



CHAPTER 1

Cisco Unified IP Phone の概要

Cisco Unified IP Phone 6901 および 6911 は、Internet Protocol (IP; インターネット プロトコル) ネットワークでの音声通信を提供します。Cisco Unified IP Phone は、デジタル ビジネス フォンとほぼ同様に機能し、コールの発信および受信に利用できます。また、次の機能も備えています。

- Cisco Unified IP Phone 6901 は、保留、リダイヤル、転送、および会議などの基本機能をサポートします。
- Cisco Unified IP Phone 6911 は、ミュート、保留、転送、会議、短縮ダイヤル、コール転送、等々の機能をサポートします。

Cisco Unified IP Phone は、他のネットワーク デバイスと同様、設定と管理が必要です。これらの電話機は、G.711a、G.711 μ 、G.729a、iLBC をエンコードし、G.711a、G.711 μ 、G.729、G.729ab、および iLBC をデコードします。

この章は、次の項で構成されています。

- 「[Cisco Unified IP Phone 6901 および 6911 について](#)」 (P.1-2)
- 「[使用されるネットワーク プロトコル](#)」 (P.1-6)
- 「[Cisco Unified IP Phone 6901 および 6911 でサポートされる機能](#)」 (P.1-9)
- 「[Cisco Unified IP Phone の設定および設置の概要](#)」 (P.1-19)
- 「[用語の違い](#)」 (P.1-23)



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 6901 および 6911 について

図 1-1 に、Cisco Unified IP Phone 6901 の主要コンポーネントを示します。

図 1-1 Cisco Unified IP Phone 6901



表 1-1 に、Cisco Unified IP Phone 6901 のボタンについて説明します。

表 1-1 Cisco Unified IP Phone 6901 の機能





1	フックスイッチ	電話機の機能（フックフラッシュ）をアクティブにします。
2	保留ボタン 	アクティブ コールを保留します。
3	リダイヤル ボタン 	最後にダイヤルした番号をダイヤルします。
4	回線ボタン 	<p>2 番めの着信コールのピックアップに使用します。回線ボタンの LED は、コールのステータスを示します。</p> <p>回線ボタンを使用することで、ユーザは着信コールに応答し、回線上の 2 つのコールを切り替えることができます。回線ボタンに関連付けられた LED が、回線のステータスを反映して点灯します。</p> <p>回線ボタンの点灯は、次のステータスを示します。</p> <ul style="list-style-type: none"> • 緑、点灯：アクティブ コール • 緑、点滅：保留中のコール • オレンジ、点滅：着信コール • オレンジ、点灯：不在転送がアクティブ • 赤、点灯：リモート回線が使用中（共有回線） • 赤、点滅：リモート回線が保留中
5	音量ボタン 	ハンドセットおよび呼出音の音量を制御します（オンフック）。
6	キーパッド	電話番号、*、# のダイヤル、およびメニュー項目の選択（項目番号を入力）に使用します。
7	ハンドセットのライトストリップ	コールの呼び出し（赤の点滅）または新しい音声メッセージ（赤の点灯）を通知します。




図 1-2 に、Cisco Unified IP Phone 6911 の主要コンポーネントを示します。







図 1-2 Cisco Unified IP Phone 6911




表 1-2 に、Cisco Unified IP Phone 6911 のボタンについて説明します。

表 1-2 Cisco Unified IP Phone 6911 の機能

1	ハンドセットのライトストリップ	コールの呼び出し（赤の点滅）または新しい音声メッセージ（赤の点灯）を通知します。
2	電話機テンプレート	名前や連絡先番号を入力できる紙片です。
3	転送ボタン 	コールを転送します。
4	会議ボタン 	会議コールを開始します。
5	保留ボタン 	アクティブ コールを保留します。

6	回線ボタン 	<p>着信コールのピックアップに使用します。回線ボタンの LED は、コールのステータスを示します。</p> <p>回線ボタンを使用することで、ユーザは着信コールに応答し、回線上の 2 つのコールを切り替えることができます。回線ボタンに関連付けられた LED が、回線のステータスを反映して点灯します。</p> <p>回線ボタンの点灯は、次のステータスを示します。</p> <ul style="list-style-type: none"> • 緑、点灯：アクティブ コール • 緑、点滅：保留中のコール • オレンジ、点滅：着信コール • オレンジ、点灯：不在転送がアクティブ • 赤、点灯：リモート回線が使用中（共有回線） • 赤、点滅：リモート回線が保留中
7	スピーカーフォンボタン 	<p>デフォルトの音声パスとしてスピーカーフォンを選択して、新しいコールを開始したり、着信コールをピックアップしたり、コールを終了したりします。コールの最中は、ボタンが緑色に点灯します。スピーカーフォン音声パスは、新しいデフォルト音声パスを選択する（たとえば、ハンドセットをピックアップする）まで変更されません。</p>
8	キーパッド	<p>電話番号、*、# のダイヤル、およびメニュー項目の選択（項目番号を入力）に使用します。</p>
9	ミュート ボタン 	<p>マイクロフォン モードのオン/オフを切り替えます。マイクロフォンがミュートになっているとき、ボタンは赤色に点灯します。</p>
10	音量ボタン 	<p>ハンドセットとスピーカーフォンの音量（オフフック）、および呼出音の音量（オンフック）を制御します。</p>
11	メッセージ ボタン 	<p>ボイス メッセージ サービスを自動的にダイヤルします（サービスによって異なります）。</p>
12	リダイヤル 	<p>最後にダイヤルした番号をダイヤルします。</p>

13	機能ボタン 	Cisco Unified Communications Manager での電話機の設定に応じて、プログラム可能な機能ボタンを利用して短縮ダイヤル、コール転送、ピックアップ、グループ ピックアップ、およびミーティングの各機能にアクセスできます。ユーザは、機能キーに最大 9 つの項目を設定できます。これらの各機能にアクセスするには、機能キーと、その機能に関連付けられた番号を順に押します。機能キーを押してから 5 秒以内に番号を押す必要があります。番号は、1 ~ 9 までの 1 桁のみです。 これらの機能には、オフフックでもオンフックでもアクセスできます。 <ul style="list-style-type: none"> • コール転送：コールを転送できます。 • ピックアップ：サードパーティ製の電話機でコールをピックアップできません。 • グループ ピックアップ：グループ内のコールをピックアップできます。 • ミーティング：会議を設定できます。 • 短縮ダイヤル：以前に保存した特定の番号をダイヤルできます。
14	ハンドセット	電話機のハンドセットです。

使用されるネットワーク プロトコル

Cisco Unified IP Phone は、音声通信に必須の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 1-3 では、Cisco Unified IP Phone 6901 および 6911 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 1-3 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
Cisco Audio Session Tunneling (CAST) (Cisco Unified IP Phone 6911 のみ)	CAST プロトコルの利用により、IP Phone とその電話機の背後にある関連アプリケーションは、Cisco Unified Communications Manager やゲートウェイなどの従来のシグナリング コンポーネントに変更を加えることなく、リモートエンドポイントを検出し、通信できます。CAST プロトコルを利用することにより、別個のハードウェア デバイスで関連するメディアを同期化できます。また、PC アプリケーションでは、PC をビデオリソースとして使用することにより、ビデオ非対応の電話機がビデオ対応になるように拡張できます。	—
Cisco Discovery Protocol (CDP; シスコ検出プロトコル)	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、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。

表 1-3 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)	<p>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。</p> <p>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。</p>	<p>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。</p> <p>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。サポートされているその他の DHCP 設定については、『Cisco Unified Communications Manager System Guide』の「Dynamic Host Configuration Protocol」と「Cisco TFTP」の章を参照してください。</p> <p>(注) オプション 150 を使用できない場合、DHCP オプション 66 の使用を試みることができます。</p>
Hypertext Transfer Protocol (HTTP; ハイパーテキスト転送プロトコル)	<p>HTTP は、インターネットや Web 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。</p>	<p>Cisco Unified IP Phone では、HTTP をトラブルシューティング用に使用しています。</p>
IEEE 802.1X	<p>IEEE 802.1X 標準は、不正なクライアントが公的にアクセスできるポートを介して LAN に接続することを禁止する、クライアント サーバベースのアクセス コントロールおよび認証プロトコルを定義します。</p> <p>クライアントが認証されるまで、802.1X アクセス コントロールにより、そのクライアントが接続されているポートでは、Extensible Authentication Protocol over LAN (EAPOL) トラフィックだけが許可されます。正常に認証された後は、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。</p>	<p>Cisco Unified IP Phone では、EAP-FAST および EAP-TLS 認証方式をサポートすることによって、IEEE 802.1X 標準が実装されています。</p> <p>電話機で 802.1X 認証が有効である場合は、音声 VLAN を無効にします。詳細については、「Cisco Unified IP Phone での 802.1X 認証のサポート (P.1-17)」を参照してください。</p>
インターネット プロトコル (IP)	<p>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。</p>	<p>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。</p> <p>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。</p>

表 1-3 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 (LLDP) (Cisco Unified IP Phone 6911 のみ)	LLDP は、一部のシスコおよびサードパーティ製デバイスでサポートされている標準化ネットワーク検出プロトコル (CDP と同様) です。	Cisco Unified IP Phone は、スイッチおよび PC ポートで LLDP をサポートしています。
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 では、次のような情報を伝達するため、SW ポートで LLDP-MED をサポートしています。 <ul style="list-style-type: none"> • 音声 VLAN の設定 • デバイス検出 • 電源管理 • 在庫管理 LLDP-MED サポートの詳細については、次の Web サイトで『 <i>LLDP-MED and Cisco Discovery Protocol</i> 』ホワイトペーパーを参照してください。 http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html
Real-Time Transport Protocol (RTP; リアルタイム転送プロトコル)	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できます。
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 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、ASCII ベースのアプリケーション レイヤの制御プロトコル (RFC 3261 で規定) で、このプロトコルを使用して、2 箇所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) のどちらかを使用するように設定できます。
Skinnny 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、システムズ独自のものです。	Cisco Unified IP Phone 6901 および 6911 では、コール制御に SCCP バージョン 20 を使用します。
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 への接続に TCP を使用します。

表 1-3 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
トランスポート レイヤ セキュリティ (TLS)	TLS は、通信の保護および認証用の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。 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。DHCP サーバが指定する以外の TFTP サーバを電話機で使用する場合は、電話機の [ネットワークの設定 (Network Configuration)] メニューを使用して、TFTP サーバの IP アドレス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」の章を参照してください。
User Datagram Protocol (UDP; ユーザ データグラム プロトコル)	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 を利用した RTP ストリームを送受信します。

関連項目

- 「他の Cisco Unified IP Communications 製品との連携について」(P.2-1)
- 「電話機の起動プロセスについて」(P.2-6)

Cisco Unified IP Phone 6901 および 6911 でサポートされる機能

Cisco Unified IP Phone は、デジタル ビジネス フォンとほぼ同様に機能し、電話コールを発信および受信できます。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。

この項は、次のトピックで構成されています。

- 「機能の概要」(P.1-10)
- 「テレフォニー機能の設定」(P.1-10)
- 「Cisco Unified IP Phone でのネットワーク パラメータの設定」(P.1-11)
- 「ユーザへの機能情報の提供」(P.1-11)

機能の概要

Cisco Unified IP Phone は、コールの転送や送信、リダイヤル、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、従来のテレフォニー機能を提供します。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およびそれらの機能の設定のヒントについては、「Cisco Unified IP Phone で使用可能なテレフォニー機能」(P.5-1) 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、およびサブネット情報など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。

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。

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.7-1)

テレフォニー機能の設定

Cisco Unified IP Phone のその他の設定値は、Cisco Unified Communications Manager の管理ページで変更できます。Cisco Unified Communications Manager の管理ページを使用して、電話機登録基準やコーリング サーチ スペースの設定などの作業を行うことができます。詳細については、「Cisco Unified IP Phone で使用可能なテレフォニー機能」(P.5-1) および Cisco Unified Communications Manager のマニュアルを参照してください。

Cisco Unified Communications Manager の管理ページの詳細については、Cisco Unified Communications Manager のマニュアル (『Cisco Unified Communications Manager Administration Guide』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/ps5556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Business Edition 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

関連項目

- 「Cisco Unified IP Phone で使用可能なテレフォニー機能」(P.5-1)

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、電話機で設定します。電話機で設定値を設定し、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」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 Web サイトにある Cisco Unified IP Phone のマニュアルをよく読んでおいてください。

http://www.cisco.com/en/US/products/ps10326/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、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がある重要な情報の要約については、付録 A「Web サイトによる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、データの改ざん、およびコール シグナリングとメディア 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 IP テレフォニー 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 IP Phone 6901 および 6911 では、電話機のセキュリティ プロファイルを使用して、デバイス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します。電話機へのセキュリティ 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。

Cisco Unified Communications Manager の管理ページでセキュリティ関連の設定を行うと、電話機の設定ファイルに重要な情報が保存されます。設定ファイルのプライバシーを確保するため、設定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 Security Guide』の「Configuring Encrypted Phone Configuration Files」の章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

表 1-4 に、このマニュアルおよび他のマニュアルにおけるセキュリティの詳細情報の参照先を示します。

表 1-4 Cisco Unified IP Phone および Cisco Unified Communications Manager のセキュリティ関連トピック

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	『 <i>Troubleshooting Guide for Cisco Unified Communications Manager</i> 』を参照してください。
Cisco Unified IP Phone でサポートされているセキュリティ機能	「サポートされているセキュリティ機能の概要」(P.1-13) を参照してください。
セキュリティ プロファイル名の表示	Cisco Unified IP Phone 6901 および 6911 でサポートされているセキュリティ機能の概要については、表 1-5 を参照してください。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、『 <i>Cisco Unified Communications Manager Security Guide</i> 』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コールの特定」(P.1-15) を参照してください。
TLS 接続	<ul style="list-style-type: none"> 「使用されるネットワーク プロトコル」(P.1-6) を参照してください。 「Cisco Unified Communications Manager データベースへの電話機の追加」(P.2-8) を参照してください。
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について」(P.2-6) 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	「Cisco Unified Communications Manager データベースへの電話機の追加」(P.2-8) 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無効化および有効化」(P.6-3) を参照してください。
トラブルシューティング	<ul style="list-style-type: none"> 「トラブルシューティングおよびメンテナンス」(P.7-1) を参照してください。 『<i>Troubleshooting Guide for Cisco Unified Communications Manager</i>』を参照してください。
電話機からの CTL ファイルの削除	「Cisco Unified IP Phone のリセットまたは復元」(P.7-10) 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」(P.7-10) を参照してください。
Cisco Unified IP Phone に対する 802.1X 認証	<p>次の項を参照してください。</p> <ul style="list-style-type: none"> 「Cisco Unified IP Phone での 802.1X 認証のサポート」(P.1-17) 「トラブルシューティングおよびメンテナンス」(P.7-1)

サポートされているセキュリティ機能の概要

表 1-5 では、Cisco Unified IP Phone 6901 および 6911 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。



(注) ほとんどのセキュリティ機能は、Certificate Trust List (CTL; 証明書信頼リスト) 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 Security Guide*』の「Configuring the Cisco CTL Client」の章を参照してください。

表 1-5 セキュリティ機能の概要

機能	説明
イメージの認証	署名付きバイナリ ファイル (.zsgn 拡張子) 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。イメージの改ざんは、電話機で認証プロセスが失敗し、新しいイメージが拒否される原因となります。
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、デバイス認証用の固有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) が含まれますが、追加のセキュリティについては、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ように指定できます。詳細については、「 Cisco Unified IP Phone のセキュリティの設定 」(P.3-10) を参照してください。
デバイス認証	Cisco Unified Communications Manager サーバと電話機間で、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 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 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	各 Cisco Unified IP Phone には、固有の Manufacturing Installed Certificate (MIC; 製造元でインストールされる証明書) が含まれており、デバイス認証にはその証明書が使用されます。MIC は、電話機に固有の永続的な ID 証明であり、Cisco Unified Communications Manager ではそれを利用して電話機を認証します。

表 1-5 セキュリティ機能の概要 (続き)

機能	説明
セキュアな SRST 参照	<p>Cisco Unified Communications Manager の管理ページでセキュリティに SRST 参照を設定してから、従属デバイスをリセットすると、TFTP サーバによって電話機の設定ファイルに SRST 証明書が追加され、そのファイルが電話機に送信されます。その後、セキュアな電話機は TLS 接続を使用して SRST 対応ルータと連携します。</p> <p>この設定ファイルには、次のいずれかの拡張子が付きます。</p> <ul style="list-style-type: none"> .cnf.xml .cnf.xml.sgn .cnf.xml.enc.sgn
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、キーのデバイスへの配布、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 サーバの間で送信されるすべての SCCP および SIP シグナリング メッセージが暗号化されるようにします。
Certificate Authority Proxy Function (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、証明書生成手順の一部を実装し、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。
セキュリティ プロファイル	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します。詳細については、「 セキュリティ プロファイルについて 」(P.1-15) を参照してください。
暗号化された設定ファイル	電話機の設定ファイルのプライバシーを確保できるようにします。
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。
電話機のセキュリティ強化	次に示すセキュリティの追加オプションです。これらのオプションは、Cisco Unified CM の管理から制御します。 <ul style="list-style-type: none"> 電話機の Web ページへのアクセスの無効化
802.1X 認証	Cisco Unified IP Phone では、802.1X 認証を使用して、ネットワークへのアクセスを要求し、取得できます。詳細については、「 Cisco Unified IP Phone での 802.1X 認証のサポート 」(P.1-17) を参照してください。
音声品質メトリック	
[MOS LQK]	<p>Listening Quality (LQK; リスニング品質) の Mean Opinion Score (MOS; 平均オピニオン評点) を客観的に評価するスコアで、音声品質が 5 (非常に良い) ~ 1 (非常に悪い) でランク付けされます。このスコアは、音声ストリームの先行 8 秒間でのフレーム損失に起因する音声秘匿イベントに基づいています。</p> <p>(注) MOS LQK スコアは、Cisco Unified IP Phone が使用するコーデックのタイプに基づいて変化する可能性があります。</p>
[平均 MOS LQK (Avg MOS LQK)]	音声ストリーム全体の平均 MOS LQK スコア。
[最小 MOS LQK (Min MOS LQK)]	音声ストリームの開始以降最も低い MOS LQK スコア。

表 1-5 セキュリティ機能の概要 (続き)

機能	説明
[最大 MOS LQK (Max MOS LQK)]	<p>音声ストリーム開始以降のベースライン MOS LQK スコアまたは最も高い MOS LQK スコア。</p> <p>次のコーデックは、フレーム損失率がゼロの通常の条件で、これらの最大 MOS LQK スコアを示します。</p> <ul style="list-style-type: none"> • G.711 : 4.5 • G.728/iLBC : 3.9 • G729A/AB : 3.7
[MOS LQK のバージョン (MOS LQK Version)]	MOS LQK のスコアを計算するために使用されるシスコ独自のアルゴリズムのバージョン。

関連項目

- 「Cisco Unified IP Phone のセキュリティ機能について」 (P.1-11)
- 「認証、暗号化、および保護されているコールの特定」 (P.1-15)

セキュリティ プロファイルについて

Cisco Unified Communications Manager 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 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 モードを表示するには、Cisco Unified Communications Manager の管理ページでセキュリティ プロファイルを表示できます。

関連項目

- 「認証、暗号化、および保護されているコールの特定」 (P.1-15)

認証、暗号化、および保護されているコールの特定

認証されたコールでは、コールの確立に参加しているすべてのデバイスが信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されています。

暗号化されたコールでは、コールの確立に参加しているすべてのデバイスが信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されています。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、高いレベルのセキュリティを実現します。

コールが PSTN などの非 IP コール レグを介してルーティングされている場合、そのコールは IP ネットワーク内で暗号化されている場合でも非セキュアである可能性があります。

保護されたコールでは、コールの始まりに、接続先の電話機でも暗号化された音声とビデオ（ビデオが含まれる場合）が送受信されていることを通知するセキュリティ トーンが再生されます。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。会議コールやシェアドラインなどの一部の機能は、保護されたコールが設定されている場合は使用できません。保護されたコールは認証されません。

関連項目

- 「Cisco Unified IP Phone のセキュリティ機能について」(P.1-11)
- 「Cisco Unified IP Phone のセキュリティ機能について」(P.1-11)

保護されたコールの確立と特定

電話機と他方の電話機に、保護されたコールが設定されている場合、保護されたコールが確立されません。他方の電話機は同一の Cisco IP ネットワーク内にある場合も、IP ネットワーク外のネットワーク内にある場合もあります。保護されたコールは、2 台の電話機間でのみ確立できます。電話会議やその他の複数回線コールはサポートされません。

保護されたコールは、次のプロセスで確立されます。

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. コールが、保護された別の電話機に接続すると、セキュリティ コールが再生されて、会話の両端が暗号化され、保護されることを示します。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 台の電話機間の会話に対してサポートされます。会議コールやシェアドラインなどの一部の機能は、保護されたコールが設定されている場合は使用できません。

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。

表 1-6 では、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。対象は、Cisco Unified IP Phone 6901 および 6911 です。

表 1-6 割り込み使用時のコール セキュリティの連携動作（Cisco Unified IP Phone 6911 のみ）

発信側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	C 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）	C 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）	C 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	C 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 1-7 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 1-7 会議コールのセキュリティの制限事項

発信側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	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	認証済みレベルのセキュアな会議
非セキュア	C 割り込み	すべての参加者が暗号化済み	会議は非セキュアに変更されます。
非セキュア	ミーティング	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」という意味のメッセージを受け取り、コールが拒否されます。
セキュア（暗号化済み）	ミーティング	最小セキュリティ レベルは、認証済み	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）	ミーティング	最小限のセキュリティ レベルが非セキュア	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 のサポートについて説明します。

- 「概要」(P.1-17)
- 「必要なネットワーク コンポーネント」(P.1-18)
- 「ベスト プラクティス：要件と推奨事項」(P.1-18)

概要

Cisco Unified IP phone および 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、従来から Cisco Discovery Protocol (CDP) を使用しています。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。したがって、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、プロキシ 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。電話機に含まれる 802.1X サプリカントの現在のリリースでは、ネットワーク認証に EAP-FAST オプションと EAP-TLS オプションが使用されています。

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、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 (または他の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。
- 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 台に制限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。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。



(注) PC ポートがあるのは、Cisco Unified IP Phone 6911 だけです。

- 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。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 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。

Cisco Unified IP Phone の設定および設置の概要

新しい IP テレフォニー 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 IP テレフォニー 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 System Guide*』の「[System Configuration Overview](#)」の章を参照してください。

IP テレフォニー 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.1-19)
- 「[Cisco Unified IP Phone の設置](#)」(P.1-21)

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 が混合モードで動作している場合はサポートされません。
- Cisco Unified Communications Manager の管理ページ
- Bulk Administration Tool (BAT; 一括管理ツール)
- BAT と Tool for Auto-Registered Phones Support (TAPS)

これらの方法の詳細については、「[Cisco Unified Communications Manager データベースへの電話機の追加](#)」(P.2-8) を参照してください。

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 IP Phone](#) : 『*Cisco Unified Communications Manager System Guide*』
- [Cisco Unified IP Phone の設定](#) : 『*Cisco Unified Communications Manager Administration Guide*』
- [自動登録の設定](#) : 『*Cisco Unified Communications Manager Administration Guide*』

Cisco Unified Communications Manager での Cisco Unified IP Phone 6901 および 6911 の設定に関するチェックリスト

表 1-8 に、Cisco Unified Communications Manager の管理ページで Cisco Unified IP Phone 6901 および 6911 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、推奨する順序に従い、電話機の設定プロセスを解説しています。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 1-8 Cisco Unified Communications Manager での Cisco Unified IP Phone 6901 および 6911 の設定に関するチェックリスト

作業	目的	参照先
1.	<p>電話機について、次の情報を収集します。</p> <ul style="list-style-type: none"> 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 パーティション、コーリング サーチ スペース、およびロケーションの情報 電話機に割り当てるための関連付けられた Directory Number (DN; 電話番号) 電話機に関連付ける Cisco Unified Communications Manager ユーザ <p>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。</p>	<p>詳細については、『<i>Cisco Unified Communications Manager System Guide</i>』の「Cisco Unified IP Phone」の章を参照してください。</p> <p>「Cisco Unified IP Phone で使用可能なテレフォニー機能」(P.5-1) を参照してください。</p>
2.	<p>電話機に対応する十分なユニット ライセンスがあることを確認します。</p>	<p>詳細については、『<i>Cisco Communications Manager Administration Guide</i>』の「License Unit Report」の章を参照してください。</p>
3.	<p>[電話の設定 (Phone Configuration)] ウィンドウ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。必須フィールドは、フィールド名の横にアスタリスク (*) を付けて示されています (たとえば、MAC アドレスやデバイス プール)。</p> <p>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。</p>	<p>詳細については、『<i>Cisco Communications Manager Administration Guide</i>』の「Cisco Unified IP Phone Configuration」の章を参照してください。</p> <p>プロダクト固有の設定については、[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。</p> <p>(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、『<i>Cisco Communications Manager Administration Guide</i>』の「User/Phone Add Configuration」の章を参照してください。</p>
4.	<p>[電話番号の設定 (Directory Number Configuration)] ウィンドウの必須フィールドに値を入力して、電話機に電話番号 (回線) を追加し、設定します。必須フィールドは、フィールド名の横にアスタリスク (*) を付けて示されています (たとえば、電話番号やプレゼンス グループ)。</p>	<p>詳細については、『<i>Cisco Unified Communications Manager Administration Guide</i>』の「Directory Number Configuration」の章を参照してください。</p> <p>「Cisco Unified IP Phone で使用可能なテレフォニー機能」(P.5-1) を参照してください。</p>

表 1-8 Cisco Unified Communications Manager での Cisco Unified IP Phone 6901 および 6911 の設定に関するチェックリスト (続き)

作業	目的	参照先
5.	<p>必須フィールドを設定して、ユーザ情報を追加します。必須フィールドは、フィールド名の横にアスタリスク (*) を付けて示されています (たとえば、ユーザ ID や姓)。</p> <p>(注) パスワード (ユーザ オプション Web ページ用) および PIN (IVR を介したネットワークメニューへのアクセス用) を割り当てます。</p> <p>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。</p>	<p>詳細については、『Cisco Unified Communications Manager Administration Guide』の「End User Configuration」の章を参照してください。</p> <p>「Cisco Unified Communications Manager へのユーザの追加」(P.5-9) を参照してください。</p> <p>(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 Add Configurations」の章を参照してください。</p>
6.	<p>ユーザをユーザグループに関連付けます。</p> <p>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。</p> <p>(注) エンドユーザが Cisco Unified CM ユーザオプションにアクセスするには、ユーザを標準 CCM エンドユーザグループに追加する必要があります。</p>	<p>『Cisco Unified Communications Manager Administration Guide』の次の項を参照してください。</p> <ul style="list-style-type: none"> 「End User Configuration」の章の「End User Configuration Settings」 「User Group Configuration」の章の「Adding Users to a User Group」
7.	<p>ユーザを電話機に割り当てます (オプション)。</p> <p>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。</p> <p>(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。</p>	<p>詳細については、『Cisco Unified Communications Manager Administration Guide』の「End User Configuration」の章の「Associating Devices to an End User」を参照してください。</p>

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。



(注) 電話機を設置する前に、現在のファームウェアイメージで電話機をアップグレードします。アップグレードの詳細については、次の Web サイトで対象の電話機の Readme ファイルを参照してください。
<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>

ファームウェアのアップグレード手順については、次の Web サイトでリリースノートを参照してください。

http://www.cisco.com/en/US/products/ps10326/prod_release_notes_list.html

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。電話機の設定を完了するには、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 6901 および 6911 の設置に関するチェックリスト

表 1-9 に、Cisco Unified IP Phone 6901 および 6911 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、推奨する順序に従い、電話機の設定プロセスを解説しています。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 1-9 Cisco Unified IP Phone 6901 および 6911 の設置に関するチェックリスト

作業	目的	参照先
1.	電話機の電源を次の中から選択します。 <ul style="list-style-type: none"> 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。	「Cisco Unified IP Phone への電力供給」(P.2-3) を参照してください。
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。	「Cisco Unified IP Phone の設置」(P.3-4) を参照してください。 「フットスタンド」(P.3-7) を参照してください。
3.	電話機の起動プロセスをモニタします。 電話機に電話番号を割り当てます。 電話機が適切に設定されていることを確認します。	「電話機の起動プロセスの確認」(P.3-9) を参照してください。
4.	電話上でネットワーク設定値を設定する場合、DHCP を使用するか、手動で IP アドレスを入力して、電話機の IP アドレスを設定します。 DHCP を使用する場合：DHCP が IVR で有効であることを確認します。IVR から表示されるプロンプトに TFTP の IP アドレスを入力することによって、代替 TFTP を設定できます。 (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かどうかを、ネットワーク管理者に相談してください。 DHCP を使用しない場合：DHCP が IVR で無効であることを確認します。次に、電話機の IVR を使用して、IP アドレス、サブネット マスク、TFTP サーバ、およびデフォルト ルータをローカルに設定する必要があります。	「起動時のネットワーク設定値の設定」(P.3-9) を参照してください。 「Cisco Unified IP Phone の設定値の設定」(P.4-1) を参照してください。
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。	「Cisco Unified IP Phone のセキュリティの設定」(P.3-10) を参照してください。

表 1-9 Cisco Unified IP Phone 6901 および 6911 (続き) の設置に関するチェックリスト (続き)

作業	目的	参照先
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。	詳細については、『 <i>Cisco Unified IP Phone 6901 and 6911 User Guide</i> 』を参照してください。
7.	エンドユーザに対して、電話機の使用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 「Web サイトによるユーザへの情報提供」を参照してください。

用語の違い

表 1-10 は、次の各マニュアルで使用される用語の重要な違いを示します。

- 『*Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager 8.5 (SCCP)*』
- 『*Cisco Unified IP Phone 6901 and 6911 Administration Guide for Cisco Unified Communications Manager 8.5 (SCCP)*』
- 『*Cisco Unified Communications Manager Administration Guide*』
- 『*Cisco Unified Communications Manager System Guide*』

表 1-10 用語の違い

ユーザガイド	アドミニストレーション ガイドおよびシステム ガイド
自動割り込み	C 割り込み
メッセージ インジケータ	Message Waiting Indicator (MWI; メッセージ受信インジケータ) またはメッセージ受信ランプ
ボイスメール システム	ボイス メッセージ システム

