Cisco Unified IP Phone 7931G

The Cisco Unified IP Phone 7931G は、VoIP ネットワークを介した通信を可能にするためのすべての機能が搭載された電話機です。 従来のキー セットに精通したユーザ向けに設計されたこの電話機は、デジタル ビジネス フォンとほぼ同様に機能し、電話コールの発受信に加えて、ミュート、保留、転送、スピード ダイヤル、コール転送などの機能を使用できます。

さらに、Cisco Unified IP Phone はユーザのデータ ネットワークに接続できるため、ネットワーク情報およびサービスへのアクセス、カスタマイズされた機能およびサービスの使用など、強力なIPテレフォニー機能を利用できます。 ファイルおよびデバイスの認証、シグナリングの暗号化、メディアの暗号化などのセキュリティ機能もサポートします。

Cisco Unified IP Phone 7931G は、バックライト付きのピクセルベースのディスプレイ、24 個の設定可能な回線ボタン、およびその他の多様な機能を備え、中規模の電話機トラフィックと固有のコール要件を持つ企業のニーズに対応します。 専用の保留、リダイヤル、および転送キーにより容易なコール操作を実現します。 点灯式のミュート キーおよびスピーカーフォン キーにより、スピーカーの状態が明確に示されます。

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.711u、G.722、G.729a、G.729ab、iLBC をエンコードし、G.711a、G.711u、G.722、および iLBC をデコードします。 また、非圧縮ワイドバンド（16 ビット、16 kHz）オーディオもサポートします。

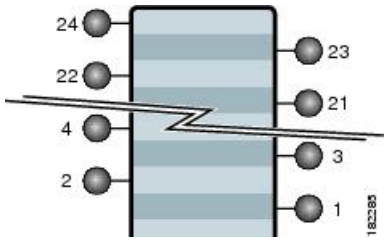
注意 セル方式の電話、携帯電話、GSM 電話、または双方向無線機を Cisco Unified IP Phone のすぐ近くで使用すると、相互干渉が発生することがあります。 詳細については、干渉デバイスの製造元の資料を参照してください。

この章は、次の項で構成されています。

- Cisco Unified IP Phone のセキュリティ機能，14 ページ
- 電話機の消費電力，27 ページ
- Cisco Unified IP Phone の導入，27 ページ

ボタンとハードウェア

次の図を使用して、電話機のボタンとハードウェアを特定します。

	項目	説明
1	プログラム可能なボタン 	設定に応じて、プログラマブル ボタン（回線キー）で次の機能にアクセスできます。 • 電話回線およびインターコム回線（回線ボタン） • スピード ダイヤルの番号（BLF スピード ダイヤルを含む、スピード ダイヤル ボタン） • Web ベースのサービス（個人アドレス帳ボタンなど） • コール機能（プライバシー、会議など） • ローカル機能（アプリケーション メニュー、ヘッドセット、設定など） 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 コールまたは双方向のインターコム コール • 緑、点滅：保留中のコール • オレンジ、点灯：プライバシー使用中、一方向のインターコム コール、サイレント、ハント グループにログイン中、ヘッドセットまたはその他のローカル機能が有効 • オレンジ、点滅：受信コールまたは保留復帰コール • 赤、点灯：リモート回線が使用中（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コール） • 赤、点滅：リモート コールが保留中 回線キーには、左から右に降順で24～1の番号が付けられています。 
2	ペーパー ラベル	各ボタンの回線情報または機能情報を識別できます。

	項目	説明
3	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。
4	保留ボタン 	コールを保留にします。
5	転送ボタン 	コールを別の番号に接続します。
6	リダイヤル ボタン 	最後にダイヤルした番号に接続します。
7	キーパッド	電話番号のダイヤル、文字の入力、およびメニュー項目の選択に使用します。
8	ミュート ボタン 	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、ボタンは点灯しています。
9	音量ボタン 	ハンドセット、ヘッドセット、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。
10	スピーカー ボタン 	スピーカーフォン モードのオン/オフを切り替えます。 スピーカー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	ハンドセット	従来のハンドセットと同様に機能します。
12	ハンドセット インジケータ ライト	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。着信コールの場合は点滅し、待機中のメッセージがある場合は点灯します。

	項目	説明
13	電話スクリーン	回線またはコールのステータス、電話番号、ソフトキーなどの情報を表示します。
14	Cisco Unified IP Phone モデル	Cisco Unified IP Phone の型番を示します。
15	4方向ナビゲーションパッドと選択ボタン（中央） 	ナビゲーション ボタン • 上下にスクロールして、メニューを表示し、項目を強調表示します。 • 左にスクロールすると詳細ビューが開き、電話番号と各回線ボタンに割り当てられている機能が表示されます（コール スクリーン時）。 • 右にスクロールすると、詳細ビューが閉じます。
		選択ボタン：ナビゲーション ボタンを使用してスクロールし、回線を選択した後、次のように機能します。 • ボタンが電話番号にマッピングされている場合 ° 回線がアイドル状態のときは、を押して新規コールを発信します。 ° 回線に保留中のコールがあるときは、を押してコールを復帰します。 ° 回線にアクティブなコールがあるときは、選択ボタンは機能しません。 • ボタンが機能にマッピングされている場合は、を押して機能にアクセスします。

電話機メニューとローカル機能

Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されると、各機能用に設定された回線ボタンを押してローカル機能にアクセスできます。

デフォルトでは、回線ボタン 21 はボイス メッセージング システムにアクセスし、回線ボタン 22 はディレクトリ メニューを表示し、回線ボタン 23 はヘッドセットをアクティブ化し、回線ボタン 24 はアプリケーション メニューを表示します。 これらのプログラム可能なボタンの割り当てを変更するには、Cisco Unified CM の管理を使用します。 詳細は、「電話ボタン テンプレート」を参照してください。

デフォルトでは、電話機が起動して Cisco Unified Communications Manager に登録される前に、右端のソフトキーが [設定（Settings）] ソフトキーとなります。 このキーを押すことで、電話機の設定メニューにアクセスできます。 この方法で、必要に応じて設定を変更でき、電話機の起動と登録のプロセスを正常に完了することができます。また、トラブルシューティングに役立つ情報を取得することもできます。

設定ファイル内のオプションにより、電話機の設定へのアクセスをブロックできます。 電話機が登録済みで設定へのアクセスをブロックする設定ファイルをダウンロード済みの場合、[設定（Settings）] ソフトキーは使用できません。 この場合、電話機を工場出荷時の状態にリセットしないと、[設定（Settings）] ソフトキーは表示されません。

ネットワーク プロトコル

Cisco Unified IP Phones は、音声通信に必須の複数の業界標準ネットワーク プロトコルとシスコ ネットワーク プロトコルをサポートしています。 表 1：Cisco Unified IP Phone でサポートされるネットワーク プロトコル, （6 ページ）に、Cisco Unified IP Phone 7931G でサポートされるネットワーク機能の概要を示します。

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

ネットワーキング プロトコル	目的	使用方法
ブートストラップ プロトコル（BootP）	BootP は、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 IP アドレスを Cisco Unified IP Phone に割り当てている場合、電話機のネットワーク構成の設定値として [BOOTP サーバ（BOOTP Server）] オプションが「はい（Yes）」と表示されます。
Cisco Discovery Protocol（CDP）	CDP は、シスコの製造するすべての装置で動作するデバイス検出プロトコルです。 デバイスは、CDP を使用して自身の存在をネットワーク内の他のデバイスにアドバタイズし、他のデバイスの情報を受信します。	Cisco Unified IP Phone では、補助 VLAN ID、ポートごとの電源管理の詳細情報、Quality of Service（QoS）設定情報などの情報を、CDP を使用して Cisco Catalyst スイッチとやり取りしています。
Cisco Peer-to-Peer Distribution Protocol（CPPDP）	CPPDP は、デバイスのピアツーピア階層を形成するために使用されるシスコ独自のプロトコルです。CPPDP は、ファームウェアや他のファイルをピア デバイスからネイバー デバイスにコピーするためにも使用します。	CPPDP は、ピア ファームウェア共有機能で使用されます。

ネットワーキング プロトコル	目的	使用方法
ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）	DHCP は、IP アドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。 DHCP を使用すると、IP Phone をネットワークに接続すれば、その電話機が機能するようになります。IP アドレスを手動で割り当てたり、ネットワーク パラメータを別途設定したりする必要はありません。	DHCP は、デフォルトで有効になっています。 無効にした場合は、個々の電話機がある場所で、IP アドレス、サブネットマスク、ゲートウェイ、および TFTP サーバを手動で設定する必要があります。 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」および「Cisco TFTP」の章を参照してください。
Hypertext Transfer Protocol（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。 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。
Hypertext Transfer Protocol Secure（HTTPS）	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、HTTP と SSL/TLS プロトコルを組み合わせたものです。	HTTP と HTTPS の両方をサポートする Web アプリケーションには 2 つの URL が設定されています。HTTPS をサポートする Cisco Unified IP Phone は、2 つの URL のうち HTTPS URL を選択します。

ネットワーキング プロトコル	目的	使用方法
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 コントロールと認証プロトコルを定義します。これにより、未承認のクライアントが一般にアクセス可能なポートから LAN に接続するのを制限します。 クライアントが認証されるまでは、802.1X アクセス コントロールによって、クライアントが接続されているポートを経由する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。 認証が完了すると、標準トラフィックがポートを通過できます。	Cisco Unified IP Phone は、EAP-FAST、EAP-TLS、および EAP-MD5 の認証方式をサポートすることで、IEEE 802.1X 標準を実装します。 電話機で 802.1X 認証が有効になっている場合、PC ポートとボイス VLAN を無効にする必要があります。 詳細については、802.1X 認証,（24 ページ）を参照してください。
インターネットプロトコル（IP）	IP は、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。	IP を使用して通信するには、ネットワーク デバイスに対して、IP アドレス、サブネット、およびゲートウェイが割り当てられている必要があります。 IP アドレス、サブネット、およびゲートウェイの識別情報は、DHCP を通じて電話機を使用する場合は、自動的に割り当てられます。 DHCP を使用しない場合は、個々の電話機にこれらのプロパティを手動で割り当てる必要があります。 Cisco Unified IP Phone は IPv4 アドレスと IPv6 アドレスの併用をサポートしています。 Cisco Unified CM の管理で 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)」の章を参照してください。

ネットワーキング プロトコル	目的	使用方法
Link Layer Discovery Protocol（LLDP）	LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコ デバイスとサードパーティ製デバイスでサポートされています。	Cisco Unified IP Phone は、PC ポートで LLDP をサポートします。
Link Layer Discovery Protocol-Media Endpoint Devices（LLDP-MED）	LLDP-MED は、音声製品用に開発された、LLDP 標準の拡張です。	Cisco Unified IP Phone は、次のような情報をやり取りするために、SW ポートで LLDP-MED をサポートします。 • ボイス VLAN の設定 • デバイスの検出 • 電源管理 • インベントリ管理 LLDP-MED サポートの詳細については、次の Web サイトで『LLDP-MED and Cisco Discovery Protocol』ホワイト ペーパーを参照してください。 http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
リアルタイム転送プロトコル（RTP）	RTP は、データ ネットワークを通じて、インタラクティブな音声やビデオなどのリアルタイム データを転送するための標準プロトコルです。	Cisco Unified IP Phone では、RTP プロトコルを使用して、リアルタイム音声トラフィックを他の電話機やゲートウェイとやり取りします。
リアルタイム転送プロトコル（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を参照してください。

ネットワーキング プロトコル	目的	使用方法
Session Initiation Protocol（SIP）	SIP は、IP を介したマルチメディア会議のための Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）標準です。SIP は、アプリケーション層の ASCII ベースの制御プロトコルであり（RFC 3261 で規定）、2 つ以上のエンドポイント間でコールを確立、維持、および終了するために使用できます。	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。 電話機が IPv6 アドレス モードで動作している場合、Cisco Unified IP Phone は SIP プロトコルをサポートしません。
Skinny Client Control Protocol（SCCP）	SCCP は、コール制御サーバとエンドポイント クライアント（IP Phone など）の間で通信を行うためのメッセージング セットを含んでいます。 SCCP は、シスコ独自のものです。	Cisco Unified IP Phone は、コール制御に SCCP を使用します。 Cisco Unified IP Phone は、SCCP または Session Initiation Protocol（SIP）のどちらかを使用するように設定できます。
セッション記述プロトコル（SDP）	SDP は SIP プロトコルの一部であり、2つのエンドポイント間で接続が確立されている間に、どのパラメータを使用できるかを決定します。 会議は、会議に参加するすべてのエンドポイントでサポートされている SDP 機能だけを使用して確立されます。	コーデック タイプ、DTMF 検出、コンフォート ノイズなどの SDP 機能は、通常は運用中の Cisco Unified Communications Manager またはメディア ゲートウェイでグローバルに設定されています。 SIP エンドポイントの中には、これらのパラメータをエンドポイント上で設定できるものがあります。
伝送制御プロトコル（TCP）	TCP は、コネクション型の転送プロトコルです。	Cisco Unified IP Phone では、Cisco Unified Communications Manager への接続、および XML サービスへのアクセスに TCP を使用します。

ネットワーキング プロトコル	目的	使用方法
トランスポート レイヤ セキュリティ（TLS）	TLS は、通信のセキュリティ保護と認証に使用される標準プロトコルです。	セキュリティが実装されると、Cisco Unified IP Phone では、Cisco Unified Communications Manager に安全に登録するときに TLS プロトコルが使用されます。 詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
トリビアル ファイル転送プロトコル（TFTP）	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 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 サーバによる指定以外の TFTP サーバを電話機で使用する場合、電話機の [ネットワークの設定（Network Configuration）] メニューから手動で TFTP サーバを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。
ユーザ データグラム プロトコル（UDP）	UDP は、データ パケットを配信するためのコネクションレス型メッセージング プロトコルです。	Cisco Unified IP Phone は、UDP を利用した RTP ストリームを送受信します。

関連トピック

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

Cisco Unified IP Phone での IPv6 サポート

Cisco Unified IP Phone はインターネット プロトコルを使用して、ネットワークで音声通信を提供します。 インターネット プロトコル バージョン 4（IPv4）では 32 ビット アドレスが使用されているため、インターネットに接続するすべてのデバイスに対する一意の IP アドレス要求の増大に対応できません。 このため、現在のインターネットプロトコルの更新バージョンであるインターネット プロトコル バージョン 6（IPv6）が策定されました。 IPv6 は 128 ビット アドレスを使用

し、エンドツーエンド セキュリティ機能、拡張 Quality Of Service（QoS）、および使用可能な IP アドレス数の増加に対応します。

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

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

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

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

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

Cisco Unified IP Phone 7931G でサポートされる機能

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。 Cisco Unified IP Phone には、従来のテレフォニー機能に加えて、電話機をネットワーク デバイスとして管理およびモニタする機能も備えています。

機能の概要

Cisco Unified IP Phone は、コール転送や転送、リダイヤル、スピード ダイヤル、会議コール、ボイス メッセージング システムへのアクセスなど、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 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を手動で設定することもできます。

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。 XML を使用すると、天気予報、株価情報、商品相場などの Web ベースの情報にユーザがアクセスできるようになります。

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

関連トピック

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

テレフォニー機能の管理

Cisco Unified IP Phone に関する設定の一部は、Cisco Unified CM の管理から変更できます。 このグラフィカル ユーザ インターフェイスは、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および『*Cisco Unified Communications Manager Administration Guide*』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 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、このアプリケーションで参照できる状況依存ヘルプも参考情報として利用できます。

Cisco Unified Communications Manager のマニュアル スイートは、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 Business Edition 5000 のマニュアル スイート一覧は、次の URL で参照できます。

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

関連トピック

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

Cisco Unified IP Phone のネットワーク パラメータ

DHCP、TFTP、IP の設定値などのパラメータは、電話機で設定できます。 また、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。

関連トピック

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

エンド ユーザへの情報

システム管理者は、多くの場合、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。 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くことを推奨します。 次の Cisco Unified IP Phone の Web サイトに必ずアクセスしてください。

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

このサイトでは、さまざまなユーザ ガイドにアクセスできます。

マニュアルの提供に加えて、利用可能な Cisco Unified IP Phone の機能（自社固有の機能やネットワーク固有の機能を含む）、およびそれらの機能へのアクセス方法とカスタマイズ方法（可能な場合）をユーザに知らせることも重要です。

関連トピック

社内のサポート Web サイト

Cisco Unified IP Phone のセキュリティ機能

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

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

表 2：*Cisco Unified IP Phone* 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	『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。
Cisco Unified IP Phone でサポートされるセキュリティ機能	サポート対象のセキュリティ機能，（16 ページ）を参照してください。
セキュリティ機能に関する制約	セキュリティ上の制約事項，（27ページ）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	セキュリティプロファイル，（19ページ）を参照してください。
セキュリティが実装されているコールの識別	認証、暗号化、および保護されているコール，（19 ページ）を参照してください。
セキュリティが実装されている会議コールの確立および識別	セキュアな会議コールの特定，（20 ページ）を参照してください。
TLS 接続	ネットワーク プロトコル，（6 ページ）を参照してください。 電話機設定ファイルを参照してください。
セキュリティと電話機の起動プロセス	電話機の起動プロセスを参照してください。
セキュリティと電話機の設定ファイル	電話機設定ファイルを参照してください。
セキュリティが実装されているときの電話機での [TFTP サーバ 1（TFTP Server 1）] または [TFTP サーバ 2（TFTP Server 2）] オプションの変更	ネットワークの設定メニューを参照してください。
電話機の [デバイス設定（Device Configuration）] メニューにある CallManager 1 ～ CallManager 5 の各オプションのセキュリティ アイコンの確認	Unified CM の設定メニューを参照してください。
電話機の [デバイス設定（Device Configuration）] メニューからアクセスする電話機の [セキュリティ設定（Security Configuration）] メニューの項目	[セキュリティ設定（Security Configuration）] メニューを参照してください。
電話機の [設定（Settings）] メニューからアクセスする電話機の [セキュリティ設定（Security Configuration）] メニューの項目	[セキュリティ設定（Security Configuration）] メニューを参照してください。
CTL ファイルおよび ITL ファイルのロック解除	CTL ファイルと ITL ファイルのロック解除を参照してください。

トピック	参照先
電話機の Web ページへのアクセスの無効化	Web ページへのアクセスの制御を参照してください。
電話機からの CTL ファイルの削除	Cisco Unified IP Phone のリセットまたは復元を参照してください。
電話機のリセットまたは復元	Cisco Unified IP Phone のリセットまたは復元を参照してください。
Cisco Extension Mobility HTTPS のサポート	ネットワーク プロトコル, （6 ページ）を参照してください。
Cisco Unified IP Phone の 802.1X 認証	次の項を参照してください。 • 802.1X 認証, （24 ページ） • [802.1X 認証（802.1X Authentication）] および [802.1X 認証ステータス（802.1X Authentication Status）] • Cisco Unified IP Phone のセキュリティの問題

サポート対象のセキュリティ機能

次の表に、Cisco Unified IP Phone 7931G でサポートされるセキュリティ機能の概要を示します。これらの機能と、Cisco Unified Communications Manager および Cisco Unified IP Phone のセキュリティの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

電話機の現在のセキュリティ設定については、電話機の [セキュリティ設定（Security Configuration）] メニューの設定を確認します。 詳細については、[セキュリティ設定（Security Configuration）] メニューおよび [セキュリティ設定（Security Configuration）] メニューを参照してください。

（注） ほとんどのセキュリティ機能は、電話機に証明書信頼リスト（CTL）がインストールされている場合にだけ使用できます。 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 3：セキュリティ機能の概要

機能	説明
イメージ認証	ファームウェアイメージが電話機にロードされる前に、署名付きバイナリ ファイル（拡張子 .sbn）を使用して、ファームウェア イメージに対する改ざんを防止します。イメージが改ざんされると、電話機は認証プロセスに失敗し、新しいイメージを拒否します。
カスタマーサイト証明書のインストール	各 Cisco Unified IP Phone は、デバイス認証に一意の証明書を必要とします。 電話機には 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 CM の管理で、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。 または、電話機の [セキュリティ設定（Security Configuration）] メニューから LSC をインストールできます。 詳細については、Cisco Unified IP Phone のセキュリティを参照してください。
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、必要に応じてトランスポート レイヤ セキュリティ（TLS）プロトコルを使用してエンティティ間にセキュアなシグナリング パスを作成します。 Cisco Unified Communications Manager で電話機を認証できない限り、Cisco Unified Communications Manager ではそれらの電話機は登録されません。
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 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 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 CM の管理で依存デバイスをリセットした後、TFTP サーバは SRST 証明書を電話機の cnf.xml ファイルに追加して、ファイルを電話機に送ります。 その後、セキュアな電話機は TLS 接続を使用して、SRST 対応ルータと相互に対話します。

機能	説明
メディアの暗号化	SRTP を使用して、サポートされるデバイス間のメディア ストリームがセキュアであることを証明し、意図したデバイスのみがデータを受け取り、読み取れるようにします。 デバイスのメディア マスターのキー ペアの作成、デバイスへのキーの配布、キーが転送される間のキーの配布のセキュリティの確保などが含まれます。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバ間で送信されるすべての SCCP と SIP シグナリング メッセージを暗号化します。
CAPF（Certificate Authority Proxy Function）	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, （19 ページ）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）	電話機の 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、[ユーザ設定（User Preferences）] メニューへのアクセスと音量変更の保存だけを許可する制限付きアクセスの提供 • 電話機の Web ページへのアクセスの無効化。 （注） 電話機の [セキュリティ設定（Security Configuration）] メニューを表示すると、[PC ポートを無効にする（PC Port Disabled）]、[GARP を使う（GARP Enabled）]、[ボイス VLAN を使う（Voice VLAN enabled）] の各オプションの現在の設定を確認できます。 詳細については、デバイス設定メニュー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の要求およびネットワーク アクセスを行います。 詳細については、802.1X 認証, （24 ページ）を参照してください。

関連トピック

セキュリティ プロファイル, （19 ページ）
認証、暗号化、および保護されているコール, （19 ページ）
802.1X 認証, （24 ページ）
デバイス設定メニュー
セキュアな会議コールの特定, （20 ページ）
セキュリティ上の制約事項, （27 ページ）

セキュリティ プロファイル

Cisco Unified Communications Manager 7.0 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 Security Guide*』を参照してください。

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

関連トピック

認証、暗号化、および保護されているコール, （19 ページ）
デバイス設定メニュー
[セキュリティ設定（Security Configuration）] メニュー
セキュアな会議コールの特定, （20 ページ）
セキュリティ上の制約事項, （27 ページ）

認証、暗号化、および保護されているコール

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

認証済みコールでは、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 によって認証されています。 コールがセットアップされて認証されると、電話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 のアイコンに変わります。

コールが暗号化された場合、そのコールの確立に関与したすべてのデバイスは信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されます。 さらに、コールのシグナリングとメディア ストリームが暗号化されます。暗号化されたコールはコールの整合性とプライバシーを提供することで、高レベルのセキュリティを提供します。 進行中のコールが暗号化さ

れると、電話機画面内の通話時間タイマーの右にあるコール進捗アイコンが のアイコンに変わります。

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

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

関連トピック

Cisco Unified IP Phone のセキュリティ機能, （14 ページ）
セキュリティ プロファイル, （19 ページ）
セキュアな会議コールの特定, （20 ページ）
セキュリティ上の制約事項, （27 ページ）

セキュアな会議コールの特定

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

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

（注） 参加者の電話機のセキュリティ モードおよびセキュアな会議ブリッジの可用性によっては、会議コールのセキュリティ レベルに影響する連携動作と制限事項があります。 このような連携動作については、コール セキュリティの連携動作と制限事項, （21 ページ）を参照してください。

保護されたコールの識別

ユーザの電話機と相手側の電話機が保護されたコール用に設定されている場合、保護されたコールが確立されます。 相手側の電話機は、同じ Cisco IP ネットワーク内にあっても、Cisco IP ネットワーク以外のネットワークにあってもかまいません。 保護されたコールは、2 台の電話機の間でのみ確立できます。 会議コールや、複数回線を使用するその他のコールはサポートされません。

保護されたコールの確立は、次のプロセスに従います。

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

（注） 保護されたコールは 2 台の電話機間の通話に対してサポートされます。 保護されたコールが設定されていると、会議、共有回線、Cisco Extension Mobility、複数ライン同時通話機能など一部の機能を使用できません。

コール セキュリティの連携動作と制限事項

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

表 *4*：割り込み使用時のコール セキュリティの連携動作

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

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

表 *5*：会議コールのセキュリティの制限事項

発信側電話機のセキュリティレベル	使用する機能	参加者のセキュリティ レベル	動作結果
非セキュア	会議	暗号化済みまたは認証済み	非セキュアな会議ブリッジ 非セキュアな会議
セキュア（暗号化済みまたは認証済み）	会議	少なくとも 1 台のメンバーが非セキュア。	セキュアな会議ブリッジ 非セキュアな会議
セキュア（暗号化済み）	会議	すべての参加者が暗号化済み	セキュアな会議ブリッジ セキュアな暗号化レベルの会議
セキュア（認証済み）	会議	すべての参加者が暗号化済みまたは認証済み。	セキュアな会議ブリッジ 認証済みレベルのセキュアな会議

発信側電話機のセキュリティレベル	使用する機能	参加者のセキュリティレベル	動作結果
非セキュア	会議	暗号化済みまたは認証済み	セキュアな会議ブリッジのみが利用可能で、使用されている。 非セキュアな会議
セキュア（暗号化済みまたは認証済み）	会議	暗号化済みまたは認証済み	非セキュアな会議ブリッジのみが利用可能で、使用されている。 非セキュアな会議
セキュア（暗号化済みまたは認証済み）	会議	セキュアまたは暗号化済み	会議はセキュアに保たれる。 参加者の1人がコールを保留音（MOH）で保留しようとすると、MOHが再生されない。
セキュア（暗号化済み）	参加	暗号化済みまたは認証済み	セキュアな会議ブリッジ 会議はセキュアな状態を維持する（暗号化されているか、認証済み）。
非セキュア	cBarge	すべての参加者が暗号化済み	セキュアな会議ブリッジ 会議が非セキュアに変更される。
非セキュア	ミートミー	最小限のセキュリティレベルが暗号化	発信側は「セキュリティレベルを満たしていません（Does not meet Security Level）」というメッセージを受け取り、コールが拒否される。
セキュア（暗号化済み）	ミートミー	最小セキュリティ レベルは、認証済み	セキュアな会議ブリッジ 会議は、暗号化済みおよび認証済みのコールを受け入れる。

発信側電話機のセキュリティレベル	使用する機能	参加者のセキュリティレベル	動作結果
セキュア（暗号化済み）	ミートミー	最小限のセキュリティレベルは非セキュア	セキュアな会議ブリッジだけが使用可能になり、使用される。 会議はすべてのコールを受け入れる。

802.1X 認証

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

概要

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

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

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

必要なネットワーク コンポーネント

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

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

- Cisco Catalyst スイッチ（またはその他のサードパーティ製スイッチ）：スイッチはオーセンティケータとして機能し、電話機と認証サーバ間でメッセージを渡すことができるよう、802.1X をサポートしている必要があります。やり取りが完了した後、スイッチはネットワークへの電話機のアクセスを許可または拒否します。

ベスト プラクティス、要件、および推奨事項

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

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - 無効：スイッチが同一ポート上の複数の 802.1X 対応デバイスをサポートしていない場合、802.1X 認証を有効化するときに PC ポートを無効にする必要があります。PC ポートを無効化せずに PC を接続しようとすると、スイッチは電話機および PC へのネットワーク アクセスを拒否します。
- ボイス VLAN の設定：802.1X 標準では VLAN が考慮されないため、ボイス VLAN の設定はスイッチのサポートに基づいて行う必要があります。
  - 有効：複数ドメインの認証をサポートするスイッチを使用している場合は、ボイス VLAN を引き続き使用できます。
  - 無効：スイッチが複数ドメインの認証をサポートしていない場合は、ボイス VLAN を無効にし、ネイティブ VLAN へのポートの割り当てを検討します。
- MD5 共有秘密の入力：電話機で 802.1X 認証を無効にするか、工場出荷時の状態にリセットすると、以前に設定された MD5 共有秘密は削除されます。

関連トピック

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

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

UCR 2008

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

- 連邦情報処理標準（FIPS）104-2 のサポート：FIPS 104-2 をサポートするために、この電話機には次のことが必要となります。
  - 適切な暗号化アルゴリズムが使用可能であることを確認するための、電源投入時自己診断テスト（POST）の使用。 電話機のファームウェアに適切なモジュールがない場合、電話機は起動できません。
  - すべてのインターネット通信での HTTPS の使用。
  - 電話機への Web アクセスの無効化。
  - Cisco Unified Communications Manager が FIPS 準拠にセットアップされること（802.1x EAP-MD5 の無効化など）。
- TVS IPv6：IPv6 アドレスが使用可能な場合、電話機には Trust Verification Service（TVS）サーバの IPv6 アドレスが表示されます。
- 80 ビット SRTCP タギング：電話機では 32 ビット SRTCP パケット ヘッダーと 80 ビット SRTCP パケット ヘッダーの両方がシームレスに処理されます。

IP Phone の管理者として、これらの機能の一部では、Cisco Unified Communications Manager の管理インターフェイスで特定のパラメータをセットアップする必要があります。

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

表 *6*：*Cisco Unified IP Phone* の *UCR 2008* 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	『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。
UCR 2008 パラメータのセットアップ	UCR 2008 のセットアップ
POST 問題のトラブルシューティング	Cisco Unified IP Phone に「セキュリティ エラー（Security Error）」メッセージが表示される

セキュリティ上の制約事項

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

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

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

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

電話機の消費電力

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

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

スイッチの管理者は、スケジュールされた時間よりも前に電話機の電源を復帰させることができます。 電話機の電源をスイッチからオンにする方法の詳細については、スイッチのマニュアルを参照してください。

Cisco Unified IP Phone の導入

新しい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。 完全な Cisco 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。

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、Cisco Unified 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 のセットアップ

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

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

Cisco Unified Communications Manager で電話機を設定する方法の詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」の章、および『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Configuration」の章を参照してください。

関連トピック

Cisco Unified Communications Manager 電話機の追加方法

Cisco Unified Communications Manager での Cisco Unified IP Phone 7931G のセットアップ

次の手順では、Cisco Unified CM の管理での Cisco Unified IP Phone 7931G の設定タスクの概要およびチェックリストを示します。 この手順では、推奨する順序に従って電話機を設定するプロセスを解説しています。 一部のタスクは、システムおよびユーザのニーズによっては省略できます。 手順および内容の詳細については、手順に示した資料を参照してください。

手順

ステップ 1 電話機について、次の情報を収集します。

- 電話機のモデル
- MAC アドレス
- 電話機の設置場所
- 電話機のユーザの名前または ID
- デバイス プール
- 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

- 回線の数と、それに関連して電話機に割り当てる電話番号（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

電話機をセットアップするための設定要件のリストを作成します。

個々の電話機を設定する前に実施する必要のある、電話ボタンテンプレートやソフトキーテンプレートなどの前提的な設定作業を特定します。

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

ステップ 2 必要に応じて電話ボタンテンプレートをカスタマイズします。プログラム可能な回線ボタンにスピード ダイヤルおよび機能を割り当てて、ユーザのニーズに対応します。
IPv4 アドレスでサービス URL を指定する必要があります。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Phone Button Template Configuration」の章および 電話ボタン テンプレートを参照してください。

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

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

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

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

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

- 電話番号（Directory Numbers）
- パーティション
- 複数コールとコール待機（Multiple Calls and Call Waiting）
- コール転送とコール ピックアップ（Call Forwarding and Pickup）（使用する場合）
- ボイス メッセージング（Voice Messaging）（使用する場合）

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

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

ステップ 5 ソフトキー テンプレートのカスタマイズ。
電話機に表示されるソフトキー機能を追加、削除、または順序変更します。

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

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

（注） ユーザは、Cisco Unified Communications Manager を使用することで、電話機上のスピード ダイヤルの設定値を変更できます。

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

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

（注） ユーザは、Cisco Unified Communications Manager ユーザ オプションを使用することで、電話機上のサービスを追加または変更できます。

IPv4 アドレスでサービス URL を指定する必要があります。

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

ステップ 8 サービスを電話ボタンに割り当てます（任意）。
ボタンを 1 回押すだけで IP Phone サービスまたは URL にアクセスできるようにします。

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

ステップ 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。

- 名前（Name）（姓を入力）
- ユーザ ID
- パスワード（Password）（Cisco Unified Communications Manager Web ページで使用）
- PIN（エクステンション モビリティおよびパーソナル ディレクトリで使用）

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

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

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

ステップ 10 ユーザをユーザ グループに追加します。
ユーザ グループ内のすべてのユーザに適用される、共通のロールと権限のリストをユーザに割り当てます。管理者は、ユーザ グループ、ロール、および権限を管理することによって、システム ユーザのアクセス レベル（つまり、セキュリティのレベル）を制御できます。

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

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

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

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「End User Configuration」の章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。 管理者は、必要な場所に電話機を設置できます。または、設置に必要な情報を電話機ユーザに提供することもできます。 『Cisco Unified IP Phone Installation Guide』（http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html で入手可能）には、電話機のフット スタンド、ハンドセット、ケーブルおよびその他のアクセサリの取り付け方法が記載されています。

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

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

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

自動登録を使用した場合は、電話機のユーザへの関連付け、ボタン テーブルの変更、または電話番号の割り当てなど、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 7931G の設置

次の手順では、Cisco Unified IP Phone 7931G の設置タスクの概要およびチェックリストを示します。 この手順では、推奨する順序に従って電話機を設置するプロセスを解説しています。 一部のタスクは、システムおよびユーザのニーズによっては省略できます。 手順および内容の詳細については、手順に示した資料を参照してください。

手順

ステップ 1 電話機の電源を次の中から選択します。

- Power over Ethernet（PoE）
- 外部電源

電話機に電力を供給する方法を決定します。

ステップ 2 電話機を組み立て、電話機の位置を調節し、ネットワーク ケーブルを接続します。
電話機の位置を決めて設置し、ネットワークに接続します。

ステップ 3 電話機の起動プロセスをモニタします。 電話機が適切に設定されていることを確認します。

ステップ 4 IPv4 ネットワーク用の電話機のネットワーク設定を行っている場合、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。

a) 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 に割り当てられるようにし、電話機を TFTP サーバに割り当てるには、[設定（Settings）] >[ネットワークの設定（Network Configuration）]> [IPv4 設定（IPv4 Configuration）] を選択し、次のようにします。

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

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

b) 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、次のようにします。
DHCP を無効にして、IP アドレスを手動で設定する場合：

1. DHCP を無効にするには、[DHCP を使う（DHCP Enabled）] を [いいえ（No）] に設定します。
2. 電話機のスタティック IP アドレスを入力します。
3. サブネット マスクを入力します。

4 デフォルト ルータの IP アドレスを入力します。

5 [代替 TFTP サーバ（Alternate TFTP Server）] を [はい（Yes）] に設定し、TFTP サーバ 1 の IP アドレスを入力します。

[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。

ステップ 5 IPv6 ネットワーク用の電話機のネットワーク設定を行っている場合、DHCP を使用するか IP アドレスを手入力して電話機の IP アドレスをセットアップできます。

a) 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、次のようにします。

- DHCPv6 を有効にするには、[DHCPv6 を使う（DHCPv6 Enabled）] 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。

b) 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）] > [IPv6 設定（IPv6 Configuration）] を選択し、次のようにします。

DHCP を無効にして、IP アドレスを手動で設定する場合：

1 DHCPv6 を無効にするには、[DHCPv6 を使う（DHCPv6 Enabled）] を [いいえ（No）] に設定します。

2 電話機のスタティック IP アドレスを入力します。

3 IPv6 プレフィックス長を入力します。

4 [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 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。

ステップ 6 電話機のセキュリティをセットアップします。 データ改ざんの脅威と電話機の ID 盗用を防止します。

ステップ 7 Cisco Unified IP Phone を使用して、コールを発信します。 電話機および機能が正常に動作することを確認します。
詳細については、『*Cisco Unified IP Phone 7931G User Guide for Cisco Unified Communications Manager (SCCP and SIP)*』を参照してください。

ステップ 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します。

関連トピック

Cisco Unified IP Phone の電源
Cisco Unified IP Phone の設置
電話機のケーブル ロック
電話機起動時の確認
ネットワーク設定
ネットワークの設定メニュー
Cisco Unified IP Phone のセキュリティ
社内のサポート Web サイト