます。 http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html で入手できる『Cisco Unified IP Phone Installation Guide』では、電話機のフットスタンド、ハンドセット、ケーブル、およびその他のアクセサリを接続する方法が記載されています。

（注） 電話機を設置する前に、最新のファームウェア イメージにアップグレードしてください。 電話機のアップグレードについては、次の URL で対象の電話機の Readme ファイルを参照してください。

http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser

電話機をネットワークに接続すると、電話機の起動プロセスが開始され、電話機が Cisco Unified Communications Manager に登録されます。 電話機の設置を完了するには、DHCP サービスを有効にするかどうかに応じて、電話機上でネットワーク設定値を設定します。

自動登録を使用した場合は、電話機をユーザに関連付ける、ボタン テーブルを変更する、電話番号を割り当てるなど、電話機の特定の設定情報をアップデートします。

Cisco Unified IP Phone 7906G および 7911G の設置

次の手順では、Cisco Unified IP Phone 7906G および 7911G の設置タスクの概要およびチェックリストを示します。 この手順では、推奨する順序で作業を示し、電話機を設置するプロセスを解説しています。 一部のタスクは、システムおよびユーザのニーズによっては省略できます。 手順および内容の詳細については、この手順に示した資料を参照してください。

手順

ステップ 1 電話機の電源を次の中から選択します。

- Power over Ethernet（PoE）
- 外部電源

電話機に電力を供給する方法を決定します。 詳細については、Cisco Unified IP Phone の電源 を参照してください

ステップ 2 電話機を組み立て、電話機の位置を調節し、ネットワーク ケーブルを接続します。
電話機の位置を決めて設置し、ネットワークに接続します。 詳細については、Cisco Unified IP Phone の設置を参照してください。

ステップ 3 電話機の起動プロセスをモニタします。

電話機が適切に設定されていることを確認します。 詳細については、電話機の起動の確認を参照してください。

ステップ 4 DHCP を使用して電話機のネットワーク設定値を設定する場合、DHCP を有効にし、DHCP サーバが自動的に IP アドレスを Cisco Unified IP Phone に割り当てられるようにし、電話機を TFTP サーバに割り当てるには、[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv4 設定（IPv4 Configuration）] を選択し、次のようにします。

- DHCP を有効にするには、[DHCP を使う（DHCP Enabled）] を [はい（Yes）] に設定します。DHCP は、デフォルトで有効になっています。
- 代替 TFTP サーバを使用するには、[代替 TFTP サーバ（Alternate TFTP Server）] を [はい（Yes）] に設定し、TFTP サーバの IP アドレスを入力します。

（注） DHCP によって割り当てられた TFTP サーバの代わりに代替の TFTP サーバを割り当てる必要がある場合は、ネットワーク管理者に相談してください。

ステップ 5 電話機のネットワーク設定値の設定に DHCP を使用しない場合は、IP アドレス、サブネット マスク、TFTP サーバ、および電話機のデフォルト ルータをローカルで設定する必要があります。[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv4 設定（IPv4 Configuration）] を選択します。
DHCP を無効にして、IP アドレスを手動で設定する場合：

a) DHCP を無効にするには、[DHCP を使う（DHCP Enabled）] を [No] に設定します。
b) 電話機のスタティック IP アドレスを入力します。
c) サブネット マスクを入力します。
d) デフォルト ルータの IP アドレスを入力します。
e) [代替 TFTP サーバ（Alternate TFTP Server）] を [はい（Yes）] に設定し、TFTP サーバ 1 の IP アドレスを入力します。

（注） [設定（Settings）] > [ネットワークの設定（Network Configuration）] を選択し、電話機が常駐しているドメイン名を入力します。

詳細については、ネットワーク設定およびネットワークの設定メニューを参照してください。

ステップ 6 電話機のセキュリティをセットアップします。
データ改ざんの脅威と電話機の ID 盗用を防止します。 詳細については、Cisco Unified IP Phone のセキュリティ を参照してください

ステップ 7 Cisco Unified IP Phone を使用して、コールを発信します。
電話機および機能が正常に動作することを確認します。 詳細については、『*Cisco Unified IP Phones 7906G and 7911G User Guide for Cisco Unified Communications Manager (SCCP and SIP)*』を参照してください。

ステップ 8 ユーザに対して、電話機の使用方法および電話機のオプションの設定方法を通知します。
ユーザが十分な情報を得て、Cisco Unified IP Phone を有効に活用できるようにします。 詳細については、社内のサポート Web サイト を参照してください