# Cisco Unified IP Phone

Cisco Unified IP Phone 7975G、7971G-GE（ギガビット イーサネット バージョン）、7970G、7965G、および7945Gは、インターネットプロトコル（IP）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。 これらの 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、Cisco Unified IP Phone はデータ ネットワークに接続されるため、IP テレフォニー機能が拡張され、ネットワーク情報やサービス、およびカスタマイズ可能な機能やサービスにアクセスできるようになります。 ファイル認証、デバイス認証、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 7975G、7971G-GE、7970G、7965G、および 7945G は、カラー画面を備えています（7975G、7971G-GE、および 7970G はタッチスクリーンです）。また、回線番号や短縮ダイヤル番号のサポート、ボタンおよび機能の状況依存オンライン ヘルプ、その他の多様で高度な機能があります。

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。 Cisco Unified IP Phone は G.711a、G.711μ、G.722、G.729a、G.729ab、iLBC をエンコードし、G.711a、G.711μ、G722、iLBC に加え、G.729、G729a、G.729b、G.729ab 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。

**注意**

セル方式の電話、携帯電話、GSM 電話、または双方向ラジオを Cisco Unified IP Phone のすぐ近くで使用すると、相互干渉が発生することがあります。 詳細については、干渉が発生するデバイスの製造元のマニュアルを参照してください。

この章は、次の項で構成されています。

- 電話機の消費電力，27 ページ
- Cisco Unified IP Phone の導入，28 ページ


# Cisco Unified IP Phone 7975G、7971G-GE、7970G、7965G、および 7945G のコンポーネント

次の各項では、電話機のコンポーネントについて説明します。

## Cisco Unified IP Phone 7975G のボタンおよびハードウェア

次の図に、電話機の重要なパーツを示します。 番号付きの項目については、ボタンとハードウェアの識別，（4 ページ）を参照してください。


## Cisco Unified IP Phone 7970G および 7971G-GE のボタンとハードウェア

次の図に、電話機の重要なパーツを示します。 番号付きの項目については、ボタンとハードウェアの識別，（4 ページ）を参照してください。


# Cisco Unified IP Phone 7965G のボタンおよびハードウェア

次の図に、電話機の重要なパーツを示します。 番号付きの項目については、ボタンとハードウェアの識別, （4 ページ）を参照してください。


# Cisco Unified IP Phone 7945G のボタンおよびハードウェア

次の図に、電話機の重要なパーツを示します。 番号付きの項目については、ボタンとハードウェアの識別, （4 ページ）を参照してください。


# ボタンとハードウェアの識別

次の表では、電話機のボタンとハードウェアについて説明します。

**表 *1*：電話機のボタンとハードウェア**

| | 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 ボタンからは次にアクセスできます。<br>• 電話回線（回線ボタン）とインターコム回線<br>• 短縮ダイヤルの番号（短縮ダイヤルボタン）（ビジーランプ フィールド（BLF）短縮ダイヤル機能を含む）<br>• Web ベースのサービス（個人アドレス帳ボタンなど）<br>• コール機能（プライバシー、保留、転送のボタンなど）<br>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。<br>• 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<br>• 緑、点滅：保留コール<br>• オレンジ、点灯：プライバシー機能が使用中、単方向インターコム コール、サイレント（DND）機能がアクティブ、またはハント グループにログイン中<br>• オレンジ、点滅：着信コールまたは復帰コール<br>• 赤、点灯：リモート回線が使用中（シェアド ライン、BLF の状態またはアクティブなモバイル コネクト コール） |

| | 項目 | 説明 |
|---|---|---|
| 2 | フットスタンド ボタン | 電話機本体の角度を調節できます。 |
| 3 | ディスプレイ ボタン  | **Cisco Unified IP Phone 7970G、7971G-GE、および 7975G**<br>• 電話スクリーンをスリープ モードから復帰させます。または、クリーニングのためタッチスクリーン機能を無効にします。<br>•  色なし：入力できる状態です。<br>•  緑の点滅：無効<br>•  緑の点灯：スリープ モード<br>**Cisco Unified IP Phone 7945G および 7965G**<br>• 電話スクリーンをスリープ モードから復帰させます。<br>•  色なし：入力できる状態です。<br>•  緑の点灯：スリープ モード |
| 4 | メッセージ ボタン  | ボイス メッセージ サービスを自動的にダイヤルします（システムによって異なります）。 |
| 5 | ディレクトリ ボタン  | [ディレクトリ（Directories）] メニューを開閉します。 このボタンを使用して、コール ログおよびディレクトリにアクセスします。 |
| 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。 このボタンを使用して、電話スクリーンおよび呼出音の設定を変更します。 |
| 8 | サービス ボタン  | サービス メニューを開閉します。 |
| 9 | 音量ボタン  | ハンドセット、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 | 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。 |
| 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。 |

| | 項目 | 説明 |
|---|---|---|
| 13 | 4 方向ナビゲーション パッドと選択ボタン（中央）  | **Cisco Unified IP Phone 7945G、7965G、および 7975G**<br>• メニューのスクロールや項目の強調表示に使用できます。選択ボタンを使用して、スクリーン上で強調表示された項目を選択します。<br>• ナビゲーションボタン：上下にスクロールすると、メニューを表示し、項目を強調表示できます。左右にスクロールすると、複数の列にまたがって表示できます。<br>• 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、行を強調表示します。  を押してメニューを開き、呼出音を再生するか、スクリーンの表示に従って他の機能にアクセスします。 |
| 14 | ナビゲーション ボタン  | **Cisco Unified IP Phone 7970G および 7971G-GE**<br>• メニューのスクロールや項目の強調表示に使用できます。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。 |
| 15 | 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できます。 |
| 16 | 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。 |
| 17 | ハンドセットのライト ストリップ | 着信コールまたは新しいボイス メッセージがあることを示します。 |
| 18 | 電話スクリーン | 電話機の機能を表示します。 |

# 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。 次の表に、Cisco Unified IP Phone 7975G、7971G-GE、7970G、7965G、および 7945G でサポートされるネットワーク プロトコルの概要を示します。

表 *2*：***Cisco Unified IP Phone*** でサポートされるネットワーク プロトコル

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| 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。<br>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、ネットワークの他のデバイスに関する情報を受信できます。 | Cisco Unified IP Phone では、補助 VLAN ID、ポートごとの電源管理の詳細情報、Quality of Service（QoS）設定情報などの情報を、CDP を使用して Cisco Catalyst スイッチとやり取りしています。 |
| 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のピア デバイスからネイバー デバイスへのコピーも行います。 | ピア ファームウェア共有機能で CPPDP が使用されます。 |
| 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） | 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。<br>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。<br>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」および「Cisco TFTP」の章を参照してください。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| 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。 電話機は、HTTP を使用して設定ファイルおよびファームウェア ロードをダウンロードします。 HTTP ダウンロードが失敗した場合、電話機は TFTP を使用してファイルを転送します。<br><br>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） | 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 の場合、2 つの URL のうち HTTPS URL を選択します。 |
| IEEE 802.1X | IEEE 802.1X 標準は、クライアント/サーバベースのアクセス 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。<br><br>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。<br><br>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,（25 ページ）を参照してください。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| 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 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。<br>IP アドレス、サブネット、およびゲートウェイの識別情報は、Dynamic Host Configuration Protocol（DHCP）を通じて Cisco Unified IP Phone を使用する場合は、自動的に割り当てられます。 DHCP を使用しない場合は、個々の電話機がある場所で、これらのプロパティを手動で割り当てる必要があります。<br>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 Communications Manager の管理ページで IP アドレッシング モード（IPv4 のみ、IPv6 のみ、または 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。 |
| 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。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| 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。<br>• ボイス VLAN の設定<br>• デバイスの検出<br>• 電源管理<br>• インベントリ管理<br>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。<br>http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml |
| Real-Time Control Protocol（RTCP; リアルタイム制御プロトコル） | RTCP は Real-Time Transport Protocol（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 の管理ページで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。 |
| 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。 |

| ネットワーク 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におけるシグナリングとセッション管理の機能に対応します。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。<br>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。<br>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、どのパラメータが使用可能かを特定します。会議は、会議に参加するすべてのエンドポイントでサポートされている SDP 機能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 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。 |

| ネットワーク 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 に安全に登録するために TLS プロトコルが使用されます。<br>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。<br>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。<br>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。 |

# 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）は、32 ビット アドレスを使用するため、インターネットに接続す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。 したがって、インターネット プロトコル バージョン 6（IPv6）が、現在のインターネット プロトコルの更新バージョンとなります。 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。 Skinny Call Control Protocol（SCCP）を使用する Cisco Unified IP Phone は、IPv6 をサポートします。 SIP を使用する Cisco Unified IP Phone は、IPv6 をサポートしません。

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 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 で入手できる『*Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*』を参照してください。

# Cisco Unified IP Phone 7975G、7971G-GE、7970G、7965G、および 7945G 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。

このセクションは、次のトピックで構成されています。

## 機能の概要

Cisco Unified IP Phone は、コール転送や転送、リダイヤル、短縮ダイヤル、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、サブネット情報、その他の値などを手動で設定することもできます。

Cisco Unified IP Phone は、IP ネットワーク上の他のサービスやデバイスと連携することで、高度な機能を提供します。 たとえば、Cisco Unified IP Phone を社内の Lightweight Directory Access Protocol 3（LDAP3）標準ディレクトリと統合すると、ユーザが同僚の連絡先情報を IP Phone で直接検索できるようになります。 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 IP Phone を使用しているときに生じた問題をトラブルシューティングするのに役立ちます。

### 関連トピック

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
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 Administration アプリケーションから変更できます。 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 Communications Manager Administration Guide*』を参照してください。

Cisco Unified Communications Manager の管理アプリケーションの詳細については、『*Cisco Unified Communications Manager System Guide*』など、Cisco Unified Communications Manager のマニュアル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 スイートには、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いてください。 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。

### 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。

これらの攻撃を軽減するために、Cisco Unified 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 7975G、7971G-GE、7970G、7965G、および 7945G では、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。 電話機へのセキュリティ プロファイルの適用については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Unified Communications Manager の管理ページでセキュリティ関連の設定を行うと、電話機の設定ファイルに重要な情報が保存されます。 設定ファイルのプライバシーを確保するには、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 3：*Cisco Unified IP Phone* および *Cisco Unified Communications Manager* のセキュリティ関連トピック

| トピック | 参照先 |
|---|---|
| Cisco Unified Communications Manager および Cisco Unified IP Phone に関するセットアップ情報、設定情報、およびトラブルシューティング情報を含む、セキュリティの詳細な説明 | 『*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，（17 ページ）を参照してください。 |
| セキュリティ機能の制約事項 | 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，（20 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電話コール，（21 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。<br>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 [Unified CM 1] ～ [Unified CM 5] の各オプションのセキュリティ アイコン | 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 [セキュリティ設定（Security Configuration）] メニュー項目 | [セキュリティ設定（Security Configuration）] メニューを参照してください。 |

| トピック | 参照先 |
|---|---|
| 電話機の [設定（Settings）] メニューからアクセスする [セキュリティ設定（Security Configuration）] メニュー項目 | [セキュリティ設定（Security Configuration）] メニューを参照してください。 |
| CTL（証明書信頼リスト）ファイルと ITL（Identity Trust List）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。 |
| 電話機の Web ページへのアクセスの無効化 | 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。 |
| 電話機からの CTL ファイルの削除 | 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。 |
| エクステンション モビリティ 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。<br>• 802.1X 認証, （25 ページ）<br>• [802.1X 認証（802.1X Authentication）] および [802.1X 認証ステータス（802.1X Authentication Status）] メニュー<br>• 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 7975G、7971G-GE、7970G、7965G、および 7945G 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）] メニューを確認します（[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）。

（注） ほとんどのセキュリティ機能は、CTL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」の章を参照してください。

**表 *4*：セキュリティ機能の概要**

| 機能 | 説明 |
|---|---|
| イメージ認証 | 署名付きのバイナリ ファイル（拡張子 .sbn）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。 あるいは、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）をインストールします。 |
| 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 プロトコルを使用する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 では、認証できない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、電話機で署名を検証します。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。 |

| 機能 | 説明 |
|---|---|
| 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 | セキュリティ目的で SRST リファレンスを設定してから、Cisco Unified Communications Manager の管理ページで従属デバイスをリセットすると、TFTP サーバは電話機の cnf.xml ファイルに SRST 証明書を追加し、そのファイルを電話機に送信します。 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。 |
| メディアの暗号化 | Secure Real-time Transport Protocol（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、および意図したデバイスのみがデータを受信し、読み取ることを保証します。 デバイスのメディア マスターのキー ペアの作成、キーのデバイスへの配布、キーが転送される間のキー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） | 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します。 |

| 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。<br>• PC ポートの無効化<br>• Gratuitous ARP（GARP）の無効化<br>• PC ボイス VLAN アクセスの無効化<br>• [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<br>• 電話機の Web ページへのアクセスの無効化<br>（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）] オプション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。 |
| 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 アクセスができます。 |

### 関連トピック

セキュリティ プロファイル, （20 ページ）
認証、暗号化、および保護されている電話コール, （21 ページ）
セキュアな会議コールの特定, （22 ページ）
デバイス設定メニュー
802.1X 認証, （25 ページ）
Cisco Unified IP Phone のセキュリティ
Cisco Unified IP Phone の設定
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 リリース 7.0 以降をサポートする Cisco Unified IP Phone は、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電話コール, （21 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電話コール

電話機にセキュリティを実装している場合は、電話スクリーンに表示されるアイコンによって、認証済みの電話コールや暗号化された電話コールを識別できます。 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。

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、Cisco Unified Communications Manager によって認証される信頼できるデバイスです。 進行中のコールが認証されると、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 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、Cisco Unified Communications Manager によって認証される信頼できるデバイスです。 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、高レベルのセキュリティを提供し、コールの整合性とプライバシーを提供します。 進行中のコールが暗号化されると、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 に変わります。

（注） コールが PSTN（公衆電話交換網）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。 保護されていない電話機にコールが接続されると、セキュリティ トーンは再生されません。

（注） 保護されたコールは、2 台の電話機間の接続に対してのみサポートされます。 保護コールを設定すると、一部の機能（会議コール、シェアド ライン、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, （15 ページ）
セキュリティ プロファイル, （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。 セキュアな会議の場合は、電話スクリーンの[会議（Conference）]の右側に、（暗号化された）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） 会議コールのセキュリティ レベルは、特定の連携動作、制約事項、および制限事項の影響を受けます。 このような連携動作は、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異なります。 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, （23 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、次のようなプロセスになります。

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、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、セキュア 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、シェアドライン、Cisco エクステンション モビリティ、回線をまたいで参加（Join Across Lines）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 *5*：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 *6*：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<br>非セキュアな会議 |

| 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 |
|---|---|---|---|
| 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<br>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<br>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<br>認証済みレベルのセキュアな会議 |
| 非セキュア | 会議 | 暗号化済みまたは認証済み | セキュアな会議ブリッジのみが利用可能で、使用されている<br>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<br>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ます。<br>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<br>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<br>会議が非セキュアに変更される |

| 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 |
|---|---|---|---|
| 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。コールは拒否されました（Does not meet Security Level, call rejected）」というメッセージを受け取ります。 |
| 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<br>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、使用されます。<br>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 認証の有効化：802.1X 標準を使用して Cisco Unified IP Phone を認証するには、電話機で802.1X標準を有効にする前に、その他のコンポーネントを正しく設定しておく必要があります。
- 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、特定のスイッチ ポートに対してデバイスを 1 つだけ認証することを推奨します。 ただし、一部のスイッチ（Cisco Catalyst スイッチなど）はマルチドメイン認証をサポートしています。 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：マルチドメイン認証をサポートするスイッチを使用する場合、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。 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 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従って行う必要があります。

- 有効：マルチドメイン認証をサポートするスイッチを使用する場合は、ボイス VLAN を引き続き使用できます。
- 無効：スイッチがマルチドメイン認証をサポートしていない場合は、ボイス VLAN を無効にし、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）] メニュー

# 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、割り込みの開始側の電話機でリオーダートーン（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 シリーズは、Cisco EnergyWise をサポートします。 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、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）ポートを使用して投入する必要があります。

EnergyWise は、電話機ごとに有効または無効に設定します。 また、エンタープライズ電話および共通電話の設定で EnergyWise パラメータを設定することもできます。 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、予定の時刻よりも前に電話機を復帰させることができます。 スイッチからの電話機の電源投入の詳細については、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。 Cisco Unified IP テレフォニー ネットワークのセットアップと設定の詳細およびチェックリストについては、『*Cisco Unified Communications Manager System Guide*』の「System Configuration Overview」の章を参照してください。

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

Cisco Unified IP Phone をネットワークに追加する手順の概要については、次の各トピックで説明します。

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

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 の管理ページ
- 一括管理ツール（BAT）
- BAT と Tool for Auto-Registered Phones Support（TAPS）

Cisco Unified Communications Manager での電話機設定の概要については、『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」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 の管理ページでの Cisco Unified IP Phone 7975G、7971G-GE、7970G、7965G、および 7945G のセットアップ

次の手順では、Cisco Unified Communications Manager の管理ページでの、Cisco Unified IP Phone 7975G、7971G-GE、7970G、7965G、および 7945G 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。

a) 電話機のモデル
b) MAC アドレス
c) 電話機の設置場所
d) 電話機のユーザの名前または ID
e) デバイス プール
f) 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
g) 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）
h) 電話機に関連付ける Cisco Unified Communications Manager ユーザ
i) 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
電話機のセットアップのための設定要件のリストを提供します。

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。

『*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。
回線ボタン、短縮ダイヤル ボタン、サービス URL ボタンの番号を変更したり、プライバシー ボタンを追加して、ユーザ 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。

『*Cisco Unified CallManager 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）] ウィンドウの必須フィールドに値を入力して、電話機を追加および設定します。 必須フィールドは、フィールド名の横にアスタリスク（*）を付けて示されています（たとえば、MAC アドレスやデバイス プール）。
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。

『*Cisco Unified CallManager 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。

**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。 必須フィールドは、フィールド名の横にアスタリスク（*）を付けて示されています（たとえば、電話番号やプレゼンス グループ）。
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。

『*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。
ユーザの電話機に表示されるソフトキー機能を追加、削除、または順序変更して、機能の利用ニーズに対応します。

『*Cisco Unified CallManager 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**　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（任意）。 短縮ダイヤル ボタンと番号を追加します。

（注）　ユーザは、Cisco Unified Communications Manager ユーザ オプション Web ページを使用することで、短縮ダイヤルの設定値を電話機上で変更できます。

『*Cisco Unified CallManager Administration Guide*』の「Cisco Unified IP Phone 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 Web ページで、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 Unified CallManager 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。
『*Cisco Unified CallManager Administration Guide*』の「Cisco Unified IP Phone Configuration」の章を参照してください。

**ステップ 9**　必須フィールドを設定して、ユーザ情報を追加します。 必須フィールドは、フィールド名の横にアスタリスク（*）を付けて示されています（たとえば、ユーザ ID や姓）。

（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 CallManager 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。

（注）　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。
『*Cisco Unified Communications Manager Administration Guide*』で以下を参照してください。

- 「End User Configuration」の章

- 「User Group Configuration」の章

**ステップ 11** ユーザを電話機に割り当てます。 ユーザが電話機を制御して、コールの転送、短縮ダイヤル番号やサービスの追加を行えるようにします。

（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。

『*Cisco Unified CallManager 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。 電話機は希望の場所に設置できます。または、設置の実行に必要な情報を電話機のユーザに提供できます。 http://www.cisco.com/en/US/products/hw/phones/ps379/prod_installation_guides_list.html で入手できる『Cisco Unified IP Phone Installation Guide』では、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を接続する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 で対象の電話機の Readme ファイルを参照してください。

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

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

自動登録を使用した場合は、電話機をユーザに関連付ける、ボタン テーブルを変更する、電話番号を割り当てるなど、電話機の特定の設定情報をアップデートします。

## Cisco Unified IP Phone 7975G、7971G-GE、7970G、7965G、および 7945G の設置

次の手順では、Cisco Unified IP Phone 7975G、7971G-GE、7970G、7965G、および 7945G を設置する作業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。

a) Power over Ethernet（PoE）

b) 外部電源
電話機に電力を供給する方法を決定する。

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する。

Cisco Unified IP Phone の設置およびフットスタンド調節を参照してください。

**ステップ 3** （任意）Cisco Unified IP Phone Expansion Module を追加します。
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。 14（Cisco Unified IP Phone Expansion Module 7914）または 24（Cisco Unified IP Phone Expansion Modules 7915 または 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 の機能を拡張します。

（注） Cisco Unified IP Phone 7971G-GE および 7970G は、Cisco Unified IP Phone Expansion Module 7915 および 7916 をサポートしません。

（注） Cisco Unified IP Phone 7945G は、拡張モジュールをサポートしません。

（注） Cisco Unified IP Phone 7975G では最大 56 の鍵を設定でき、Cisco Unified IP Phone 7965G では最大 54 の鍵を設定できます。

Cisco Unified IP Phone Expansion Moduleを参照してください。

**ステップ 4** 電話機の起動プロセスをモニタします。 電話機が適切に設定されていることを確認する。
電話機の起動プロセスを参照してください。

**ステップ 5** IPv4 ネットワーク用の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 アドレスをセットアップできます。
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、次の設定を行います。

- 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 で割り当てられる TFTP サーバを使用する代わりに、代替 TFTP サーバを割り当てる必要がある場合は、ネットワーク管理者に相談してください。
- 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ローカルの電話機で設定する必要があります。そのためには、[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv4 設定（IPv4 Configuration）] を選択します。

DHCP を無効にして、IP アドレスを手動で設定する場合：

a) [DHCP を使う（DHCP Enabled）] を [いいえ（No）] に設定します。
b) 電話機のスタティック 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 ルータの IP アドレスを入力します。
e) [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 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。 IPv4 アドレスのみ、IPv6 アドレスのみ、または IPv4 アドレスと IPv6 アドレスの両方をサポートするように、Cisco Unified Communications Manager を設定できます。

ネットワーク設定およびネットワークの設定メニューを参照してください。

**ステップ 6** IPv6 ネットワーク用の電話上でネットワーク設定値を設定する場合、DHCPv6 を使用するか、手動で IP アドレスを入力して、電話機の IP アドレスをセットアップできます。
DHCPv6 を使用する場合：DHCPv6 を有効にして DHCPv6 サーバで IP アドレスを Cisco Unified IP Phone に自動的に割り当て、電話機に TFTP サーバを指定できるようにするには、次の手順を実行します。

- [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。
- [DHCPv6 有効（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（IPv6 TFTP Server 1）] の IP アドレスを入力します。
  （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）] > [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場合：

a) [DHCPv6 有効（DHCPv6 Enabled）] を [いいえ（No）] に設定します。
b) 電話機のスタティック IP アドレスを入力します。
c) IPv6 プレフィッ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（IPv6 TFTP Server 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 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。 IPv4 アドレスのみ、IPv6 アドレスのみ、または IPv4 アドレスと IPv6 アドレスの両方をサポートするように、Cisco Unified Communications Manager を設定できます。

ネットワーク設定およびネットワークの設定メニューを参照してください。

**ステップ 7** 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。
Cisco Unified IP Phone のセキュリティを参照してください。

**ステップ 8** 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。
電話機のユーザ ガイドを参照してください。

**ステップ 9** 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。