



Cisco Unified IP Phone の概要

Cisco Unified IP Phone 7975G は、Internet Protocol (IP; インターネットプロトコル) ネットワークで音声通信を行うための機能をすべて搭載した電話機です。Cisco Unified IP Phone 7975G 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加えて、ミュート、保留、転送、短縮ダイヤル、コール転送などの機能を使用できます。また、Cisco Unified IP Phone はデータネットワークに接続されるため、IP テレフォニー機能が拡張され、ネットワーク情報とサービス、およびカスタマイズ可能な機能とサービスにアクセスできるようになります。この電話機は、ファイルの認証、デバイスの認証、シグナリングの暗号化、メディアの暗号化を含むセキュリティ機能もサポートしています。

Cisco Unified IP Phone 7975G はカラー タッチスクリーンを備え、最大 8 個の回線番号または短縮ダイヤル番号のサポート、ボタンや機能に対応した状況依存オンライン ヘルプ、およびその他の高度な各種機能を提供します。

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.722、G.729a、G.729ab、および iLBC をエンコードし、G.711a、G.711u、G.722、iLBC、G.729、G.729a、G.729b、および G.729ab をデコードします。また、非圧縮のワイドバンド (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。

- [Cisco Unified IP Phone 7975G について \(P.1-2\)](#)
- [使用されるネットワーク プロトコル \(P.1-4\)](#)
- [Cisco Unified IP Phone 7975G でサポートされる機能 \(P.1-7\)](#)
- [Cisco Unified IP Phone のセキュリティ機能について \(P.1-9\)](#)
- [Cisco Unified IP Phone の設定および設置の概要 \(P.1-18\)](#)



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 7975G について

図 1-1 に、Cisco Unified IP Phone 7975G の主要コンポーネントを示します。

図 1-1 Cisco Unified IP Phone 7975G



1	プログラム可能なボタン 	<p>設定に応じて、プログラム可能なボタンから次に示す項目にアクセスできます。</p> <ul style="list-style-type: none"> 電話回線（回線ボタン） 短縮ダイヤル番号（短縮ダイヤル ボタン、BLF 短縮ダイヤル機能を含む） Web ベースのサービス（Personal Address Book ボタンなど） 電話機の機能（プライバシー ボタンなど） <p>表示されるボタンの色によって、回線の状態が次のように示されます。</p> <ul style="list-style-type: none">  緑、点灯：アクティブなコールまたは双方向インターコム コール  緑、点滅：保留中のコール  オレンジ、点灯：プライバシー機能が有効、一方向のインターコム コール、サイレント機能がアクティブ、またはハントグループにログイン  オレンジ、点滅：着信コールまたは復帰コール  赤、点灯：リモート回線が使用中（シェアラインまたは BLF ステータス）
2	フットスタンド調節ボタン	電話機本体の角度を調節します。
3	ディスプレイ ボタン 	<p>タッチスクリーンをスリープ モードから復帰させたり、クリーニングのためにタッチスクリーンの機能を無効にします。</p> <ul style="list-style-type: none">  色なし：入力可能な状態  緑、点滅：無効  緑、点灯：スリープ モード

4	メッセージ ボタン 	ボイス メッセージ サービスに自動ダイヤルします (サービスによって異なります)。
5	ディレクトリ ボタン 	[ディレクトリ] メニューを開閉します。履歴およびディレクトリへのアクセスに使用します。
6	ヘルプ ボタン 	[ヘルプ] メニューをアクティブにします。
7	設定ボタン 	[設定] メニューを開閉します。タッチスクリーンと呼出音の設定を変更するために使用します。
8	サービス ボタン 	[サービス] メニューを開閉します。
9	音量ボタン 	ハンドセット、スピーカフォン、およびヘッドセットの音量 (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。
10	スピーカ ボタン 	スピーカフォンのオン/オフを切り替えます。
11	ミュート ボタン 	ミュート機能のオン/オフを切り替えます。
12	ヘッドセット ボタン 	ヘッドセット モードのオン/オフを切り替えます。
13	4 方向のナビゲーション パッドと選択ボタン (中央) 	メニューのスクロールや項目の強調表示に使用します。選択ボタンを使用して、スクリーン上で強調表示されている項目を選択します。 ナビゲーション ボタン <ul style="list-style-type: none"> 上下にスクロールして、メニューの表示や項目の強調表示を行います。 左右にスクロールして、複数カラムの表示を水平方向に移動します。 選択ボタン: ナビゲーション ボタンを使用して行を強調表示した後に、次の操作を行います。 <ul style="list-style-type: none">  を押して、メニューを開きます。  を押して、呼出音を再生します。  を押して、スクリーンに示されている他の機能にアクセスします。  (注) 選択ボタンでは、メニュー項目の操作は実行されません。
14	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。
15	ソフトキー ボタン 	タッチ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。
16	ハンドセットのライト ストリップ	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。
17	タッチスクリーン	電話機の機能を表示します。

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 7975G 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。
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 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。	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。
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.1-15 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。

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
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。
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。
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。
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。 <ul style="list-style-type: none"> 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『 <i>LLDP-MED and Cisco Discovery Protocol</i> 』を参照してください。 http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Control Protocol (RTCP)	RTCP はリアルタイム転送プロトコル (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 の [電話の設定 (Phone Configuration)] ページ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.4-25 の「ネットワークの設定」を参照してください。
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。

■ 使用されるネットワーク プロトコル

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。
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。
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。DHCP サーバで指定された TFTP サーバとは別の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] メニューを使用して、TFTP サーバを手動で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 RTP ストリームを送信および受信しますが、このストリームで UDP を利用しています。

関連項目

- [他の Cisco Unified IP コミュニケーション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 \(P.2-7\)](#)
- [ネットワークの設定メニュー \(P.4-6\)](#)

Cisco Unified IP Phone 7975G 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。従来のテレフォニー機能に加えて、Cisco Unified 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 \(P.1-7\)](#)
- [テレフォニー機能の設定 \(P.1-8\)](#)
- [Cisco Unified IP Phone でのネットワーク パラメータの設定 \(P.1-8\)](#)
- [ユーザへの機能情報の提供 \(P.1-8\)](#)

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、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については、[P.5-2 の「電話機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.5-15 の「社内ディレクトリの設定」](#)および[P.5-17 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ディング 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「電話機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

- 電話機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、現在の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 IP テレフォニー 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 ストリームとコール シグナリングを暗号化します。

Cisco Unified IP Phone シリーズは、電話セキュリティ プロファイルを使用します。このプロファイルは、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するものです。電話機へのセキュリティ 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。

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 および Cisco Unified Communications Manager 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.1-10 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.1-17 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 プロファイル名の表示	P.1-12 の「セキュリティ プロファイルについて」を参照してください。
セキュリティが実装された電話コールの識別	P.1-13 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。
TLS 接続	P.1-4 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.2-6 の「電話機の設定ファイルについて」を参照してください。
セキュリティおよび電話機の起動プロセス	P.2-7 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.2-6 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.4-6 の「ネットワークの設定メニュー」の表 4-2 を参照してください。

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

トピック	参照先
電話機の [デバイス設定] メニューにある [Unified CM 1] ~ [Unified CM 5] オプションのセキュリティアイコンの意味	P.4-12 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.4-23 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.4-29 の「セキュリティ設定メニュー」を参照してください。
CTL ファイルのロック解除	P.4-30 の「CTL ファイル メニュー」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.8-3 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.9-10 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。
電話機からの CTL ファイルの削除	P.9-16 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.9-16 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。 <ul style="list-style-type: none"> • Cisco Unified IP Phone での 802.1X 認証のサポート (P.1-15) • 802.1X 認証およびステータス (P.4-32) • Cisco Unified IP Phone のセキュリティのトラブルシューティング (P.9-10)

サポートされているセキュリティ機能の概要

表 1-3 に、Cisco Unified IP Phone 7975G 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、電話機の [セキュリティ設定] メニューを確認してください ([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』の「Cisco CTL クライアントの設定」の章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 .sgn) 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。
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 LSC をインストールすることもできます。詳細については、P.3-17 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、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、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。
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 には、製造元でインストールされる一意の証明書 (MIC) が組み込まれており、この証明書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	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。
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、および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、P.1-12 の「セキュリティ プロファイルについて」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	<p>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。</p> <ul style="list-style-type: none"> PC ポートの無効化。 Gratuitous ARP (GARP) の無効化。 PC ボイス VLAN アクセスの無効化。 [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。 <p> (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.4-12 の「デバイス設定メニュー」を参照してください。</p>
802.1X 認証	<p>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.1-15 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。</p>

関連項目

- [セキュリティ プロファイルについて \(P.1-12\)](#)
- [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 \(P.1-13\)](#)
- [デバイス設定メニュー \(P.4-12\)](#)
- [Cisco Unified IP Phone での 802.1X 認証のサポート \(P.1-15\)](#)
- [セキュリティに関する制限事項 \(P.1-17\)](#)

セキュリティ プロファイルについて

Cisco Unified Communications Manager 6.0 以降をサポートしている Cisco Unified IP Phone は、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.4-23 の「セキュリティ設定メニュー」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 \(P.1-13\)](#)
- [デバイス設定メニュー \(P.4-12\)](#)
- [セキュリティに関する制限事項 \(P.1-17\)](#)

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。処理中のコールが認証されている場合は、電話機の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場合は、電話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ない可能性があります。

関連項目

- [Cisco Unified IP Phone のセキュリティ機能について \(P.1-9\)](#)
- [セキュリティ プロファイルについて \(P.1-12\)](#)
- [セキュリティに関する制限事項 \(P.1-17\)](#)

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。
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	メンバーが MOH を使用してコールを保留にする	保留音は再生されません。 会議はセキュアに保たれます。

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)	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	ミーティング	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。
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	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)	ミーティング	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 \(P.1-15\)](#)
- [必要なネットワーク コンポーネント \(P.1-16\)](#)
- [ベスト プラクティス：要件と推奨事項 \(P.1-16\)](#)

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。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、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 サプリカントの最初のリリースには、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 サブリカントとして動作します。このサブリカントは、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わ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。詳細については、P.4-32 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/tsd_products_support_category_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.4-23 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 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.4-23 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.4-32 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、ユーザが割り込みを開始した電話機では、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、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 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 IP テレフォニー ネットワークのひとつ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。

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 \(P.1-18\)](#)
- [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 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.2-9](#) 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 7975G の設定に関するチェックリスト

表 1-6 に、Cisco Unified Communications Manager の管理ページで Cisco Unified IP Phone 7975G 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 7975G の設定に関するチェックリスト

作業	目的	参照先
<p>1. 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情報 回線の数、および電話機に割り当てる関連電話番号 (DN) 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 	<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する。</p> <p>個々の電話機を設定する前に実施する必要がある、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する。</p>	<p>『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> <p>P.5-2 の「電話機で使用可能なテレフォニー機能」を参照してください。</p>
<p>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。</p>	<p>回線ボタン、短縮ダイヤル ボタン、サービス URL ボタンの数を変更したり、プライバシー ボタンを追加したりして、ユーザのニーズに対応する。</p>	<p>『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> <p>P.5-16 の「電話ボタン テンプレートの変更」を参照してください。</p>
<p>3. [電話の設定 (Phone Configuration)] ウィンドウで、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。</p> <ul style="list-style-type: none"> 電話タイプ MAC アドレス デバイス プール ボタン テンプレート プロダクト固有の設定 ソフトキー テンプレート (カスタマイズする場合) 	<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する。</p>	<p>『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。</p> <p>[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 [I] ボタン ヘルプを参照してください。</p>

表 1-6 Cisco Unified Communications Manager での Cisco Unified IP Phone 7975G の設定に関するチェックリスト (続き)

作業	目的	参照先
<p>4. [電話番号の設定 (Directory Number Configuration)] ウィンドウで、次の必須フィールドに値を入力して、電話機の電話番号 (回線) を追加および設定します。</p> <ul style="list-style-type: none"> • 電話番号 • 複数コール / コール待機 • コール転送とコールピックアップ (使用する場合) • ボイス メッセージ (使用する場合) 	<p>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する。</p>	<p>『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。</p> <p>P.5-2 の「電話機で使用可能なテレフォニー機能」を参照してください。</p>
<p>5. ソフトキー テンプレートをカスタマイズします。</p>	<p>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する。</p>	<p>『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> <p>P.5-17 の「ソフトキー テンプレートの設定」を参照してください。</p>
<p>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)。</p>	<p>短縮ダイヤルのボタンと番号を追加する。</p> <p> (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。</p>	<p>『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」の章の「短縮ダイヤル ボタンの設定」の項を参照してください。</p>
<p>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)。</p>	<p>IP Phone サービスを提供する。</p> <p> (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。</p>	<p>『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> <p>P.5-17 の「サービスのセットアップ」を参照してください。</p>
<p>8. サービスを電話ボタンに割り当てます (オプション)。</p>	<p>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する。</p>	<p>『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。</p>

表 1-6 Cisco Unified Communications Manager での Cisco Unified IP Phone 7975G の設定に関するチェックリスト (続き)

作業	目的	参照先
<p>9. 次の必須フィールドを設定して、ユーザ情報を追加します。</p> <ul style="list-style-type: none"> 名前 (姓) ユーザ ID パスワード (ユーザ オプション Web ページ用) PIN (エクステンション モビリティとパーソナルディレクトリで使用) 	<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する。</p>	<p>『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> <p>P.5-18 の「Cisco Unified Communications Manager へのユーザの追加」を参照してください。</p>
<p>10. 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する。</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>『Cisco Unified Communications Manager アドミニストレーションガイド』の「エンドユーザとデバイスとの関連付け」の項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。電話機のハンドセット、ケーブル、およびその他のアクセサリを接続する方法は、各電話機の『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。アップグレードについては、次の URL にある電話機の 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 7975G の設置に関するチェックリスト

表 1-7 に、Cisco Unified IP Phone 7975G 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 7975G の設置に関するチェックリスト

作業	目的	参照先
<p>1. 電話機の電源を次の中から選択します。</p> <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する。	P.2-4 の「電話機への電力供給」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する。	<p>P.3-8 の「Cisco Unified IP Phone の設置」を参照してください。</p> <p>P.3-12 の「Cisco Unified IP Phone の位置の調節」を参照してください。</p>
3. 1 台または 2 台の Cisco Unified IP Phone 7914 拡張モジュールを SCCP Cisco Unified IP Phone に追加します (オプション。SIP では使用不可)。	14 のライン アピアランスまたは短縮ダイヤル番号を追加することで、Cisco Unified IP Phone の機能を拡張する。	<p>P.3-10 の「Cisco Unified IP Phone 7914 拡張モジュールの接続 (SCCP 電話機のみ)」を参照してください。</p> <p>『Cisco Unified IP Phone 7914 拡張モジュール電話ガイド』を参照してください。</p>
4. 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.3-15 の「電話機の起動プロセスの確認」を参照してください。
<p>5. 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。</p> <p>DHCP を有効にする場合：</p> <ul style="list-style-type: none"> [DHCP を使う] を [Yes] に設定する 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>DHCP を無効にする場合：</p> <ul style="list-style-type: none"> [DHCP を使う] を [No] に設定する 電話機のスタティック IP アドレスを入力する サブネット マスクを入力する デフォルト ルータの IP アドレスを入力する 電話機が配置されるドメイン名を入力する [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>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。</p> <p> (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。</p> <p>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。</p>	<p>P.3-16 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> <p>P.4-6 の「ネットワークの設定メニュー」を参照してください。</p>
6. 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 盗用から保護する。	P.3-17 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 7975G の設置に関するチェックリスト (続き)

作業	目的	参照先
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する。	『Cisco Unified IP Phone 7975G 電話ガイド for Cisco Unified Communications Manager 6.1 (SCCP/SIP)』を参照してください。
8. 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する。	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。

