Cisco IP 電話 8800 シリーズ アドミニストレーション ガイド（Cisco Unified Communications Manager 用）

初版：2015 年 7 月 13 日

最終更新：2023 年 6 月 16 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。 これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。 この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。 これらの制限は、住宅地で使用したときに、有害な干渉を防止する適切な保護を規定したものです。 この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。干渉しているかどうかは、装置の電源のオン/オフによって判断できます。

- 受信アンテナの向きを変えるか、場所を移動します。
- 機器と受信装置の距離を広げる。
- 受信装置が接続されている回路とは別の回路のコンセントに機器を接続する。
- 販売業者またはラジオやテレビに詳しい技術者に連絡します。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

定型　このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。　定型　マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この文書の印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理対象外と見なされます。 最新版については、現在のオンライン バージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。 各オフィスの住所と電話番号は、当社の Web サイトwww.cisco.com/jp/go/offices をご覧ください。

目 次

はじめに

概要

『*Cisco IP* 電話 *8800* シリーズ アドミニストレーション ガイド（*Cisco Unified Communications Manager* 用）』では、VoIP ネットワーク上の電話機の理解、設置、設定、管理、およびトラブルシューティングに必要な情報について説明します。

IP テレフォニー ネットワークは複雑なため、このマニュアルでは、Cisco Unified Communications Manager またはその他のネットワーク デバイスで実行する必要がある手順のすべてについては説明していません。

対象読者

このマニュアルは、ネットワーク エンジニア、システム管理者、および電気通信技術者を対象としており、Cisco IP 電話 をセットアップするために必要な手順について説明しています。 このマニュアルで説明されている作業には、電話機のユーザを対象にしていないネットワーク設定値の設定が含まれます。 このマニュアルの作業を実行するには、Cisco Unified Communications Manager に精通していることが必要です。

ガイドの表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で表記されています。
[]	角カッコの中の要素は、省略可能です。
{x | y | z}	必ずどれか1つを選択しなければならない必須キーワードは、波カッコで囲み、区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角括弧で囲み、縦棒で区切っています。
文字列	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符すると、その引用符も含めて string とみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示してい
`input` フォント	ユーザが入力しなければならない情報は、**`input`** フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の *screen* フォントで示しています
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組わせは、Ctrl キーを押しながら D キーを押すことを意味します。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。

注目 安全上の重要な注意事項

「危険」の意味です。 人身事故を予防するための注意事項が記述されています。 装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。 各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。 ステートメント 1071

これらの注意事項を保管しておいてください。

関連資料

関連情報を入手するには、以下のセクションを参照してください。

Cisco IP 電話 8800 シリーズのマニュアル

Cisco IP Phone 8800 シリーズの製品サポートページで、使用する言語、電話機のモデル、およびコール制御システムに固有のドキュメントを検索してください。

導入ガイドは、次の URL で参照できます。

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Cisco Unified Communications Managerのマニュアル

製品のサポートページで『*Cisco Unified Communications Manager Documentation Guide*』およびお使いの Cisco Unified Communications Manager リリースに特化したその他の文書を参照してください。

Cisco Business Edition 6000 マニュアル

『*Cisco Business Edition 6000* ドキュメンテーション ガイド』およびお使いの Cisco Business Edition 6000 リリースに対応した資料を参照してください。次の URL から入手できます。

https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html

マニュアル、サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。Cisco の新規および改訂版の技術マニュアルの一覧も示されています。

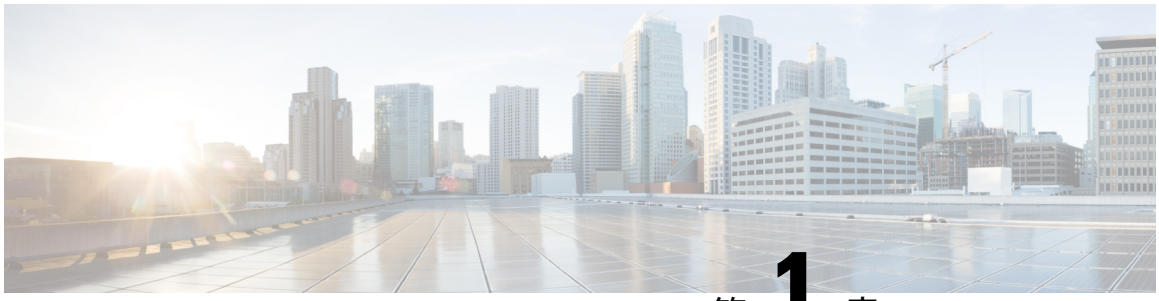
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。Cisco は現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国の法律の対象となります。 Cisco の暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。 輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。 本製品を使用するにあたっては、関係法令の順守に同意したものと見なされます。 米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、https://www.bis.doc.gov/policiesandregulations/ear/index.htm をご覧ください。



第 1 章

新規および変更情報

ファームウェア リリース 14.2(1) の新規および変更情報

次の情報は、ファームウェアリリース 14.2(1) の新規または変更された情報です。

機能	新機能および変更情報
SRST での SIP OAuth のサポート	電話ネットワークのセキュリティ強化機能 （95 ページ）
シスコ ヘッドセット 730 USB アダプタを使用したエクステンションモビリティのログインの簡略化	電話機能 （136 ページ）
Cisco ヘッドセット 500 シリーズの Bluetooth ミュート同期	電話機能 （136 ページ）

機能	新機能および変更情報
Cisco ヘッドセット 500 シリーズの新しい設定: ドックイベントと常時オンモード	電話機能 （136 ページ）

ファームウェアリリース 14.1(1) の新規および変更情報

次の情報は、ファームウェアリリース 14.1(1) の新規または変更された情報です。

機能	新機能および変更情報
プロキシ TFTP サポート用の SIP OAuth	電話ネットワークのセキュリティ強化機能 （95 ページ）
改善されたハントグループのコールアラート	電話機能 （136 ページ）
拡張回線モードで設定可能な電話番号表示	プロダクト固有の設定
設定可能な遅延 PLAR	電話機能 （136 ページ）
Cisco ヘッドセットを使用したエクステンションモビリティのログインに対する MRA サポート	電話機能 （136 ページ）
移行読込のない電話機の移行	マルチプラットフォーム フォンへの電話機の直接移行 （222 ページ）

ファームウェアリース14.0(1) の新規および変更情報

表 *1:* 新規および変更情報

機能	新機能および変更情報
コール パーク モニタリングの機能拡張	プロダクト固有の設定 （161 ページ）
SIP OAuth の機能拡張	電話ネットワークのセキュリティ強化機能 （95 ページ）
ユーザ インターフェイスの強化	Survivable Remote Site Telephony （84 ページ） 電話機能 （136 ページ）
MRA の OAuth の機能拡張	Expressway 経由でのモバイルおよび Remote Access （203 ページ）

ファームウェア リリース 14.0 では、電話機は DTLS 1.2 をサポートしています。DTLS 1.2 には、Cisco Adaptive Security Appliance (ASA) リリース 9.10 以降が必要です。ASA の VPN 接続用に DTLS の最低バージョンを構成します。詳細については、*ASDM* ブック *3*：*Cisco ASA* シリーズ *VPN ASDM 7.12* コンフィギュレーション ガイド (https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html) をご覧ください。

ファームウェアリース 12.8(1) の新規および変更情報

以下の情報は、ファームウェアリリース 12.8 (1) に対して新規または変更事項です。

機能	新しいまたは変更されたコンテンツ
電話データの移行	ユーザの電話モデルを変更 （72 ページ）
ヘッドセット更新の機能拡張	デバイス情報 （271 ページ）
シスコヘッドセットを使用したエクステンションモビリティのログインの簡略化	電話機能 （136 ページ）
機能管理の変更	プロダクト固有の設定 （161 ページ）、新しいフィールドは、**音声アラートを下げ**、**コールをスパムとしてマークします。**
一般的な変更	Wi-fi と PC ポートを明確にするには、次のようにします。 • セットアップ メニューからの電話の設定 （52 ページ） • 電話機でのワイヤレス LAN の有効化 （55 ページ）
Web アクセスのフィールドに関する情報を追加	プロダクト固有の設定 （161 ページ）
サポートされていない機能の削除	電話機能 （136 ページ）

ファームウェア リリース 12.7(1) の新規および変更情報

表 *2*：ファームウェア リリース *12.7 (1)* に合わせた *Cisco IP* 電話 *8800* ユーザ ガイドの改訂

改訂	更新されたセクション
キー拡張モジュールの壁紙のためにアップデートされました。	カスタム背景イメージ （129 ページ）

改訂	更新されたセクション
シスコ ヘッドセット 730 のサポート向け更新	デバイス情報 （271 ページ）
シスコヘッドセット500シリーズファームウェアリリース 2.0 が更新されました。	デバイス情報 （271 ページ） Cisco Unified Communications Managerの旧バージョンでのヘッドセット管理 （237 ページ）
着信ハントグループのコール用に更新されます。	電話機能 （136 ページ）
E フックの設定情報が削除されました。	プロダクト固有の設定 （161 ページ）

ファームウェア リリース 12.1(1) の新規および変更情報

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

表 *3 :* ファームウェアリース *12.6(1)* に関する *Cisco IP* 電話 *8800* アドミニストレーションガイドのリビジョン

改訂	更新されたセクション
セッションラインモードでのプライマリ回線への復帰のサポート。	プロダクト固有の設定 （161 ページ） セッション回線モードの環境 （187 ページ）

ファームウェア リリース 12.5 (1) SR3 の 更新情報

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

表 *4 :* ファームウェア リリース *12.5 (1) SR3* に関する *Cisco IP* 電話 *8800* アドミニストレーション ガイドのリビジョン

改訂	更新されたセクション
アクティベーション コードオンボーディングとモバイルおよびRemote Access へのサポート	アクティベーション コードオンボーディングとモバイルおよびリモート アクセス （47ページ）
Cisco Unified Communications Manager の問題レポートツール使用のサポート。	Cisco Unified Communications Manager から電話機の問題レポートを作成する （309 ページ）
新しいトピック	コンピュータとの有線ネットワーク接続の共有 （52 ページ）

改訂	更新されたセクション
新しいトピック	ビデオフォンのカメラの保護 （41 ページ）

ファームウェア リリース 12.5（1）SR1の新機能

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

表 *5*：ファームウェア リリース *12.5*（*1*）*SR1* に合わせた *Cisco IP* 電話 *8800* アドミニストレーション ガイドの改訂

改訂	更新されたセクション
楕円曲線サポートのサポート	サポート対象のセキュリティ機能 （96 ページ）
ロールオーバー回線を使用する拡張回線モードの通話履歴の機能強化のサポート	拡張回線モードで使用可能な機能 （231 ページ）
Cisco Unified Communications Manager Express でのウィスパーページングのサポート	Cisco Unified Communications Manager Express の連携 （24 ページ）
中国語のサポート	言語の制限 （326 ページ）
アクティベーションコードによるオンボーディング	オンプレミス電話用のアクティベーションコードのオンボーディング （46 ページ）
メディアパスと対話型接続確立（ICE）のサポート	メディア ルーティングを向上させる Interactive Connectivity Establishment（ICE） （205 ページ）
TLS 暗号の無効化のサポート	プロダクト固有の設定 （161 ページ）
ヘッドセットでオーディオ パスが維持できるようにハンドセットを無効にする	プロダクト固有の設定 （161 ページ）
ヘッドセットパラメータのリモート設定のサポート	Cisco Unified Communications Managerの旧バージョンでのヘッドセット管理 （237 ページ）

ファームウェアリリース 12.1(1)SR1 の新着情報

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

表 *6 :* ファームウェア リリース *12.1(1)SR1* に関する *Cisco IP* 電話 *8800* アドミニストレーション ガイドのリビジョン

改訂	更新されたセクション
桁間タイマー T.302 拡張のための一括ダイヤル。	プロダクト固有の設定 （161 ページ）

ファームウェア リリース 12.1（1）の新機能

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

表 *7 :* ファームウェア リリース *12.1(1)* に関する *Cisco IP* 電話 *8800* アドミニストレーション ガイドのリビジョン

改訂	更新されたセクション
Expressway 経由モバイルおよび Remote Access、拡張回線モードがサポートされるようになりました。	Expressway 経由でのモバイルおよび Remote Access で利用可能な電話機能 （205 ページ）
	Expressway 経由でのモバイルおよび Remote Access （203 ページ）
	拡張回線モードで使用可能な機能 （231 ページ）
Web サーバへのアクセス用に TLS 1.2 を有効または無効にする機能がサポート対象になりました。	プロダクト固有の設定 （161 ページ）
G722.2 AMR-WB オーディオコーデックがサポートされました。	電話機の概要 （31 ページ）
	コール統計のフィールド （266 ページ）

ファームウェア リリース 12.0（1）の新機能

電話機能 （136 ページ）に記載のすべての機能が追加されました。

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

表 *8 :* ファームウェア リリース *12.0(1)* に関する *Cisco IP* 電話 *8800* アドミニストレーション ガイドのリビジョン

改訂	更新されたセクション
コール パーク、コール パークの回線ステータス、グループ ピックアップ、および拡張回線モードでのハント グループのサポートについて更新されています。	拡張回線モードで使用可能な機能 （231 ページ）

ファームウェア リリース 11.7（1）の新機能

ファームウェア リリース 11.7(1) に管理更新は不要でした。

ファームウェア リリース 11.5（1）SR1 の新機能

電話機能 （136 ページ）に記載のすべての機能が追加されました。

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

表 *9 :* ファームウェア リリース *11.5(1)SR1* に合わせた *Cisco IP* 電話 *8800* アドミニストレーション ガイドの改訂

改訂	更新されたセクション
Cisco IP 電話 8865NR サポート用の更新	• 電話機の所要電力 （16 ページ） • ネットワーク プロトコル （18 ページ） • 電話機の概要 （31 ページ） • ボタンとハードウェア （38 ページ）
拡張回線モードでの記録およびモニタのサポート用の更新	拡張回線モードで使用可能な機能 （231 ページ）
WLAN スキャン リスト サポート用の更新	電話機でのワイヤレス LAN の有効化 （55 ページ）
	電話機からのワイヤレス LAN のセットアップ （57 ページ）
	ネットワークの設定 （63 ページ）
MLPP でのサイレント サポート用の更新	サイレントの設定 （196 ページ）
設定可能な呼出音サポート用の更新	プロダクト固有の設定 （161 ページ）

改訂	更新されたセクション
セキュリティ強化	電話ネットワークのセキュリティ強化機能（95 ページ）
一般的な変更	Cisco IP 電話の Web ページ（270 ページ）に対する更新 Cisco Unified Communications Manager での電話機機能設定の新しい表示 電話機の機能設定（159 ページ）

ファームウェア リリース 11.5（1）の新機能

表 *10 :* ファームウェア リリース *11.5(1)* に合わせた *Cisco IP* 電話 *8800* アドミニストレーション ガイドの改訂

改訂	更新されたセクション
拡張回線モードがサポートされます。	追加回線キーのセットアップ（230 ページ） 拡張回線モードで使用可能な機能（231 ページ）
新しいディスプレイ用に、サイレント（DND）が更新されました。	サイレントの設定（196 ページ）
Opus コーデックがサポートされます。	電話機の概要（31 ページ）
FIPS モードが追加されました。	FIPS モードの有効化（104 ページ）
WLAN 設定が更新されました。	電話機からのワイヤレス LAN のセットアップ（57 ページ）
Cisco IP 電話 8861 および 8865 用の WLAN プロファイルがサポートされます。	Cisco Unified Communications Manager を使用した Wi-Fi プロファイルの設定（60 ページ）
	Cisco Unified Communications Manager を使用した Wi-Fi グループの設定（62 ページ）
WLAN認証の試行の設定がサポートされます。	WLAN 認証試行の回数の設定（58 ページ）
WLANプロンプトモードの有効化がサポートされます。	WLAN プロンプト モードの有効化（59 ページ）
ダイヤル トーンのカスタマイズがサポートされます。	ダイヤルトーンのカスタマイズ（133ページ）

改訂	更新されたセクション
[ネットワーク情報（Network Info）] 画面の表示がサポートされます。	[ネットワーク情報（Network Information）] 画面の表示 （260 ページ）

ファームウェア リリース 11.0 の新機能

電話機能 （136 ページ）に記載のすべての機能が追加されました。

すべての Cisco Unified Communications Manager リリースをサポートするよう Cisco Unified Communications Manager のマニュアルに対するすべての参照が更新されています。

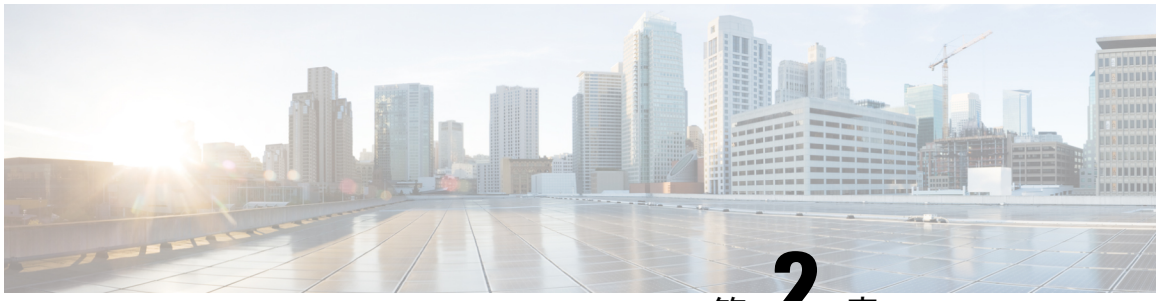
表 *11 : Cisco IP* 電話 *8800* アドミニストレーション ガイドのファームウェア リリース *11.0* に関するリビジョン

改訂	更新されたセクション
明確化の更新、および不具合に対処した更新	• VPN の設定 （229 ページ） • ネットワークの設定 （63 ページ） • スイッチおよび PC ポート用の Energy Efficient Ethernet のセットアップ （201 ページ） • ビデオ送信解像度のセットアップ （235 ページ） • Enhanced Survivable Remote Site Telephony （88 ページ）
セクション電話機デバッグ オプション サポートの改善に関する更新	• Cisco Unified Communications Manager からのデバッグ情報の制御 （314 ページ）.
EAP-TLS + SCEP、PEAP-GTC、および X.509 デジタル証明書サポートの改善に関する更新	• WLAN セキュリティ （107 ページ）. • 認証モードのセットアップ （111 ページ） • ワイヤレス セキュリティ クレデンシャル （111 ページ）
問題報告ツール（PRT）サポートの改善に関する更新	• 問題レポート ツール （208 ページ）. • カスタマー サポート アップロード URL の設定 （209 ページ）.
アプリケーション ダイヤル ルールサポートに関する情報を追加	• アプリケーション ダイヤル ルール （88 ページ）

改訂	更新されたセクション
回線テキストラベルに関する情報を追加	• 回線のラベルの設定 （211 ページ）.

第 I 部

Cisco IP 電話について



第 2 章

技術的な詳細

物理環境および動作環境に関する仕様

次の表に、Cisco IP 電話 8800 シリーズの物理仕様および動作環境仕様を示します。

表 *12*：物理仕様および動作環境仕様

仕様	値または範囲
動作温度	0 ～ 40 °C（32 ～ 104 °F）
動作時の相対湿度	動作時：10 ～ 90 %（結露なし） 非動作時：10 ～ 95%（結露なし）
保管温度	–10 ～ 60 °C（14 ～ 140 °F）

仕様	値または範囲
高さ(T)：	229.1 mm（9.02 インチ）
幅	257.34 mm（10.13 インチ）
奥行	40 mm（1.57 インチ）
重量	2.62 ポンド（1.19 kg）
電源	AC アダプタ使用時：100 ～ 240 VAC、50 ～ 60 Hz、0.5 A ネットワーク ケーブル経由のインライン電源使用時：48 VDC、0.2
ケーブル	10 Mbps ケーブルの場合はカテゴリ 3/5/5e/6 の 4 ペア 100 Mbps ケーブルの場合はカテゴリ 5/5e/6 の 4 ペア 1000-Mbps ケーブルの場合はカテゴリ 5e/6 を 4 ペア （注） ケーブルは、合計 8 本のコンダクタに対して 4 ペアのワ されています。
距離要件	イーサネット仕様でサポートされているとおり、各 Cisco IP 電話 と のケーブル長は最大 330 フィート（100 m）とします。

ケーブル仕様

次の情報は、ケーブル仕様の一覧です。

- ハンドセットおよびヘッドセット接続用の RJ-9 ジャック（4 コンダクタ）。
- LAN 10/100/1000BaseT 接続（電話機の 10/100/1000 ネットワーク ポート）用の RJ-45 ジャック
- 2 番目の 10/100/1000BaseT 準拠接続用の RJ-45 ジャック（電話機の 10/100/1000 コンピュータ ポート）
- スピーカー接続の場合は 3.5 mm ジャック（Cisco IP 電話 8861 のみ）
- 48 ボルト電源コネクタ
- USB ポート/コネクタ：Cisco IP 電話 8851 用 USB ポート X 1、Cisco IP 電話 8861 用 USB ポート X 2
- Cisco IP 電話 8851 および 8861 の USB コネクタと見なされる 3 つのキー拡張モジュール コネクタ

ネットワーク ポートとコンピュータ ポートのピン割り当て

ネットワーク ポートとコンピュータ（アクセス）ポートはいずれもネットワーク接続に使用されますが、それぞれ異なる目的で使用され、ポートのピン割り当ても異なっています。

- ネットワーク ポートは、Cisco IP 電話上の 10/100/1000 SW ポートです。
- コンピュータ（アクセス）ポートは、Cisco IP 電話上の 10/100/1000 PC ポートです。

ネットワーク ポート コネクタ

次の表に、ネットワーク ポート コネクタのピン割り当てを示します。

表 *13*：ネットワーク ポート コネクタのピン割り当て

ピン番号	機能
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
（注） BI は双方向を表し、DA、DB、DC、DD はそれぞれデータ A、データ B、データ C、データ D を表します。	

コンピュータ ポート コネクタ

次の表に、コンピュータ ポート コネクタのピン割り当てを示します。

表 *14*：コンピュータ（アクセス）ポート コネクタのピン割り当て

ピン番号	機能
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+

ピン番号	機能
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
（注） BI は双方向を表し、DA、DB、DC、DD はそれぞれデータ A、データ B、データ C、データ D を表します。	

電話機の所要電力

Cisco IP 電話は、外部電源または Power over Ethernet（PoE）で電力を供給できます。外部電源は個別の電源装置によって提供されます。スイッチは電話機のイーサネット ケーブル経由で PoE を供給できます。

Cisco IP 電話 8861 および 8865 は PoE Class 4 デバイスであり、追加機能をサポートするには Class 4 機能を備えたスイッチまたはライン カードが必要です。

電話機の電力要件の詳細については、その電話機のデータ シートを参照してください。

外部電源を使用する電話機を設置した場合、電話機にイーサネット ケーブルを接続する前に、電源装置を接続してください。外部電源から電力が供給されている電話機を取り外す場合は、電源装置を取り外す前に、イーサネット ケーブルを電話機から取り外してください。

表 *15 : Cisco IP* 電話の電源に関するガイドライン

電源の種類	ガイドライン
外部電源：CP-PWR-CUBE-4 = 外部電源を通じて電力を供給	Cisco IP 電話シリーズでは、CP-PWR-CUBE-4 電源を使用します。
PoE 電源：イーサネット ケーブルを介して電話機に接続されているスイッチを通じて電力を供給	Cisco IP 電話s 8851、8851NR、8861、8865、および 8865NR はアクセサリ用 PoE をサポートします。詳細については、電話機のデータ シートを参照い。 スイッチには、電話機の無停止動作のためのバックアップ電源が必要で スイッチ上で実行されている CatOS または IOS のバージョンが、目的と配置をサポートしていることを確認します。オペレーティング システムンに関する情報については、スイッチのマニュアルを参照してください。
Universal Power over Ethernet（UPoE）	Cisco IP 電話 8865 および 8865NR は、UPoE をサポートしています。

次の表にあるドキュメントは、次のトピックに関する詳細情報を提供します。

- Cisco IP 電話と連携する Cisco スイッチ
- 双方向電力ネゴシエーションをサポートしている Cisco IOS リリース
- 電力に関するその他の要件および制限事項

表 *16* : 追加情報

ドキュメントのトピック	URL
PoE ソリューション	http://www.cisco.com/c/en/us/solutions/enterprise-networ power-over-ethernet-solutions/index.html
UPoE	http://www.cisco.com/c/en/us/solutions/enterprise-networ
Cisco Catalyst スイッチ	http://www.cisco.com/c/en/us/products/switches/index.htm
サービス統合型ルータ	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS ソフトウェア	http://www.cisco.com/c/en/us/products/ios-nx-os-software

停電

電話機を経由して緊急サービスにアクセスするには、その電話機が電力を受信する必要があります。 停電が発生した場合、電源が復旧するまでは、電話サービスおよび緊急コール サービス ダイヤルが機能しません。 電源の異常および障害が発生した場合は、装置をリセットまたは再設定してから、電話サービスおよび緊急コール サービス ダイヤルを利用する必要があります。

電力削減

省電力モードまたは EnergyWise（Power Save Plus）モードを使用して、Cisco IP 電話が消費する電力を削減できます。

省電力（Power Save）

Power Save モードでは、電話機が使用されていないときにはスクリーンのバックライトが消灯します。 電話機は、ユーザがハンドセットを持ち上げるか、任意のボタンを押さない限り、スケジュールされた期間中、Power Save モードのままになります。

Power Save Plus（EnergyWise）

Cisco IP 電話は Cisco EnergyWise（Power Save Plus）モードをサポートします。 ネットワークに EnergyWise（EW）コントローラが含まれている場合（たとえば、Cisco スイッチで EnergyWise 機能が有効になっている場合）、これらの電話機をスケジュールに基づいてスリープ状態（電源オフ）およびウェイク状態（電源オン）になるように設定して、電力消費をさらに抑えることができます。

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、他のパラメータとともに、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。

LLDP での電力ネゴシエーション

電話機とスイッチは、電話機が消費する電力のネゴシエーションを行います。 Cisco IP 電話は複数の電力設定で動作し、これにより、使用する電力が少ないときの電力消費を削減します。

電話機のリブートの後、スイッチは電力ネゴシエーションの 1 つのプロトコル（CDP または LLDP）にロックされます。 スイッチは、電話機が送信した最初のプロトコル（電力の [しきい値限度値 [TLV]（Threshold Limit Value [TLV]）] を含む）にロックされます。 システム管理者が電話機でそのプロトコルを無効にすると、スイッチがもう一方のプロトコルでの電力要求に応答しないため、電話機はアクセサリの電源を投入できなくなります。

電力ネゴシエーションをサポートするスイッチに接続する場合は、常に電力ネゴシエーションを有効（デフォルト）にすることをお勧めします。

電力ネゴシエーションを無効にすると、スイッチは電話機の電源を切断する場合があります。スイッチが電力ネゴシエーションをサポートしていない場合は、アクセサリの電源を PoE+ で投入する前に、電力ネゴシエーション機能を無効にしてください。電力ネゴシエーション機能を無効にすると、電話機は IEEE 802.3af-2003 規格で許容される最大値まで、アクセサリに電力を供給できます。

（注）
- CDP と電力ネゴシエーションを無効にすると、電話機は最大 15.4 W までアクセサリに電力を供給できます。

ネットワーク プロトコル

Cisco IP 電話 8800 シリーズは、音声通信に必要な業界標準ネットワーク プロトコルおよびシスコ ネットワーク プロトコルを複数サポートしています。次の表に、電話でサポート対象ネットワーク プロトコルの概要を示します。

表 *17 : Cisco IP* 電話 *8800* シリーズでサポート対象ネットワーク プロトコル

ネットワーク プロトコル	目的	使用上の注意
Bluetooth	Bluetooth は、短距離におけるデバイスの通信方法を指定する Wireless Personal Area Network（WPAN）プロトコルです。	Cisco IP 電話s 8845、8865、および 8851 は Bluetooth 4.1 をサポートしています。 Cisco IP 電話 8861 は Bluetooth 4.0 をサポートしています。 Cisco IP 電話 8811、8841、8851NR、および 8865NR は Bluetooth をサポートしていません。
Bootstrap Protocol (BootP)	BootP は、特定の起動情報（IP アドレスなど）を Cisco IP 電話 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。	—
Cisco Audio Session Tunnel（CAST）	CAST プロトコルでは、電話機や関連アプリケーションが、シグナリング コンポーネントへの変更を必要とせずにリモート IP 電話と通信できます。	Cisco IP 電話は CAST を CUVA と Cisco Unified Communications Manager の間のインターフェイスとして使用し、Cisco IP 電話 を SIP プロキシとして使用します。
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することができます。	Cisco IP 電話では、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するシスコ独自のプロトコルです。この階層はピアデバイスからネイバーデバイスにファームウェア ファイルを配布するために使用されます。	CPPDP は、ピア ファームウェア共有機能で使用されます。

ネットワーク プロトコル	目的	使用上の注意
Dynamic Host Configuration Protocol（DHCP）	DHCPは、IPアドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。 DHCP を使用すると、IP 電話機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。 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。この方式では、TFTPサーバの IP アドレスをオプション値として設定しています。詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。 （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。
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 IP 電話では、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。
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 IP 電話は、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。 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し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。認証に成功すると、通常のトラフィックはポートを通過できるようになります。	Cisco IP 電話では、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。 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。

ネットワーク プロトコル	目的	使用上の注意
IEEE 802.11n/802.11ac	IEEE 802.11 標準は、ワイヤレス ローカル エリア ネットワーク（WLAN）におけるデバイスの通信方法を指定します。 802.11n は 2.4 GHz 帯域と 5 GHz 帯域で動作し、802.11ac は 5 GHz 帯域で動作します。	802.11 インターフェイスは、イーサネットのケーブル接続が利用できないか望ましくない場合の展開オプションです。 Cisco IP 電話 8861 および 8865 のみ WLAN をサポートします。
インターネットプロトコル（IP）	IPは、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。	IP を使用して通信するには、ネットワーク デバイスに対して、IP アドレス、サブネット、およびゲートウェイが割り当てられている必要があります。 IP アドレス、サブネット、およびゲートウェイの識別情報は、Dynamic Host Configuration Protocol（DHCP）を通じて Cisco IP Phone を使用する場合は、自動的に割り当てられます。DHCP を使用しない場合は、個々の電話機がある場所で、これらのプロパティを手動で割り当てる必要があります。 Cisco IP 電話は、IPv6 アドレスをサポートしています。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。
リンク層検出プロトコル（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 IP 電話は、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LLDP標準の拡張です。	Cisco 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
Real-Time Transport Protocol（RTP）	RTP は、インタラクティブな音声のようなリアルタイム 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 IP 電話は、RTP プロトコルを使用して、他の電話機やゲートウェイとリアルタイム音声トラフィックを送受信します。
Real-Time Control Protocol (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、デフォルトでは有効になっています。

ネットワーク プロトコル	目的	使用上の注意
Session Description Protocol （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がサポートする 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。
Session Initiation Protocol （SIP）	SIP は、IP を介したマルチメディア会議のためのインターネット技術特別調査委員会（IETF）標準です。SIP は、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通話情報を伝送することが可能になります。セッション管理は、エンドツーエンド コールの属性を制御する機能です。 Cisco IP 電話は、電話機が IPv6 のみ、IPv4 のみ、または IPv4 と IPv6 の両方で動作している場合に SIP プロトコルをサポートします。
Transmission Control Protocol（TCP）	TCP は、接続型の転送プロトコルです。	Cisco IP 電話では、Cisco Unified Communications Manager への接続、および XML サービスへのアクセスに TCP を使用します。
Transport Layer Security（TLS）	TLS は、通信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 IP 電話では、Cisco Unified Communications Manager へのセキュアな登録で TLS プロトコルが使用されます。
Trivial File Transfer Protocol（TFTP）	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 Cisco IP Phone で TFTP を使用すると、電話機タイプに固有の設定ファイルを取得できます。	TFTP は DHCP サーバが自動的に識別する TFTP サーバがネットワーク内に必要です。DHCP サーバで指定されたもの以外の TFTP サーバを電話機で使用する場合は、電話機の [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、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。
User Datagram Protocol（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。	UDP は RTP ストリームにのみ使用されます。電話機の SIP シグナリングは UDP をサポートしていません。

LLDP-MED サポートの詳細については、LLDP-MED および『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

関連トピック

802.1X 認証 （125 ページ）
ネットワークの設定
電話機の起動確認 （71 ページ）
VLAN の連携 （23 ページ）
Cisco Unified Communications Manager の連携 （24 ページ）
Cisco Unified Communications Manager Express の連携 （24 ページ）
音声ポートとビデオ ポートの範囲設定 （215 ページ）
Cisco Unified Communications Managerのマニュアル （xvii ページ）

VLAN の連携

Cisco IP 電話は内蔵イーサネット スイッチを備えているため、電話機や、電話機の背面にあるコンピュータ（アクセス）ポートおよびネットワーク ポートにパケットを転送できます。

コンピュータ（アクセス）ポートにコンピュータを接続した場合、コンピュータと電話機は、スイッチへの同じ物理リンクとスイッチ上の同じポートを共有します。 このように物理リンクが共有されるため、ネットワークのVLAN設定について、次のような考慮事項が存在します。

- 現在の VLAN を IP サブネット ベースで設定することは可能です。 ただし、追加の IP アドレスを取得して、同じポートに接続されている他のデバイスと同じサブネットに電話機を割り当てることはできません。
- VLAN をサポートしている電話機上に存在するデータ トラフィックによって、VoIP トラフィックの品質が低下することがあります。
- ネットワーク セキュリティを確保するために、VLAN 音声トラフィックと VLAN データ トラフィックの分離が必要になることがあります。

これらの問題は、音声トラフィックを別の VLAN 上に分離することで解決できます。 電話機の接続先となるスイッチ ポートには、伝送用に、それぞれ別個の VLAN を設定します。

- IP 電話で送受信される音声トラフィック（Cisco Catalyst 6000 上などの補助 VLAN）
- IP 電話のコンピュータ（アクセス）ポート経由でスイッチに接続されている PC で送受信されるデータ トラフィック（ネイティブ VLAN）

複数の電話機を別々の補助 VLAN に分離すると、音声トラフィックの品質が向上するとともに、各電話機に割り当てる IP アドレスが十分にない既存ネットワークに対しても、多数の電話機を追加できます。

詳細については、Cisco スイッチに添付されているマニュアルを参照してください。 スイッチに関する情報には、次の URL からもアクセスできます。

http://cisco.com/en/US/products/hw/switches/index.html

Cisco Unified Communications Manager の連携

Cisco Unified Communications Manager は、業界標準のオープンなコール処理システムです。Cisco Unified Communications Manager ソフトウェアは、従来の PBX 機能を企業の IP ネットワークに統合して、電話機間のコールを確立および切断します。 Cisco Unified Communications Manager は、電話会議やルート プランなどの機能で必要になるテレフォニー システムのコンポーネント（電話機、アクセス ゲートウェイ、およびリソース）を管理します。 また、Cisco Unified Communications Manager には、次の機能もあります。

- 電話機のファームウェアの提供
- TFTP と HTTP サービスのを使用した証明書信頼リスト（CTL）および Identity Trust List（ITL）
- 電話機の登録
- コールの保存。この機能により、プライマリ Communications Manager と電話機間でシグナリングが消失してもメディア セッションが続行されます。

この章で説明されている電話と連携するための Cisco Unified Communications Manager の設定方法については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

（注） 設定しようとする電話のモデルが、Cisco Unified Communications Manager Administration の [Phone Type] ドロップダウン リストに表示されない場合は、Cisco.com にアクセスして、使用している Cisco Unified Communications Manager の最新のデバイス パッケージをインストールします。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

Cisco Unified Communications Manager Express の連携

電話が Cisco Unified Communications Manager Express（Unified CME）と連携する場合は、電話機をCME モードにする必要があります。

ユーザが会議機能を起動すると、タグにより、電話機はローカルまたはネットワーク ハードウェアのどちらかの会議ブリッジを使用できます。

電話では、次のアクションはサポートされていません。

- [転送（Transfer）] -接続されたコール転送のシナリオでのみサポートされます。
- [会議（Conference）] -接続されたコール転送のシナリオでのみサポートされます。

- 参加 - [会議（Conference）]ボタンまたはフックフラッシュアクセスを使用してサポートされます。
- 保留 - [保留（Hold）] を使用してサポートされます。
- 割り込みおよびマージ - サポートされていません。
- 直接転送 - サポートされていません。
- 選択 - サポートされていません。

ユーザは、異なる回線にわたる会議および転送コールを作成できません。

Unified CME は、ウィスパーページングとも呼ばれるインターコムコールをサポートします。しかし、通話中は電話でページが拒否されます。

CME モードでは、セッション回線モードと拡張回線モードの両方がサポートされています。

ボイス メッセージ システムの連携

Cisco Unified Communications Manager を使用すると、Cisco Unity Connection ボイス メッセージング システムなどのさまざまなボイス メッセージング システムと統合できます。 各種システムと統合できるため、特定のシステムの使用方法に関する情報をユーザに提供する必要があります。

ユーザがボイスメールに転送できるようにするには、*xxxxxダイヤルパターンを設定し、それを[すべてボイスメールに転送]として設定します。 詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

次の情報を、各ユーザに提供してください：

- ボイス メッセージ システム アカウントへのアクセス方法。

  Cisco Unified Communications Manager を使用して、Cisco IP 電話の [Messages] ボタンを設定しておく必要があります。

- ボイス メッセージ システムにアクセスするための初期パスワード。

  すべてのユーザが使用できるボイス メッセージ システムのデフォルト パスワードを設定します。

- ボイス メッセージの受信が電話機でどのように示されるか。

  Cisco Unified Communications Manager を使用して、メッセージ受信インジケータ（MWI）メソッドを設定します。

電話機起動の概要

Cisco IP 電話 を VoIP ネットワークに接続すると、標準の起動プロセスが実行されます。 実際のネットワークの設定によっては、Cisco IP Phone で実行される手順が次の手順の一部のみの場合があります。

1. スイッチからの電力の取得。 電話機が外部電源を使用していない場合、電話機に接続されているイーサネット ケーブル経由でスイッチからのインライン パワーが供給されます。
2. （ワイヤレス LAN 上の Cisco IP 電話 8861 および 8865 のみ）アクセス ポイントのスキャン。 Cisco IP 電話 8861 および 8865 は、RF カバレッジ エリアを無線でスキャンします。 電話機はネットワーク プロファイルを検索し、SSID と認証タイプが一致するアクセス ポイントをスキャンします。 電話機は、ネットワーク プロファイルと一致する最も高い RSSI をアクセス ポイントに関連付けます。
3. （ワイヤレス LAN 上の Cisco IP 電話 8861 および 8865 のみ）アクセス ポイントによる認証。 Cisco IP 電話は、認証プロセスを開始します。 次の表では、認証プロセスについて説明します。

認証タイプ	キー管理オプション	説明
Open	None	すべてのデバイスでアクセス ポイントに認証できます。 セキュリティを高めるため、オプションとして静的 WEP 暗号化を使用できます。
Shared Key	None	電話機は WEP キーを使用してチャレンジ テキストを暗号化します。アクセス ポイントは、チャレンジ テキストの暗号化に使用された WEP キーを検証してから、ネットワーク アクセスを使用可能にする必要があります。
PEAP または EAP-FAST	None	RADIUS サーバがユーザ名とパスワードを認証してから、ネットワーク アクセスが使用可能になります。

4. 保存されている電話イメージのロード。 起動時に、電話機はブートストラップ ローダーを実行して、フラッシュ メモリに保存されている電話機ファームウェアをロードします。 このイメージを使用して、電話機はソフトウェアとハードウェアを初期化します。
5. VLAN の設定。 Cisco IP 電話 を Cisco Catalyst スイッチに接続している場合、スイッチは、スイッチ上に定義されているボイス VLAN を電話機に通知します。 電話機は、Dynamic Host Configuration Protocol（DHCP）要求を使用して IP アドレスの取得を開始するには、VLAN メンバーシップをあらかじめ把握している必要があります。

6. IP アドレスの取得。 Cisco IP 電話で DHCP を使用して IP アドレスを取得する場合、電話機は DHCP サーバにクエリを発行してアドレスを取得します。 ネットワークで DHCP を使用していない場合は、個々の電話機がある場所でスタティック IP アドレスを手動で割り当てる必要があります。

7. CTL ファイルの要求。 TFTP サーバに、CTL ファイルが保管されています。 このファイルには、電話機と Cisco Unified Communications Manager の間の安全な接続を確立するために必要な証明書も含まれています。

   詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

8. ITL ファイルの要求。 電話機は、まず CTL ファイルを要求し、次に ITL ファイルを要求します。 ITL ファイルは電話機が信頼できるエンティティの証明書を含んでいます。 証明書がサーバとのセキュア接続の認証、またはサーバによるデジタル署名の認証に使用されます。 Cisco Unified Communications Manager 8.5 以降は ITL ファイルをサポートします。

9. TFTP サーバへのアクセス。 DHCP サーバは、IP アドレスを割り当てるとともに、Cisco IP 電話 を TFTP サーバに転送します。 電話機の IP アドレスを静的に定義した場合は、電話機がある場所で TFTP サーバを設定する必要があります。設定すると、電話機は TFTP サーバに直接アクセスします。

（注） DHCP で割り当てられる TFTP サーバの代わりに、代替 TFTP サーバを割り当てて使用することもできます。

10. 設定ファイルの要求。 TFTP サーバは、設定ファイルを保持しています。このファイルは、Cisco Unified Communications Manager に接続するためのパラメータに加え、電話機に関するその他の情報を定義しています。

11. Cisco Unified Communications Manager への接続。 設定ファイルは、Cisco IP 電話が Cisco Unified Communications Manager と通信する方法を定義し、電話機にロード ID を提供します。 設定ファイルを TFTP サーバから取得した後、電話機は、リスト上で最も優先順位が高い Cisco Unified Communications Manager との接続を試みます。

    （暗号化または認証された）セキュアなシグナリングのために電話機のセキュリティ プロファイルを設定し、Cisco Unified Communications Manager をセキュア モードに設定している場合、電話機は TLS 接続を実行します。 それ以外の場合は、電話機は非セキュア TCP 接続を実行します。

    電話機がデータベースに手動で追加された場合、Cisco Unified Communications Manager はその電話機を識別します。 電話機がデータベースに手動で追加されたものではなく、自動登録が Cisco Unified Communications Manager で有効化されている場合、その電話機は、Cisco Unified Communications Manager データベースに対してその電話機自体の自動登録を試みます。

（注） CTL クライアントを設定している場合、自動登録は無効になっています。 その場合、電話機を手動で Cisco Unified Communications Manager データベースに追加する必要があります。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

外部デバイス

不要な無線周波数（RF）信号および可聴周波数（AF）信号を遮断する高品質の外部デバイスを使用することをお勧めします。外部デバイスには、ヘッドセット、ケーブル、コネクタが含まれます。

これらのデバイスの品質や、携帯電話および双方向ラジオなど他のデバイスとの間隔によっては、雑音が入ることもあります。 その場合は、次の方法で対処することをお勧めします。

- RF または AF の信号源から外部デバイスを離す。
- RF または AF の信号源から外部デバイスのケーブルの経路を離す。
- 外部デバイス用にシールドされたケーブルを使用するか、高品質なシールドおよびコネクタを備えたケーブルを使用する。
- 外部デバイスのケーブルを短くする。
- 外部デバイスのケーブルに、フェライトまたは同様のデバイスを適用する。

シスコでは、外部デバイス、ケーブル、およびコネクタのパフォーマンスを保証できません。

注意 欧州連合諸国では、EMC Directive [89/336/EC] に完全に準拠した外部スピーカ、マイクロフォン、ヘッドセットだけを使用してください。

USB ポート情報

Cisco IP 電話 8851、8851NR、8861、8865、および 8865NR は、各 USB ポートに接続されたデバイスを 5 台までサポートします。 電話機に接続された各デバイスは、最大デバイス数に含まれます。 たとえば、ご使用の電話機は側面ポートで 5 台の USB デバイス、背面ポートでさらに 5 台の標準 USB デバイスをサポートできます。 多くのサードパーティ製 USB 製品は複数の USB デバイスとしてカウントされます。たとえば、USB ハブとヘッドセットを含むデバイスは、2 台の USB デバイスとしてカウントできます。 詳細については、USB デバイスのマニュアルを参照してください。

（注）
- 通電していないハブはサポートされません。また、電力供給されていても 5 個以上のポートを備えたハブはサポートされません。
- USB ハブを経由して電話機に接続している USB ヘッドセットはサポートされません。

電話機に接続された各キー拡張モジュールは、USBデバイスとしてカウントされます。3台のキー拡張モジュールが電話機に接続されている場合、これらは 3 台の USB デバイスとしてカウントされます。

電話機設定ファイル

電話機設定ファイルは TFTP サーバに保存されており、Cisco Unified Communications Manager に接続するためのパラメータを定義しています。通常、電話機のリセットが必要となるような変更を Cisco Unified Communications Manager に加えると、その変更内容は、電話機設定ファイルに自動的に反映されます。

設定ファイルには、電話機がどのイメージ ロードを実行するかも記述されています。 このイメージロードが電話機にロードされているものと異なる場合、電話機は TFTP サーバにアクセスし、必要なロード ファイルを要求します。

Cisco Unified Communications Manager Administration でセキュリティ関連の設定値を設定すると、電話機のコンフィギュレーション 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、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。 Cisco Unified Communications Manager でリセットおよび登録されるたびに、電話機は設定ファイルを要求します。

次の条件を満たしている場合、電話機は、TFTP サーバにある XmlDefault.cnf.xml という名前のデフォルト設定ファイルにアクセスします。

- Cisco Unified Communications Manager で自動登録を有効にした。
- 該当する電話機が、Cisco Unified Communications Manager データベースにまだ追加されていない。
- 該当する電話機を初めて登録する。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

ネットワーク輻輳時の電話機の挙動

ネットワークパフォーマンスの低下の原因となるものは、音声とビデオの品質にも影響を及ぼすため、場合によっては、通話が中断される可能性があります。 ネットワーク パフォーマンスの低下は、次のような原因が考えられます。

- 内部ポート スキャンやセキュリティ スキャンなどの管理タスク。
- サービス拒否攻撃など、ネットワーク上で発生した攻撃。

2 つのネットワーク ルータを持つネットワークの電話機の動作

Cisco IP 電話 8800 シリーズは、ファイアウォールを使用して、中間者攻撃などのサイバー侵入から保護します。 このファイアウォールを無効にすることはできません。 ただし、同じサブネット内の 2 つのネットワーク ルータと IP リダイレクトでネットワークが設定されている場合、この機能によって電話機のトラフィックが中断されてしまう場合があります。

このネットワーク設定は中間者攻撃と似ているので、電話機のファイアウォールによってトラフィックが中断されてしまいます。 電話機は、その電話機とは異なるサブネットにあるさまざまな IP 宛てのリダイレクト パケットを受信します。 電話機は、複数のルータがあるネットワーク上にあり、デフォルト ルータは 2 番目のルータにトラフィックを送信します。

ファイアウォールがトラフィックを中断していることが疑われるときは、電話機のログを確認してください。 オペレーティング システムで、接続を確立しようとしたときにエラー コード 1 の通知が出ていないか確認してください。 シグニチャの 1 つは、次のとおりです。

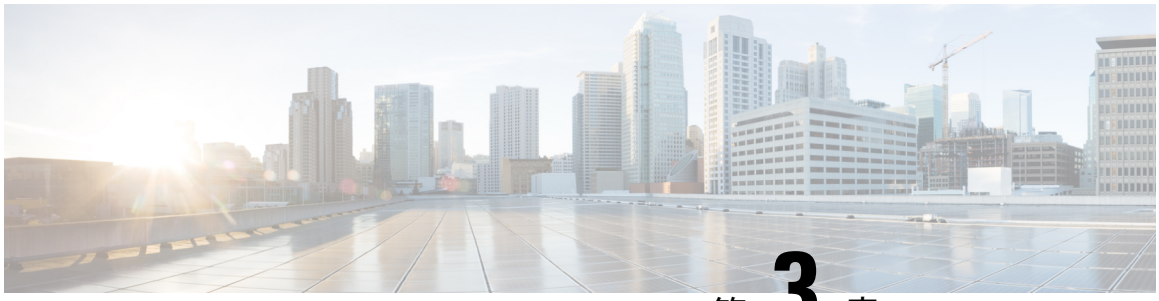
```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

同じサブネット内の2つのネットワーク ルータとIPリダイレクトを使用するネットワークは、一般的な設定ではありません。 このネットワーク設定を使用している場合、1つのサブネットにつきルータを1つだけ使用することを検討してください。 しかし、同じサブネットの2つのネットワーク ルータが必要な場合は、ルータの IP リダイレクトを無効にし、電話機を再起動してください。

アプリケーション プログラミング インターフェイス

シスコは、サードパーティ製アプリケーション開発者によってテストされ、シスコから認定されたサードパーティ製アプリケーションによる電話機の API 使用をサポートしています。 認定されていないアプリケーション間のやりとりに関連する電話の問題は、サードパーティが対処する必要があり、シスコでは対処しません。

シスコ認定のサードパーティ製アプリケーション/ソリューションのサポート モデルについては、シスコ ソリューション パートナー プログラムの Web サイトで詳細を参照してください。



第 3 章

Cisco IP 電話のハードウェア

電話機の概要

Cisco IP 電話 8800 シリーズは、Internet Protocol（IP）ネットワーク経由の音声通信を提供します。 Cisco IP 電話は、デジタル ビジネス フォンとほぼ同様に機能し、電話の発信に加えて、ミュート、保留、転送などの機能を使用できます。 また、データ ネットワークに接続するため、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。

Cisco IP 電話 8811 は、グレースケール LCD 画面を備えています。 Cisco IP 電話 8841、8845、8851、8851NR、8861、8865、および 8865NR は、24 ビット カラー LCD 画面を備えています。

電話回線キーに機能を追加する場合、使用できる回線キーの数には制限があります。 使用している電話機の回線キーの数を超えて機能を追加することはできません。

Cisco IP 電話の機能は次のとおりです。

- [セッション回線モード（Session Line Mode）] で最大 5 回線、[拡張回線モード（Enhanced Line Mode）] で最大 10 回線をサポートするプログラム可能な機能ボタン。
- フル ビデオ機能（Cisco IP 電話 8845、8865、および 8865NR のみ）
- ギガビット イーサネット接続機能
- ワイヤレス ヘッドセット用 Bluetooth のサポート（Cisco IP 電話 8845、8851、8861、および 8865 のみ。 この機能は、Cisco IP 電話 8811、8841、8851NR、および 8865NR ではサポートされていません）

- 外部マイクロフォンとスピーカーのサポート（Cisco IP 電話 8861、8865、および 8865NR のみ）
- Wi-Fi によるネットワーク接続機能（Cisco IP 電話 8861 および 8865 のみ。 Wi-Fi は、Cisco IP 電話 8865NR ではサポートされません）
- USB ポート：
  - Cisco IP 電話 8851 および 8851NR には USB ポート X 1
  - Cisco IP 電話 8861、8865、8865NR には USB ポート X 2

Cisco IP 電話 8845、8865、および 8865NR は、内蔵ビデオ カメラによるビデオ コールをサポートしています。 この機能を使用すれば、友人や同僚とコラボレーションしたり、電話機を使ってフェイスツーフェイス会議を開催することができます。

（注） Cisco IP 電話 8845、8865、および 8865NR では、ボックスと梱包を保存する必要があります。これらの電話機のカメラは脆弱です。 電話機を移動する場合は、電話機を元のボックスにパックしてカメラを保護することを推奨します。 詳細については、ビデオフォンのカメラの保護（41 ページ） を参照してください。

ビデオ コールには次の機能があります。

- [PIP]：右下、右上、左上、左下の 4 つのポジションから選択します。 PIP 表示をオフにすることもできます。
- [スワップ（Swap）]：PIP ビュー内で表示を切り替えます。 [スワップ（Swap）] ソフトキーは PIP がオフになっているときは無効です。
- [ビデオのセルフビュー（Self-view Video）]：[ビデオのセルフビュー（Self-view Video）] を選択すると、ビデオに表示される場合と同様に画像が表示されます。
- [ビデオ UI および会議/転送開始（Video UI and Conference/Transfer Initiation）]：会議を開始する場合に選択します。

ビデオ コールの詳細については、『*Cisco IP* 電話 *8800 Series User Guide for Cisco Unified Communications Manager*』および該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

他のデバイスと同様に、Cisco IP 電話 は設定し、管理する必要があります。 これらの電話機は、次のコーデックのエンコードとデコードを行います。

- G.711 a-law
- G.711 mu-law
- G.722
- G722.2 AMR-WB
- G.729a/G.729ab

- G.726
- iLBC
- Opus
- iSAC

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 IP 電話のすぐ近くで使用すると、相互干渉が発生することがあります。 詳細については、干渉が発生するデバイスの製造元のマニュアルを参照してください。

Cisco IP 電話は、通話転送や転送、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 IP 電話では、さらにその他の各種の機能も提供します。

Cisco IP 電話は、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内容が少なくなります。 ただし、お使いのネットワークで必要な場合は、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。

Cisco IP 電話は、IP ネットワーク上の他のサービスやデバイスと連携することで、高度な機能を提供できます。 たとえば、Cisco Unified Communications Manager 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 電話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 IP 電話はネットワーク 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することができます。 この情報は、ユーザが IP 電話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。 また、アクティブ 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。

Cisco IP 電話を IP テレフォニー ネットワークで機能させるには、IP 電話を Cisco Catalyst スイッチなどのネットワーク デバイスに接続する必要があります。 また、コールを送受信する前に、Cisco IP 電話を Cisco Unified Communications Manager システムに登録する必要があります。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

Cisco IP Phone 8811

以下の項では、Cisco IP Phone 8811 の属性について説明します。

フォンの接続

次の図に示されているように、組織の IP テレフォニー ネットワークに電話機を接続します。

1	DC アダプタ ポート（DC48V）。	5	アクセス ポート（10/100/1000 PC）接続
2	AC-DC 電源装置（オプション）。	6	補助ポート
3	AC 電源コンセント（オプション）。	7	ハンドセットの接続。
4	ネットワーク ポート（10/100/1000 SW）接続。 IEEE 802.3at 電源対応	8	アナログ ヘッドセットの接続（オプション）。

（注） Cisco IP Phone 8811 はキー拡張モジュールをサポートしていません。

Cisco IP 電話 8841 および 8845

次のセクションでは、Cisco IP 電話 8841 および 8845 の属性について説明します。

電話機の接続部

次のダイヤグラムを使用して、電話機を会社の IP テレフォニー ネットワークに接続します。

1	DC アダプタ ポート（DC48V）	5	アクセス ポート（10/100/1000 PC）接続
2	AC-DC 電源装置（オプション）。	6	補助ポート
3	AC 電源コンセント（オプション）。	7	ハンドセットの接続。
4	ネットワーク ポート（10/100/1000 SW）接続。 IEEE 802.3at 電源対応	8	アナログヘッドセットの接続（オプション）。

（注） Cisco IP 電話 8841 および 8845 はキー拡張モジュールをサポートしていません。

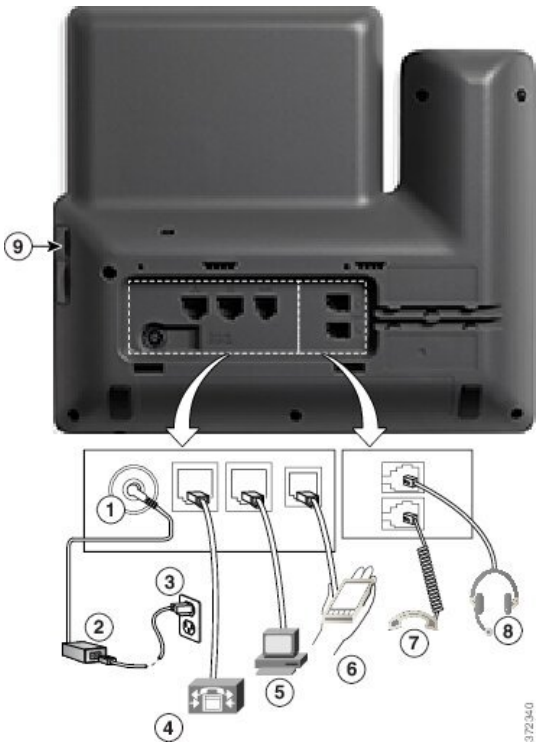
Cisco IP 電話 8851 および 8851NR

以降の項では、Cisco IP 電話 8851 および 8851NR の属性について説明します。

（注） Cisco IP 電話 8851NR は Bluetooth をサポートしていません。 その点を除き、Cisco IP 電話 8851 と Cisco IP 電話 8851NR は同じ機能をサポートしています。

電話接続

次の図に示されているように、企業 IP テレフォニー ネットワークに電話機を接続します。



1	DC アダプタ ポート（DC48V）	6	補助ポート
2	AC-DC 電源装置（オプション）。	7	ハンドセットの接続。
3	AC 電源コンセント（オプション）。	8	アナログ ヘッドセットの接続（オプション）。
4	ネットワーク ポート（10/100/1000 SW）接続。 IEEE 802.3at 電源対応	9	USB ポート
5	アクセス ポート（10/100/1000 PC）接続		

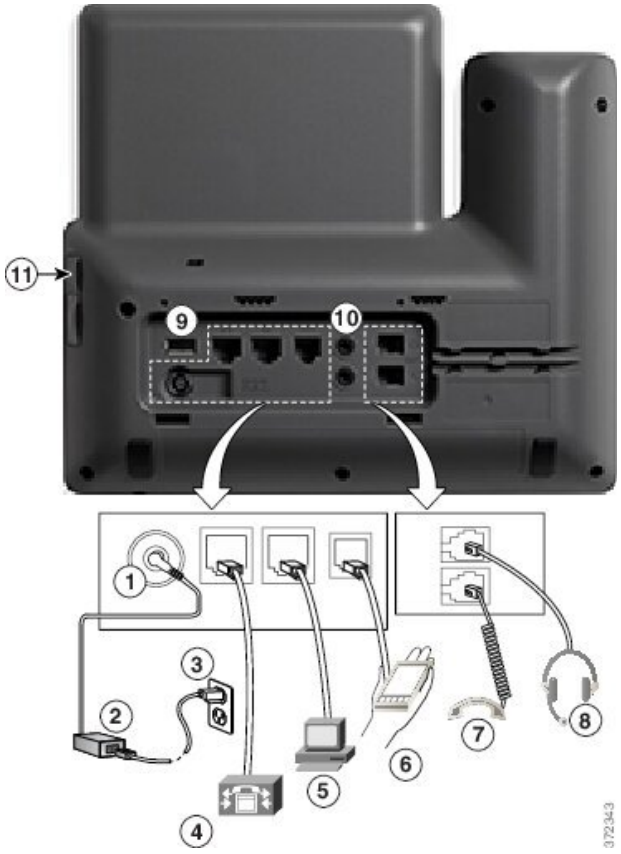
（注） 各USBポートは、最大5台のサポート対象デバイスおよび非サポートデバイスの接続をサポートしています。 電話機に接続された各デバイスは、最大デバイス数に含まれます。 たとえば、電話機は5台のUSBデバイス（2台のキー拡張モジュール、1台のヘッドセット、1台のハブ、および1台の別の標準USBデバイスなど）を側面ポートでサポートします。 第三者製のUSB製品の多くは複数のUSBデバイスとしてカウントされる場合があります。たとえば、あるデバイスにUSBハブとヘッドセットが含まれる場合は2台のUSBデバイスとして扱われることがあります。 詳細については、USBデバイスのマニュアルを参照してください。

Cisco IP 電話 8861、8865、および 8865NR

以降の項では、Cisco IP 電話 8861、8865 および 8865NR の属性について説明します。

電話機の接続部

次の図に示されているように、企業 IP テレフォニー ネットワークに電話機を接続します。



1	DC アダプタ ポート（DC48V）	7	ハンドセットの接続。

2	AC-DC 電源装置（オプション）。	8	アナログ ヘッドセットの接続（オプション）。
3	AC 電源コンセント（オプション）。	9	USB ポート
4	ネットワーク ポート（10/100/1000 SW）接続。 IEEE 802.3at 電源対応	10	オーディオ イン/アウト ポート
5	アクセス ポート（10/100/1000 PC）接続	11	USB ポート
6	補助ポート		

（注） 各USBポートは、最大5台のサポート対象デバイスおよび非サポートデバイスの接続をサポートしています。 電話機に接続された各デバイスは、最大デバイス数に含まれます。 たとえば、電話機では5台のUSBデバイス（たとえば3台のキー拡張モジュール、1台のハブ、もう1台の標準USBデバイス）を側面ポートでサポートし、さらに5台の標準USBデバイスを背面ポートでサポートできます 第三者製のUSB製品の多くは複数のUSBデバイスとしてカウントされる場合があります。たとえば、あるデバイスにUSBハブとヘッドセットが含まれる場合は2台のUSBデバイスとして扱われることがあります。 詳細については、USBデバイスのマニュアルを参照してください。

ボタンとハードウェア

Cisco IP 電話 8800 シリーズには、次に示す 2 つの異なるハードウェア タイプがあります。

- Cisco IP 電話 8811、8841、8851、8851NR、および 8861：カメラなし。
- Cisco IP 電話 8845、8865、および 8865NR：内蔵カメラ付き。

次の図は、Cisco IP 電話 8845 を示しています。

図 *1 : Cisco IP* 電話 *8845* のボタンおよびハードウェア

次の表は、Cisco IP 電話 8800 シリーズのボタンについて説明しています。

表 *18 : Cisco IP* 電話 *8800* シリーズのボタン

1	ハンドセットとハンドセット ライト ストリップ	着信コール（赤色に点滅）または新しいボイス メッセージ（赤色に点灯）があるかどうかを示します。
2	カメラ Cisco IP 電話 8845、8865、および 8865NR のみ	ビデオ コールのためにカメラを使用します。
3	プログラム可能な機能ボタンと回線ボタン	: 電話回線、機能、およびコールセッションにアクセスします。 電話回線キーに機能を追加する場合、使用できる回線キーの数には制限があります。 使用している電話機の回線キーの数を超えて機能を追加することはできません。 詳細については、「Cisco IP 電話 ハードウェア」の章の「ソフトキー、回線ボタン、機能ボタン」の項を参照してください。
4	ソフトキー ボタン	: 関数とサービスにアクセスします。 詳細については、「Cisco IP 電話 ハードウェア」の章の「ソフトキー、回線ボタン、機能ボタン」の項を参照してください。

5	戻る、ナビゲーションクラスタ、およびリリース	戻る：前の画面またはメニューに戻ります。 ナビゲーション クラスタ ナビゲーション リングと[選択（Select）]ボタン：メニューをスクロールしたり、項目を強調表示したり、強調表示されている項目を選択したりできます。 リリース：接続されているコールまたはセッションを終了します。
6	保留/再開、会議、および転送	保留/再開：アクティブ コールを保留にしたり、保留中のコールを再開したりします。 会議：電話会議を作成します。 転送：コールを転送します。
7	スピーカーフォン、ミュート、およびヘッドセット	[スピーカーフォン（**Speakerphone**）]：スピーカフォンのオン/オフを切り替えます。 スピーカフォンがオンになっているとき、ボタンは点灯しています。 [ミュート（**Mute**）]：マイクロフォンのオン/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。 **ヘッドセット**：ヘッドセットをオンに切り替えます。ヘッドセットがオンの場合、ボタンは点灯します。ヘッドセット モードを終了するには、ハンドセットを持ち上げるか、**スピーカーフォン**を選択します。
8	連絡先、アプリケーション、およびメッセージ	連絡先：個人用ディレクトリや社内ディレクトリにアクセスします。 [アプリケーション（Applications）]：発着信履歴、ユーザ設定、電話機設定、および電話機モデル情報にアクセスします。 メッセージ：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。
9	**音量** ボタン	:ハンドセット、ヘッドセット、およびスピーカーフォンの音量（オフ フック）と呼出音の音量（オン フック）を調整します。

ソフトキー、回線ボタン、機能ボタン

電話機で対話式に機能を操作する方法がいくつかあります。

- ソフトキーは画面の下にあり、ソフトキーの上の画面に表示されている機能にアクセスできます。 ソフトキーは、その時点で行っている操作に応じて変化します。 **[その他...（More...）]** ソフトキーは、その他にも使用可能な機能があることを示しています。
- スクリーンの両側にある機能ボタンと回線ボタンを使用すると、電話機能および電話回線にアクセスできます。
  - 機能ボタン：短縮ダイヤルやコール ピックアップなどの機能で使用します。また、別の回線での自分のステータスを表示するために使用します。
  - 回線ボタンを使用すると、コールに応答したり、保留中のコールを再開したりできます。 アクティブ コールに対して使用されないときは、不在着信の表示などの電話機能を開始できます。

機能ボタンと回線ボタンの点灯は、次のようなステータスを示します。

LED のカラーと状態	**標準回線モード: 回線ボタン**	**標準回線モード: 機能ボタン** **[拡張回線モード（Enhanced Line Mode）]**
緑色で一定の LED	アクティブコールまたは双方向インターコムコール、保留コール、使用中のプライバシー	アクティブコールまたは双方向インターコムコール、使用中のプライバシー
緑色、LED 点滅	なし	保留された通話
オレンジ色、点灯 LED	ハントグループにログインした着信コール、復帰コール、一方向インターコムコール	ハントグループにログインした一方向インターコムコール
オレンジ色、LED 点滅	なし	着信コール、復帰コール
赤色、点灯 LED	使用中のリモート回線、保留中のリモート回線、アクティブに応答不可	使用中のリモート回線、アクティブな応答がありません
赤色、LED 点滅	なし	リモート回線が保留中

管理者は、いくつかの機能をソフトキーまたは機能ボタンとして設定できます。 さらに、ソフトキーや関連するハード ボタンを使っていくつかの機能にアクセスすることもできます。

ビデオフォンのカメラの保護

ビデオフォンのカメラが壊れやすく、電話機の配送中に壊れる可能性があります。

始める前に

次のいずれかが必要です。

- 元の電話箱と梱包材
- エアクッションや泡の回り込みなどのパッケージング素材

手順

ステップ 1 元のボックスを使用している場合は、次のようになります。

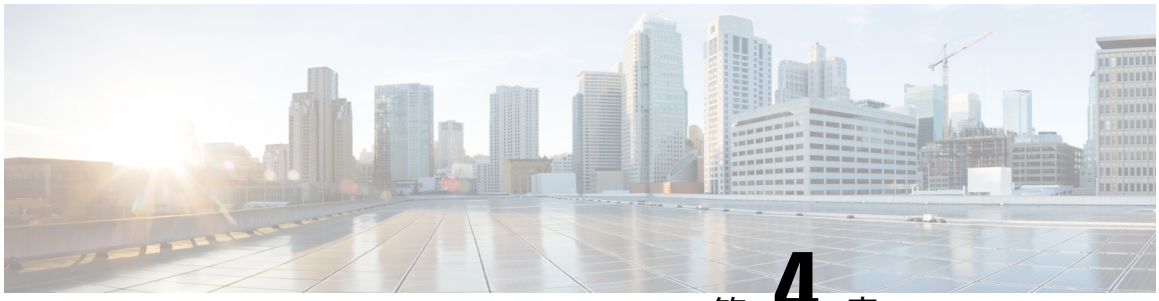
a) レンズがきちんと保護されていることを示すために、カメラにエアクッションを配置します。

b) 電話機を元のボックスに置きます。

ステップ 2 ボックスを持っていない場合は、電話機をエアクッションまたは泡の回りにして、カメラを保護します。どの方向からでもカメラを何も押しられないようにエアクッションがカメラを保護し囲むようにします。または、カメラが輸送中に破損することがあります。

第 II 部

Cisco IP 電話の設置



第 4 章

Cisco IP 電話の設置

ネットワーク セットアップの確認

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 ネットワークのセットアップと設定のチェックリストについては、特定の Cisco Unified Communications Manager リリース向けのドキュメントを参照してください。

電話機がネットワーク内のエンドポイントとして正常に動作するためには、電話ネットワークが特定の要件を満たしている必要があります。 1 つの要件は適切な帯域幅です。 電話機は、Cisco Unified Communications Manager への登録時には、推奨される 32 kbps を超える帯域幅を必要とします。 QoS 帯域幅を設定する際は、これ以上の帯域幅要件を考慮してください。 詳細については、『*Cisco Collaboration System 12.x Solution Reference Network Designs (SRND)*』またはそれ以降（https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html）を参照してください。

（注） 電話機は、Cisco Unified Communications Managerから取得した日時を表示します。 電話機に表示される時間は、Cisco Unified Communications Managerの時間と 10 秒以内の誤差がある場合があります。

手順

ステップ 1 次の要件を満たすように VoIP ネットワークを設定します。

- ルータおよびゲートウェイ上で VoIP が設定されている。
- Cisco Unified Communications Manager がネットワークにインストールされ、コール処理用に設定されている。

ステップ 2 次のいずれかをサポートするようにネットワークをセットアップします。

- DHCP のサポート
- 手動による IP アドレス、ゲートウェイ、およびサブネット マスクの割り当て

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

オンプレミス電話用のアクティベーションコードのオンボーディング

アクティベーションコードオンボーディングを使用すると、自動登録なしで新しい電話機をすばやく設定できます。 この方法では、次のいずれかを使用して電話のオンボーディングプロセスを制御します。

- Cisco Unified Communications Manager 一括管理ツール（BAT）
- [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）]インターフェイスを開きます。
- Administrative XML Web Service（AXL）

からこの機能を有効にする**デバイス情報** Phone Configuration ページのセクション。 選択する**オンボーディング用のアクティベーションコードを要求する**この機能を 1 つのオンプレミス電話に適用したい場合。

電話を登録する前に、ユーザはアクティベーションコードを入力する必要があります。 アクティベーションコードオンボーディングは、個々の電話機、電話機のグループ、またはネットワーク全体に適用できます。

ユーザは 16 桁のアクティベーションコードを入力するだけなので、ユーザが自分の電話機に搭載するのは簡単な方法です。 コードは手動で入力するか、電話機にビデオカメラがある場合はQR コードを入力します。 ユーザにこの情報を提供するには、安全な方法を使用することをお勧めします。 ユーザーに電話機が割り当てられている場合、その情報は Self Care Portal で利用できます。 監査ログは、ユーザがポータルからコードにアクセスしたときに記録します。

アクティベーションコードは 1 回しか使用できず、デフォルトでは 1 週間後に期限切れになります。 コードの有効期限が切れた場合は、ユーザに新しいコードを提供する必要があります。

製造元設置証明書（MIC）とアクティベーションコードが検証されるまで電話を登録できないため、このアプローチはネットワークを安全に保つための簡単な方法であることがわかります。 この方法は、自動登録電話サポート（TAPS）または自動登録のためのツールを使用しないため、オンボード電話を一括処理するのにも便利な方法です。 オンボーディングの速度は、1 秒あたり 1 台の電話、または 1 時間あたり約 3600 台の電話です。 電話機は、Cisco Unified Communications Manager の管理機能、管理 XML Web サービス（AXL）、または BAT を使用して追加できます。

既存の電話機は、アクティベーションコードのオンボーディング用に設定された後にリセットされます。 アクティベーションコードが入力され、電話機の MIC が確認されるまで、登録は行われません。 あなたがそれを実装する前にあなたがアクティベーションコードオンボーディングに向かって動いていることを現在のユーザに知らせてください。

詳細については、*Cisco Unified Communications Manager* および *IM and Presence Service* リリース *12.0(1)* 以降のアドミニストレーション ガイドを参照します。

アクティベーションコードオンボーディングとモバイルおよびリモート アクセス

リモートユーザ用の Cisco IP 電話を導入する場合は、モバイルおよび Remote Access でアクティベーション コードオンボーディングを使用できます。 この機能は、自動登録が不要な場合に、オフプレミスの電話機を導入するための安全な方法です。 ただし、オンプレミスの場合は自動登録用に、電話機をオフプレミスの場合はアクティベーションコードとして設定できます。 この機能は、オンプレミスの電話機のアクティベーションコードオンボーディングと似ていますが、オフプレミスの電話機でもアクティベーションコードを利用できます。

モバイルおよび Remote Access のアクティベーションコードのオンボーディングでは、Cisco Unified Communications Manager 12.5 (1) SU1 以降、および Cisco Expressway X12.5 以降が必要です。 また、スマートライセンスも有効にする必要があります。

この機能は、Cisco Unified Communications Manager の管理から有効にすることができます。ただし、次の点に注意してください。

- からこの機能を有効にする**デバイス情報** Phone Configuration ページのセクション。

- この機能を1つのオンプレミス電話に適用したい場合は、**オンボーディング用のアクティベーション コードを要求する**を選択します。
- アクティベーション オンボーディング機能を 1 つのオフプレミス電話に適用したい場合は、**MRA 経由でアクティベーション コードを許可する** および **オンボーディング用のアクティベーション コードを要求する** を選択します。 電話機がオンプレミスの場合は、モバイルおよび Remote Access モードに変更され、Expressway を使用します。 電話機が Expressway にアクセスできない場合、その電話機がオフプレミスになるまで登録されません。

詳細については、次のマニュアルを参照してください。

- *Cisco Unified Communications Manager* および *IM and Presence Service* リリース *12.0(1)* アドミニストレーション ガイド
- Cisco Expressway X12.5 以降用 *Cisco Expressway* 経由のモバイル & *Remote Access*

電話機の自動登録の有効化

Cisco IP 電話 は、コールの処理に Cisco Unified Communications Manager を必要とします。 Cisco Unified Communications Manager を正しくセットアップして、電話機を管理し、コールを適切にルーティングおよび処理するには、該当する Cisco Unified Communications Manager リリースまたは Cisco Unified Communications Manager Administration の状況依存ヘルプを参照してください。

Cisco IP 電話を設置する前に、電話機を Cisco Unified Communications Manager データベースに追加する方法を選択しておく必要があります。

電話機を設置する前に自動登録を有効にしておくと、次のことが可能になります。

- 事前に電話機から MAC アドレスを収集することなく、電話機を追加する。
- Cisco IP 電話を IP テレフォニー ネットワークに物理的に接続したときに、その電話機を Cisco Unified Communications Manager データベースに自動的に追加する。 自動登録中に、Cisco Unified Communications Manager は連続する電話番号の中から次に使用可能なものを電話機に割り当てます。
- 電話機を Cisco Unified Communications Manager データベースにすばやく登録し、電話番号などの設定を Cisco Unified Communications Manager から変更する。
- 自動登録された電話機を新しい場所に移動し、電話番号を変更しないまま別のデバイス プールに割り当てる。

自動登録は、デフォルトでは無効になっています。 自動登録を使用しない方がよい場合もあります。たとえば、電話機に特定の電話番号を割り当てる場合や、Cisco Unified Communications Manager とのセキュア接続を使用する場合です。 自動登録の有効化の詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。 Cisco CTL クライアントを通じてクラスタを混合モードに設定すると、自動登録が自動的に無効になりま

すが、これを有効に設定できます。 Cisco CTL クライアントを通じてクラスタを非セキュアモードに設定すると、自動登録は自動的には有効になりません。

自動登録と TAPS（Tool for AutoRegistered Phones Support）を使用すると、MAC アドレスを最初に電話機から収集しなくても、電話機を追加することができます。

TAPS は、一括管理ツール（BAT）と連携して、Cisco Unified Communications Manager データベースにダミー MAC アドレスを使用して追加された一連の電話機をアップデートします。TAPS を使用して、MAC アドレスを更新し、デバイス向けに事前定義された設定をダウンロードします。

自動登録と TAPS は、ネットワークに追加する電話機が 100 台未満の場合に使用することを推奨します。 100 台を超える電話機をネットワークに追加するには、一括管理ツール（BAT）を使用します。

TAPS を利用するには、管理者またはエンドユーザが TAPS の電話番号をダイヤルして、音声プロンプトに従います。 このプロセスが完了した後、電話機には電話番号とその他の設定値が含まれており、電話機は正しい MAC アドレスを使用して Cisco Unified Communications Manager の管理ページで更新されます。

ネットワークに Cisco IP 電話を接続する前に、自動登録が Cisco Unified Communications Manager の管理ページで有効になっていて、正しく設定されていることを確認します。 自動登録の有効化および設定の詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

TAPS が機能するためには、Cisco Unified Communications Manager の管理ページで自動登録を有効にする必要があります。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、 **[システム（System）]** > **[Cisco Unified CM]** をクリックします。

ステップ 2 [検索（Find）]をクリックして、必要なサーバを選択します。

ステップ 3 [自動登録の情報（Auto-registration Information）]で、これらのフィールドを設定します。

- **[ユニバーサルデバイステンプレート(Universal Device Template)]**
- **[ユニバーサル回線テンプレート(Universal Line Template)]**
- **[開始電話番号(Starting Directory Number)]**
- **終了電話番号（Ending Directory Number）**

ステップ 4 [この Cisco Unified CM では自動登録は無効にする（Auto-registration Disabled on this Cisco Unified Communications Manager）]チェックボックスをオフにします。

ステップ 5 **[保存]** をクリックします。

ステップ 6 **[設定の適用（Apply Config）]** をクリックします。

Cisco IP 電話の設置

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

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

（注） 外部デバイスを使用する前に、外部デバイス （28 ページ）を参照してください。

アクセサリの設置については、『*Cisco IP 電話 7800 and 8800 Series Accessories Guide for Cisco Unified Communications Manager*』を参照してください。

机上にLANケーブルが1本しかない場合、SWポートで電話機をLANに接続し、コンピュータをPCポートに接続します。 詳細については、コンピュータとの有線ネットワーク接続の共有 （52 ページ） を参照してください。

また、2台の電話機をデイジーチェーンで接続することもできます。 1台目の電話機のPCポートを2台目の電話機のSWポートに接続します。

注意 SWポートとPCポートはLANに接続しないでください。

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

詳細については、電話機の所要電力 （16 ページ） を参照してください。

ステップ2 ハンドセットをハンドセットポートに接続し、電話機のチャネルにケーブルを押し込みます。

ワイドバンド対応ハンドセットは、Cisco IP電話で使用するために特別に設計されたものです。ハンドセットは、着信コールやボイス メッセージがあることを通知する、ライト ストリップを備えています。

注意 電話機のチャネルにケーブルを押し込むことに失敗すると、プリント回路基板が損傷する可能性があります。 ケーブルチャネルにより、コネクタとプリント回路ボードにかかる負担が軽減されます。

ステップ 3 ヘッドセットまたはワイヤレス ヘッドセットを接続します。 ヘッドセットは設置の際に接続しなくても、後から追加できます。

ケーブルをケーブル チャネルに差し込みます。

注意 電話機のチャネルにケーブルを押し込むことに失敗すると、電話機内部のプリント回路基板が損傷する可能性があります。 ケーブル チャネルにより、コネクタとプリント回路ボードにかかる負担が軽減されます。

ステップ 4 ストレート イーサネット ケーブルを使用して、スイッチを Cisco IP 電話の 10/100/1000 SW というラベルの付いたネットワーク ポートに接続します。 Cisco IP 電話には、イーサネット ケーブルが 1 本同梱されています。

10 Mbps 接続にはカテゴリ 3、5、5e、または 6 のケーブル接続を使用します。100 Mbps 接続には 5、5e、または 6 を使用します。1000 Mbps 接続にはカテゴリ 5e または 6 を使用します。 ガイドラインの詳細については、ネットワーク ポートとコンピュータ ポートのピン割り当て（15 ページ）を参照してください。

ステップ 5 ストレート イーサネット ケーブルを使用して、デスクトップ コンピュータなどの他のネットワーク デバイスを Cisco IP 電話のコンピュータ ポートに接続します。 別のネットワーク デバイスは、ここで接続しなくても後で接続できます。

10 Mbps 接続にはカテゴリ 3、5、5e、または 6 のケーブル接続を使用します。100 Mbps 接続には 5、5e、または 6 を使用します。1000 Mbps 接続にはカテゴリ 5e または 6 を使用します。 ガイドラインの詳細については、ネットワーク ポートとコンピュータ ポートのピン割り当て（15 ページ）を参照してください。

ステップ 6 電話機を机の上に置く場合は、フットスタンドを調整します。 電話機を壁に取り付ける場合は、受話器が受け台から滑り落ちないようにハンドセットの受け台を調整する必要があります。

ステップ 7 電話機の起動プロセスをモニタします。この手順では、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、電話機が正しく設定されていることを確認します。

ステップ 8 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。

ネットワークの設定 （63 ページ）およびネットワークのセットアップ （275 ページ）を参照してください。

ステップ 9 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ます。

ワイヤレス接続の品質と帯域幅によっては、WLAN インターフェイスを通じたファームウェアのアップグレードは、有線インターフェイスより時間がかかることがあります。 一部のアップグレードでは完了までに 1 時間を超える場合があります。

ステップ 10 Cisco IP 電話でコールを発信し、電話機と各機能が正常に動作することを確認します。

『*Cisco IP 電話 8800 Series User Guide*』を参照してください。

ステップ 11 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。 この手順では、ユーザが十分な情報を得て、Cisco IP 電話 を有効に活用できるようにします。

コンピュータとの有線ネットワーク接続の共有

電話機とお使いのコンピュータは、正常に機能するようにネットワークに接続する必要があります。イーサネットポートが1つしかない場合は、デバイスでネットワーク接続を共有できます。

始める前に

管理者は、使用する前に、Cisco Unified Communications Manager PC ポートを有効にする必要があります。

手順

ステップ 1 イーサネットケーブルを使用して、電話機 SW ポートを LAN に接続します。

ステップ 2 コンピュータをイーサネット ケーブルで AP のイーサネット ポートに接続します。

セットアップ メニューからの電話の設定

Cisco IP 電話には、次の設定メニューが用意されています。

- [ネットワークのセットアップ（Network Setup）]：IPv4 専用、IPv6 専用、WLAN、イーサネットといったネットワーク設定の表示や設定のオプションを提供します。
- [イーサネットのセットアップ（Ethernet Setup）]：このサブメニューのメニュー項目には、イーサネット ネットワークを介して Cisco IP 電話 を設定するための設定オプションがあります。
- [Wi-Fi クライアントのセットアップ（Wi-Fi client setup）]：このサブメニューのメニュー項目には、ワイヤレス ローカル エリア ネットワーク（WLAN）を介して Cisco IP 電話 を設定するための設定オプションがあります。 Wi-Fi は Cisco IP 電話 8861 および 8865 でのみサポートされます。

（注） 電話機で Wi-Fi を有効にすると、電話機の PC ポートが無効になります。

- [IPv4 のセットアップ（IPv4 Setup）] と [IPv6 のセットアップ（IPv6 Setup）] : これらのサブメニューは、[イーサネットのセットアップ（Ethernet Setup）] メニューと [Wi-Fi クライアントのセットアップ（Wi-Fi client setup）] メニューのサブメニューで、ネットワーク オプションを追加します。
- [セキュリティのセットアップ（Security Setup）] : セキュリティ モード、信頼リスト、802.1X 認証といったセキュリティ設定などの表示や設定のオプションを提供します。

[ネットワークのセットアップ（Network Setup）] メニューにあるオプション設定値を変更するには、オプションのロックを編集のために解除しておく必要があります。

（注） Cisco Unified Communications Manager Administration の [電話の設定（Phone Configuration）] ウィンドウにある [設定アクセス（Settings Access）] フィールドを使用すると、電話機から [設定（Settings）] メニューやこのメニューのオプションにアクセスできるかどうかを制御できます。 設定アクセス フィールドでは、次の値を設定できます。

- [有効（Enabled）] : [設定（Settings）] メニューへのアクセスを許可します。
- [無効（Disabled）] : [設定（Settings）] メニューへのアクセスを禁止します。
- [非許可（Restricted）] : [ユーザ設定（User Preferences）] メニューへのアクセスを許可し、音量の設定変更の保存を許可します。 [設定（Settings）] メニューの他のオプションへのアクセスは禁止します。

[管理者設定（Administrator Settings）] メニューのオプションにアクセスできない場合は、設定アクセス フィールドを確認してください。

手順

ステップ 1 **[アプリケーション (Applications)]** を押します。

ステップ 2 [管理者設定（Admin Settings）]を選択します。

ステップ 3 [ネットワークのセットアップ（Network Setup）]または[セキュリティのセットアップ（Security Setup）]を選択します。

ステップ 4 必要に応じてユーザ ID とパスワードを入力し、[ログイン（Sign-In）]をクリックします。

ステップ 5 次のいずれかの操作を実行して、目的のメニューを表示します。

- ナビゲーション矢印を使用して目的のメニューを選択し、[選択（Select）]を押します。
- 電話機のキーパッドを使用して、メニューに対応する番号を入力します。

ステップ 6 サブメニューを表示するには、ステップ 5 を繰り返します。

ステップ 7 メニューを終了するには、[終了（Exit）]または U ターン型の矢印 を押します。

電話機パスワードの適用

電話機にパスワードを適用できます。 適用すると、[管理者設定（Admin Settings）] 電話スクリーンでパスワードを入力しない限り、電話機の管理者オプションは変更できません。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウに移動します（**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[共通の電話プロファイル（Common Phone Profile）]**）。

ステップ 2 [電話ロック解除パスワード（Local Phone Unlock Password）] オプションで、パスワードを入力します。

ステップ 3 電話機が使用する共通の電話プロファイルに、パスワードを適用します。

電話機からのテキストとメニューの入力

オプション設定値を編集するときは、次のガイドラインに従ってください。

- 編集するフィールドを強調表示するには、ナビゲーションパッドの矢印を使用します。次にナビゲーションパッドの [選択（Select）]を押すとフィールドがアクティブになります。フィールドがアクティブになったら、値を入力できます。
- 数値と文字を入力するには、キーパッド上のキーを使用します。
- キーパッドを使用して文字を入力するには、対応する数値キーを使用します。 キーを 1 回または何回か押して、個々の文字を表示します。 たとえば、**2** キーを 1 回押して 「a」、すばやく 2 回押して 「b」、すばやく 3 回押して 「c」 を表示します。一時停止すると、カーソルが自動的に進み、次の文字を入力できます。
- 入力を誤ったときは、矢印ソフトキー ↰ を押します。 このソフトキーを押すと、カーソルの左側にある文字が削除されます。
- 変更内容を保存しない場合は、**[保存]** を押す前に、**[キャンセル]** を押します。
- IP アドレスを入力するには、ユーザ用に分割されている 4 個のセグメントに値を入力します。左端からピリオドまでの数字を入力し終わったら、右向き矢印キーを使用して次のセグメントに移動します。 左端の数字の後のピリオドは自動的に挿入されます。
- IPv6 アドレスのコロンを入力するには、キーパッドの ***** を押します。

（注） Cisco IP 電話では、必要に応じて、いくつかの方法でオプション設定値をリセットまたは復元することができます。

関連トピック

基本的なリセット （317 ページ）
電話機パスワードの適用 （54 ページ）

電話機でのワイヤレス LAN の有効化

ワイヤレス LAN を設定する前に、電話機でワイヤレスの使用がサポートされていることを確認します。 Cisco IP 電話 8861 および 8865 は、ワイヤレス LAN 導入環境をサポートしています。 Cisco IP 電話 8865NR はワイヤレス LAN をサポートしていません。

ワイヤレス LAN が導入されている場所の Wi-Fi カバレッジが音声パケットの送信に最適であることを確認します。

音声の Wi-Fi 接続を有効にしてあり、EAP-FAST または PEAP セキュリティ モードを使用している場合、WLAN サインインアプリケーションを使用して Wi-Fi ネットワークを認証します。 WEP、PSK、オープン セキュリティ モードは、Wi-Fi ネットワークで認証します。

Wi-Fi ユーザには、高速セキュア ローミング方式をお勧めします。

（注） 電話機で Wi-Fi を有効にすると、電話機の PC ポートが無効になります。

完全な設定情報については、次の場所にある『*Cisco IP* 電話 *8800 Wireless LAN Deployment Guide*』を参照してください。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

『*Cisco IP* 電話 *8800 Wireless LAN Deployment Guide*』には、次の設定情報が記載されています。

- ワイヤレス ネットワークの設定
- [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] でのワイヤレス ネットワークの設定
- Cisco IP 電話 でのワイヤレス ネットワークの設定

始める前に

Wi-Fi が電話で有効であり、イーサネット ケーブルが切断されていることを確認します。

手順

ステップ 1 アプリケーションを有効にするには、**[アプリケーション（Applications）]** を押します。

ステップ 2 **[管理者設定（Admin Settings）]** > **[ネットワークのセットアップ（Network Setup）]** > **[Wi-Fi クライアントのセットアップ（Wi-Fi Client setup）]** > **[ネットワーク名（Network name）]** を選択します。

ユーザが接続可能なワイヤレス アクセス ポイントの一覧が表示されます。

ステップ 3 ワイヤレス ネットワークを有効にします。

Cisco Unified Communications Manager からのワイヤレス LAN のセットアップ

Cisco Unified Communications Manager Administration で、ワイヤレス Cisco IP 電話の「「Wi-Fi」」というパラメータを有効にする必要があります。

（注） Cisco Unified Communications Manager Administration の [電話の設定（Phone Configuration）] ウィンドウ（**[デバイス（Device）]** > **[電話機（Phone）]**）で、MAC アドレスの設定時に、有線の MAC アドレスを使用します。 Cisco Unified Communications Manager の登録では、無線 MAC アドレスを使用しません。

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、次の手順を実行します。

手順

ステップ 1 特定の電話機でワイヤレス LAN を有効にするには、次の手順を実行します。

a) **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。
b) 対象の電話を特定します。
c) [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの [Wi-Fi] パラメータに対して [有効化（Enabled）]設定を選択します。
d) [共通設定の上書き（Override Common Settings）]チェックボックスをオンにします。

ステップ 2 電話機のグループに対してワイヤレス LAN を有効にするには、

a) **[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[共通の電話プロファイル（Common Phone Profile）]** の順に選択します。
b) [Wi-Fi] パラメータに対して [有効化（Enabled）]設定を選択します。

（注） この手順の設定を機能させるには、手順 1d で言及されている [共通設定の上書き（Override Common Settings）]チェック ボックスのチェックを外します。

c) [共通設定の上書き（Override Common Settings）]チェックボックスをオンにします。
d) **[デバイス（Device）]** > **[電話（Phone）]** を使用して、電話機を共通プロファイルと関連付けます。

ステップ 3 ネットワークのすべての WLAN 対応電話機に対してワイヤレス LAN を有効にするには、

a) **[システム（System）]** > **[エンタープライズ電話の設定（Enterprise Phone Configuration）]** を選択します。

b) [Wi-Fi] パラメータに対して [有効化（Enabled）]設定を選択します。

（注） この手順の設定を機能させるには、手順 1d と手順 2c で言及されている [共通設定の上書き（Override Common Settings）]チェック ボックスのチェックを外します。

c) [共通設定の上書き（Override Common Settings）]チェックボックスをオンにします。

電話機からのワイヤレス LAN のセットアップ

Cisco IP 電話を WLAN に接続可能にするには、先に適切な WLAN 設定で電話機のネットワーク プロファイルを設定する必要があります。電話機の [ネットワークのセットアップ（Network Setup）] メニューを使用して [Wi-Fi クライアントのセットアップ（Wi-Fi client setup）] サブメニューにアクセスし、WLAN 設定をセットアップすることができます。

（注） 電話機で Wi-Fi を有効にすると、電話機の PC ポートが無効になります。

（注） Wi-Fi が Cisco Unified Communications Manager で無効にされている場合、[ネットワーク設定（Network Setup）] メニューには [Wi-Fi クライアントのセットアップ（Wi-Fi client setup）] オプションが表示されません。

詳細情報については、http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html にある『*Cisco IP* 電話 *8800 Series WLAN Deployment Guide*』を参照してください。

ワイヤレス LAN プロファイルの **[ユーザが変更可能（User Modifiable）]** フィールドは、電話機のセキュリティモードをユーザーが設定できるかどうかを制御します。ユーザが変更できないフィールドがある場合、それらのフィールドはグレー表示されます。

始める前に

Cisco Unified Communications Manager からワイヤレス LAN を設定します。

手順

ステップ 1 **[アプリケーション（Applications）]** を押します。

ステップ 2 **[管理者設定（Administrator Settings）]** > **[ネットワークのセットアップ（Network Setup）]** > **[Wi-Fi クライアントのセットアップ（Wi-Fi client setup）]** の順に選択します。

ステップ 3 次の表に示すようにワイヤレス設定をセットアップします。

表 *19 : [Wi-Fi* クライアントのセットアップ（*Wi-Fi client setup*）*]* メニュー オプション

オプション	説明	変更の手順
ネットワーク名	ワイヤレス アクセス ポイントにアクセスする固有識別情報、サービス セット ID（SSID）を指定します。 利用可能なワイヤレス アクセス ポイントの一覧が表示されます。	ネットワークの設定 （63 ページ）してください。
IPv4 専用セットアップ	[IPv4 のセットアップ（IPv4 Setup）] 設定サブメニューでは、次の作業を実行できます。 • DHCP サーバが割り当てた IP アドレスの、電話機による使用のオン/オフ。 • IP アドレス、サブネット マスク、デフォルト ルータ、DNS サーバ、および代替 TFTP サーバの手動設定。 IPv4 アドレス フィールドの詳細については、IPv4 フィールド （65 ページ）を参照してください。	[IPv4 のセットアップ（IPv4 Set クロールし、**選択**を押します。
IPv6 専用セットアップ	[IPv6 のセットアップ（IPv4 Setup）] 設定サブメニューでは、次の作業を実行できます。 • IPv6 対応ルータを介して SLAAC が取得した、または DHCPv6 サーバによって割り当てられた IPv6 アドレスの使用を、電話機で有効または無効にします。 • IPv6 アドレス、プレフィックス長、デフォルト ルータ、DNS サーバ、および代替 TFTP サーバを手動設定します。 IPv6 アドレス フィールドの詳細については、IPv6 フィールド （68 ページ）を参照してください。	[IPv6 のセットアップ（IPv6 Set クロールし、**選択ボタン**を押し
MAC Address	電話機固有のメディア アクセス コントロール（MAC）アドレス。	表示のみ。 変更不可。
ドメイン名	電話機が所属するドメイン ネーム システム（DNS）ドメインの名前。	ネットワークの設定 （63 ページ）してください。

ステップ 4 [保存（Save）] を押して変更を行うか、[復元（Revert）] を押して接続を破棄します。

WLAN 認証試行の回数の設定

認証要求は、ユーザのサインイン クレデンシャルの確認です。 これは、Wi-Fi ネットワークにすでに参加している電話機が Wi-Fi サーバへの再接続を試行するたびに発生します。 たとえ

ば、Wi-Fi セッションがタイムアウトしたとき、また Wi-Fi 接続が失われて再取得されるときなどです。

Wi-Fi 電話機が Wi-Fi サーバに認証要求を送信する回数を設定できます。 デフォルトの試行回数は 2 回ですが、このパラメータを 1 から 3 の範囲で設定することができます。電話が認証に失敗した場合、ユーザーは再度ログインするように求められます。

個々の電話機、電話機のプール、またはネットワーク内のすべての Wi-Fi 電話機に [WLAN 認証の試行（WLAN Authentication Attempts）] を適用できます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択し、電話機を見つけます。

ステップ 2 [プロダクト固有の設定（Product Specific Configuration）] 領域に移動して、[WLAN 認証の試行（WLAN Authentication Attempts）] フィールドを設定します。

ステップ 3 **保存**を選択します。

ステップ 4 [設定の適用（Apply Config）]を選択します。

ステップ 5 電話機を再起動します。

WLAN プロンプト モードの有効化

ユーザの電話機で電源を入れるかリセットしたときに Wi-Fi ネットワークにログインする場合には、WLAN プロファイル 1 プロンプト モードを有効にします。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 設定する電話機を特定します。

ステップ 3 [プロダクト固有の設定]領域に移動し、**[WLANプロファイル1プロンプトモード（WLAN Profile 1 Prompt Mode）]** フィールドを **[有効（Enable）]** に設定します。

ステップ 4 **保存**を選択します。

ステップ 5 [設定の適用（Apply Config）]を選択します。

ステップ 6 電話機を再起動します。

Cisco Unified Communications Manager を使用した Wi-Fi プロファイルの設定

Wi-Fi プロファイルを設定して、そのプロファイルを、Wi-Fi をサポートする電話機に割り当てることができます。 プロファイルには、電話機が Wi-Fi を使用して Cisco Unified Communications Manager に接続するために必要なパラメータが含まれています。 Wi-Fi プロファイルを作成して使用する際、管理者およびユーザが個々の電話機に対してワイヤレス ネットワークの設定を行う必要はありません。

Wi-Fi プロファイルは、Cisco Unified Communications Manager リリース 10.5(2) 以降でサポートされます。 EAP-FAST、PEAP-GTC-GTC、および PEAP-MSCHAPv2 は、Cisco Unified Communications Manager リリース 10.0 以降でサポートされています。 Cisco Unified Communications Manager リリース 11.0 以降では、EAP-TLS もサポート対象です。

Wi-Fi プロファイルによって、ユーザが電話機の Wi-Fi 設定を変更できないようにしたり、制限したりすることができます。

Wi-Fiプロファイルを使用する際、キーとパスワードを保護するため、TFTP暗号化が有効にされたセキュアなプロファイルを使用することをお勧めします。

EAP-FAST、PEAP-MSCHAPV、または PEAP-GTC 認証を使用するように電話機を設定する場合、ユーザは個々のユーザー ID とパスワードを使用して、電話機にサインインする必要があります。

Cisco IP 電話 8832 は、SCEP または手動インストール方法のいずれかでインストールできるサーバ証明書を1つだけサポートしています。両方の方法ではサポートされていません。 電話機は TFTP による証明書のインストール方法をサポートしていません。

（注） Cisco Unified Communications Manager に接続するために Expressway 経由で Mobile and Remote Access を使用する電話機は、Wi-Fiプロファイルを使用できません。 ユーザの電話機の SSID、認証モード、およびログイン クレデンシャルがないため、電話機のワイヤレス LAN プロファイルを設定できません。

手順

ステップ 1 Cisco Unified Communications Administration で、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[ワイヤレス LAN プロファイル（Wireless LAN Profile）]** の順に選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ワイヤレス LAN プロファイル情報（Wireless LAN Profile Information）]セクションで、以下のようにパラメータを設定します。

- [名前（Name）]：Wi-Fiプロファイルの固有の名前を入力します。 電話機にこの名前が表示されます。

- [説明（Description）]：このプロファイルを他の Wi-Fi プロファイルから区別するための Wi-Fi プロファイルの説明を入力します。
- [ユーザが変更可能（User Modifiable）]：次のオプションの中から選択します。
  - [許可（Allowed）]：ユーザが電話機から Wi-Fi 設定を変更できることを示します。 このオプションは、デフォルトで選択されます。
  - [拒否（Disallowed）]：ユーザが電話機から Wi-Fi 設定を変更できないことを示します。
  - [制限（Restricted）]：ユーザが電話機の Wi-Fi ユーザ名およびパスワードを変更できることを示します。 ただし、電話機のその他の Wi-Fi 設定は変更できません。

ステップ 4 [Wireless Settings] セクションで、次のパラメータを設定します。

- [SSID（ネットワーク名）（SSID (Network Name)）]：電話機を接続可能なユーザ環境で使用できるネットワーク名を入力します。 この名前は、電話機で使用可能なネットワークリストの下に表示され、その電話機はこのワイヤレス ネットワークに接続できます。
- [周波数帯域（Frequency Band）]：使用可能なオプションは [自動（Auto）]、[2.4 GHz]、[5 GHz] です。 このフィールドは、ワイヤレス接続で使用する周波数帯域を決定します。 [自動（Auto）] を選択すると、電話機は 5 GHz 帯域の使用を最初に試行し、5 GHz 帯域が使用できない場合のみ、2.4 GHz 帯域を使用します。

ステップ 5 [Authentications Settings] セクションで、[Authentication Method] を [EAP-FAST]、[EAP-TLS]、[PEAP-MSCHAPv2]、[PEAP-GTC]、[PSK]、[WEP]、または [None] のいずれかの認証方式に設定します。

このフィールドを設定したら、設定する必要がある追加フィールドが表示されることがあります。

- [ユーザ証明書（User certificate）]：EAP-TLS 認証に必要です。 [製造元でインストール（Manufacturing installed）] または [ユーザによってインストール（User installed）] を選択します。 電話機では証明書を、SCEP から自動で、または電話の管理ページから手動でインストールする必要があります。
- [PSK パスフレーズ（PSK passphrase）]：PSK 認証に必要です。 8 ～ 63 文字の ASCII または 64 文字の 16 進数文字のパスフレーズを入力します。
- [WEP キー（WEP Key）]：WEP 認証に必要です。 40/102 または 64/128 の ASCII または 16 進数の WEP キーを入力します。
  - 40/104 ASCII は 5 文字です。
  - 64/128 ASCII は 13 文字です。
  - 40/104 の 16 進数は 10 文字です。
  - 64/128 の 16 進数は 26 文字です。

- **共有ログイン情報の指定**：EAP-FAST、PEAP-MSCHAPv2、および PEAP-GTC 認証に必要です。
  - ユーザがユーザ名とパスワードを管理する場合、[ユーザ名（Username）] と [パスワード（Password）] のフィールドは空白のままにします。
  - すべてのユーザが同じユーザ名とパスワードを共有する場合、ここで [ユーザ名（Username）] と [パスワード（Password）] のフィールドに情報を入力できます。
  - [パスワードの説明（Password Description）] フィールドに説明を入力します。

（注） 各ユーザに固有のユーザ名とパスワードを割り当てる必要がある場合、各ユーザのプロファイルを作成する必要があります。

（注） [ネットワーク アクセス プロファイル（Network Access Profile）] フィールドは、Cisco IP 電話 8861 および 8865 ではサポートされません。

ステップ 6 **[保存]** をクリックします。

次のタスク

[WLAN プロファイル グループ（WLAN Profile Group）] をデバイス プール（**[システム（System）]**>**[デバイス プール（Device Pool）]**）、または直接電話機に（**[デバイス（Device）]**>**[電話（Phone）]**）に適用します。

Cisco Unified Communications Manager を使用した Wi-Fi グループの設定

ワイヤレス LAN プロファイル グループを作成し、そのグループにワイヤレス LAN プロファイルを追加することができます。 その後、電話機のセットアップ時に、プロファイル グループを電話機に割り当てることができます。

手順

ステップ 1 Cisco Unified Communications Administration で、**[デバイス（Device）]**>**[デバイスの設定（Device Settings）]**>**[ワイヤレス LAN プロファイル グループ（Wireless LAN Profile Group）]** の順に選択します。

また、**[システム（System）]**>**[デバイス プール（Device Pool）]** からワイヤレス LAN プロファイル グループを定義できます。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ワイヤレス LAN プロファイル グループ情報（Wireless LAN Profile Group Information）]セクションで、グループ名と説明を入力します。

ステップ 4 [ワイヤレス LAN プロファイル グループのプロファイル（Profiles for this Wireless LAN Profile Group）]セクションで、[使用可能なプロファイル（Available Profiles）]リストから使用可能な

プロファイルを選択し、選択したプロファイルを [選択したプロファイル（Selected Profiles）] リストに移動します。

複数のワイヤレス LAN プロファイルを選択した場合、電話機は最初のワイヤレス LAN プロファイルのみを使用します。

ステップ 5 **[保存]** をクリックします。

ネットワークの設定

手順

ステップ 1 アプリケーション を押します。

ステップ 2 [ネットワーク設定（Network Settings）] メニューにアクセスするには、**[管理者設定（Admin settings）]** > **[イーサネットのセットアップ（Ethernet setup）]** を選択します。

ステップ 3 イーサネット設定フィールド （63 ページ）の説明に従って、フィールドを設定します。

ステップ 4 フィールドを設定した後、[適用（Apply）] および [保存（Save）] を選択します。

ステップ 5 電話機をリブートします。

イーサネット設定フィールド

[ネットワークのセットアップ（Network Setup）] メニューには、IPv4 と IPv6 のためのフィールドとサブメニューが含まれています。 いくつかのフィールドを変更するには、まず DHCP を無効にしてください。

VPN 接続を確立してイーサネット データ フィールドを上書きします。

表 *20 : [イーサネットのセットアップ（Ethernet Setup）] メニューのオプション*

エントリー	タイプ（Type）	説明
IPv4 のセットアップ（IPv4 setup）	メニュー	IPv4 フィールドに関するセクションを参照してください。 このオプションは、電話機が IPv4 専用モードまたは IPv4/IP 合にのみ表示されます。
IPv6 のセットアップ（IPv6 setup）	メニュー	「IPv6 フィールド」のセクションを参照してください。
MAC Address	文字列	電話機固有のメディア アクセス コントロール（MAC）ア 表示のみ。 変更不可。

エントリー	タイプ（Type）	説明
ドメイン名	文字列	電話機が所属するドメイン ネーム システム（DNS）ドメインの このフィールドを変更するには、DHCP を無効にしてください
接続先 VLAN ID（Operational VLAN ID）		電話機が所属する、Cisco Catalyst スイッチに設定された補助 V この設定は、補助 VLAN または管理 VLAN が設定されている 電話機が補助 VLAN をまだ受信していない場合、このオプショ います。 Cisco Discovery Protocol または Link Level Discovery Protocol Me 効になっている場合、電話機は管理 VLAN から接続先 VLAN VLAN ID を手動で割り当てるには、[管理 VLAN ID（Admin V 用します。
[管理 VLAN ID（Admin VLAN ID）]		電話機がメンバーになっている補助 VLAN。 電話機がスイッチから補助VLANを受信していない場合のみ使 が無視されます。
PC VLAN		ボイス VLAN をサポートしないサードパーティ スイッチと電話 ます。 このオプションを変更する前に、[管理 VLAN ID（Adm を設定する必要があります。
SWポートのセットアップ（SW port setup）	Auto Negotiate 1000 フル（10 Full） 100 ハーフ（100 Half） 10 ハーフ（100 Half） 10 フル（10 Full）	ネットワーク ポートの速度と二重化モード。 次の有効な値を指 • [自動ネゴシエーション（Auto Negotiate）]（デフォルト） • [1000 フル（1000 Full）]：1000-BaseT/全二重 • [100 ハーフ（100 Half）]：100-BaseT/半二重 • [100 フル（100 Full）]：100-BaseT/全二重 • [10 ハーフ（10 Half）]：10-BaseT/半二重 • [10 フル（10 Full）]：10-BaseT/全二重 電話機がスイッチに接続されている場合は、スイッチ ポートを るか、両方を自動ネゴシエーションに設定します。 この設定を編集する場合には、ネットワーク設定オプションを このオプションの設定値を変更する場合は、[PC ポート設定（ プションを同じ設定値に変更する必要があります。

エントリー	タイプ（Type）	説明
PC ポートのセットアップ（PC port setup）	Auto Negotiate 1000 フル（10 Full） 100 ハーフ（100 Half） 10 ハーフ（100 Half） 10 フル（10 Full）	コンピュータ（アクセス）ポートの速度とデュプレックス。 す。 • [自動ネゴシエーション（Auto Negotiate）]（デフォル • [1000 フル（1000 Full）]：1000-BaseT/全二重 • [100 ハーフ（100 Half）]：100-BaseT/半二重 • [100 フル（100 Full）]：100-BaseT/全二重 • [10 ハーフ（10 Half）]：10-BaseT/半二重 • [10 フル（10 Full）]：10-BaseT/全二重 電話機がスイッチに接続されている場合は、スイッチ上のポ 定するか、両方を自動ネゴシエーションに設定します。 このフィールドを変更する場合には、ネットワーク設定オプ さい。 この設定値を変更する場合は、[SW ポート設定（SW ンを同じ設定値に変更する必要があります。 複数の電話機の設定を同時に行うには、[エンタープライズ Configuration）] ウィンドウ（**[システム（System）] > [エン** （**Enterprise Phone Configurations**）]）で [リモートポート設 を有効化します。 Cisco Unified Communications Manager で [リモート ポート設定 にポートが設定されている場合は、電話機でデータを変更

IPv4 フィールド

表 21 : [IPv4 のセットアップ（IPv4 Setup）] メニューのオプション

エントリー	説明
DHCP を使う（DHCP Enabled）	電話機の DHCP が有効か無効かを示します。 DHCP が有効な場合、DHCP サーバによって電話機に IP アドレスが割り当てられます。DHCP が無効な場合、管理者が、電話機に手動で IP アドレスを割り当てる必要があります。 詳細については、DHCP を使用するための電話機のセットアップ （69 ページ）およびDHCP を使用しないための電話機のセットアップ （70 ページ）を参照してください。
IP アドレス（IP Address）	電話機のインターネット プロトコル（IP）アドレス。 IP アドレスをこのオプションで割り当てる場合は、サブネットマスクとデフォルトルータも割り当てる必要があります。 この表の [サブネット マスク（Subnet Mask）] オプションと [デフォルト ルータ（Default Router）] オプションを参照してください。

エントリー	説明
サブネット マスク（Subnet Mask）	電話機で使用されるサブネット マスク。
Default Router	電話機で使用される、デフォルト ルータ。
DNS サーバ 1 DNS Server 2 DNS Server 3	電話機で使用されるプライマリ DNS サーバ（[DNS サーバ 1（DNS Server 1）]）およびオプションのバックアップ DNS サーバ（[DNS サーバ 2（DNS Server 2）] ～ [DNS サーバ 3（DNS Server 3）]）。
代替 TFTP（Alternate TFTP）	電話機が代替 TFTP サーバを使用しているかどうかを示します。
TFTP サーバ 1（TFTP Server 2）	電話機で使用される、プライマリの Trivial File Transfer Protocol（TFTP）サーバ。 ネットワークで DHCP を使用していない場合、このサーバを変更するには [TFTP サーバ 1（TFTP Server 1）] オプションを使用する必要があります。 [代替 TFTP（Alternate TFTP）] オプションを [オン（On）] に設定した場合は、[TFTP サーバ 1（TFTP Server 1）]オプションに 0 以外の値を入力する必要があります。 プライマリ TFTP サーバもバックアップ TFTP サーバも、電話機の CTL ファイルまたは ITL ファイルに記述されていない場合は、[TFTP サーバ 1（TFTP Server 1）] オプションの変更内容を保存する前に、これらのファイルをロック解除する必要があります。 この場合、[TFTP サーバ 1（TFTP Server 1）] オプションへの変更を保存すると、ファイルは削除されます。 新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 1 アドレスからダウンロードされます。 電話機が TFTP サーバを探すとき、プロトコルに関係なく、手動で割り当てられた TFTP サーバが優先されます。 IPv6 と IPv4 の両方の TFTP サーバが設定に含まれる場合、電話機は、手動で割り当てられた IPv6 TFTP サーバおよび IPv4 TFTP サーバを優先することによって、TFTP サーバを探す順序の優先順位を決定します。 電話機は、次の順序で TFTP サーバを探します。 **1.** 手動で割り当てられた IPv4 TFTP サーバ **2.** 手動で割り当てられた IPv6 サーバ **3.** DHCP が割り当てられた TFTP サーバ **4.** DHCPv6 が割り当てられた TFTP サーバ （注） CTL ファイルおよび ITL ファイルの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

エントリー	説明
TFTP サーバ 2（TFTP Server 2）	プライマリの TFTP サーバが使用不能の場合に、電話機で使用されるオプションのバックアップ TFTP サーバ。 プライマリ TFTP サーバもバックアップ TFTP サーバも、電話機の CTL ファイルまたは ITL ファイルに記述されていない場合は、[TFTP サーバ 2（TFTP Server 2）] オプションの変更内容を保存する前に、これらのファイルのいずれかをロック解除する必要があります。 この場合、[TFTP サーバ 2（TFTP Server 2）] オプションへの変更を保存すると、ファイルのいずれかは削除されます。 新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 2 アドレスからダウンロードされます。 CTL ファイルまたは ITL ファイルのロックを解除し忘れた場合、どちらかのファイルで TFTP サーバ 2 アドレスを変更した後、[セキュリティ設定（Security Configuration）] メニューから [削除（Erase）] を押すことによって、それらのファイルを削除できます。 新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 2 アドレスからダウンロードされます。 電話機が TFTP サーバを探すとき、プロトコルに関係なく、手動で割り当てられた TFTP サーバが優先されます。 IPv6 と IPv4 の両方の TFTP サーバが設定に含まれる場合、電話機は、手動で割り当てられた IPv6 TFTP サーバおよび IPv4 TFTP サーバを優先することによって、TFTP サーバを探す順序の優先順位を決定します。 電話機は、次の順序で TFTP サーバを探します。 **1.** 手動で割り当てられた IPv4 TFTP サーバ **2.** 手動で割り当てられた IPv6 サーバ **3.** DHCP が割り当てられた TFTP サーバ **4.** DHCPv6 が割り当てられた TFTP サーバ （注） CTL または ITL ファイルの詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。
BOOTP Server	電話機が IP アドレスを DHCP サーバではなく BOOTP サーバから受信するかどうかを示します。
DHCP アドレス解放（DHCP Address Released）	DHCP で割り当てられた IP アドレスを解放します。 このフィールドは DHCP が有効な場合に編集できます。 VLAN から電話機を削除して、再割り当てのために電話機の IP アドレスを解放する場合は、このオプションを [はい（Yes）] に設定し、[適用（Apply）] を押します。

IPv6 フィールド

IPv6 セットアップ オプションをデバイスで設定する前に、IPv6 を Cisco Unified Communication Administration で有効化し、設定する必要があります。次のデバイス設定フィールドが IPv6 設定に適用されます。

- IP アドレッシング モード（IP Addressing Mode）
- シグナリング用の IP アドレッシングモード設定（IP Addressing Mode Preference for Signalling）

IPv6 が Unified クラスタで有効な場合、IP アドレッシング モードのデフォルト設定は [IPv4 と IPv6（IPv4 and IPv6）] です。このアドレッシング モードでは、電話機が 1 つの IPv4 アドレスと 1 つの IPv6 アドレスを取得して使用します。メディアの必要に応じて IPv4 および IPv6 アドレスを使用できます。電話機は、コール制御シグナリングに IPv4 または IPv6 のいずれかのアドレスを使用します。

IPv6 の展開の詳細については、『IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0』を参照してください。

IPv6 は、次のメニューのいずれかからセットアップします。

- Wi-Fi が無効になっている場合：**[イーサネットのセットアップ（Ethernet Setup）]**>**[IPv6 のセットアップ（IPv6 Setup）]**
- WiFi が有効になっている場合：**[Wi-Fi クライアントのセットアップ（Wi-Fi client setup）]**>**[IPv6 のセットアップ（IPv6 Setup）]**

電話機のキーパッドを使用して、IPv6 アドレスを入力または編集します。コロンを入力するには、キー パッドのアスタリスク（*）を押します。16 進数の a、b、c を入力するには、キー パッドの 2 を押し、スクロールして数字を選んでから、Enter を押します。16 進数の d、e、f を入力するには、キー パッドの 3 を押し、スクロールして数字を選んでから、Enter を押します。

次の表は、[IPv6] メニューにある IPv6 関連情報について説明します。

表 *22 : [IPv6* のセットアップ（*IPv6 Setup*）*]* メニューのオプション

エントリー	デフォルト値	説明
DHCPv6 有効（DHCPv6 Enabled）	はい	電話機で IPv6 専用アドレスを取得 DHCPv6 が有効の場合、電話機は I DHCPv6 サーバから IPv6 アドレス サーバからの）またはステートレス

エントリー	デフォルト値	説明
IPv6 アドレス	::	電話機の現在の IPv6 専用アドレ 有効な IPv6 アドレスはサブネッ 式がサポートされます。 • コロンによって区切られた • 圧縮形式では、ゼロ グルー このオプションを使用して IP ア 割り当てる必要があります。
IPv6 プレフィックス長（IPv6 Prefix Length）	0	サブネットの現在のプレフィッ ます。 サブネット プレフィックス長は
IPv6デフォルトルータ	::	電話機で使用されるデフォルト ことができます。
IPv6 DNS サーバ 1（IPv6 DNS Server 1）	::	電話機で使用されるプライマリ す。
IPv6 DNS サーバ 2（IPv6 DNS Server 1）	::	電話機で使用されるセカンダリ することができます。
IPv6 代替 TFTP（IPv6 Alternate TFTP）	不可	ユーザが代替（セカンダリ）IPv
IPv6 TFTP サーバ 1（IPv6 TFTP Server 1）	::	電話機で使用されるプライマリ りすることができます。
IPv6 TFTP サーバ 2（IPv6 TFTP Server 2）	::	（任意）プライマリ IPv6 TFTP ユーザに新しいセカンダリ TFT
IPv6 アドレス解放（IPv6 Address Released）	不可	ユーザが IPv6 関連情報を解放て

DHCP を使用するための電話機のセットアップ

DHCP を有効にして、DHCP サーバが自動的に IP アドレスを Cisco IP 電話に割り当て、TFTP サーバに電話を転送できるようにするには、次の手順を実行します。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Admin Settings）]** > **[ネットワークのセットアップ（Network Setup）]** > **[イーサネットのセットアップ（Ethernet Setup）]** > **[IPv4のセットアップ（IPv4 Setup）]** を選択します。

ステップ 3 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、デフォルトでは有効になっています。

ステップ 4 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かどうかを、ネットワーク管理者に相談してください。

ステップ 5 [適用（Apply）]を押します。

DHCP を使用しないための電話機のセットアップ

DHCP を使用しない場合は、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。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Admin Settings）]** > **[ネットワークのセットアップ（Network Setup）]** > **[イーサネットのセットアップ（Ethernet Setup）]** > **[IPv4のセットアップ（IPv4 Setup）]** を選択します。

ステップ 3 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。

ステップ 4 [適用（Apply）]を押します。

ロード サーバ

ロードサーバは、電話機ファームウェアアップグレードのインストール時間を最適化し、WAN の負荷を軽減するために使用されます。これは、イメージをローカルに保存することによって、電話機の各アップグレードが WAN リンクを通過する必要性を排除することで実現されます。

ロード サーバには、電話機のアップグレードに使用するファームウェアを取得する（TFTP サーバ 1 または TFTP サーバ 2 以外の）別の TFTP サーバの IP アドレスまたは名前を設定できます。 [ロード サーバ（Load Server）] オプションを設定すると、電話機は、ファームウェア アップグレードのために指定されたサーバと通信します。

（注） [ロードサーバ（Load Server）] オプションでは、電話機のアップグレード用の代替 TFTP サーバのみを指定できます。 電話機は引き続き TFTP サーバ 1 または TFTP サーバ 2 を使用して、設定ファイルを取得します。 [ロード サーバ（Load Server）] オプションでは、プロセスの管理およびファイルの管理（ファイルの転送、圧縮、削除など）を行いません。

ロード サーバは、[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウから設定します。 Cisco Unified Communications Manager の管理から、[デバイス（Device）]> [電話（Phone）]> [エンタープライズ電話の設定（Enterprise Phone Configuration）]を選択します。

電話機の起動確認

Cisco IP 電話 を電源に接続すると、次の手順が繰り返され、電話機の起動診断プロセスが開始されます。

1. 起動時のさまざまな段階で、電話機がハードウェアをチェックする間、機能ボタンとセッション ボタンがオレンジ色に点滅し、続いて緑色に点滅します。
2. メイン画面に「Cisco Unified Communications Manager への登録（`Registering to Cisco Unified Communications Manager`）」と表示されます。

電話機がこれらの段階を正常に完了すると、正常に起動し、選択されるまで **[選択（Select）]** ボタンが点灯します。

ユーザの電話サービスの設定

ユーザが IP フォンの Cisco IP 電話 サービスにアクセスできるように設定することができます。また、さまざまな電話のサービスにボタンを割り当てることも可能です。 これらのサービスは、テキストと画像によるインタラクティブ コンテンツを電話機に表示するための XML アプリケーションとシスコ署名付き Java MIDlet を含んでいます。 IP フォンは各サービスを個別のアプリケーションとして管理します。 サービスの例としては、映画の上映時刻、株式相場、天気予報などがあります。

ユーザがサービスにアクセスできるようにするには、前もって次の作業が必要です。

- Cisco Unified Communications Manager Administration を使用して、デフォルトで提供されないサービスを設定する必要があります。

- ユーザがCisco Unified Communications セルフケアポータルを使用してサービスを登録する必要があります。 この Web ベース アプリケーションは、IP フォンのアプリケーションをエンド ユーザが設定するための限定的なグラフィカル ユーザ インターフェイス（GUI）を提供します。 ただし、エンタープライズ登録として設定するサービスにユーザは登録できません。

詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。

サービスを設定する前に、設定するサイトの URL アドレスをすべて入手し、ユーザが社内 IP テレフォニー ネットワークからこれらのサイトにアクセスできるかどうかを確認してください。 このアクティビティは、シスコが提供するデフォルト サービスには適用されません。

手順

ステップ 1 Cisco Unified Communications Manager Administrationで、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [IP Phone サービス（Phone Services）]** を選択します。

ステップ 2 ユーザがCisco Unified Communications セルフケアポータルにアクセスでき、そこから設定済みのサービスを選択して登録できることを確認します。

エンド ユーザに提供する必要がある情報については、セルフケアポータルの管理 （91 ページ）を参照してください。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

ユーザの電話モデルを変更

ユーザは、ユーザの電話機モデルを変更できます。 この変更は、次のようにいくつかの理由で必要になる場合があります。

- Cisco Unified Communications Manager (ユニファイド CM) を電話機モデルをサポートしていないソフトウェアバージョンに更新しました。
- ユーザは、現在のモデルからの別の電話機モデルが必要です。
- 電話機を修理または交換する必要があります。

Unified CM は、古い電話機を識別し、古い電話機の MAC アドレスを使用して古い電話機の設定を識別します。 Unified CM によって、古い電話機の設定が新しい電話機のエントリにコピーされます。 その後、新しい電話機は古い電話機と同じ設定になります。

SCCP ファームウェアを含む古い電話をCisco IP 電話 8800 シリーズ でモデルに変更した場合、新しい電話機はセッション回線モード用に設定されます。

古い電話機にキー拡張モデルが設定されている場合、Unified CM は新しい電話機に同時に拡張モジュール情報をコピーします。ユーザが互換性のあるキー拡張モジュールを新しい電話機に接続すると、新しい拡張モジュールによって移行済み拡張モジュールの情報が取得されます。

旧電話機にキー拡張モデルが設定されていて、新しい電話機が拡張モジュールをサポートしていない場合、Unified CM は 拡張モジュールの情報をコピーしません。

制限（Limitation）：古い電話機が新しい電話よりも多くの回線または回線ボタンを使用している場合は、新しい電話機に追加回線や回線ボタンは設定されません。

設定が完了すると、電話機が再起動します。

始める前に

*Feature Configuration Guide for Cisco Unified Communications Manager*にしたがって、Cisco Unified Communications Managerをセットアップします。

ファームウェアリリース 12.8 (1) 以降に、新しい、使用されていない電話機がプレインストールされている必要があります。

手順

ステップ 1 古い電話機の電源をオフにします。

ステップ 2 新しい電話機の電源を入れます。

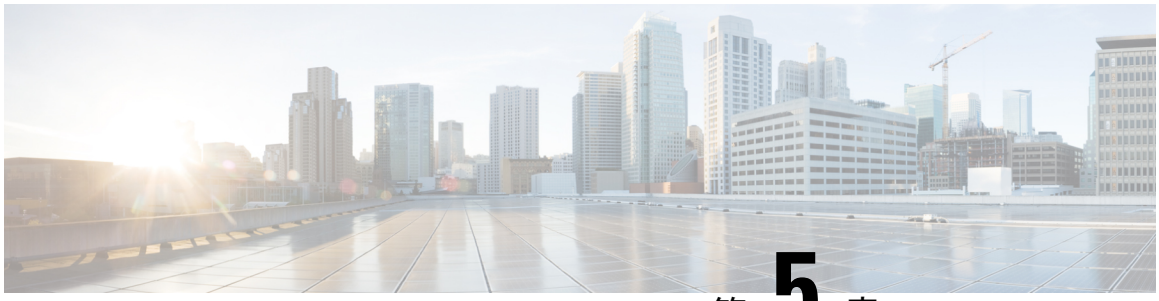
ステップ 3 新しい電話機で、**[既存の電話を置き換える (Replace)]** を選択します。

ステップ 4 古い電話機のプライマリ内線番号を入力します。

ステップ 5 古い電話機に暗証番号が割り当てられている場合は、暗証番号を入力します。

ステップ 6 [送信（Submit）]を押します。

ステップ 7 ユーザに複数のデバイスが存在する場合は、置き換えるデバイスを選択して**[続行 (Continue)]** を押します。



第 5 章

Cisco Unified Communications Manager での電話機の設定

Cisco IP 電話のセットアップ

自動登録が有効ではなく、電話機が Cisco Unified Communications Manager データベースに存在しない場合、Cisco Unified Communications Manager の管理で Cisco IP 電話 を手動で設定する必要があります。 この手順の一部のタスクは、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。

Cisco Unified Communications Manager の詳細な管理方法については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco Unified Communications Manager の管理ページを使用して、次の手順で設定を実行してください。

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、電話機能、IP 電話サービス、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

この情報では、電話機をセットアップするための設定要件のリストを示します。また、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などの前提的な設定作業を特定します。

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。

ステップ 3 （必要に応じて）回線ボタン、スピードダイヤル ボタン、サービス URL ボタンを変更して、電話ボタンテンプレートカスタマイズします。**[デバイス（Device）]**>**[デバイス設定（Device Settings）]** > **[電話ボタン テンプレート（Phone Button Template）]** を選択して、テンプレートの作成と更新を行います。

プライバシー、すべてのコール、モビリティ ボタンを追加して、ユーザのニーズに対応します。

詳細については、電話ボタン テンプレート （225 ページ） を参照してください。

ステップ 4 デバイス プールを定義します。 **[システム（System）]** > **[デバイス プール（Device Pool）]** を選択します。

デバイス プールは、デバイスに共通の特性（リージョン、日時グループ、ソフトキー テンプレート、および MLPP 情報など）を定義します。

ステップ 5 共通の電話プロファイルを定義します。 **[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[共通の電話プロファイル（Common Phone Profile）]** の順に選択します。

共通の電話プロファイルは Cisco TFTP サーバが要求するデータとともに、サイレント オプションおよび機能制御オプションなど、共通の電話の設定を提供します。

ステップ 6 コーリング サーチ スペースを定義します。 Cisco Unified Communications Manager の管理ページで、**[コール ルーティング（Call Routing）]** > **[コントロールのクラス（Class of Control）]** > **[コーリング サーチ スペース（Calling Search Space）]** をクリックします。

コーリング サーチ スペースは、着信番号のルーティング方法を決定するために検索されるパーティションのコレクションです。デバイス用のコーリング サーチ スペースと電話番号用のコーリング サーチ スペースは併用することができます。 電話番号の CSS は、デバイスの CSS に優先します。

ステップ 7 デバイス タイプおよびプロトコルのセキュリティ プロファイルを設定します。 **[システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）]** を選択します。

ステップ 8 [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。

この手順は、デバイスをデフォルトの設定で Cisco Unified Communications Manager データベースに追加します。

[プロダクト固有の設定（Product Specific Configuration）] フィールドについては、「?」 ボタンヘルプ（[電話の設定（Phone Configuration）] ウィンドウ内）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、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

ステップ 9 [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。

この手順では、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。

（注） プライマリ電話番号を設定していない場合、ユーザの電話機に `Unprovisioned` のメッセージが表示されます。

ステップ 10 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。

ユーザは、Cisco Unified Communications セルフ ケア ポータルを使用することで、スピード ダイヤルの設定値を電話機上で変更できます。

ステップ 11 Cisco Unified IP 電話 サービスを設定し、IP Phone サービスを提供するサービス（任意）を割り当てます。

ユーザは、Cisco Unified Communications セルフ ケア ポータルを使用して、電話機のサービスを追加または変更できます。

（注） ユーザが IP 電話サービスに登録できるのは、Cisco Unified Communications Manager の管理ページで IP 電話のサービスを最初に設定したときに、[エンタープライズ登録（Enterprise Subscription）] チェックボックスをオフにしている場合だけです。

（注） シスコが提供する一部のデフォルト サービスは、エンタープライズ登録に分類されているため、ユーザはそれらをセルフ ケア ポータルから追加することはできません。 このサービスは電話機にデフォルトで実装されているため、Cisco Unified Communications Manager の管理ページで無効にした場合に限り電話機から削除できます。

ステップ 12 IP 電話のサービスや URL へのアクセスを提供するために、プログラム可能なボタン（オプション）にサービスを割り当てます。

ステップ 13 必須フィールドを設定して、ユーザ情報を追加します。フィールド名の隣のアスタリスク（*）は必須フィールドを示します。たとえば、ユーザー ID と姓です。この手順により、Cisco Unified Communications Manager のグローバルディレクトリにユーザー情報が追加されます。

（注） パスワード（セルフケア ポータルの場合）と PIN（Cisco Extension Mobility またはパーソナル ディレクトリの場合）を割り当てます。

（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。

（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、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

ステップ 14 ユーザをユーザ グループに関連付けます。 この手順では、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。 たとえば、ユーザをシスコの標準 CCM エンド ユーザ グループに追加する必要があります。こうすると、ユーザが Cisco Unified Communications Manager のセルフ ケア ポータルにアクセスできるようになります。

ステップ 15 ユーザを電話機に割り当てます（任意）。 この手順では、コールの転送、スピード ダイヤル番号やサービスの追加などについて、ユーザが電話機を制御できるようにします。

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。

ステップ 16 [エンドユーザの設定（End User Configuration）] ウィンドウが表示されていない場合は、**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択して、設定の最後の作業を行います。[検索（Search）] フィールドと [検索（Find）]を使用してユーザ（例：John Doe）を見つけた後、ユーザ ID をクリックして、そのユーザの [エンド ユーザの設定（End User Configuration）] ウィンドウを開きます。

ステップ 17 画面の [電話番号の割り当て（Directory Number Associations）] 領域で、ドロップダウン リストからプライマリ内線を設定します。

ステップ 18 [モビリティ情報（Mobility Information）] 領域で、[モビリティの有効化（Enable Mobility）] ボックスをオンにします。

ステップ 19 [権限情報（Permissions Information）] 領域で、[ユーザ グループ（User Group）] ボタンを使用して、このユーザを任意のユーザ グループに追加します。

たとえば、「標準 CCM エンドユーザ グループ」として定義されたグループに、ユーザを追加することができます。

ステップ 20 設定されているすべてのユーザ グループを表示するには、**[ユーザ管理（User Management）] > [ユーザ グループ（User Groups）]** の順に選択します。

ステップ 21 [エクステンション モビリティ（Extension Mobility）] 領域で、ユーザがクラスタ間のエクステンション モビリティ サービスを許可している場合は、[クラスタ間のエクステンション モビリティの有効化（Enable Extension Mobility Cross Cluster）] チェックボックスをオンにします。

ステップ 22　**保存**を選択します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

電話機の MAC アドレスの決定

Cisco Unified Communications Manager に電話機を追加するには、電話機の MAC アドレスを決定する必要があります。

手順

次のいずれかの操作を実行します。

- 電話機の [アプリケーション（Applications）] を押し、[電話の情報（Phone Information）] を選択して、[MAC アドレス（MAC Address）] フィールドを確認する。
- 電話機の背面にある MAC ラベルを確認する。
- 電話機の Web ページを表示し、[デバイス情報（Device Information）]を選択する。

電話機の追加方法

Cisco IP 電話をインストールしたら、次のオプションの 1 つを選択して、電話機を Cisco Unified Communications Manager データベースに追加できます。

- Cisco Unified Communications Manager の管理で個別に電話機を追加する
- 一括管理ツール（BAT）を使用して複数の電話を追加する
- 自動登録
- BAT と Tool for Auto-Registered Phones Support（TAPS）

個別に、または BAT を使用して電話機を追加する前に、電話機の MAC アドレスが必要です。詳細については、電話機の MAC アドレスの決定 （79 ページ） を参照してください。

一括管理ツールの詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

電話機の個別の追加

Cisco Unified Communications Manager に追加する電話機の MAC アドレスおよび電話機情報を収集します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、**[デバイス（Device）] > [電話（Phone）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 電話機のタイプを選択します。

ステップ 4 [次へ（Next）]を選択します。

ステップ 5 MAC アドレスを含む電話機の情報を入力します。

Cisco Unified Communications Manager の手順の詳細と概要については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

ステップ 6 **保存**を選択します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

BAT 電話テンプレートを使用した電話機の追加

Cisco Unified Communications 一括管理ツール（BAT）を使用すると、複数の電話機の登録などのバッチ操作を実行できます。

（TAPS と組み合わせずに）BAT だけを使用して電話機を追加するには、各電話機の適切な MAC アドレスを取得する必要があります。

BAT の使用の詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

ステップ 1 Cisco Unified Communications Administration から、**[一括管理（Bulk Administration）] > [電話（Phones）] > [電話テンプレート（Phone Template）]** の順に選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [電話のタイプ（Phone Type）] を選択し、[次へ（Next）]をクリックします。

ステップ 4 [デバイス プール（Device Pool）]、[電話ボタン テンプレート（Phone Button Template）]、[デバイス セキュリティ プロファイル（Device Security Profile）] など、電話固有の詳細なパラメータを入力します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 BAT 電話テンプレートを使用して電話機を追加するには、**[デバイス（Device）] > [電話（Phone）] > [新規追加（Add New）]** を選択します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

Cisco Unified Communications Manager におけるユーザーの追加

Cisco Unified Communications Manager に登録されているユーザに関する情報を表示および管理できます。 また、Cisco Unified Communications Manager で各ユーザは次のタスクを実行できます。

- Cisco IP 電話 から、社内ディレクトリや他のカスタマイズ済みディレクトリにアクセスする。
- パーソナル ディレクトリを作成する。
- 短縮ダイヤルとコール転送の番号をセットアップする。
- Cisco IP 電話 からアクセスできるサービスに登録する。

手順

ステップ 1 ユーザを個別に追加するには、Cisco Unified Communications Manager にユーザを直接追加する（82 ページ）を参照してください。

ステップ 2 ユーザを一括して追加するには、一括管理ツールを使用します。 この方法では、すべてのユーザに対して同一のデフォルト パスワードを設定することもできます。

詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

外部 LDAP ディレクトリからのユーザーの追加

ユーザを LDAP ディレクトリ（Cisco Unified Communications Server ではないディレクトリ）に追加した場合、LDAP ディレクトリと、ユーザおよびその電話機が追加される Cisco Unified Communications Manager を即時に同期できます。

（注） LDAP ディレクトリを Cisco Unified Communications Manager と即時に同期しない場合は、[LDAP ディレクトリ（LDAP Directory）] ウィンドウの [LDAPディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] で、次回の自動同期化スケジュールを決定できます。 新規ユーザをデバイスに関連付けるには、その前に同期を完了しておく必要があります。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページにサイン インします。

ステップ 2 **[システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）]** を選択します。

ステップ 3 [検索（Find）]を使用して LDAP ディレクトリを見つけます。

ステップ 4 LDAP ディレクトリ名をクリックします。

ステップ 5 **[Perform Full Sync Now（完全同期を今すぐ実施）]** をクリックします。

Cisco Unified Communications Manager にユーザを直接追加する

Lightweight Directory Access Protocol（LDAP）ディレクトリを使用しない場合、次の手順に従って、Cisco Unified Communications Manager Administration で直接ユーザを追加することができます。

（注） LDAP が同期している場合、ユーザを Cisco Unified Communications Manager の管理ページに追加できません。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、**[ユーザ管理（User Management）] > [エンドユーザ（End User）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ユーザ情報（User Information）] ペインで、次の情報を入力します。

- ユーザー ID：エンドユーザ認証名を入力します。Cisco Unified Communications Manager では作成後のユーザー ID の変更は許可されません。 姓に使用できる特殊文字は、=、+、<, >、#、;、\、「」、および空白です。 **例**：johndoe
- [パスワード（Password）] および [パスワードの確認（Confirm Password）]：エンド ユーザのパスワードとして、5 文字以上の英数字または特殊文字を入力します。 姓に使用できる特殊文字は、=、+、<, >、#、;、\、「」、および空白です。

- 姓：エンドユーザの姓を入力します。使用できる特殊文字: =, +,<, >, #, ;, \,,「」、および空白スペースです。 **例**：doe
- [電話番号（Telephone Number）]：エンド ユーザのプライマリ電話番号を入力します。 エンドユーザは、電話機に複数の回線を接続できます。 **例**：26640（John Doe の社内電話番号）

ステップ 4 **[保存]** をクリックします。

エンド ユーザ グループにユーザを追加する

ユーザを Cisco Unified Communications Manager の標準エンドユーザ グループに追加するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページから、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[アクセス コントロール グループ（Access Control Group）]** を選択します。

[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索（Find）]をクリックします。

ステップ 3 [標準 CCM エンド ユーザ（Standard CCM End Users）]リンクを選択します。 対象の標準 CCM エンドユーザについての [ユーザ グループの設定（User Group Configuration）] ウィンドウが表示されます。

ステップ 4 [グループにエンド ユーザを追加（Add End Users to Group）]を選択します。 [ユーザの検索と一覧表示（Find and List Users）] ウィンドウが表示されます。

ステップ 5 [ユーザの検索（Find User）] ドロップダウン リスト ボックスを使用して、追加するユーザを探し、[検索（Find）]をクリックします。

検索条件に一致するユーザのリストが表示されます。

ステップ 6 表示されるレコードのリストで、このユーザ グループに追加するユーザのチェックボックスをクリックします。 リストが長い場合は、下部のリンクを使用すると、さらに多くの結果を表示できます。

（注） 検索結果のリストには、すでにそのユーザ グループに属しているユーザは表示されません。

ステップ 7 [選択項目の追加（Add Selected）]を選択します。

電話機とユーザの関連付け

Cisco Unified Communications Manager の [エンド ユーザ（End User）] ウィンドウから、電話機をユーザに関連付けます。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページから、**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** の順に選択します。

[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索（Find）]をクリックします。

ステップ 3 表示されるレコードのリストで、ユーザのリンクを選択します。

ステップ 4 [デバイスの割り当て（Device Associations）]を選択します。

[ユーザデバイス割り当て（User Device Association）] ウィンドウが表示されます。

ステップ 5 適切な検索条件を入力し、[検索（Find）]をクリックします。

ステップ 6 デバイスの左にあるボックスをオンにして、ユーザに関連付けるデバイスを選択します。

ステップ 7 [選択/変更の保存（Save Selected/Changes）]を選択して、デバイスをユーザに関連付けます。

ステップ 8 ウィンドウの右上にある [関連リンク（Related Links）] ドロップダウン リストから、[ユーザの設定に戻る（Back to User）] を選択し、[移動（Go）]をクリックします。

[エンド ユーザの設定（End User Configuration）] ウィンドウが表示され、選択した関連付けられたデバイスが [制御するデバイス（Controlled Devices）] ペインに表示されます。

ステップ 9 [選択/変更の保存（Save Selected/Changes）]を選択します。

Survivable Remote Site Telephony

Conference Bridge Setup（SRST）機能は、WAN 接続が失われた場合にも、基本的な電話機の機能を提供します。このシナリオでは、電話機は進行中のコールをアクティブなまま保持し、ユーザは使用可能な機能のサブセットにアクセスできます。フェールオーバーが発生すると、ユーザの電話機にアラート メッセージが表示されます。

サポートされているファームウェアおよび Survivable Remote Site Telephony に関する詳細は、Cisco.com の「*Cisco Unified Survivable Remote Site Telephony Compatibility Information*」のページ（http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html）を参照してください。

次の表は、フェールオーバー中の機能の利用可能性について説明します。

表 *23 : SRST* 機能のサポート

機能	サポートあり	注
発信	はい	
終了	はい	
リダイヤル	はい	
回答	はい	
保留	はい	
再開	はい	
会議	はい	
アクティブ コールへの会議（参加）	なし	[アクティブコール（Active Calls）] ソフトキーは表示されません。
会議リスト	なし	
転送	はい	
アクティブ コールへの転送（直接転送）	なし	
自動応答	はい	
コール待機	はい	
発信者 ID	はい	
オーディオ メッセージ受信インジケータ	はい	
すべてのコールのプログラマブル回線キー	はい	
応答のプログラマブル回線キー	はい	
統合セッション表示	はい	他の機能により制限されるため、会議が唯一サポートされている機能です。
ボイスメール	はい	ボイスメールは Cisco Unified Communications Manager クラスタの他のユーザと同期されません。

機能	サポートあり	注
不在転送	はい	転送ステートはSRSTモードにシェアド ライン アピアランスがないため転送を設定する電話機でのみ使用できます。[すべてのコールの転送（Call Forward All）] 設定は、Cisco Unified Communications Manager から SRST へのフェールオーバーまたはSRSTからCommunications Manager へのフェールバックには保存されません。Communications Manager で引き続きアクティブな元の [すべてのコールの転送（Call Forward All）] は、フェールオーバー後にデバイスがCommunications Manager に再接続されると表示される必要があります。
短縮ダイヤル	はい	
サービス IRL プログラマブル回線キー	はい	
ボイスメールへ（即転送）	なし	[即転送（iDivert）] ソフトキーは表示されません。
回線フィルタ	一部	回線はサポートされますが、共有できません。
パーク モニタリング	なし	[パーク（Park）] ソフトキーが表示されません。
割込み	なし	[割り込み（Barge）] ソフトキーは表示されません。
拡張メッセージ待機インジケータ	なし	メッセージ数のバッジは、電話スクリーンに表示されません。 [メッセージ受信（Message Waiting）] アイコンのみが表示されます。
ダイレクト コール パーク	なし	ソフトキーは表示されません。
BLF	一部	BLF 機能キーはスピード ダイアル キーのように動作します。
保留復帰	なし	コールは、無期限で保留状態になります。

機能	サポートあり	注
リモート回線の保留	なし	コールは、内線保留コールとして表示されます。
ミートミー	なし	[ミートミー（Meet Me）] ソフトキーが表示されません。
ピックアップ	なし	ソフトキーを押しても何も実行されません。
グループ ピックアップ	なし	ソフトキーを押しても何も実行されません。
その他のグループ ピックアップ	なし	ソフトキーを押しても何も実行されません。
迷惑呼 ID	なし	ソフトキーを押しても何も実行されません。
QRT	なし	ソフトキーを押しても何も実行されません。
ハント グループ	なし	ソフトキーを押しても何も実行されません。
インターコム	なし	ソフトキーを押しても何も実行されません。
モビリティ	なし	ソフトキーを押しても何も実行されません。
プライバシー	なし	ソフトキーを押しても何も実行されません。
折り返し	なし	[折返し（Call Back）] ソフトキーが表示されません。
ビデオ	はい	ビデオ会議はサポートされません。
ビデオ	はい	ビデオ会議はサポートされません。
共有回線	なし	
BLF スピードダイヤル	はい	

Enhanced Survivable Remote Site Telephony

Enhanced Survivable Remote Site Telephony （E-SRST）機能は、WAN 接続が失われても、追加の電話機の機能へは引き続きアクセスできるようにします。Survivable Remote Site Telephony(SRST) によってサポートされている機能の他に、E-SRST は以下をサポートしています。

- 共有回線
- ビジー ランプ フィールド（BLF ）
- ビデオ コール

サポートされているファームウェアおよび Survivable Remote Site Telephony に関する詳細は、Cisco.com の「*Cisco Unified Survivable Remote Site Telephony Compatibility Information*」のページ（http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-device-support-tables-list.html）を参照してください。

アプリケーション ダイヤル ルール

アプリケーション ダイヤル ルールは、携帯電話の連絡先共有番号をネットワークでダイヤル可能な番号へ変換するために使用されます。 アプリケーション ダイヤル ルールは、ユーザが番号を手動でダイヤルしている時、もしくはユーザによってコールが発信される前に番号が編集された場合は、適用されません。

アプリケーション ダイヤル ルールがCisco Unified Communications Managerに設定されます。

ダイヤル ルールの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』「の「Configure Dial Rules」」の章を参照してください。

アプリケーション ダイヤル ルールの設定

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[コール ルーティング（Call Routing）]**>**[ダイヤル ルール（Dial Rules）]**>**[アプリケーション ダイヤル ルール（Application Dial Rules）]** に移動します。

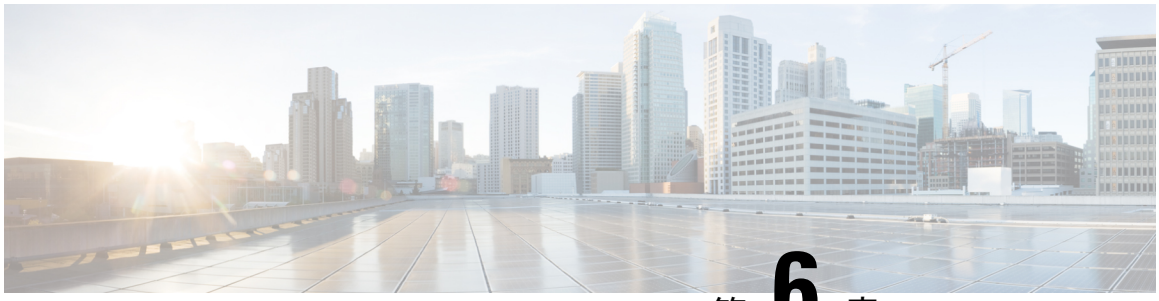
ステップ 2 [新規追加（Add New）] をクリックして新しいアプリケーション ダイヤル ルールを作成するか、既存のアプリケーション ダイヤル ルールを選択して編集します。

ステップ 3 次のフィールドに入力します。

- [名前（Name）]：ダイヤルルールの一意の名前を入力します。名前には最長 20 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、アンダースコア（_）を任意に組み合わせて使用できます。

- [説明（Description）]：このフィールドには、ダイヤルルールの簡単な説明を入力します。
- [開始番号（Number BeginsWith）]：このアプリケーション ダイヤル ルールを適用するディレクトリ番号の先頭部分の数字を入力します。
- [桁数（Number ofDigits）]：この必須フィールドには、アプリケーション ダイヤル ルールを適用するディレクトリ番号の先頭部分の数字を入力します。
- [削除する合計桁数（Total Digitsto be Removed）]：この必須フィールドには、ダイヤル ルールに適用する、Cisco Unified Communications Manager によってディレクトリ番号から削除する桁数を入力します。
- [プレフィックス パターン（Prefix WithPattern）]：この必須フィールドには、アプリケーション ダイヤル ルールに適用する、ディレクトリ番号に付加するパターンを入力します。
- [アプリケーション ダイヤル ルール優先順位（Application Dial RulePriority）]：このフィールドは、[プレフィックス パターン（Prefix With Pattern）] に入力すると表示されます。 アプリケーション ダイヤル ルールの優先順位を設定することができます。

ステップ 4 Cisco Unified Communications Manager を再起動します。



第 6 章

セルフケアポータルの管理

セルフケアポータルの概要

Cisco Unified Communications セルフケアポータルから、電話の機能や設定をカスタマイズし、制御できます。

管理者は、セルフケアポータルへのアクセスを制御します。また、ユーザがセルフケアポータルにアクセスできるように、情報を提供する必要があります。

ユーザーが Cisco Unified Communications セルフケアポータルにアクセスする前に、Cisco Unified Communications Manager Administration を使用してそのユーザーを標準の Cisco Unified Communications Manager エンドユーザグループに追加する必要があります。

エンド ユーザには、必ず、セルフケアポータルに関する次の情報を提供してください。

- アプリケーションにアクセスするための URL。 この URL は、次のとおりです。

  https://<server_name:portnumber>/ucmuser/（server_name は Web サーバーがインストールされているホスト、portnumber はホストのポート番号です）。

- アプリケーションにアクセスするためのユーザー ID とデフォルト パスワード。
- ユーザがポータルを使用して実行できるタスクの概要。

これらの設定値は、ユーザーを Cisco Unified Communications Manager に追加したときに入力した値と同じです。

手順の詳細については、特定のリリースのマニュアルを参照してください。Cisco Unified Communications Manager

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

セルフケアポータルへのユーザのアクセスの設定

セルフケアポータルにアクセスするには、事前にアクセスを許可しておく必要があります。

手順

ステップ 1 Cisco Unified Communications Manager管理で、**[ユーザ管理]** > **[エンドユーザ]** を選択します。
ステップ 2 ユーザを検索します。
ステップ 3 ユーザー ID リンクをクリックします。
ステップ 4 ユーザのパスワードと PIN が設定されていることを確認します。
ステップ 5 [Permissions Information] セクションで、グループ リストに [Standard CCM End Users] が含まれていることを確認します。
ステップ 6 **保存**を選択します。

セルフケアポータルの表示のカスタマイズ

セルフケアポータルにはほとんどのオプションが表示されます。 ただし、Cisco Unified Communications Manager Administration のエンタープライズ パラメータ設定で次のオプションを指定する必要があります。

- Show Ring Settings
- Show Line Label Settings

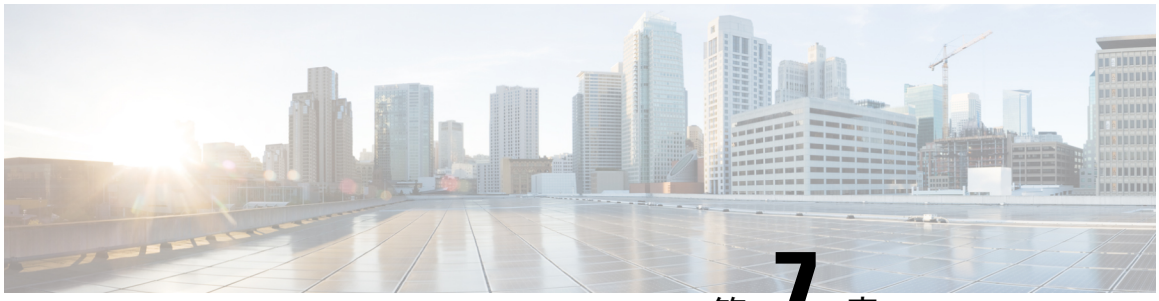
（注） この設定値は、サイトのすべてのセルフケアポータル ページに適用されます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[System]** > **[Enterprise Parameters]** を選択します。
ステップ 2 [Self Care Portal] 領域で、[Self Care Portal Default Server]フィールドを設定します。
ステップ 3 ポータルでユーザがアクセスできるパラメータをイネーブルまたはディセーブルにします。
ステップ 4 **保存**を選択します。

第 III 部

Cisco IP 電話の管理



第 7 章

Cisco IP 電話のセキュリティ

電話ネットワークのセキュリティ強化機能

Cisco Unified Communications Manager 11.5(1) および 12.0(1) では、強化されたセキュリティ環境での動作が可能です。これらの強化機能により、電話ネットワークが、一連の厳密なセキュリティ管理とリスク管理の制御下で動作するようになり、自分自身とユーザが保護されます。

Cisco Unified Communications Manager 12.5 (1)は拡張セキュリティ環境に対応していません。Cisco Unified Communications Manager 12.5 (1)にアップグレードする前に FIPS を無効にすると、TFTP やその他のサービスが正しく機能しなくなります。

強化されたセキュリティ環境には、次の機能が含まれています。

- 連絡先検索認証。
- リモート監査ロギングのデフォルト プロトコルとしての TCP。
- FIPS モード。
- クレデンシャル ポリシーの改善。
- デジタル署名のための SHA-2 ファミリ ハッシュのサポート。
- 512 および 4096 ビットの RSA キー サイズのサポート。

Cisco Unified Communications Manager リリース 14.0 および Cisco IP 電話ファームウェア リリース 14.0 以降では、電話機は SIP OAuth 認証をサポートします。

OAuth は、Cisco Unified Communications Manager リリース 14.0(1) SU1 以降のプロキシ トリビアル ファイル転送プロトコル（TFTP）および Cisco IP 電話ファームウェア リリース 14.1(1) でサポートされます。プロキシ TFTP およびプロキシ TFTP 用の OAuth は、Mobile and Remote Access (MRA) ではサポートされません。

セキュリティ設定に関するその他の情報については、以下を参考にしてください。

- *Cisco Unified Communications Manager* システム設定ガイド、リリース 14.0(1) 以降（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）。
- *Cisco IP* 電話 *7800*および*8800*シリーズのセキュリティの概要 (https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html)
- *Cisco Unified Communications Manager* セキュリティガイド (https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html)

（注） Cisco IP 電話には、限られた数の Identity Trust List（ITL）ファイルのみ保存できます。Cisco Unified Communications Manager が電話機に送信できるファイルの数を制限する必要があるため、電話機の ITL ファイルは最大 64K に制限されています。

サポート対象のセキュリティ機能

セキュリティ機能は、電話機の ID やデータへの脅威など、複数の脅威を防止します。 セキュリティ機能は、電話機と Cisco Unified Communications Manager サーバ間に認証された通信ストリームを確立し、これを維持するとともに、電話機がデジタル署名されたファイルのみ使用することを確認します。

Cisco Unified Communications Manager リリース 8.5(1) 以降のはデフォルトでセキュリティ機能が搭載されており、CTL クライアントを実行しなくても、Cisco IP 電話 に次のセキュリティ機能が提供されます。

- 電話機の設定ファイルの署名
- 電話機の設定ファイルの暗号化
- HTTPS with Tomcat および他の Web サービスの利用

（注） シグナリングおよびメディア機能を保護するには、引き続き、CTL クライアントを実行し、ハードウェア eToken を使用する必要があります。

Cisco Unified Communications Manager システムにセキュリティを実装すると、電話機や Cisco Unified Communications Manager サーバの 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 Unified IP テレフォニー ネットワークは、電話機とサーバの間にセキュアな（暗号化された）通信ストリームを確立し、維持します。ファイルはデジタル署名してから電話機に転送し、Cisco IP 電話 間では、メディア ストリームとコール シグナリングを暗号化します。

認証局プロキシ関数（CAPF）に関連付けられた必要なタスクの実行後、ローカルで有効な証明書（LSC）が電話機にインストールされます。 LSC は Cisco Unified Communications Manager の管理ページで設定できます。詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。 あるいは、電話機の [セキュリティのセットアップ（Security Setup）] メニューから LSC のインストールを開始することもできます。 このメニューでは、LSC の更新および削除も実行できます。

WLAN 認証を使用する EAP-TLS のユーザ証明書として LSC を使用することはできません。

電話機では電話セキュリティ プロファイルを使用します。この中では、デバイスがセキュリティ保護の対象になるかどうかを定義します。 電話へセキュリティ プロファイルを適用する方法の詳細は、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco Unified Communications Manager の管理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、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco IP 電話 8800 シリーズは、連邦情報処理標準（FIPS）に準拠します。 正常に機能するには、FIPS モードで 2048 ビット以上のキー サイズが必要です。 証明書が 2048 ビット未満の場合、電話機は Cisco Unified Communications Manager に登録されず、「電話機を登録できませんでした。 [証明書のキー サイズは FIPS に準拠していません（Cert key size is not FIPS compliant）]が表示されます。

電話機に LSC がある場合、FIPS を有効にする前に、LSC キー サイズを 2048 ビット以上に更新しておく必要があります。

次の表に、電話機でサポート対象セキュリティ機能の概要を示します。詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。

セキュリティ モード、信頼リスト、802.1X 認証など電話機の現在のセキュリティ設定を表示するには、**[アプリケーション（Applications）]** を押し、**[管理者設定（Admin Settings）]**> **[セキュリティのセットアップ（Security setup）]** の順に選択します。

表 *24 :* セキュリティ機能の概要

機能	説明
イメージ認証（Image authentication）	署名付きのバイナリ ファイル（拡張子 .sgn）によって、ファームウェアイメージが電話機へのロード前に改ざんされることを防止します。 イメージが改ざんされると、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。
イメージの暗号化	暗号化バイナリ ファイル（拡張子 .sebn）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。

機能	説明
カスタマーサイト証明書のインストール	各 Cisco IP 電話は、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 Communications Manager の管理ページで、Certificate Authority Proxy Function（CAPF; 認証局プロキシ関数）を使用して証明書のインストールを指定できます。 あるいは、電話機の [セキュリティ設定（Security Configuration）] メニューからローカルで有効な証明書（LSC）をインストールします。
[デバイス認証（Device authentication）]	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 では、認証できない電話機は登録されません。
ファイル認証（File authentication）	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。
ファイルの暗号化	暗号化により、ファイルの機密性の高い情報が電話機に転送される間に漏えいしないように保護されます。 さらに、電話機でも、ファイルが作成後に改ざんされていないことを、署名を確認することで確認します。 認証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。
Manufacturing Installed Certificate（製造元でインストールされる証明書）	各 Cisco IP 電話には、固有の製造元でインストールされる証明書（MIC）が内蔵されており、デバイス認証に使用されます。 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を提供し、Cisco Unified Communications Manager はこれを使用して電話機を認証します。
メディア暗号化	SRTP を使用して、サポート対象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プライマリキーペアの作成、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。
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。

機能	説明
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。 この表の他の項目は、セキュリティ機能について説明しています。
暗号化された設定ファイル（Encrypted configuration files）	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 サーバの無効化（オプション）	セキュリティ上の目的で、電話機の Web ページ（ここには電話機のさまざまな処理の統計情報が表示される）とセルフ ケア ポータルへのアクセスを防止できます。
電話のセキュリティ強化（Phone hardening）	Cisco Unified Communications Manager の管理ページから制御する追加セキュリティ オプションです。 • 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、[設定（Preferences）] メニューにアクセスすること、音量の変更を保存することのみ可能な、限定的なアクセスの提供 • 電話機の Web ページへのアクセスの無効化 • Bluetooth アクセサリ ポートの無効化 • TLS 暗号の制限
802.1X 認証	Cisco IP 電話は 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。 詳細については、802.1X 認証 （125 ページ）を参照してください。
SRST 向けのセキュアな SIP フェールオーバー	セキュリティ目的で Survivable Remote Site Telephony（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。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバの間で送信されるすべての 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。
信頼リストの更新アラーム	電話機で信頼リストが更新されると、Cisco Unified Communications Manager は更新の成功または失敗を示すアラームを受信します。 詳細については、以下の表を参照してください。

機能	説明
AES 256 暗号化（AES 256 Encryption）	Cisco Unified Communications Manager リリース 10.5(2)以降の 以降に接続している電話機は、シグナリングとメディア暗号化に関する TLS および SIP の AES 256 暗号化をサポートします。 これにより電話機は、SHA-2（Secure Hash Algorithm）標準および Federal Information Processing Standard（FIPS）に準拠する AES-256 ベースの暗号を使用して TLS 1.2 接続を開始し、サポートすることができます。 暗号は次のとおりです。 • TLS 接続用： • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • sRTP 用： • AEAD_AES_256_GCM • AEAD_AES_128_GCM 詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。
楕円曲線デジタル署名アルゴリズム（ECDSA）証明書	コモンクライテリア（共通基準、CC）認証の一部として、バージョン 11.0 の ECDSA 証明書が Cisco Unified Communications Manager によって追加されました。 これはバージョン CUCM 11.5 およびそれ以降からのすべての Voice Operating System（VOS）製品に影響を与えます。

次の表に、信頼リストの更新アラームのメッセージとその意味を示します。 詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

表 *25*：信頼リストの更新アラームのメッセージ

コードおよびメッセージ	説明
1 - TL_SUCCESS	新しい CTL や ITL を受信
2 - CTL_INITIAL_SUCCESS	新しい CTL を受信、既存の TL なし
3 - ITL_INITIAL_SUCCESS	新しい ITL を受信、既存の TL なし
4 - TL_INITIAL_SUCCESS	新しい CTL および ITL を受信、既存の TL なし
5 - TL_FAILED_OLD_CTL	新しい CTL への更新に失敗したが、以前の TL あり
6 - TL_FAILED_NO_TL	新しい TL への更新に失敗、古い TL なし
7 - TL_FAILED	一般的な障害
8 - TL_FAILED_OLD_ITL	新しい ITL への更新に失敗したが、以前の TL あり
9 - TL_FAILED_OLD_TL	新しい TL への更新に失敗したが、以前の TL あり

[セキュリティのセットアップ（Security Setup）] メニューには、さまざまなセキュリティ設定に関する情報が表示されます。 メニューでは、[信頼リスト（Trust List）] メニューにもアクセスでき、CTL ファイルまたは ITL ファイルが電話機にインストールされているかどうかを示します。

次の表に、[セキュリティのセットアップ（Security Setup）] メニューのオプションを示します。

表 *26 : [*セキュリティのセットアップ（***Security Setup***）*]* メニュー

オプション	説明	変更の手順
セキュリティ モード	電話機に設定されているセキュリティ モードを表示します。	From Cisco Unified Communications Manager の管理で、**[デバイス（Device）] > [電話（Phone）]** を選択します。 この設定は [電話の設定（Phone Configuration）] ウィンドウの [プロトコル固有情報（Protocol Specific Information）] の部分に表示されます。
LSC	セキュリティ機能で使用される、ローカルで有効な証明書が電話機にインストールされている（[はい（Yes）]）かインストールされていない（[いいえ（No）]）かを示します。	電話機における LSC の詳しい管理方法については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

オプション	説明	変更の手順
信頼リスト	[信頼リスト（Trust List）]は、CTL ファイル、ITL ファイル、および署名済み設定ファイル用のサブメニューを備えています。 [CTL ファイル（CTL File）]サブメニューは、CTL ファイルの内容を表示します。 [ITL ファイル（ITL File）]サブメニューは、ITL ファイルの内容を表示します。 [信頼リスト（Trust List）]メニューには、次の情報が表示されます。 • [CTL 署名（CTL Signature）]：CTL ファイルの SHA1 ハッシュ • [Unified CM/TFTP サーバ（Unified CM/TFTP Server）]：電話機で使用される Cisco Unified Communications Manager と TFTP サーバの名前。 このサーバに証明書がインストールされている場合は、証明書アイコンが表示されます。 • [CAPF サーバ（CAPF Server）]：電話機が使用する CAPF サーバの名前。 このサーバに証明書がインストールされている場合は、証明書アイコンが表示されます。 • [SRST ルータ（SRST Router）]：電話機で使用可能な、信頼できる SRST ルータの IP アドレス。 このサーバに証明書がインストールされている場合は、証明書アイコンが表示されます。	詳細については、重要な証明書のローカルでのセットアップ （102 ページ） を参照してください。
802.1X 認証	この電話機に 802.1X 認証を有効にできます。	802.1X 認証 （125 ページ） を参照してください。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

重要な証明書のローカルでのセットアップ

この作業は、認証文字列方式を使用した LSC の設定に適用されます。

始める前に

次の点を調べて、対象の Cisco Unified Communications Manager および認証局プロキシ関数（CAPF）のセキュリティ設定が完了していることを確認してください。

- CTL ファイルまたは ITL ファイルに CAPF 証明書が含まれていること。
- Cisco Unified Communications オペレーティング システムの管理ページで、CAPF 証明書がインストールされていることを確認してください。
- CAPF が実行および設定されていること。

これらの設定の詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

ステップ 1 CAPF の設定時に設定された CAPF 認証コードを入手します。

ステップ 2 電話機から、[アプリケーション（Applications）]を押します。

ステップ 3 **[管理設定（Admin Settings）]** > **[セキュリティ設定（Security Setup）]**を選択します。

（注） Cisco Unified Communications Manager の管理ページの [電話の設定（Phone Configuration）] ウィンドウにある設定アクセス フィールドを使用すると、[設定（Settings）] メニューへのアクセスを制御できます。

ステップ 4 [LSC]を選択し、[選択（Select）]または [更新（Update）]を押します。

認証文字列を要求するプロンプトが電話機に表示されます。

ステップ 5 認証コードを入力し、[送信（Submit）]を押します。

CAPF の設定に応じて、電話機で LSC のインストール、更新、または削除が開始されます。この作業の間、[セキュリティ設定（Security Configuration）] メニューの [LSC] オプション フィールドに一連のメッセージが表示されるので、進捗状況をモニタできます。手順が完了すると、電話機に [インストール済み（Installed）] または [未インストール（Not Installed）] と表示されます。

LSC のインストール、更新、または削除プロセスは、完了するのに長時間かかることがあります。

電話機のインストール手順が正常に実行されると、「インストール済み（Installed）」メッセージが表示されます。電話機に「未インストール（Not Installed）」と表示された場合は、認証文字列に誤りがあるか、電話機のアップグレードが有効になっていない可能性があります。CAPF 操作で LSC を削除し、電話機に「未インストール（Not Installed）」と表示された場合、それは操作が成功したことを示しています。CAPF サーバはこのエラー メッセージをログに記録します。ログを見つけ、エラー メッセージの意味を理解するには、CAPF サーバ ドキュメントを参照してください。

FIPS モードの有効化

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択し、電話機を見つけます。

ステップ 2 [Product Specific Configuration] 領域まで移動します。

ステップ 3 [FIPS モード（FIPS Mode）] フィールドを [有効（Enabled）] に設定します。

ステップ 4 [設定の適用（Apply Config）]を選択します。

ステップ 5 **保存**を選択します。

ステップ 6 電話機を再起動します。

電話コールのセキュリティ

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、セキュアな電話コールや暗号化された電話コールを識別できます。また、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、接続された電話機がセキュアであり保護されているかどうかも判断できます。

セキュアなコールでは、すべてのコール シグナリングとメディア ストリームが暗号化されます。 セキュアなコールは高度なレベルのセキュリティを提供し、コールに整合性とプライバシーを提供します。 処理中のコールが暗号化されているときは、電話スクリーンのコール時間タイマーの右側にあるコール進捗アイコンが、次のアイコン  に変化します。

（注） 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。

セキュアなコールではコールの開始時にセキュリティ トーンが再生され、接続先の電話機もセキュアな音声を送受信していることを示します。セキュアで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） セキュアなコールは、2 台の電話機間でのみサポートされます。 電話会議や共有回線などの一部の機能は、セキュアなコールが設定されているときは使用できません。

Cisco Unified Communications Manager で電話機をセキュア（暗号化および信頼された）として設定した場合、その電話機には「保護」ステータスを割り当てることができます。その後、必

要に応じて、保護された電話機は、コールの初めに通知トーンを再生するように設定できます。

- [保護されたデバイス（Protected Device）]：セキュアな電話機のステータスを保護に変更するには、Cisco Unified Communications Manager の管理ページの [電話の設定（Phone Configuration）] ウィンドウにある [保護されたデバイス（Protected Device）] チェックボックスをオンにします（**[デバイス（Device）]** > **[電話（Phone）]**）。
- [セキュア インディケーション トーンの再生（Play Secure Indication Tone）]：保護された電話機で、セキュアまたは非セキュアな通知トーンの再生を有効にするには、[セキュア インディケーション トーンの再生（Play Secure Indication Tone）] 設定を [はい（True）] に設定します。 デフォルトでは、[セキュア インディケーション トーンの再生（Play Secure Indication Tone）] は [いいえ（False）] に設定されます。 このオプションは、Cisco Unified Communications Manager の管理（**[システム（System）]** > **[サービス パラメータ（Service Parameters）]**）で設定します。 サーバを選択してから、Unified Communications Manager サービスを選択します。 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、[機能 - セキュア トーン（Feature - Secure Tone）] 領域内にあるオプションを選択します。 デフォルトは False です。

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。セキュアな電話会議は、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で会議を開始します。
2. Cisco Unified Communications Manager が、コールにセキュアな会議ブリッジを割り当てます。
3. 参加者が追加されると、Cisco Unified Communications Manager は、各電話機のセキュリティ モードを検証し、セキュアな会議の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。 セキュアな会議では、電話機の画面の [**会議（Conference）**] の右側にセキュア アイコン が表示されます。

（注） セキュアなコールは、2 台の電話機の間でサポートされます。保護された電話機では、セキュアなコールが設定されている場合、会議コール、シェアド ライン、エクステンション モビリティなどの一部の機能を使用できません。

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 レベルの変更に関する情報を示しています。

表 *27:* 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	セキュア	非セキュアな会議ブリッジ 非セキュアな会議
セキュア	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	会議	セキュア	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
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 ん。コールを拒否します（Does not me Level, call rejected）」というメッセー る。
セキュア	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 会議はすべてのコールを受け入れる。

セキュアな電話コールの識別

ユーザの電話機および相手側の電話機でセキュアなコールが設定されている場合にセキュアな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。 セキュアなコールは 2 台の電話機間でのみ形成できます。セキュアな会議ブリッジのセットアップ後、電話会議ではセキュアなコールがサポートされます。

セキュアなコールは、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（セキュリティ モードで保護された電話機）でコールを開始します。
2. 電話スクリーンにセキュア アイコン  が表示されます。 このアイコンは、この電話機がセキュアなコール用に設定されていることを示しますが、接続する他の電話機もセキュアであるという意味ではありません。
3. そのコールが別のセキュアな電話機に接続された場合は、ユーザにセキュリティ トーンが聞こえ、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。 コールが非セキュアな電話機に接続された場合は、ユーザにはセキュリティ トーンが聞こえません。

（注） セキュアなコールは、2台の電話機の間でサポートされます。保護された電話機では、セキュアなコールが設定されている場合、会議コール、シェアド ライン、エクステンション モビリティなどの一部の機能を使用できません。

保護された電話機だけで、セキュアまたは非セキュアなインディケーション トーンが再生されます。 保護されていない電話機ではトーンは聞こえません。 コール中にコール全体のステータスが変化すると、それに従って通知トーンも変化し、保護された電話機は対応するトーンを再生します。

このような状況にない場合、保護された電話機はトーンを再生しません。

- [セキュア インディケーション トーンの再生（Play Secure Indication Tone）] オプションが有効になっている場合
  - エンドツーエンドのセキュアなメディアが確立され、コール ステータスがセキュアになった場合、電話機はセキュア インディケーション トーン（間に小休止を伴う 3 回の長いビープ音）を再生します。
  - エンドツーエンドの非セキュアなメディアが確立され、コール ステータスが非セキュアになった場合、電話機は、非セキュアのインディケーション トーンを再生します（間に小休止を伴う 6 回の短いビープ音）。

[セキュア インディケーション トーンの再生（Play Secure Indication Tone）] オプションが無効になっている場合、トーンは再生されません。

割り込みの暗号化

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。

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 トーン（速いビジー音）が聞こえます。

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電話機からセキュアでないコールに割り込むことができます。 割り込みが発生すると、Cisco Unified Communications Manager はそのコールを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。

WLAN セキュリティ

通信圏内にあるすべての WLAN デバイスは他の WLAN トラフィックをすべて受信できるため、WLAN内の音声通信の保護は重要です。侵入者による音声トラフィックの操作や傍受を防止するため、Cisco SAFE セキュリティ アーキテクチャは、Cisco IP 電話 と Cisco Aironet AP を

サポートします。ネットワーク内のセキュリティの詳細については、http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html を参照してください。

Cisco Wireless IP テレフォニー ソリューションは、ワイヤレス Cisco IP 電話がサポートする次の認証方式を使用して、不正ログインおよび改ざんされた通信を防ぐワイヤレス ネットワーク セキュリティを提供します。

- オープン認証：オープン システムでは、任意のワイヤレス デバイスが認証を要求できます。要求を受けた AP は、任意のリクエスタまたはユーザのリスト上にあるリクエスタだけに認証を与える場合があります。ワイヤレス デバイスと AP との間の通信は暗号化されない可能性もあります。暗号化される場合、デバイスは有線と同等のプライバシー（WEP）キーを使用してセキュリティを提供できます。WEP を使用しているデバイスは、WEP を使用している AP での認証だけを試みます。

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）認証：このクライアント サーバのセキュリティ アーキテクチャは、AP と、Cisco Access Control Server（ACS）などの RADIUS サーバとの間の Transport Level Security（TLS）トンネル内の EAP トランザクションを暗号化します。

  TLS トンネルでは、クライアント（電話機）と RADIUS サーバの間の認証に Protected Access Credential（PAC）が使用されます。サーバは Authority ID（AID）をクライアント（電話機）に送信します。それを受けてクライアントは適切な PAC を選択します。クライアント（電話機）は PAC-Opaque を RADIUS サーバに返します。サーバは、プライマリ キーで PAC を復号します。これで両方のエンドポイントに同じ PAC キーが含まれ、TLS トンネルが構築されます。EAP-FAST では、自動 PAC プロビジョニングがサポートされていますが、RADIUS サーバ上で有効にする必要があります。

（注） Cisco ACS での PAC の有効期限は、デフォルトで 1 週間です。電話機に期限切れの PAC が存在する場合、電話機が新しい PAC を取得するまでの間は、RADIUS サーバでの認証に比較的長い時間がかかります。PAC プロビジョニングの遅延を回避するには、ACS サーバまたは RADIUS サーバで PAC の有効期間を 90 日以上に設定します。

- 拡張認証プロトコル - トランスポート層セキュリティ（EAP-TLS）認証：EAP-TLS では、認証とネットワークアクセスにクライアント証明書が必要です。有線 EAP-TLS の場合、クライアント証明書は電話機の MIC または LSC のいずれかです。LSC は、有線 EAP-TLS に推奨されるクライアント認証証明書です。

- Protected Extensible Authentication Protocol（PEAP）：クライアント（電話機）と RADIUS サーバ間の、シスコ独自のパスワードベースの相互認証方式です。Cisco IP 電話 は、ワイヤレス ネットワークでの認証に PEAP を使用できます。PEAP-MSCHAPV2 と PEAP-GTC の両方の認証メカニズムがサポートされます。

次の認証方式では、RADIUS サーバを使用して認証キーを管理します。

- WPA/WPA2: 一意の認証キーを生成するために RADIUS サーバの情報を使用します。これらのキーは、中央集中型の RADIUS サーバで生成されるため、WPA/WPA2 は、AP および電話機に格納されている WPA 事前共有キーよりも高いセキュリティを提供します。
- 高速安全ローミング： RADIUS サーバとワイヤレス ドメイン サーバ（WDS）上の情報を使用してキーを管理および認証します。WDS は、高速でセキュアな再認証用に、CCKM 対応クライアント デバイスのセキュリティ クレデンシャルのキャッシュを作成します。Cisco IP 電話 8800 シリーズは 802.11r（FT）をサポートしています。高速セキュアローミングを可能にするために、11r（FT）と CCKM の両方がサポートされています。しかしシスコは 802.11r（FT）無線方式を利用することを強く推奨します。

WPA/WPA2 および CCKM では、暗号化キーは電話機に入力されず、AP と電話機の間で自動的に生成されます。ただし認証で使用する EAP ユーザ名とパスワードは、各電話機に入力する必要があります。

音声トラフィックの安全性を確保するため、Cisco IP 電話 では、暗号化方式として WEP、TKIP、および Advanced Encryption Standards（AES）をサポートします。暗号化にこれらのメカニズムを使用すると、AP と Cisco IP 電話 との間で、シグナリング SIP パケットと音声リアルタイム トランスポート プロトコル（RTP）パケットの両方が暗号化されます。

WEP

ワイヤレス ネットワークで WEP を使用すると、オープン認証または共有キー認証を使用することにより、AP で認証が行われます。正常に接続させるには、電話機で設定された WEP キーと AP で設定された WEP キーが一致する必要があります。Cisco IP 電話 は、40 ビット暗号化または 128 ビット暗号化を使用し、電話機および AP で静的なままの WEP キーをサポートしています。

EAP と CCKM の認証では、暗号化に WEP キーを使用できます。RADIUS サーバは WEP キーを管理し、すべての音声パケットの暗号化を認証した後で一意のキーを AP に渡します。そのため、次の WEP キーを各認証で変更できます。

TKIP

WPA と CCKM は、WEP にいくつかの改良が加えられた TKIP 暗号化を使用します。TKIP は、パケットごとのキーの暗号化、および暗号化が強化されたより長い初期ベクトル（IV）を提供します。さらに、メッセージ完全性チェック（MIC）は、暗号化されたパケットが変更されていないことを確認します。TKIP は、侵入者が WEP を使用して WEP キーを解読する可能性を排除します。

AES

WPA2 認証に使用される暗号化方式。この暗号化の国内規格は、暗号化と復号化に同じキーを持つ対称型アルゴリズムを使用します。AES は、128 ビットサイズの暗号ブロック連鎖（CBC）暗号化を使用し、最小のキー サイズとして 128、192、および 256 ビットのキーをサポートします。Cisco IP 電話 は 256 ビットのキー サイズをサポートします。

（注） Cisco IP 電話 は、CMIC による Cisco Key Integrity Protocol（CKIP）をサポートしません。

認証方式と暗号化方式は、ワイヤレス LAN 内で設定されます。VLAN は、ネットワーク内および AP 上で設定され、認証と暗号化の異なる組み合わせを指定します。SSID は、VLAN と VLAN の特定の認証および暗号化方式に関連付けられます。ワイヤレス クライアント デバイスを正常に認証するには、認証および暗号化方式で使用する SSID と同じ SSID を AP と Cisco IP 電話 に設定する必要があります。

一部の認証方式では、特定のタイプの暗号化が必要です。オープン認証では、セキュリティを高めるために、暗号化で静的 WEP を使用できます。ただし、共有キー認証を使用している場合は、暗号化に静的 WEP を設定し、電話機で WEP キーを設定する必要があります。

（注）
- WPA 事前共有キーまたは WPA2 事前共有キーを使用する場合、その事前共有キーを電話機で静的に設定する必要があります。これらのキーは、AP に存在するキーと一致している必要があります。
- Cisco IP 電話 は、自動 EAP ネゴシエーションをサポートしていません。EAP-FAST モードを使用するには、EAP-FAST モードを指定する必要があります。

次の表に、Cisco IP 電話がサポートしている、Cisco Aironet AP で設定される認証方式と暗号化方式のリストを示します。表には、AP の設定に対応する電話機のネットワーク設定オプションを示します。

表 *28 :* 認証方式と暗号化方式

Cisco IP 電話の設定	**AP の設定**			
Security Mode	セキュリティ	Key Management	暗号化	高速ローミング
なし	なし	なし	なし	該当なし
WEP	Static WEP	スタティック	WEP	該当なし
PSK	PSK	WPA	TKIP	なし
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM

Cisco IP 電話の設定	AP の設定			
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM
PEAP-GTC	PEAP-GTC	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM

認証方式と暗号化方式を AP に設定する方法の詳細については、次の URL で入手可能なご使用のモデルおよびリリースの『*Cisco Aironet Configuration Guide*』を参照してください。

http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

認証モードのセットアップ

このプロファイルの認証モードを選択するには、次の手順を実行します。

手順

ステップ 1 設定するネットワーク プロファイルを選択します。

ステップ 2 認証モードを選択します。

（注） 選択したモードによっては、[ワイヤレス セキュリティ（Wireless Security）] または [ワイヤレス暗号化（Wireless Encryption）] で追加オプションを設定する必要があります。 詳細については、WLAN セキュリティ （107 ページ）を参照してください。

ステップ 3 [保存（Save）]をクリックして変更を加えます。

ワイヤレス セキュリティ クレデンシャル

ネットワークで EAP-FAST および PEAP がユーザ認証に使用されている場合、リモート認証ダイヤルインユーザ サービス（RADIUS）と電話機で必要な場合にユーザ名およびパスワードの両方を設定する必要があります。

（注） ネットワーク内のドメインを使用している場合、*domain\username* の形式でユーザ名とドメイン名を入力する必要があります。

次の操作によって、既存の Wi-Fi パスワードがクリアされる可能性があります。

- 無効なユーザ ID またはパスワードを入力する
- EAP タイプが PEAP-MSCHAPV2 または PEAP-GTC に設定されているときに、無効または期限切れのルート CA 証明書をインストールする
- 新しい EAP タイプに電話機を変更する前に、電話機によって使用される RADIUS サーバの EAP タイプを無効にする

EAP タイプを変更するには、示されている順序で以下を実行します。

- RADIUS の新しい EAP タイプを有効にします。
- 電話機の EAP タイプを新しい EAP タイプに変更します。

新しい EAP タイプが RADIUS サーバで有効にされるまで、電話機に設定された現在の EAP タイプを保持します。 新しい EAP タイプが RADIUS サーバで有効にされたら、電話機の EAP タイを変更できます。 すべての電話機が新しい EAP タイプに変更されたら、必要に応じて前の EAP タイプを無効にすることができます。

ユーザ名とパスワードのセットアップ

ネットワーク プロファイルのユーザ名またはパスワードを入力または変更するには、RADIUS サーバに設定されているものと同じユーザ名およびパスワード文字列を使用する必要があります。 ユーザ名またはパスワード エントリの最大長は、64 文字です。

[ワイヤレス セキュリティ クレデンシャル（Wireless Security Credentials）] でユーザ名とパスワードをセットアップするには、次の手順を実行します。

手順

ステップ 1 ネットワーク プロファイルを選択します。

ステップ 2 [ユーザ名（UserName）] フィールドに、このプロファイルのネットワーク ユーザ名を入力します。

ステップ 3 [パスワード（Password）] フィールドに、このプロファイルのネットワーク パスワード文字列を入力します

ステップ 4 [保存（Save）]をクリックして変更を加えます。

事前共有キーの設定

次のセクションを使用して、事前共有キーを設定するときにガイドしてください。

事前共有キーの形式

Cisco IP 電話 は、ASCII 形式と 16 進数形式をサポートしています。 WPA 事前共有キーを設定している場合は、次の形式のいずれかを使用する必要があります。

16 進数

16 進数のキーの場合は、64 の 16 進数（0 ～ 9、A ～ F）を入力します。たとえば、AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C のように入力します。

ASCII

ASCII キーの場合は、0 ～ 9、A ～ Z（大文字と小文字）、すべての記号を使用した文字列を、長さ 8 ～ 63 文字で入力します。たとえば、GREG12356789ZXYW のように入力します。

PSK のセットアップ

[ワイヤレス クレデンシャル（Wireless Credentials）] 領域で PSK をセットアップするには、次の手順を実行します。

手順

ステップ 1 [自動（AKM）（Auto (AKM)）] を使用するネットワーク プロファイルを選択し、WPA 事前共有キーまたは WPA2 事前共有キーをイネーブルにします。

ステップ 2 [キーの種類] 領域に適切なキーを入力します。

ステップ 3 [パスフレーズ/事前共有キー（Passphrase/Pre-shared key）] フィールドに ASCII 文字列または 16 進数を入力します。

ステップ 4 [保存（Save）]をクリックして変更を加えます。

ワイヤレス暗号化

ワイヤレス ネットワークが WEP 暗号化を使用しており、認証モードを [オープン+WEP（Open+WEP）] または [共有キー+WEP（Shared Key+WEP）] に設定している場合は、ASCII WEP キーまたは 16 進数 WEP キーを入力する必要があります。

電話機の WEP キーとアクセス ポイントに割り当てられた WEP キーは一致する必要があります。 Cisco IP 電話 および Cisco Aironet アクセス ポイントは、40 ビットおよび 128 ビットの両方の暗号キーをサポートしています。

WEP キーの形式

WEP キーの設定時には、次の形式のいずれかを使用する必要があります。

16 進数

16 進数キーの場合は、次のいずれかのキー サイズを使用します。

40 ビット

16 進数（0 ～ 9、A ～ F）を使用する 10 桁の暗号化キー文字列を入力します。たとえば、ABCD123456 のように入力します。

128 ビット

16 進数（0 ～ 9、A ～ F）を使用する 26 桁の暗号化キー文字列を入力します。たとえば、AB123456789CD01234567890EF のように入力します。

ASCII

ASCII キーの場合は、0 ～ 9、A ～ Z（大文字と小文字）およびすべての記号を使用する、次のいずれかのキー サイズの文字列を入力します。

40 ビット

5 文字の文字列を入力します。たとえば、GREG5 のように入力します。

128 ビット

13 文字の文字列を入力します。たとえば、GREGSSECRET13 のように入力します。

WEP キーのセットアップ

WEP キーを設定するには、次の手順を実行します。

手順

ステップ 1 [オープン+WEP（Open+WEP）] または [共有+WEP（Shared+WEP）] を使用するネットワークプロファイルを選択します。

ステップ 2 [キーの種類] 領域に適切なキーを入力します。

ステップ 3 [キー サイズ（Key Size）] 領域で、次の文字形式のいずれかを選択します。

- **40**
- **128**

ステップ 4 選択したキー タイプとキー サイズに基づいて、[暗号キー（Encryption Key）] フィールドに適切なキー文字列を入力します。 WEP キーの形式 （113 ページ）を参照してください。

ステップ 5 [保存（Save）]をクリックして変更を加えます。

Microsoft 証明書サービスを使用した CA 証明書のエクスポート

ACS から認証サーバ ルート証明書をエクスポートします。 追加情報については、CA または RADIUSのドキュメントを参照してください。

製造元でインストールされる証明書

シスコでは、工場出荷時に製造元でインストールされる証明書（MIC）を電話機に組み込んでいます。

EAP-TLS 認証時には、ACS サーバは電話機の信頼度を確認し、電話機は ACS サーバの信頼度を確認する必要があります。

MIC を確認するには、製造元ルート証明書と製造元認証局（CA）証明書を Cisco IP 電話 からエクスポートし、Cisco ACS サーバにインストールする必要があります。 これらの 2 つの証明書は、Cisco ACS サーバによる MIC の確認に使用される、信頼証明書チェーンの一部です。

Cisco ACS 証明書を確認するには、Cisco ACS サーバの信頼される下位証明書（ある場合）とルート証明書（CA が作成）をエクスポートし、電話機にインストールする必要があります。これらの証明書は、ACS サーバからの証明書の信頼度を確認するために使用される信頼証明書チェーンの一部です。

ユーザがインストールした証明書

ユーザがインストールした証明書を使用するには、証明書署名要求（CSR）が生成されて、承認のために CA へ送信されている必要があります。 ユーザ証明書は、CSR なしで CA によって生成することもできます。

EAP-TLS 認証時には、ACS サーバは電話機の信頼度を確認し、電話機は ACS サーバの信頼度を確認します。

ユーザがインストールした証明書の信頼性を確認するには、ユーザ証明書を承認した CA からの信頼される下位証明書（ある場合）とルート証明書を Cisco ACS サーバにインストールする必要があります。 これらの証明書は、ユーザがインストールした証明書の信頼度を確認するために使用される信頼証明書チェーンの一部です。

Cisco ACS 証明書を確認するには、Cisco ACS サーバの信頼される下位証明書（ある場合）とルート証明書（CA が作成）をエクスポートし、エクスポートした証明書を電話機にインストールします。 これらの証明書は、ACS サーバからの証明書の信頼度を確認するために使用される信頼証明書チェーンの一部です。

EAP-TLS 認証証明書のインストール

EAP-TLS の認証証明書をインストールするには、次の手順を実行します。

手順

ステップ 1 電話機の Web ページで、電話機に Cisco Unified Communications Manager の日付と時刻を設定します。

ステップ 2 製造元でインストールされる証明書（MIC）を使用する場合：

a) 電話機の Web ページで、CA ルート証明書と製造元 CA 証明書をエクスポートします。

b) Internet Explorer で、Cisco ACS サーバに証明書をインストールし、信頼リストを編集します。

c) ルート CA を電話機にインポートします。

詳細については、以下を参照してください。

- ACS での証明書のエクスポートおよびインストール （116 ページ）
- Microsoft 証明書サービスを使用した CA 証明書のエクスポート （117 ページ）

ステップ 3 ACS 設定ツールを使用して、ユーザ アカウントを設定します。

詳細については、以下を参照してください。

- ACS ユーザ アカウントのセットアップと証明書のインストール （119 ページ）
- 『*User Guide for Cisco Secure ACS for Windows*』（http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html）

Set Date and Time

EAP-TLS で使用される証明書ベースの認証では、Cisco IP 電話の内部クロックが正しく設定されている必要があります。 電話機の日付と時刻は、Cisco Unified Communications Manager に登録されたときに変わる場合があります。

（注） 新しいサーバ認証証明書が要求され、ローカル時間がグリニッジ標準時（GMT）よりも遅れている場合は、認証証明書の検証に失敗します。 GMT よりも先にローカルの日付と時刻を設定することをお勧めします。

電話機を正しいローカルの日付と時刻に設定するには、次の手順を実行します。

手順

ステップ 1 左側のナビゲーション ペインで [日付および時刻（Date & Time）]を選択します。

ステップ 2 [現在の電話機の日時（Current Phone Date & Time）] フィールドの設定値が [ローカルの日時（Local Date & Time）] フィールドと異なる場合は、[電話機のローカルの日時を設定（Set Phone to Local Date & Time）]をクリックします。

ステップ 3 [電話機の再起動（Phone Restart）]をクリックし、次に [OK]をクリックします。

ACS での証明書のエクスポートおよびインストール

MIC を使用するには、製造元ルート証明書と製造元 CA 証明書をエクスポートし、Cisco ACS サーバにインストールします。

製造元ルート証明書と製造元 CA 証明書を ACS サーバにエクスポートするには、次の手順を実行します。

手順

ステップ 1 電話機の Web ページで、[証明書（Certificates）] を選択します。

ステップ 2 製造元ルート証明書の横にある [エクスポート（Export）] をクリックします。

ステップ 3 証明書を保存し、それを ACS サーバにコピーします。

ステップ 4 製造元 CA 証明書に関して、ステップ 1 と 2 を繰り返します。

ステップ 5 [ACS サーバ システム設定（ACS Server System Configuration）] ページで、各証明書へのファイル パスを指定し、証明書をインストールします。

（注） ACS 設定ツールの使用方法の詳細については、ACS のオンライン ヘルプまたは『*User Guide for Cisco Secure ACS for Windows*』（http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html）を参照してください。

ステップ 6 [証明書信頼リスト（CTL）の編集（Edit the Certificate Trust List (CTL)）] ページで、ACS によって信頼されている証明書を追加します。

ACS 証明書のエクスポート方法

ACS からエクスポートする証明書のタイプによって、次の方式のいずれかを使用します。

- ユーザがインストールした証明書または ACS 証明書が署名された ACS サーバから CA 証明書をエクスポートするには、Microsoft 証明書サービスを使用した CA 証明書のエクスポート （117 ページ）を参照してください。
- 自己署名証明書を使用する ACS サーバから CA 証明書をエクスポートするには、Internet Explorer を使用して ACS から CA 証明書をエクスポートする （118 ページ）を参照してください。

Microsoft 証明書サービスを使用した CA 証明書のエクスポート

ユーザがインストールした証明書または ACS 証明書が署名された ACS サーバから CA 証明書をエクスポートする場合は、この方式を使用します。

[Microsoft 証明書サービス（Microsoft Certificate Services）] Web ページを使用して CA 証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1 [Microsoft 証明書サービス（Microsoft Certificate Services）] Web ページで、[CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain or CRL）] をクリックします。

ステップ 2 次のページで、テキスト ボックス内の現在 CA 証明書を強調表示し、[エンコード方式（Encoding Method）] として [DER] を選択し、[CA 証明書のダウンロード（Download CA certificate）] をクリックします。

ステップ 3 CA 証明書を保存します。

Internet Explorer を使用して ACS から CA 証明書をエクスポートする

自己署名証明書を使用する ACS サーバから CA 証明書をエクスポートする場合は、この方式を使用します。

Internet Explorer を使用して ACS サーバから証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1 Internet Explorer で [ツール（Tools）] > [インターネット オプション（Internet Options）] > を選択し、[コンテンツ（Content）] タブをクリックします。

ステップ 2 [証明書（Certificates）] 下で、[証明書（Certificates）] をクリックし、[信頼されたルート証明機関（Trusted Root Certification Authorities）]タブをクリックします。

ステップ 3 ルート証明書を強調表示し、[エクスポート（Export）]をクリックします。 [証明書のエクスポート ウィザード（Certificate Import Wizard）] が表示されます。

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 次のウィンドウで [DER encoded binary X.509 (.CER)]を選択し、[次へ（Next）]をクリックします。

ステップ 6 証明書の名前を指定し、[次へ（Next）]をクリックします。

ステップ 7 電話機にインストールする CA 証明書を保存します。

ユーザがインストールした証明書の要求およびインポート

証明書を要求して電話機にインストールするには、次の手順を実行します。

手順

ステップ 1 電話機の Web ページで、EAP-TLS を使用しているネットワーク プロファイルを選択し、[EAP-TLS 証明書（EAP-TLS Certificate）] フィールドで [ユーザによってインストールされる証明書（User Installed）] を選択します。

ステップ 2 [Certificates]をクリックします。

[ユーザ証明書のインストール（User Certificate Installation）] ページの [一般名（Common Name）] フィールドは、ACS サーバのユーザ名と一致している必要があります。

（注） [一般名（Common Name）] フィールドは、必要に応じて編集できます。 編集した場合も、ACS サーバのユーザ名と一致していることを確認してください。ACS ユーザ アカウントのセットアップと証明書のインストール（119 ページ）を参照してください。

ステップ 3 証明書に表示する情報を入力し、[送信（Submit）]をクリックして証明書署名要求（CSR）を生成します。

認証サーバ ルート証明書のインストール

電話機に認証サーバ ルート証明書をインストールには、次の手順を実行します。

手順

ステップ 1 ACS から認証サーバ ルート証明書をエクスポートします。 ACS 証明書のエクスポート方法（117 ページ）を参照してください。

ステップ 2 電話機の Web ページに移動し、[証明書（Certificates）]を選択します。

ステップ 3 認証サーバ ルート証明書の横にある [インポート（Import）]をクリックします。

ステップ 4 電話機を再起動します。

ACS ユーザ アカウントのセットアップと証明書のインストール

ユーザ アカウント名を設定し、電話機の MIC ルート証明書を ACS にインストールするには、次の手順を実行します。

（注） ACS 設定ツールの使用方法の詳細については、ACS のオンライン ヘルプまたは『*User Guide for Cisco Secure ACS for Windows*』を参照してください。

手順

ステップ 1 ACS 設定ツールの [ユーザ セットアップ（User Setup）] ページで、電話機のユーザ アカウント名を作成します（未設定の場合）。

通常、ユーザ名には末尾に電話機の MAC アドレスを含めます。 EAP-TLS の場合は、パスワードは不要です。

（注） ユーザ名が、[ユーザ証明書のインストール（User Certificate Installation）] ページの [一般名（Common Name）] フィールドと一致していることを確認してください。 ユーザがインストールした証明書の要求およびインポート（118 ページ）を参照してください。

ステップ 2 [システム設定（System Configuration）] ページの [EAP-TLS] セクションで次のフィールドをイネーブルにします。

- **Allow EAP-TLS**
- **証明書 CN の比較（Certificate CN comparison）**

ステップ 3 [ACS 認証局のセットアップ（ACS Certification Authority Setup）] ページで、製造元ルート証明書と製造元 CA 証明書を ACS サーバに追加します。

ステップ 4 [ACS 証明書信頼リスト（ACS Certificate Trust List）] で製造元ルート証明書と製造元 CA 証明書の両方をイネーブルにします。

PEAP の設定

Protected Extensible Authentication Protocol（PEAP）は、サーバ側の公開キー証明書を使用してクライアントを認証するために、クライアントと認証サーバの間に暗号化された SSL/TLS トンネルを構築します。

Cisco IP 電話 8865 は、SCEP 経由または手動インストール方法のいずれかでインストールできるサーバ証明書を 1 つだけサポートしていますが、両方はサポートしていません。 電話機は TFTP による証明書のインストール方法をサポートしていません。

（注） 認証サーバの検証は、認証サーバ証明書をインポートすることによってイネーブルにできます。

事前準備

電話機の PEAP 認証を設定する前に、次の Cisco Secure ACS 要件を満たしていることを確認します。

- ACS ルート証明書がインストールされていること。
- 証明書をインストールして、PEAP のサーバ検証を有効にすることもできます。 サーバ証明書をインストールすると、サーバ検証が自動的に有効になります。
- [EAP-MSCHAPv2 を許可（Allow EAP-MSCHAPv2）] 設定がイネーブルになっていること。
- ユーザ アカウントとパスワードが設定されていること。
- パスワード認証の場合は、ローカル ACS データベースまたは外部データベース（Windows または LDAP）を使用できること。

PEAP 認証の有効化

手順

ステップ 1 [電話の設定(Phone Configuration)] Web ページで、認証モードとして [PEAP] を選択します

ステップ 2 ユーザ名とパスワードを入力します。

ワイヤレス LAN セキュリティ

Wi-Fi をサポートするシスコの電話機には追加のセキュリティ要件があり、追加の設定が必要になります。 これらの追加手順には、証明書のインストール、および電話機と Cisco Unified Communications Manager でのセキュリティの設定が含まれます。

追加情報については、『*Security Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco IP 電話の管理ページ

Wi-Fi をサポートするシスコの電話機には、他の電話機のページとは異なる特別な Web ページがあります。 Simple Certificate Enrollment Protocol（SCEP）を使用できない場合に、電話機のセキュリティを設定するため、これらの特別な Web ページを使用します。 これらのページを使用して、セキュリティ証明書を手動で電話機にインストールしたり、セキュリティ証明書をダウンロードしたり、電話機の日時を手動で設定したりします。

これらの Web ページには、デバイス情報、ネットワーク設定、ログ、統計情報など、他の電話機の Web ページに表示されるものと同じ情報が表示されます。

関連トピック

Cisco IP 電話の Web ページ （270 ページ）

電話機の管理ページの設定

管理 Web ページは、電話機が工場から出荷された時点で有効になっていて、パスワードは「Cisco」に設定されています。 ただし、電話機を Cisco Unified Communications Manager に登録する場合は、管理 Web ページを必ず有効にし、新しいパスワードを設定する必要があります。

電話機を登録した後、Web ページを初めて使用する前に、この Web ページを有効にして、サインイン クレデンシャルを設定します。

有効にすると、管理 Web ページには、HTTPS ポート 8443（**`https://x.x.x.x:8443`**（x.x.x.x は電話機の IP アドレスです））でアクセスできます。

始める前に

管理 Web ページを有効にする前に、パスワードを決定します。 パスワードには文字と数字を任意に組み合わせて指定できますが、長さは 8 ～ 127 文字の間にする必要があります。

ユーザ名は admin に固定されています。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 電話機を特定します。

ステップ 3 **[プロダクト固有の設定]** の項で、**[Web 管理（Web Admin）]** を **[有効（Enabled）]** に設定します。

ステップ 4 [管理パスワード（**Admin Password**）] フィールドにパスワードを入力します。

ステップ 5 [保存（Save）]を選択し、[OK]をクリックします。

ステップ 6 **[設定の適用（Apply Config）]** を選択し、**[OK]** をクリックします。

ステップ 7 電話機を再起動します。

電話管理の Webページにアクセスします。

管理 Web ページにアクセスするとき、管理ポートを指定する必要があります。

手順

ステップ 1 次のように電話機の IP アドレスを取得します。

- Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択し、電話機を見つけます。 Cisco Unified Communications Manager に登録されている電話機の IP アドレスが、[Find and List Phones] ウィンドウと [Phone Configuration] ウィンドウの上部に表示されます。
- 電話機で**[アプリケーション（Applications）]** を押して、**[電話の情報]** を選択し、[IPv4 アドレス（IPv4 address）] フィールドまでスクロールします。

ステップ 2 Web ブラウザを開いて、次の URL を入力します。ここで、*IP_address* は Cisco IP 電話の IP アドレスです。

```
https://<IP_address>:8443
```

ステップ 3 [Password] フィールドにパスワードを入力します。

ステップ 4 [送信（Submit）]をクリックします。

電話機の管理 Web ページからユーザ証明書をインストールする

Simple Certificate Enrollment Protocol（SCEP）を使用できない場合、電話機にユーザ証明書を手動でインストールすることができます。

製造元でインストールされる証明書（MIC）を EAP-TLS 用のユーザ証明書として使用できます。

ユーザ証明書をインストールした後、RADIUS サーバの信頼リストに追加する必要があります。

始める前に

電話機のユーザ証明書をインストールするには、その前に以下を用意する必要があります。

- PC に保存されたユーザ証明書。 証明書は PKCS #12 形式である必要があります。

• 証明書の抽出パスワード。

手順

ステップ 1 電話機の管理 Web ページで、[証明書（Certificates）] を選択します。

ステップ 2 [ユーザインストール（User install）] フィールドを見つけて [インストール（Install）] をクリックします。

ステップ 3 PC の証明書を参照します。

ステップ 4 [抽出パスワード（Extract password）]フィールドに、証明書の抽出パスワードを入力します。

ステップ 5 [アップロード（Upload）]をクリックします。

ステップ 6 アップロードが完了したら、電話機を再起動します。

電話機の管理 Web ページから認証サーバ証明書をインストールする

Simple Certificate Enrollment Protocol（SCEP）を使用できない場合、電話機に認証サーバ証明書を手動でインストールすることができます。

RADIUS サーバ証明書を発行したルート CA 証明書は、EAP-TLS 用にインストールする必要があります。

始める前に

電話機に証明書をインストールするには、その前に認証サーバ証明書を PC に保存する必要があります。 証明書は PEM（Base 64）または DER 形式でエンコードする必要があります。

手順

ステップ 1 電話機の管理 Web ページで、[証明書（Certificates）] を選択します。

ステップ 2 [認証サーバ CA（管理 Web ページ）（Authentication server CA (Admin webpage)）] フィールドを見つけて [インストール（Install）]をクリックします。

ステップ 3 PC の証明書を参照します。

ステップ 4 [アップロード（Upload）]をクリックします。

ステップ 5 アップロードが完了したら、電話機を再起動します。

複数の証明書をインストールする場合は、電話機を再起動する前に、すべての証明書をインストールします。

電話機の管理 Web ページからセキュリティ証明書を手動で削除する

Simple Certificate Enrollment Protocol（SCEP）を使用できない場合、電話機からセキュリティ証明書を手動で削除することができます。

手順

ステップ 1 電話機の管理 Web ページで、[証明書（Certificates）] を選択します。
ステップ 2 [Certificates] ページで証明書を見つけます。
ステップ 3 [削除（Delete）]をクリックします。
ステップ 4 削除プロセスが完了したら、電話機を再起動します。

手動での電話機の日時の設定

証明書ベースの認証では、電話機に正しい日時を表示する必要があります。認証サーバは、電話機の日時を証明書の失効日と照合します。電話機とサーバの日時が一致しないと、電話機は動作を停止します。

電話機がネットワークから正しい情報を受信していない場合、次の手順を使用して電話機の日時を手動で設定します。

手順

ステップ 1 電話機の管理 Web ページで、[Date & Time] までスクロールします。
ステップ 2 次のいずれかの選択肢を実行します。

- ローカルサーバーに電話機を同期する場合は、**[電話機のローカルの日時を設定（Set Phone to Local Date & Time）]** をクリックします。
- **[日付および時刻の指定（Specify Date & Time）]** フィールドで、メニューを使用して、月、日、年、時、分、秒を選択し、**[電話機を特定の日時に設定（Set Phone to Specific Date & Time）]** をクリックします。

SCEP セットアップ

Simple Certificate Enrollment Protocol（SCEP）は、証明書の自動プロビジョニングおよび更新の標準です。 これにより、電話機に証明書を手動でインストールせずに済みます。

SCEP プロダクト固有の設定パラメータの設定

電話機の Web ページで次の SCEP パラメータを設定する必要があります。

- RA IP アドレス
- SCEP サーバのルート CA 証明書の SHA-1 または SHA-256 フィンガープリント

Cisco IOS の登録局（RA）は、SCEP サーバへのプロキシとして機能します。 電話機の SCEP クライアントは、Cisco Unified Communications Manager からダウンロードされたパラメータを

使用します。 パラメータを設定すると、電話機から RA に SCEP getcs 要求が送信され、定義されたフィンガープリントを使用してルート CA 証明書が検証されます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]**>**[電話（Phone）]** を選択します。

ステップ 2 電話機を特定します。

ステップ 3 [Product Specific Configuration Layout] 領域までスクロールします。

ステップ 4 **[WLAN SCEP Server]** チェックボックスをオンにして、SCEP パラメータをアクティブ化します。

ステップ 5 [WLAN Root CA Fingerprint (SHA256 or SHA1)]チェックボックスをオンにして、SCEP QED パラメータをアクティブ化します。

Simple Certificate Enrollment Protocol サーバのサポート

Simple Certificate Enrollment Protocol（SCEP）サーバを使用する場合、サーバはユーザとサーバ証明書を自動的に維持できます。 SCEP サーバで、次のように SCEP 登録エージェント（RA）を設定します。

- PKI トラスト ポイントとして機能する
- PKI RA として機能する
- RADIUS サーバを使用してデバイス認証を実行する

詳細については、SCEP サーバのマニュアルを参照してください。

802.1X 認証

Cisco IP 電話 は 802.1X 認証をサポートします。

Cisco IP 電話 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 IP 電話は、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 IP 電話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 メカニズムにより、IP フォン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際 LAN スイッチとして動作しません。

Cisco IP 電話はまた、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 フォンから切断された場合でも、LAN スイッチと IP フォン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 フォン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。

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 IP 電話: 電話機は、ネットワークへのアクセス要求を開始します。Cisco IP 電話には、802.1x サプリカントが含まれています。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。電話機に含まれる 802.1X サプリカントの現在のリリースでは、ネットワーク認証に EAP-FAST オプションと EAP-TLS オプションが使用されています。
- 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。

802.1X を設定するには、次の手順を実行する必要があります。

- 電話機で 802.1X 認証をイネーブルにする前に、他のコンポーネントを設定します。
- PC ポートの設定：802.1X 標準では VLAN 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定されます。
  - 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 IP 電話 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 ポートを無効にするようにしてください。このポートを無効にしないで PC を接続しようとすると、スイッチは電話機と PC の両方に対してネットワーク 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。

802.1X 認証へのアクセス

次の手順に従って、802.1X 認証の設定にアクセスできます。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Admin settings）] > [セキュリティのセットアップ（Security Setup）] > [802.1X 認証（802.1X Authentication）]** を選択します。

ステップ 3 [802.1X 認証（802.1X Authentication）] オプション （127 ページ）の説明に従ってオプションを設定します。

ステップ 4 メニューを終了するには、[終了（Exit）]を押します。

[802.1X 認証（802.1X Authentication）] オプション

次の表では、802.1X 認証オプションについて説明します。

表 *29 : 802.1X* 認証の設定

オプション	説明	変更の手順
デバイス認証	802.1X 認証が有効かどうかを示します。 • [有効（Enabled）]：電話機は 802.1X 認証を使用してネットワーク アクセスを要求します。 • [無効（Disabled）]：デフォルト設定です。 電話機は、CDP を使用して VLAN およびネットワーク アクセスを取得します。	[デバイス認証（Device Au フィールドの設定 （128 ペ してください。
Transaction Status（トランザクション ステータス）	[状態（State）]：802.1x 認証の状態を表示します。 • [切断済み（Disconnected）]：802.1x 認証が電話機に設定されていないことを示します。 • [認証済み（Authenticated）]：電話が認証されたことを示します。 • [保留（Held）]：認証プロセスが進行中であることを示します。 [プロトコル（Protocol）]：802.1x 認証に使用される EAP 方式を表示します（EAP-FAST または EAP-TLS である場合があります）。	表示のみ。 変更不可。

[デバイス認証（Device Authentication）] フィールドの設定

手順

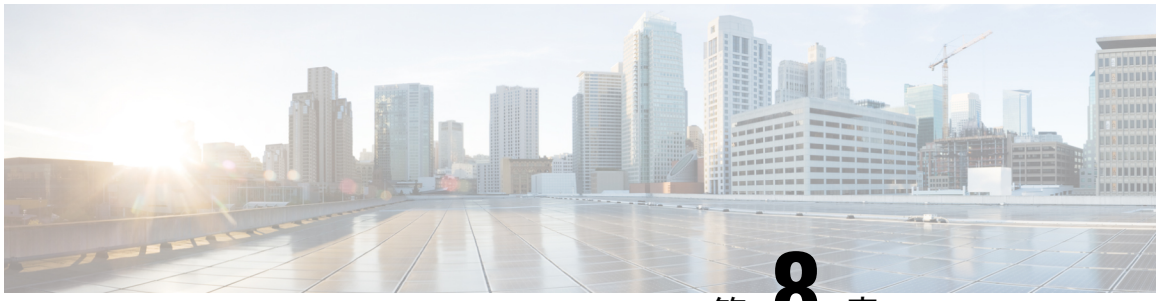
ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Admin settings）]** > **[セキュリティのセットアップ（Security Setup）]** > **[802.1X 認証（802.1X Authentication）]** を選択します。

ステップ 3 [デバイス認証（Device Authentication）] オプションを設定します。

- はい
- なし

ステップ 4 [適用（Apply）]を押します。



第 8 章

Cisco IP 電話のカスタマイズ

カスタム電話呼出音

電話機には、「Sunshine」、「Chirp」、「Chirp1」という 3 つの呼び出し音が付属しており、これらはハードウェアに内蔵されています。

Cisco Unified Communications Manager には、一連の追加の電話呼出音もデフォルトで付属しており、これらはパルス符号変調（PCM）ファイルとしてソフトウェアに実装されています。PCM ファイルは、サイトで使用できる呼出音リスト オプションを記述した XML ファイル（Ringlist-wb.xml）とともに、各 Cisco Unified Communications Manager サーバの TFTP ディレクトリに配置されています。

注目 すべてのファイル名で大文字と小文字が区別されます。ファイル名に Ringlist-wb.xml を使用すると、電話機には変更が適用されません。

詳細については、Cisco Unified Communications Manager release 12.0(1) 以降の『Feature Configuration Guide for Cisco Unified Communications Manager』の「Custom Phone Rings and Backgrounds」の章を参照してください。

カスタム背景イメージ

Cisco IP 電話の背景画像または壁紙をカスタマイズできます。壁紙のカスタマイズは、企業のロゴや画像を表示するための一般的な手段であり、多くの組織は電話機を際立たせるためにそれらを使用しています。

ファームウェアリリース 12.7(1) 以降では、電話機とキー拡張モジュールの両方で壁紙をカスタマイズできます。ただし、電話機に 1 つの画像、拡張モジュールに 1つの画像が必要です。

電話機は壁紙の色を分析し、フォントとアイコンの色を変更して読み取れるようにします。壁紙が暗い場合、フォントとアイコンは白に変更されます。壁紙が明るい場合、フォントとアイコンは黒で表示されます。

背景には単色やパターンなどの単純な画像を選択することをお勧めします。コントラストの高い画像は避けてください。

カスタマイズされた壁紙は、次の 2 つの方法のいずれかで追加します。

- リスト ファイルの使用
- 共通の電話プロファイルの使用

ユーザが電話機で利用可能なさまざまな壁紙の中から画像を選択できるようにするには、一覧ファイルを変更します。しかし、電話機に画像をプッシュする場合は、共通の電話プロファイルを作成するか、既存の共通の電話プロファイルを変更します。

どちらの方法を採る場合も、次の点に注意してください。

- 画像は PNG 形式で、フル サイズの画像は次の寸法以内である必要があります。
  - サムネイル画像：139 ピクセル（幅）× 109 ピクセル（高さ）です。
  - Cisco IP 電話 8800 シリーズ：800 × 480 ピクセル
  - Cisco IP 電話 8851 および 8861 キー拡張モジュール、デュアル LCD 画面： 320 x 480 ピクセル
  - Cisco IP 電話 8865 キー拡張モジュール、デュアル LCD 画面：320 x 480 ピクセル
  - Cisco IP 電話 8800 キー拡張モジュール、シングル LCD 画面： 272 x 480 ピクセル
- 画像、サムネイル、およびリストファイルを TFTP サーバにアップロードします。ディレクトリは、次のとおりです。
  - Cisco IP 電話 8800 シリーズ：デスクトップ/800x480x24
  - Cisco IP 電話 8851 および 8861 キー拡張モジュール（デュアル LCD 画面）：デスクトップ/320x480x24
  - Cisco IP 電話 8865 キー拡張モジュール、デュアル LCD 画面： デスクトップ/320x480x24
  - Cisco IP 電話 8800 キー拡張モジュール、シングル LCD 画面： デスクトップ/272x480x24

  アップロードが完了したら、TFTP サーバーを再起動します。
- ユーザーが独自の壁紙を選択できないようにする場合は、**[電話機の背景画像設定へのエンドユーザーアクセスを有効にする（Enable End User Access to Phone Background Image Setting）]** を無効にします。電話プロファイルを保存し、適用します。電話機を再起動して、変更を有効化します。

（注） **[共通電話プロファイル（Common Phone Profile）]** を使用して、電話機の背景画像を一括して適用できます。ただし、一括設定では、**[電話機の背景画像設定へのエンドユーザーを有効にする（Enable End User Access to Phone Background Image Setting）]** を無効にする必要があります。背景画像の一括設定の詳細については、「カスタマイズされた壁紙のベストプラクティス Cisco IP 電話 8800シリーズ」の「「共通電話プロファイルの設定」」の章を参照してください。

壁紙のカスタマイズの詳細については、次のマニュアルを参照してください。

- カスタマイズされた壁紙のベストプラクティス Cisco IP 電話 8800シリーズ。
- Cisco Unified Communications Manager リリース 12.0(1) 以降の『Cisco Unified Communications Manager 機能設定ガイド』の「電話のカスタム呼出音と背景」の章。
- 『Cisco IP 電話 8800 シリーズユーザガイド』の 「設定」 の章。

ワイドバンド コーデックのセットアップ

デフォルトでは、Cisco IP 電話 に G.722 コーデックが有効化されています。 Cisco Unified Communications Manager が G.722 を使用するように設定されており、通話先が G.722 をサポートしている場合、G.711 の代わりに G.722 コーデックを使用してコールを接続します。

この状態は、ユーザがワイドバンド ヘッドセットまたはワイドバンド ハンドセットを有効にしているかどうかを問わず発生します。ヘッドセットまたはハンドセットが有効になっている場合、ユーザはコール中の音声の感度がより高く感じられます。感度が高いことで音声の明瞭さは増しますが、紙が擦れる音や近くの会話といった、通話先周囲のノイズもより多く聞こえます。 ワイドバンドヘッドセットまたはハンドセットがない場合でも、G.722 の高い感度を煩わしく感じるユーザもいます。 ユーザの中には G.722 の高い感度を好むユーザもいます。

[G.722 および iSAC コーデックのアドバタイズ（Advertise G.722 and iSAC Codec）] サービス パラメータは、パラメータが設定されている [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] ウィンドウによって、この Cisco Unified Communications Manager サーバまたは特定の電話機に登録されたすべてのデバイスに対してワイド バンドがサポートされているかどうかに影響します。

手順

ステップ 1 すべてのデバイスにワイド バンドのサポートを設定する方法：

a) Cisco Unified Communications Manager の管理で、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

b) [G.722 および iSAC コーデックのアドバタイズ（Advertise G.722 and iSAC Codec）] フィールドを設定します。

このエンタープライズ パラメータのデフォルト値は Trueです。この Cisco Unified Communications Manager に登録されているすべての Cisco IP 電話 モデルが Cisco Unified Communications Manager に G.722 をアドバタイズすることを意味します。 コールにおいて通話元および通話先の電話機が機能セットで G.722 をサポートしている場合、Cisco Unified Communications Manager は可能な限りこのコーデックを選択します。

ステップ 2 特定のデバイスにワイド バンドのサポートを設定する方法：

a) From Cisco Unified Communications Manager の管理で、**[デバイス（Device）] > [電話（Phone）]** を選択します。

b) [プロダクト固有の設定（Product Specific Configuration Layout）] 領域の [G.722 および iSAC コーデックのアドバタイズ（Advertise G.722 and iSAC Codec）] パラメータを設定します。

この製品固有のパラメータのデフォルト値には、エンタープライズ パラメータで指定されている値を使用します。 電話機ごとにこれを上書きする場合は、[有効（Enabled）]または [無効（Disabled）]を選択します。

未使用時画面のセット アップ

電話機のスクリーンに表示されるアイドル表示（テキストのみ。テキスト ファイルのサイズは 1 MB 以下）を指定できます。アイドル表示は XML サービスです。このサービスは、指定された期間にわたって電話機がアイドル（未使用）状態にあり、機能メニューが開いていない場合に、電話機によって呼び出されます。

アイドル表示の作成および表示方法の詳細については、次の URL で『*Creating Idle URL Graphics on Cisco IP* 電話』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

また、次の情報については、ご使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

- アイドル表示 XML サービスの URL の指定
  - 1 台の電話機に指定する場合：Cisco Unified Communications Manager の管理ページの [電話の設定（Phone configuration）] ウィンドウにある [アイドル（Idle）] フィールド。
  - 複数の電話機に同時に指定する場合：[エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウにある [URL アイドル（URL Idle）] フィールド、または一括管理ツール（BAT）の [アイドル（Idle）] フィールド
- アイドル表示 XML サービスを起動するまでの電話機の未使用時間の指定

- 1 台の電話機に指定する場合：Cisco Unified Communications Manager の管理ページの [電話の設定（Phone configuration）] ウィンドウにある [アイドル タイマー（Idle Timer）] フィールド。
- 複数の電話機に同時に指定する場合：[エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウにある [URL アイドル時間（URL Idle Time）] フィールド、または一括管理ツール（BAT）の [アイドル タイマー（Idle Timer）] フィールド

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 [アイドル（Idle）] フィールドに、未使用時画面 XML サービスの URL を入力します。

ステップ 3 [アイドル タイマー（Idle Timer）] フィールドに、未使用時画面 XML サービスを表示するまでアイドル状態の電話機が待機する時間を入力します。

ステップ 4 **保存**を選択します。

ダイヤル トーンのカスタマイズ

内部コールと外部コールで異なるダイヤル トーンが鳴るように電話機をセットアップできます。 必要に応じて、3 つのダイヤル トーンのオプションから選択できます。

- [デフォルト（Default）]：内部コールと外部コールに異なるダイヤル トーンを使用します。
- [内部（Inside）]：内部用のダイヤル トーンをすべてのコールに使用します。
- [外部（Outside）]：外部用のダイヤル トーンをすべてのコールに使用します。

[常に使用するダイヤル トーン（Always Use Dial Tone）] は、Cisco Unified Communications Manager の必須フィールドです。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 該当するサーバを選択します。

ステップ 3 サービスとして [Cisco CallManager] を選択します。

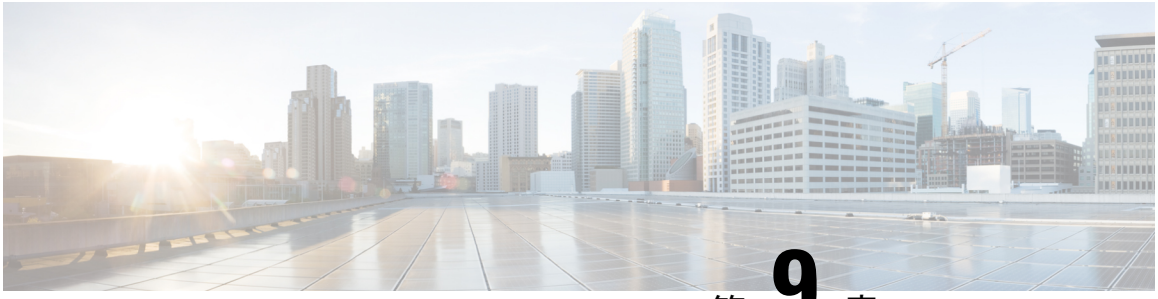
ステップ 4 [クラスタ全体のパラメータ（Clusterwide Parameters）] ペインまでスクロールします。

ステップ 5 [常に使用するダイヤル トーン（Always Use Dial Tone）] を次のいずれかに設定します。

- 外側
- 内側
- デフォルト

ステップ 6 **保存**を選択します。

ステップ 7 電話機を再起動します。



第 9 章

電話機の機能および設定

電話機の機能および設定の概要

Cisco IP 電話 をネットワークに設置し、ネットワークの設定値を設定して、IP Phone を Cisco Unified Communications Manager に追加した後は、Cisco Unified Communications Manager の管理アプリケーションを使用して、テレフォニー機能を設定する必要があります。必要に応じて、電話テンプレートの修正、サービスのセットアップ、ユーザの割り当ても行います。

Cisco IP 電話のその他の設定値は、Cisco Unified Communications Manager の管理ページで変更できます。 この Web ベースのアプリケーションを使用して、電話機登録基準とコーリング サーチ スペースのセットアップ、社内ディレクトリとサービスの設定、電話ボタンテンプレートの修正、その他のタスクを行うことができます。

電話回線キーに機能を追加する場合、使用できる回線キーの数には制限があります。使用している電話機の回線キーの数を超えて機能を追加することはできません。

Cisco IP 電話 ユーザのサポート

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 IP 電話 ユーザの主な情報源になります。 最新の詳細な情報をエンド ユーザに提供する必要があります。

Cisco IP 電話の機能（サービスおよびボイス メッセージ システムのオプションなど）を正常に使用するには、ユーザはシステム管理者やシステム管理者のネットワーク チームから情報を入手する必要があります。また、システム管理者に支援を依頼できる環境が必要です。 支援を求める際の連絡先の担当者の名前、およびそれらの担当者に連絡する手順をユーザに提供しておく必要があります。

エンド ユーザに Cisco IP 電話に関する重要な情報を提供するために、社内のサポート サイトに Web ページを作成することをお勧めします。

このサイトには、次のタイプの情報を含めるように考慮してください。

- サポートされているすべての Cisco IP 電話 モデルのユーザ ガイド
- Cisco Unified Communications セルフケアポータルへのアクセス方法について
- サポートされている機能のリスト
- ボイスメール システムのユーザ ガイドまたはクイック リファレンス

電話機能

Cisco IP 電話 を Cisco Unified Communications Manager に追加した後、電話機に機能を追加できます。次の表に、サポートされているテレフォニー機能のリストを示します。これらの多くは、Cisco Unified Communications Manager の管理ページを使用して設定できます。

電話機でのこれらの機能の使用に関する詳細については、『*Cisco IP* 電話 *8800 Series User Guide*』を参照してください。プログラム可能ボタンおよび専用のソフトキーや機能ボタンとして設定できる機能の一覧については、機能ボタンとソフトキー（157ページ）を参照してください。

（注） Cisco Unified Communications Manager の管理ページには、各種のテレフォニー機能を設定するためのサービス パラメータもいくつかあります。サービス パラメータのアクセスと設定についての詳細は、誤使用の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

サービスの機能の詳細については、プロダクト固有の設定 ウィンドウでパラメータ名を選択するか、ヘルプ ボタン（?）を選択します。

詳細については、特定の Cisco Unified Communications Manager リリースのマニュアルを参照してください。

機能	説明と詳細情報
短縮ダイヤル	ユーザは、事前に割り当てておいたインデックス コード（1 ～ 199）を電話機のキーパッドで入力することで、電話番号をすばやくダイヤルできます。 （注）　短縮ダイヤルは、オンフックでもオフフックでも使用できます。 ユーザはセルフ ケア ポータルからインデックス コードを割り当てます。
実行可能な着信呼警告	着信呼警告を制御するさまざまなオプションを提供します。呼警告を無効または有効にできます。また、発信者 ID 表示をアクティブ化/非アクティブ化することもできます。 プロダクト固有の設定 （161 ページ）の「実行可能な着信呼警告」を参照してください。
電話機での AES 256 暗号化サポート	TLS 1.2 および新しい暗号をサポートすることで、セキュリティが向上します。詳細については、サポート対象のセキュリティ機能 （96 ページ）を参照してください。
エージェントのグリーティング	エージェントが事前録音したグリーティングを作成したり更新したりできるようにします。このグリーティングは、エージェントが発信者と話しはじめる前に、顧客コールの開始時に再生されます。エージェントは、必要に応じて 1 つまたは複数のグリーティングを事前録音できます。 エージェント グリーティングの有効化 （197 ページ）を参照してください。
すべてのコール ピックアップ	コールがどのように電話機にルーティングされたかに関係なく、ユーザはコール ピックアップ グループ内の任意の回線でコールをピックアップできます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコール ピックアップの情報を参照してください。
アプリケーション ダイヤル ルール	共有された携帯電話の連絡先の番号を、ネットワークでダイヤル可能な番号へ変換するために使用されます。 アプリケーション ダイヤル ルール （88 ページ）を参照してください。
処理されたダイレクト コール パーク	ユーザは、ダイレクト パーク機能を使用して、1 つのボタンを押すだけでコールをパークすることができます。管理者は、ビジー ランプ フィールド（BLF）の [処理されたダイレクト コール パーク（Assisted Directed Call Park）] ボタンを設定する必要があります。アクティブ コールに対してアイドルな BLF の [処理されたダイレクト コール パーク（Assisted Directed Call Park）] ボタンを押すと、アクティブ コールは、[処理されたダイレクト コール パーク（Assisted Directed Call Park）] ボタンに関連付けられたダイレクト パーク スロットにパークされます。 該当する Cisco Unified Communications Manager リリースのマニュアルの処理されたダイレクト コール パークの情報を参照してください。

機能	説明と詳細情報
オーディオメッセージ受信インジケータ（AMWI）	ハンドセット、ヘッドセット、またはスピーカーフォンから聞こえるスタッタ音により、ユーザが回線で新しいボイスメッセージを1つ以上受信したことが示されます。 （注） スタッター音は回線によって異なります。この音が聞こえるのは、使用中の回線でメッセージを受信した場合のみです。
自動応答	呼出音を 1 ～ 2 回鳴らした後に、着信コールを自動的に接続します。 自動応答は、スピーカーフォンとヘッドセットのどちらでも機能します。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。
自動ポート同期	電話機のポート間で最も低い速度にポートを同期し、パケット損失を防止します。 プロダクト固有の設定 （161 ページ）の「自動ポート同期」を参照してください。
自動ピックアップ	ユーザは、コールピックアップのための、ワンタッチのピックアップ機能を使用できます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコールピックアップの情報を参照してください。
割込み	ユーザは、ターゲットの電話に組み込まれた会議ブリッジを使用して三者電話会議を確立することにより、コールに割り込むことができます。 この表の「c 割込」を参照してください。
外線から外線への転送のブロック	外線コールをユーザが別の外線コールに転送することを禁止します。 該当する Cisco Unified Communications Manager リリースのマニュアルの外部コールの転送の情報を参照してください。
Bluetooth マルチ接続	複数のデバイスを電話機にペアリングできます。したがって、Bluetooth を使用するモバイル デバイスと Bluetooth ヘッドセットを同時に接続できます。 Cisco IP 電話 8851NR は Bluetooth をサポートしていません。
ビジー ランプ フィールド（BLF）	ユーザは、電話機のスピード ダイヤル ボタンに関連付けられている電話番号のコール状態をモニタできます。 該当する Cisco Unified Communications Manager リリースのマニュアルのプレゼンスの情報を参照してください。

機能	説明と詳細情報
ビジー ランプ フィールド（BLF）ピックアップ	BLF 短縮ダイヤルの拡張機能です。ユーザが着信コールをモニタリングできるように、電話番号を設定できます。電話番号が着信コールを受信すると、モニタリングしているユーザに対してシステムからアラートが発生し、コールをピックアップすることができます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコールピックアップの情報を参照してください。
折返し	通話の相手が話し中や通話不能だった場合、その相手が通話可能になったときに、ユーザの電話機に音声による通知と画面表示による通知が送信されます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコールバックの情報を参照してください。
コール表示の制限	発信回線および接続回線について表示する情報を、コールに関係する通話相手に応じて決定します。 該当する Cisco Unified Communications Manager リリースのマニュアルのルーティング計画およびコール表示の制限の情報を参照してください。
コール転送	ユーザは、着信コールを別の番号にリダイレクトできます。コール転送オプションには、すべてのコールの転送、話中転送、無応答時転送、およびカバレッジなし時転送があります。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報およびセルフケアポータルの表示のカスタマイズ （92 ページ）を参照してください。
不在転送ループのブレークアウト	不在転送ループを検出して防止します。不在転送ループが検出されると、[すべてのコールの転送（Call Forward All）] の設定が無視されて呼出音が鳴ります。
すべてのコールの転送のループ防止	不在転送ループを検出して防止します。不在転送ループが検出されると、[すべてのコールの転送（Call Forward All）] の設定が無視されて呼出音が鳴ります。
コール転送時の表示内容の設定	ユーザが、[すべてのコールの転送（Call Forward All）] の接続先を電話機で直接設定する際に、不在転送ループが生じたり、既存の Forward Maximum Hop Count サービスパラメータに定められたホップ数の上限を超える不在転送チェーンが生じたりしないように防止します。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。

機能	説明と詳細情報
不在転送の接続先の無効化	管理者は、すべてのコールの転送（CFA）の接続先が CFA の転送元にコールを発信する場合にはCFA を無効にすることができます。この機能により、CFA の接続先は、重要なコールがある場合に CFA の転送元に到達できるようになります。この上書きは、CFA の宛先電話番号が内部と外部のどちらであっても機能します。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。
コールの転送通知	転送されたコールを受信したときに表示される情報を設定できます。 コールの転送通知のセット アップ （199 ページ）を参照してください。
共有電話のコール履歴	電話機の通話履歴に共有電話のアクティビティを表示できるようにします。この機能により次の内容が可能になります。 • 共有回線の不在着信をログに記録する • 共有回線のすべての応答済み着信と発信履歴をログに記録する
コール パーク	ユーザがコールをパーク（一時的に保存）し、Cisco Unified Communications Manager システムの別の電話機を使用してそのコールに応答できます。 **[プロダクト固有の設定（Product Specific Configuration Layout）]** ペインで**[コール パーク専用の 1 回線 (Dedicate one line for call park)]** フィールドを設定して、コールを元の回線または別の回線にパークできます。 このフィールドが有効になっている場合、パークされたコールはユーザの回線に残り、**再開 (Resume)** ソフトキーを使用してコールをピックアップできます。電話機のディスプレイに、パークされているコールの内線番号が表示されます。 このフィールドを無効にすると、パークされたコールはコール パーク回線に転送されます。ユーザの回線がアイドル状態に戻り、ポップアップ ウィンドウにコール パーク内線が表示されます。ユーザが内線をダイヤルして電話を取ります。 該当する Cisco Unified Communications Manager リリースのマニュアルのコール パークの情報を参照してください。
コール ピックアップ	ユーザは、自分のピックアップ グループに属する別の電話機で呼出音が鳴っている場合に、そのコールを自分の電話機にリダイレクトできます。 電話機のプライマリ回線に、音声によるアラートと画面表示によるアラートを設定できます。このアラートによって、ピックアップ グループ内でコールの呼び出しがあることが通知されます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコール ピックアップの情報を参照してください。

機能	説明と詳細情報
通話録音	スーパーバイザは、アクティブ コールを記録できます。コールが記録されている場合、コール中に記録音声アラート トーンがユーザに聞こえることがあります。 コールがセキュアな場合、そのコールのセキュリティ ステータスが Cisco IP 電話に鍵のアイコンとして表示されます。コールがセキュアであり、記録されていることを示す音声アラート トーンは、接続先の通話者にも聞こえることがあります。 （注） アクティブ コールがモニタまたは記録されている場合、インターコム コールの受信または発信は可能ですが、インターコム コールを発信するとアクティブ コールが保留になります。これにより、録音セッションは終了し、モニタリング セッションは一時停止されます。モニタリング セッションを再開するには、コールをモニタされている通話者がコールを再開する必要があります。 該当する Cisco Unified Communications Manager リリースのマニュアルのモニタリングおよび録音の情報を参照してください。
コール待機	コールの最中に別の着信コールの呼出音が鳴っていることを通知し、ユーザが応答できるようにします。また、着信通話情報を電話スクリーンに表示します。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。
コール待機呼び出し音	標準ビープ音の代わりに呼び出し音を鳴らすオプションを、コール待機中のユーザに提供します。 オプションは、[一度鳴らす（Ring Once）] および [鳴らす（Ring）] です。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。
発信者 ID	電話番号、名前、その他の説明テキストなど、発信者の識別情報を電話スクリーンに表示します。 該当する Cisco Unified Communications Manager リリースのマニュアルのルーティング計画、コール表示の制限、および電話番号の情報を参照してください。
発信者 ID ブロック	発信者 ID が有効になっている電話機から、ユーザが自分の電話番号または電子メール アドレスをブロックできるようにします。 該当する Cisco Unified Communications Manager リリースのマニュアルのルーティング計画および電話番号の情報を参照してください。

機能	説明と詳細情報
発信側正規化	発信側の正規化では、ダイヤル可能な電話番号として電話番号がユーザに示されます。エスケープ コードが番号に付加されるため、ユーザは簡単に発信者に再度接続できます。ダイヤル可能な番号は通話履歴に保存され、個人アドレス帳に保存できます。
SIP の CAST サポート	Cisco Unified Video Advantage（CUVA）と Cisco IP 電話の間の通信を確立し、IP Phone がビデオ機能を装備していない場合でも PC でビデオを使用できるようにします。
C 割り込み	共有電話回線でプライベート コール以外のコールに参加できます。C 割込によってユーザがコールに追加され、会議に変換されることにより、ユーザと他の通話者が会議機能にアクセス可能になります。電話会議は、Cisco Unified Communications Manager の会議ブリッジ機能を使用して作成されます。 C 割り込みを正しく機能させるには、ソフトキーと Conference Bridge の両方の機能を有効にする必要があります。 ファームウェア リリース 10.2(2) 以降では、C 割り込み機能には [割り込み（Berge）] ソフトキーを使用してアクセスします。 詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』の「Barge」の章を参照してください。
モバイル デバイスの充電	Cisco IP 電話の USB ポートに接続することで、モバイル デバイスを充電できます。 『*Cisco IP 電話 8800 Series User Guide*』を参照してください。
Cisco Extension Mobility	共有 Cisco IP 電話 からの回線の状態、サービス、短縮ダイヤルなどの、Cisco IP 電話 設定へのアクセス権をユーザに付与します。 Cisco エクステンション モビリティは、社内の複数の場所でユーザが業務を実行する場合や、作業場を同僚と共有する場合に便利です。
Cisco Extension Mobility Cross Cluster（EMCC）	特定のクラスタで設定されたユーザが、別のクラスタにある Cisco IP 電話にログインできるようにします。ユーザはホーム クラスタから、訪問先クラスタにある Cisco IP 電話にログインします。 （注） EMCC を設定する前に、Cisco IP 電話で Cisco Extension Mobility を設定してください。
Cisco IP Manager Assistant（IPMA）	コール ルーティングやその他のコール管理機能を提供し、マネージャおよびアシスタントがより効率的に電話機を扱えるようにします。 Cisco IP Manager Assistant のセットアップ （216 ページ）を参照してください。

機能	説明と詳細情報
Cisco IP 電話 8800 キー拡張モジュール Cisco IP Phone 8851/8861 キー拡張モジュール Cisco IP 電話 8865 キー拡張モジュール	拡張モジュールを電話機に追加することによって、追加のキーを提供します。 詳細については、『*Cisco IP 電話 7800 and 8800 Series Accessories Guide for Cisco Unified Communications Manager*』を参照してください。
Cisco IP Phone 8811 サポート	のサポートを提供しますCisco IP Phone 8811。
Cisco IP 電話 8851NR のサポート	Cisco IP 電話 8851NR に対するサポートを提供します。
Cisco Unified Communications Manager Express（Unified CME）のバージョンネゴシエーション	Cisco Unified Communication Manager Express は、電話機に送信される情報内で特殊なタグを使用して自身を識別します。このタグにより、電話機はスイッチがサポートしているサービスをユーザに提供できます。 次を参照してください。 • 『*Cisco Unified Communications Manager Express System Administrator Guide*』 • Cisco Unified Communications Manager Express の連携 （24 ページ）
Cisco Unified Video Advantage（CUVA）	Cisco IP 電話、パーソナル コンピュータ、およびビデオ カメラを使用することにより、ユーザがビデオ コールを発信できます。 （注） [電話の設定（Phone Configuration）] の [プロダクト固有の設定（Product Specific Configuration Layout）] で、ビデオ機能のパラメータを設定します。 Cisco Unified Video Advantage のマニュアルを参照してください。
Cisco WebDialer	Webおよびデスクトップ アプリケーションから電話をかけることができます。
従来の呼出音	電話機ファームウェア組み込みの、またはCisco Unified Communications Managerからダウンロードされる呼出音をサポートします。この機能により、使用可能な呼出音を他の Cisco IP 電話 と共通化できます。 カスタム電話呼出音 （129 ページ）を参照してください。

機能	説明と詳細情報
会議	ユーザは、各参加者を個別に呼び出して、複数の通話相手と同時に話すことができます。会議機能には、会議とミートミーがあります。 標準（アドホック）会議では、開催者以外でも参加者を追加または削除できます。また、どの会議参加者でも同じ回線上の 2 つの標準会議を結合できます。 [拡張アドホック会議（Advance Adhoc Conference）] サービス パラメータ（Cisco Unified Communications Manager の管理ページではデフォルトで無効になっています）を使用すれば、これらの機能を有効化できます。 （注） ユーザに対し、これらの機能がアクティブであるかどうかを必ず通知してください。
PC用およびスイッチ ポート用の設定可能な Energy Efficient Ethernet（EEE）	EEE を有効または無効にすることにより、 PC ポートとスイッチ ポートでの EEE 機能を制御する手段を提供します。この機能は両方のタイプのポートを個別に制御します。デフォルト値は [有効（Enabled）] です。 スイッチおよび PC ポート用の Energy Efficient Ethernet のセットアップ （201 ページ）を参照してください。
設定可能なフォント サイズ	フォント サイズを変更することにより、IP phone に表示される [通話履歴（Call History）] および [コール画面（Call Screen）] の最大文字数を増減できます。 フォントが小さいと表示される最大文字数が増加し、フォントが大きいと表示される最大文字数が減少します。
CTI アプリケーション	Computer Telephony Integration（CTI）ルート ポイントでは、仮想デバイスを指定して、アプリケーションが宛先変更を制御している多重同時コールを受信することができます。
すべて拒否	ユーザは、呼び出し中のコール、接続されたコール、または保留中のコールを、ボイス メッセージ システムに直接転送できます。コールが拒否されると、その回線は新しいコールの発信または受信に使用できるようになります。 該当する Cisco Unified Communications Manager リリースのマニュアルの即時転送の情報を参照してください。
デバイスから呼び出された録音	エンドユーザがソフトキーを使用して電話コールを録音できる機能を提供します。 また、管理者はCTIユーザ インターフェイスを使用して電話コールの録音を継続できます。 該当する Cisco Unified Communications Manager リリースのマニュアルのモニタリングおよび録音の情報を参照してください。

機能	説明と詳細情報
ダイレクト コール パーク	ユーザが、使用可能なダイレクト コール パーク番号をダイヤルまたは短縮ダイヤルし、その番号にアクティブなコールを転送できる機能です。コール パーク BLF ボタンは、ダイレクト コール パーク番号が使用中かどうかを表示するとともに、ダイレクト コール パーク番号への短縮ダイヤル アクセスにも使用できます。 （注） ダイレクト コール パーク機能を実装する場合は、[パーク（Park）] ソフトキーを設定しないでください。これは、ユーザが2つのコール パーク機能を混同するのを防ぐためです。 該当する Cisco Unified Communications Manager リリースのマニュアルのコール パークの情報を参照してください。
バッテリ強度アイコンおよび信号強度アイコンの表示	Bluetooth を使用して携帯電話が IP 電話に接続されている場合に、携帯電話のバッテリおよび信号の強度を IP 電話に表示します。 Cisco IP 電話 8851NR は Bluetooth をサポートしていません。
固有呼び出し音	ユーザは、着信コールや新しいボイス メッセージを電話機で示す方法をカスタマイズできます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコール ピックアップの情報を参照してください。
サイレント（DND）	DND をオンにすると、コールが呼び出し状態になっても呼出音が鳴らなくなります。またあらゆる種類の表示や音による通知も、一切行われません。 有効にすると、電話機のヘッダーの色が赤色に変わり、電話機に「サイレント（Do Not Disturb）」と表示されます。 Multilevel Precedence and Preemption（MLPP）が設定されていて、ユーザが高優先度コールを受信した場合、電話機で特殊な呼出音が鳴ります。 サイレントの設定 （196 ページ）を参照してください。
JAL/TAL の有効化/無効化	管理者が複数ライン同時通話（JAL）機能および回線間直接転送（TAL）機能を制御できます。 プロダクト固有の設定 （161 ページ）の「参加および直接転送ポリシー」を参照してください。
EnergyWise	省エネのために、あらかじめ決められた時刻に IP 電話をスリープ（電源オフ）および復帰（電源オン）させることができます。 Cisco IP 電話 での EnergyWise のスケジュール （191 ページ）を参照してください。

機能	説明と詳細情報
拡張回線モード	拡張回線モードを有効にすると、電話画面の両側にあるボタンを回線キーとして使用できるようになります。 「追加回線キーのセットアップ （230 ページ）」を参照。
セキュアな拡張機能の機能強化	ネットワークとセキュリティの設定がログイン電話で保存されるため、セキュアな拡張機能が強化されます。これにより、セキュリティ ポリシーが保持され、ネットワーク帯域幅が維持されて、訪問先クラスタ（VC）内のネットワーク障害が回避されます。
ファスト ダイヤル サービス	ユーザは、ファスト ダイヤル コードを入力してコールを発信できます。ファスト ダイヤル コードは、電話番号または [個人アドレス帳（Personal Address Book）] エントリに割り当てることができます。この表の「サービス」を参照してください。 PAB またはファスト ダイヤル用の電話ボタン テンプレートの変更 （228 ページ）を参照してください。
グループ コール ピックアップ	ユーザが、別のグループの電話番号で呼び出し音が鳴っているコールに応答することができます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコール ピックアップの情報を参照してください。
ヘッドセットの側音の制御	管理者は、有線ヘッドセットの側音レベルを設定できます。
保留復帰	コールの保留時間を制限します。制限時間が経過すると、コールは保留にした側の電話機に復帰し、ユーザにアラートが通知されます。 復帰コールの通知は、着信コールの場合とは異なり、1 回の呼出音（回線の新規コール インジケータの設定によってはビープ音）によって行われます。この通知は、コールが再開されるまで、一定の間隔で繰り返されます。 コールが保留復帰した場合は、さらに、コール バブルにアニメーションのアイコンが表示されます。コールのフォーカス優先度を着信コールまたは復帰コールのどちらかに設定できます。
保留状態	共有電話を持つ電話機では、ローカル回線とリモート回線のいずれがコールを保留したのかを区別できます。
保留または復帰	ユーザは、接続されたコールをアクティブな状態から保留状態に移行できます。 • 設定は必要ありません。ただし、保留音を使用する場合には必要です。詳細については、この表の「保留音」を参照してください。 • この表の「保留復帰」を参照してください。

機能	説明と詳細情報
HTTP ダウンロード	HTTP をデフォルトで使用することで、電話機へのファイルのダウンロード プロセスが向上します。HTTP ダウンロードが失敗した場合、電話機は TFTP ダウンロードの使用に戻ります。
ハント グループ	主要な電話番号へのコールに対して、ロードシェアリングを行います。ハント グループには、着信コールに応答できる一連の電話番号が含まれています。ハント グループ内の最初の電話番号が話し中の場合、システムは、グループ内で次に使用可能な電話番号を所定の順序で検索して特定し、その電話機にコールを転送します。 ハントグループコールの着信アラートに**発信者 ID**（発信者 ID が設定されている場合)、**電話番号**、**ハントグループパイロット番号**を表示できます。ハント グループの番号は、「ハントグループ（Hunt Group）」というラベルの後に表示されます。 該当する Cisco Unified Communications Manager リリースのマニュアルのハント グループおよびルーティング計画の情報を参照してください。
着信コール Toast タイマー	電話機の画面に着信コール Toast（通知）が表示される時間を設定できます。 プロダクト固有の設定 （161 ページ）の「着信コール Toast タイマー」を参照してください。
インテリジェントプロキシミティ	Bluetooth を使用してモバイル デバイスと電話機をペアリングし、電話機を使用してモバイル コールの発信および受信ができるようになります。 インテリジェント プロキシミティの有効化 （235 ページ）を参照してください。 Cisco IP 電話 8811、8841、および 8851NR は、Bluetooth およびインテリジェント プロキシミティをサポートしていません。
インターコム	ユーザが、プログラム可能な電話のボタンを使用して、インターコムコールを発信したり受信したりできます。インターコム回線のボタンを設定すると、次を実行できます。 • 特定のインターコム内線番号への直接的なダイヤル。 • インターコムコールを開始してから、有効なインターコム番号の入力をユーザに要求。 （注） ユーザが毎日同じ電話機にログインする場合は、それらのユーザの Cisco Extension Mobility のプロファイルを使用し、インターコム情報を含む電話ボタン テンプレートをユーザのプロファイルに割り当て、その電話機をインターコム回線のデフォルトのインターコム デバイスとして指定します。

機能	説明と詳細情報
IPv6 専用のサポート	Cisco IP 電話での拡張 IP アドレッシングをサポートします。IPv4 と IPv6 の構成が推奨されており、完全にサポートされます。機能の中にはスタンドアロン設定でサポートされていないものもあります。IPv6アドレスのみが割り当てられます。 ネットワークの設定 （63 ページ）を参照してください。
ジッター バッファ	ジッター バッファ機能は、オーディオ ストリームについて 10 ミリ秒（ms）～ 1000 ms のジッターを処理します。 これは、Adaptive モードで動作し、ジッターの量に合わせて動的に調整されます。
参加	ユーザが、同一電話回線上にある 2 つのコールを、1 つの会議コールとして接続したうえで、そのコールに留まることができます。
コール リストの回線ステータス	ユーザは、モニタ対象の回線番号の回線ステータス（可用性ステータス）を通話履歴リストで確認できます。回線ステータスには、次の状態があります。 • オフライン • 利用可能 • 使用中 • サイレント コール リストの BLF の有効化 （200 ページ）を参照してください。
社内ディレクトリの回線ステータス	社内ディレクトリの連絡先のステータスを表示できます。 • オフライン • 利用可能 • 使用中 • サイレント コール リストの BLF の有効化 （200 ページ）を参照してください。
回線テキスト ラベル	電話番号の代わりに電話回線のテキスト ラベルを設定します。 回線のラベルの設定 （211 ページ）を参照してください。

機能	説明と詳細情報
ハント グループからのログアウト	ユーザは、コールを受けることができない場合に、ハント グループからログアウトし、一時的にユーザの電話機で呼出音が鳴らないようにすることができます。ハント グループからログアウトしても、ハント グループ以外のコールでは、引き続き電話機で呼出音が鳴ります。 該当する Cisco Unified Communications Manager リリースのマニュアルのルーティング計画の情報を参照してください。
迷惑呼 ID（MCID）	ユーザが、不審なコールを受信したことをシステム管理者に通知できる機能です。
Meet-Me 会議	ユーザがミートミー会議を開始し、参加ユーザは予定の時刻に、あらかじめ決められた番号にコールをかけます。
メッセージ待機	メッセージ待機のオンおよびオフのインジケータに対する電話番号を定義します。直接接続型のボイス メッセージ システムでは、指定された電話番号を使用して、特定の Cisco IP 電話のメッセージ待機インジケータを設定したりクリアしたりします。 該当する Cisco Unified Communications Manager リリースのマニュアルのメッセージ受信およびボイス メールの情報を参照してください。
メッセージ待機インジケータ	ハンドセットのランプの 1 つで、ユーザに対する 1 つまたは複数の新着ボイス メッセージが届いていることを示します。 該当する Cisco Unified Communications Manager リリースのマニュアルのメッセージ受信およびボイス メールの情報を参照してください。
最小呼出音量	IP 電話の最小呼び出し音量レベルを設定します。
不在履歴のログ	ユーザが、特定のラインアピアランスで不在履歴を不在履歴ディレクトリに記録するかどうかを指定できるようにします。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。
モバイル コネクト	ユーザは、1 つの電話番号を使用してビジネス コールを管理したり、デスクトップ電話機および携帯電話などのリモート デバイスで、進行中のコールをピックアップしたりすることができます。また、電話番号や時刻に応じて、発信者グループを制限できます。 該当する Cisco Unified Communications Manager リリースのマニュアルの Cisco Unified Mobility の情報を参照してください。
Expressway 経由でのモバイルおよび Remote Access	これを使用すると、リモート ワーカーは、仮想プライベート ネットワーク（VPN）クライアント トンネルを使用しなくても企業のネットワークに簡単かつ安全に接続できます。 「Expressway 経由でのモバイルおよび Remote Access （203 ページ）」を参照。

機能	説明と詳細情報
モバイル ボイス アクセス	モバイル コネクト機能が拡張され、ユーザは自動音声応答（IVR）システムにアクセスして、携帯電話などのリモートデバイスからコールを発信できるようになります。 該当する Cisco Unified Communications Manager リリースのマニュアルの Cisco Unified Mobility を参照してください。
モニタリングと録音	スーパーバイザは、アクティブ コールのサイレント モニタリングを実行できます。スーパーバイザの音声はコールのどちらの側にも聞こえません。コールがモニタされている場合、コール中にモニタリング音声アラート トーンがユーザに聞こえることがあります。 コールがセキュアな場合、そのコールのセキュリティ ステータスが Cisco IP 電話に錠前アイコンとして表示されます。コールがセキュアであり、モニタリングされていることを示す音声アラート トーンは、接続先の通話者にも聞こえることがあります。 （注） アクティブ コールがモニタまたは録音されている場合、ユーザはインターコム コールを受信または発信できますが、インターコム コールを発信するとアクティブ コールが保留になります。これにより、録音セッションは終了し、モニタリング セッションは一時停止されます。モニタリング セッションを再開するには、コールをモニタされている通話者がコールを再開する必要があります。
Multilevel Precedence and Preemption	軍や官庁のような特別な環境にいるユーザが緊急または重要なコールを発信/受信できるようにします。 Multilevel Precedence and Preemption （222 ページ）を参照してください。
ラインアピアランス1つあたりのコール数	各回線は複数のコールに対応できます。デフォルトで、電話機は 1 回線あたり 2 つのアクティブ コールをサポートし、最大で 1 回線あたり 6 つのアクティブ コールをサポートします。ある時点では 1 コールだけが接続でき、他のコールは自動的に保留になります。 システムでは、最大コール/ビジー トリガーを 6/6 以下で設定できます。6/6 を超える設定は公式にはサポートされていません。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。
保留音	発信者が保留状態になっている間、音楽を再生します。
ミュート	ハンドセットまたはヘッドセットのマイクをミュート状態にします。
アラート名なし	元の発信者の電話番号を表示することで、エンドユーザが転送されたコールを簡単に識別できるようにします。コールはアラート コールとして表示され、その後に発信者の電話番号が表示されます。

機能	説明と詳細情報
オンフック ダイヤル	ユーザは、オフ フックにすることなく、番号をダイヤルできます。次に、ハンドセットを持ち上げるか、[ダイヤル（Dial）] を押します。
他グループ コール ピックアップ	ユーザは、ユーザのグループに関連付けられている別のグループの電話機で呼出音が鳴っている場合に、そのコールに応答できます。 該当する Cisco Unified Communications Manager リリースのマニュアルのコール ピックアップの情報を参照してください。
エクステンション モビリティ ユーザ向けの電話機の表示メッセージ	この機能は、わかりやすいメッセージを提供することで、エクステンション モビリティ ユーザの電話インターフェイスを拡張します。
Cisco Unified Communications Manager の電話機信頼リスト通知	信頼リスト（TL）が更新されたときに、電話機が Cisco Unified Communications Manager にアラームを送信できるようになります。 サポート対象のセキュリティ機能 （96 ページ）を参照してください。
キュー統計情報の PLK サポート	キュー統計情報の PLK サポート機能により、ユーザは、ハント パイロットのコール キュー統計を照会することができ、情報が電話機の画面に表示されます。
プラス ダイヤル	ユーザが先頭にプラス（+）記号を付けて E.164 番号をダイヤルできるようにします。 +記号をダイヤルするには、ユーザはアスタリスク（*）キーを1秒以上押し続ける必要があります。これは、オンフック（編集モードを含む）またはオフフック コールの最初の桁のダイヤルに適用されます。
LLDP での電力ネゴシエーション	電話機では Link Level Endpoint Discovery Protocol（LLDP）および Cisco Discovery Protocol（CDP）を使用して電力をネゴシエートできます。 プロダクト固有の設定 （161 ページ）の「電力ネゴシエーション」を参照してください。
プレディクティブ ダイヤリング	コールの発信を簡略化します。ダイヤルしている番号と類似した電話番号のみを表示するように通話履歴リストが変更されます。 プレディクティブ ダイヤリングは、[拡張回線モード（Enhanced Line Mode）] が有効になっているときに有効になります。プレディクティブ ダイヤリングを機能させるには、[簡易発信 UI（Simplified New Call UI）] を無効にする必要があります。
プライバシー	回線を共有しているユーザが、コールに自分を追加すること、および他のユーザのコールに関する情報を電話ディスプレイに表示することを禁止します。 該当する Cisco Unified Communications Manager リリースのマニュアルの割り込みおよびプライバシーの情報を参照してください。

機能	説明と詳細情報
Private Line Automated Ringdown（PLAR）	Cisco Unified Communications Manager の管理者は、ハンドセットをオフ フックにすると Cisco IP 電話がただちにダイヤルする電話番号を設定できます。これは、緊急番号や 「ホットライン」 番号のコール用に指定された電話機で役立つことがあります。 管理者は、最大 15 秒の遅延を設定できます。これにより、電話機がデフォルトでホットライン番号に設定される前にコールを発信する時間がユーザーに与えられます。このタイマーは、パラメータ **[オフフックから最初の数字タイマー（Off Hook To First Digit Timer）]**（**[デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP プロファイル（SIP Profile）]**）で設定可能です。 詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。
エラー レポート ツール（PRT）	電話機のログを送信するか、問題を管理者に報告します。 問題レポート ツール （208 ページ）を参照してください。
プログラマブル機能ボタン	発信、折り返し、不在転送などの機能を回線ボタンに割り当てることができます。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話機ボタン テンプレートの情報を参照してください。
Quality Reporting Tool（QRT; 品質レポートツール）	ユーザが、ボタンを押して、問題のあるコールの情報を送信できます。QRT は、QRT に必要なユーザ インタラクションの量に応じて、2 つのユーザ モードのどちらかに設定できます。
通話履歴	ユーザが、最近の 150 件の個別コールおよびコール グループを確認できます。最近ダイヤルした番号や不在履歴を表示したり、通話レコードを削除したりできます。
リダイヤル	ユーザは、ボタンを押すか、[リダイヤル（Redial）] ソフトキーを押して、最後にダイヤルした電話番号にコールをかけることができます。
リモート ポート設定	Cisco Unified Communications Manager の管理ページを使用して、電話機のイーサネット ポートの速度とデュプレックス機能をリモートで設定できます。これにより、具体的なポート設定を伴う大規模な導入のパフォーマンスが向上します。 （注） Cisco Unified Communications Manager のリモート ポート設定用にポートが設定されている場合は、電話機のデータを変更することはできません。 プロダクト固有の設定 （161 ページ）の「リモート ポート設定」を参照してください。

機能	説明と詳細情報
リモート接続先へのダイレクト コールの会社電話番号への再ルーティング	ユーザの携帯電話に直接かかってきたコールを会社の電話番号（固定電話）にルーティングできます。リモート接続先（携帯電話）への着信コールでは、リモート接続先でのみ呼出音が鳴り、デスクトップフォンの呼出音は鳴りません。携帯電話でコールに応答すると、デスクトップフォンに「リモートで使用中（Remote In Use）」というメッセージが表示されます。これらのコール中、ユーザは自身の携帯電話のさまざまな機能を使用できます。 該当する Cisco Unified Communications Manager リリースのマニュアルの Cisco Unified Mobility の情報を参照してください。
「通話終了（Call Ended）」のプロンプト タイマーの削除	電話画面の `Call ended` メッセージ表示を削除することにより、通話終了の応答時間を改善します。
呼出音の設定	電話機に別のアクティブ コールが着信したときに、回線で使用される呼出音タイプを指定します。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報およびカスタム電話呼出音 （129 ページ）を参照してください。
SIP の RTCP 保留	保留中のコールがゲートウェイによってドロップされないようにします。ゲートウェイでは RTCP ポートのステータスを確認して、コールがアクティブかどうかが判別されます。電話ポートを開いたままにしておくことによって、ゲートウェイは保留中のコールを終了しません。
セキュアな会議	セキュアな電話機で、セキュアな会議ブリッジを使用して会議コールを発信できます。[会議（Confrn）]、[参加（Join）]、または [割り込み（Barge）] ソフトキーまたは MeetMe 会議を使用して新しい参加者が追加されると、すべての参加者がセキュアな電話機を使用している場合にセキュア コールのアイコンが表示されます。 会議の各参加者のセキュリティ レベルが [会議リスト（Conference List）] に表示されます。開催者は、非セキュアの参加者を [会議参加者リスト（Conference List）] から削除できます。[拡張アドホック会議（Advanced Adhoc Conference）] に [有効（Enabled）] パラメータが設定されていれば、開催者でなくても会議参加者を追加または削除できます。 該当する Cisco Unified Communications Manager リリースのマニュアルの会議ブリッジおよびセキュリティの情報およびサポート対象のセキュリティ機能 （96 ページ）を参照してください。
セキュア EMCC	リモート オフィスから電話機にログインするユーザに強化されたセキュリティを提供することで、EMCC 機能を改善します。

機能	説明と詳細情報
サービス	Cisco Unified Communications Manager の管理にある [IP 電話サービスの設定（IP Phone Services Configuration）] メニューを使用して、ユーザが登録できる IP 電話サービスのリストを定義して管理できます。 該当する Cisco Unified Communications Manager リリースのマニュアルのサービス情報を参照してください。
サービス URL ボタン	ユーザは、電話機の [サービス（Services）] メニューの代わりにプログラム可能なボタンを使用して、サービスにアクセスすることができます。 該当する Cisco Unified Communications Manager リリースのマニュアルのサービス情報を参照してください。
発信者 ID および発信者番号の表示	電話機に、着信コールの発信者 ID と発信者番号の両方を表示できます。IP 電話の LCD ディスプレイのサイズによって、表示される発信者 ID と発信者番号の長さが制限されます。 発信者 ID および発信者番号の表示機能は、着信コールのアラートのみに適用されます。コール転送とハント グループの機能は変更されません。 この表の「発信者 ID」を参照してください。
シスコヘッドセットを使用したエクステンションモビリティのログインの簡略化	ユーザは、自分のシスコヘッドセットを使用してエクステンションモビリティにサインインできます。 電話機が MRA モードの場合、ユーザーはヘッドセットを使用して電話機にログインできます。 この機能には、Cisco Unified Communications Manager（UCM）リリース 11.5(1) SU8、11.5(1) SU.9、12.5(1) SU3 以降が必要です。 詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』、リリース 11.50(1)SU8以降またはリリース 12.5(1)SU3以降を参照してください。
簡素化タブレット サポート	Android タブレットや iOS タブレットのユーザが Bluetooth を使用してタブレットを電話機にペアリングして、タブレットでのコールの音声部分に電話機を使用することができます。 インテリジェント プロキシミティの有効化 （235 ページ）を参照してください。 Cisco IP 電話 8851NR は Bluetooth をサポートしていません。
短縮ダイヤル	記憶されている指定番号をダイヤルします。

機能	説明と詳細情報
SSH アクセス（SSH Access）	[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] を使用して、SSHアクセス設定を有効または無効にできます。SSHサーバを有効にすると、電話機が SSH 接続を受け入れるようになります。電話機の SSH サーバ機能を無効にすると、その電話機への SSH アクセスがブロックされます。 プロダクト固有の設定（161ページ）の「SSHアクセス」を参照してください。
Time-of-Day ルーティング	指定したテレフォニー機能へのアクセスを時間帯によって制限します。 該当する Cisco Unified Communications Manager リリースのマニュアルの時間帯および Time-of-Day ルーティングの情報を参照してください。
タイム ゾーンのアップデート	タイム ゾーンの変更に伴い、Cisco IP 電話を更新します。 該当する Cisco Unified Communications Manager リリースのマニュアルの日時情報を参照してください。
転送	ユーザは、接続されているコールを自分の電話機から別の番号にリダイレクトできます。
転送（直接転送）	転送：転送では、常にまずアクティブ コールを保留にした後、同じ電話番号を使用して新しいコールを開始します。 ユーザは、アクティブ コールの転送機能を使用して直接転送できます。 一部の JTAPI/TAPI アプリケーションでは、Cisco IP 電話の参加および直接転送機能と互換性がないため、参加および直接転送ポリシーを設定して、同一回線上や、場合によっては複数の回線をまたいだ参加と直接転送を無効にする必要があります。 該当する Cisco Unified Communications Manager リリースのマニュアルの電話番号の情報を参照してください。
信頼検証サービス（TVS）	信頼検証サービス（TVS）により、証明書信頼リスト（CTL）のサイズを増やしたり、更新された CTL ファイルを電話機にダウンロードしたりせずに、電話機が署名済みの設定を認証し、他のサーバまたはピアを認証することができます。TVS はデフォルトで有効になっています。 電話機の [セキュリティ設定（Security Setting）] メニューに TVS の情報が表示されます。

機能	説明と詳細情報
UCR 2013	Cisco IP 電話は、次の機能を提供することによって Unified Capabilities Requirements（UCR）2013 をサポートします。 • 連邦情報処理標準（FIPS）140-2 のサポート • 80 ビット SRTCP タギングのサポート IP 電話管理者は、Cisco Unified Communications Manager の管理ページで該当するパラメータを設定する必要があります。
未設定のプライマリ回線通知	プライマリ回線が設定されていない場合、ユーザにアラートを送信します。ユーザの電話画面に `Unprovisioned` のメッセージが表示されます。
リスト、アラート、ビジュアル ボイスメールのユーザ インターフェイスの更新	アプリケーション ウィンドウのサイズが拡大され、切り捨てられる文字列が最小限になります。
ビデオ モード	ユーザが、ビデオ会議を表示するためのビデオ ディスプレイ モードを選択できます。これは、システムに設定されているモードによって異なります。 該当する Cisco Unified Communications Manager リリースのマニュアルのビデオ情報を参照してください。 Cisco IP 電話 8845、8865、および 8865NR で利用可能。
ビデオ サポート	電話機のビデオ サポートを有効にします。Cisco Unified Communications Manager の [電話の設定（Phone Configuration）] ウィンドウで、ビデオ コールに対してビデオ機能のパラメータを有効化する必要があります。デフォルトではイネーブルです。 Cisco IP 電話 8845、8865、および 8865NR で利用可能。
PC からのビデオ	Cisco Unified IP 電話、パーソナル コンピュータ、および外付けビデオ カメラを使用することにより、ユーザがビデオ コールを発信できるようにします。 この機能では、ユーザが Cisco Jabber または Cisco Unified Video Advantage 製品を使用したビデオ コールを行うこともできます。
ビジュアル ボイスメール	グラフィカル インターフェイスでボイスメールのオーディオ プロンプトを置き換えます。 http://www.cisco.com/en/US/partner/products/ps9829/prod_installation_guides_list.html#anchor3 にある『*Installation and Configuration Guide for Visual Voicemail*』を参照してください。
ボイス メッセージ システム	コールに応答がない場合に、発信者がメッセージを残せるようにします。 該当する Cisco Unified Communications Manager リリースのマニュアルのボイスメールの情報およびビジュアル ボイスメールのセットアップ（219 ページ）を参照してください。

機能	説明と詳細情報
VPN	信頼されたネットワークの外側にある場合、または電話機と Unified CM 間のネットワーク トラフィックが信頼されていないネットワークを通過する必要がある場合に、SSL を使用して、Cisco Unified IP 電話にバーチャル プライベート ネットワーク（VPN）接続を提供します。
デフォルトで Web アクセスを無効にする	HTTP など、すべての Web サービスへのアクセスを無効にすると、セキュリティが強化されます。Web アクセスを有効にすると、ユーザは Web サービスにのみアクセスできます。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

機能ボタンとソフトキー

次の表に、ソフトキーで使用可能な機能、専用機能ボタンで使用可能な機能、さらにプログラム可能な機能ボタンとして設定する必要がある機能を示します。この表の「X」は、その機能が対応するボタンのタイプまたはソフトキーでサポート対象ことを意味します。2 つのボタン タイプとソフト キーのうち、プログラム可能な機能ボタンだけは Cisco IP 電話の管理ページでの設定が必要です。

プログラム可能な機能ボタンの設定の詳細については、電話ボタン テンプレート （225 ページ）を参照してください。

表 *30*：機能とボタンおよびソフトキーの対応

機能名	専用機能ボタン	プログラム可能な機能ボタン	ソフトキー
呼び出しコール	サポート対象外	サポートされる	サポート対象外
すべてのコール	サポート対象外	サポートされる	サポート対象外
応答	サポート対象外	サポートされる	サポートされる
C 割り込み	サポート対象外	サポート対象外	サポートされる
コールバック	サポート対象外	サポートされる	サポートされる
すべてのコールの転送	サポート対象外	サポート対象外	サポートされる
コール パーク	サポート対象外	サポートされる	サポートされる
コール パーク回線ステータス	サポート対象外	サポートされる	サポート対象外

機能名	専用機能ボタン	プログラム可能な機能ボタン	ソフトキー
コール ピックアップ（ピックアップ）	サポート対象外	サポートされる	サポートされる
コール ピックアップ回線ステータス	サポート対象外	サポートされる	サポート対象外
会議	サポートされる	サポート対象外	サポートされる
即転送	サポート対象外	サポート対象外	サポートされる
取り込み中	サポート対象外	サポートされる	サポートされる
グループ ピックアップ	サポート対象外	サポートされる	サポートされる
保留 (Hold)	サポートされる	サポート対象外	サポートされる
ハント グループ	サポート対象外	サポートされる	サポート対象外
インターコム	サポート対象外	サポートされる	サポート対象外
Malicious Call Identification（MCID; 迷惑呼 ID）	サポート対象外	サポートされる	サポートされる
ミートミー	サポート対象外	サポートされる	サポートされる
Merge	サポート対象外	サポート対象外	サポートされる
モバイル コネクト（モビリティ）	サポート対象外	サポートされる	サポートされる
ミュート	サポートされる	サポート対象外	サポート対象外
その他のピックアップ	サポート対象外	サポートされる	サポートされる
キューのステータス用の PLK のサポート	サポート対象外	サポート対象外	サポートされる
[プライバシー（Privacy）]	サポート対象外	サポートされる	サポート対象外
Queue Status	サポート対象外	サポートされる	サポート対象外

機能名	専用機能ボタン	プログラム可能な機能ボタン	ソフトキー
Quality Reporting Tool（QRT; 品質レポートツール）	サポート対象外	サポートされる	サポートされる
録音	サポート対象外	サポート対象外	サポートされる
Redial	サポート対象外	サポートされる	サポートされる
スピード ダイヤル	サポート対象外	サポートされる	サポート対象外
短縮ダイヤル回線ステータス	サポート対象外	サポートされる	サポート対象外
USB ヘッドセット上の保留ボタンのサポート	サポート対象外	サポート対象外	サポートされる
転送	サポートされる	サポート対象外	サポートされる

電話機の機能設定

ユーザのニーズに基づいて、さまざまな機能を備えるように電話機をセットアップできます。すべての電話、電話機のグループ、または個々の電話機に機能を適用することもできます。

機能を設定する際には、Cisco Unified Communications Manager Administration ウィンドウに、すべての電話機に適用される情報、およびその電話機モデルに適用される情報が表示されます。電話機モデルに固有の情報は、ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] のエリアにあります。

すべての電話モデルに適用されるフィールドについては、Cisco Unified Communications Manager のマニュアルを参照してください。

ウィンドウ間には優先順位があるため、フィールドを設定する際に重要なのは、フィールド設定の対象となるウィンドウです。 優先順序は、次のとおりです。

1. 個々の電話（優先順位最高）
2. 電話機グループ
3. すべての電話（優先順位最低）

たとえば、特定のユーザ群が電話機 Web ページにアクセスしないようにしつつ、その他のユーザはそのページにアクセスできるようにするには、次のようにします。

1. すべてのユーザに対して、電話機 Web ページへのアクセスを有効にします。

2. 個々のユーザそれぞれについて、電話機 Web ページへのアクセスを無効にするか、またはユーザ グループを設定し、そのユーザ グループから電話機 Web ページへのアクセスを無効にします。
3. ユーザ グループ内の特定のユーザが電話機 Web ページへのアクセスを必要とする場合には、その特定のユーザに対して有効にすることができます。

すべての電話機の電話機能の設定

手順

ステップ 1 Cisco Unified Communications Manager管理に管理者としてサインインします。
ステップ 2 **[システム]** > **[エンタープライズ電話の設定]** を選択します。
ステップ 3 変更するフィールドを設定します。
ステップ 4 変更フィールドの [エンタープライズ設定を上書き（Override Enterprise Settings）]チェックボックスを選択します。
ステップ 5 **[保存]** をクリックします。
ステップ 6 **[設定の適用（Apply Config）]** をクリックします。
ステップ 7 電話機を再起動します。

（注） これは、組織内のすべての電話機に影響します。

電話機グループの電話機能の設定

手順

ステップ 1 Cisco Unified Communications Manager管理に管理者としてサインインします。
ステップ 2 **[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[共通の電話プロファイル（Common Phone Profile）]** の順に選択します。
ステップ 3 プロファイルを探します。
ステップ 4 [製品固有の構成レイアウト（Product Specific Configuration Layout）] ペインに移動し、フィールドを設定します。
ステップ 5 変更フィールドの [エンタープライズ設定を上書き（Override Enterprise Settings）]チェックボックスを選択します。
ステップ 6 **[保存]** をクリックします。
ステップ 7 **[設定の適用（Apply Config）]** をクリックします。

ステップ 8 電話機を再起動します。

単一の電話機の電話機能の設定

手順

ステップ 1 Cisco Unified Communications Manager管理に管理者としてサインインします。

ステップ 2 **[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 3 ユーザに関連付けられた電話機を見つけます。

ステップ 4 [製品固有の構成レイアウト（Product Specific Configuration Layout）] ペインに移動し、フィールドを設定します。

ステップ 5 変更されたフィールドについて、[共通設定の上書き（Override Common Settings）]チェックボックスをオンにします。

ステップ 6 **[保存]** をクリックします。

ステップ 7 **[設定の適用（Apply Config）]** をクリックします。

ステップ 8 電話機を再起動します。

プロダクト固有の設定

次の表に、[プロダクト固有の設定（Product Specific Configuration Layout）] ペインのフィールドを示します。

表 *31 : [プロダクト固有の設定（Product Specific Configuration）]* フィールド

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
スピーカーフォンを無効にする	チェックボックス	オフ	電話機のスピーカーフォン機能をオフにします。
スピーカーフォンとヘッドセットを無効にする（Disable Speakerphone and Headset）	チェックボックス	オフ	電話機のスピーカーフォンおよびヘッドセット機能をオフにします。
ハンドセットを無効にする	チェックボックス	オフ	電話機のハンドセット機能をオフにします。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
PC Port	[有効（Enabled）] 無効	[有効（Enabled）]	コンピュータを LAN に接続するために PC ポートを使用する機能を制御します。
アクセスの設定	無効 [有効（Enabled）] [制限（Restricted）]	[有効（Enabled）]	設定アプリのローカル電話設定へのアクセスを有効、無効、または非許可にします。 • [無効（Disabled）] : [設定（Settings）] メニューにオプションが表示されません。 • [有効（Enabled）] : [設定（Settings）] メニューのすべてのエントリが、アクセス可能です。 • [制限（Restricted）] : 電話設定メニューのみアクセス可能です。
PC の音声 VLAN へのアクセス（PC Voice VLAN Access）	[有効（Enabled）] 無効	[有効（Enabled）]	電話の PC ポートに接続されたデバイスから音声 VLAN へのアクセスを許可するかどうかを指定します。 • [無効（Disabled）] : PC は音声 VLAN 上や電話機からデータを送受信することはできません。 • [有効（Enabled）] : PC は音声 VLAN 上や電話機からデータを送受信できます。 電話のトラフィックのモニタリングを必要とするアプリケーションが PC 上で実行されている場合は、このフィールドを [有効（Enabled）] に設定してください。 それらのアプリケーションには、モニタリングおよび録音アプリケーション、分析のためのネットワーク モニタリング ソフトウェアの使用が含まれます。
Video Capabilities	[有効（Enabled）] 無効	8845、8865、および 8865NR：[有効（Enabled）] 8811、8851、8851NR、8861：[無効（Disabled）]	Cisco IP 電話、パーソナル コンピュータ、およびビデオ カメラを使用することにより、ユーザがビデオ コールを発信できます。
Web アクセス（Web Access）	無効 [有効（Enabled）]	無効	Web ブラウザによる電話 Web ページへのアクセスを有効または無効にします。 **注意** このフィールドを有効にすると、電話機に関する機密情報が公開される場合があります。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Webアクセス用のTLS 1.0およびTLS 1.1を無効にする	無効 [有効（Enabled）]	無効	Web サーバ接続に TLS 1.2 の使用を制御します。 • [無効（Disabled）]： TLS1.0、TLS 1.1 または TLS1.2 用に設定されている電話機は、HTTPS サーバとして機能できます。 • [有効（Enabled）]：TLS1.2 用に設定されている電話機のみ HTTPS サーバとして機能できます。
一括ダイヤル	無効 [有効（Enabled）]	無効	ダイヤル方法を制御します。 • [無効（Disabled）]：ダイヤルプランまたはルートパターンの重複がある場合、Cisco Unified Communications Manager は桁間タイマーが満了するのを待ちます。 • [有効（Enabled）]：ダイヤルが完了すると、ダイヤルされた文字列全体が Cisco Unified Communications Manager に送信されます。 T.302 タイマーのタイムアウトを回避するために、ダイヤルプランまたはルートパターンが重複している場合は常に一括ダイヤルを有効にすることをお勧めします。 強制承認コード（FAC）またはクライアント識別コード（CMC）は一括ダイヤルに対応していません。 FAC または CMC を使用して通話アクセスとアカウンティングを管理している場合は、この機能を使用できません。
ディスプレイ非点灯日（Days Display Not Active）	Days of the week		[ディスプレイ点灯時刻（Display On Time）] フィールドで指定された時刻になっても、ディスプレイを自動的にオンにしない日を定義します。 ドロップダウン リストから単一または複数の曜日を選択します。 複数の曜日を選択するには、**Ctrl キーを押しながら**目的の各曜日をクリックします。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
ディスプレイ点灯時刻（Display On Time）	hh:mm		毎日ディスプレイを自動的にオンにする時刻（[ディスプレイ非点灯日（Days Display Not Active）] フィールドで指定されている日を除く）を定義します。 このフィールドには、24 時間形式で入力します（0:00 は午前 0 時）。 たとえば、午前 7 時（0700）にディスプレイを自動的にオンにするには、 7:00 と入力します。 午後 2 時 (1400) にディスプレイをオンにするには、 （1400）にバックライトをオンにするには、14:00 と入力します。 このフィールドがブランクの場合、ディスプレイは午前 0 時に自動的にオンになります。
ディスプレイ点灯継続時間（Display On Duration）	hh:mm		[ディスプレイ点灯時刻（Display On Time）] フィールドで指定した時刻にディスプレイがオンになった後、オン状態を保つ時間の長さを定義します。 たとえば、ディスプレイを自動的にオンにしてから 4 時間 30 分にわたってオン状態を保つには、04:30 と入力します。 このフィールドがブランクの場合、電話機は午前 0 時（0:00）にオフになります。 [ディスプレイ点灯時刻（Display On Time）] が 0:00 で、[ディスプレイ点灯継続時間（Display On Duration）] がブランク（または 24:00）の場合、ディスプレイはオフになりません。
ディスプレイ放置時自動消灯（Display Idle Timeout）	hh:mm	01:00	ディスプレイをオフにするまでの電話機のアイドル時間を定義します。 ディスプレイがスケジュールどおりにオフで、ユーザが（電話機ボタンを押す、またはハンドセットを持ち上げる操作で）オンにした場合にのみ適用されます。 このフィールドには、時間:分の形式で値を入力します。 たとえば、ユーザがディスプレイをオンにしてから 1 時間 30 分にわたって電話機がアイドル状態にあった場合にディスプレイをオフにするには、01:30 と入力します。 詳細については、未使用時画面のセット アップ （132 ページ） を参照してください。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
着信コール時に点灯（Display On When Incoming Call）	無効 [有効（Enabled）]	[有効（Enabled）]	着信コールがあるとアイドル表示がオンに変わります。
Enable Power Save Plus	Days of the week		電話機の電源をオフにする日のスケジュールを定義します。 ドロップダウン リストから単一または複数の曜日を選択します。 複数の曜日を選択するには、**Ctrl キーを押しながら**目的の各曜日をクリックします。 [Power Save Plus の有効化（Enable Power Save Plus）] がオンになっていると、緊急（e911）の問題について警告するメッセージを受け取ります。 **注意** Power Save Plus モード（「モード」）が有効である間は、モードに設定されたエンドポイントは、緊急コールでは無効で、着信コールの受信ができません。 このモードを選択することにより、次の条項に同意したものと見なされます。（i）モードが有効である間、緊急コールとコールの受信用の代替方法を責任を持って用意する必要があります。（ii）シスコはこのモードの選択に関して何の責任を負いません。このモードを有効にすることは、お客様の責任で行っていただきます。（iii）コール、発信、およびその他について、このモードを有効にした場合の影響をユーザにすべて通知する必要があります。 Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオフにする必要があります。 [Power Save Plus の有効化（Enable Power Save Plus）] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオンにしたままにしておくと、Power Save Plus は無効になりません。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
電話機をオンにする時刻（Phone On Time）	hh:mm		[Power Save Plus の有効化（Enable Power Save Plus）] フィールドにある日について、電話機の電源を自動的にオンにする時刻を決定します。 このフィールドには、24 時間形式で入力します（0:00 は午前 0 時）。 たとえば、午前7時（0700）に自動的に電話機の電源をオンにする場合は、 7:00 と入力します。 午後 2 時（1400）に電話機の電源をオンにするには、 （1400）にバックライトをオンにするには、14:00 と入力します。 デフォルト値はブランクで、これは 00:00 を意味します。 [電話機をオンにする時刻（Phone On Time）] は、[電話機をオフにする時刻（Phone Off Time）] より 20 分以上遅い時刻に設定する必要があります。 たとえば、[電話機をオフにする時刻（Phone Off Time）] が 7:00 の場合、[電話機をオンにする時刻（Phone On Time）] は 7:20 より前に設定しないでください。
電話機をオフにする時刻（Phone Off Time）	hh:mm		[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択した日について、電話機の電源をオフにする時刻を特定します。 [電話機をオンにする時刻（Phone On Time）] フィールドと [電話機をオフにする時刻（Phone Off Time）] フィールドに同じ値が含まれている場合、電話機はオフになりません。 このフィールドには、24 時間形式で入力します（0:00 は午前 0 時）。 たとえば、午前7時（0700）に自動的に電話機の電源をオフにする場合は、 7:00 と入力します。 午後 2 時（1400）に電話機の電源をオフにするには、 （1400）にバックライトをオンにするには、14:00 と入力します。 デフォルト値はブランクで、これは 00:00 を意味します。 [電話機をオンにする時刻（Phone On Time）] は、[電話機をオフにする時刻（Phone Off Time）] より 20 分以上遅い時刻に設定する必要があります。 たとえば、[電話機をオフにする時刻（Phone Off Time）] が 7:00 の場合、[電話機をオンにする時刻（Phone On Time）] は 7:20 より前に設定しないでください。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Phone Off Idle Timeout	20 ～ 1440 分	60	電話機の電源をオフにする前に、電話機をアイドル状態にしておく必要がある時間の長さを示します。 タイムアウトは次の条件で発生します。 • 電話機がスケジュールどおりに Power Save Plus モードになっていたが、電話機のユーザが [選択（Select）] キーを押したために、Power Save Plus モードが解除された場合。 • 接続スイッチで電話機が再びオンになった場合。 • [電話機をオフにする時刻（Phone Off Time）] になったが、通話中の場合。
Enable Audible Alert	チェックボックス	オフ	これを有効にすると、[電話機をオフにする時刻（Phone Off Time）] で指定した時刻の 10 分前に電話機で音声アラートの再生が開始されます。 このチェックボックスが表示されるのは、[Power Save Plus の有効化（Enable Power Save Plus）] リストボックスで 1 日以上が選択されている場合だけです。
EnergyWise Domain	最大 127 文字です。		その電話機が含まれる EnergyWise ドメインを特定します。
EnergyWise シークレット	最大 127 文字です。		EnergyWise ドメイン内でエンドポイントとの通信に使用されるセキュリティの秘密パスワードを指定します。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Allow EnergyWise Overrides	チェックボックス	オフ	電話機に電源レベルの更新を送信するための EnergyWise ドメイン コントローラのポリシーを許可するかどうかを決定します。 次の条件が適用されます。 • [Power Save Plus の有効化（Enable Power Save Plus）] フィールドで 1 日以上を選択する必要があります。 • Cisco Unified Communications Manager の管理ページの設定は、EnergyWise がオーバーライドを送信しても、スケジュールに適用されます。 たとえば、[電話機をオフにする時刻（Phone Off Time）] が 22:00（午後 10 時）に設定されていると仮定すると、[電話機をオンにする時刻（Phone On Time）] フィールドの値は 06:00（午前 6 時）となり、[Power Save Plus の有効化（Enable Power Save Plus）] では 1 日以上が選択されています。 • EnergyWise が 20:00（午後 8 時）に電話機をオフにするように指示すると、この指示は、午前 6 時に設定された [電話機をオンにする時刻（Phone On Time）] まで有効となります（電話機ユーザによる介入が発生しないと仮定した場合）。 • 午前 6 時になると、電話機はオンとなり、Cisco Unified Communications Manager の管理での設定から電力レベルの変更の受信を再開します。 • 電力レベルを電話機で再び変更するには、EnergyWise は電力レベル変更コマンドを新たに再発行する必要があります。 Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオフにする必要があります。 [Power Save Plus の有効化（Enable Power Save Plus）] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオンにしたままにしておくと、Power Save Plus は無効になりません。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Join and Direct Transfer Policy	[同一回線、回線全体で有効（Same line, across line enable）] [同一回線のみで有効（Same line enable only）] [同一回線、回線全体で無効（Same, across line disable）]	[同一回線、回線全体で有効（Same line, across line enable）]	コールに参加し、転送するユーザの機能を制御します。 • [同一回線、回線全体で有効（Same line, across line enable）]：ユーザは、現在の回線上のコールを別の回線上の別のコールに直接転送するか、コールに参加できます。 • [同一回線のみで有効（Same line enable only）]：ユーザは、両方のコールが同じ回線上のものである場合にのみ、コールの直接転送または参加ができます。 • [同一回線、回線全体で無効（Same line, across line disable）]：ユーザは、同一回線上のコールに参加したり転送したりできません。 参加機能と転送機能は無効であり、ユーザは直接転送も参加機能も実行できません。
Span to PC Port	無効 [有効（Enabled）]	無効	ネットワーク ポートで送受信されるパケットをアクセス ポートに転送するかどうかを表示します。
録音トーン	無効 [有効（Enabled）]	無効	ユーザがコールを記録する際のトーンの再生を制御します。
録音トーンのローカルボリューム	整数 0 ～ 100	100	ローカル ユーザに対する録音トーンのボリュームを制御します。
録音トーンのリモート音量	整数 0 ～ 100	50	リモート ユーザに対する録音トーンのボリュームを制御します。
録音トーンの長さ	整数、1 ～ 3000 ミリ秒		録音トーンの長さを制御します。
ログサーバー	256 文字以下の文字列。		電話デバッグ出力用の IPv4 syslog サーバを指定します。 アドレスの形式: **address:<port>@@base=<0-7>;pfs=<0-1>**
Cisco Discovery Protocol（CDP）：Switch Port	無効 [有効（Enabled）]	[有効（Enabled）]	電話機の SW ポートでの Cisco Discovery Protocol の制御。
Cisco Discovery Protocol（CDP）：PC Port	無効 [有効（Enabled）]	[有効（Enabled）]	電話機の PC ポートでの Cisco Discovery Protocol の制御。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Link Layer Discovery Protocol - Media Endpoint Discover（LLDP-MED）：スイッチ ポート（Link Layer Discovery Protocol - Media Endpoint Discover（LLDP-MED）：Switch Port）	無効 [有効（Enabled）]	[有効（Enabled）]	SW ポートで LLDP-MED を有効にします。
Link Layer Discovery Protocol（LLDP）：PC Port	無効 [有効（Enabled）]	[有効（Enabled）]	PC ポートで LLDP を有効にします。
LLDP Asset ID	32 文字以下の文字列。		在庫管理のため電話機に割り当てられているアセット ID を識別します。
LLDP 電力の優先順位（LLDP Power Priority）	不明 低 高 クリティカル（Critical）	不明	電話機の電源優先度をスイッチに割り当て、スイッチが電力を適切に電話機に供給できるようにします。
802.1X 認証	ユーザ制御（User Controlled） [有効（Enabled）] 無効	ユーザ制御（User Controlled）	802.1x 認証機能のステータスを指定します。 • [ユーザ制御（User Controlled）]：ユーザは電話機に 802.1x を設定できます。 • [無効（Disabled）]：802.1x 認証は使用されません。 • [有効（Enabled）]：802.1x 認証が使用され、電話の認証を設定します。
Automatic Port Synchronization	無効 [有効（Enabled）]	無効	電話機のポート間で最も低い速度にポートを同期し、パケット損失を防止します。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Switch Port Remote Configuration	無効 [有効（Enabled）]	無効	電話機SWポートの速度とデュプレックス機能のリモート設定ができます。 これにより、具体的なポート設定を伴う大規模な導入のパフォーマンスが向上します。 Cisco Unified Communications Manager のリモート ポート設定用にSWポートが設定されている場合は、電話機のデータを変更することはできません。
PC Port Remote Configuration	無効 [有効（Enabled）]	無効	電話機PCポートの速度とデュプレックス機能のリモート設定ができます。 これにより、具体的なポート設定を伴う大規模な導入のパフォーマンスが向上します。 Cisco Unified Communications Manager のリモート ポート設定用にポートが設定されている場合は、電話機のデータを変更することはできません。
SSH アクセス	無効 [有効（Enabled）]	無効	ポート 22 を経由する SSH デーモンへのアクセスを制御します。ポート 22 を開いたままにしておくと、電話機はサービス拒否（DoS）攻撃を受けやすい状態となります。
Incoming Call Toast Timer	0, 3, 4, 5, 6, 7, 8, 9, 10, 15, 30, 60	5	Toast が表示される時間を秒単位で指定します。 この時間には、ウィンドウのフェードインとフェードアウトの時間も含まれます。 0は、着信コール トーストが無効であることを意味します。
呼出音ロケール（Ring Locale）	デフォルト 日本	デフォルト	呼出音パターンを制御します。
TLS 再開タイマー	整数、0 ～ 3600 秒	3600	TLS認証プロセス全体を繰り返すことなくTLSセッションを再開する機能を制御します。 このフィールドが 0 に設定されている場合、TLS セッション再開は無効です。
FIPS モード	無効 [有効（Enabled）]	無効	電話機上で連邦情報処理標準（FIPS）モードを有効または無効にします。
共有電話からの通話履歴を記録（Record Call Log from Shared Line）	無効 [有効（Enabled）]	無効	共有回線コールをコール ログに記録するかどうかを指定します。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
呼出音の最小音量（Minimum Ring Volume）	0：サイレント 1–15	0：サイレント	電話機の最小呼出音量を制御します。 呼出音をオフにすることができないように電話機を設定できます。
ピア ファームウェア共有（Peer Firmware Sharing）	無効 [有効（Enabled）]	[有効（Enabled）]	電話機がサブネット上にある同一モデルの他の電話機を検出し、更新されたファームウェア ファイルを共有できるようにします。電話機に新しいファームウェア ロードがある場合、他の電話機とそのロードを共有できます。 他の電話機の 1 つに新しいファームウェア ロードがある場合、TFTP サーバからではなくその電話機からファームウェアをダウンロードできます。 ピア ファームウェア共有により、以下が実現します。 • 中央集中型リモート TFTP サーバへの TFTP 転送における輻輳が制限されます。 • ファームウェアのアップグレードを手動で制御する必要がなくなります。 • アップグレード時に多数のデバイスが同時にリセットされた場合の電話機のダウンタイムが削減されます。 • 帯域幅が制限された WAN リンクを経由するブランチまたはリモート オフィス導入シナリオでのファームウェアのアップグレードに役立ちます。
ロード サーバ	256 文字以下の文字列。		電話機がファームウェア ロードとアップグレードを取得するために使用する代替 IPv4 サーバを指定します。 アドレスの形式: **address:<port>@@base=<0-7>;pfs=<0-1>**
IPv6 負荷サーバ（IPv6 Load Server）	256 文字以下の文字列。		電話機がファームウェア ロードやアップグレードを取得する際に使用する代替 IPv6 サーバを指定します。 アドレスの形式： **[address]:<port>@@base=<0-7>;pfs=<0-1>**
Wideband Headset UI Control	無効 [有効（Enabled）]	[有効（Enabled）]	ユーザが、アナログ ヘッドセット用ワイドバンド コーデックを使用できるようにします。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Wideband Headset	無効 [有効（Enabled）]	[有効（Enabled）]	電話機のワイドバンド ヘッドセットの使用を有効または無効にします。 [ユーザ制御のワイドバンド ヘッドセット（User Control Wideband Headset）] と組み合わせて使用します。 詳細については、ワイドバンドコーデックのセットアップ （131 ページ） を参照してください。
Wi-Fi	無効 [有効（Enabled）]	[有効（Enabled）]	Cisco IP 電話 8861 と 8865 から Wi-Fi ネットワークに接続できるようにします。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
背面USBポート	無効 [有効（Enabled）]	8861、8865、および 8865NR：有効	Cisco IP 電話 8861 および 8865 の背面の USB ポートを使用する機能を制御します。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
側面 USB ポート	無効 [有効（Enabled）]	[有効（Enabled）]	Cisco IP 電話 8851、8851NR、8861、8865、および 8865NR の側面の USB ポートを使用する機能を制御します。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
[コンソール アクセス（Console Access）]	無効 [有効（Enabled）]	無効	シリアル コンソールを有効にするか無効にするかを指定します。
Bluetooth	無効 [有効（Enabled）]	[有効（Enabled）]	電話機の Bluetooth オプションを有効または無効にします。 無効にした場合、ユーザは電話機上で Bluetooth を有効化できません。 Cisco IP 電話 8845、8851、8861、および 8865 でサポートされます。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Bluetooth 連絡先のインポートを許可（Allow Bluetooth Contacts Import）	無効 [有効（Enabled）]	[有効（Enabled）]	ユーザが、Bluetooth を使用することにより、接続されたモバイル デバイスから連絡先をインポートできるようにします。 無効にすると、ユーザは電話機に接続されたモバイル デバイスから連絡先をインポートすることはできません。 Cisco IP 電話 8845、8851、8861、および 8865 でサポートされます。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
Bluetooth モバイル ハンズフリー モードを許可（Allow Bluetooth Mobile Handsfree Mode）	無効 [有効（Enabled）]	[有効（Enabled）]	ユーザが、モバイル デバイスやタブレットで電話機の音響特性を利用できるようにします。ユーザはBluetoothを使用してモバイル デバイスやタブレットを電話機にペアリングします。 無効にすると、ユーザはモバイル デバイスまたはタブレットを電話機とペアリングすることはできません。 モバイル デバイスがペアリングされると、ユーザは電話機でモバイル コールの発信および受信ができるようになります。 タブレットを使用する場合、タブレットから電話機に音声をルーティングできます。 複数のモバイル デバイス、タブレット、Bluetooth ヘッドセットを電話機にペアリングできます。 ただし、同時に接続できるのは1つのデバイスと1つのヘッドセットのみです。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
Bluetooth プロファイル（Bluetooth Profiles）	[ハンズフリー（Handsfree）] ヒューマンインターフェイス デバイス	[ハンズフリー（Handsfree）]	電話機のどの Bluetooth プロファイルが有効/無効であるかを示します。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
Gratuitous ARP	無効 [有効（Enabled）]	無効	電話機が Gratuitous ARP から MAC アドレスを学習する能力を有効または無効にします。 この機能は、音声ストリームをモニタまたは記録するために必要です。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
プライマリ回線にすべての通話の表示	無効 [有効（Enabled）]	無効	この電話機に送られるすべてのコールがプライマリ回線で表示されるかどうかを指定します。 このフィールドの目的は、コールを表示する回線を選択するのではなく、エンド ユーザがすべての回線上のすべてのコールをひと目で簡単に確認できるようにすることです。 つまり、電話に複数の回線が設定されている場合、通常はすべての回線上のすべてのコールを1つに統合表示して確認できるようにするほうが便利です。この機能が有効化されている場合、すべてのコールがプライマリ回線に表示されますが、これまで通り特定の回線を選択して表示内容をフィルタリングし、特定の回線に関するコールのみを表示することもできます。
HTTPS サーバ（HTTPS Server）	HTTP および HTTPS 対応 [HTTPS のみ（HTTPS only）]	HTTP および HTTPS 対応	電話機への通信のタイプを制御します。 [HTTPS のみ（HTTPS only）] を選択すると、電話機の通信はより安全になります。
IPv6 ログサーバー	256 文字以下の文字列。		IPv6 ログ サーバを指定します。 アドレスの形式： **[address]:<port>@@base=<0-7>;pfs=<0-1>**
リモート ログ（Remote Log）	無効 [有効（Enabled）]	無効	Syslog サーバにログを送信する機能を制御します。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
ログプロファイル	デフォルト プリセット テレフォニー SIP UI ネットワーク Media アップグレード アクセサリ セキュリティ Wi-Fi [VPN] EnergyWise [MobileRemoteAc]	プリセット	事前定義されたロギング プロファイルを指定します。 • [デフォルト（Default）]：デフォルトのデバッグ ロギング レベル • [プリセット（Preset）]：電話ローカル デバッグ ロギングの設定を上書きしません • [テレフォニー（Telephony）]：電話またはコール機能に関する情報をログに記録します • [SIP]：SIP シグナリングに関する情報をログに記録します • [UI]：電話ユーザインターフェイスに関する情報をログに記録します • [ネットワーク（Network）]：ネットワーク情報をログに記録します • [メディア（Media）]：メディア情報をログに記録します • [アップグレード（Upgrade）]：アップグレード情報をログに記録します • [アクセサリ（Accessory）]：アクセサリ情報をログに記録します • [セキュリティ（Security）]：セキュリティ情報をログに記録します • [Wi-Fi]：Wi-Fi 情報をログに記録します • [VPN]：バーチャル プライベート ネットワーク情報をログに記録します • [Energywise]：省エネルギー情報をログに記録します • [MobileRemoteAC]：Expressway によるモバイルおよび Remote Accessの情報をログに記録します

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
G.722およびiSAC コーデックをアドバタイズする	[システムデフォルトの使用（Use System Default）] 無効 [有効（Enabled）]	[システムデフォルトの使用（Use System Default）]	電話機が G.722 および iSAC コーデックを Cisco Unified Communications Manager にアドバタイズするかどうかを指定します。 • [システムデフォルトの使用（Use System Default）]：エンタープライズ パラメータ Advertise G.722 Codec で指定された設定に従います。 • [無効（Disabled）]：Cisco Unified Communications Manager に G.722 をアドバタイズしません。 • [有効（Enabled）]：Cisco Unified Communications Manager に G.722 をアドバタイズします。 詳細については、表の後の注記を参照してください。
Unified CM接続障害の検出	標準 [遅延（Delayed）]	標準	バックアップ Unified CM/SRST へのデバイスのフェールオーバーが発生する前の最初のステップである、Cisco Unified Communications Manager（Unified CM）への接続失敗を検出するための電話機の感度を決定します。 • [標準（Normal）]：標準のシステム レートで発生する Unified CM 接続エラーの検出。 Unified CM 接続エラーの高速認識のためには、この値を選択します。 • [遅延（Delayed）]：Unified CM 接続フェールオーバーの検出は、標準の約 4 分の 1 の速度で発生します。 接続を再確立できるようにするためにフェールオーバーを少し遅らせる場合、この値を選択します。 [Normal] と [Delayed] の接続エラー検出の正確な時間の差は、常に変化する多数の変数に応じて異なります。 このフィールドは、有線のイーサネット接続にのみ適用されます。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
電力ネゴシエーション（Power Negotiation）	無効 [有効（Enabled）]	[有効（Enabled）]	電話機では Link Level Endpoint Discovery Protocol（LLDP）および Cisco Discovery Protocol（CDP）を使用して電力をネゴシエートできます。 電話機が電力ネゴシエーションをサポートしているスイッチに接続されている場合は、電力ネゴシエーションを無効にしないでください。 無効にした場合、スイッチによって電話機に対する電力がオフになる可能性があります。
リリースボタンからダイヤルトーンを提供（Provide Dial Tone from Release Button）	無効 [有効（Enabled）]	無効	リリース キーが押された場合に、ユーザがダイヤル トーンを聞くようにするかどうかを制御します。 • [無効（Disabled）] : ユーザがダイヤル トーンを聞かないようにします。 • [有効（Enabled）] : ユーザがダイヤル トーンを聞くようにします。
背景画像	64 文字以下の文字列。		デフォルトの壁紙ファイルを指定します。 デフォルトの壁紙が設定されている場合、ユーザは電話機の壁紙を変更できません。
簡易発信UI（Simplified New Call UI）	無効 [有効（Enabled）]	無効	オフフック ダイヤルのユーザ インターフェイスを制御します。 有効にすると、ユーザは、最近の通話リストから番号を選択することができません。 有効にした場合、このフィールドにより、ユーザがコールを発信するための簡素化されたウィンドウが提供されます。 電話機がオフフックの場合に表示される通話履歴ポップアップ ウィンドウは、ユーザに対して表示されません。 ポップアップ ウィンドウの表示は便利なので、[簡易化された新しいコール UI（Simplified New Call UI）] はデフォルトで無効になっています。
すべてのコールに戻る（Revert to All Calls）	無効 [有効（Enabled）]	無効	コールに対してプライマリ回線、すべてのコール、またはアラート コール以外のフィルタが適用されていると、コール終了後に電話が [すべてのコール（All Calls）] に戻るかどうかを指定します。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
選択した回線のみのコール履歴の表示（Show Call History for Selected Line Only）	無効 [有効（Enabled）]	無効	通話履歴リストの表示を制御します。 • [無効（Disabled）]：通話履歴リストには、すべての回線の通話履歴が表示されます。 • [有効（Enabled）]：通話履歴リストには、選択した回線の通話履歴が表示されます。
Actionable Incoming Call Alert	無効 すべての着信コールの表示 [非表示着信コールで表示（Show for Invisible Incoming Call）]	すべての着信コールの表示	電話画面に表示される着信コール アラートのタイプを制御します。 このフィールドの目的は、エンド ユーザがコールに応答するために必要なボタンを押す回数を減らすことです。 • [無効（Disabled）]：実行可能な着信呼警告が無効になり、ユーザには従来の着信コール ポップアップ アラートが表示されます。 • [すべての着信コールについて表示（Show for all Incoming Call）]：可視性に関係なくすべてのコールの実行可能な着信呼警告が表示されます。 • [非表示の着信コールについて表示（Show for Invisible Incoming Call）]：電話機に表示されないコールの実行可能な着信呼警告が表示されます。このパラメータは、着信アラートのポップアップ通知と同様に動作します。
DF ビット（DF Bit）	0 1	0	ネットワーク パケットの送信方法を制御します。パケットをさまざまなサイズのチャンク（フラグメント）で送信できます。 DF ビットがパケット ヘッダーで 1 に設定されると、ネットワーク ペイロードは、スイッチやルータなどのネットワークを通過するときにフラグメント化しません。 フラグメント化させないことで受信側の解析の誤りを回避できますが、わずかにスピードが低下します。 DF ビット設定は、ICMP、VPN、VXC VPN、DHCP トラフィックには適用されません。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
デフォルトの回線フィルタ（Default Line Filter）	電話デバイス名をカンマで区切ったリスト		デフォルト フィルタにある電話のリストが表示されます。 デフォルトの回線フィルタが設定されている場合、電話の **[設定]**>**[初期設定]** メニューにある **[コール通知]** で、[日次スケジュール] という名前のフィルタがユーザに対して表示されます。 [毎日のスケジュール（Daily schedule）] フィルタは、[すべての通話（All Calls）] フィルタの追加です。 デフォルト回線フィルタが設定されていない場合、電話機はプロビジョニングされたすべての回線を検査します。 設定されている場合、[デフォルト（Default）] フィルタがアクティブ フィルタとして選択されているか、カスタム フィルタがないのであれば、Cisco Unified Communications Manager で設定された回線を検査します。 カスタム回線フィルタを使用すると、高優先順位回線でのフィルタリングが有効になり、アラート アクティビティを減らすことができます。 アラート フィルタの対象となる回線のサブセットに対し、呼び出しコール通知の優先順位を設定できます。 カスタム フィルタは、選択した回線の着信コールに対して、従来のポップアップ アラートまたは実行可能なアラートを生成します。 フィルタごとに、適用される回線のサブセットだけがアラートを生成します。 この機能では、複数の回線を使用するユーザが優先度の高い回線からのアラートのみにフィルタリングして表示することにより、アラート アクティビティを削減できます。 エンド ユーザはこれを自分で設定できます。 また、デフォルト回線フィルタをプログラムし、電話機にフィルタをプッシュすることもできます。
最低警告回線状態優先順位（Lowest Alerting Line State Priority）	無効 [有効（Enabled）]	無効	共有電話を使用している場合のアラート状態を指定します。 • [無効（Disabled）]：共有回線で着信コール警告が発生すると、リモート使用中の代わりに、LED/回線状態アイコンに警告状態が反映されます。 • [有効（Enabled）]：共有回線で着信コール警告が発生すると、ユーザに対して、リモート使用中のアイコンが表示されます。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
KEM を 1 列表示（One Column Display for KEM）	無効 [有効（Enabled）]	無効	キー拡張モジュールでの表示を制御します。 • [無効（Disabled）]：拡張モジュールで 2 列モードを使用します。 • [有効（Enabled）]：拡張モジュールで 1 列モードを使用します。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
Energy Efficient Ethernet（EEE）：PC ポート（Energy Efficient Ethernet (EEE): PC Port）	無効 [有効（Enabled）]	無効	PC ポート上の EEE を制御します。
Energy Efficient Ethernet（EEE）：SW ポート（Energy Efficient Ethernet (EEE): SW Port）	無効 [有効（Enabled）]	無効	スイッチ ポート上の EEE を制御します。
[開始ビデオ ポート（Start Video Port）]			ビデオコールのポート範囲の開始を定義します。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
[終了ビデオ ポート（Stop Video Port）]			ビデオコールのポート範囲の終了を定義します。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Expressway サインインに対するユーザ クレデンシャルの永続性（User Credentials Persistent for Expressway Sign In）	無効 [有効（Enabled）]	無効	電話機にユーザのサインイン クレデンシャルを保存するかどうかを制御します。 無効にすると、ユーザに対して、モバイルおよび Remote Access（MRA）の Expressway サーバにサインインするためのプロンプトが常に表示されます。 ユーザが簡単にログインできることが望ましい場合は、このフィールドを有効にすることによって、Expressway のログイン クレデンシャルを永続的なものとすることができます。 ユーザは初回のみログイン クレデンシャルを入力する必要があります。 それ以降は、構外で電話機の電源を入れたときにはいつでもログイン情報がサインイン画面に事前入力されます。 詳細については、Expressway 経由でのモバイルおよび Remote Access （203 ページ）を参照してください。
カスタマー サポートのアップロード URL（Customer support upload URL）	256 文字以下の文字列。		問題レポート ツール（PRT）の URL を入力します。 Expressway 経由でのモバイルおよび Remote Accessを使用してデバイスを導入している場合、Expressway サーバの HTTP サーバ許可リストへの PRT サーバ アドレスの追加も必要となります。 詳細については、Expressway 経由でのモバイルおよび Remote Access （203 ページ）を参照してください。
Web 管理（Web Admin）	無効 [有効（Enabled）]	無効	Web ブラウザによる電話 Web ページへの管理者アクセス権を有効または無効にします。 詳細については、電話機の管理ページの設定 （121 ページ）を参照してください。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
Admin パスワード	8 ～ 127 文字の文字列		管理者として電話機 Web ページにアクセスする際の管理者パスワードを定義します。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
WLAN SCEP サーバ（WLAN SCEP Server）	256 文字以下の文字列。		この電話機で WLAN 認証の証明書を取得するために使用する SCEP サーバを指定します。 サーバのホスト名または IP アドレスを入力します（標準の IP アドレス形式を使用します）。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
WLAN ルート CA フィンガープリント（WLAN Root CA Fingerprint）（SHA256 または SHA1）	95 文字以下の文字列。		WLAN 認証の証明書発行時に、SCEP プロセスで検証用に使用するルート CA の SHA256 または SHA1 フィンガープリントを指定します。 SHA256 フィンガープリントの使用をお勧めします。それは、OpenSSL（openssl x509 -in rootca.cer -noout -sha256 -fingerprint など）により、または Web ブラウザを使用して証明書の詳細を調べることにより、取得できます。 SHA256 フィンガープリントの場合は 64 桁の 16 進数文字値、SHA1 フィンガープリントの場合は 40 桁の 16 進数文字値を、一般的な区切り記号（コロン、ハイフン、ピリオド、スペース）を使用して、または区切り記号なしで入力します。 区切り記号を使用する場合、その区切り記号は、SHA256 フィンガープリントの場合は 16 進数文字 2、4、8、16、または 32 文字ごとに、また SHA1 フィンガープリントの場合は 16 進数文字 2、4、または 8 文字ごとに一貫して挿入する必要があります。 この機能をサポートしていない電話機の場合、このフィールドは表示されません。
WLAN認証試行（WLAN Authentication Attempts）			この機能をサポートしていない電話機の場合、このフィールドは表示されません。
WLANプロファイル1プロンプトモード（WLAN Profile 1 Prompt Mode）	無効 [有効（Enabled）]	無効	この機能をサポートしていない電話機の場合、このフィールドは表示されません。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
回線モード（Line Mode）	[セッション回線モード（Session Line Mode）] [拡張回線モード（Enhanced Line Mode）]	[セッション回線モード（Session Line Mode）]	電話機での回線表示を設定します。 • [セッション回線モード（Session Line Mode）]：画面の片側のボタンが回線キーです。 • [拡張回線モード（Enhanced Line Mode）]：電話画面の両側のボタンが回線キーです。デフォルトで、プレディクティブ ダイヤリングおよび適用可能な着信コールは、拡張回線モードで有効になります。
Admin Configurable Ringer	無効 [Sunrise] [Chirp1] [Chirp2]	無効	呼出音、およびユーザが呼出音を設定する機能を制御します。 • [無効（Disabled）] に設定した場合、ユーザは、電話機のデフォルトの呼出音を設定できます。 • 他のすべての値の場合、ユーザは呼出音を変更できません。 [設定（Settings）] メニューの [呼出音（Ringtone）] メニュー項目は、灰色表示になります。
カスタマーサポート使用（Customer Support Use）	64 文字以下の文字列。	Empty	Cisco TAC 専用です。
TLS暗号を無効にする	トランスポート層セキュリティ暗号を無効にする （188 ページ）を参照してください。	None	選択した TLS 暗号を無効にします。 複数の暗号スイートを無効にするには、コンピュータのキーボードで**Ctrl**キーを押したままにします。 すべての電話暗号を選択した場合、電話 TLS サービスが影響を受けます。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
Lower Your Voice アラート	[有効（Enabled）] 無効	[有効（Enabled）]	Lower Your Voice アラートを管理します。 • [Disabled]： • この電話機には、**[設定 (Settings)]**メニューの**[声を小さく（Lower Your Voice）]**メニュー項目が表示されません 。 • ユーザは大きな声で話すと、メッセージが出ても画面に表示されません。 • Enabled: • ユーザ は、**[設定 (Settings)]** メニューの**[声を小さく（Lower Your Voice）]**から機能を管理します。デフォルトでは、このフィールドは**[オン（On）]**に設定されています。
コールをスパムとしてマーク	[有効（Enabled）] 無効	[有効（Enabled）]	コールをスパム機能として[マーク（Mark）]を管理します。 • [Disabled]： • この電話機は、**[スパムのマーク（Mark spam）**を表示しません。 • **[設定 (Settings)]** メニューの **[スパムリスト（Spam list）]**項目は表示されません。 • スパムリストが存在する場合、そのリストは消去され、復元することはできません。 • Enabled: • この電話機は、**[スパムのマーク（Mark spam）**のソフトキーを表示します。 • **[設定 (Settings)]** メニューの **[スパムリスト（Spam list）]**項目を表示します。
コール パーク専用の 1 回線	無効 [有効（Enabled）]	[有効（Enabled）]	パークされたコールが1回線を占有するかどうかを制御します。 詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

フィールド名	フィールド タイプ または選択肢	デフォルト	説明と使用上のガイドライン
ELM での回線のテキストラベルの表示	無効 [有効（Enabled）]	[有効（Enabled）]	拡張回線モードが設定されている場合の通話中の回線ラベル表示を制御します。 • [有効（Enabled）] • 発信者名が設定されている場合、コール セッションの 1 行目に名前が表示され、2 行目にローカル回線ラベルが表示されます。 • 発信者名が設定されていない場合、1行目にリモート番号が表示され、2行目にローカル回線ラベルが 表示されます。 • 無効 • 発信者名が設定されている場合、コール セッションの 1 行目に名前が表示され、2 行目に番号が表示されます。 • 発信者名が設定されていない場合、リモート番号**のみ**表示されます。 このフィールドは必須です。

（注） コーデックのネゴシエーションでは、次の 2 つの手順が実行されます。

1. 電話機が、サポートされるコーデックを Cisco Unified Communications Manager にアドバタイズするかどうかを指定します。 すべてのエンドポイントがコーデックの同じ集合をサポートしているわけではありません。
2. Cisco Unified Communications Manager が、コール試行に関連するすべての電話機からサポートされるコーデックのリストを取得すると、リージョンペア設定などのさまざまな要因に基づいて一般にサポートされるコーデックが選択されます。

機能設定のベスト プラクティス

電話の機能は、ユーザのニーズに合わせて設定できます。 しかし実際に役立つ特定の状況や導入に関するいくつかの推奨事項があります。

通話量が多い環境

通話量が多い環境では、一部の機能を特定の方法で設定することをお勧めします。

フィールド	管理エリア	推奨される設定
[常にプライム回線を使用する(Always Use Prime Line)]	デバイス情報	off または on 詳細については、フィールド：[常にプライム回線を使用する（Always Use Prime Line）]（188ページ）を参照してください。
Actionable Incoming Call Alert	プロダクト固有の設定	すべての着信コールの表示
プライマリ回線にすべての通話の表示	プロダクト固有の設定	[有効（Enabled）]
すべてのコールに戻る（Revert to All Calls）	プロダクト固有の設定	[有効（Enabled）]

多回線環境

多回線環境では、一部の機能を特定の方法で設定することをお勧めします。

フィールド	管理エリア	推奨される設定
[常にプライム回線を使用する(Always Use Prime Line)]	デバイス情報	オフ 詳細については、フィールド：[常にプライム回線を使用する（Always Use Prime Line）]（188ページ）を参照してください。
Actionable Incoming Call Alert	プロダクト固有の設定	すべての着信コールの表示
プライマリ回線にすべての通話の表示	プロダクト固有の設定	[有効（Enabled）]
すべてのコールに戻る（Revert to All Calls）	プロダクト固有の設定	[有効（Enabled）]

セッション回線モードの環境

拡張回線モードは、ほとんどのコール環境の処理に適したツールです。しかし、拡張回線モードがニーズに適合しない場合は、セッション回線モードを使用してください。

フィールド	管理エリア	セッション回線モードの推奨設定
プライマリ回線にすべての通話の表示	プロダクト固有の設定	無効
すべてのコールに戻る（Revert to All Calls）	プロダクト固有の設定	無効
Actionable Incoming Call Alert	プロダクト固有の設定	デフォルトで有効（ファームウェア リリース 11.5(1) 以降）。

関連トピック

追加回線キーのセットアップ （230 ページ）
拡張回線モードで使用可能な機能 （231 ページ）

フィールド：[常にプライム回線を使用する（Always Use Prime Line）]

このフィールドは、ユーザがオフフックにしたときに IP 電話のプライマリ回線が選択されるかどうかを指定します。 このパラメータが True に設定されている場合、電話がオフフックになるとプライマリ回線が選択され、アクティブ回線になります。ユーザのセカンダリ回線で電話が鳴っている場合でも、電話がオフフックになると、プライマリ回線のみをアクティブにします。 セカンダリ回線の着信コールには応答しません。 この場合、ユーザはセカンダリ回線を選択してコールに応答する必要があります。 このデフォルト値は False に設定されています。

[常にプライム回線を使用する（Always Use Prime Line）] フィールドの目的は、[プライマリ回線にすべてのコールを表示（Show All Calls on the Primary Line）] と [すべてのコールに戻る（Revert to All Calls）] を組み合わせて使用し、両方の機能を有効化している場合と非常によく似ています。 ただし、主な違いは、[常にプライム回線を使用する（Always Use Prime Line）] が有効になっている場合は、セカンダリ回線では着信コールへの応答が行われないということです。 ダイヤル トーンはプライム回線でしか聞こえません。 このユーザ エクスペリエンスが求められるのは、通話量が多い特定の環境です。 一般的には、この機能を必要とする通話量が多い環境以外では、このフィールドを無効のままにしておくことを推奨します。

トランスポート層セキュリティ暗号を無効にする

[TLS暗号の無効化]パラメータを使用して、トランスポート層セキュリティ（TLS）暗号を無効にできます。これにより、既知の脆弱性に合わせてセキュリティを調整したり、ネットワークを暗号化に関する会社のポリシーに合わせることができます。

すべてデフォルト設定ではありません。

複数の暗号スイートを無効にするには、コンピュータのキーボードで**Ctrl**キーを押したままにします。すべての電話暗号を選択した場合、電話TLSサービスが影響を受けます。選択肢は、次のとおりです。

- なし
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

電話セキュリティの詳細については、*Cisco IP* 電話 *7800* および *8800* シリーズセキュリティの概要ホワイトペーパー（https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html）を参照してください。

共有回線のコール履歴の有効化

通話履歴に共有回線のアクティビティを表示できるようにします。この機能の目的は次のとおりです。

- 共有電話の不在着信をログに記録する。
- 共有電話のすべての応答済み着信と発信履歴をログに記録する。

始める前に

共有回線の通話履歴を有効にする前にプライバシーを無効にします。これを実行しないと、通話履歴に他のユーザが応答した通話が表示されません。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]**>**[電話（Phone）]** を選択します。

ステップ 2 設定する電話を特定します。

ステップ 3 製品固有の設定領域、共有回線ドロップダウンの [レコードコールログ (Record Call Log)] に移動します。

ステップ 4 ドロップダウン リストから [有効（Enabled）]を選択します。

ステップ 5 **保存**を選択します。

Cisco IP 電話 での省電力のスケジュール

電力を節約し、電話スクリーンディスプレイの寿命を確実に延ばすには、不要なときに表示をオフにするように設定します。

Cisco Unified Communications Manager の管理ページを使用すると、ディスプレイを特定の曜日の指定時刻にオフにし、他の曜日では終日オフにするように設定できます。 たとえば、ディスプレイを平日の勤務時間後にオフにし、土曜日と日曜日では終日オフにするように選択できます。

ディスプレイがオフのときはいつでも、次の操作でディスプレイをオンにできます。

- 電話機の任意のボタンを押す。

  ディスプレイがオンになり、そのボタンで指定されているアクションが実行されます。

- ハンドセットを持ち上げる。

ディスプレイは、オンにするとそのままオン状態になりますが、指定された期間にわたって電話機がアイドル状態にあると、自動的にオフになります。

詳細については、プロダクト固有の設定 （161 ページ） を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 設定する電話機を特定します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動して、次のフィールドを設定します。

- ディスプレイ非点灯日（Days Display Not Active）
- ディスプレイ点灯時刻（Display On Time）
- ディスプレイ点灯継続時間（Display On Duration）
- ディスプレイ放置時自動消灯（Display Idle Timeout）

表 *32 : PowerSave* の設定フィールド

フィールド	説明
ディスプレイ非点灯日（Days Display Not Active）	[ディスプレイ点灯時刻（Display On Time）] フィールドで指定された時刻になっても、ディスプレイを自動的にオンにしない日。 ドロップダウン リストから単一または複数の曜日を選択します。 複数の曜日を選択するには、Ctrl キーを押しながら目的の各曜日をクリックします。

フィールド	説明
ディスプレイ点灯時刻（Display On Time）	毎日ディスプレイを自動的にオンにする時刻（[ディスプレイ非点灯日（Days Display Not Active）] フィールドで指定されている日を除く）。 このフィールドには、24 時間形式で入力します（0:00 は午前 0 時）。 たとえば、午前 7:00（0700）にディスプレイを自動的にオンにするには、**07:00** と入力します。 午後 2 時 にディスプレイをオンにするには （1400）にバックライトをオンにするには、**14:00** と入力します。 このフィールドがブランクの場合、ディスプレイは午前 0 時に自動的にオンになります。
ディスプレイ点灯継続時間（Display On Duration）	[ディスプレイ点灯時刻（Display On Time）] フィールドで指定した時刻にディスプレイがオンになった後、オン状態を保つ時間の長さ。 このフィールドには、時間:分の形式で値を入力します。 たとえば、ディスプレイを自動的にオンにしてから 4 時間 30 分にわたってオン状態を保つには、**4:30** と入力します。 このフィールドがブランクの場合、電話機は午前 0 時（0:00）にオフになります。 （注） [ディスプレイ点灯時刻（Display On Time）] が 0:00 で、[ディスプレイ点灯継続時間（Display On Duration）] がブランク（または 24:00）の場合、電話機は常にオン状態になります。
ディスプレイ放置時自動消灯（Display Idle Timeout）	ディスプレイをオフにするまでの電話機のアイドル時間。ディスプレイがスケジュールどおりにオフで、ユーザが（電話機ボタンを押す、またはハンドセットを持ち上げる操作で）オンにした場合にのみ適用されます。 このフィールドには、時間:分の形式で値を入力します。 たとえば、ユーザがディスプレイをオンにしてから 1 時間 30 分にわたって電話機がアイドル状態にあった場合にディスプレイをオフにするには、**1:30** と入力します。 デフォルト値は 1:00 です。

ステップ 4 **保存**を選択します。

ステップ 5 [設定の適用（Apply Config）]を選択します。

ステップ 6 電話機を再起動します。

Cisco IP 電話 での EnergyWise のスケジュール

消費電力を減らすには、ご使用のシステムにEnergyWiseコントローラが含まれている場合に、電話機をスリープ（電源オフ）とウェイク（電源オン）に設定します。

Cisco Unified Communications Manager の管理で、EnergyWise を有効にして、スリープ時間とウェイク時間の設定を行います。 これらのパラメータは、電話機の表示設定パラメータと緊密に結びついています。

EnergyWiseが有効になっていて、スリープ時間が設定されていると、電話機を設定時刻に復帰させるように、電話機からスイッチに要求が送信されます。 この要求の受諾または拒否が、スイッチから戻ります。 スイッチが要求を拒否した場合、またはスイッチが応答しない場合は、電話機はオフになりません。 スイッチが要求を受諾すると、アイドル状態の電話機がスリープ状態となり、消費電力をあらかじめ決められたレベルに減らすことができます。 アイドル状態になっていない電話機にはアイドルタイマーが設定され、タイマーの期限が切れると、電話機がスリープ状態になります。

電話機をウェイクさせるには、選択ボタンを押します。 スケジュールされているウェイク時間になると、システムは電話機の電力を元に戻して電話機を復帰させます。

詳細については、プロダクト固有の設定 （161 ページ） を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 設定する電話機を特定します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動して、次のフィールドを設定します。

- Enable Power Save Plus
- 電話機をオンにする時刻（Phone On Time）
- 電話機をオフにする時刻（Phone Off Time）
- Phone Off Idle Timeout
- Enable Audible Alert
- EnergyWise Domain
- EnergyWise シークレット
- Allow EnergyWise Overrides

表 *33 : EnergyWise Configuration Fields*

フィールド	説明
Enable Power Save Plus	電話機の電源をオフにする日のスケジュールを選択します。 スケジュールを設定する日をクリックしたら、Control キーを押したままにして、複数日を選択します。 デフォルトでは、どの日も選択されていません。 [Power Save Plus の有効化（Enable Power Save Plus）] がオンになっていると、緊急（e911）の問題について警告するメッセージを受け取ります。 **注意** Power Save Plus モード（「モード」）が有効である間は、モードに設定されたエンドポイントは、緊急コールでは無効で、インバウンドコールの受信ができません。このモードを選択することにより、次の条項に同意したものと見なされます。（i）モードが有効である間、緊急コールとコールの受信用の代替方法を責任を持って用意する必要があります。（ii）シスコはこのモードの選択に関して何の責任を負いません。このモードを有効にすることは、お客様の責任で行っていただきます。（iii）コール、発信、およびその他について、このモードを有効にした場合の影響をユーザにすべて通知する必要があります。 （注） Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオフにする必要があります。 [Power Save Plus の有効化（Enable Power Save Plus）] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオンにしたままにしておくと、Power Save Plus は無効になりません。
電話機をオンにする時刻（Phone On Time）	[Power Save Plus の有効化（Enable Power Save Plus）] フィールドにある日について、電話機の電源を自動的にオンにする時刻を決定します。 このフィールドには、24 時間形式で入力します（0:00 は午前 0 時）。 たとえば、午前 7 時（0700）に自動的に電話機の電源をオンにする場合は、 7:00 と入力します。 午後 2 時（1400）に電話機の電源をオンにするには、14:00 と入力します。 デフォルト値はブランクで、これは 00:00 を意味します。 （注） [電話機をオンにする時刻（Phone On Time）] は、[電話機をオフにする時刻（Phone Off Time）] より 20 分以上遅い時刻に設定する必要があります。たとえば、[電話機をオフにする時刻（Phone Off Time）] が 7:00 の場合、[電話機をオンにする時刻（Phone On Time）] は 7:20 より前に設定しないでください。

フィールド	説明
電話機をオフにする時刻（Phone Off Time）	[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択した日について、電話機の電源をオフにする時刻。 [電話機をオンにする時刻（Phone On Time）] フィールドと [電話機をオフにする時刻（Phone Off Time）] フィールドに同じ値が含まれている場合、電話機はオフになりません。 このフィールドには、24 時間形式で入力します（0:00 は午前 0 時）。 たとえば、午前 7 時（0700）に自動的に電話機の電源をオフにする場合は、 7:00 と入力します。 午後 2 時（1400）に電話機の電源をオフにするには、 （1400）にバックライトをオンにするには、14:00 と入力します。 デフォルト値はブランクで、これは 00:00 を意味します。 （注） [電話機をオンにする時刻（Phone On Time）] は、[電話機をオフにする時刻（Phone Off Time）] より 20 分以上遅い時刻に設定する必要があります。たとえば、[電話機をオフにする時刻（Phone Off Time）] が 7:00 の場合、[電話機をオンにする時刻（Phone On Time）] は 7:20 より前に設定しないでください。
Phone Off Idle Timeout	電話機の電源をオフにする前に、電話機をアイドル状態にしておく必要がある時間の長さ。 タイムアウトは次の条件で発生します。 • 電話機がスケジュールどおりに Power Save Plus モードになっていたが、電話機のユーザが [選択（Select）]キーを押したために、Power Save Plus モードが解除された場合。 • 接続スイッチで電話機が再びオンになった場合。 • [電話機をオフにする時刻（Phone Off Time）] になったが、通話中の場合。 このフィールドの範囲は 20 ～ 1440 分です。 デフォルト値は 60 分です。

フィールド	説明
Enable Audible Alert	これを有効にすると、[電話機をオフにする時刻（Phone Off Time）] で指定した時刻の 10 分前に電話機で音声アラートの再生が開始されます。 音声アラートは、電話機の呼出音を使用します。この音は、10 分間のアラート期間中の特定期間、短く再生されます。 呼出音は、ユーザが指定した音声レベルで再生されます。 音声アラートのスケジュールは次のとおりです。 • 電源オフの 10 分前に、呼出音が 4 回再生されます。 • 電源オフの 7 分前に、呼出音が 4 回再生されます。 • 電源オフの 4 分前に、呼出音が 4 回再生されます。 • 電源オフの30秒前に、呼出音は、15回再生されるか、電話機の電源がオフになるまで再生されます。 このチェックボックスが表示されるのは、[Power Save Plus の有効化（Enable Power Save Plus）] リストボックスで 1 日以上が選択されている場合だけです。
EnergyWise Domain	その電話機が含まれる EnergyWise ドメイン。 このフィールドの最大長は 127 文字です。
EnergyWise シークレット	EnergyWise ドメイン内でエンドポイントとの通信に使用されるセキュリティの秘密パスワード。 このフィールドの最大長は 127 文字です。

フィールド	説明
Allow EnergyWise Overrides	このチェックボックスにより、電話機に電源レベルの更新を送信するためのEnergyWiseドメイン コントローラのポリシーを許可するかどうかを決定します。 次の条件が適用されます。 • [Power Save Plus の有効化（Enable Power Save Plus）] フィールドで 1 日以上を選択する必要があります。 • Cisco Unified Communications Manager の管理ページの設定は、EnergyWise がオーバーライドを送信しても、スケジュールに適用されます。 たとえば、[電話機をオフにする時刻（Phone Off Time）] が 22:00（午後 10 時）に設定されていると仮定すると、[電話機をオンにする時刻（Phone On Time）] フィールドの値は 06:00（午前 6 時）となり、[Power Save Plus の有効化（Enable Power Save Plus）] では 1 日以上が選択されています。 • EnergyWise が 20:00（午後 8 時）に電話機をオフにするように指示すると、この指示は、午前 6 時に設定された [電話機をオンにする時刻（Phone On Time）] まで有効となります（電話機ユーザによる介入が発生しないと仮定した場合）。 • 午前 6 時になると、電話機はオンとなり、Unified Communications Manager の管理ページの設定から電力レベルの変更の受信を再開します。 • 電力レベルを電話機で再び変更するには、EnergyWise は電力レベル変更コマンドを新たに再発行する必要があります。 （注） Power Save Plus を無効にするには、[EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオフにする必要があります。 [Power Save Plus の有効化（Enable Power Save Plus）] フィールドで、日数を選択しないまま [EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）] チェックボックスをオンにしたままにしておくと、Power Save Plus は無効になりません。

ステップ 4 **保存**を選択します。

ステップ 5 [設定の適用（Apply Config）]を選択します。

ステップ 6 電話機を再起動します。

サイレントの設定

サイレント（DND）をオンにすると、コールが呼び出し状態になっても呼出音が鳴らなくなります。またあらゆる種類の表示や音による通知も、一切行われません。

サイレント（DND）を有効にすると、電話画面のヘッダー セクションの色が変更され、電話機に「サイレント（Do Not Disturb）」と表示されます。

電話ボタン テンプレートの機能の 1 つとして DND を選択して、電話機を設定できます。

詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルの取り込み中情報を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]**>**[電話（Phone）]** を選択します。

ステップ 2 設定する電話を特定します。

ステップ 3 次のパラメータを設定します。

- [サイレント（Do Not Disturb）]：このチェックボックスを使用すると、電話機の DND を有効にすることができます。
- DND オプション：[呼出音オフ（Ring Off）]、[コール拒否（Call Reject）]、または [共通の電話プロファイル設定を使用（Use Common Phone Profile Setting）]。

  DND がオンのときにプライオリティ（MLPP）コールでこの電話の呼出音が鳴るようにする場合は、[コール拒否（Call Reject）] を選択しないでください。
- [DND 着信呼警告（DND Incoming Call Alert）]：電話機で DND がアクティブのときに着信コールに対して発生させるアラート（存在する場合）のタイプを選択します。

  （注） このパラメータは、[共通の電話プロファイル（Common Phone Profile）] ウィンドウと [電話の設定（Phone Configuration）] ウィンドウにあります。[電話の設定（Phone Configuration）] ウィンドウの値が優先されます。

ステップ 4 **保存**を選択します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

エージェント グリーティングの有効化

エージェント グリーティング機能では、エージェントが事前録音したグリーティングを作成したり更新したりできます。このグリーティングは、エージェントが発信者と話しはじめる前に、顧客コールなどのコールの開始時に再生されます。エージェントは、必要に応じて 1 つまたは複数のグリーティングを事前録音し、グリーティングを作成および更新できます。

顧客が電話をかけてきた場合、エージェントと発信者が事前録音したグリーティングを聴くことになります。エージェントは、グリーティングが終わるまで待つこともできますし、グリーティングの途中で応答することもできます。

エージェント グリーティング コールでは、電話機でサポートされるすべてのコーデックがサポートされます。

詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルの割り込みおよびプライバシー情報を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページから **[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 ユーザが設定する IP フォンを特定します。

ステップ 3 [デバイス情報レイアウト（Device Information Layout）] ペインまでスクロールし、[ビルトイン ブリッジ（Built In Bridge）] を [オン（On）] または [デフォルト（Default）] に設定します。

ステップ 4 **保存**を選択します。

ステップ 5 ブリッジの設定を確認します。

a) **[System（システム）]** > **[Service Parameters（サービス パラメータ）]** を選択します。
b) 適切なサーバおよびサービスを選択します。
c) [クラスタワイド パラメータ（デバイス - 電話）（Clusterwide Parameters (Device - Phone)）] ペインまでスクロールして、[ビルト イン ブリッジの有効（Builtin Bridge Enable）] を [オン（On）] に設定します。
d) **保存**を選択します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

モニタリングと録音のセットアップ

モニタリングと録音の機能によって、スーパーバイザはアクティブ コールのモニタリングをサイレントに実行できます。 スーパーバイザの音声はコールのどちらの側にも聞こえません。 ユーザには、コールがモニタされている間、モニタ中であることを示す音声アラートが聞こえる場合があります。

コールがセキュリティで保護されている場合は、ロック アイコンが表示されます。 発信者にも、コールがモニタされていることを示す音声アラートが聞こえる場合があります。 コールがセキュアであり、モニタされていることを示す音声アラートは、接続先の通話者にも聞こえることがあります。

アクティブ コールがモニタまたは録音されている場合、ユーザは、インターコムコールを受信または発信できます。ただし、ユーザがインターコムコールを発信した場合、アクティブ コールは保留されます。 この処理によって録音セッションは終了し、モニタリング セッションは中断されます。 中断されたモニタリング セッションを再開するには、モニタされているユーザがコールを再開する必要があります。

詳細については、ご使用の Cisco Unified Communications Manager リリースのマニュアルのモニタリングおよび録音情報を参照してください。

以下の手順によって、標準モニタ ユーザ グループにユーザが追加されます。

始める前に

Cisco Unified Communications Manager は、モニタリングと録音をサポートするように設定する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、**[ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）]** を選択します。

ステップ 2 Standard CTI Allow Call Monitoring および Standard CTI Allow Call Recording ユーザ グループを確認します。

ステップ 3 **[選択項目の追加(Add Selected)]** をクリックします。

ステップ 4 [ユーザ グループに追加（Add to User Group）]をクリックします。

ステップ 5 アプリケーション ユーザの制御デバイスのリストにユーザの電話機を追加します。

ステップ 6 **保存**を選択します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

コールの転送通知のセット アップ

コール転送設定を制御できます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）] > [電話（Phone）]** を選択します。

ステップ 2 セット アップする電話を特定します。

ステップ 3 [コールの転送通知（Call Forward Notification）] フィールドを設定します。

フィールド	説明
Caller Name	このチェックボックスをオンにした場合、発信者名が通知ウィンドウに表示されます。 デフォルトでは、このチェックボックスはオンになっています。
Caller Number	このチェックボックスをオンにした場合、発信者番号が通知ウィンドウに表示されます。 デフォルトでは、このチェックボックスはオフになっています。

フィールド	説明
Redirected Number	このチェックボックスをオンにした場合、コールを最後に転送した発信者に関する情報が通知ウィンドウに表示されます。 例：発信者 A が B にコールを発信したが、B はすべてのコールを C に転送し、C はすべてのコールを D に転送した場合、D に対して表示される通知ボックスには、発信者 C の電話機情報が表示されます。 デフォルトでは、このチェックボックスはオフになっています。
Dialed Number	このチェックボックスをオンにした場合、コールの最初の受信者に関する情報が通知ウィンドウに表示されます。 例：発信者 A が B にコールを発信したが、B はすべてのコールを C に転送し、C はすべてのコールを D に転送した場合、D に対して表示される通知ボックスには、発信者 B の電話機情報が表示されます。 デフォルトでは、このチェックボックスはオンになっています。

ステップ 4 **保存**を選択します。

コール リストの BLF の有効化

[コールリストのBLF（BLF for Call Lists）] フィールドでも、社内ディレクトリの回線ステータス機能を制御します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 [コールリストのBLF（BLF for Call Lists）] フィールドで、この機能を有効または無効にします。

デフォルトでは、この機能はディセーブルです。

[プロダクト固有の設定（Product Specific Configuration）] エリアで設定したパラメータは、さまざまなデバイスの [デバイス設定（Device Configuration）] ウィンドウと [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウにも表示されることがあります。 これらの他のウィンドウでも同じパラメータを設定した場合、優先される設定は、次の順序で決定されます。

1. [デバイス設定(Device Configuration)] ウィンドウの設定値
2. [共通の電話プロファイル(Common Phone Profile)] ウィンドウの設定値

3. [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウの設定値

ステップ 3 **保存**を選択します。

スイッチおよび PC ポート用の Energy Efficient Ethernet のセットアップ

IEEE 802.3 標準の拡張である IEEE 802.3az Energy Efficient Ethernet（EEE）は、ネットワークインターフェイスの重要な機能を損なうことなくエネルギー使用量を減らす方法を提供します。 設定可能な EEE を使用すると、管理者は PC ポートとスイッチ ポートでの EEE 機能を制御することができます。

（注） 管理者は、すべての適用可能な UCM ページで [オーバーライド（Override）] チェックボックスがオンになっていることを確認する必要があります。オンになっていないと、EEE は機能しません。

管理者は、次の 2 つのパラメータで EEE 機能を制御します。

- **Energy Efficient Ethernet**：パーソナル コンピュータとのシームレスな接続を提供します。管理者は、[有効（Enabled）] または [無効（Disabled）] のオプションを選択して機能を制御します。
- **Energy Efficient Ethernet**:スイッチ ポート（Energy Efficient Ethernet:Switch Port）：シームレスな接続を提供します。

詳細は、プロダクト固有の設定 （161 ページ）を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、次のいずれかのウィンドウを選択してください。

- **[デバイス（Device）] > [電話（Phone）]**
- **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]**
- **[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configurations）]**

複数のウィンドウにパラメータを設定した場合、優先順位は次のとおりです。

1. **[デバイス（Device）] > [電話（Phone）]**
2. **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]**
3. **[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configurations）]**

ステップ 2 必要に応じて、電話機を特定します。

ステップ 3 [Energy Efficient Ethernet: PC ポート（Energy Efficient Ethernet: PC Port）]および [Energy Efficient Ethernet: スイッチ ポート（Energy Efficient Ethernet: Switch Port）]フィールドを設定します。

- Energy Efficient Ethernet: PC ポート（Energy Efficient Ethernet: PC Port）
- Energy Efficient Ethernet: スイッチ ポート（Energy Efficient Ethernet: Switch Port）

ステップ 4 **保存**を選択します。

ステップ 5 [設定の適用（Apply Config）]を選択します。

ステップ 6 電話機を再起動します。

RTP/sRTP ポート範囲のセットアップ

SIP プロファイルでリアルタイム転送プロトコル（RTP）およびセキュア リアルタイム転送プロトコル（sRTP）のポートの値を設定します。 RTP と sRTP ポートの値の範囲は 2048 から 65535 で、デフォルトの範囲は 16384 から 32764 です。RTP と sRTP のポート値の範囲は他の電話サービス用に指定されています。 これらのポートは RTP および SRTP 用に設定できません。

詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルの SIP プロファイル情報を参照してください。

手順

ステップ 1 **[デバイス（Device）]>[デバイスの設定（Device Settings）]>[SIP プロファイル（SIP Profile）]** の順に選択します。

ステップ 2 使用する検索条件を選択し、[検索（Find）]をクリックします。

ステップ 3 変更するプロファイルを選択します。

ステップ 4 ポート範囲の開始と終了を含むように [開始メディアポート（Start Media Port）] および [終了メディアポート（Stop Media Port）] を設定します。

次のリストでは、他の電話サービスに使用されるため、RTP および SRTP で利用できない UDP ポートを判別します。

ポート 4051

ピア ファームウェア共有（PFS）機能に使用される

ポート 5060

UDP を介した SIP に使用される

ポート 49152 ～ 53247

ローカル エフェメラル ポートに使用される

ポート 53248 ～ 65535

VxC シングル トンネル VPN 機能に使用される

ステップ 5 **[保存]** をクリックします。

ステップ 6 **[設定の適用（Apply Config）]** をクリックします。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

Expressway 経由でのモバイルおよび Remote Access

Expressway 経由でのモバイルおよび Remote Access(MRA) を使用すると、リモート ワーカーは、仮想プライベート ネットワーク（VPN）クライアント トンネルを使用しなくても企業のネットワークに簡単かつ安全に接続できます。Expressway は、Transport Layer Security（TLS）を使用してネットワーク トラフィックを保護します。電話機が Expressway 証明書を認証し、TLS セッションを確立するには、Expressway 証明書に、電話機のファームウェアが信頼しているパブリック認証局による署名が必要です。Expressway 証明書の認証に対して、電話機で他の CA 証明書をインストールしたり信頼したりすることはできません。

電話機ファームウェアに組み込まれているの CA 証明書の一覧は、http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html から入手できます。

Expressway 経由でのモバイルおよび Remote Access (MRA) は、Cisco Expressway で動作します。このため、『*Cisco Expressway Administrator Guide*』、『*Cisco Expressway Basic Configuration Deployment Guide*』などの Cisco Expressway のマニュアルをよくお読みいただく必要があります。Cisco Expressway のマニュアルは、http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html にあります。

ユーザに対しては、IPv4 プロトコルのみが Expressway 経由でのモバイルおよび Remote Access サポートされます。

Expressway 経由でのモバイルおよび Remote Access の操作方法については、以下の資料も参照してください。

- *Cisco Preferred Architecture for Enterprise Collaboration, Design Overview*
- *Cisco Preferred Architecture for Enterprise Collaboration, CVD*
- *Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide*
- *Cisco TelePresence Video Communication Server (VCS), Configuration Guides*
- *Cisco Expressway*展開ガイドによるモバイルおよび *Remote Access*

電話の登録プロセス中に、電話機に表示される日時が Network Time Protocol（NTP）サーバと同期されます。MRA では、日時の同期に指定される NTP サーバの IP アドレスを特定するた

めに DHCP オプション 42 タグが使用されます。DHCP オプション 42 タグが設定情報の中に見つからない場合、電話機は 0.tandberg.pool.ntp.org タグを検索して NTP サーバを識別します。

登録後、電話機は SIP メッセージの情報を使って表示日時を同期します（ただし Cisco Unified Communications Manager 電話設定で NTP サーバが設定されている場合を除く）。

（注） いずれかの電話機の電話セキュリティ プロファイルで TFTP 暗号化設定にチェックマークが付いている場合、Mobile and Remote Access でその電話機を使用することはできません。MRA ソリューションでは、認証局プロキシ機能（CAPF）とデバイスとのインタラクティブなやり取りをサポートしていません。

Expressway 経由でのモバイルおよび Remote Access は拡張回線モードをサポートします。

SIP OAuth モードは、MRA でサポートされています。このモードでは、セキュアな環境での認証に OAuth アクセス トークンを使用できます。

（注） モバイルおよびリモート アクセス (MRA) モードの SIP OAuth の場合は、電話機を導入する際に、モバイルおよびリモート アクセスでのアクティベーション コードの導入のみを使用します。ユーザ名とパスワードを使用したアクティベーションはサポートされていません。

SIP OAuth モードでは、Expressway x14.0(1) 以降、または Cisco Unified Communications Manager 14.0 (1) 以降が必要です。

SIP OAuth モードの詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』、リリース 14.0(1) 以降を参照してください。

展開シナリオ

次のセクションで、Expressway 経由でのモバイルおよび Remote Access のさまざまな導入シナリオを示します。

オフプレミス ユーザが企業ネットワークにログインします。

Expressway 経由でのモバイルおよび Remote Access が配置されている場合は、オンプレミスのときにエンタープライズネットワークにログインします。 ネットワークを検出すると、電話は Cisco Unified Communications Manager に登録します。

オフプレミス ユーザが企業ネットワークにログインします。

オフィスから離れていると、電話機は構外モードであることを検出します。 のExpressway 経由でのモバイルおよび Remote Accessサインインウィンドウが表示され、企業ネットワークに接続します。

次の点に注意してください。

- ネットワークに接続するには、有効なサービス ドメイン、ユーザ名、パスワードが必要です。
- 企業ネットワークにアクセスする前に、サービス モードをリセットして、代替 TFTP 設定をクリアする必要があります。 これにより代替 TFTP サーバ設定がクリアされるため、電話機が構外ネットワークを検出し、VPN 接続の確立を停止します。 電話機を初めて配置する場合は、この手順を省略してください。
- ネットワーク ルータで DHCP オプション 150 またはオプション 66 が有効になっている場合は、企業ネットワークにサインインできない場合があります。 MRA モードにするには、サービス モードをリセットする必要があります。

オフプレミス ユーザがVPNで企業ネットワークにログインします。

Expressway 経由でのモバイルおよび Remote Access 導入後、オフプレミスの場合、VPN を使用して企業ネットワークにログインします。

電話機にエラーが発生した場合は、基本リセットを実行して電話機の設定をリセットします。

代替 TFTP 設定を構成する必要があります（**[管理者設定]** > **[ネットワーク設定]** > **[IPv4]** の **[代替 TFTP サーバ 1]** フィールド）。

関連トピック

基本的なリセット （317 ページ）

メディア ルーティングを向上させる Interactive Connectivity Establishment（ICE）

ファイアウォールまたはネットワークアドレス変換（NAT）を通過する Mobile and Remote Access（MRA）コールの信頼性を向上させるために、Interactive Connectivity Establishment（ICE）を配置できます。 ICE は、NAT サービスの周囲でシリアルトンネリングおよびトラバーサル リレーを使用してコールに最適なメディアパスを選択するオプションの展開です。

セカンダリターンサーバおよびターンサーバフェイルオーバーはサポートされていません。

MRA および ICEサービスの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager* リリース *12.0(1)*以降』を参照してください。 インターネット技術特別調査委員会（IETF）の Request for Comment 文書にも追加情報があります。

- 『*Traversal Using Relays around NAT (TURN)*』：*Session Traversal Utilities for NAT*（*STUN*）のためのリレー拡張(RFC 5766)
- 『*Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols*』(RFC 5245)

Expressway 経由でのモバイルおよび Remote Access で利用可能な電話機能

Expressway 経由でのモバイルおよび Remote Access を使用すれば、シスコのモバイルおよびリモート ユーザは、VPN を使用せずに安全にコラボレーション サービスにアクセスできます。 ただし、ネットワーク セキュリティを維持するために、電話機能の一部が制限されます。

次に、Expressway 経由でのモバイルおよび Remote Access で利用可能な電話機能のリストを示します。

表 *34 :* 機能サポートおよび *Expressway* 経由でのモバイルおよび *Remote Access*

電話機能	電話ファームウェアのリリース
短縮ダイヤル	10.3(1) 以降
最初のコールへ応答	11.5(1)SR1 以降
処理されたダイレクト コール パーク	10.3(1) 以降
自動応答	11.5(1)SR1 以降
割り込みと C 割り込み	11.5(1)SR1 以降
話中 ランプ フィールド（BLF）	10.3(1) 以降
ビジー ランプ フィールド（BLF）ピックアップ	10.3(1) 以降
ビジーランプ フィールド（BLF）スピードダイヤル	10.3(1) 以降
コールバック	10.3(1) 以降
通話転送	10.3(1) 以降
コールの転送通知	10.3(1) 以降
コール パーク	10.3(1) 以降
コール ピックアップ	10.3(1) 以降
Cisco Unified Serviceability	11.5(1)SR1 以降
クライアント アクセス ライセンス（CAL）	11.5(1)SR1 以降
会議	10.3(1) 以降
会議リスト/参加者の削除	11.5(1)SR1 以降
社内ディレクトリ(Corporate Directory)	11.5(1)SR1 以降
CTI アプリケーション（CTI 制御）	11.5(1)SR1 以降
直接転送	10.3(1) 以降
ダイレクト コール パーク	10.3(1) 以降
固有呼び出し音	11.5(1)SR1 以降

電話機能	電話ファームウェアのリリース
即転送	10.3(1) 以降
拡張回線モード	12.1(1) 以降
即転送	10.3(1) 以降
強制アクセス コードおよびクライアント識別コード	11.5(1)SR1 以降
グループ コール ピックアップ	10.3(1) 以降
保留または復帰	10.3(1) 以降
保留復帰	10.3(1) 以降
即時転送	10.3(1) 以降
参加（Join）	10.3(1) 以降
迷惑呼 ID（MCID）	11.5(1)SR1 以降
Meet-Me 会議	10.3(1) 以降
メッセージ受信インジケータ	10.3(1) 以降
モバイル コネクト	10.3(1) 以降
モバイル ボイス アクセス	10.3(1) 以降
Multilevel Precedence and Preemption（MLPP）	11.5(1)SR1 以降
マルチライン	11.5(1)SR1 以降
保留音	10.3(1) 以降
ミュート	10.3(1) 以降
ネットワーク プロファイル（自動）	11.5(1)SR1 以降
オフフック ダイヤル	10.3(1) 以降
オンフック ダイヤル	10.3(1) 以降
プラス ダイヤル	10.3(1) 以降
[プライバシー（Privacy）]	11.5(1)SR1 以降
Private Line Automated Ringdown（PLAR）	11.5(1)SR1 以降
Redial	10.3(1) 以降

電話機能	電話ファームウェアのリリース
スピード ダイヤル（ポーズはサポートしていません）	10.3(1) 以降
サービス URL ボタン	11.5(1)SR1 以降
転送	10.3(1) 以降
Uniform Resource Identifier（URI）ダイヤリング	10.3(1) 以降

Expressway サインイン用ユーザ クレデンシャル パーシステントの設定

Expressway 経由でのモバイルおよび Remote Access でネットワークにサインインすると、そのユーザはサービス ドメイン、ユーザ名、パスワードの入力を求められます。 Expressway サインイン用のユーザ クレデンシャル パーシステントのパラメータを有効化すると、ユーザのログイン クレデンシャルが保存され、この情報を再入力する必要がなくなります。 このパラメータはデフォルトでは無効になっています。

単一の電話機、電話機グループ、またはすべての電話機について、クレデンシャルが永続的なものとなるように設定できます。

関連トピック

電話機の機能設定 （159 ページ）
プロダクト固有の設定 （161 ページ）

MRA サインイン用の QR コードの生成

カメラ付き電話を持つユーザは、サービス ドメインとユーザ名を手動で入力する代わりに、QR コードをスキャンして MRA にサインインできます。

手順

ステップ 1 QR コードは、QR コード ジェネレータを使用して生成します。それには、サービス ドメインのみか、サービス ドメインとユーザ名をカンマで区切って指定します。 例：mra.example.com または mra.example.com,username。

ステップ 2 QR コードを印刷し、ユーザに提供します。

問題レポート ツール

ユーザが問題レポートを送信する際は、問題レポート ツールを使用します。

（注） 問題レポート ツールのログは、Cisco TAC で問題をトラブルシューティングするときに必要となります。 電話機を再起動すると、ログは消去されます。 電話機を再起動する前に、ログを収集してください。

問題レポートを発行するには、ユーザは問題レポート ツールにアクセスし、問題の発生日時、および問題の説明を提供します。

PRT のアップロードが失敗した場合は、電話機を使用して URL **HTTP://<phone-ip-address>/FS/<prt-file-name>** から PRT ファイルにアクセスできます。 この URL は、次の場合に電話機に表示されます。

- 電話機が工場出荷時の状態の場合。 URL の表示時間は 1 時間です。 1 時間経過後は、電話機ログの送信を再度試行する必要があります。
- 電話機に設定ファイルをダウンロード済みで、コール制御システムで電話への Web アクセスが許可されている場合。

Cisco Unified Communications Manager の [カスタマー サポート アップロード URL（Customer Support Upload URL）] フィールドにサーバ アドレスを追加する必要があります。

Expressway 経由で Mobile and Remote Access を使用してデバイスを導入している場合、Expressway サーバの HTTP サーバ許可リストへの PRT サーバ アドレスの追加も必要となります。

カスタマー サポート アップロード URL の設定

サーバでアップロード スクリプトを使用して PRT ファイルを受信する必要があります。 PRT は HTTP POST 機構を使用します。その際、アップロードに次のパラメータを含めます（マルチパート MIME 符号化を使用）。

- devicename（例：「SEP001122334455」）
- serialno（例：「FCH12345ABC」）
- ユーザ名（Cisco Unified Communications Managerに設定されているユーザ名、デバイスの所有者）
- prt_file（例：「probrep-20141021-162840.tar.gz」）

スクリプトのサンプルを次に示します。 このスクリプトは参考用としてのみ提供されます。シスコでは、お客様のサーバにインストールされたアップロードスクリプトのサポートは提供していません。

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);
```

```
// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

（注） 電話機は、HTTP Url のみをサポートしています。

手順

ステップ 1 PRT アップロード スクリプトを実行できるサーバを設定します。

ステップ 2 上記パラメータを処理できるスクリプトを記述するか、必要に応じて提供されたサンプル スクリプトを編集します。

ステップ 3 サーバにスクリプトをアップロードします。

ステップ 4 Cisco Unified Communications Manager で、個々のデバイス設定ウィンドウ、[共通の電話プロファイル（Common Phone Profile）] ウィンドウ、または [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動します。

ステップ 5 [カスタマー サポートのアップロード URL（Customer support upload URL）] をオンにし、アップロード サーバ URL を入力します。

例：

http://example.com/prtscript.php

ステップ 6 変更を保存します。

回線のラベルの設定

電話番号の代わりにテキスト ラベルを表示するよう電話機をセットアップすることができます。 このラベルを使用し、回線を名前または機能で特定します。 たとえば、ユーザが電話機の回線を共有している場合、回線を共有するユーザの名前で回線を特定できます。

キー拡張モジュールにラベルを追加すると、最初の 25 文字だけが行に表示されます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 設定する電話を特定します。

ステップ 3 回線インスタンスを特定し、[回線のテキスト ラベル（Line Text Label）] フィールドを設定します。

ステップ 4 （任意） 回線を共有する別のデバイスにラベルを適用する必要がある場合は、[共有デバイス設定の更新（Update Shared Device Settings）] チェックボックスをオンにして、[選択対象を反映（Propagate Selected）] をクリックします。

ステップ 5 **保存**を選択します。

デュアル バンク情報のセットアップ

デュアルバンク情報をセット アップするには、次の手順に従います。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[デバイスのデフォルト（Device Defaults）]** を選択します。

ステップ 2 [非アクティブ ロード情報（Inactive Load Information）] フィールドで、ロード情報をチェックします。

ステップ 3 **[一括管理（Bulk Administration）]** > **[インポート/エクスポート（Import/Export）]** > **[エクスポート（Export）]** > **[デバイスのデフォルト（Device Defaults）]** と選択し、エクスポート ジョブをスケジュールします。

ステップ 4 エクスポートされた tar ファイルをダウンロードし、untar します。

ステップ 5 エクスポートされた CSV ファイルでファイル形式をチェックし、その CSV ファイルに、値が正しい [非アクティブ ロード情報（Inactive Load Information）] の列があることを確認します。

（注） CSV ファイルの値は、[Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] ウィンドウの [デバイスのデフォルト（Device Default）] 値と一致する必要があります。

パーク モニタリング

パーク モニタリングがサポート対象のは、Cisco IP 電話でコールをパークする場合のみです。パーク モニタリングによって、パークされたコールのステータスがモニタされます。 パーク中のコールが取得されるか、またはパークされたコールによって破棄されるまで、パーク モニタリング コール バブルはクリアされません。 このパークされたコールは、コールをパークした電話機で同じコール バブルを使用して取得できます。

パーク モニタリング タイマーのセットアップ

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] には、パーク モニタリング用として、パーク モニタリング復帰タイマー、パーク モニタリング定期復帰タイマー、未取得時のパーク モニタリング転送タイマーという 3 種類のクラスタ全体に対応するサービス タイマー パラメータがあります。 各サービス パラメータにはデフォルトが含まれており、特別な設定は必要ありません。 これらのタイマー パラメータはパーク モニタリング専用です。コール パーク表示タイマーとコール パーク復帰タイマーはパーク モニタリングには使用できません。 これらのパラメータの詳細については、次の表を参照してください。

[Cisco Unified CM サービスパラメータ（Cisco Unified Communications Manager Service Parameters）] ページでタイマーを設定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [クラスタ全体のパラメータ（機能：一般）（Clusterwide Parameters (Feature-General)）] ペインにある、[パークモニタリング復帰タイマー（Park Monitoring Reversion Timer）]、[パーク モニタリング定期復帰タイマー（Park Monitoring Periodic Reversion Timer）]、[未取得時のパーク モニタリング転送タイマー（Park Monitoring Forward No Retrieve Timer）] フィールドを更新します。

表 *35*：パーク モニタリングのサービス パラメータ

フィールド	説明
[パークモニタリング復帰タイマー(Park Monitoring Reversion Timer)]	デフォルト値は 60 秒です。 このパラメータは、ユーザがパークしたコールを取 ユーザに求めるまで、Cisco Unified Communications Manager が待機する秒数を決 のタイマーが開始するのは、ユーザが電話機の Park を押したときです。タイマ なるとアラームが鳴ります。 このサービス パラメータに指定された値は [電話番号の設定（Directory Number C ウィンドウの [パーク モニタリング（Park Monitoring）] セクションで回線ごと す（このウィンドウを表示するには、Cisco Unified Communications Manager の管 **[コール ルーティング（Call Routing）] > [電話番号（Directory Number）]** を選 値 0 を指定すると、Park Monitoring Periodic Reversion Timer サービス パラメータ 期復帰期間がただちに使用されます。（次の説明を参照してください）。たと メータを 0 に設定し、パーク モニタリング定期復帰タイマーを 15 に設定した場 たコールについてユーザにすぐに通知され、その後も未取得時のパーク モニタ マー（下記を参照）が時間切れになるまで 15 秒おきに通知されます。
パーク モニタリング定期復帰タイマー（Park Monitoring Periodic Reversion Timer）	デフォルトは 30 秒です。 このパラメータは、Cisco Unified Communications Mana がパークされていることをユーザに再通知するまでに待機する間隔（秒）を決定 ザはこのような通知の際にオフフックにするだけで、パークされたコールに接続 コールがパークされており、未取得時のパーク モニタリング転送タイマー（以 照）に指定した時間が経過するまでは、Cisco Unified Communications Manager に いるコールについてユーザに通知し続けます。 値として 0 を指定すると、パー に関する定期的な通知は無効になります。
未取得時のパーク モニタリング転送タイマー（Park Monitoring Forward No Retrieve Timer）	デフォルト値は 300 秒です。 このパラメータによって、パーク アラート通知が 決定されます。アラート通知後に、パークされたコールが、パーク元の [電話番号 Number Configuration)] ウィンドウで指定したパーク モニタリング転送未取得時 されます（Cisco Unified Communications Manager の管理で転送先が指定されてい ルは、パークされたときの回線に返されます）。 [パークモニタリング復帰タイ Monitoring Reversion Timer）] のサービス パラメータが時間切れになると、この 始します。 [未取得時のパーク モニタリング転送タイマー（Park Monitoring Forw Timer）] が時間切れになると、コールはパークから削除され、指定された接続先 か、パークしたユーザの回線に返されます。

電話番号のパーク モニタリング パラメータ設定

[電話番号の設定（Directory Number Configuration）] ウィンドウには、3 種類のパラメータを設定できる [パークモニタリング（Park Monitoring）] 領域が含まれます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、**[コールルーティング（Call Routing）] > [電話番号（Directory Number）]** を選択します。

ステップ 2 次の表に示すように、パーク モニタリングのフィールドを設定します。

表 *36* : パーク モニタリング パラメータ

フィールド	説明
[パークモニタリング転送非取得時の接続先(外部)(Park Monitoring Forward No Retrieve Destination External)]	パークされている側が外部の場合、パークしたユーザの [未取得時のパーク モニタリング転送の接続先（外部）（Park Monitoring Forward No Retrieve Destination External）] パラメータに指定された接続先にコールが転送されます。 [未取得時のパーク モニタリング転送の接続先（外部）（Park Monitoring Forward No Retrieve Destination External）] フィールドの値が空の場合、パークされた側のコールはパークしたユーザの回線にリダイレクトされます。
[パークモニタリング転送非取得時の接続先(内部)(Park Monitoring Forward No Retrieve Destination Internal)]	パークされている側が内部の場合、パークしたユーザの [未取得時のパーク モニタリング転送の接続先（内部）（Park Monitoring Forward No Retrieve Destination External）] パラメータに指定された接続先にコールが転送されます。 [未取得時のパーク モニタリング転送の接続先（内部）（Park Monitoring Forward No Retrieve Destination Internal）] が空の場合、パークされた側のコールはパークしたユーザの回線にリダイレクトされます。
[パークモニタリング復帰タイマー(Park Monitoring Reversion Timer)]	このパラメータは、ユーザがパークしたコールを取得するようにユーザに求めるまで、Cisco Unified Communications Manager が待機する秒数を決定します。 このタイマーが開始するのは、ユーザが電話機の Park を押したときです。タイマーが時間切れになるとアラームが鳴ります。 デフォルト：60 秒 0 以外の値を設定すると、その値により、[サービスパラメータ(Service Parameters)] ウィンドウで設定されたこのパラメータの値が上書きされます。 ただし、ここで値 0 を設定すると、[サービスパラメータ(Service Parameters)] ウィンドウの値が使用されます。

ハント リストのパーク モニタリングのセットアップ

ハントリストを介してルーティングされたコールがパークされているとき、未取得時のパークモニタリング転送タイマーが時間切れになると、ハントパイロットの [未取得時のパーク モニタリング転送の接続先（Park Monitoring Forward No Retrieve Destination）] パラメータの値が使用されます（空白でない場合）。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ハントパイロット（Hunt Pilot）]** と選択します。

ステップ 2 [未取得時のパーク モニタリング転送の接続先（Park Monitoring Forward No Retrieve Destination）] パラメータを設定します。

ハント パイロットの [未取得時のパーク モニタリング転送の接続先（Park Monitoring Forward No Retrieve Destination）] パラメータの値が空白の場合、未取得時のパーク モニタリング転送タイマーが時間切れになると、コールは [電話番号の設定（Directory Number Configuration）] ウィンドウで設定された接続先に転送されます。

音声ポートとビデオ ポートの範囲設定

Quality of Service（QoS）向上のため、音声トラフィックとビデオ トラフィックを異なる RTP ポート範囲に送信することができます。

ポート範囲を制御するには、[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] の次のフィールドを使用します。

- オーディオ ポート（Audio ports）
  - 開始メディアポート（Start Media Port）（デフォルト：16384）
  - 終了メディアポート（Stop Media Port）（デフォルト：32766）
- ビデオ ポート
  - [ビデオの開始（Start Video）]（ビデオの開始ポート設定用）
    - 最小値：2048
    - 最大値：65535
  - [ビデオの停止（Stop Video）]（ビデオの終了ポート設定用）
    - 最小値：2048
    - 最大値：65535

ビデオ ポートのフィールドの設定では、次のルールが適用されます。

[開始ビデオ RTP ポート（Start Video RTP Port）] と [終了ビデオ RTP ポート（Stop Video RTP Port）] が設定されると、電話機はビデオ トラフィックにビデオ ポート範囲内のポートを使用します。 音声トラフィックはメディア ポートを使用します。

音声ポートとビデオ ポートの範囲が重複すると、重複したポートは、音声トラフィックとビデオ トラフィックの両方を伝送します。 ビデオ ポート範囲が正しく設定されていない場合、電話機は、設定されている音声ポートを音声トラフィックとビデオ トラフィックの両方に使用します。

詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

ステップ 1 Cisco Unified Communications Manager Administration の管理で、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）]** を選択します。

ステップ 2 音声ポート範囲の [開始メディアポート（Start Media Port）] および [終了メディアポート（Stop Media Port）] フィールドを設定します。

ステップ 3 **保存**を選択します。

ステップ 4 次のウィンドウのいずれかを選択します。

- **[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]**
- **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]**
- **[デバイス（Device）] > [電話（Phone）] > [電話の設定（Phone Configuration）]**

ステップ 5 [開始ビデオ RTP ポート（Start Video RTP Port）] と [終了ビデオ RTP ポート（Stop Video RTP Port）] を必要なポート範囲に設定します。

ビデオ ポートのフィールドの設定では、次のルールが適用されます。

- [終了ビデオ RTP ポート（Stop Video RTP Port）] フィールドの値は [開始ビデオ RTP ポート（Start Video RTP Port）] フィールドの値より大きくする必要があります。
- [開始ビデオ RTP ポート（Start Video RTP Port）] フィールドと [終了ビデオ RTP ポート（Stop Video RTP Port）] フィールドの差は 16 以上である必要があります。

ステップ 6 **保存**を選択します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

Cisco IP Manager Assistant のセットアップ

Cisco IP Manager Assistant（IPMA）は、コール ルーティングやその他電話管理機能を提供し、マネージャおよびアシスタントがより効果的に電話の対応をできるよう支援します。

Cisco Unified Communications Manager にユーザがアクセスする前に、IPMA サービスが設定されている必要があります。 IPMA の設定については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

IPMA には、3 種類の主要コンポーネントがあります。

マネージャ（Manager）

マネージャは、コール ルーティング サービスによってコールを代行受信させることができます。

アシスタント

アシスタントはマネージャに代わってコールを処理します。

Assistant Console[AssistantConsole]

アシスタント コンソールとは、アシスタントがタスクを実行したり、ほとんどの機能の管理を実行したりするために使用できるデスクトップ アプリケーションです。

プロキシ回線サポートと共有回線サポートの2つのオペレーション モードをサポートしています。 どちらのモードも、マネージャ用の回線ごとに複数のコールをサポートしています。 IPMA サービスは、クラスタ内でプロキシ回線サポートと共有回線サポートの両方をサポートしています。

共有回線モードでは、マネージャとアシスタントが電話番号を共有し、コールは共有回線で対応されます。 共有回線でコールが受信されると、マネージャの電話機およびアシスタントの電話機の両方が鳴ります。 共有回線モードは、デフォルトのアシスタント選択、Assistant Watch、コール フィルタリング、および DivertAll はサポートされません。

Cisco IPMA を共有回線モードに設定すると、マネージャとアシスタントが電話番号（1701 など）を共有できるため、アシスタントは共有する電話番号でマネージャの通話を処理することができます。 マネージャが電話番号 1701 でコールを受信した場合、マネージャの電話機およびアシスタントの電話機の両方が鳴ります。

共用回線モードでは、デフォルトのアシスタント選択、Assistant Watch、コール フィルタリング、および DivertAll を含め、すべての IPMA 機能が使用できるわけではありません。 アシスタントは、アシスタント コンソール アプリケーションでこれらの機能を確認したり、アクセスしたりできません。 アシスタントの電話機には、[全て転送（Divert All）]機能のソフトキーがついていません。 マネージャの電話機には、[アシスタント モニタ（Assistant Watch）]、[コール代行受信（Call Intercept）]、または [全て転送（Divert All）] 機能のソフトキーがついていません。

ユーザ デバイスの共有回線のサポートにアクセスするためには、Cisco Unified Communications Manager Administration を使用して、Cisco IP Manager Assistant サービスを設定し、開始する必要があります。

プロキシ回線モードでは、アシスタントがプロキシ番号を使用してマネージャに代わってコールの対応をします。 プロキシ回線モードにより、すべての IPMA 機能がサポートされます。

プロキシ回線モードで Cisco IPMA を設定する場合、マネージャとアシスタントは電話番号を共有しません。 アシスタントは、マネージャ宛のコールをプロキシ番号を使用して処理します。 プロキシ番号は、マネージャの電話番号ではありません。 これは、システムによって選

択された代替番号であり、アシスタントがマネージャのコールを処理するために使用されます。 プロキシ回線モードでは、マネージャとアシスタントにIPMA で使用できるすべての機能へのアクセスが与えられます。これには、デフォルトでのアシスタント選択、Assistant Watch、コール フィルタリング、および DivertAll が含まれます。

ユーザ デバイスのプロキシ回線のサポートにアクセスするためには、Cisco Unified Communications Manager Administration を使用して、Cisco IP Manager Assistant サービスを設定し、開始する必要があります。

IPMA の機能には、ソフトキーを使用し、電話サービスによってアクセスします。 ソフトキー テンプレートは、Cisco Unified Communications Manager で設定されます。 IPMA は次の標準ソフトキー テンプレートをサポートします。

Standard Manager

プロキシ モードのマネージャをサポートします。

Standard Shared Mode Manager

共有モードのマネージャをサポートします。

Standard Assistant

プロキシまたは共有モードでアシスタントをサポートします。

次の表に、ソフトキー テンプレートで使用できるソフトキーについて説明します。

表 *37 : IPMA* ソフトキー

ソフトキー	コール状態	説明
リダイレクト	呼び出し中、接続中、保留中	事前設定されたターゲットに選択したコールを転送します。
代行受信（Intercept）	すべての状態	コールをアシスタントの電話機からマネージャの電話機に転送し、自動応答します。
モニタ（Set Watch）	すべての状態	アシスタントが処理しているコールの状態を確認します。
VM 転送（TransVM）	呼び出し中、接続中、保留中	選択されたコールをマネージャのボイス メールにリダイレクトします。
全て転送（Divert All）	すべての状態	マネージャにルーティングされたすべてのコールを事前設定されたターゲットに転送します。

（注） [代行受信（Intercept）]、[モニタ（Set Watch）]、[全て転送（Divert All）] は、プロキシ回線モードでマネージャの電話機にのみ設定するようにします。

次の手順は、必要な手順の概要です。

手順

ステップ 1 電話機とユーザを設定します。
ステップ 2 電話機をユーザに関連付けます。
ステップ 3 [サービス アクティベーション（Service Activation）] ウィンドウで Cisco IP Manager Assistant サービスを有効にします。
ステップ 4 システム管理パラメータを設定します。
ステップ 5 必要に応じて、IPMA クラスタ全体のサービス パラメータを設定します。
ステップ 6 （任意） ユーザ CAPF プロファイルを設定します。
ステップ 7 （任意） セキュリティの IPMA サービス パラメータを設定します。
ステップ 8 IPMA サービスを停止し、再起動します。
ステップ 9 ソフトキー テンプレートを含む、電話パラメータ、マネージャ、補助設定を設定します。
ステップ 10 Cisco Unified Communications Manager Assistant アプリケーションを設定します。
ステップ 11 ダイヤル ルールを設定します。
ステップ 12 アシスタント コントロール アプリケーションをインストールします。
ステップ 13 マネージャ アプリケーションとアシスタント コンソール アプリケーションを設定します。

ビジュアル ボイスメールのセットアップ

ビジュアル ボイスメールは、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] から、すべての Cisco IP 電話 または個別ユーザまたはユーザ グループに設定されます。

（注） 設定情報については、http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html で Cisco ビジュアル ボイスメールのマニュアルを参照してください。

ビジュアル ボイスメール クライアントは、Cisco IP 電話 8800 電話機の MIDlet としてはサポートされません。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[Phone サービス（Phone Services）]** を選択します。

ステップ 2 [新規追加（Add New）] を選択し、ビジュアル ボイスメールの新しいサービスを作成します。

ステップ 3 [IP 電話サービスの設定（IP Phone Services Configuration）] ウィンドウで、各フィールドに次の情報を入力します。

- サービス名（Service Name）：**`VisualVoiceMail`** を入力します。
- ASCII サービス名（ASCII Service Name）：**`VisualVoiceMail`** を入力します。
- サービス URL（Service URL）：**`Application:Cisco/VisualVoiceMail`** として入力します。
- サービス カテゴリ（Service Category）：プルダウン メニューから [XMLサービス（XML Service）] を選択します。
- サービス タイプ（Service Type）：プルダウン メニューから [メッセージ（Messages）] を選択します。

ステップ 4 [有効（Enable）] をチェックし、[保存（Save）] をクリックします。

（注） [エンタープライズ登録（Enterprise Subscription）] はチェックしないでください。

ステップ 5 [サービス パラメータ情報（Service Parameter Information）] ウィンドウで、[新規パラメータ（New Parameter）] をクリックし、各フィールドに次の情報を入力します。

- [パラメータ名（Parameter Name）]。voicemail_server を入力します。
- [パラメータ表示名（Parameter Display Name）]。voicemail_server を入力します。
- [デフォルト値（Default Value）]。プライマリ Unity サーバのホスト名を入力します。
- [パラメータの説明（Parameter Description）]

ステップ 6 [パラメータは必須（Parameter is Required）] をオンにして、[保存（Save）] をクリックします。

（注） [パラメータはパスワード（コンテンツをマスクする）（Parameter is a Password (mask contents)）] はチェックしないでください。

ステップ 7 ウィンドウを閉じ、[Phone サービスの設定（Phone Services Configuration）] ウィンドウで [保存（Save）] をもう一度選択します。

特定ユーザのビジュアル ボイスメールのセット アップ

特定のユーザにビジュアル ボイスメールを設定する場合は、次の手順を使用します。

（注） 設定情報については、http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.html で Cisco ビジュアル ボイスメールのマニュアルを参照してください。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、**[デバイス（Device）]**>**[電話（Phone）]** を選択します。

ステップ 2 目的のユーザに関連付けられているデバイスを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウンで、[サービスの登録/登録解除（Subscribe/Unsubscribe Services）] を選択し、[移動（Go）] をクリックします。

ステップ 4 作成した VisualVoiceMail サービスを選択し、**[次へ（Next）]**>**[登録（Subscribe）]** を選択します。

ユーザ グループのビジュアル ボイスメールのセットアップ

複数の Cisco IP 電話 を一括で Cisco Unified Communications Manager にビジュアル ボイスメールが登録された状態で追加するには、各電話機テンプレートで、電話機タイプに応じた BAT ツールで電話機テンプレートを作成します。Visual Voicemail サービス、登録、電話を挿入するテンプレートを使用します。

すでに Cisco IP 電話 を登録してある状態から、ビジュアル ボイスメール サービスへの登録を実行する場合は、BAT で電話機テンプレートを作成し、テンプレート内でビジュアル ボイスメール サービスに登録し、それから BAT ツールを使用して電話機を更新します。

詳細については、http://www.cisco.com/c/en/us/support/unified-communications/visual-voicemail/model.htmlを参照してください。

Assured Services SIP

Assured Services SIP（AS-SIP）は、Cisco IP 電話 およびサードパーティ製の電話機に非常に安全なコールフローを提供する機能とプロトコルの集まりです。 次の機能はまとめて AS-SIP と呼ばれます。

- Multilevel Precedence and Preemption（MLPP）
- DiffServ コード ポイント（DSCP）
- トランスポート層セキュリティ（TLS）および Secure Real-Time Transport Protocol（SRTP）
- インターネット プロトコル バージョン 6（IPv6）

AS-SIP は、緊急時の通話に優先順位を付けるために、マルチレベル優先順位およびプリエンプション（MLPP）と共に使用されることがよくあります。 MLPP を使用すると、レベル 1（低）からレベル 5（高）まで、発信通話に優先レベルを割り当てることができます。 ユーザがコールを受信すると、電話機の発信者名の横に優先レベル アイコンが表示されます。

AS-SIP の設定を行うには、Cisco Unified Communications Manager で次のタスクを実行します。

- ダイジェストユーザを設定する：SIP 要求にダイジェスト認証を使用するようにエンドユーザを設定します。

- SIP 電話のセキュア ポートの設定 — Cisco Unified Communications Manager は、SIP 電話からの SIP 回線登録をリッスンするためにこの TLS ポートを使用します。
- サービスの再起動：セキュアポートを設定した後、Cisco Unified Communications Manager および Cisco CTL Provider サービスを再起動します。 この手順で、AS-SIP エンドポイントおよび SIP トランクの SIP 設定を使用して SIP プロファイルを設定します。 電話機固有のパラメータはサードパーティ製 AS-SIP 電話機にダウンロードされません。 これらは Cisco Unified Manager によってのみ使用されます。 サードパーティ製電話機では同じ設定値をローカルに設定する必要があります。
- AS-SIP 用の電話セキュリティプロファイルの設定：電話セキュリティプロファイルを使用して、TLS、SRTP、ダイジェスト認証などのセキュリティ設定を割り当てることができます。
- AS-SIP エンドポイントの設定：AS-SIP サポートを使用して、Cisco IP 電話 またはサードパーティのエンドポイントを設定します。
- デバイスを最終用途に関連付ける - エンドポイントをユーザに関連付けます。
- AS-SIP の SIP トランクセキュリティプロファイルの設定：SIP トランクセキュリティプロファイルを使用して、TLS やダイジェスト認証などのセキュリティ機能を SIP トランクに割り当てることができます。
- AS-SIP 用の SIP トランクの設定 - AS-SIP サポートを使用して SIP トランクを設定します。
- AS-SIP 機能の設定：MLPP、TLS、V.150、IPv6 などの追加の AS-SIP 機能を設定します。

AS-SIPの設定の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure AS-SIP Endpoints」の章を参照してください。

マルチプラットフォーム フォンへの電話機の直接移行

移行ファームウェアロードを使用せずに、1 つの手順で企業の電話機をマルチプラットフォームフォンに簡単に移行することができます。必要なのは、サーバーから移行ライセンスを取得して承認することだけです。

詳細については、「https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/MPP/MPP-conversion/enterprise-to-mpp/cuip_b_conversion-guide-ipphone.html」を参照してください。

Multilevel Precedence and Preemption

Multilevel Precedence and Preemption（MLPP）を使用すると、緊急事態やその他の危機的状況での通話に優先順位を付けることができます。 発信通話には 1 から 5 の優先順位を指定します。着信通話には通話の優先順位を示すアイコンが表示されます。 認証されたユーザは、対象のステーション向けに、または完全にサブクライブされた TDM トランクを介してコールをプリエンプション処理できます。

この機能によって、階級の高い人物が重要な組織および担当者に確実に連絡を取ることができるようになります。

MLPP は多くの場合、Assured Services SIP（AS-SIP）で使用されます。 MLPPの設定の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure Multilevel Precedence and Preemption」の章を参照してください。

ソフトキー テンプレートの設定

Cisco Unified Communications Manager の管理ページを使用して、最大 18 のソフトキーを電話機でサポートされているアプリケーションに関連付けることができます。 Cisco Unified Communications Manager では、Standard User および Standard Feature というソフトキー テンプレートがサポートされています。

ソフトキーをサポートするアプリケーションには、関連付けられた標準ソフトキーテンプレートが 1 つ以上あります。 標準ソフトキー テンプレートを変更するには、コピーしてリネームしてから、新しいテンプレートを更新します。 非標準のソフトキー テンプレートも修正できます。

[ソフトキーの制御（Softkey Control）] パラメータは、電話機のソフトキーがソフトキー テンプレート機能によって制御されるかどうかを示します。 [ソフトキーの制御（Softkey Control）] パラメータは必須入力フィールドです。

この機能の設定の詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco IP 電話は、Cisco Unified Communications Manager の管理の [ソフトキーテンプレートの設定（Softkey Template Configuration）] で設定可能なすべてのソフトキーをサポートしているわけではありません。 Cisco Unified Communications Manager では、管理ポリシー設定によって一部のソフトキーを有効/無効にできます。 次の表に、機能およびソフトキー テンプレートで設定可能なソフトキー、および Cisco IP 電話でのサポートの有無を示します。

（注） Cisco Unified Communications Manager では、ソフトキー テンプレートに任意のソフトキーを設定できますが、サポートされていないソフトキーは、電話機に表示されません。

表 *38* : 設定可能なソフトキー

機能	ソフトキーテンプレートの設定で設定可能なソフトキー	ソフトキーとしてサポー
応答	応答（Answer）	サポートされる
コールバック	折り返し（CallBack）	サポートされる
すべてのコールの転送	不在転送（cfwdAll）	サポートされる
コール パーク	パーク（Park）	サポートされる

機能	ソフトキーテンプレートの設定で設定可能なソフトキー	ソフトキーとしてサポート
コール ピックアップ	ピック（Pickup）	サポートされる
割込み	割込み	サポートされる
C 割り込み	会議への割り込み（Conference Barge）	サポートされる
会議	会議（Confrn）	サポートされる
会議リスト	参加者（ConfList）	サポートされる
即転送	即転送（iDivert）	サポートされる
取り込み中	サイレント（DND）	サポートされる
終了	終了（EndCall）	サポートされる
グループ ピックアップ	グループ ピック（GPickUp）	サポートされる
保留 (Hold)	保留（Hold）	サポートされる
ハント グループ	ハント（HLog）	サポートされる
参加（Join）	参加（Join）	サポート対象外
迷惑呼 ID	迷惑呼 ID（MCID）	サポートされる
ミートミー	ミートミー（MeetMe）	サポートされる
モバイル コネクト	モビリティ（Mobility）	サポートされる
発信	発信（NewCall）	サポートされる
その他のピックアップ	その他のピックアップ（oPickup）	サポートされる
キュー統計情報の PLK サポート	Queue Status	サポート対象外
品質レポート ツール	Quality Reporting Tool（QRT; 品質レポートツール）	サポートされる
Redial	リダイヤル（Redial）	サポートされる
会議の最後の参加者の削除	会議の最後の参加者の削除（Remove）	サポート対象外

機能	ソフトキーテンプレートの設定で設定可能なソフトキー	ソフトキーとしてサポー
復帰	復帰（Resume）	サポートされる
選択	選択（Select）	サポート対象外
スピード ダイヤル	短縮（AbbrDial）	サポートされる
転送	転送（Trfr）	サポートされる
ビデオ モード コマンド	ビデオ（VidMode）	サポート対象外

手順

ステップ 1 Cisco Unified Communications Manager の管理で、次のいずれかのウィンドウを選択してください。

- ソフトキーテンプレートを設定するには、**[デバイス（Device）]**>**[デバイスの設定（Device Settings）]** > **[ソフトキーテンプレート（Softkey Template）]** を選択します。
- ソフトキー テンプレートを電話機に割り当てるには、**[デバイス（Device）]** > **[電話（Phone）]** を選択し、[ソフトキー テンプレート（Softkey Template）] フィールドを設定します。

ステップ 2 変更を保存します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

電話ボタン テンプレート

電話ボタン テンプレートを使用すると、スピード ダイヤルやコール処理機能をプログラム可能なボタンに割り当てることができます。ボタンに割り当てられるコール処理機能には、応答（Answer）、モビリティ（Mobility）、すべてのコール（All Calls）が含まれます。

テンプレートの変更は、可能な限り電話機をネットワークに登録する前に行ってください。この順序に従うと、登録の実行中、カスタマイズした電話ボタン テンプレート オプションに Cisco Unified Communications Manager からアクセスできます。

電話ボタン テンプレートの変更

IP 電話サービスおよび回線ボタンの設定の詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[電話ボタン テンプレート（Phone Button Template）]** を選択します。

ステップ 2 **[検索(Find)]** をクリックします。

ステップ 3 電話機のモデルを示します。

ステップ 4 [コピー（Copy）]を選択し、新しいテンプレートの名前を入力して、[保存（Save）]を選択します。

[電話ボタン テンプレートの設定（Phone Button Template Configuration）] ウィンドウが表示されます。

ステップ 5 割り当てるボタンを確認して、機能が表示されるドロップダウン リストから、その回線に関連付ける [サービス URL（Service URL）]を選択します。

ステップ 6 [保存（Save）]を選択して、サービス URL を使用して新しい電話ボタン テンプレートを作成します。

ステップ 7 **[デバイス（Device）]** > **[電話（Phone）]** を選択して、電話機の [電話の設定（Phone Configuration）] ウィンドウを開きます。

ステップ 8 [電話ボタン テンプレート（Phone Button Template）] ドロップダウン リストから、新しい電話ボタン テンプレートを選択します。

ステップ 9 [保存（Save）]を選択して変更内容を保存してから、[設定の適用（Apply Config）]を選択して変更を実装します。

これで電話機のユーザが、セルフケアポータルにアクセスして、電話機のボタンにサービスを関連付けることができます。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

すべてのコールの電話ボタン テンプレートの割り当て

複数のシェアドラインを持つユーザに、電話テンプレートの [すべてのコール（All Calls）] ボタンを割り当てます。

電話機に [すべてのコール（All Calls）] ボタンを設定すると、ユーザはそのボタンを使用して次の操作を実行できます。

- 電話機の全回線から、現在のコールの全リストを表示します。
- （[通話履歴（Call History）] の下に）電話機の全回線から、すべての不在着信の一覧を表示します。
- ユーザがオフフックにすると、ユーザのプライマリ回線でコールを発信できます。すべてのコール（All Calls）のデフォルトは、すべての発信コールに関してユーザのプライマリ回線になります。

手順

ステップ 1 [すべてのコール（All Calls）] ボタンを含むように電話ボタン テンプレートを変更します。

ステップ 2 電話機にテンプレートを割り当てます。

IP 電話サービスとしての PAB またはスピード ダイヤルのセットアップ

電話ボタン テンプレートを変更して、サービス URL をプログラム可能なボタンに関連付けることができます。 これを行うと、ユーザは、1 つのボタンで、PAB とスピード ダイヤルにアクセスできます。 電話ボタン テンプレートを変更する前に、PAB やスピード ダイヤルを IP 電話サービスとして設定する必要があります。 詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。

（まだサービスでない）PAB やスピード ダイヤルを IP 電話サービスとして設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [Phone サービス（Phone Services）]** を選択します。

[IP 電話サービスの検索と一覧表示（Find and List IP Phone Services）] ウィンドウが表示されます。

ステップ 2 [新規追加] をクリックします。

[IP 電話サービスの設定（IP Phone Services Configuration）] ウィンドウが表示されます。

ステップ 3 次の設定値を入力します。

- [サービス名（Service Name）] : [個人アドレス帳（Personal Address Book）]を入力します。
- [サービスの説明（Service Description）] :（オプション）サービスの説明を入力します。
- サービス URL（Service URL）

  PAB の場合は、次の URL を入力します。

  http://<Unified CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=pab**

  ファスト ダイヤルの場合は、次の URL を入力します。

  http://<Unified-CM-server-name>**:8080/ccmpd/login.do?name=#DEVICENAME#&service=fd**
- [セキュア サービス URL（Secure Service URL）]

  PAB の場合は、次の URL を入力します。

https://<Unified CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=pab**

ファスト ダイヤルの場合は、次の URL を入力します。

https://<Unified-CM-server-name>**:8443/ccmpd/login.do?name=#DEVICENAME#&service=fd**

- [サービス カテゴリ（Service Category）]：[XML サービス（XML Service）]を選択します。
- [サービス タイプ（Service Type）]：[ディレクトリ（Directories）]を選択します。
- [有効（Enable）]：チェックボックスを選択します。

http://<IP_address> or *https://<IP_address>*（Cisco IP 電話がサポートするプロトコルによって異なります）

ステップ 4 **保存**を選択します。

（注） サービス URL を変更した場合、IP 電話サービス パラメータを削除した場合、またはユーザの登録先の IP Phone サービス名を変更した場合は、[登録の更新（Update Subscriptions）]をクリックして、現在のすべての登録ユーザを更新し、変更を適用する必要があります。このボタンをクリックしなかった場合は、ユーザがそのサービスに登録して、正しい URL を再作成する必要があります。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

PAB またはファスト ダイヤル用の電話ボタン テンプレートの変更

電話ボタン テンプレートを変更して、サービス URL をプログラム可能なボタンに関連付けることができます。 これを行うと、ユーザは、1 つのボタンで、PAB とスピード ダイヤルにアクセスできます。 電話ボタン テンプレートを変更する前に、PAB やスピード ダイヤルを IP 電話サービスとして設定する必要があります。

IP 電話サービスおよび回線ボタンの設定の詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[電話ボタン テンプレート（Phone Button Template）]** を選択します。

ステップ 2 **[検索(Find)]** をクリックします。

ステップ 3 電話機のモデルを示します。

ステップ 4 [コピー（Copy）]を選択し、新しいテンプレートの名前を入力して、[保存（Save）]を選択します。

[電話ボタン テンプレートの設定（Phone Button Template Configuration）] ウィンドウが表示されます。

ステップ 5 割り当てるボタンを確認して、機能が表示されるドロップダウン リストから、その回線に関連付ける [サービス URL（Service URL）]を選択します。

ステップ 6 [保存（Save）]を選択して、サービス URL を使用して新しい電話ボタン テンプレートを作成します。

ステップ 7 **[デバイス（Device）]** > **[電話（Phone）]** を選択して、電話機の [電話の設定（Phone Configuration）] ウィンドウを開きます。

ステップ 8 [電話ボタン テンプレート（Phone Button Template）] ドロップダウン リストから、新しい電話ボタン テンプレートを選択します。

ステップ 9 [保存（Save）]を選択して変更内容を保存してから、[設定の適用（Apply Config）]を選択して変更を実装します。

これで電話機のユーザが、セルフケアポータルにアクセスして、電話機のボタンにサービスを関連付けることができます。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

VPN の設定

Cisco VPN 機能は、ユーザが企業ネットワークに安全かつ信頼性の高い方法で接続できるようにしながら、ネットワーク セキュリティを維持できます。この機能は、次のような場合に使用します。

- 電話機が信頼ネットワークの外側にある
- 電話機と Cisco Unified Communications Manager 間のネットワーク トラフィックが信頼できないネットワークと交差する

VPN を使用する場合、一般的なクライアント認証の方法には、次の 3 つがあります。

- デジタル証明書
- パスワード
- ユーザ名とパスワード

各方法にはそれぞれの利点があります。しかし、企業のセキュリティ ポリシーで許可されているのであれば、証明書ベースの方法をお勧めします。証明書を使用すれば、ユーザの介入なしのシームレスなサインインが可能になります。LSC 証明書と MIC 証明書の両方がサポートされます。

VPN機能を設定するには、まずオンプレミスのプロビジョニングを行い、その後、オフプレミスにデバイスを導入できます。

証明書認証および VPN ネットワークでの作業の詳細については、Technical Note『*AnyConnect VPN Phone with Certificate Authentication on an ASA Configuration Example*』を参照してください。このマニュアルの URL は

http://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html です。

パスワード、またはユーザ名とパスワードによる方法では、サインイン資格情報の入力がユーザに求められます。会社のセキュリティ ポリシーに従ってユーザのサインイン クレデンシャルを設定します。ユーザ パスワードが電話機で保存されるよう [永続的パスワードを有効化（Enable Password Persistence）] を設定することもできます。ログイン試行に失敗するか、ユーザが手動でパスワードをクリアするか、電話がリセットされるか、または電源が切れるまで、ユーザのパスワードは保存されます。

[自動ネットワーク検出を有効化（Enable Auto Network Detection）] 設定も便利なツールです。このチェックボックスが有効になっていると、VPN クライアントは、企業ネットワークの外にいることを検出した場合に限り動作します。デフォルトでは、この機能はディセーブルになっています。

ご使用の Cisco 電話機は、クライアントタイプとして Cisco SVC IPPhone クライアント v1.0 をサポートしています。

VPN を使用した仮想プライベート ネットワークの維持、設定、および操作の詳細については、『*Security Guide for Cisco Unified Communications Manager*』の『Virtual Private Network Setup』の章を参照してください。このマニュアルの URL は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html です。

Cisco VPN 機能はセキュア ソケット レイヤ (SSL) を使用してネットワーク セキュリティを保持します。

（注） 組み込みクライアントを使用して SSL VPN から ASA へのオフプレミスの電話機を設定するときは、代替の TFTP サーバ設定を入力します。

追加回線キーのセットアップ

拡張回線モードを有効にすると、電話画面の両側にあるボタンを回線キーとして使用できるようになります。 デフォルトで、プレディクティブ ダイヤリングおよび適用可能な着信コールは、拡張回線モードで有効になります。

始める前に

カスタマイズした電話ボタン テンプレートを新たに作成する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 設定する電話機を特定します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration）] 領域に移動して、[回線モード（Line Mode）] フィールドを [拡張回線モード（Enhanced Line Mode）] に設定します。

ステップ 4 [デバイス情報（Device Information）] 領域に移動し、[電話ボタン テンプレート（Phone Button Template）] フィールドをカスタマイズしたテンプレートに設定します。

ステップ 5 [設定の適用（Apply Config）]を選択します。

ステップ 6 **保存**を選択します。

ステップ 7 電話機を再起動します。

関連トピック

セッション回線モードの環境 （187 ページ）

拡張回線モードで使用可能な機能

Enhanced Line Mode（ELM）Expressway 経由でのモバイルおよび Remote Accessと併用できます。

ELM は、ロールオーバー回線、つまり最初の共有回線が使用中の場合にコールが別の共有回線に転送されるコールルーティング設定でも使用できます。 ELM がロールオーバー回線で使用されている場合、最近の共有回線へのコールは単一の電話番号にまとめられます。 ロールオーバー回線の詳細については、Cisco Unified Communications Manager release 12.0(1) 以降の『*Feature Configuration Guide for Cisco Unified Communications Manager*』の「Custom Phone Rings and Backgrounds」の章を参照してください。

ELM はほとんどの機能をサポートしますが、すべての機能をサポートするわけではありません。 機能を有効にできたとしても、サポート対象とは限りません。 機能がサポートされていることを確認するには、次の表を参照してください。

表 *39* : 機能のサポートと拡張回線モード

機能	サポートされる	ファームウェア リリース
応答	可	11.5(1) 以降
コールへの自動応答	可	11.5(1) 以降
割り込み/C 割り込み	可	11.5(1) 以降
BLF でのダイレクト コール パーク	可	12.0(1) 以降
Bluetooth スマートフォン統合	不可	-
Bluetooth USB ヘッドセット	可	11.5(1) 以降
コールバック	可	11.5(1) 以降

機能	サポートされる	ファームウェア リリース
コール監視人	不可	-
すべてのコールの転送	可	11.5(1) 以降
コール パーク	可	12.0(1) 以降
コール パーク回線ステータス	可	12.0(1) 以降
コール ピックアップ	可	11.5(1) 以降
コール ピックアップ回線ステータス	可	11.5(1) 以降
複数回線でのすべてのコールの転送	可	11.5(1) 以降
クラスタ間の Cisco エクステンション モビリティ	可	この機能は、12.0(1) 以降でサポートされています。
Cisco IP Manager Assistant（IPMA）	不可	-
Cisco Unified Communications Manager Express	不可	-
会議	可	11.5(1) 以降
コンピュータ テレフォニー インテグレーション（CTI）アプリケーション	可	11.5(1) 以降
却下	可	11.5(1) 以降
デバイスから呼び出された録音	可	11.5(1)SR1 以降
取り込み中	可	11.5(1) 以降
拡張 SRST	不可	-
エクステンションモビリティ	可	11.5(1) 以降
グループ ピックアップ	可	この機能は、12.0(1) 以降でサポートされています。
保留 (Hold)	可	11.5(1) 以降
ハント グループ	はい。	12.0(1) 以降

機能	サポートされる	ファームウェア リリース
設定可能なタイマーを使用した着信コール アラート	不可	-
インターコム	可	11.5(1) 以降
キー拡張モジュール	Cisco IP 電話 8851/8861 キー拡張モジュールおよび Cisco IP 電話 8865 キー拡張モジュールは、拡張回線モードをサポートします	12.0(1) 以降
Malicious Call Identification（MCID; 迷惑呼 ID）	可	11.5(1) 以降
ミートミー	可	11.5(1) 以降
モバイル コネクト	可	11.5(1) 以降
Multilevel Precedence and Preemption	不可	-
ミュート	可	11.5(1) 以降
その他のグループ ピックアップ	可	12.0(1) 以降
キュー ステータスのプログラム可能な改選期（PLK）サポート	可	11.5(1) 以降
[プライバシー（Privacy）]	可	11.5(1) 以降
Queue Status	可	11.5(1) 以降
Quality Reporting Tool（QRT; 品質レポートツール）	可	11.5(1) 以降
右から左へのロケール サポート	不可	-
Redial	可	11.5(1) 以降
サイレント モニタリングと録音	可	11.5(1)SR1 以降
スピード ダイヤル	可	11.5(1) 以降
Survivable Remote Site Telephony（SRST）	可	11.5(1) 以降

機能	サポートされる	ファームウェア リリース
転送	可	11.5(1) 以降
Uniform Resource Identifier（URI）ダイヤリング	可	11.5(1) 以降
ビデオ通話	可	11.5(1) 以降
ビジュアル ボイスメール	可	11.5(1) 以降
ボイスメール	可	11.5(1) 以降

関連トピック

セッション回線モードの環境 （187 ページ）

TLS 再開タイマーのセットアップ

TLS セッション再開は、認証プロセス全体を繰り返さずに TLS セッションを再開できるようにします。 TLS 接続のデータ交換にかかる時間を大幅に短縮できます。

電話機は TLS セッションをサポートしていますが、すべての TLS セッションが TLS 再開をサポートするとは限りません。 次に、さまざまなセッションと TLS 再開のサポートについて説明します。

- SIP シグナリングの TLS セッション：再開をサポートします
- HTTPS クライアント：再開をサポートします
- CAPF：再開をサポートします
- TVS：再開をサポートします
- EAP-TLS：再開をサポートしません
- EAP-FAST：再開をサポートしません
- VPN クライアント：再開をサポートしません

詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 [TLS 再開タイマー（TLS Resumption Timer）] パラメータを設定します。

タイマーの範囲は 0 から 3600 秒です。デフォルト値は 3600 です。このフィールドに 0 を指定すると、TLS セッションの再開が無効になります。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

インテリジェント プロキシミティの有効化

（注） この手順は、Bluetooth 対応の電話機のみに適用されます。 Cisco IP 電話 8811、8841、8851NR、および 8865NR は Bluetooth をサポートしていません。

インテリジェント プロキシミティを使用することで、ユーザのモバイル デバイスやタブレットで電話機の音響特性を利用できるようになります。 ユーザは Bluetooth を使用してモバイル デバイスやタブレットを電話機にペアリングします。

モバイル デバイスがペアリングされると、ユーザは電話機でモバイル コールの発信および受信ができるようになります。タブレットを使用する場合、タブレットから電話機に音声をルーティングできます。

複数のモバイル デバイス、タブレット、Bluetooth ヘッドセットを電話機にペアリングできます。 ただし、同時に接続できるのは 1 つのデバイスと 1 つのヘッドセットのみです。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、**[電話（Phone）]** > **[デバイス（Device）]** を選択します。

ステップ 2 変更する電話機を特定します。

ステップ 3 [Bluetooth] フィールドを [有効（Enabled）]に設定します。

ステップ 4 [Bluetoothによるモバイルハンズフリーモードを許可（Allow Bluetooth Mobile Handsfree Mode）] フィールドを [有効（Enabled）]に設定します。

ステップ 5 変更を保存し、電話機に適用します。

ビデオ送信解像度のセットアップ

Cisco IP 電話 8845、8865、および 8865NR は、次のビデオ形式をサポートしています。

- 720p（1280 X 720）
- WVGA（800 X 480）

- 360p（640 X 360）
- 240p（432x240）
- VGA（640 x 480）
- CIF（352 X 288）
- SIF（352 X 240）
- QCIF（176x144）

ビデオ機能付き Cisco IP 電話は、電話機の設定や解像度の制限に基づいて帯域幅での最適な解像度をネゴシエートします。 例：88x5 から 88x5 への直接コールでは、電話機は正確に 720p は送らず、800x480 を送ります。 この制限は単に、88x5 の 5 インチ WVGA 画面解像度が 800 X 480 であることに起因します。

ビデオの種類	ビデオ解像度	フレーム/秒（**fps**）	ビデオ ビット レート範囲
720p	1,280 X 720	30	1360 ～ 2500 kbps
720p	1,280 X 720	15	790 ～ 1359 kbps
WVGA	800 x 480	30	660 ～ 789 kbps
WVGA	800 x 480	15	350 ～ 399 kbps
360p	640 x 360	30	400 ～ 659 kbps
360p	640 x 360	15	210–349kbps
240P	432 x 240	30	180–209kbps
240P	432 x 240	15	64–179kbps
VGA	640 X 480	30	520 ～ 1500 kbps
VGA	640 X 480	15	280 ～ 519 kbps
CIF	352 X 288	30	200 ～ 279 kbps
CIF	352 X 288	15	120 ～ 199 kbps
SIF	352 X 240	30	200 ～ 279 kbps
SIF	352 X 240	15	120 ～ 199 kbps
QCIF	176 x 144	30	94 ～ 119 kbps
QCIF	176 x 144	15	64 ～ 93 kbps

Cisco Unified Communications Managerの旧バージョンでのヘッドセット管理

12.5(1)SU1 以前のバージョンの Cisco Unified Communications Manager を使用する場合、オンプレミスの電話機を使用して Cisco ヘッドセット設定をリモートで構成できます。

Cisco Unified Communications Manager バージョン 10.5 (2)、11.0 (1)、11.5 (1)、12.0 (1)、および 12.5 (1) でリモートヘッドセット構成を行うには、Cisco ソフトウェアダウンロード web サイトからファイルをダウンロードし、ファイルを編集し、Cisco Unified Communications Manager TFTP サーバにファイルをアップロードする必要があります。 ファイルは JavaScript オブジェクト通知 (JSON) ファイルです。 更新されたヘッドセット構成は10～30 分の時間枠でエンタープライズヘッドセットに適用され、TFTP サーバのトラフィックバックログを回避することができます。

（注） Cisco Unified Communications Manager管理バージョン 11.5 (1) SU7 を使用して、ヘッドセットを管理し構成することができます。

JSON ファイルを扱う際には、次の点に注意してください。

- コードに括弧が抜けている場合、設定は適用されません。 JSON Formatter などのオンラインツールを使用して、フォーマットを確認してください。
- **updatedTime** 設定を現在のエポック時間に設定しない場合は、設定が適用されません。 もしくは、**updatedTime**値を 1 増やし、旧バージョンよりも大きくすることもできます。
- パラメータ名を変更しないでください。設定が適用されません。

TFTP サービスの詳細については、*Cisco Unified Communications Manager* および *IM* およびプレゼンスサービスのアドミニストレーションガイドの「デバイスファームウェア管理」の章を参照してください。

`defaultheadsetconfig.json`ファイルを適用する前に、電話機を最新のファームウェアリリースにアップグレードしてください。 次の表では、JSON ファイルを使用して調整できるデフォルト設定を説明します。

デフォルトのヘッドセット構成ファイルのダウンロード

ヘッドセットパラメータをリモートで構成する前に、最新の JavaScript オブジェクト表記 (JSON) サンプルファイルをダウンロードする必要があります。

手順

ステップ 1 次の URL にアクセスしてください：https://software.cisco.com/download/home/286320550

ステップ 2 **Headsets 500 シリーズ**を選択します。

ステップ 3 ヘッドセットシリーズを選択してください。

ステップ 4 リリースフォルダを選択して、zip ファイルを選択します。

ステップ 5 [**ダウンロード (Download)**] または [**カートに追加 (Add to cart)**] ボタンをクリックして、プロンプトの指示に従います。

ステップ 6 PC のディレクトリにファイルを解凍します。

次のタスク

デフォルトのヘッドセット構成ファイルの変更 （238 ページ）

デフォルトのヘッドセット構成ファイルの変更

JavaScript Object Notation （JSON） ファイルを扱う際は、次の点に注意してください。

- コードに括弧が抜けている場合、設定は適用されません。 JSON Formatter などのオンラインツールを使用して、フォーマットを確認してください。
- **UpdatedTime** の設定を現在のエポック時間に設定するか、または設定が適用されません。
- **firmwareName** が最新バージョンであるかを確認してください。最新でない場合は構成が適用されません。
- パラメータ名を変更しないでください。設定が適用されません。

手順

ステップ 1 `defaultheadsetconfig.json`ファイルをテキストエディタで開きます。

ステップ 2 変更する updatedTime とヘッドセットパラメータ値を編集します。

スクリプトのサンプルを次に示します。 このスクリプトは参考用としてのみ提供されます。ヘッドセットパラメータを構成する際のガイドとして使用してください。 ファームウェアロードに含まれている JSON ファイルを使用します。

```
{
  "headsetConfig": {
    "templateConfiguration": {
      "configTemplateVersion": "1",
      "updatedTime": 1537299896,
      "reportId": 3,
      "modelSpecificSettings": [
        {
          "modelSeries": "530",
          "models": [
            "520",
            "521",
            "522",
            "530",
            "531",
```

```
      "532"
    ],
    "modelFirmware": [
      {
        "firmwareName": "LATEST",
        "latest": true,
        "firmwareParams": [
          {
            "name": "Speaker Volume",
            "access": "Both",
            "usageId": 32,
            "value": 7
          },
          {
            "name": "Microphone Gain",
            "access": "Both",
            "usageId": 33,
            "value": 2
          },
          {
            "name": "Sidetone",
            "access": "Both",
            "usageId": 34,
            "value": 1
          },
          {
            "name": "Equalizer",
            "access": "Both",
            "usageId": 35,
            "value": 3
          }
        ]
      }
    ]
  },
  {
    "modelSeries": "560",
    "models": [
      "560",
      "561",
      "562"
    ],
    "modelFirmware": [
      {
        "firmwareName": "LATEST",
        "latest": true,
        "firmwareParams": [
          {
            "name": "Speaker Volume",
            "access": "Both",
            "usageId": 32,
            "value": 7
          },
          {
            "name": "Microphone Gain",
            "access": "Both",
            "usageId": 33,
            "value": 2
          },
          {
            "name": "Sidetone",
            "access": "Both",
            "usageId": 34,
            "value": 1
```

```
                },
                {
                  "name": "Equalizer",
                  "access": "Both",
                  "usageId": 35,
                  "value": 3
                },
                {
                  "name": "Audio Bandwidth",
                  "access": "Admin",
                  "usageId": 36,
                  "value": 0
                },
                {
                  "name": "Bluetooth",
                  "access": "Admin",
                  "usageId": 39,
                  "value": 0
                },
                {
                  "name": "DECT Radio Range",
                  "access": "Admin",
                  "usageId": 37,
                  "value": 0
                }
                {
                   "name": "Conference",
                  "access": "Admin",
                  "usageId": 41,
                  "value": 0
              ]
            }
          ]
        }
      ]
    }
  }
}
```

ステップ 3 Defaultheadsetconfig. json を保存します。

次のタスク

デフォルトの構成ファイルをインストールします。

Cisco Unified Communications Manager にデフォルト構成ファイルをインストールする

Defaultheadsetconfig. jsonファイルを編集した後、TFTP ファイル管理ツールを使用して Cisco Unified Communications Manager にインストールします。

手順

ステップ 1 Cisco Unified OS 管理で**[ソフトウェアアップグレード（Software Upgrades）]** > **[TFTPファイル管理（TFTP File Management）]** を選択します。

ステップ 2 [ファイルのアップロード（Upload File）]を選択します。

ステップ 3 [**ファイルを**選択 (Choose File)] を選択して、`defaultheadsetconfig. json`ファイルに移動します。

ステップ 4 [ファイルのアップロード（Upload File）]を選択します。

ステップ 5 **[閉じる（Close）]** をクリックします。

Cisco TFTP サーバの再起動

`Defaultheadsetconfig. json`ファイルをTFTPディレクトリにアップロードした後、Cisco TFTP サーバを再起動し、電話機をリセットします。 約 10 ~ 15 分後に、ダウンロードプロセスが開始され、新しい構成がヘッドセットに適用されます。設定が適用されるまでに、さらに10ー30 分かかります。

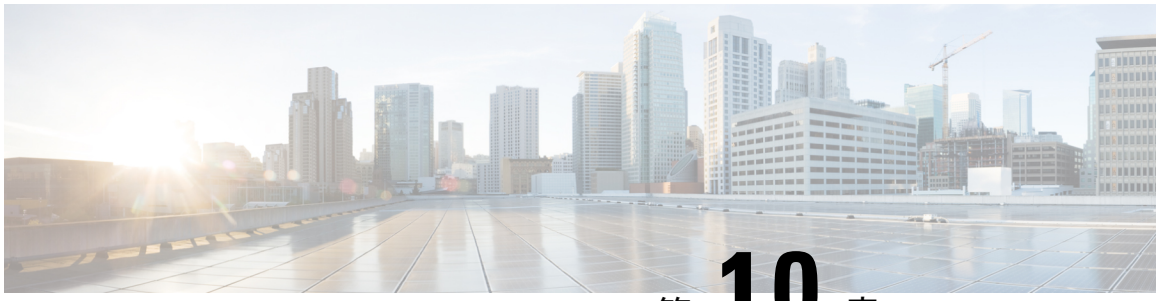
手順

ステップ 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）]** > **[コントロールセンタ - 機能サービス（Control Center - Feature Services）]**を選択します。

ステップ 2 **サーバ（Server）**ドロップダウンリストボックスから、Cisco TFTP サービスが実行されているサーバを選択します。

ステップ 3 **Cisco TFTP** サービスに対応するラジオボタンをクリックします。

ステップ 4 **再起動（Restart）**をクリックします。



第 10 章

社内ディレクトリとパーソナル ディレクトリ

社内ディレクトリのセットアップ

社内ディレクトリによって、ユーザが同僚の電話番号を調べることができます。 この機能をサポートするには、社内ディレクトリを設定する必要があります。

Cisco Unified Communications Manager は、Cisco Unified Communications Manager（LDAP）ディレクトリを使用して、Cisco Unified Communications Manager とインタフェースする Cisco Unified Communications Manager アプリケーションのユーザーについての認証情報と承認情報を保存します。 認証によって、システムに対するユーザのアクセス権が確立します。 認可とは、ユーザが使用を許可されるテレフォニー リソース、たとえば特定の電話内線などを識別することです。

Cisco IP 電話は、クライアントとサーバの両方で SecureApp に動的割り当てを使用します。 これにより、電話機は4KBを超える証明書を確実に読み取ることができ、ユーザーが自分のディレクトリにアクセスしたときに[ホストが見つかりません（Host Not Found）]エラーメッセージが表示される頻度が少なくなります。

手順の詳細については、特定のリリースのマニュアルを参照してください。Cisco Unified Communications Manager

LDAPディレクトリの設定が完了すると、ユーザは電話機の社内ディレクトリ サービスを使用して、社内ディレクトリでユーザを検索できるようになります。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

パーソナル ディレクトリのセットアップ

パーソナル ディレクトリには、ユーザが一連の個人の番号を保存できます。

パーソナル ディレクトリは、次の機能で構成されています。

- 個人アドレス帳（PAB）
- スピード ダイヤル
- アドレス帳同期化ツール（TABSynch）

ユーザはこれらの方法を使用してパーソナル ディレクトリの機能を利用できます。

- Webブラウザから：ユーザは、Cisco Unified CommunicationsセルフケアポータルからPABおよびスピードダイヤル機能にアクセスできます。
- Cisco IP 電話から：企業ディレクトリまたはユーザの個人ディレクトリを検索するには、**[連絡先（Contact）]**を選択します。
- Microsoft Windows アプリケーションから：TABSynch ツールを使用して、PAB を Microsoft Windows Address Book（WAB）と同期化することができます。 Microsoft Outlook Address Book（OAB）を使用するユーザは、まず OAB から WAB にデータをインポートする必要があります。 次に TabSync を使用して WAB をパーソナル ディレクトリと同期化します。 TABSync の使用方法については、Cisco IP 電話 Address Book Synchronizer のダウンロード（245 ページ）およびSynchronizer のセットアップ （246 ページ）を参照してください。

Cisco IP 電話は、クライアントとサーバの両方で SecureApp に動的割り当てを使用します。 これにより、電話機は4KBを超える証明書を確実に読み取ることができ、ユーザーが自分のディレクトリにアクセスしたときに[ホストが見つかりません（Host Not Found）]エラーメッセージが表示される頻度が少なくなります。

Cisco IP 電話 Address Book Synchronizer を使用しているユーザが、エンド ユーザ データのみにアクセスできるようにするには、Cisco Unified サービスアビリティで Cisco UXL Web Service をアクティブ化します。

パーソナル ディレクトリを Web ブラウザから設定するには、ユーザがセルフケアポータルにアクセスする必要があります。 管理者は、ユーザに対して URL とサインイン情報を提供する必要があります。

ユーザのパーソナル ディレクトリのエントリのセットアップ

ユーザは、Cisco IP 電話 で、パーソナル ディレクトリのエントリを設定できます。 パーソナル ディレクトリを設定するには、ユーザが以下にアクセスできる必要があります。

- セルフケアポータル：セルフケアポータルへのアクセス方法をユーザに必ず伝えてください。 詳細については、セルフケアポータルへのユーザのアクセスの設定 （92 ページ）を参照してください。
- Cisco IP 電話 Address Book Synchronizer：ユーザにインストーラを必ず配布してください。Cisco IP 電話 Address Book Synchronizer のダウンロード （245 ページ）を参照してください。

（注） Cisco IP 電話アドレス帳のシンクロナイザは、サポートされていないバージョンの Windows (たとえば、Windows XP 以前) でのみサポートされています。 このツールは、新しいバージョンの Windows ではサポートされていません。 将来、Cisco Unified Communications Manager プラグインの一覧から削除されます。

Cisco IP 電話 Address Book Synchronizer のダウンロード

Synchronizer のコピーをダウンロードしてユーザに送信するには、次の手順を実行します。

手順

ステップ 1 インストーラを入手するには、Cisco Unified Communications Manager の管理で、**[Application]** > **[Plugins]** を選択します。

ステップ 2 Cisco IP 電話 Address Book Synchronizer プラグイン名の横にある [Download]を選択します。

ステップ 3 ファイルをダウンロードするダイアログボックスが表示されたら、[保存（Save）]を選択します。

ステップ 4 TabSyncInstall.exe ファイル、およびCisco IP 電話 Address Book Synchronizer の導入 （245 ページ）の手順を、このアプリケーションを必要としているすべてのユーザに送信します。

Cisco IP 電話 Address Book Synchronizer の導入

Cisco IP 電話 Address Book Synchronizer は、Microsoft Windows のアドレス帳に格納されているデータを、Cisco Unified Communications Manager ディレクトリおよびセルフケアポータルの個人アドレス帳サービスと同期させることができます。

ヒント Windows のアドレス帳と個人アドレス帳を適切に同期させるには、次の手順を実行する前に、Windows アドレス帳のすべてのユーザを Windows アドレス帳に入力する必要があります。

Synchronizer のインストール

Cisco IP 電話 Address Book Synchronizer をインストールするには、次の手順を実行します。

手順

ステップ 1 システム管理者から Cisco IP 電話 Address Book Synchronizer のインストーラ ファイルを入手してください。

ステップ 2 管理者から提供された TabSyncInstall.exe ファイルをダブルクリックします。

ステップ 3 [Run]を選択します。

ステップ 4 [次へ（Next）]を選択します。

ステップ 5 ライセンス契約に関する情報を読み、[I Accept]を選択します。 [次へ（Next）]を選択します。

ステップ 6 アプリケーションのインストール先ディレクトリを選択し、[Next]を選択します。

ステップ 7 [Install]を選択します。

ステップ 8 [Finish]を選択します。

ステップ 9 プロセスを完了するために、Synchronizer のセットアップ （246 ページ）の手順を実行します。

Synchronizer のセットアップ

Cisco IP 電話 Address Book Synchronizer を設定するには、次の手順を実行します。

手順

ステップ 1 Cisco IP 電話 Address Book Synchronizer を開きます。

デフォルトのインストールディレクトリを受け入れた場合は、**[Start]** > **[All Programs]** > **[Cisco Systems]** > **[TabSync]** を選択することでアプリケーションを開くことができます。

ステップ 2 ユーザ情報を設定するには、[User]を選択します。

ステップ 3 Cisco IP 電話のユーザ名とパスワードを入力し、[OK]を選択します。

ステップ 4 Cisco Unified Communications Manager サーバ情報を設定するには、[サーバ（Server）]を選択します。

ステップ 5 Cisco Unified Communications Manager サーバの IP アドレスまたはホスト名とポート番号を入力し、[OK]を選択します。

この情報が不明な場合は、システム管理者に問い合わせてください。

ステップ 6 ディレクトリ同期プロセスを開始するには、[Synchronize]を選択します。

[Synchronization Status] ウィンドウに、アドレス帳の同期の状況が表示されます。 重複エントリに関するルールでユーザによる調整を選択しており、アドレス帳のエントリが重複している場合は、[Duplicate Selection] ウィンドウが表示されます。

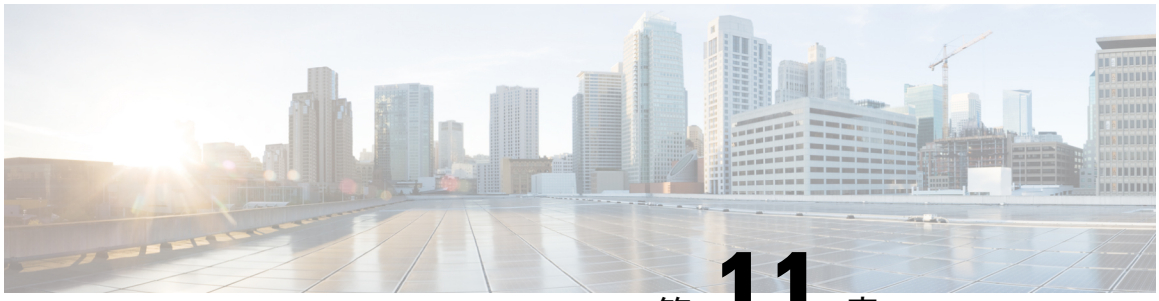
ステップ 7 個人アドレス帳に登録するエントリを選択し、[OK]を選択します。

ステップ 8 同期化が完了したら、[Exit]を選択して Cisco Unified CallManager Address Book Synchronizer を閉じます。

ステップ 9 同期化が機能しているかを確認するには、セルフケアポータルにログインし、[Personal Address Book]を選択します。 機能している場合は、Windows のアドレス帳のユーザが表示されます。

第 IV 部

Cisco IP 電話のトラブルシューティング



第 11 章

電話システムのモニタリング

Cisco IP 電話のステータス

このセクションでは、Cisco IP 電話 8800 シリーズでモデル情報、ステータス メッセージ、およびネットワーク統計を表示する方法について説明します。

- [モデル情報（Model Information）]：電話機のハードウェアとソフトウェアに関する情報を表示します。
- [ステータス（Status）] メニュー：ステータス メッセージ、ネットワーク統計、および現在のコールに関する統計を表示する画面にアクセスできます。

これらの画面に表示される情報は、電話機の操作のモニタやトラブルシューティングに役立てることができます。

また、これらの情報の大半およびその他の関連情報は、電話機の Web ページからリモートで取得することもできます。

トラブルシューティングの詳細については、トラブルシューティング （295 ページ） を参照してください。

[電話の情報（Phone Information）] ウィンドウの表示

[モデル情報（Model Information）] 画面を表示するには、次の手順を実行します。

手順

ステップ 1 アプリケーション を押します。

ステップ 2 [電話の情報]を選択します

ユーザがセキュアまたは認証済みのサーバに接続している場合、サーバオプションの右側にある [電話の情報（Phone Information）] 画面に、対応するアイコン（錠前または証明書マーク）が表示されます。ユーザがセキュアまたは認証済みのサーバに接続していない場合、アイコンは表示されません。

ステップ 3 [モデル情報（Model Information）] 画面を終了するには、[終了（Exit）]を押します。

[電話機情報（Phone Information）] のフィールド

次の表で電話機情報の設定について説明します。

表 *40 : [*電話機情報（*Phone Information***）*]* の設定**

オプション	説明
モデル番号	電話機のモデル番号。
IPv4 アドレス	電話機の IP アドレス。
ホスト名	電話機のホスト名。
アクティブ ロード（Active Load）	現在、電話機にインストールされているファームウェアのバージョン。 ユーザは、[詳細（Details）]を押して詳細を確認できます。
非アクティブロード（Inactive Load）	[非アクティブロード（Inactive Load）] は、ダウンロードの進行中のみ表示されます。 ダウンロード アイコン、および「[アップグレード中（Upgrade in Progress）]」または「[アップグレードに失敗しました（Upgrade Failed）]」という状態も表示されます。 ユーザがアップグレード中に [詳細（Details）]を押すと、ダウンロード ファイル名とコンポーネントがリストされます。 新しいファームウェアイメージは、保守ウィンドウより先にダウンロードするよう設定できます。この場合、すべての電話機でファームウェアがダウンロードされるまで待たずに、非アクティブ ステータスに対する既存ロードのリセットから、新しいロードのインストールへと急速に切り替えられます。 ダウンロードが完了したときに、アイコンは完了ステータスを示すように変更され、ダウンロードの成功に対してチェックマークが表示され、ダウンロードの失敗に対して「X」が表示されます。 可能な場合は、残りのロードのダウンロードが継続されます。
前回のアップグレード（Last Upgrade）	前回ファームウェアをアップグレードした日付。

オプション	説明
アクティブ サーバ（Active server）	電話機が登録されているサーバのドメイン名。
スタンバイサーバ（Stand-by Server）	スタンバイ サーバのドメイン名。

[ステータス（Status）] メニューの表示

[ステータス（Status）] メニューには次のオプションが含まれます。これらは電話機とその動作に関する情報を示します。

- [ステータス メッセージ（Status Messages）] : [ステータス メッセージ（Status Messages）] 画面を表示します。ここには、重要なシステム メッセージのログが示されます。
- [イーサネット統計（Ethernet Statistics）] : [イーサネット統計（Ethernet Statistics）] 画面を表示します。ここには、イーサネット トラフィック統計が表示されます。
- [ワイヤレス統計（Wireless Statistics）] : [ワイヤレス統計（Wireless Statistics）] 画面が表示されます（該当する場合）。
- [コール統計（Call Statistics）] : 現在のコールのカウンタおよび統計を表示します。
- [現在のアクセス ポイント（Current Access Point）] : [現在のアクセス ポイント（Current Access Point）] 画面が表示されます（該当する場合）

[ステータス（Status）] メニューを表示するには、次の手順を実行します。

手順

ステップ 1 [ステータス] メニューを表示するには、**[アプリケーション]** を押します。
ステップ 2 **[管理者設定（Admin Settings）]** > **[ステータス（Status）]** を選択します。
ステップ 3 [ステータス（Status）] メニューを終了するには、[終了（Exit）]を押します。

[ステータス メッセージ（Status Messages）] ウィンドウの表示

[ステータス メッセージ（Status Messages）] 画面には、電話機が最近生成したステータス メッセージが 30 件表示されます。 この画面には、電話機が起動を完了していない場合でも、いつでもアクセスできます。

手順

ステップ 1 アプリケーション を押します。

ステップ 2 **[管理者設定（Admin Settings）] > [ステータス（Status）] > [ステータスメッセージ（Status Messages）]** を選択します。

ステップ 3 現在のステータス メッセージを削除するには、[クリア（Clear）]を押します。

ステップ 4 [ステータス メッセージ（Status Messages）]画面を終了するには、[終了（Exit）]を押します。

ステータス メッセージのフィールド

次の表に、電話機の [ステータス メッセージ（Status Messages）] 画面に表示されるステータス メッセージを示します。

表 *41 : Cisco Unified IP* 電話のステータス メッセージ

メッセージ	説明	考えられる状況と対処方法
CFG TFTP サイズ エラー（CFG TFTP Size Error）	電話機のファイル システムに対して、設定ファイルのサイズが大きすぎます。	電話機の電源をオフ/オンにしま
チェックサム エラー（Checksum Error）	ダウンロードしたソフトウェア ファイルが破損しています。	電話機のファームウェアの新し それを TFTPPath ディレクトリに をこのディレクトリにコピーで バ ソフトウェアがシャットダウ けです。それ以外の場合にコピ が破損する可能性があります。
DHCP から IP アドレスを取得できませんでした（Could not acquire an IP address from DHCP）	電話機は DHCP サーバから IP アドレスを取得していません。 工場出荷時の状態にリセットした場合に、このメッセージが表示される可能性があります。	DHCP サーバが使用可能であり ドレスが利用できることを確認
CTL と ITL がインストールされました（CTL and ITL installed）	電話機に Certificate Trust List（CTL）ファイルおよび証明書信頼リスト（ITL）ファイルがインストールされています。	なし。 これは情報メッセージで ITL ファイルのどちらも、過去に いません。
CTL がインストールされました（CTL Installed）	証明書信頼リスト（CTL）ファイルが電話機にインストールされました。	なし。 これは情報メッセージで 過去にインストールされていま
CTL の更新失敗（CTL update failed）	電話機で証明書信頼リスト（CTL）ファイルを更新できませんでした。	TFTP サーバの CTL ファイルに

メッセージ	説明	考えられる状況と対処方法
DHCP タイムアウト（DHCP timeout）	DHCP サーバが応答しませんでした。	ネットワークがビジーになっ ネットワーク負荷が軽減さ ます。 DHCP サーバと電話機との間 ない：ネットワーク接続を確 DHCP サーバがダウンしてい を確認してください。 エラーが続く：スタティック ることを検討してください。
DNS タイムアウト（DNS timeout）	DNS サーバが応答しませんでした。	ネットワークがビジーになっ ネットワーク負荷が軽減さ ます。 DNS サーバと電話機との間 い：ネットワーク接続を確認 DNS サーバがダウンしてい 確認してください。
DNS 不明ホスト（DNS unknown host）	DNS が TFTP サーバまたは Cisco Unified Communications Manager の名前を解決できませんでした。	TFTP サーバまたは Cisco Un Manager のホスト名が DNS ことを確認してください。 ホスト名ではなく、IP アド 討してください。
IP が重複しています（Duplicate IP）	別のデバイスが、電話機に割り当てられた IP アドレスを使用中です。	電話機にスタティック IP ア いる場合は、重複する IP ア いことを確認してください。 DHCP を使用している場合は 確認してください。
CTL および ITL ファイルを削除中（Erasing CTL and ITL files）	CTL および ITL ファイルを削除中です。	なし。 これは情報メッセー

メッセージ	説明	考えられる状況と対処方法
ロケールの更新エラー（Error update locale）	1 つ以上のローカリゼーション ファイルが TFTPPath ディレクトリで見つからなかったか、または有効ではありませんでした。 ロケールは変更されませんでした。	Cisco Unified Communications Op ページから、次のファイルが [（TFTP File Management）] のサ 在することを確認してください • ネットワーク ロケールと同 クトリに存在するファイル • tones.xml • ユーザ ロケールと同じ名前 に存在するファイル： • glyphs.xml • dictionary.xml • kate.xml
ファイルが見つかりません <Cfg File>	TFTP サーバで、名前ベースのデフォルトの設定ファイルが見つかりませんでした。	電話機の設定ファイルは、電話 Communications Manager データ きに作成されます。 電話機が C Communications Manager データ 合、TFTP サーバは「**CFG ファ ん（CFG File Not Found）」 ます。 • 電話機が Cisco Unified Com に登録されていません。 電話機を自動登録できない 機を Cisco Unified Commun 加する必要があります。詳 機の追加方法 （79 ページ） い。 • DHCP を使用している場合 しい TFTP サーバを指定して ください。 • スタティック IP アドレスを TFTP サーバの設定を確認
ファイルが見つかりません <CTLFile.tlv>	Cisco Unified Communications Manager クラスタがセキュア モードでない場合にこのメッセージが電話機に表示されます。	影響はありません。引き続き電 Communications Manager に登録

メッセージ	説明	考えられる状況と対処方法
IP アドレス解放（IP address released）	電話機は、IP アドレスを解放するように設定されます。	電話機は、電源をオフ/オンアドレスをリセットするまです。
ITL がインストールされました（ITL installed）	電話機に ITL ファイルがインストールされています。	なし。 これは情報メッセー過去にインストールされて
拒否された HC のロード（Load rejected HC）	ダウンロードされたアプリケーションには、電話機のハードウェアとの互換性がありません。	この電話機でのハードウェアないバージョンのソフトウェうとすると発生します。 電話機に割り当てられたロー（Cisco Unified Communicati**（Device）] > [電話（Phone**話機に表示されたロードを再
デフォルト ルータがありません（No default router）	DHCP またはスタティック設定でデフォルト ルータが指定されていませんでした。	電話機にスタティック IP アいる場合は、デフォルト ルとを確認してください。 DHCP を使用している場合はルト ルータを提供していま定を確認してください。
DNS サーバ IP がありません（No DNS server IP）	名前は指定されていましたが、DHCP またはスタティック IP 設定で DNS サーバのアドレスが指定されていませんでした。	電話機にスタティック IP アいる場合は、DNS サーバが認してください。 DHCP を使用している場合はサーバを提供していません。確認してください。
信頼リストがインストールされていません（No Trust List installed）	CTL ファイルまたは ITL ファイルが電話機にインストールされていません。	信頼ファイルが Cisco Unifie で設定されていません。Cis Manager はデフォルトではセません。
電話機を登録できませんでした。（Phone failed to register.） 証明書のキー サイズは FIPS に準拠していません。（Cert key size is not FIPS compliant.）	FIPS では、RSA サーバ証明書は 2048 ビット以上である必要があります。	証明書を更新してください。
「Cisco Unified Communications Manager 要求による再起動（Restart requested by CUCM）」	Cisco Unified Communications Manager（CUCM）からの要求に基づいて電話機が再起動します。	Cisco Unified Communications変更が行われ、変更を有効（Apply）] ボタンが押され

メッセージ	説明	考えられる状況と対処方法
TFTP アクセス エラー（TFTP access error）	TFTP サーバが、存在しないディレクトリを指定しています。	DHCP を使用している場合は、 TFTP サーバを指定しているこい。 スタティック IP アドレスを使用 TFTP サーバの設定を確認して
TFTP エラー（TFTP error）	電話機が TFTP サーバから提供されたエラー コードを認識しません。	Cisco TAC にお問い合わせくだ
TFTP タイムアウト（TFTP timeout）	TFTP サーバが応答しませんでした。	ネットワークがビジーになって ネットワーク負荷が軽減される ます。 TFTP サーバと電話機との間にネい：ネットワーク接続を確認し TFTP サーバがダウンしている を確認してください。
タイムアウト（Timed Out）	サプリカントが 802.1X トランザクションを実行しようとしましたが、オーセンティケータが存在しないためにタイムアウトになりました。	通常は、802.1X がスイッチに設に認証がタイムアウトします。

メッセージ	説明	考えられる状況と対処方法
信頼リストの更新に失敗しました（Trust List update failed）	CTL ファイルおよび ITL ファイルの更新に失敗しました。	電話機は CTL ファイルおよ トールしていますが、新しい ITL ファイルの更新に失敗し 失敗の理由として次が考えら • ネットワークの障害が発 • TFTP サーバがダウンし • CTL ファイルの署名に使 リティ トークン、および に使用された TFTP 証明書 機の現在の CTL ファイル は使用できない。 • 内部的な電話障害が発生 解決策として次が考えられま • ネットワーク接続を確認 • TFTP サーバがアクティブ るかどうかを確認する。 • Transactional Vsam Service Unified Communications ている場合は、TVS サー 常に機能しているかどう • セキュリティ トークンが 効かどうかを確認する。 上述の解決策がすべて失敗し ファイルおよび ITL ファイル セットする。
信頼リストが更新されました（Trust List updated）	CTL ファイル、ITL ファイル、またはその両方が更新されます。	なし。 これは情報メッセー
バージョン エラー（Version error）	電話機のロード ファイルの名前が不正です。	電話機のロード ファイルが 確認してください。
XmlDefault.cnf.xml（または電話機のデバイス名に対応した.cnf.xml）	コンフィギュレーション ファイルの名前。	なし。 このメッセージは、 を示します。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

[ネットワーク情報（Network Information）] 画面の表示

[ネットワーク情報（Network Information）] 画面に表示される情報を利用して、電話機の接続問題を解決します。

電話ネットワークへの接続に問題があるときに、メッセージが電話機に表示されます。

手順

ステップ 1 [ステータス] メニューを表示するには、**[アプリケーション]** を押します。

ステップ 2 **[管理者設定（Admin Settings）]** > **[ステータス（Status）]** > **[ステータスメッセージ（Status Messages）]** を選択します。

ステップ 3 [ネットワーク情報（Network Info）] を選択します。

ステップ 4 [ネットワーク情報（Network Info）] を終了するには、[終了（Exit）]を押します。

[ネットワーク統計（Network Statistics）] 画面の表示

[ネットワーク統計（Network Statistics）] 画面には、電話機およびネットワークのパフォーマンスに関する情報が表示されます。

[ネットワーク統計（Network Statistics）] 画面を表示するには、次の手順を実行します。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 [管理者設定（Admin Settings）]>[ステータス（Status）]>[ネットワーク統計（Network Statistics）] を選択します。

ステップ 3 [Rx Frames]、[Tx Frames]、および [Rx Broadcasts] の統計を 0 にリセットするには、[クリア（Clear）]を押します。

ステップ 4 [イーサネット統計（Ethernet Statistics）] 画面を終了するには、[終了（Exit）]を押します。

イーサネット統計情報

次の表では、[イーサネット統計（Ethernet Statistics）] 画面の情報について説明します。

表 *42*：イーサネット統計情報

項目	説明
Rx フレーム	電話機が受信した パケット。
Tx フレーム（Tx Frames）	電話機が送信したパケットの数。

項目	説明
Rx Broadcasts	電話機が受信したブロードキャスト パケットの数。
リスタートの原因	電話機が最後にリセットされた原因。 次のいずれかの値を指定します。 • 初期化 • TCP-timeout • CM-closed-TCP • TCP-Bad-ACK • CM-reset-TCP • CM-aborted-TCP • CM-NAKed • KeepaliveTO • Failback • Phone-Keypad • Phone-Re-IP • Reset-Reset • Reset-Restart • Phone-Reg-Rej • 拒否された HC のロード（Load Rejected HC） • CM-ICMP-Unreach • Phone-Abort
経過時間	電話機が最後にリブートしてから経過した時間。
ポート 1	ネットワーク ポートのリンク状態と接続。 たとえば、**Auto 100 Mb Full-Duplex** は、ネットワーク ポートがリンク アップ状態で、全二重の 100 Mbps 接続を自動ネゴシエーションしたことを意味します。
ポート 2	PC ポートのリンク状態と接続。
DHCP 状態（IPv4/IPv6）	• IPv4 専用モードでは、DHCP BOUND などの DHCPv4 状態だけが表示されます。 • IPv6 モードでは、ROUTER ADVERTISE などの、DHCPv6 状態だけが表示されます。 • DHCPv6 状態情報が表示されます。

次の表に、DHCPv4 および DHCPv6 状態の表示メッセージについて説明します。

表 *43 : DHCPv4* のイーサネット統計メッセージ

DHCPv4 状態	説明
CDP INIT	CDP がバインドされていないか、WLAN が稼働していない
DHCP BOUND	DHCPv4 は BOUND
DHCP DISABLED	DHCPv4 は無効
DHCP INIT	DHCPv4 は INIT
DHCP INVALID	DHCPv4 は INVALID（これが初期状態）
DHCP RENEWING	DHCPv4 は RENEWING
DHCP REBINDING	DHCPv4 は REBINDING
DHCP REBOOT	DHCPv4 は init-reboot
DHCP REQUESTING	DHCPv4 は要求中
DHCP RESYNC	DHCPv4 は RESYNCH
DHCP WAITING COLDBOOT TIMEOUT	DHCPv4 は起動中
DHCP UNRECOGNIZED	認識されない DHCPv4 状態
DISABLED DUPLICATE IP	重複した IPv4 アドレス
DHCP TIMEOUT	DHCPv4 タイムアウト
IPV4 STACK TURNED OFF	電話機は IPv6 のみモードで、IPv4 スタックはオフ
ILLEGAL IPV4 STATE	不正な IPv4 状態、発生すべきでない

表 *44 : DHCPv6* のイーサネット統計メッセージ

DHCPv6 状態	説明
CDP INIT	CDP を初期化中
DHCP6 BOUND	DHCPv6 は BOUND
DHCP6 DISABLED	DHCPv6 は DISABLED
DHCP6 RENEW	DHCPv6 は更新中
DHCP6 REBIND	DHCPv6 は再バインド中

DHCPv6 状態	説明
DHCP6 INIT	DHCPv6 は初期化中
DHCP6 SOLICIT	DHCPv6 は請求中
DHCP6 REQUEST	DHCPv6 は要求中
DHCP6 RELEASING	DHCPv6 は解放中
DHCP6 RELEASED	DHCPv6 は解放済み
DHCP6 DISABLING	DHCPv6 は無効化中
DHCP6 DECLINING	DHCPv6 は拒否中
DHCP6 DECLINED	DHCPv6 は拒否された
DHCP6 INFOREQ	DHCPv6 は INFOREQ
DHCP6 INFOREQ DONE	DHCPv6 は INFOREQ DONE
DHCP6 INVALID	DHCPv6 は INVALID（これが初期状態）
DISABLED DUPLICATE IPV6	DHCP6 は DISABLED だが、DUPLICATE IPV6 DETECTED
DHCP6 DECLINED DUPLICATE IP	DHCP6 は DISABLED -- DUPLICATE IPV6 DETECTED
ROUTER ADVERTISE., (DUPLICATE IP)	重複した自動設定 IPv6 アドレス
DHCP6 WAITING COLDBOOT TIMEOUT	DHCPv6 は起動中
DHCP6 TIMEOUT USING RESTORED VAL	DHCPv6 タイムアウト、フラッシュ メモリに保存された値を使用
DHCP6 TIMEOUT CANNOT RESTORE	DHCP6 はタイムアウト、フラッシュ メモリからのバックアップなし
IPV6 STACK TURNED OFF	電話機は IPv4 のみモードで、IPv6 スタックはオフ
ROUTER ADVERTISE., (GOOD IP)	
ROUTER ADVERTISE., (BAD IP)	
UNRECOGNIZED MANAGED BY	IPv6 アドレスはルータまたは DHCPv6 サーバからのものではない
ILLEGAL IPV6 STATE	不正な IPv6 状態、発生すべきでない

[ワイヤレス統計（Wireless Statistics）] 画面の表示

この手順は、ワイヤレスの Cisco IP 電話 8861 のみに適用されます。

[ワイヤレス統計（Wireless Statistics）] 画面を表示するには、次の手順を実行します。

手順

ステップ 1 アプリケーション を押します。

ステップ 2 [管理者設定（Admin Settings）]>[ステータス（Status）]>[ワイヤレス統計（Wireless Statistics）] を選択します。

ステップ 3 ワイヤレス統計を 0 にリセットするには、[クリア（Clear）]を押します。

ステップ 4 [ワイヤレス統計（Wireless Statistics）] 画面を終了するには、[終了（Exit）]を押します。

WLAN 統計

次の表に、電話機での WLAN 統計を示します。

表 *45 : Cisco Unified IP* 電話の *WLAN* 統計

項目	説明
Tx バイト（tx bytes）	電話機が送信したバイト数。
Rx バイト（rx bytes）	電話機が受信したバイト数。
Tx パケット（tx packets）	電話機が送信したパケットの数。
rx パケット（rx packets）	電話機が受信した パケット。
tx パケット ドロップ（tx packets dropped）	送信中にドロップされたパケット数。
Rx パケット ドロップ（rx packets dropped）	受信中にドロップされたパケット数。
tx パケット エラー（tx packet errors）	電話機が送信したエラー パケット数。
rx パケット エラー（rx packet errors）	電話機が受信したエラー パケット数。
Tx フレーム	正常に送信された MSDU の数。
tx マルチキャスト フレーム	正常に送信されたマルチキャスト MSDU の数。
tx リトライ	1 つまたは複数の再送信後に正常に送信された MSDU の数。

項目	説明
tx マルチ リトライ（tx multi retry）	1 つまたは複数の再送信後に正常に送信されたマルチキャスト MSDU の数。
Tx 失敗（tx failure）	送信の試行数が再試行の限度を超えたために、正常に送信されなかった MSDU の数。
RTS 成功（rts success）	このカウンタは、RTS の応答として CTS を受信したときに増分されます。
RTS 失敗（rts failure）	このカウンタは、RTS の応答としての CTS を受信しなかったときに増分されます。
ACK 失敗（ack failure）	このカウンタは、予期されている場合に ACK を受信しなかったときに増分されます。
Rx 重複フレーム（rx duplicate frames）	Sequence Control フィールドで重複が示されているフレームを受信した回数。
Rx フラグメント パケット（rx fragmented packets）	タイプがデータまたは管理の MPDU を正常に受信した数。
ローミング カウント（roaming count）	正常にローミングされた数。

[コール統計（Call Statistics）] ウィンドウの表示

電話機の [コールの統計（Call Statistics）] 画面にアクセスすると、最新のコールのカウンタ、統計、および音声品質メトリックを表示できます。

（注） また Web ブラウザを使用して [ストリームの統計（Streaming Statistics）] Web ページにアクセスすることにより、リモートでコール統計情報を表示することもできます。 この Web ページには、電話機では表示できない追加の RTCP 統計が含まれています。

単一のコールが複数の音声ストリームを使用する場合がありますが、最後の音声ストリームに関するデータだけがキャプチャされます。 音声ストリームは、2 つのエンドポイント間のパケット ストリームです。 一方のエンドポイントが保留になると、コールが引き続き接続されている場合でも、音声ストリームは停止します。 コールが再開されると、新しい音声パケット ストリームが開始され、以前のコールデータは新しいコールデータによって上書きされます。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Admin Settings）] > [ステータス（Status）] > [コール統計（Call Statistics）]** を選択します。

ステップ 3 [コール統計（Call Statistics）] 画面を終了するには、[終了（Exit）]を押します。

コール統計のフィールド

次の表に、[コール統計（Call Statistics）] 画面の項目を示します。

表 *46 : Cisco Unified Phone* の *[*コール統計（*Call Statistics*）*]* の項目

項目	説明
[受信コーデック（Receiver Codec）]	受信した音声ストリームの種類（コーデックからのRTPストリーミング オーディオ）： • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC • Opus • iSAC
[送信コーデック（Sender Codec）]	送信した音声ストリームの種類（コーデックからのRTPストリーミング オーディオ）： • G.729 • G.722 • G722.2 AMR-WB • G.711 mu-law • G.711 A-law • iLBC • Opus • iSAC
[受信サイズ（Receiver Size）]	受信中の音声ストリーム（RTPストリーミングオーディオ）の音声パケット サイズ（ミリ秒）。

項目	説明
[送信サイズ（Sender Size）]	送信中の音声ストリームの音声パケット サイズ（ミリ秒）。
受信パケット（Receiver Packets）	音声ストリームが開始されてから受信された RTP 音声パケットの数。 （注） コールが保留されていた可能性があるため、この数値は、必ずしもコールが開始されてから受信された RTP 音声パケットの数と同じであるとは限りません。
[送信パケット（Sender Packets）]	音声ストリームが開始されてから送信された RTP 音声パケットの数。 （注） コールが保留されていた可能性があるため、この数値は、必ずしもコールが開始されてから送信された RTP 音声パケットの数と同じであるとは限りません。
[平均ジッター（Avg Jitter）]	受信中の音声ストリームが開始されてから測定された、RTP パケット ジッターの推定平均値（パケットがネットワークを経由する際の動的な遅延）（ミリ秒単位）。
[最大ジッター（Max Jitter）]	受信中の音声ストリームが開始されてから測定された最大ジッター（ミリ秒単位）。
[受信破棄（Receiver Discarded）]	受信中の音声ストリームで廃棄された RTP パケットの数（不良パケット、過度の遅延などによる）。 （注） シスコ ゲートウェイが生成したペイロード タイプ 19 のコンフォート ノイズ パケットはこのカウンタを増分するため、電話機はこれらのパケットを破棄します。
受信喪失パケット（Receiver Lost Packets）	失われた RTP パケット（転送中に喪失）。
音声品質メトリック（Voice Quality Metrics）	
Cumulative conceal ratio	隠蔽フレームの総数を、音声ストリームの開始以降に受信された音声フレームの総数で割った値。
直近フレーム損失率（Interval Conceal Ratio）	アクティブな音声に先行する 3 秒間の間隔における、音声フレームに対する隠蔽フレームの比率。 音声アクティビティ検出（VAD）を使用する場合は、アクティブな音声を 3 秒集めるために、もっと長い間隔が必要になる可能性があります。
Max conceal ratio	音声ストリームの開始以降、最も高い間隔の隠蔽率。

項目	説明
フレーム損失発生秒数（Conceal Seconds）	音声ストリームの開始以降、隠蔽イベント（フレーム損失）があった秒数（[深刻なフレーム損失発生秒数（Severely Conceal Secs）] の値を含む）。
深刻なフレーム損失発生秒数（Severely Conceal Seconds）	音声ストリームの開始以降、5 % を超える隠蔽イベント（フレーム損失）があった秒数。
遅延	ネットワーク遅延の推定値（ミリ秒単位）。ラウンドトリップ遅延の実行中の平均値を表します。これは、RTCP 受信レポート ブロックの受信時に測定されます。

[現在のアクセス ポイント（Current Access Point）] ウィンドウの表示

[現在のアクセス ポイント（Current Access Point）] 画面には、Cisco IP 電話 8861 がワイヤレス通信に使用するアクセス ポイントに関する統計情報が表示されます。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Admin Settings）]** > **[ステータス（Status）]** > **[現在のアクセス ポイント（Current Access Point）]** を選択します。

ステップ 3 [現在のアクセス ポイント（Current Access Point）] 画面を終了するには、[終了（Exit）]を押します。

[現在のアクセス ポイント（Current Access Point）] のフィールド

次の表に、[現在のアクセス ポイント（Current Access Point）] 画面のフィールドを示します。

表 *47 : [*現在のアクセス ポイント（*Current Access Point*）*]* の項目

項目	説明
AP 名	CCX 準拠している場合は AP 名、それ以外は MAC アドレスが表示されます。
MAC アドレス	AP の MAC アドレス。
頻度（Frequency）	この AP で測定された最新の周波数。
現在のチャネル（Current Channel）	この AP で測定された最新のチャネル。

項目	説明
前回の RSSI（Last RSSI）	この AP で測定された最新の RSSI。
ビーコン間隔（Beacon Interval）	ビーコン間の時間単位の数。 時間単位は 1.024 msec です。
機能	このフィールドには、要求またはアドバタイズされたオプション機能を示すのに使用されるサブフィールド数が含まれます。
基本レート（Basic Rates）	AP が要求し、ステーションが動作に対応している必要がある AP のデータ レート。
オプション レート（Optional Rates）	APがサポートし、ステーションにとってオプションで動作するAPのデータ レート。
サポート対象 VHT(rx) レート	AP から受け取った VHT 対応 RX MCS Set。
サポート対象 VHT(tx) レート	AP から受け取った VHT 対応 TX MCS Set。
サポートされる HT MCS	AP から受け取った VHT 対応 MCS Set。
DTIM 期間（DTIM Period）	すべての nth ビーコンが DTIM 時間です。 各 DTIM ビーコン後に、APは、電力節約デバイスに対してキューに入っているブロードキャスト パケットまたはマルチキャスト パケットを送信します。
国番号	2 桁の国番号。 国情報要素（IE）がビーコン内に存在しない場合は表示されません。
チャネル	（国 IE で）サポートされているチャネルのリスト。
電力制限（Power Constraint）	規制区域の制限から最大伝送パワーが減らされる電力量。
電力上限（Power Limit）	そのチャネルに許容される dBm での最大送信電力。
チャネルの使用率	AP によって検知されたメディアがビジーである、255 に正規化された時間の割合。物理または仮想キャリア検知（CS）メカニズムによって示されます。
ステーション数（Station Count）	この AP に現在関連付けられている STA の総数。

項目	説明
アドミッションキャパシティ（Admission Capacity）	明示的なアドミッション コントロールを通じて使用可能なメディアの残り時間を指定する符号なし整数（32 マイクロ秒/秒の単位）。 値が 0 の場合、AP はこの情報要素をサポートせず、キャパシティはわかりません。
WMMサポート済み（WMM Supported）	Wi-Fi マルチメディア エクステンションのサポート。
UAPSD サポート済み（UAPSD Supported）	AP は Unscheduled Automatic Power Save Delivery をサポートします。 WMM がサポートされている場合だけ使用可能です。 この機能はワイヤレス IP 電話での通話時間と最大コール密度の達成にとって重要です。
プロキシ ARP	CCX 準拠 AP は、関連ステーションに代わって IP ARP 要求に対して応答します。 この機能は、ワイヤレス IP 電話のスタンバイ時間にとって重要です。
CCX バージョン（CCX Version）	AP が CCX 準拠の場合、このフィールドは CCX バージョンを表示します。
ベスト エフォート	ベスト エフォート キューに関連した情報が記載されています。
背景	バックグラウンド キューに関連した情報が記載されています。
ビデオ	ビデオ キューに関連した情報が記載されています。
音声	音声キューに関連した情報が記載されています。

Cisco IP 電話の Web ページ

Cisco IP 電話 には、それぞれ Web ページがあります。この Web ページで、電話機に関する次のような情報を表示できます。

- [デバイス情報（Device Information）]：電話機のデバイスの設定および関連情報を表示します。
- [ネットワークのセットアップ（Network Setup）]：ネットワークのセットアップ情報およびその他の電話設定に関する情報を表示します。
- [ネットワーク統計情報（Network statistics）]：ネットワーク トラフィックに関する情報を提供するハイパーリンクを表示します。
- [デバイス ログ（Device Logs）]：トラブルシューティングに利用できる情報を提供する次のハイパーリンクを表示します。
- [ストリームの統計（Streaming Statistic）]：さまざまなストリーミング統計情報を表示するハイパーリンクを示します。

• [システム（System）]：電話機を再起動するためのハイパーリンクを示します。

この項では、電話機の Web ページから取得可能な情報について説明します。 この情報は、電話機の操作のリモート モニタやトラブルシューティングに役立てることができます。

また、この情報の多くは、電話機から直接取得することもできます。

電話機の Web ページへのアクセス

電話機の Web ページにアクセスするには、次の手順を実行します。

（注） Webページにアクセスできない場合は、デフォルトでアクセスが無効になっている可能性があります。

手順

ステップ 1 次の方法のいずれかを使用して、Cisco IP 電話の IP アドレスを入手します。

a) Cisco Unified Communications Manager の管理で **[デバイス（Device）]** > **[電話（Phone）]** の順に選択して、電話機を検索します。 Cisco Unified Communications Manager に登録されている電話機の IP アドレスが、[Find and List Phones] ウィンドウと [Phone Configuration] ウィンドウの上部に表示されます。

b) Cisco IP 電話でアプリケーション を押し、**[管理者設定（Admin settings）]**>**[ネットワークのセットアップ（Network setup）]**>**[イーサネットのセットアップ（Ethernet setup）]**>**[IPv4のセットアップ（IPv4 Setup）]** を選択して、[IPアドレス（IP Address）] フィールドまでスクロールします。

ステップ 2 Web ブラウザを開いて、次の URL を入力します。ここで、*IP_address* は Cisco IP 電話の IP アドレスです。

http://*IP_address*

デバイス情報

電話機の Web ページの [デバイス情報（Device Information）] エリアには、電話機のデバイス設定と関連情報が表示されます。 次の表に、これらの項目を示します。

（注） 次の表にリストしている一部の項目は、すべての電話機モデルに適用されません。

[デバイス情報（Device Information）] 領域を表示するには、電話機の Web ページへのアクセス（271 ページ） の説明に従って、電話機の Web ページにアクセスしてから、[デバイス情報（Device Information）] ハイパーリンクをクリックします。

表 *48 : [*デバイス情報（*Device Information*）*]* 領域の項目

項目	説明
Service mode	電話機のサービス モード。
サービス名	サービスのドメイン。
サービスの状態（Service state）	サービスの現在の状態。
MAC Address	電話機のメディア アクセス コントロール（MAC）アドレス。
ホスト名	電話機の MAC アドレスに基づいて電話機に自動的に割り当てられる一意の固定された名前。
電話機の電話番号	電話機に割り当てられている電話番号。
[アプリケーション ロード ID（App load ID）]	電話機で実行されているアプリケーションのファームウェア バージョン。
[起動ロード ID（Boot load ID）]	起動ファームウェア バージョン。
バージョン	電話機で作動しているファームウェアの ID。
[キー拡張モジュール 1（Key expansion module 1）]	該当する場合、最初のキー拡張モジュールの ID。 Cisco IP 電話 8851、8851NR、8861、8865、8865NR に適用可能。
[キー拡張モジュール 2（Key expansion module 2）]	該当する場合、第 2 のキー拡張モジュールの ID。 Cisco IP 電話 8851、8851NR、8861、8865、8865NR に適用可能。
[キー拡張モジュール 3（Key expansion module 3）]	該当する場合、第 3 のキー拡張モジュールの ID。 Cisco IP 電話 8851、8851NR、8861、8865、8865NR に適用可能。
[ハードウェア リビジョン（Hardware revision）]	電話機のハードウェアのマイナーリビジョン値。
[シリアル番号（Serial number）]	電話機の固有のシリアル番号。

項目	説明
モデル番号	電話機のモデル番号。
メッセージ受信	この電話機のプライマリ回線で受信したボイスメッセージがあるかどうかを示します。
UDI	電話機に関する次の Cisco Unique Device Identifier（UDI）情報を表示します。 • [デバイス タイプ（Device type）]：ハードウェア タイプを示します。たとえば、すべての電話モデルに対して「電話機」が表示されます。 • [デバイスの説明（Device description）]：示されたモデル タイプに関連付けられている電話機の名前を表示します。 • [製品 ID（Product identifier）]：電話のモデルを指定します。 • バージョン ID (VID): 主要なハードウェアバージョン番号を指定します。 • [シリアル番号（Serial number）]：電話機の一意のシリアル番号を表示します。
[キー拡張モジュール UDI（Key Expansion Module UDI）]	キー拡張モジュールの Cisco Unique Device Identifier（UDI）。 Cisco IP 電話 8851、8851NR、8861、8865、8865NR に適用可能。

項目	説明
ヘッドセットの名前	左側のカラムに接続されている Cisco ヘッドセットの名前を表示します。右の列には、次の情報が含まれています。 • [ポート (Port)] : ヘッドセットが電話機に接続する方法を表示します。 • USB • AUX • [バージョン (Version)]: ヘッドセットのファームウェアバージョンが表示されます。 • [無線範囲]: DECT 無線機用に設定された強度を表示します。 シスコ ヘッドセット 560シリーズのみに適用されます。 • [帯域幅 (帯域幅)]: ヘッドセットがワイドバンドまたは狭い帯域を使用する場合)。 シスコ ヘッドセット 560シリーズのみに適用されます。 • [Bluetooth]: Bluetooth が有効または無効になっている場合に表示されます。 シスコ ヘッドセット 560シリーズのみに適用されます。 • [会議]: 会議機能が有効または無効になっている場合に表示されます。シスコ ヘッドセット 560シリーズのみに適用されます。 • ファームウェアソース: 許可されているファームウェアのアップグレード方法を表示します。 • UCM のみに制限 • UCM または Cisco Cloud から許可する シスコ ヘッドセット 560シリーズのみに適用されます。
時刻	電話機が属する日時グループの時間。 この情報は、Cisco Unified Communications Manager から取得されます。
タイム ゾーン	電話機が属する日時グループのタイム ゾーン。 この情報は、Cisco Unified Communications Manager から取得されます。
日付（Date）	電話機が属する日時グループの日付。 この情報は、Cisco Unified Communications Manager から取得されます。
[システム空きメモリ（System Free Memory）]	電話機の未使用メモリの量
[Java ヒープ空きメモリ（Java heap free memory）]	Java の内部ヒープ メモリの空き領域の容量

項目	説明
[Java プール空きメモリ（Java pool free memory）]	Java の内部プール メモリの空き領域の容量
[FIPS モード有効（FIPS Mode Enabled）]	連邦情報処理標準（FIPS）モードが有効かどうかを示します。

ネットワークのセットアップ

電話機の Web ページにある [ネットワークのセットアップ（Network Setup）] エリアには、ネットワークの設定情報と電話機のその他の設定に関する情報が表示されます。 次の表に、これらの項目を示します。

これらの項目の多くは、Cisco IP 電話の [ネットワークのセットアップ（Network Setup）] メニューで表示し、設定できます。

（注） 次の表にリストしている一部の項目は、すべての電話機モデルに適用されません。

[ネットワークのセットアップ（Network Setup）] 領域を表示するには、電話機の Web ページへのアクセス （271 ページ） の説明に従って電話機の Web ページにアクセスし、次に [ネットワークのセットアップ（Network Setup）] ハイパーリンクをクリックします。

表 *49 : [ネットワークのセットアップ（Network Setup）] 領域の項目*

項目	説明
MAC アドレス	電話機のメディア アクセス コントロール（MAC）アドレス。
ホスト名	DHCP サーバが電話機に割り当てたホスト名。
ドメイン名（Domain Name）	電話機が所属するドメイン ネーム システム（DNS）ドメインの名前。
[DHCP サーバ（DHCP server）]	電話機の IP アドレス取得元となる Dynamic Host Configuration Protocol（DHCP アドレス。
[BOOTP サーバ（BOOTP server）]	電話機が設定をブートストラップ プロトコル（BootP）サーバから取得するか ます。
DHCP	電話機が DHCP を使用するかどうかを示します。
IP アドレス(IP address)	電話機のインターネット プロトコル（IPv4）アドレス。

項目	説明
サブネット マスク（Subnet mask）	電話機で使用されるサブネットマスク。
[デフォルト ルータ（Default router）]	電話機で使用される、デフォルト ルータ。
DNS サーバ 1～3	電話機で使用されるプライマリ DNS サーバ（[DNS サーバ 1（DNS Server 1）]） ションのバックアップ DNS サーバ（[DNS サーバ 2（DNS Server 2）] ～ [DNS サー Server 3）]）。
代替 TFTP（Alternate TFTP）	電話機が代替 TFTP サーバを使用しているかどうかを示します。
TFTP サーバ 1（TFTP Server 1）	電話機で使用される、プライマリの Trivial File Transfer Protocol（TFTP）サーバ。
TFTP サーバ 2	電話機で使用される、バックアップの Trivial File Transfer Protocol（TFTP）サー
[DHCP アドレス解放（DHCP address released）]	電話機の [ネットワークの設定（Network Configuration）] メニューの [DHCP ア （DHCP address Released）] オプションの設定を示します。
接続先 VLAN ID（Operational VLAN ID）	電話機が所属する、Cisco Catalyst スイッチに設定された接続先 Virtual Local Area (VLAN)。
[管理 VLAN ID（Admin VLAN ID）]	電話機がメンバーになっている補助 VLAN。

項目	説明
CUCM サーバ 1 ～ 5（CUCM server 1 ～ 5）	電話機を登録可能な Cisco Unified Communications Manager サーバのホスト名 レス（優先度順）。 限定された Cisco Unified Communications Manager 機能を SRST ルータが使用可能な場合、項目にそのルータの IP アドレスが表示される す。 使用可能なサーバについては、この項目に Cisco Unified Communications Mana IP アドレスと、次の状態のいずれかが表示されます。 • [アクティブ（Active）]：現在、この電話機に対してコール処理サービス る Cisco Unified Communications Manager サーバです。 • [スタンバイ（Standby）]：現在のサーバが使用不能になった場合に、この 替え先とする Cisco Unified Communications Manager サーバです。 • ブランク：現在、この Cisco Unified Communications Manager サーバへの接 ん。 項目には、Survivable Remote Site Telephony（SRST）指定も含めることができま 限定された Cisco Unified Communications Manager 機能を提供できる SRST ルー す。 このルータは、他のすべての Cisco Unified Communications Manager サー になった場合に、コールの処理を引き継ぎます。 SRST Cisco Unified Communi は、アクティブであっても、常にサーバのリストの最後尾に表示されます。 アドレスは、[Cisco Unified CM の設定（Cisco Unified Communications Manager C ウィンドウの [デバイス プール（Device Pool）] セクションで設定します。
情報 URL	電話機に表示されるヘルプ テキストの URL。
ディレクトリ URL（Directories URL）	電話機がディレクトリ情報を取得するサーバの URL。
メッセージ URL（Messages URL）	電話機でメッセージ サービスの取得元となるサーバの URL。
Services URL	電話機が Cisco Unified IP 電話サービスを取得するサーバの URL。
アイドル URL（Idle URL）	電話機が [URLのアイドル時間（Idle URL Time）] フィールドで指定された時 使用されず、メニューが開かれていない場合に表示される URL。
[URL のアイドル時間（Idle URL time）]	電話機がアイドル状態で、いかなるメニューも開かれない時間（秒数）であり 経過後、[アイドルURL（Idle URL）] で指定した XML サービスがアクティブ
[プロキシ サーバ URL（Proxy server URL）]	電話機の HTTP クライアントの代わりにローカル以外のホスト アドレスに H 信し、ローカル以外のホストから電話機の HTTP クライアントへの応答を提供 サーバの URL。
認証 URL（Authentication URL）	電話機の Web サーバに発行された要求を検証するために、電話機が使用する

項目	説明
SWポートのセットアップ（SW port setup）	スイッチ ポートの速度とデュプレックス。次のいずれかになります。 • [A]：自動ネゴシエーション • [10H]：10-BaseT/半二重 • [10F]：10-BaseT/全二重 • [100H]：100-BaseT/半二重 • [100F]：100-BaseT/全二重 • [1000F]：1000-BaseT/全二重 • [リンクがありません（No Link）]：スイッチ ポートへの接続がありません。
PCポートのセットアップ（PC port setup）	PC ポートの速度およびデュプレックス モード。次のいずれかになります。 • [A]：自動ネゴシエーション • [10H]：10-BaseT/半二重 • [10F]：10-BaseT/全二重 • [100H]：100-BaseT/半二重 • [100F]：100-BaseT/全二重 • [1000F]：1000-BaseT/全二重 • [リンクがありません（No Link）]：PC ポートへの接続がありません。
PCポートを無効にする（PC port disabled）	電話機の PC ポートがイネーブルかディセーブルかを示します。
ユーザ ロケール	電話機のユーザに関連付けられているユーザ ロケール。 言語、フォント、日付式、および英数字キーボードのテキスト情報など、ユーザをサポートするための情報を示します。
ネットワーク ロケール	電話機のユーザに関連付けられているネットワーク ロケール。 電話機が使用す断続周期の定義など、特定の場所にある電話機をサポートするための一連の詳細ます。
[ユーザ ロケール バージョン（User locale version）]	電話機にロードされたユーザ ロケールのバージョン。
[ネットワーク ロケール バージョン（Network locale version）]	電話機にロードされたネットワーク ロケールのバージョン。
[スピーカーを使う（Speaker enabled）]	電話機のスピーカーフォンが有効になっているかどうかを示します。
[GARP を使う（GARP enabled）]	電話機が Gratuitous ARP 応答から MAC アドレスを取得するかどうかを示します

項目	説明
PC ポートへのスパン（Span to PC port）	ネットワーク ポートで送受信されるパケットをアクセス ポートに転送するか します。
ビデオ機能を使う（Video capability enabled）	適切に準備されたカメラに接続されたときに、電話機がビデオ コールに参加 かを示します。
ボイス VLAN を使う（Voice VLAN enabled）	電話機が、PC ポートに接続されたデバイスに、ボイス VLAN へのアクセスを うかを示します。
PC VLAN を使う（PC VLAN enabled）	PC に送信されたパケットから 802.1P/Q タグを識別し、削除する VLAN。
[自動回線選択を使う（Auto line select enabled）]	電話機がオフフックになる際に、電話が自動的に回線を選択するかどうかを
DSCP プロトコル制御（DSCP protocol control）	コール制御シグナリングの DSCP IP 分類。
[設定の DSCP（DSCP for configuration）]	電話機の設定転送の DSCP IP 分類。
[サービスの DSCP（DSCP for services）]	電話機ベースのサービスの DSCP IP 分類。
セキュリティ モード（非セキュア）（Security mode (nonsecure)）	電話機に設定されているセキュリティ モード。
Web アクセス可能（Web access enabled）	電話機の Web アクセスが有効（[はい（Yes）]）か無効（[いいえ（No）]）か
[SSH アクセス有効（SSH access enabled）]	SSH ポートが有効になっているか無効になっているかを示します。

項目	説明
CDP：SW ポート（CDP: SW Port）	スイッチポートでCDPがサポートされているかどうかを示します（デフォルトで 電話機、電力ネゴシエーション、QoS 管理、および 802.1x セキュリティに VLA てる場合は、スイッチ ポートで CDP を有効にします。 電話機を Cisco スイッチに接続した場合は、スイッチ ポートで CDP を有効にし CDP が Cisco Unified Communications Manager で無効になっているときは、電話機 イッチ以外のスイッチに接続した場合に限り、スイッチ ポートで CDP を無効に あることを示す警告が表示されます。 PC ポートとスイッチ ポートの CDP に関する現在の値は、[設定（Settings）] メ 示されます。
[CDP：PC ポート（CDP: PC Port）]	PC ポートで CDP がサポートされているかどうかを示します（デフォルトでは有 Cisco Unified Communications Manager で CDP が無効になっている場合は、PC ポ を無効にすると CVTA が動作しなくなることを示す警告が表示されます。 PC ポートとスイッチ ポートの CDP に関する現在の値は、[設定（Settings）] メ 示されます。
LLDP-MED：SW ポート（LLDP-MED:SW Port）	スイッチ ポートで Link Layer Discovery Protocol Media Endpoint Discovery（LLDP 有効になっているかどうかを示します。
LLDP-MED：PC ポート（LLDP-MED:PC Port）	LLDP-MED が PC ポートで有効かどうかを示します。
LLDP 電力の優先順位（LLDP Power Priority）	電話機の電源優先度をスイッチに割り当て、スイッチが電力を適切に電話機に供 うにします。 次の設定があります。 • 不明（Unknown）：これがデフォルト値です。 • 低 • 高 • クリティカル（Critical）
LLDP Asset ID	在庫管理のため電話機に割り当てられているアセット ID。
CTL ファイル	CTL ファイルの MD5 ハッシュ。
[ITL ファイル（ITL File）]	ITL ファイルには最初の信頼リストが含まれます。
[ITL 署名（ITL signature）]	ITL ファイルの MD5 ハッシュ
[CAPF サーバ（CAPF server）]	使用中の CAPF サーバ

項目	説明
TVS	デフォルト セキュリティの主要コンポーネント。 Cisco Unified IP 電話 は Tru Services（TVS）を使用して、HTTPS 確立時に EM サービス、ディレクトリ、アプリケーション サーバを認証できます。
TFTP サーバ（TFTP server）	電話機で使用される TFTP サーバの名前。
TFTP サーバ（TFTP server）	電話機で使用される TFTP サーバの名前。
自動ポート同期	パケット損失をなくすために、電話が自動的にポート速度を同期するとかどす。
スイッチ ポートのリモート設定（Switch port remote configuration）	SW ポートがリモートで制御されるかどうかを示します。
PC ポートのリモート設定（PC port remote configuration）	PC ポートがリモートで制御されるかどうかを示します。
IP アドレッシング モード	アドレッシング モードを指定します。 • IPv4 のみ • IPv4 と IPv6 • IPv6 のみ
IP preference mode control	電話機で IPv4 と IPv6 の両方が使用できる場合、電話機が Cisco Unified Comm Manager とのシグナリング中に使用する IP アドレスのバージョンを示します
[メディアの IP 設定モード（IP preference mode for media）]	
[IPv6 自動設定（IPv6 auto configuration）]	メディアに関してデバイスが IPv4 アドレスを使用して Cisco Unified Communic に接続することを示します。
IPv6 重複アドレスの保護（IPv6 duplicate address protection）	
IPv6 accept redirect message	宛先番号に使用されている同じルータからのリダイレクト メッセージを電話るかどうかを示します。
IPv6 reply multicast echo request	IPv6 専用アドレスに送信されるエコー要求メッセージへの応答として電話機メッセージを送信することを示します。

項目	説明
IPv6 負荷サーバ	各電話機のアップグレードでWANリンクを通過する必要がないように、イメールに保存することによって、電話機ファームウェアのアップグレードのためのイ時間を最適化し、WAN の負荷を軽減するために使用されます。
IPv6 ログ サーバ	
IPv6 CAPF サーバ	電話機からのログ メッセージの送信先になるリモート ログ マシンの IP アドレスを示します。
DHCPv6	電話機で IPv6 専用アドレスを取得するために使用する方法を示します。 DHCPv6 が有効の場合、電話機は IPv6 対応ルータによって送信された RA によからまたは DHCPv6 サーバから IPv6 アドレスを取得します。 DHCPv6 が無効の機がステートフル（DHCPv6 サーバからの）またはステートレス（SLAAC から）ドレスを持つことはありません。 （注） DHCPv4 とは異なり、DHCPv6 が無効の場合でも、自動設定が有効にれば電話機が SLAAC アドレスを生成できます。
IPv6 アドレス	電話機の現在の IPv6 専用アドレスを表示します。 次の 2 種類のアドレス形式がサポートされます。 • コロンによって区切られた、8 グループの 16 進数 X:X:X:X:X:X:X:X • 圧縮形式では、ゼロ グループが連続する 1 箇所を二重コロンに短縮して表し
IPv6 プレフィックス長	サブネットの現在の IPv6 専用プレフィックス長を表示します。
IPv6 デフォルト ルータ	電話機で使用されるデフォルトの IPv6 ルータが表示されます。
IPv6 DNS サーバ 1 ～ 2	電話機が使用するプライマリ DNSv6 サーバとセカンダリ DNSv6 サーバを表示し
IPv6 代替 TFTP（IPv6 Alternate TFTP）	代替 IPv6 TFTP サーバを使用するかどうかを表示されます。
IPv6 TFTP サーバ 1 ～ 2（IPv6 TFTP server 1–2）	電話機が使用するプライマリおよびセカンダリ IPv6 TFTP サーバを表示します。
IPv6 アドレス解放	ユーザが IPv6 関連の情報を解放したかどうかが表示されます。
EnergyWise 電力レベル（EnergyWise power level）	電話機がスリープ状態の場合に使用される電力レベル。
EnergyWise ドメイン（EnergyWise domain）	その電話機が含まれる EnergyWise ドメイン。

項目	説明
[DF_BIT]	パケットの DF ビット設定を表示します。

ネットワーク統計（Network Statistics）

電話機の Web ページにある次のネットワーク統計ハイパーリンクには、電話機のネットワーク トラフィックに関する情報が表示されます。

- [イーサネット情報（Ethernet Information）]：イーサネット トラフィックに関する情報を表示します。
- [アクセス（Access）]：電話機の PC ポートとの間で送受信されるネットワーク トラフィックに関する情報を表示します。
- [ネットワーク（Network）]：電話機のネットワーク ポートとの間で送受信されるネットワーク トラフィックに関する情報を表示します。

ネットワーク統計領域を表示するには、電話機の Web ページにアクセスして、[イーサネット情報（EthernetInformation）]、[アクセス（Access）]、または[ネットワーク（Network）]ハイパーリンクをクリックします。

[イーサネット情報（Ethernet Information）] Web ページ

次の表では、[イーサネット情報（Ethernet Information）] Web ページの内容について説明しています。

表 *50 : [イーサネット情報（Ethernet Information）]* の項目

項目	説明
Tx フレーム（Tx Frames）	電話機が送信するパケットの総数。
Tx ブロードキャスト	電話機が送信するブロードキャスト パケットの総数。
Tx マルチキャスト	電話機が送信するマルチキャスト パケットの総数。
Tx ユニキャスト	電話機が送信するユニキャスト パケットの総数。
Rx フレーム	電話機が受信したパケットの総数。
Rx ブロードキャスト	電話機が受信するブロードキャスト パケットの総数。
Rx マルチキャスト	電話機が受信するマルチキャスト パケットの総数。
Rx ユニキャスト	電話機が受信するユニキャスト パケットの総数。

項目	説明
Rx PacketNoDes	ダイレクト メモリ アクセス（DMA）記述子がないため廃棄されたパケットの総数。

[アクセスおよびネットワーク（Access and Network）] の Web ページ

次の表に [アクセスおよびネットワーク（Access and Network）] の Web ページの情報を示します。

表 *51 : [アクセスおよびネットワーク（Access and Network）] のフィールド*

項目	説明
Rx totalPkt	電話機が受信したパケットの合計数。
Rx crcErr	CRC が失敗した、受信されたパケットの合計数。
Rx alignErr	フレーム チェック シーケンス（FCS）が無効であり、長さが 64 ～ 1522 バイトの受信されたパケットの合計数。
Rx マルチキャスト	電話機が受信したマルチキャスト パケットの合計数。
Rx ブロードキャスト	電話機が受信したブロードキャスト パケットの合計数。
Rx ユニキャスト	電話機が受信したユニキャスト パケットの合計数。
Rx shortErr	サイズが 64 バイトより小さい、受信された FCS エラー パケットまたは Align エラー パケットの合計数。
Rx shortGood	サイズが 64 バイトより小さい、受信された有効なパケットの合計数。
Rx longGood	サイズが 1522 バイトより大きい、受信された有効なパケットの合計数。
Rx longErr	サイズが 1522 バイトより大きい、受信された FCS エラー パケットまたは Align エラー パケットの合計数。
Rx size64	無効なパケットを含め、サイズが 0 ～ 64 バイトまでの受信されたパケットの合計数。
Rx size65to127	無効なパケットを含め、サイズが 65 ～ 127 バイトまでの受信されたパケットの合計数。
Rx size128to255	無効なパケットを含め、サイズが 128 ～ 255 バイトまでの受信されたパケットの合計数。
Rx size256to511	無効なパケットを含め、サイズが 256 ～ 511 バイトまでの受信されたパケットの合計数。

項目	説明
Rx size512to1023	無効なパケットを含め、サイズが 512 ～ 1023 バイトまでの受信されたパケットの合計数。
Rx size1024to1518	無効なパケットを含め、サイズが 1024 ～ 1518 バイトまでの受信されたパケットの合計数。
Rx tokenDrop	リソース不足（FIFO オーバーフローなど）が原因でドロップされたパケットの合計数。
Tx excessDefer	メディアが使用中であることが原因で送信が遅延したパケットの合計数。
Tx lateCollision	パケット転送の開始後 512 ビット時間過ぎてから衝突が起こった回数。
Tx totalGoodPkt	電話機が受信した有効なパケット（マルチキャスト、ブロードキャスト、およびユニキャスト）の合計数。
Tx Collisions	パケットの送信中に生じた衝突の合計回数。
Tx excessLength	パケット送信が 16 回試行されたために送信されなかったパケットの合計数。
Tx ブロードキャスト	電話機が送信したブロードキャスト パケットの合計数。
Tx マルチキャスト	電話機が送信したマルチキャスト パケットの合計数。
LLDP FramesOutTotal	電話機から送信された LLDP フレームの合計数。
LLDP AgeoutsTotal	キャッシュ内でタイムアウトになった LLDP フレームの合計数。
LLDP FramesDiscardedTotal	必須 TLV のいずれかについて、欠落している、順序に誤りがある、または範囲を超える文字列長が含まれているために廃棄された LLDP フレームの合計数。
LLDP FramesInErrorsTotal	検出可能なエラーが 1 つ以上含まれる状態で受信された LLDP フレームの合計数。
LLDP FramesInTotal	電話機が受信した LLDP フレームの合計数。
LLDP TLVDiscardedTotal	破棄された LLDP TLV の総数。
LLDP TLVUnrecognizedTotal	電話機で認識されなかった LLDP TLV の総数。
CDP ネイバー デバイス ID	CDP で検出されたこのポートに接続されているデバイスの ID。
CDP ネイバー IPv6 アドレス（CDP Neighbor IPv6 address）	CDP プロトコルで検出されたネイバー デバイスの IP アドレス。

項目	説明
CDP ネイバー ポート	CDP プロトコルで検出された、電話機が接続されているネイバー デバイスのポート。
LLDP ネイバー デバイス ID	LLDP で検出された、このポートに接続されているデバイスの ID。
LLDP ネイバー IPv6 アドレス（LLDP Neighbor IPv6 address）	LLDP プロトコルで検出されたネイバー デバイスの IP アドレス。
LLDP ネイバー ポート	LLDP プロトコルで検出された、電話機が接続されているネイバー デバイスのポート。
ポート情報	速度とデュプレックス モード。

デバイス ログ

電話機の Web ページにある次のデバイス ログのハイパーリンクには、電話機のモニタとトラブルシューティングに役立つ情報が表示されます。

- [コンソールログ（Console Logs）]：個々のログ ファイルへのハイパーリンクが含まれています。 コンソール ログ ファイルには、電話機が受信したデバッグ メッセージとエラー メッセージが含まれます。
- [コアダンプ（Core Dumps）]：個々のダンプ ファイルへのハイパーリンクが含まれています。 コア ダンプ ファイルには、電話のクラッシュ時のデータが含まれています。
- [ステータスメッセージ（Status Messages）]：電話機に最後に電源が投入されてから電話機が生成したステータス メッセージの中で最近のものを最大 10 件表示します。 電話機の [ステータス メッセージ（Status Messages）] 画面にも、この情報が表示されます。
- [デバッグの表示（Debug Display）]：トラブルシューティングのサポートを依頼する際に、Cisco TAC に有用なデバッグ メッセージを提供します。

ストリームの統計

Cisco Unified IP 電話は、同時に最大で 3 つのデバイスとの間で情報をストリーミングできます。 電話機は、コール中、または音声やデータの送受信サービスの作動中に、情報をストリーミングします。

電話機の Web ページにある [ストリームの統計（Streaming Statistics）] 領域には、ストリームに関する情報が表示されます。

次の表に、[ストリームの統計（Streaming Statistics）] 領域の項目を示します。

表 *52 : [*ストリームの統計（***Streaming Statistics***）*]* 領域の項目

項目	説明
Remote address	ストリームの宛先の IP アドレスおよび UDP ポート。
[ローカルアドレス（Local address）]	電話機の IP アドレスおよび UPD ポート。
開始時刻	Cisco Unified Communications Manager が電話機にパケットの送信開始を要 を示す内部タイム スタンプ。
[ストリームステータス（Stream Status）]	ストリーミングがアクティブかどうかを示します。
ホスト名	電話機の MAC アドレスに基づいて電話機に自動的に割り当てられる一意 た名前。
[送信パケット（Sender Packets）]	この接続の開始以降に電話機が送信した RTP データ パケットの総数。 接 用モードに設定されている場合、値は 0 です。
[送信オクテット（Sender Octets）]	この接続の開始以降に電話が RTP データ パケットで送信したペイロード の総数。 接続が受信専用モードに設定されている場合、値は 0 です。
[送信コーデック（Sender Codec）]	送信ストリームに対応する音声符号化のタイプ。
[送信した送信レポート（Sender Reports Sent）] （注を参照）	RTCP 送信レポートが送信された回数。
[送信した送信レポート時間（Sender Report Time Sent）] （注を参照）	最後に RTCP 送信レポートが送信された時間を示す内部タイム スタンプ
[受信喪失パケット（Rcvr Lost Packets）]	この接続でのデータの受信を開始してから失われた RTP データ パケット 期されたパケット数から実際に受信されたパケット数を差し引いた値と れます。受信パケット数には、遅延または重複パケットも含まれます。 専用モードに設定されていた場合、値は 0 として表示されます。
[平均ジッター（Avg Jitter）]	RTP データ パケットの内部到着時間の平均偏差の推定値（ミリ秒単位） 信専用モードに設定されていた場合、値は 0 として表示されます。
[受信コーデック（Receiver Codec）]	受信ストリームに使用された音声符号化のタイプ。

項目	説明
[送信した受信レポート（Receiver Reports Sent）] （注を参照）	RTCP 受信レポートが送信された回数。
[送信した受信レポート時間（Receiver Report Time Sent）] （注を参照）	RTCP 受信レポートが送信された時間を示す内部タイム スタンプ。
[受信パケット（Rcvr Packets）]	この接続でのデータ受信開始以降に電話機が受信した RTP データ パケット マルチキャスト コールの場合は、さまざまな送信元から受信したパケット ます。 接続が送信専用モードに設定されていた場合、値は 0 として表示さ
[受信オクテット（Rcvr octets）]	この接続でのデータ受信開始以降にデバイスが RTP データ パケットで受信 ロード オクテットの総数。 マルチキャスト コールの場合は、さまざまな送 受信したパケットが含まれます。 接続が送信専用モードに設定されていた は 0 として表示されます。
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 で、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 の先行 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 細については、音声品質のモニタリング （321 ページ） を参照してくださ （注） MOS LQK スコアは、Cisco Unified IP 電話が使用するコーデック に基づいて変化する可能性があります。
平均 MOS LQK（Avg 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（Min 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。
最大 MOS LQK（Max MOS LQK）	音声ストリームの開始以降に測定されたベースライン MOS LQK スコアまた い MOS LQK スコア。 これらのコーデックは、フレーム損失なしの通常の条件で次の最大 MOS LQ を提供します。 • G.711 のスコア：4.5。 • G.729 A /AB のスコア：3.7。
[MOS LQK のバージョン（MOS LQK Version）]	MOS LQK 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 ン。
Cumulative conceal ratio	隠蔽フレームの総数を、音声ストリームの開始以降に受信された音声フレ 数で割った値。

項目	説明
直近フレーム損失率（Interval Conceal Ratio）	アクティブな音声の直前の 3 秒間の音声フレームに対する隠蔽フレーム 声アクティビティ検出（VAD）を使用している場合、3秒間のアクティ 積するには、より長い間隔が必要になることがあります。
Max conceal ratio	音声ストリームの開始以降、最も高い間隔の損失率。
[フレーム損失発生秒数（Conceal Secs）]	音声ストリームの開始以降、隠蔽イベント（フレーム損失）があった秒 フレーム損失発生秒数（Severely Conceal Secs）] の値を含む）。
[深刻なフレーム損失発生秒数（Severely Conceal Secs）]	音声ストリームの開始以降、5% を超える隠蔽イベント（フレーム損失） 数。
遅延 （注を参照）	ネットワーク遅延の推定値（ミリ秒単位）。 ラウンドトリップ遅延の実 値を表します。これは、RTCP 受信レポート ブロックの受信時に測定さ
[最大ジッター（Max Jitter）]	瞬時ジッターの最大値（ミリ秒単位）。
[送信サイズ（Sender Size）]	送信ストリームの RTP パケット サイズ（ミリ秒単位）。
[受信した送信レポート（Sender Reports received）] （注を参照）	RTCP 送信レポートが受信された回数。
[受信した送信レポート時間（Sender Report Time received）] （注を参照）	RTCP 送信レポートが最後に受信された時間。
[受信サイズ（Receiver Size）]	受信ストリームの RTP パケット サイズ（ミリ秒単位）。
[受信破棄（Receiver Discarded）]	ネットワークから受信されたが、ジッター バッファから廃棄された RP
[受信した受信レポート（Receiver Reports received）] （注を参照）	RTCP 受信レポートが受信された回数。
[受信した受信レポート時間（Receiver Report Time received）] （注を参照）	RTCP 受信レポートが最後に受信された時間。
[受信暗号化（Rcvr encrypted）]	受信者が暗号化を使用しているかどうかを示します。

項目	説明
[送信暗号化（Sender encrypted）]	送信者が暗号化を使用しているかどうかを示します。
[送信フレーム（Sender frames）]	送信されたフレーム数。
[送信部分フレーム（Sender partial frames）]	送信されたパーシャル フレームの数。
[送信者の i フレーム（Sender i frames）]	送信された I フレームの数。 I フレームは、ビデオ伝送に使用されます。
[送信者の IDR フレーム（Sender IDR frames）]	送信された Instantaneous Decoder Refresh（IDR）フレームの数。 IDR フレーデオ伝送に使用されます。
[送信フレーム レート（Sender frame rate）]	送信者がフレームを送信するレート。
[送信帯域幅（Sender bandwidth）]	送信者の帯域幅。
[送信解像度（Sender resolution）]	送信者のビデオ解像度。
[受信フレーム（Rcvr frames）]	受信されたフレーム数。
[受信部分フレーム（Rcvr partial frames）]	受信された部分フレームの数。
[受信 i フレーム（Rcvr i frames）]	受信された I フレームの数。
[受信 IDR フレーム（Rcvr IDR frames）]	受信された IDR フレームの数。
[受信 I フレーム要求（Rcvr IFrames req）]	受信された要求 IDR フレームの数。
[受信フレーム レート（Rcvr frame rate）]	受信側がフレームを受信するレート。
[受信フレーム損失（Rcvr frames lost）]	受信されなかったフレームの数。
[受信フレーム エラー（Rcvr frame errors）]	受信されなかったフレームの数。

項目	説明
[受信帯域幅（Rcvr bandwidth）]	受信側の帯域幅。
[受信解像度（Rcvr resolution）]	受信者のビデオ解像度。
ドメイン（Domain）	電話機が存在するドメイン。
[送信参加（Sender joins）]	送信者が参加した回数。
[受信参加（Rcvr joins）]	受信者が参加した回数。
BYE（Byes）	「Bye」フレームの数。
[送信開始時間（Sender start time）]	送信者が開始した時刻。
[受信開始時間（Rcvr start time）]	受信者が開始した時刻。
Row status	電話機がストリーミング中かどうか。
[送信ツール（Sender tool）]	ストリームに使用された音声符号化のタイプ。
[送信レポート（Sender reports）]	RTCP 送信者レポート。
[送信レポート時間（Sender report time）]	RTCP 送信レポートが最後に送信された時間。
[受信ジッタ（Tcvr Jitter）]	ストリームの最大ジッタ
[受信ツール（Receiver tool）]	ストリームに使用された音声符号化のタイプ。
[受信レポート（Rcvr reports）]	このストリーミング統計レポートが Web ページからアクセスされた回数
[受信レポート時刻（Rcvr report time）]	ストリーミング統計レポートが生成された時間を示す内部タイムスタン
[ビデオ（Is video）]	コールがビデオ コールまたは音声のみだったかどうかを示します。
コール ID	コールの ID
グループ ID（Group ID）	電話機が属するグループの ID。

（注） RTP制御プロトコルが無効になっている場合、このフィールドのデータは生成されないため、0 が表示されます。

XML での電話からの情報要求

トラブルシューティングの目的で、電話機からの情報を要求できます。 結果の情報はXML形式です。 表示される情報は次のとおりです。

- CallInfo は特定の回線のコール セッション情報です。
- LineInfo は電話機の回線設定情報です。
- ModeInfo は電話モードの情報です。

始める前に

情報を入手するために Web アクセスが有効になっている必要があります。

電話機がユーザに関連付けられている必要があります。

手順

ステップ 1 Call Info については、ブラウザに次の URL を入力します。**http://<phone ip address>/CGI/Java/CallInfo<x>**

値は次のとおりです。

- <*phone ip address*> は、電話の IP アドレスです
- <*x*> は、情報を取得する回線番号です。

コマンドは XML ドキュメントを返します。

ステップ 2 Line Info については、ブラウザに次の URL を入力します。**http://<phone ip address>/CGI/Java/LineInfo**

値は次のとおりです。

- <*phone ip address*> は、電話の IP アドレスです

コマンドは XML ドキュメントを返します。

ステップ 3 Model Info については、ブラウザに次の URL を入力します。**http://<phone ip address>/CGI/Java/ModeInfo**

値は次のとおりです。

- <*phone ip address*> は、電話の IP アドレスです

コマンドは XML ドキュメントを返します。

CallInfo の出力例

次の XML コードは、CallInfo のコマンドの出力例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneCallLineInfo>
  <Prompt/>
  <Notify/>
  <Status/>
  <LineDirNum>1030</LineDirNum>
  <LineState>CONNECTED</LineState>
  <CiscoIPPhoneCallInfo>
     <CallState>CONNECTED</CallState>
     <CallType>INBOUND</CallType>
     <CallingPartyName/>
     <CallingPartyDirNum>9700</CallingPartyDirNum>
     <CalledPartyName/>
     <CalledPartyDirNum>1030</CalledPartyDirNum>
     <HuntPilotName/>
     <CallReference>30303060</CallReference>
     <CallDuration>12835</CallDuration>
     <CallStatus>null</CallStatus>
     <CallSecurity>UNAUTHENTICATED</CallSecurity>
     <CallPrecedence>ROUTINE</CallPrecedence>
     <FeatureList/>
   </CiscoIPPhoneCallInfo>
   <VisibleFeatureList>
     <Feature Position="1" Enabled="true" Label="End Call"/>
     <Feature Position="2" Enabled="true" Label="Show Detail"/>
   </VisibleFeatureList>
</CiscoIPPhoneCallLineInfo>
```

LineInfo の出力例

次の XML コードは LineInfo コマンドからの出力例を示します。

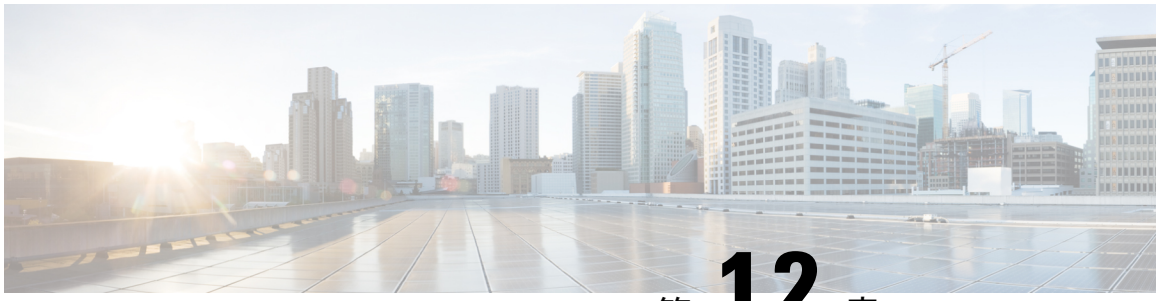
```
<CiscoIPPhoneLineInfo>
   <Prompt/>
   <Notify/>
   <Status>null</Status>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1028</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>
     <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
     <LineType>9</LineType>
     <lineDirNum>1029</lineDirNum>
     <MessageWaiting>NO</MessageWaiting>  <RingerName>Chirp1</RingerName>
     <LineLabel/>
     <LineIconState>ONHOOK</LineIconState>
   </CiscoIPPhoneLines>
   <CiscoIPPhoneLines>
```

```
      <LineType>9</LineType>
      <lineDirNum>1030</lineDirNum>
      <MessageWaiting>NO</MessageWaiting>
      <RingerName>Chirp1</RingerName>
      <LineLabel/>
      <LineIconState>CONNECTED</LineIconState>
    </CiscoIPPhoneLines>
    <CiscoIPPhoneLines>
      <LineType>2</LineType>
      <lineDirNum>9700</lineDirNum>
      <MessageWaiting>NO</MessageWaiting>
      <LineLabel>SD9700</LineLabel>
      <LineIconState>ON</LineIconState>
  </CiscoIPPhoneLines>
</CiscoIPPhoneLineInfo>
```

ModeInfo の出力例

次の XML コードは ModeInfo コマンドからの出力例を示します。

```
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneModeInfo>
   <PlaneTitle>Applications</PlaneTitle>
   <PlaneFieldCount>12</PlaneFieldCount>
   <PlaneSoftKeyIndex>0</PlaneSoftKeyIndex>
   <PlaneSoftKeyMask>0</PlaneSoftKeyMask>
   <Prompt></Prompt>
   <Notify></Notify>
   <Status></Status>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Call History</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   <CiscoIPPhoneFields>
      <FieldType>0</FieldType>
      <FieldAttr></FieldAttr>
      <fieldHelpIndex>0</fieldHelpIndex>
      <FieldName>Preferences</FieldName>
      <FieldValue></FieldValue>
   </CiscoIPPhoneFields>
   ...
</CiscoIPPhoneModeInfo>
```



第 12 章

トラブルシューティング

一般的なトラブルシューティング情報

次の表に、Cisco IP 電話の一般的なトラブルシューティング情報を示します。

表 *53 : Cisco IP* 電話のトラブルシューティング

サマリー	説明
Cisco IP 電話から別の Cisco IP 電話への接続	シスコでは、PC ポートを介した IP 電話間の接続はサポートし各 IP 電話はスイッチ ポートに直接接続する必要があります。ポートを使用して 1 つの回線にまとめて接続されていると、機は動作しません。
長時間のブロードキャスト ストームのために、IP 電話がリセットされたり、コールの発信や応答ができなかったりすることがあります。	ボイス LAN 上の長時間（数分間）にわたるレイヤ 2 ブロートームのために、IP 電話がリセットされたり、アクティブなれたり、コールの発信や応答ができなくなることがあります。スト ストームが終了するまで、電話機が起動しないことがあ

サマリー	説明
ネットワーク接続の電話機からワークステーションへの移行	ネットワーク接続を介して電話機に電力を供給している場合は、ネットワーク接続を外して、そのケーブルをデスクトップ コン接続する際に注意する必要があります。 **注意** コンピュータのネットワーク カードには、ネットワ介して電力を供給できないため、接続を介して電力と、ネットワーク カードが破損する場合があります。ワーク カードを保護するために、電話機からケーブル後、10秒以上待機してから、そのケーブルをコンピ続してください。 この待機している間に、スイッチ回線に存在しなくなったことを認識し、ケーブルへの停止することができます。
電話機の設定変更	デフォルトでは、ネットワーク接続に影響を与える可能性のあるザが加えないように、ネットワーク設定オプションはロックされネットワーク設定オプションを設定する前に、それらをロック要があります。 詳細については、電話機パスワードの適用 （54を参照してください。 （注） 共通の電話機プロファイルに管理者パスワードが設ない場合、ユーザはネットワーク設定を変更できま
電話機と他のデバイスのコーデックの不一致	RxType 統計および TxType 統計に、この Cisco IP 電話 と他のデやり取りに使用されているコーデックが表示されます。 これらの値は、一致している必要があります。 コーデックが一致しな手側のデバイスがコーデック会話を処理できるかどうか、またコーダがサービスを処理するように設置されているかどうかを確
電話機と別のデバイスの音声サンプルの不一致	RxSize 統計および TxSize 統計に、この Cisco IP 電話 と他のデバり取りに使用される音声パケットのサイズが表示されます。 こ情報の値は、一致している必要があります。
ループバック状態	ループバック状態は、次の条件を満たすと発生します。 • 電話機の [ネットワークの設定（Network Configuration）] メ[SW ポート設定（SW Port Configuration）] オプションが [10Half）]（10-BaseT/半二重）に設定されている。 • 電話機に外部電源から電力が供給されている。 • 電話機の電源が切れている（電源装置が接続されていない） この場合、電話機のスイッチ ポートが無効になり、次のメッセーチのコンソール ログに表示されます。 HALF_DUX_COLLISION_EXCEED_THRESHOLD この問題を解決するには、スイッチからポートを再度有効にし

起動時の問題

下の関連項目で説明するとおり、ネットワークに電話機を設置し、Cisco Unified Communications Manager に追加すると、電話機は起動します。

電話機が正しく起動しない場合は、次の各セクションのトラブルシューティング情報を参照してください。

関連トピック

電話機の起動確認 （71 ページ）

Cisco IP 電話が通常の起動プロセスを実行しない

問題

Cisco IP 電話をネットワーク ポートに接続したとき、関連項目で説明されている通常の起動プロセスを電話機が実行せず、電話画面に情報が表示されません。

原因

電話機が起動プロセスを実行しない場合、ケーブル不良、不正な接続、ネットワークの停止、電力の不足、または電話機が機能していないなどの原因が考えられます。

ソリューション

電話機が動作しているかどうかを確認するには、次の推奨事項に従って、考えられる他の問題を排除します。

- ネットワーク ポートが動作していることを確認します。
  - イーサネット ケーブルを、動作することがわかっているケーブルと交換します。
  - 別のポートから正常に動作している Cisco IP 電話を取り外してこのネットワーク ポートに接続し、このポートがアクティブかどうかを確認します。
  - 起動しない Cisco IP 電話を、正常であることがわかっている別のネットワーク ポートに接続します。
  - 起動しない Cisco IP 電話をスイッチのポートに直接接続して、オフィスのパッチ パネル接続を回避します。
- 電話機に電力が供給されていることを確認します。
  - 外部電源を使用している場合は、電気のコンセントが機能していることを確認します。
  - インラインパワーを使用している場合は、代わりに外部電源を使用します。

- 外部電源を使用している場合は、動作することがわかっているユニットに切り替えます。

- 電話機が正常に起動しない場合は、バックアップ ソフトウェア イメージから電話機の電源を入れます。
- これらを試しても、電話機が正常に起動しない場合は、電話機を工場出荷時の状態にリセットします。
- これらの解決策を試みた後、最低 5 分経過しても Cisco IP 電話の電話画面に何も表示されない場合は、シスコのテクニカルサポートの担当者に連絡して、サポートを受けてください。

関連トピック

電話機の起動確認 （71 ページ）

Cisco IP 電話が Cisco Unified Communications Manager に登録されない

電話機が起動プロセスの第1段階（LEDボタンが点滅する）を完了しても、引き続き電話スクリーンにメッセージが表示される場合、電話機は正常に起動していません。 電話機は、イーサネット ネットワークに接続されており、Cisco Unified Communications Manager サーバに登録されていないと、正常に起動できません。

これ以外に、セキュリティ上の問題によって電話機が正常に起動しないこともあります。 詳細については、トラブルシューティング手順 （309 ページ）を参照してください。

電話機にエラー メッセージが表示される

問題

ステータス メッセージには、起動中のエラーが表示されます。

ソリューション

電話機が起動プロセスを繰り返している間は、問題の原因に関する情報を提供するステータス メッセージにアクセスできます。

関連トピック

[ステータス メッセージ（Status Messages）] ウィンドウの表示 （253 ページ）

電話機が TFTP サーバまたは Cisco Unified Communications Manager に接続できない

問題

電話機と、TFTP サーバまたは Cisco Unified Communications Manager の間のネットワークがダウンしている場合は、電話機が正しく起動できません。

ソリューション

現在、ネットワークが作動していることを確認してください。

電話機が TFTP サーバに接続できない

問題

TFTP サーバの設定が正しくない可能性があります。

ソリューション

TFTP 設定を確認します。

関連トピック

TFTP 設定の確認 （310 ページ）

電話機がサーバに接続できない

問題

IP アドレッシングおよびルーティングのフィールドが正しく設定されていない可能性があります。

ソリューション

電話機の IP アドレッシングおよびルーティングの設定を確認する必要があります。 DHCP を使用している場合は、DHCP サーバがこれらの値を提供します。 電話機にスタティック IP アドレスを割り当てている場合は、これらの値を手動で入力する必要があります。

電話機が DNS を使用して接続できない

問題

DNS 設定が誤っている可能性があります。

ソリューション

TFTP サーバまたは Cisco Unified Communications Manager へのアクセスに DNS を使用する場合は、DNS サーバを指定してあることを確認してください。

Cisco Unified Communications Manager および TFTP サービスの未作動

問題

Cisco Unified Communications Manager または TFTP サービスが作動していない場合は、電話機が正常に起動できないことがあります。 このような状況では、システム全体にわたる障害が発生しており、他の電話機やデバイスも正しく起動できない可能性があります。

ソリューション

Cisco Unified Communications Manager サービスが作動していない場合は、コールを確立するためにこのサービスに依存しているネットワーク上のすべてのデバイスが影響を受けます。 TFTP サービスが作動していない場合は、多数のデバイスが正常に起動できません。 詳細については、サービスの開始 （313 ページ） を参照してください。

設定ファイルの破損

問題

この章に記載された他の解決策を試みても解決しない問題が特定の電話機で存続する場合は、設定ファイルが破損している可能性があります。

ソリューション

電話機の新しい設定ファイルを作成します。

Cisco Unified Communications Manager での電話機の登録

問題

電話機が Cisco Unified Communications Manager に登録されていません。

ソリューション

Cisco IP 電話 は、電話機がサーバに追加されている場合、または自動登録が有効になっている場合にのみ、Cisco Unified Communications Manager サーバに登録できます。 電話機の追加方法（79 ページ）の情報と手順を見直して、電話機が Cisco Unified Communications Manager データベースに追加されていることを確認します。

電話機が Cisco Unified Communications Manager データベースに登録されていることを確認するには、Cisco Unified Communications Manager Administration から **[デバイス（Device）]** > **[検索（Find）]** を選択します。 MAC アドレスに基づいて電話機を検索するには、[Find]をクリックします。 MAC アドレスの確認方法については、電話機の MAC アドレスの決定 （79 ページ）を参照してください。

電話機がすでに Cisco Unified Communications Manager データベースに登録されている場合は、設定ファイルが損傷している可能性があります。 解決策については、設定ファイルの破損 （300 ページ）を参照してください。

Cisco IP 電話が IP アドレスを取得できない

問題

電話機が起動時に IP アドレスを取得できない場合は、その電話機が DHCP サーバと同じネットワークまたは VLAN 上に存在しないか、または電話機が接続されている先のスイッチ ポートが無効になっている可能性があります。

ソリューション

電話機が接続されている先のネットワークまたは VLAN が DHCP サーバにアクセスできること、およびスイッチ ポートが有効になっていることを確認します。

電話機が登録されない

問題

電話画面に「アクティベーション コードまたはサービス ドメインを入力（Enter activation code or service domain）」のプロンプトが表示されます。

ソリューション

電話機に TFTP アドレスがありません。 オプション 150 が DHCP サーバによって提供されているか、または代替 TFTP が手動で設定されていることを確認してください。

電話機のリセットの問題

電話機が通話中やアイドル状態のときにリセットされるという報告をユーザから受けた場合は、原因を調査する必要があります。 ネットワーク接続と Cisco Unified Communications Manager の接続が安定している場合は、電話機がリセットされることはありません。

一般的に、電話機がリセットされるのは、ネットワークまたは Cisco Unified Communications Manager への接続に問題がある場合です。

断続的なネットワークの停止によって電話機がリセットされる

問題

ネットワークで断続的な停止が発生している可能性があります。

ソリューション

断続的なネットワークの停止は、データ トラフィックと音声トラフィックにそれぞれ異なる影響を与えます。 ネットワークで断続的な停止が、検出されずに発生している可能性があります。 この場合、データ トラフィックでは喪失パケットを再送信し、パケットが受信および送

信されたことを確認できます。ただし、音声トラフィックでは、喪失パケットを取り戻すことはできません。電話機は、失われたネットワーク接続を再送信するのではなく、ネットワークをリセットして再接続しようとします。音声ネットワークでの既知の問題については、システム管理者にお問い合わせください。

DHCP の設定エラーによって電話機がリセットされる

問題

DHCP 設定が正しくない可能性があります。

ソリューション

電話機が DHCP を使用するように正しく設定されていることを確認します。 DHCP サーバが正しくセットアップされていることを確認します。 DHCP リース期間を確認します。 リース期間を 8 日に設定することを推奨します。

誤ったスタティック IP アドレスによる電話機のリセット

問題

電話機に割り当てられたスタティック IP アドレスが正しくない可能性があります。

ソリューション

電話機にスタティック IP アドレスが割り当てられている場合は、正しい設定値が入力されていることを確認します。

ネットワーク使用量が多いときの電話機のリセット

問題

ネットワーク使用量が多いときに電話機がリセットされるように思われる場合は、ボイス VLAN が設定されていない可能性があります。

ソリューション

電話機を個別の補助 VLAN に分離することで、音声トラフィックの品質が向上します。

意図的なリセットによる電話機のリセット

問題

Cisco Unified Communications Manager へのアクセス権を持つ管理者が 1 人だけではない場合は、他の管理者が意図的に電話機をリセットしていないかどうかを確認する必要があります。

ソリューション

Cisco IP 電話が Cisco Unified Communications Manager からコマンドを受信したかどうかを確認するには、電話機の **[アプリケーション（Applications）]** を押し、**[管理者設定（Admin Settings）]** > **[ステータス（Status）]** > **[ネットワーク統計（Network Statistics）]** の順に選択します。

- [リスタートの原因（Restart Cause）] フィールドに [Reset-Reset]が表示される場合、電話機は Cisco Unified Communications Manager の管理ページからリセット/リセットを受信しています。
- [Restart Cause] フィールドに [Reset-Restart]が表示される場合、電話機は Cisco Unified Communications Manager Administration からリセット/リスタートを受信したために切断されました。

DNS エラーまたは他の接続の問題による電話機のリセット

問題

電話機のリセットが続いており、DNS またはその他の接続の問題が疑われます。

ソリューション

電話機が引き続きリセットされる場合は、DNS または接続の問題の特定 （310 ページ）の手順に従って、DNS またはその他の接続エラーを排除します。

電話機に電源が入らない

問題

電話機に電源が入っているように見えません。

ソリューション

電話機が再起動するのは、ほとんどの場合、外部電源から電源が供給されていたが、その接続が失われて PoE に切り替わったときです。 同様に、PoE を使用して電力が供給されている電話機が外部電源に接続された場合にも、電話機が再起動することがあります。

電話機が LAN に接続できない

問題

LAN への物理的な接続が切断されている可能性があります。

ソリューション

Cisco IP 電話が接続されているイーサネット接続が動作していることを確認します。 たとえば、電話機が接続されている先の特定のポートまたはスイッチがダウンしていないか、またスイッチが再起動中でないかどうかを確認します。また、ケーブルの切断が存在しないことも確認してください。

Cisco IP 電話のセキュリティの問題

ここでは、Cisco IP 電話のセキュリティ機能のトラブルシューティングに関する情報を示します。 これらの問題の任意の解決方法、およびセキュリティに関するトラブルシューティングの詳細情報については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

CTL ファイルの問題

ここでは、CTL ファイルの問題のトラブルシューティングについて説明します。

認証エラー。電話機が CTL ファイルを認証できない

問題

デバイスの認証エラーが発生しました。

原因

CTL ファイルに Cisco Unified Communications Manager の証明書がないか、証明書が不正です。

ソリューション

適切な証明書をインストールします。

電話機が CTL ファイルを認証できない

問題

電話機が CTL ファイルを認証できない。

原因

電話機の CTL ファイル内に、更新された CTL ファイルに署名したセキュリティ トークンがありません。

ソリューション

CTL ファイル内のセキュリティ トークンを変更し、新しいファイルを電話機にインストールします。

CTL ファイルは認証されるが、他の設定ファイルが認証されない

問題

電話機が CTL ファイル以外の設定ファイルを認証できません。

原因

不正な TFTP レコードが存在するか、電話機の信頼リストの対応する証明書によって設定ファイルが署名されていない可能性があります。

ソリューション

TFTP レコード、および信頼リストの証明書を確認します。

ITL ファイルは認証されるが、他の設定ファイルが認証されない

問題

電話機が ITL ファイル以外の設定ファイルを認証できない。

原因

設定ファイルは、電話機の信頼リストの対応する証明書によって署名されていない可能性があります。

ソリューション

正しい証明書を使用してコンフィギュレーション ファイルに再署名します。

TFTP 認証が失敗する

問題

電話機が TFTP 認証の失敗を報告する。

原因

CTL ファイルに電話機の TFTP アドレスがありません。

新しい TFTP レコードを含む新しい CTL ファイルを作成した場合は、電話機上の既存の CTL ファイルには新しい TFTP サーバ用のレコードが含まれない可能性があります。

ソリューション

電話機の CTL ファイルの TFTP アドレス設定を確認します。

電話機が登録されない

問題

電話機が Cisco Unified Communications Manager に登録されない。

原因

CTL ファイルに Cisco Unified Communications Manager サーバ用の正しい情報が含まれていません。

ソリューション

CTL ファイル内の Cisco Unified Communications Manager サーバの情報を変更します。

署名付き設定ファイルが要求されない

問題

電話機が、署名付き設定ファイルを要求しない。

原因

CTL ファイルに証明書付きの TFTP エントリが含まれていません。

ソリューション

証明書付きの TFTP エントリを CTL ファイルに設定します。

ビデオ コールの問題

2 台の Cisco IP Video Phone の間でビデオが表示されない

問題

2 台の Cisco IP Video Phone の間でビデオがストリーミングしません。

ソリューション

メディア ターミネーション ポイント（MTP）がコール フローの中で使用されていないことを確認してください。

ビデオの途切れまたはフレーム落ち

問題

ビデオ コール中に、ビデオがバッファ待ち状態になったり、フレーム落ちしたりします。

ソリューション

画像の品質はコールの帯域幅によって異なります。 ビット レートを上げるとビデオの品質が向上しますが、より多くのネットワーク リソースが必要になります。 ビデオのタイプに最適なビット レートを常に使用してください。 720p、15 フレーム/秒のビデオ コールには 790 kbps 以上のビット レートが必要です。 720p、30 フレーム/秒のビデオ コールには 1360 kbps 以上のビット レートが必要です。

帯域幅については、「電話機の機能および設定」の章の「ビデオ送信解像度のセットアップ」の項を参照してください。

ソリューション

ビデオ コールの最大セッション ビット レートのパラメータが、少なくとも最小ビデオ ビット レートの範囲に設定されていることを確認してください。 Cisco Unified Communications Manager で、**[システム（System）]**>**[リージョン情報（Region Information）]**>**[リージョン（Region）]** に移動します。

ビデオ コールを転送できない

問題

ビデオ コールを自分のデスク フォンからモバイル デバイスに転送できません。

ソリューション

Cisco Unified Mobility は、ビデオ コールには拡張されません。 デスク フォンで受信したビデオ通話を携帯電話で取ることはできません。

電話会議中にビデオがない

問題

2 人以上がコールに加わると、ビデオ コールが音声通話になります。

アドホック ビデオ会議やミートミー ビデオ会議では、ビデオ会議ブリッジを使用する必要があります。

コールに関する一般的な問題

次の各項は、電話のコールに関する一般的な問題のトラブルシューティングに役立ちます。

コールを確立できない

問題

ユーザからコールを発信できないことについての苦情があります。

原因

DHCP IP アドレスが割り当てられていない電話機は、Cisco Unified Communications Manager に登録できません。 LCD画面付きの電話機には、「IPを設定中（Configuring IP）」または「登録（Registering）」というメッセージが表示されます。 LCD 画面のない電話機では、ユーザがコールを発信しようとすると、ハンドセットで（ダイヤル トーンの代わりに）リオーダー音が再生されます。

ソリューション

1. 次のことを確認してください。
    1. イーサネット ケーブルが接続されている。
    2. Cisco CallManager サービスが Cisco Unified Communications Manager サーバで作動している。
    3. 両方の電話機が同じ Cisco Unified Communications Manager に登録されている。
2. 両方の電話機で、オーディオ サーバ デバッグとキャプチャ ログが有効になっています。必要な場合は、Java デバッグを有効にしてください。

電話機が DTMF ディジットを認識しないか、または数字が遅い

問題

ユーザから、キーパッドを使用しているときに数字が消えるか、または遅いという苦情があります。

原因

キーを速く押しすぎると、数字が消えたり、遅くなったりすることがあります。

ソリューション

キーをあまり速く押さないでください。

トラブルシューティング手順

これらの手順を使用すると、問題を識別したり、解決したりすることができます。

Cisco Unified Communications Manager から電話機の問題レポートを作成する

Cisco Unified Communications Manager から電話機の問題レポートを生成することができます。この操作によって、Problem Report Tool (PRT) のソフトキーが電話機で生成するものと同じ情報が得られます。

問題レポートには、電話機とヘッドセットに関する情報が含まれています。

手順

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] で、**[デバイス (Device)]** > **[電話 (Phone)]**を選択します。

ステップ 2 **[検索 (Search)]** をクリックして、1 つまたは複数の Cisco IP 電話を選択します。

ステップ 3 選択した Cisco IP 電話 上で使用されているヘッドセットの PRT ログを収集するには、**[選択対象のPRTを生成する (Generate PRT for Selected)]**をクリックします。

電話機からのコンソールログの作成

電話機がネットワークに接続されず、問題レポートツール (PRT) にアクセスできない場合は、コンソールログを生成します。

始める前に

コンソールケーブルを電話機の背面にある補助ポートに接続します。

手順

ステップ 1 電話機で、**[アプリケーション（Applications）]** を押します。

ステップ 2 [**管理設定** > **AUX ポート**]に移動します。

ステップ 3 **コンソールログ収集 (collect)** を選択して、デバイスログを収集します。

TFTP 設定の確認

手順

ステップ 1 Cisco IP 電話で、アプリケーション ボタン を押し、**[管理者設定（Admin settings）]** > **[ネットワークのセットアップ（Network setup）]** > **[イーサネットのセットアップ（Ethernet setup）]** > **[IPv4のセットアップ（IPv4 setup）]** > **[FTPサーバ1（FTP Server 1）]** を選択します。

ステップ 2 電話機にスタティック IP アドレスを割り当てている場合は、手動で [TFTP サーバ 1（TFTP Server 1）] オプションに設定値を入力する必要があります。

ステップ 3 DHCP を使用している場合は、電話機は TFTP サーバのアドレスを DHCP サーバから取得します。 オプション 150 で、IP アドレスが設定されていることを確認します。

ステップ 4 また、電話機が代替 TFTP サーバを使用できるように設定することもできます。 このような設定は、電話機の場所を最近移動した場合などに特に役立ちます。

ステップ 5 ローカル DHCP が正しい TFTP アドレスを提供しない場合は、電話機で代替 TFTP サーバが使用できるようにします。

これは多くの場合、VPN シナリオで必要です。

DNS または接続の問題の特定

手順

ステップ 1 [Reset Settings] メニューを使用して、電話機をデフォルト値にリセットします。

ステップ 2 次の操作を実行して、DHCP および IP の設定を変更します。

a) DHCP を無効にします。
b) 電話機にスタティック IP 値を割り当てます。 機能している他の電話機で使用しているものと同じデフォルト ルータの設定を使用します。
c) TFTP サーバを割り当てます。 機能している他の電話機で使用しているものと同じ TFTP サーバを使用します。

ステップ 3 Cisco Unified Communications Manager サーバで、正しい IP アドレスにマッピングされている正しい Cisco Unified Communications Manager サーバ名がローカル ホスト ファイルに指定されていることを確認します。

ステップ 4 Cisco Unified Communications Manager から **[システム（System）]** > **[サーバ（Server）]** の順に選択し、サーバが DNS 名ではなく IP アドレスで参照されていることを確認します。

ステップ 5 Cisco Unified Communications Manager から、**[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。 この電話機を検索するには、[Find]をクリックします。 この Cisco IP 電話 に正しい MAC アドレスが割り当てられていることを確認します。

ステップ 6 電話機の電源をオフ/オンにします。

関連トピック

基本的なリセット （317 ページ）
電話機の MAC アドレスの決定 （79 ページ）

DHCP 設定の確認

手順

ステップ 1 電話機で**[アプリケーション（Applications）]** を押します。

ステップ 2 **[Wi-Fi]** > **[Network Setup]** > **[IPv4 Setup]** の順に選択して、次のオプションを確認します。

- [DHCP Server]：電話機にスタティック IP アドレスを割り当てている場合は、[DHCP Server] オプションに値を入力する必要はありません。ただし、DHCP サーバを使用している場合は、このオプションに値が指定されている必要があります。値が見つからない場合は、IP ルーティングおよび VLAN の設定を確認してください。『*Troubleshooting Switch Port and Interface Problems*』を参照してください。このマニュアルは、次の URL から入手できます。

  http://www.cisco.com/en/US/customer/products/hw/switches/ps708/prod_tech_notes_list.html

- [IP Address]、[Subnet Mask]、[Default Router]：電話機にスタティック IP アドレスを割り当てている場合は、これらのオプションの設定値を手動で入力する必要があります。

ステップ 3 DHCP を使用している場合は、DHCP サーバによって配布された IP アドレスを確認してください。

『*Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks*』を参照してください。このマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml

電話機の新しい設定ファイルの作成

Cisco Unified Communications Manager データベースから電話機を削除すると、設定ファイルが Cisco Unified Communications Manager TFTP サーバから削除されます。 電話機の電話番号（1 つまたは複数）は、Cisco Unified Communications Manager データベースに残ります。 これらは、「未定義の DN」と呼ばれ、他のデバイスで使用できます。 未定義の DN を他のデバイスで使用しない場合は、Cisco Unified Communications Manager データベースから削除します。 ルート プラン レポートを使用すると、未定義の DN を表示および削除できます。 詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。

電話ボタン テンプレートのボタンを変更したり、異なる電話ボタン テンプレートを電話機に割り当てたりすると、電話機から電話番号にアクセスできなくなることがあります。 Cisco Unified Communications Manager データベースでは、引き続き電話番号が電話機に割り当てられていますが、コールに応答するためのボタンがないためです。 これらの電話番号は、電話機から消去し、必要に応じて削除してください。

手順

ステップ 1 Cisco Unified Communications Manager で、**[デバイス（Device）]** > **[電話（Phone）]** を選択し、[検索（Find）]をクリックして、問題が発生している電話機を特定します。

ステップ 2 [Delete]を選択して、電話機を Cisco Unified Communications Manager データベースから削除します。

（注） Cisco Unified Communications Manager データベースから電話機を削除すると、設定ファイルが Cisco Unified Communications Manager TFTP サーバから削除されます。電話機の電話番号（1 つまたは複数）は、Cisco Unified Communications Manager データベースに残ります。 これらは、「未定義の DN」と呼ばれ、他のデバイスで使用できます。 未定義の DN を他のデバイスで使用しない場合は、Cisco Unified Communications Manager データベースから削除します。 ルート プラン レポートを使用すると、未定義の DN を表示および削除できます。

ステップ 3 電話機を Cisco Unified Communications Manager データベースに追加し直します。

ステップ 4 電話機の電源をオフ/オンにします。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）
電話機の追加方法 （79 ページ）

802.1X 認証の問題の識別

手順

ステップ 1 必要なコンポーネントが正しく設定されていることを確認します。

ステップ 2 電話機で共有秘密が設定されていることを確認します。

- 共有秘密が設定されている場合は、認証サーバにそれと同じ共有秘密があることを確認します。
- 電話機に共有秘密が設定されていない場合は、共有秘密を入力し、認証サーバの共有秘密と一致することを確認します。

DNS 設定の確認

DNS 設定を確認するには、次の手順を実行します。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Administrator Settings）] > [ネットワークのセットアップ（Network Setup）] > [IPv4 のセットアップ（IPv4 Setup）] > [DNS サーバ 1（DNS Server 1）]** を選択します。

ステップ 3 また、DNS サーバに、TFTP サーバと Cisco Unified Communications Manager システムの CNAME エントリが作成されていることを確認する必要もあります。

また、DNS が逆ルックアップを実行するように設定されていることも確認する必要があります。

サービスの開始

サービスを開始または停止するには、事前にサービスをアクティブにする必要があります。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[ナビゲーション（Navigation）] ドロップダウン リストから [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）]を選択し、[移動（Go）]をクリックします。

ステップ 2 **[ツール（Tool）] > > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 3 [サーバ（Server）] ドロップダウン リストで、プライマリの Cisco Unified Communications Manager サーバを選択します。

ウィンドウに、選択したサーバのサービス名、サービスのステータス、およびサービスを停止または開始するためのサービス コントロール パネルが表示されます。

ステップ 4 サービスが停止している場合は、対応するオプション ボタンをクリックし、[Start]ボタンをクリックします。

[[サービスのステータス（Service Status）] 記号が四角形から矢印に変わります。

Cisco Unified Communications Manager からのデバッグ情報の制御

お客様が解決できない電話機の問題が発生した場合は、Cisco TAC でサポートを受けることができます。電話機のデバッグをオンにして問題を再現し、デバッグをオフにして、分析のために TAC にログを送信する必要があります。

デバッグでは詳細情報を取り込むため、通信量によって電話が遅くなり応答が遅れる可能性があります。ログを検出したら、電話の動作を確保するためにデバッグをオフにする必要があります。

デバッグ情報には、状況の重大度を表す1桁のコードが含まれることがあります。状況は次のようにランクが付けられています。

- 0 - 緊急事態
- 1 - アラート
- 2 - クリティカル
- 3 - エラー
- 4 - 警告
- 5 - 通知
- 6 - 情報
- 7 - デバッグ

詳細情報およびサポートについては、Cisco TAC にお問い合わせください。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で次のウィンドウのいずれかを選択します。

- **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]**
- **[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]**
- **[デバイス（Device）] > [電話（Phone）]**

ステップ 2 次のパラメータを設定します。

- ログのプロファイル - 値：プリセット（デフォルト）、デフォルト、テレフォニー、SIP、UI、ネットワーク、メディア、アップグレード、アクセサリ、セキュリティ、Wi-Fi、VPN、EnergyWise、MobileRemoteAccess

（注） パラメータのマルチレベルおよびマルチセクション サポートを実装するには、[ログ プロファイル（Log Profile）] チェックボックスをオンにします。

- リモート ログ - 値：無効（デフォルト）、有効
- IPv6 ログ サーバまたはログ サーバ - IP アドレス（IPv4 アドレスまたは IPv6 アドレス）

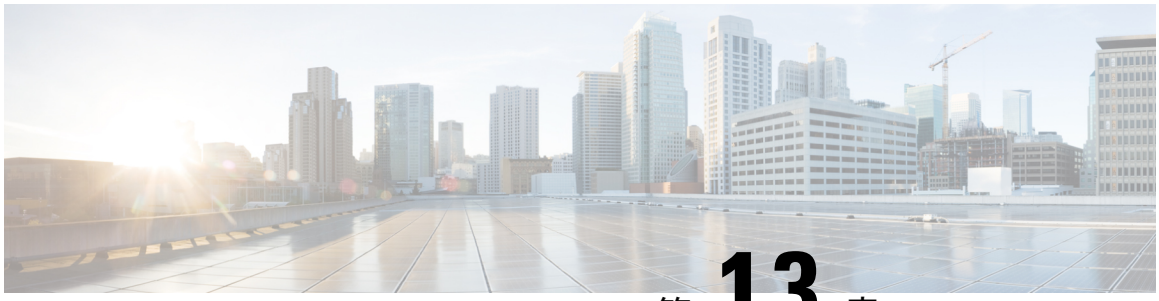
（注） ログ サーバに到達できない場合、電話機はデバッグ メッセージの送信を停止します。

- IPv4 ログサーバのアドレスの形式は、**address:<port>@@base=<0-7>;pfs=<0-1>**
- IPv6 ログサーバのアドレスの形式は、**[address]:<port>@@base=<0-7>;pfs=<0-1>**
- ここで、
  - IPv4 アドレスはドット（.）で区切ります。
  - IPv6 アドレスはコロン（:）で区切ります。

トラブルシューティングに関する追加情報

電話機のトラブルシューティングに関する詳細については、次に示すシスコの Web サイトにアクセスして、該当の電話機モデルに移動してください。

https://www.cisco.com/cisco/web/psa/troubleshoot.html



第 13 章

メンテナンス

基本的なリセット

Cisco IP Phone の基本的なリセットを実行すると、電話機にエラーが発生している状態から復旧したり、各種の設定およびセキュリティ設定をリセットまたは復元したりすることができます。

次の表で、基本的なリセットの実行方法を説明します。 電話機が起動した後は、これらのいずれかの操作で電話機をリセットできます。 状況に応じて適切な操作を選択します。

表 *54* : 基本的なリセットの方法

操作	操作	説
電話機の再起動	**[アプリケーション（Applications）]** を押します。 **[管理者設定（Admin settings）] > [設定のリセット（Reset settings）] > [デバイス リセット（Reset device）]** に移動します。	コ話セ

操作	操作	説明
設定のリセット	設定をリセットするには、**[アプリケーション（Applications）]** を押し、**[管理者設定（Administrator Settings）]** > **[設定のリセット（Reset Settings）]** > **[ネットワーク（Network）]** を選択します。	ユーリセ
	CTL ファイルをリセットするには、**[アプリケーション（Applications）]** を押し、**[管理者設定（Administrator Settings）]** > **[設定のリセット（Reset Settings）]** > **[セキュリティ（Security）]** を選択します。	CTL

電話のキーパッドを使用した、工場出荷時設定へのリセット

電話機を工場出荷時の設定にリセットできます。リセットにより、電話機のすべてのパラメータが消去されます。

手順

ステップ 1 電話機から電源を取り外すには、次のいずれかの方法を使用します。

- 電源アダプタを取り外します。
- LAN ケーブルを抜きます。

ステップ 2 5 秒間待ちます。

ステップ 3 **[#]** を押したままにし、電話機のプラグを再度差し込みます。**[ヘッドセット]** ボタンおよび **[スピーカー]** ボタンが点灯している場合にのみ **[#]** を放します。

（注） 一部のハードウェアバージョンでは、電話機のプラグを再度差し込んだときに、**[ヘッドセット]** ボタンおよび **[スピーカー]** ボタンと一緒に **[ミュート]** ボタンも点灯します。この場合は、すべてのボタンが消灯するのを待ち、**[ヘッドセット]** ボタンおよび **[スピーカー]** ボタンが再度点灯した場合にのみ **[#]** を放します。

ステップ 4 次のキー操作を入力します。

```
123456789*0#
```

[1] キーを押すと、**[ヘッドセット]** ボタンのライトがオフになります。 キー シーケンスを入力した後、[ミュート（Mute）] ボタンが点灯します。

注意 工場出荷時の状態にリセットするプロセスが完了して、メイン画面が表示されるまで、電話機の電源を切らないでください。

電話機がリセットされます。

電話メニューからすべての設定のリセットを実行する

このタスクは、ユーザとネットワークのセットアップ設定をデフォルト値にリセットする場合に実行します。

手順

ステップ 1 [アプリケーション（Applications）] ボタン を押します。

ステップ 2 **[管理者設定（Administrator Settings）] > [設定のリセット（Reset Settings）] > [すべての設定（All settings）]** を選択します。

必要に応じて、電話機のオプションのロックを解除します。

バックアップイメージからの電話機の再起動

Cisco IP 電話 には、デフォルトのイメージが危険にさらされたときに電話機を回復できる 2 つ目のバックアップイメージがあります。

バックアップイメージから電話機を再起動するには、次の手順を実行します。

手順

ステップ 1 電源モジュール ケーブルを取り外します。

ステップ 2 （アスタリスク キー）を押します。

ステップ 3 電源を再び接続します。 ミュート LED が消えるまでスターキーを押し続けます。

ステップ 4 スターキーを離します。
電話機がバックアップイメージから再起動します。

ネットワーク設定のリセット

ネットワーク設定をデフォルト値にリセットし、電話機をリセットします。 この方法を実行すると、DHCP が電話機の IP アドレスを再設定します。

手順

ステップ 1 [管理者設定（Admin Settings）] メニューから、必要に応じて、電話機のオプションのロックを解除します。

ステップ 2 **[設定のリセット（Reset Settings）]** > **[ネットワークのセットアップ（Network Setup）]** を選択します。

ユーザとネットワークの設定のリセット

ユーザ設定およびネットワーク設定に変更を加えていても、電話機がフラッシュ メモリに書き込んでいない場合は、以前に保存された設定にリセットされます。

手順

ステップ 1 [管理者設定（Admin Settings）] メニューから、必要に応じて、電話機のオプションのロックを解除します。

ステップ 2 **[設定のリセット（Reset Settings）]** > **[デバイスのリセット（Reset Device）]** を選択します。

CTL ファイルの削除

電話機から CTL ファイルのみを削除します。

手順

ステップ 1 [管理者設定（Admin Settings）] メニューから、必要に応じて、電話機のオプションのロックを解除します。

ステップ 2 **[設定のリセット（Reset Settings）]** > **[セキュリティ設定（Security Settings）]** を選択します。

品質レポート ツール

品質レポート ツール（QRT）は、Cisco IP 電話の音声品質と一般的な問題をレポートするツールです。 QRT 機能は、Cisco Unified Communications Manager のインストレーションの一環としてインストールされます。

QRT を使用してユーザの Cisco IP 電話 を設定できます。 この設定により、ユーザは [品質のレポート（Report Quality）] を押すことによって、電話機のコールの問題を報告できるようになります。 このソフトキーまたはボタンは、Cisco IP 電話が [接続時（Connected）]、[接続時（会議打診）（Connected Conference）]、[接続時（転送打診）（Connected Transfer）]、または [オンフック（On Hook）] の状態のときにだけ使用できます。

ユーザが[品質のレポート（Report Quality）]を押すと、問題のカテゴリのリストが表示されます。ユーザが該当する問題カテゴリを選択すると、このフィードバックがXMLファイルに記録されます。実際に記録される情報は、ユーザがどのカテゴリを選択したか、また送信先のデバイスがCisco IP 電話かどうかによって異なります。

QRTの使用の詳細については、ご使用のCisco Unified Communications Managerリリースのマニュアルを参照してください。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

音声品質のモニタリング

ネットワーク内で送受信されるコールの音声品質を測定するために、Cisco IP 電話では隠蔽イベントに基づく次の統計メトリックを使用します。DSPは、音声パケットストリーム内でフレーム損失の部分をマスクするために、隠蔽フレームを再生します。

- フレーム損失率のメトリック：音声フレームの総数に対する秘匿フレームの比率を示します。直近フレーム損失率は、3秒ごとに計算されます。
- フレーム損失発生秒数のメトリック：損失フレームが原因でDSPが秘匿フレームを処理する場合の処理秒数を示します。深刻な「フレーム損失発生秒数」は、DSPが5 %を超える隠蔽フレームを処理する場合の秒数です。

（注） フレーム損失率とフレーム損失発生秒数は、フレーム損失に基づいた主要な測定値です。フレーム損失率がゼロの場合は、IPネットワークが損失なく時間どおりにフレームやパケットを配信していることを示しています。

Cisco IP 電話から音声品質メトリックにアクセスするには、[コール統計（Call Statistics）]画面を使用するか、または、リモートで[ストリーム統計（Streaming Statistics）]画面を使用します。

音声品質のトラブルシューティングのヒント

メトリックに大幅な変化が継続的に見られた場合は、次の表の一般的なトラブルシューティング情報を使用してください。

表 *55*：音声品質メトリックの変化

メトリックの変化	条件
フレーム損失率とフレーム損失発生秒数が大幅に増加した	パケット損失または高いジッターによるネットワーク障害。

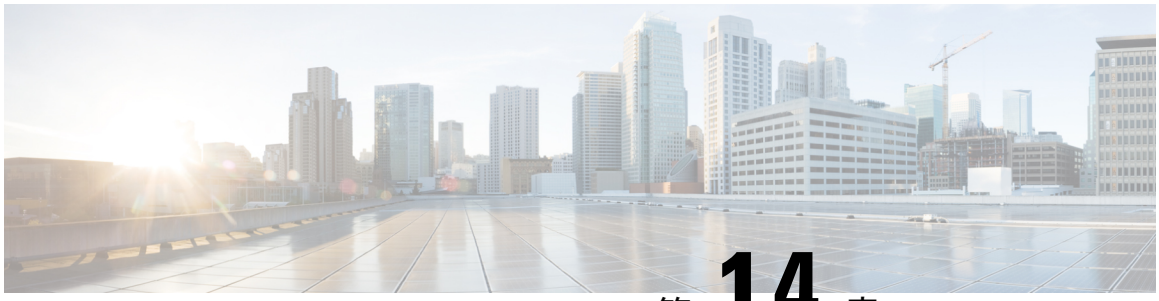
メトリックの変化	条件
フレーム損失率はほとんどゼロであるが、音声品質が悪い。	• 音声チャネルのノイズや歪み（エコー レベルやオーディオ レベルなど）。 • 複数のエンコード/デコードが使用されているタンデム コール（セルラー ネットワークや電話カード ネットワークへのコールなど）。 • スピーカーフォン、ハンドフリー携帯電話、またはワイヤレス ヘッドセットなどから発生する音響問題。 送信パケット（TxCnt）と受信パケット（RxCnt）のカウンタをチェックし、音声パケットが流れていることを確認します。
MOS LQK スコアが著しく減少	パケット損失または高いジッター レベルによるネットワーク障害。 • 平均 MOS LQK の減少は、広範囲の画一的な障害を示している可能性があります。 • 個別の MOS LQK の減少は、集中的な障害を示している可能性があります。 フレーム損失率とフレーム損失発生秒数を照合して、パケット損失やジッターがないか確認してください。
MOS LQK スコアが著しく増加	• 電話機が適切なコーデック（RxTypeおよびTxType）を使用しているかどうかを確認してください。 • MOS LQKのバージョンがファームウェア アップグレード以降に変更されたかどうかを確認してください。

（注） 音声品質メトリックでは、ノイズや歪みは考慮されません。フレーム損失だけが考慮されます。

Cisco IP 電話のクリーニング

Cisco IP 電話をクリーニングする際は、必ず乾いた柔らかい布を使用して電話機と画面を軽く拭いてください。 液体や粉末を電話機に直接付けないでください。 すべての非耐候性の電子機器と同様に、液体や粉末はコンポーネントを損傷し、障害を引き起こすことがあります。

電話がスリープモードのとき、画面はブランクで、[選択]ボタンは点灯していません。電話がこの状態のとき、画面のクリーンアップを行うことができます。ただし、クリーンアップが完了するまで電話がスリープ状態になることがわかっている必要があります。



第 14 章

各言語ユーザのサポート

Unified Communications Manager Endpoints Locale Installer

デフォルトでは、Cisco IP 電話は英語（米国）のロケール用に設定されます。 それ以外のロケールで Cisco IP 電話を使用するには、そのロケール固有のバージョンの Unified Communications Manager Endpoints Locale Installer を、クラスタ内の各 Cisco Unified Communications Manager サーバにインストールする必要があります。 Locale Installer は電話機のユーザ インターフェイス用の最新版の翻訳テキストおよび国別の電話トーンをシステムにインストールし、Cisco IP 電話に使用できるようにします。

特定のリリースに必要なロケール インストーラにアクセスするには、ソフトウェアのダウンロードページにアクセスし、お使いの電話機モデルに移動して、Unified Communications Manager エンドポイント ロケール インストーラのリンクを選択します。

手順の詳細については、特定のリリースのマニュアルを参照してください。Cisco Unified Communications Manager

（注） 最新の Locale Installer がすぐに利用できるとは限らないため、Web サイトの更新を継続的に確認してください。

関連トピック

Cisco Unified Communications Managerのマニュアル （xvii ページ）

国際コールのロギングのサポート

ご使用の電話システムで国際コールのロギング（発信側の正規化）が設定されている場合、通話履歴、リダイヤル、コール ディレクトリの各エントリに通話場所の国際エスケープ コード

を表す「+」記号が表示されることがあります。 電話システムの設定によっては、「+」記号ではなく正しい国際ダイヤル コードが表示される場合があります。国際ダイヤル コードが表示されない場合は、必要に応じて、「+」記号を通話場所の国際エスケープ コードに手動で置き換えて番号を編集した後にダイヤルします。 また、コール ログやディレクトリ エントリには受信コールの完全な国際電話番号が表示され、電話機のディスプレイには国際コード（国番号）が省略された国内用の短い番号が表示される場合もあります。

言語の制限

次のアジア ロケールについては、ローカライズされた Keyboard Alphanumeric Text Entry（KATE）のサポートはありません。

- 中国語（香港）
- 中国語（台湾）
- 日本語（日本）
- 韓国語（韓国）

その代わり、デフォルトとして英語（米国）の KATE がユーザに表示されます。

たとえば、電話画面には韓国語でテキストが表示されるとしてもキーパッドの **2** キーには、**a b c 2 A B C** と表示されます。

中国語の入力は、中国語の PC や携帯電話と同じように機能します。 中国語入力が機能するには、中国語ロケールインストーラが必要です。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。