CHAPTER 1

Cisco Unified IP Phone の概要

Cisco Unified IP Phone 7962G、7942G、7961G、7961G-GE（ギガビット イーサネット バージョン）、7941G/7941G-GE（ギガビット イーサネット バージョン）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すべての機能が搭載された電話機です。ギガビット イーサネット バージョンの Cisco Unified IP Phone 7961G-GE および 7941G-GE は、ギガビット イーサネット VoIP テレフォニーの最新テクノロジーを提供します。Cisco Unified IP Phone は、デジタル ビジネス電話機と同じように機能し、コールの発信や着信のほか、ミュート、保留、転送、短縮ダイヤル、コール転送などの機能も利用できます。さらに、ご使用のデータ ネットワークに接続できるため、IP テレフォニー機能により、ネットワーク情報およびサービス、カスタマイズ可能な機能およびサービスなども利用できます。また、ファイル認証、デバイス認証、シグナリングの暗号化、およびメディアの暗号化などの機能もサポートしています。

Cisco Unified IP Phone は、他のネットワーク デバイスと同様に設定と管理を行う必要があります。これらの電話機は、G.711a、G.711μ、G.722、G.729a、G.729ab、iLBC を符号化し、G.711a、G.711u、G.722、iLBC、G.729、G729a、G729b、および G729ab をデコードします。これらの電話機は、圧縮解除されたワイドバンド（16 ビット、16 kHz）オーディオもサポートします。

この章は、次の項で構成されています。

注意 Cisco Unified IP Phone の非常に近くで携帯電話、GSM 電話、または双方向ラジオを使用すると、干渉が起こる場合があります。詳細については、干渉デバイスの製造元の資料を参照してください。

Cisco Unified IP Phone 7962G/7942G について

図 1-1 は、Cisco Unified IP Phone 7962G の主なコンポーネントを示しています。

図 1-2 は、Cisco Unified IP Phone 7942G の主なコンポーネントを示しています。

図 1-3 は、Cisco Unified IP Phone 7961G および 7961G-GE の主なコンポーネントを示しています。

図 1-4 は、Cisco Unified IP Phone 7941G および 7941G-GE の主なコンポーネントを示しています。

図 1-1　Cisco Unified IP Phone 7962G

図 1-2　Cisco Unified IP Phone 7942G

図 1-3　Cisco Unified IP Phone 7961G/7961G-GE

図 1-4　Cisco Unified IP Phone 7941G/7941G-GE

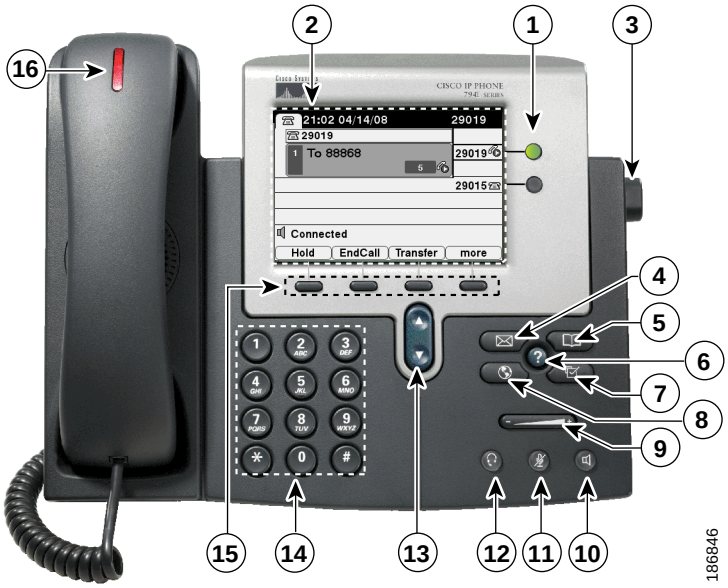

表 1-1 は、Cisco Unified IP Phone 7962G/7942G のボタンを示しています。

表 1-1　Cisco Unified IP Phone 7962G、7942G、7961G、7961G-GE、7941G、および 7941 G-GE の機能

1	プログラマブル ボタン 	設定に応じて、プログラマブル ボタンからは次にアクセスできます。 • 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（PAB; 個人アドレス帳）ボタンなど） • 電話機の機能（プライバシー ボタンなど） 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。  緑、点灯：アクティブ コールです。  緑、点滅：コールは保留状態です。  オレンジ、点灯：プライバシー機能が使用中です。  オレンジ、点滅：コールが着信しています。  赤、点灯：リモート回線が使用中です（共有回線、BLF ステータス、またはアクティブなモバイル接続応答コール）。
2	電話スクリーン	電話機の機能を表示します。
3	フットスタンド ボタン	電話機本体の角度を調節します。
4	メッセージ ボタン 	サービスによって異なりますが、ボイス メッセージ サービスに自動ダイヤルします。
5	ディレクトリ ボタン 	[ディレクトリ（Directories）] メニューを開閉します。履歴およびディレクトリにアクセスするために使用します。
6	ヘルプ ボタン 	[ヘルプ（Help）] メニューをアクティブにします。
7	設定ボタン 	[設定（Settings）] メニューを開閉します。電話スクリーンのコントラストおよび呼び出し音を制御するために使用します。
8	サービス ボタン 	[サービス（Services）] メニューを開閉します。
9	音量ボタン 	受話器、ヘッドセット、スピーカフォンの音量（オフフック）、および呼び出し音の音量（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 モードのオン/オフを切り替えます。スピーカフォンがオンになっているとき、ボタンは点灯しています。
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。ミュート機能がオンになっているとき、ボタンは点灯しています。
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。ヘッドセットがオンになっているとき、ボタンは点灯しています。
13	ナビゲーション ボタン 	メニュー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とき、発信履歴ログに含まれる電話番号を表示します。
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 	各ボタンは、電話スクリーンに表示されているソフトキーのオプションをそれぞれアクティブにします。

16	受話器のライト 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。

使用するネットワーク プロトコル

Cisco Unified IP Phone は、音声通信に必要な、複数の業界標準ネットワーク プロトコルおよびシスコ ネットワーク プロトコルをサポートしています。表 1-2 は、Cisco Unified IP Phone 7962G/7942G の電話機がサポートしているネットワーク プロトコルの概要を説明しています。

表 1-2　Cisco Unified IP Phone がサポートしているネットワーク プロトコル

ネットワーク プロトコル	目的	使用上の注意
Bootstrap Protocol（BootP; ブートストラップ プロトコル）	BootP を使用すると、ネットワーク デバイス（Cisco Unified IP Phone など）は特定の起動情報（そのデバイスの IP アドレスなど）を検出できます。	BootP を使用して IP アドレスを Cisco Unified IP Phone に割り当てている場合、電話機のネットワーク構成の設定値として [BOOTP サーバ（BOOTP Server）] オプションが「Yes」と表示されます。
Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）	すべてのシスコ製の機器上で実行されるデバイス検出プロトコルです。 CDP を使用すると、デバイスはその存在を他のデバイスにアドバタイズし、ネットワーク内の他のデバイスに関する情報を受け取ることができます。	Cisco Unified IP Phone は、CDP を使用して、補助 VLAN ID、ポート単位の電源管理の詳細、Quality of Service（QoS; サービス品質）設定情報などを Cisco Catalyst スイッチとの間で通信します。
Cisco Peer-to-Peer Distribution Protocol（CPPDP）	CPPDP は、デバイスのピアツーピア階層を形成するために使用するシスコ独自のプロトコルです。CPPDP は、ファームウェアや他のファイルをピア デバイスから近接デバイスにコピーするためにも使用します。	CPPDP は、ピア ファームウェア共有機能によって使用されます。
Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）	IP アドレスをネットワーク デバイスに動的に配分し、割り当てます。 DHCP を使用すると、手動による IP アドレスの割り当てやその他のネットワーク パラメータ設定を行わずに、IP Phone をネットワークに接続して操作可能にすることができます。	DHCP はデフォルトで有効になっています。無効になっている場合は、各電話機にローカルで 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。 DHCP カスタム オプション 150 の使用をお勧めします。この方式を使用すると、TFTP サーバの IP アドレスをオプション値として設定できます。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」および「Cisco TFTP」を参照してください。
HyperText Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）	HTTP は、インターネットと Web で情報を転送し、文書を移動する標準的な方法です。	Cisco Unified IP Phone は、HTTP を XML サービスやトラブルシューティングの目的で使用します。 Cisco Unified IP Phone は、URL での IPv6 アドレスの使用をサポートしません。IPv6 アドレスにマップされるホスト名や URL で IPv6 アドレスを使用することはできません。

表 1-2　Cisco Unified IP Phone がサポートしているネットワーク 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
Hypertext Transfer Protocol Secure（HTTPS）	Hypertext Transfer Protocol Secure（HTTPS）は、サーバの暗号化とセキュアな ID を確保できるように、ハイパーテキスト転送プロトコルと SSL/TLS プロトコルを組み合せたものです。	HTTP と HTTPS の両方をサポートする Web アプリケーションには 2 つの URL が設定されています。HTTPS をサポートする Cisco Unified IP Phone は、2 つの URL のうち HTTPS URL を選択します。
IEEE 802.1X	IEEE 802.1X 標準は、許可されていないクライアントが一般にアクセス可能なポートを経由して LAN に接続できないよう制限するクライアントサーバベースのアクセス コントロールと認証プロトコルを定義します。 クライアントが認証されるまで、802.1X アクセス制御は、クライアントが接続されるポートで Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみを許可します。認証に成功した後、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 EAP-FAST、EAP-TLS、EAP-MD5 の認証方法をサポートすることによって IEEE 802.1X 標準を実装します。 802.1X 認証が電話機で有効になっている場合、PC ポートとボイス VLAN を無効にする必要があります。詳細については、「Cisco Unified IP Phone での 802.1X 認証のサポート」（P.1-19）を参照してください。
インターネット プロトコル（IP）	ネットワーク上でパケットをアドレス指定し、送信するメッセージ プロトコルです。	IP を使用した通信では、ネットワーク デバイスに IP アドレス、サブネット、およびゲートウェイを割り当てる必要があります。 ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）を指定して Cisco Unified IP Phone を使用する場合は、IP アドレス、サブネット、およびゲートウェイの識別情報が自動的に割り当てられます。DHCP を使用しない場合は、各電話機にローカル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 Unified IP Phone は、IPv4 アドレスと IPv6 アドレスを同時にサポートします。Cisco Unified Communications Manager Express で IP アドレッシング モード（IPv4 のみ、IPv6 のみ、IPv4 と IPv6 の両方）を設定します。詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』の「Internet Protocol Version 6 (IPv6)」を参照してください。
Link Layer Discovery Protocol（LLDP; リンク層検出プロトコル）	LLDP は、一部のシスコおよびサードパーティ デバイスでサポートされる（CDP と同様の）標準のネットワーク検出プロトコルです。	Cisco Unified IP Phone は、PC ポートで LLDP をサポートします。

表 1-2　Cisco Unified IP Phone がサポートしているネットワーク 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; メディア エンドポイント デバイス用リンク層検出プロトコル）	LLDP-MED は、音声製品用に開発された LLDP 標準の拡張です。	Cisco Unified IP Phone は、次のような情報を通信するために、SW ポート上で LLDP-MED をサポートします。 • ボイス VLAN 設定 • デバイス検出 • 電源管理 • コンポーネント管理 LLDP-MED サポートの詳細については、『*LLDP-MED and Cisco Discovery Protocol*』のホワイト ペーパーを参照してください。 http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
Real-Time Transport Protocol（RTP; リアルタイム転送プロトコル）	対話型の音声やビデオなどのリアルタイム データをデータ ネットワークを介して転送するための標準プロトコルです。	Cisco Unified IP Phone は、RTP プロトコルを使用して、他の電話機やゲートウェイとの間でリアルタイムの音声トラフィックを送受信します。
Real-Time Control Protocol（RTCP; リアルタイム制御プロトコル）	RTCP は RTP と共に機能し、RTP ストリーム上で QoS データ（ジッタ、遅延、およびラウンドトリップ遅延）を提供します。	RTCP はデフォルトで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。詳細については、「ネットワークの設定メニュー」（P.4-38）を参照してください。
Session Description Protocol（SDP; セッション記述プロトコル）	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の接続中に使用できるパラメータを判別します。会議の確立には、会議のすべてのエンドポイントでサポートされている SDP 機能だけが使用されます。	SDP 機能（コーデック タイプ、DTMF 検出、コンフォート ノイズなど）は、通常、動作中の Cisco Unified Communications Manager またはメディア ゲートウェイによってグローバルに設定されます。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自身で設定できるものもあります。
Session Initiation Protocol（SIP; セッション開始プロトコル）	SIP は、IP を介したマルチメディア会議用の 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層制御プロトコルであり（RFC 3261 で定義）、複数のエンドポイント間のコールの確立、維持、および終了に使用できます。	他の VoIP プロトコルと同様に、SIP はパケット テレフォニー ネットワーク内のシグナリングとセッション管理の機能を扱うように設計されています。シグナリングにより、ネットワークの境界を越えてコール情報を転送できます。セッション管理により、エンドツーエンドのコールのアトリビュートを制御できます。 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。電話機が IPv6 アドレス モードで動作している場合、Cisco Unified IP Phone は SIP プロトコルをサポートしません。
Skinny Client Control Protocol（SCCP; Skinny クライアント制御プロトコル）	SCCP には、コール制御サーバとエンドポイント クライアント（たとえば IP Phone）の間の通信を可能にするメッセージング セットが含まれています。SCCP は、シスコシステムズの独自のプロトコルです。	Cisco Unified IP Phone は、コール制御に SCCP を使用します。Cisco Unified IP Phone は、SCCP または Session Initiation Protocol（SIP）のどちらかを使用するように設定できます。

表 1-2　Cisco Unified IP Phone がサポートしているネットワーク 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; 伝送制御プロトコル）	コネクション型の転送プロトコルです。	Cisco Unified IP Phone は、TCP を使用して Cisco Unified Communications Manager に接続し、XML サービスにアクセスします。
Transport Layer Security（TLS; トランスポート層セキュリティ）	通信の保護と認証を行うための標準プロトコルです。	セキュリティが実装されている場合、Cisco Unified IP Phone は、Cisco Unified Communications Manager への安全な登録を行う際に、TLS プロトコルを使用します。 詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）	ネットワークでのファイル転送を可能にするプロトコルです。 Cisco Unified IP Phone では、TFTP を使用すると、電話機タイプ固有の設定ファイルを取得できます。	TFTP を使用するには、ネットワーク内に TFTP サーバが必要です。このサーバは、DHCP サーバから自動的に識別できます。DHCP サーバに指定された以外の TFTP サーバを電話機が使用するようにする場合、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」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）	データ パケットを配送するためのコネクションレス型メッセージ プロトコルです。	Cisco Unified IP Phone は、UDP を利用する RTP ストリームを送受信します。

Cisco Unified IP Phone での IPv6 サポート

Cisco Unified IP Phone はインターネット プロトコルを使用して、ネットワークで音声通信を提供します。Cisco Unified Communications Manager リリース 7.1 以前は、インターネット プロトコル バージョン 4（IPv4）だけがサポートされていました。32 ビット アドレスを使用するため、IPv4 はインターネットに接続できるすべてのデバイスの一意の IP アドレスの要求増加に対応できません。インターネット プロトコル バージョン 6（IPv6）は、現在のインターネット プロトコルである IPv4 の更新バージョンです。IPv6 は 128 ビット アドレスを使用し、エンドツーエンド セキュリティ機能、拡張 Quality Of Service（QoS）、および使用可能な IP アドレス数の増加に対応します。

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

Cisco Unified IP Phone は、IPv4 アドレスと IPv6 アドレスの両方を透過的にサポートするため、ユーザは慣れた電話機のすべてのコールを処理できます。Cisco Unified IP Phone は、Cisco Unified Communications Manager リリース 7.1 と Skinny Call Control Protocol（SCCP）でのみ IPv6 の使用をサポートします。

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

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

Cisco Unified Communications ネットワークでの IPv6 の導入の詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』の「Internet Protocol Version 6 (IPv6)」と『*Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 8.0*』を参照してください。

関連項目

- 「他の Cisco Unified IP Telephony 製品とのやり取りの概要」（P.2-1）
- 「電話機の起動プロセスの概要」（P.2-7）
- 「ネットワークの設定メニュー」（P.4-6）

Cisco Unified IP Phone 7962G/7942G でサポートされている機能

Cisco Unified IP Phone は、デジタル ビジネス電話機と同じように機能し、発信や着信を行うことができます。このような従来のテレフォニー機能に加えて、Cisco Unified IP Phone には、電話機をネットワーク デバイスとして管理し、モニタリングできる機能が含まれています。

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.1-9）
- 「テレフォニー機能の設定」（P.1-10）
- 「Cisco Unified IP Phone を使用したネットワーク パラメータの設定」（P.1-10）
- 「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、コール転送、リダイヤル、短縮ダイヤル、会議コール、およびボイス 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 は、この他にも多様な機能を備えています。Cisco Unified IP Phone がサポートするテレフォニー機能の概要およびそ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。

他のネットワーク デバイスと同様に、Cisco Unified IP Phone についても、Cisco Unified Communications Manager や IP ネットワーク全体にアクセスできるように設定しておく必要があります。DHCP を使用すると、電話機に設定する設定値の数が少なくなりますが、ネットワークで必要な場合には 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できます。Cisco Unified IP Phone でネットワークを設定する手順については、「Cisco Unified IP Phone の設定値の設定」を参照してください。

Cisco Unified IP Phone には、IP ネットワーク上の他のサービスやデバイスとの相互対話による拡張機能が用意されています。たとえば、Cisco Unified IP Phone を社内の Lightweight Directory Access Protocol 3（LDAP3）標準ディレクトリに統合すると、ユーザは他の社員の連絡先情報を自分の IP Phone から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 ベースの情報にアクセスすることもできます。これらのサービスの設定については、「社内ディレクトリの設定」（P.5-23）および「サービスの設定」（P.5-27）を参照してください。

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 Cisco Unified IP Phone から直接取得できます。このステータス情報は、IP Phone の使用時に発生した問題のトラブルシューティングに役立ちます。詳細については、「Cisco Unified IP Phone でのモデル情報、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とメンテナンス」（P.9-1）

テレフォニー機能の設定

Cisco Unified IP Phone に関するいくつかの設定は、Cisco Unified CM の管理から変更できます。この Web ベースのアプリケーションは、主に、電話機の登録基準やコーリング サーチ スペースの設定、社内のディレクトリやサービスの設定、および電話ボタン テンプレートの変更に使用します。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 CM の管理の詳細については、『*Cisco Unified Communications Manager Administration Guide*』を含む Cisco Unified Communications Manager のマニュアルを参照してください。また、アプリケーションに用意されているコンテキスト ヘルプをガイダンスとして使用することもできます。

Cisco Unified Communications Manager のマニュアルは、次の URL で参照できます。

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

Cisco Unified Communications Manager Business Edition のマニュアルは、次の URL で参照できます。

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 を使用したネットワーク パラメータの設定

DHCP、TFTP、IP の設定値などのパラメータは、電話機自体で設定できます。電話機の現在のコールやファームウェア バージョンに関する統計情報も取得できます。

電話機での機能の設定と統計情報の表示の詳細については、「Cisco Unified IP Phone の設定値の設定」および「Cisco Unified IP Phone でのモデル情報、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、自分が管理するネットワークや社内の Cisco Unified IP Phone ユーザから質問を受ける立場にあります。最新の機能や手順に関する情報を提供できるように、Cisco Unified IP Phone のマニュアルを十分に理解しておく必要があります。次の Cisco Unified IP Phone の Web サイトに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

このサイトでは、さまざまなユーザ ガイドを閲覧できます。

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

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主要な情報については、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の概要

Cisco Unified Communications Manager システムにセキュリティを実装すると、電話機や Cisco Unified Communications Manager サーバでのなりすまし、データ改ざん、およびコール シグナリングやメディア ストリームの改ざんを防止できます。

これらの攻撃を軽減するために、シスコの IP テレフォニー ネットワークは、電話機とサーバ間に認証および暗号化された通信ストリームを確立し、それを維持するとともに、ファイルが電話機に転送される前にそのファイルにデジタル署名します。また、Cisco Unified IP Phone 間のメディア ストリームおよびコール シグナリングの暗号化も行います。

Cisco Unified IP Phone 7962G/7942G は、電話機のセキュリティ プロファイルを使用します。このプロファイルでは、デバイスが非セキュア、認証済み、または暗号化済みのいずれであるかが定義されます。セキュリティ プロファイルを電話機に適用する方法については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

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

表 1-3 は、本書および他のマニュアルに記載されているセキュリティに関する追加情報の参照先を示しています。

表 1-3　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
Cisco Unified Communications Manager および Cisco Unified IP Phone のセットアップ、設定、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説明	『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。
Cisco Unified IP Phone でサポートされ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。
セキュリティ機能に関する制約事項	「セキュリティの制約事項」（P.1-21）を参照してください。

表 1-3　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
セキュリティ プロファイル名の表示	「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。
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、および保護コールの識別」（P.1-16）を参照してください。
TLS 接続	• 「使用するネットワーク プロトコル」（P.1-5）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.2-9）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の概要」（P.2-7）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.2-9）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、電話機の TFTP サーバ 1 または TFTP サーバ 2 オプションの変更	「ネットワークの設定メニュー」（P.4-6）の表 4-2 を参照してください。
電話機の [デバイス設定（Device Configuration）] メニューにある Unified CM1 ～ Unified CM5 の各オプションのセキュリティ アイコンの確認	「Unified CM の設定メニュー」（P.4-21）を参照してください。
電話機の [デバイス設定（Device Configuration）] メニューからアクセスできる [セキュリティ設定（Security Configuration）] メニューの項目	「セキュリティ設定メニュー」（P.4-36）を参照してください。
電話機の [設定（Settings）] メニューからアクセスできる [セキュリティ設定（Security Configuration）] メニューの項目	「セキュリティ設定メニュー」（P.4-43）を参照してください。
CTL ファイルおよび ITL ファイルのロック解除	「CTL および ITL ファイルのロック解除」（P.4-45）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有効化および無効化」（P.8-3）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.9-13）を参照してください。
電話機のリセットと復旧	「Cisco Unified IP Phone のリセットまたは復元」（P.9-13）を参照してください。

表 1-3　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
シスコ エクステンション モビリティ HTTPS のサポート	「使用するネットワーク プロトコル」（P.1-5）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。 • 「Cisco Unified IP Phone での 802.1X 認証のサポート」（P.1-19） • 「セキュリティ設定メニュー」（P.4-36） • 「ステータス メニュー」（P.7-2） • 「Cisco Unified IP Phone のセキュリティのトラブルシューティング」（P.9-9）

サポートされているセキュリティ機能の概要

表 1-4 は、Cisco Unified IP Phone 7962G/7942G の電話機がサポートしているセキュリティ機能の概要を説明しています。これらの機能の詳細、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 Security Guide*』を参照してください。

電話機の現在のセキュリティ設定を参照するには、[設定（Settings）] > [セキュリティ設定（Security Configuration）] を選択し、[設定（Settings）] > [デバイス設定（Device Configuration）] > [セキュリティ設定（Security Configuration）] を選択します。詳細については、「セキュリティ設定メニュー」（P.4-36）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にだけ利用可能になります。CTL の詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Configuring the Cisco CTL Client」を参照してください。

表 1-4　セキュリティ機能の概要

機能	説明
イメージの認証	ファームウェア イメージが電話機にロードされる前に、署名付きバイナリ ファイル（拡張子 .sbn）を使用して、ファームウェア イメージに対する改ざんを防止します。イメージが改ざんされると、電話機は認証プロセスに失敗し、そのイメージを拒否します。
お客様サイトの証明書のインストール	各 Cisco Unified IP Phone は、デバイス認証に使用する固有の証明書を要求します。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）が含まれていますが、Cisco Unified CM の管理で Certificate Authority Proxy Function（CAPF）を使用して証明書がインストールされることを指定して、セキュリティを強化できます。または、電話機の [セキュリティ設定（Security Configuration）] メニューから Locally Significant Certificate（LSC; ローカルで有効な証明書）をインストールできます。詳細については、「Cisco Unified IP Phone のセキュリティ設定」（P.3-15）を参照してください。

表 1-4　セキュリティ機能の概要（続き）

機能	説明
デバイスの認証	各エンティティが他のエンティティの証明書を受信したときに、Cisco Unified Communications Manager サーバと電話機の間で実行されます。デバイス認証は、電話機と Cisco Unified Communications Manager の間で安全な接続が行われるかどうかを判別します。また、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安全なシグナリング パスを作成します。Cisco Unified Communications Manager は、認証できない電話機は登録しません。
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検証します。電話機は、署名を検証して、ファイル作成後にファイルが改ざんされていないことを確認します。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て、それ以上処理しません。
シグナリングの認証	TLS プロトコルを使用して、伝送中のシグナリング パケットに対して改ざんが行わ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 は、デバイス認証に使用する固有の、製造元でインストールされる証明書（MIC）が含まれています。MIC は、個々の電話機を識別するために長期的に割り当てられた証明であり、Cisco Unified Communications Manager はこれを使用して電話機を認証します。
セキュアな Survivable Remote Site Telephony（SRST）リファレンス	セキュリティのために SRST リファレンスを設定し、Cisco Unified Communications Manager 管理ページで依存デバイスをリセットした後、TFTP サーバは SRST 証明書を電話機の cnf.xml ファイルに追加して、ファイルを電話機に送ります。その後、セキュアな電話機は TLS 接続を使用して SRST 対応のルータと対話します。
メディアの暗号化	SRTP を使用して、サポートされているデバイス間のメディア ストリームをセキュリティで保護するとともに、目的のデバイスだけがデータを受信して読み取ることができるようにします。具体的には、デバイスのメディア マスター キー ペアの作成、デバイスへのキーの送信、および転送中のキーの送信に対するセキュリティ保護を行います。
シグナリングの暗号化	デバイスと Cisco Unified Communications Manager サーバ間で送信されるすべての SCCP と SIP シグナリング メッセージを暗号化します。
Certificate Authority Proxy Function（CAPF）	非常に煩雑な証明書生成手順の一部を電話機のために実行します。また、電話機と相互対話しながら、キーの生成と証明書のインストールを行います。電話機に代わって、お客様固有の認証局から証明書を要求するように 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設定できます。
セキュリティ プロファイル	電話機が非セキュア、認証済み、暗号化済み、または保護済みのいずれであるかを定義します。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）	電話機の多様な操作統計情報を表示する Web ページへのアクセスを禁止できます。

表 1-4　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の強化	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。 • 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（Setting）] メニューへのアクセスの無効化、またはアクセス制限（[ユーザ設定（User Preferences）] メニューへのアクセスおよび音量の設定変更の保存だけを許可する） • 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（PC Port Disabled）]、[GARP を使う（GARP Enabled）]、および [ボイス VLAN を使う（Voice VLAN enabled）] の現在の設定値を表示するには、電話機の [セキュリティ設定（Security Configuration）] メニューを調べます。詳細については、「デバイス設定メニュー」（P.4-20）を参照してください。
802.1X 認証	Cisco Unified IP Phone は 802.1X 認証を使用して、ネットワークへのアクセスを要求し、アクセスできます。詳細については、「Cisco Unified IP Phone での 802.1X 認証のサポート」（P.1-19）を参照してください。

関連項目

- 「セキュリティ プロファイルについて」（P.1-15）
- 「認証、暗号化、および保護コールの識別」（P.1-16）
- 「セキュリティの制約事項」（P.1-21）
- 「デバイス設定メニュー」（P.4-20）

セキュリティ プロファイルについて

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

電話機に設定されているセキュリティ モードを表示するには、[セキュリティ設定（Security Configuration ）] メニューの [セキュリティ モード（Security Mode ）] 設定を確認してください。詳細については、「セキュリティ設定メニュー」（P.4-36）を参照してください。

関連項目

- 「認証、暗号化、および保護コールの識別」（P.1-16）
- 「セキュリティの制約事項」（P.1-21）
- 「デバイス設定メニュー」（P.4-20）

認証、暗号化、および保護コールの識別

電話機にセキュリティが実装されている場合、認証および暗号化されたコールは、電話機のスクリーンに表示されるアイコンで識別できます。セキュリティ トーンがコールの最初に再生されると、接続されている電話機がセキュアで保護されているかどうかを判断することもできます。

コールが認証された場合、そのコールの確立に関与したすべてのデバイスは信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されます。進行中のコールが認証されると、電話機の LCD スクリーンの通話時間を表示するタイマーの右側にあるコールの状態を示すアイコンが  アイコンに変わります。

コールが暗号化された場合、そのコールの確立に関与したすべてのデバイスは信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されます。またコール シグナリングとメディア ストリームも暗号化されます。コールを暗号化することで高いレベルのセキュリティが確保され、コールの完全性とプライバシーが保たれます。進行中のコールが暗号化されると、電話機の LCD スクリーンの通話時間を表示するタイマーの右側にあるコールの状態を示すアイコンが  アイコンに変わります。

（注） IP 以外のコール レッグ（たとえば PSTN）を介してルーティングされるコールは、IP ネットワーク内では暗号化されているとしても、またロック アイコンがそのコールに関連付けられているとしても、非セキュアになります。

コールが保護された場合、コールの最初にセキュリティ トーンが再生され、他の接続された電話機も暗号化されたオーディオとビデオ（ビデオが関係している場合）を受信し、送信していることを示します。コールが保護されていない電話機に接続されている場合、セキュリティ トーンは再生されません。

（注） 保護コールは、2 つの電話機間の接続でのみサポートされます。保護コールが設定されている場合、会議コール、共有回線、エクステンション モビリティ、回線をまたいで参加などの一部の機能は使用できません。保護されているコールは認証されません。

関連項目

- 「セキュリティ プロファイルについて」（P.1-15）
- 「Cisco Unified IP Phone のセキュリティ機能の概要」（P.1-11）
- 「セキュリティの制約事項」（P.1-21）

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 レベルをモニタリングできます。セキュアな会議コールは、次の手順で確立します。

1. ユーザはセキュアな電話機（暗号化または認証されたセキュリティ モード）から会議を開始します。
2. Cisco Unified Communications Manager がセキュアな会議ブリッジをコールに割り当てます。
3. 参加者が追加されると、Cisco Unified Communications Manager は（暗号化または認証された）各電話機のセキュリティ モードを確認し、会議のセキュリティ レベルを維持します。
4. 電話機は会議コールのセキュリティ レベルを表示します。セキュアな会議には、電話スクリーンの「会議」の右側に  （暗号化済み）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 モードとセキュアな会議ブリッジのアベイラビリティ応じて、会議コールのセキュリティ レベルに影響を与える相互作用、制約事項、および制限事項があります。これらの相互作用については、表 1-5 と表 1-6 を参照してください。

保護コールの確立と識別

保護コールは、電話機、およびもう一方の電話機が保護コール用に設定されると確立されます。もう一方の電話機は同じ Cisco IP ネットワークまたは IP ネットワーク外のネットワークに配置できます。保護コールは 2 つの電話機間でのみ可能です。会議コールやその他の複数回線のコールはサポートされていません。

保護コールは、次の手順で確立します。

1. ユーザは保護された電話機（保護されたセキュリティ モード）からコールを開始します。
2. 電話機は電話スクリーン上に  アイコン（暗号化済み）を表示します。このアイコンは、電話機がセキュアな（暗号化された）コール用に設定されていることを示しますが、これは他の接続された電話機も保護されていることを意味するものではありません。
3. コールが別の保護された電話機に接続されるとセキュリティ トーンが再生され、会話の双方が暗号化され、保護されていることを示します。コールが保護されていない電話機に接続されると、セキュリティ トーンは再生されません。

（注）　保護コールは、2 つの電話機間の会話でサポートされます。保護コールが設定されている場合、会議コール、共有回線、シスコ エクステンション モビリティ、回線をまたいで参加などの一部の機能は使用できません。

コールのセキュリティの相互作用と制約事項

会議が確立されると、Cisco Unified Communications Manager は、電話機のセキュリティのステータスを確認し、会議のセキュリティ指示を変更するか、コールの完了を阻止してシステムの完全性とセキュリティを維持します。表 1-5 は、割り込みを使用している場合のコールのセキュリティ レベルの変更についての情報を記載しています。

表 1-5　割り込みを使用している場合のコールのセキュリティの相互作用

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	操作の結果
非セキュア	割り込み	暗号化されたコール	割り込まれたコールと非セキュア コールと識別されたコール
セキュア（暗号化済み）	割り込み	認証されたコール	割り込まれたコールと認証されたコールと識別されたコール
セキュア（認証済み）	割り込み	暗号化されたコール	割り込まれたコールと認証されたコールと識別されたコール
非セキュア	割り込み	認証されたコール	割り込まれたコールと非セキュア コールと識別されたコール

表 1-6 は、発信側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、セキュアな会議ブリッジのアベイラビリティに応じた会議のセキュリティ レベルの変更についての情報を記載しています。

表 1-6　会議コールのセキュリティの制約事項

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	操作の結果
非セキュア	会議	暗号化または認証済み	非セキュアな会議ブリッジ 非セキュアな会議
セキュア（暗号化または認証済み）	会議	少なくとも 1 人のメンバが非セキュア	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	参加者すべてが暗号化済み	セキュアな会議ブリッジ セキュアな暗号化済みレベル会議
セキュア（認証済み）	会議	参加者すべてが暗号化または認証済み	セキュアな会議ブリッジ セキュアな認証済みレベル会議
非セキュア	会議	暗号化または認証済み	セキュアな会議ブリッジのみが使用可能で使用中 非セキュアな会議
セキュア（暗号化または認証済み）	会議	暗号化または認証済み	Cisco Unified IP Phone 7962G および 7942G 非セキュアな会議ブリッジのみが使用可能で使用中 非セキュアな会議 Cisco Unified IP Phone 7961G および 7941G 会議はセキュアなまま 参加者の 1 人がコールを MOH で保留しようとすると、MOH が再生されない
セキュア（暗号化または認証済み）	会議	Cisco Unified IP Phone 7962G および 7942G の場合： 暗号化またはセキュア Cisco Unified IP Phone 7961G および 7941G の場合： メンバがコールを MOH で保留	Cisco Unified IP Phone 7962G および 7942G の場合： 会議はセキュアなまま 参加者の 1 人がコールを MOH で保留しようとすると、MOH が再生されない Cisco Unified IP Phone 7961G および 7941G の場合： 保留時に音楽は再生されない 会議はセキュアなまま
セキュア（暗号化済み）	参加	暗号化または認証済み	セキュアな会議ブリッジ 会議はセキュアなまま（暗号化または認証済み）
非セキュア	C 割り込み	参加者すべてが暗号化済み	セキュアな会議ブリッジ 会議は非セキュアに変更
非セキュア	ミートミー	最低限のセキュリティ レベルは暗号化済み	発信側が「セキュリティ レベルを満たしていません（Does not meet Security Level）」というメッセージを受信し、コールは拒否される

表 1-6　会議コールのセキュリティの制約事項（続き）

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	操作の結果
セキュア（暗号化済み）	ミートミー	最低限のセキュリティ レベルは認証済み	セキュアな会議ブリッジ 会議は暗号化されたコールと認証されたコールを受け入れ
セキュア（暗号化済み）	ミートミー	最低限のセキュリティ レベルは非セキュア	セキュアな会議ブリッジのみが使用可能で使用中 会議はすべてのコールを受け入れ

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

ここでは、Cisco Unified IP Phone での 802.1X のサポートについての情報を記載します。

- 「概要」（P.1-19）
- 「必要なネットワーク コンポーネント」（P.1-19）
- 「ベスト プラクティス：要件と推奨事項」（P.1-20）

概要

Cisco Unified IP phones と Cisco Catalyst スイッチは従来、互いを識別し、VLAN 割り当てやインライン パワー要件などのパラメータを特定するために Cisco Discovery Protocol（CDP）を使用してきました。しかし、ローカルに接続された PC を識別するために CDP は使用されません。このため、Cisco Unified IP Phone は EAPOL パススルー メカニズムを使用します。これによって、IP 電話にローカルに接続された PC は EAPOL メッセージを LAN スイッチで 802.1X オーセンティケータにパススルーする場合があります。これは、IP 電話がオーセンティケータとして機能するのを防ぎますが、ネットワークにアクセスする前に LAN スイッチがデータ エンド ポイントを認証するのを許可します。

EAPOL パススルー メカニズムと共に、Cisco Unified IP Phone はプロキシ EAPOL ログオフ メカニズムを提供します。ローカルに接続された PC が IP 電話から接続切断されても、LAN スイッチと IP 電話間のリンクが維持されるため、LAN スイッチは物理リンクの障害を認識しません。ネットワークの完全性が脅かされるのを避けるため、IP 電話はダウンストリーム PC の代わりに EAPOL ログオフ メッセージをスイッチに送ります。これは、LAN スイッチにダウンストリーム PC の認証エントリをクリアさせます。

Cisco Unified IP Phone には、EAPOL パススルー メカニズムだけでなく 802.1X サプリカントも含まれます。このサプリカントはネットワーク管理者が IP 電話の LAN スイッチ ポートへの接続を制御するのを許可します。電話の 802.1X サプリカントの現行のリリースはネットワーク認証に EAP-FAST、EAP-TLS、および EAP-MD5 オプションを使用します。

必要なネットワーク コンポーネント

Cisco Unified IP Phone での 802.1X 認証のサポートには、次のコンポーネントを含むいくつかのコンポーネントが必要です。

- Cisco Unified IP Phone：電話機は 802.1X *サプリカント*として機能します。これはネットワークへのアクセス要求を開始します。
- Cisco Secure Access Control Server（ACS）（またはその他のサードパーティの認証サーバ）：認証サーバと電話機はどちらも電話機の認証に使用される共有秘密で設定される必要があります。

- Cisco Catalyst Switch（またはその他のサードパーティのスイッチ）：スイッチは 802.1X をサポートする必要があります。このため、*オーセンティケータ*として機能し、電話機と認証サーバ間でメッセージを送信できます。やり取りが完了すると、スイッチはネットワークへの電話機アクセスを許可または拒否します。

ベスト プラクティス：要件と推奨事項

- 802.1X の有効化：802.1X 標準を Cisco Unified IP Phone の認証に使用する場合、電話機で有効にする前に他のコンポーネントを正しく設定していることを確認してください。詳細については、「802.1X 認証およびステータス」（P.4-48）を参照してください。
- PC ポートの設定：802.1X 標準は VLAN の使用を考慮しないため、各スイッチ ポートにデバイスを 1 つだけ認証することをお勧めします。しかし、一部のスイッチ（Cisco Catalyst スイッチを含む）はマルチドメイン認証をサポートします。スイッチ設定によって PC を電話機の PC ポートに接続できるかどうかが決まります。
  - 有効化：マルチドメイン認証をサポートするスイッチを使用している場合、PC ポートを有効にして PC を接続できます。この場合、Cisco Unified IP Phone はスイッチと接続された PC 間の認証のやり取りをモニタリングするために、プロキシ EAPOL ログオフをサポートします。Cisco Catalyst スイッチでの IEEE 802.1X サポートの詳細については、次の場所にある Cisco Catalyst のスイッチ設定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
  - 無効化：スイッチが同じポートで複数の 802.1X 互換デバイスをサポートしない場合、802.1X 認証を有効にすると PC ポートを無効にする必要があります。詳細については、「セキュリティ設定メニュー」（P.4-36）を参照してください。このポートを無効にせずにその後 PC を接続しようとすると、スイッチは電話機と PC の両方へのネットワーク アクセスを拒否します。
- ボイス VLAN の設定：802.1X 標準が VLAN を考慮しないため、スイッチのサポートに基づいてこの設定を行う必要があります。
  - 有効化：マルチドメイン認証をサポートするスイッチを使用している場合、ボイス VLAN を継続して使用できます。
  - 無効化：スイッチがマルチドメイン認証をサポートしない場合、ボイス VLAN を無効にしてポートのネイティブ VLAN への割り当てを検討します。詳細については、「セキュリティ設定メニュー」（P.4-36）を参照してください。
- MD5 共有秘密の入力：802.1X 認証を無効にするか、電話機を出荷時の状態にリセットすると、以前に設定した MD5 共有秘密は削除されます。詳細については、「802.1X 認証およびステータス」（P.4-48）を参照してください。

セキュリティの制約事項

割り込みに使用される電話機に暗号化が設定されていない場合、ユーザは暗号化されたコールに対して割り込みを実行できません。この場合、割り込みが失敗したときに、割り込みを実行した電話機でリオーダー音（速いビジー音）が再生されます。

発信側の電話機に暗号化が設定されている場合、割り込みの発信側は、暗号化された電話機から認証されたコールまたは非セキュア コールに対して割り込みを実行できます。Cisco Unified Communications Manager は、割り込みが実行されたコールを非セキュアとして分類します。

発信側の電話機に暗号化が設定されている場合、割り込みの発信側は、暗号化されたコールに対して割り込みを実行でき、その電話機は対象のコールが暗号化されていることを示します。

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

Cisco Unified IP Phone の設定と設置の概要

IP テレフォニー システムの導入時に、システム管理者とネットワーク管理者は初期設定タスクを実行して、IP テレフォニー サービス用にネットワークを準備する必要があります。完全な IP テレフォニー ネットワークのセットアップと設定のための情報とチェックリストについては、『*Cisco Unified Communications Manager System Guide*』の「System Configuration Overview」の章を参照してください。

Cisco Unified Communications Manager で IP テレフォニー システムをセットアップし、システム全体の機能を設定した後、IP Phone をシステムに追加できます。

次のトピックでは、Cisco Unified IP Phone をネットワークに追加する手順の概要を説明します。

- 「Cisco Unified Communications Manager での Cisco Unified IP Phone の設定」（P.1-21）
- 「Cisco Unified IP Phone の設置」（P.1-24）

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、次の方法を使用できます。

- 自動登録
- Cisco Unified Communications Manager Administration
- BAT（Bulk Administration Tool）
- 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.2-9）を参照してください。

Cisco Unified Communications Manager での電話機の設定の詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phone」を参照してください。

Cisco Unified Communications Manager 管理ページでの Cisco Unified IP Phone 7962G/7942G の設定のためのチェックリスト

表 1-7 は、Cisco Unified CM の管理で Cisco Unified IP Phone 7962G/7942G を設定する際のタスクの概要とチェックリストです。このリストでは、電話機の設定プロセスを手順に沿って示しています。一部のタスクはオプションです。システムやユーザの必要に応じて実行します。これらの手順の詳細については、参照先欄の資料を参照してください。

表 1-7　Cisco Unified Communications Manager での Cisco Unified IP Phone 7962G/7942G の設定のためのチェックリスト

タスク	目的	参照先
1.	電話機に関する次の情報を収集します。 • 電話機のモデル • MAC アドレス • 電話機が設置される物理的な場所 • 電話機のユーザの名前とユーザ 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 • 電話機に割り当てる回線数と関連付けられた電話番号（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、電話機の機能、IP Phone サービス、または電話機のアプリケーションに影響を与える電話機の使用情報 電話機をセットアップするための設定要件のリストを提供します。 個別の電話機を設定する前に実行が必要な、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予備設定を明確にします。	『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」を参照してください。 「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。
2.	必要であれば、電話ボタン テンプレートをカスタマイズします。 ユーザ ニーズに合せて回線ボタン、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ます。 IPv4 アドレスでサービス URL を指定する必要があります。	『*Cisco Communications Manager Administration Guide*』の「Phone Button Template Configuration」を参照してください。 「電話ボタン テンプレートの変更」（P.5-24）を参照してください。

表 1-7　Cisco Unified Communications Manager での Cisco Unified IP Phone 7962G/7942G の設定のためのチェックリスト（続き）

タスク	目的	参照先
3.	[電話の設定（Phone Configuration）] ウィンドウの必須フィールドに入力して、電話機を追加し、設定します。必須フィールドは、フィールド名の隣のアスタリスク（*）で示されています。たとえば、MAC アドレスやデバイス プールなどです。 デバイスをデフォルト設定で Cisco Unified Communications Manager データベースに追加します。	『*Cisco Communications Manager Administration Guide*』の「Cisco Unified IP Phone Configuration」を参照してください。 [プロダクト固有の設定（Product Specific Configuration）] フィールドの詳細については、[電話の設定（Phone Configuration）] ウィンドウの [?] ボタンを押して表示されるヘルプを参照してください。
4.	[電話番号の設定（Directory Number Configuration）] ウィンドウの必須フィールドに入力して、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、フィールド名の隣のアスタリスク（*）で示されています。たとえば、ディレクトリ番号やプレゼンス グループなどです。 プライマリ電話番号とセカンダリ電話番号、および電話番号に関連する機能を電話機に追加します。	『*Cisco Unified Communications Manager Administration Guide*』の「Directory Number Configuration」を参照してください。 「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。
5.	ソフトキー テンプレートをカスタマイズします。 ユーザのソフトキーの使用方法に合せて、電話機に表示されるソフトキー機能の追加、削除、表示順序の変更を行います。	『*Cisco Unified Communications Manager Administration Guide*』の「Softkey Template Configuration」を参照してください。 「ソフトキー テンプレートの設定」（P.5-26）を参照してください。
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）。 短縮ダイヤルのボタンおよび番号を追加します。 **（注）** ユーザは、Cisco Unified CM のユーザ オプションで、使用している電話機の短縮ダイヤル設定を変更できます。	『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Configuration」の章の「Configuring Speed-Dial Buttons」の項を参照してください。
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 のサービスを提供します。 **（注）** ユーザは、Cisco Unified CM ユーザ オプションで、使用している電話機のサービスを追加または変更できます。 **（注）** IPv4 アドレスでサービス URL を指定する必要があります。	『*Cisco Communications Manager Administration Guide*』の「Cisco Unified IP Phone Services Configuration」を参照してください。 「サービスの設定」（P.5-27）を参照してください。
8.	サービスを電話ボタンに割り当てます（オプション）。 ボタンを 1 回押すだけで IP Phone サービスまたは URL にアクセスできるようにします。	『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Configuration」の章の「Adding a Cisco Unified IP Phone Service to a Phone Button」の項を参照してください。

表 1-7　Cisco Unified Communications Manager での Cisco Unified IP Phone 7962G/7942G の設定のためのチェックリスト（続き）

タスク	目的	参照先
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。必須フィールドはアスタリスク（*）で示されています。たとえば、ユーザ ID や姓などです。 （注）　パスワード（ユーザ オプション Web ページ用）と PIN（エクステンション モビリティおよびパーソナル ディレクトリ用）を割り当てます。 Cisco Unified Communications Manager のグローバル ディレクトリにユーザ情報を追加します。	『*Cisco Unified Communications Manager Administration Guide*』の「End User Configuration」を参照してください。 「Cisco Unified Communications Manager へのユーザの追加」（P.5-28）を参照してください。 （注）　ユーザの情報を保存するために会社が Lightweight Directory Access Protocol（LDAP）ディレクトリを使用している場合、既存の LDAP ディレクトリを使用するために Cisco Unified Communications をインストールして設定できます。「社内ディレクトリの設定」（P.5-23）を参照してください。 （注）　電話機とユーザの両方を同時に Cisco Unified Communications Manager データベースに追加するには、『*Cisco Unified Communications Manager Administration Guide*』の「User/Phone Add Configuration」の章を参照してください。
10.	ユーザをユーザ グループに追加します。 ユーザをユーザ グループ内のすべてのユーザに適用されるロールと許可のコモン リストに割り当てます。管理者はユーザ グループ、ロール、許可を管理して、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 Administration Guide*』の次の項を参照してください。 • 「End User Configuration」の章の「End User Configuration Settings」の項 • 「User Group Configuration」の章の「Adding Users to a User Group」の項
11.	ユーザを電話機に関連付けます（オプション）。 ユーザが、コール転送や短縮ダイヤルの追加などの電話機能やサービスを設定できるようにします。 （注）　会議室の電話機など、ユーザを関連付けない電話機もあります。	『*Cisco Unified Communications Manager Administration Guide*』の「End User Configuration」の章の「Associating Devices to a User」の項を参照してください。

Cisco Unified IP Phone の設置

電話機を Cisco Unified Communications Manager データベースに追加したら、次は電話機を設置します。電話機は、ユーザの指定する場所に設置できます。Cisco.com Web サイトで入手できる『Cisco Unified IP Phone Installation Guide』では、電話機の受話器、ケーブル、その他のアクセサリを取り付ける手順を説明しています。

（注）　新しく購入した電話機であっても、最新のファームウェア イメージにアップグレードする必要があります。電話機のアップグレードの詳細については、http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser にある Readme ファイルを参照してください。

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し、電話機が Cisco Unified Communications Manager に登録されます。最後に、DHCP サービスを有効にするか無効にするかによって、電話機の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、電話機とユーザの関連付けやボタン テーブルの変更、電話番号など、電話機に関する特定の設定情報を更新する必要があります。

Cisco Unified IP Phone 7962G/7942G の設置に関するチェックリスト

表 1-8 は、Cisco Unified IP Phone 7962G/7942G を設置する際のタスクの概要とチェックリストです。このリストでは、電話機の設置作業を手順に沿って示しています。一部のタスクはオプションです。システムやユーザの必要に応じて実行します。これらの手順の詳細については、参照先欄の資料を参照してください。

表 1-8　Cisco Unified IP Phone 7962G/7942G の設置に関するチェックリスト

タスク	目的	参照先
1.	電話機の電源を次の中から選択します。 • Power over Ethernet（PoE） • 外部電源 電話機に電力を供給する方法を決定します。	「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、配置を調整して、ネットワーク ケーブルを接続します。 電話機を配置し、ネットワークに設置します。	「Cisco Unified IP Phone の設置」（P.3-6）を参照してください。 「Cisco Unified IP Phone の機能キー容量増加」（P.3-10）を参照してください。
3.	Cisco Unified IP Phone 拡張モジュールを追加します。 デバイスをデフォルト設定で Cisco Unified Communications Manager データベースに追加します。 14（7914）または 24（7915 および 7916）のライン アピアランスまたは短縮ダイヤル番号を追加して、Cisco Unified IP Phone 7962G の機能を拡張します。 14（7914）のライン アピアランスまたは短縮ダイヤル番号を追加して、Cisco Unified IP Phone 7961G および 7961G-GE の機能を拡張します。 （注）　Cisco Unified IP Phone 7914 拡張モジュールは、Cisco Unified IP Phone 7942G、7941G、および 7941G-GE ではサポートされていません。 （注）　Cisco Unified IP Phone 7915 および 7916 拡張モジュールは、Cisco Unified IP Phone 7942G、7961G、7961G-GE、7941G、および 7941G-GE ではサポートされていません。 （注）　Cisco Unified IP Phone 7975G では最大 56 の鍵を設定でき、Cisco Unified IP Phone 7965G および 7962G では最大 54 の鍵を設定できます。	「Cisco Unified IP Phone 拡張モジュールの取り付け」（P.3-9）を参照してください。

表 1-8　Cisco Unified IP Phone 7962G/7942G の設置に関するチェックリスト（続き）

タスク	目的	参照先
4.	電話機の起動プロセスをモニタリングします。 プライマリ電話番号とセカンダリ電話番号、および電話番号に関連する機能を電話機に追加します。 電話機が正しく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.3-14）を参照してください。

表 1-8　Cisco Unified IP Phone 7962G/7942G の設置に関するチェックリスト（続き）

タスク	目的	参照先
5.	IPv4 ネットワーク用の電話機のネットワーク設定行っている場合、DHCP を使用するか IP アドレスを手入力して電話機の IP アドレスを設定できます。 DHCP を使用する場合：DHCP を有効にし、DHCP サーバが自動的に IP アドレスを Cisco Unified IP Phone に自動的に割り当てられるようにし、電話機を TFTP サーバに割り当てるには、[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv4 設定（IPv4 Configuration）] を選択して次を設定します。 • DHCP を有効にするには、[DHCP を使う（DHCP Enabled）] を [Yes] に設定します。DHCP はデフォルトで有効になっています。 • 代替 TFTP サーバを使用するには、[代替 TFTP サーバ（Alternate TFTP Server）] を [Yes] に設定し、TFTP サーバの IP アドレスを入力します。 （注）　DHCP によって割り当てられた TFTP サーバの代わりに代替の TFTP サーバを割り当てる必要があるか判断する場合は、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：IP アドレス、サブネットマスク、TFTP サーバ、およびデフォルトのルータを電話機でローカルに設定する必要があります。[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv4 設定（IPv4 Configuration）] を選択します。 DHCP を無効にして IP アドレスを手動で設定するには、次の手順を実行します。 a. DHCP を無効にするには、[DHCP を使う（DHCP Enabled）] を [No] に設定します。 b. 電話機の固定 IP アドレスを入力します。 c. サブネット マスクを入力します。 d. デフォルトのルータ IP アドレスを入力します。 e. [代替 TFTP サーバ（Alternate TFTP Server）] を [Yes] に設定し、TFTP サーバ 1 の IP アドレスを入力します。 [設定（Settings）] > [ネットワークの設定（Network Configuration）] を選択して、電話機のあるドメイン名も入力する必要があります。 Cisco Unified IP Phone では、IPv4 アドレスと IPv6 アドレスを同時に持つことができます。IPv4 アドレスのみ、IPv6 アドレスのみ、IPv4 アドレスと IPv6 アドレスの両方をサポートするよう Cisco Unified Communications Manager を設定できます。	「起動時のネットワーク設定値の設定」（P.3-15）を参照してください。 「ネットワークの設定メニュー」（P.4-6）を参照してください。

表 1-8　Cisco Unified IP Phone 7962G/7942G の設置に関するチェックリスト（続き）

タスク	目的	参照先
6.	IPv6 ネットワーク用の電話機のネットワーク設定行っている場合、DHCPv6 を使用するか IP アドレスを手入力して電話機の IP アドレスを設定できます。 DHCPv6 を使用する場合：DHCPv6 を有効にし、DHCPv6 サーバが自動的に IP アドレスを Cisco Unified IP Phone に自動的に割り当てられるようにし、電話機を TFTP サーバに割り当てるには、[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv6 設定（ IPv6 Configuration）] を選択して次を設定します。 • DHCPv6 を有効にするには、[DHCPv6] を [はい（Yes）] に設定します。DHCPv6 はデフォルトで有効になっています。 • 代替 TFTP サーバを使用するには、[IPv6 代替 TFTP サーバ（IPv6 Alternate TFTP Server）] を [はい（Yes）] に設定し、IPv6 TFTP サーバ 1 の IP アドレスを入力します。 （注）　DHCP によって割り当てられた TFTP サーバの代わりに代替の TFTP サーバを割り当てる必要がある場合は、ネットワーク管理者に相談してください。 DHCP を使用しない場合：IP アドレス、サブネットマスク、TFTP サーバを電話機でローカルに設定する必要があります。[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv6 設定（IPv6 Configuration）] を選択します。 DHCP を無効にして IP アドレスを手動で設定するには、次の手順を実行します。 a. DHCPv6 を無効にするには、[DHCPv6] を [いいえ（No）] に設定します。 b. 電話機の固定 IP アドレスを入力します。 c. IPv6 プレフィクス長を入力します。 d. [IPv6 代替 TFTP サーバ（IPv6 Alternate TFTP Server）] を [はい（Yes）] に設定し、IPv6 TFTP サーバ 1 の IP アドレスを入力します。 [設定（Settings）] > [ネットワークの設定（Network Configuration）] を選択して、電話機のあるドメイン名も入力する必要があります。 （注）　Cisco Unified IP Phone では、IPv4 アドレスと IPv6 アドレスを同時に持つことができます。IPv4 デバイスのみ、IPv6 デバイスのみ、IPv4 デバイスと IPv6 デバイスの両方をサポートするよう Cisco Unified Communications Manager を設定できます。	「起動時のネットワーク設定値の設定」（P.3-15）を参照してください。 「ネットワークの設定メニュー」（P.4-6）を参照してください。

表 1-8　Cisco Unified IP Phone 7962G/7942G の設置に関するチェックリスト（続き）

タスク	目的	参照先
7.	電話機にセキュリティ機能を設定します。 データ改ざんやなりすましから保護します。	「Cisco Unified IP Phone のセキュリティ設定」（P.3-15）を参照してください。
8.	Cisco Unified IP Phone で電話をかけます。 電話機や機能が正しく動作することを確認します。	『*Cisco Unified IP Phone 7962G and 7942G Phone Guide*』および『*Cisco Unified IP Phone 7961G/7961G-GE or 7941G/7941G-GE Phone Guide*』を参照してください
9.	電話機の使用方法と電話オプションの設定方法をエンド ユーザに知らせます。 Cisco Unified IP Phone を正しく使用するために必要な情報をユーザが持っていることを確認します。	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。