Cisco IP Phone 8800 シリーズ アドミニストレーション ガイド

初版：2015 年 07 月 13 日

最終更新：2016 年 02 月 24 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、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、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。
- 装置と受信機との距離を離します。
- 受信機と別の回路にあるコンセントに装置を接続します。
- 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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.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。

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。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。

Cisco および Cisco ロゴは、シスコや米国および他の国の関連会社の商標です。To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xv

概要 xv

対象読者 xv

ガイドの表記法 xv

関連資料 xvii

Cisco IP Phone 8800 シリーズ のマニュアル xvii

Cisco Unified Communications Manager のマニュアル xvii

Cisco Business Edition 3000 のマニュアル xvii

Cisco Business Edition 6000 のマニュアル xviii

マニュアルおよびテクニカル サポート xviii

シスコ製品のセキュリティの概要 xviii

新機能および変更情報 1

ファームウェア リリース 11.0 の新機能 1

Cisco IP Phone について 3

技術的な詳細情報 5

物理仕様および動作環境仕様 5

ケーブル仕様 6

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 7

ネットワーク ポート コネクタ 7

コンピュータ ポート コネクタ 7

電話機の所要電力 8

停電 10

電力削減 10

LLDP での電力ネゴシエーション 10

ネットワーク プロトコル 11

VLAN の連携 16

Cisco Unified Communications Manager の連携 17
Cisco Unified Communications Manager Express の連携 18
ボイス メッセージ システムの連携 18
電話機起動の概要 19
外部デバイス 21
USB ポート情報 21
電話機設定ファイル 22
ネットワーク輻輳時の電話の動作 23
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 23
Cisco IP Phone ハードウェア 25
電話機の概要 25
Cisco IP Phone 8811 27
電話機の接続 27
Cisco IP Phone 8841 および 8845 28
電話機の接続 29
Cisco IP Phone 8851 および 8851NR 30
電話機の接続 30
Cisco IP Phone 8861 および 8865 31
電話機の接続 31
ボタンとハードウェア 33
用語の違い 35
ソフトキー、回線ボタン、機能ボタン 35
Cisco IP Phone の設置 37
Cisco IP Phone の設置 39
ネットワーク設定の確認 39
電話機の自動登録の有効化 40
Cisco IP Phone の設置 42
セットアップ メニューからの電話の設定 43
電話機パスワードの適用 44
電話機からのテキスト メニューの入力 45
ワイヤレス LAN のセットアップ 46

Cisco Unified Communications Manager からのワイヤレス LAN のセットアップ 46
電話機からのワイヤレス LAN のセットアップ 47
ネットワークの設定 53
ロード サーバ 58
IPv4 のセット アップ 58
IPv6 のセット アップ 62
[ドメイン名（Domain Name）] フィールドの設定 66
[管理 VLAN ID（Admin VLAN ID）] フィールドの設定 66
[PC VLAN（PC VLAN）] フィールドの設定 66
[SW ポートのセットアップ（SW Port Setup）] フィールドの設定 67
[PC ポートのセットアップ（SW Port Setup）] フィールドの設定 67
[ワイヤレス（Wireless）] フィールドの設定 67
[WLAN サインインアクセス（WLAN Sign In Access）]、 フィールドの設定 68
[SSID] フィールドの設定 68
[セキュリティ モード（Security Mode）] フィールドの設定 68
[802.11 モード（802.11 Mode）] フィールドの設定 68
[DHCP を使う（DHCP Enabled）] フィールドの設定 69
[IP アドレス（IP Address）] フィールドの設定 69
[サブネット マスク（Subnet Mask）] フィールドの設定 69
[デフォルト ルータ（Default Router）] フィールドの設定 70
[DNS サーバ（DNS Server）] フィールドの設定 70
[代替 TFTP（Alternate TFTP）] フィールドの設定 70
[TFTP サーバ 1（TFTP Server 1）] フィールドの設定 71
[TFTP サーバ 2（TFTP Server 2）] フィールドの設定 71
DHCP を使用するための電話機のセットアップ 71
DHCP を使用しないための電話機のセットアップ 72
電話機の起動確認 72
ユーザの電話サービスの設定 73
Cisco Unified Communications Manager での電話機の設定 75
Cisco IP Phone のセットアップ 75
電話機の MAC アドレスの決定 79
電話機の追加方法 79

電話機の個別の追加 79
BAT 電話テンプレートを使用した電話機の追加 80
Cisco Unified Communications Manager へのユーザの追加 81
外部 LDAP ディレクトリからのユーザの追加 81
Cisco Unified Communications Manager へのユーザの直接追加 82
エンド ユーザ グループへのユーザの追加 83
電話機とユーザの関連付け 83
Survivable Remote Site Telephony 84
Enhanced Survivable Remote Site Telephony 88
Cisco Unified Communications Manager 機能のセットアップ 88
セルフ ケア ポータルの管理 91
セルフ ケア ポータルの概要 91
セルフ ケア ポータルへのアクセスの設定 92
セルフ ケア ポータルの表示のカスタマイズ 92
ハードウェアとアクセサリの設置 93
Cisco IP Phone のアクセサリ 95
アクセサリ サポート 95
フットスタンドの接続 96
ケーブル ロックによる電話機の固定 97
外部スピーカおよびマイクロフォン 97
ヘッドセット 97
音質 98
アナログのヘッドセット 98
アナログ ヘッドセットでのワイドバンドの有効化 98
アナログ ヘッドセットでのワイドバンド コーデックの有効化 99
有線ヘッドセット 100
有線ヘッドセットへの接続 100
有線ヘッドセットの無効化 100
USB ヘッドセット 100
USB ヘッドセットの有効化 100
USB ヘッドセットの無効化 101
ワイヤレス ヘッドセット 101
電子フックスイッチの有効化 102

Bluetooth ワイヤレス ヘッドセット 102
Bluetooth ワイヤレス ヘッドセットの有効化 104
Cisco IP Phone キー拡張モジュール 105
Cisco IP Phone は、拡張モジュールのセットアップの概要を調整します 105
KEM 電源情報 106
Cisco IP Phone への 1 台の KEM の接続 109
Cisco IP Phone への 2 ～ 3 台の KEM の接続 113
キー拡張モジュールの Cisco Unified CM の管理でのセットアップ 117
キー拡張モジュール セットアップへのアクセス 119
キー拡張モジュールのリセット 120
キー拡張モジュールのトラブルシューティング 120
壁面取り付け 123
壁面取り付けオプション 123
ロックできない壁面取り付けコンポーネント 123
電話へのロック非対応壁面取り付けキットの取り付け 125
ロック非対応壁面取り付けからの電話機の取り外し 129
キー拡張モジュール付き電話用ロック非対応壁面取り付けコンポーネント 130
キー拡張モジュール付き電話用ロック非対応壁面取り付けキットの装着 132
ロック非対応壁面取り付けからの電話機とキー拡張モジュールの取り外し 136
電話機のロック対応壁面取り付けコンポーネント 137
ブラケットの取り付け 138
キー拡張モジュール付き電話用ロック対応壁面取り付けコンポーネント 143
KEM 付き電話用取り付けブラケット 143
ハンドセット レストの調整 148
Cisco IP Phone の管理 151
Cisco IP Phone のセキュリティ 153
サポート対象のセキュリティ機能 153
ローカルで有効な証明書のセットアップ 159
電話コールのセキュリティ 160
セキュアな会議コールの特定 161
セキュアな電話コールの識別 163
割り込みの暗号化 164

WLAN セキュリティ 164
認証モードのセットアップ 167
ワイヤレス セキュリティ クレデンシャル（Wireless Security Credentials） 168
ユーザ名とパスワードのセットアップ 168
事前共有キーの設定 169
事前共有キーの形式 169
PSK のセットアップ 169
ワイヤレス暗号化（Wireless Encryption） 169
WEP キーの形式 170
WEP キーのセットアップ 170
EAP-TLS 認証証明書 171
製造元でインストールされる証明書 171
ユーザがインストールした証明書 171
EAP-TLS 認証証明書のインストール 172
日付と時刻の設定 173
ACS での証明書のエクスポートおよびインストール 173
ACS 証明書のエクスポート方法 174
Microsoft 証明書サービスを使用した CA 証明書のエクスポート 174
Internet Explorer を使用して ACS から CA 証明書をエクスポートする 174
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 175
認証サーバ ルート証明書のインストール 176
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 176
PEAP の設定 177
はじめる前に 177
PEAP 認証の有効化 178
802.1X 認証 178
802.1X 認証へのアクセス 179
[802.1X 認証（802.1X Authentication）] オプション 179
[デバイス認証（Device Authentication）] フィールドの設定 180
Cisco IP Phone のカスタマイズ 183
カスタム電話呼出音 183

カスタム電話呼出音のセットアップ 184

カスタム呼出音のファイル形式 184

カスタム背景イメージ 185

カスタム背景イメージのセットアップ 186

カスタム背景ファイル形式 187

ワイドバンド コーデックのセットアップ 189

未使用時画面のセット アップ 190

電話機の機能および設定 191

電話機の機能および設定の概要 193

Cisco IP Phone ユーザのサポート 193

電話機能 193

機能ボタンとソフトキー 213

Expressway 経由での Mobile and Remote Access 215

導入シナリオ 216

Expressway 経由での Mobile and Remote Access で利用可能な電話機能 217

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 219

特定の電話機に対する Expressway サインイン用ユーザ クレデンシャル パーシステントの有効化 219

電話機グループに対する Expressway サインイン用ユーザ クレデンシャル パーシステントの有効化 219

ネットワーク全体における Expressway サインイン用ユーザ クレデンシャル パーシステントの有効化 220

MRA サインイン用の QR コードの生成 220

VPN の設定（VPN Configuration） 220

スピーカーフォンを無効にする 221

Cisco IP Phone での省電力のスケジュール 222

Cisco IP Phone での Power Save Plus（EnergyWise）のスケジュール 224

エージェント グリーティングの有効化 228

DF ビットのセットアップ 229

サイレントの設定 230

モニタリングと録音のセットアップ 231

LLDP の電力ネゴシエーションのセットアップ 232

Bluetooth プロファイルのセットアップ 232
自動ポート同期の設定 233
SSH アクセスの設定 234
コールの転送通知のセット アップ 234
C 割り込みの設定 236
クライアント識別コードのセット アップ 236
スイッチおよび PC ポート用の Energy Efficient Ethernet のセットアップ 237
コール リストの BLF の有効化 238
デュアル バンク情報のセットアップ 239
強制承認コードの設定 239
着信コール Toast タイマーの設定 240
ピア ファームウェア共有のセット アップ 241
リモート ポート設定のセット アップ 242
ヘッドセットの側音制御の設定 243
Release ボタンからのダイヤル トーンのセットアップ 244
パーク モニタリング 245
パーク モニタリング タイマーのセットアップ 245
電話番号のパーク モニタリング パラメータ設定 247
ハント リストのパーク モニタリングのセットアップ 248
実行可能な着信呼警告の有効化 248
コール履歴表示拡張の有効化 249
共有回線のコール履歴の有効化 250
デフォルト回線フィルタのセットアップ 251
カスタム回線フィルタのセットアップ 251
電話ボタン テンプレート 252
電話ボタン テンプレートの変更 252
すべてのコールの電話ボタン テンプレートの割り当て 253
IP Phone 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 253
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 254
電話機の Web ページへのアクセスの制御 255
ソフトキー テンプレートの設定 256
RTP/sRTP ポート範囲のセットアップ 259

TLS 再開タイマーのセットアップ 260
音声ポートとビデオ ポートの範囲設定 261
Cisco IP Manager Assistant のセットアップ 263
Visual Voicemail のセットアップ 265
特定ユーザのビジュアル ボイスメールのセット アップ 267
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 267
インテリジェント プロキシミティの有効化 267
複数ライン同時通話（Join Across Lines）機能および回線間転送（Transfer Across Lines）機能の管理 268
コンピュータからのビデオのセット アップ 269
ビデオ送信解像度のセットアップ 270
問題レポート ツール 271
カスタマー サポートのアップロード URL の設定 272
プライマリ回線における全コールを表示 273
プライマリ回線における全コール表示の設定 274
回線のラベルの設定 274
社内ディレクトリとパーソナル ディレクトリ 275
社内ディレクトリのセットアップ 275
パーソナル ディレクトリのセットアップ 275
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 276
Cisco IP Phone Address Book Synchronizer のダウンロード 276
Cisco IP Phone Address Book Synchronizer の導入 277
Synchronizer のインストール 277
Synchronizer のセットアップ 278
アプリケーション ダイヤル ルール 278
アプリケーション ダイヤル ルールの設定 279
Cisco IP Phone のトラブルシューティング 281
電話システムの監視 283
Cisco IP Phone のステータス 283
[モデル情報（Model Information）] ウィンドウの表示 283
[モデル情報（Model Information）] のフィールド 284
[ステータス（Status）] メニューの表示 285

[ステータス メッセージ（Status Messages）] ウィンドウの表示 286
ステータス メッセージ フィールド 286
[ネットワーク統計（Network Statistics）] 画面の表示 295
イーサネット統計情報 295
[ワイヤレス統計（Wireless Statistics）] 画面の表示 299
WLAN 統計情報 299
[コール統計（Call Statistics）] ウィンドウの表示 301
コール統計のフィールド 301
[現在のアクセス ポイント（Current Access Point）] ウィンドウの表示 303
[現在のアクセスポイント（Current Access Point）] のフィールド 303
Cisco IP Phone Web ページ 306
電話機の Web ページへのアクセス 306
デバイス情報 307
ネットワークのセットアップ 309
ネットワーク統計 314
[イーサネット情報（Ethernet Information）] Web ページ 315
[アクセスおよびネットワーク（Access and Network）] の Web ページ 315
デバイス ログ 318
ストリームの統計 318
XML での電話からの情報要求 322
CallInfo の出力例 323
LineInfo の出力例 324
ModeInfo の出力例 324
トラブルシューティング 327
一般的なトラブルシューティング情報 327
起動時の問題 329
Cisco IP Phone が通常の起動プロセスを実行しない 329
Cisco IP Phone が Cisco Unified Communications Manager に登録されない 330
電話機にエラー メッセージが表示される 331
電話機が TFTP サーバまたは Cisco Unified Communications Manager に接続できない 331

電話機が TFTP サーバに接続できない 331
電話機がサーバに接続できない 331
電話機が DNS を使用して接続できない 332
Cisco Unified Communications Manager および TFTP サービスの未作動 332
設定ファイルの破損 332
Cisco Unified Communications Manager での電話機の登録 333
Cisco IP Phone が IP アドレスを取得できない 333
Cisco IP Phone のリセットの問題 333
断続的なネットワークの停止による電話機のリセット 334
DHCP の設定エラーによって電話機がリセットされる 334
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 334
ネットワーク使用量が多いときの電話機のリセット 335
意図的なリセットでの電話機リセット 335
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 335
電話機に電源が入らない 336
電話機が LAN に接続できない 336
Cisco IP Phone のセキュリティの問題 336
CTL ファイルの問題 336
認証エラー。電話機が CTL ファイルを認証できない 336
電話機が CTL ファイルを認証できない 337
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 337
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 337
TFTP 認証が失敗する 338
電話機が登録されない 338
署名付き設定ファイルが要求されない 338
コールに関する一般的な問題 338
コールを確立できない 339
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 339
トラブルシューティング手順 339
TFTP 設定の確認 340
DNS または接続の問題の特定 340
DHCP 設定の確認 341

新しい電話機設定ファイルの作成 342
802.1X 認証の問題の識別 343
DNS 設定の確認 343
サービスの開始 343
Cisco Unified Communications Manager からのデバッグ情報の制御 344
その他のトラブルシューティング情報 345
メンテナンス 347
基本的なリセット 347
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 348
電話メニューからすべての設定のリセットを実行する 349
ネットワーク設定のリセット 349
ユーザとネットワークの設定のリセット 349
CTL ファイルの削除 350
Quality Report Tool 350
音声品質のモニタリング 351
音声品質のトラブルシューティングのヒント 351
Cisco IP Phone のクリーニング 352
各言語ユーザのサポート 355
Unified Communications Manager Endpoints Locale インストーラ 355
国際コールのロギングのサポート 356

はじめに

- 概要，xv ページ
- 対象読者，xv ページ
- ガイドの表記法，xv ページ
- 関連資料，xvii ページ
- マニュアルおよびテクニカル サポート，xviii ページ

概要

『*Cisco IP Phone 8800* アドミニストレーション ガイド』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ています。

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、ネットワーク技術者、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 Phone 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
太字体	コマンドおよびキーワードは太字で示しています。
italic フォント	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、縦棒で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、角カッコで囲み、縦棒で区切って示しています。
string	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。引用符を使用すると、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ます。
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 というキーの組み合わせは、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。 機器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。警告文 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

次の項を使用して、関連情報を取得してください。

Cisco IP Phone 8800 シリーズ のマニュアル

お使いの言語、電話機モデル、およびコール制御システムを参照してください。次のドキュメント URL から参照してください。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-series-home.html

診断ガイドは、次の URL にあります。

http://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

『*Cisco Unified Communications Manager Documentation Guide*』およびご使用の 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。次のドキュメント URL から参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

Cisco Business Edition 3000 のマニュアル

『*Cisco Business Edition 3000 Documentation Guide*』およびご使用の Cisco Business Edition 3000 リリースに特化したその他の文書を参照してください。次のドキュメントURLから参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/business-edition-3000/tsd-products-support-series-home.html

Cisco Business Edition 6000 のマニュアル

『*Cisco Business Edition 6000 Documentation Guide*』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。

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

マニュアルおよびテクニカル サポート

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。シスコ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/en/US/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。シスコは現在、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、配布および使用に際しては、米国および他国の法律が適用されます。シスコ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、http://www.bis.doc.gov/policiesandregulations/ear/index.htm をご覧ください。

第 1 章

新機能および変更情報

- ファームウェア リリース 11.0 の新機能, 1 ページ

ファームウェア リリース 11.0 の新機能

すべての新しい機能が電話機能, （193 ページ）に追加されています。

すべての Cisco Unified Communications Manager リリースをサポートするために、Cisco Unified Communications Manager マニュアルが更新されています。

表 1：*Cisco IP Phone 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

リビジョン	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（VPN Configuration）, （220 ページ） • IPv6 のセット アップ, （62 ページ） • KEM 電源情報, （106 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, （237 ページ） • ビデオ送信解像度のセットアップ, （270 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, （344 ページ）.

リビジョン	更新されたセクション
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，（164 ページ）。 • 認証モードのセットアップ，（167 ページ） • ワイヤレス セキュリティ クレデンシャル（Wireless Security Credentials），（168 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，（271 ページ）。 • カスタマー サポートのアップロード URL の設定，（272 ページ）。
プライマリ回線における全コールを表示に関する情報を追加	• プライマリ回線における全コールを表示，（273 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，（278 ページ）
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，（274 ページ）。

第 I 部

Cisco IP Phone について

- 技術的な詳細情報，5 ページ
- Cisco IP Phone ハードウェア，25 ページ

第 2 章

技術的な詳細情報

- 物理仕様および動作環境仕様，5 ページ
- ケーブル仕様，6 ページ
- 電話機の所要電力，8 ページ
- ネットワーク プロトコル，11 ページ
- VLAN の連携，16 ページ
- Cisco Unified Communications Manager の連携，17 ページ
- Cisco Unified Communications Manager Express の連携，18 ページ
- ボイス メッセージ システムの連携，18 ページ
- 電話機起動の概要，19 ページ
- 外部デバイス，21 ページ
- USB ポート情報，21 ページ
- 電話機設定ファイル，22 ページ
- ネットワーク輻輳時の電話の動作，23 ページ
- 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，23 ページ

物理仕様および動作環境仕様

次の表に、Cisco IP Phone 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 *2*：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	32 ～ 104°F（0 ～ 40°C）

仕様	値または範囲
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	14 ～ 140°F（–10 ～ 60°C）
高さ	229.1 mm（9.02 インチ）
幅	257.34 mm（10.13 インチ）
奥行き	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 A
ケーブル	10-Mbps ケーブルの場合はカテゴリ 3/5/5e/6 を 4 ペア 100-Mbps ケーブルの場合はカテゴリ 5/5e/6 を 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 ペアのワイヤで構成されています。
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 Phone とスイッチ間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）
- スピーカー接続用の 3.5 mm ジャック
- 48 ボルト電源コネクタ

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 Phone 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 Unified IP Phone 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 *3*：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、および DD はそれぞれ、データ A、データ B、データ C、およびデータ 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 *4*：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-

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

電話機の所要電力

Cisco IP Phone には、外部電源または Power over Ethernet（PoE）から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 を提供できます。

（注） 外部電源を使用する場合、イーサネット ケーブルを電話機に接続する前に、電源装置を電話機に接続する必要があります。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。

次の表に、Cisco IP Phone の電源に関するガイドラインを示します。

表 5：***Cisco IP Phone* 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 Phone は、CP-PWR-CUBE-4 電源を使用します。
外部電源：Cisco IP Phone パワーインジェクタを通じて電力を供給。	Cisco IP Phone パワー インジェクタは、どの Cisco IP Phone にも使用できます。インジェクタは、ミッドスパンデバイスとして機能し、接続されている電話機にインラインパワーを供給します。Cisco IP Phone パワー インジェクタは、スイッチ ポートと IP Phone 間に接続されます。また、通電していないスイッチと IP Phone 間で最大 100 m のケーブル長をサポートします。

電源の種類	ガイドライン
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 Phone は、IEEE 802.3af Class 1 の電力供給（シグナル ペアおよびスペア ペア）をサポートしています。 Cisco IP Phone は、外部アドオン デバイス対応の IEEE 802.3af をサポートしています。 Cisco IP Phone 8851、8851NR、8861、および 8865 は、スマートフォン充電用に IEEE 802.3af をサポートしています。Cisco IP Phone 8861 および 8865 は、タブレット充電用に IEEE 802.3at をサポートしています。 電話機を無停電で運用するには、スイッチがバックアップ電源を備えている必要があります。 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、予定している電話機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 システムのバージョ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。 802.3at のサポート：Cisco IP Phone は、802.3at スイッチのサポートがある場合に限り、IEEE 802.3af よりも強力なパワーを引き出すことができます。
Universal Power Over Ethernet（UPoE）	Cisco IP Phone 8865 は、UPoE をサポートしています。

Cisco IP Phone 8800 キー拡張モジュール の電力要件の詳細については、KEM 電源情報, （106 ページ）を参照してください。

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 Phone 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

ドキュメントのトピック	URL
Cisco IP Phone パワー インジェクタ	http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-power-injector/index.html
PoE ソリューション	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
UPoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe/index.html
Cisco Catalyst スイッチ	http://www.cisco.com/c/en/us/products/switches/index.html

ドキュメントのトピック	URL
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/index.html

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

関連トピック

Cisco IP Phone での Power Save Plus（EnergyWise）のスケジュール，（224 ページ）
Cisco IP Phone での省電力のスケジュール，（222 ページ）

LLDP での電力ネゴシエーション

電話機とスイッチは、電話機で消費する電力のネゴシエーションを行います。Cisco IP Phone は、複数の電源設定で動作し、使用可能な電力が少ないときには電力消費量を低減します。

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上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対して応答しないため、電話機が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してい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にすることを推奨します（デフォルト）。

無効にした場合、スイッチが電話機に対して電力を供給しない可能性があります。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ます。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 規格で許容されている最大値まで、アクセサリに電源を供給できます。

（注） CDP および電力ネゴシエーション機能を無効にすると、電話機は 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 Phone 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、電話機でサポートされるネットワーク プロトコルの概要を示します。

表 *6*：***Cisco IP Phone 8800*** シリーズでサポートされるネットワーク プロトコル

ネットワーク プロトコル	目的	使用上の注意
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 Phone 8845 および 8865 では、 Bluetooth 4.1。 Cisco IP Phone 8811、8841、および 8851NR は Bluetooth をサポートしていません。 Cisco IP Phone 8851 および 8861 では、 Bluetooth 4.0。
ブートストラッププロトコル（BootP）	BootP は、特定の起動情報（自身の IP アドレスなど）を Cisco IP Phone などのネットワーク デバイスが検出できるようにするものです。	—
Cisco Audio Session Tunnel（CAST）	CAST プロトコルを使用すると、Cisco IP Phone およびその関連アプリケーションでリモート IP Phone を検出し、その IP Phone と通信することができます。その際、Cisco Unified Communications Manager（CM）やゲートウェイなどの従来のシグナリング コンポーネントに変更を加える必要はありません。	Cisco IP Phone は CAST を CUVA と Cisco Unified CM の間のインターフェイスとして使用し、Cisco IP Phone 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 Phone では、補助 VLAN ID、ポートごとの電源管理の詳細情報、Quality of Service（QoS）設定情報などの情報を、CDP を使用して Cisco Catalyst スイッチとやり取りします。
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
ダイナミック ホスト コンフィギュレーションプロトコル（DHCP）	DHCP は、IP アドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。 DHCP を使用すると、IP 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、デフォルトで有効になっています。無効にした場合は、個々の電話機がある場所で、IP アドレス、サブネット マスク、ゲートウェイ、および TFTP サーバを手動で設定する必要があります。 DHCP のカスタム オプション 150 を使用することを推奨します。この方法では、TFTP サーバの IP アドレスをオプション値として設定します。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。 （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。
ハイパーテキスト転送プロトコル（HTTP）	HTTP は、インターネットや Web 経由で情報を転送し、ドキュメントを移送するための標準的な手段です。	Cisco IP Phone では、XML サービスおよびトラブルシューティングに HTTP を使用します。
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 Phone 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。 クライアントが認証されるまでは、802.1X アクセス コントロールによって、クライアントが接続されているポートを経由する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。認証が完了すると、標準トラフィックがポートを通過できます。	Cisco IP Phone では、EAP-FAST および EAP-TLS 認証方式をサポートすることによって、IEEE 802.1X 標準が実装されています。 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。
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 Phone 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。
Link Layer Discovery Protocol（LLDP）	LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコデバイスとサードパーティ製デバイスでサポートされています。	Cisco IP Phone は、PC ポートで LLDP をサポートします。

ネットワーク プロトコル	目的	使用上の注意
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 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
リアルタイム転送プロトコル（RTP）	RTP は、インタラクティブな音声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 Phone では、RTP プロトコルを使用して、リアルタイム音声トラフィックを他の電話機やゲートウェイとやり取りします。
リアルタイム制御プロトコル（RTCP）	RTCP は RTP と連動して、RTP ストリーム上で QoS データ（ジッター、遅延、ラウンドトリップ遅延など）を伝送します。	RTCP はデフォルトで有効になっています。
セッション記述プロトコル（SDP）	SDP は SIP プロトコルの一部であり、2 つのエンドポイント間で接続が確立されている間に、どのパラメータを使用できるかを決定します。会議は、会議に参加するすべてのエンドポイントがサポートする 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。

ネットワーク プロトコル	目的	使用上の注意
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コール情報を伝送することが可能になります。セッション管理とは、エンドツーエンド コールの属性を制御する機能を提供することです。 Cisco IP Phone は、電話機が IPv6 アドレス モード、IPv4 アドレス モード、またはデュアルスタック モードで実行されているときに SIP プロトコルをサポートします。
伝送制御プロトコル（TCP）	TCP は、コネクション型の転送プロトコルです。	Cisco IP Phone では、Cisco Unified Communications Manager への接続、および XML サービスへのアクセスに TCP を使用します。
トランスポート層セキュリティ（TLS）	TLS は、通信のセキュリティ保護と認証に使用される標準プロトコルです。	セキュリティが実装されると、Cisco IP Phone 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。

ネットワーク プロトコル	目的	使用上の注意
トリビアルファイル転送プロトコル（TFTP）	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 Cisco IP Phone で TFTP を使用すると、電話タイプ固有の設定ファイルを取得できます。	TFTP 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 サーバが指定する以外の TFTP サーバを電話機で使用する場合は、電話機の [ネットワークの設定（Network Configuration）] メニューを使用して、TFTP サーバの IP アドレスを手動で割り当てる必要があります。 詳細については、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。
ユーザ データグラム プロトコル（UDP）	UDP は、データ パケットを配信するためのコネクションレス型メッセージング プロトコルです。	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。

関連トピック

802.1X 認証, （178 ページ）
ネットワークの設定, （53 ページ）
電話機の起動確認, （72 ページ）
VLAN の連携, （16 ページ）
Cisco Unified Communications Manager の連携, （17 ページ）
Cisco Unified Communications Manager Express の連携, （18 ページ）
音声ポートとビデオ ポートの範囲設定, （261 ページ）
Cisco Unified Communications Manager のマニュアル, （xvii ページ）

VLAN の連携

Cisco IP Phone 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、同じポートに接続し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 Phone 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 Phone 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）

電話機を独立した補助 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ための 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るようになります。

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 IP 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 サービス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 セッションが継続されます。

この章で説明されている IP Phone 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 Cisco IP Phone のモデルが、Cisco Unified Communications Manager の管理ページの [電話のタイプ（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 の最新のサポート パッチ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

Cisco IP Phone 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。

Cisco IP Phone では、次のアクションはサポートされていません。

- 転送：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：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：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。

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 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。

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 Phone のメッセージ 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ておく必要があります。

- 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）メソッドを設定しておく必要があります。

電話機起動の概要

Cisco IP Phone 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 Phone 8861 および 8865 のみ）アクセス ポイントのスキャン。Cisco IP Phone 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 Phone 8861 および 8865 のみ）アクセス ポイントによる認証。Cisco IP Phone 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
オープン	なし	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。
共有キー	なし	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	なし	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 Phone 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 Phone 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 Phone 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 Phone 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、シールドおよびコネクタが高品質の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ー、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 Phone 8851、8851NR、8861、および 8865 は、各 USB ポートに接続される最大 5 台のデバイスをサポートします。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 Cisco IP Phone 8800 キー拡張モジュール（KEM）は、USB デバイスとしてカウントされます。3 台の KEM 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 CM の管理 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、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 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の動作

ネットワーク パフォーマンスを低下させるすべての要因によって Cisco IP Phone の音声とビデオの品質が影響を受ける可能性があり、場合によっては通話が切断されることもあります。ネットワーク速度低下の原因として、たとえば次のようなアクティビティがあります。

- 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
- ネットワークで発生する DoS 攻撃などの攻撃

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 Phone 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。

第 3 章

Cisco IP Phone ハードウェア

- 電話機の概要，25 ページ
- Cisco IP Phone 8811，27 ページ
- Cisco IP Phone 8841 および 8845，28 ページ
- Cisco IP Phone 8851 および 8851NR，30 ページ
- Cisco IP Phone 8861 および 8865，31 ページ
- ボタンとハードウェア，33 ページ
- 用語の違い，35 ページ
- ソフトキー、回線ボタン、機能ボタン，35 ページ

電話機の概要

Cisco IP Phone 8800 シリーズは、インターネット プロトコル（IP）ネットワーク経由の音声通信を提供します。Cisco IP Phone は、デジタル ビジネス フォンとほぼ同様に機能し、電話コールの発受信に加えて、ミュート、保留、転送、スピード ダイヤル、コール転送などの機能を使用できます。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 Phone 8811 は、グレースケール LCD 画面を備えています。

Cisco IP Phone 8841、8845、8851、8851NR、8861、および 8865 は、24 ビット カラー LCD 画面を備えています。

Cisco IP Phone の機能は次のとおりです。

- 最大 5 回線をサポートするプログラム可能な機能ボタン。このボタンには他の機能をプログラムすることもできます。
- フル ビデオ機能（Cisco IP Phone 8845 および 8865 のみ）
- ギガビット イーサネット接続機能

- ワイヤレス ヘッドセットの Bluetooth サポート（Cisco IP Phone 8845、8851、8861、および 8865 のみ。この機能は Cisco IP Phone 8811、8841、および 8851NR ではサポートされません）
- 外部マイクロフォンとスピーカーのサポート（Cisco IP Phone 8861 および 8865 のみ）
- Wi-Fi によるネットワーク接続機能（Cisco IP Phone 8861 および 8865 のみ）
- USB ポート：
  - Cisco IP Phone 8851 および 8851NR には USB ポート X 1
  - Cisco IP Phone 8861 および 8865 には USB ポート X 2

Cisco IP Phone 8845 および 8865 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。

ビデオ コールには次の機能があります。

- ピクチャイン ピクチャ（PIP）：右下、右上、左上、左下の 4 つのポジションから選択。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。PIP がオフになっているときは、切り替えソフトキーはグレー表示になります。
- 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。

Cisco IP Phone 8845 と 8865 には手動シャッターがあります。シャッターを開くと、ビデオ コールを開始されます。シャッターを閉じると、ビデオ ブロードキャストが停止されます。次の発信者にビデオがブロードキャストされるのを防止するために、各コールの後にはカメラのシャッターを閉じてください。

ビデオ コールの詳細については、『*Cisco IP Phone 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。

Cisco IP Phone は、他のネットワーク デバイスと同様に設定と管理を行う必要があります。これらの電話機は、次のコード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
- G.729a/G.729ab
- G.726
- iLBC
- L16

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

Cisco IP Phone は、コール転送や転送、リダイヤル、スピードダイヤル、会議コール、ボイスメッセージング システムへのアクセスなど、従来のテレフォニー機能を提供します。Cisco Unified IP Phone では、さらにその他の各種の機能も提供します。

Cisco Unified IP Phone は、他のネットワーク デバイスと同様に、Cisco Unified Communications Manager および IP ネットワークの他の部分にアクセスできるように設定する必要があります。DHCP を使用すると、電話機上で設定する内容が少なくなります。ただし、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 Unified IP Phone は、IP ネットワーク上の他のサービスやデバイスと連携することで、高度な機能を提供できます。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 Phone で直接検索できるようになります。XML を使用すると、天気予報、株価情報、商品相場といった Web ベースの情報にユーザがアクセスできるようになります。

さらに、Cisco Unified IP Phone はネットワーク デバイスであるため、詳細なステータス情報を IP Phone から直接取得することができます。この情報は、ユーザが IP Phone を使用しているときに生じた問題をトラブルシューティングするのに役立ちます。また、現在のコールに関する統計情報や、ファームウェアのバージョンも電話機で取得できます。

Cisco IP Phone を IP テレフォニー ネットワークで機能させるには、IP Phone 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 Phone 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

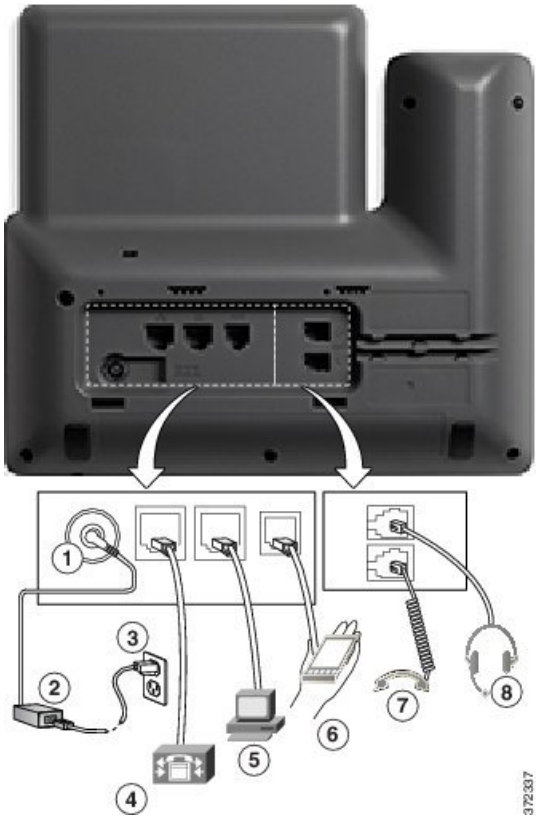
Cisco Unified Communications Manager のマニュアル, （xvii ページ）

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。

電話機の接続

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（DC 48 V）	5	アクセス ポート（10/100/1000 PC）接続
2	AC-DC 電源装置（任意）	6	補助ポート
3	AC 電源コンセント（任意）	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 ヘッドセット接続（任意）

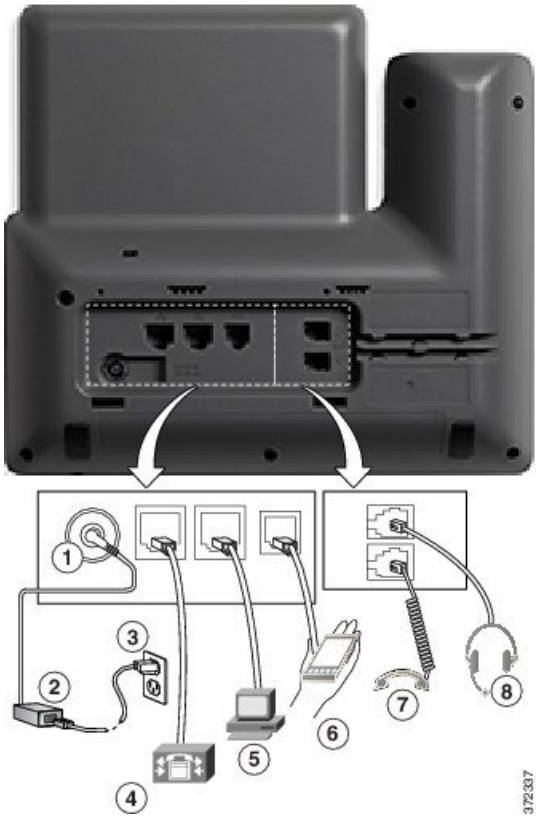
（注） Cisco IP Phone 8811 は Cisco IP Phone 8800 キー拡張モジュール をサポートしません。

Cisco IP Phone 8841 および 8845

以降の項では、Cisco IP Phone 8841 および 8845 の属性について説明します。

電話機の接続

次の図を使用して、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）	5	アクセス ポート（10/100/1000 PC）接続
2	AC-DC 電源装置（任意）	6	補助ポート
3	AC 電源コンセント（任意）	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 ヘッドセット接続（任意）

（注） Cisco IP Phone 8841 および 8845 は、Cisco IP Phone 8800 キー拡張モジュールをサポートしていません。

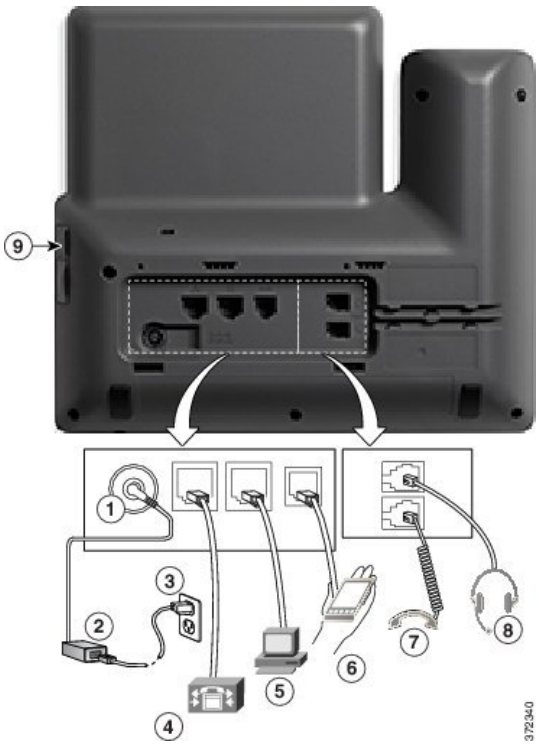
Cisco IP Phone 8851 および 8851NR

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

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

電話機の接続

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）	5	アクセス ポート（10/100/1000 PC）接続	9	USB ポート
2	AC-DC 電源装置（任意）	6	補助ポート		
3	AC 電源コンセント（任意）	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 ヘッドセット接続（任意）		

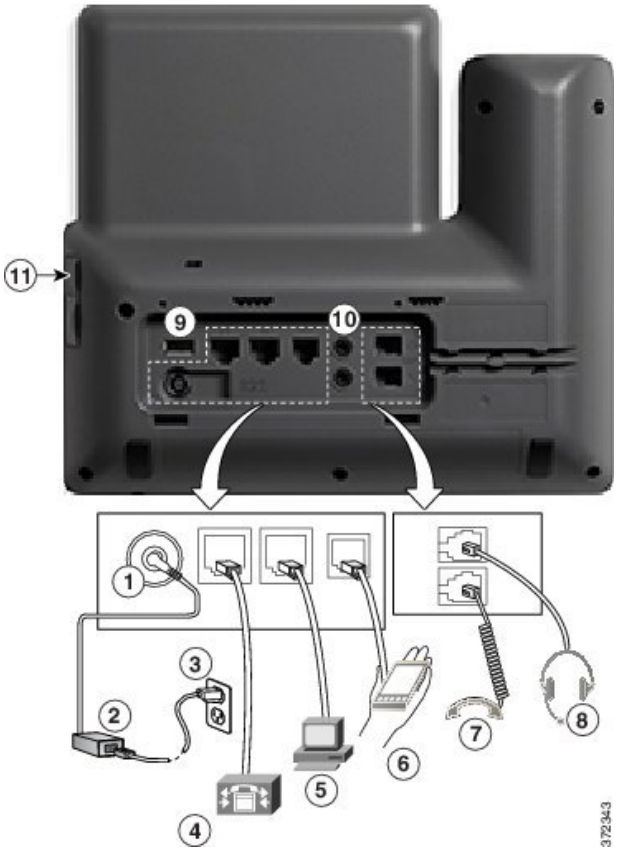
（注） 各 USB ポートは、最大 5 個のサポート対象デバイスおよびサポート外デバイスとの接続をサポートします。電話機に接続された各デバイスは、最大デバイス数に含まれます。たとえば、電話機は 5 台の USB デバイス（2 台の Cisco IP Phone 8800 キー拡張モジュール、1 台のヘッドセット、1 台のハブ、および 1 台の別の標準 USB デバイスなど）を側面ポートでサポートできます。多くのサードパーティ製 USB 製品は複数の USB デバイスとしてカウントされます。たとえば、USB ハブとヘッドセットを含むデバイスは、2 台の USB デバイスとしてカウントできます。詳細については、USB デバイスのマニュアルを参照してください。

Cisco IP Phone 8861 および 8865

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

電話機の接続

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	11	USB ポート
2	AC-DC 電源装置（任意）	7	ハンドセットの接続		
3	AC 電源コンセント（任意）	8	アナログ ヘッドセット接続（任意）		
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	10	オーディオイン/アウトポート		

（注） 各 USB ポートは、最大 5 個のサポート対象デバイスおよびサポート外デバイスとの接続をサポートします。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、電話機では 5 台の USB デバイス（たとえば 3 台の Cisco IP Phone 8800 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。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。

ボタンとハードウェア

Cisco IP Phone 8800 シリーズでは、次に示す 2 種類のハードウェアが提供されています。

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

次の図は、Cisco IP Phone 8845 を示しています。

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

1	ハンドセット、および ライト ストリップ付き ハンドセット	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 Phone 8845 および 8865 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、コール セッションにアクセスできます。 詳細については、ソフトキー、回線ボタン、機能ボタン，（35 ページ）を参照してください。
4	ソフトキー ボタン	機能およびサービスにアクセスできます。 詳細については、ソフトキー、回線ボタン、機能ボタン，（35 ページ）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することができます。 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：スピーカフォンのオン/オフを切り替えます。スピーカーフォンがオンになっているとき、ボタンは点灯しています。 ミュート：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：ヘッドセットのオン/オフを切り替えます。ヘッドセットがオンのときは、ボタンが点灯します。

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：通話履歴、ユーザ設定、電話機の設定、電話機の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、スピーカフォンの音量（オフフック）および呼出音の音量（オンフック）を調節します。

用語の違い

次の表に、『*Cisco IP Phone 8800 Series User Guide for Cisco Unified Communications Manager*』、『*Cisco IP Phone 8800 Series Administration Guide for Cisco Unified Communications Manager*』、および『*Cisco Unified Communications Manager Administration Guide*』との間に見られる用語の違いについて示します。

表 *7*：用語の違い

ユーザ ガイド	アドミニストレーション ガイド
回線ステータス	ビジー ランプ フィールド（BLF）
メッセージ インジケータ	メッセージ受信インジケータ（MWI）またはメッセージ受信ランプ
プログラム可能な機能ボタン	プログラム可能なボタンまたはプログラム可能な回線キー（PLK）
[簡易発信（New Call）] ウィンドウ	[簡易発信（New Call）] バブル
ボイスメール システム	ボイス メッセージ システム

ソフトキー、回線ボタン、機能ボタン

電話機では、次のいくかの方法により、対話式に機能を操作することができます。

- スクリーンの下にあるソフトキーを使用すると、電話機の操作が容易になります。その内容は、現在の操作内容に応じて変化します。[...] ソフトキーは、追加のソフトキーが使用可能であることを示します。
- 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。
  - 機能ボタンを使用すると、回線のコールを表示したり、短縮ダイヤルなどの機能にアクセスできます。
  - 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。

- 緑、点灯：アクティブ コールまたは双方向のインターコム コール
- 緑、点滅：保留中のコール
- オレンジ、点灯：プライバシー機能が使用中、単方向インターコム コール、サイレント（DND）機能がアクティブ、またはハント グループにログイン中
- オレンジ、点滅：着信コールまたは復帰コール
- 赤、点灯：リモート回線の使用中（共有回線または回線ステータス）
- 赤、点滅：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。

第 II 部

Cisco IP Phone の設置

- Cisco IP Phone の設置，39 ページ
- Cisco Unified Communications Manager での電話機の設定，75 ページ
- セルフ ケア ポータルの管理，91 ページ

第 4 章

Cisco IP Phone の設置

- ネットワーク設定の確認，39 ページ
- 電話機の自動登録の有効化，40 ページ
- Cisco IP Phone の設置，42 ページ
- セットアップ メニューからの電話の設定，43 ページ
- ワイヤレス LAN のセットアップ，46 ページ
- ネットワークの設定，53 ページ
- 電話機の起動確認，72 ページ
- ユーザの電話サービスの設定，73 ページ

ネットワーク設定の確認

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 ネットワークおよびそのセットアップと設定のチェックリストについては、 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。

電話機がネットワークでエンドポイントとして正常に動作するためには、ネットワークが所定の要件を満たしている必要があります。

（注） 電話機では Cisco Unified Communications Manager からの日時を表示します。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。

- Cisco 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設定します。

- DHCP 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）

電話機の自動登録の有効化

Cisco IP Phone 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 Phone 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 Phone 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、自動登録は自動的に無効になります。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 Phone 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 必要なサーバを選択し、[自動登録（Autoregister）] チェックボックスを選択します。

ステップ 3 [自動登録情報（Auto-registration Information）] で、ユニバーサル デバイス テンプレート、ユニバーサル回線テンプレート、開始電話番号、終了電話番号を設定します。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

電話機の追加方法, （79 ページ）

Cisco IP Phone の設置

電話機がネットワークに接続されると、電話機の起動プロセスが開始され、電話機が Cisco Unified Communications Manager に登録されます。電話機の設置を完了するには、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，（21 ページ）を参照してください。

手順

ステップ 1 電話機の電源を次の中から選択します。

- Power over Ethernet（PoE）
- 外部電源

詳細については、電話機の所要電力，（8 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 ポートに接続します。
ワイドバンド対応ハンドセットは、Cisco IP Phone 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。

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。詳細については、ヘッドセット，（97 ページ）またはワイヤレス ヘッドセット，（101 ページ）を参照してください。

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 Phone 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 Phone には、イーサネット ケーブルが 1 箱に 1 本添付されています。
10 Mbps 接続にはカテゴリ 3、5、5e、または 6 のケーブルを使用し、100 Mbps 接続にはカテゴリ 5、5e、または 6 のケーブル、1000 Mbps 接続にはカテゴリ 5e または 6 ケーブルを使用してください。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，（7 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、他のネットワーク デバイスを Cisco IP Phone 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 のケーブルを使用し、100 Mbps 接続にはカテゴリ 5、5e、または 6 のケーブル、1000 Mbps 接続にはカテゴリ 5e または 6 ケーブルを使用してください。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，（7 ページ）を参照してください。

ステップ 6 電話機が机の上にある場合は、フット スタンドを調節します。詳細については、フットスタンドの接続, （96 ページ）を参照してください。電話機が壁に取り付けられている場合は、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。詳細については、次を参照してください。ハンドセット レストの調整, （148 ページ）

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, （53 ページ）およびネットワークのセットアップ, （309 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てください。
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 Phone を使用してコールを発信し、電話機と機能が正常に動作することを確認します。
『*Cisco IP Phone 8800 Series User Guide for Cisco Unified Communications Manager*』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 Phone を有効に活用できるようにします。

セットアップ メニューからの電話の設定

Cisco IP Phone 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、IPv6、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 Phone 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 Phone を設定するための設定オプションがあります。
  - [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 CM の管理 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 ボタン 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。

- ナビゲーションの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

[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を変更できないよう、電話機にパスワードを適用できます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[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）] を使用して [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。

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 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 回押すと「a」が入力され、2 回素早く押すと「b」、3 回素早く押すと「c」が入力されます。少し間を置くと、カーソルが次の文字を入力する位置に自動的に移動します。
- 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（Save）] を押す前に、[キャンセル（Cancel）] 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 Phone 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，（347 ページ）

電話機パスワードの適用, （44 ページ）

ワイヤレス LAN のセットアップ

Cisco IP Phone 8861 および 8865 のみ無線 LAN をサポートします。

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。

音声用の Wi-Fi 接続が Cisco IP Phone に有効にされていて、EAP-FAST または PEAP セキュリティモードを使用している場合、アプリケーションメニュー内の WLAN サインインを使用して、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。

詳細については、次の場所にある『*Cisco IP Phone 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 Phone 8800 Wireless LAN Deployment Guide*』には、次の設定情報が含まれています。

- ワイヤレス ネットワークの設定
- Cisco Unified Communications Manager Administration でのワイヤレス ネットワーク設定
- Cisco IP Phone でのワイヤレス ネットワーク設定

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 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）] > [Wi-Fiログインアクセス（Wi-Fi Sign in access）] を選択します。

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 CM の管理（Cisco Unified Communications Manager Administration）] で、ワイヤレス Cisco Unified IP Phone 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 [設定の有効化（Enable Setting）] 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チェックします。

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 [設定の有効化（Enable Setting）] を選択します。
c) [共通設定の上書き（Override Common Settings）] チェックボックスをチェックします。
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 [設定の有効化（Enable Setting）] を選択します。
c) [共通設定の上書き（Override Common Settings）] チェックボックスをチェックします。

電話機からのワイヤレス LAN のセットアップ

Cisco IP Phone 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） ワイヤレス設定の値は、Cisco IP Phone キーパッドでのみ設定できます。Cisco IP Phone をワイヤレス モードで使用している場合は、AC アダプタを使用する必要があります。イーサネットに接続すると、ワイヤレスは無効になります。

（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。

詳細については、『Cisco IP Phone 8800 Series WLAN Deployment Guide』を参照してください。

手順

ステップ 1 アプリケーション 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）] > [Wi-Fi クライアントのセットアップ（Wi-Fi client setup）] を選択します。

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 8 : *[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
ワイヤレス	Cisco IP Phone の無線をオンまたはオフにします。次の有効な値を指定します。 • [オン（On）] : 電話機の無線をオンにします。 • [オフ（Off）] : 電話機の無線をオフにします。 デフォルト : [オン（On）]	[ワイヤレス（Wireless）] フィールドの設定, （67 ページ）を参照してください。

オプション	説明	変更の手順
ワイヤレスサインインアクセス（Wireless Sign in Access）	メインの [アプリケーション（Applications）] メニューで、[ワイヤレスサインインアクセス（Wireless Sign in Access）] ウィンドウの表示を有効にします。 • [オン（On）] : [ワイヤレスサインインアクセス（Wireless Sign in Access）] ウィンドウが表示されます。この値をオンにすると、メインの [アプリケーション（Applications）] メニューで、ワイヤレスユーザ ID およびパスワードのサイン インまたは変更ができます。オンにせずにサイン イン情報を変更するには、[セキュリティ（Security）] メニュー レベルまで移動してから、サイン インクレデンシャルが必要な PEAP または EAP-FAST のいずれかの方法を選択します。 • [オフ（Off）] : [ワイヤレスサインインアクセス（Wireless Sign in Access）] ウィンドウは表示されません。 デフォルト : Off	[WLAN サインインアクセス（WLAN Sign In Access）]、フィールドの設定, （68 ページ）を参照してください。
IPv4 のセットアップ（IPv4 Setup）	[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 のセット アップ, （58 ページ）を参照してください。	[IPv4 のセットアップ（IPv4 Setup）] までスクロールし、選択を押します。

オプション	説明	変更の手順
IPv6 のセットアップ（IPv6 Setup）	[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 のセット アップ, （62 ページ）を参照してください。	[IPv6 のセットアップ（IPv6 Setup）] までスクロールし、選択ボタンを押します。
MAC アドレス（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。	表示専用。変更不可。
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。	[ドメイン名（Domain Name）] フィールドの設定, （66 ページ）を参照してください。
SSID	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。	[SSID] フィールドの設定, （68 ページ）を参照してください。

オプション	説明	変更の手順
セキュリティモード（Security Mode）		[セキュリティ モード（Security Mode）] フィールドの設定, （68 ページ）を参照してください。

オプション	説明	変更の手順
	電話機が WLAN へのアクセスに使用する認証のタイプです。次の有効な値を指定します。 • [オープン（Open）]：暗号化せず、すべてのアクセスポイント（AP）にアクセスします。 • [WEP]：802.11 認証を行ったうえでオープンにするが、データの暗号化に有線と同等のプライバシー（WEP）を使用します。すべての AP へのアクセスおよび、ローカル AP での WEP キーを通じた認証を指定します。 • [PSK]：共有キー認証は、AES または TKIP 暗号化を使用します。 • [EAP-FAST]：Extensible Authentication Protocol Flexible Authentication via Secure Tunneling（EAP-FAST）では、ユーザ名と暗号化されたセキュアなパスワードをネットワークの RADIUS サーバと交換します。このネットワークでは、Protected Access Credential（PAC）を使用することで認証用のセキュアなトンネルが確立されています。EAP-FAST では WPA および WPA2 をサポートしています。 • [EAP-TLS]：Extensible Authentication Protocol via Transport Layer Security では、ユーザ名と暗号化されたセキュアなパスワードとを、ネットワークの RADIUS サーバと交換します。このネットワークでは、Protected Access Credential（PAC）を使用することで認証用のセキュアなトンネルが確立されます。EAP-TLS では WPA および WPA2 をサポートしています。EAP-TLS 認証では、製造元でインストール	

オプション	説明	変更の手順
	された内蔵の証明書か、ユーザがインストールした証明書がユーザ証明書として使用されます。 • [PEAP(MSCHAPV2)]：Protected Extensible Authentication Protocol（LEAP）の認証では、ユーザ名と暗号化されたセキュアなパスワードをネットワークの RADIUS サーバと交換します。PEAP は、シスコ独自バージョンの EAP です。PEAP では WPA および WPA2 をサポートしています。 • PEAP-MSCHAPV2 および PEAP-GTC：Protected Extensible Authentication Protocol（LEAP）の認証では、ユーザ名と暗号化されたセキュアなパスワードをネットワークの RADIUS サーバと交換します。PEAP は、シスコ独自バージョンの EAP です。PEAP では WPA および WPA2 をサポートしています。	
802.11 モード（802.11 Mode）	WLAN で使用されるワイヤレス信号規格を指定します。次の有効な値を指定します。 • [自動（Auto）]：デフォルト値。 • 2.4 GHz • 5.0 GHz	[802.11 モード（802.11 Mode）] フィールドの設定，（68 ページ）を参照してください。

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

ネットワークの設定

ネットワークで DHCP を使用していない場合は、Cisco IP Phone をネットワークに設置した後に、電話機上で次のネットワーク設定値を設定する必要があります。

- IP アドレス
- IP サブネット情報
- IPv6 形式のアドレス
- TFTP サーバの IP アドレス

必要に応じて、ドメイン名と DNS サーバ設定値も設定できます。

[イーサネットのセットアップ（Ethernet Setup）] メニューは、さまざまなネットワーク設定値を表示および設定するためのオプションを提供します。次の表に、これらのオプションの説明を示します。また、該当する場合には、それらの変更方法についても併せて説明します。

（注） 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 9 : *[イーサネットのセットアップ（Ethernet Setup）] メニューおよび [イーサネットの設定（Ethernet）] メニューのオプション*

オプション	説明	変更の手順
IPv4 のセットアップ（IPv4 Setup）	[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。 このオプションは、電話機が IPv4 専用モードまたはデュアル スタック モードで設定されている場合にのみ表示されます。	[IPv4 のセットアップ（IPv4 Setup）] までスクロールし、選択を押します。 IPv4 のセットアップ, （58 ページ）を参照してください。
IPv6 のセットアップ（IPv6 Setup）	電話機の IPv6 設定。	[IPv6 のセットアップ（IPv6 Setup）] までスクロールし、選択を押します。 IPv6 のセットアップ, （62 ページ）を参照してください。

オプション	説明	変更の手順
MAC アドレス（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。	表示専用。変更不可。
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。	[ドメイン名（Domain Name）] フィールドの設定，（66 ページ）を参照してください。
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 VLAN。 電話機が補助 VLAN をまだ受信していない場合、このオプションは管理 VLAN を示しています。 補助 VLAN と管理 VLAN のいずれも設定されていない場合、このオプションは空白になります。	表示専用。変更不可。 電話機は、Cisco Discovery Protocol（CDP）または Link Level Discovery Protocol Media Endpoint Discovery（LLDP-MED）を通じて接続先 VLAN ID を取得します。ID の情報は電話機が接続されているスイッチから提供されます。VLAN ID を手動で割り当てるには、[管理 VLAN ID（Admin VLAN ID）] オプションを使用します。
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用され、その他の場合は値が無視されます。	[管理 VLAN ID（Admin VLAN ID）] フィールドの設定，（66 ページ）を参照してください。
PC VLAN	ボイス VLAN をサポートしないサードパーティ スイッチと電話機が連携できるようにします。このオプションを変更する前に、[管理 VLAN ID（Admin VLAN ID）] オプションを設定する必要があります。	[PC VLAN（PC VLAN）] フィールドの設定，（66 ページ）を参照してください。

オプション	説明	変更の手順
SW ポートのセットアップ（SW Port Setup）	ネットワーク ポートの速度と二重化モード。次の有効な値を指定します。 • 自動ネゴシエーション（Auto Negotiate） • [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、スイッチ上のポートを電話機と同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。 このオプションの設定値を変更する場合は、[PC ポート設定（PC Port Configuration）] オプションを同じ設定値に変更する必要があります。	[SW ポートのセットアップ（SW Port Setup）] フィールドの設定,（67 ページ）を参照してください。

オプション	説明	変更の手順
PC ポートのセットアップ（PC Port Setup）	コンピュータ（アクセス）ポートの速度とデュプレックス。有効な値は、次のとおりです。 • 自動ネゴシエーション（Auto Negotiate） • [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、スイッチ上のポートを電話機と同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。 このオプションの設定値を変更する場合は、[SW ポート設定（SW Port Configuration）] オプションを同じ設定値に変更する必要があります。	[PC ポートのセットアップ（SW Port Setup）] フィールドの設定,（67 ページ）を参照してください。 複数の電話機の設定を同時に行うには、[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ（[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configurations）]）で [リモートポート設定（Remote Port Configuration）] を有効化します。 （注） Cisco Unified Communications Manager で [リモートポート設定（Remote Port Configuration）] 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することはできません。

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（Administrator Settings）] > [ネットワークのセットアップ（Network Setup）] を選択します。

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。

IPv4 のセット アップ

次の表で、[IPv4 のセットアップ（IPv4 Setup）] メニューのオプションを説明します。

表 *10*：*[IPv4* のセットアップ（*IPv4 Setup*）*]* メニューのオプション

オプション	説明	変更の手順
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，（71 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，（72 ページ）を参照してください。	[DHCP を使う（DHCP Enabled）] フィールドの設定，（69 ページ）を参照してください。

オプション	説明	変更の手順
[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。	[IP アドレス（IP Address）] フィールドの設定,（69 ページ）を参照してください。
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。	[サブネット マスク（Subnet Mask）] フィールドの設定,（69 ページ）を参照してください。
デフォルト ルータ	電話機で使用される、デフォルト ルータ。	[デフォルト ルータ（Default Router）] フィールドの設定,（70 ページ）を参照してください。
DNS サーバ 1（DNS Server 1） DNS サーバ 2（DNS Server 2） DNS サーバ 3（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）]）。	[DNS サーバ（DNS Server）] フィールドの設定,（70 ページ）を参照してください。
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。	[代替 TFTP（Alternate TFTP）] フィールドの設定,（70 ページ）を参照してください。

オプション	説明	変更の手順
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。	[TFTP サーバ 1（TFTP Server 1）] フィールドの設定, （71 ページ）を参照してください。

オプション	説明	変更の手順
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。 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。	[TFTP サーバ 2（TFTP Server 2）] フィールドの設定, （71 ページ）を参照してください。 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。
BOOTP サーバ（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。	表示専用。

オプション	説明	変更の手順
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。

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（Administrator Settings）] > [ネットワークのセットアップ（Network Setup）] を選択します。

ステップ 3 [IPv4設定（IPv4 settings）] メニューにアクセスするには、[イーサネットの設定（Ethernet configuration）] > [IPv4のセットアップ（IPv4 Setup）] から IPv4 のオプションに移動します。

IPv6 のセット アップ

IPv6 アドレッシングが電話機でサポートされます。有効な IPv6 アドレスはサブネット プレフィックスを含めて最大 128 ビットです。

IPv6 アドレスは、次の形式のいずれかでなければなりません。

- コロンで区切られた、4 桁の 16 進数の 8 つのグループで構成され、左端の数字が最上位ビットを表します。各グループの先行する 0 または末尾の 0 は省略されることがあります。
- 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ます。これは、あるアドレスについて 1 度だけ可能なことに注意してください。

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

IPv6 が Unified クラスタで有効な場合、[IP アドレッシング モード（IP Addressing Mode）] のデフォルトは [IPv4 と IPv6（IPv4 and IPv6）]（デュアル スタック）です。このアドレッシング モードでは、電話機は IPv4 アドレス 1 個と IPv6 アドレス 1 個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、Unified CM へのコール制御シグナリングに IPv4 または IPv6 アドレスのいずれかを使用します。

詳細については、『*Cisco Unified Communications Manager Feature and Services Guide*』の「IPv6 Support in Cisco Unified Communications Devices」から「Common Device Configuration」についてのセクションを参照してください。

（注） 電話アドレッシング モードの設定として [IPv4 と IPv6（IPv4 and IPv6）] をお勧めします。IPv6 Only は、IPv4 インストール ベースと比べて機能にギャップがあるため、実稼働環境では推奨されていません。

IPv6 は、次のメニューのいずれかからセットアップします。

- WiFi が無効化されている場合：[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 が有効化されている場合：[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）]

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

オプション	Default value	説明
DHCPv6 有効（DHCPv6 Enabled）	有効	電話機が IPv6 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 によって SLAAC からまたは DHCPv6 サーバから IPv6 アドレスを取得します。DHCPv6 が無効の場合、電話機がステートフル（DHCPv6 サーバからの）またはステートレス（SLAAC から）の IPv6 ア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、自動設定が有効になっていれば電話機が SLAAC アドレスを生成できます。

オプション	Default value	説明
IPv6 アドレス（IPv6 Address）	::	電話機の現在の IPv6 アドレスを表示したり、新しい IPv6 アドレスを入力したりすることができます。 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ます。 このオプションを使用して IP アドレスを割り当てる場合は、IPv6 プレフィックス長とデフォルト ルータも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クス長を表示したり、新しいプレフィックス長を入力したりすることができます。 サブネット プレフィックス長は、10 進数で 1 ～ 128 です。
IPv6 デフォルトルータ（IPv6 Default Router）	::	電話機で使用されるデフォルト ルータを表示したり、新しい IPv6 デフォルト ルータを入力したりすることができます。
IPv6 DNS サーバ 1（IPv6 DNS Server 1）	::	電話機で使用されるプライマリ DNSv6 サーバを表示したり、新しいサーバを入力したりすることができます。
IPv6 DNS サーバ 2（IPv6 DNS Server 2）	::	電話機で使用されるセカンダリ DNSv6 サーバを表示したり、新しいセカンダリ DNSv6 サーバを設定したりすることができます。
IPv6 代替 TFTP（IPv6 Alternate TFTP）	なし	ユーザが代替（セカンダリ）IPv6 TFTP サーバを使用できるようにします。
IPv6 TFTP サーバ 1（IPv6 TFTP Server 1）	::	電話機で使用されるプライマリ IPv6 TFTP サーバを表示したり、新しいプライマリ TFTP サーバを設定した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 サーバが使用できないときにセカンダリ IPv6 TFTP サーバを表示するか、ユーザに新しいセカンダリ TFTP サーバの設定を許可します。
IPv6 アドレス解放（IPv6 Address Released）	なし	ユーザが IPv6 関連情報を解放できるようにします。

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 [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（Administrator Settings）] > [ネットワークのセットアップ（Network Setup）] を選択します。

ステップ 3 [IPv6 設定（IPv6 settings）] メニューにアクセスするには、次の手順のいずれかを実行します。

- Cisco Unified Communications Manager で Wi-Fi が無効化されている場合：[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）] に移動します。
- Cisco Unified Communications Manager で Wi-Fi 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）] に移動します。

ステップ 4 IPv6 アドレスを入力するには、

a) 入力するフィールドをクリックします。

b) フィールドの内容を変更します（次の情報を参照してください）。

次の表では、アドレス形式について説明します。

フォーマット	説明
X:X:X:X:X:X:X:X	コロンによって区切られた、8 グループの 16 進数。各グループの先行する 0 または末尾の 0 は省略されることがあります。 例：2001:db8:0:0:0:52:0:1
圧縮	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ます。 例：2001:db8::52:0:1

- アドレスにコロン（ : ）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。
- アドレスの各部分を入力してから、[適用（Apply）] または [復帰（Revert）] を押します。

ステップ 5 次の手順でトグル フィールドを変更します。

a) オプションが [いいえ（No）] に設定されている場合、[はい（Yes）] を押して有効にします。オプションが [はい（Yes）] に設定されている場合、[いいえ（No）] を押して無効にします。

b) [適用（Apply）] を押して変更を適用するか、[復帰（Revert）] を押して変更をキャンセルします。

[ドメイン名（Domain Name）] フィールドの設定

手順

ステップ 1 [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。

ステップ 2 [ドメイン名（Domain Name）] オプションまでスクロールし、[選択（Select）] を押して、新しいドメイン名を入力します。

ステップ 3 [適用（Apply）] を押します。

[管理 VLAN ID（Admin VLAN ID）] フィールドの設定

手順

ステップ 1 [管理 VLAN ID（Admin VLAN ID）] オプションまでスクロールし、[編集（Edit）] を押します。

ステップ 2 新しい VLAN ID 設定を入力します。

ステップ 3 [適用（Apply）] を押します。

ステップ 4 [保存（Save）] を押します。

[PC VLAN（PC VLAN）] フィールドの設定

手順

ステップ 1 [管理 VLAN ID（Admin VLAN ID）] オプションが設定されていることを確認します。

ステップ 2 PC VLAN オプションまでスクロールして [編集（Edit）] を押します。

ステップ 3 新しい PC VLAN 設定を入力します。

ステップ 4 [適用（Apply）] を押します。

ステップ 5 [保存（Save）] を押します。

[SW ポートのセットアップ（SW Port Setup）] フィールドの設定

手順

ステップ 1 [ネットワークの設定（Network Configuration）] のオプションのロックを解除します。

ステップ 2 [SW ポートのセットアップ（SW Port Setup）] オプションまでスクロールし、[選択（Select）] を押します。

ステップ 3 目的の設定値までスクロールし、[選択（Select）] を押します。

[PC ポートのセットアップ（SW Port Setup）] フィールドの設定

手順

ステップ 1 [ネットワークの設定（Network Configuration）] のオプションのロックを解除します。

ステップ 2 [PC ポートのセットアップ（SW Port Setup）] オプションまでスクロールし、[選択（Select）] を押します。

ステップ 3 目的の設定値までスクロールし、[選択（Select）] を押します。

[ワイヤレス（Wireless）] フィールドの設定

手順

ステップ 1 [ワイヤレス（Wireless）] オプションまでスクロールしてからトグル スイッチを使用すると、オンとオフの設定値を切り替えることができます。

ステップ 2 [適用（Apply）] を押します。

[WLAN サインインアクセス（WLAN Sign In Access）]、 フィールドの設定

手順

ステップ 1 [ワイヤレス サイン イン（Wireless Sign In）] オプションまでスクロールしてから、トグル スイッチを使用すると、オンとオフの設定値を切り替えることができます。

ステップ 2 [適用（Apply）] を押します。

[SSID] フィールドの設定

手順

ステップ 1 [SSID] オプションにスクロールし、[選択（Select）] を押し、SSID を入力します。

ステップ 2 [適用（Apply）] を押します。

[セキュリティ モード（Security Mode）] フィールドの設定

手順

ステップ 1 [セキュリティ モード（Security Mode）] オプションまでスクロールし、目的の値を強調表示します。

ステップ 2 [適用（Apply）] をクリックします。

[802.11 モード（802.11 Mode）] フィールドの設定

手順

ステップ 1 [802.11 モード（802.11 Mode）] オプションまでスクロールし、目的の値を強調表示します。

ステップ 2 [適用（Apply）] をクリックします。

[DHCP を使う（DHCP Enabled）] フィールドの設定

手順

ステップ 1 [DHCP を使う（DHCP Enabled）] オプションまでスクロールします。

ステップ 2 DHCP を無効にするには、[いいえ（No）] を押し、DHCP を有効にするには、[はい（Yes）] を押します。

[IP アドレス（IP Address）] フィールドの設定

手順

ステップ 1 [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。

ステップ 2 [IP アドレス（IP Address）] オプションまでスクロールし、[選択（Select）] を押して、新しい IP アドレスを入力します。

ステップ 3 [適用（Apply）] を押します。

[サブネット マスク（Subnet Mask）] フィールドの設定

手順

ステップ 1 [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。

ステップ 2 [サブネット マスク（Subnet Mask）] オプションまでスクロールし、[選択（Select）] を押して、新しいサブネット マスクを入力します。

ステップ 3 [適用（Apply）] を押します。

[デフォルト ルータ（Default Router）] フィールドの設定

手順

ステップ 1 [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。

ステップ 2 適切な [デフォルト ルータ（Default Router）] オプションまでスクロールし、[選択（Select）] を押して、新しいルータの IP アドレスを入力します。

ステップ 3 [適用（Apply）] を押します。

[DNS サーバ（DNS Server）] フィールドの設定

手順

ステップ 1 [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。

ステップ 2 適切な [DNS サーバ（DNS Server）] オプションまでスクロールし、[選択（Select）] を押して、新しい DNS サーバの IP アドレスを入力します。

ステップ 3 [適用（Apply）] を押します。

ステップ 4 複数の DNS サーバが設定できる場合、必要に応じて手順 2 と 3 を繰り返してバックアップ DNS サーバを割り当てます。

[代替 TFTP（Alternate TFTP）] フィールドの設定

手順

ステップ 1 [代替 TFTP（Alternate TFTP）] オプションにスクロールします。

ステップ 2 [編集（Edit）] を押します。

ステップ 3 電話機で代替 TFTP サーバを使用する場合は、[はい（Yes）] を押します。

ステップ 4 電話機で代替 TFTP サーバを使用しない場合は、[いいえ（No）] を押します。

[TFTP サーバ 1（TFTP Server 1）] フィールドの設定

手順

ステップ 1 必要に応じて（電話機の管理ドメインを変更する場合など）、CTL ファイルまたは ITL ファイルをロック解除します。CTL ファイルと ITL ファイルの両方がある場合は、いずれかのファイルをロック解除します。

ステップ 2 DHCP を有効にしている場合は、[代替 TFTP（Alternate TFTP）] オプションを [はい（Yes）] に設定します。

ステップ 3 [TFTP サーバ 1（TFTP Server 1）] オプションまでスクロールし、[選択（Select）] を押して、新しい TFTP サーバの IP アドレスを入力します。

ステップ 4 [適用（Apply）] を押し、[保存（Save）] を押します。

[TFTP サーバ 2（TFTP Server 2）] フィールドの設定

手順

ステップ 1 必要に応じて（電話機の管理ドメインを変更する場合など）、CTL ファイルまたは ITL ファイルをロック解除します。CTL ファイルと ITL ファイルの両方がある場合は、どちらかのファイルをロック解除します。

ステップ 2 [ネットワークの設定（Network Configuration）] のオプションのロックを解除します。

ステップ 3 [TFTP サーバ 1（TFTP Server 1）] オプションに IP アドレスを入力します。

ステップ 4 [TFTP サーバ 2（TFTP Server 2）] オプションまでスクロールし、[選択（Select）] を押して、新しいバックアップ TFTP サーバの IP アドレスを入力します。セカンダリの TFTP サーバがない場合は、[削除（Delete）] を使用して前の値のフィールドをクリアします。

ステップ 5 [適用（Apply）] を押してから、[保存（Save）] を押します。

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 Phone 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 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 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。

電話機の起動確認

Cisco IP Phone 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 Phone 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 CM の管理 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、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。

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 CM の管理で、[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）

第 5 章

Cisco Unified Communications Manager での電話機の設定

- Cisco IP Phone のセットアップ，75 ページ
- 電話機の MAC アドレスの決定，79 ページ
- 電話機の追加方法，79 ページ
- Cisco Unified Communications Manager へのユーザの追加，81 ページ
- エンド ユーザ グループへのユーザの追加，83 ページ
- 電話機とユーザの関連付け，83 ページ
- Survivable Remote Site Telephony，84 ページ
- Enhanced Survivable Remote Site Telephony，88 ページ
- Cisco Unified Communications Manager 機能のセットアップ，88 ページ

Cisco IP Phone 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 Phone 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 Phone サービス、または電話アプリケーションに影響する、電話機の使用状況情報

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，（252 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、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。

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 Phone 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 Phone サービスに登録できるのは、Cisco Unified Communications Manager の管理ページで IP Phone 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 Phone 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。フィールド名の横にあるアスタリスク（*）は、ユーザ ID や姓などの必須フィールドを示します。この手順では、Cisco Unified Communications Manager のグローバル ディレクトリにユーザ情報を追加します。

（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、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。

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（Save）] 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、Cisco IP Phone 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 ボタン > [電話の情報（Phone Information）] を押し、[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 Phone 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 の管理ページを使用して、個別の電話機を追加します。
- 一括管理ツール（BAT）を使用して複数の電話を追加します。
- 自動登録
- BAT と Tool for Auto-Registered Phones Support（TAPS）

電話機を個別に追加するか BAT を使用して追加するには、電話機の MAC アドレスを特定する必要があります。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、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。

関連トピック

電話機の自動登録の有効化, （40 ページ）

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（Add New）] 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、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。

ステップ 6 [保存（Save）] 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 の使用に関する詳細については、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 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（Add New）] 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（Save）] 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 へのユーザの追加

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。Cisco Unified Communications Manager によって、各ユーザは次のタスクを実行できます。

- Cisco IP Phone 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 Phone 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 へのユーザの直接追加, （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、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。

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

Cisco Unified Communications Manager へのユーザの直接追加

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 CM 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（Add New）] 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 ID（User ID）] : エンド ユーザの識別名を入力します。Cisco Unified Communications Manager では、ユーザ ID の作成後の変更はできません。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。使用できる特殊文字は、=、+、<、>、#、;、\、,、""、および空白です。
- [姓（Last Name）] : エンドユーザの姓を入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、""、および空白です。**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（Save）] をクリックします。

エンド ユーザ グループへのユーザの追加

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 *12*：*SRST* 機能のサポート

機能	サポート対象	注記
発信	あり	
終了	あり	
リダイヤル	あり	
応答	あり	
保留	あり	
復帰	あり	

機能	サポート対象	注記
会議	あり	
会議のアクティブ コール（参加）	なし	[アクティブ コール（Active Calls）] ソフトキーが表示されません。
会議リスト	なし	
転送	あり	
アクティブコールへの転送（直接転送）	なし	
自動応答	あり	
コール待機	あり	
発信者 ID	あり	
オーディオ メッセージ受信インジケータ	あり	
すべてのコールのプログラム可能な回線キー	あり	
応答のプログラム可能な回線キー	あり	
ユニファイド セッション プレゼンテーション	あり	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	あり	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	サポート対象	注記
すべてのコールの転送	あり	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。
スピード ダイヤル	あり	
サービスIRLのプログラム可能な回線キー	あり	
ボイスメールへの転送（即転送）	なし	[即転送（iDivert）] ソフトキーが表示されません。
回線のフィルタ	一部	回線はサポートされていますが、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。
拡張されたメッセージ待機インジケータ	なし	メッセージのカウント バッジが電話の画面に表示されません。 [メッセージ受信（Message Waiting）] アイコンのみが表示されます。

機能	サポート対象	注記
ダイレクト コール パーク	なし	ソフトキーが表示されません。
BLF	一部	BLF 機能キーはスピード ダイヤルキーのように動作します。
保留復帰	なし	コールは無期限に保留状態のままになります。
リモート回線の保留	なし	コールはローカル保留の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（PickUp）	なし	ソフトキーによるアクションがありません。
グループ ピックアップ	なし	ソフトキーによるアクションがありません。
その他のグループ ピックアップ	なし	ソフトキーによるアクションがありません。
迷惑呼 ID	なし	ソフトキーによるアクションがありません。
QRT	なし	ソフトキーによるアクションがありません。
Hunt Group	なし	ソフトキーによるアクションがありません。
インターコム	なし	ソフトキーによるアクションがありません。
モビリティ（Mobility）	なし	ソフトキーによるアクションがありません。
プライバシー	なし	ソフトキーによるアクションがありません。
折り返し	なし	[折返し（Call Back）] ソフトキーが表示されません。

機能	サポート対象	注記
[ビデオ（Video）]	○	ビデオ会議はサポートされません。
[ビデオ（Video）]	○	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（BLF Speed Dial）	○	

Enhanced Survivable Remote Site Telephony

Enhanced Conference Bridge Setup（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
- 話中ランプ 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。

Cisco Unified Communications Manager 機能のセットアップ

Cisco Unified CM の管理で、Cisco IP Phone のプロダクト固有の設定パラメータを設定できます。

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）]（[電話の設定（Phone Configuration）] ウィンドウ）[プロダクト固有の設定（Product Specific Configuration）] 部分
- [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）]（[共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウ）

- [システム（System）]>[エンタープライズ電話の設定（Enterprise Phone Configuration）]（[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ）

ステップ 2 パラメータの説明については、Cisco Unified CM の管理の [?] ボタンをクリックします。

ステップ 3 パラメータを設定するときは、更新する設定ごとに [共通設定の上書き（Override Common Settings）] チェックボックスを選択します。
このボックスをチェックしないと、対応するパラメータ設定が有効になりません。

3 つの設定ウィンドウでパラメータを設定した場合、設定の優先順序は次のとおりです。

1. [電話の設定（Phone Configuration）] ウィンドウ
2. [共通の電話プロファイル（Common Phone Profile）] ウィンドウ
3. [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ

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，91 ページ
- セルフ ケア ポータルへのアクセスの設定，92 ページ
- セルフ ケア ポータルの表示のカスタマイズ，92 ページ

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。

ユーザを Cisco Unified Communications セルフ ケア ポータルにアクセス可能にする前に、Cisco Unified Communications Manager Administration を使用して、ユーザを標準の 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（Self Care Portal）] 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。

  http://<server_name:portnumber>/ucmuser/（server_name は Web サーバ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 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、ユーザを Cisco Unified Communications Manager に追加したときに入力した値と同じです。

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。

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 ポータルへのアクセスの設定

ユーザがセルフケア ポータルにアクセスできるようにするには、この手順を使用します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] 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 ユーザを検索し、ユーザ ID のリンクをクリックします。

ステップ 3 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 4 [保存（Save）] 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。

- 呼出音設定の表示（Show Ring Settings）
- 回線のラベル設定の表示（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 CMの管理（Cisco Unified Communications Manager Administration）] 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 [セルフ ケア ポータル（Self Care Portal）] 領域で、[セルフ ケア ポータルのデフォルト サーバ（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（Save）] を選択します。

第 III 部

ハードウェアとアクセサリの設置

- Cisco IP Phone のアクセサリ，95 ページ
- Cisco IP Phone キー拡張モジュール，105 ページ
- 壁面取り付け，123 ページ

第 7 章

Cisco IP Phone のアクセサリ

- アクセサリ サポート，95 ページ
- フットスタンドの接続，96 ページ
- ケーブル ロックによる電話機の固定，97 ページ
- 外部スピーカおよびマイクロフォン，97 ページ
- ヘッドセット，97 ページ

アクセサリ サポート

次の表に、Cisco IP Phone 8800 シリーズでサポートされるアクセサリを示します。「X」は特定の電話モデルのサポートを示し、ダッシュ（—）はサポートされていないことを意味します。

表 *13*：*Cisco IP Phone 8800* シリーズのアクセサリ サポート

アクセサリ	タイプ	Cisco IP Phone 8811	Cisco IP Phone 8841	Cisco IP Phone 8845	Cisco IP Phone 8851	Cisco IP Phone 8851NR	Cisco IP Phone 8861	Cisco IP Phone 8865
シスコ製アクセサリ								
Cisco IP Phone 8800 キー拡張モジュール	アドオンモジュール	-	-	-	X	X	X	X
サードパーティ製アクセサリ								

アクセサリ	タイプ	Cisco IP Phone 8811	Cisco IP Phone 8841	Cisco IP Phone 8845	Cisco IP Phone 8851	Cisco IP Phone 8851NR	Cisco IP Phone 8861	Cisco IP Phone 8865
ヘッドセット：ヘッドセット，（97 ページ）を参照してください。この項では、各ヘッドセット タイプについて説明しています。	アナログ	X	X	X	X	X	X	X
	アナログ ワイドバンド	X	X	X	X	X	X	X
	Bluetooth	-	-	X	X	-	X	X
	USB（有線またはワイヤレス）	-	-	-	X	X	X	X
マイクロフォン：外部スピーカおよびマイクロフォン，（97 ページ）を参照してください。	外部 PC	-	-	-	-	-	X	X
スピーカー：外部スピーカおよびマイクロフォン，（97 ページ）を参照してください。	外部 PC	-	-	-	-	-	X	X

フットスタンドの接続

ユーザの電話機を卓上や机上に設置する場合、フットスタンドを電話機の背面に接続します。

手順

ステップ 1 コネクタをスロットに挿入します。

ステップ 2 コネクタがはまるまで、フットスタンドを押します。

ステップ 3 電話機の角度を調節します。

ケーブル ロックによる電話機の固定

最大 20 mm 幅のラップトップ ケーブル ロックで電話機を固定することができます。

手順

ステップ 1 ケーブル ロックのループの端を取り、電話機の固定場所となる物の周りに巻き付けます。

ステップ 2 ロックをケーブルのループの端まで通します。

ステップ 3 ケーブル ロックのロックを解除します。

ステップ 4 ロック ボタンを押したままにして、ロックの歯の位置を合わせます。

ステップ 5 ケーブル ロックを電話機のロック スロットに挿入し、ロック ボタンを放します。

ステップ 6 ケーブル ロックをロックします。

外部スピーカおよびマイクロフォン

外部スピーカおよびマイクロフォンは、プラグアンドプレイ式のアクセサリです。Cisco IP Phone では、外部 PC タイプのマイクロフォン、および増幅器で電力が供給されるスピーカーを、ラインイン/アウトのジャックを使用して接続できます。外部マイクロフォンを接続すると内部マイクロフォンが無効になり、外部スピーカを接続すると電話機の内部スピーカが無効になります。

（注） 低品質の外部オーディオデバイスを使用してラウドスピーカーを極端な大音量で再生したり、マイクロフォンをラウドスピーカーのごく近くに設置したりすると、スピーカーフォンの通話相手に不快なエコーが聞こえる場合があります。

ヘッドセット

シスコでは、Cisco IP Phone で使用するサードパーティ製ヘッドセットについて社内でテストを実施していますが、ヘッドセットや受話器のベンダーの製品については動作の保証やサポートは行っていません。

電話機を使用すると、ヘッドセットのマイクロフォンが検出するバックグラウンド ノイズの一部が軽減されますが、さらにこのバックグラウンド ノイズを削減して全体的なオーディオ品質を改善するには、ノイズを遮断するヘッドセットを使用することを推奨します。

シスコでは、不要な無線周波数（RF）信号および可聴周波数（AF）信号を遮蔽する高品質のヘッドセットといった外部デバイスの使用を推奨しています。ヘッドセットの品質や、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、雑音やエコーが入ることもあります。可聴ハム雑音などのノイズは、相手方だけに聞こえる場合もあれば、Cisco IP Phone のユーザおよび

相手方の両方に聞こえる場合もあります。ハム音やブザーのような雑音は、電灯、電気モーター、大型の PC モニタなど、さまざまな外部ソースが原因となり得ます。

（注） 場合によっては、ローカル電源キューブやパワー インジェクタを使用することにより、ハム雑音を軽減または除去できることがあります。

Cisco IP Phone を実際に展開する場合は、環境やハードウェアにより不整合が発生することもあるので、すべての環境に対してオールマイティなヘッドセットを見出すことは不可能です。

ヘッドセットを選定して環境に大規模に展開する前に、実際の環境での使用に最適かどうかをテストすることをお勧めします。

関連トピック

外部デバイス，（21 ページ）

音質

物理的、機械的、および技術的な性能以上に、ヘッドセットの音質がユーザと通話相手の双方にとって良質である必要があります。音質の判断は主観によるため、シスコが特定のヘッドセットのパフォーマンスを保証することは不可能です。しかし、大手メーカーのさまざまなヘッドセットについて、Cisco IP Phone で良好に作動することが報告されています。

詳細については、次の各項を参照してください。 http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html

アナログのヘッドセット

電話機はアナログ ヘッドセットが接続されたことを検出できません。このため、デフォルトで電話機画面の [アクセサリ（Accessories）] ウィンドウにアナログ ヘッドセットが表示されています。

デフォルトでアナログヘッドセットを表示すると、ユーザはアナログヘッドセットに対してワイドバンドを有効にすることができます。

関連トピック

アクセサリ サポート，（95 ページ）

アナログ ヘッドセットでのワイドバンドの有効化

アナログヘッドセットが電話機でサポートされていますが、電話機はアナログヘッドセットが接続されたことを検出できません。このため、デフォルトで電話スクリーンの [アクセサリ（Accessories）] ウィンドウにアナログ ヘッドセットが表示されています。

デフォルトでアナログヘッドセットを表示すると、ユーザはアナログヘッドセットに対してワイドバンドを有効にすることができます。

電話機はヘッドセットでワイドバンド コーデックをサポートしているかどうかを検出できませんが、ユーザは次の手順でアナログのヘッドセットでワイドバンドを有効化できます。

手順

ステップ 1 Cisco IP Phone で、アプリケーション を押します。

ステップ 2 [アクセサリ（Accessories）] を選択します。

ステップ 3 アナログのヘッドセットを強調表示し、[セットアップ（Setup）] を押します。

ステップ 4 ワイドバンドを有効にするには[オン（On）] を押し、ワイドバンドを無効にするには[オフ（Off）] を押します。

アナログ ヘッドセットでのワイドバンド コーデックの有効化

アナログヘッドセットが電話機でサポートされていますが、電話機はアナログヘッドセットが接続されたことを検出できません。このため、デフォルトで電話スクリーンの [アクセサリ（Accessories）] ウィンドウにアナログ ヘッドセットが表示されています。

デフォルトでアナログヘッドセットを表示すると、ユーザはアナログヘッドセットに対してワイドバンドを有効にすることができます。

画面にオン/オフ ソフトキーが表示されない場合は、次の手順に従って、ユーザがアナログ ヘッドセットでワイドバンド コーデックを有効にできることを確認してください。

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 [電話の検索と一覧表示（Find and List Phones）] ウィンドウで、アナログのヘッドセットを追加する電話機の検索条件を入力し、[検索（Find）] をクリックします。

ステップ 3 目的の [デバイス名（Device Name）] をクリックします。[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration）] のレイアウト部分で、[ワイドバンド ヘッドセット UI 設定（Wideband Headset UI Control）] というオプションが有効になっていることを確認します。このオプションは、デフォルトで有効です。

ステップ 5 [電話の設定（Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration）] レイアウト部分で、[ワイドバンド ヘッドセット（Wideband Headset）] オプションを設定することもできます。（このオプションもデフォルトで有効です）。

有線ヘッドセット

有線ヘッドセットでは、音量ボタンやミュートボタンも含めて、Cisco IP Phone のすべての機能を使用できます。これらのボタンを使用して、ヘッドセットの音量を調整したり、ヘッドセット マイクからの音声が相手に聞こえないようにしたりすることができます。

有線ヘッドセットへの接続

有線ヘッドセットを Cisco IP Phone に接続するには、次の手順を実行します。

手順

ステップ 1 ヘッドセットを電話機の背面にあるヘッドセット ポートに差し込みます。

ステップ 2 電話の発信または応答を行うには、電話機のヘッドセット ボタンを押します。

有線ヘッドセットの無効化

ヘッドセットを無効にするには、Cisco Unified Communications Manager の管理ページを使用します。ヘッドセットを無効にすると、スピーカフォンも無効になります。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページでヘッドセットを無効にするには、[デバイス（Device）] > [電話（Phone）] を選択し、変更する電話機を見つけます。

ステップ 2 [電話の設定（Phone Configuration）] ウィンドウ（[プロダクト固有の設定（Product Specific Configuration）] レイアウト部分）で、[スピーカーフォンとヘッドセットの無効化（Disable Speakerphone and Headset）] チェックボックスをオンにします。

USB ヘッドセット

有線およびワイヤレスの USB ヘッドセットがサポートされています。背面 USB ポート（ユーザの電話機にこのポートがある場合）または側面 USB ポートに USB ヘッドセット（またはワイヤレス ヘッドセットの場合はベース ステーション）を接続できます。

USB ヘッドセットの有効化

Cisco Unified Communications Manager の管理ページ（表示されるウィンドウの [プロダクト固有の設定（Product Specific Configuration）] のレイアウト部分）で、使用可能な USB ポート（背面 USB ポートのパラメータまたは側面 USB ポートのパラメータ）を有効にする必要があります。また、

Cisco Unified Communications Manager の管理ページで、USB クラスを有効化/無効化するパラメータとして [オーディオ クラス（Audio Class）] が選択されていることも確認します。

手順

ステップ 1 次のいずれかのウィンドウで USB ヘッドセットを有効にします。

- [電話の設定（Phone Configuration）]（[デバイス（Device）] > [電話（Phone）]）。
- [エンタープライズ電話の設定（Enterprise Phone Configuration）]（[システム（System）]>[エンタープライズ電話の設定（Enterprise Phone Configuration）]）。
- [共通の電話プロファイルの設定（Common Phone Profile 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）]）。

ステップ 2 設定ウィンドウで対応する [共通設定の上書き（Override Common Settings）] パラメータを確認します。

USB ヘッドセットの無効化

USB ヘッドセットを無効化するには、Cisco Unified Communications Manager の管理ページで有効化した USB ポート（またはオーディオ クラスのパラメータ）を無効化します。また、電話機の [アクセサリ（Accessories）] ウィンドウから別のタイプのヘッドセットを選択することもできます。この選択により、直前に有効にしていたヘッドセットが無効になります。

手順

ステップ 1 次のいずれかのウィンドウで USB ヘッドセットを無効にします。

- [電話の設定（Phone Configuration）]（[デバイス（Device）] > [電話（Phone）]）。
- [エンタープライズ電話の設定（Enterprise Phone Configuration）]（[システム（System）]>[エンタープライズ電話の設定（Enterprise Phone Configuration）]）。
- [共通の電話プロファイルの設定（Common Phone Profile 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）]）。

ステップ 2 設定ウィンドウで対応する [共通設定の上書き（Override Common Settings）] パラメータを確認します。

ワイヤレス ヘッドセット

Cisco IP Phone では、ワイヤレス ヘッドセットを使用できます。

シスコの Web サイトではご使用の IP 電話機で動作するワイヤレス ヘッドセットについて説明しています。次の URL にアクセスします。

http://www.cisco.com/en/US/partner/prod/voicesw/ucphone_headsets.html

ヘッドセットの接続およびこの機能の使用については、ワイヤレス ヘッドセットのマニュアルを参照してください。

電子フックスイッチの有効化

電子フックスイッチ機能は、次のヘッドセット デバイスをサポートします。

- Jabra
  - PRO9400 および GO6400 シリーズ
  - PRO930
  - GN9300 シリーズ
  - GN9120
- Plantronics
  - Savi DECT 740、CS5xx DECT

手順

ステップ 1 [Cisco Unified CM の管理（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 [ワイヤレス ヘッドセット フックスイッチ コントロール（Wireless Headset Hookswitch Control）] セクションにスクロールします。

ステップ 3 [有効（Enable）] または [無効（Disable）] を選択します。

Bluetooth ワイヤレス ヘッドセット

Cisco IP Phone 8811、8841、および 8851NR は Bluetooth ワイヤレス ヘッドセットをサポートしていません。

サポートされているヘッドセットのリストについては、http://www.cisco.com/c/en/us/products/unified-communications/ucphone_headsets.html を参照してください。

Bluetooth では、66 フィート（20 m）の範囲内の低帯域幅でワイヤレス接続を行えます。最大のパフォーマンスが得られるのは、1 ～ 2 m（3 ～ 6 フィート）の範囲内です。Bluetooth ワイヤレス テクノロジーは、2.4 GHz 帯域で動作します。これは 802.11b/g 帯域と同じです。これは干渉が発生する可能性があります。シスコでは次を推奨しています。

- 5 GHz 帯域で動作する 802.11a、802.11n または 802.11ac を使用します。

- 他の 802.11b/g デバイス、Bluetooth デバイス、電子レンジ、大型の金属製品との間隔をあけます。

Cisco IP Phone は、共有キーによる認証と暗号化方式を利用してヘッドセットと接続します。Cisco IP Phone は最大 50 のヘッドセットをひとつずつ接続できます。最後に接続されたヘッドセットがデフォルトとして使用されます。通常、ペアリングはヘッドセットごとに 1 回実行されます。

デバイスがペア化された後、両方のデバイス（電話機とヘッドセット）が有効化済みで、相互の有効範囲内にある限り、その Bluetooth 接続が維持されます。この接続は通常、一方のデバイスの電源が切断された後、再び電源が投入されると、自動的に接続を再確立します。ただし、一部のヘッドセットでは、ユーザによる接続の再確立が必要です。

Bluetooth アイコン は、デバイスが接続されているかどうかに関係なく、Bluetooth がオンかどうかを示します。

干渉が発生する可能性が考えられます。シスコでは、他の 802.11b/g デバイス、Bluetooth デバイス、電子レンジ、大型の金属製の物体を近くに置かないように推奨しています。可能であれば、他の 802.11 デバイスで 802.11a チャネルを使用するように設定してください。

Bluetooth ワイヤレス ヘッドセットが動作するために、ヘッドセットが電話機の直接の見通し線内にある必要はありませんが、壁やドアなどの障害物、および他の電子デバイスからの干渉が接続に影響を及ぼすことがあります。

ヘッドセットが Cisco IP Phone から 30 フィート（10 m）を超えて離れていると、Bluetooth の接続は 15 ～ 20 秒間のタイムアウト後にドロップされます。ペア化されたヘッドセットが Cisco IP Phone の範囲内に戻ってきたときに、当該電話機が別の Bluetooth ヘッドセットに接続されていなければ、範囲内にある Bluetooth ヘッドセットと自動的に再接続します。電力節約モードで動作する一部のタイプの電話機では、再接続を開始するために、ユーザがオペレーション ボタンを押してヘッドセットを「ウェイクアップ」させることができます。

ヘッドセットを有効にしてから、電話アクセサリとして追加します。

電話機はさまざまハンズフリー プロファイル機能をサポートしており、電話機を操作しなくてもハンズフリーデバイス（Bluetooth ワイヤレス ヘッドセットなど）を使用して特定のタスクを実行できます。たとえば、電話機で [リダイヤル（Redial）] を押す代わりに、Bluetooth ワイヤレス ヘッドセットからそのメーカーの手順に従って電話番号をリダイヤルできます。

次の各ハンズフリー機能は、Cisco IP Phone 8845、8851、8861、および 8865 で使用する Bluetooth ワイヤレス ヘッドセットに適用されます。

- コールへの応答
- コールの終了
- ヘッドセットのコールの音量を変更する
- リダイヤル
- 発信者 ID
- 転送
- 保留して許可

- リリースして許可

各種ハンズフリー デバイスは、それぞれ機能のアクティブ化方法が異なります。デバイスのメーカーが、同じ機能を指すときに異なる用語を使用している可能性もあります。

重要 常に 1 つのヘッドセット タイプしか機能しないため、Bluetooth ヘッドセットとアナログ ヘッドセットの両方を使用しており、アナログ ヘッドセットを電話機に接続している場合は、Bluetooth ヘッドセットを有効にするとアナログ ヘッドセットが無効になります。アナログ ヘッドセットを有効にする場合は、Bluetooth ヘッドセットを無効にします。Bluetooth ヘッドセットが有効になっている電話機に USB ヘッドセットを接続すると、Bluetooth とアナログの両方のヘッドセットが無効になります。USB ヘッドセットの接続を外した場合は、Bluetooth ヘッドセットの有効化またはアナログ ヘッドセットを使用するための Bluetooth ヘッドセットの無効化のいずれかができるようになります。

Bluetooth ワイヤレス ヘッドセットの使用方法については、次の資料を参照してください。

- 『*Cisco IP Phone 8800 Series User Guide for Cisco Unified Communications Manager*』
- ヘッドセットに付属するユーザ ガイド

Bluetooth ワイヤレス ヘッドセットの有効化

ユーザが Bluetooth ワイヤレス ヘッドセットを使用する前にイネーブル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、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 変更する電話機を特定し、その電話機の [電話の設定（Phone Configuration）] ウィンドウに進みます。

ステップ 3 [電話の設定（Phone Configuration）] ウィンドウで、Bluetooth の設定に [有効（Enable）] を選択し、[Bluetooth のプロファイル（Bluetooth Profiles）] の設定に [ハンズフリー（Handsfree）] を選択します。

ステップ 4 変更を保存します。

第 8 章

Cisco IP Phone キー拡張モジュール

- Cisco IP Phone は、拡張モジュールのセットアップの概要を調整します，105 ページ
- KEM 電源情報，106 ページ
- Cisco IP Phone への 1 台の KEM の接続，109 ページ
- Cisco IP Phone への 2 ～ 3 台の KEM の接続，113 ページ
- キー拡張モジュールの Cisco Unified CM の管理でのセットアップ，117 ページ
- キー拡張モジュール セットアップへのアクセス，119 ページ
- キー拡張モジュールのリセット，120 ページ
- キー拡張モジュールのトラブルシューティング，120 ページ

Cisco IP Phone は、拡張モジュールのセットアップの概要を調整します

Cisco IP Phone 8800 キー拡張モジュール（KEM）により、ライン アピアランス、短縮ダイヤル、またはプログラム可能なボタンを電話機に追加できます。プログラム可能ボタンは、電話回線ボタン、短縮ダイヤル ボタン、または電話機能ボタンとして設定できます。

次の表に、電話機のモデルと、各モデルでサポートされるキー拡張モジュールの数を示します。

表 *14*：*Cisco IP Phone* とサポートされる *KEM* の数

Cisco IP Phone モデル	サポートされる KEM の数
Cisco IP Phone 8851 および 8851NR	KEM 2 台（72 の回線またはボタン）
Cisco IP Phone 8861	KEM 3 台（108 の回線またはボタン）
Cisco IP Phone 8865	KEM 3 台（108 の回線またはボタン）

関連トピック

壁面取り付け，（123 ページ）
アクセサリ サポート，（95 ページ）

KEM 電源情報

Cisco IP Phone 8800 キー拡張モジュール電力消費量と電源要件は次のとおりです。

消費電力

KEM 1 台あたり 48V DC、5W

電源要件

電話機は 1 台の KEM に直接電力を供給できます。詳細については、次の表を参照してください。

スマートフォンまたはタブレットを充電する場合は、次の点に注意してください。

- 側面の USB：最大 500mA/2.5W の充電。
- 背面の USB：高速充電。最大 2.1A/10.5W の充電。

表 *15*：*Cisco IP Phone 8800* シリーズ：電力概要

	Cisco IP Phone 8851 および 8851NR	Cisco IP Phone 8861 および 8865
スマートフォンの充電	あり（802.3af）	あり（802.3af）
タブレットの充電	N/A（背面 USB なし）	あり（802.3 aT）（スマートフォンの充電も可能）
KEM X 1	あり（802.3af）	あり（802.3 aT）（スマートフォンの充電も可能）

	Cisco IP Phone 8851 および 8851NR	Cisco IP Phone 8861 および 8865
KEM X 2	あり（電源ブリック）	あり（802.3 aT）（スマートフォンの充電も可能）
KEM X 3	N/A（2 KEM のみ）	あり（802.3 aT）（スマートフォンの充電も可能）
KEM X 1 + タブレットの充電	N/A（背面 USB なし）	あり（802.3 aT）（スマートフォンの充電も可能）
KEM X 2 + タブレットの充電	N/A（背面 USB なし）	あり（電源ブリック）または UPOE（Cisco IP Phone 8865）
KEM X 3 + タブレットの充電	N/A（2 KEM のみ）	あり（電源ブリック）または UPOE（Cisco IP Phone 8865）

表 *16*：キー拡張モジュールの電源

	Cisco IP Phone 8851 および 8851NR			Cisco IP Phone 8861			Cisco IP Phone 8865		
アクセサリ	802.3af PoE	802.3at PoE	Cisco IP Phone Power Cube 4	802.3af PoE	802.3at PoE	Cisco IP Phone Power Cube 4	802.3af PoE	802.3at PoE	Cisco IP Phone Power Cube 4
1 台の KEM	サポート対象	802.3at は 802.3af との後方互換性があるため、KEM は強化されます。	サポート対象	未サポート	サポート対象	サポート対象	未サポート	サポート対象	サポート対象
2 台の KEM	未サポート	未サポート	サポート対象	未サポート	サポート対象	サポート対象	未サポート	サポート対象	サポート対象
3 台の KEM	未サポート	未サポート	N/A	未サポート	サポート対象	サポート対象	未サポート	サポート対象	サポート対象
1 台の KEM + タブレット充電	未サポート	未サポート	未サポート	未サポート	サポート対象	サポート対象	未サポート	サポート対象	サポート対象

	Cisco IP Phone 8851 および 8851NR			Cisco IP Phone 8861			Cisco IP Phone 8865		
アクセサリ	802.3af PoE	802.3at PoE	Cisco IP Phone Power Cube 4	802.3af PoE	802.3at PoE	Cisco IP Phone Power Cube 4	802.3af PoE	802.3at PoE	Cisco IP Phone Power Cube 4
2 台の KEM + タブレット充電	未サポート	未サポート	未サポート	未サポート	未サポート	サポート対象	未サポート	未サポート	サポート対象
3 台の KEM + タブレット充電	未サポート	未サポート	未サポート	未サポート	未サポート	サポート対象	未サポート	未サポート	サポート対象
スマートフォンの充電（KEM の接続なし）	○	○	未サポート	○	○	未サポート	○	○	○
タブレットの充電	○	○	未サポート	○	○	未サポート	○	○	○

（注） 複数の KEM を Cisco IP Phone 8861 および 8865 に接続する場合、背面の USB ポートを使用した高速充電機能はサポートされません。この場合、背面ポートによってデバイスは低速で充電されます。

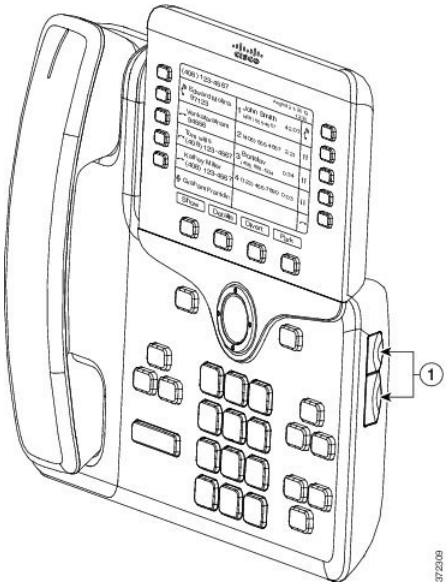
Cisco IP Phone への 1 台の KEM の接続

手順

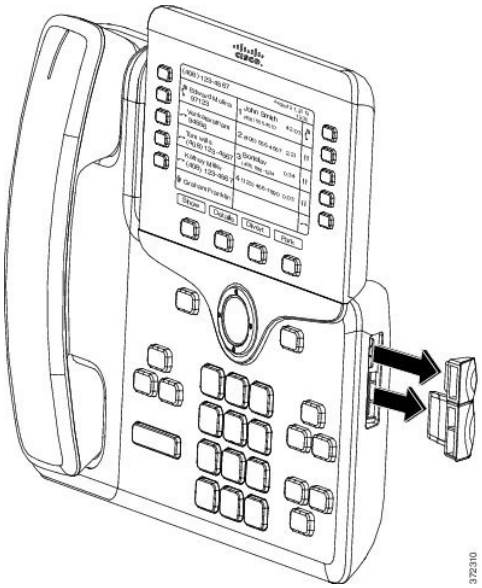
ステップ 1 電話機からイーサネット ケーブルを抜き取ります。

ステップ 2 装着されている場合、電話機からフットスタンドを取り外します。

ステップ 3 電話機側面のアクセサリ コネクタ カバーを探します。
次の図は、アクセサリ コネクタ カバーの位置を示します。



ステップ 4 2 つのアクセサリ コネクタ カバーを取り外します。
次の図は、アクセサリ コネクタ カバーの取り外しを示します。



注目　スロットはスパイン コネクタ専用に設計されています。他の物体を挿入すると、修理が必要な損傷が電話機に発生します。

ステップ 5　電話機の正面を上に向けます。

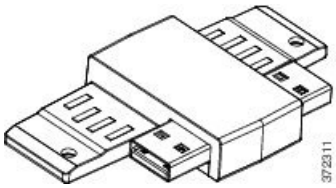
ステップ 6　KEM スパイン コネクタの一端を Cisco IP Phone のアクセサリ コネクタに差し込みます。

a) アクセサリ コネクタ ポートとスパイン コネクタの位置を合わせます。

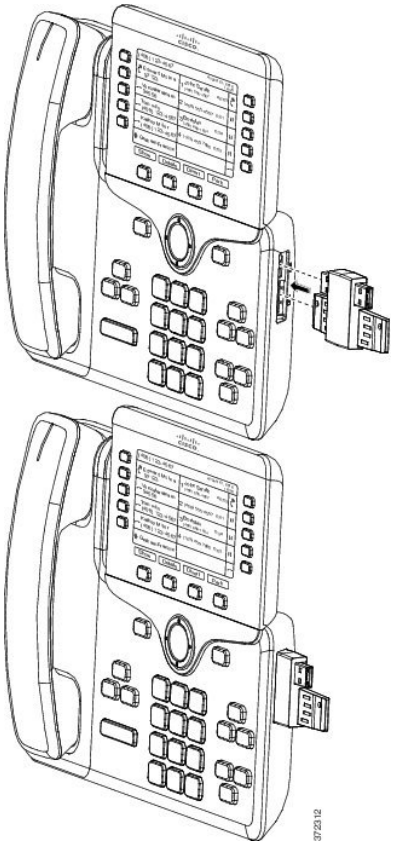
（注）　次の図に示す向きにコネクタを取り付けます。

b) 電話機へスパイン コネクタをしっかり押し込みます。

次の図は、スパイン コネクタを示します。



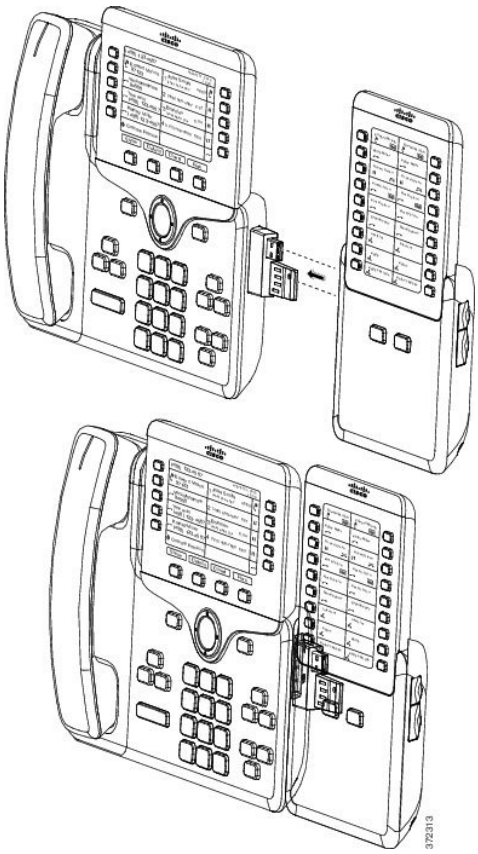
次の図は、スパイン コネクタの取り付け図を示します。



ステップ 7 次の図に示すように、スパイン コネクタのもう一方の端を KEM に接続します。

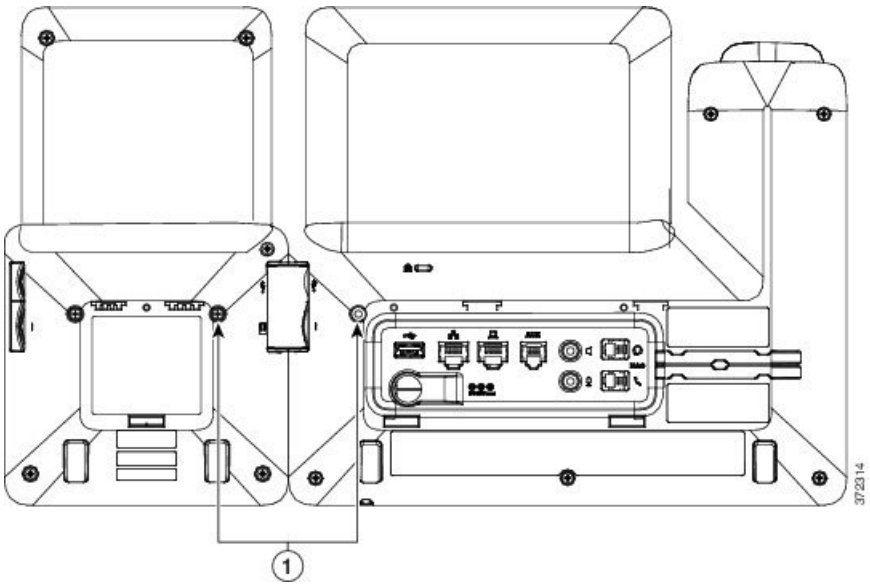
a) KEM アクセサリ コネクタ ポートとスパイン コネクタの位置を合わせます。

b) KEM をスパイン コネクタにしっかり押し込みます。



ステップ 8　ドライバを使用して電話機にネジを固定します。

この手順によって、電話機と KEM が確実に常時接続されるようにします。次の図は、電話機と KEM のネジ穴の位置を示します。



（注）　ネジが電話機にしっかり挿入され、締め付けられていることを確認します。

ステップ 9 （任意） フット スタンドを電話機と KEM に装着し、作業場所に平らに置けるよう両方のフット スタンドを調節します。

ステップ 10 電話機にイーサネット ケーブルを挿入します。

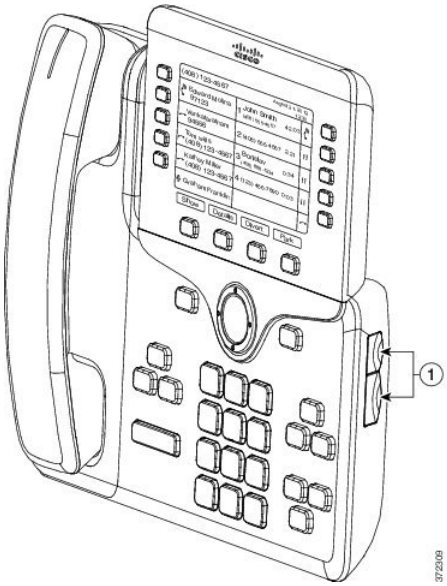
Cisco IP Phone への 2 ～ 3 台の KEM の接続

手順

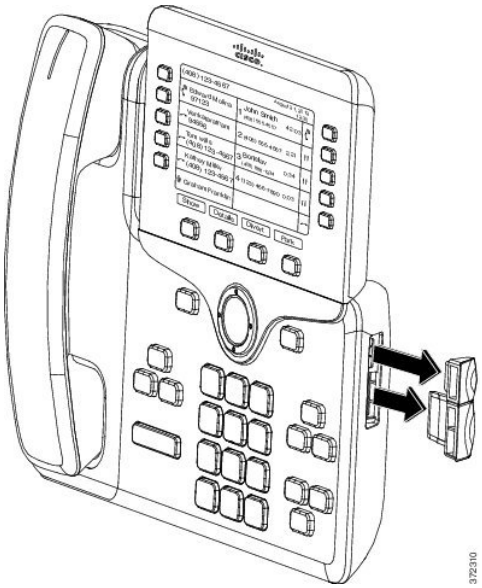
ステップ 1 電話機からイーサネット ケーブルを抜き取ります。

ステップ 2 装着されている場合、電話機からフットスタンドを取り外します。

ステップ 3 電話機側面のアクセサリ コネクタ カバーを探します。
次の図は、アクセサリ コネクタ カバーの位置を示します。



ステップ 4 2 つのアクセサリ コネクタ カバーを取り外します。
次の図は、アクセサリ コネクタ カバーの取り外しを示します。



注目　スロットはスパイン コネクタ専用に設計されています。他の物体を挿入すると、修理が必要な損傷が電話機に発生します。

ステップ 5　電話機の正面を上に向けます。

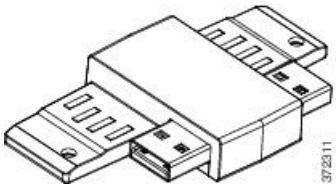
ステップ 6　KEM スパイン コネクタの一端を Cisco IP Phone のアクセサリ コネクタに差し込みます。

a) アクセサリ コネクタ ポートとスパイン コネクタの位置を合わせます。

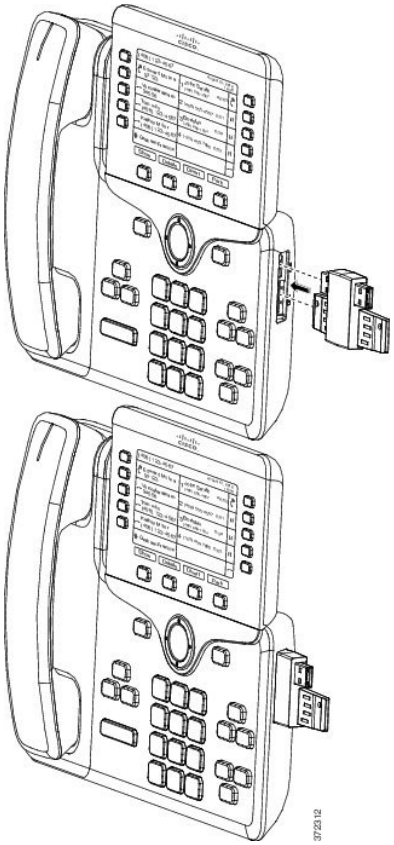
（注）　次の図に示す向きにコネクタを取り付けます。

b) 電話機へスパイン コネクタをしっかり押し込みます。

次の図は、スパイン コネクタを示します。



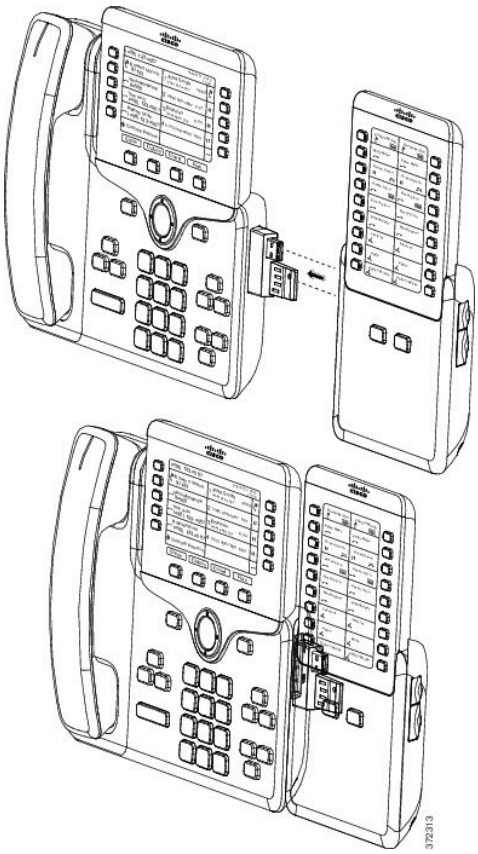
次の図は、スパイン コネクタの取り付け図を示します。



ステップ 7　次の図に示すように、スパイン コネクタのもう一方の端を KEM に接続します。

a) KEM アクセサリ コネクタ ポートとスパイン コネクタの位置を合わせます。

b) KEM をスパイン コネクタにしっかり押し込みます。

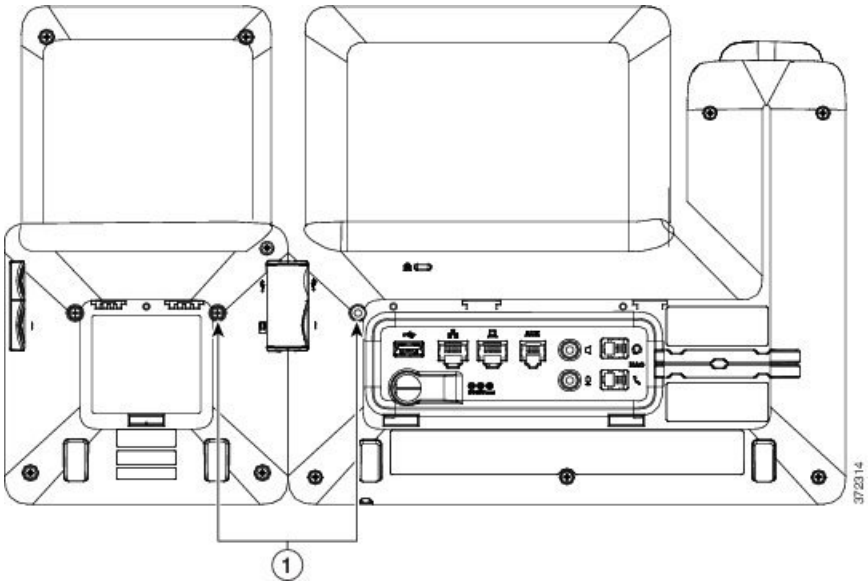


1 台目の KEM が Cisco IP Phone に接続されました。

ステップ 8 別の KEM スパイン コネクタを使用して、2 台目の KEM を 1 台目の KEM に接続します。

ステップ 9 3 つ目の KEM スパイン コネクタを使用して、3 台目の KEM を 2 台目（中間）の KEM に接続します。次の図は、3 台の KEM を接続した Cisco IP Phone です。

ステップ 10 ドライバを使用して電話機および各 KEM にネジを固定します。
この手順によって、電話機と KEM が確実に常時接続されるようにします。次の図は、ネジ穴の位置を示します。



（注） ネジが電話機にしっかり挿入され、締め付けられていることを確認します。

ステップ 11 （任意） フット スタンドを電話機と KEM に装着し、作業場所に平らに置けるようすべてのフットスタンドを調節します。

ステップ 12 電話機にイーサネット ケーブルを挿入します。

キー拡張モジュールの Cisco Unified CM の管理でのセットアップ

キー拡張モジュール（KEM）のセットアップ時に、KEM の表示を 1 列モードまたは 2 列モードに設定できます。

1 列モード

1 列モードでは、画面の各行が 1 本の回線に対応し、この回線には左側のボタンと右側のボタンのいずれかでアクセスできます。この設定では、キー拡張モジュールは 1 ページ目に 9 回線、2 ページ目に 9 回線を表示します。次の図は、1 列モードを示します。

2 列モード

2列モードでは、画面の左側のボタンと右側のボタンとが、それぞれ異なる回線に割り当てられます。この設定では、キー拡張モジュールは 1 ページ目に 18 回線、2 ページ目に 18 回線を表示します。次の図は、2 列モードを示します。

（注） 1 列モードおよび 2 列モードの両方で、ラベルが表示スペースより長い場合、テキスト省略記号（…）が含まれます。

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。
[電話の検索と一覧表示（Find and List Phones）] ウィンドウが表示されます。Cisco IP Phone 8800 キー拡張モジュール を設定する 1 つ以上の電話機を検索できます。

ステップ 2 検索条件を選択するか入力して、[検索（Find）] をクリックします
[電話の検索と一覧表示（Find and List Phones）] ウィンドウに、検索基準を満たす電話機の一覧が表示されます。

ステップ 3 Cisco IP Phone 8800 キー拡張モジュール を設定する電話機をクリックします。[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウの右側にあるペインで [拡張モジュール情報（Expansion Module Information）] セクションまでスクロール ダウンし、[モジュール 1（Module 1）]、[モジュール 2（Module 2）]、[モジュール 3（Module 3）] の順にこれらのフィールドで適切な拡張モジュールを選択します（または [なし（none）]）。
電話機のモデルごとにサポートされる KEM 台数については、Cisco IP Phone は、拡張モジュールのセットアップの概要を調整します，（105 ページ） を参照してください。

ステップ 5 電話機に接続されている KEM を最大限に活用できるように設定された電話ボタン テンプレート（[電話の設定（Phone Configuration）] ウィンドウの [デバイス情報（Device Information）]）を選択してください。

ステップ 6 要件に応じて、1 列モードの場合は [KEM を 1 列表示（One Column Display for KEM）] フィールドを有効にし、2 列モードの場合は無効にします。

ステップ 7 [保存（Save）] をクリックします。

キー拡張モジュール セットアップへのアクセス

電話機に 1 台以上の KEM を取り付けて、Cisco Unified Communications Manager の管理ページで設定すると、KEM は電話機によって自動的に認識されます。

複数の KEM が取り付けられている場合は、電話機に接続された順に番号が付きます。

- キー拡張モジュール 1 は電話機に一番近い KEM です。
- キー拡張モジュール 2 は中央の KEM です。
- キー拡張モジュール 3 は一番右側の KEM です。

KEM を選択してから、次のいずれかのソフトキーを選択します。

- [終了（Exit）] : [アプリケーション（Applications）] メニューに戻ります。
- [詳細（Details）] : 選択された KEM の詳細を提供します。
- [セットアップ（Setup）] : 選択した KEM の明るさを設定できます。明るさの設定は、電話機の [設定（Preferences）] メニューでも実行できます。

手順

ステップ 1 電話機で、アプリケーション を押します。

ステップ 2 [アクセサリ（Accessories）] を押します。
適切に取り付けられ、設定された KEM はすべて、アクセサリのリストに表示されます。

キー拡張モジュールのリセット

この手順では、拡張モジュールを工場出荷時の状態にリセットする方法を説明します。

手順

ステップ 1 KEM に電源を入れ、[ページ 1（Page 1）] を押し、キーを押したままにします。LCD が白に変わってから少なくとも 1 秒間、ページ 1 を押し続けます。

ステップ 2 ページ 1 を離すと、LED が赤くなります。すぐに [ページ 2（Page 2）] を押し、少なくとも 1 秒間は [ページ 2（Page 2）] を押し続けます。

ステップ 3 ページ 2 を離すと、すべての LED がオレンジになります。

ステップ 4 回線 5、14、1、18、10、9 の順に押します。
LCD が青に変わり、スピニング ローダのアイコンが中央に表示されます。

KEM がリセットされます。

キー拡張モジュールのトラブルシューティング

キー拡張モジュール（KEM）のトラブルシューティング情報を取得するには、次の手順を実行します。

手順

ステップ 1 CLI を開きます。

ステップ 2 次のコマンドを入力してデバッグ モードを開始します。
debugsh

ステップ 3 「?」を入力すると、使用可能なすべてのコマンドとオプションが表示されます。

ステップ 4 適切なコマンドとオプションを使用して、必要な KEM 情報を検索します。

ステップ 5 デバッグ モードを終了するには、Ctrl キーを押した状態で C キーを押します。

第 9 章

壁面取り付け

- 壁面取り付けオプション，123 ページ
- ロックできない壁面取り付けコンポーネント，123 ページ
- キー拡張モジュール付き電話用ロック非対応壁面取り付けコンポーネント，130 ページ
- 電話機のロック対応壁面取り付けコンポーネント，137 ページ
- キー拡張モジュール付き電話用ロック対応壁面取り付けコンポーネント，143 ページ
- ハンドセット レストの調整，148 ページ

壁面取り付けオプション

次の壁面取り付けオプションを入手できます。

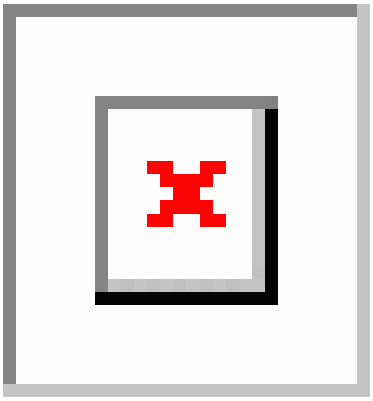
- Cisco IP Phone 8800 シリーズ壁面取り付けキット：Cisco IP Phone 8800 シリーズ用のロック非対応壁面取り付けキット。このキットは、Cisco IP Phone 8811、8841、8851、8851Nr、および 8861 に該当します。PID は CP-8800-WMK= です。
- Cisco IP Phone 8800 ビデオ シリーズ用壁面取り付けキット：Cisco IP Phone 8845 および 8865 に装着されるロック対応壁面取り付けキット。PID は CP-8800-VID-WMK= です。
- Cisco IP Phone 8800 シリーズ壁面取り付けキットと 1 台の KEM：キットは Cisco IP Phone 8800 キー拡張モジュールが接続された Cisco IP Phone 8851、8851NR、および 8861 に装着されます。PID は CP-8800-BEKEM-WMK= です

ロックできない壁面取り付けコンポーネント

ここでは、Cisco IP Phone 8800 シリーズ壁面取り付けキット の取り付け方法について説明します。

次の図は、Cisco IP Phone 8800 シリーズ壁面取り付けキット のコンポーネントを示しています。

図 *2*：コンポーネント

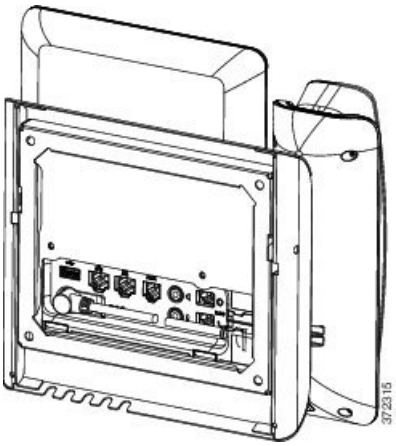


同梱物は、次のとおりです。

- 電話機用ブラケット x 1 個
- 壁面用ブラケット x 1 個
- #8-18 x 1.25 インチのプラス ネジ x 4 個、アンカー x 4 個
- K30 x 8 mm のセルフタッピング ネジ x 2 本
- 6 インチのイーサネット ケーブル X 1 本

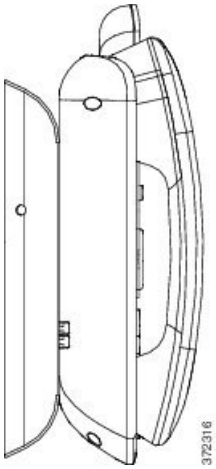
次の図は、電話機に設置されている壁面取り付けキットを示します。

図 *3*：電話機に装着した壁面取り付けキットの背面



次の図は、壁面取り付けキットが設置された電話機の側面を示します。

図 *4*：電話機に装着した壁面取り付けキットの側面



電話へのロック非対応壁面取り付けキットの取り付け

壁面取り付けキットはコンクリート、れんが、または同様の硬い表面を含むほとんどの表面に配置できます。コンクリート、れんが、または同様の硬い表面にキットを取り付けるには、壁の表面に合ったネジとアンカーを用意する必要があります。

はじめる前に

ブラケットの取り付けには、次の工具が必要です。

- #1 と #2 のプラス ドライバー
- 水準器
- 鉛筆

現在、目的の位置に電話用のイーサネットジャックが存在しない場合は、イーサネットジャックも設置します。このジャックには、イーサネット接続のために適切に配線されている必要があります。通常の電話ジャックは使用できません。

手順

ステップ 1 取り付け位置に、壁面用ブラケットを取り付けます。ブラケットをイーサネット ジャックにかぶせて取り付けることも、近くのジャックまでイーサネットネットワーク ケーブルを配線することもできます。

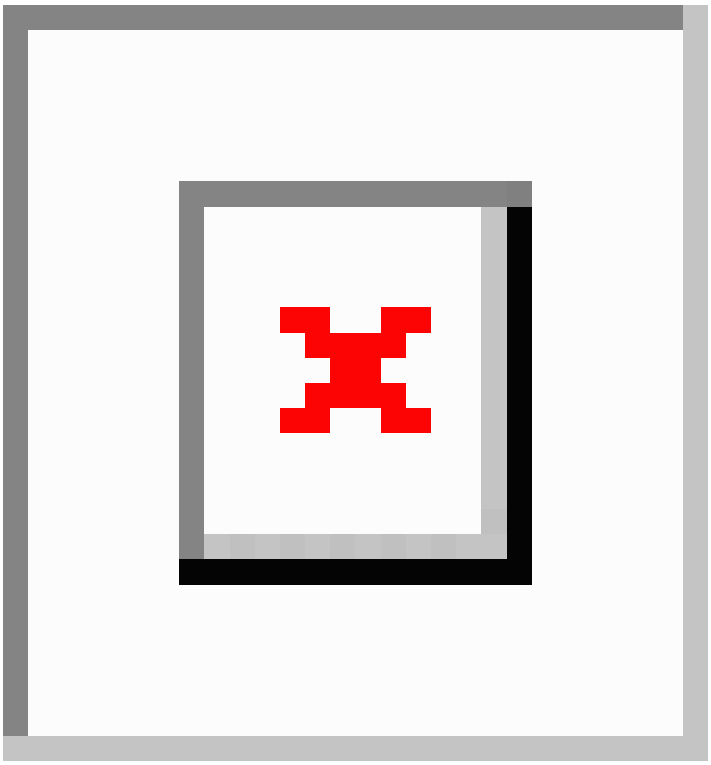
（注） ジャックを電話機の背面に配置する場合は、イーサネット ジャックを壁にぴったり付けるか、埋め込む必要があります。

a) ブラケットの背面の矢印が上向きになるように、ブラケットを壁に設置します。

b) 水準器を使用してブラケットが水平であることを確認した後、鉛筆でネジ穴の位置に印を付けます。
c) #2 のプラス ドライバーを使用して、鉛筆で付けた印にアンカーの中心を慎重に合わせ、アンカーを壁面に押し込みます。
d) アンカーを時計回りの方向に回し、壁面と平らになるまで押し込みます。
e) 付属のネジと #2 のプラス ドライバーを使用して、ブラケットを壁面に装着します。

次の図は、ブラケットの取り付け手順を示します。

図 *5*: ブラケットの取り付け

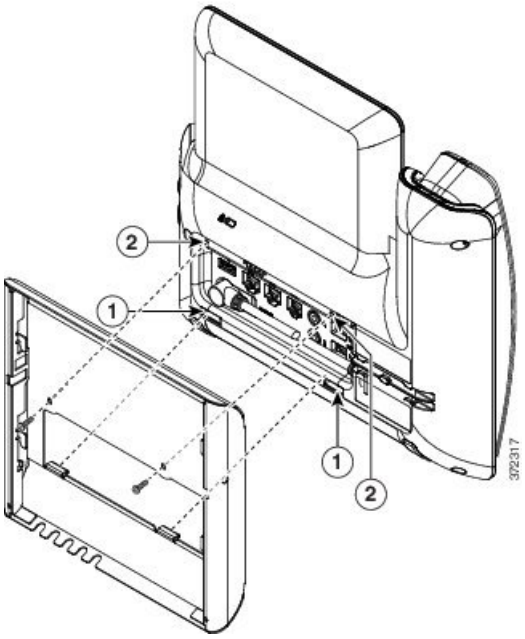


ステップ 2 IP Phone に電話機用ブラケットを装着します。

a) 電話本体から、ハンドセットのコード（ヘッドセットがある場合はヘッドセット コード）以外、電源コードと他のすべてのコードを抜きます。
b) ブラケットのタブを電話機背面の取り付け用タブに挿入して、電話機用ブラケットを装着します。ブラケットの穴から、電話機のポートにアクセスできることを確認してください。
c) 1 番のプラス ドライバを使用し、電話機用ブラケットをセルフタッピング ネジで IP Phone に固定します。
d) コードを元通りに装着し、電話本体に付いているクリップで固定します。

次の図に、ブラケットを電話機に装着する方法を示します。

図 *6*：電話機用ブラケットの装着



ステップ 3　ケーブルを電話機に接続します。

a) イーサネット ケーブルを 10/100/1000 SW ネットワーク ポートと壁面のジャックに接続します。

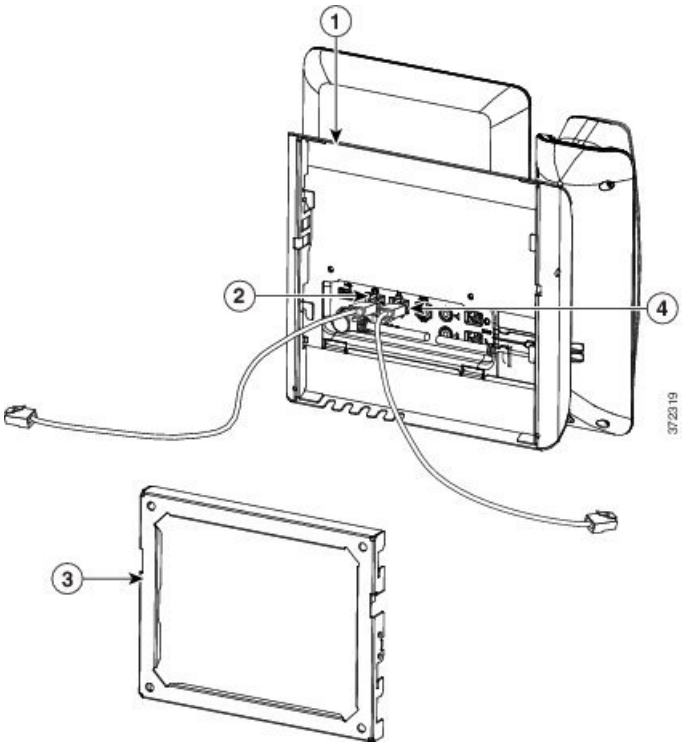
b) （任意） 電話機にネットワーク デバイス（コンピュータなど）を接続する場合、ケーブルを 10/100/1000 コンピュータ（PC アクセス）ポートに装着します。

c) （任意） 外部電源を使用する場合、電源コードを電話機に差し込み、電話本体の PC ポートの横に付いているクリップで、コードをはさんで固定します。

d) （任意） ケーブルの終端が壁面ブラケットの中にある場合は、ケーブルをジャックに接続します。

次の図は、ケーブルを示します。

図 7: **ケーブルの接続**

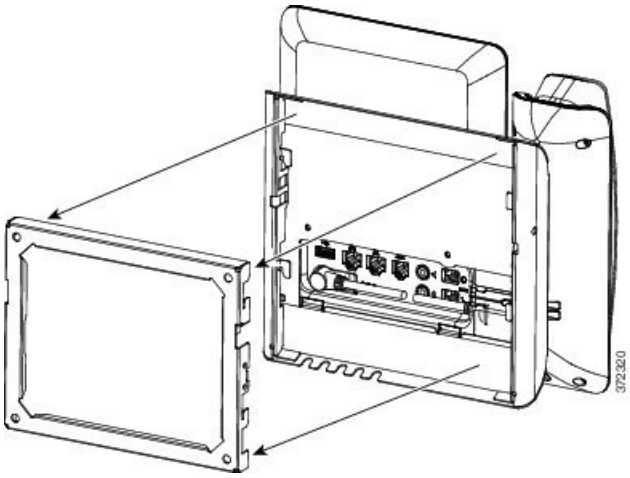


ステップ 4 壁面ブラケットの上部にあるタブを電話機ブラケットのスロットに挿入して、電話機をブラケットに装着します。

ケーブルの終端がブラケットの外に出る場合は、ブラケット下部のケーブル差し込み口を使用して、ブラケット背面の壁に終端がない電源コードやその他のケーブルを配置します。電話機用ブラケットと壁面用ブラケットの開口部によって、複数の円形の開口部ができ、1 つの開口部に 1 本のケーブルを通すことができるようになっています。

次の図は、壁面用ブラケットへの電話機の設置方法を示します。

図 *8*：壁面用ブラケットへの電話の設置



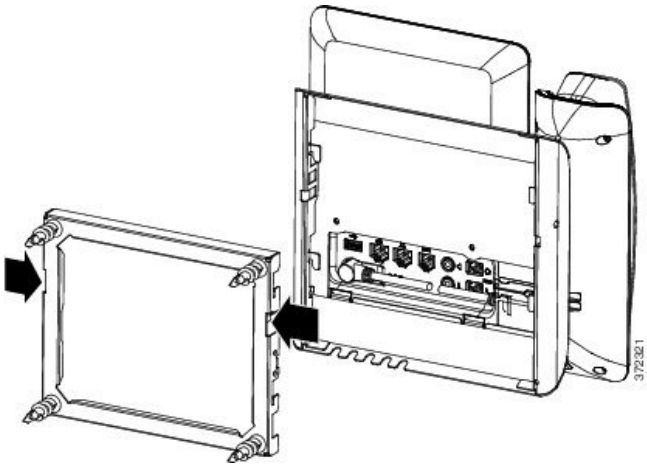
ステップ 5 電話機を壁面ブラケットにしっかりと押し付け、下にスライドします。カチッという音がしてブラケットのタブが位置に収まります。

ステップ 6 ハンドセット レストの調整, （148 ページ）に進みます。

ロック非対応壁面取り付けからの電話機の取り外し

壁面用ブラケットには、電話機のマウント プレートにプレートをロックするためのタブが 2 個付いています。次の図は、タブの位置と形状を示します。

図 *9*：タブの位置



壁面用ブラケットから電話とマウント プレートを取り外すには、これらのタブを外す必要があります。

はじめる前に

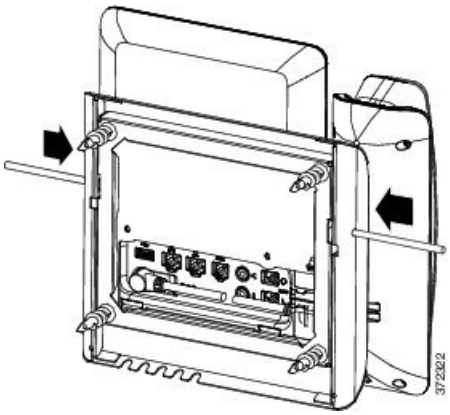
金属棒 2 本が必要です。

手順

ステップ 1 電話マウント プレートにある左右の穴に棒を 0.75 インチ（2.0 cm）ほど差し込みます。

ステップ 2 内側にしっかりと押して（電話に向けて）タブを解除し、電話機を持ち上げて壁面用ブラケットから電話を取り外し、自分の方に電話を引き寄せます。

図 *10*：タブの解除

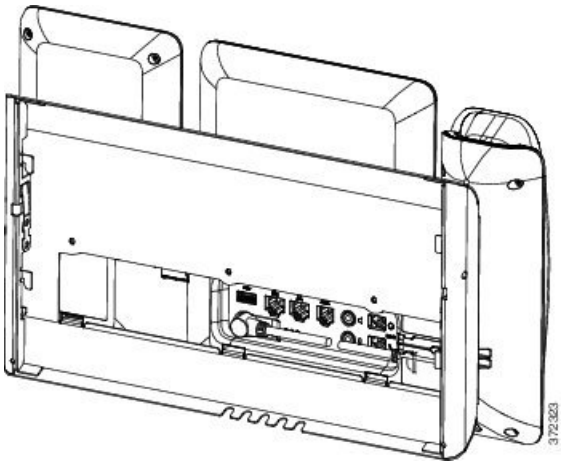


ステップ 3 タブをしっかりと押し込んで外すと同時に電話機を持ち上げ、壁面用ブラケットから電話機を取り外します。

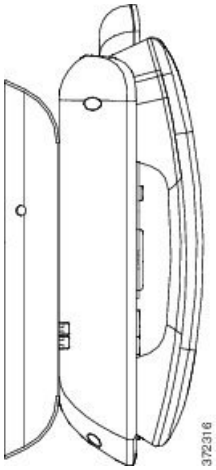
キー拡張モジュール付き電話用ロック非対応壁面取り付けコンポーネント

ここでは、電話機がキー拡張モジュールと接続された場合に、電話機へ Cisco IP Phone 8800 シリーズ壁面取り付けキットと 1 台の KEM を取り付ける方法について説明します。

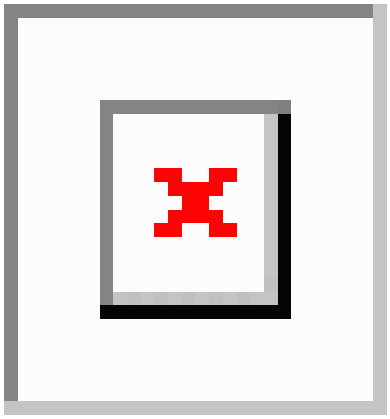
次の図は、電話機に設置されている壁面取り付けキットを示します。



次の図は、壁面取り付けキットが設置された電話機の側面を示します。



次の図は、Cisco IP Phone 8800 シリーズ壁面取り付けキットと 1 台の KEM のコンポーネントを示しています。



同梱物は、次のとおりです。

- 電話機用ブラケット x 1 個
- 壁面用ブラケット x 1 個

- #8-18 x 1.25 インチのプラス ネジ x 6 個、アンカー x 6 個
- K30 x 8 mm のセルフタッピング ネジ x 3 本
- 6 インチのイーサネット ケーブル X 1 本

キー拡張モジュール付き電話用ロック非対応壁面取り付けキットの装着

壁面取り付けキットはコンクリート、れんが、または同様の硬い表面を含むほとんどの表面に配置できます。コンクリート、れんが、または同様の硬い表面にキットを取り付けるには、壁の表面に合ったネジとアンカーを用意する必要があります。

はじめる前に

ブラケットの取り付けには、次の工具が必要です。

- #1 と #2 のプラス ドライバー
- 水準器
- 鉛筆

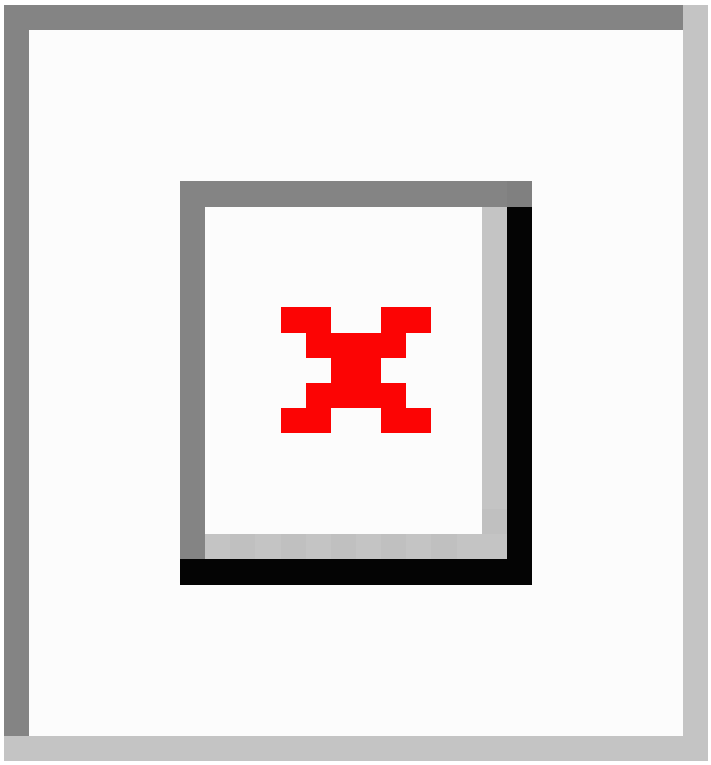
現在、目的の位置に電話用のイーサネットジャックが存在しない場合は、イーサネットジャックも設置します。このジャックには、イーサネット接続のために適切に配線されている必要があります。通常の電話ジャックは使用できません。

手順

ステップ 1 取り付け位置に、壁面用ブラケットを取り付けます。ブラケットをイーサネット ジャックにかぶせて取り付けることも、近くのジャックまでイーサネットネットワーク ケーブルを配線することもできます。

（注） ジャックを電話機の背面に配置する場合は、イーサネット ジャックを壁にぴったり付けるか、埋め込む必要があります。

a) 壁面用ブラケットを壁面に合わせます。壁面用ブラケットの向きについては、次の図を参照してください。
b) 水準器を使用してブラケットが水平であることを確認した後、鉛筆でネジ穴の位置に印を付けます。
c) #2 のプラス ドライバーを使用して、鉛筆で付けた印にアンカーの中心を慎重に合わせ、アンカーを壁面に押し込みます。
d) アンカーを時計回りの方向に回し、壁面と平らになるまで押し込みます。
e) 付属のネジと #2 のプラス ドライバーを使用して、ブラケットを壁面に装着します。



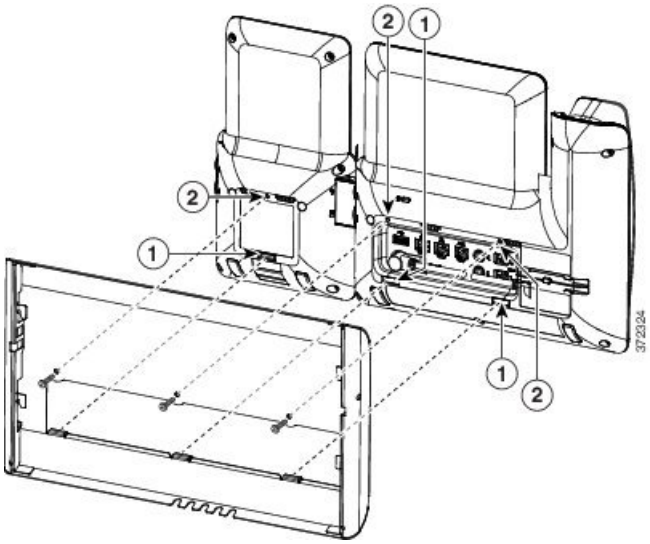
ステップ 2 電話機用ブラケットを IP Phone とキー拡張アセンブリに取り付けます。

a) 電話本体から、ハンドセットのコード（ヘッドセットがある場合はヘッドセット コード）以外、電源コードと他のすべてのコードを抜きます。

b) ブラケットのタブを電話機背面の取り付け用タブに挿入して、電話機用ブラケットを装着します。ブラケットの穴から、電話機のポートにアクセスできることを確認してください。

c) 1 番のプラス ドライバを使用し、電話機用ブラケットをセルフタッピング ネジで IP Phone に固定します。

d) コードを元通りに装着し、電話本体に付いているクリップで固定します。



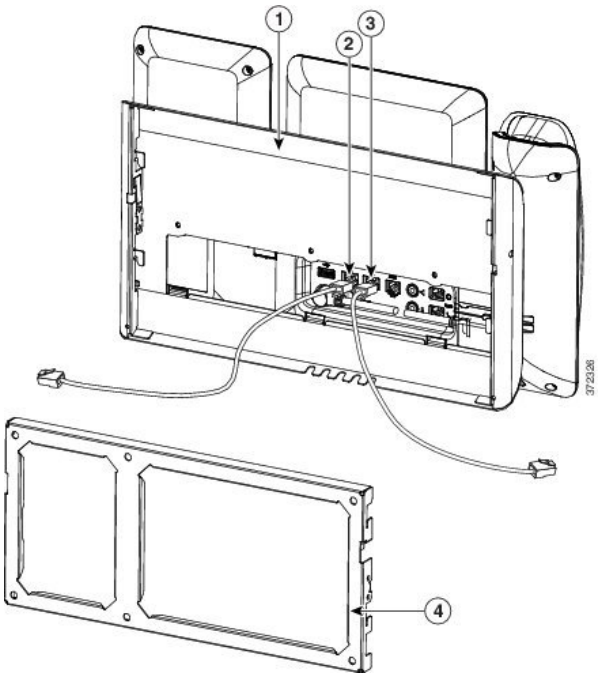
ステップ 3　ケーブルを接続します。

a) イーサネット ケーブルを 10/100/1000 SW ネットワーク ポートと壁面のジャックに接続します。

b) （任意） 電話機にネットワーク デバイス（コンピュータなど）を接続する場合、ケーブルを 10/100/1000 コンピュータ（PC アクセス）ポートに装着します。

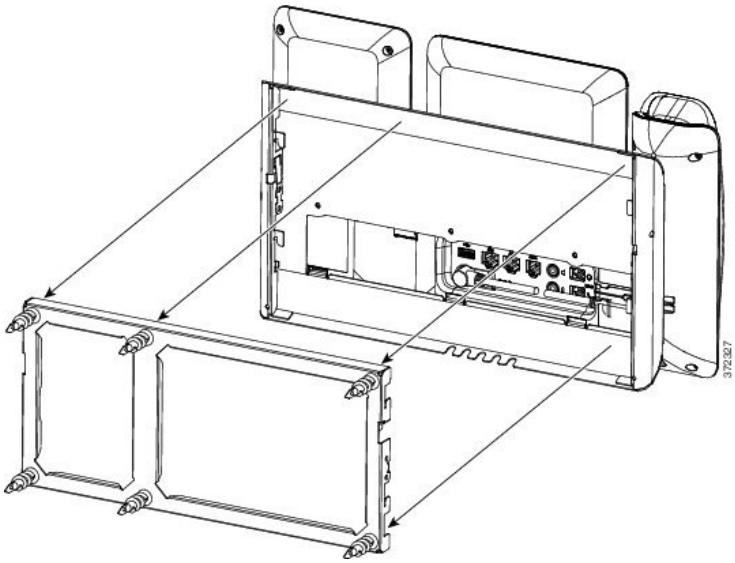
c) （任意） 外部電源を使用する場合、電源コードを電話機に差し込み、電話本体の PC ポートの横に付いているクリップで、コードをはさんで固定します。

d) （任意） ケーブルの終端が壁面ブラケットの中にある場合は、ケーブルをジャックに接続します。



ステップ 4 電話機用ブラケットの上部にあるタブを壁面ブラケットのスロットに挿入して、電話機を壁面ブラケットに装着します。

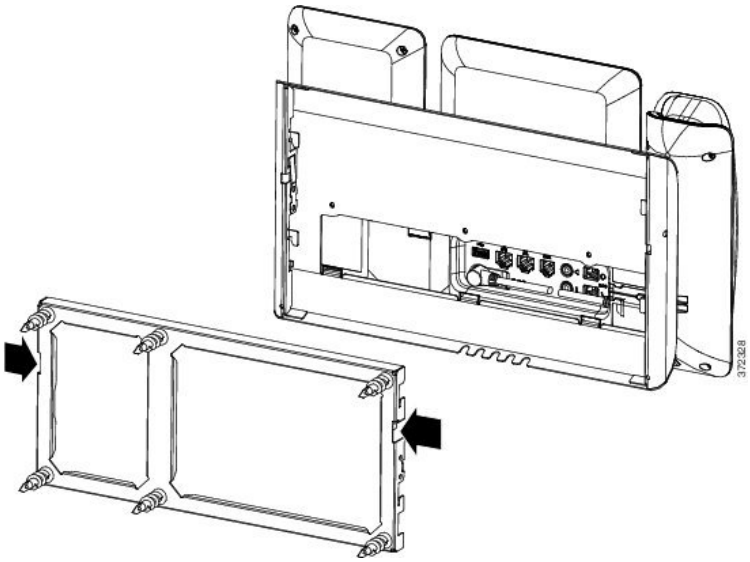
ケーブルをブラケット外で終端する場合は、ブラケット下部のケーブル差し込み口を使用して電源コードやブラケットの後ろの壁で終端しない他のケーブルを配置します。電話機用ブラケットと壁面用ブラケットの開口部によって、複数の円形の開口部ができ、1 つの開口部に 1 本のケーブルを通すことができるようになっています。



ステップ 5 ハンドセット レストの調整, （148 ページ）に進みます。

ロック非対応壁面取り付けからの電話機とキー拡張モジュールの取り外し

壁面用ブラケットには、電話機のマウント プレートにプレートをロックするためのタブが 2 個付いています。次の図は、タブの位置と形状を示します。



壁面用ブラケットから電話とマウント プレートを取り外すには、これらのタブを外す必要があります。

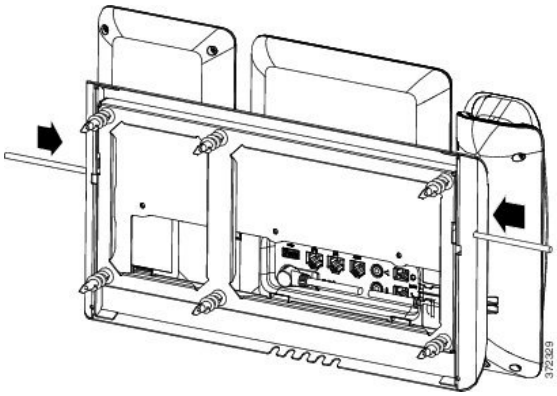
はじめる前に

金属棒 2 本が必要です。

手順

ステップ 1 電話マウント プレートにある左右の穴に棒を 0.75 インチ（2.0 cm）ほど差し込みます。

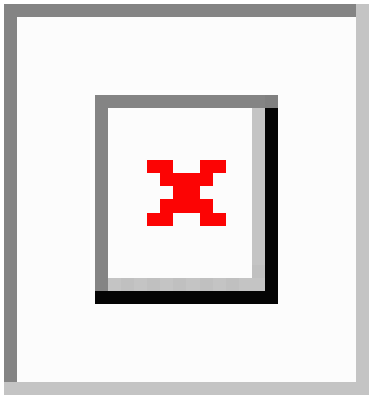
ステップ 2 内側にしっかりと押して（電話に向けて）タブを解除し、電話機を持ち上げて壁面用ブラケットから電話を取り外し、自分の方に電話を引き寄せます。



電話機のロック対応壁面取り付けコンポーネント

ここでは、Cisco IP Phone 8845、および 8865 の壁面取り付けキットの取り付け方法について説明します。

図 *11*：単一の電話アセンブリ用壁面取り付けキット



パッケージには、次の項目が含まれています。

- 電話機用ブラケット x 1 個
- 壁面用ブラケット x 1 個
- #10-12x1 インチのプラス ネジ x 4 個、アンカー x 4 個
- シート メタル ネジ X 1 個（表示されません）
- #4-40x1/4 インチのマシン ネジ x 2 個
- 6 インチのイーサネット ケーブル X 1 本

- ブラケットにオプションのロックが付いている場合は鍵 x 1 個

ブラケットの取り付け

はじめる前に

ブラケットの取り付けには、次の工具が必要です。

- #1 と #2 のプラス ドライバー
- 水準器
- 鉛筆

現在、目的の位置に電話用のイーサネット ジャックが存在しない場合は、イーサネット ジャックも設置します。このジャックには、イーサネット接続のために適切に配線されている必要があります。通常の電話ジャックは使用できません。

手順

ステップ 1 取り付け位置に、壁面用ブラケットを取り付けます。ブラケットをイーサネット ジャックにかぶせて取り付けることも、近くのジャックまでイーサネット ネットワーク ケーブルを配線することもできます。

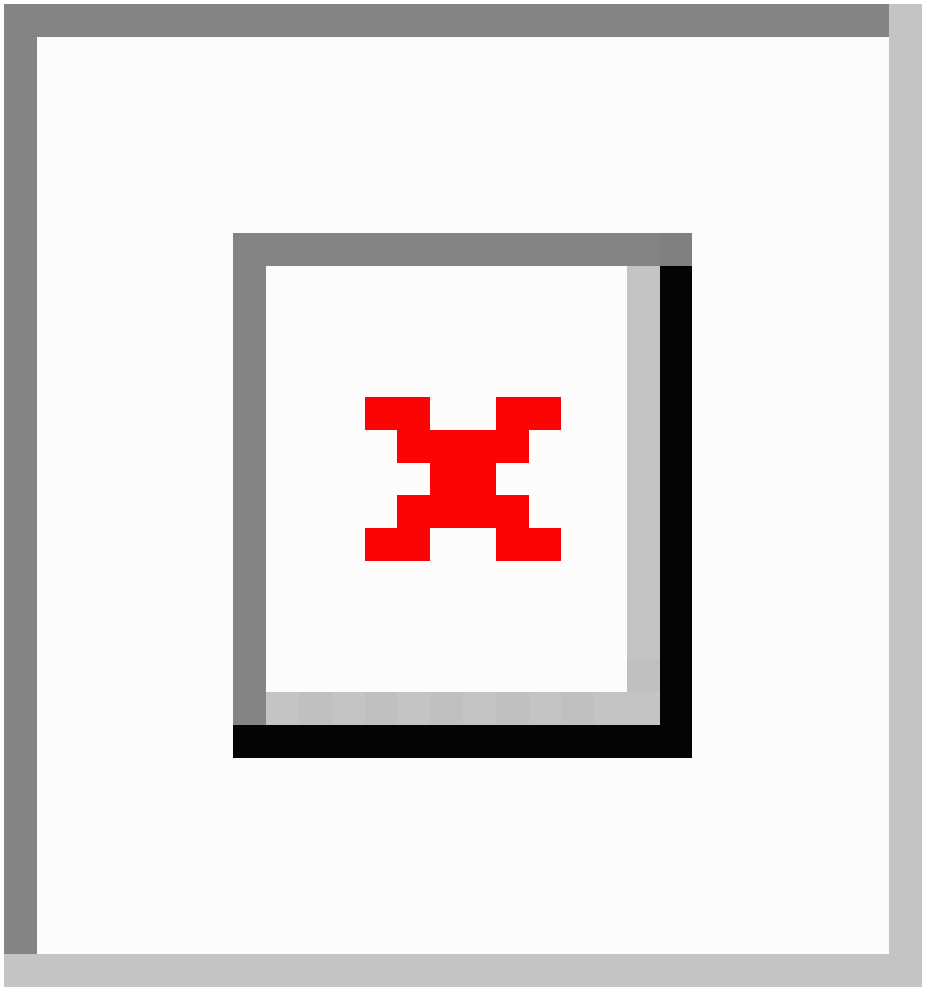
a) 水準器を使用してブラケットが水平であることを確認した後、鉛筆でネジ穴の位置に印を付けます。

b) #2 のプラス ドライバーを使用して、鉛筆で付けた印にアンカーの中心を慎重に合わせ、アンカーを壁面に押し込みます。

c) アンカーを時計回りの方向に回し、壁面と平らになるまで押し込みます。

d) 付属のネジと #2 のプラス ドライバーを使用して、ブラケットを壁面に装着します。

図 *12* : 壁面用ブラケットの取り付け



ステップ 2 IP Phone に電話機用ブラケットを装着します。

a) 電話本体からハンドセットのコード（およびヘッドセットがある場合は、ヘッドセットのコード）、電源コード、その他のすべてのコードを取り外します。

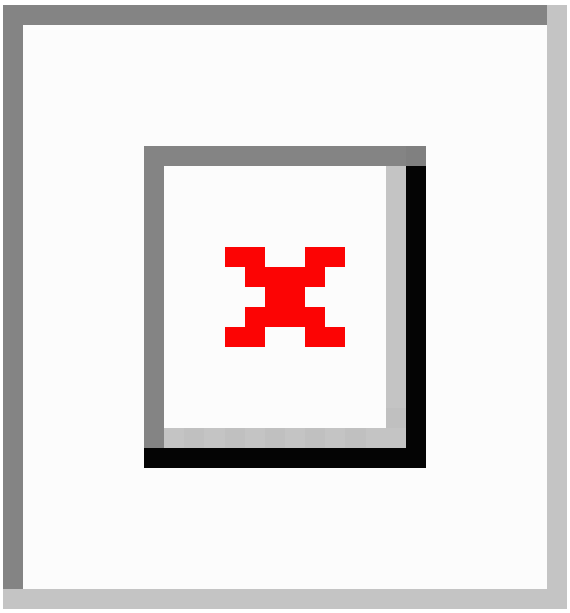
b) ネジ穴を隠しているラベル カバーを外します。

c) ブラケットのタブを電話機の取り付け用タブに挿入して、電話機用ブラケットを装着します。ブラケットの穴から、電話機のポートにアクセスできることを確認してください。

d) 機械ネジを使用して、電話に電話機用ブラケットを固定します。

e) ハンドセットのコード（および使用する場合は、ヘッドセットのコード）をブラケットの穴に通します。コードを元通りに装着し、電話本体に付いているクリップで固定します。

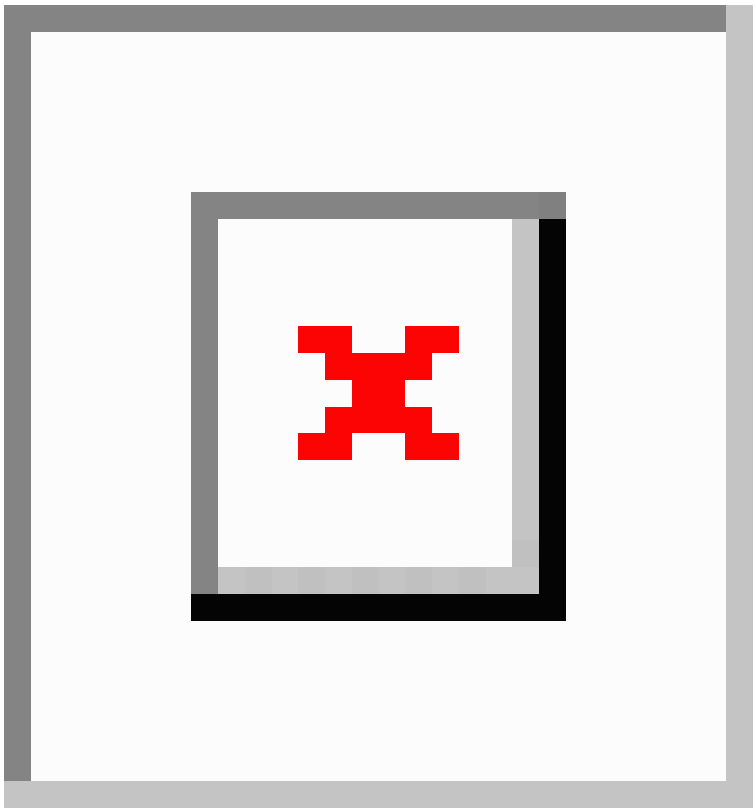
図 *13*：電話機用ブラケットの装着



ステップ 3　イーサネット ケーブルを 10/100/1000 SW ネットワーク ポートと壁面のジャックに接続します。電話機にネットワーク デバイス（コンピュータなど）を接続する場合、ケーブルを 10/100/1000 コンピュータ（PC アクセス）ポートに装着します。

外部電源を使用する場合、電源コードを電話機に差し込み、電話本体の PC ポートの横に付いているクリップで、コードをはさんで固定します。

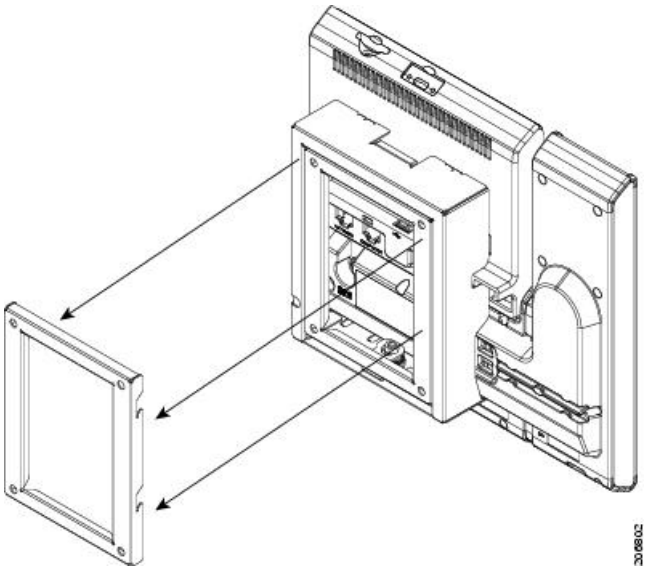
図 *14*：ケーブルの接続



ステップ 4 電話機用ブラケットの上部にあるタブを壁面ブラケットのスロットに挿入して、電話機を壁面ブラケットに装着します。ブラケット背後の壁面に差し込み口がある場合を除き、すべての電源コードやその他のケーブルが、ブラケット下部のケーブル アクセス用開口部を通っていることを確認

します。電話機用ブラケットと壁面用ブラケットの開口部によって、複数の円形の開口部ができ、1 つの開口部に 1 本のケーブルを通すことができるようになっています。

図 *15*：壁面用ブラケットへの電話の設置



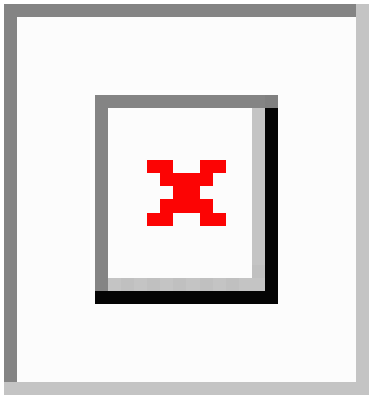
ステップ 5　ロックの鍵を使用して、電話を壁面用ブラケットにロックします。

ステップ 6　ハンドセット レストの調整, （148 ページ）に進みます。

キー拡張モジュール付き電話用ロック対応壁面取り付けコンポーネント

ここでは、Cisco IP Phone 8851、8851NR、および 8861 の壁面取り付けキットの取り付け方法について説明します。

図 *16*：キー拡張モジュール付き電話用壁面取り付けキット



パッケージには、次の項目が含まれています。

- 電話機用ブラケット x 1 個
- 壁面用ブラケット x 1 個
- #10-12x1 インチのプラス ネジ x 4 個、アンカー x 4 個
- シート メタル ネジ X 1 個
- #4-40 X 1/4 インチのマシン ネジ X 3 個
- 6 インチのイーサネット ケーブル X 1 本
- ブラケットにオプションのロックが付いている場合は鍵 x 1 個

KEM 付き電話用取り付けブラケット

（注） 電話機用ブラケットを取り付ける前に、Cisco Unified IP Phone がキー拡張モジュールに接続されていることを確認してください。

はじめる前に

ブラケットの取り付けには、次の工具が必要です。

- #1 と #2 のプラス ドライバー

- 水準器
- 鉛筆

現在、目的の位置に電話用のイーサネットジャックが存在しない場合は、イーサネットジャックも設置します。このジャックには、イーサネット接続のために適切に配線されている必要があります。通常の電話ジャックは使用できません。

手順

ステップ 1 取り付け位置に、壁面用ブラケットを取り付けます。ブラケットをイーサネット ジャックにかぶせて取り付けることも、近くのジャックまでイーサネットネットワーク ケーブルを配線することもできます。

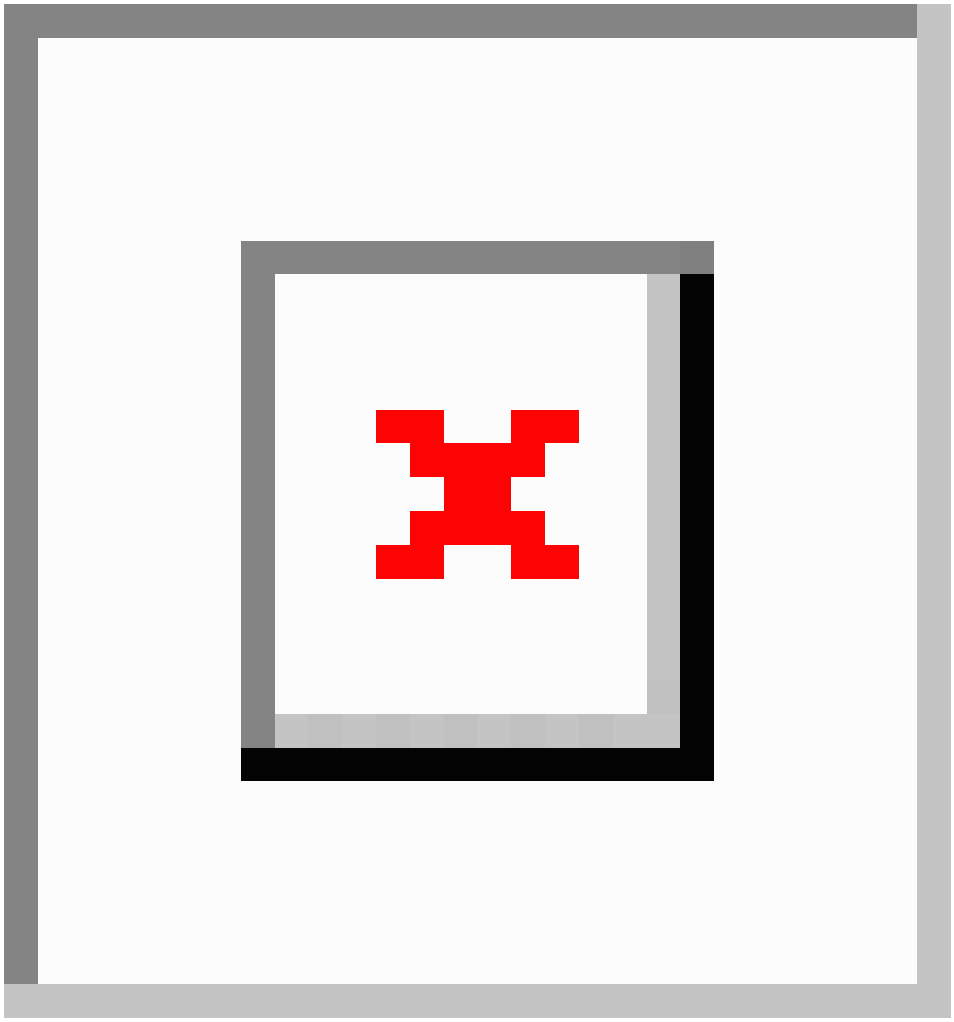
a) 水準器を使用してブラケットが水平であることを確認した後、鉛筆でネジ穴の位置に印を付けます。

b) #2 のプラス ドライバーを使用して、鉛筆で付けた印にアンカーの中心を慎重に合わせ、アンカーを壁面に押し込みます。

c) アンカーを時計回りの方向に回し、壁面と平らになるまで押し込みます。

d) 付属のネジと #2 のプラス ドライバーを使用して、ブラケットを壁面に装着します。

図 *17*：壁面用ブラケットの取り付け



ステップ 2 電話機用ブラケットを IP Phone とキー拡張アセンブリに取り付けます。

a) 電話本体からハンドセットのコード（およびヘッドセットがある場合は、ヘッドセットのコード）、電源コード、その他のすべてのコードを取り外します。

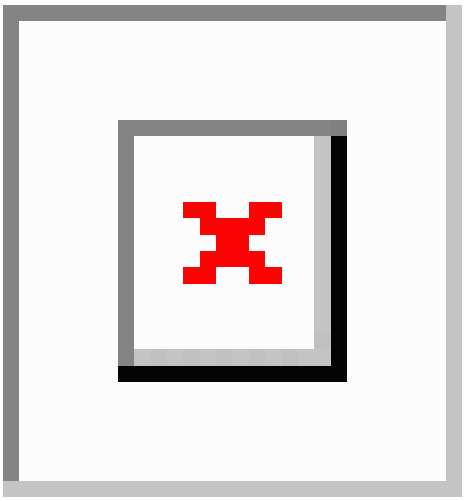
b) ネジ穴を隠しているラベル カバーを外します。

c) ブラケットのタブを電話機の取り付け用タブに挿入して、電話機用ブラケットを装着します。ブラケットの穴から、電話機のポートにアクセスできることを確認してください。

d) 機械ネジを使用して、電話に電話機用ブラケットを固定します。

e) ハンドセットのコード（および使用する場合は、ヘッドセットのコード）をブラケットの穴に通します。コードを元通りに装着し、電話本体に付いているクリップで固定します。

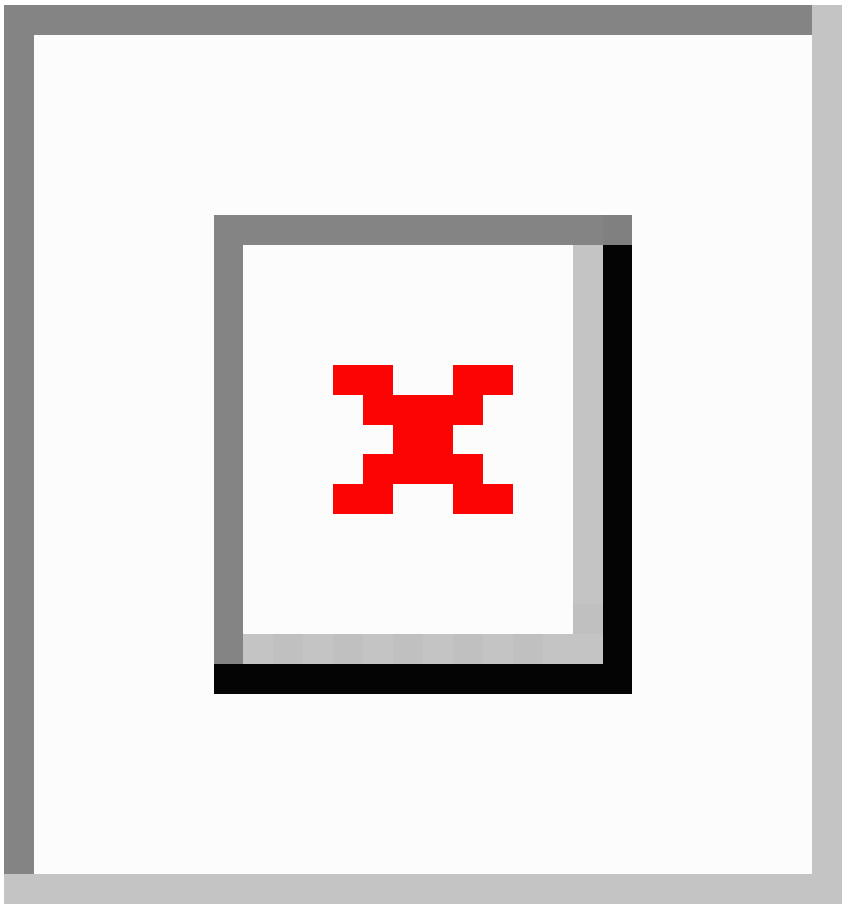
図 *18*：電話機用ブラケットの装着



ステップ 3　イーサネット ケーブルを 10/100/1000 SW ネットワーク ポートと壁面のジャックに接続します。電話機にネットワーク デバイス（コンピュータなど）を接続する場合、ケーブルを 10/100/1000 コンピュータ（PC アクセス）ポートに装着します。

外部電源を使用する場合、電源コードを電話機に差し込み、電話本体の PC ポートの横に付いているクリップで、コードをはさんで固定します。

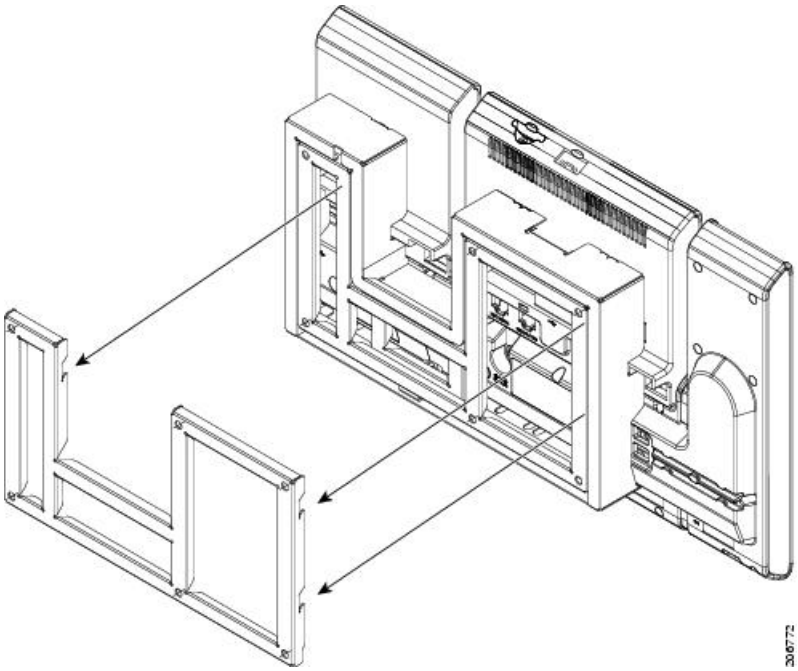
図 *19*：ケーブルの接続



ステップ 4 電話機用ブラケットの上部にあるタブを壁面ブラケットのスロットに挿入して、電話機を壁面ブラケットに装着します。
ブラケット背後の壁面に差し込み口がある場合を除き、すべての電源コードやその他のケーブルが、ブラケット下部のケーブル アクセス用開口部を通っていることを確認します。電話機用ブラ

ケットと壁面用ブラケットの開口部によって、複数の円形の開口部ができ、1 つの開口部に 1 本のケーブルを通すことができるようになっています。

図 *20*：壁面用ブラケットへの電話の設置

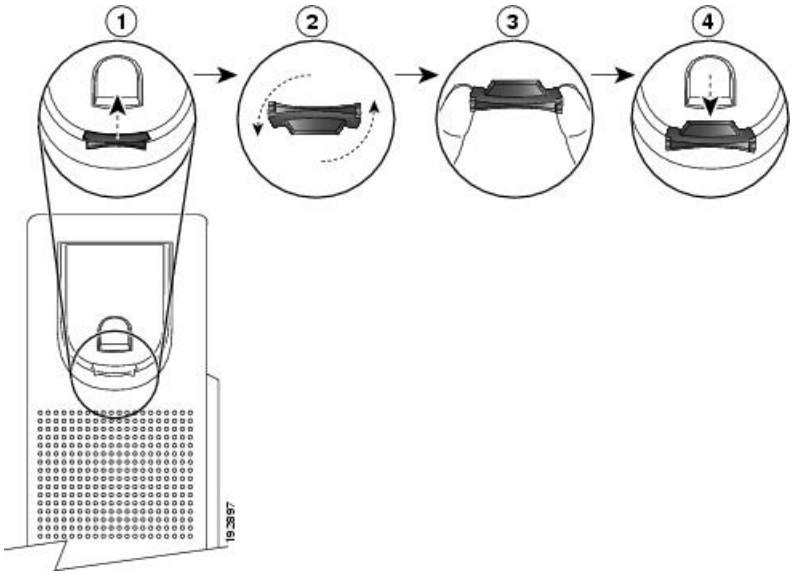


ステップ 5　ロックの鍵を使用して、電話を壁面用ブラケットにロックします。

ステップ 6　次も項に進みます。 ハンドセット レストの調整, （148 ページ）

ハンドセット レストの調整

電話機が壁に取り付けられている場合、またはハンドセットが受け台からすぐに滑り落ちる場合には、受話器が受け台から滑り落ちないようにハンドセット レストを調整する必要があります。



手順

ステップ 1 受け台からハンドセットを外し、ハンドセット レストからプラスチック タブを引き出します。

ステップ 2 タブを 180 度回します。

ステップ 3 角のノッチが手前になるように、2 本指でタブを持ちます。

ステップ 4 タブを受け台のスロットに合わせ、タブをスロット内に均等に押し込みます。回したタブの上部から突起が出ている状態になります。

ステップ 5 ハンドセットをハンドセット レストに戻します。

第 IV 部

Cisco IP Phone の管理

- Cisco IP Phone のセキュリティ，153 ページ
- Cisco IP Phone のカスタマイズ，183 ページ
- 電話機の機能および設定，191 ページ
- 社内ディレクトリとパーソナル ディレクトリ，275 ページ

第 10 章

Cisco IP Phone のセキュリティ

- サポート対象のセキュリティ機能，153 ページ

サポート対象のセキュリティ機能

セキュリティ機能を使用すると、なりすましやデータ改ざんの脅威から電話機を保護できます。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 Release 8.5(1) 以降に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 Phone 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 Phone 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。

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 CM 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。

次の表に、電話機でサポートされるセキュリティ機能の概要を示します。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。

電話機の現在のセキュリティ設定を確認するには、 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）] を選択します。

表 *17*：セキュリティ機能の概要

機能	説明
イメージ認証	署名付きのバイナリ ファイル（拡張子 .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。
カスタマーサイト証明書のインストール	各 Cisco IP Phone は、デバイス認証に一意の証明書を必要とします。電話機には Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）が含まれますが、追加のセキュリティについては、Cisco Unified 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。

機能	説明
デバイス認証	Cisco Unified Communications Manager サーバと電話機間で、一方のエンティティが他方のエンティティの証明書を受け入れるときに行われます。電話機と Cisco Unified Communications Manager の間でセキュアな接続を確立するかどうかを判別し、必要に応じて TLS プロトコルを使用してエンティティ間にセキュアなシグナリング パスを作成します。Cisco Unified Communications Manager では、認証できない電話機は登録されません。
ファイル認証	電話機がダウンロードするデジタル署名ファイルを検証します。ファイルの作成後、ファイルの改ざんが発生しないように、電話機でシグニチャを検証します。認証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。
製造元でインストールされる証明書	各 Cisco IP Phone 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。
メディアの暗号化	SRTP を使用して、サポートされるデバイス間のメディア ストリームがセキュアであること、および意図したデバイスのみがデータを受信し、読み取ることを保証します。デバイスのメディアマスターのキーペアの作成、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。
セキュリティ プロファイル（Security profile）	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	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。

機能	説明
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。詳細については、電話機の Web ページへのアクセスの制御, （255 ページ）を参照してください。
電話機のセキュリティ強化	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。 • 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
802.1X 認証（802.1X Authentication）	Cisco IP Phone は 802.1X 認証を使用して、ネットワークへのアクセスの要求およびネットワーク アクセスができます。詳細については、802.1X 認証, （178 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	Cisco Unified Communications Manager リリース 10.5(2) 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。新しい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。

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 *18*：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

コードおよびメッセージ	説明
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 *19*：*[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（Security Mode）	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。	Cisco Unified CM 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（Trust List）	[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、ローカルで有効な証明書のセットアップ，（159 ページ）を参照してください。
802.1X 認証（802.1X Authentication）	この電話機に 802.1X 認証を有効にできます。	802.1X 認証，（178 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）

ローカルで有効な証明書のセットアップ

電話機に LSC を設定するには、次の手順を使用します。

はじめる前に

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 は実行および設定されています。

これら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 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 ボタンを押し、[管理者設定（Administrator Settings）] > [セキュリティのセットアップ（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（Settings Access）] 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 3 [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 4 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成功すると、[インストール済み（Installed）] という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、電話機がアップグレード用に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）] と表示された場合は、操作が成功したことを示しています。CAPF サーバはエラー メッセージをログに記録します。ログの位置を調べ、エラー メッセージの意味を理解するには、CAPF サーバのマニュアルを参照してください。

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。デフォルト設定は [いいえ（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 *20*：会議コールのセキュリティの制限事項

発信側の電話機のセキュリティ レベル	使用される機能	参加者のセキュリティ レベル	アクションの結果
非セキュア	会議	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 レベルを満たしていません。コールを拒否します（Does not meet Security Level, call rejected）」というメッセージを受け取る。
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。

（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。

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 Phone 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 Phone 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、そのマスターキーで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。

- 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 Phone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。
- Cisco Centralized Key Management（CCKM）：RADIUSサーバとワイヤレス ドメイン サーバ（WDS）の情報を使用して、キーの管理および認証をします。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 Phone 8800シリーズは802.11r（FT）をサポートしています。

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 Phone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 Phone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 Phone 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 Phone は 256 ビットのキー サイズをサポートします。

（注） Cisco IP Phone 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 Phone 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 Phone 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 Phone 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 *21*：認証方式と暗号化方式

Cisco IP Phone の設定	**AP の設定**			
セキュリティ モード	セキュリティ	キー管理	暗号化	高速ローミング
なし	なし	なし	なし	該当なし
WEP	静的 WEP	静的	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
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，（164 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（Wireless Security Credentials）

ネットワークで EAP-FAST、EAP-TLS、PEAP、または WPA2、CCKM がユーザ認証に使用されている場合、Access Control Server（ACS）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。

ここでは、セキュリティ クレデンシャルの設定について説明します。

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、32 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

[WPA 事前共有キーでの自動（Auto (AKM) for WPA Pre-shared key）] または [WPA2 事前共有キー（WPA2 Pre-shared key）] を認証に使用している場合は、[ワイヤレス セキュリティ クレデンシャル（Wireless Security Credentials）] 領域でパスフレーズ/事前共有キーを設定する必要があります。

事前共有キーの形式

Cisco IP Phone 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 タイプ（Key Type）] 領域で、次の文字形式のいずれかを選択します。

- 16 進数
- ASCII

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（Wireless Encryption）

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 Phone 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 タイプ（Key Type）] 領域で、次の文字形式のいずれかを選択します。

- 16 進数
- ASCII

ステップ 3 [暗号化キー 1（Encryption Key 1）] で、[送信キー（Transmit Key）] をクリックします。

ステップ 4 [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 5 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, （170 ページ）を参照してください。

ステップ 6 [保存（Save）] をクリックして変更を加えます。

EAP-TLS 認証証明書

EAP-TLS は、2 つ以上のエンティティ間で信頼関係が必要となる証明書ベースの認証です。各エンティティは、自身の ID を証明する証明書を持ち、信頼された認証局によって署名されます。これらの証明書は、EAP-TLS 認証時に交換および検証されます。

（注） EAP-TLS 証明書ベースの認証では、Cisco IP Phone の内部時計が正しく設定されている必要があります。EAP-TLS 認証を使用する前に、電話機の Web ページを使用して、電話機の時計を設定してください。

EAP-TLS を使用するには、Cisco IP Phone と Cisco Secure Access Control Server（ACS）の両方に証明書がインストールされ正しく設定されている必要があります。ワイヤレス ネットワークが認証に EAP-TLS を使用している場合、電話機での認証には、製造元でインストールされる証明書（MIC）、またはユーザがインストールした証明書を使用できます。

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 Phone 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）が電話機で生成されて、承認のために CA へ送信され、承認済みの証明書が Cisco IP Phone にインストールされている必要があります。

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) Microsoft 証明書サービスで、ACS サーバから CA 証明書をエクスポートし、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，（173 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，（174 ページ）

ステップ 3 ユーザがインストールした証明書を使用する場合は、電話機の Web ページで、次の手順を実行します。

a) 証明書署名要求（CSR）を生成します。

b) CSR を CA に送信し署名を取得します。

c) 証明書をインポートします。

d) 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。

e) CA 証明書を ACS サーバからダウンロードし、電話機にインポートします。
詳細については、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，（175 ページ）を参照してください。

ステップ 4 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，（176 ページ）

- 『*User Guide for Cisco Secure ACS for Windows*』

日付と時刻の設定

EAP-TLS で使用される証明書ベースの認証では、Cisco IP Phone 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*』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,（174 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,（174 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 [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 [証明書（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, （176 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。

ステップ 4 次の画面で、テキストボックスの内容全体（エンコードされた CSR テキスト）を選択し、コピーします。このデータを CA 管理者に送信し、署名を要請します。
CSR テキストは、電子メールまたは CA 管理者が決定した別の方法で送信します。次の手順では、CA Web ページでの基本的な CSR 承認プロセスについて説明します。

ステップ 5 [Microsoft 証明書サービス（Microsoft Certificate Services Request）] の [証明書の要求（Request a Certificate）] ページで、[証明書の要求の詳細設定（Advanced certificate request）] を選択し、署名要求を開始します。

ステップ 6 [証明書の要求の詳細設定（Advanced Certificate Request）] ページで、[Base 64 エンコード PKCS CMC を使用して証明書要求を送信する（Submit a certificate request by using a base-64-encoded PKCS CMC）] を選択します。

ステップ 7 Cisco Unified Wireless IP Phone から証明書データをコピーし、それを [保存された要求（Saved Request）] テキスト ボックスに貼り付け、[送信（Submit）] をクリックします。

ステップ 8 CSR が承認された後、証明書を DER エンコード形式でエクスポートし、要求元に送信する必要があります。

ステップ 9 電話機の Web ページに戻り、[証明書（Certificates）] を選択して署名付き証明書をインポートします。

ステップ 10 [証明書（Certificates）] ページで、ユーザによってインストールされた証明書の行を検索し、[インポート（Import）] をクリックします。

ステップ 11 PC 上で証明書を参照し、電話機にインポートします。

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, （174 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（たとえば、CP-7925G-SEPxxxxxxxxxxxx）。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，（175 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。

- EAP-TLS を許可（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。

（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。

はじめる前に

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。
- [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。

802.1X 認証

Cisco IP Phone は 802.1X 認証をサポートします。

Cisco IP Phone と Cisco Catalyst スイッチは、従来 Cisco Discovery Protocol（CDP）を使用して互いを識別し、VLAN 割り当てやインライン所要電力などのパラメータを決定します。CDP では、ローカルに接続されたワークステーションは識別されません。Cisco IP Phone は、EAPOL パススルー メカニズムを提供します。このメカニズムを使用すると、Cisco IP Phone に接続されたワークステーションは、LAN スイッチにある 802.1X オーセンティケータに EAPOL メッセージを渡すことができます。パススルー メカニズムにより、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 Phone はまた、プロキシ EAPOL ログオフ メカニズムも提供します。ローカルに接続された PC が IP 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 Phone: 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 Phone 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、複数ドメインの認証をサポートしているスイッチもあります（Cisco Catalyst スイッチなど）。スイッチの設定により、PC を電話機の PC ポートに接続できるかどうかが決定されます。
  - 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 Phone はプロキシ EAPOL ログオフをサポートします。Cisco Catalyst スイッチでの IEEE 802.1X サポートの詳細については、次の URL にある Cisco Catalyst スイッチのコンフィギュレーション ガイドを参照してください。

    http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
  - 無効：スイッチで同じポート上の複数の 802.1X 準拠デバイスがサポートされていない場合は、802.1X 認証を有効にするときに PC ポート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 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, （179 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 *22*：*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（Device Authentication）	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 Authentication）] フィールドの設定, （180 ページ）を参照してください。
トランザクション ステータス（Transaction Status）	[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（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）。	表示専用。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）] 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（Yes）]

- [いいえ（No）]

ステップ 4 [適用（Apply）] を押します。

第 11 章

Cisco IP Phone のカスタマイズ

- カスタム電話呼出音，183 ページ
- カスタム背景イメージ，185 ページ
- ワイドバンド コーデックのセットアップ，189 ページ
- 未使用時画面のセット アップ，190 ページ

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、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。

関連トピック

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

カスタム電話呼出音のセットアップ

手順

ステップ 1 各カスタム呼出音の PCM ファイルを作成します（ファイルごとに呼出音 1 つ）。PCM ファイルが、カスタム呼出音のファイル形式, （184 ページ）に示す形式のガイドラインに準拠していることを確認します。

ステップ 2 作成した新しい PCM ファイルを、クラスタ内の各 Cisco Unified Communications Manager の Cisco TFTP サーバにアップロードします。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。

ステップ 3 テキスト エディタを使用して Ringlist-wb.xml ファイルを編集します。このファイルの形式とサンプルの Ringlist.xml ファイルについては、カスタム呼出音のファイル形式, （184 ページ）を参照してください。

ステップ 4 修正内容を保存し、Ringlist-wb.xml ファイルを閉じます。

ステップ 5 新しい Ringlist-wb.xml ファイルをキャッシュするには、Cisco Unified Serviceability を使用して TFTP サービスを停止してから起動するか、「起動時の定数および bin ファイルのキャッシングの有効化（Enable Caching of Constant and Bin Files at Startup）」TFTP サービス パラメータ（[拡張サービスパラメータ（Advanced Service Parameters）] 領域に含まれる）を無効にしてから再度有効にします。

関連トピック

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

カスタム呼出音のファイル形式

Ringlist.xml ファイルは、電話呼出音タイプのリストを保持した XML オブジェクトを定義しています。このファイルには、呼出音タイプを 50 個まで記述します。呼出音タイプごとに、呼出音タイプに使用される PCM ファイルへのポインタ、および 電話機の [呼出音タイプ（Ring Type）] メニューに表示されるテキストを記述します。このファイルは、各 Cisco Unified Communications Manager の Cisco TFTP サーバに保持されます。

CiscoIPPhoneRinglist XML オブジェクトは、次の簡単なタグ セットを使用して情報を記述します。

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRingList>
```

定義名については、次の規則があります。 それぞれの電話呼出音タイプについて、必須の DisplayName と FileName を記述する必要があります。

- DisplayNameには、関連付けられたPCMファイルのカスタム呼出音の名前を指定します。この名前は、電話機の [呼出音タイプ（Ring Type）] メニューに表示されます。
- FileNameには、DisplayNameに関連付けるカスタム呼出音のPCMファイルの名前を指定します。

（注） DisplayNameフィールドとFileNameフィールドは、長さ25文字以下にする必要があります。

次に、2つの電話呼出音タイプを定義したRinglist.xmlファイルの例を示します。

```
<CiscoIPPhoneRingList>
   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRingList>
```

呼出音のPCMファイルを電話機で正常に再生するには、ファイルが次の要件を満たしている必要があります。

- 未加工のPCM（ヘッダーなし）。
- サンプリング回数：8,000回/秒。
- 1サンプルあたり8ビット。
- Mu-law圧縮
- 呼出音の最大サイズ = 16080サンプル
- 呼出音の最小サイズ = 240サンプル
- 呼出音のサンプル数 = 240の倍数。
- 呼出音は、ゼロ交差で開始および終了する。

カスタム呼出音のPCMファイルを作成するには、これらのファイル形式の要件をサポートする標準オーディオ編集パッケージを使用します。

カスタム背景イメージ

電話機のLCDスクリーンに表示される背景イメージ（または壁紙）をユーザに提供し、選択させることができます。ユーザは、電話機でアプリケーション>[設定（Settings）]>[壁紙（Wallpaper）] を選択して、背景イメージを選択できます。

ユーザに見える画像の種類は、電話機が使用しているTFTPサーバに保存されているPNG画像とXMLファイル（List.xml）を元にしています。独自のPNGファイルを保存し、TFTPサーバ上の

XML ファイルを編集すれば、ユーザが選択できる背景イメージを指定できます。この方法を利用すれば、会社のロゴなどのカスタム画像をユーザに提供することができます。

（注） PNG と List.xml イメージの寸法は 800 X 480 X 24 内である必要があります。

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 list.xml を使用すると、電話機には変更が適用されません。

Cisco Unified Communications Manager Administration（[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 [共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウで [背景イメージ設定へのアクセスの有効化（Enable End User Access to Phone Background Image Setting）] チェックボックスへのエンドユーザアクセスをオフにして、背景イメージを選択するユーザのオプションをディセーブルにできます。このチェックボックスがオフになっている場合、壁紙メニューは電話機に表示されません。

カスタム背景イメージのセットアップ

手順

ステップ 1 各画像に 2 つの PNG ファイル（フルサイズ画像とサムネール画像）を作成します。PNG ファイルが、カスタム背景ファイル形式, （187 ページ）に示す形式のガイドラインに準拠していることを確認します。

ステップ 2 作成した新しい PNG ファイルを、Cisco Unified Communications Manager の TFTP サーバの次のサブディレクトリにアップロードします。
Desktops/800 X 480 X 24

（注） ファイル名とサブディレクトリのパラメータは大文字と小文字を区別します。サブディレクトリのパスを指定する場合は、前方スラッシュ「/」を使用してください。

ファイルをアップロードするには、Cisco Unified Communications Operating System の管理ページで、[ソフトウェア アップグレード（Software Upgrades）] > [TFTP サーバ ファイルのアップロード（Upload TFTP Server File）] を選択します。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。

（注） フォルダが存在しない場合、フォルダが作成され、そのフォルダにファイルがアップロードされます。

ステップ 3 カスタマイズした画像とファイルは、電話機がファイルを取得するためにアクセスする可能性がある他の TFTP サーバにもコピーする必要があります。

（注） カスタム画像ファイルのバックアップ コピーを他の場所にも保存することをお勧めします。これらのバックアップ コピーは、Cisco Unified Communications Manager のアップグレードの際、カスタマイズしたファイルが上書きされてしまうときに使用することができます。

ステップ 4 テキスト エディタを使用して、List.xml ファイルを編集します。このファイルがある場所、形式の要件、およびサンプルファイルについては、カスタム背景ファイル形式, （187ページ）を参照してください。

ステップ 5 修正内容を保存し、List.xml ファイルを閉じます。

（注） Cisco Unified Communications Manager をアップグレードする際、デフォルトの List.xml ファイルによって、カスタマイズした List.xml ファイルが置き換えられます。List.xml ファイルをカスタマイズした後、ファイルのコピーを作成し他の場所に保存してください。Cisco Unified Communications Manager をアップグレードした後、デフォルトの List.xml ファイルを保存しておいたコピーに置き換えます。

ステップ 6 新しい List.xml ファイルをキャッシュするには、Cisco Unified Serviceability を使用して TFTP サービスを停止してから起動するか、「起動時の定数および bin ファイルのキャッシングの有効化（Enable Caching of Constant and Bin Files at Startup）」TFTP サービス パラメータ（[拡張サービス パラメータ（Advanced Service Parameters）] 領域に含まれる）を無効にしてから再度有効にします。

関連トピック

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

カスタム背景ファイル形式

List.xml ファイルは、背景イメージのリストを保持した XML オブジェクトを定義しています。List.xml ファイルは TFTP サーバ上の次のサブディレクトリに保存されます。

Desktops/800 X 480 X 24

ヒント ディレクトリ構造と List.xml ファイルを手動で作成する場合、TFTP サービスで使用されるユーザ（CCMService）からディレクトリとファイルがアクセスできることを確認してください。

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。

List.xml ファイルには、背景イメージを 50 個まで記述できます。画像は電話機の [背景イメージ（Background Images）] メニューに表示される順番にします。各画像に対して、List.xml ファイルに ImageItem と呼ばれる要素タイプを 1 つ記述します。ImageItem 要素には 2 つの属性があります。

- Image：電話機の [背景イメージ（Background Images）] メニューに表示されるサムネール画像の取得先を示す Uniform Resource Identifier（URI）。
- URL：フルサイズ画像の取得先を指定する URI。

次の例は、2 つの画像を定義した List.xml ファイルを示しています。それぞれの画像について、必須の Image および URL 属性を記述する必要があります。フルサイズ画像とサムネール画像にリン

クするメソッドとしては、例で示されている TFTP URI のみがサポートされています。HTTP URL はサポートされていません。

List.xml の例

```
<CiscoIPPhoneImageList>
<ImageItem Image="TFTP:Desktops/800x480x24/TN-Fountain.png"
URL="TFTP:Desktops/800x480x24/Fountain.png"/>
<ImageItem Image="TFTP:Desktops/800x480x24/TN-FullMoon.png"
URL="TFTP:Desktops/800x480x24/FullMoon.png"/>
</CiscoIPPhoneImageList>
```

電話機ファームウェアには、デフォルトの背景イメージが含まれています。List.xml ファイルでは、この画像を定義していません。デフォルト画像は、常に電話機の [背景イメージ（Background Images）] メニューの最初に表示されます。

背景イメージごとに 2 つの PNG ファイルが必要です。

- フルサイズ画像：電話機で表示される画像。
- サムネール画像：ユーザが画像を選択できる [背景イメージ（Background Images）] 画面に表示される画像。フルサイズ画像の 25% のサイズである必要があります。

ヒント　多くの画像プログラムで画像のサイズを変更する機能を提供しています。サムネール画像を作成する簡単な方法としては、まずフルサイズ画像を作成して保存します。そして、画像プログラムのサイズ変更機能を使用して元のサイズの 25% の画像を作成します。サムネール画像には異なる名前を付けて保存します。

背景画像の PNG ファイルを電話機で正常に表示するには、ファイルが次の要件を満たしている必要があります。

- フル サイズ イメージ：800 ピクセル（幅）X 480 ピクセル（高さ）
- サムネール画像：139 ピクセル（幅）X 109 ピクセル（高さ）

ヒント　グレースケール用のポスタリゼーション機能をサポートする画像プログラムを使用している場合、チャネルごとの階調レベルの数を 16 に設定すると、画像は 16 段階のグレースケールになるようポスタリゼーションがかかります。

関連トピック

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

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 Phone 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など通話先から聞こえる背景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 CM 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 Phone 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) Cisco Unified CM 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 Phone*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801c0764.shtml

さらに、以下の情報については、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。

- 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 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 [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（Save）] を選択します。

第 12 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，193 ページ
- Cisco IP Phone ユーザのサポート，193 ページ
- 電話機能，193 ページ
- 機能ボタンとソフトキー，213 ページ
- Expressway 経由での Mobile and Remote Access，215 ページ
- VPN の設定（VPN Configuration），220 ページ
- スピーカーフォンを無効にする，221 ページ
- Cisco IP Phone での省電力のスケジュール，222 ページ
- Cisco IP Phone での Power Save Plus（EnergyWise）のスケジュール，224 ページ
- エージェント グリーティングの有効化，228 ページ
- DF ビットのセットアップ，229 ページ
- サイレントの設定，230 ページ
- モニタリングと録音のセットアップ，231 ページ
- LLDP の電力ネゴシエーションのセットアップ，232 ページ
- Bluetooth プロファイルのセットアップ，232 ページ
- 自動ポート同期の設定，233 ページ
- SSH アクセスの設定，234 ページ
- コールの転送通知のセット アップ，234 ページ
- C 割り込みの設定，236 ページ
- クライアント識別コードのセット アップ，236 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，237 ページ

- コール リストの BLF の有効化，238 ページ
- デュアル バンク情報のセットアップ，239 ページ
- 強制承認コードの設定，239 ページ
- 着信コール Toast タイマーの設定，240 ページ
- ピア ファームウェア共有のセット アップ，241 ページ
- リモート ポート設定のセット アップ，242 ページ
- ヘッドセットの側音制御の設定，243 ページ
- Release ボタンからのダイヤル トーンのセットアップ，244 ページ
- パーク モニタリング，245 ページ
- 実行可能な着信呼警告の有効化，248 ページ
- コール履歴表示拡張の有効化，249 ページ
- 共有回線のコール履歴の有効化，250 ページ
- デフォルト回線フィルタのセットアップ，251 ページ
- カスタム回線フィルタのセットアップ，251 ページ
- 電話ボタン テンプレート，252 ページ
- 電話機の Web ページへのアクセスの制御，255 ページ
- ソフトキー テンプレートの設定，256 ページ
- RTP/sRTP ポート範囲のセットアップ，259 ページ
- TLS 再開タイマーのセットアップ，260 ページ
- 音声ポートとビデオ ポートの範囲設定，261 ページ
- Cisco IP Manager Assistant のセットアップ，263 ページ
- Visual Voicemail のセットアップ，265 ページ
- インテリジェント プロキシミティの有効化，267 ページ
- 複数ライン同時通話（Join Across Lines）機能および回線間転送（Transfer Across Lines）機能の管理，268 ページ
- コンピュータからのビデオのセット アップ，269 ページ
- ビデオ送信解像度のセットアップ，270 ページ
- 問題レポート ツール，271 ページ
- プライマリ回線における全コールを表示，273 ページ
- 回線のラベルの設定，274 ページ

電話機の機能および設定の概要

Cisco IP Phone 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 Phone 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。

関連トピック

Cisco IP Phone ユーザのサポート，（193 ページ）
Cisco Unified Communications Manager のマニュアル，（xvii ページ）
各言語ユーザのサポート，（355 ページ）

Cisco IP Phone 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 Phone 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 Phone の機能（スピード ダイヤル、サービス、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、システム管理者またはシステム管理者ネットワーク チームからユーザが情報を入手する必要があります。また、システム管理者に問い合わせてサポートを受けられる環境も必要です。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 Phone 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。

- サポートするすべての Cisco IP Phone 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関する情報
- 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 Phone 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 Phone 8800 Series User Guide for Cisco Unified Communications Manager*』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,（213 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 パラメータへのアクセス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。

サービスの機能の詳細については、[サービス パラメータ設定（Service Parameter Configuration）] 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、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。

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。 実行可能な着信呼警告の有効化,（248 ページ）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,（153 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,（228 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。

機能	説明と詳細情報
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, （278 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。
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ー音により、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。 自動ポート同期の設定, （233 ページ）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。

機能	説明と詳細情報
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 Phone 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。
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。
折り返し	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。

機能	説明と詳細情報
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。
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。この無効化は、CFA の接続先の電話番号が内部か外部かに関係なく動作します。 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, （234 ページ）を参照してください。
共有回線のコール履歴	電話機のコール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 参照先 共有回線のコール履歴の有効化, （250 ページ）
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。 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。

機能	説明と詳細情報
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。
コール録音	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 Phone 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、着信コールの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。

機能	説明と詳細情報
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（Caller ID Blocking）	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。
発信側の正規化	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 Phone 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。 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。 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および C 割り込みの設定, （236 ページ）を参照してください。
モバイル デバイスの充電	Cisco IP Phone 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 Phone 8800 Series User Guide for Cisco Unified Communications Manager*』を参照してください。

機能	説明と詳細情報
Cisco エクステンション モビリティ	共有 Cisco IP Phone から自分の Cisco IP Phone の設定（ライン アピアランス、サービス、スピードダイヤルなど）に一時的にアクセスできます。それには、共有 Cisco IP Phone の Cisco エクステンション モビリティ サービスにログインする際に、自分の電話機の Cisco エクステンション モビリティ サービスにログインします。 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行う場合や、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 Phone にログインできます。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 Phone にログインします。 （注） EMCC を設定する前に、Cisco IP Phone で Cisco エクステンション モビリティを設定してください。
Cisco IP Phone 8800 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。 Cisco IP Phone キー拡張モジュール, （105 ページ）を参照してください。
Cisco IP Phone 8811 のサポート	Cisco IP Phone 8811 に対するサポートを提供します。
Cisco IP Phone 8851NR のサポート	Cisco IP Phone 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。 参照先： • 『*Cisco Unified Communications Manager Express System Administrator Guide*』 • Cisco Unified Communications Manager Express の連携, （18 ページ）
Cisco Unified Video Advantage（CUVA）	Cisco IP Phone、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。

機能	説明と詳細情報
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 Phone と共通化できます。 カスタム電話呼出音，（183 ページ）を参照してください。
クライアント識別コード（CMC）	コールが特定のクライアントに関連するように指定できます。 クライアント識別コードのセットアップ，（236ページ）を参照してください。
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，（237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。

機能	説明と詳細情報
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。
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 Phone 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 Phone に表示します。 Cisco IP Phone 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、ユーザの電話画面に DND アイコンが表示されます。 サイレントの設定, （230 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。 複数ライン同時通話（Join Across Lines）機能および回線間転送（Transfer Across Lines）機能の管理, （268 ページ）を参照してください。

機能	説明と詳細情報
EnergyWise	省エネのために、あらかじめ決められた時刻に IP Phone 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 Phone での Power Save Plus（EnergyWise）のスケジュール, （224 ページ）を参照してください。
クラスタ間のセキュアなエクステンション モビリティの機能強化（EMCC）	この拡張によって、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、クラスタ間のセキュアなエクステンションモビリティ（EMCC）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, （254 ページ）を参照してください。
Forced Authorization Code（FAC）	特定のユーザが発信できるコールのタイプを制御します。 強制承認コードの設定, （239 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。 ヘッドセットの側音制御の設定, （243 ページ）を参照してください。
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	共有回線を持つ電話機では、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。

機能	説明と詳細情報
保留/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。
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。
Hunt Group	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。 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。 着信コール Toast タイマーの設定, （240 ページ）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, （267 ページ）を参照してください。 Cisco IP Phone 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 のサポート	Cisco IP Phone での拡張 IP アドレッシングをサポートします。Ipv6 では、デュアルスタック設定が推奨されており、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。デュアルスタック モードでは、内容にかかわらず、電話機は IPv4 および IPv6 を使用して同時に通信できます。 ネットワークの設定, （53 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。
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 • 応対可 • 使用中 • サイレント コール リストの BLF の有効化, （238 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 • 応対可 • 使用中 • サイレント コール リストの BLF の有効化, （238 ページ）を参照してください。
回線のテキストラベル	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, （274 ページ）を参照してください。
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。

機能	説明と詳細情報
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。
ミートミー会議	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。
メッセージ受信	メッセージ受信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 Phone のメッセージ受信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。
メッセージ受信インジケータ	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 Phone の最小呼出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 Mobile and 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。 参照先 Expressway 経由での Mobile and Remote Access, （215 ページ）
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。

機能	説明と詳細情報
モニタリングおよび録音	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 Phone 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、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。
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。
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。
他のグループのピックアップ	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。

機能	説明と詳細情報
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,（153 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。 LLDP の電力ネゴシエーションのセットアップ,（232 ページ）を参照してください。
問題レポート 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,（271 ページ）を参照してください。
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。
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 Phone 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。 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。
プログラム可能な機能ボタン	発信、折返し、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。

機能	説明と詳細情報
品質レポート ツール（QRT）	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。
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。 リモート ポート設定のセット アップ, （242 ページ）を参照してください。
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, （183 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。

機能	説明と詳細情報
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, （153 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。
サービス	Cisco Unified Communications Manager の管理にある [IP Phone 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 Phone 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 電話機の 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。
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, （267 ページ）を参照してください。 Cisco IP Phone 8851NR は Bluetooth をサポートしていません。

機能	説明と詳細情報
スピード ダイヤル	記憶されている指定番号をダイヤルします。
SSH アクセス	Cisco Unified Communications Manager の管理を使用して、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。 SSH アクセスの設定, （234 ページ）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 Phone 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 Phone 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。
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 Phone 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 Phone 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 Phone 8845 および 8865 のみで利用可能
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。デフォルトでは有効になっています。 Cisco IP Phone 8845 および 8865 のみで利用可能
PC からのビデオ	Cisco Unified IP Phone、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。 Cisco IP Phone 8845 および 8865 のみで利用可能
表示によるボイスメール	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。

機能	説明と詳細情報
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 Visual Voicemail のセットアップ, （265 ページ）を参照してください。
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 Phone 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。
Web アクセスはデフォルトで無効になっています。	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されることを意味します。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 Phone 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, （252 ページ）を参照してください。

表 *23*：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
アラート コール		X	
すべてのコール		X	
応答		X	X
C 割り込み			X
折り返し		X	X

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
すべてのコールの転送			X
コール パーク		X	X
コールパークの回線ステータス		X	
コール ピックアップ（ピックアップ）		X	X
コールピックアップの回線ステータス		X	
会議	X		X
転送			X
サイレント		X	X
グループ ピックアップ		X	X
保留	X		X
ハント グループ		X	
インターコム		X	
迷惑呼 ID（MCID）		X	X
ミートミー		X	X
モバイルコネクト（モビリティ）		X	X
ミュート	X		
その他のピックアップ		X	X
キュー ステータスの PLK サポート			X
プライバシー		X	
キュー ステータス		X	

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
品質レポート ツール（QRT）		X	X
録音			X
リダイヤル		X	X
スピード ダイヤル		X	X
スピードダイヤルの回線ステータス		X	X
USBヘッドセットの保留ボタンのサポート			X
転送	X		X

Expressway 経由での Mobile and Remote Access

Expressway 経由での Mobile and Remote Access 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。電話機で Expressway 証明書を認証して TLS セッションを確立するには、Expressway 証明書に、電話機ファームウェアが信頼するパブリック認証局による署名が付いていなければなりません。Expressway 証明書の認証のために、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 Mobile and Remote Access は Cisco Expressway と関連して機能するため、『*Cisco Expressway Administrator Guide*』、『*Cisco Expressway Basic Configuration Deployment Guide*』などの Cisco Expressway のマニュアルの内容をよく把握しておいてください。

Expressway 経由での Mobile and Remote Access を使用する場合は、IPv4 プロトコルのみがサポートされます。

Expressway 経由での Mobile and 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*

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。Expressway 経由での Mobile and Remote Access 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。ただし、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。この制限は、MRA ソリューションが CAPF（Certificate Authority Proxy Function）とインタラクティブに機能するデバイスをサポートしないことによるものです。

導入シナリオ

次の表に、Expressway 経由での Mobile and Remote Access のさまざまな導入シナリオを示します。

シナリオ	アクション
Expressway 経由での Mobile and Remote Access 導入後に、社内ユーザが企業ネットワークにログインします。	企業ネットワークが検出され、電話機が Cisco Unified Communications Manager に正常に登録されます。

シナリオ	アクション
オフプレミス ユーザが Expressway 経由での Mobile and Remote Access で企業ネットワークにログインします。	電話機はオフプレミスモードになっていることを検出し、Expressway 経由での Mobile and Remote Access サインイン ウィンドウが表示されて、ユーザが企業ネットワークに接続します。 ユーザが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。 また、ユーザは、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もあります。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。 電話機を出荷時の状態で導入する場合は、サービス モードのリセットの要件はスキップできます。 ユーザのネットワーク 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ログ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。
Expressway 経由での Mobile and Remote Access 導入後、オフプレミス ユーザは VPN を使用して企業ネットワークにログインします。	ユーザは、基本リセットを実行する必要があります。詳細については、『*Cisco IP Phone 8800 Series User Guide for Cisco Unified Communications Manager*』の「Maintenance」の章の「Basic Reset」の項を参照してください。 ユーザは代替 TFTP 設定を構成する必要があります（[ネットワーク設定（Network settings）] > [代替TFTP設定（Alternate TFTP setting）]）。

Expressway 経由での Mobile and Remote Access で利用可能な電話機能

Expressway 経由での Mobile and 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 Mobile and Remote Access で利用可能な電話機能のリストを示します。

- 短縮ダイヤル
- 処理されたダイレクト コール パーク

- ビジー ランプ フィールド（BLF）
- ビジー ランプ フィールド（BLF）ピックアップ
- ビジー ランプ フィールド（BLF）スピード ダイヤル
- 折り返し
- コール転送
- コールの転送通知
- コール パーク
- コール ピックアップ
- 会議
- 直接転送
- ダイレクト コール パーク
- ディレクトリ サービス
- 転送
- グループ コール ピックアップ
- 保留/復帰
- 保留復帰
- 即時転送
- 参加
- ミートミー会議
- メッセージ受信インジケータ
- モバイル コネクト
- モバイル ボイス アクセス
- 保留音
- ミュート
- オンフック ダイヤル
- プラス ダイヤル
- 問題レポート ツール
- リダイヤル
- スピード ダイヤル
- 転送
- Uniform Resource Identifier（URI）ダイヤリング

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 Mobile and Remote Access でネットワークにサインインすると、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を保存でき、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。

特定の電話機に対する Expressway サインイン用ユーザ クレデンシャル パーシステントの有効化

特定の電話機で Expressway サインイン用のユーザ クレデンシャル パーシステントを有効にするには、次の手順を実行します。

手順

ステップ 1 [デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 対象の電話を特定します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで、Expressway サインイン機能に対して [ユーザクレデンシャルパーシステントの設定の有効化（Enable setting for the User Credentials Persistent）] を選択します。

電話機グループに対する Expressway サインイン用ユーザ クレデンシャル パーシステントの有効化

電話機のグループに対する Expressway サインイン用のユーザ クレデンシャル パーシステントを有効にするには、次の手順を実行します。

手順

ステップ 1 [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）] を選択します。

ステップ 2 Expressway サインイン機能に対して [ユーザクレデンシャルパーシステントの設定の有効化（Enable setting for the User Credentials Persistent）] を選択します。

ステップ 3 [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 4 [デバイス（Device）] > [電話（Phone）] を使用して、電話機を共通電話機プロファイルと関連付けます。

ネットワーク全体における Expressway サインイン用ユーザ クレデンシャル パーシステントの有効化

ネットワークのすべての電話機に対する Expressway サインイン用のユーザ クレデンシャル パーシステントを有効にするには、次の手順を実行します。

手順

ステップ 1 [システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）] を選択します。

ステップ 2 Expressway サインイン機能に対して [ユーザクレデンシャルパーシステントの設定の有効化（Enable setting for the User Credentials Persistent）] を選択します。

ステップ 3 [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。

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コ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。

VPN の設定（VPN Configuration）

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
- ユーザ名およびパスワード

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、この設定はディセーブルになっています。

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。

スピーカーフォンを無効にする

デフォルトでは、Cisco IP Phone でスピーカーフォンが有効です。

スピーカを無効にするには、Cisco Unified Communications Manager の管理ページを使用します。スピーカーフォンが無効になっているときには、ユーザがスピーカフォン ボタンを押しても、リダイヤル、発信、不在転送のソフトキーが電話機に表示されません。ソフトキーのラベルがグレー表示になるか、除去されます。

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 変更する電話機を選択します。

ステップ 3 電話機の [電話の設定（Phone Configuration）] ウィンドウで、[スピーカーフォンの無効化（Disable Speakerphone）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] を選択します。

Cisco IP Phone 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伸ばすには、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。

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 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。

表 *24*：*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。
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、7:00（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 2:00 時（1400）にディスプレイをオンにするには、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（Save）] を選択します。

Cisco IP Phone での Power Save Plus（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 CM 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。

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 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。

表 *25*：*EnergyWise* の設定フィールド

フィールド	説明
Power Save Plus の有効化（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（00:00 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（00:00 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、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。
電話機をオフにするアイドルタイムアウト（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
音声アラートを有効にする（Enable Audio 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 ドメイン（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 secret）	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
EnergyWise オーバーライドを許可（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（Save）] を選択します。

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、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。

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（Save）] 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) [システム（System）] > [サービス パラメータ（Service Parameters）] 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（Save）] 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）

DF ビットのセットアップ

設定可能な DF ビット機能は、ネットワークがどのように送信されるかを制御します。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。デフォルトでは、DF ビットは 0 に設定されます。

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。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、次のいずれかのウィンドウに移動します。

- [システム（System）] > [エンタープライズ電話（Enterprise 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）]
- [デバイス（Device）] > [電話（Phone）]

ステップ 2 [DF ビット（DF Bit）] フィールドを設定します。

サイレントの設定

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。

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、該当する Cisco Unified Communications Manager リリースのマニュアルのサイレントについての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 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）] ウィンドウおよび [電話の設定（Phone Configuration）] ウィンドウの両方にあります。[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（Save）] 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、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。

はじめる前に

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（Save）] 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）

LLDP の電力ネゴシエーションのセットアップ

LLDP の電力ネゴシエーション機能によって、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。

電力ネゴシエーション機能は、デフォルトで有効になっています。

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 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）] 領域で、電力ネゴシエーション パラメータを設定します。

ステップ 4 [保存（Save）] を選択します。

Bluetooth プロファイルのセットアップ

（注） この手順は、Bluetooth 対応の電話機のみに適用されます。Cisco IP Phone 8811、8841、および 8851NR は Bluetooth をサポートしていません。

Bluetooth プロファイルの詳細については、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 の管理ページで、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 Cisco Unified Communications Manager に表示された電話のリストからお使いの電話を検索します。

ステップ 3 電話機の [デバイス名（Device Name）] をクリックします。

[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] レイアウト エリアに移動し、[Bluetooth プロファイル（Bluetooth Profiles）] ドロップダウン リストから、適切なプロファイルを選択します。
ハンズフリー プロファイルは、デフォルトで選択されています。

ステップ 5 更新する [プロダクト固有の設定（Product Specific Configuration）] エリアで、任意の設定に対して [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。

- このチェックボックスをオンにしないと、対応するパラメータ設定が有効になりません。
- [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（最も高い優先順位）
2. [共通の電話プロファイルの設定（Common Phone Profile Configuration）] 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（最も低い優先順位）

関連トピック

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

自動ポート同期の設定

単一の電話機または電話機のグループで同期を設定できます。

手順

ステップ 1 単一の電話機の自動ポート同期を設定するには、

a) Cisco Unified Communications Manager の管理アプリケーションで、[デバイス（Device）] > [電話（Phone）] を選択します。
b) 電話機を特定します。
c) [プロダクト固有の設定（Product Specific Configuration Layout）] ペインで、自動ポート同期パラメータを設定します。
d) [保存（Save）] を選択します。

ステップ 2 電話機のグループに対して自動ポート同期を設定するには、

a) Cisco Unified Communications Manager の管理アプリケーションで、[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) 自動ポート同期パラメータを設定します。
c) [保存（Save）] を選択します。

SSH アクセスの設定

ポート 22 を経由する SSH デーモンへのアクセスを有効または無効にすることができます。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になります。デフォルトでは、SSH ドメインは無効になっています。

SSH アクセス パラメータはデフォルトで無効になっています。これらの電話機のユーザが SSH を使用する前に、SSH アクセス パラメータ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、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）] > [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）]

（注） 両方のウィンドウでパラメータを設定すると、[デバイス（Device）] > [電話（Phone）] > [電話の設定（Phone Configuration）] ウィンドウの設定が優先されます。

ステップ 2 適切な電話機を選択します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration Layout）] ペインまでスクロールし、[SSH アクセス（SSH Access）] ドロップダウン リスト ボックスから [有効（Enable）] を選択します。

ステップ 4 [保存（Save）] を選択します。

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 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 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。

表 *26*：*[コールの転送通知（Call Forward Notification）]* フィールド

フィールド	説明
発信者名（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。
発信者番号（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。
転送元番号（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。
ダイヤル番号（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（Save）] を選択します。

C 割り込みの設定

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することを許可します。cBarge 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。

詳細については、以下を参照してください。

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

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 [回線キー割込み（Line Key Barge）] パラメータを見つけて、必要な設定を選択します。
使用可能な設定は次のとおりです。

- オフ（Off）：回線キーを押したときに新しいコールが開始されます。
- ソフトキーをオンにする（Turn on Softkey）：回線キーを押すと、リモート使用中で設定されたソフトキーがオンになり、C 割り込みを介してコールに参加できます
- デフォルト（Default）：回線キーを押すと、コールに参加できます。

ステップ 3 [保存（Save）] を選択します。

クライアント識別コードのセット アップ

クライアント識別コード（CMC）を使用して、クライアントや職務権限の識別ができます。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。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、[コール ルーティング（Call Routing）] > [クライアント識別コード（Client Matter Code）] を選択します。

ステップ 2 [クライアント識別コードが必須（Require Client Matter Code）] フィールドを設定します。
このチェックボックスでは、コールの発信時に CMC の入力をユーザに求めるかどうかを制御します。

ステップ 3 [保存（Save）] 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）

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。

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。

フィールド	説明
Energy Efficient Ethernet: PC ポート（Energy Efficient Ethernet: PC Port）	スイッチ/PC ポート上の Energy Efficient Ethernet（EEE）を有効化または無効化します。 表示されるオプションには、次のものがあります。 • **[有効（Enabled）]** • **[無効（Disabled）]**
Energy Efficient Ethernet: スイッチ ポート（Energy Efficient Ethernet: Switch Port）	スイッチ/PC ポート上の Energy Efficient Ethernet（EEE）を有効化または無効化します。 表示されるオプションには、次のものがあります。 • **[有効（Enabled）]** • **[無効（Disabled）]**

ステップ 4 [設定の適用（Apply Config）] 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（Save）] 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。

強制承認コードの設定

強制承認コード（FAC）は、ユーザに発信権限を確実に与えます。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。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、[コール ルーティング（Call Routing）] > [強制承認コード（Forced Authorization Code）] を選択します。

ステップ 2 次のフィールドを設定します。

フィールド	説明
強制承認コードが必須（Require Forced Authorization Code）	FAC の入力をユーザに要求するには、このチェックボックスをオンにします。
承認レベル（Authorization Level）	コールの発信を承認されるために、ユーザが入力する必要があるコード。

ステップ 3 [保存（Save）] 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）

着信コール Toast タイマーの設定

着信コール Toast（着信コール通知ウィンドウ）がユーザの電話機に表示される時間を設定できます。

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（Enterprise Phone）]

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（Enterprise Phone）]

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 [着信コール Toast タイマー（Incoming Call Toast Timer ）] フィールドを設定します。

フィールド	説明
着信コール Toast タイマー（Incoming Call Toast Timer）	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。 有効値は、0、3、4、および 5 です。 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。

ステップ 4 [保存（Save）] を選択します。

ピア ファームウェア共有のセット アップ

この機能を有効にすると、電話機は、ファームウェア イメージを構成するファイルを要求しているサブネット上の同じ電話機を検出し、転送階層をファイル単位で自動的に構築できます。ファームウェア イメージを構成する個々のファイルは、階層内のルートの電話機だけを使用して TFTP から取得され、これらのファイルは TCP 接続によって転送階層に沿ってサブネット上の他の電話機に迅速に転送されます。

この機能は、高速キャンパス LAN 設定で次のメリットを提供します。

- 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電話機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遠隔オフィス導入シナリオでは、ピア ファームウェア共有がファームウェアのアップグレードに役立つ場合もあります。

このメニューオプションは、電話機がピア ファームウェア共有をサポートしているかどうかを示します。次の設定があります。

- 有効（Enabled）（デフォルト値）
- 無効（Disabled）

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 Cisco Unified Communications Manager に関連付けられた電話のリストからお使いの電話を検索します。

ステップ 3 電話機の [デバイス名（Device Name）] をクリックします。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration）] レイアウト エリアに移動し、[ピア ファームウェア共有（Peer Firmware Sharing）] ドロップダウン リストから [有効（Enable）] を選択します。
ピア ファームウェア共有は、デフォルトで有効になっています。

ステップ 5 更新する [プロダクト固有の設定（Product Specific Configuration）] エリアで、任意の設定に対して [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。

- このチェックボックスをオンにしないと、対応するパラメータ設定が有効になりません。
- [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 [電話の設定（Phone 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（最も高い優先順位）
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（最も低い優先順位）

ステップ 6 [保存（Save）] を選択します。

リモート ポート設定のセット アップ

スイッチ リモート ポート設定パラメータまたは PC のリモート ポート設定パラメータを設定するには、個々の電話機または複数の電話機を設定できます。

手順

ステップ 1 個々の電話機にパラメータを設定するには、次の手順を実行します。

a) 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。

b) 適切な IP Phone を選択します。
c) [プロダクト固有の設定（Product Specific Configuration Layout）]（スイッチ ポートのリモート設定または PC ポートのリモート設定）領域にスクロールして、パラメータを設定します。
d) [保存（Save）] を選択します。

ステップ 2 複数の電話機の設定を同時に設定するには、次の手順を実行します。

a) Cisco Unified Communications Manager の管理ページで、[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) リモート ポート設定パラメータを設定します。
c) [保存（Save）] を選択します。

ヘッドセットの側音制御の設定

ユーザがヘッドセットを使用してコールを処理する場合、話し中にフィードバックが聞こえると感じることがあります。このような追加音声は側音と呼ばれます。側音が多すぎると、ユーザにはヘッドセットの受話口に自分の声が聞こえるので、この側音が邪魔になります。側音の量はヘッドセットによって異なります。

側音レベルは調整が可能です。使用可能な側音レベルは次のとおりです。

- 大（High）
- 標準（Normal）（デフォルト）
- 低（Low）
- オフ（Off）

手順

ステップ 1 Cisco Unified Communications Manager の管理に移動し、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 電話機のリストから電話機を検索します。

ステップ 3 電話機の [デバイス名（Device Name）] をクリックします。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動し、[ワイドバンド ヘッドセット UI 設定（Wideband Headset UI Control）] ドロップダウン リスト ボックスから、適切なプロファイルを選択します。
[オフ（Off）] オプションがデフォルトで選択されます（ユーザのヘッドセットがワイドバンドをサポートする場合だけイネーブルにします）。

[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 5 [保存（Save）] を選択します。

Release ボタンからのダイヤル トーンのセットアップ

アクティブ コールから [発信（New Call）] ウィンドウおよびダイヤル トーンへの 1 ボタン アクセスをユーザに提供できます。

次の表に、Release ボタン機能のダイヤル トーンのフィールドについて説明します。

フィールド	説明
リリースボタンからダイヤルトーンを提供（Provide Dial Tone from Release Key）	Release キーを押したとき、ユーザにダイヤル トーンが聞こえるか（[有効（Enabled）]）聞こえないか（[無効（Disabled）]）を指定します。 [有効（Enabled）] または [無効（Disabled）] を指定します。 デフォルトは [無効（Disabled）] です。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、次のいずれかのウィンドウに移動します。

- [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 2 [リリースボタンからダイヤルトーンを提供（Provide Dial Tone from Release Key）] フィールドを設定します。

パーク モニタリング

パーク モニタリングがサポートされるのは、Cisco IP Phone 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 *27*：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。 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 Configuration）] 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に上書きできます（このウィンドウを表示するには、Cisco Unified Communications Manager の管理ページで、[コール ルーティング（Call Routing）] > [電話番号（Directory Number）] を選択します）。値として 0 を指定すると、[パーク モニタリング定期復帰タイマー（Park Monitoring Periodic Reversion Timer）] サービス パラメータに指定された定期復帰間隔がすぐに利用されます。（次の説明を参照してください）。たとえば、このパラメータを 0 に設定し、パーク モニタリング定期復帰タイマーを 15 に設定した場合、パークし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 モニタリング転送タイマー（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。
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 Manager が、コール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）を決定します。ユー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できます。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（以下の説明を参照）に指定した時間が経過するまでは、Cisco Unified Communications Manager はパークされて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、パークされたコールに関する定期的な通知は無効になります。
Park Monitoring Forward No Retrieve Timer	デフォルトは 300 秒です。このパラメータは、パーク アラーム通知が発生するまでの秒数を決定します。その後、パークされたコールは、パークしたユーザが [電話番号の設定（Directory Number Configuration）] ウィンドウで指定した未取得時のパーク モニタリング転送の接続先に転送されます（Cisco Unified Communications Manager の管理で転送先が指定されていない場合、コールは、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マー（Park Monitoring Reversion Timer）] のサービス パラメータが時間切れになると、このパラメータが開始します。[未取得時のパーク モニタリング転送タイマー（Park Monitoring Forward No Retrieve Timer）] が時間切れになると、コールはパークから削除され、指定された接続先に転送されるか、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 *28*：パーク モニタリング パラメータ

フィールド	説明
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。
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）	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。 デフォルトは 60 秒です。 0 以外の値を設定すると、その値によって、[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。

実行可能な着信呼警告の有効化

この機能が有効である場合、着信コールがあったときに実行可能なアラートが表示されます。アラートは従来の着信コールのポップアップ通知に代わるもので、ユーザはアラートに応答する必要があります。

（注） カスタム ライン フィルタと実行可能な着信コール アラート機能の両方を有効にすると、実行可能なコール アラートはフィルタの対象回線だけに適用されます。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、次のいずれかを選択してください。

- [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）]

ステップ 2 実行可能な着信コール アラートのフィールドを特定し、適切な設定にフィールドを設定します。設定可能なフィールドの値は次のとおりです。

- [無効（Disabled）]：（デフォルト）実行可能な着信コールアラートは無効になっています。従来の着信コールのポップアップ 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アラートを表示します。
- [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アラートを表示します。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。

他のウィンドウでこのフィールドを設定すると、設定の優先順位は次のとおりです。

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（Save）] を選択します。

コール履歴表示拡張の有効化

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] に移動して、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 Cisco Unified CM に関連付けられた電話機のリストからユーザの電話機を探します。

ステップ 3 電話機の [デバイス名（Device Name）] をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動し、[ログ表示（Logging Display）] ドロップダウン リスト ボックスから、[有効（Enable）] を選択します。
[無効（Disabled）] オプションはデフォルトで選択されています。

[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

共有回線のコール履歴の有効化

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 CM の管理（Cisco Unified Communications Manager Administration）] に移動して、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 Cisco Unified CM に関連付けられた電話機のリストからユーザの電話機を探します。

ステップ 3 電話機の [デバイス名（Device Name）] をクリックします。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動し、[ログ表示（Logging Display）] ドロップダウン リスト ボックスから、適切なプロファイルを選択します。
[無効（Disabled）] オプションはデフォルトで選択されています。

[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

関連トピック

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

デフォルト回線フィルタのセットアップ

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] に移動して、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 [デフォルト回線フィルタ（Default line filter）] フィールドを見つけ、回線 DN を入力します。デバイス名エントリはカンマで区切ります。
指定された回線がデフォルト フィルタに追加されます。

カスタム回線フィルタのセットアップ

カスタム回線フィルタ機能は、必要に応じて優先度の高い回線だけにアラートをフィルタリングすることでアラート アクティビティを減らす、設定可能なオプションを提供します。デフォルトの電話フィルタだけを設定または編集できます。

デフォルトの回線フィルタが設定されると、[毎日のスケジュール（Daily schedule）] というフィルタを、電話機の [設定（Settings）] > [初期設定（Preferences）] メニューにある [コール通知（Call notifications）] から使用できるようになります。[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。

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 [デフォルト回線フィルタ（Default line filter）] フィールドを設定します。
デフォルト フィルタに含める電話機デバイス名のカンマ区切りリスト。

デフォルトではリストは空白で、プロビジョニングされたすべての回線が検査されます。

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 Phone 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 CM 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 Phone 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 Phone 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、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。

（まだサービスでない）PAB やスピード ダイヤルを IP Phone 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）] > [IP Phone サービス（Phone Services）] を選択します。
[IP Phone 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（Add New）] をクリックします。
[IP Phone 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> または *https://<IP_address>*（Cisco Unified IP Phone 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（Save）] を選択します。

（注） サービス URL を変更した場合、IP Phone 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 Phone サービスとして設定する必要があります。

IP Phone 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 CM 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できるようになり、電話機のボタンにサービスが関連付けられました。

関連トピック

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

電話機の Web ページへのアクセスの制御

セキュリティ上の理由から、電話機の Web ページへのアクセスはデフォルトで無効になっています。これにより、電話機の Web ページおよび Cisco Unified Communications セルフ ケア ポータルへのアクセスが禁止されます。

（注） Cisco Quality Report Tool などの一部の機能は、電話機の Web ページにアクセスしないと正しく動作しません。また、Web アクセスを無効にすると、CiscoWorks などの Web アクセスに依存するサービスアビリティ アプリケーションにも影響します。

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 電話機の検索条件を指定して [検索（Find）] を選択します。または、[検索（Find）] を選択してすべての電話機を表示します。

ステップ 3 デバイス名を選択して、そのデバイスの [電話の設定（Phone Configuration）] ウィンドウを開きます。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration）] 領域までスクロールします。

ステップ 5 アクセスを有効にするには、[Web アクセス（Web Access）] ドロップダウン リストで、[有効（Enabled）] を選択します。

ステップ 6 アクセスを無効にするには、[Web アクセス（Web Access）] ドロップダウン リストで、[無効（Disabled）] を選択します。

ステップ 7 [保存（Save）] を選択します。

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機能管理ポリシーとソフトキーテンプレート機能のどちら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。

デフォルトは、[機能管理ポリシー（Feature Control Policy）] 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 Phone 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 Phone 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 *29*：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ト	注記
応答	応答（Answer）	○	—
折り返し	折返し（CallBack）	○	—
すべてのコールの転送	不在転送（cfwdAll）	○	電話機は [不在転送（Forward all）] または [不在オフ（Forward off）] を表示。
コール パーク	パーク（Park）	○	—
コール ピックアップ	ピック（Pickup）	○	—
割込み	割込み	○	割り込みは、組み込みの会議ブリッジを使用します。
C 割り込み	会議への割り込み	○	C 割り込みは、Cisco Unified Communications Manager の会議ブリッジを使用します。ソフトキーラベルは割り込みです。
会議	会議（Confrn）	○	会議は専用ボタンです。
会議リスト	参加者（ConfList）	○	電話機は [詳細の表示（Show detail）] と表示。
転送	即転送（iDivert）	○	電話機は [拒否（Decline）] と表示。
サイレント	サイレント（DND）	○	サイレントをプログラム可能な回線ボタンまたはソフトキーとして設定します。

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	注記
終了	終了（EndCall）	○	—
グループ ピックアップ	G ピック（GPickUp）	○	—
保留	保留（Hold）	○	保留は専用ボタンです。
ハント グループ	ハント（HLog）	○	ハント グループは、プログラム可能な回線ボタンとして設定します。
参加	参加（Join）	なし	—
迷惑呼 ID	迷惑呼 ID（MCID）	○	迷惑呼 ID をプログラム可能な機能ボタンまたはソフトキーとして設定します。
ミートミー	ミートミー（MeetMe）	○	—
モバイル コネクト	モビリティ（Mobility）	○	モバイル コネクトをソフトキーとして設定します。
発信	発信（NewCall）	○	—
その他のピックアップ	他 Grp（oPickup）	○	—
キュー統計情報の PLK サポート	キュー ステータス（Queue Status）	なし	—
品質レポート ツール	品質レポート ツール（QRT）	○	品質レポート ツールをプログラム可能な機能ボタンまたはソフトキーとして設定します。
リダイヤル	リダイヤル（Redial）	○	—
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）	なし	—
復帰	復帰（Resume）	○	—

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	注記
選択	選択（Select）	なし	—
スピードダイヤル	短縮（AbbrDial）	○	電話機には、[スピード ダイヤル（SpeedDial）] と表示されます。
転送	転送（Trfr）	○	転送は専用ボタンです。
ビデオ モード コマンド	ビデオ（VidMode）	なし	—

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 変更内容を保存します。

関連トピック

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

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 および sRTP ポートの値の範囲は 2048 ～ 65535 で、デフォルト範囲は 16384 ～ 32764 です。RTP および sRTP ポート範囲内のポート値の一部は、他の電話サービス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（Save）] 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）

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、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 の管理ページで、[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 ～ 3600 秒です。デフォルト値は 3600 です。フィールドが 0 に設定された場合は、 TLS セッション再開はディセーブルです。

関連トピック

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

音声ポートとビデオ ポートの範囲設定

音声およびビデオ トラフィックは、Quality of Service（QoS）向上のため異なる RTP ポート範囲に送信できます。

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] の次のフィールドで、ポート範囲を制御します。

- 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
  - 開始ビデオ RTP ポート（Start Video RTP Port）
  - 終了ビデオ RTP ポート（Stop Video RTP Port）

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、電話機は音声トラフィックとビデオ トラフィックの両方に設定された音声ポートを使用します。

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。

手順

ステップ 1 Cisco Unified CM 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。
音声ポートは、ポート 16384 ～ 32766 を使用するように設定できます。

ステップ 3 [保存（Save）] 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。

- 各フィールドは、2048 ～ 65535 の数字である必要があります。
- [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（Save）] 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。

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）

マネージャとは、着信コールがルーティング サービスによって代行受信されるユーザのことです。

アシスタント（Assistant）

アシスタントは、マネージャに代わってそのコールに応対するユーザです。

アシスタント コンソール（Assistant Console）

アシスタントコンソールとは、アシスタントが使用するデスクトップアプリケーションで、タスクを実行し、ほとんどの機能の管理を行います。

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。

共用回線モードで Cisco IPMA を設定すると、マネージャとアシスタントは電話番号を共有します。ここでは例として、1701 とします。アシスタントは共用電話番号でマネージャのコールを処理します。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、アクセスすることはできません。アシスタントの電話機には、DivertAll 機能用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、Assistant Watch、コール代行受信、DivertAll 機能用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、プロキシ番号を使用して、マネージャへのコールを処理します。プロキシ番号は、マネージャの電話番号ではありませんが、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します。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 機能は、ソフトキーおよび電話サービスによってアクセスされます。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。

標準マネージャ

プロキシ モードのマネージャをサポートします。

標準共有モード マネージャ

共有モードのマネージャをサポートします。

標準アシスタント

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 *30*：*IPMA* ソフトキー

ソフトキー	コール状態	説明
リダイレクト（Redirect）	Ringing、Connected、OnHold	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）	Ringing、Connected、OnHold	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。

ソフトキー	コール状態	説明
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。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 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。

関連トピック

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

Visual Voicemail 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 Phone 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。

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）] > [電話サービス（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 Phone 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 Phone 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。

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。

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 Phone 8811、8841、および 8851NR 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。

複数ライン同時通話（Join Across Lines）機能および回線間転送（Transfer Across Lines）機能の管理

複数ライン同時通話（JAL）機能では、ユーザが（異なる電話番号、または同じ電話番号で異なるパーティション）の複数の電話回線のコールに参加して会議を作成することができます。回線間転送（TAL）機能では、ユーザが 1 つの確立済みコールを（異なる電話回線または同じ回線の）別の確立済みコールに転送することができます。JAL および TAL の機能を無効化すると、ユーザが誤ってコールに参加したり、コールを転送することを防止できます。

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（Enterprise Phone）]

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（Enterprise Phone）]

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 [参加および直接転送ポリシー（Join and Direct Transfer Policy）] フィールドで次の設定のいずれかを選択します。

- [同一回線、回線全体で有効（Same line, across line enable）]（デフォルト）
- [同一回線で有効（Same line enable）]
- [同一回線、回線全体で無効（Same, across line disable）]

ステップ 4 [保存（Save）] を選択します。

コンピュータからのビデオのセット アップ

コンピュータによるビデオのサポート機能によって、コンピュータが電話機に接続されている場合、コンピュータでビデオを送信または受信できます。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。

（注） デフォルトでは、[コンピュータからのビデオ（Video through Computer）] オプションは無効化されています。

ユーザは [設定（Preferences）] メニューで [コンピュータからのビデオ（Video through Computer）] オプションを有効化または無効化できます。[コンピュータからのビデオ（Video on Computer）] オプションが有効化されている場合：

- ビデオ機能を使う：ビデオは PC で受信および表示され、電話機に音声が維持されます。
- ビデオ機能を使わない：ビデオは、電話機にも PC にも表示されません。

この機能は、SCCP または SIP プロトコルに依存します。SIP ファームウェアを使用する IP Phone はビデオを送信せずにビデオを受信できます。SCCP ファームウェアを使用する IP Phone はビデオを個別に送受信できません。

（注） 電話機は、PC で最初のネットワーク インターフェイス カード（NIC1）に物理的に接続されている必要があります。

[コンピュータからのビデオ（Video through Computer）] を使用する場合、Windows 9.7(5) 以降、および Cisco メディア サービス インターフェイス（MSI）の最新バージョンが必要です。ハードウェアとソフトウェアの要件のリストについては、『*Cisco Jabber for Windows 9.7(5) Release Notes*』またはそれ以降のバージョンのリリース ノート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 ビデオ機能のオプションをイネーブルにします。

関連トピック

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

ビデオ送信解像度のセットアップ

Cisco IP Phone 8845 および 8865 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（432 X 240）
- VGA（640 X 480）
- CIF（352 X 288）
- SIF（352 X 240）
- QCIF（176 X 144）

ビデオ機能付き Cisco IP Phone 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。

表 *31*：*Cisco Unified IP Phone 8845* および *8865* のビデオ送信解像度と機能

ビデオのタイプ	ビデオ解像度	フレーム/秒（fps）	ビデオ ビット レート範囲
720p	1280 X 720	30	1360 ～ 2500 kbps
720p	1280 X 720	15	790 ～ 1359 kbps
WVGA	800 X 480	30	660 ～ 789 kbps
WVGA	800 X 480	15	350 ～ 399 kbps

ビデオのタイプ	ビデオ解像度	フレーム/秒（fps）	ビデオ ビット レート範囲
360p	640 X 360	30	400 ～ 659 kbps
360p	640 X 360	15	210 ～ 349 kbps
240p	432 X 240	30	180 ～ 209 kbps
240p	432 X 240	15	64 ～ 179 kbps
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

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。

ユーザが問題レポートを発行するには、問題レポート ツールにアクセスし、問題が発生した日時、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機への 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 サポートのアップロード URL の設定

PRT ファイルを受信するには、サーバにアップロード スクリプトが必要です。PRT では、HTTP POST 機構と、アップロードに含まれる次のパラメーターが使用されます（マルチパート MIME 符号化を使用）。

- devicename（例：「SEP001122334455」）
- serialno（例：「FCH12345ABC」）
- username（CUCM で設定される、デバイス所有者のユーザ名）
- prt_file（例：「probrep-20141021-162840.tar.gz」）

スクリプト例を次に示します。このスクリプトは参考情報として掲載しています。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 スクリプトをサポートしていません。

```
<?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.");
}

?>
```

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ようサーバをセットアップします。

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、提供されているサンプル スクリプトを必要に応じて編集します。

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）] をオンにして、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。

プライマリ回線における全コールを表示

ボタン テンプレートを使用する代わりにプライマリ回線の現在のコールや不在着信の一覧を表示するよう電話機を設定できます。

この機能は、複数の回線を使用している場合に便利です。この機能では、すべての回線上のすべてのコールを単一の画面で確認することができます。しかし、特定の回線をフィルタリングすることもできます。また、別の専用タスクに使用できる機能キーを設定することもできます。

Cisco Unified Communications Manager のデバイス ページから [プライマリ回線でのすべてのコールの表示（View All Calls on Primary Line）] を有効にします。

また、[プライマリ回線でのすべてのコールの表示（Show All Calls on Primary Line）] と [すべてのコールに戻る（Revert to All Calls）] も有効にします。[すべてのコールに戻る（Revert All Calls）] だけを有効にすると、電話機に [すべてのコール（All Calls）] フィルタ ビューが表示されます。しかし、その表示はデフォルトでプライマリ回線にはなりません。プライマリ回線または [呼び出しコール（Alerting Calls）] フィルタを選択した場合、すべてのコールに戻る機能が失敗します。[すべてのコールに戻る（Revert to All Calls）] 機能を使用するには、[すべてのコール PLK（All Calls PLK）] と [プライマリ回線でのすべてのコールの表示（Show All Calls on Primary Line）] のどちらかが必要です。

[プライマリ回線における全コールを表示（View All Calls on Primary Line）] を設定すると、[すべてのコール（All Calls）] フィルタに関連付けられているすべての機能が有効になります。

関連トピック

すべてのコールの電話ボタン テンプレートの割り当て，（253 ページ）

プライマリ回線における全コール表示の設定

手順

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

ステップ 2 [プライマリ回線でのすべてのコールの表示（Show All Calls on the Primary Line）] 設定を見つけます。

ステップ 3 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 4 [設定の適用（Apply Config）] を選択します。

ステップ 5 [保存（Save）] を選択します。

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。

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 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） 回線を共有する他のデバイスにこの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（Save）] を選択します。

第 13 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，275 ページ
- パーソナル ディレクトリのセットアップ，275 ページ
- 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，276 ページ
- アプリケーション ダイヤル ルール，278 ページ

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 では、Cisco Unified Communications Manager と連動する Cisco Unified Communications Manager アプリケーションのユーザの認証情報と認可情報を保存するために、Lightweight Directory Access Protocol（LDAP）ディレクトリを使用しています。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。

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。

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（Speed Dials）
- 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：Cisco Unified Communications セルフ ケア ポータルから PAB やスピード ダイヤル機能を利用できます。
- Cisco IP Phone から：連絡先を選択して、社内ディレクトリやユーザのパーソナル ディレクトリを検索できます。
- 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 Phone Address Book Synchronizer のダウンロード，（276 ページ）およびSynchronizer のセットアップ，（278 ページ）を参照してください。

Cisco IP Phone 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 Phone 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 ポータルへのアクセスの設定，（92 ページ）を参照してください。
- Cisco IP Phone 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 Phone Address Book Synchronizer のダウンロード，（276 ページ）を参照してください。

Cisco IP Phone 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 CM の管理で、[アプリケーション（Application）] > [プラグイン（Plugins）] を選択します。

ステップ 2 Cisco IP Phone Address Book Synchronizer プラグイン名の横にある [ダウンロード（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 Phone Address Book Synchronizer の導入, （277 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 Phone Address Book Synchronizer の導入

Cisco IP Phone 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 Phone 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 Phone 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 [実行（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、[同意します（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、[次へ（Next）] を選択します。

ステップ 7 [インストール（Install）] を選択します。

ステップ 8 [完了（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, （278 ページ）の手順を実行します。

Synchronizer のセットアップ

Cisco IP Phone 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 Phone 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、[開始（Start）] > [すべてのプログラム（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、[ユーザ（User）] を選択します。

ステップ 3 Cisco IP Phone 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、[同期（Synchronize）] を選択します。
[同期の状況（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、[選択の重複（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、[終了（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、[個人アドレス帳（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。

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、もしくはユーザが発信す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。

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 CM の管理（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 次のフィールドを入力します。

- [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 Begins With）]：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 of Digits）]：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 Digits to 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 With Pattern）]：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 Rule Priority）]：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 V 部

Cisco IP Phone のトラブルシューティング

- 電話システムの監視，283 ページ
- トラブルシューティング，327 ページ
- メンテナンス，347 ページ
- 各言語ユーザのサポート，355 ページ

第 14 章

電話システムの監視

- Cisco IP Phone のステータス，283 ページ
- Cisco IP Phone Web ページ，306 ページ
- XML での電話からの情報要求，322 ページ

Cisco IP Phone のステータス

ここでは、Cisco IP Phone 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，（327ページ） を参照してください。

[モデル情報（Model 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 ボタンを押します。

ステップ 2 [電話の情報（Phone Information）] 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（ロックまたは認証マーク）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。

[モデル情報（Model Information）] のフィールド

次の表で、[モデル情報（Model Information）] 設定フィールドを説明します。

表 *32*：モデル情報の設定

オプション	説明
モデル番号（Model Number）	電話機のモデル番号。
IPv4 アドレス（IPv4 Address）	電話機の IP アドレス。
ホスト名（Host name）	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。

オプション	説明
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の一覧が表示されます。 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。
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（Status）] メニューを表示するには、アプリケーション 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）] 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 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。信頼リストの詳細については、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。

表 33 : *Cisco Unified IP Phone* 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/オンにします。

メッセージ	説明	考えられる状況と対処方法
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いコピーを入手し、それをTFTPPathディレクトリに置きます。ファイルをこのディレクトリにコピーできるのは、TFTPサーバ ソフトウェアがシャットダウンされているときだけです。それ以外の場合にコピーすると、ファイルが破損する可能性があります。
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。このメッセージは情報を通知するだけです。CTLファイルとITLファイルのどちらも、過去にインストールされていません。
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。このメッセージは情報を通知するだけです。CTLファイルは過去にインストールされていません。
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ファイルに問題があります。
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ている：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。 DHCPサーバと電話機との間にネットワーク接続がない：ネットワーク接続を確認してください。 DHCPサーバがダウンしている：DHCPサーバの設定を確認してください。 エラーが続く：スタティックIPアドレスを割り当てることを検討してください。

メッセージ	説明	考えられる状況と対処方法
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ている：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。 DNS サーバと電話機との間にネットワーク接続がない：ネットワーク接続を確認してください。 DNS サーバがダウンしている：DNS サーバの設定を確認してください。
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 Unified Communications Manager のホスト名が DNS に正しく設定されていることを確認してください。 ホスト名ではなく、IP アドレスを使用することを検討してください。
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 アドレスが割り当てられている場合は、重複する IP アドレスを割り当てていないことを確認してください。 DHCP を使用している場合は、DHCP サーバの設定を確認してください。
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。このメッセージは情報を通知するだけです。

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 Operating System の管理ページから、次のファイルが [TFTP ファイルの管理（TFTP File Management）] のサブディレクトリに存在することを確認してください。 • ネットワーク ロケールと同じ名前のサブディレ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のサブディレクトリに存在するファイル： ◦ glyphs.xml ◦ dictionary.xml ◦ kate.xml

メッセージ	説明	考えられる状況と対処方法
ファイルが見つかりません <Cfg ファイル>（File not found <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、電話機が Cisco Unified Communications Manager データベースに追加されたときに作成されます。電話機が Cisco Unified Communications Manager データベースに存在しない場合、TFTP サーバは「CFG ファイルが見つかりません（CFG File Not Found）」という応答を生成します。 • 電話機が Cisco Unified Communications Manager に登録されていません。 電話機を自動登録できない場合は、手動で電話機を Cisco Unified Communications Manager に追加する必要があります。詳細については、電話機の追加方法, （79 ページ）を参照してください。 • DHCP を使用している場合は、DHCP サーバが正しい TFTP サーバを指定していることを確認してください。 • スタティック IP アドレスを使用している場合は、TFTP サーバの設定を確認してください。
「ファイルが見つかりません <CTLFile.tlv>（File Not Found <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。引き続き電話機は Cisco Unified Communications Manager に登録できます。
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/オンにするか、または DHCP アドレスをリセットするまで、アイドル状態のままです。

メッセージ	説明	考えられる状況と対処方法
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。このメッセージは情報を通知するだけです。ITL ファイルは過去にインストールされていません。
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変更をサポートしていないバージョンのソフトウェアをインストールしようとすると発生します。 電話機に割り当てられたロード ID を確認します（Cisco Unified Communications Manager で [デバイス（Device）] > [電話（Phone）] を選択します）。電話機に表示されたロードを再入力します。
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 アドレスが割り当てられている場合は、デフォルト ルータが設定されていることを確認してください。 DHCP を使用している場合は、DHCP サーバがデフォルト ルータを提供していません。DHCP サーバの設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 アドレスが割り当てられている場合は、DNS サーバが設定されていることを確認してください。 DHCP を使用している場合は、DHCP サーバが DNS サーバを提供していません。DHCP サーバの設定を確認してください。
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 Unified Communications Manager で設定されていません。Cisco Unified Communications Manager はデフォルトではセキュリティをサポートしません。

メッセージ	説明	考えられる状況と対処方法
「CUCM 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 Manager で電話機の設定変更が行われ、変更を有効にするために [適用（Apply）] ボタンが押された可能性があります。
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、DHCP サーバが正しい TFTP サーバを指定していることを確認してください。 スタティック IP アドレスを使用している場合は、TFTP サーバの設定を確認してください。
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 に連絡してください。
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いる：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。 TFTP サーバと電話機との間にネットワーク接続がない：ネットワーク接続を確認してください。 TFTP サーバがダウンしている：TFTP サーバの設定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。	認証は一般的に、スイッチで 802.1x が設定されていない場合に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。	

メッセージ	説明	考えられる状況と対処方法
		電話機はCTLファイルおよびITLファイルをインストールしていますが、新しいCTLファイルおよびITLファイルの更新に失敗しました。 失敗の理由として次が考えられます。 • ネットワークの障害が発生した。 • TFTPサーバがダウンしていた。 • CTLファイルの署名に使用された新しいセキュリティトークン、および、ITLファイルの署名に使用されたTFTP証明書が導入されたが、電話機の現在のCTLファイルおよびITLファイルには使用できない。 • 内部的な電話障害が発生した。 解決策として次が考えられます。 • ネットワーク接続を確認します。 • TFTPサーバがアクティブで、正常に機能しているかどうかを確認する。 • Transactional Vsam Services（TVS）サーバがCisco Unified Communications Managerでサポートされている場合は、TVSサーバがアクティブで、正常に機能しているかどうかを確認する。 • セキュリティ トークンおよびTFTPサーバが有効かどうかを確認する。

メッセージ	説明	考えられる状況と対処方法
		上述の解決策がすべて失敗した場合は、手動で CTL ファイルおよびITL ファイルを削除し、電話機をリセットする。
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。このメッセージは情報を通知するだけです。
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 ファイルが正しい名前であることを確認してください。
XmlDefault.cnf.xml（または電話機のデバイス名に対応した .cnf.xml）	設定ファイルの名前。	なし。このメッセージは、電話機の設定ファイル名を示します。

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 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 *34*：イーサネット統計情報

項目	説明
Rx フレーム（Rx Frames）	電話機が受信したパケットの数。
Tx フレーム（Tx Frames）	電話機が送信したパケットの数。
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（Restart Cause）	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。 • Initialized • 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（Elapsed Time）	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（Port 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（Port 2）	PC ポートのリンク状態と接続。

項目	説明
DHCP 状態（DHCP state）（IPv4/IPv6）	• IPv4 モードでは、表示の 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., (GOOD IP) など、DHCPv6 状態だけが表示されます。 • デュアル スタック モードでは、DHCPv4 および DHCPv6 両方の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 *35*：*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

DHCPv4 状態	説明
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 *36*：*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
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

DHCPv6 状態	説明
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 Phone 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 統計情報

次の表に、電話機での WLAN 統計を示します。

表 *37*：*Cisco Unified IP Phone* 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の数。
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（Tx frames）	正常に送信された MSDU の数。
Tx マルチキャスト フレーム（tx multicast frames）	正常に送信されたマルチキャスト MSDU の数。
Tx リトライ（tx retry）	1 つまたは複数の再送信後に正常に送信された MSDU の数。
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。

項目	説明
Rx 重複フレーム（rx duplicate frames）	[シーケンス制御（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 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）] > [コールの統計（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 *38*：*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）	受信された音声ストリームのタイプ（RTP ストリーミング オーディオの送信元コーデック）。G.729、G.722、G.711 mu-law、G.711 A-law、iLBC。
送信コーデック（Sender Codec）	送信された音声ストリームのタイプ（RTP ストリーミング オーディオの送信元コーデック）。G.729、G.722、G.711 mu-law、G.711 A-law、iLBC。
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）。
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）	

項目	説明
累積フレーム損失率（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。
最大フレーム損失率（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 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 Phone 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 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 *39*：*[*現在のアクセス ポイント（*Current Access Point*）*]* の項目

項目	説明
AP 名（AP name）	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。
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（Capability）	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。
サポートされる VHT(rx)レート	AP から受け取った VHT 対応 RX MCS Set。
サポートされる 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 HT 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。
国コード（Country code）	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（Channels）	（国 IE で）サポートされているチャネルのリスト。

項目	説明
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。
チャネル使用率（Channel utilization）	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。
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 Phone 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（Proxy 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 Phone 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（Best Effort）	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。
バックグラウンド（Background）	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（Video）	ビデオ キューに関連した情報が記載されています。
音声（Voice）	音声キューに関連した情報が記載されています。

Cisco IP Phone Web ページ

Cisco IP Phone 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。

ここでは、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 Phone の IP アドレスを入手します。

a) Cisco Unified CM 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、[電話の検索と一覧表示（Find and List Phones）] ウィンドウと [電話の設定（Phone Configuration）] ウィンドウの上部に表示されます。

b) Cisco IP Phone 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 Phone 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,（306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 40 : [デバイス情報（*Device Information*）] 領域の項目

項目	説明
MAC アドレス（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（Host name）	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。
電話番号（Phone DN）	電話機に割り当てられている電話番号。
バージョン（Version）	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 KEM の ID。
キー拡張モジュール 2（Key Expansion Module 2）	該当する場合、2 番目の KEM の ID。
キー拡張モジュール 3（Key Expansion Module 3）	該当する場合、3 番目の KEM の ID。

項目	説明
ハードウェアのリビジョン（Hardware Revision）	電話機のハードウェアのリビジョン値。
シリアル番号（Serial Number）	電話機の固有のシリアル番号。
モデル番号（Model Number）	電話機のモデル番号。
メッセージ受信（Message Waiting）	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）]：電話機モデルを指定します。 • [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）	KEM の Cisco 固有デバイス識別情報（UDI）。
時刻（Time）	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（Time Zone）	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。
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 Phone 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。

[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，（306 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 *41*：*[ネットワークのセットアップ（Network Setup）]* 領域の項目

項目	説明
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）サーバの IP 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どうかを示します。
MAC アドレス（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（Host Name）	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。
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。
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。
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。
TFTP サーバ 2（TFTP Server 2）	電話機で使用される、バックアップの Trivial File Transfer Protocol（TFTP）サーバ。
デフォルト ルータ 1（Default Router 1）	電話機で使用される、デフォルト ルータ。

項目	説明
DNS サーバ 1-3（DNS Server 1-5）	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）]）。
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 Networks（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。
CUCM サーバ 1（CUCM Server 1）～CUCM サーバ 5（CUCM Server 5）	電話機を登録可能な Cisco Unified Communications Manager サーバのホスト名または IP アドレス（優先度順）。限定された Cisco Unified Communications Manager 機能を提供できる 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こともあります。 使用可能なサーバについては、この項目に Cisco Unified Communications Manager サーバの 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）]：電話機が現在コール処理サービスを受けている Cisco Unified Communications Manager サーバです。 • [スタンバイ（Standby）]：現在のサーバがダウンした場合に、電話機が切り替える先の Cisco Unified Communications Manager サーバ。 • [空白（Blank）]：この Cisco Unified Communications Manager サーバへの接続は現在ありません。 項目には、Survivable Remote Site Telephony（SRST）指定も含めることができます。これは、限定された Cisco Unified Communications Manager 機能を提供できる SRST ルータを特定します。このルータは、他のすべての Cisco Unified Communications Manager サーバが到達不能になった場合に、コールの処理を引き継ぎます。SRST Cisco Unified Communications Manager 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。SRST ルータ アドレスは、[Cisco Unified CM の設定（Cisco Unified Communications Manager Configuration）] 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（Information 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）	電話機でディレクトリ情報の取得元となるサーバの URL。

項目	説明
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。
サービス URL（Services URL）	電話機が Cisco Unified IP Phone サービスを取得するサーバの URL。
DHCP	電話機が DHCP を使用するかどうかを示します。
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 アドレス解放（DHCP Address Released）] オプションの設定を示します。
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。
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間にわたって使用されず、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、この時間の経過後、[アイドル URL（Idle URL）] で指定した XML サービスがアクティブになります。
プロキシ サーバの 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 HTTP 要求を送信し、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するプロキシ 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 URL。
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。

項目	説明
PC ポートのセットアップ（PC 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）]：PC ポートへの接続がありません。
ユーザ ロケール（User Locale）	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、日付と時刻の形式、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一連の詳細情報を示します。
ネットワーク ロケール（Network Locale）	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。電話機が使用するトーンと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情報を示します。
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。
PC ポートを無効にする（PC Port Disabled）	電話機の PC 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。
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。
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 コールに参加できるかどうかを示します。

項目	説明
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 へのアクセスを許可するかどうかを示します。
通話制御の DSCP（DSCP for Call 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（Security Mode）	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）]）かを示します。
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どうかを表示します。
PC VLAN	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。
PC ポートの CDP（CDP on 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（デフォルトでは有効）。 Cisco Unified Communications Manager で CDP が無効になっている場合は、PC ポートで CDP 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）] メニューに表示されます。

項目	説明
SW ポートの CDP（CDP on 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（デフォルトでは有効）。 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 VLAN を割り当てる場合は、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 を有効にします。 CDP が Cisco Unified Communications Manager で無効になっているときは、電話機を Cisco ス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 を無効にする必要が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）] メニューに表示されます。
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-MED）が有効になっているかどうかを示します。
LLDP：PC ポート（LLDP: PC Port）	リンク層検出プロトコル（LLDP）が PC ポートで有効かどうかを示します。
LLDP 電源優先度（LLDP Power Priority）	電話機の電源優先度をスイッチにアドバタイズし、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。次の設定があります。 • 不明（Unknown）：これがデフォルト値です。 • 低（Low） • 大（High） • クリティカル（Critical）
LLDP アセット 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 を識別します。

ネットワーク統計

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（Ethernet Information）]、[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 *42*：*[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（Tx broadcast）	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（Tx multicast）	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（Tx unicast）	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（Rx Frames）	電話機が受信したパケットの総数。
Rx ブロードキャスト（Rx broadcast）	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（Rx multicast）	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（Rx unicast）	電話機が受信するユニキャスト パケットの総数。
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 *43* : *[*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（Rx multicast）	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（Rx broadcast）	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（Rx unicast）	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
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

項目	説明
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（Tx broadcast）	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（Tx multicast）	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 Neighbor Device ID）	CDP が検出した、このポートに接続されているデバイスの ID

項目	説明
CDP ネイバー IPv6 アドレス	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
CDP ネイバー ポート（CDP Neighbor Port）	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 Neighbor Device 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 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 Neighbor Port）	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（Port Information）	速度と二重化モード。

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 Phone 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 44 : [ストリームの統計（*Streaming Statistics*）] 領域の項目

項目	説明
リモートアドレス（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（Start time）	Cisco Unified Communications Manager が電話機にパケットの送信開始を要求した時間を示す内部タイム 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（Host name）	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。
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 オクテットの総数。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 パケットの総数。予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して定義されます。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。接続が送信専用モードに設定されていた場合、値は 0 として表示されます。

項目	説明
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）。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。
送信した受信レポート（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（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 パケットの総数。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が含まれます。接続が送信専用モードに設定されていた場合、値は 0 として表示されます。
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 パケットで受信したペイロード オクテットの総数。マルチキャスト コールの場合は、さまざまな送信元から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場合、値は 0 として表示されます。
累積フレーム損失率（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）	アクティブな音声の直前の 3 秒間の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）を使用している場合、3 秒間のアクティブな音声を蓄積するには、より長い間隔が必要になることがあります。
最大フレーム損失率（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。
	リスニング品質（LQK）の平均オピニオン評点（MOS）を客観的に評価するスコアで、5（優良）～ 1（不良）でランク付けされます。このスコアは、音声ストリームの先行 8 秒間でのフレーム損失に起因する音声隠蔽イベントに基づいています。詳細については、音声品質のモニタリング，（351 ページ）を参照してください。 （注） MOS LQK スコアは、Cisco Unified IP Phone が使用するコーデック タイプに基づいて変化する可能性があります。

項目	説明
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 スコアまたは最も高い 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 LQK スコアを提供します。 • 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 スコアを計算するために使用されるシスコ独自のアルゴリズムのバージョン。
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 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）があった秒数。
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。
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。

項目	説明
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 RPT パケット。
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 Receiveds） （注を参照）	RTCP 受信レポートが最後に受信された時間。

（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。次の情報を参照できます。

- 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。

はじめる前に

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>
説明：

- <*phone ip address*> は電話機の 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
説明：

- <*phone ip address*> は電話機の 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/ModelInfo
説明：

- <*phone ip address*> は電話機の 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 15 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，327 ページ
- 起動時の問題，329 ページ
- Cisco IP Phone のリセットの問題，333 ページ
- 電話機が LAN に接続できない，336 ページ
- Cisco IP Phone のセキュリティの問題，336 ページ
- コールに関する一般的な問題，338 ページ
- トラブルシューティング手順，339 ページ
- Cisco Unified Communications Manager からのデバッグ情報の制御，344 ページ
- その他のトラブルシューティング情報，345 ページ

一般的なトラブルシューティング情報

次の表は、Cisco IP Phone の一般的なトラブルシューティング情報を示しています。

表 45 : *Cisco IP Phone* のトラブルシューティング

要約	説明
Cisco IP Phone から別の Cisco IP Phone への接続。	シスコでは、PC ポートを介した IP Phone 間の接続はサポートしていません。各 IP Phone はスイッチ ポートに直接接続する必要があります。電話機が PC 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場合、それらの電話機は動作しません。

要約	説明
長時間のブロードキャスト ストームのために、IP Phone 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 ブロードキャスト ストームのために、IP Phone がリセットされたり、アクティブなコールが失われたり、コールの発信や応答ができなくなることがあります。ブロードキャスト ストームが終了するまで、電話機が起動しないことがあります。
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、電話機の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 コンピュータに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、ネットワーク接続を介して電力を供給できないため、接続を介して電力を供給すると、ネットワーク カードが破損する場合があります。ネットワーク カードを保護するために、電話機からケーブルを抜いた後、10 秒以上待機してから、そのケーブルをコンピュータに接続してください。この待機している間に、スイッチは電話機が回線に存在しなくなったことを認識し、ケーブルへの電力供給を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変更をユー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ています。ネットワーク設定オプションを設定する前に、それらをロック解除する必要があります。詳細については、電話機パスワードの適用, （44 ページ）を参照してください。 **（注）** 管理者パスワードが共通の電話プロファイルで設定されていない場合、ユーザはネットワーク設定を変更できます。
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 Phone と他のデバイスとのやり取りに使用されているコーデックが表示されます。これらの統計情報の値は、一致している必要があります。コーデックが一致しない場合、相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、またはトランス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認します。
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 Phone と他のデバイスとのや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。これらの統計情報の値は、一致している必要があります。

要約	説明
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）] メニューの [SW ポート設定（SW Port Configuration）] オプションが [10 ハーフ（10 Half）]（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、次のメッセージがスイッチのコンソール 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ます。

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 Cisco IP Phone 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、次の項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, （72 ページ）

Cisco IP Phone が通常の起動プロセスを実行しない

問題

Cisco IP Phone をネットワーク ポートに接続したとき、電話機が関連項目で説明されている通常の起動プロセスを実行せず、電話スクリーン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。
  - 動作している Cisco IP Phone を別のポートから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であることを確認します。
  - 起動しない Cisco IP Phone 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 Phone をスイッチのポートに直接接続して、オフィスのパッチ パネル接続を省きます。
- 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。
- これらを実行しても電話機が正常に起動しない場合は、ハンドセットをオフフックにして電話機の電源を入れます。この方法で電話機に電源を投入すると、電話機はバックアップ ソフトウェア イメージを起動しようとします。
- 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、5 分経過しても Cisco IP Phone の電話スクリーン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, （72 ページ）

Cisco IP Phone 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、Cisco Unified Communications Manager サーバに登録されていない限り、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, （339 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, （286 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, （340 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。

関連トピック

DHCP 設定の確認, （341 ページ）

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, （343 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。詳細については、新しい電話機設定ファイルの作成, （342 ページ）を参照してください。

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 Phone 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、[検索（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, （332 ページ）を参照してください。

Cisco IP Phone 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。

Cisco IP Phone のリセットの問題

電話機が通話中やデスク上で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、Cisco IP Phone がリセットされることはありません。

通常は、イーサネット 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に電話機がリセットされます。

断続的なネットワークの停止による電話機のリセット

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。

関連トピック

DHCP 設定の確認, （341 ページ）

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Cisco IP Phone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。

意図的なリセットでの電話機リセット

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 PhoneがCisco Unified Communications Managerからリセット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。
- [リスタートの原因（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の管理ページからリセット/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，（340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 Phone が接続されている先の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 Phone のセキュリティの問題

ここでは、Cisco IP Phone 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ない。

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。

コールに関する一般的な問題

次の各項は、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。
   - **a** イーサネット ケーブルが接続されている。
   - **b** Cisco CallManager サービスが Cisco Unified Communications Manager サーバで作動している。
   - **c** 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。

TFTP 設定の確認

手順

ステップ 1 Cisco IP Phone 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 [設定のリセット（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 Cisco IP Phone 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 Cisco IP Phone 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、[検索（Find）] をクリックします。この Cisco IP Phone 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，（347 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 Cisco IP Phone で、アプリケーション 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）] > [IPv4 のセットアップ（IPv4 Setup）] を選択して、次のオプションを確認します。

- [DHCP サーバ（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 サーバ（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 アドレス（IP Address）]、[サブネット マスク（Subnet Mask）]、[デフォルト ルータ（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

新しい電話機設定ファイルの作成

（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。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。
- 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。

新しい設定ファイルを作成するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager 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 [削除（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 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

（注） 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。

サービスを開始するには、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、[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（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] の順に選択します。

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、[開始（Start）] ボタンをクリックします。
[サービス状況（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の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。

その他のトラブルシューティング情報

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、次の Cisco Web サイトにアクセスして、目的の電話機モデルに移動してください。

http://www.cisco.com/cisco/web/psa/troubleshoot.html

第 16 章

メンテナンス

- 基本的なリセット，347 ページ
- ネットワーク設定のリセット，349 ページ
- ユーザとネットワークの設定のリセット，349 ページ
- CTL ファイルの削除，350 ページ
- Quality Report Tool，350 ページ
- 音声品質のモニタリング，351 ページ
- Cisco IP Phone のクリーニング，352 ページ

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 *46*：基本的なリセットの方法

操作	操作	説明
電話機の再起動	[サービス（Services）]、[アプリケーション（Applications）]、または [ディレクトリ（Directories）] を押し、次に **#** を押します。	ユーザ セットアップおよびネットワーク セットアップ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、その後、電話機が再起動されます。

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 ボタンを押し、[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。	ユーザ セットアップおよびネットワーク セットアップの設定値をデフォルト値にリセットし、電話機を再起動します。
	CTL ファイルをリセットするには、アプリケーション ボタンを押し、[管理者設定（Admin Settings）] > [設定のリセット（Reset Settings）] > [セキュリティ（Security）] を選択します。	CTL ファイルがリセットされます。

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 # を押したままにして電話機のプラグを再接続します。

ステップ 4 [ヘッドセット（Headset）] ボタンと [スピーカー（Speaker）] ボタンが点灯したら、次のキー シーケンスを入力します。
123456789*0#

1 キーを押すと、[スピーカー（Speaker）] 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

電話機を工場出荷時の状態にリセットするには、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 ボタンを押します。

ステップ 2 リセットの設定はすべて、[管理者設定（Administrator Settings）]>[設定のリセット（Reset Settings）]>[すべて（All）] 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。

関連トピック

電話機パスワードの適用，（44 ページ）

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。

関連トピック

電話機パスワードの適用，（44 ページ）

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。

関連トピック

電話機パスワードの適用, （44 ページ）

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。

関連トピック

電話機パスワードの適用, （44 ページ）

Quality Report Tool

品質レポートツール（QRT）は、Cisco IP Phone 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 Phone 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 Phone 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 Phone かどうかによって異なります。

QRT の使用に関する詳細については、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。

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 Phone では隠匿イベントに基づいて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隠蔽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 が隠蔽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再生する秒数です。

（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。

[コール統計（Call Statistics）] 画面を使用して、Cisco IP Phone から音声品質メトリックにアクセスできます。また、[ストリームの統計（Streaming Statistics）] 画面を使用してリモートにアクセスすることもできます。

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 47：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 Phone のクリーニング

Cisco IP Phone をクリーニングするには、必ず乾いた柔らかい布で軽く電話機とスクリーンを拭いてください。液体や粉末を直接電話機に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。

電話機がスリープ モードになっているときは、スクリーンは空白で、選択ボタンは点灯しません。電話機がこの状態のときはスクリーンをクリーニングできますが、クリーニングを終了するまで電話機のスリープ状態が続くことがわかっている場合に限ります。

第 17 章

各言語ユーザのサポート

- Unified Communications Manager Endpoints Locale インストーラ，355 ページ
- 国際コールのロギングのサポート，356 ページ

Unified Communications Manager Endpoints Locale インストーラ

デフォルトでは、Cisco IP Phone 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 Phone 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。ロケールインストーラ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 Phone に使用できるようにします。

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、http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245 にアクセスし、お使いの電話機モデルに移動して、Unified Communications Manager Endpoints Locale Installer リンクを選択します。

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。

（注） 最新のロケール インストーラ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。