CHAPTER 1

Cisco Unified IP Phone の概要

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提供します。標準的なデジタル ビジネス フォンとほぼ同様に機能し、電話コールの発信および受信に加えて、ミュート、保留、転送、短縮ダイヤルなどの機能を使用できます。また、データ ネットワークに接続されるため、生産性向上のための機能が拡張され、ネットワーク情報、XML アプリケーション、およびカスタマイズ可能な機能にアクセスできるようになります。

Cisco Unified IP Phone は、他のネットワーク デバイスと同様に、設定および管理が必要です。この電話機は、G.711a、G.711μ、G.729a、G.729ab、G.728/iLBC のエンコードと、G.711 のすべてのバリアント、G.728/iLBC、および G.729 のデコードを行います。また、ワイドバンド（16 ビット、16 kHz）オーディオもサポートしています。

この章は、次の項で構成されています。

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、干渉が発生するデバイスの製造元のマニュアルを参照してください。

Cisco Unified IP Phone 7906G と 7911G について

Cisco Unified IP Phone 7906G および 7911G は、談話室、教室、工場の作業場、倉庫、ロビーなど、電話機がユーザの通信デバイス セットの補助に過ぎない場所や、使用頻度が低い場所で使用するために設計された基本的な IP Phone です。Cisco Unified IP Phone 7906G および 7911G には、次の特徴があります。

- 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ィカルな表示。一連の基本的なビジネス機能に簡単にアクセス可能
- 1 つの電話番号で 6 つまでのコールをサポート
- インラインパワーのサポート（シスコ　インラインパワーと　IEEE　802.3af Power over Ethernet の両方）
- 次の内容を含む高度なセキュリティ機能のサポート
  - 製造元および現場でインストール可能な証明書
  - 安全なメディアおよびシグナリング
  - 設定の認証
- 高度なコール機能、および音声とテキストを使用する XML アプリケーションのサポート
- 統合された 10/100 Mbit イーサネット スイッチ。PC を接続し、設置場所ごとのケーブル配線を 1 本に集約可能（Cisco Unified IP Phone 7911G のみ）

図 1-1 に、Cisco Unified IP Phone 7906G および 7911G の主要コンポーネントを示します。

図 1-1　Cisco Unified IP Phone 7906G および 7911G

1	電話スクリーン	電話番号、コール ステータス、ソフトキーなどの電話機の機能を表示します。
2	Cisco Unified IP Phone の名称	Cisco Unified IP Phone のモデル シリーズを示します。
3	ソフトキー	電話スクリーンに表示された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は、短縮ダイヤルが表示されます。

5	アプリケーション メニュー ボタン 	ボイス メッセージ システム、電話のログとディレクトリ、設定、およびサービスにアクセスするための［アプリケーション］メニューを表示します。
6	保留ボタン 	アクティブなコールを保留にし、保留中のコールを再開します。アクティブなコールと保留中のコールを切り替えます。
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、および呼出音の音量を制御します。
9	ハンドセット	従来のハンドセットと同様に機能します。ハンドセットの上部にあるライト ストリップは、電話機の呼出音が鳴ると点滅し、新しいボイス メッセージがある場合は点灯したままになります（ボイス メッセージ システムによって異なります）。
10	フットスタンド	机上または卓上に、使用しやすい角度で電話機を設置できます。また、壁面取り付けのために取り外して、取り付けネジや Cisco Unified IP Phone 壁面取り付けキットを使用することもできます。

使用されるネットワーク プロトコル

Cisco Unified IP Phone は、音声通信で必要になるいくつか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。表 1-1 に、Cisco Unified IP Phone 7906G および 7911G がサポートしているネットワーク プロトコルの概要を示します。

表 1-1　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	使用上の注意
ブートストラップ プロトコル（BootP）	BootP は、特定の起動情報（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 Cisco Unified IP Phone に IP アドレスを割り当てている場合は、電話機のネットワーク設定にある［BOOTP サーバ］オプションが Yes になります。
シスコ検出プロトコル（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、他のデバイスの情報を受信することができます。	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、QoS（Quality of Service）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 はシスコ独自のプロトコルで、デバイスのピアツーピア階層を形成するために使用されます。また、CPPDP は、ピア デバイスから近接デバイスにファームウェアやその他のファイルをコピーするときにも使用されます。	CPPDP は、ピア ファームウェア共有機能で使用されます。

表 1-1　Cisco Unified IP Phone でサポートされるネットワーク プロトコル（続き）

ネットワーク プロトコル	目的	使用上の注意
Dynamic Host Configuration Protocol（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 を使用することをお勧めします。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 システム ガイド*』の「Cisco TFTP」の章を参照してください。
ハイパーテキスト転送プロトコル（HTTP）	HTTP は、インターネットや WWW 経由で情報を転送し、ドキュメントを移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。

表 1-1　Cisco Unified IP Phone でサポートされるネットワーク プロトコル（続き）

ネットワーク プロトコル	目的	使用上の注意
IEEE 802.1X	IEEE 802.1X 標準は、クライアント / サーバベースのアクセス制御および認証プロトコルを定義し、無許可のクライアントが公的にアクセス可能なポートを経由して LAN に接続することを禁止します。 クライアントが認証されるまでは、802.1X アクセス制御により、そのクライアントが接続されたポートを通過できるトラフィックは Extensible Authentication Protocol over LAN（EAPOL）トラフィックに制限されます。認証に成功すると、通常のトラフィックがポートを通過できるようになります。	Cisco Unified IP Phone は IEEE 802.1X 標準を実装し、802.1X 認証の EAP-MD5 オプションをサポートしています。 802.1X 認証を電話機で有効にした場合は、PC ポートおよびボイス VLAN を無効にする必要があります。詳細については、P.1-24 の「Cisco Unified IP Phone での 802.1X 認証のサポート」を参照してください。
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、個々の電話機がある場所で、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。
Link Layer Discovery Protocol（LLDP）	LLDP は、標準化されたネットワーク検出プロトコル（CDP に類似）で、一部のシスコ製およびサードパーティ製のデバイスでサポートされています。	Cisco Unified IP Phone では、LLDP は PC ポートでサポートされています。

表 1-1　Cisco Unified IP Phone でサポートされるネットワーク プロトコル（続き）

ネットワーク プロトコル	目的	使用上の注意
Link Layer Discovery Protocol-Media Endpoint Devices（LLDP-MED）	LLDP-MED は LLDP の標準機能を拡張したものであり、音声製品向けに開発されています。	Cisco Unified IP Phone では、LLDP-MED は SW ポートで次のような情報を通信するためにサポートされています。 • ボイス VLAN 設定 • デバイス検出 • 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 URL にある White Paper 『*LLDP-MED and Cisco Discovery Protocol*』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映像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）	RTCP は RTP と連動して、RTP ストリーム上で QoS データ（ジッタ、遅延、ラウンドトリップ遅延など）を伝送します。	RTCP は、デフォルトでは無効になっていますが、Cisco Unified Communications Manager を使用して電話機ごとに有効にすることができます。詳細については、P.4-36 の「ネットワークの設定」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）	SRTP は、RTP を使用する場合に付加的に使用できます。SRTP は、データの伝送中にメディア ストリームを暗号化することで、セキュリティを強化します。	SRTP が機能するには、コール先の電話機も 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電話機では、セキュア メディア ストリームを復号化できません。

表 1-1　Cisco Unified IP Phone でサポートされるネットワーク プロトコル（続き）

ネットワーク プロトコル	目的	使用上の注意
セッション開始プロトコル（SIP）	SIP は、IP を介したマルチメディア会議のためのインターネット技術特別調査委員会（IETF）標準です。SIP は、RFC 3261 で定義されている ASCII ベースのアプリケーション層プロトコルです。このプロトコルを使用して、2 つまたはそれ以上のエンドポイント間でコールを確立、維持、および終了することができます。	他の VoIP プロトコルと同様に、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 コールのアトリビュートを制御する機能を提供することです。 Cisco Unified IP Phone は、SIP を使用するように設定することも、Skinny Client Control Protocol（SCCP）を使用するように設定することもできます。
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、シスコシステムズ独自のものです。	Cisco Unified IP Phone では、コール制御に SCCP を使用します。Cisco Unified IP Phone は、SCCP を使用するように設定することも、セッション開始プロトコル（SIP）を使用するように設定することもできます。
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 機能のみ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。

表 1-1　Cisco Unified IP Phone でサポートされるネットワーク プロトコル（続き）

ネットワーク プロトコル	目的	使用上の注意
Transmission Control Protocol（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。
Transport Layer Security（TLS）	TLS は、通信をセキュリティで保護し、認証するための標準プロトコルです。	セキュリティを実装すると、Cisco Unified IP Phone は TLS を使用して、Cisco Unified Communications Manager への登録をセキュリティで保護します。
Trivial File Transfer Protocol（TFTP）	TFTP を使用すると、ファイルをネットワーク経由で転送することができます。 Cisco Unified IP Phone で TFTP を使用すると、電話タイプ固有の設定ファイルを取得できます。	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。ネットワーク上で複数の TFTP サーバが動作している場合は、電話機ごとに、TFTP サーバを手動でローカルに割り当てる必要があります。
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。

関連項目

- 他の Cisco Unified Communications 製品との連携について（P.2-2）
- 電話機の起動プロセスについて（P.2-10）
- ネットワークの設定メニュー（P.4-9）

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。従来のテレフォニー機能に加えて、各 Cisco IP Phone は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。

この項では、次のトピックについて取り上げます。

機能の概要

Cisco Unified IP Phone は、コール転送や転送、リダイヤル、短縮ダイヤル、会議コール、ボイス メッセージ システムへのアクセスなど、基本的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 がサポートしているテレフォニー機能の概要については、P.5-2 の「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。

Cisco Unified IP Phone は、他のネットワーク デバイスと同様に、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 を使用すると、電話機上で設定する設定値が少なくなりますが、必要に応じて、IP アドレス、TFTP サーバ、およびサブネット マスクを手動で設定することもできます。Cisco Unified IP Phone 上でネットワーク設定値を設定する手順については、第 4 章「Cisco Unified IP Phone の設定値の設定」を参照してください。

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 IP Phone 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。また、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。これらのサービスの設定については、P.5-21 の「社内ディレクトリとパーソナル ディレクトリの設定」およびP.5-25 の「サービスのセットアップ」を参照してください。

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 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。詳細については、第 7 章「Cisco Unified IP Phone のモデル情報、ステータス、および統計の表示」を参照してください。

関連項目

- Cisco Unified IP Phone の設定値の設定（P.4-1）
- 機能、テンプレート、サービス、およびユーザの設定（P.5-1）
- トラブルシューティングおよびメンテナンス（P.9-1）

テレフォニー機能の設定

Cisco Unified IP Phone の一部の設定値は、Cisco Unified Communications Manager の管理ページ アプリケーションで変更することができます。この Web ベース 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などを行うことができます。詳細については、P.5-2 の「Cisco Unified IP Phone で使用可能なテレフォニー機能」および『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。

Cisco Unified Communications Manager の管理ページ アプリケーションの詳細については、Cisco Unified Communications Manager のマニュアル（『*Cisco Unified Communications Manager システム ガイド*』など）を参照してください。また、このページ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 のマニュアル一式には、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

関連項目

- Cisco Unified IP Phone で使用可能なテレフォニー機能（P.5-2）

Cisco Unified IP Phone でのネットワーク パラメータの設定

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。

電話機で機能を設定し、統計情報を表示する方法については、第 4 章「Cisco Unified IP Phone の設定値の設定」および第 7 章「Cisco Unified IP Phone のモデル情報、ステータス、および統計の表示」を参照してください。

ユーザへの機能情報の提供

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。次の Cisco Unified IP Phone 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、クイック リファレンスを含む各種のユーザ ガイドにアクセスできます。

重要なのは、ユーザにマニュアルを提供することのほかに、使用可能な Cisco Unified IP Phone の機能を伝えること（企業やネットワーク独自の機能を含む）、およびそれらの機能にアクセスし、必要に応じてカスタマイズする方法を教えることです。

システム管理者が電話機のユーザに提供する必要のある重要な情報の要約については、付録 A「ユーザへの情報提供」を参照してください。

Cisco Unified IP Phone のセキュリティ機能について

Cisco Unified Communications Manager システムにセキュリティを実装すると、電話機と Cisco Unified Communications Manager サーバの ID 盗用や、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を防止できます。

これらの脅威を軽減するため、Cisco Unified Communications ネットワークは、電話機とサーバの間に認証済みの暗号化通信ストリームを確立し、維持します。ファイルはデジタル署名してから電話機に転送し、Cisco Unified IP Phone 間では、メディア ストリームを暗号化します。

セキュリティ関連の設定値を Cisco Unified Communications Manager の管理ページで設定すると、電話機の設定ファイルには機密情報が保持されます。設定ファイルのプライバシーを確保するには、ファイルに暗号化を設定する必要があります。詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』の「暗号化された電話機設定ファイルの設定」の章を参照してください。

表 1-2 に、このマニュアルおよび他のマニュアルで、セキュリティに関する詳細情報が記載された箇所を示します。

表 1-2　Cisco Unified IP Phone のセキュリティに関するトピック

トピック	参照先
セキュリティの詳細な説明（Cisco Unified Communications Manager および Cisco Unified IP Phone のセットアップ、設定、およびトラブルシューティングに関する情報を含む）	『*Cisco Unified Communications Manager セキュリティ ガイド*』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	P.1-16 の「サポートされているセキュリティ機能の概要」を参照してください。
セキュリティ機能に関する制限事項	P.1-27 の「セキュリティに関する制限事項」を参照してください。
セキュリティが実装された電話コールの識別	P.1-20 の「暗号化された電話コールと認証された電話コールの識別」を参照してください。
Transport Layer Security（TLS）接続	• P.1-5 の「使用されるネットワーク　プロトコル」を参照してください。 • P.2-8 の「電話機の設定ファイルについて」を参照してください。

表 1-2　Cisco Unified IP Phone のセキュリティに関するトピック（続き）

トピック	参照先
Cisco Unified IP Phone の 802.1X 認証	次の項を参照してください。 • P.1-24 の「Cisco Unified IP Phone での 802.1X 認証のサポート」 • P.4-42 の「セキュリティ設定メニュー」 • P.4-48 の「802.1X 認証およびステータス」 • P.9-14 の「Cisco Unified IP Phone のセキュリティのトラブルシューティング」
セキュリティおよび電話機の起動プロセス	P.2-10 の「電話機の起動プロセスについて」を参照してください。
セキュリティおよび電話機の設定ファイル	P.2-8 の「電話機の設定ファイルについて」を参照してください。
セキュリティが実装されている場合の［TFTP サーバ 1］オプションまたは［TFTP サーバ 2］オプションの電話機による変更	P.4-9 の「ネットワークの設定メニュー」を参照してください。
電話機の［デバイス設定］メニューにある［CallManager 1］～［CallManager 5］オプションのセキュリティ アイコンの意味	P.4-18 の「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］メニューからアクセスする［セキュリティ設定］メニューの項目	P.4-34 の「セキュリティ設定メニュー」を参照してください。
電話機の［設定］メニューからアクセスする［セキュリティ設定］メニューの項目	P.4-42 の「セキュリティ設定メニュー」を参照してください。
証明書信頼リスト（CTL）ファイルのロック解除	P.4-44 の「CTL ファイル画面」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	P.8-5 の「Web ページへのアクセスの無効化および有効化」を参照してください。
トラブルシューティング	• P.9-14 の「Cisco Unified IP Phone のセキュリティのトラブルシューティング」を参照してください。 • 『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。

表 1-2　Cisco Unified IP Phone のセキュリティに関するトピック（続き）

トピック	参照先
電話機からの CTL ファイルの削除	P.9-21 の「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旧	P.9-21 の「Cisco Unified IP Phone のリセットまたは復元」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。 • P.1-24 の「Cisco Unified IP Phone での 802.1X 認証のサポート」 • P.4-48 の「802.1X 認証およびステータス」 • P.9-14 の「Cisco Unified IP Phone のセキュリティのトラブルシューティング」

サポートされているセキュリティ機能の概要

この項では、電話機がサポートしているセキュリティ機能の概要を示します。これらの機能および Cisco Unified Communications Manager と Cisco Unified IP Phone のセキュリティの詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』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］メニューを確認してください（**アプリケーション メニュー** ボタンを押し、**［設定］**>**［セキュリティ設定］**を選択するか、**［設定］**>**［デバイス設定］**>**［セキュリティ設定］**を選択します）。詳細については、第 4 章「Cisco Unified IP Phone の設定値の設定」を参照してください。

（注） セキュリティ機能のほとんどは、証明書信頼リスト（CTL）が電話機にインストールされている場合のみ使用できます。CTL の詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。

表 1-3　セキュリティ機能の概要

機能	説明
イメージの認証	署名付きのバイナリ ファイル（拡張子 .sbn）によって、ファームウェア イメージが電話機へのロード前に改ざんされることを防止します。イメージが改ざんされている場合、電話機は認証プロセスに不合格として、新しいイメージを拒否します。
802.1X 認証	Cisco Unified IP Phone では、ネットワークへのアクセスを要求および実行するときに、802.1X 認証を使用できます。詳細については、P.1-24 の「Cisco Unified IP Phone での 802.1X 認証のサポート」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 には、デバイス認証のためにそれぞれ一意の証明書が必要です。電話機には、Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）が組み込まれていますが、セキュリティを強化するには、Cisco Unified Communications Manager の管理ページで、Certificate Authority Proxy Function（CAPF; 認証局プロキシ関数）を使用して証明書をインストールすることを指定します。また、電話機の［セキュリティ設定］メニューから Locally Significant Certificate（LSC; ローカルで有効な証明書）をインストールすることもできます。詳細については、P.3-19 の「Cisco Unified IP Phone でのセキュリティの設定」を参照してください。
デバイスの認証	Cisco Unified Communications Manager サーバと電話機の間で、各エンティティが他方のエンティティの証明書を受け付けるときに発生します。電話機と Cisco Unified Communications Manager の間にセキュアな接続が必要かどうかを判別し、必要な場合には、Transport Layer Security（TLS）プロトコルを使用してエンティティ間にセキュア シグナリング パスを作成します。Cisco Unified Communications Manager は、電話機が Cisco Unified Communications Manager によって認証されない限り、認証済みモードまたは暗号化済みモードに設定された電話機を登録しません。
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付きファイルを確認します。電話機は、ファイルが作成後に改ざんされていないことを、署名を確認することで確認します。認証に失敗したファイルは、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、以降の処理を実行しません。

表 1-3　セキュリティ機能の概要（続き）

機能	説明
シグナリングの認証	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確認します。
製造元でインストールされる証明書	各 Cisco Unified IP Phone 7906G および 7911G には、一意の MIC が組み込まれており、この MIC はデバイスの認証に使用されます。MIC は、電話機の ID が永続的に一意であることの証明になり、Cisco Unified Communications Manager で電話機を認証できるようにします。
セキュアな SRST 参照先 （SCCP 電話機のみ）	Cisco Unified Communications Manager の管理ページで SRST 参照先のセキュリティを設定してから従属デバイスをリセットすると、TFTP サーバが SRST 証明書を電話機の cnf.xml ファイルに追加し、ファイルを電話機に送信します。これで、セキュアな電話機は、TLS 接続を使用して SRST 対応ルータと対話するようになります。
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 ストリームが安全であること、およびデータを受信して読み取るのが、意図したデバイスのみであることを保証します。この処理には、デバイスで使用されるメディア マスター キー ペアの作成、デバイスへのキーの配信、キー伝送中のキー配送の保護が含まれます。
シグナリングの暗号化 （SCCP 電話機のみ）	デバイスと Cisco Unified Communications Manager サーバの間で送信される、すべての SCCP シグナリング メッセージを確実に暗号化します。
CAPF（認証局プロキシ関数）	電話機に非常に高い処理負荷がかかる、証明書の生成手順を一部実装して、キーの生成および証明書のインストールで電話機と連携します。CAPF は、証明書を電話機に代わってお客様指定の認証局から要求するように設定することも、証明書をローカルに生成するように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 Web ページに対するアクセスを禁止できます。この Web ページには、電話機に関する各種の動作統計情報が表示されます。

表 1-3　セキュリティ機能の概要（続き）

機能	説明
電話機のセキュリティ強化	Cisco Unified Communications Manager の管理ページから制御する追加セキュリティ オプション。 • PC ポートの無効化（7911G のみ）。 • Gratuitous Address Resolution Protocol（GARP）の無効化。 • PC ボイス LAN アクセスの無効化（7911G のみ）。 • ［設定］メニューへのアクセスの無効化。または、［ユーザ設定］メニューにアクセスすること、音量の変更を保存することのみ可能な、限定的なアクセスの提供 • 電話機の Web ページへのアクセスの無効化。 **（注）** ［PC ポートを無効にする］、［GARP を使う］、および［ボイス VLAN を使う］の各オプションの現在の設定値は、電話機の［セキュリティ設定］メニューを表示することで確認できます。詳細については、P.4-18 の「デバイス設定メニュー」を参照してください。

関連項目

- 暗号化された電話コールと認証された電話コールの識別（P.1-20）
- Cisco Unified IP Phone での 802.1X 認証のサポート（P.1-24）
- セキュリティに関する制限事項（P.1-27）
- デバイス設定メニュー（P.4-18）

セキュリティ プロファイルについて

Cisco Unified Communications Manager 5.0 以降をサポートしている Cisco Unified IP Phone は、すべてセキュリティ プロファイルを使用します。このプロファイルは、電話機がセキュリティ保護、認証、または暗号化の対象になるかどうかを定義するものです。セキュリティ プロファイルの設定、および電話機へのプロファイルの適用については、『*Cisco Unified Communications Manager セキュリティ ガイド*』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 モードを表示するには、[セキュリティ設定] メニューで [セキュリティモード] の設定を参照します。詳細については、P.4-34 の「セキュリティ設定メニュー」の項を参照してください。

関連項目

- 暗号化された電話コールと認証された電話コールの識別（P.1-20）
- セキュリティに関する制限事項（P.1-27）

暗号化された電話コールと認証された電話コールの識別

電話機にセキュリティを実装している場合は、電話機の LCD スクリーンに表示されるアイコンによって、認証された電話コールや暗号化された電話コールを識別できます。

認証されたコールでは、コールの確立に参加するすべてのデバイスが、Cisco Unified Communications Manager によって認証されています。処理中のコールがエンドツーエンドで認証されている場合は、電話機の LCD スクリーンの通話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。

暗号化されたコールでは、コールの確立に参加するすべてのデバイスが、Cisco Unified Communications Manager によって認証されています。さらに、コール 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、最高レベルのセキュリティを提供し、コールに整合性とプライバシーを提供します。処理中のコールが暗号化されているときは、電話機の LCD スクリーンの通話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）　IP 以外のコール レッグ（PSTN など）を通じてルーティングされるコールは、IP ネットワーク内で暗号化されてロック アイコンが関連付けられている場合でも、セキュリティ保護されません。

関連項目

- Cisco Unified IP Phone のセキュリティ機能について（P.1-14）
- Cisco Unified IP Phone での 802.1X 認証のサポート（P.1-24）
- セキュリティに関する制限事項（P.1-27）

セキュアな会議コールの確立と識別

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（暗号化済みまたは認証済みセキュリティ　モード）で会議を開始します。
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（暗号化済みまたは認証済み）を確認し、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。セキュアな会議の場合は、電話スクリーン上の「会議」の右側に（暗号化済み）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た場合、会議は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 レベルに影響を及ぼす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、表 1-4 および表 1-5 を参照してください。

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。表 1-4 は、割り込み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 1-4　割り込み使用時のコール セキュリティの連携動作

会議開催者の電話機のセキュリティ レベル	使用する機能	コールのセキュリティ レベル	動作結果
非セキュア	割り込み	暗号化されたコール	コールは割り込みを受け、非セキュアなコールとして識別されます。
セキュア（暗号化済み）	割り込み	認証されたコール	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。
セキュア（認証済み）	割り込み	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	割り込み	認証されたコール	コールは割り込みを受け、非セキュアなコールとして識別されます。

表 1-5 は、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 1-5　会議コールに対するセキュリティの制限事項

会議開催者の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 人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。

表 1-5　会議コールに対するセキュリティの制限事項（続き）

会議開催者の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
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。 暗号化済みレベルのセキュアな会議。
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だけが使用可能になり、使用されます。 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だけが使用可能になり、使用されます。 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ます。 1 人の参加者が MOH を使用してコールを保留にしようとしても、MOH は再生されません。
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。 会議はセキュアに保たれます（暗号化済みまたは認証済み）。
非セキュア	C 割り込み	すべての参加者が暗号化済み	セキュアな会議ブリッジ。 会議は非セキュアに変更されます。
非セキュア	ミートミー	最小セキュリティ レベルは、暗号化済み	会議開催者に「Does not meet Security Level」というメッセージが表示され、コールが拒否されます。

表 1-5　会議コールに対するセキュリティの制限事項（続き）

会議開催者の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
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ます。
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、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、使用されます。 会議はすべてのコールを受け入れます。

Cisco Unified IP Phone での 802.1X 認証のサポート

次の各項では、Cisco Unified IP Phone での 802.1X サポートについて説明します。

- 概要（P.1-24）
- 必要なネットワーク コンポーネント（P.1-25）
- ベスト プラクティス：要件と推奨事項（P.1-25）

概要

Cisco Unified IP Phone と Cisco Catalyst スイッチでは、相互に識別し、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判別するために、シスコ検出プロトコル（CDP）を従来使用しています。ただし、CDP は、ローカルに接続された PC を識別するときには使用されません。そのため、Cisco Unified IP Phone には EAPOL パススルー メカニズムが組み込まれています。このメカニズムにより、IP Phone にローカルに接続された PC は、LAN スイッチ内の 802.1X オーセンティケータに EAPOL メッセージをパススルーできます。この機能によって、IP Phone はオーセンティケータとして動作する必要がなくなります。この場合でも、LAN スイッチはネットワークに接続しようとするデータ エンドポイントを認証できます。

Cisco Unified IP Phone には、EAPOL パススルー メカニズムとともに、EAPOL-Logoff メカニズムも組み込まれています。ローカルに接続された PC が IP Phone から切断された場合、LAN スイッチは物理リンクの障害を認識しません。これは、LAN スイッチと IP Phone 間のリンクが保持されているためです。ネットワークの整合性が損なわれないようにするために、ダウンストリーム PC に代わって IP Phone が EAPOL-Logoff メッセージをスイッチに送信します。その結果、LAN スイッチがダウンストリーム PC の認証エントリをクリアします。

EAPOL パススルー メカニズムに加えて、Cisco Unified IP Phone には、802.1X サプリカントも組み込まれています。このサプリカントを使用すると、ネットワーク管理者は IP Phone から LAN スイッチ ポートへの接続を制御できます。IP Phone の 802.1X サプリカントには、802.1X 認証の EAP-MD5 オプションが実装されています。

必要なネットワーク コンポーネント

Cisco Unified IP Phone で 802.1X 認証をサポートするには、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動作します。このサプリカントは、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）（またはサードパーティ製の認証サーバ）：認証サーバと電話機の両方に、電話機を認証するための共有シークレットが設定されている必要があります。
- Cisco Catalyst スイッチ（またはサードパーティ製のスイッチ）：スイッチは 802.1X をサポートして、*オーセンティケータ*として動作し、電話機と認証サーバ間でメッセージを通過させることができる必要があります。メッセージ交換が完了すると、スイッチは電話機に対してネットワークへ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 認証を有効にする：802.1X 標準を使用して Cisco Unified IP Phone を認証する場合は、電話機で 802.1X 認証を有効にする前に、他のコンポーネントを正しく設定したことを確認します。詳細については、P.4-48 の「802.1X 認証およびステータス」を参照してください。

- PC ポートを設定する：802.1X 標準では VLAN の使用は考慮されていないため、特定のスイッチ ポートに対して認証するデバイスは 1 つに制限することをお勧めします。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。PC を電話機の PC ポートに接続できるかどうかは、スイッチの設定で決まります。
  - 有効：マルチドメイン認証をサポートするスイッチを使用する場合は、PC ポートを有効にして、PC を接続することができます。この場合、Cisco Unified IP Phone はプロキシ EAPOL-Logoff をサポートし、接続された PC とスイッチ間の認証交換をモニタします。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：スイッチが同じポートで複数の 802.1X 準拠デバイスをサポートしていない場合、802.1X 認証を有効にしたときは、PC ポートを無効にする必要があります。詳細については、P.4-34 の「セキュリティ設定メニュー」を参照してください。このポートを無効にしないで PC を接続した場合は、スイッチによって、電話機と PC の両方へのネットワーク アクセスが拒否されます。
- ボイス VLAN を設定する：802.1X 標準では VLAN が考慮されていないため、この設定はスイッチのサポート状況に基づいて行う必要があります。
  - 有効：マルチドメイン認証をサポートするスイッチを使用する場合は、ボイス VLAN を継続して使用できます。
  - 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、ポートをネイティブ VLAN に割り当てることを検討します。詳細については、P.4-34 の「セキュリティ設定メニュー」を参照してください。
- MD5 共有シークレットを入力する：802.1X 認証を無効にした場合や、電話機で工場出荷時の状態にリセットした場合、以前に設定した MD5 共有シークレットは削除されます。詳細については、P.4-48 の「802.1X 認証およびステータス」を参照してください。

セキュリティに関する制限事項

ユーザは、割り込みに使用する電話機が暗号化用に設定されていない場合、暗号化されたコールには割り込めません。この場合、割り込みを開始した側の電話機では、割り込みが失敗した時点でリオーダー トーン（ファースト ビジー トーン）が再生されます。

割り込みを開始する側の電話機が暗号化用に設定されている場合、割り込みを開始するユーザは、認証されたコールや安全でないコールに対して、暗号化された電話機から割り込むことができます。割り込みが発生すると、Cisco Unified Communications Manager はそのコールを安全でないコールに分類します。

割り込みを開始する側の電話が暗号化用に設定されている場合、割り込みを開始するユーザは、暗号化されたコールに割り込むことができます。電話機には、コールが暗号化されていることが示されます。

ユーザは、割り込みに使用する電話機が安全でない場合でも、認証されたコールに割り込むことができます。割り込みを開始する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、そのコールの認証済みデバイスでは、認証アイコンが引き続き表示されます。

Cisco Unified IP Phone の設定および設置の概要

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。Cisco Unified Communications ネットワークのひととおりのセットアップと設定、およびそのチェックリストについては、『*Cisco Unified Communications Manager システム ガイド*』の「システム コンフィギュレーションの概要」の章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 IP Phone をネットワークに追加する手順の概要については、次の各トピックで説明します。

- Cisco Unified Communications Manager での Cisco Unified IP Phone の設定（P.1-28）
- Cisco Unified IP Phone の設置（P.1-35）

Cisco Unified Communications Manager での Cisco Unified IP Phone の設定

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 Communications Manager の管理ページ
- 一括管理ツール（BAT）
- BAT と Tool for Auto-Registered Phones Support（TAPS）

これらの方法の詳細については、P.2-12 の「Cisco Unified Communications Manager データベースへの電話機の追加」を参照してください。

電話機を Cisco Unified Communications Manager で設定する方法の概略については、『*Cisco Unified Communications Manager システム ガイド*』の「Cisco Unified IP Phone」の章、および『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「Cisco Unified IP Phone の設定」の章を参照してください。

Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G の設定に関するチェックリスト

表 1-6 に、Cisco Unified Communications Manager で Cisco Unified IP Phone 7906G および 7911G を設定する作業について、概要およびチェックリストを示します。このリストは、お勧めする作業順序を表しており、電話機の設定プロセスについて順に解説しています。一部の作業は、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、リストに示した資料を参照してください。

表 1-6　Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G の設定に関するチェックリスト

設定の手順と目的		参照先
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 スペースとロケーションの情報（使用する場合） • 回線の数、および電話機に割り当てる関連電話番号（DN）とパーティション • 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 電話機をセットアップするための設定要件のリストを作成します。 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。	『*Cisco Unified Communications Manager システム ガイド*』の「Cisco Unified IP Phone」の章を参照してください。 P.5-2 の「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。

表 1-6　Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G の設定に関するチェックリスト（続き）

設定の手順と目的		参照先
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。 ユーザのニーズに応じてプライバシー機能を追加します。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「電話ボタン テンプレートの設定」の章を参照してください。 P.5-23 の「電話ボタン テンプレートの変更」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） • 電話ボタンテンプレート（Phone 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）（カスタマイズした場合） 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。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「Cisco Unified IP Phone の設定」の章を参照してください。 ［プロダクト固有の設定（Product Specific Configuration）］のフィールドについては、［電話の設定（Phone Configuration）］ウィンドウの ？ボタン ヘルプを参照してください。

表 1-6　Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G の設定に関するチェックリスト（続き）

設定の手順と目的		参照先
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、電話機の電話番号を追加および設定します。 • 電話番号（Directory Number） • デバイス x の複数コール / コール待機設定（Multiple Call/Call Waiting Settings on Device x） • コール転送とコールピックアップの設定（Call Forward and Call Pickup Settings）（使用する場合） • ボイスメッセージング（使用する場合） 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。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の次の項を参照してください。 • 「電話番号の設定」の章 • 「Cisco Unity または Cisco Unity Connection ボイスメールボックスの作成」の章 P.5-2 の「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（オプション）。 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。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「ソフトキー テンプレートの設定」の章を参照してください。 P.5-24 の「ソフトキー テンプレートの設定」を参照してください。
ステップ 6	短縮ダイヤル ボタンを設定し、短縮ダイヤル番号を割り当てます（オプション）。 短縮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、短縮ダイヤルの設定値を電話機上で変更できます。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「Cisco Unified IP Phone サービスの設定」の章の「短縮ダイヤル ボタンの設定」の項を参照してください。

表 1-6　Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G の設定に関するチェックリスト（続き）

設定の手順と目的		参照先
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（オプション）。 IP Phone サービスを提供します。 **（注）** ユーザは、Cisco Unified Communications Manager ユーザ オプションを使用することで、サービスを電話機上で追加または変更できます。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「IP Phone サービスの設定」の章を参照してください。 P.5-25 の「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（オプション）。 IP Phone のサービスや URL にボタン 1 つでアクセスできるようにします。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「IP Phone サービスの設定」の章の「IP Phone サービスの電話ボタンへの追加」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（オプション）。 • 姓（Last Name） • ユーザ ID（User ID） • パスワード（Password）（ユーザ オプション Web ページ用） • PIN（PIN、半角数字のみ）（エクステンション モビリティで使用） ユーザ情報を Cisco Unified Communications Manager のグローバル ディレクトリに追加します。 **（注）** ユーザを社内ディレクトリ内で検索するには、ユーザを Cisco Unified Communications Manager に追加する必要があります。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「エンド ユーザの設定」の章を参照してください。 P.5-26 の「Cisco Unified Communications Manager へのユーザの追加」を参照してください。

表 1-6　Cisco Unified Communications Manager での Cisco Unified IP Phone 7906G および 7911G の設定に関するチェックリスト（続き）

設定の手順と目的		参照先
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、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。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「ユーザ グループの設定」の章の「ユーザ グループへのユーザの追加」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（オプション）。 コールの転送、短縮ダイヤル番号やサービスの追加などについて、ユーザが電話機を制御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。	『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「エンド ユーザの設定」の章にある「エンド ユーザとデバイスとの関連付け」の項を参照してください。

Cisco Unified IP Phone の設置

Cisco Unified Communications Manager データベースに電話機を追加した後は、電話機を設置できる状態になります。電話機は、管理者（または電話機のユーザ）がユーザの作業場所に設置します。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は、Cisco.com で入手可能な『*Cisco Unified IP Phone Installation Guide*』に記載されています。

（注） 電話機は、新品の場合でも、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 にある電話機モデルの 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 テーブルや電話番号を変更するなど、電話機の特定の設定情報をアップデートする必要があります。

Cisco Unified IP Phone 7906G および 7911G の設置に関するチェックリスト

表 1-7 に、Cisco Unified IP Phone 7906G および 7911G を設置する作業について、概要およびチェックリストを示します。このリストは、お勧めする作業順序を表しており、電話機の設置プロセスについて順に解説しています。一部の作業は、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、リストに示した資料を参照してください。

表 1-7　Cisco Unified IP Phone 7906G および 7911G の設置に関するチェックリスト

設置の手順と目的		参照先
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する。	P.2-5 の「Cisco Unified IP Phone 7906G および 7911G への電力供給」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する。	P.3-10 の「Cisco Unified IP Phone の設置」を参照してください。 P.3-10 の「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する。	P.3-17 の「電話機の起動プロセスの確認」を参照してください。
ステップ 4	電話機で［**設定**］>［**ネットワークの設定**］を選択して、次のネットワーク設定値を設定します。 **（注）** これらの変更を電話機から行うには、電話機の設定のロックを解除する必要があります。 DHCP を有効にする場合： **1.** ［DHCP を使う］を［**Yes**］に設定する。 **2.** 代替 TFTP サーバを使用するには、［代替 TFTP］を［**Yes**］に設定する。［TFTP サーバ 1］に IP アドレスを入力する。	P.3-18 の「起動時のネットワーク設定値の設定」を参照してください。 P.4-9 の「ネットワークの設定メニュー」を参照してください。

表 1-7　Cisco Unified IP Phone 7906G および 7911G の設置に関するチェックリスト（続き）

設置の手順と目的		参照先
	DHCP を無効にする場合： 1. ［DHCP を使う］を［**No**］に設定する。 2. 電話機のスタティック IP アドレスを入力する。 3. サブネット マスクを入力する。 4. デフォルト ルータの IP アドレスを入力する。 5. 電話機が配置されるドメイン名を入力する。 6. ［代替 TFTP］を［**Yes**］に設定する。 ［TFTP サーバ 1］に IP アドレスを入力する。 DHCP を使用する場合：IP アドレスが自動的に割り当てられ、Cisco Unified IP Phone に TFTP サーバが指定されます。 **（注）** DHCP で割り当てられる TFTP サーバを使用する代わりに、代替 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連絡してください。 DHCP を使用しない場合：IP アドレス、TFTP サーバ、サブネット マスク、ドメイン名、およびデフォルト ルータを電話機の場所で設定する必要があります。	
ステップ 5	電話機にセキュリティを設定します。 データ改ざんの脅威や、電話機の ID 盗用から保護します。	P.3-19 の「Cisco Unified IP Phone でのセキュリティの設定」を参照してください。

表 1-7　Cisco Unified IP Phone 7906G および 7911G の設置に関するチェックリスト（続き）

設置の手順と目的		参照先
ステップ 6	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。	『*Cisco Unified IP Phone 7906G/7911G 電話ガイド*』を参照してください。
ステップ 7	エンド 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。	付録 A「ユーザへの情報提供」を参照してください。