



Cisco Unified IP Phone

Cisco Unified IP Phone 6901 および 6911 は、インターネットプロトコル (IP) ネットワーク経由の音声通信を提供します。Cisco Unified IP Phone は、デジタル ビジネス フォンとほぼ同様に機能し、コールの発信および受信に利用できます。このマニュアルでの Cisco Unified IP Phone には、次の属性があります。

- Cisco Unified IP Phone 6901 は、保留、リダイヤル、転送、会議などの基本機能をサポートします。
- Cisco Unified IP Phone 6911 は、ミュート、保留、転送、会議、短縮ダイヤル、コール転送などの高度な機能をサポートします。

Cisco Unified IP Phone は、他のネットワーク デバイスと同様、設定と管理が必要です。これらの電話機は、G.711a、G.711u、G.729a、G.729ab、および iLBC コーデックをエンコードし、G.711a、G.711u、G.729、G.729ab、および iLBC コーデックをデコードします。これらの電話機は、これらのコーデックを同様の方法でエンコードおよびデコードします。



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、干渉デバイスの製造元の資料を参照してください。

詳細については、『*Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*』を参照してください。

- [Cisco Unified IP Phone 6901, 2 ページ](#)
- [Cisco Unified IP Phone 6911, 5 ページ](#)
- [一般的な電話情報, 8 ページ](#)
- [ネットワーク プロトコル, 11 ページ](#)
- [Cisco Unified IP Phone 6901 および 6911 でサポートされる機能, 16 ページ](#)
- [Cisco Unified IP Phone のセキュリティ機能, 18 ページ](#)
- [Cisco Unified IP Phone の導入, 28 ページ](#)

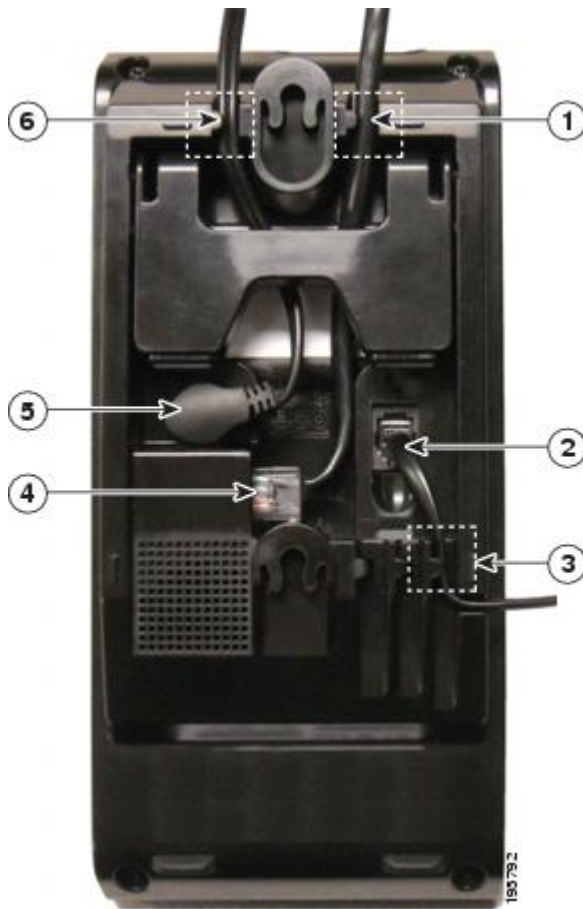
- 電話機の電力消費量の節減, 32 ページ
- 用語の違い, 33 ページ

Cisco Unified IP Phone 6901

ここでは、Cisco Unified IP Phone 6901 のハードウェアについて説明します。

電話機の接続

電話機を動作させるには、電話機が企業のIPテレフォニーネットワークに接続されている必要があります。







1	イーサネット ケーブル用スロット	4	ネットワークポート (10/100 SW) 接続 IEEE 802.3af 電源対応
2	ハンドセットの接続	5	DC アダプタ ポート (DC48V)

3	ハンドセット ケーブル用スロット	6	DC アダプタ ケーブル用スロット
---	------------------	---	-------------------

ボタンとハードウェア



1	フックスイッチ	電話機の機能（フックフラッシュ）をアクティブにします。
2	保留ボタン 	接続したコールを保留にします。

3	リダイヤル ボタン 	最後にダイヤルした番号をダイヤルします。
4	回線ボタン 	<p>別の着信コールをピックアップできます。回線ボタンのLEDは、コールステータスを示します。</p> <p>呼び出し中のコールへの応答や、同一回線上の2つのコールの切り替えができます。また、電話機がアイドル状態のときは、回線ボタンを使用して新しいコールを発信できます。回線ボタンに関連付けられたLEDが、回線のステータスを反映して点灯します。</p> <p>LEDの色は回線の状態を次のように示します。</p> <ul style="list-style-type: none"> • 緑、点灯：アクティブ コール • 緑、点滅：保留中のコール • オレンジ色に点滅：着信コール • オレンジ、点灯：不在転送がアクティブ • 赤、点灯：リモート回線が使用中（共有回線） • 赤、点滅：リモート回線が保留中
5	音量ボタン 	ハンドセットの音量（オフフック時）と呼出音の音量（オンフック時）を制御します。
6	キーパッド	電話番号をダイヤルできます。
7	ライトストリップを備えたハンドセット	呼び出し中のコール（赤色の点滅）または新しいボイスメッセージ（赤色の点灯）を、ライトで知らせます。

フックスイッチ ボタン

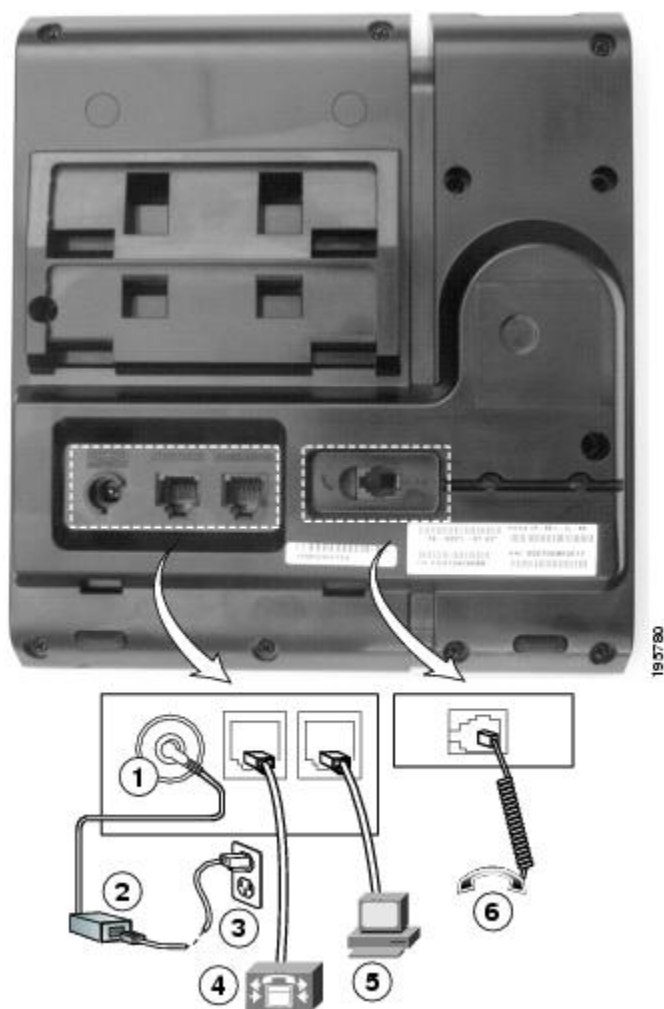
電話機の受け台には、フックスイッチ ボタンが含まれています。フックスイッチ ボタンを押してからすばやく放すと、電話機の各機能を有効にすることができます（フックフラッシュ）。

Cisco Unified IP Phone 6911

ここでは、Cisco Unified IP Phone 6901 のハードウェアについて説明します。

電話機の接続

電話機を動作させるには、電話機が企業のIPテレフォニーネットワークに接続されている必要があります。





1	DC アダプタ ポート (DC48V)	4	ネットワーク ポート (10/100 SW) 接続 IEEE 802.3af 電源対応
2	AC-DC 電源装置 (任意)	5	アクセス ポート (10/100 PC) 接続


3	AC 電源コンセント (任意)	6	ハンドセットの接続
---	-----------------	---	-----------

ボタンとハードウェア



1	ライト ストリップを備えたハンドセット	コールの呼び出し (赤の点滅) または新しい音声メッセージ (赤の点灯) を通知します。
2	ペーパー ラベル	ペーパー ストリップは、名前や連絡先の電話番号を記入するために使用します。
3	転送ボタン 	コールを転送します。
4	会議ボタン 	会議コールを開始します。

5	保留ボタン 	アクティブ コールを保留します。
6	回線ボタン 	2 番目の着信コールをピックアップしたり、保留中のコールを再開したりできます。LED はコール ステータスを示します。
7	スピーカーフォン ボタン 	デフォルトの音声パスとしてスピーカーフォンを選択して、新しいコールを開始したり、着信コールをピックアップしたり、コールを終了したりします。コール中、ボタンは緑色に点灯します。スピーカーフォン音声パスは、（たとえば、ハンドセットをピックアップすることによって）新しい音声パスを選択するまで変更されません。
8	キーパッド	電話番号をダイヤルできます。
9	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。マイク音声ミュートになっているとき、ボタンは赤色に点灯します。
10	音量ボタン 	ハンドセットとスピーカーフォンの音量（オフフック時）および呼出音の音量（オンフック時）を制御します。
11	メッセージ ボタン 	ボイス メッセージング システムを自動的にダイヤルします。
12	リダイヤル ボタン 	最後にダイヤルした番号をダイヤルします。

13	機能ボタン 	<p>機能ボタンを使用すると、電話機のセットアップに応じて、短縮ダイヤル、すべてのコールの転送、ピックアップ、グループピックアップ、およびミーティングの各機能にアクセスできます。機能ボタンでは、最大9つの項目を設定できます。これらの機能にアクセスするには、機能ボタンを押した後、その機能に関連付けられた番号を入力します。機能ボタンと番号は、互いに5秒以内に押す必要があります。この数字には、1から9の1桁の数字だけを指定できます。</p> <p>オフフック時またはオンフック時に、次の機能にアクセスできます。</p> <ul style="list-style-type: none"> • すべてのコールの転送：コールを転送できます。 • ピックアップ：サードパーティ製の電話機のコールをピックアップできます。 • グループピックアップ：グループ内のコールをピックアップできます。 • ミートミー：会議を設定できます。
14	ハンドセット	電話機のハンドセットです。

ペーパー ラベル

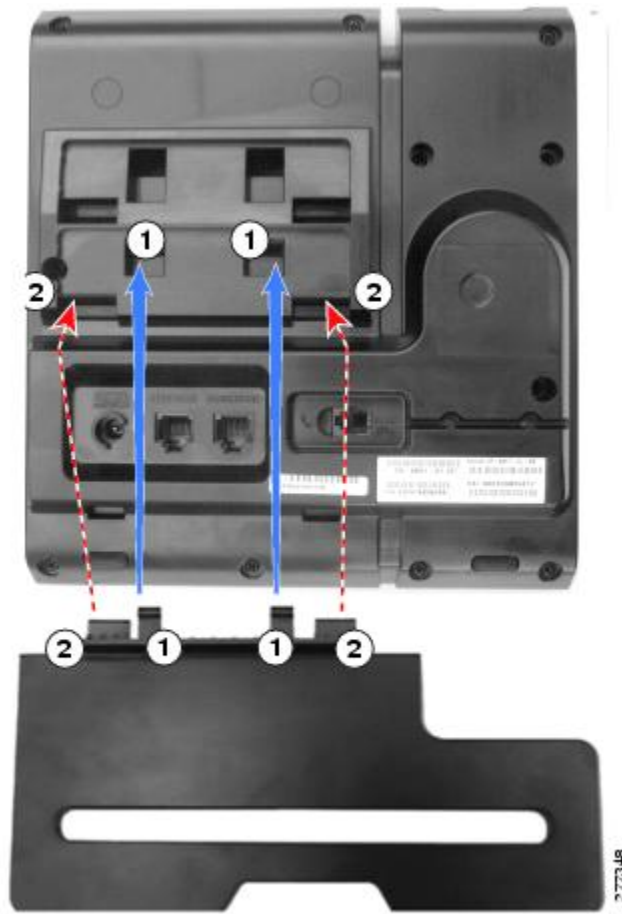
Cisco Unified IP Phone 6911 には、LCD 画面は搭載されていません。シスコでは、名前や連絡先の番号を入力するために使用できるペーパー ストリップを提供しています。

一般的な電話情報

この項には、このマニュアルのすべての IP Phone モデルに共通の情報が含まれています。

フットスタンド

電話機をテーブルまたは机の上に置いている場合は、フットスタンドを電話機の背面に取り付けます。表示角度は好みに応じて調整できます。



1	コネクタを下のスロットに差し込みます。	2	コネクタが上のスロットにはまるまでフットスタンドを持ち上げます。
---	---------------------	---	----------------------------------

電話機の表示角度

電話機の角度を上げる

手順

次の図に示すように、高めの表示角度用の下方のスロットにフットスタンドを接続します。



電話機の角度を下げる

手順

次の図に示すように、低めの表示角度用の上方のスロットにフットスタンドを接続します。



ネットワーク プロトコル

Cisco Unified IP Phone は、音声通信に必要な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。次の表は、Cisco Unified IP Phone 6901 および 6911 でサポートされているネットワーク プロトコルの概要を示しています。

表 1 : Cisco Unified IP Phone でサポートされ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
Cisco Audio Session Tunneling (CAST) (Cisco Unified IP Phone 6911 のみ)	CAST プロトコルの利用により、IP Phone とその電話機の背後にある関連アプリケーションは、Cisco Unified Communications Manager やゲートウェイなどの従来のシグナリング コンポーネントに変更を加えることなく、リモート エンドポイントを検出し、通信できます。CAST プロトコルを利用することにより、別個のハードウェア デバイスで関連するメディアを同期化できます。また、PC アプリケーションでは、PC をビデオリソースとして使用することにより、ビデオ非対応の電話機がビデオ対応になるように拡張できます。	-
Cisco Discovery Protocol (CDP)	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。 CDP を使用することにより、デバイスは自身の存在を他のデバイスにアドバタイズしたり、ネットワーク内の他のデバイスに関する情報を受信したりします。	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。

ネットワーク プロトコル	目的	使用上の注意
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)	<p>DHCP は、IP アドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。</p> <p>DHCP を使用すると、IP Phone をネットワークに接続するだけで、IP アドレスを手動で割り当てたり、追加のネットワーク パラメータを設定したりしなくてもその電話機を機能させることができます。</p>	<p>デフォルトでは、電話機の DHCP は有効になっています。無効にした場合は、個々の電話機がある場所で、IP アドレス、サブネットマスク、ゲートウェイ、および TFTP サーバを手動で設定する必要があります。</p> <p>シスコでは、DHCP のカスタム オプション 150 を使用することを推奨します。この方法では、TFTP サーバの IP アドレスをオプション値として設定します。サポートされているその他の DHCP 設定については、『Cisco Unified Communications Manager System Guide』の「Dynamic Host Configuration Protocol」と「Cisco TFTP」の章を参照してください。</p> <p>(注) オプション 150 を使用できない場合、DHCP オプション 66 の使用を試みることができます。</p>
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、HTTP をトラブルシューティング用に使用しています。
IEEE 802.1X	<p>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。</p> <p>802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続されているポート経由では Extensible Authentication Protocol over LAN (EAPOL) トラフィックしか許可されません。認証が成功した後は、通常のトラフィックがそのポートを通過します。</p>	<p>Cisco Unified IP Phone では、EAP-FAST および EAP-TLS 認証方式をサポートすることによって、IEEE 802.1X 標準が実装されています。</p> <p>電話機で 802.1X 認証が有効である場合は、ボイス VLAN を無効にします。詳細については、802.1X 認証、(26 ページ) を参照してください。</p>

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。	<p>IP を使用して通信するには、ネットワークデバイスに対して、IP アドレス、サブネット、およびゲートウェイが割り当てられている必要があります。</p> <p>Cisco Unified IP Phone を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) で使用している場合は、IP アドレス、サブネット、およびゲートウェイが自動的に割り当てられます。DHCP を使用しない場合は、個々の電話機がある場所で、これらのプロパティを手動で割り当てる必要があります。</p> <p>Cisco Unified IP Phone は、IPv6 アドレスをサポートしています。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。</p>
Link Layer Discovery Protocol (LLDP) (Cisco Unified IP Phone 6911 のみ)	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 6911 は、スイッチおよび PC ポートで LLDP をサポートしています。
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED は、音声製品用に開発された、LLDP 標準の拡張です。	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <p>http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html</p>

ネットワークプロトコル	目的	使用上の注意
リアルタイム転送プロトコル (RTP)	RTP は、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データ ネットワーク経由で転送するための標準プロトコルです。	Cisco Unified IP Phone では、RTP プロトコルを使用して、リアルタイム音声トラフィックを他の電話機やゲートウェイとやり取りします。
Real-Time Control Protocol (RTCP; リアルタイム制御プロトコル)	RTCP は RTP と連動して、RTP ストリーム上で QoS データ (ジッター、遅延、ラウンドトリップ遅延など) を伝送します。	デフォルトでは、電話機の RTCP は無効になっていますが、Cisco Unified Communications Manager を使用して個々の電話機で有効にすることができます。
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) のいずれかを使用するように設定できます。
Skinny Client Control Protocol (SCCP)	SCCP は、コール制御サーバとエンドポイント クライアント (IP Phone など) の間で通信を行うためのメッセージング セットを含んでいます。SCCP は、シスコ独自のものです。	Cisco Unified IP Phone 6901 および 6911 では、コール制御に SCCP バージョン 20 を使用します。
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 への接続に TCP を使用します。

ネットワークプロトコル	目的	使用上の注意
トランスポートレイヤセキュリティ (TLS)	TLS は、通信の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、『 <i>Cisco Unified Communications Manager Security Guide</i> 』を参照してください。
トリビアルファイル転送プロトコル (TFTP)	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 Cisco Unified IP Phone で TFTP を使用すると、電話タイプ固有の設定ファイルを取得できます。	TFTP では、ネットワーク内に TFTP サーバが必要です。このサーバは、DHCP サーバで自動的に識別できます。DHCP サーバが指定する以外の TFTP サーバを電話機で使用する場合は、電話機の [ネットワークの設定 (Network Configuration)] メニューを使用して、TFTP サーバの IP アドレスを手動で割り当てる必要があります。 詳細については、『 <i>Cisco Unified Communications Manager System Guide</i> 』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 を使用する 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](#)

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

Cisco Unified IP Phone は、デジタル ビジネス フォンとほぼ同様に機能し、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 には、電話機をネットワーク デバイスとして管理したりモニタしたりできる機能も含まれています。

機能の概要

Cisco Unified IP Phone は、従来のテレフォニー機能、コール転送、転送、リダイヤル、会議、およびボイス メッセージ システム アクセスを提供します。Cisco Unified IP Phone では、さらにその他の各種の機能も提供します。これらの機能の詳細については、『*Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*』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。ネットワークに必要な場合は、IP アドレス、TFTP サーバ、サブネット情報などの情報を手動で設定できます。

最後に、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電話機から直接取得できます。この情報は、ユーザが IP Phone を使用しているときに生じた問題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 の設定](#)

[機能、テンプレート、サービス、およびユーザ セットアップ](#)

[トラブルシューティングとメンテナンス](#)

テレフォニー機能の管理

Cisco Unified IP Phone の追加の設定値は、Cisco Unified Communications Manager から変更できます。特に、電話機の登録基準やコーリング サーチ スペースを設定するには、Cisco Unified Communications Manager を使用します。

Cisco Unified Communications Manager 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。

関連トピック

[Cisco Unified IP Phone で使用可能なテレフォニー機能](#)

[関連資料](#)

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、電話機で設定します。

関連トピック

[Cisco Unified IP Phone の設定](#)

エンドユーザ向けの情報

システム管理者は、多くの場合、ネットワーク内や社内の Cisco Unified IP Phone ユーザの主な情報源になります。機能や手順について確実に最新の情報を伝えるために、Cisco Unified IP Phone の Web サイトにある Cisco Unified IP Phone のマニュアルをよく読んでおいてください。

マニュアルの提供に加えて、ユーザに電話機で有効になっている機能（企業またはネットワークに固有の機能を含む）を通知するようにしてください。また、必要に応じて、ユーザにこれらの機能にアクセスしたり、カスタマイズしたりする方法も伝えるようにしてください。社内のサポート Web サイトを使用して、ユーザに常に情報を通知するようにもできます。

関連トピック

[社内のサポート Web サイト](#)

[Cisco Unified IP Phone 6900 シリーズのマニュアル](#)

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に、Cisco IP テレフォニー ネットワークは、電話機とサーバの間で認証および暗号化された通信ストリームを確立して維持し、電話機に転送される前のファイルにデジタル署名し、Cisco Unified IP Phone 間のメディアストリームおよびコールシグナリングを暗号化します。

Cisco Unified IP Phone 6901 および 6911 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している電話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電話機への適用については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Unified Communications Manager でセキュリティ関連の設定を行うと、電話機の設定ファイルに機密情報が保存されます。設定ファイルのプライバシーを確保するには、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」の章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 および Cisco Unified Communications Manager のセキュリティ関連トピック

トピック	参照
Cisco Unified Communications Manager および Cisco Unified IP Phone に関するセットアップ情報、設定情報、およびトラブルシューティング情報を含む、セキュリティの詳細な説明	『 <i>Troubleshooting Guide for Cisco Unified Communications Manager</i> 』および『 <i>Cisco Unified Communications Manager Security Guide</i> 』
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, (20ページ)
セキュリティ プロファイル名の表示	Cisco Unified IP Phone 6901 および 6911 でサポートされるセキュリティ機能の概要については、 サポート対象のセキュリティ機能, (20ページ) を参照してください。これらの機能と、Cisco Unified Communications Manager および Cisco Unified IP Phone のセキュリティの詳細については、『 <i>Cisco Unified Communications Manager Security Guide</i> 』を参照してください。
セキュリティが実装されているコールの識別	認証、暗号化、および保護されているコール, (23 ページ)
TLS 接続	<ul style="list-style-type: none"> • ネットワーク プロトコル, (11 ページ) • Cisco Unified Communications Manager での電話機の追加方法
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
セキュリティと電話機の設定ファイル	Cisco Unified Communications Manager での電話機の追加方法
電話機の Web ページへのアクセスの無効化	Web ページへのアクセスの無効化および有効化
トラブルシューティング	<ul style="list-style-type: none"> • トラブルシューティングとメンテナンス • 『<i>Troubleshooting Guide for Cisco Unified Communications Manager</i>』
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
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

トピック	参照
Cisco Unified IP Phone の 802.1X 認証	<ul style="list-style-type: none"> • 802.1X 認証, (26 ページ) • トラブルシューティングとメンテナンス

サポート対象のセキュリティ機能

次の表は、Cisco Unified IP Phone 6901 および 6911 でサポートされているセキュリティ機能の概要を示しています。これらの機能と、Cisco Unified Communications Manager および Cisco Unified IP Phone のセキュリティの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。



(注) ほとんどのセキュリティ機能は、電話機に証明書信頼リスト (CTL) が含まれている場合のみ使用できます。CTLの詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Configuring the Cisco CTL Client」の章を参照してください。

表 3: セキュリティ機能の概要

機能	説明
イメージ認証	署名付きバイナリ ファイル (.zz.sgn 拡張子) によって、ファームウェア イメージが電話機へのロード前に改ざんされることを防止します。イメージが改ざんされると、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的な証明書が必要とします。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 Communications Manager の管理ページで、Certificate Authority Proxy Function (CAPF; 認証局プロキシ関数) を使用して証明書をインストールするように指定できます。

機能	説明
デバイス認証	Cisco Unified Communications Manager サーバと電話機間で、一方のエンティティが他方のエンティティの証明書を受け入れるときに行われます。電話機と Cisco Unified Communications Manager の間でセキュアな接続を確立するかどうかを判別し、必要に応じて TLS プロトコルを使用してエンティティ間にセキュアなシグナリングパスを作成します。Cisco Unified Communications Manager で電話機を認証できない限り、Cisco Unified Communications Manager ではそれらの電話機は登録されません。
ファイル認証	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。電話機は認証されていないファイルを拒否し、それ以上の処理を行いません。
シグナリング認証	TLS プロトコルを使用して、シグナリング パケットが転送中に改ざんされていないことを検証します。
製造元でインストールされる証明書	各 Cisco Unified IP Phone には、固有の Manufacturing Installed Certificate (MIC; 製造元でインストールされる証明書) が内蔵されており、デバイス認証に使用されます。MIC は、電話機に固有の永続的な ID 証明であり、Cisco Unified Communications Manager ではそれを利用して電話機を認証します。
セキュアな SRST リファレンス	Cisco Unified Communications Manager でセキュリティに Cisco Unified Survivable Remote Site Telephony (SRST) 参照を設定し、依存デバイスをリセットすると、TFTP サーバによって SRST 証明書が電話機の設定ファイルに追加され、そのファイルが電話機に送信されます。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。 この設定ファイルは、次のいずれかの拡張子を使用します。 <ul style="list-style-type: none"> • .cnf.xml • .cnf.xml.sgn • .cnf.xml.enc.sgn
メディアの暗号化	SRTP を使用して、サポートされる電話機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、意図した電話機のみがデータを受信して読み取れるようにします。電話機のメディアマスターのキーペアの作成、電話機へのキーの配布、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。

機能	説明
シグナリング暗号化	電話機と Cisco Unified Communications Manager サーバの間で送信されるすべての SCCP および SIP シグナリングメッセージが暗号化されるようにします。
Certificate Authority Proxy Function (CAPF)	電話機に非常に高い処理負荷がかかる、証明書生成手順の一部を実装します。また、キーの生成および証明書のインストールのために電話機と対話します。電話機の代わりに、お客様指定の認証局に証明書を要求するよう CAPF を設定できます。または、ローカルで証明書を生成するように CAPF を設定することもできます。
セキュリティプロファイル	電話機がセキュリティ保護、認証、または暗号化の対象になるかどうかを定義します。
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)	電話機のさまざまな操作統計情報を表示する電話機の Web ページへのアクセスを防止します。
電話機のセキュリティ強化	次に、Cisco Unified Communications Manager から制御する追加のセキュリティ オプションを示します。 <ul style="list-style-type: none"> • 電話機の Web ページへのアクセスの無効化
802.1X 認証	ネットワークへのアクセスを要求および取得するための 802.1X 認証の使用を定義します。
音声品質メトリック	
MOS LQK	リスニング品質 (LQK) の平均オピニオン評点 (MOS) を客観的に評価するスコアで、音声品質が 5 (優良) ~ 1 (不良) でランク付けされます。このスコアは、音声ストリームの先行する 8 秒間でのフレーム損失に起因する音声隠蔽イベントに基づいています。 <p>(注) MOS LQK スコアは、Cisco Unified IP Phone が使用するコーデックのタイプに基づいて変化する可能性があります。</p>
平均 MOS LQK	音声ストリーム全体で測定された平均 MOS LQK スコア。
最小 MOS LQK	音声ストリームの開始以降に測定された最も低い MOS LQK スコア。

機能	説明
最大 MOS LQK	音声ストリーム開始以降に測定されたベースライン MOS LQK スコアまたは最も高い MOS LQK スコア。 フレーム損失のない通常の条件下で最大 MOS LQK スコアを提供するコーデックを次に示します。 <ul style="list-style-type: none"> • G.711 : 4.5 • G.728/iLBC : 3.9 • G729A/AB : 3.7
MOS LQK のバージョン	MOS LQK のスコアを計算するために使用されるシスコ独自のアルゴリズムのバージョン。

関連トピック

- [Cisco Unified IP Phone のセキュリティ機能, \(18 ページ\)](#)
- [セキュリティ プロファイル, \(23 ページ\)](#)
- [802.1X 認証, \(26 ページ\)](#)
- [認証、暗号化、および保護されているコール, \(23 ページ\)](#)
- [Cisco Unified IP Phone のセキュリティ](#)

セキュリティ プロファイル

Cisco Unified Communications Manager をサポートしている Cisco Unified IP Phone は、すべてセキュリティ プロファイルを使用します。このプロファイルは、電話機がセキュリティ保護、認証、または暗号化の対象になるかどうかを定義するものです。セキュリティ プロファイルの設定、およびプロファイルの電話機への適用については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

電話機のセキュリティ モードを表示するには、Cisco Unified Communications Manager でセキュリティ プロファイルを表示できます。

関連トピック

- [認証、暗号化、および保護されているコール, \(23 ページ\)](#)

認証、暗号化、および保護されているコール

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。

暗号化されたコールでは、コールの確立に参加しているすべてのデバイスが信頼できるデバイスであり、Cisco Unified Communications Manager によって認証されています。さらに、コールのシグナリングとメディアストリームが暗号化されます。暗号化されたコールはコールの整合性とプライバシーを提供することで、高レベルのセキュリティを提供します。

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

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) 2台の電話機間の接続では、保護されたコールがサポートされます。電話会議や共有回線など一部の機能は、保護されたコールが設定されているときは使用できません。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, \(18 ページ\)](#)

保護されたコールの識別

お使い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は、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コールでは、保護されたコールはサポートされません。

保護されたコールは、次のプロセスを使用して確立されます。

- 1 ユーザが保護された電話機（保護されたセキュリティ モード）からコールを開始します。
- 2 そのコールが別の保護された電話機に接続された場合は、セキュリティ トーンが再生され、通話の両端が暗号化および保護されていることを示します。そのコールが保護されていない電話機に接続された場合、セキュリティ トーンは再生されません。



- (注) 2台の電話機間の接続では、保護されたコールがサポートされます。電話会議や共有回線など一部の機能は、保護されたコールが設定されている場合は使用できません。

コールセキュリティの連携動作と制限事項

Cisco Unified Communications Manager は、会議の確立時に電話機のセキュリティステータスを確認し、会議のセキュリティ表示を変更するか、またはコールの完了をブロックしてシステム内の整合性とセキュリティを維持します。

次の表は、Cisco Unified IP Phone 6911 の場合の、割り込み使用時のコールのセキュリティレベルの変更にに関する情報を示しています。

表 4: 割り込み使用時のコールセキュリティの連携動作 (Cisco Unified IP Phone 6911 のみ)

発信側の電話機のセキュリティレベル	使用される機能	コールのセキュリティレベル	アクションの結果
非セキュア	cBarge	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)	cBarge	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)	cBarge	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	cBarge	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た、会議のセキュリティレベルの変更にに関する情報を示しています。

表 5: 会議コールのセキュリティの制限事項

発信側の電話機のセキュリティレベル	使用される機能	参加者のセキュリティレベル	アクションの結果
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	非セキュアな会議

発信側の電話機のセキュリティレベル	使用される機能	参加者のセキュリティレベル	アクションの結果
セキュア (暗号化済み)	会議	すべての参加者が暗号化済み	セキュアな暗号化レベルの会議
セキュア (認証済み)	会議	すべての参加者が暗号化済みまたは認証済み	認証済みレベルのセキュアな会議
非セキュア	cBarge	すべての参加者が暗号化済み	会議が非セキュアに変更されます。
非セキュア	ミーティング	最小限のセキュリティレベルが暗号化	発信側は、「セキュリティレベルを満たしていません (Does not meet Security Level)」というメッセージを受信し、コールは拒否されます。
セキュア (暗号化済み)	ミーティング	最小セキュリティレベルは、認証済み	会議は、暗号化済みおよび認証済みのコールを受け入れます。
セキュア (暗号化済み)	ミーティング	最小限のセキュリティレベルは非セキュア	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。

802.1X 認証

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

概要

Cisco Unified IP Phone と Cisco Catalyst スイッチは、従来 Cisco Discovery Protocol (CDP) を使用して互いを識別し、VLAN 割り当てやインライン所要電力などのパラメータを決定します。CDP では、ローカルに接続されたワークステーションは識別されません。Cisco Unified IP Phone は、EAPOL パススルーメカニズムを提供します。このメカニズムを使用すると、Cisco Unified IP Phone に接続されたワークステーションは、LAN スイッチにある 802.1X オーセンティケータに EAPOL メッセージを渡すことができます。パススルーメカニズムでは、IP Phone が、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ための LAN スイッチとしては機能しないことが保証されます。

Cisco Unified IP Phone はまた、プロキシ EAPOL ログオフメカニズムも提供します。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 の間のリンクは維持されるため、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 にはまた、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、ネットワークにアクセスするための要求を開始する 802.1x サプリカントとして機能します。
- 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、電話機を認証するための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の間でメッセージを渡すことができるように、802.1X をサポートしている必要があります。この交換が完了した後、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 プラクティスの要件と推奨事項

- 802.1X 認証の有効化 : 802.1X 標準を使用して Cisco Unified IP Phone を認証する場合は、電話機でその標準を有効にする前に、その他のコンポーネントが正しく設定されていることを確認してください。
- PC ポートの設定 : 802.1X 標準では VLAN の使用が考慮されないため、シスコでは、特定のスイッチポートに対して認証するデバイスを 1 台だけにするのを推奨しています。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)。スイッチの設定により、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。



(注) PC ポートを備えているのは Cisco Unified IP Phone 6911 だけです。

- 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、PC ポートを有効にしてそこに PC を接続することができます。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：スイッチで同じポート上の複数の 802.1X 準拠デバイスがサポートされていない場合は、802.1X 認証を有効にするときに PC ポートが無効にするようにしてください。PC ポートが無効化せずに PC を接続しようとする、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、この設定をスイッチのサポートに基づいて行うようにしてください。
 - 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：スイッチで複数ドメインの認証がサポートされていない場合は、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。Cisco IP テレフォニー ネットワークおよびそのセットアップと設定のチェックリストについては、『*Cisco Unified Communications Manager System Guide*』の「System Configuration Overview」の章を参照してください。

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

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 Communications Manager が混合モードで動作している場合はサポートされません。
- Cisco Unified Communications Manager
- 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、次の資料を参照してください。

- 「Cisco Unified IP Phone」：『*Cisco Unified Communications Manager System Guide*』
- 「Cisco Unified IP Phone Configuration」：『*Cisco Unified Communications Manager Administration Guide*』

- 「Autoregistration Configuration」 : 『Cisco Unified Communications Manager Administration Guide』

次に、詳細について説明します。

Cisco Unified Communications Manager での Cisco Unified IP Phone 6901 および 6911 のセットアップ

次の手順は、Cisco Unified Communications Manager の管理ページでの Cisco Unified IP Phone 6901 および 6911 に対する設定タスクの概要を示しています。この手順は、電話機の設定プロセスを実行するための推奨される順序を示しています。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。詳細な手順および情報については、この手順に示されている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
- 電話機に割り当てるための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。

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 電話機に対応する十分なユニットライセンスがあることを確認します。詳細については、『Cisco Unified Communications Manager Administration Guide』の「License Unit Report」の章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。フィールド名の横にあるアスタリスク (*) は、MAC アドレスやデバイスプールなどの必須フィールドを示します。

デフォルト設定値を持つ電話機が Cisco Unified Communications Manager データベースに追加されます。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。

[プロダクト固有の設定 (Product Specific Configuration)] フィールドについては、[電話の設定 (Phone Configuration)] ウィンドウで [?] ボタンのヘルプを参照してください。

(注) Cisco Unified Communications Manager データベースに電話機とユーザの両方を同時に追加する場合は、『*Cisco Communications Manager Administration Guide*』の「User/Phone Add 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。フィールド名の横にあるアスタリスク (*) は、電話番号やプレゼンス グループなどの必須フィールドを示します。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 必須フィールドを設定して、ユーザ情報を追加します。フィールド名の横にあるアスタリスク (*) は、ユーザ ID や姓などの必須フィールドを示します。

(注) パスワード (ユーザオプション Web ページ用) および PIN (音声自動応答装置 (IVR) からのネットワーク メニューへのアクセス用) を割り当てます。

Cisco Unified Communications Manager (Unified CM) のグローバルディレクトリにユーザ情報を追加します。

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 へのユーザの追加](#) を参照してください。

(注) Cisco Unified Communications Manager データベースに電話機とユーザの両方を同時に追加する場合は、『*Cisco Unified Communications Manager Administration Guide*』の「User/Phone Add Configurations」の章を参照してください。

ステップ 6 ユーザをユーザ グループに関連付けます。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。

(注) エンドユーザが Cisco Unified CM ユーザ オプションにアクセスするには、ユーザを標準 Cisco CCM エンドユーザ グループに追加する必要があります。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の次の項を参照してください。

- 「End User Configuration」の章にある「End User Configuration Settings」。
- 「User Group Configuration」の章にある「Adding Users to a User Group」。

ステップ 7 ユーザを電話機に関連付けます。ユーザが、コールの転送や、短縮ダイヤル番号またはサービスの追加などのアクションのために自分の電話機を制御できるようにします。

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

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「End User Configuration」の章にある「Associating Devices to an End User」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（または電話機のユーザ）は、電話機をユーザの作業場所に設置できます。



(注) 電話機を設置する前に、現在のファームウェア イメージで電話機をアップグレードします。アップグレードについては、次の URL にある、お使いの電話機の **Readme** ファイルを参照してください。

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>

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

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

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

自動登録を使用した場合は、電話機をユーザに関連付ける、ボタンテーブルや電話番号を変更するなど、電話機の特定の設定情報をアップデートする必要があります。

Cisco Unified IP Phone 6901 および 6911 の設置

次の手順は、Cisco Unified IP Phone 6901 および 6911 の設置作業の概要を示しています。この手順は、電話機の設定を実行するための推奨される順序を示しています。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。詳細な手順および情報については、この手順に示されている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。詳細については、[Cisco Unified IP Phone の電源](#)を参照してください。

ステップ 2 電話機を組み立て、電話機の位置を調節し、ネットワーク ケーブルを接続します。電話機の位置を決めて設置し、ネットワークに接続します。[Cisco Unified IP Phone の設置](#)を参照してください。

[フットスタンド](#), [\(8 ページ\)](#) を参照してください。

ステップ 3 電話機の起動プロセスをモニタします。電話番号を電話機に関連付け、電話機が正しく設定されていることを確認します。

[電話機の起動確認](#)を参照してください。

ステップ 4 電話上でネットワーク設定値を設定する場合、DHCP を使用するか、手動で IP アドレスを入力して、電話機の IP アドレスを設定します。

- **DHCP の使用**

IVR を使用して、電話機の DHCP が有効になっていることを確認します。IVR から入力を求められたら TFTP の IP アドレスを入力することにより、代替 TFTP サーバを設定できます。

(注) DHCP で割り当てられる TFTP サーバを使用する代わりに、代替 TFTP サーバを割り当てる必要があるかどうかを、ネットワーク管理者に相談してください。

- **DHCP を使用しない場合**

IVR を使用して、電話機の DHCP が無効になっていることを確認します。次に、電話機で IVR を使用して、IP アドレス、サブネットマスク、TFTP サーバ、およびデフォルトルータをローカルに設定する必要があります。

詳細については、[ネットワーク設定](#)および[Cisco Unified IP Phone のネットワーク設定値のセットアップ](#)を参照してください。

ステップ 5 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。

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。

ステップ 6 Cisco Unified IP Phone を使用して、コールを発信します。電話機および機能が正常に動作することを確認します。詳細については、『*Cisco Unified IP Phone 6901 and 6911 User Guide for Cisco Unified Communications Manager (SCCP and SIP)*』を参照してください。

ステップ 7 エンドユーザに対して、電話機の使用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。

[社内のサポート Web サイト](#)を参照してください。

電話機の電力消費量の節減

Cisco Unified IP Phone 6901 および 6911 は、Cisco EnergyWise (EW) (Power Save Plus と呼ばれる) をサポートしています。ネットワークに EnergyWise コントローラが含まれている場合は、消費電力を削減するために、これらの電話機をスケジュールに従ってスリープ (電源オフ) および復帰 (電源オン) するように設定できます。

EnergyWiseは、電話機ごとに有効または無効に設定します。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、電話機の設定ファイルの一部として電話機に送信されます。

関連トピック

[電話機設定ファイル](#)

[Cisco Unified IP Phone 6901 および 6911 での EnergyWise のセットアップ](#)

用語の違い

次の表は、次のドキュメントで使用されている用語の重要な違いのいくつかを示しています。

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

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

