Cisco Unified Communications Manager リリース 11.5(1)SU1 システム設定ガイド

初版：2016 年 08 月 19 日

最終更新：2017 年 11 月 30 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。

目 次

システム設定の概要 1

システムの設定について 1

構成ツールの概要 1

Cisco Unified CM の管理 1

[Cisco Unified CM の管理（Cisco Unified CM Administration）] へのログイン 2

Cisco Unified Communications Manager Serviceability 3

Cisco Unified Communications Manager Serviceability にログイン 3

システム設定のハイレベルなフロー 4

システムの初期パラメータを設定 7

初期設定の概要 9

初期設定について 9

初期設定タスク フロー 9

システム ライセンスの設定 11

システム ライセンスの概要 11

Cisco Prime License Manager 12

システム ライセンスの前提条件 12

システム ライセンス設定のタスク フロー 13

Cisco Prime License Manager へのクラスタの統合 13

クラスタの同期 15

ライセンス計画の作成 15

ライセンス ファイルのインストール 16

ライセンス連携動作と制限事項 18

システム ライセンスの連携動作 18

システム ライセンスの制限事項 19

サーバ情報の設定 21

システム情報の概要 21

サーバ設定のタスク フロー 21

サーバ情報の設定 22
ポートの設定 22
ポート設定 23
ホスト名の設定 24
システムとエンタープライズ パラメータを設定 27
初期システムおよびエンタープライズ パラメータの概要 27
システムとエンタープライズの初期設定タスク フロー 28
初期システム パラメータとエンタープライズ パラメータの設定 28
システムおよびエンタープライズの初期設定 31
iOS Cisco Jabber の SSO ログインの動作設定 36
RTMT への SSO の設定 37
サービス パラメータの設定 39
サービス パラメータの概要 39
サービス パラメータの設定タスク フロー 40
サービスのアクティブ化と非アクティブ化 40
パブリッシャ ノードの推奨サービス パラメータ 41
サブスクライバ ノードの推奨サービス パラメータ 42
ノードのサービス パラメータの設定 43
サービスおよびサービス パラメータ設定の表示 44
デバイス プールのコア設定 47
デバイス プールのコア設定の概要 47
電話用 NTP リファレンス 47
日時グループ 47
リージョン 48
Unified Communications Manager グループ 50
Device Pools 51
デバイス プールのコア設定の前提条件 51
デバイス プールのタスク フローのコア設定 51
電話用 NTP リファレンスの追加 52
日時グループの追加 53
地域の追加 54
Cisco Unified Communications Manager グループの設定 55

基本的なデバイス プールの設定 56
基本的なデバイス プール設定フィールド 57
発着信コールの有効化 59
発着信コールの概要 61
着信コールと発信コールについて 61
着信コールと発信コールの設定 61
ゲートウェイの設定 63
ゲートウェイの概要 63
ポートとトランクの接続のタイプ 64
ゲートウェイ設定の前提条件 66
ゲートウェイの設定タスク フロー 67
MGCP ゲートウェイを設定 68
MGCP（IOS）ゲートウェイの設定 69
FXS ポートの設定 70
FXO ポートの設定 71
MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定 73
MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加 73
デジタル アクセス PRI ポートの設定 75
BRI ポートの設定 76
ゲートウェイのリセット 77
SCCP ゲートウェイの設定 78
SIP ゲートウェイの設定 79
SIP プロファイルの設定 80
SIP トランク セキュリティ プロファイルの設定 80
SIP ゲートウェイに対する SIP トランクの設定 81
H.323 ゲートウェイの設定 82
ゲートウェイに対するクラスタ全体のコール分類の設定 83
OffNet ゲートウェイ転送のブロック 83
SIP の正規化および透明性の設定 85
SIP の正規化および透明性の概要 85
SIP の正規化と透明性のデフォルト スクリプト 86
SIP の正規化および透明性の前提条件 86

SIP の正規化および透明性設定のタスク フロー 87
新しい SIP の正規化および透明性透明性スクリプトの作成 87
SIP トランクに正規化または透明性スクリプトを適用 88
正規化または透明性スクリプトの SIP 回線への適用 89
SDP 透明性プロファイルの設定 91
SDP 透明性プロファイルの概要 91
SDPの透明性プロファイルの制限事項 92
SDP 透明性プロファイルの前提条件 92
SDP 透明性プロファイルの設定 92
SIP プロファイルの設定 95
SIP プロファイルの概要 95
SIP プロファイルの設定 96
デュアル スタックの IPv6 の設定 97
デュアル スタック アドレッシングの概要 97
デュアル スタック IPv6 の前提条件 98
デュアル スタック IPv6 設定のタスク フロー 98
オペレーティング システムでの IPv6 の設定 99
IPv6 のサーバの設定 100
IPv6 の有効化 100
IP アドレッシングの優先順位の設定 101
クラスタの IP アドレッシングの設定 101
デバイス用 IP アドレッシング モードの優先順位の設定 102
サービスの再起動 103
SIP トランクの設定 105
SIP トランクの概要 105
SIP トランクのセキュリティプロファイル概要 106
SIP トランク設定の前提条件 107
SIP トランクの設定タスク フロー 107
SIP トランク セキュリティ プロファイルの設定 108
共通デバイス設定の実行 109
SIP トランクの設定 110
H.323 トランクの設定 113

H.323 トランクの概要 113
H.323 トランクの前提条件 114
H.323 トランクの設定 114
SRST の設定 117
Survivable Remote Site Telephony の概要 117
Survivable Remote Site Telephony の設定タスク フロー 118
SRST リファレンスの設定 118
デバイス プールへの SRST リファレンスの割り当て 119
クラスタの接続モニタ間隔の設定 120
デバイス プールの接続モニタ間隔の設定 121
SRST ゲートウェイの SRST を有効にする 122
SRST の制限事項 123
ダイヤル プランの設定 125
ダイヤル プランの概要 127
ダイヤル プランについて 127
ダイヤル プランの前提条件 127
ダイヤル プラン設定 127
パーティションの設定 131
パーティションの概要 131
サービス クラス 131
パーティション設定のタスク フロー 133
パーティションの設定 133
パーティション名のガイドライン 135
コーリング サーチ スペースの設定 135
パーティションの連携動作と制約事項 137
パーティションの制限 137
国内番号計画のインストール 139
国内番号計画の概要 139
国内番号計画の前提条件 139
国内番号計画インストールのタスク フロー 140
COP ファイルのインストール 140
COP ファイル インストールのフィールド 141

国内の番号計画のインストール 142
CallManager サービスの再起動 142
コール ルーティングの設定 145
コール ルーティングの概要 145
コール ルーティングの前提条件 146
コール ルーティング設定のタスク フロー 146
ルート パターンの設定 147
ルート パターンのワイルドカードと特殊文字 148
ドット前の番号削除の例 151
番号プレフィックスの例 151
オンネットおよびオフネット パターンの例 151
ブロックおよびルート パターンの例 152
ルート グループの設定 152
ルート リストの設定 153
ローカル ルート グループを設定 154
ローカル ルート グループ名の設定 155
ローカル ルート グループとデバイス プールの関連付け 156
ルート リストへのローカル ルート グループの追加 156
ルート フィルタの設定 157
ルート フィルタ タグ 158
ルート フィルタの演算子 160
ルート フィルタの例 161
時間帯ルーティングの設定 161
時間帯の設定 162
タイム スケジュールの設定 162
パーティションとスケジュールの関連付け 163
ハント パイロットの設定 165
ハント パイロットの概要 165
ハント パイロットの設定タスク フロー 166
回線グループの設定 166
ハント リストの設定 167
ハント パイロットの設定 167

ハント パイロットのワイルドカードと特殊文字 168
ハント パイロットのパフォーマンスと拡張性 171
トランスレーション パターンの設定 173
トランスレーション パターンの概要 173
トランスレーション パターンの前提条件 173
トランスレーション パターンの設定タスク フロー 174
トランスレーション パターンの設定 174
トランスフォーメーション パターンの設定 175
変換パターンの概要 175
トランスフォーメーション パターンの設定タスク フロー 175
発信側トランスフォーメーション パターンの設定 176
着信側トランスフォーメーション パターンの設定 177
トランスフォーメーション プロファイルの設定 177
ダイヤル ルールの設定 179
ダイヤル ルールの概要 179
ダイヤル ルールの前提条件 179
ダイヤル ルールの設定タスク フロー 180
アプリケーション ダイヤル ルールの設定 180
ディレクトリ検索ダイヤル ルールの設定 181
SIP ダイヤル ルールの設定 182
パターン形式 183
SIP ダイヤル ルールの設定 183
SIP ダイヤル ルールのリセット 184
SIP ダイヤル ルール設定と SIP 電話機の同期 185
ダイヤル ルールの再優先順位付け 186
ダイヤル ルールの連携動作と制約事項 187
SIP ダイヤル ルール連携動作 187
ディレクトリ検索ダイヤル ルールの制限 187
クラスタ間ルックアップ サービスの設定 189
クラスタ間検索サービスの概要 189
ハブ クラスタ 189
スポーク クラスタ 190

グローバル ダイヤル プランのインポート カタログ 190
ILS の前提条件 190
ILS 設定のタスク フロー 190
クラスタ間検索サービスの有効化 191
クラスタ ID の設定 192
リモート クラスタの設定 193
ハブ クラスタでの ILS のアクティブ化 194
スポーク クラスタでの ILS 有効化 194
クラスタ間の TLS 認証の有効化 195
クラスタ間のパスワード認証を有効にする 196
クラスタ間の TLS パスワード認証の有効化 197
グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする 198
ILS ネットワークへのカタログのインポート 198
ILS の連携動作と制限事項 200
ILS の連携動作 200
ILS の制限事項 201
ILS のトラブルシューティング 202
グローバル ダイヤル プラン レプリケーションの設定 205
グローバル ダイヤル プラン レプリケーションの概要 205
グローバル ダイヤル プラン レプリケーションの前提条件 208
グローバル ダイヤル プラン レプリケーションのタスクフロー 208
グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする 209
代替番号の設定 210
代替番号のアドバタイズ パターンの設定 211
PSTN フェールオーバーの設定 212
ルート パーティションの割り当て 213
学習パターンのブロック 214
学習されたデータに対するデータベース制限の設定 215
グローバル ダイヤル プランのデータをインポート 216
URI ダイヤリングの設定 219

URI ダイヤリングの概要 219
ディレクトリ URI 形式 219
URI ダイヤリングの前提条件 220
URI ダイヤリング設定のタスク フロー 221
ユーザへのディレクトリ URI の割り当て 222
電話番号とディレクトリ URI の関連付け 222
デフォルト ディレクトリ URI パーティションの割り当て 223
URI ダイヤルの SIP プロファイルの設定 224
URI ダイヤルの SIP トランクの設定 225
SIP ルート パターンの設定 226
ディレクトリ URI カタログのインポート 227
コール アドミッション制御の設定 229
コール アドミッション制御の概要 231
コール アドミッション制御について 231
コール アドミッション制御の構成 231
拡張ロケーション コール アドミッション制御の設定 233
拡張ロケーション コール アドミッション制御の概要 233
ネットワーク モデリング 233
Location Bandwidth Manager; ロケーション帯域幅マネージャ 234
クラスタ間の拡張ロケーション コール アドミッション制御 234
拡張ロケーション コール アドミッション制御の前提条件 235
拡張ロケーション コール アドミッション制御のタスク フロー 235
LBM サービスのアクティブ化 236
LBM グループの作成 237
場所と場所リンクの設定 238
内部ロケーションの帯域幅の割り当て 238
外部通信の確立 239
拡張ロケーションのコール アドミッション制御向け SIP クラスタ間トランクの設定 240
ビデオ コール用音声プールからオーディオ帯域幅を除外する 241
拡張ロケーション コール アドミッション制御の連携動作と制限事項 241
拡張ロケーション コール アドミッション制御 241

拡張ロケーション コール アドミッション制御の制限 242
Resource Reservation Protocol（RSVP）の設定 243
RSVP コール アドミッション制御の概要 243
RSVP コール アドミッション制御の前提条件 243
RSVP 設定のタスク フロー 244
クラスタ全体のデフォルトの RSVP ポリシーの設定 245
ロケーション ペア RSVP ポリシーの設定 245
RSVP の再試行の設定 246
通話中の RSVP エラー処理の設定 247
MLPP から RSVP へのプライオリティ マッピングの設定 248
アプリケーション ID の設定 249
DSCP マーキングの設定 250
エンド ユーザの設定 251
エンド ユーザの設定の概要 253
エンド ユーザの設定について 253
End User Configuration 253
ユーザ アクセスの設定 257
ユーザ アクセスの概要 257
ロールの概要 258
アクセス コントロール グループの概要 259
ユーザ ランクの概要 259
ユーザ アクセスの前提条件 260
ユーザ アクセス設定のタスク フロー 260
カスタム ユーザ ランクの作成 261
カスタム ロールの作成 261
既存のロールのコピー 263
アクセス コントロール グループの作成 264
アクセス コントロール グループのコピー 264
アクセス コントロール グループへの権限の割り当て 265
重複する権限ポリシーの設定 266
標準権限とアクセス コントロール グループ 267
クレデンシャル ポリシーの設定 277

クレデンシャル ポリシーの概要 277
クレデンシャル ポリシーの設定タスク フロー 278
クレデンシャル ポリシーの設定 279
クレデンシャル ポリシーのデフォルト クレデンシャルの設定 279
ユーザ プロファイルの設定 281
ユーザ プロファイルの概要 281
ユーザ プロファイルの前提条件 282
ユーザ プロファイルの設定タスク フロー 282
ユニバーサル回線テンプレートの設定 282
ユニバーサル デバイス テンプレートの設定 283
ユーザ プロファイルの設定 284
サービス プロファイルの設定 285
サービス プロファイルの概要 285
サービス プロファイルの設定タスク フロー 286
ボイスメール サービスの追加 286
メールストア サービスの追加 287
会議サービスの追加 288
ディレクトリ サービスの追加 289
IM and Presence サービスの追加 290
CTI サービスの追加 291
ビデオ会議のスケジューリング サービスの追加 292
サービス プロファイルの設定 293
機能グループ テンプレートの設定 295
機能グループ テンプレートの概要 295
機能グループ テンプレートの前提条件 296
機能グループ テンプレートの設定 296
LDAP ディレクトリからユーザをインポート 297
LDAP 同期の概要 297
[エンドユーザ用LDAP認証（LDAP Authentication for End Users）] 298
Cisco Mobile およびリモート アクセス クライアントとエンドポイントのディレクトリ サーバ ユーザ検索 298
LDAP 同期の前提条件 299

LDAP 同期設定のタスク フロー 300
Cisco DirSync サービスの有効化 301
LDAP ディレクトリの同期化の有効化 302
LDAP フィルタの作成 302
LDAP ディレクトリの同期の設定 303
エンタープライズ ディレクトリ ユーザ検索の設定 305
ディレクトリ サーバの UDS 検索用の LDAP 属性 306
LDAP 認証の設定 307
LDAP アグリーメント サービス パラメータのカスタマイズ 308
LDAP ディレクトリ サービスのパラメータ 309
LDAP同期済みユーザのローカル ユーザへの変換 310
アクセス コントロール グループへの LDAP 同期ユーザの割り当て 310
手動によるエンドユーザのプロビジョニング 313
エンド ユーザの手動プロビジョニングの概要 313
エンドユーザの手動プロビジョニングの前提条件 313
一括管理を使用したエンド ユーザのインポート 314
手動エンドユーザ設定のタスク フロー 314
新規エンド ユーザの追加 315
アクセス コントロール グループへのエンド ユーザの割り当て 315
エンドユーザへのクレデンシャル ポリシーの適用 316
ローカル エンドユーザへの機能グループ テンプレートの割り当て 316
エンドポイント デバイスの設定 319
エンドポイント デバイスの概要 321
エンドポイント デバイス設定について 321
エンドポイント デバイス設定 321
アナログ電話アダプタの設定 323
アナログ電話アダプタの概要 323
アナログ電話アダプタの設定 324
アナログ電話アダプタ 186 設定フィールド 324
アナログ電話アダプタ 187 設定フィールド 332
アナログ電話アダプタ 190 設定フィールド 347
ソフトウェアベースのエンドポイントの設定 363

ソフトウェアベースのエンドポイントの設定 363
CTI ポートの設定 363
CTI Port Settings 364
H.323 クライアントを設定 374
H.323 クライアントの設定 375
Cisco IP Communicator の設定 375
Cisco IP Phone の設定 377
Cisco IP Phone の概要 377
Cisco IP Phone の設定タスク フロー 378
電話の設定 379
SIP 電話のセキュア ポートの設定 380
サービスの再起動 380
SIP プロファイルの設定 381
電話セキュリティ プロファイルの設定 382
電話の設定 383
Cisco Unified IP Phoneサービスの設定 384
EnergyWise の設定 385
EnergyWise の設定フィールド 386
クライアント サービス フレームワーク デバイスの設定 387
クライアント サービス フレームワーク デバイスの追加 388
クライアント サービス フレームワーク デバイスの設定フィールド 389
エンドユーザとデバイスの関連付け 390
CTI リモート デバイスの設定 390
CTI リモート デバイスの設定 391
CTI リモート デバイス設定フィールド 391
デバイスへの電話番号の追加 395
リモート接続先の設定 396
リモート接続先の設定フィールド 397
Cisco Spark リモート デバイスの設定 398
Cisco Spark リモート デバイスの設定 398
Cisco Spark リモート デバイス設定フィールド 398
Cisco Spark デバイスへの電話番号の追加 403

電話データを移行 404
電話テンプレートの作成 404
電話データを移行 405
Cisco Unified IP Phone の診断とレポートの設定 407
診断およびレポートの概要 407
コール診断の概要 407
品質レポート ツールの概要 408
前提条件 408
コール診断の前提条件 408
Quality Report Tool の前提条件 409
診断およびレポート設定タスク フロー 410
コール診断の設定 411
品質レポート ツールの設定 411
QRT ソフトキーのソフトキー テンプレートの設定 412
QRT ソフトキー テンプレートと共通デバイス設定の関連付け 414
共通デバイス設定への QRT ソフトキー テンプレートの追加 414
電話機と共通デバイス設定の関連付け 415
電話機への QRT ソフトキー テンプレートの追加 416
Cisco Unified Serviceability での QRT の設定 416
Cisco Extended Functions サービスの有効化 417
アラームの設定 417
トレースの設定 418
品質レポート ツールのサービス パラメータの設定 420
品質レポート ツールのサービス パラメータ 420
サードパーティ製 SIP 電話の設定 423
サードパーティ製 SIP エンドポイントの概要 423
サードパーティ製 SIP エンドポイント設定のタスク フロー 424
ダイジェスト ユーザの設定 425
SIP プロファイルの設定 425
電話セキュリティ プロファイルの設定 426
サードパーティ SIP エンドポイントの追加 427
エンドユーザとデバイスの関連付け 428

サードパーティのインタラクションと制限事項 429
サードパーティの制限事項 429
サービス プロファイルとテンプレート 431
デバイス プロファイルとテンプレートの概要 431
デバイス プロファイル 431
エンドポイントの SIP プロファイル 431
サービス プロファイルとテンプレート 431
ピアツーピア イメージの分配 432
デバイス プロファイルとテンプレートの設定タスク フロー 432
デフォルト デバイス プロファイルでのソフトキー テンプレートの設定 434
共通デバイス設定とソフトキー テンプレートの関連付け 435
共通デバイス設定へのソフトキー テンプレートの追加 435
電話機と共通デバイス設定の関連付け 436
電話機とソフトキー テンプレートの関連付け 437
機能管理ポリシーの設定 437
電話機能一覧の生成 438
機能管理ポリシーの作成 438
電話への機能管理ポリシーの適用 440
共通の電話プロファイルへの機能管理ポリシーの適用 440
すべての電話への機能管理ポリシーの適用 441
電話ボタン テンプレートの設定 441
電話機とボタン テンプレートの関連付け 442
デバイス プロファイルの設定 443
エンドポイントの SIP プロファイルの設定 444
デフォルトのデバイス プロファイルの設定 444
電話のピアツーピア イメージの配信機能の設定 445
ユーザとエンドポイントの関連付け 447
ユーザとエンドポイントの関連付けの概要 447
ユーザとエンドポイントの関連付けに関する前提条件 447
ユーザおよびデバイス設定のタスク フロー 447
エンド ユーザとデバイスの関連付け 448
エンド ユーザおよびデバイス構成時の設定 449

アプリケーション ユーザとデバイスの関連付け 451
ユーザとエンドポイントの関連付けに関する連携動作と制約事項 452
ユーザとエンドポイントの関連付けに関する連携動作 452
ユーザとエンドポイントの関連付けに関する制約事項 453
アプリケーションの統合 455
アプリケーションの統合の概要 457
アプリケーションの統合 457
アプリケーションの統合 457
アプリケーション サーバの設定 461
アプリケーション サーバの概要 461
アプリケーション サーバの前提条件 461
アプリケーション サーバのタスク フロー 461
アプリケーション サーバの設定 462
Cisco WebDialer サーバの設定 463
プラグインのインストール 465
プラグインの概要 465
プラグインのインストールのタスク フロー 466
プラグインのダウンロード 466
プラグイン URL の更新 467
プレゼンス冗長グループの設定 469
プレゼンス冗長グループの概要 469
高可用性 470
プレゼンス冗長グループの前提条件 470
プレゼンス冗長グループのタスク フロー 470
データベース レプリケーションの確認 471
確認サービス 472
プレゼンス冗長グループの設定 473
障害検出パラメータの設定 474
高可用性を有効にする 475
ユーザ割り当てモードの設定 475
冗長性の連携動作と制約事項 476
ボイスメールおよびメッセージング向けの Cisco Unity Connection の設定 477

Cisco Unity Connection 477
Cisco Unity Connection のボイスメールとメッセージング設定タスク フロー 479
PIN 同期の有効化 479
Cisco Unified Contact Center Enterprise の設定 481
Cisco Unified Contact Center Enterprise 481
Cisco Unified Contact Center Express の設定 483
Cisco Unified Contact Center Express 483
CTI アプリケーションの設定 485
CTI アプリケーションの概要 485
CTI ルート ポイントの概要 486
Cisco Unified Communications Manager の CTI 冗長性 486
CTIManager の CTI 冗長性 487
アプリケーションの障害に対する CTI の冗長性 487
CTI アプリケーションの前提条件 487
CTI アプリケーションの設定タスク フロー 487
CTIManager サービスの有効化 489
CTIManager および Cisco Unified Communications Manager のサービス パラメータの設定 489
CTI ルート ポイントの設定タスク フロー 490
CTI ルート ポイントの設定 491
新しいコール受け入れタイマーの設定 491
アクティブな多重同時コールの設定 492
CTI ルート ポイントの同期 493
CTI デバイスの電話番号の設定 493
デバイスとグループの関連付け 494
エンド ユーザとアプリケーション ユーザの追加 494
アクセス コントロール グループの設定オプション 495
アプリケーション障害時の CTI 冗長性の設定 496
Cisco TelePresence の設定 499
Cisco TelePresence 499
Cisco TelePresence Conductor 499
Cisco TelePresence 会議ブリッジ 499
Cisco TelePresence Video Communication Server 500

Cisco Jabber の設定 501
Cisco Jabber の設定 501
Cisco Jabber のインタラクションと制限事項 502
メディア リソースの設定 503
メディア リソースの概要 505
メディア リソースについて 505
メディア リソースの設定 505
メディア リソースの定義 507
メディア リソース グループの概要 507
[メディアリソースグループリスト（Media Resource Group List）] 508
メディア リソース グループの前提条件 508
メディア リソース グループのタスク フロー 508
メディア リソース グループの設定 509
メディア リソース グループへのデバイスの割り当て 510
メディア リソース グループ リストの作成 510
メディア リソース グループ リストへのメディア リソース グループの割り当て 511
デバイスまたはデバイス プールへのメディア リソース グループ リストの割り当て 512
メディア リソース冗長性の設定 513
メディア リソース グループの連携動作と制約事項 513
メディア リソース グループの連携動作 513
メディア リソース グループの制約事項 514
トラステッド リレー ポイントの設定 515
トラステッド リレー ポイントの概要 515
トラステッド リレー ポイントのタスク フロー 516
デバイスのトラステッド リレー ポイントの設定 516
メディア ターミネーション ポイントのトラステッド リレー ポイントの設定 517
トランスコーダに対するトラステッド リレー ポイントの設定 518
トラステッド リレー ポイントのサービス パラメータの有効化 519

MTP および TRP サービス パラメータを選択したときのコール ステータス 520
MTP と TRP サービス パラメータが選択されない場合のコール ステータス 521
トラステッド リレー ポイントの連携動作と制約事項 521
トラステッド リレー ポイントの連携動作 521
トラステッド リレー ポイントの制限事項 522
アナンシエータの設定 525
アナンシエータの概要 525
デフォルトのアナウンスとトーン 526
会議ブリッジでのアナンシエータの使用 528
アナンシエータ設定タスク フロー 528
アナンシエータのアクティブ化 529
メディア ストリームのデフォルトの番号の変更 530
アナンシエータのセキュリティ モードを上書き 531
アナンシエータがあるメディア リソース グループ リストを表示 532
会議ブリッジのアナンシエータの設定 532
自動音声応答の設定 535
自動音声応答の概要 535
デフォルトのアナウンスとトーン 535
自動音声応答の制限 537
自動音声応答の設定のタスク フロー 537
自動音声応答装置のアクティブ化 538
IVR を保持するメディア リソース グループのリストの表示 538
IVR 設定 539
IVR パラメータの変更 541
Video On Hold サーバの設定 543
保留中ビデオの概要 543
保留ビデオ設定のタスク フロー 544
Cisco MediaSense サーバへの SIP トランクの作成 544
保留ビデオ サーバの設定 545
保留中ビデオの制限事項 546

アナウンスの設定 547
アナウンス設定の概要 547
デフォルトのアナウンス 547
アナウンスの設定タスク フロー 548
アナウンスの設定 549
カスタマイズされたアナウンスのアップロード 550
会議ブリッジの設定 553
会議ブリッジの概要 553
会議ブリッジ タイプ 553
コール保持 558
コール保持のシナリオ 559
会議ブリッジの設定タスク フロー 561
会議ブリッジの設定 561
会議ブリッジのサービス パラメータの設定 561
フレキシブル DSCP マーキングおよびビデオ プロモーションの設定 563
フレキシブル DSCP マーキングおよびビデオ プロモーションの概要 563
ユーザに対するカスタム QoS の設定 564
トラフィック クラスのラベル 565
DSCP の設定構成のタスク フロー 565
フレキシブル DSCP マーキングおよびビデオ プロモーション ポリシーの設定 566
フレキシブル DSCP マーキングおよびビデオ プロモーション サービス パラメータ 567
ユーザのカスタム QoS ポリシーの設定 568
SIP プロファイルのカスタム QoS の設定 569
電話機へのカスタム QoS ポリシーの適用 570
フレキシブル DSCP マーキングおよびビデオ プロモーションのインタラクションと制約事項 571
フレキシブル DSCP マーキングおよびビデオ プロモーションの連携動作 571
フレキシブル DSCP マーキングおよびビデオ プロモーションの制約事項 571
トランスコーダおよびメディア ターミネーション ポイントの設定 573
トランスコーダとメディア ターミネーション ポイントの概要 573

トランスコーダ 573
トランスコーダおよびメディア リソース マネージャ 574
メディア ターミネーション ポイントとしてのトランスコーダ 574
トランスコーダ タイプ 574
トランスコーダのフェールオーバーおよびフォールバック 577
メディア ターミネーション ポイント 577
MTP フェールオーバーおよびフォールバック 578
ソフトウェア メディア ターミネーション ポイントの種類 578
トランスコーダと MTP 設定のタスク フロー 579
トランスコーダの設定 579
トランスコーダの追加 580
メディア リソース グループへのトランスコーダの追加 580
トランスコーダの同期 581
ソフトウェア MTP の設定 582
ソフトウェア MTP の追加 582
メディア リソース グループへのソフトウェア MTP の追加 583
トランスコーダと MTP の連携動作と制約事項 584
トランスコーダの制限 584
メディア ターミネーション ポイントの制限 585
登録デバイス 587
登録デバイスの概要 589
デバイスの登録について 589
デバイスの登録 589
TFTP サーバの設定 591
プロキシ TFTP 導入の概要 591
冗長とピア プロキシ TFTP サーバ 591
IPv4 および IPv6 デバイスの TFTP サポート 592
TFTP 導入でのエンドポイントと設定ファイル 592
TFTP のセキュリティに関する考慮事項 593
TFTP サーバの設定タスク フロー 593
TFTP サーバの動的設定 594
TFTP サーバの手動設定 595

TFTP サーバ ピア関係を追加 596
TFTP サーバの CTL ファイルの更新 597
TFTP サーバの非設定ファイルの変更 597
TFTP サービスの停止および開始 598
デバイスのデフォルトの更新 601
デバイスのデフォルトの概要 601
デバイスのデフォルトの更新タスク フロー 601
デバイスのデフォルト設定の更新 602
デバイスのデフォルト設定 603
自動登録の設定 605
自動登録の概要 605
自動登録の設定タスク フロー 606
自動登録用パーティションの設定 607
自動登録用コーリング サーチ スペースの設定 608
自動登録のデバイス プールの設定 609
自動登録のデバイス プロトコル タイプの設定 610
自動登録を有効にする 610
自動登録の無効化 613
再利用の自動登録の数 613
電話機の手動登録 615
電話の手動登録の概要 615
手動によるデバイス登録タスク フロー 615
システムへの電話機の手動での追加 616
電話機に対する電話番号の手動設定 616
セルフプロビジョニングの設定 619
セルフプロビジョニングの概要 619
セルフプロビジョニングの前提条件 620
セルフプロビジョニングの設定タスク フロー 621
セルフプロビジョニングのサービスの有効化 621
セルフプロビジョニング用自動登録の有効化 622
CTI ルート ポイントの設定 623
CTI ルート ポイントへの電話番号の割り当て 623

セルフプロビジョニング用アプリケーション ユーザの設定 624

システムのセルフプロビジョニング設定 625

応用的なコール処理の設定 627

応用的なコール処理の概要 629

応用的なコール処理について 629

応用的なコール処理の設定 629

APIC-EM コントローラによる QoS の設定 633

APIC-EM コントローラの概要 633

APIC-EM コントローラの前提条件 634

APIC-EM コントローラ設定タスク フロー 634

APIC-EM コントローラの設定 635

APIC-EM コントローラ証明書のアップロード 636

APIC-EM コントローラへの HTTPS 接続の設定 637

システム向けに外部の QoS サービスを有効にする 637

SIP プロファイル レベルの外部 QoS サービスの設定 638

電話機への SIP プロファイルの割り当て 639

コール制御検出の設定 641

コール制御検出の概要 641

コール制御検出の前提条件 641

コール制御検出の設定タスク フロー 642

SAF セキュリティ プロファイルの設定 644

SAF フォワーダの設定 644

SIP トランクと H.323 クラスタ間トランクの設定 645

ホスト DN グループの設定 646

ホスト DN パターンの設定 646

アドバタイジング サービスの設定 647

コール制御検出のパーティションの設定 648

要求サービスの設定 648

学習パターンのブロック 649

コール制御検出の連携動作と制限事項 650

コール制御検出の連携動作 650

コール制御検出の制限 652

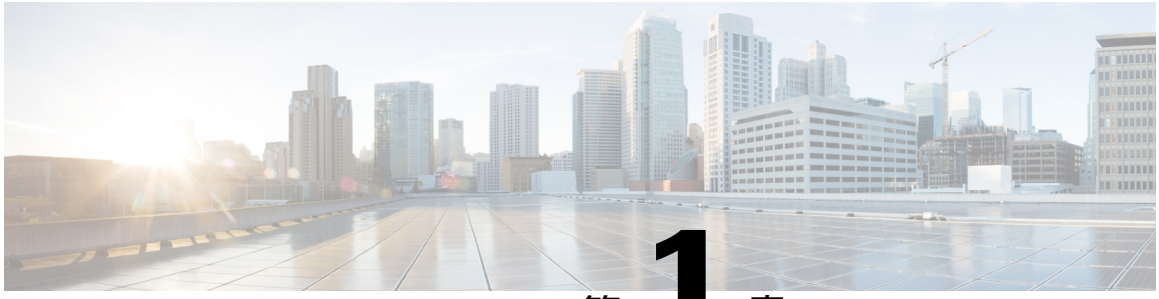
外部コール制御の設定 653
外部コール制御の概要 653
外部コール制御の前提条件 654
外部コール制御の設定タスク フロー 654
外部コール制御用コーリング サーチ スペースの設定 655
外部コール制御プロファイルの設定 656
トランスレーション パターンへのプロファイルの割り当て 657
ルーティング サーバの証明書のトラステッド ストアへのインポート 658
自己署名証明書をルーティング サーバにエクスポートする 659
監察機能の設定 659
カスタマイズされたアナウンスの設定 661
外部コール制御の連携動作と制限事項 662
外部コール制御の連携動作 662
外線コール制御の制限事項 664
コール キューイングの設定 667
コール キューイングの概要 667
コール キューイングの前提条件 669
コール キューイング タスク フロー 669
アナウンスの設定 669
保留音の設定 670
保留音のオーディオ ソース フィールド 671
ハント パイロット キューイングの設定 676
無応答時のハント メンバーの自動ログアウト 678
コール キューイングの連携動作と制限 679
コール キューイングの連携動作 679
コール キューイングの制約事項 680
コール キューイングが有効なハント パイロットのパフォーマンスと拡張性 681
コール スロットリングの設定 683
コール スロットリングの概要 683
コール スロットリングの設定 684
コール スロットリング サービス パラメータ 684

発信側の正規化 687
発信側の正規化の概要 687
発信側の正規化の前提条件 688
発信側の正規化の設定タスク フロー 689
発信側番号のグローバル化 690
コーリング サーチ スペースの設定 691
発信側トランスフォーメーション パターンの作成 691
コーリング サーチ スペースへの発信側トランスフォーメーション パターンの適用 692
発信側の正規化サービス パラメータの例 693
発信側の正規化の連携動作と制約事項 694
発信側の正規化の連携動作 694
発信側の正規化の制約事項 697
論理パーティション分割の設定 699
論理パーティション分割の概要 699
論理パーティション設定タスク フロー 699
Enable Logical Partitioning 701
地理位置情報の設定 701
地理位置情報の定義 702
地理位置情報の割り当て 702
デフォルトの地理位置情報の設定 703
論理パーティション分割のデフォルト ポリシーの設定 704
論理パーティショニング チェックを回避するためのデバイス設定 704
地理位置情報フィルタの設定 705
フィルタ ルールの定義 706
地理位置情報フィルタの割り当て 706
デフォルトの地理位置情報フィルタの設定 707
論理パーティション ポリシー レコードの定義 708
ロケーション伝達の有効化 708
論理的なパーティション分割の連携動作と制約事項 709
論理パーティショニングの連携動作 709
論理パーティショニングの制約事項 711

地理位置情報とロケーション伝達の設定 713
地理位置情報とロケーション伝達の概要 713
地理位置情報とロケーションの配信タスク フロー 713
地理位置情報の設定 714
地理位置情報の設定 715
地理位置情報の割り当て 715
デフォルトの地理位置情報の設定 716
ロケーション配信の設定 716
地理位置情報フィルタの設定 717
地理位置情報フィルタの設定 718
地理位置情報フィルタの割り当て 718
デフォルトの地理位置情報フィルタの設定 719
ロケーション認識の設定 721
ロケーション認識の概要 721
ワイヤレス ネットワークの更新 722
有線ネットワークの更新 723
場所の認識の前提条件 723
Location Awareness の設定タスク フロー 723
無線インフラストラクチャ同期のサービスの開始 724
ワイヤレス アクセス ポイント コントローラの設定 725
インフラストラクチャ デバイスの挿入 726
インフラストラクチャ デバイス トラッキングの非アクティブ化 727
関連資料 728
自動代替ルーティングの設定 729
自動代替ルーティングの概要 729
AAR 設定タスク フロー 729
クラスタ全体の AAR を有効にする 730
自動代替ルーティングの設定 730
マルチレベルの優先とプリエンプション 733
Multilevel Precedence and Preemption の概要 733
Multilevel Precedence and Preemption の前提条件 733
Multilevel Precedence and Preemption Precendence のタスク フロー 733

ドメインおよびドメイン リストの設定 736
Multilevel Precedence and Preemption ドメインの設定 737
リソース プライオリティ ネームスペース ネットワーク ドメインの設定 737
リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定 738
共通デバイス設定での Multilevel Precedence and Preemption 設定 739
Multilevel Precedence and Preemption のエンタープライズ パラメータの設定 740
Multilevel Precedence and Preemption のエンタープライズ パラメータ 741
Multilevel Precedence and Preemption のパーティションの設定 742
パーティション名のガイドライン 743
Multilevel Precedence and Preemption のコーリング サーチ スペースの設定 744
Multilevel Precedence and Preemption（MLPP）のルート パターンの設定 745
Multilevel Precedence and Preemption のルート パターン設定フィールド 746
Multilevel Precedence and Preemption のトランスレーション パターンの設定 747
ゲートウェイの Multilevel Precedence and Preemption の設定 748
電話機のMultilevel Precedence and Preemption の設定 749
電話の Multilevel Precedence and Preemption 設定 750
Multilevel Precedence and Preemption コールの電話番号の設定 752
Multilevel Precedence and Preemption のユーザ デバイス プロファイルの設定 752
Multilevel Precedence and Preemption のデフォルトのデバイス プロファイルの設定 754
Multilevel Precedence and Preemption の連携動作と制限事項 755
Multilevel Precedence and Preemption（MLPP） 755
Multilevel Precedence and Preemption の制約事項 757
参考情報 763
Cisco Unified Communications Manager での TCP および UDP ポートの使用 765
Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要 765
ポートの説明 767
Cisco Unified Communications Manager サーバがクラスタ間で使用するポート 767
共通サービス ポート 770
Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート 773

CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求 774
Cisco Unified Communications Manager から電話機への Web 要求 774
電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信 775
ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信 777
アプリケーションと Cisco Unified Communications Manager との間の通信 781
CTL クライアントとファイアウォールとの通信 783
HP サーバ上の特殊なポート 784
ポート参照 784
ファイアウォール アプリケーション インスペクション ガイド 784
IETF TCP/UDP ポート割り当てリスト 784
IP テレフォニー設定とポート使用に関するマニュアル 784
VMware ポート割り当てリスト 785
IM and Presence Service のポート使用状況の情報 787
IM and Presence サービス ポートの使用方法の概要 787
テーブルで照合する情報 788
IM and Presence サービス ポート リスト 788



第 1 章

システム設定の概要

- システムの設定について，1 ページ
- 構成ツールの概要，1 ページ
- システム設定のハイレベルなフロー，4 ページ

システムの設定について

このドキュメントには、コール制御システムを設定するために実行が必要なタスクについての情報が記載されています。タスク フロー、手順、前提条件などの情報が含まれています。

システムの計画については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.htmlを参照してください。

構成ツールの概要

このガイドの手順では、次の 2 つの構成ツールを使用する必要があります。

- Cisco Unified CM の管理
- Cisco Unified Serviceability

この章では、ツールとそれらにアクセスする方法について簡単に説明します。

Cisco Unified CM の管理

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] は、Unified Communications Manager ノードの設定を個別に手動で変更できる Web ベースのアプリケーションです。このガイドでは、このアプリケーションを使用して機能を設定する手順について説明します。

一括設定タスクを実行する必要があり、設定プロセスを自動化する場合には、Cisco Unified Communications Manager 一括管理ツール（BAT）を使用して、多数の設定変更を同時に実行できます。詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

[Cisco Unified CM の管理（Cisco Unified CM Administration）] へのログイン

次の手順を使用して、Cisco Unified Communications Manager Administration にログインします。Cisco Unified Communications Manager Administration にログインした後、ウィンドウに Cisco Unified Communications Manager の現在の状況を示すメッセージが表示されることがあります。たとえば、Cisco Unified Communications Manager で次の状況が確認されることがあります。

- Cisco Unified Communications Manager は現在、スターター（デモ）ライセンスで動作しているので、適切なライセンス ファイルをアップロードします。
- Cisco Unified Communications Manager は、現在、ライセンス数が不足している状態なので、追加のライセンス ファイルをアップロードしてください。
- Cisco Unified Communications Manager は現在、適切なソフトウェア機能のライセンスを使用していません。この状況では、Cisco CallManager サービスは停止し、適切なソフトウェア バージョンのライセンスをアップロードして Cisco CallManager サービスを再起動するまで開始しません。

次の手順でサーバを参照して、Cisco Unified Communications Manager Administration にログインします。

手順

ステップ 1 優先オペレーティング システムのブラウザを開始します。

ステップ 2 Web ブラウザのアドレス バーに、大文字と小文字を区別して次の URL を入力します。

```
https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do
```

ここで、`<Unified CM-サーバ名>` は、サーバの名前または IP アドレスと同じです。

（注） オプションで、ポート番号を指定できます。

ステップ 3 [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。適切なボタンをクリックします。

ステップ 4 [Cisco Unified Communications Manager Administration] ウィンドウで、Cisco Unified Communications Manager のインストール時に指定したユーザ名とパスワードを入力し、[ログイン（Login）] をクリックします（両方のフィールドの内容をクリアするには [リセット（Reset）] をクリックします）。

（注） セキュリティ上の理由で、無活動状態が 30 分続くと Cisco Unified Communications Manager Administration はユーザをログアウトするので、ログインしなおす必要があります。

Cisco Unified Communications Manager Serviceability

このガイドの一部の手順では、Cisco Unified Communications Manager ノードでサービスを開始または再開するために Cisco Unified Serviceability アプリケーションを使用する必要があります。

Web ベースのトラブルシューティング ツールである Cisco Unified Serviceability は次の機能を提供します。

- トラブルシューティング用にアラームとイベントを保存し、アラーム メッセージの定義を提供する。
- トレース情報を、トラブルシューティング用にログ ファイル保存します。
- Cisco Unified Real-Time Monitoring Tool（Unified RTMT）を使用して、コンポーネントの動作をリアルタイムで監視します。
- ユーザによる、またはユーザ処理の結果としてのシステムの設定変更を記録することによって、監査機能を提供します。この機能は、Cisco Unified Communications Manager および Cisco Unity Connection の情報保証機能をサポートします。
- [サービスの開始（Service Activation）] ウィンドウによりアクティブ化、非アクティブ化、および表示を行うことができる機能サービスを提供します。
- 日次レポート（警告サマリーやサーバ統計レポートなど）の生成とアーカイブ。
- Cisco Unified Communications Manager、IM and Presence Service、Cisco Unity Connection が、シンプル ネットワーク管理プロトコル（SNMP）のリモート管理およびトラブルシューティングの管理対象デバイスとして機能できるようにします。
- 1 つのノード（またはクラスタ内のすべてのノード）のログ パーティションのディスク使用をモニタします。
- システム内のスレッドとプロセスの数をモニタする。キャッシュを使用してパフォーマンスを向上させる。
- Cisco Unified Communications Manager のみ：Cisco Unified Communications Manager CDR Analysis and Reporting を使用して、サービス品質、トラフィック、請求情報の Cisco Unified Communications Manager レポートを生成します。

Cisco Unified Communications Manager Serviceability にログイン

次の手順で、Cisco Unified Serviceability にログインします。

手順

ステップ 1 優先オペレーティング システムのブラウザを開始します。

ステップ 2 Web ブラウザのアドレス バーに、大文字と小文字を区別して次の URL を入力します。

```
https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do
```

ここで、<Unified CM-サーバ名> は、サーバの名前または IP アドレスと同じです。

ステップ 3 [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。適切なボタンをクリックします。

ステップ 4 [Unified Communications Manager Administration] ウィンドウで、ナビゲーション メニューから [シスコ統合保守性（Cisco Unified Serviceability）] を選択します。

ステップ 5 Cisco Unified Communications Manager のインストール中に指定したユーザ名とパスワードを入力し、[ログイン（Login）] をクリックします。

（注） セキュリティ目的で、30 分間無活動状態が続くとログアウトされ、ログインし直す必要があります。

システム設定のハイレベルなフロー

次の順序でシステム設定を実行します。この手順は、共通システムコンポーネントグループの設定に関するセクションとリンクしています。

手順

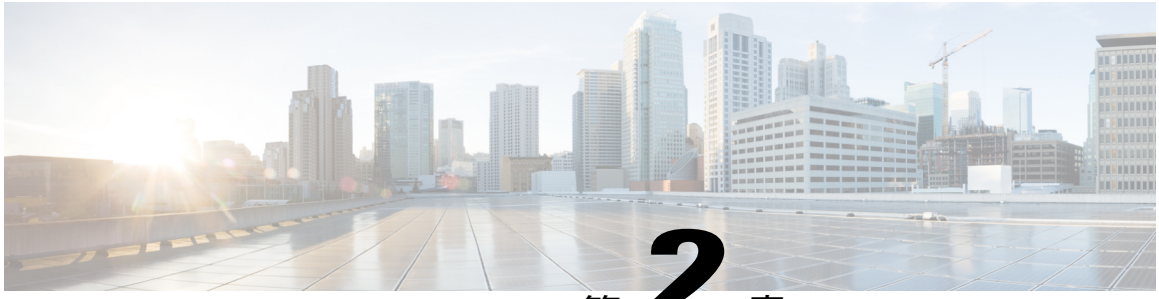
	コマンドまたはアクション	目的
ステップ 1	初期設定タスク フロー, （9 ページ）	ライセンス、サーバ情報、デバイスプール、ポート設定などのシステムの初期パラメータを設定するには、ガイドのこの部分の設定を実行します。
ステップ 2	着信コールと発信コールの設定, （61 ページ）	ゲートウェイおよび存続可能なリモートテレフォニーシステムを設定するには、ガイドのこの部分の設定を実行します。
ステップ 3	ダイヤル プラン設定, （127 ページ）	ルート プラン、ハント パイロット変換、URI ダイヤルなどのダイヤルプラン要素を設定するには、ガイドのこの部分の設定を実行します。
ステップ 4	コール アドミッション制御の構成, （231 ページ）	コールアドミッション制御を設定するには、ガイドのこの部分の設定を実行します。
ステップ 5	End User Configuration, （253 ページ）	役割やアクセスコントロールグループを設定したり、エンドユーザとそのプロファイルを設定するには、ガイドのこの部分の設定を実行します。
ステップ 6	エンドポイント デバイス設定, （321 ページ）	アナログ電話アダプタ（ATA）、Cisco IP Phone、サードパーティ製 SIP 電話機、ソフトウェアベースのエンドポイントなどのエンドポイントデバイスを設定するには、ガイドのこの部分の設定を実行します。ここでは、エンドポイントデバイスのテンプレートおよびプ

	コマンドまたはアクション	目的
		ロファイルの設定方法や Cisco IP Phone の診断およびレポートを有効にする方法についても説明します。
ステップ 7	アプリケーションの統合, （457 ページ）	CTI アプリケーション、Cisco Unity Connection、Cisco IM and Presence サービス、Unified Contact Center Enterprise および Express、Cisco TelePresence などのその他のアプリケーションと連動するように Cisco Unified Communications Manager を設定するには、ガイドのこの部分の設定を実行します。
ステップ 8	メディア リソースの設定, （505 ページ）	音声およびビデオリソース、アナンシエータ、トランスコーダ、メディア ターミネーション ポイント、および会議ブリッジを設定するには、ガイドのこの部分の設定を実行します。
ステップ 9	デバイスの登録, （589 ページ）	エンドポイントデバイスを自動または手動で登録するには、ガイドのこの部分の設定を実行します。
ステップ 10	応用的なコール処理の設定, （629 ページ）	コールをアドバタイズする方法、キューに入れる方法、抑制する方法など、コール制御を設定するには、ガイドのこの部分の設定を実行します。ここでは、論理パーティショニング、発信側の正規化、地理位置情報の伝達、自動代替ルーティング（AAR）、および Multilevel Precedence and Preemption（MLPP）の設定方法についても説明します。
ステップ 11	Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要, （765 ページ）IM and Presence サービス ポートの使用方法の概要, （787 ページ）	ガイドのこの部分では、Cisco Unified Communications Manager と IM and Presence サービスでクラスタ内接続や外部アプリケーションまたは外部デバイスとの通信に使用されるポートについて説明します。

第 I 部

システムの初期パラメータを設定

- 初期設定の概要，9 ページ
- システム ライセンスの設定，11 ページ
- サーバ情報の設定，21 ページ
- システムとエンタープライズ パラメータを設定，27 ページ
- サービス パラメータの設定，39 ページ
- デバイス プールのコア設定，47 ページ



第 2 章

初期設定の概要

- 初期設定について，9 ページ
- 初期設定タスク フロー，9 ページ

初期設定について

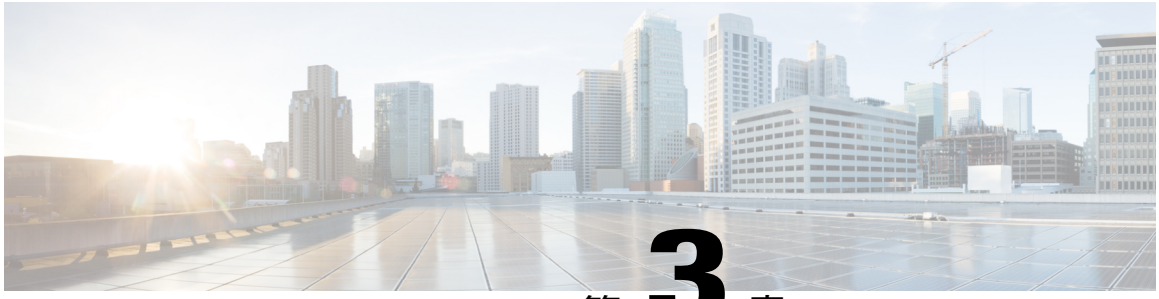
このセクションの章では、コール制御システムを設定する前に、完了する必要がある初期設定タスクについて説明します。

初期設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	システム ライセンス設定のタスク フロー，（13 ページ）	システムのライセンス要件を管理します。
ステップ 2	サーバ設定のタスク フロー，（21 ページ）	サーバ名やポートの設定などの、基本サーバ情報を設定します。
ステップ 3	システムとエンタープライズの初期設定タスク フロー，（28 ページ）	ノードを初めて設定する際に必要なシステム全体のパラメータを設定します。
ステップ 4	サービス パラメータの設定タスク フロー，（40 ページ）	ノードを初めて設定する際に必要なサービス パラメータを設定します。
ステップ 5	デバイス プールのタスク フローのコア設定，（51 ページ）	サーバ グループ、タイムゾーン情報、領域（コーデックの選択）などのコア システムを設定します。これらの設定は基本的で、基本的なデバイス プールの基盤になります。

	コマンドまたはアクション	目的



第 3 章

システム ライセンスの設定

- システム ライセンスの概要，11 ページ
- システム ライセンスの前提条件，12 ページ
- システム ライセンス設定のタスク フロー，13 ページ
- ライセンス連携動作と制限事項，18 ページ

システム ライセンスの概要

システムでは一元化されたライセンス管理が使用されるため、ライセンスの使用は、デバイスベースのライセンスからユーザベースのライセンスに移行します。このユーザ中心のモデルは、システムの全体的な要件およびユーザが実際に使用する内容（1 人のユーザと関連付けられている複数のデバイスなど）に合致します。このモデルでは、システムのライセンスは、ユーザ自体、ユーザ機能、および設定済みデバイスの総数によって決まります。

ユーザのニーズをカバーするために、次のライセンス オプションを使用できます。

Cisco Unified Workspace Licensing

Cisco Unified Workspace Licensing（UWL）は、シスコ コラボレーション アプリケーションおよびサービスの最も一般的なバンドルをコスト効率の高いシンプルなパッケージで提供します。このパッケージには、ソフト クライアント、アプリケーション サーバ ソフトウェア、およびユーザごとのライセンスが含まれています。

Cisco User Connect Licensing

個々の Cisco Unified Communications アプリケーションに対するユーザベースのライセンスで、アプリケーション サーバ ソフトウェア、ユーザ ライセンス、ソフト クライアントが含まれています。User Connect Licensing（UCL）は、必要なデバイスのタイプとデバイスの数に応じて、Essential、Basic、Enhanced、および Enhanced Plus の各バージョンから選択できます。

これらのライセンス タイプと使用可能なバージョンの詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.htmlを参照してください。

Cisco Prime License Manager

Cisco Prime License Manager は、システム内にある全 Cisco Unified Communications Managers のすべてのライセンス要件を統合して、インストールされている使用可能なライセンスの数と全要件を比較します。システムのユーザ、電話、またはその他のサービスをプロビジョニングする際にライセンス要件が計算されます。この手順の後、対応するライセンス要件が Cisco Unified Communications Manager から Cisco Prime License Manager に送信されます。その後、インストールされている使用可能なライセンスとシステムのライセンス要件が比較されて、ライセンスが適合であるか、非適合であるかの報告が返されます。データは継続的に同期され、システム ライセンスのスナップショットは最新の状態で維持されます。

システム ライセンスの前提条件

- Unified Communications （UC）のライセンス構造を理解します。http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.htmlを参照してください。
- Cisco Prime License Manager のインストール手順を実行します。この手順の詳細については、http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-license-manager/products-user-guide-list.html で『*Cisco Prime License Manager User Guide*』を参照してください。

以前のリリースからライセンスを移行する場合、次の要件を確認します。

- License Count Utility（リリース 6.x ～ 8.x まで）からレポートを実行します。このツールの使用方法については、『*Using Cisco Unified Communications Manager License Count Utility*』を参照してください。 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
- アップグレードする前に、すべての 9.x 以前のライセンスを Cisco Unified Communications Manager に適用します。
- シスコ デバイス割り当てツール を実行することでユーザとデバイスと一致させます。このツールの使用方法については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で『*User Guide for Cisco Device Assignment Tool*』を参照してください。

移行のサポートを受けるには、次のいずれかのオプションを選択します。

- 次の Web サイトでサービス要求を作成します： https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case
- licensing@cisco.com でサービス要求を作成します（Cisco.com ユーザ ID を含めます）。
- 次の Web サイトに示されている国別番号に電話をかけ、サービス要求を作成します： http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

システム ライセンス設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Prime License Manager へのクラスタの統合, （13 ページ）	Unified Communications Manager パブリッシャ ノードを製品インスタンスとして Cisco Prime ライセンス マネージャに追加します。このタスクによって、2 つのシステム間でライセンス要件と使用状況が確実に同期されます。Cisco Prime ライセンス マネージャは、24 時間ごとにシステムをポーリングします。パブリッシャ ノードを追加することで、クラスタを追加します。
ステップ 2	クラスタの同期, （15 ページ）	すべてのデバイス データをクラスタからアップロードして、ライセンス マネージャがライセンスを割り当てられるように、クラスタと Cisco Prime ライセンス マネージャを同期します。
ステップ 3	ライセンス計画の作成, （15 ページ）	システムの新しいライセンスを取得するには、ライセンスの追加ウィザードの手順に従い、ライセンス要求を準備します。
ステップ 4	ライセンスファイルのインストール, （16 ページ）	ライセンスの履行手順に従い、システムの適切なライセンスをインストールします。これらの手順によって、システムのコンプライアンスが確保されます。

Cisco Prime License Manager へのクラスタの統合

Unified Communications Manager パブリッシャ ノードを製品インスタンスとして Cisco Prime ライセンス マネージャに追加します。このタスクによって、2 つのシステム間でライセンス要件と使用状況が確実に同期されます。Cisco Prime ライセンス マネージャは、24 時間ごとにシステムをポーリングします。パブリッシャ ノードを追加することで、クラスタを追加します。

はじめる前に

追加する製品インスタンスに残りのライセンスをインストールします。このステップによりライセンスが移行に適していることを確認できます。

次のコマンドを使用してアカウントのステータスを確認します。**show accountlocking**製品インスタンスの追加時に 401 エラーが発生しないようにするには、アカウントのロック設定を **disabled** に設定する必要があります。

手順

ステップ 1 インストールが完了したら、作成したアプリケーション ユーザ名とパスワードを使用して Cisco Prime License Manager にログインします。

ステップ 2 [製品インスタンス（Product Instances）] を選択します。

ステップ 3 [追加（Add）] をクリックします。[製品の追加（Product Add）] ダイアログボックスが表示されます。

ステップ 4 次の情報を入力します。

- [名前（Name）]
- 説明（Description）（任意）
- [製品のタイプ（Product Type）]
- ホスト名/IP アドレス（Hostname/IP Address）
- [ユーザ名（Username）]
- [パスワード（Password）]

（注） クレデンシャルとは、製品の OS 管理者のユーザ名とパスワードのことです。

ステップ 5 [OK] をクリックして、製品インスタンスを追加します。

ステップ 6 製品インスタンスが追加された時点で、製品が [製品インスタンス（Product Instances）] テーブルに表示されます。

（注） [製品インスタンス（Product Instances）] ページで [今すぐ同期（Synchronize Now）] をクリックし、新しい製品のライセンス情報を要求します。同期させないと、次回のスケジュールされた同期が完了するまで、Cisco Prime License Manager に最新の製品インスタンス情報が表示されません。

次の作業

クラスタの同期, （15 ページ）

クラスタの同期

すべてのデバイスデータをクラスタからアップロードして、ライセンスマネージャがライセンスを割り当てられるように、クラスタと Cisco Prime ライセンス マネージャを同期します。

はじめる前に

Cisco Prime License Manager へのクラスタの統合, （13 ページ）

（注） 複数のクラスタがある場合、最初の同期を実行する前にすべてのクラスタを追加することを推奨します。

手順

ステップ 1 Cisco Prime License Manager で、[製品インスタンス（Product Instances）] を選択します。

ステップ 2 [今すぐ同期（Synchronize Now）] をクリックします。
同期が完了したことを確認するメッセージが表示されます。

次の作業

ライセンス計画の作成, （15 ページ）

ライセンス計画の作成

システムの新しいライセンスを取得するには、ライセンスの追加ウィザードの手順に従い、ライセンス要求を準備します。

はじめる前に

クラスタの同期, （15 ページ）

手順

ステップ 1 Cisco Prime License Manager の [ライセンス（Licenses）]>[計画（Planning）] ウィンドウで、[ライセンス追加計画の作成（Create an Add Licenses Plan）] をクリックします。

ステップ 2 [製品の選択（Choose Product）] セクションで、ライセンスを追加する製品の製品タイプとライセンス バージョンを選択します。[Next] をクリックします。

ステップ 3 [ライセンス数（License Counts）] セクションで、各タイプのライセンスに割り当てるライセンスの数を調整し、[保存（Save）]をクリックしてそのライセンスタイプに対する変更を保存します。また、[コンプライアンスチェックの実行（Run Compliance Check）] をクリックしてコンプライアンス チェックを実行したり、[値のリセット（Reset Values）] をクリックしてライセンスの値をリ

セットしたりすることも可能です。ライセンス数が設定されたら、[次へ（Next）] をクリックします。
各ライセンスタイプの横の矢印をクリックすると、そのライセンスタイプの詳細情報が表示されます。

ステップ 4 コンプライアンス チェックに合格しなかった場合は、[ライセンス数（License Counts）] に戻って追加の変更を行うことができます。コンプライアンスチェックに合格した場合は、[次へ（Next）] をクリックして次のセクションに移動します。

ステップ 5 [要約と次の手順（Summary and Next Steps）] セクションで、行った変更の要約を確認して保存できます。また、独自の要約名と説明を入力することも可能です。

ステップ 6 要約を表示するには、[要約の表示（View Summary）] をクリックします。デフォルトで、[Cisco Prime License Managerに要約を保存（Save Summary in Cisco Prime License Manager）] オプションが選択されます。また、要約のデフォルト名は、<product-type>-add-<date-time-stamp> のフォーマットで [名前（Name）] フィールドに表示されます。発注やライセンスの履行に関する説明も、このセクションに表示されます。

ステップ 7 [完了（Finish）] をクリックします。

次の作業

ライセンス ファイルのインストール, （16 ページ）

ライセンス ファイルのインストール

ライセンスの履行手順に従い、システムの適切なライセンスをインストールします。これらの手順によって、システムのコンプライアンスが確保されます。

はじめる前に

ライセンス計画の作成, （15 ページ）

手順

ステップ 1 Cisco Prime License Manager のメイン メニューから、[ライセンス（Licenses）]>[履行（Fulfillment）] を選択します。

ステップ 2 電子履行モードで、[ライセンスをPAKから履行（Fulfill Licenses from PAK）] をクリックします。

ステップ 3 [新しいPAKからライセンスを追加（Add licenses from a new PAK）] を選択し、製品認証キー（PAK）コードを入力します。
Cisco Prime License Manager で PAK を入力済みの場合は、[部分履行をサポートするインストール済みの PAK からライセンスを追加（Add licenses from an already-installed PAK that supports partial

fulfillment）] を選択できます。このオプションを選択した場合は、ドロップダウン メニューから既存の PAK コードを選択します。

ステップ 4 [Next] をクリックします。Cisco.com のアカウント情報を求められた場合は、Cisco.com に登録したときに入力したユーザ名とパスワードを入力します。

ステップ 5 [OK] をクリックします。
履行する残りのライセンスがある場合（およびPAK のユーザ名とパスワードが確認されている場合）、[ライセンスを履行（Fulfill Licenses）] セクションが表示されます。

ライセンスは、最初に発行された cisco.com のアカウントを使用しないと履行できません。

ステップ 6 PAK でライセンスは SKU 名別に表示されます。各ライセンスの数はいくつかの見出しの下に分類され、履行済みのライセンスの数と履行前の残りのライセンスの数が示されます。
履行するライセンスの数を指定するには、そのライセンス タイプの [操作（Actions）] 列で [履行（Fulfill）] を選択します。[ライセンスの履行（Fulfill Licenses）] ウィンドウで、ライセンスのバージョン、機能、または両方を指定し、[保存（Save）] をクリックしてから [OK] をクリックしてウィンドウを閉じます。これで、更新された数が、[ライセンスを履行（Fulfill Licenses）] テーブルの [履行（Fulfill）] 列に表示されます。

（注） 一部の PAK は、部分履行に適していません。これらの PAK はまとめてパッケージ化されているため、1 つのトランザクションの 1 つの Cisco Prime License Manager でのみ履行できます。たとえば、NFR（再販なし）の注文は 20 個の CUWL Pro Unified CM および Unity Connection ライセンス、5 個の TelePresence Room ライセンスが含まれるパッケージとして販売されています。

（注） （[ライセンスの履行（Fulfill Licenses）] テーブルの [履行前（Before Fulfillment）] で）ライセンスが [履行済み（Fulfilled）] と表示されている場合、それらのライセンスは、現行または別の Cisco Prime License Manager によってすでに履行されています。

（注） 選択したライセンスを履行したら、[コンプライアンス チェックの実行（Run Compliance Check）] をクリックして、適合していることを確認できます。

ステップ 7 [次へ（Next）] をクリックして変更を確認します。まだ変更する必要がある場合は、[前へ（Previous）] をクリックして [ライセンスの履行（Fulfill Licenses）] に戻ります。変更を完了した場合は、[次へ（Next）] をクリックして次のセクションに移動します。

ステップ 8 [ライセンスの履行（Fulfill Licenses）] セクションで [次へ（Next）] をクリックすると、[トランザクション オプション（Transaction Options）] と [使用許諾契約書（License Agreement）] セクションが開きます。このセクションでは、説明を入力できます（任意）。また、オプションを選択してドロップダウン リストからライセンス要約の名前を選択することによって、このトランザクションを保存されているライセンス要約に関連付けることができます。

ステップ 9 チェックボックスを選択し、エンド ユーザ ライセンス契約書の条項に同意します。

ステップ 10 [終了（Finish）] をクリックします。
電子履行プロセスが正常に完了すると、新しい履行が [ライセンスの履行（License Fulfillment）] テーブルに表示されます。

ライセンス連携動作と制限事項

- システム ライセンスの連携動作, （18 ページ）
- システム ライセンスの制限事項, （19 ページ）

システム ライセンスの連携動作

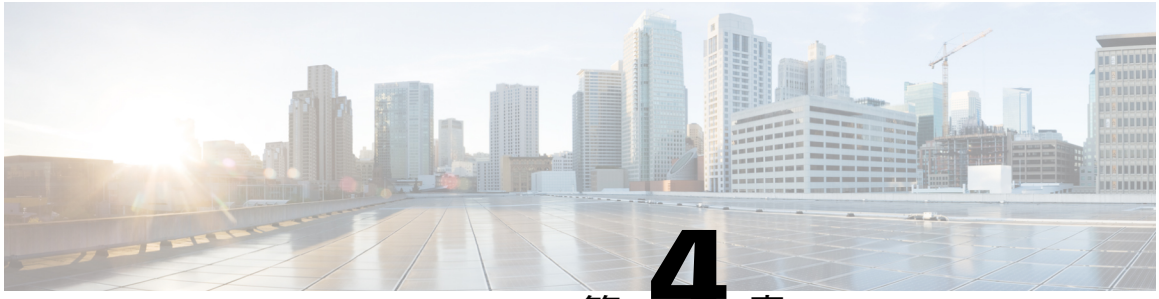
表 *1*：システム ライセンスの連携動作

機能	データのやり取り
エクステンション モビリティ（Extension Mobility）	Extension Mobility が設定されているが、デバイスに関連付けられていないユーザには、Essential ライセンスは必要ありません。
MGCP	MGCP FXS ポートは、アナログ電話であると見なされないため、ライセンスは必要ありません。
Telepresence Room	多目的 TelePresence デバイスとイマーシブ テレプレゼンス デバイスは、個別のデバイス ライセンス タイプの TelePresence Room ライセンスに基づいてライセンス付与されます。TelePresence Room ライセンスは、電話に入力されているユーザ ID と TelePresence デバイスの [オーナーのユーザ ID（OwnerUserID）] フィールドに入力されているユーザ ID が同じ場合のみ、TelePresence デバイスと登録済み電話の両方をカバーします。 TelePresense デバイスと電話の両方にオーナーのユーザ ID として同じユーザ ID が入力されていない場合は、デバイスと電話は関連付けられず、2 つのライセンスが必要となります。つまり、デバイス用に 1 つの TelePresence Room ライセンスと電話用に 1 つの拡張ユーザ接続ライセンス（UCL）が必要です。TelePresence Touch デバイスは登録されないため、個別のライセンスまたはオーナーのユーザ ID との関連付けは必要ありません。

システム ライセンスの制限事項

表 *2*：システム ライセンスの制限事項

制約事項	説明
ユーザごとの最大デバイス数	必須、基本、拡張の各 User Connect License（UCL）は、関連付けられた 1 デバイスを使用するユーザをサポートします。そのデバイスでは、[OwnerUserId] フィールドに、ユーザ ID が入力されています。Enhanced Plus UCL ライセンスは、関連付けられた 2 デバイスを使用するユーザをサポートします。Unified Workspace Licensing（UWL）Standard および UWL プレミアムは、関連付けられた 3 から最大 10 デバイスを使用するユーザをサポートします。
製品認証キー	一部の製品認証キー（PAK）は、部分履行に適していません。これらの PAK はまとめてパッケージ化されているため、単一 Cisco Prime License Manager でのみ履行できます。たとえば、再販なし（NFR）の注文は 20 個の CUWL Pro Unified Communications Manager および Unity Connection ライセンス、5 個の TelePresence Room ライセンスが含まれるパッケージとして販売されています。



第 4 章

サーバ情報の設定

- システム情報の概要，21 ページ
- サーバ設定のタスク フロー，21 ページ

システム情報の概要

この章では、Cisco Unified Communications Manager ノードのプロパティを設定する方法について説明します。

サーバ設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	サーバ情報の設定，（22 ページ）	Cisco Unified Communications Manager ノードの名前を指定し、説明を追加します。
ステップ 2	ポートの設定，（22 ページ）	次のポートを設定します。 • イーサネット電話ポート • MGCP リッスン ポート • MGCP キープアライブ ポート • SIP 電話ポート（SIP Phone Port） • SIP 電話セキュア ポート

サーバ情報の設定

Cisco Unified Communications Manager ノードの名前を指定し、説明を追加します。この手順で、次の読み取り専用情報を表示することもできます。

- コンピュータ テレフォニー インテグレーション ID（CTI ID）。
- Cisco Unified Communications Manager がインストールされているサーバ。

手順

ステップ 1 [Cisco Unified CMの管理（Cisco Unified CM Administration）] で、[システム（System）] > [Cisco Unified CM] を選択します。
[Cisco Unified CM の検索と一覧表示（Find and List Cisco Unified CMs）] 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。
一致するすべての Cisco Unified Communications Manager が表示されます。

ステップ 3 表示する [Cisco Unified CM（Cisco Unified CM）] を選択します。
[Cisco Unified CM の設定（Cisco Unified CM Configuration）] ウィンドウが表示されます。

ステップ 4 [名前（Name）] フィールドで、この Cisco Unified Communications Manager に割り当てる名前を入力します。

ステップ 5 [説明（Description）] フィールドに、ノードの説明を入力します。
説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 6 [保存（Save）] をクリックします。

ポートの設定

（注） 通常、デフォルトのポート設定を変更する必要はありません。デフォルトを変更することが必要な場合にのみ、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CMの管理（Cisco Unified CM Administration）] で、[システム（System）] > [Cisco Unified CM] を選択します。
[Cisco Unified CM の検索と一覧表示（Find and List Cisco Unified CMs）] 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。

一致するすべての Cisco Unified Communications Manager が表示されます。

ステップ 3 表示する [Cisco Unified CM（Cisco Unified CM）] を選択します。
[Cisco Unified CM の設定（Cisco Unified CM Configuration）] ウィンドウが表示されます。

ステップ 4 [このサーバの Cisco Unified Communications Manager TCP ポートの設定（Cisco Unified Communications Manager TCP Port Settings for this Server）]セクションに移動します。

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。

ステップ 7 [OK] をクリックします。

関連トピック

ポート設定, （23 ページ）

ポート設定

フィールド	説明
イーサネット電話ポート	システムは、この TCP ポートを使用してネットワークの Cisco Unified IP Phone（SCCP 専用）と通信します。 • このポートがシステムですでに使用されていなければ、デフォルトのポート値 2000 を受け入れます。2000 を選択すると、このポートは安全でないと識別します。 • すべてのポート エントリは一意であることを確認します。 • 有効なポート番号の範囲は 1024 ～ 49151 です。
MGCP リッスン ポート	システムは、関連 MGCP ゲートウェイからのメッセージを検出するのにこの TCP ポートを使用します。 • このポートがすでにシステムで使用中でなけば、デフォルトの 2427 ポートを受け入れます。 • すべてのポート エントリは一意であることを確認します。 • 有効なポート番号の範囲は 1024 ～ 49151 です。

フィールド	説明
MGCP キープアライブ ポート	システムは、キープアライブ メッセージを関連付けられた MGCP ゲートウェイと交換するためにこの TCP ポートを使用します。 • このポートがすでにシステムで使用中でなけば、デフォルトの 2428 ポートを受け入れます。 • すべてのポート エントリは一意であることを確認します。 • 有効なポート番号の範囲は 1024 ～ 49151 です。
SIP 電話ポート（SIP Phone Port）	このフィールドは、Cisco Unified Communications Manager が TCP と UDP 上の SIP のライン登録をリッスンするために使用するポート番号を指定します。
SIP 電話セキュア ポート	このフィールドは、 TLS 上の SIP のライン登録をリッスンするために使用されるポート番号を指定します。

ホスト名の設定

次の表に、Unified Communications Manager サーバのホスト名を設定できる場所、ホスト名として指定できる文字数、および推奨されるホスト名の先頭文字と最終文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が期待通りに機能しない可能性があります。

注意 次の表に示すいずれかの場所でホスト名や IP アドレスを変更する前に、『*Changing the IP Address and Host Name for Cisco Unified Communications Manager*』を参照してください。設定後のホスト名や IP アドレスを正しく更新しないと、Unified Communications Manager に問題が発生することがあります。

表 *3*：*Cisco Unified Communications Manager* におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IP アドレス（Host Name/ IP Address）] フィールド Cisco Unified Communications Manager Administration の [システム（System）] > [サーバ（Server）]	クラスタ内のサーバのホスト名を追加または変更できます。	2 ～ 63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications Manager インストールウィザード	クラスタ内のサーバのホスト名を追加できます。	1 ～ 63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications オペレーティングシステムの [設定（Settings）]> [IP] > [イーサネット（Ethernet）]	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ～ 63	英字	英数字
set network hostname hostname コマンドライン インターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ～ 63	英字	英数字

ヒント このホスト名は、ARPANET ホスト名の規則に従う必要があります。ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

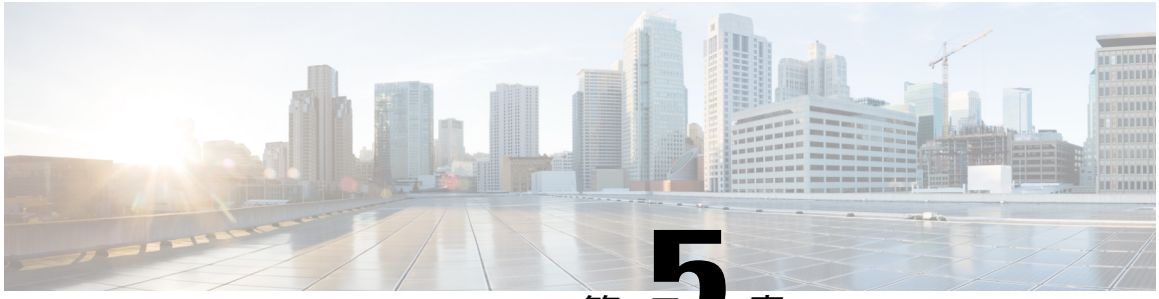
いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定（Server Configuration）] ウィンドウの [ホスト名/IP アドレス（Host Name/IP Address）] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。
  Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。Unified Communications Managerサブスクライバ ノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバ ノードの IP アドレスまたはホスト名を入力してください。

  このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。

ヒント　DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために（つまり、スタティック ネットワークを使用する場合に）パブリッシャ サーバのホスト名（必須）と IP アドレスを入力します。
  Unified Communications Manager サブスクライバ ノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャとサブスクライバ間の検証を確認できるようにしてください。さらに、サブスクライバ ノードのホスト名と IP アドレスも入力する必要があります。Unified Communications Manager のインストール時にサブスクライバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の（[ホスト名/IP アドレス（Host Name/IP Address）] フィールドでサブスクライバ サーバのホスト名を設定した場合に）[サーバの設定（Server Configuration）] ウィンドウに表示される値を入力します。



第 5 章

システムとエンタープライズ パラメータを設定

- 初期システムおよびエンタープライズ パラメータの概要，27 ページ
- システムとエンタープライズの初期設定タスク フロー，28 ページ

初期システムおよびエンタープライズ パラメータの概要

初めて Cisco Unified Communications Manager ノードを設定する場合は、次のシステム全体のパラメータを考慮します。必要に応じて、導入におけるシステム全体のパラメータを変更できますが、ほとんどの場合、推奨されるデフォルト設定で動作します。

- IP フォンのフォールバック接続モニタ期間を設定します。
- すべてのユーザに対して社内ディレクトリの検索を許可します。
- クラスタの完全修飾電話番号（FQDN）と組織のトップレベル ドメインを設定します。
- ビデオ対応の Cisco Jabber 開始条件を設定します。
- （オプション）クラスタが MLPP を使用している場合は、Multilevel Precedence and Preemption（MLPP）を有効にします。
- （オプション）ネットワークが IPv6 を使用している場合は、IPv6 を有効にします。
- （オプション）リモート syslog サーバ名前を入力します。
- （オプション）導入をトラブルシューティングするためのコール トレース ログを設定します。
- （オプション）依存関係レコードを有効にします。

システムとエンタープライズの初期設定タスク フロー

はじめる前に

Cisco Unified Communications Manager ノードとポートの設定をセットアップします。

手順

	コマンドまたはアクション	目的
ステップ 1	初期システム パラメータとエンタープライズ パラメータの設定, （28 ページ）	Cisco Unified Communications Manager ノードの初期セットアップに必要なシステム全体のパラメータを設定します。推奨されるシステム設定のリストについては、システムおよびエンタープライズの初期設定, （31 ページ）を参照してください。
ステップ 2	iOS Cisco Jabber の SSO ログインの動作設定, （36 ページ）	制御されたモバイル デバイス管理（MDM）の環境で IdP による証明書ベースの認証を Cisco Jabber で実行するために必要なエンタープライズパラメータを設定します。
ステップ 3	RTMT への SSO の設定, （37 ページ）	Cisco Unified Communications Manager を介してエンタープライズ パラメータを設定し、Real-Time Monitoring Tool（RTMT）の SAML SSO を有効にします。

次の作業

Cisco Unified Communications Manager クラスタで設定されているすべてのデバイスに適用する共通設定を確立する目的で、デバイスプールに対してコア設定を設定するためには、デバイスプールのタスク フローのコア設定, （51 ページ）を参照します。

初期システム パラメータとエンタープライズ パラメータの設定

Cisco Unified Communications Manager Administration を使用して、特定の導入環境でシステムおよびエンタープライズ パラメータを設定できます。システムの初期セットアップに重要であるパラメータを記載していますが、推奨するデフォルト設定は、ほとんどの導入環境で問題なく動作します。

コール トレース ログの有効化など、トラブルシューティングに役立つパラメータは、ネットワークのパフォーマンスに影響があるため、問題が解決した後は無効にする必要があります。

ほとんどのパラメータは、変更を有効にするためにすべてのデバイスをリセットする必要があります。すべての設定手順を完了してから、すべてのデバイスをリセットしてください。すべてのデバイスをリセットするのは、稼働率の低い時間帯に実行することを推奨します。

（注） リリース 10.0(1) から、Cisco Unified Communications Manager および IM and Presence サービスに同じエンタープライズ パラメータを使用します。IM and Presence サービスのエンタープライズ パラメータの値を変更する場合、変更した値は Cisco Unified Communications Manager に自動で反映されます。

手順

ステップ 1 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。

ステップ 2 クラスタの IP フォンが、TCP 接続が使用可能になったときに、プライマリ ノードに戻るまでの時間を、[エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] セクションの [接続モニタ間隔（Connection Monitor Duration）] フィールドに秒数を入力してから、[保存（Save）] をクリックします。デフォルト値は 120 秒です。

ヒント すべてのデバイスをリセットしないで、クラスタ内の影響を受けるデバイスに変更を適用するには、[設定の適用（Apply Config）] をクリックしてからし、[OK（OK）] をクリックします。

ステップ 3 [ユーザ データ サービス パラメータ（User Data Service Parameters）] セクションの [ユーザ検索をすべて有効にする（Enable All User Search）] セクションで、[True（True）] を選択して、姓、名、または電話番号が指定されていないときに、すべてのユーザを組織内名簿で検索することを許可します。

ステップ 4 [クラスタ全体のドメイン設定（Clusterwide Domain Configuration）] セクションで、クラスタ全体のドメインをセットアップします。

a) [組織の最上位ドメイン（Organization Top Level Domain）] フィールドで組織の最上位ドメインを入力します。255 文字まで指定できます。

b) [クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）] フィールドに、クラスタの完全修飾ドメイン名（FQDN）を入力します。255 文字まで指定できます。
複数の FQDN はスペースで区切る必要があります。アスタリスク（*）を使用して、FQDN 内でワイルドカードを指定することができます。たとえば、cluster-1.cisco.com *.cisco.com です。

ステップ 5 [Cisco Jabber（Cisco Jabber）] セクションで、[ビデオありコールを開始しない（Never Start Call with Video）] フィールドから [False（False）] を選択します。

ステップ 6 （任意） [MLPP および機密アクセス レベル パラメータ（MLPP and Confidential Access Level Parameters）] セクションで、Multilevel Precedence and Preemption（MLPP）ドメインを入力し、デバイスで MLPP の使用を有効にします。

a) [MLPP ドメイン ID（MLPP Domain Identifier）] フィールドに MLPP サービスのドメインを入力します。このパラメータには 16 進値（0x で始まる値）を指定します。

b) [MLPP 通知ステータス（MLPP Indication Status）] フィールドで、[MLPP 通知をオンにする（MLPP indication turned on）] を選択します。

ステップ 7 （任意） [IPv6（IPv6）] セクションで、[IPv6 を有効にする（Enable IPv6）] フィールドに [True（True）] を設定します。

ステップ 8 （任意） [Cisco Syslog エージェント（Cisco Syslog Agent）] セクションでは、[リモート syslog サーバ名 1（Remote Syslog Server Name 1）] に、リモート syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified Serviceability は syslog メッセージを送信しません。

ステップ 9 （任意） [セッション トレース用コール トレース ログの設定（Call Trace Log Configuration for Session Trace）] セクションで、セッション トレースの SIP コール情報を収集するコール トレース ログをセットアップします。
Real-Time Monitoring Tool（RTMT）のセッション トレース機能は、トラブルシューティングに利用できるコールのフロー図を生成するためにこの情報を使用します。

a) [コール トレース ログを有効にする（Enable Call Trace Log）] フィールドに [True（True）] を設定します。

b) Cisco Unified Communications Manager が生成できる SIP コール トレース ログ ファイルの最大数を [コール トレース ログ ファイルの最大数（Max Number of Call Trace Log Files）] フィールドに入力します。
デフォルト値は 2000 です。有効な範囲は 5 ～ 4000 です。

c) [コールトレースログ（Call Trace Log）] フィールドに SIP コール トレース ログ ファイルの最大サイズ（MB）を入力します。
デフォルト値は 2 です。有効な範囲は 1 ～ 10 です。

（注） SIP コール トラフィックが多い時間帯では、パフォーマンスが低下することがあります。システム パフォーマンスへの影響を低減するために、Cisco CallManager サービス パラメータの [セッション トレースのコール関連 REFER/NOTIFY/SUBSCRIBE SIP メッセージのログ（Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace）] に False を設定します。これにより、SIP コール トレースから REFER/NOTIFY/SUBSCRIBE メッセージを除外します。

ステップ 10 [CCMAdmin パラメータ（CCMAdmin Parameters）] セクションの [依存関係レコードを有効化（Enable Dependency Records）] フィールドで [True（True）] を選択します。

ステップ 11 [保存（Save）] をクリックします。

ステップ 12 [リセット（Reset）] をクリックし、[OK] をクリックしてすべてのデバイスをリセットします。
すべてのデバイスをリセットするのは、稼働率の低い時間帯に実行することを推奨します。

ヒント すべてのデバイスをリセットするために、システム内の全デバイス プールをリセットできます。

関連トピック

システムおよびエンタープライズの初期設定, （31 ページ）

システムおよびエンタープライズの初期設定

表 4：*Cisco Unified Communications Manager* の初期設定のシステムおよびエンタープライズ パラメータ

カテゴリ（**Category**）	パラメータ名	説明
エンタープライズ パラメータ	接続モニタ間隔（Connection Monitor Duration）	クラスタ内の IP フォンがセカンダリ ノードに登録された場合に、このパラメータを使用して、プライマリ ノードが使用可能になった後、それがフォールバックして再登録される前に、IP フォンが待機する時間を設定します。このパラメータは、特定のセキュア Survivable Remote Site Telephony（SRST）ルータに対応するすべてのセキュアなデバイスに影響します。 詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。 デフォルトは 120 秒です。 変更内容を反映するには、すべてのサービスを再起動してください。
CCMAdmin パラメータ	[依存性レコードを有効化（Enable Dependency Records）]	このパラメータは、トラブルシューティングに必要な依存関係レコードを表示するために使用されます。依存関係レコードを表示すると、初期システム設定時に役立つ場合があります。 依存関係レコードを表示すると、CPU使用率が急増し、コール処理に影響する可能性があります。考えられるパフォーマンス問題を回避するために、システム設定の完了後は、このパラメータを無効にします。負荷の低い時間帯またはメンテナンス ウィンドウの間のみに依存関係レコードを表示することを推奨します。 有効にするには、Cisco Unified Communications Manager の管理を使用して大半の設定ウィンドウからアクセスできる [関連リンク（Related Links）] ドロップダウン リストから [依存関係レコード（Dependency Records）] を選択できます。 デフォルト：[いいえ（False）]

カテゴリ（Category）	パラメータ名	説明
MLPP および機密アクセス レベル パラメータ	MLPP Domain Identifier	この Multilevel Precedence and Preemption（MLPP）パラメータは、MLPP サービスのドメインを指定します。MLPP ドメイン内の MLPP サブスクライバからのコールには優先度レベルが割り当てられます。同じ MLPP ドメイン内のより優先度の高いコールのみをプリエンプション処理できます。 このパラメータには 16 進値（0x で始まる値）を指定できます。 デフォルト：000000 変更内容を反映するには、すべてのデバイスを再起動してください。すべてのデバイスをリセットするには、システム内の全デバイス プールをリセットします。
	MLPP 表示ステータス（MLPP Indication Status）	MLPP ドメイン内のデバイスが MLPP サービスを使用できるように、このパラメータを有効にします。MLPP サービスには、トーン、特殊な表示、MLPP 情報要素（IE）/信号 IE/原因 IE の送信が含まれます。 デフォルト：MLPP 表示はオフ 変更内容を反映するには、すべてのデバイスを再起動してください。すべてのデバイスをリセットするには、システム内の全デバイス プールをリセットします。
ユーザ データ サービス パラメータ	Enable All User Search	このパラメータを使用して、ユーザは、名、姓、電話番号が指定されていない場合でも、社内ディレクトリですべてのユーザを検索できます。このパラメータは、[Cisco CallManager セルフ ケア（Cisco CallManager Self Care）]（CCMUser）ウィンドウでのディレクトリ検索にも適用されます。 デフォルト：[はい（True）]

カテゴリ（**Category**）	パラメータ名	説明
クラスタ全体のドメイン設定	[組織の最上位ドメイン（Organization Top Level Domain）]	このパラメータは、組織のトップ レベル ドメインを定義します。例：cisco.com 最大長：255 文字 有効な値：大文字と小文字、数字（0-9）、ハイフン、ドット（ドメイン ラベル区切り記号として）を使用した有効なドメイン。ドメイン ラベルの先頭文字をハイフンにすることはできません。最後のラベルの先頭文字を数字にすることはできません。たとえば、cisco.1om といったドメインは無効です。
	[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）]	このパラメータに、このクラスタの 1 つまたは複数の完全修飾ドメイン名（FQDN）を定義します。複数の FQDN はスペースで区切る必要があります。アスタリスク（*）を使用して、FQDN 内でワイルドカードを指定することができます。例：`cluster-1.cisco.com *.cisco.com` このパラメータのいずれかの FQDN に一致するホスト部分がある URL を含む要求（SIP コールなど）は、クラスタと接続されたデバイスにルーティングされます。 最大長：255 文字 有効な値：FQDN または * ワイルドカードを使用した部分的な FQDN。大文字と小文字、数字（0-9）、ハイフン、ドット（ドメイン ラベル区切り記号として）。ドメイン ラベルの先頭文字をハイフンにすることはできません。最後のラベルの先頭文字を数字にすることはできません。たとえば、cisco.1om といったドメインは無効です。

カテゴリ（**Category**）	パラメータ名	説明
IPv6	IPv6を有効化（Enable IPv6）	このパラメータは、Cisco Unified Communications Manager がインターネット プロトコル バージョン 6（IPv6）をネゴシエートできるかどうか、電話で IPv6 機能をアドバタイズできるかどうかを指定します。 このパラメータを有効にする前に、すべてのノードのプラットフォームに含まれている他のすべてのネットワーク コンポーネントで IPv6 を有効にする必要があります。それ以外の場合、システムは引き続き IPv4 専用モードで稼動します。 必須フィールドです。 デフォルト：False（IPv6 は無効です） IPv6 パラメータの変更を反映するため以下のサービスを再起動し、さらに IM およびプレゼンス サービス クラスタ内の影響を受けるサービスも再起動する必要があります。 • Cisco CallManager • Cisco IP Voice Media Streaming App • Cisco CTIManager • Cisco Certificate Authority Proxy Function
Cisco Syslog Agent	リモート Syslog サーバ名 1（Remote Syslog Server Name 1）	リモート Syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified Serviceability は Syslog メッセージを送信しません。このパラメータは、ログ用に Syslog サーバを使用している場合にのみ必須です。 最大長：255 文字 有効な値：大文字と小文字、数字（0-9）、ハイフン、およびドットを使用した有効なリモート Sylog サーバ名。 接続先として別の Cisco Unified Communications Manager ノードを指定しないでください。

カテゴリ（Category）	パラメータ名	説明
セッション トレースのコール レース ログの設定	コール トレース ログを有効にする（Enable Call Trace Log）	このパラメータは、Cisco Unified Communications Manager が、デバイス名、IP ドレス、およびコール中に使用される SIP 方式を含む、SIP コールの情報を収集できるようにします。Real-Time Monitoring Tool（RTMT）のセッション トレース機能は、トラブルシューティングに役立つコール フロー図を生成するためにこの情報を使用します。 SIP コール トラフィック量が多い期間は、ある程度のパフォーマンスの低下が生じることがあります。システム パフォーマンスの影響を低減するには、[セッション トレースのコール関連の REFER/NOTIFY/SUBSCRIBE SIP メッセージをログに記録する（Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace）] という Cisco CallManager サービス パラメータを [False] に設定します。これによって、SIP コール トレースから REFER、NOTIFY、および SUBSCRIBE メッセージが除外されます。 デフォルト：True（SIP コール トレースのロギングは有効）
	コール トレース ログ ファイルの最大数（Max Number of Call Trace Log Files）	このパラメータは、Cisco Unified Communications Manager が生成できる SIP コール トレース ログ ファイルの最大数を指定します。Real-Time Monitoring Tool（RTMT）のセッション トレース機能は、トラブルシューティングに役立つコール フロー図を生成するためにその情報を使用します。 コール トレース ログ ファイルのサイズは、[コール トレース ログ ファイルのサイズ（MB）（Call Trace Log File Size (MB)）] パラメータを使用して設定されます。 コール トレース ログ ファイルは、ラウンドロビン形式で上書きされます。たとえば、コール トレース ログ ファイルの数として 10 を指定し、コール トレース ログ ファイルのサイズを 5 MB に設定した場合、最初のコール トレース ログ ファイルのデータが 5 MB に達すると、Cisco Unified Communications Manager は 2 番目のコール トレース ログ ファイルを作成するといった具合になります。10 個のファイルが上書きされた後は、最も古いコール トレース ログ ファイルが最新の情報で上書きされます。 デフォルト：2000 最小値：5 最大値：4000

カテゴリ（**Category**）	パラメータ名	説明
	コール トレース ログ ファイルのサイズ（MB）（Call Trace Log File Size (MB)）	このパラメータは、SIP コール トレース ログ ファイルの最大ファイルサイズをメガバイト単位で指定します。Real-Time Monitoring Tool（RTMT）のセッション トレース機能は、トラブルシューティングに役立つコール フロー図を生成するためにこの情報を使用します。[コール トレース ログ ファイル パラメータの最大数（Max Number of Call Trace Log Files）] パラメータが大きな数値に設定されている場合は、ディスク容量をより適切に使用できるように、このパラメータの値を小さくすることを検討してください。 デフォルト：2 最小値：1 最大値：10
Cisco Jabber	ビデオとともにコールを開始しない（Never Start Call with Video）	このパラメータは、ビデオ コールの開始時に、ビデオを送信するかどうかを決定します。すぐにビデオを送信せずにビデオ コールを開始するには、[True] を選択します。ビデオコール中はいつでも、ビデオの送信開始を選択できます。 このパラメータは、IM およびプレゼンス サービスの優先度をオーバーライドします。False に設定すると、IM およびプレゼンス サービスに設定されている優先度に従ってビデオコールが開始します。 デフォルト：[いいえ（False）]

iOS Cisco Jabber の SSO ログインの動作設定

手順

ステップ 1 Cisco Unified CM の管理から、[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 オプトイン制御を設定するには、[SSO の設定（SSO Configuration）] セクションで、[iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）] パラメータで、[ネイティブ ブラウザの使用（Use Native Browser）] オプションを選択します。

（注） [iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）] パラメータには次のオプションが含まれます。

- [組み込みブラウザの使用（Use Embedded Browser）]：このオプションを有効にすると、Cisco Jabber は SSO の認証に、組み込みブラウザを使用します。このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。このオプションは、デフォルトで有効です。
- [ネイティブ ブラウザの使用（Use Native Browser）]：このオプションを有効にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー（IdP）を利用する証明書ベースの認証を実行します。

  （注） ネイティブ ブラウザの使用は組み込みブラウザの使用ほど安全ではないため、制御された MDM の導入での利用を除いては、このオプションの設定を推奨しません。

ステップ 3 [保存（Save）] をクリックします。

RTMT への SSO の設定

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] の順に選択します。

ステップ 2 RTMT に SSO を設定するには、[SSO の設定（SSO Configuration）] セクションで、[RTMT での SSO の使用（Use SSO for RTMT）] パラメータに [True] を選択します。

（注） [RTMT での SSO の使用（Use SSO for RTMT）] パラメータには、次のオプションが含まれます。

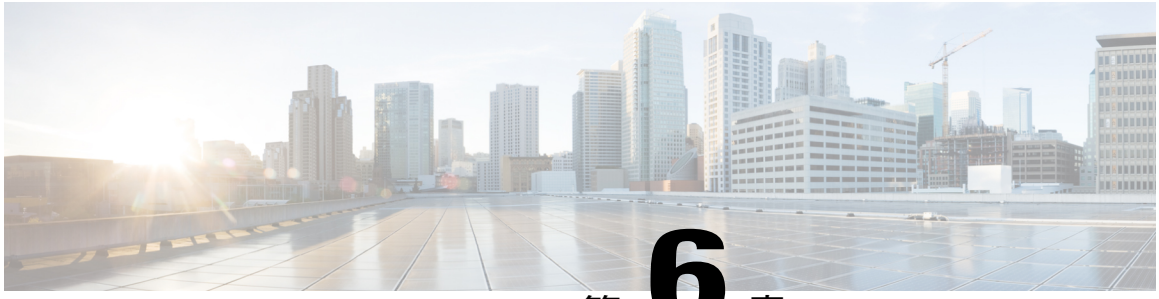
- [True]：このオプションを選択すると、RTMT は、SAML SSO ベースの IdP ログイン ウィンドウを表示します。

  （注） 新規インストール時には、[RTMT での SSO の使用（Use SSO for RTMT）] パラメータのデフォルト値は [True] になっています。

- [False]：このオプションを選択すると、RTMT は、基本認証のログイン ウィンドウを表示します。

  （注） [RTMT での SSO の使用（Use SSO for RTMT）] パラメータがない Cisco Unified Communications Manager のバージョンからアップグレードする場合、新しいバージョンに表示されるこのパラメータのデフォルト値は [False] です。

ステップ 3 [保存（Save）] をクリックします。



第 6 章

サービス パラメータの設定

- サービス パラメータの概要，39 ページ
- サービス パラメータの設定タスク フロー，40 ページ

サービス パラメータの概要

各 Cisco Unified Communications Manager ノードには、そのノードで利用可能なサービスのリストがあります。アクティブなサービスは、パブリッシャ ノードまたはサブスクライバ ノードや、選択して設定する機能によって異なります。

機能サービスとネットワーク サービスがあります。これらの一部はクラスタ全体にわたり、クラスタ内の全ノードに適用されます。ほとんどのサービスにはパラメータがあります。導入に際して具体的に変更する必要がなければ、デフォルトのサービス パラメータの設定を保持することを推奨します。

機能サービスは、Cisco Unified Serviceability の [サービス アクティベーション（Service Activation）] ウィンドウで有効化できます。ただし、ネットワーク サービスはデフォルトで有効であり、基本機能に必要です。トラブルシューティングのためにネットワーク サービスを停止して開始する必要がある場合は、Cisco Unified Serviceability の [コントロール センター - ネットワーク サービス（Control Center - Network Services）] ウィンドウを使用する必要があります。

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] または Cisco Unified Serviceability を使用して、サービスのステータスを表示できます。サービス パラメータ設定とサービス パラメータの説明を表示するには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] を使用します。

サービス パラメータの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	サービスのアクティブ化と非アクティブ化, （40 ページ）	Cisco Unified Serviceability を使用するノードでサービスをアクティブ化および非アクティブ化できます。パブリッシャ ノードの推奨サービス リストについては、パブリッシャ ノードの推奨サービス パラメータ, （41 ページ）を参照してください。サブスクライバ ノードの推奨サービス リストについては、サブスクライバ ノードの推奨サービス パラメータ, （42 ページ）を参照してください。
ステップ 2	ノードのサービス パラメータの設定, （43 ページ）	クラスタ内の Cisco Unified Communication Manager パブリッシャ ノードおよびサブスクライバ ノードのサービス パラメータを設定します。
ステップ 3	サービスおよびサービス パラメータ設定の表示, （44 ページ）	Cisco Unified Communications Manager Administration および Cisco Unified Serviceability を使用するノードのサービスを表示できます。サービス パラメータ設定およびパラメータの説明を表示するには、Cisco Unified Communications Manager Administration を使用します。

サービスのアクティブ化と非アクティブ化

サービスをアクティブまたは非アクティブにするには、Cisco Unified Serviceability を使用する必要があります。

サービスのステータスを変更すると、Cisco Unified Communications Manager Administration と Cisco Unified Serviceability の両方で情報が更新されます。サービスを無効化すると、Cisco Unified Communications Manager は現在のサービス パラメータ値を保持します。サービスを再開すると、Cisco Unified Communications Manager はサービス パラメータ値を更新します。

手順

ステップ 1 Cisco Unified Serviceability から、[ツール（Tools）]>[サービスのアクティブ化（Service Activation）] を選択します。

ステップ 2 ドロップダウン メニューから [サーバ（Server）] を選択して、[移動（Go）] をクリックします。サービスと現在のステータスが表示されます。

ステップ 3 サービスを有効にするには、有効にするサービスの隣にあるチェックボックスをオンにします。

ステップ 4 サービスを無効にするには、無効にするサービスの隣にあるチェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。
サービスのアクティブ化が完了するには数分かかることがあります。ステータスの変更を確認するには、ページを更新します。

次の作業

ノードのサービス パラメータの設定, （43 ページ）

パブリッシャ ノードの推奨サービス パラメータ

次の表は、専用 TFTP サーバ以外を使用する場合の Cisco Unified Communications Manager パブリッシャ ノードの推奨サービスを示します。

表 *5*：非専用 *TFTP* サーバ展開で推奨されるパブリッシャ ノード サービス

タイプ（Type）	サービス名（Service Name）
CM サービス	Cisco CallManager
	Cisco Unified Mobile Voice Access Service
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extended Functions
	シスコ クラスタ間検索サービス
	シスコ ロケーション帯域幅マネージャ
	Cisco TFTP
CTI サービス	Cisco IP Manager Assistant
	Cisco WebDialer Web Service

タイプ（Type）	サービス名（Service Name）
CDR サービス	Cisco SOAP - CDRonDemand サービス
	Cisco CAR Web Service
データベースおよび管理者サービス	Cisco Bulk Provisioning サービス
	AXL Web Service
	Cisco URL Web サービス
パフォーマンスおよびモニタリング サービス	Cisco Serviceability Reporter
	Cisco Certificate Authority Proxy Function
ディレクトリ サービス	Cisco DirSync

ヒント　その他のサービスは、使用する計画がなければ安全に無効化できます。

- Cisco Messaging Interface
- Cisco DHCP Monitor サービス
- Cisco TAPS サービス
- Cisco Directory Number Alias Sync
- Cisco Directory Number Alias SyncCisco Dialed Number Analyzer Server
- Cisco Dialed Number Analyzer
- Self Provisioning IVR

サブスクライバ ノードの推奨サービス パラメータ

次の表は、専用 TFTP サーバ以外を使用する場合の Cisco Unified Communications Manager サブスクライバ ノードの推奨サービスを示します。

ヒント　その他のサービスは、使用する計画がなければ安全に無効化できます。

表 *6*：非専用 *TFTP* サーバ展開で推奨されるサブスクライバ ノード サービス

タイプ（**Type**）	サービス名（**Service Name**）
CM サービス	Cisco CallManager
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco エクステンション モビリティ
	Cisco Extended Functions
	Cisco TFTP

クラスタ内の各 IM and Presence Service ノードで次のサービスをアクティブにする必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

ノードのサービス パラメータの設定

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] を使用して、ノード上のサービス パラメータを設定できます。クラスタ全体としてマークされているサービス パラメータは、クラスタ内の全ノードに影響を及ぼします。

注意 サービス パラメータの一部の変更は、システム障害の原因になることがあります。変更しようとしている機能を完全に理解している場合と、Cisco Technical Assistance Center（TAC）から変更の指定があった場合を除いて、サービス パラメータに変更を加えないようにしてください。

はじめる前に

- Cisco Unified Communications Manager のノードが設定されていることを確認します。
- サービスがアクティブであることを確認します。詳細は、サービスのアクティブ化と非アクティブ化, （40 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM 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 [サーバ（Server）] ドロップダウン リストのノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストのサービスを選択します。
選択したノードに適用されるすべてのパラメータが表示されます。[クラスタ全体のパラメータ（一般）（Clusterwide Parameters（General））] セクションに表示されるパラメータは、クラスタ内の全ノードに適用されます。

ヒント [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウ の ? アイコンをクリックして、サービス パラメータのリストと説明を表示します。

ステップ 4 サービス パラメータを変更し、[保存（Save）] をクリックします。ウィンドウが更新され、サービス パラメータ値が更新されます。
[デフォルトに設定（Set to Default）] ボタンをクリックして、すべてのパラメータを、[パラメータ値（Parameter Value）] フィールドの後に表示される提案値に更新できます。パラメータに提案値が設定されていない場合は、[デフォルトに設定（Set to Default）] ボタンをクリックしてもサービス パラメータ値は変更されません。

次の作業

サービスおよびサービス パラメータ設定の表示, （44 ページ）

サービスおよびサービス パラメータ設定の表示

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] および Cisco Unified Serviceability を使用して、クラスタ内のノードのサービスのステータスを表示できます。サービス パラメータ設定およびパラメータの説明を表示するには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] を使用します。

はじめる前に

ノードのサービス パラメータの設定, （43 ページ）

手順

ステップ 1 サービスを表示し、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] を使用して、ノードのサービス パラメータ設定を表示するには、次の手順を実行します。

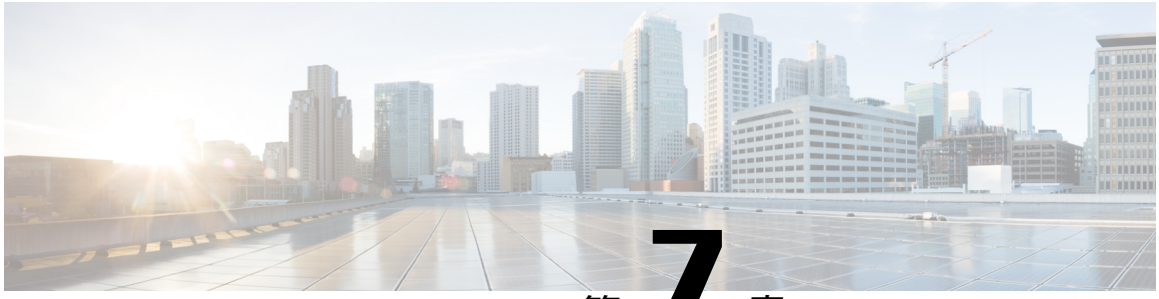
a) [システム（System）] > [サービス パラメータ（Service Parameters）] の順に選択します。
b) [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、[サーバー（Server）] ドロップダウン ボックスのノードを選択します。
c) [サービス（Service）] ドロップダウン ボックスのサービスを選択します。

選択したノードに適用されるすべてのパラメータが表示されます。[クラスタ全体のパラメータ（一般）（Clusterwide Parameters（General））] セクションに表示されるパラメータは、クラスタ内の全ノードに適用されます。

d) [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウの（?）アイコンをクリックし、サービス パラメータと説明のリストを表示します。

ステップ 2 クラスタ内の全ノードに関する特定のサービスのサービスパラメータを表示するには、[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウン ボックスの [すべてのサーバに対するパラメータ（Parameters for All Servers）] を選択し、[Go] をクリックします。
[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウが表示されます。表示されているサーバ名またはパラメータ値をクリックして、関連する [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウを開くことができます。

ステップ 3 クラスタ内の全ノードに関する特定のサービスの同期外れサービス パラメータを表示するには、[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウの [関連リンク（Related Links）] ドロップダウン ボックスの [すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] を選択し、[Go] をクリックします。
[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] ウィンドウが表示されます。表示されているサーバ名またはパラメータ値をクリックして、関連する [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウを開くことができます。



第 7 章

デバイス プールのコア設定

- デバイス プールのコア設定の概要，47 ページ
- デバイス プールのコア設定の前提条件，51 ページ
- デバイス プールのタスク フローのコア設定，51 ページ

デバイス プールのコア設定の概要

Cisco Unified Communications Manager で、コア システム設定（サーバ グループ、タイム ゾーン情報、リージョン（コーデック選択）など）を行います。これらの設定は基本的なもので、基本デバイス プールの基礎になります。

電話用 NTP リファレンス

Cisco Unified CM の管理の Network Time Protocol（NTP）リファレンスにより、SIP を実行中の IP フォンは NTP サーバから確実に日時を取得できます。SIP を実行中の電話がプロビジョニングされた“電話用 NTP リファレンス”から日時情報を取得できない場合、その電話はCisco Unified Communications Managerに登録したときに日時情報を受信します。

日時グループ

日時グループを使用すると、Cisco Unified Communications Manager に接続されているさまざまなデバイスのタイム ゾーンを定義できます。デフォルト グループである CMLocal は、インストール時に自動的に設定されます。ただし、ローカルタイムゾーンごとにグループを設定することを推奨します。

（注） CMLocal の場合、システムの再起動時や新しいリリースへのアップグレード時に、常にオペレーティングシステムの日時と同期が行われます。CMLocal の名前は変更しないでください。

リージョン

リージョンを使用することで、WAN リンク経由で送信される個々のコールの帯域幅を制限し、内線コールには高い帯域幅を使用する必要がある、Cisco Unified Communications Manager マルチサイト導入のキャパシティを制御できます。さらに、システムは特定のコーデックのみをサポートするアプリケーションに対してリージョンを使用します。

Cisco Unified Communications Manager は、ビデオ ストリームの暗号化および次の音声コーデックをサポートしています

オーディオ コーデック	説明
G.711	公衆電話交換網に使用される、最も広くサポートされているコーデック。
G.722	ビデオ会議でよく使用されるワイドバンド コーデック。G.722 は無効になっていない限り、Cisco Unified Communications Manager では常に G.711 より優先されます。
G.722.1	24 および 32 kb/s で動作する低複雑度のワイドバンド コーデック。使用するビット レートはほぼ半分ですが、音声品質は G.722 の品質に近づいています。
G.728	ビデオ エンドポイントがサポートする低ビット レート コーデック。
G.729	Cisco Unified IP Phone 7900 でサポートされている 8 kb/s 圧縮を使用する低ビット レート コーデック。通常は、WAN リンクを通過するコールに使用されます。
GSM	Global System for Mobile Communications（GSM）コーデック。GSM を使用すると、GSM ワイヤレス ハンドセット用の MNET システムを Cisco Unified Communications Manager で動作させることができます。
L16	Advanced Audio Coding-Low Delay（AAC-LD）は、音声と音楽向けに優れた音質を提供するスーパー広帯域オーディオ コーデックです。このコーデックは、低ビット レートの場合でも、古いコーデックと同等以上の音質を提供します。
AAC-LD（mpeg4-generic）	SIP デバイス、特に、Cisco TelePresence Systems に対してサポートされています。

オーディオ コーデック	説明
AAC-LD（MP4A-LATM）	Low-overhead MPEG-4 Audio Transport Multiplex（LATM）は優れた音を提供するスーパー広帯域オーディオ コーデックです。TANDBERG や一部のサードパーティのエンドポイントを含む、SIP デバイスに対してサポートされています。 （注） AAC-LD（mpeg4-generic）と AAC-LD（MPA4-LATM）の間に互換性はありません。
Internet Speech Audio Codec（iSAC）	特に、低ビット レートと中ビット レートの両アプリケーションにおいて、低遅延でワイドバンド音質を提供するように設計された適応型広帯域オーディオ コーデック。
インターネット低ビット レート コーデック（iLBC）	個別にエンコードされた音声フレームに起因する損失性ネットワークでのグレースフルな音声品質の低下を許可している間に、15.2 および 13.3 kb/s のビット レートで G.711 と G.729 の間の音声品質を提供します。iLBC は、SIP、SCCP、H323、および MGCP デバイスに対してサポートされています。 （注） H.323 アウトバウンド FastStart は iLBC コーデックをサポートしていません。
アダプティブ マルチレート（AMR）	GSM（WDMA、EDGE、GPRS）に基づいた 2.5G/3G ワイヤレス ネットワークに必要な標準コーデック。このコーデックは、4.75 ～ 12.2 kb/s の範囲の可変ビット レートでナローバンド（200 ～ 3400 Hz）信号をエンコードし、7.4 kb/s で始まる公衆電話交換網レベルの音声品質を提供します。AMR は SIP デバイスでのみサポートされます。
アダプティブ マルチレート ワイドバンド（AMR-WB）	正式にはワイドバンドとして知られている ITU-T 標準音声コーデックである G.722.2 として体系化されており、約 16 kb/s で音声をコード化します。このコーデックは、広い音声帯域幅（50 ～ 7000 Hz）によって、より良い音声品質を提供できるため、その他のナローバンド音声コーデック（AMR や G.711 など）より優先されます。AMR-WB は SIP デバイスでのみサポートされます。

オーディオ コーデック	説明
Opus	Opus コーデックはインタラクティブな音声およびオーディオ コーデックです。特に、Voice over IP、ビデオ会議、ゲーム内チャット、ライブ配信の音楽パフォーマンスなど、さまざまなインタラクティブ オーディオ アプリケーションに対応するために設計されています。 このコーデックは、ナローバンド低ビットレートから非常に高品質のビット レート（6 ～ 510 kb/s）まで拡大します。 Opus は SIP デバイスでのみサポートされます。Opus コーデック サービス パラメータの [Opus コーデックを有効にする （Opus Codec Enabled）] は、デフォルトでは [すべてのデバイスに対して有効にする（Enabled for All Devices）] に設定されています。サービス パラメータの設定は、[サービス パラメータの設定（Service Parameter Configuration）] ウィンドウで、[すべての非録音デバイスに対して Opus コーデックを有効化（Enable Opus codec for all non-recording devices）] または [無効化（Disabled）] に設定できます。 （注） [エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] ウィンドウの [G.722 コーデックのアドバタイズ（Advertise G.722 Codec）] サービス パラメータは、Opus コーデックを使用する SIP デバイスに対しては [有効化（Enabled）] に設定する必要があります。エンタープライズ パラメータの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151.html）を参照してください。

Unified Communications Manager グループ

システムのバックアップ Cisco Unified Communications Manager の署名を解除します。これらは、システムの停止または障害が発生しているノードのコール処理を処理します。

Cisco Unified Communications Manager グループは、最大 3 つのノードの優先順位リストです。各グループにはプライマリ ノードを含める必要があり、グループには 1 つまたは 2 つのバックアップ ノードを含めることができます。グループ内のノードのリスト順により、ノードの優先順位が決まります。

Cisco Unified Communications Manager グループは、コール処理の冗長性と分散型コール処理の両方を提供します。グループ間でのデバイス、デバイス プール、およびノードの分散方法により、システムの冗長性とロード バランシングのレベルが決まります。ほとんどの場合、グループ内のいずれかのノードで障害が発生した場合に、他のノードがオーバーロード状態になるのを防ぐようにデバイスを分散させる必要があります。

Device Pools

デバイスプールを使用して、デバイス固有の設定をグループ化します。デバイスプールを作成すると、各デバイスを個別に設定する代わりに、各デバイスがデバイス プールの設定を継承するように関連付けることができます。

新しいデバイスプールの追加は、そのデバイスプールで実行したい内容に基づいて行います。たとえば、サーバのロードバランシングや物理的な場所を考慮して設定されているデバイスプールを使用できます。

この項では、基本的なデバイス プールの設定手順について説明します。システムに追加機能を設定する際には、追加したデバイス プール（複数可）に戻り、適用する設定でそれらのデバイス プールを更新できます。

デバイス プールのコア設定の前提条件

Cisco Unified Communications Manager が最新のタイム ゾーン情報を含むことを確認するため、Cisco Unified Communications Manager のインストール後にタイム ゾーン情報を更新する Cisco Option Package（COP）ファイルをインストールできます。主なタイム ゾーンの変更イベントの後で、最新の COP ファイルを https://software.cisco.com/download/navigator.html でダウンロードできることをお知らせします。

CMLocal の設定はいつでもローカル日時に変更できます。

デバイス プールのタスク フローのコア設定

手順

	コマンドまたはアクション	目的
ステップ 1	電話用 NTP リファレンスの追加, （52 ページ）	SIP を実行している IP フォンが NTP サーバから時刻と日付の情報を取得することを確認するには、電話 Network Time Protocol（NTP）の参照を設定します。 （注） NTP の参照を作成後、その参照を日付/時刻グループに追加する必要があります。日付/時刻のグループで、電話に連絡させる最初のサーバから始めて、電話の NTP 参照に優先順位を付けます。
ステップ 2	日時グループの追加, （53 ページ）	システムに接続される各種デバイスのタイム ゾーンを定義します。データベースに新しい日付/時刻グループを追加したらデバイス プールに割り当て、そのデバイス プールの日付/時刻情報を設定します。

	コマンドまたはアクション	目的
ステップ 3	地域の追加, （54 ページ）	内線通話でより広い帯域幅を使用できるようにすると同時に、WAN リンク全体に送信される個々のコールの帯域幅を制限します。 ヒント　デフォルトの G.711 オーディオ コーデックのみ使用しているのなら、地域を設定する必要はありません。
ステップ 4	Cisco Unified Communications Manager グループの設定, （55 ページ）	Cisco Unified Communications Manager グループを設定して、デバイスが登録、コール処理、および停止時の冗長性に使用できる 3 つのノードをまとめてグループ化するように設定します。
ステップ 5	基本的なデバイス プールの設定, （56 ページ）	デバイスを追加するたびに同じ設定を定義するのではなく、デバイスに割り当てられる共通設定を含むデバイス プールを設定します。Unified Communications Manager、日時情報、関連付けられたデバイスが使用するコーデックを設定するための基本的なデバイス プールから開始します。

電話用 NTP リファレンスの追加

SIP を実行している IP フォンが NTP サーバから時刻と日付の情報を取得することを確認するには、電話 Network Time Protocol（NTP）の参照を設定します。

（注）　NTP の参照を作成後、その参照を日付/時刻グループに追加する必要があります。日付/時刻のグループで、電話に連絡させる最初のサーバから始めて、電話の NTP 参照に優先順位を付けます。

（注）　Cisco Unified Communications Manager は、マルチキャストおよびエニーキャスト モードをサポートしていません。これらのモードのいずれかを選択すると、システムはデフォルトで、ダイレクト ブロードキャスト モードを選択します。

はじめる前に

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [電話用 NTP リファレンス（Phone NTP Reference）] 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 [IP アドレス（IP Address）] フィールドに、SIP を実行している電話機が日付と時刻を取得するために使用する NTP サーバの IP アドレスを入力します。

ステップ 4 [説明（Description）] フィールドに、電話用 NTP リファレンスの説明を入力します。

ステップ 5 [モード（Mode）] ドロップダウン リストから、次のオプションに従い、電話用 NTP リファレンスのモードを選択してください。

- [ユニキャスト（Unicast）]：このモードを選択すると、電話機は、指定した NTP サーバに NTP クエリ パケットを送信します。
- [ダイレクト ブロードキャスト（Directed Broadcast）]：このデフォルトの NTP モードを選択すると、電話機は任意の NTP サーバの日時情報を利用しますが、リストされている NTP サーバ（1 番目 = プライマリ、2 番目 = セカンダリ）を優先します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

日時グループの追加, （53 ページ）

日時グループの追加

システムに接続される各種デバイスのタイムゾーンを定義します。データベースに新しい日付/時刻グループを追加したらデバイス プールに割り当て、そのデバイス プールの日付/時刻情報を設定します。

変更を適用するには、デバイスをリセットする必要があります。

ヒント Cisco Unified IP Phone の世界的な流通のため、24 のタイム ゾーンそれぞれの日時グループを作成します。

はじめる前に

電話用 NTP リファレンスの追加, （52 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [日時グループ（Date/Time Group）] 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 [日付グループの設定（Date/Time Group Configuration）] ウィンドウ内の各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

地域の追加, （54 ページ）

地域の追加

内線通話でより広い帯域幅を使用できるようにすると同時に、WAN リンク全体に送信される個々のコールの帯域幅を制限します。

ヒント デフォルトの G.711 オーディオ コーデックのみ使用しているのなら、地域を設定する必要はありません。

拡張性の強化と、少ないリソースを使用するシステムの実現に向けて、音声通話とビデオ通話の最大ビット レート、およびリンク損失タイプを指定する [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウでデフォルト値を設定することを推奨します。さらに、地域を設定する場合は、[地域設定（Region Configuration）] ウィンドウでデフォルト設定を選択します。

はじめる前に

日時グループの追加, （53 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 ノードを選択します。

ステップ 3 Cisco CallManager サービスを選択します。

ステップ 4 [クラスタ全体のパラメータ（システムの場所と地域）（Clusterwide Parameters (System-Location and Region)）] ペインまでスクロールします。

ステップ 5 地域を作成し、この地域内とそのほかの地域との間で発生するコールの最大ビット レートを指定します。

- 音声通話では、地域内のデフォルト値は 64 kb/s です（そのコールには G.722 または G.711 が使用される可能性があり、高音質という点で G.722 が好まれるでしょう）。
- 音声通話では、地域間のデフォルト値は 8 kb/s （G.729）です。
- ビデオ通話（音声を含む）では、デフォルト値は 384 kb/s です。

（注） Cisco Unified Communications Manager では、最大 2000 地域を追加できます。地域を使用しているデバイスに最大ビット レートを指定する必要があります。

ステップ 6 [Save] をクリックします。

次の作業

Cisco Unified Communications Manager グループの設定, （55 ページ）

Cisco Unified Communications Manager グループの設定

Cisco Unified Communications Manager グループを設定して、デバイスが登録、コール処理、および停止時の冗長性に使用できる 3 つのノードをまとめてグループ化するように設定します。

（注） デフォルト サーバ グループは名前から内容がわからず、混乱が起きる可能性があるため、使用しないでください。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [Cisco Unified CM グループ（Cisco Unified CM Group）] を選択します。

ステップ 2 [名前（Name）] フィールドに、名前を入力します。
名前でノードの順序を特定できるように考慮します。たとえば、CUCM_PUB-SUB のように他のグループと簡単に区別できるようにします。

ステップ 3 [利用可能な Cisco Unified Communications Manager（Available Cisco Unified Communications Managers）] リストから、このグループに追加するノードを選択します。

ステップ 4 [選択された Cisco Unified Communications Manager（Selected Cisco Unified Communications Managers）] リストにノードを移動するには、下矢印をクリックします。

ステップ 5 必要に応じて、このグループに他のすべてのノードを追加します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

基本的なデバイス プールの設定, （56 ページ）

基本的なデバイス プールの設定

デバイスを追加するたびに同じ設定を定義するのではなく、デバイスに割り当てられる共通設定を含むデバイス プールを設定します。Unified Communications Manager、日時情報、関連付けられたデバイスが使用するコーデックを設定するための基本的なデバイス プールから開始します。

（注） 識別できず、混乱を招く恐れがあるため、デフォルトのデバイス プールは使用しないでください。

はじめる前に

- Cisco Unified Communications Manager グループの設定, （55 ページ）
- 日時グループの追加, （53 ページ）
- 地域の追加, （54 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [デバイス プール（Device Pool）] 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 [デバイス プールの設定（Device Pool Configuration）] ウィンドウの各フィールドを設定します。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

基本的なデバイス プール設定フィールド, （57 ページ）

基本的なデバイス プール設定フィールド

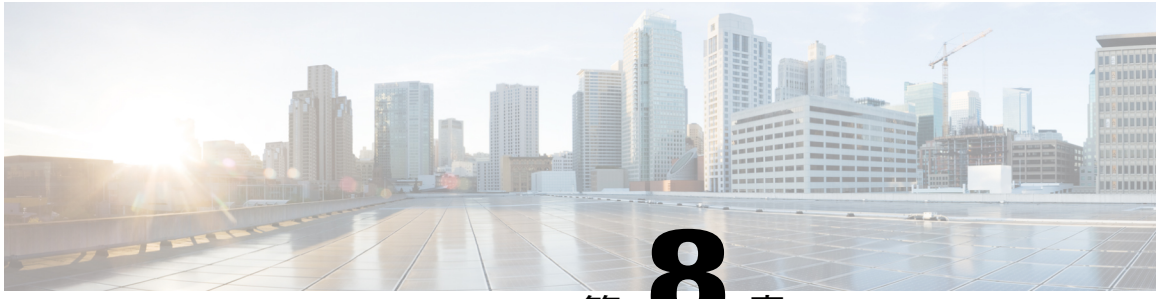
表 7：基本的なデバイス プール設定フィールド

フィールド	説明
[デバイスプール名（Device Pool Name）]	新しいデバイス プールの名前を入力します。英数字、ピリオド（.）、ハイフン（-）、下線（_）、スペースを含む最大 50 文字までを入力できます。
[Cisco Unified CMグループ（Cisco Unified Communications Manager Group）]	このデバイス プール内のデバイスに割り当てる Cisco Unified Communications Manager グループを選択します。Cisco Unified Communications Manager グループは、最大 3 つの Cisco Unified Communications Manager ノードの優先順位付けされたリストを指定します。リストの最初のノードはそのグループのプライマリ ノードとして動作し、グループの他のメンバーは、冗長性のためのバックアップ ノードとして動作します。
[日時グループ（Date/Time Group）]	このデバイス プール内のデバイスに割り当てる日時グループを選択します。日時グループは、タイム ゾーンと日時の表示形式を指定します。
地域	このデバイス プール内のデバイスに割り当てる地域を選択します。地域の設定は、地域内および他の地域間との通信に使用できる音声コーデックとビデオ コーデックを指定します。

第 II 部

発着信コールの有効化

- 発着信コールの概要，61 ページ
- ゲートウェイの設定，63 ページ
- SIP の正規化および透明性の設定，85 ページ
- SDP 透明性プロファイルの設定，91 ページ
- SIP プロファイルの設定，95 ページ
- デュアル スタックの IPv6 の設定，97 ページ
- SIP トランクの設定，105 ページ
- H.323 トランクの設定，113 ページ
- SRST の設定，117 ページ



第 8 章

発着信コールの概要

- 着信コールと発信コールについて，61 ページ
- 着信コールと発信コールの設定，61 ページ

着信コールと発信コールについて

このパートでは、システムの発信コールと着信コールを設定する方法を説明します。

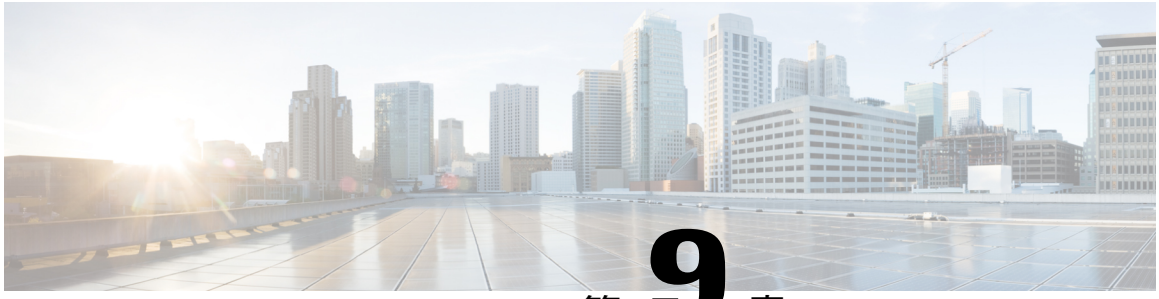
着信コールと発信コールの設定

次のタスク フローを実行すると、システムの着信コールと発信コールを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ゲートウェイの設定タスク フロー，（67 ページ）	ゲートウェイをシステムに追加します。
ステップ 2	SIP の正規化および透明性設定のタスク フロー，（87 ページ）	これはオプションです。相互運用性の問題を解決するために SIP トランクまたは SIP デバイスに割り当てられる、SIP 正規化と透明性スクリプトを設定します。
ステップ 3	SDP 透明性プロファイルの設定，（92 ページ）	これはオプションです。SIP を導入するために Cisco Unified Communications Manager がネイティブで対応していない SDP 属性をサポートする必要があれば、サポートされていない属性を含む SDP 透明性プロファイルをセットアップします。

	コマンドまたはアクション	目的
ステップ 4	SIP プロファイルの概要, （95 ページ）	SIP トランクおよび SIP デバイスの SIP プロファイルを設定します。
ステップ 5	デュアル スタック IPv6 設定のタスク フロー, （98 ページ）	これはオプションです。SIP を導入するのに IPv6 デバイスをサポートする必要があれば、システムでデュアル スタック IPv6 サポートを設定します。デュアル スタックは SIP 導入用にのみ設定できます。
ステップ 6	SIP トランクの設定タスク フロー, （107 ページ）	システムに SIP トランクを設定します。
ステップ 7	H.323 トランクの概要, （113 ページ）	システムに H.323 トランクを設定します。
ステップ 8	Survivable Remote Site Telephony の設定タスク フロー, （118 ページ）	SRST 用にシステムを設定します。



第 9 章

ゲートウェイの設定

- ゲートウェイの概要，63 ページ
- ゲートウェイ設定の前提条件，66 ページ
- ゲートウェイの設定タスク フロー，67 ページ

ゲートウェイの概要

シスコは広範な音声およびビデオ ゲートウェイを提供しています。ゲートウェイは、ユニファイドコミュニケーションネットワークと外部ネットワークとの通信を可能にするインターフェイスを提供します。従来、ゲートウェイは、PSTN、構内交換機（PBX）、またはアナログ電話やFAX装置を含むレガシー デバイスなどのレガシー電話インターフェイスに IP ベースのユニファイド コミュニケーション ネットワークを接続するために使用されてきました。最も単純な形では、音声ゲートウェイがIPインターフェイスとレガシー電話インターフェイスを備え、2つのネットワークが通信できるようにゲートウェイが 2 つのネットワーク間でメッセージを変換します。

ゲートウェイ プロトコル

大半のシスコのゲートウェイには、複数の導入オプションがあり、多数のプロトコルのいずれかを使用して導入できます。導入するゲートウェイに応じて、次の通信プロトコルのいずれかを使用してゲートウェイを設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）
- Skinny Call Control Policy（SCCP）
- Session Initiation Protocol（SIP）
- H.323

ベンダー インターフェイス カード

外部ネットワーク用の接続インターフェイスを提供するには、ベンダーインターフェイスカード（VIC）がゲートウェイにインストールされている必要があります。大半のゲートウェイには複

数の VIC オプションがあり、各 VIC がアナログとデジタルの両方の接続に対応する多数の異なるポートと接続タイプを備えている場合があります。

ゲートウェイで提供されているプロトコル、カード、接続については、ゲートウェイのドキュメントを参照してください。

ポートとトランクの接続のタイプ

以下は、ゲートウェイに設定できるポート接続の主なタイプです。

- Foreign Exchange Station（FXS）：FXS ポートは、アナログ電話、スピーカーフォン、従来のボイスメール システムなど、アナログ ステーションへの接続を提供します。
- Foreign Exchange Office（FXO）：FXO ポートは、PSTN またはレガシー PBX へのアナログ接続を提供します。
- T1 Channel Assocatied Signaling（T1/E1 CAS）：T1/E1 CAS 接続は、セントラル オフィス、PBX、またはそのほかのアナログ デバイスにデジタル トランク接続を提供します。
- 一次郡速度インターフェイス（T1/E1 PRI）：デジタル アクセス PRI 接続は企業向け通信で広く使用されています。T1 PRI は北米と日本で広く使用されており、音声およびデータ用の 23 本の B チャネルと共通線信号用の速度 1.544 Mb/s の 1 本の D チャネルを提供します。E1 は欧州で広く使用されており、音声およびデータ用の 30 本の B チャネル、共通線信号用の 1 本の D チャネル、および 1 本のフレーミング チャネルを提供します。E1 は、2.048 Mbps の速度を使用します。
- 基本速度インターフェイス（BRI）：BRI はデジタル テレフォニー プロトコルです。小規模オフィスおよび家庭用通信リンクで使用され、音声とデータ用の 2 本の B チャネルと信号用の 1 本の D チャネルを提供します。

プロトコルごとの接続タイプ

MGCP ゲートウェイは次の接続タイプを提供します。

- TI/E1 PRI デジタル アクセス
- T1 CAS
- BRI
- FXO
- FXS

SCCP ゲートウェイは次の接続タイプを提供します。

- FXS
- BRI

SIP ゲートウェイは次の接続を提供します。

- FXS

- FXS-DID
- E&M
- BRI
- BRI QSIG
- T1 CAS
- T1 FGD
- E1 CAS
- T1/E1 PRI
- T1/E1 QSIG
- T1/E1 NFAS
- T1/E1 PRI（MegacomISDN）
- Centralized Automatic Message Accounting（CAMA）
- J1

H.323 ゲートウェイは次の接続タイプを提供します。

- FXS
- FXS-DID
- E&M
- BRI
- BRI QSIG
- T1 CAS
- T1 FGD
- E1 CAS
- T1/E1 PRI
- T1/E1 QSIG
- T1/E1 NFAS
- T1/E1 PRI（MegacomISDN）
- Centralized Automatic Message Accounting（CAMA）
- J1

ゲートウェイ設定の前提条件

ハードウェアのインストール

Cisco Unified Communications Manager にゲートウェイを設定する前に、ゲートウェイ ハードウェアに対して次の作業を行う必要があります。

- ゲートウェイのインストールと設定
- ゲートウェイに任意のベンダー インターフェイス カード（VIC）をインストールします。
- CLI を使用して、ゲートウェイの IOS を設定します。

詳細については、使用ゲートウェイに付属しているハードウェアとソフトウェアのマニュアルを参照してください。

（注） 多くのゲートウェイ デバイスの場合、デフォルトの Web ページは、そのゲートウェイの IP アドレスを使用して表示できます。ハイパーリンクの URL を http://x.x.x.x/ にします。ここで、x.x.x.x はデバイスのドット形式の IP アドレスです。各ゲートウェイの Web ページには、ゲートウェイのデバイス情報とリアルタイムのステータスが含まれています。

ゲートウェイの導入計画

Cisco Unified Communications Manager にゲートウェイを設定する前に、ゲートウェイに設定する接続のタイプを十分に考慮してください。多くのゲートウェイは、MGCP、SIP、H.323、または SCCP のいずれかをゲートウェイ プロトコルとして使用して設定できます。各導入タイプの接続タイプは、選択するプロトコルおよびゲートウェイにインストールされている VIC によって異なります。次の点を確認してください。

- 使用ゲートウェイでサポートされているゲートウェイ プロトコル。
- ゲートウェイの VIC でサポートされているポート接続のタイプ。
- 設定予定の接続のタイプ。
- アナログ接続の場合、PSTN、レガシー PBX、またはレガシー デバイスに接続しているか。
- デジタル アクセス接続の場合、T1 CAS インターフェイスまたは PRI インターフェイスに接続しているか。
- FXO 接続の場合、着信コールをどのように転送するか。着信コールを IVR や自動応答機能に転送しているか。

ゲートウェイの設定タスク フロー

ネットワークのゲートウェイを Cisco Unified Communications Manager に追加するには、次のタスクを実行します。

はじめる前に

ゲートウェイ設定の前提条件, （66 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Communications Manager でゲートウェイを設定します。導入するプロトコルに従って、次の手順のいずれかを実行します。 • MGCP ゲートウェイを設定, （68 ページ） • SCCP ゲートウェイの設定, （78 ページ） • SIP ゲートウェイの設定, （79 ページ） • H.323 ゲートウェイの設定, （82 ページ）	多数のシスコ製ゲートウェイは、MGCP、SCCP、SIP、または H.323 のいずれかをゲートウェイ プロトコルとして使用して導入できます。ゲートウェイがサポートするプロトコルの種類と、導入環境に最適なプロトコルを判断するにはゲートウェイのマニュアルを参照してください。 SCCP ゲートウェイが接続できるのは、アナログ アクセスまたは ISDN BRI 接続だけです。
ステップ 2	ゲートウェイに対するクラスタ全体のコール分類の設定, （83 ページ）	これはオプションです。自分のネットワークのゲートウェイのポートからコールが来ているとき、内部（OnNet）で、外部ゲートウェイでは外部（OffNet）と分類するためにクラスタ全体のサービス パラメータを設定します。 （注） 個々のゲートウェイ ポート インターフェイスに対するポート設定にあるコールの分類の設定はクラスタ全体の設定をオーバーライドします。ただし、ゲートウェイ ポートのデフォルト設定はクラスタ全体のサービス パラメータの設定を使用できます。
ステップ 3	OffNet ゲートウェイ転送のブロック, （83 ページ）	これはオプションです。Cisco Unified Communications Manager が外部（OffNet）ゲートウェイから別の外部ゲートウェイにコールを転送できないようにする場合、[OffNet から OffNet への転送をブロック（Block OffNet

	コマンドまたはアクション	目的
		to OffNet Transfer）] サービス パラメータを設定します。デフォルトでは、このサービス パラメータは、外部（OffNet）ゲートウェイから別のゲートウェイへの転送を許可するように設定されています。

MGCP ゲートウェイを設定

MGCP 設定を使用するためにシスコのゲートウェイを設定するには、次のタスクを実行します。

はじめる前に

ゲートウェイ設定の前提条件, （66 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	MGCP（IOS）ゲートウェイの設定, （69 ページ）	Cisco Unified CM の管理にゲートウェイを追加し、ゲートウェイ プロトコルとして [MGCP] を選択します。適切なスロットとベンダーのインターフェイス カード（VIC）でゲートウェイを設定します。
ステップ 2	ゲートウェイ ポートのインターフェイスを設定します。設定するインターフェイスのタイプによって、次の任意のタスクを選択します。 • デジタル アクセス PRI ポートの設定, （75 ページ） • MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ） • FXS ポートの設定, （70 ページ） • FXO ポートの設定, （71 ページ） • BRI ポートの設定, （76 ページ）	ゲートウェイにインストールされている VIC に接続するデバイスのポート接続を設定します。ほとんどの VIC には複数のポート接続とオプションがあります。したがって、いくつか別のポートのインターフェイス タイプを設定する必要がある場合があります。 **ヒント** ポートのインターフェイスを設定後、[関連リンク（Related Links）] ドロップダウン リスト ボックスで、[ゲートウェイの設定（Gateway Configuration）] ウィンドウに戻るために [MGCP 設定に戻る（Back to MGCP Configuration）] オプションを選択します。ここで、別のポート インターフェイスを選択して設定します。

	コマンドまたはアクション	目的
ステップ 3	MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加, （73 ページ）	これはオプションです。デジタルアクセスT1 CAS ポート インターフェイスを設定したら、ゲートウェイにT1 CAS ポートを追加します。個別にポートを追加したり、同時にポート範囲を追加したりできます。
ステップ 4	ゲートウェイのリセット, （77 ページ）	ゲートウェイをリセットすると、設定の変更が反映されます

関連トピック

コール ルーティングの概要, （145 ページ）

MGCP（IOS）ゲートウェイの設定

Cisco Unified Communications Manager に MGCP（IOS）ゲートウェイを追加し設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）]>[ゲートウェイ（Gateway）] 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 [ゲートウェイ タイプ（Gateway Type）] ドロップダウン リスト ボックスから、ゲートウェイを選択して、[次へ（Next）] をクリックします。

ステップ 4 [プロトコル（Protocol）] ドロップダウン リスト ボックスから、[MGCP（MGCP）] を選択し、[次へ（Next）] をクリックします。

ステップ 5 [設定済みスロット、VIC、エンドポイント（Configured Slots, VICs and Endpoints）] 領域で、次の手順を実行します。

a) それぞれの [モジュール（Module）] ドロップダウン リスト ボックスから、ゲートウェイにインストールされている Network Interface Module（NIM）ハードウェアに対応するスロットを選択します。

b) それぞれの [サブユニット（Subunit）] ドロップダウン リスト ボックスから、ゲートウェイにインストールされている VIC を選択します。

c) [保存（Save）] をクリックします。

ポートのアイコンが表示されます。各ポートのアイコンは、ゲートウェイで使用可能なポートインターフェイスに対応します。ポートインターフェイスを設定するには、該当するポートのアイコンをクリックします。

ステップ 6 [ゲートウェイの設定（Gateway Configuration）] ウィンドウでその他のフィールドを設定します。フィールドの詳細については、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次の作業

ゲートウェイのポート インターフェイスの設定

- FXS ポートの設定, （70 ページ）
- FXO ポートの設定, （71 ページ）
- デジタル アクセス PRI ポートの設定, （75 ページ）
- MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ）
- BRI ポートの設定, （76 ページ）

FXS ポートの設定

MGCP ゲートウェイで Foreign Exchange Station（FXS）のポートを設定します。単純な旧式の電話サービス（POTS）のレガシー電話機、または FAX、スピーカーフォン、従来のボイスメッセージング システム、IVR などのレガシー デバイスにゲートウェイを接続するために FXS ポートを使用できます。

はじめる前に

ポートを設定する前に、ゲートウェイを追加する必要があります。

手順

ステップ 1 Cisco Unified CM の管理で、[デバイス（Device）] > [ゲートウェイ（Gateway）] を選択します。

ステップ 2 [検索（Find）] をクリックして、FXS ポートを設定するゲートウェイを選択します。

ステップ 3 [設定済みスロット、VIC、エンドポイント（Configured Slots, VICs, and Endpoints）] エリアで、設定するポートに対する FXS ポート アイコンをクリックします。
[ポートの選択（Port Selection）] エリアが表示されます。

ステップ 4 [ポート タイプ（Port Type）] ドロップダウン リスト ボックスから、設定する接続のタイプを選択します。

- [POTS]：従来の電話機などの POTS デバイスにこのポートを接続するには、このオプションを選択します。

- [グラウンド スタート（Ground Start）]：FAX、従来のボイスメッセージング システム、IVR など無人のレガシー デバイスにこのポートを接続するためにグラウンド スタート シグナリングを使用するには、このオプションを選択します。
- [ループ スタート（Loop Start）]：FAX、従来のボイスメッセージング システム、IVR など無人のレガシー デバイスにこのポートを接続するためにループ スタート シグナリングを使用するには、このオプションを選択します。

ステップ 5 [Next] をクリックします。
[ポートの設定（Port Configuration）] ウィンドウは、デバイス プロトコルとしてアナログ アクセスに対するポート インターフェイスの設定を表示します。

ステップ 6 [デバイス プール（Device Pool）] ドロップダウン リスト ボックスから、デバイス プールを選択します。

ステップ 7 [ポートの設定（Port Configuration）] ウィンドウでその他のフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 これはオプションです。MGCP IOS ゲートウェイで追加のポート インターフェイスを設定するには、[関連リンク（Related Links）] ドロップダウン リスト ボックスから [ゲートウェイに戻る（Back to Gateway）] を選択し、[Go（Go）] をクリックします。
[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイで使用可能なポートが表示されます。

次の作業

追加のポートを設定する場合：

- FXO ポートの設定, （71 ページ）
- デジタル アクセス PRI ポートの設定, （75 ページ）
- MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ）
- BRI ポートの設定, （76 ページ）

ポートの設定が完了している場合：

- ゲートウェイのリセット, （77 ページ）

FXO ポートの設定

MGCP（IOS）ゲートウェイの Foreign Exchange Office (FXO) を設定します。FXO ポートを使用して、ゲートウェイを PSTN またはレガシー PBX に接続できます。

（注） Cisco Unified Communications Manager では、ループスタート トランクに確実な接続解除監視がないことを前提としています。 グラウンド スタートとして、確実な接続解除監視を使用して設定するため、サーバがフェールオーバしても、アクティブ コールが保持されます。

はじめる前に

MGCP（IOS）ゲートウェイの設定, （69 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [ゲートウェイ（Gateway）] を選択します。

ステップ 2 [Find（検索）] をクリックして、FXO ポートを設定するゲートウェイを選択します。

ステップ 3 [設定済のスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、FXO ポートインターフェイスを設定する FXO ポートを含む [モジュール（Module）] と [サブユニット（Subunit）] を指定し、設定するポートのポート アイコンをクリックします。

ステップ 4 [ポート タイプ（Port Type）] ドロップダウンリストから、[グラウンドスタート（Ground-Start）] または [ループスタート（Loop-Start）] を選択します。

（注） VIC-2 FXO ポートを設定している場合は、サブユニット モジュールの両方のポートに同じポート タイプを選択する必要があります。

ステップ 5 [デバイス プール（Device Pool）] ドロップダウン リスト ボックスから、デバイス プールを選択します。

ステップ 6 [アテンダントDN（Attendant DN）]ボックスに、このポート接続からのすべての着信コールをルーティングする電話番号を入力します。たとえば、ゼロまたは担当者の電話番号です。

ステップ 7 [ポートの設定（Port Configuration）] ウィンドウの他のフィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 これはオプションです。MGCP IOS ゲートウェイで追加のポート インターフェイスを設定するには、[関連リンク（Related Links）] ドロップダウン リスト ボックスから [ゲートウェイに戻る（Back to Gateway）] を選択し、[Go（Go）] をクリックします。
[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイで使用可能なポートが表示されます。

次の作業

追加のポートを設定する場合：

- FXS ポートの設定, （70 ページ）
- FXO ポートの設定, （71 ページ）
- デジタル アクセス PRI ポートの設定, （75 ページ）

- MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ）
- BRI ポートの設定, （76 ページ）

ポートの設定が完了している場合：

- ゲートウェイのリセット, （77 ページ）

MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定

MGCP （IOS）ゲートウェイでデジタル アクセス T1 CAS ポートのポート インターフェイスを設定します。

はじめる前に

MGCP（IOS）ゲートウェイの設定, （69 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）]>[ゲートウェイ（Gateway）] を選択します。

ステップ 2 [検索（Find）] をクリックして、T1 ポートを設定するゲートウェイを選択します。

ステップ 3 [設定済みスロット、VIC、エンドポイント（Configured Slots, VICs and Endpoints）] 領域で、デジタルアクセスT1（T1-CAS）ポートを設定するモジュールとサブユニットを見つけ、該当するポート アイコンをクリックします。

ステップ 4 [デバイス プロトコル（Device Protocol）] ドロップダウン リスト ボックスから、[デジタル アクセス T1（Digital Access T1）] を選択し、[次へ（Next）] をクリックします。

ステップ 5 適切なゲートウェイ設定を入力します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

次の作業

デジタル アクセス T1 CAS ポート インターフェイスにポートを追加します。

- MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加, （73 ページ）

MGCP ゲートウェイでのデジタル アクセス *T1* ポートの追加

MGCP ゲートウェイで、T1 CAS ポートを T1 デジタル アクセス ポート インターフェイスに追加および設定します。最大 24 の T1 CAS ポートを追加および設定できます。個別に、または特定のポート範囲で同時に、ポートの追加および設定ができます。特定のポート範囲を入力すると、Cisco Unified Communications Manager が、その設定をそのポート範囲全体に適用します。

はじめる前に

MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[デバイス（Device）] > [ゲートウェイ（Gateway）] を選択します。

ステップ 2 [検索（Find）] をクリックし、T1 CAS ポート インターフェイスを含むゲートウェイを選択します。

ステップ 3 [新規ポートの追加（Add a New Port）] をクリックします。

ステップ 4 [ポート タイプ（Port Type）] ドロップダウン リスト ボックスから、追加するポートのタイプを選択して、[次へ（Next）] をクリックします。

ステップ 5 [開始ポート番号（Beginning Port Number）] と [終了ポート番号（Ending Port Number）] フィールドにポート番号を入力し、追加と設定を行うポート範囲を指定します。たとえば、1 から 10 のポートを、ポート インターフェイスに同時に追加するには、1 と 10 を入力します。

ステップ 6 [通信の方向（Port Direction）] ドロップダウン リスト ボックスから、このポートを通過するコールの方向を設定します。

- [双方（Bothways）]：発着信コールの両方を許可する場合、このオプションを選択します。
- [インバウンド（Inbound）]：着信コールのみを許可する場合、このオプションを選択します。
- [アウトバウンド（Outbound）]：アウトバウンド コールのみを許可する場合、このオプションを選択します。

ステップ 7 EANDM ポートの場合、[発信者選択（Calling Party Selection）] ドロップダウン リスト ボックスから、このポートに接続されているデバイスからのアウトバウンド コールの発信者番号をどのように表示させるかを選択します。

- [発信元（Originator）]：発信側デバイスの電話番号を送信します。
- [最初のリダイレクト番号（First Redirect Number）]：リダイレクト側デバイスの電話番号を送信します。
- [最後のリダイレクト番号（Last Redirect Number）]：コールをリダイレクトする最後のデバイスの電話番号を送信します。
- [最初のリダイレクト番号（外線）（First Redirect Number (External)）]：外部電話マスクが適用されている、リダイレクトを行う最初のデバイスの電話番号を送信します。
- [最後のリダイレクト番号（外線）（First Redirect Number (External)）]：外部電話マスクが適用されている、リダイレクトを行う最後のデバイスの電話番号を送信します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 これはオプションです。MGCP ゲートウェイに追加のポートを設定するには、[関連リンク（Related Links）] から、[ゲートウェイに戻る（Back to Gateway）] を選択し、[移動（Go）] をクリックします。デジタル アクセス T1 ポート インターフェイスが表示されたら、次のいずれかの手順を実行します。

- このポート インターフェイスに、デジタル アクセス T1 CAS ポートをさらに追加するには、この手順のステップ 3 に戻ります。
- ゲートウェイで追加のポート インターフェイスを設定するには、[関連リンク（Related Links）] から、[MGCP の設定に戻る（Back to MGCP Configuration）] を選択し、[移動（Go）] をクリックします。[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイのサブユニット モジュールで使用可能なポートが表示されます。

次の作業

ゲートウェイで追加のポート インターフェイスを設定する場合：

- FXS ポートの設定, （70 ページ）
- FXO ポートの設定, （71 ページ）
- MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ）
- デジタル アクセス PRI ポートの設定, （75 ページ）
- BRI ポートの設定, （76 ページ）

ポートの設定を完了した場合：

- ゲートウェイのリセット, （77 ページ）

デジタル アクセス PRI ポートの設定

MGCP (IOS) ゲートウェイの PRI ポート インターフェイスを設定します。

はじめる前に

MGCP（IOS）ゲートウェイの設定, （69 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [ゲートウェイ（Gateway）] を選択します。

ステップ 2 [検索（Find）] をクリックし、PRI ポートを設定するゲートウェイを選択します。

ステップ 3 [設定済のスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、設定する BRI ポートを含むモジュールおよびサブユニットを指定し、設定する BRI ポートに対応するポート アイコンをクリックします。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、BRI ポート インターフェイスが表示されます。

ステップ 4 [デバイス プール（Device Pool）] ドロップダウン リスト ボックスから、デバイス プールを選択します。

ステップ 5 [ゲートウェイの設定（Gateway Configuration）] ウィンドウで、その他のフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 これはオプションです。ゲートウェイで追加のポートインターフェイスを設定するには、[関連リンク（Related Links）] ドロップダウン リスト ボックスから、[MGCP設定に戻る（Back to MGCP Configuration）] を選択し、[Go（Go）] をクリックします。
[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、ゲートウェイで使用可能なポートインターフェイスが表示されます。

次の作業

追加のポート インターフェイスを設定する場合：

- FXS ポートの設定, （70 ページ）
  - FXO ポートの設定, （71 ページ）
- MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ）
- BRI ポートの設定, （76 ページ）

ポートの設定が完了している場合：

- ゲートウェイのリセット, （77 ページ）

BRI ポートの設定

MGCP（IOS）ゲートウェイの BRI ポート インターフェイスを設定します。

はじめる前に

MGCP（IOS）ゲートウェイの設定, （69 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [ゲートウェイ（Gateway）] を選択します。

ステップ 2 [検索（Find）] をクリックして、BRI ポートを設定するゲートウェイを選択します。

ステップ 3 [設定済みスロット、VIC、エンドポイント（Configured Slots, VICs and Endpoints）] セクションで、BRI ポートを使用するサブユニットを検索し、設定するポートのポート アイコンをクリックします。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウに BRI ポート インターフェイスの情報が表示されます。

ステップ 4 [デバイス プール（Device Pool）] ドロップダウン リスト ボックスから、デバイス プールを選択します。

ステップ 5 適切なゲートウェイおよびポートの設定情報を入力します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 これはオプションです。ゲートウェイで追加のポートインターフェイスを設定するには、[関連リンク（Related Links）] ドロップダウン リスト ボックスから [MGCP 設定に戻る（Back to MGCP Configuration）] を選択し、[移動（Go）] をクリックします。
[ゲートウェイの設定（Gateway Configuration）] ウィンドウに、MGCP ゲートウェイに使用可能なポート インターフェイスが表示されます。

次の作業

ゲートウェイの追加ポートを設定するには、次の手順を実行します:

- FXS ポートの設定, （70 ページ）
- FXO ポートの設定, （71 ページ）
- MGCP ゲートウェイ用デジタル アクセス T1 ポートの設定, （73 ページ）
- デジタル アクセス PRI ポートの設定, （75 ページ）

ポートの設定が完了した場合：

- ゲートウェイのリセット, （77 ページ）

ゲートウェイのリセット

ほとんどのゲートウェイは、設定の変更が適用されるようにリセットする必要があります。リセットを行う前に、必要なゲートウェイ設定をすべて完了することをお勧めします。

（注） H.323 ゲートウェイをリセットしても Cisco Unified Communications Manager が読み込んだ設定を再初期化するだけで、ゲートウェイを物理的に再起動したり、リセットしたりはしません。

手順

ステップ 1 Cisco Unified CM の管理から、[Device] > [Gateway] を選択します。

ステップ 2 [検索（Find）] をクリックして、ゲートウェイを選択します。

ステップ 3 リセットするゲートウェイの横のチェック ボックスをクリックして、[リセット選択済み（Reset Selected）] をクリックします。[デバイス リセット（Device Reset）] ダイアログ ボックスが表示されます。次のいずれか 1 つの処理を実行します。

ステップ 4 [リセット（Reset）] をクリックします。

SCCP ゲートウェイの設定

SCCP として ゲートウェイ プロトコルを使用するようにシスコのゲートウェイを設定します。この導入オプションは、FXS ポートまたは BRI ポートを使用して、アナログ アクセス デバイスと ISDN BRI のデバイスに Cisco Unified Communications Manager を接続するために使用できます。SCCP ゲートウェイをデジタル アクセスの T1 トランクまたは E1 トランクに接続することはできません。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [ゲートウェイ（Gateway）] 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 [ゲートウェイ タイプ（Gateway Type）] ドロップダウン リスト ボックスで、SCCP を使用するゲートウェイを選択し、[次へ（Next）] をクリックします。

ステップ 4 [プロトコル（Protocol）] ドロップダウン リスト ボックスで、[SCCP（SCCP）] を選択します。

ステップ 5 [設定済のスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）] 領域で、次の手順を実行します。

a) 各 [モジュール（Module）] ドロップダウン リスト ボックスで、ゲートウェイにインストールされているネットワーク インターフェイスのモジュール ハードウェアに対応するスロットを選択します。

b) 各 [サブユニット（Subunit）] で、ゲートウェイにインストールされている VIC を選択します。

ステップ 6 [ゲートウェイの設定（Gateway Configuration）] ウィンドウで、その他のフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 7 [Save] をクリックします。
ポートのアイコンが、サブユニット モジュールの横に表示されます。各ポートのアイコンは、ゲートウェイで設定可能なポートのインターフェイスに対応します。該当するポートのアイコンをクリックして、ポートのアナログ アクセスまたは ISDN BRI 電話を設定できます。

ステップ 8 アップデートが完了したら、次の手順を実行して、ゲートウェイの変更を適用します。

a) [ゲートウェイのリセット（Reset Gateway）] をクリックします。[ゲートウェイの再起動（Restart Gateway）] のポップアップが表示されます。
b) [リセット（Reset）] をクリックします。

次の作業

関連トピック

コール ルーティングの設定, （145 ページ）
アナログ アクセス電話の設定
ISDN BRI 電話の設定

SIP ゲートウェイの設定

Cisco Unified Communications Manager で SIP ゲートウェイを設定するには、次のタスクを実行します。シスコのゲートウェイやサードパーティのゲートウェイの多くは、SIP を使用して設定できます。Cisco Unified Communications Manager には、SIP ゲートウェイ用のゲートウェイ デバイス タイプは含まれないことに注意してください。

はじめる前に

Cisco Unified Communications Manager でゲートウェイを追加する前に、ネットワークにゲートウェイのハードウェアをインストールし、ゲートウェイの IOS ソフトウェアを設定する必要があります。詳細については、ゲートウェイの前提条件を参照してください。

- ゲートウェイ設定の前提条件, （66 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイルの設定, （80 ページ）	SIP を設定し、SIP ゲートウェイに接続するトランクによって使用される SIP プロファイルに適用します。
ステップ 2	SIP トランク セキュリティ プロファイルの設定, （80 ページ）	SIP ゲートウェイに接続するトランクによって使用される SIP トランク セキュリティプロファイルを設定します。デバイスのセキュリティ モード、ダイジェスト認証、着信転送タイプや発信転送タイプの設定などのセキュリティ設定が行えます。
ステップ 3	SIP ゲートウェイに対する SIP トランクの設定, （81 ページ）	SIP ゲートウェイを指し示す SIP トランクを設定します。SIP プロファイルと SIP トランク セキュリティプロファイルを SIP トランクに適用します。

関連トピック

コール ルーティングの設定, （145 ページ）

SIP プロファイルの設定

SIP ゲートウェイ接続の SIP プロファイルを設定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [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 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。
- 既存のプロファイルを選択するには、[検索（Find）] をクリックして SIP プロファイルを選択します。

ステップ 3 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウの各フィールドを設定します。フィールドを含むヘルプは、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

SIP トランク セキュリティ プロファイルの設定, （80 ページ）

SIP トランク セキュリティ プロファイルの設定

SIP ゲートウェイに接続するトランクのセキュリティ設定を含む SIP トランク セキュリティプロファイルを設定します。

はじめる前に

SIP プロファイルの設定, （80 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティプロファイル（SIP Trunk Security Profile）] を選択します。

ステップ 2 次のいずれかの手順を実行します。

a) 既存のプロファイルを選択するには、[検索（Find）] をクリックし、既存のプロファイルを選択します。

b) 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。

ステップ 3 [SIP トランク セキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウの各フィールドに入力します。フィールドの詳細説明については、オンライン ヘルプを参照してください。

ステップ 4 [Save] をクリックします。

次の作業

SIP ゲートウェイに対する SIP トランクの設定, （81 ページ）

SIP ゲートウェイに対する SIP トランクの設定

SIP を使用する Cisco またはサード パーティ製のゲートウェイに Cisco Unified Communications Manager を接続するために SIP トランクを設定します。この設定では、[ゲートウェイの設定（Gateway Configuration）] ウィンドウでデバイスとしてゲートウェイを入力する必要がなくなります。

はじめる前に

SIP トランク セキュリティ プロファイルの設定, （80 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [トランク（Trunk）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックして、新しい SIP トランクを設定します。

ステップ 3 [トランク タイプ（Trunk Type）] ドロップダウン リスト ボックスから [SIP トランク（SIP Trunk）] を選択します。

ステップ 4 [プロトコル（Protocol）] ドロップダウン リスト ボックスから [なし（None）] を選択します。

ステップ 5 [SIP 情報（SIP Information）] ペインの [宛先アドレス（Destination Address）] フィールドに、SIP ゲートウェイの IP アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

ステップ 6 [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] ドロップダウン リスト ボックスから、このゲートウェイに設定した SIP トランク セキュリティ プロファイルを選択します。

ステップ 7 [SIP プロファイル（SIP Profile）] ドロップダウン リスト ボックスから、このゲートウェイに設定した SIP プロファイルを選択します。

ステップ 8 [SIP トランク設定（SIP Trunk Configuration）] ウィンドウで各フィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

コール ルーティングの設定, （145 ページ）

H.323 ゲートウェイの設定

Cisco Unified Communications Manager で H.323 ゲートウェイを設定して、ゲートキーパー非制御の H.323 を導入します。

（注） H.323 ゲートキーパーを導入しない場合は、ゲートキーパー制御の H.225 トランクをセットアップして、H.323 ゲートウェイを追加することもできます。ゲートキーパーの使用率は、近年減少傾向にあるため、このシナリオは本書には記載していません。ゲートキーパーおよび H.225 ゲートキーパー制御のトランクを設定するには、『*Cisco Unified Communications Manager* アドミニストレーション ガイド リリース *10.0(1)*』を参照してください。

（注） ゲートウェイが Cisco Unified Communications Manager で登録されている場合、ゲートウェイの登録ステータスは、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] に不明として表示される場合があります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [ゲートウェイ（Gateway）] 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 [ゲートウェイ タイプ（Gateway Type）] ドロップダウン リスト ボックスから、H.323 ゲートウェイ を選択します。

ステップ 4 [デバイス名（Device Name）] フィールドに、ゲートウェイの IP アドレスまたはホスト名を入力します。

ステップ 5 H.235 を使用してセキュア チャネルを設定するには、[H.235 データのパススルー（H.235 Data Passthrough）] チェックボックスをオンにします。

ステップ 6 [ゲートウェイの設定（Gateway Configuration）] ウィンドウのフィールドを設定します。
フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 [リセット（Reset）] をクリックしてゲートウェイをリセットし、変更を適用します。
ほとんどのゲートウェイでは、設定の変更を適用するためにリセットする必要があります。必要なすべてのゲートウェイを設定してからリセットを実行することを推奨します。

関連トピック

コール ルーティングの設定, （145 ページ）

ゲートウェイに対するクラスタ全体のコール分類の設定

ネットワーク ゲートウェイの [コールの分類（Call Classification）] を設定します。この設定は、システムがネットワークでゲートウェイが内部（OnNet）、または外部（OffNet）であると見なすかどうかを決定します。

[コールの分類（Call Classification）] フィールドが、個々のゲートウェイ ポート インターフェイスの設定ウィンドウに表示されます。デフォルトでは、各ゲートウェイ ポートインターフェイスはクラスタ全体のサービス パラメータの設定を使用するように設定されています。ただし、ポートの [コールの分類（Call Classification）] がクラスタ全体のサービス パラメータと異なる設定である場合、そのポートの設定がサービス パラメータ設定をオーバーライドします。

手順

ステップ 1 Cisco Unified CM の管理から、[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 [サーバ（Server）] ドロップダウン リストボックスから、Cisco CallManager サービスが動作しているサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストボックスから、[Cisco CallManager （Cisco CallManager ）]を選択します。

ステップ 4 [クラスタ全体のパラメータ（デバイス - 概要）（Clusterwide Parameters (Device - General)）] で、[コールの分類（Call Classification）] サービス パラメータに次の値のいずれかを設定します。

- [OnNet（OnNet）] — このゲートウェイからのコールが、企業ネットワーク内から発信されているものと分類されます。
- [OffNet（OffNet）] — このゲートウェイからのコールが、企業ネットワーク外から発信されているものと分類されます。

ステップ 5 [保存（Save）] をクリックします。

次の作業

OffNet ゲートウェイ転送のブロック, （83 ページ）

OffNet ゲートウェイ転送のブロック

この手順は、ある外部（OffNet）ゲートウェイから別の外部（OffNet）ゲートウェイに転送されるコールをブロックするようにシステムを設定する場合に使用します。デフォルトでは、ある外部ゲートウェイから別の外部ゲートウェイへの転送は許可されます。

ゲートウェイが外部（OffNet）であるか内線（OnNet）であるかどうかを判別する設定は、コール分類設定によって決定されます。このフィールドはクラスタ全体のサービス パラメータを使用するか、または、次のポート インターフェイスのいずれかを設定することで、設定できます。

- MGCP T1/E1 ポート インターフェイス
- MGCP FXO ポート インターフェイス
- H.323 ゲートウェイ
- SIP トランク

はじめる前に

ゲートウェイに対するクラスタ全体のコール分類の設定, （83 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）]>[サービス パラメータ（Service Parameters）] の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストボックスから、Cisco CallManager サービスが動作しているサーバを選択します。

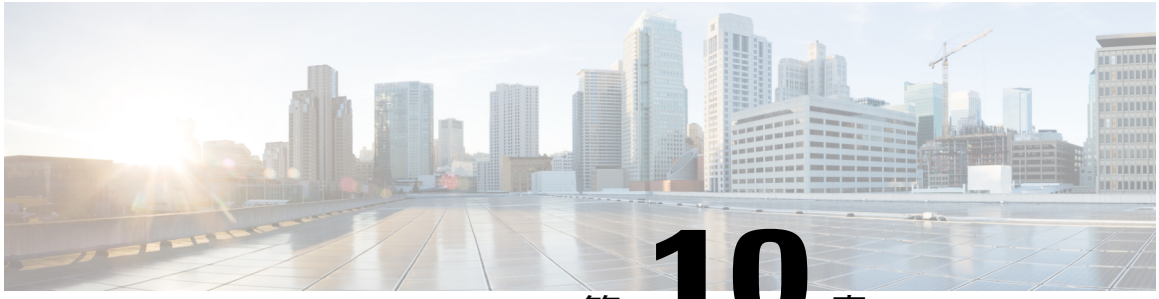
ステップ 3 [サービス（Service）] ドロップダウン リスト ボックスから、[Cisco CallManager] を選択します。

ステップ 4 [OffNet から OffNet への転送をブロック（Block OffNet to Offnet Transfer）] サービス パラメータを設定します。

- [True]：2 つの外部（OffNet）ゲートウェイ間の転送を無効にするには、このオプションを選択します。
- [False]：2 つの外部（OffNet）ゲートウェイ間の転送を許可するには、このオプションを選択します。これがデフォルトのオプションです。

ステップ 5 [保存（Save）] をクリックします。

（注） また、ゲートウェイをルート パターンに関連付け、[ルート パターンの設定（Route Pattern Configuration）] ウィンドウで [コールの分類（Call Classification）] を設定することで、ゲートウェイを介してコールを OnNet または OffNet として分類することもできます。



第 10 章

SIP の正規化および透明性の設定

- SIP の正規化および透明性の概要，85 ページ
- SIP の正規化および透明性の前提条件，86 ページ
- SIP の正規化および透明性設定のタスク フロー，87 ページ

SIP の正規化および透明性の概要

SIP の正規化と透明性は、Cisco Unified Communications Manager と、SIP を別の仕方で実装するエンドポイント、サービス プロバイダー、PBX、ゲートウェイとの間の SIP 相互運用性の問題を扱う、オプションの機能です。SIP の正規化と透明性を設定するには、SIP トランクまたは SIP 回線に対して、カスタマイズされた Lua スクリプトを適用します。Cisco Unified Communications Manager は、SIP トランクまたは SIP 回線を介して伝送される SIP メッセージにこのスクリプトを適用します。

インストール時に、Cisco Unified Communications Manager には、システムの SIP トランクと SIP プロファイルに割り当てられる、デフォルトの正規化と透明性スクリプトが含まれています。また、独自のカスタマイズされたスクリプトを作成し、インポートできます。

SIP の正規化

SIP の正規化スクリプトは、着信および発信 SIP メッセージを変更します。たとえば、Cisco TelePresence Video Communication Server で Cisco Unified Communications Manager を相互運用していたら、その 2 つを接続する *vcs-interop* スクリプトを適用します。このスクリプトは、2 つの製品が通信できるように SIP メッセージの違いを解決します。

正規化スクリプトは、どの SIP トランク接続にも適用できます。SIP トランクを結合するエンドポイントで使用されているプロトコルには関係ありません。

SIP の透明性

SIP 透明性スクリプトを使用すると、Cisco Unified Communications Manager は独自のヘッダーや 1 つのコール レッグから他への SIP 情報を透過的に渡します。透明性が有効になるには、両方のコール レッグが SIP である必要があります。

SIP の透明性のもう 1 つの特徴は REFER 透明性です。これは、REFER 要求に作用することなく、Cisco Unified Communications Manager が REFER要求を渡すことを可能にします。REFER 透明性をコールセンター環境で使用できます。コールセンターでは、中央集中型エージェントがコールに応答すると、その発信者と同じ地理的領域にいるエージェントにコールを転送します。REFER 透明性により、中央集中型の Cisco Unified Communications Manager はそのコールを除外し、コール制御を新しいエージェントに移します。

SIP の正規化と透明性のデフォルト スクリプト

インストール時に、Cisco Unified Communications Manager には、SIP の正規化と透明性に対応する次のデフォルト スクリプトが含まれます。これらのスクリプトは SIP トランクまたは SIP プロファイルに適用できますが、これらのスクリプトを編集することはできません。

- HCS-PCV-PAI passthrough：エンタープライズ IMS と Cisco HCS プラットフォームとの統合を提供します。
- cisco-telepresence-conductor-interop：TelePresence Conductor に登録されたエンドポイントの相互運用性を提供します。
- cisco-telepresence-mcu-ts-direct-interop：Cisco Unified Communications Manager と Cisco TelePresence MCU または Cisco TelePresence Server のいずれかとの間に相互運用性を提供します。
- diversion-counter：転送カウンタを調整するための機能を提供します。
- refer-passthrough：SIP トランク間のブラインド転送に起因してコールから Cisco Unified Communications Manager を削除します。
- vcs-interop：Cisco TelePresence Video Communications Server に登録されているエンドポイントの相互運用性を提供します。

SIP の正規化および透明性の前提条件

SIP の正規化と透明性を設定する前に、次の前提条件を確認してください。

- 導入しようとしている SIP デバイスが SIP を実装している方法を理解していることを確認します。たとえば、Cisco Unified Communications Manager を Cisco TelePresence Video Communication Server と相互運用しているときは、その 2 つの製品を接続する SIP トランクに vcs-interop スクリプトを適用する必要があります。
- デフォルトのスクリプトを確認し、ニーズを満たすことを確認します。詳細は、SIP の正規化と透明性のデフォルト スクリプト，（86 ページ）を参照してください。
- Cisco Unified Communications Manager をサードパーティの SIP 製品と相互運用する計画がある場合は、カスタム スクリプトを作成する必要があるかどうかを判断できるように、サードパーティの製品が SIP を実装している方法を十分理解しておいてください。
- 独自のカスタム スクリプトを開発するつもりであれば、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/

products-programming-reference-guides-list.html の、「*Developer Guide for SIP Normalization and Transparency*」を確認します。

SIP の正規化および透明性設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	新しい SIP の正規化および透明性透明性スクリプトの作成, （87 ページ）	これはオプションです。事前インストール済みスクリプトのいずれもニーズを満たしていない場合は、次の手順を使用して、カスタマイズされたスクリプトを設定します。[SIP 正規化スクリプトの設定（SIP Normalization Script Configuration）] ウィンドウで新しいスクリプトを作成するか、またはカスタマイズされたスクリプトをインポートできます。
ステップ 2	SIP トランクに正規化または透明性スクリプトを適用, （88 ページ）	[トランクの設定（Trunk Configuration）] ウィンドウで、SIP トランクにスクリプトを直接適用します。Cisco Unified Communications Manager は、トランクを通過するすべての SIP メッセージングにスクリプトを適用します。
ステップ 3	正規化または透明性スクリプトの SIP 回線への適用, （89 ページ）	SIP 回線に正規化スクリプトまたは透明性スクリプトを適用する場合は、その SIP 回線に関連付けられている SIP プロファイルにスクリプトを適用します。Cisco Unified Communications Manager は、その SIP プロファイルを使用するすべての SIP メッセージングにスクリプトを適用します。

新しい SIP の正規化および透明性透明性スクリプトの作成

デフォルトの正規化と透明性スクリプトが要望を満たさない場合は、次の手順を使用して新しい LUA スクリプトを作成します。Cisco Unified Communications Manager で新しいスクリプトを作成するか、またはシステムにファイルをインポートします。

ヒント　ユーザが作成するスクリプトがデフォルトのスクリプトに類似していたら、[SIP 正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウでデフォルト スクリプトを開き、[コンテンツ（Contents）] テキスト ボックスをコピーします。新しいスクリプトを作成して、その内容を [コンテンツ（Contents）] テキスト ボックスに貼り付けます。これで、新しいスクリプトの内容を編集できます。

手順

ステップ 1　[Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP 正規化スクリプト（SIP Normalization Script）] 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。
[SIP 正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウが表示されます。

ステップ 3　スクリプトの [名前（Name）] と [説明（Description）] を入力します。

ステップ 4　新しいスクリプトを作成している場合は、[コンテンツ（Contents）] テキストボックスのスクリプトを編集します。

ステップ 5　これはオプションです。インポートする外部ファイルがあれば、次の手順を実行します

a) [ファイルのインポート（Import File）] をクリックします。
b) [参照（Browse）] してファイルを見つけ、選択します。
c) [ファイルのインポート（Import File）] をクリックします。
[SIP 正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウに、[コンテンツ（Contents）] テキスト ボックスにインポートしたファイルの内容が表示されます。

ステップ 6　[SIP正規化スクリプト設定（SIP Normalization Script Configuration）] ウィンドウのフィールドを完成します。フィールドとその内容のヘルプは、オンライン ヘルプを参照してください。

ステップ 7　[保存（Save）] をクリックします。

次の作業

スクリプトを SIP プロファイルまたは SIP トランクに指定します。

- SIP トランクに正規化または透明性スクリプトを適用，（88 ページ）
- 正規化または透明性スクリプトの SIP 回線への適用，（89 ページ）

SIP トランクに正規化または透明性スクリプトを適用

SIP トランクに SIP の正規化または透明性スクリプトを適用するには、次の手順を使用します。Cisco Unified Communications Manager は、トランクを通過する SIP メッセージにスクリプトを適用します。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [トランク（Trunk）] を選択します。

ステップ 2 [検索（Find）] をクリックして、 スクリプトを適用するトランクを選択します。

ステップ 3 [正規化スクリプト（Normalization Script）] ドロップダウン リスト ボックスから、トランクに適用するスクリプトを選択します。

ステップ 4 これはオプションです。SIP メッセージング内の特定のパラメータを正規化するには、次の手順を実行します。

a) 正規化する [パラメータ名（Parameter Name）] および、パラメータに適用する値を [パラメータ値（Parameter Value）] に入力します。たとえば、パラメータ名として場所、パラメータ値としてノースカロライナと入力できます。

b) そのほかのパラメータを追加するには、[（+）] ボタンをクリックし、追加のパラメータと値を入力する行を作成します。

ステップ 5 これはオプションです。スクリプトに SDI トレースを実行するには、[トレースを有効化（Enable Trace）] チェックボックスをオンにします。

（注） スクリプトをデバッグする時には、トレースを有効化することを推奨します。

ステップ 6 [保存（Save）] をクリックします。

正規化または透明性スクリプトの SIP 回線への適用

正規化または透明性スクリプトを SIP 回線に適用するには、その SIP 回線で使用する SIP プロファイルにスクリプトを適用します。Cisco Unified Communications Manager は、そのスクリプトを、その SIP プロファイルを使用するすべての SIP メッセージングに適用します。

手順

ステップ 1 Cisco Unified CM の管理から、[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 [検索（Find）] をクリックして、スクリプトを適用する SIP プロファイルを選択します。

ステップ 3 [正規化スクリプト（Normalization Script）] ドロップダウン リスト ボックスから、トランクに適用するスクリプトを選択します。

ステップ 4 これはオプションです。SIP メッセージング内の特定のパラメータを正規化するには、次の手順を実行します。

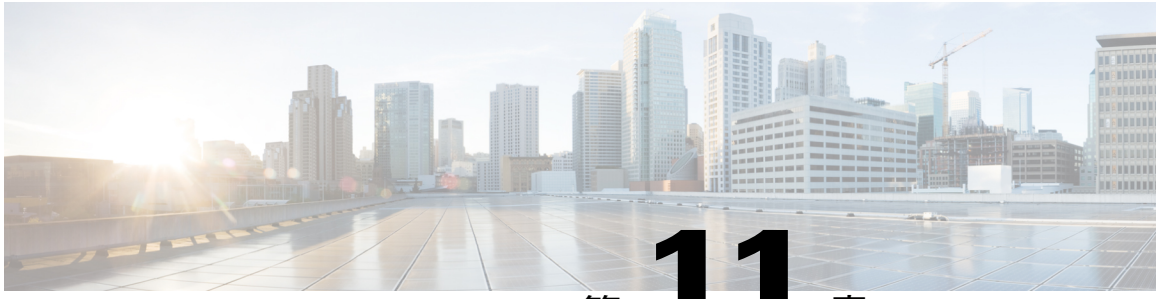
a) 正規化する [パラメータ名（Parameter Name）] および、パラメータに適用する値を [パラメータ値（Parameter Value）] に入力します。たとえば、パラメータ名として場所、パラメータ値としてノースカロライナと入力できます。

b) そのほかのパラメータを追加するには、[（+）] ボタンをクリックし、追加のパラメータと値を入力する行を作成します。

ステップ 5 これはオプションです。スクリプトに SDI トレースを実行するには、[トレースを有効化（Enable Trace）] チェックボックスをオンにします。

（注） スクリプトをデバッグする時には、トレースを有効化することを推奨します。

ステップ 6 [保存（Save）] をクリックします。



第 11 章

SDP 透明性プロファイルの設定

- SDP 透明性プロファイルの概要，91 ページ
- SDPの透明性プロファイルの制限事項，92 ページ
- SDP 透明性プロファイルの前提条件，92 ページ
- SDP 透明性プロファイルの設定，92 ページ

SDP 透明性プロファイルの概要

SDP 透明性プロファイルには、システムが Cisco Unified Communications Manager によってネイティブでサポートされていない宣言的属性を入力コール レッグから出力コール レッグにパス スルーできるようにする宣言的SDP 属性のルールセットが含まれています。SDP透明性プロファイルがないと、Cisco Unified Communications Manager はサポートされていな SDP 属性をドロップします。

SDP 透明性プロファイルに複数のルールを設定し、それらを SIP プロファイルを介して SIP デバイスまたはトランクに適用できます。SDP 透明性プロファイルを適用するには、両方のコール レッグが SIP である必要があります。次のタイプの SDP 属性ルールを設定できます。

- プロパティ：ルールがプロパティ属性に対して設定されると、Cisco Unified Communications Manager は、属性に値がある場合を除き、SDP 属性をパス スルーします。
- 任意の値：ルールが任意の値に対して設定されると、値が 1 つ以上の空白以外の文字で構成されている限り、SDP 属性はパス スルーされます。
- リストからの値：ルールがこのオプションを使用して設定されると、値が指定された値のいずれかに一致する限り、SDP 属性はパス スルーされます。最大 5 つの候補値を設定できます。

SDPの透明性プロファイルの制限事項

次の制約事項は、SDP 透明性プロファイルに適用されます。これらの状況のいずれかが出力コール レッグに発生すると、Cisco Unified Communications Manager は宣言型 SDP 属性を通過させません。

- パススルーをサポートしていない、1つ以上のメディア ターミネーション ポイント（MTPs）またはトラステッド リレー ポイントが割り当てられます
- [メディア ターミネーション ポイントが必要（Media Termination Point Required）] チェックボックスを、SIP トランク用にチェックします
- トランスコーダが使用されます
- RSVP が使用されます
- 入力コール レッグでは遅延オファーが使用されている一方、出力コール レッグでは早期オファーが使用されている場合。
- メディアの回線は拒否されました（port=0）
- いずれかのコール レッグが、SIP 以外のプロトコルを使用している場合

SDP 透明性プロファイルの前提条件

サードパーティ製 SIP 製品の導入を計画している場合は、その製品が Session Description Protocol（SDP）を実装している方法を理解していることを確認します。

SDP 透明性プロファイルの設定

Cisco Unified Communications Manager でネイティブでサポートされていない宣言された SDP 属性のルール セットを SDP 透明性プロファイルに設定します。SDP 透明性プロファイルが SIP デバイスに適用される場合、Cisco Unified Communications Manager は入力コール レッグから出力コール レッグに SDP 属性を渡します。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [デバイス設定（Device Settings）] > [SDP 透明性プロファイル（SDP Transparency Profile）] 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。

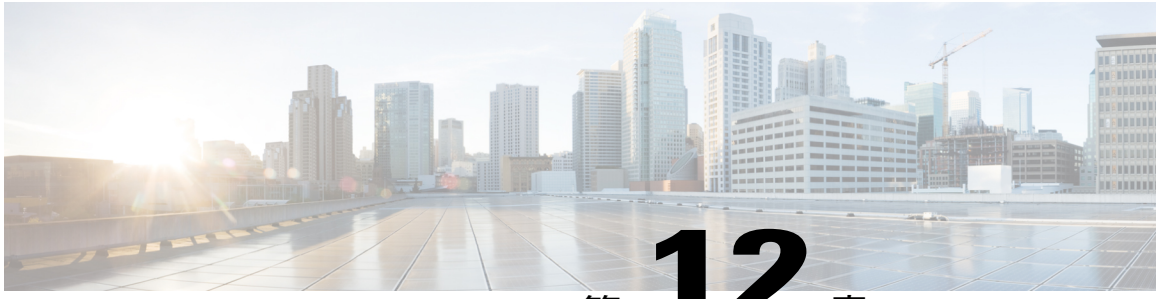
ステップ 3 [名前（Name）] と [説明（Description）] に入力します。

ステップ 4 [属性情報（Attribute Information）] ペインで、パススルーする SDP 属性のルールを作成します。

- プロパティ属性をパススルーするには、[名前（Name）] テキスト ボックスに属性（たとえばa=recvonly）を入力し、[タイプ（Type）] ドロップダウン リスト ボックスから [プロパティ（Property）] を選択します。
- 値属性をパススルーするには、[名前（Name）]テキストボックスに属性（たとえばa=rtpmap）を入力し、[タイプ（Type）] ドロップダウン リスト ボックスから [値（Any Value）] を選択します。
- 最大5つの値がある値属性をパススルーするには、[名前（Name）] フィールドに属性（たとえば a=rtpmap）を入力し、[タイプ（Type）] ドロップダウン リスト ボックスから [値（Any Value）] を選択します。結果の [値（Value）] テキスト ボックスに、属性の値を入力します。[+] をクリックして、この属性に最大 5 つの値を追加できます。

ステップ 5 この透明性プロファイルの追加SDP属性を入力できる新しい行を作成するために[（+）]をクリックします。

ステップ 6 [保存（Save）] をクリックします。



第 12 章

SIP プロファイルの設定

- SIP プロファイルの概要，95 ページ
- SIP プロファイルの設定，96 ページ

SIP プロファイルの概要

SIP プロファイル は、共通の SIP 設定で成り立つテンプレートです。ネットワーク内のすべての SIP トランクと SIP デバイスに SIP プロファイルを割り当てる必要があります。SIP プロファイルを設定し、SIP トランクまたは SIP デバイスにそのプロファイルを割り当てるとき、SIP の設定がそのトランクまたはデバイスに適用されます。

SIP プロファイルがなければ、ネットワーク上のそれぞれの SIP トランクと SIP デバイスに SIPを個別に設定する必要があります。ただし、SIP プロファイルを使用して、次のようなさまざまな SIP の設定を割り当てることができます。

- MTP テレフォニー ペイロード タイプ
- SIP ヘッダー詳細
- SIP メッセージのタイマーとカウンタ
- SDP の相互運用性のための SDP の透明性プロファイル
- SIP 回線の SIP 標準化と透明性スクリプト
- SIP OPTIONS の設定
- SIP Early Offer サポート
- コール ピックアップ URI

SIP プロファイルの設定

SIP プロファイルを設定するには、この手順を使用します。インストール時に、Cisco Unified Communications Manager にはデフォルト SIP プロファイルのグループが含まれます。デフォルトの SIP プロファイルを編集、または新しい SIP プロファイルを作成できます。

手順

ステップ 1 Cisco Unified CM の管理から、[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 次のいずれかの手順を実行します。

- 既存のプロファイルを編集するには、[検索（Find）] をクリックし、SIP プロファイルを選択します。
- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。

ステップ 3 SIP 電話およびトランクで IPv4 と IPv6 の両方のスタックをサポートする場合、デュアル スタック SIP トランクおよび SIP デバイスを設定する場合は、[ANATの有効化（Enable ANAT）] チェックボックスを選択して代替ネットワークアドレスタイプを有効にします。この設定では、デバイスまたはトランクの SIP シグナリングに、IPv4 アドレスと IPv6 アドレスの両方を同時に含めることができます。

ステップ 4 この SIP プロファイルを使用するトランクやデバイスに SDP の透明性プロファイルを割り当てる場合、[SDP の透明性プロファイル（SDP Transparency Profile）] ドロップダウン リスト ボックスから、プロファイルを選択します。

ステップ 5 この SIP プロファイルを使用する SIP デバイスに正規化または透明性スクリプトを割り当てる場合、[正規化スクリプト（Normalization Script）] ドロップダウン リスト ボックスから、適用するスクリプトを選択します。

ステップ 6 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

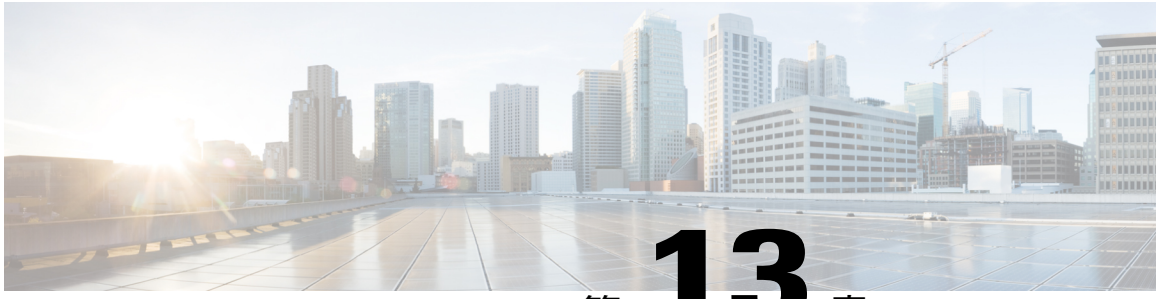
ステップ 7 [保存（Save）] をクリックします。

次の作業

トランクまたはデバイスでSIPプロファイルを使用できるようにするには、[トランクの設定（Trunk Configuration）] ウィンドウでトランクに、または [電話の設定（Phone Configuration）] ウィンドウでデバイスにプロファイルを関連付ける必要があります。

関連トピック

SIP トランクの設定, （105 ページ）



第 13 章

デュアル スタックの IPv6 の設定

- デュアル スタック アドレッシングの概要，97 ページ
- デュアル スタック IPv6 の前提条件，98 ページ
- デュアル スタック IPv6 設定のタスク フロー，98 ページ

デュアル スタック アドレッシングの概要

SIP 導入に IPv6 アドレッシングが必要な場合は、デュアル スタック IPv4 および IPv6 アドレッシングをサポートするように、Cisco Unified Communications Manager を設定できます。デフォルトでは、Cisco Unified Communications Manager は IPv4 アドレッシングに対して有効になっています。システムは引き続き IPv4 のみをサポートするデバイスとやり取りする必要があるため、システム レベルで IPv6 のみをサポートするように Cisco Unified Communications Manager を設定することはできません。ただし、IPv6 アドレッシングが必要な場合は、デュアル スタック トランクとデバイスを設定できます。

システム レベルでのデュアル スタック IPv6

Cisco Unified Communications Manager がデュアル スタック アドレッシング対応として設定されている場合、システムは次のシナリオのコールを設定できます。

- コール内の全デバイスが IPv4 のみをサポートしている
- コール内の全デバイスが IPv6 のみをサポートしている
- コール内の全デバイスがデュアル スタック モードである：このシナリオでは、システムはシグナリング イベントの [シグナリングの IP アドレッシング モード設定（IP Addressing Mode Preference for Signaling）] 設定とメディア イベントの [メディアの IP アドレッシング モード設定（IP Addressing Mode Preference for Media）] エンタープライズ パラメータを設定することで、IP アドレスのタイプを判別します。
- 一方のデバイスが IPv4 のみをサポートし、他方は IPv6 のみをサポートしている：このシナリオでは、Cisco Unified Communications Manager は MTP をコール パスに挿入し、2 つのアドレッシング タイプの間でシグナリングを変換します。

Cisco Unified Communications Manager は、SIP 環境でのみ IPv6 アドレスをサポートします。H.323 導入の場合、IPv4 デバイスと IPv6 デバイスが通信できるように、システムは MTP をコール パスに挿入します。

デバイスのデュアル スタック IPv6

デバイス レベルでは、電話、ゲートウェイ、会議ブリッジなどの多数のデバイスとメディア リソースを設定できます。それらは、IPv4 アドレッシングのみ、IPv6 アドレッシングのみ、またはデュアルスタックを使用するように設定できます。シグナリングとメディアイベントの両方に対して優先されるアドレッシング方式を設定できます。

SIP デバイスの場合、Alternate Network Address Type（ANAT）機能を設定することもできます。この機能によって、登録済みの SIP デバイスは、IPv4 アドレスと IPv6 アドレスを同時に保持できます。デバイスはいずれかのアドレス タイプを使用して通信できるため、IPv4 ネットワークと IPv6 ネットワークの両方でシームレスに相互運用できます。デバイスに割り当てられた SIP プロファイルで ANAT を有効にすることで、SIP デバイスの ANAT を有効化できます。

デュアル スタック IPv6 の前提条件

Cisco Unified Communications Manager にデュアル スタック IPv6 サポートを設定する前に、IPv6 をサポートするように、次のネットワーク サーバとデバイスを設定する必要があります。詳細については、デバイスのユーザ ドキュメントを参照してください。

- DHCP および DNS サーバに IPv6 サポートをプロビジョニングします。Cisco Network Registrar サーバは、DHCP および DNS 対応の IPv6 をサポートします。
- ゲートウェイ、ルータ、MTP などのネットワーク デバイスの IOS に IPv6 サポートを設定します。
- IPv6 を実行するための TFTP サーバを設定します。

デュアル スタック IPv6 設定のタスク フロー

システムのデュアル スタック IPv6 を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	オペレーティング システムでの IPv6 の設定，（99 ページ）	IPv6 アドレスをサポートするオペレーティング システムを設定します。
ステップ 2	IPv6 のサーバの設定，（100 ページ）	IPv6 アドレスを使用して、クラスタのサーバを設定します。

	コマンドまたはアクション	目的
ステップ 3	IPv6 の有効化, （100 ページ）	IPv6 のシステムを有効にするエンタープライズ パラメータを設定します。
ステップ 4	IP アドレッシングの優先順位の設定, （101 ページ）	IP アドレッシング方式が推奨されるクラスタ設定を設定します。
ステップ 5	サービスの再起動, （103 ページ）	次のネットワーク サービスを再起動します。 • Cisco CallManager • Cisco CTIManager • Cisco IP Voice Media Streaming App • Cisco Certificate Authority Proxy Function

次の作業

デュアル スタックのトランクを設定する方法については、SIP トランクの設定の章を参照してください。

- SIP トランクの設定タスク フロー, （107 ページ）

SIP デバイスのデュアル スタックを設定する方法については、設定する SIP デバイスのセクションを参照してください。

オペレーティング システムでの IPv6 の設定

Cisco Unified OS の管理でイーサネット IPv6 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 [Cisco Unified OS の管理（Cisco Unified OS Administration）] で、[設定（Settings）] > [IPv6] > [イーサネット（Ethernet）].を選択します。

ステップ 2 [IPv6 を有効にする（Enable IPv6）] チェックボックスをオンにします。

ステップ 3 [アドレス ソース（Address Source）] ドロップダウン リスト ボックスから、システムが IPv6 アドレスを取得する方法を設定します。

- [ルータ アドバタイズメント（Router Advertisement）] : システムが IPv6 アドレスを取得するためにステートレス自動設定を使用します。
- [DHCP] : システムが DHCP サーバから IPv6 アドレスを取得します。

- [手動入力（Manual Entry）]：IPv6アドレスを手動で入力する場合は、このオプションを選択します。

ステップ 4 IPv6 アドレスの取得方法として手動入力を設定した場合は、次のフィールドに入力します。

- [IPv6 アドレス（IPv6 Address）] を入力します。例：fd62:6:96:2le:bff:fecc:2e3a。
- [IPv6 マスク（IPv6 Mask）] を入力します。例：64。

ステップ 5 保存した後でシステムを再起動するには、[再起動後に更新（Update with Reboot）] チェック ボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

IPv6 のサーバの設定, （100 ページ）

IPv6 のサーバの設定

IPv6 アドレスを使用して、クラスタのサーバを設定します。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [サーバ（Server）] を選択します。

ステップ 2 [IPv6名（IPv6 Name）] フィールドで、次のいずれかの値を選択します。

- DNS 設定済みで、DNS サーバが IPv6 対応の場合は、サーバのホスト名を入力します。
- それ以外の場合は、非リンク ローカル IPv6 アドレスを入力します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 各クラスタ ノードで上記の手順を繰り返します。

次の作業

IPv6 の有効化, （100 ページ）

IPv6 の有効化

システムで IPv6 サポートを設定する場合、システムで IPv6 デバイスをサポートできるようにする必要があります。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] の順に選択します。

ステップ 2 [IPv6 を有効化（Enable IPv6）] エンタープライズ パラメータの値を [True（True）] に設定します。

ステップ 3 [保存（Save）] をクリックします。

次の作業

IP アドレッシングの優先順位の設定, （101 ページ）

IP アドレッシングの優先順位の設定

IP アドレスの優先順位を含む共通デバイス設定を実行し、その設定をトランクやデバイスに適用することで、個別のトランクや SIP デバイスに対して IP アドレッシングの優先順位を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	クラスタの IP アドレッシングの設定, （101 ページ）	クラスタ全体のエンタープライズパラメータを使用して、システム レベルの IP アドレスの優先順位を設定します。この設定は、クラスタ内のすべての SIP デバイスとトランクに適用されます。ただし、共通デバイス設定によってトランクやデバイスが上書きされる場合は除きます。
ステップ 2	デバイス用 IP アドレッシングモードの優先順位の設定, （102 ページ）	共通デバイス設定で IP アドレッシングの優先順位を設定します。SIP トランク、SIP 電話、会議ブリッジ、トランスコーダなどのデュアルスタック デバイスに設定を適用できます。 （注） 共通デバイス設定の IP アドレッシングの優先順位設定は、共通デバイス設定を使用するデバイスに対するクラスタ全体のエンタープライズパラメータ設定を上書きします。

クラスタの IP アドレッシングの設定

デュアル スタック IPv6 でクラスタ全体の IP アドレッシング モードの優先順位を設定するには、この手順でエンタープライズ パラメータを使用します。変更中の共通デバイス設定が特定のトラ

ンクまたはデバイスに適用されている場合を除き、システムは、その設定をすべての SIP トランクおよびデバイスに適用します。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] の順に選択します。

ステップ 2 [メディア用のIPアドレッシングモード設定（IP Addressing Mode Preference for Media）] のエンタープライズ パラメータの値を [IPv4（IPv4）] または [IPv6（IPv6）] に設定します。

ステップ 3 [シグナリング用のIPアドレッシングモード設定（IP Addressing Mode Preference for Media）] のエンタープライズ パラメータの値を [IPv4（IPv4）] または [IPv6（IPv6）] に設定します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

共通デバイス設定を使用して、IP アドレスの設定を特定の SIP デバイスに適用します。詳細は、IP アドレッシングの優先順位の設定, （101 ページ）を参照してください。

デバイス用 IP アドレッシング モードの優先順位の設定

共通デバイス設定で優先順位を設定することで、個々のデバイスにIPアドレッシングモードの優先順位を設定できます。トランク、電話機、会議ブリッジ、トランスコーダなどの IPv6 アドレッシングをサポートする SIP デバイスに共通デバイス設定を適用できます。

（注） 共通デバイス設定の IP アドレスの設定は、その共通デバイス設定を使用するデバイスのクラスタ全体のエンタープライズ パラメータ設定をオーバーライドします。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通デバイス設定（Common Device Configuration）] 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 [共通デバイス設定（Common Device Configuration）] ウィンドウで各フィールドを設定します。フィールドとその説明については、オンライン ヘルプを参照してください。

ステップ 4 SIP トランクまたは SCCP 電話機では、[IP アドレッシング モード（IP Addressing Mode）] ドロップダウン リスト ボックスの値を選択してください。

- [IPv4 のみ（IPv4 Only）] —デバイスはメディアやシグナリングに IPv4 アドレスだけを使用します。
- [IPv6 のみ（IPv6 Only）] —デバイスはメディアやシグナリングに IPv6 アドレスだけを使用します。

- [IPv4 および IPv6（IPv4 and IPv6）] —（デフォルト）デバイスはデュアルスタック デバイスで、利用できる IP アドレスのタイプを使用します。両方の IP アドレスのタイプがデバイスに設定されている場合、デバイスのシグナリングには、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] 設定を使用し、メディア デバイスには、[メディア用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Media）] エンタープライズ パラメータの設定を使用します。

ステップ 5 デュアル スタックの電話やトランクでは、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] ドロップダウン リスト ボックスで次の IP アドレッシング モード優先設定を入力します。

- [IPv4（IPv4）]—デュアル スタック デバイスでシグナリングに IPv4 アドレスを優先して使用します。
- [IPv6（IPv6）]—デュアル スタック デバイスでシグナリングに IPv6 アドレスを優先して使用します。
- [システム デフォルトを使用（Use System Default）]—デバイスは、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] エンタープライズ パラメータの設定を使用します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

IPv6 設定が完了したら、サービスの再起動, （103 ページ）。

サービスの再起動

システムの IPv6 設定したら、基本的なサービスを再起動します。

手順

ステップ 1 Cisco Unified Serviceability にログインして、[ツール（Tools）]>[コントロール センター - 機能サービス（Control Center - Feature Services）] を選択します。

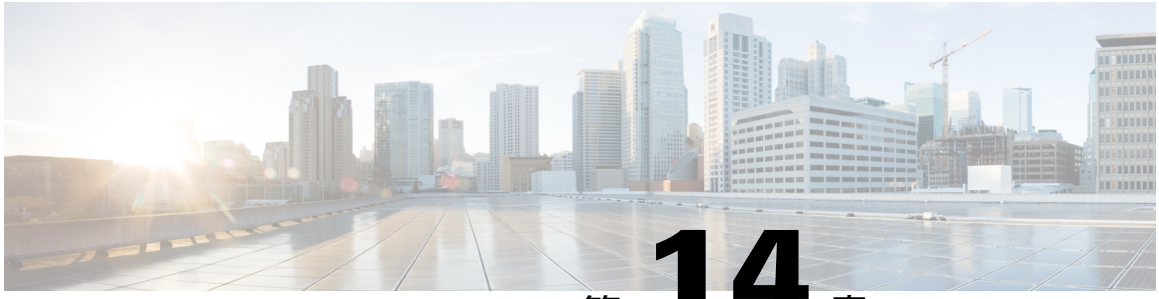
ステップ 2 次のそれぞれのサービスに対応するチェックボックスをオンにします。

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function

- Cisco IP Voice Media Streaming App

ステップ 3 [再起動（Restart）] をクリックします。

ステップ 4 [OK] をクリックします。



第 14 章

SIP トランクの設定

- SIP トランクの概要，105 ページ
- SIP トランク設定の前提条件，107 ページ
- SIP トランクの設定タスク フロー，107 ページ

SIP トランクの概要

コール制御シグナリングの SIP を展開している場合、SIP ゲートウェイ、SIP プロキシ サーバ、Unified Communications アプリケーション、リモート クラスタ、またはセッション管理エディションなどの外部デバイスに Cisco Unified Communications Manager を接続する SIP トランクを設定します。

Cisco Unified CM の管理の内部で、[SIP Trunk Configuration] ウィンドウには、Cisco Unified Communications Manager が SIP コールの管理に使用する SIP シグナリング設定が含まれています。

SIP トランクには最大 16 の異なる接続先アドレスを割り当てられます。これには、IPv4 または IPv6 アドレッシング、完全修飾ドメイン名、単一の DNS SRV レコードを使用します。

SIP トランクの次の機能を設定できます。

- 回線と名前の識別サービス
- Delayed Offer、Early Offer、Best Effort Early Offer
- シグナリング暗号化と認証
- SRTP によるメディア暗号化
- IPv6 デュアル スタックのサポート
- [ビデオ（Video）]
- BFCP と共有するプレゼンテーション
- 遠端カメラ制御
- DTMF リレー

- 発信側の正規化
- URI ダイヤル
- Q.SIG サポート
- T.38 ファックス サポート
- SIP オプション
- DTMF シグナリングの選択

（注） クラスタ A からクラスタ B で小規模 IP テレフォニー（SIPT）の Q.SIG を有効にした場合、匿名またはテキストで "INVITE" を受領しても、Cisco Unified Communications Manager は "INVITE" を Q.SIG データにエンコードしません。リーフ クラスタで同じようにデコードすると、何も表示されず、空の番号が転送されます。

（注） Q.SIG を有効にすると、URI ダイヤルが予期したとおりに応答しません。Q.SIG を無効にすると、Cisco Call Back が 2 つのクラスタ間で応答しません。

IPv6 デュアル スタックのサポート

また、一般的なデバイス設定で IP アドレッシング モードを設定することで、デュアル スタック サポートで SIP トランクを設定することもできます。詳細をここに追加します。

安全な SIP トランク

SIP トランク セキュリティ プロファイルを設定して、ダイジェスト認証、シグナリングとメディアの暗号化などのセキュリティで自分のトランクを設定することもできます。このプロファイルにはダイジェスト認証や TLS シグナリングが含まれ、そのプロファイルをネットワークの SIP トランクに関連付けます。発信メディアを暗号化するには、SRTP メディアを有効にするためにトランクを設定する必要もあります。

SIP トランクのセキュリティプロファイル概要

ネットワークの各 SIP トランクに SIP トランク セキュリティ プロファイルを割り当てる必要があります。デフォルトでは、Cisco Unified Communications Manager がすべての SIP トランクに、事前に定義された非セキュアな SIP トランク セキュリティ プロファイルを適用します。

SIP トランク セキュリティ プロファイルを使用することにより、ネットワークの SIP トランクの TLS シグナリング暗号化とダイジェスト認証のようなセキュリティを設定できます。SIP トランク セキュリティ プロファイルを設定し、そのプロファイルを SIP トランクに割り当てると、プロファイルのセキュリティの設定がトランクに適用されます。

ネットワークに異なる SIP トランクの設定がある場合に、複数の SIP トランク セキュリティ プロファイルを設定することで、さまざまなセキュリティ要件に対応できます。

（注） ネットワークにセキュリティを設定するには、CTL クライアントをセットアップし、IPSec を設定する必要もあります。詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。

SIP トランク設定の前提条件

SIP トランクを設定する前に、次の手順を実行します。

- トランク接続を把握できるように、ネットワーク トポロジを計画します。
- トランクの接続先のデバイスと、それらのデバイスが SIP をどのように実装するかを確実に理解します。それらのデバイスが SIP を実装している場合は、SIP 正規化スクリプトを適用する必要が生じることがあります。
- トランクの SIP プロファイルを設定します。

さらに、SIP トランクを設定する前に、次を設定します。

- SIP の正規化および透明性設定のタスク フロー, （87 ページ）
- SIP プロファイルの設定, （96 ページ）

SIP トランクの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	SIP トランク セキュリティ プロファイルの設定, （108 ページ）	SIP トランクに適用する任意のセキュリティ設定を使用して、SIP トランク セキュリティ プロファイルを設定します。たとえば、ダイジェスト認証、デバイス セキュリティ モード、および SIP シグナリングの TLS 暗号化を設定できます。 SIP トランク セキュリティ プロファイルを設定しなければ、デフォルトで、Cisco Unified Communications Manager によって非セキュアの SIP トランク セキュリティ プロファイルが適用されます。
ステップ 2	共通デバイス設定の実行, （109 ページ）	トランクの共通デバイス設定を実行します。デュアルスタック トランクの場合、IP アドレッシングの優先順位を設定します。
ステップ 3	SIP トランクの設定, （110 ページ）	ネットワークの SIP トランクを設定します。[トランクの設定（Trunk Configuration）] ウィンドウで、トランクの SIP 設定

	コマンドまたはアクション	目的
		を実行します。SIPプロファイル、SIP トランク セキュリティ プロファイル、および共通デバイス設定を SIP トランクに割り当てます。また、トランク接続に必要な SIP の正規化および透明性スクリプトを割り当てます。たとえば、SIP トランクが Cisco TelePresence VCS に接続する場合、*vcs-interop* スクリプトを SIP トランクに割り当てる必要があります。

SIP トランク セキュリティ プロファイルの設定

ネットワークで SIP トランクに割り当てられる SIP トランク セキュリティ プロファイルを設定するには、次の手順を使用します。ダイジェスト認証や TLS 暗号化シグナリングのようなセキュリティ機能を設定するために、SIP トランクにプロファイルを割り当てることができます。SIP トランク セキュリティ プロファイルを設定しない場合、Cisco Unified Communications Manager により、ネットワークの SIP トランクにセキュアではないプロファイルが割り当てられます。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] 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 TLS の SIP シグナリング暗号化を有効にするには、次の手順を実行します。

a) [デバイス セキュリティ モード（Device Security Mode）] ドロップダウン リスト ボックスから、[暗号化（Encrypted）] を選択します。

b) [着信転送タイプ（Incoming Transport Type）] と [発信転送タイプ（Outgoing Transport Type）] ドロップダウン リスト ボックスから、[TLS（TLS）] を選択します。

c) デバイスの認証で、[X.509 のサブジェクト名（X.509 Subject Name）] フィールドで、X.509 証明書のサブジェクト名を入力します。

d) [着信ポート（Incoming Port）] フィールドに、TLS リクエストを受信するポートを入力します。TLS のデフォルトは 5061 です。

ステップ 4 ダイジェスト認証を有効にするには、次の内容を実行します。

a) [ダイジェスト認証を有効化（Enable Digest Authentication）] チェックボックスをオンにします。

b) システムが新しいナンスを生成するまでの時間（秒数）を [ナンス有効時間（Nonce Validity Time）] に入力します。デフォルトは 600（10 分）です。

c) アプリケーションのダイジェスト認証を有効にするには、[アプリケーションレベル認証を有効化（Enable Application Level Authorization）] チェックボックスをオンにします。

ステップ 5 [SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウで追加フィールドを設定します。フィールドとその説明については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

（注） ネットワーク セキュリティ セットアップの詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。

次の作業

SIP トランクに SIP トランク セキュリティ プロファイルを割り当てるには、次の手順を使用します。

- SIP トランクの設定, （110 ページ）

共通デバイス設定の実行

共通デバイス設定は、ユーザ固有のサービス属性と機能属性で構成されています。デュアル スタックの電話やトランクを設定している場合、共通デバイス設定でIPアドレッシング モードの優先順位を設定できます。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通デバイス設定（Common Device Configuration）] 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 [共通デバイス設定（Common Device Configuration）] ウィンドウで各フィールドを設定します。フィールドとその説明については、オンライン ヘルプを参照してください。

ステップ 4 SIP トランクまたは SCCP 電話機では、[IP アドレッシング モード（IP Addressing Mode）] ドロップダウン リスト ボックスの値を選択してください。

- [IPv4 のみ（IPv4 Only）] —デバイスはメディアやシグナリングに IPv4 アドレスだけを使用します。
- [IPv6 のみ（IPv6 Only）] —デバイスはメディアやシグナリングに IPv6 アドレスだけを使用します。
- [IPv4 および IPv6（IPv4 and IPv6）] —（デフォルト）デバイスはデュアルスタック デバイスで、利用できる IP アドレスのタイプを使用します。両方の IP アドレスのタイプがデバイスに設定されている場合、デバイスのシグナリングには、[シグナリグ用IPアドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] 設定を使用し、メディア デバイス

には、[メディア用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Media）] エンタープライズ パラメータの設定を使用します。

ステップ 5 デュアル スタックの電話やトランクでは、[シグナリング用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] ドロップダウン リスト ボックスで次の IP アドレッシング モード優先設定を入力します。

- [IPv4（IPv4）]—デュアル スタック デバイスでシグナリングに IPv4 アドレスを優先して使用します。
- [IPv6（IPv6）]—デュアル スタック デバイスでシグナリングに IPv6 アドレスを優先して使用します。
- [システム デフォルトを使用（Use System Default）]—デバイスは、[シグナリング用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）] エンタープライズ パラメータの設定を使用します。

ステップ 6 [保存（Save）] をクリックします。

SIP トランクの設定

SIP トランクの設定を行うには、次の手順を実行します。

はじめる前に

SIP トランク セキュリティ プロファイルの設定, （108 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [トランク（Trunk）] 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 [トランク タイプ（Trunk Type）] ドロップダウン リスト ボックスから、[SIP トランク（SIP Trunk）] を選択します。

ステップ 4 [プロトコル タイプ（Protocol Type）] ドロップダウン リスト ボックスから、設定する SIP トランクのタイプを選択します。

- [なし（デフォルト）（None (Default)）]：トランクは、コール制御検出、Extension Mobility Cross Cluster、Intercompany Media Engine、または IP Multimedia System サービス コントロールには使用されません。
- [コール制御検出（Call Control Discovery）]：トランクはコール制御検出機能をサポートします。
- [Extension Mobility Cross Cluster]：トランクは Extension Mobility Cross Cluster をサポートします。

- [Cisco Intercompany Media Engine]：トランクは Intercompany Media Engine（IME）をサポートします。トランク タイプを設定する前に、IME サーバがインストールされていることを確認します。
- [IP Multimedia System サービス コントロール（IP Multimedia System Service Control）]：トランクの IP Multimedia System サービス コントロールのサポートを有効にするには、このオプションを選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 このトランクに共通デバイス設定を適用する場合は、[共通デバイス設定（Common Device Configuration）] ドロップダウン リスト ボックスから設定を選択します。

ステップ 7 SIP トランクの宛先アドレスを設定します。

a) [宛先アドレス（Destination Address）] テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv4 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

b) トランクがデュアル スタック トランクの場合は、[宛先アドレス IPv6（Destination Address IPv6）] テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv6 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

c) 宛先が DNS SRV レコードの場合は、[宛先アドレスは SRV（Destination Address is an SRV）] チェック ボックスをオンにします。

d) 宛先を追加するには、[+] ボタンをクリックします。SIP トランクには最大 16 個の宛先を追加できます。

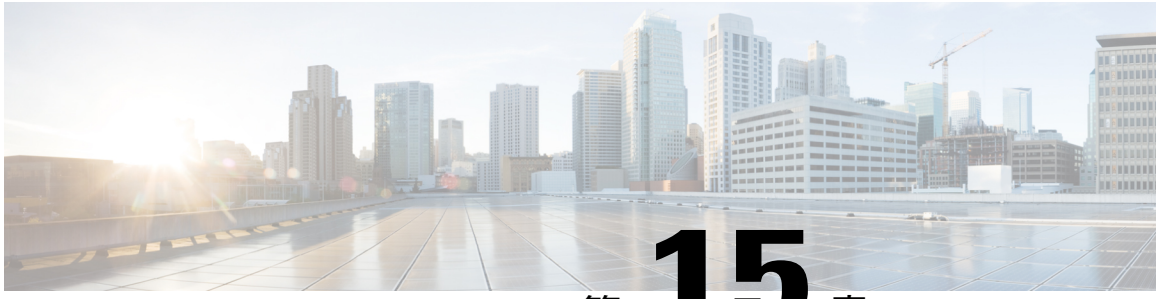
ステップ 8 [SIP トランク セキュリティプロファイル（SIP Trunk Security Profile）] ドロップダウン リスト ボックスから、このトランクに SIP トランク セキュリティプロファイルを割り当てます。

ステップ 9 [SIP プロファイル（SIP Profile）] ドロップダウン リスト ボックスから、このトランクに SIP プロファイルを割り当てます。

ステップ 10 （オプション）この SIP トランクに正規化スクリプトを割り当てる場合は、[正規化スクリプト（Normalization Script）] ドロップダウン リスト ボックスから、割り当てるスクリプトを選択します。

ステップ 11 [トランクの設定（Trunk Configuration）] ウィンドウのその他のフィールドを設定します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 12 [保存（Save）] をクリックします。



第 15 章

H.323 トランクの設定

- H.323 トランクの概要，113 ページ
- H.323 トランクの前提条件，114 ページ
- H.323 トランクの設定，114 ページ

H.323 トランクの概要

H.323 を導入している場合は、H.323 トランクがリモート クラスタと、ゲートウェイなどのその他の H.323 デバイスに接続を提供します。H.323 トランクは、Cisco Unified Communications Manager がクラスタ内通信用にサポートするオーディオおよびビデオ コーデックのほとんどをサポートします。ただし、ワイドバンド オーディオおよびワイドバンド ビデオについてはサポートしません。H.323 トランクは、コール制御シグナリング用に H.225 プロトコルを使用し、メディア シグナリング用に H.245 プロトコルを使用します。

Cisco Unified CM の管理で、クラスタ間トランク（ゲートキーパー非制御）トランク タイプとプロトコル オプションを使用して H.323 トランクを設定できます。

ゲートキーパー非制御の H.323 を導入している場合は、ローカル Cisco Unified Communications Manager が IP WAN 経由でコールを発信できるリモート クラスタ内のデバイス プールごとに個別のクラスタ間トランクを設定する必要があります。クラスタ間トランクは、リモート デバイスの IPv4 アドレスまたはホスト名を静的に指定します。

単一のトランクには最大 16 件の宛先アドレスを設定できます。

クラスタ間トランク

2 つのリモート クラスタ間にクラスタ間トランク接続を設定する場合は、一方のトランクが使用する宛先アドレスがリモート クラスタのトランクが使用するコール処理ノードと一致するように、クラスタごとにクラスタ間トランクを設定し、トランク設定を一致させる必要があります。次に例を示します。

- リモート クラスタ トランクが [すべてのアクティブ ノードで実行（Run on all Active Nodes）] を使用する：リモート クラスタ トランクは、コール処理とロード バランシングにすべての

ノードを使用します。ローカル クラスタ内から始まるローカル クラスタ間トランクでは、リモート クラスタ内の各サーバの IP アドレスまたはホスト名を追加します。

- リモート クラスタは [すべてのアクティブ ノードで実行（Run on all Active Nodes）] を使用しない：リモート クラスタ トランクは、コール処理とロード バランシングに、トランクのデバイス プールに割り当てられた Cisco Unified Communications Manager グループ内のサーバを使用します。ローカル クラスタ間トランク設定で、リモート クラスタ トランクのデバイス プールが使用する Cisco Unified Communications Manager グループ内の各ノードの IP アドレスまたはホスト名を追加する必要があります。

セキュア トランク

H.323 トランクのセキュアなシグナリングを設定するには、トランクに IPSec を設定する必要があります。詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。メディア暗号化を許可するようにトランクを設定するには、[トランクの設定（Trunk Configuration）] ウィンドウで [SRTP を許可する（SRTP allowed）] チェックボックスをオンにします。

（注） ゲートキーパーは今では広く使用されていませんが、ゲートキーパー制御のトランクを使用するように H.323 導入を設定することもできます。ゲートキーパー制御のトランクを設定する方法の詳細については、『*Cisco Unified Communications Manager Administration Guide, Release 10.0(1)*』を参照してください。

H.323 トランクの前提条件

H.323 導入トポロジの計画を立案します。クラスタ間トランクの場合は、対応するリモート クラスタ トランクがコール処理とロードバランシングにどのサーバを使用するかを明確化します。リモート クラスタ内のトランクによって使用される各コール処理サーバに接続するようにローカル クラスタ間トランクを設定する必要があります。

トランクのロード バランシングにトランクのデバイス プールに割り当てられた Cisco Unified Communications Manager グループを使用している場合は、次の設定を完了します。

- デバイス プールのタスク フローのコア設定, （51 ページ）

H.323 トランクの設定

H.323 を導入したトランクを設定するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、[デバイス（Device）]>[トランク（Trunk）] 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 [トランク タイプ（Trunk Type）] ドロップダウン リスト ボックスから [クラスタ間トランク（ゲートキーパー制御なし）（Inter-Cluster Trunk (Non-Gatekeeper Controlled)）] を選択します。

ステップ 4 [プロトコル（Protocol）] ドロップダウン リスト ボックスから [クラスタ間トランク（Inter-Cluster Trunk）] を選択します。

ステップ 5 [デバイス名（Device Name）] テキストボックスに、トランクの固有 ID を入力します。

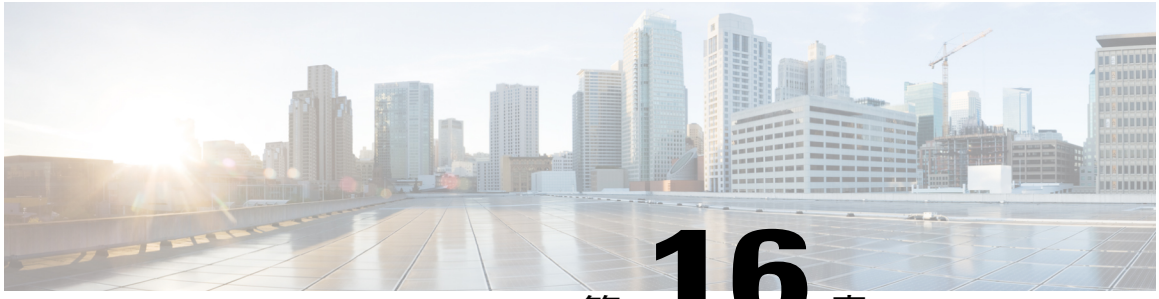
ステップ 6 [デバイス プール（Device Pool）] ドロップダウン リスト ボックスから、このトランクに設定したデバイス プールを選択します。

ステップ 7 このトランクの処理のためにローカルクラスタのすべてのノードを使用するには、[すべてのアクティブな Unified CM ノードで実行する（Run on all Active Unified CM Nodes）] チェックボックスをオンにします。

ステップ 8 トランクで暗号化されたメディアを許可するには、[SRTP の許可（SRTP Allowed）] チェックボックスをオンにします。

ステップ 9 H.235 パス スルーを設定するには、[H.235 パス スルーを許可（H.235 Pass Through Allowed）] チェックボックスをオンにします。

ステップ 10 [リモート Cisco Unified Communications Manager 情報（Remote Cisco Unified Communications Manager Information）] セクションで、このトランクを接続する各リモート サーバの IP アドレスまたはホスト名を入力します。



第 16 章

SRST の設定

- Survivable Remote Site Telephony の概要, 117 ページ
- Survivable Remote Site Telephony の設定タスク フロー, 118 ページ
- SRST の制限事項, 123 ページ

Survivable Remote Site Telephony の概要

Survivable Remote Site Telephony（SRST）はサイトのオプション機能で、Cisco Unified Communications Manager ノードへのワイドエリア ネットワーク（WAN）接続によって異なります。Cisco Unified CM の管理インターフェイスで設定されている SRST リファレンスを使用すると、WAN の停止時に、IP ゲートウェイからリモート サイトにある IP フォンに限定されたテレフォニー サービスを提供できます。

- リモート サイトの IP フォンは互いにコールできます。
- PSTN からのコールは IP フォンに到達できます。
- IP フォンからのコールは PSTN を介して外部に到達できます。

リモート サイトの IP フォンは、関連付けられたすべての Cisco Unified Communications Manager ノードへの接続を失うと、SRST リファレンス IP ゲートウェイに接続します。IP フォンのステータス行には、IP フォンがバックアップ SRST ゲートウェイにフェールオーバーしたことが示されます。Cisco Unified Communications Manager への接続が復元されると、IP フォンが Cisco Unified Communications Manager に再登録されて、すべてのテレフォニー サービスが復元されます。

SRST は、PSTN ゲートウェイ アクセスに加えて、SCCP および SIP エンドポイントが混在している可能性があるリモート サイトをサポートします。

Survivable Remote Site Telephony の設定タスク フロー

はじめる前に

ダイヤル プランを検証します。ダイヤル プランに 7 か 8 桁の数字があるとき、場合によりトランスレーションルールを設定する必要があります。トランスレーションルールの詳細については、トランスレーション パターンの設定タスク フロー，（174 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	SRST リファレンスの設定，（118 ページ）	デバイスに対して他のすべての Cisco Unified Communications Manager ノードが到達不能であるとき、Cisco Unified Communications Manager の限定機能を備えたゲートウェイを設定します。
ステップ 2	デバイス プールへの SRST リファレンスの割り当て，（119ページ）	各デバイス プールに対して、Cisco Unified Communications Manager が使用できない場合に、コールの完了を試みるとき、コーリング デバイス サーチのゲートウェイを割り当てます。
ステップ 3	次のいずれかの作業を実行します。 • クラスタの接続モニタ間隔の設定，（120 ページ） • デバイスプールの接続モニタ間隔の設定，（121 ページ）	これはオプションです。クラスタ全体またはデバイス プールに対して、接続モニタ間隔の値を設定します。クラスタの場合は、デフォルト値は 120 秒です。デバイス プールに値が定義されていない場合、クラスタに定義された値が使用されます。
ステップ 4	SRST ゲートウェイの SRST を有効にする，（122 ページ）	ゲートウェイの SRST パラメータを設定します。

SRST リファレンスの設定

SRST リファレンスは、デバイスのその他すべての Cisco Unified Communications Manager ノードが到達不能の場合に、Cisco Unified Communications Manager の一部機能を利用できるゲートウェイで構成されます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] にログインし、[システム（System）] > [SRST（SRST）] 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 [SRSTリファレンスの設定（SRST Reference Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

デバイス プールへの SRST リファレンスの割り当て, （119 ページ）

デバイス プールへの SRST リファレンスの割り当て

電話機の各デバイス プールに SRST を設定できます。デバイス プールに SRST リファレンスを割り当てると、デバイス プールのすべての電話機が、Cisco Unified Communications Manager のノードに到達できない場合、割り当てた SRST に接続を試みます。

はじめる前に

SRST リファレンスの設定, （118 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [デバイス プール（Device Pool）] を選択します。

ステップ 2 [検索（Find）] をクリックし、リモート IP フォンが登録されているデバイス プールを選択します。

ステップ 3 [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] エリアの [SRST リファレンス（SRST Reference）] ドロップダウン リストから SRST を選択します。
[SRST リファレンス（SRST Reference）] ドロップダウン リストには次のオプションがあります。

- [無効（Disable）]：電話機は、Cisco Unified Communications Manager のいずれのノードにも到達できない場合、SRST ゲートウェイへの接続を試みません。
- [デフォルト ゲートウェイを使用（Use Default Gateway）]：電話機は、Cisco Unified Communications Manager のいずれのノードにも到達できない場合、IP ゲートウェイを SRST ゲートウェイとして接続を試みます。
- [ユーザ定義（User-defined）]：電話機は、Cisco Unified Communications Manager のいずれのノードにも到達できない場合、この SRST ゲートウェイへの接続を試みます。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- 次のいずれかの作業を実行します。
  - クラスタの接続モニタ間隔の設定，（120 ページ）
  - デバイス プールの接続モニタ間隔の設定，（121 ページ）
- SRST ゲートウェイの SRST を有効にする，（122 ページ）

クラスタの接続モニタ間隔の設定

ワイド エリア ネットワーク（WAN）経由で SRST ゲートウェイに接続された IP フォンは、WAN リンク経由で Cisco Unified Communications Manager との接続を確立できるようになるとすぐに、自分自身を Cisco Unified Communications Manager に再接続します。ただし、WAN リンクが不安定である場合は、SRST ゲートウェイと Cisco Unified Communications Manager 間で IP フォンの切り替えが頻発します。この状況では、電話サービスの一時損失（ダイヤルトーンなし）が発生します。こうした再接続試行は、WAN リンクのフラッピング問題と呼ばれ、IP フォンが正常に Cisco Unified Communications Manager に再接続するまで続きます。

Cisco Unified Communications Manager と SRST ゲートウェイ間の WAN リンク フラッピング問題を解決するには、接続モニタ間隔（秒）を定義します。これは SRST ゲートウェイから登録解除し、Cisco Unified Communications Manager を再登録する前に、IP フォンが Cisco Unified Communications Manager に接続しないようにモニタする間隔を調整できます。IP フォンは、XML 設定ファイルの接続モニタ間隔値を受信します。

この手順は任意です。接続モニタ間隔のシステム値（エンタープライズ パラメータ）を変更する場合だけ、この手順を完了します。

はじめる前に

デバイス プールへの SRST リファレンスの割り当て，（119 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] の順に選択します。

ステップ 2 [接続モニタ間隔（Connection Monitor Duration）] フィールドに値を入力します。デフォルト値は 120 秒です。フィールドに入力できる最大秒数は、2592000 秒です。

ステップ 3 [保存（Save）] をクリックします。
変更を有効にするにはすべてのサービスを再起動する必要があります。

次の作業

SRST ゲートウェイの SRST を有効にする，（122 ページ）

デバイス プールの接続モニタ間隔の設定

ワイド エリア ネットワーク（WAN）経由で SRST ゲートウェイに接続された IP フォンは、WAN リンク経由で Cisco Unified Communications Manager との接続を確立できるようになるとすぐに、自分自身を Cisco Unified Communications Manager に再接続します。ただし、WAN リンクが不安定である場合は、SRST ゲートウェイと Cisco Unified Communications Manager 間で IP フォンの切り替えが頻発します。この状況では、電話サービスの一時損失（ダイヤルトーンなし）が発生します。こうした再接続試行は、WAN リンクのフラッピング問題と呼ばれ、IP フォンが正常に Cisco Unified Communications Manager に再接続するまで続きます。

Cisco Unified Communications Manager と SRST ゲートウェイ間の WAN リンク フラッピング問題を解決するには、接続モニタ間隔（秒）を定義します。これは SRST ゲートウェイから登録解除し、Cisco Unified Communications Manager を再登録する前に、IP フォンが Cisco Unified Communications Manager に接続しないようにモニタする間隔を調整できます。IP フォンは、XML 設定ファイルの接続モニタ間隔値を受信します。

ヒント デバイス プールの接続モニタ間隔の値を変更する場合、値は更新されるデバイス プールだけに適用されます。その他すべてのデバイス プールは、各自の [接続モニタ間隔（Connection Monitor Duration）] フィールドの値を使用するか、[接続モニタ間隔（Connection Monitor Duration）] エンタープライズ パラメータで設定されたクラスタ全体用の値を使用します。

この手順は任意です。この操作は、次の項目に該当する場合に限り実行します。

- 接続モニタ間隔にクラスタ全体用の値を使用することを希望しない、および
- このデバイス プール個別の接続モニタ間隔の値を定義することを希望する

はじめる前に

デバイス プールへの SRST リファレンスの割り当て，（119 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [デバイス プール（Device Pool）] を選択します。

ステップ 2 [検索（Find）] をクリックし、リモート IP フォンが登録されているデバイス プールを選択します。

ステップ 3 [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] エリアで、[接続モニタ間隔（Connection Monitor Duration）] フィールドに値を入力します。フィールドに入力できる最大秒数は、2592000 秒です。

（注） この設定は、エンタープライズ パラメータの接続モニタ間隔設定をオーバーライドします。

ステップ 4 [保存（Save）] をクリックします。

次の作業

SRST ゲートウェイの SRST を有効にする，（122 ページ）

SRST ゲートウェイの SRST を有効にする

はじめる前に

- デバイス プールへの SRST リファレンスの割り当て，（119 ページ）
- （オプション）次のいずれかのタスクを実行します。
  - クラスタの接続モニタ間隔の設定，（120 ページ）
  - デバイス プールの接続モニタ間隔の設定，（121 ページ）

手順

ステップ 1 SRST ゲートウェイ（ルータ）にログインします。

ステップ 2 **Call-manager-fallback** コマンドを入力します。
このコマンドは、ルータの SRST を有効にします。

ステップ 3 **max-ephones**max-phones コマンドを入力します。ここで、max-phones は、サポート対象の Cisco IP Phone の最大数です。

ステップ 4 **max-dn**max-directory-numbers コマンドを入力します。ここで、max-directory-numbers は、ルータでサポートされている電話番号（DN）の最大数または仮想音声ポートです。

ステップ 5 **ip source-address**ip-address コマンドを入力します。ここで、ip-address は、一般的にルータのイーサネット ポートのアドレスの 1 つであるルータ IP アドレスよりも前から存在します。
このコマンドは、SRST ルータで、特定の IP アドレスの Cisco IP phones からのメッセージを受信できるようにします。

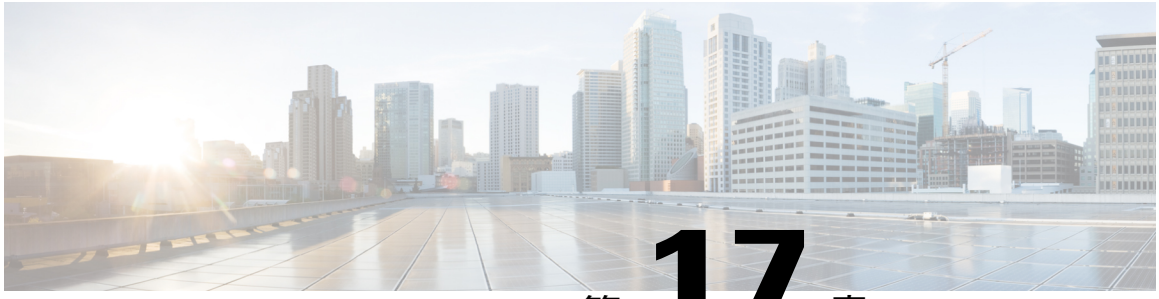
SRST の制限事項

制約事項	説明
SRST リファレンスの削除	デバイスプールまたはそのほかの項目によって使用中の SRST リファレンスは削除できません。SRST リファレンスを使用しているデバイスプールを特定するには、[SRST リファレンスの設定（SRST Reference Configuration）] ウィンドウの [依存関係レコード（Dependency Records）] リンクをクリックします。システムで依存関係レコードが有効でない場合、[依存関係レコード要約（Dependency Records Summary）] ウィンドウにメッセージが表示されます。使用中の SRST リファレンスを削除しようとすると、Cisco Unified Communications Manager はエラー メッセージを表示します。現在使用中の SRST リファレンスを削除する前に、次のタスクのいずれかまたは両方を実行します。 • 削除する SRST リファレンスを使用しているすべてのデバイス プールに別の SRST リファレンスを割り当てます。 • 削除する SRST リファレンスを使用しているデバイス プールを削除します。 （注） 削除してもよい SRST リファレンスかどうかを必ず確認し、SRST リファレンスを削除します。削除した SRST リファレンスを元に戻すことはできません。間違って削除した SRST リファレンスは、再作成する必要があります。

第 III 部

ダイヤル プランの設定

- ダイヤル プランの概要，127 ページ
- パーティションの設定，131 ページ
- 国内番号計画のインストール，139 ページ
- コール ルーティングの設定，145 ページ
- ハント パイロットの設定，165 ページ
- トランスレーション パターンの設定，173 ページ
- トランスフォーメーション パターンの設定，175 ページ
- ダイヤル ルールの設定，179 ページ
- クラスタ間ルックアップ サービスの設定，189 ページ
- グローバル ダイヤル プラン レプリケーションの設定，205 ページ
- URI ダイヤリングの設定，219 ページ



第 17 章

ダイヤル プランの概要

- ダイヤル プランについて，127 ページ
- ダイヤル プランの前提条件，127 ページ
- ダイヤル プラン設定，127 ページ

ダイヤル プランについて

ダイヤル プランで、Cisco Unified Communications Manager システムにコールのルーティングに関する指示を出します。ダイヤル プランを設定する場合、次のようなルールを定義します。

- 許可するコールのタイプ
- コールの発信時にシステムが使用する優先パスと代替パス
- 内線番号のダイヤル方法
- 着信者番号と発信者番号の表示方法

ダイヤル プランの前提条件

ダイヤル プランを設定する前に、次のタスクを完了します。

- 初期設定タスク フロー，（9 ページ）
- 着信コールと発信コールの設定，（61 ページ）

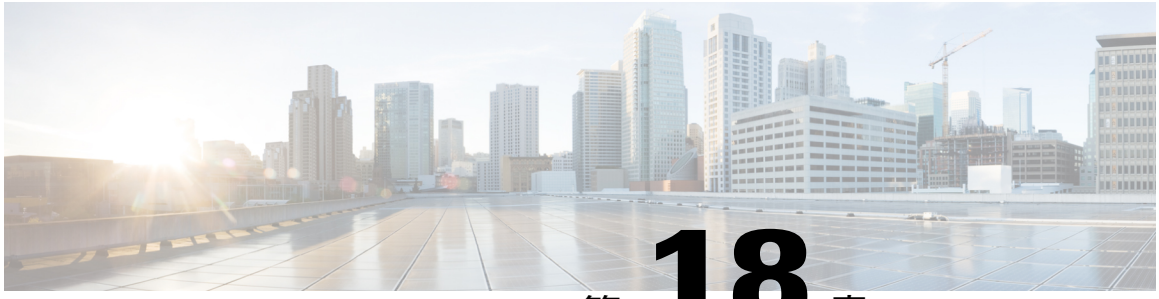
ダイヤル プラン設定

次のタスク フローを実行すると、システムのダイヤル プランを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	パーティション設定のタスク フロー, （133 ページ）	パーティションを設定して、電話番号（DN）の論理グループと、到達可能性の特徴が類似したルート パターンを作成します。パーティションを作成することで、ルート プランが組織、場所、コール タイプに基づいた論理サブセットに分割されることになり、コール ルーティングが容易になります。
ステップ 2	国内番号計画インストールのタスク フロー, （140 ページ）	これはオプションです。[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] では、デフォルトで、北米番号計画（NANP）を使用できます。設定されているダイヤル プラン要件が異なる国の場合は、シスコの国際ダイヤル プランをインストールし、それを使用して、要件特有の一意の番号計画を作成できます。国内の番号計画を使用している場合は、@ 記号とルート フィルタを使用するルート パターンを設定して、国内コール、国際コール、長距離コール、緊急コール用にパターンを作成できます。 国内番号のダイヤル プランの使用はオプションです。国内の番号契約を使用しない場合は、手動で設定できます。
ステップ 3	コール ルーティング設定のタスク フロー, （146 ページ）	ルート プランを設定して、内線コールおよび外線コールをプライベート ネットワークまたは公衆電話交換網（PSTN）にルーティングします。
ステップ 4	ハント パイロットの設定タスク フロー, （166 ページ）	コールを1つ以上の番号のリストに拡張する場合は、ハント パイロットを設定し、各リストでハント オーダーを指定します。コールをこれらのリストからハント パーティに拡張し、パーティが応答できない、または話し中の場合、ハンティングは、次のハント パーティで再開します。
ステップ 5	トランスレーション パターンの設定タスク フロー, （174 ページ）	トランスレーション パターンを設定して、音声ゲートウェイから Cisco Unified Communications Manager に着信番号を操作します。システムが着信エンドポイントにコールを転送する前に、トランスレーション パターンを使用して発信者番号および着信者番号を変更できます。このトランスレーションは透過的なため、公衆電話からの内線をプライベート ネットワークに紐付けることができます。
ステップ 6	トランスフォーメーション パターンの設定タス	着信コールに表示される発信者番号を変更する場合は、電話のトランスフォーメーション パターンを設定します。発信者番号を変更する場合、または着信者番号の表示が発信コー

	コマンドまたはアクション	目的
	ク フロー, （175 ページ）	ルに表示される場合は、ゲートウェイまたはトランクのトランスフォーメーション パターンを設定します。または、トランスフォーメーション パターンを使用して、アウトバウンドのリダイレクト番号（SIP デバイスの Diversion ヘッダーとして知られる）を変更することもできます。
ステップ 7	ダイヤル ルールの設定タスク フロー, （180 ページ）	さまざまな種類のダイヤル ルール（アプリケーション ダイヤル ルール、ディレクトリ検索ダイアル ルール、SIP ダイヤル ルール）を設定できます。 • Cisco Web Dialer および Cisco Unified Communications Manager Assistant など、アプリケーションのダイアル ルールの優先順位を追加し、ソートするには、アプリケーション ダイヤル ルールを設定します。 • ディレクトリ検索ダイヤル ルールを設定して、発信者の識別情報を、ディレクトリで検索可能な番号に変換します。 • SIP ダイヤル ルールを設定して、SIP を実行している電話のダイヤルパターンを作成します。これは、レガシーの SIP 電話の一般的な手順です。
ステップ 8	ILS 設定のタスク フロー, （190 ページ）	クラスタ間検索サービス（ILS）を設定して、リモートの Cisco Unified Communications Manager クラスタのネットワークを作成します。ペアのクラスタに ILS を設定し、それらのクラスタに参加して、ILS ネットワークを形成します。
ステップ 9	グローバル ダイヤル プラン レプリケーションのタスクフロー, （208 ページ）	クラスタ間検索サービス（ILS）ネットワークを設定している場合は、国際ダイヤルプランの複製を設定して、ILS ネットワーク全体を対象とした国際ダイヤル プランを作成できます。その結果、クラスタ間のディレクトリ URI ダイアルおよび代替番号が含まれます。
ステップ 10	URI ダイヤリング設定のタスク フロー, （221 ページ）	ディレクトリ URI をコール アドレスとして使用して、コールをエンドポイントにルーティングする場合の URI ダイヤルを設定します。ディレクトリ URI の形式は username@host で、ホスト部分は IPv4 アドレスまたは完全修飾ドメイン名です。



第 18 章

パーティションの設定

- パーティションの概要，131 ページ
- パーティション設定のタスク フロー，133 ページ
- パーティションの連携動作と制約事項，137 ページ

パーティションの概要

パーティションとは次のいずれかの論理グループです。

- ルート パターン
- 電話番号（DN）
- トランスレーション パターン
- 変換パターン
- ユニバーサル リソース識別子（URI）
- ハント パイロット

パーティションを作成することで、ルートプランが組織、場所、コールタイプに基づいた論理サブセットに分割されることになり、コール ルーティングが容易になります。

パーティションはコーリング サーチ スペース（CSS）と一緒に機能します。コーリング サーチ スペースとは、パーティションの順序付きリストです。コーリングサーチスペースは、コールを行うときに、IPフォン、ソフトフォン、ゲートウェイなどの発信側デバイスが検索できるパーティションを決定します。

サービス クラス

パーティションとコーリング サーチ スペース（CSS）を使用してサービス クラスを設定できます。次の表に、PSTN アクセスを提供するサービス クラス用に作成できるパーティションとコーリング サーチ スペースの例を示します。

- 緊急コール
- ローカル コール
- 国内コール
- 国際ダイヤリング

表 *8*：パーティションとコーリング サーチ スペースの例

[コーリングサーチスペース（**Calling Search Space**）]	ルート パーティション **1**	ルート パーティション **2**	ルート パーティション **3**	機能
Base_CSS	Base_PT	—	—	• 緊急（Emergency） • On-net
LocalPSTN_CSS	PSTN_Local_PT	—	—	• 緊急（Emergency） • On-net • [ローカル（Local）]
NationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	—	• 緊急（Emergency） • On-net • [ローカル（Local）] • 国内
InternationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	PSTN_Intl_PT	• 緊急（Emergency） • On-net • [ローカル（Local）] • 国内 • 国際

デバイスは自動的に、Base_CSS などのコーリング サーチ スペースに登録されます。これにより、すべてのデバイスでオフネット番号と緊急オンネット番号の両方にダイヤルできるようになります。ローカル 7 桁またはローカル 10 桁、国内、および国際ダイヤリング機能を提供するには、ユーザ デバイス プロファイルで残りのコーリング サーチ スペースを電話番号に割り当てる必要があります。

パーティション設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	パーティションの設定, （133 ページ）	パーティションを設定して、到達可能性の特徴が類似したシステム リソースの論理グループを作成します。次のいずれに対してもパーティションを作成できます。 • ルート パターン • 電話番号（DN） • トランスレーション パターン • 変換パターン • ユニバーサル リソース識別子（URI） • ハント パイロット パーティションを作成することで、ルートプランが組織、場所、コールタイプに基づいた論理サブセットに分割されることになり、コール ルーティングが容易になります。
ステップ 2	コーリング サーチ スペースの設定, （135 ページ）	コーリング サーチ スペースは、デバイスに割り当てられたパーティションの番号付きリストです。コーリング サーチ スペースでは、発信側デバイスが電話を終了しようとする際に検索できるパーティションが決定されます。

パーティションの設定

パーティションを設定して、到達可能性の特徴が類似したシステム リソースの論理グループを作成します。次のいずれに対してもパーティションを作成できます。

- ルート パターン

- 電話番号（DN）
- トランスレーション パターン
- 変換パターン
- ユニバーサル リソース識別子（URI）
- ハント パイロット

パーティションを作成することで、ルートプランが組織、場所、コールタイプに基づいた論理サブセットに分割されることになり、コール ルーティングが容易になります。複数のパーティションを設定できます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックして新しいパーティションを作成します。

ステップ 3 [パーティション名、説明（Partition Name, Description）] フィールドに、ルート プランに固有のパーティション名を入力します。
パーティション名には、英数字とスペースの他にハイフン（-）とアンダースコア（_）を使用できます。パーティション名に関するガイドラインについては、オンライン ヘルプを参照してください。

ステップ 4 パーティション名の後にカンマ（,）を入力し、パーティションの説明を同じ行に入力します。
説明には、任意の言語で最大50文字を使用できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）、角括弧（[]）は使用できません。
説明を入力しなかった場合は、Cisco Unified Communications Manager が、このフィールドに自動的にパーティション名を入力します。

ステップ 5 複数のパーティションを作成するには、各パーティション エントリごとに 1 行を使います。

ステップ 6 [スケジュール（Time Schedule）] ドロップダウン リストから、このパーティションに関連付けるスケジュールを選択します。
スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）] を選択した場合は、パーティションが常にアクティブになります。

ステップ 7 次のオプション ボタンのいずれかを選択して、[タイム ゾーン（Time Zone）] を設定します。

- [発信側デバイス（Originating Device）]：このオプション ボタンを選択すると、発信側デバイスのタイムゾーンと [スケジュール（Time Schedule）] が比較され、パーティションが着信コールの受信に使用できるかどうかが判断されます。
- [特定のタイム ゾーン（Specific Time Zone）]：このオプション ボタンを選択した後、ドロップダウン リストからタイム ゾーンを選択します。選択されたタイム ゾーンと [スケジュール

（Time Schedule）] が比較され、着信コールの受信にパーティションが使用できるかどうかが判断されます。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

パーティション名のガイドライン, （135 ページ）

パーティション名のガイドライン

コーリング サーチ スペースのパーティションのリストは最大 1024 文字に制限されています。つまり、CSS 内のパーティションの最大数は、パーティション名の長さによって異なります。次の表を使用して、パーティション名が固定長である場合のコーリングサーチスペースに追加できるパーティションの最大数を決定します。

表 *9*：パーティション名のガイドライン

パーティション名の長さ	パーティションの最大数
2 文字	340
3 文字	256
4 文字	204
5 文字	172
。..	...
10 文字	92
15 文字	64

コーリング サーチ スペースの設定

コーリング サーチ スペースは、通常はデバイスに割り当てられるルート パーティションの番号付きリストです。コーリングサーチスペースでは、発信側デバイスが電話を終了しようとする際に検索できるパーティションが決定されます。

はじめる前に

パーティションの設定, （133 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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 [名前（Name）] フィールドに、名前を入力します。
各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

ステップ 4 [説明（Description）] フィールドに、説明を入力します
説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 [使用可能なパーティション（Available Partitions）] ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。
- パーティションが複数ある場合は、コントロール（Ctrl）キーを押したまま、適切なパーティションを選択します。

ステップ 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）] フィールドにパーティションを移動させます。

ステップ 7 （任意） [選択されたパーティション（Selected Partitions）] ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

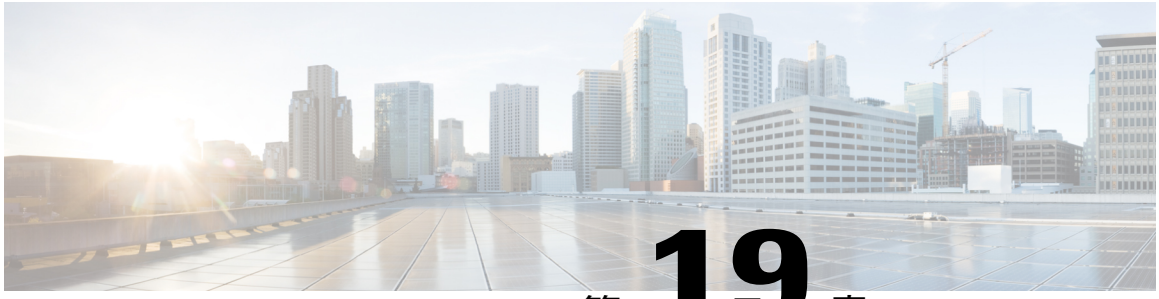
ステップ 8 [保存（Save）] をクリックします。

パーティションの連携動作と制約事項

パーティションの制限

表 *10* : パーティションの制限

機能またはアクション	制約事項
パーティションの削除	パーティションを削除する前に、次のいずれかのタスクが完了していることを確認します。 • コーリング サーチ スペース、デバイス、または削除するパーティションを使用しているその他の項目に異なるパーティションを割り当てる。 • コーリング サーチ スペース、デバイス、または削除するパーティションを使用しているその他の項目を削除する。 削除されたパーティションは取得できなくなるため、正しいパーティションを削除していることを慎重に確認してください。誤ってパーティションを削除した場合は、それを再構築する必要があります。



第 19 章

国内番号計画のインストール

- 国内番号計画の概要，139 ページ
- 国内番号計画の前提条件，139 ページ
- 国内番号計画インストールのタスク フロー，140 ページ

国内番号計画の概要

Cisco Unified Communications Manager はデフォルトの北米番号計画（NANP）を提供します。ダイヤルプランの要件が異なる国では、シスコ国際ダイヤルプランをインストールし、要件に固有の一意の番号計画を作成するために使用できます。

この章では、国内番号計画をインストールする方法について説明します。国内番号計画の使用方法の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager Dial Plan Deployment Guide*』を参照してください。

国内番号計画の前提条件

北米以外の国で国内番号計画をインストールする場合、現在のリリースの国際ダイヤル計画を含む Cisco Option Package（COP）ファイルをダウンロードします。COP ファイルは、IDP v.*x* の命名規則を使用し、シスコの Web サイトから入手できます。

- https://software.cisco.com/download/navigator.html

このファイルを Cisco Unified Communications Manager がアクセスできる外部 FTP または SFTP サーバに配置します。

国内番号計画インストールのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	COP ファイルのインストール, （140 ページ）	これはオプションです。北米以外の国における番号計画をインストールするには、現在のリリース用の国際ダイヤルプランを含むシスコのオプションパッケージ（COP）ファイルをダウンロードします。
ステップ 2	国内の番号計画のインストール, （142 ページ）	クラスタ内のそれぞれの Cisco Unified Communications Manager ノードに国内の番号計画をインストールします。北米以外の国における国内の番号計画をインストールしている場合に限って、次の手順を実行します。
ステップ 3	CallManager サービスの再起動, （142 ページ）	サービスを再起動すると変更が反映されます。

COP ファイルのインストール

国際ダイヤルプランを含むシスコのオプションパッケージ（COP）ファイル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 Cisco Unified Communications Manager のパブリッシャ ノードで、この手順を開始します。Cisco Unified Communications OS 管理で、[ソフトウェア アップグレード（Software Upgrades）] > I[インストール（nstall）] を選択します。
[ソフトウェアのインストール/アップグレード（Software Installation/Upgrade）] ウィンドウが表示されます。

ステップ 2 [ソース（Source）] フィールドで、[リモート ファイル システム（Remote File System）] を選択します。

ステップ 3 [ソフトウェアのインストール/アップグレード（Software Installation/Upgrade）] ウィンドウで、フィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」を参照してください。

ステップ 4 [Next] をクリックします。

ウィンドウが更新され、使用可能なソフトウェアのオプションとアップグレードのリストが表示されます。

ステップ 5 [オプション/アップグレード（Options/Upgrades）] ドロップダウンリストで、[DP COP] ファイルを選択して、[次へ（Next）] をクリックします。
[インストール ファイル（Installation File）] ウィンドウが開き、FTP サーバからファイルをダウンロードします。ウィンドウにダウンロードの進捗が表示されます。

ステップ 6 [チェックサム（Checksum）] ウィンドウが表示されたら、そのチェックサムの値をダウンロードしたファイルのチェックサムの値と比較検証します。

ステップ 7 [次へ（Next）] をクリックして、ソフトウェア アップグレードに進みます。
警告メッセージとして、インストールするために選択した DP COP ファイルが表示されます。

ステップ 8 [Install（インストール）] をクリックします。
[インストール状況（Install Status）] ウィンドウが表示されます。

ステップ 9 [終了（Finish）] をクリックします。

ステップ 10 Unified Communications Manager サブスクライバ ノードで、この手順を繰り返します。クラスタ内の全ノードに COP ファイルをインストールする必要があります。

次の作業

国内の番号計画のインストール, （142 ページ）

関連トピック

COP ファイル インストールのフィールド, （141 ページ）

COP ファイル インストールのフィールド

フィールド	説明
[ディレクトリ（Directory）]	COP ファイルが配置されているディレクトリを入力します。
リモート サーバ（Remote Server）	COP ファイルが配置されているサーバのホスト名または IP アドレスを入力します。
リモート ユーザ（Remote User）	リモート サーバのユーザ名を入力します。
リモート パスワード（Remote Password）	リモート サーバのパスワードを入力します。
[転送プロトコル（Transfer Protocol）]	リモート サーバと接続する場合に使用するプロトコルを選択します。

国内の番号計画のインストール

北米以外の国における国内の番号計画をインストールしている場合に限って、次の手順を実行します。

クラスタ内のそれぞれの Cisco Unified Communications Manager ノードに国内の番号計画をインストールします。Cisco Unified Communications Manager publisher ノードから始めます。

はじめる前に

COP ファイルのインストール, （140 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[コールルーティング（Call Routing）] > [ダイヤルプランインストーラ（Dial Plan Installer）] を選択します。

ステップ 2 検索条件を入力して [検索（Find）] をクリックします。

ステップ 3 インストールするダイヤル プランのバージョンを [利用可能なバージョン（Available Version）] ドロップダウンリストから選択します。

ステップ 4 [Install（インストール）] をクリックします。
ステータスに、ダイヤル プランがインストールされたことが表示されます。

ステップ 5 クラスターのサブスクライバ ノードごとにこの手順を繰り返します。

次の作業

CallManager サービスの再起動, （142 ページ）

CallManager サービスの再起動

はじめる前に

国内の番号計画のインストール, （142 ページ）

手順

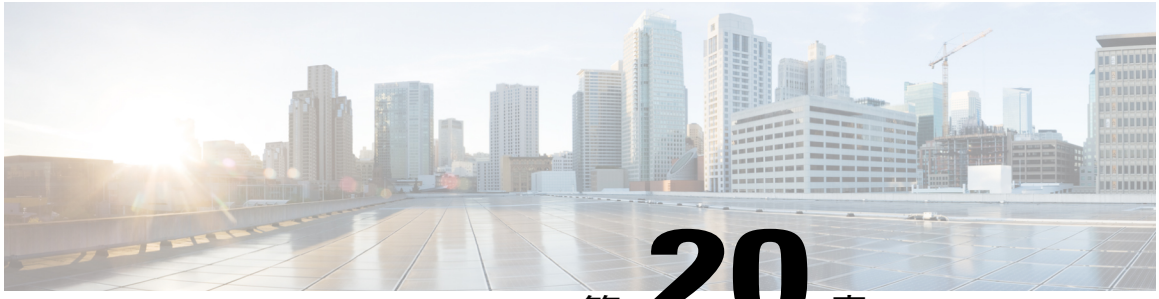
ステップ 1 Cisco Unified Serviceability インターフェイスで、[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] を選択します。

ステップ 2 [サーバ（Servers）] ドロップダウンリストから、[Cisco Unified Communications Manager] サーバを選択します。
CM のサービス領域で、[サービス名（Service Name）] 列の Cisco CallManager が表示されます。

ステップ 3 Cisco CallManager サービスに対応するラジオ ボタンをクリックします。

ステップ 4 [再起動（Restart）] をクリックします。

サービスが再起動し、「サービスは正常に再起動しました（Service Successfully Restarted）」というメッセージが表示されます。



第 20 章

コール ルーティングの設定

- コール ルーティングの概要，145 ページ
- コール ルーティングの前提条件，146 ページ
- コール ルーティング設定のタスク フロー，146 ページ

コール ルーティングの概要

システムは、クラスタ間のコールをルーティングする方法と、外部のコールをプライベート ネットワークまたは公衆電話交換網（PSTN）にルーティングする方法をルート プランにより判断します。設定したルート プランにより、各コール タイプをルーティングするためにシステムが使用するパスが指定されます。たとえば、オンネット コールに IP ネットワークを使うルート プラン、またはローカル PSTN コールにあるキャリアを使い、国際コールに別のキャリアを使うルート プランを作成できます。

システムは、ルート プランに、次のコンポーネントを使用する 3 階層のアプローチを用います。

- ルート パターン：外部の着信番号に一致するルート パターン設定を検索して、一致した番号により、ゲートウェイまたは対応するルート リストを選択します。
- ルート リスト：コールが使用できるパスの優先順位付けリスト
- ルート グループ：使用可能なパスのグループ。コールをゲートウェイおよびトランクに配信します。

これらの構成要素に加えて、ルート プランは次のコンポーネントを含みます。

- ローカル ルート グループ：ゲートウェイへのアクセスに使用されるルート パターンから PSTN ゲートウェイの場所を切り離します。
- ルート フィルタ：ルート パターンが適用されないように、特定の番号を制限します。
- 自動代替ルーティング：十分な帯域幅がない場合に、PSTN またはそのほかのネットワークを介したコールを、自動的に再ルーティングします。

- 時刻ルーティング：スケジュールを作成し、着信コールを受信するパーティションを使用できる時間を指定します。

コール ルーティングの前提条件

- パーティション設定のタスク フロー, （133 ページ）の操作を実行します。
- 次の情報について確認してください。
  - 内線番号
  - 各ゲートウェイにルーティングするコールの一覧表

コール ルーティング設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ルート パターンの設定, （147 ページ）	特定のデバイスにコールを導き、特定の数字パターンを含めるか排除するようにルート パターンを設定します。ゲートウェイ、トランク、1つ以上のルート グループを含むルート リストにルートパターンを割り当てることができます。
ステップ 2	ルート グループの設定, （152 ページ）	これはオプションです。ゲートウェイのデバイスの選択順序を設定するようにルート グループを設定します。ルート グループには、1 つ以上のデバイスが含まれています。
ステップ 3	ルート リストの設定, （153 ページ）	これはオプションです。ルート リストには、1つ以上のルート グループが含まれています。ルート グループの選択順序を制御するためにルート リストを設定します。ルート リストを設定すると、少なくとも 1 つのルート グループを設定する必要があります。
ステップ 4	ローカルなルート グループを設定するには、次のサブマスクを完成します。 • ローカル ルート グループ名の設定, （155 ページ） • ローカル ルート グループとデバイス	これはオプションです。ローカル ルート グループを設定して、必要なルート リストの数を減らすことができます。リストのポイントを、PSTN ゲートウェイの場所に基づいて、システムが発信をルーティングするのに使用する PSTN ゲートウェイにルーティングします。代替として、ゲートウェイへのアクセスに使用されるルート パターンから PSTN ゲートウェイの場所を分離するためにローカル ルート グループを使用できます。この設定により、異なる場所からの電話機その他のデバイスが単一のルート パターンのセッ

	コマンドまたはアクション	目的
	プールの関連付け, （156 ページ） • ルート リストへのローカル ルート グループの追加, （156 ページ）	トを使用すると同時に、Cisco Unified Communication Manager がコールをルーティングする正しいゲートウェイを選択できます。 たとえば、ローカルルートグループを使用すると、国のすべての市で別々のダイヤル プランを持つのではなく、国全体で単一のダイヤル プランを持つことができます。このアプローチが有効なのは、一元化されたコール導入のシナリオについてだけです。
ステップ 5	ルート フィルタの設定, （157 ページ）	ルート パターンが許可する特定の数字を制限するためにルーティングのフィルタを使用します。ダイヤルプランインストーラを使用している場合、ルート フィルタは必須です。つまり、ダイヤル プラン ファイルをインストールして、その番号計画に基づいてルート パターンを設定します。ダイヤル プランを手動で設定している場合、ルート フィルタはオプションです。 ダイヤル プランを手動で設定すると、@ワイルドカードを含むルートパターンがあるたびにルートフィルタを設定する必要があります。ルート パターンに@ワイルドカードが含まれていると、システムは、ルート フィルタで指定する番号計画に応じて、コールをルーティングします。
ステップ 6	時間帯ルーティングの設定, （161 ページ）	これはオプションです。あるパーティションがいつ、着信コールの受信に利用可能かを指定するタイム スケジュールを作成します。

ルート パターンの設定

Cisco Unified Communications Manager は、ルート パターンを使用して、内部コールと外部コールをルーティングまたはブロックします。ルート パターンは、ゲートウェイ、トランク、または 1 つ以上のルート グループを含むルート リストに割り当てることができます。

（注） ルート パターンでゲートウェイを直接指定することもできますが、ルート リストおよびルート グループを設定することを推奨します。このアプローチでは、コール ルーティングの柔軟性に加え、拡張性を最大限に発揮します。

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）] > [ルート/ハント（Route/Hunt）] > [ルート パターン（Route Pattern）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいルート パターンを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存のルート パターンの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストからルート パターンを選択します。

[ルート パターンの設定（Route Pattern Configuration）] ウィンドウが表示されます。

ステップ 3 [ルート パターンの設定（Route Pattern Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

（オプション） ルート グループの設定, （152 ページ）

関連トピック

ルート パターンのワイルドカードと特殊文字, （148 ページ）
ドット前の番号削除の例, （151 ページ）
番号プレフィックスの例, （151 ページ）
オンネットおよびオフネット パターンの例, （151 ページ）
ブロックおよびルート パターンの例, （152 ページ）

ルート パターンのワイルドカードと特殊文字

ルート パターンにワイルドカードおよび特殊文字を使用すると、1 つのルート パターンで、ある電話番号（アドレス）の範囲を指定できます。また、これらのワイルドカードおよび特殊文字を使って指示を組み立てると、Cisco Unified Communications Manager が処理した番号を隣接システムに送信できます。

Cisco Unified Communications Manager がサポートするワイルドカードおよび特殊文字を次の表で説明します。

表 *11*：ワイルドカードおよび特殊文字

文字	説明	例
@	@ 記号（@）ワイルドカードは、国別番号計画のすべての番号に一致します。 各ルート パターンで、@ ワイルドカードは 1 文字だけ使用できます。	ルート パターン 9.@ は、国別番号計画が認識するすべての電話番号をルーティングまたはブロックします。 @ ワイルドカードが含む、国別番号計画の番号のルート パターンの例を次に示します。 • [0] • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X ワイルドカードは、0 ～ 9 の範囲にある数字の任意の 1 桁に一致します。	ルート パターン 9XXX は、9000 ～ 9999 の範囲のすべての数字をルーティングするか、またはブロックします。
!	感嘆符（!）ワイルドカードは、0 ～ 9 の範囲にある数字の 1 桁以上に一致します。	ルート パターン 91! は、910 ～ 91999999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
?	疑問符（?）ワイルドカードは、直前の数字またはワイルドカード値の 0 回以上の繰り返しに一致します。	ルート パターン 91X? は、91 ～ 91999999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
+	プラス記号（+）ワイルドカードは、直前の数字またはワイルドカード値の 1 回以上の繰り返しに一致します。	ルート パターン 91X+ は、910 ～ 91999999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
[]	角カッコ（[ ]）文字は、値の範囲を囲みます。	ルート パターン 813510[012345] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。

文字	説明	例
-	ハイフン（-）文字は、角カッコと一緒に使用して値の範囲を示します。	ルート パターン 813510[0-5] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
^	ハット（^）文字は、角カッコと一緒に使用して値の範囲外を示します。この文字は、開始角カッコ（[）の直後に配置してください。 各ルート パターンで、^ 文字は 1 文字だけ使用できます。	ルート パターン 813510[^0-5] は、8135106 ～ 8135109 の範囲のすべての数字をルーティングするか、またはブロックします。
.	デリミタとして使用されるドット（.）文字は、Cisco Unified Communications Manager のアクセス コードをディレクトリ番号から分離します。 この特殊文字を、桁を無視する指定と一緒に使用すると、隣接システムに番号を送信する前に Cisco Unified Communications Manager のアクセス コードを削除できます。 各ルート パターンで、（.）文字は 1 文字だけ使用できます。	ルート パターン 9.@ は、最初の 9 を、国別番号計画に発信する Cisco Unified Communications Manager アクセス コードとして認識します。
*	アスタリスク（*）文字は、特別な着信番号の追加の桁として利用できます。	ルート パターン *411 を設定して、内部オペレータのディレクトリ案内の利用を可能にします。
#	シャープ（#）文字は、一般にダイヤルシーケンスの終了を特定します。 # 文字がパターンの最後の文字になるようにします。	ルート パターン 901181910555# は、国別番号計画内からダイヤルされる国際番号をルーティングまたはブロックします。末尾の 5 の後の # 文字は、この桁をシーケンスの最後の桁として特定します。
\+	\+ のように、バックスラッシュにプラス記号が続くと、国際番号用エスケープ文字 + の設定を示します。	\+ の使用は、国際番号用エスケープ文字 + がワイルドカードではなく、ダイヤル可能な桁であることを意味します。

ドット前の番号削除の例

ルート パターンでのドット前の番号削除の一例は、外部回線に接続するために、電話ユーザがアクセス コードをダイヤルするように設定する場合です。北米では、電話ユーザは通常、9 をダイヤルして外部回線にアクセスします。これは、次のルート パターンを使用して指定できます。

- ローカル コール：9.@ または 9.[2-9]XXXXXX
- 国内コール：9.1[2-9]XX
- 国際コール：9.011!#

これらのパターンでは、9 が外部回線のアクセス コードであり、ドット（.）はどの番号がネットワーク内部のもので、どの番号が外部の番号であるかを示すことでルート パターンを形式化するために役立つ区切り文字です。システムがダイヤルされた番号を PSTN へ送信する場合は、PSTN がコールをルーティングできるように、ディジット破棄オプションを使用して、ドット前の番号をダイヤルされた文字列から取り除くことができます。

関連トピック

ルート パターンのワイルドカードと特殊文字, （148 ページ）
ルート パターンの設定, （147 ページ）

番号プレフィックスの例

ルートパターンで番号プレフィックスを使用する一例は、サイト間でオンネットダイヤリングを設定する場合です。組織内のユーザが 8＋XXX-XXXX をダイヤルしてサイト間でコールを発信できるように、ルート パターンを作成できます。オフネット コールの場合は、コールを E.164 形式で PSTN にルーティングできるように、プレフィックス番号（8）を削除し、新しいプレフィックス 1<area code> を追加できます。

関連トピック

ルート パターンのワイルドカードと特殊文字, （148 ページ）
ルート パターンの設定, （147 ページ）

オンネットおよびオフネット パターンの例

[コールの分類（Call Classification）] フィールドを使用して、ルート パターンを OffNet または OnNet として設定できます。ユーザがセカンダリ ダイヤル トーンによって、コールが組織の外部に接続されることを認識できるようにする場合は、コールをオフネットとして分類できます。たとえば、外部回線にアクセスするには 9 をダイヤルするようにユーザに求めるルート パターンを作成し、それをオフネットパターンとして分類した場合、システムは次のダイヤル トーンを提供します。

- ユーザが 9 をダイヤルする前に電話がオフフックされたときのダイヤル トーン
- ユーザが 9 をダイヤルした後のセカンダリ ダイヤル トーン。これは、システムが公衆電話交換網（PSTN）にコールを発信する準備が整ったことを示します。

このオプションを使用する場合は、必ず、[デバイスのオーバーライドを許可（Allow Device Override）] チェックボックスをオフにしてください。

関連トピック

ルート パターンのワイルドカードと特殊文字, （148 ページ）
ルート パターンの設定, （147 ページ）

ブロックおよびルート パターンの例

ブロックおよびルート パターンを使用して、ルーティングする必要のない発信コールまたは着信コールを阻止できます。ブロック パターンを使用すると、次を実行できます。

- 特定のパターンをブロックする。たとえば、パターン 91900XXXXXXX は、ユーザが 900 サービスにコールを発信するのを阻止します。
- 特定の市外局番と場所へのコールをブロックすることで電話料金の詐欺行為を防ぐ

関連トピック

ルート パターンのワイルドカードと特殊文字, （148 ページ）
ルート パターンの設定, （147 ページ）

ルート グループの設定

システムが発信コール用ゲートウェイを選択するときの優先順位を示したルート グループを設定します。グループ内の任意のゲートウェイでコールを発信できるように、同様の特性を持つゲートウェイをグループ化するには、次の手順を使用します。ルート グループを設定したときに指定した順序で、システムは使用するゲートウェイを選択します。

1 つのデバイスを複数のルート グループに割り当てることができます。

はじめる前に

ルート パターンの設定, （147 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[コール ルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルート グループ（Route Group）] を選択します。[ルート グループの設定（Route Group Configuration）] ウィンドウが表示されます。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいルート グループを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存のルート グループの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストからルート グループを選択します。

[ルート グループの設定（Route Group Configuration）] ウィンドウが表示されます。

ステップ 3 [ルート グループの設定（Route Group Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ルート リストの設定, （153 ページ）

これはオプションです。ローカル ルート グループ名の設定, （155 ページ）

ルート リストの設定

一連のルート グループを特定し、優先順位を付けるには、ルート リストを設定します。Cisco Unified Communications Manager はルート リストの順番を使用して、発信コールで使用可能なデバイスを検索します。

ルート リストに含められるのは、ルート グループとローカル ルート グループだけです。

（注） 発信コールがルート リストを介して伝送されると、コールが終了する前に警告メッセージを送信しないように、ルート リストのプロセスは、発信デバイスをロックします。発信デバイスがロックされた後は、ハント リストが着信コールの追跡を停止します。

はじめる前に

ルート グループの設定, （152 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）]>[ルート/ハント（Route/Hunt）]>[ルート リスト（Route List）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいルート リストを追加するには、[新規追加（Add New）] ボタンをクリックします。

- 既存のルート リストの設定を修正するには、検索条件を入力し、[検索（Find）] をクリックして表示された一覧からルート リストを選択します。

ステップ 3 [ルート リストの設定（Route List Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 ルート リストにルート グループを追加するには、[ルート グループの追加（Add Route Group）] ボタンをクリックします。

ステップ 5 [ルート グループ（Route Group）] ドロップダウン リストから、ルート リストに追加するルート グループを選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [設定の適用（Apply Config）] をクリックします。

次の作業

（オプション） ローカル ルート グループを設定, （154 ページ）

ローカル ルート グループを設定

これはオプションです。ローカル ルート グループを設定して、必要なルート リストの数を減らすことができます。リストのポイントを、PSTN ゲートウェイの場所に基づいて、システムが発信をルーティングするのに使用する PSTN ゲートウェイにルーティングします。代替として、ゲートウェイへのアクセスに使用されるルート パターンから PSTN ゲートウェイの場所を分離するためにローカル ルート グループを使用できます。この設定により、異なる場所からの電話機その他のデバイスが単一のルート パターンのセットを使用すると同時に、Cisco Unified Communication Manager がコールをルーティングする正しいゲートウェイを選択できます。

たとえば、ローカル ルート グループを使用すると、国のすべての市で別々のダイヤル プランを持つのではなく、国全体で単一のダイヤル プランを持つことができます。このアプローチが有効なのは、一元化されたコール導入のシナリオについてだけです。

（注） リダイレクトされたコールのローカル ルート グループが最後にリダイレクトするパーティのローカル ルート グループに設定されている場合、Extend and Connect は標準ローカル ルート グループでのみ動作します。

リダイレクトされたコールのローカル ルート グループが発呼側のローカル ルート グループに設定されている場合、モバイル音声アクセスは標準ローカル ルート グループでのみ動作します。

はじめる前に

ルート グループの設定, （152 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	ローカル ルート グループ名の設定, （155 ページ）	これはオプションです。システムは、標準ローカル ルート グループと呼ばれるデフォルトのローカル ルート グループを提供しますが、追加のローカル ルート グループを設定できます。追加のローカル ルート グループを指定するには、次の手順を使用します。
ステップ 2	ローカル ルート グループとデバイス プールの関連付け, （156 ページ）	システムの各デバイスがそのローカル ルート グループを知るためにプロビジョニングされることを確認するためには、ローカル ルート グループをデバイス プールに関連付けます。
ステップ 3	ルート リストへのローカル ルート グループの追加, （156 ページ）	これはオプションです。ルート リストに追加できるローカル ルート グループを設定します。ローカル ルート グループを作成すると、システムはデバイス プール レベルのユーザに対して定義されたゲートウェイに発信コールをルーティングします。

ローカル ルート グループ名の設定

これはオプションです。システムは、標準ローカル ルート グループと呼ばれるデフォルトのローカル ルート グループを提供しますが、追加のローカル ルート グループを設定できます。追加ローカル ルート グループを指定するには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[コール ルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ローカル ルート グループ名（Local Route Group Names）] を選択します。

ステップ 2 [行の追加（Add Row）] をクリックします。

ステップ 3 新しいローカル ルート グループの名前と説明を入力します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ローカル ルート グループとデバイス プールの関連付け, （156 ページ）

ローカル ルート グループとデバイス プールの関連付け

発信側デバイスのデバイス プールの設定に基づいて、ローカル ルート グループが既存のルート グループを使用するよう割り当てることができます。この設定では、異なる場所にある電話機などのデバイスでルート パターンの単一のセットを使用できます。また、Cisco Unified Communication Manager では、適切なゲートウェイを選択してコールをルーティングします。

システムの各デバイスがそのローカル ルート グループを認識するようにプロビジョニングするには、ローカル ルート グループをデバイス プールに関連付けます。

はじめる前に

これはオプションです。 ローカル ルート グループ名の設定, （155 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [デバイス プール（Device Pool）] を選択します。

ステップ 2 検索条件を入力して [検索（Find）] をクリックし、結果の一覧からデバイス プールを選択します。

ステップ 3 [ローカル ルート グループの設定（Local Route Group Settings）] 領域で、[標準ローカル ルート グループ（Standard Local Route Group）] ドロップダウンリストからルート グループを選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ルート リストへのローカル ルート グループの追加, （156 ページ）

ルート リストへのローカル ルート グループの追加

ルート リストに追加するローカル ルート グループを設定します。ローカル ルート グループを作成すると、システムは、デバイス プール レベルでユーザに定義したゲートウェイに発信コールをルーティングします。

はじめる前に

ローカル ルート グループとデバイス プールの関連付け, （156 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルート リスト（Route List）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいルート リストを追加するには、[新規追加（Add New）] ボタンをクリックします。

- 既存のルート リストの設定を修正するには、検索条件を入力し、[検索（Find）] をクリックして表示された一覧からルート リストを選択します。

[ルート リストの設定（Route List Configuration）] ウィンドウが表示されます。

ステップ 3 ルート リストにローカル ルート グループを追加するには、[ルート グループの追加（Add Route Group）] ボタンをクリックします。

ステップ 4 [ルート グループ（Route Group）] ドロップダウン リストから、ルート リストに追加するローカル ルート グループを選択します。標準ローカル ルート グループの追加、または作成したカスタム ローカル ルート グループの追加ができます。

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。

ルート フィルタの設定

ルート フィルタは、コールの処理方法を決定するためにダイヤル数字列を使用します。ルート フィルタは、ワイルドカード @ を含むルート パターンを設定するときにのみ適用されます。ルート パターンにワイルドカード @ が含まれると、Cisco Unified Communications Manager は、この手順で指定した番号計画に従ってコールをルーティングします。

（注） コール ルーティングを設定する場合、単一ルート フィルタを多くのルート パターンに割り当てないようにしてください。数百のルート パターンが関連付けられたルート フィルタを編集した場合、システム コアに発生します。これは、ルート フィルタを使用するすべてのルート パターンのコール ルーティングの更新に新たなシステム処理が必要になるためです。発生しないようにするには、重複するルート フィルタを作成します。詳細については、CSCup04938 を参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [ルート フィルタ（Route Filter）] を選択します。

ステップ 2 [番号計画（Numbering Plan）] ドロップダウン リストからダイヤル プランを選択し、[次へ（Next）] をクリックします。

ステップ 3 [ルート フィルタ名（Route Filter Name）] フィールドに名前を入力します。
各ルート フィルタ名がルート プランに一意であることを確認します。

ステップ 4 ルート フィルタのタグと演算子を選択し、該当する場合は、このルート フィルタのフレーズを作成するためのデータを入力します。
使用可能なルート フィルタのタグに関する情報については、「関連項目」セクションを参照してください。

（注） EXISTS、DOES-NOT-EXIST、NOT-SELECTED の演算子を使用するタグにはルート フィルタのタグ値を入力しないでください。

ステップ 5 ルートフィルタの演算子を選択し、該当する場合は、このルートフィルタのフレーズを作成するためにデータを入力します。
使用可能なルート フィルタの演算子に関する情報については、「関連項目」セクションを参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [設定の適用（Apply Config）] をクリックします。

関連トピック

ルート フィルタ タグ, （158 ページ）
ルート フィルタの演算子, （160 ページ）
ルート フィルタの例, （161 ページ）

ルート フィルタ タグ

このタグはルートフィルタのコアコンポーネントとして機能します。タグはダイヤルされた数字列のサブセットに名前を適用します。たとえば、NANP 番号 972-555-1234 は、LOCAL-AREA-CODE（972）、OFFICE-CODE（555）、および SUBSCRIBER（1234）のルート フィルタ タグで構成されます。

ルートフィルタ タグには演算子が必要です。さらに、フィルタ対象のコールを判断するために追加の値が必要になる場合があります。

ルート フィルタ タグ フィールドの値は、ワイルドカード文字 X、*、#、[,]、-、^ および 0 ～ 9 の数字を使用できます。次の表の説明は、表記 [2-9] と XXXX を使用して実際の数字を表します。この表記の [2-9] は 2 ～ 9 の範囲で任意の 1 桁を表し、X は 0 ～ 9 の範囲で任意の 1 桁を表します。したがって、[2-9]XX の形式の 3 桁の市外局番は、実際の数字 200 ～ 999 を入力するか、すべてワイルドカードを入力するか、または該当範囲のパターンになるような実際の数字とワイルドカードを組み合わせて入力できるということです。

ルート フィルタ タグは、[ルート フィルタ設定（Route Filter Configuration）] ウィンドウの [番号計画（Numbering Plan）] ドロップダウン リスト ボックスから選択する番号計画によって変わります。次の表は、北米番号計画のルート フィルタ タグを示します。

表 *12*：ルート フィルタ タグ

タグ	説明
AREA-CODE	[2-9]XX の形式のこの 3 桁の市外局番は、長距離コールの市外局番を特定します。
COUNTRY CODE	この 1 桁、2 桁、または 3 桁のコードは、国際コールの宛先の国を指定します。

タグ	説明
END-OF-DIALING	この単一文字は、ダイヤル数字列の終了を特定します。#文字は、NANP内に着信する国際番号のダイヤル信号の終了として作用します。
INTERNATIONAL-ACCESS	この2桁のアクセスコードは、国際ダイヤルを指定します。米国内で発信するコールは、このコードに01を使用します。
INTERNATIONAL-DIRECT-DIAL	この1桁のコードは、ダイヤル直通の国際コールを指定します。米国内で発信するコールは、このコードに1を使用します。
INTERNATIONAL-OPERATOR	この1桁のコードは、オペレータが支援する国際コールを指定します。米国内で発信するコールは、このコードに0を指定します。
LOCAL-AREA-CODE	[2-9]XX の形式のこの 3 桁のローカル エリア コードは、10 桁のローカル コールのローカル エリア コードを指定します。
LOCAL-DIRECT-DIAL	この 1 桁のコードは、ダイヤル直通のローカル コールを指定します。NANP コールはこのコードに 1 を使用します。
LOCAL-OPERATOR	この 1 桁のコードは、オペレータが支援するローカル コールを指定します。NANP コールはこのコードに0を使用します。
LONG-DISTANCE-DIRECT-DIAL	この1桁のコードは、ダイヤル直通の長距離コールを指定します。NANP コールはこのコードに 1 を使用します。
LONG-DISTANCE-OPERATOR	これらの1桁または2桁のコードは、NANP内のオペレータが支援する長距離電話を指定します。オペレータが支援するコールはこのコードに 0 を使用し、オペレータ アクセスは 00 を使用します。
NATIONAL-NUMBER	このタグは、国際コールの数字列のうち国固有の部分を指定します。
OFFICE-CODE	このタグは、7 桁の電話番号の最初の 3 桁を [2-9]XX の形式で指定します。
SATELLITE-SERVICE	この1桁のコードは、国際コールの衛星接続へのアクセスを提供します。

タグ	説明
SERVICE	この 3 桁のコードは、緊急用の 911、修理用の 611、情報用の 411 などのサービスを指定します。
SUBSCRIBER	このタグは、7 桁の電話番号の最後の 4 桁をXXXX の形式で指定します。
TRANSIT-NETWORK	この 4 桁の値は、長距離キャリアを指定します。 TRANSIT NETWORK 値には、先行する 101 のキャリア アクセス コードのプレフィックスを含めないでください。詳細は、TRANSIT-NETWORK-ESCAPE を参照してください。
TRANSIT-NETWORK-ESCAPE	この 3 桁の値は、長距離キャリア ID に先行します。このフィールドの値は 101 を指定します。 TRANSIT-NETWORK-ESCAPE 値には 4 桁のキャリア ID コードを含めないでください。詳細は、TRANSIT-NETWORK を参照してください。

ルート フィルタの演算子

ルートフィルタタグの演算子は、そのタグに関連付けられるダイヤル数字列に基づいて、コールをフィルタリングするかどうかを決定します。演算子 EXISTS および DOES-NOT-EXIST は、ダイヤル数字列のその部分が存在するかどうかを単純に確認します。演算子 == は、特定の値またはパターンと実際のダイヤル番号を照合します。次の表に、ルートフィルタタグで使用できる演算子の説明を示します。

表 *13*：ルート フィルタの演算子

演算子	説明
NOT-SELECTED	このタグに関連付けられるダイヤル数字列に基づいて、コールをフィルタ処理しないように指示します。 （注） 演算子が関連付けられるタグの有無によって、Cisco Unified Communications Manager がコールをルーティングすることが妨げられることはありません。
EXISTS	このタグに関連付けられるダイヤル数字列が見つかった場合、コールのフィルタ処理を指示します。 （注） Cisco Unified Communications Manager は、タグに関連付けられている任意の数字シーケンスがダイヤル数字列に含まれる場合のみ、コールをルーティングするかブロックします。

演算子	説明
DOES-NOT-EXIST	このタグに関連付けられるダイヤル数字列が見つからなかった場合、コールのフィルタ処理を指示します。 （注） Cisco Unified Communications Manager は、タグに関連付けられている任意の数字シーケンスがダイヤル数字列に含まれない場合のみ、コールをルーティングするかブロックします。
==	このタグに関連付けられるダイヤル数字列が指定された値に一致した場合、コールのフィルタ処理を指示します。 （注） Cisco Unified Communications Manager は、タグに関連付けられていて、関連するフィールドで指定された番号範囲内である任意の数字シーケンスがダイヤル数字列に含まれる場合のみ、コールをルーティングするかブロックします。

ルート フィルタの例

例 1：AREA-CODE および演算子 DOES-NOT-EXIST を使用するルート フィルタは、市外局番を含まないすべてのダイヤル数字列を選択します。

例 2：AREA-CODE、演算子 ==、およびエントリ 515 を使用するルート フィルタは、市外局番 515 を含むすべてのダイヤル数字列を選択します。

例 3：AREA-CODE、演算子 ==、およびエントリ 5[2-9]X を使用するルート フィルタは、520 から 599 までの市外局番を含むすべてのダイヤル数字列を選択します。

例 4：TRANSIT-NETWORK、演算子 ==、およびエントリ 0288 を使用するルート フィルタは、キャリア アクセス コード 1010288 を含むすべてのダイヤル数字列を選択します。

時間帯ルーティングの設定

これはオプションです。着信コールを受信するためにパーティションが利用可能となる時間帯を指定するスケジュールを作成します。

（注） 時間帯ルーティングは、メッセージ待機インジケータ（MWI）の代行に対しては機能しません。

手順

	コマンドまたはアクション	目的
ステップ 1	時間帯の設定, （162 ページ）	時間帯を定義するには、この手順を使用します。開始時刻および終了時刻を定義し、さらに年次カレン

	コマンドまたはアクション	目的
		ダーで指定日または曜日として繰り返し間隔を指定します。
ステップ 2	タイム スケジュールの設定,（162 ページ）	スケジュールを作成するには、この手順を実行します。上記の手順で設定した時間帯は、このスケジュールの構成要素です。複数のスケジュールに時間帯を割り当てることができます。
ステップ 3	パーティションとスケジュールの関連付け,（163 ページ）	特定の時間帯に通話の完了を試みたときに、発信側デバイスが検索する場所を特定するためにパーティションとスケジュールを関連付けます。

時間帯の設定

時間帯を定義するには、この手順を使用します。開始時刻および終了時刻を定義し、さらに年次カレンダーで指定日または曜日として繰り返し間隔を指定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）]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）]>[時間帯（Time Period）] を選択します。

ステップ 2 [時間帯の設定（Time Period Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

タイム スケジュールの設定,（162 ページ）

タイム スケジュールの設定

スケジュールを作成するには、次の手順を実行します。上記の手順で設定した時間帯は、このスケジュールの構成要素です。時間帯は、複数のスケジュールに割り当てることができます。

手順

ステップ 1 [コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [タイム スケジュール（Time Schedule）] をクリックします。

ステップ 2 [スケジュールの設定（Time Schedule Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

パーティションとスケジュールの関連付け, （163 ページ）

パーティションとスケジュールの関連付け

特定の時間中にコールを完了しようとする場合、パーティションとスケジュールを関連付けてコーリング デバイスの検索が行われる場所を決定します。

はじめる前に

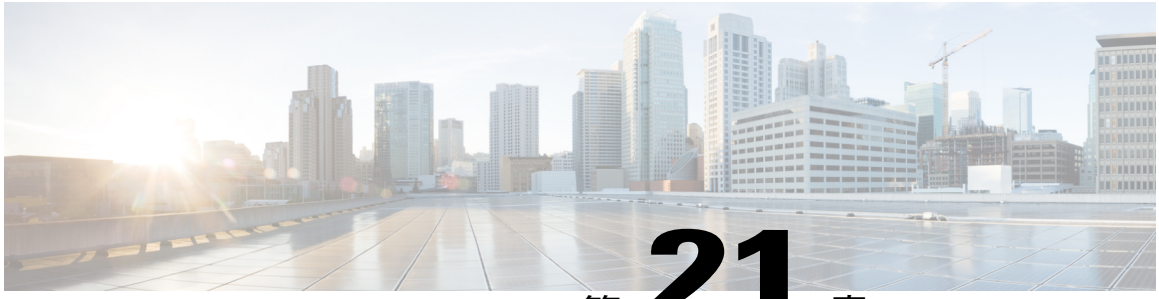
タイム スケジュールの設定, （162 ページ）

手順

ステップ 1 [コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）] をクリックします。

ステップ 2 [スケジュール（Time Schedule）] ドロップダウン リストから、このパーティションに関連付けるスケジュールを選択します。
スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）] を選択した場合は、パーティションが常にアクティブになります。

ステップ 3 [保存（Save）] をクリックします。



第 21 章

ハント パイロットの設定

- ハント パイロットの概要，165 ページ
- ハント パイロットの設定タスク フロー，166 ページ

ハント パイロットの概要

ハントパイロットは、システムがコールを電話番号（DN）にルーティングするために使用する数字とワイルドカードの文字列です。ハントパイロットはハントリストと連携して動作します。ハント リストは、着信コールに適したパスの優先順位付けされたリスト（回線グループ）です。コールがハント パイロット DN に発信されると、システムは、ハント リストで指定された最初の回線グループにコールを提供します。最初の回線グループ内でどの回線もコールに応答しない場合、システムは、ハント リストで指定された次の回線グループにコールを提供します。回線グループは、コールがグループ内の電話に配信される順序を制御します。それらは、特定の内線番号（通常は、IP フォンの内線番号またはボイスメール ポート）を指しています。回線グループは、コンピュータ テレフォニー インテグレーション（CTI）ポートと CTI ルート ポイントを指すことができないため、ハント パイロットを使用して、Cisco Customer Response Solution（CRS）や IP 自動音声応答（IP IVR）などの CTI アプリケーションを介して制御されているエンドポイントにコールを配信することはできません。

ハントパイロットは、回線グループとハントパイロットが異なるパーティションに存在する場合でも、割り当てられた回線グループのいずれかにコールを配信できます。ハント パイロットが分配するコールは、すべてのパーティションおよびコーリング サーチ スペース制限を上書きします。

ハント パイロットの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	回線グループの設定, （166 ページ）	複数の電話で、1 つの電話番号（DN）に直通するコールに応答できるようにする回線グループを作成します。
ステップ 2	ハント リストの設定, （167 ページ）	回線グループを優先するハント リストを設定します。ハントリストを介してコールをルーティングする際、システムはハントリストに定義した順で回線グループを使用します。
ステップ 3	ハントパイロットの設定, （167 ページ）	ハント パイロットを設定して、コールを電話番号（DN）にルーティングするためにシステムで使用される数字とワイルドカードの文字列を指定します。

回線グループの設定

複数の電話が 1 つの電話番号（DN）に転送されるコールに応答できるようにするには、回線グループを作成します。着信コールをグループ内の電話機に配信する順序を回線グループは制御します。

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）]>[ルート/ハント（Route/Hunt）]>[回線グループ（Line Group）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい回線グループを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存の回線グループの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストから回線グループを選択します。

[回線グループの設定（Line Group Configuration）] ウィンドウが表示されます。

ステップ 3 [回線グループの設定（Line Group Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ハント リストの設定, （167 ページ）

ハント リストの設定

ハントリストとは、回線グループの優先順位を記載したリストです。システムは、ハントリストを使用してコールをルーティングするときに、ハント リストで定義した順序で回線グループを使用します。

はじめる前に

回線グループの設定, （166 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）]>[ルート/ハント（Route/Hunt）]>[ハント リスト（Hunt List）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいハント リストを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存のハント リストの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、ハント リストを結果リストから選択します。

[ハント リストの設定（Hunt List Configuration）] ウィンドウが表示されます。

ステップ 3 [ハント リストの設定（Hunt List Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ハント パイロットの設定, （167 ページ）

ハント パイロットの設定

電話番号（DN）にコールをルーティングするため、システムで使用する数字とワイルドカードの文字列を指定するハント パイロットを設定します。

はじめる前に

ハント リストの設定, （167 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 次のいずれかのオプションを選択します。

- 新しいハント パイロットを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存のハント パイロットの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果の一覧からハント パイロットを選択します。

[ハント パイロットの設定（Hunt Pilot Configuration）] ウィンドウが表示されます。

ステップ 3 [ハント パイロットの設定（Hunt Pilot Configuration）] ウィンドウ内の各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。使用できるワイルドカードと特殊文字の詳細については、ハント パイロットのワイルドカードと特殊文字, （168 ページ）を参照してください。

ステップ 4 [保存（Save）] をクリックします。

ハント パイロットのワイルドカードと特殊文字

ハントパイロットにワイルドカードと特殊文字を使用すると、ハントパイロットで、ある電話番号（アドレス）の範囲を指定できます。また、これらのワイルドカードおよび特殊文字を使って指示を組み立てると、Cisco Unified Communications Manager が処理した番号を隣接システムに送信できます。

Cisco Unified Communications Manager がサポートするワイルドカードおよび特殊文字を次の表で説明します。

表 *14*：ワイルドカードおよび特殊文字

文字	説明	例
@	@ 記号（@）ワイルドカードは、国別番号計画のすべての番号に一致します。 各ルート パターンで、@ ワイルドカードは 1 文字だけ使用できます。	ルート パターン 9.@ は、国別番号計画が認識するすべての電話番号をルーティングまたはブロックします。 @ ワイルドカードが含む、国別番号計画の番号のルート パターンの例を次に示します。 • [0] • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X ワイルドカードは、0 ～ 9 の範囲にある数字の任意の 1 桁に一致します。	ルート パターン 9XXX は、9000 ～ 9999 の範囲のすべての数字をルーティングするか、またはブロックします。
!	感嘆符（!）ワイルドカードは、0 ～ 9 の範囲にある数字の 1 桁以上に一致します。	ルート パターン 91! は、910 ～ 91999999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
?	疑問符（?）ワイルドカードは、直前の数字またはワイルドカード値の 0 回以上の繰り返しに一致します。	ルート パターン 91X? は、91 ～ 91999999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
+	プラス記号（+）ワイルドカードは、直前の数字またはワイルドカード値の 1 回以上の繰り返しに一致します。	ルート パターン 91X+ は、910 ～ 91999999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
[]	角カッコ（[ ]）文字は、値の範囲を囲みます。	ルート パターン 813510[012345] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。

文字	説明	例
-	ハイフン（-）文字は、角カッコと一緒に使用して値の範囲を示します。	ルート パターン 813510[0-5] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
^	ハット（^）文字は、角カッコと一緒に使用して値の範囲外を示します。この文字は、開始角カッコ（[）の直後に配置してください。 各ルート パターンで、^ 文字は 1 文字だけ使用できます。	ルート パターン 813510[^0-5] は、8135106 ～ 8135109 の範囲のすべての数字をルーティングするか、またはブロックします。
.	デリミタとして使用されるドット（.）文字は、Cisco Unified Communications Manager のアクセス コードをディレクトリ番号から分離します。 この特殊文字を、桁を無視する指定と一緒に使用すると、隣接システムに番号を送信する前に Cisco Unified Communications Manager のアクセス コードを削除できます。 各ルート パターンで、（.）文字は 1 文字だけ使用できます。	ルート パターン 9.@ は、最初の 9 を、国別番号計画に発信する Cisco Unified Communications Manager アクセス コードとして認識します。
*	アスタリスク（*）文字は、特別な着信番号の追加の桁として利用できます。	ルート パターン *411 を設定して、内部オペレータのディレクトリ案内の利用を可能にします。
#	シャープ（#）文字は、一般にダイヤルシーケンスの終了を特定します。 # 文字がパターンの最後の文字になるようにします。	ルート パターン 901181910555# は、国別番号計画内からダイヤルされる国際番号をルーティングまたはブロックします。末尾の 5 の後の # 文字は、この桁をシーケンスの最後の桁として特定します。
\+	\+ のように、バックスラッシュにプラス記号が続くと、国際番号用エスケープ文字 + の設定を示します。	\+ の使用は、国際番号用エスケープ文字 + がワイルドカードではなく、ダイヤル可能な桁であることを意味します。

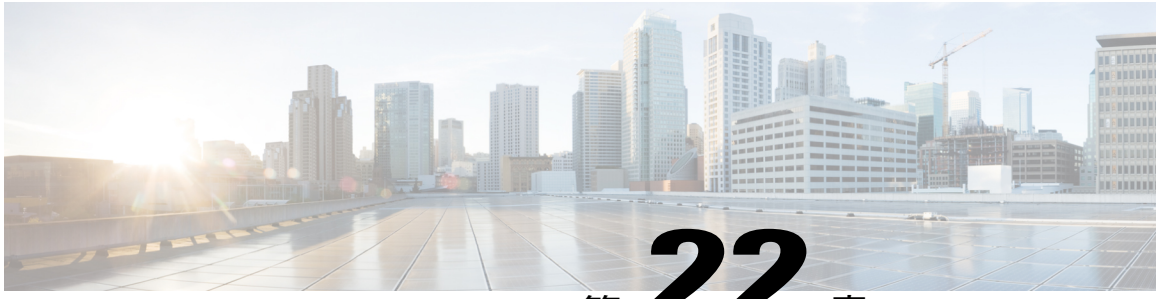
ハント パイロットのパフォーマンスと拡張性

次のパフォーマンスと拡張性の制限事項が適用されます。

- 単一の Unified CM クラスタは、最大 15,000 のハント リスト デバイスをサポートします。
- 単一の Unified CM サブスクライバは、コール キューイングが有効になっている状態でノードごとに最大 100 のハント パイロットをサポートします。
- ハント リスト デバイスは、各ハント リストに 10 台の IP フォンを含む 1500 のハント リスト、各ハント リストに 20 台の IP フォンを含む 750 のハント リストの組み合わせ、または同様の組み合わせにすることができます。

（注） コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハント リスト デバイスの数は、Busy Hour Call Attempts（BHCA）の数によって制限されます。ブロードキャスト アルゴリズムを使用して、10 台の電話機を含むハント リストまたはハント グループを指すハント パイロットに対して 10 回の BHCA を行うことは、10 回の BHCA を行う 10 台の電話機と同じです。

- 各ハント パイロットのキューに設定できる同時発信者の最大数は 1 ～ 100 です（デフォルトは 32）。
- 各ハント パイロットのキューに設定できる最大待機時間は 0 ～ 3600 秒です（デフォルトは 900）。ハント リストの数が増えると、Unified Communications Manager のサービス パラメータで指定するダイヤル プラン初期化タイマーの値を大きくする必要があります。1500 のハント リストを設定している場合は、ダイヤル プラン初期化タイマーを 600 秒に設定することを推奨します。
- コール キューイングとともにブロードキャスト アルゴリズムを使用している場合は、単一の回線グループに対して 35 を超える電話番号を設定しないでください。また、ブロードキャスト回線グループの数は、Busy Hour Call Completion（BHCC）レートによって異なります。Unified CM システム内に複数のブロードキャスト回線グループがある場合、1 回線グループの電話番号の最大数は 35 未満にする必要があります。すべてのブロードキャスト回線グループの最繁時呼数（BHCA）の数が、1 秒あたり 35 コール セットアップを超えないようにします。



第 22 章

トランスレーション パターンの設定

- トランスレーション パターンの概要，173 ページ
- トランスレーション パターンの前提条件，173 ページ
- トランスレーション パターンの設定タスク フロー，174 ページ

トランスレーション パターンの概要

任意のタイプのコール用に数字を処理するトランスレーション パターンを設定できます。トランスレーションパターンは、ルートパターンと同じ一般規則に従い、同じワイルドカードを使用します。ルートパターンと同じように、トランスレーションパターンをパーティションに割り当てます。ただし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Cisco Unified Communications Manager は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

トランスレーション パターンの前提条件

トランスレーション パターンを設定する前に、次のタスクを完了する必要があります。

- パーティション設定のタスク フロー，（133 ページ）
- コール ルーティング設定のタスク フロー，（146 ページ）

（注） 作成した各トランスレーション パターンで、パーティション、ルート フィルタ、および番号計画の組み合わせが一意であることを確認します。重複入力を示すエラーを受け取った場合、ルート パターンまたはハント パイロット、トランスレーション パターン、電話番号、コール パーク番号、コール ピックアップ番号、またはミートミー番号の設定ウィンドウを確認します。

トランスレーション パターンの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	トランスレーション パターンの設定, （174 ページ）	トランスレーション パターンを設定し、発信後にコールをルーティングする方法を指定します。

トランスレーション パターンの設定

発信後にコールのルーティング方法を指定するには、トランスレーション パターンを設定します。トランスレーション パターンを設定すると、Cisco Unified Communications Manager で発信および着信番号を適切に操作できます。Cisco Unified Communications Manager では、パターンの一致を検出すると、トランスレーション パターンに設定されたコーリング サーチ スペースを使用して、さらに一致があるかどうかを確認します。

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）>[トランスレーション パターン（Translation Pattern）] を選択します。

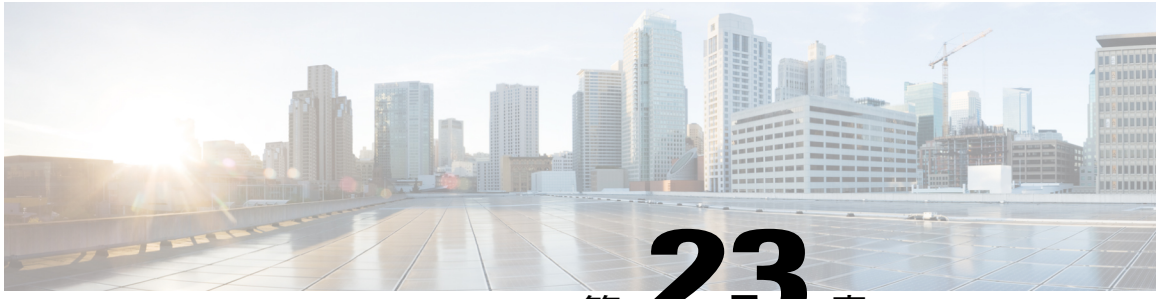
ステップ 2 次のいずれかのオプションを選択します。

- 新しいトランスレーション パターンを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存のトランスレーションパターンの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストからトランスレーション パターンを選択します。

[トランスレーション パターンの設定（Translation Pattern Configuration）] ウィンドウが表示されます。

ステップ 3 [トランスレーション パターンの設定（Translation Pattern Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。



第 23 章

トランスフォーメーション パターンの設定

- 変換パターンの概要，175 ページ
- トランスフォーメーション パターンの設定タスク フロー，175 ページ

変換パターンの概要

トランスフォーメーション パターンは、着信コールまたは発信コールでダイヤルされた番号をどのように処理するかを決定します。発信者番号または着信者番号を変更する必要があるとき、システムが電話機またはPSTNに送信する前にトランスフォーメーション パターンを設定できます。

トランスフォーメーション パターンを使用して、数字を廃棄したり、プレフィックスを付けたり、発信側の変換マスクを追加したり、発信側番号のプレゼンテーションを制御したりできます。

次の操作を実行できます。

- 着信側トランスフォーメーションCSSが指定された発信側トランスフォーメーション パターンをヒットします。
- 発信側トランスフォーメーションCSSが指定された着信側トランスフォーメーション パターンをヒットします。

トランスフォーメーション パターンの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	発信側トランスフォーメーション パターンの設定，（176 ページ）	この手順を使用して、発信者番号を変換します。たとえば、PSTN にコールするときに発信者の内線番号とオフィスの代表番号を置き換えるトランスフォーメーション パターンを設定できます。

	コマンドまたはアクション	目的
ステップ 2	着信側トランスフォーメーション パターンの設定, （177 ページ）	この手順を使用して、着信者番号を変換します。たとえば、10 桁の番号でダイヤルされたコールの最後の 5 桁のみを保持するトランスフォーメーション パターンを設定できます。
ステップ 3	トランスフォーメーション プロファイルの設定, （177 ページ）	これはオプションです。Cisco Intercompany Media Engine（Cisco IME）を使用している場合にのみ、この手順を実行します。ダイヤルされた番号を E.164 形式に変換するには、トランスフォーメーション プロファイルを設定する必要があります。

発信側トランスフォーメーション パターンの設定

この手順を使用して、発信者番号を変換します。たとえば、PSTN で発信するとき、発信者の内線番号をオフィスの代表番号に置き換えるトランスフォーメーション パターンを設定できます。

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [トランスフォーメーション（Transformation）] > [トランスフォーメーション パターン（Transformation Pattern）] > [発信側トランスフォーメーション パターン（Calling Party Transformation Pattern）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい発信側トランスフォーメーション パターンを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存の発信側トランスフォーメーション パターンの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストからパターンを選択します。

[発信側トランスフォーメーション パターンの設定（Calling Party Transformation Pattern Configuration）] ウィンドウが表示されます。

ステップ 3 [発信側トランスフォーメーション パターンの設定（Calling Party Transformation Pattern Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

着信側トランスフォーメーション パターンの設定, （177 ページ）

着信側トランスフォーメーション パターンの設定

着信者番号を変換するには、次の手順を使用します。たとえば、10 桁の数字としてダイヤルしたコールの最後の 5 桁のみ保持するトランスフォーメーション パターンを設定できます。

はじめる前に

発信側トランスフォーメーション パターンの設定, （176 ページ）

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）] >[トランスフォーメーション（Transformation）]>[トランスフォーメーション パターン（Transformation Pattern）]> [着信側トランスフォーメーション パターン（Called Party Transformation Pattern）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい着信側トランスフォーメーション パターンを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存の着信側トランスフォーメーション パターンを変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のユーザを選択します。

[着信側トランスフォーメーションパターンの設定（Called Party Transformation Pattern Configuration）] ウィンドウが表示されます。

ステップ 3 [着信側トランスフォーメーションパターンの設定（Called Party Transformation Pattern Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

これはオプションです。 トランスフォーメーション プロファイルの設定, （177 ページ）

トランスフォーメーション プロファイルの設定

Cisco Intercompany Media Engine（Cisco IME）を使用している場合にのみ、この手順を実行します。ダイヤルされた番号を E.164 形式に変換するには、トランスフォーメーション プロファイルを設定する必要があります。E.164 形式では、国際対応の「+」が先頭につきます。たとえば、「+14085551212」です。

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [トランスフォーメーション（Transformation）] > [トランスフォーメーション プロファイル（Transformation Profile）] を選択します。

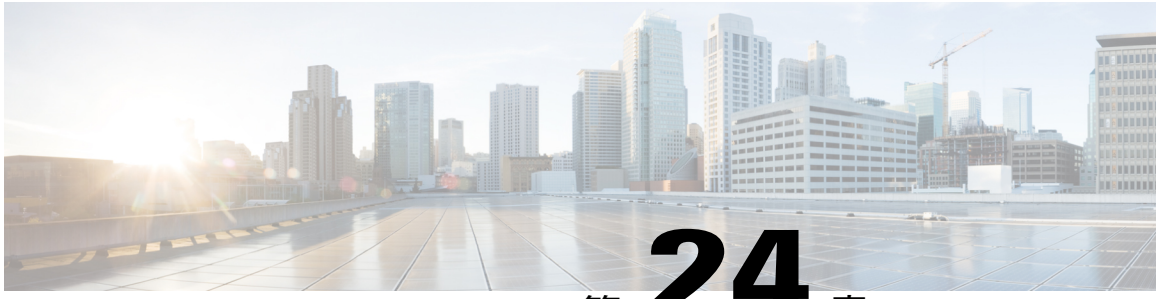
ステップ 2 次のいずれかのオプションを選択します。

- 新しいトランスフォーメーション プロファイルを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存のトランスフォーメーションプロファイルの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、検索結果の一覧からパターンを選択します。

[トランスフォーメーション プロファイルの設定（Transformation Profile Configuration）] ウィンドウが表示されます。

ステップ 3 [トランスフォーメーション プロファイルの設定（Transformation Profile Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。



第 24 章

ダイヤル ルールの設定

- ダイヤル ルールの概要，179 ページ
- ダイヤル ルールの前提条件，179 ページ
- ダイヤル ルールの設定タスク フロー，180 ページ
- ダイヤル ルールの連携動作と制約事項，187 ページ

ダイヤル ルールの概要

Cisco Unified Communications Manager は、次のタイプのダイヤル ルールをサポートしています。

- アプリケーション ダイヤル ルール
- ディレクトリ検索ダイヤル ルール
- SIP ダイヤル ルール

管理者はアプリケーション ダイヤル ルールを使用して、Cisco Web Dialer や Cisco Unified Communications Manager Assistant などのアプリケーションのダイヤル ルールの優先順位を追加およびソートします。

管理者はディレクトリ検索ダイヤル ルールを使用して発信者の識別番号を変換し、Cisco Unified Communications Manager Assistant などのアプリケーションで、Assistant Console からディレクトリ検索を実行します。

管理者はSIPダイヤルルールを使用して、システムのデジタル分析とルーティングを実行します。管理者は SIP ダイヤル ルールを設定し、コール処理が実行される前に、その SIP ダイヤル ルールを Cisco Unified IP Phone に追加します。

ダイヤル ルールの前提条件

- SIP ダイヤル ルールを設定するには、デバイスで SIP を実行している必要があります。

- 管理者は、次のデバイスに SIP ダイヤル ルールを関連付けます：Cisco Unified IP Phone 7911、7940、7941、7960、7961、7970、および 7971

ダイヤル ルールの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーション ダイヤル ルールの設定，（180 ページ）	Cisco Web Dialer、Cisco Unified Communications Manager Assistant などのアプリケーションのダイヤル ルールの優先順位を追加し並べ替える、アプリケーション ダイヤル ルールを設定します。
ステップ 2	ディレクトリ検索ダイヤル ルールの設定，（181 ページ）	発信者の ID 番号をディレクトリで検索可能な番号に変換するには、ディレクトリ検索ダイヤル ルールを設定します。
ステップ 3	SIP ダイヤル ルールの設定，（182 ページ）	SIP を実行している電話のダイヤル プランを設定するには、SIP ダイヤル ルールの設定を使用します。
ステップ 4	ダイヤル ルールの再優先順位付け，（186 ページ）	これはオプションです。複数のダイヤル ルールがある場合は、[Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] ウィンドウでダイヤル ルールの優先順位を変更します。

アプリケーション ダイヤル ルールの設定

Cisco Unified Communications Manager は、アプリケーション ダイヤル ルールをサポートし、Cisco Web Dialer や Cisco Unified Communications Manager Assistant のようなアプリケーションのダイヤル ルールの優先順位の追加と並べ替えができます。アプリケーション ダイヤル ルールを適用すると、ユーザがダイヤルする電話番号に対して数字の追加と削除が自動的に行われます。たとえば、外線発信する場合にはアプリケーションのダイヤル ルールにより、7 桁の電話番号の先頭に番号 9 が自動で付加されます。

（注） Cisco Unified Communications Manager は自動的に、CTI リモート デバイスのすべてのリモート接続先番号にアプリケーション ダイヤル ルールを適用します。

新しいアプリケーション ダイヤル ルールを追加する、または既存のアプリケーション ダイヤル ルールを更新するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理で、[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）] の順に選択します。

ステップ 2 [アプリケーション ダイヤル ルールの検索と一覧表示（Find and List Application Dial Rules）] ウィンドウで、次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックします。
- [検索（Find）] をクリックし、既存のアプリケーション ダイヤル ルールを選択します。

ステップ 3 [アプリケーション ダイヤル ルールの設定（Application Dial Rule Configuration）] ウィンドウのフィールドを設定します。フィールドの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

次の作業を実行します。

- ディレクトリ検索ダイヤル ルールの設定, （181 ページ）
- SIP ダイヤル ルールの設定, （182 ページ）

ディレクトリ検索ダイヤル ルールの設定

ディレクトリ検索ダイヤル ルールは、発信者の識別情報を、ディレクトリで検索可能な番号に変換します。各ルールでは、先頭の数字および番号の長さに基づいて、変換する数字を指定します。たとえば、10 桁の電話番号から市外局番と 2 桁の局番を自動的に削除するディレクトリ検索ダイヤル ルールを作成できます。たとえば、4085551212 は、51212 になります。

新しいディレクトリ検索ダイヤルルールを追加するか、既存のディレクトリ検索ダイヤルルールを更新するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] から、[コール ルーティング（Call Routing）] > [ダイヤル ルール（Dial Rules）] > [ディレクトリ検索ダイヤル ルール（Directory Lookup Dial Rules）] を選択します。

ステップ 2 [ディレクトリ検索ダイヤル ルールの検索と一覧表示（Directory Lookup Dial Rule Find and List）] ウィンドウで、以下のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックします。

- [検索（Find）] をクリックし、既存のディレクトリ検索ダイヤル ルールを選択します。

ステップ 3 [ディレクトリ検索ダイヤル ルール（Directory Lookup Dial Rules）] ウィンドウ内の各フィールドを設定します。フィールドの説明の詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

SIP ダイヤル ルールの設定, （182 ページ）

SIP ダイヤル ルールの設定

SIP ダイヤル ルールは、SIP を実行している Cisco Unified IP Phone のローカル ダイヤル プランを提供するため、ユーザは、コールが処理される前に、キーを押したり、タイマーを待機する必要はありません。管理者が SIP ダイヤル ルールを設定し、SIP を実行している電話機に適用します。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP ダイヤル ルールの設定, （183 ページ）	SIP ダイヤル ルールを設定および更新し、それらを SIP を実行している電話機と関連付けます。
ステップ 2	SIP ダイヤル ルールのリセット, （184 ページ）	SIP ダイヤル ルールを更新したときに、新しい SIP ダイヤル ルールで電話機が更新されるよう、SIP を実行している電話機をリセットまたは再起動します。
ステップ 3	SIP ダイヤル ルール設定と SIP 電話機の同期, （185 ページ）	（オプション）設定を変更した SIP ダイヤル ルールと SIP 電話機を同期します。これによって、最小限の割り込みで未適用の設定を適用します。たとえば、影響を受ける SIP 電話機の一部でリセットまたは再起動を行うは必要ありません。

関連トピック

パターン形式, （183 ページ）

パターン形式

表 *15* : ***SIP*** ダイヤル ルールのパターン形式

ダイヤル ルールのパターン	値
7940_7960_OTHER	• ピリオド（.）は任意の文字と一致します。 • シャープ記号（#）は終了キーとして機能し、># とのマッチングが見つかった後でのみ、終了を適用できます。そのため、>* は終了文字にアスタリスク（*）が指定されていることを意味します。つまり、終了キーは大なり記号（>）の後に続く必要があります。 （注） 7940_7960_OTHER で有効になるように、パターン フィールドのシャープ記号を設定する必要があります。 • アスタリスク（*）は 1 つ以上の文字に一致し、ワイルドカードとして処理されます。これは、* の前にバックスラッシュ（\）のエスケープ シーケンスを付け、* シーケンスを作ることで上書きできます。電話機は自動的に \ を削除するため、出力ダイヤル文字列には表示されません。* がダイヤル番号として受け取られると、ワイルドカード文字 * およびピリオド（.）によってマッチングされます。 • カンマ（,）は電話機に 2 番目のダイヤル トーンを生成させます。 たとえば、7.... は 7 で始まる任意の 4 桁の DN に一致します。8,..... は 8 に一致し、2 番目のダイヤル トーン（デフォルト値）が再生され、次に任意の 5 桁の DN に一致します。

SIP ダイヤル ルールの設定

SIP を実行している電話のダイヤル プランを設定します。

手順

ステップ 1 [Cisco Unified Communications Manager 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）] > [SIP ダイヤル ルール（SIP Dial Rules）].を選択します。

ステップ 2 [SIP ダイヤル ルールの検索/一覧表示（Find and List SIP Dial Rules）] ウィンドウで、次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリック
- [検索（Find）] をクリックし、既存の SIP ダイヤル ルールを選択

ステップ 3 [SIP ダイヤル ルールの設定（SIP Dial Rule Configuration）] ウィンドウの各フィールドを設定します。フィールドの詳細説明については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

（注） [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] で SIP ダイヤル ルールを追加または更新すると、Cisco TFTP サービスによってすべての電話設定ファイルが再構築されるため、特に多くの電話が接続された大規模なシステムでは、Cisco TFTP サービスを実行するサーバ上の CPU にスパイクが発生する可能性があります。CPU にスパイクを発生させないためには、SIP ダイヤル ルールの追加や更新をメンテナンス ウィンドウで行うか、設定変更を行う前に Cisco Unified Serviceability で Cisco TFTP サービスを一時的に停止してください。Cisco TFTP サービスを停止した場合は、SIP ダイヤル ルールを追加または更新した後、必ず Cisco Unified Serviceability でサービスを再開してください。

次の作業

SIP ダイヤル ルールのリセット, （184 ページ）

関連トピック

パターン形式, （183 ページ）

SIP ダイヤル ルールのリセット

SIP ダイヤル ルールを更新したときに、新しい SIP ダイヤル ルールで電話機が更新されるよう、次の手順を実行して SIP を実行している電話機をリセットまたは再起動します。

はじめる前に

SIP ダイヤル ルールの設定, （183 ページ）

手順

ステップ 1 Cisco Unified Communications Manager の管理から、[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）] の順に選択します。

ステップ 2 [SIP ダイヤル ルールの検索と一覧表示（Find and List SIP Dial Rules）] ウィンドウで、[検索（Find）] をクリックし、リセットする既存の SIP ダイヤル ルールを選択します。

ステップ 3 [SIP ダイヤル ルールの設定（SIP Dial Rule Configuration）] ウィンドウで、[リセット（Reset）] をクリックします。

ステップ 4 [デバイス リセット（Device Reset）] ダイアログ ボックスで、次のタスクのいずれかを実行します。

- 選択したデバイスをシャット ダウンせずに再起動し、Cisco Unified Communications Manager に登録するには、[再起動（Restart）] をクリックします。
- デバイスをシャット ダウンしてから再起動するには、[リセット（Reset）] をクリックします。
- 操作を実行せずに [デバイス リセット（Device Reset）] ダイアログ ボックスを閉じるには、[閉じる（Close）] をクリックします。

管理者が SIP ダイヤル ルールを設定して SIP を実行している電話機に適用すると、データベースから TFTP サーバに通知が送信されます。これによって、SIP を実行している電話機の新しい設定ファイルを作成できます。TFTP サーバは Cisco Unified Communications Manager に新しい設定ファイルを通知します。更新された設定ファイルは電話機に送信されます。詳細については、SIP を実行している Cisco Unified IP Phone の TFTP サーバの設定を参照してください。

次の作業

SIP ダイヤル ルール設定と SIP 電話機の同期, （185 ページ）

SIP ダイヤル ルール設定と SIP 電話機の同期

SIP 電話機と設定が変更された SIP ダイヤル ルールを同期するには、次の手順を実行します。

はじめる前に

SIP ダイヤル ルールのリセット, （184 ページ）

手順

ステップ 1 Cisco Unified Communications Manager の管理から、[コール ルーティング（Call Routing）] > [ダイヤル ルール（Dial Rules）] > [SIP ダイヤルルール（SIP Dial Rules）] の順に選択します。

ステップ 2 [SIP ダイヤル ルールの検索と一覧表示（Find and List SIP Dial Rules）] ウィンドウで、[検索（Find）] をクリックし、適切な SIP 電話機を同期する既存の SIP ダイヤル ルールを選択します。

ステップ 3 追加の設定変更を行い、[SIP ダイヤル ルールの設定（SIP Dial Rule Configuration）] で [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 [OK] をクリックします。

ダイヤル ルールの再優先順位付け

[ダイヤル ルールの設定（Dial Rule Configuration）] ウィンドウでダイヤル ルールの優先順位を追加およびソートするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理から、[コール ルーティング（Call Routing）] > [ダイヤル ルール（Dial Rules）] を選択します。

ステップ 2 次のいずれかを選択します。

- アプリケーション ダイヤル ルール（Application Dial Rules）
- ディレクトリ検索ダイヤル ルール（Directory Lookup Dial Rules）
- SIP ダイヤル規則

ステップ 3 [検索と一覧表示（Find and List）] ウィンドウで、ダイヤル ルールを選択し、ダイヤル ルールの名前をクリックします。
[ダイヤル ルールの設定（Dial Rule Configuration）] ウィンドウが表示されます。

ステップ 4 ダイヤル ルールをリストで上下に移動するには、上矢印および下矢印を使用します。

ステップ 5 順序の優先順位付けが完了したら、[保存（Save）] をクリックします。

ダイヤル ルールの連携動作と制約事項

SIP ダイヤル ルール連携動作

SIP ダイヤル ルール連携動作

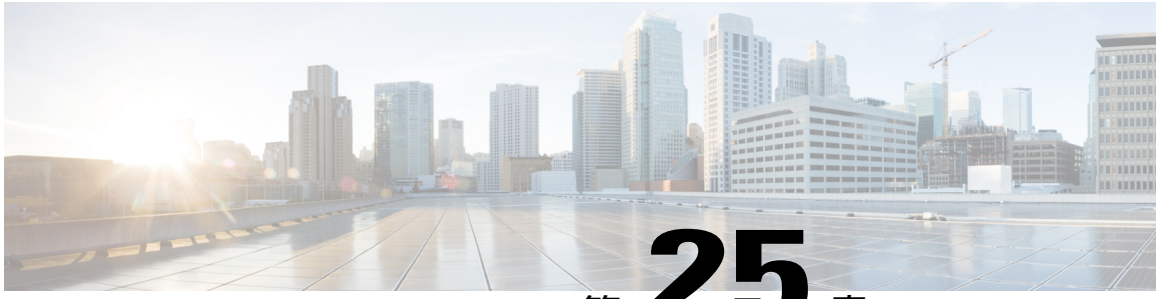
Cisco Unified IP Phone	データのやり取り
SIP を実行している 7911、7941、7961、7970、7971	これらの電話機は、7940_7960_OTHER ダイヤル ルール パターンを使用します。キー プレス マークアップ言語（KPML）では、Cisco Unified Communications Manager に数字を 1 桁ごとに送信できます。 SIP ダイヤル ルールを使用すると、Cisco Unified Communications Manager に送信する前に、電話で数字のパターンをローカルに収集できます。SIP ダイヤル ルールを設定しないと、KPML が使用されます。Cisco Unified Communications Manager のパフォーマンスを向上させるために（処理されるコール数の増加）、シスコはSIP ダイヤル ルールを設定することをお勧めします。
SIP を実行している 7940 および 7960	これらの電話機は、7940_7960_OTHER ダイヤル ルール パターンを使用しており、KPML をサポートしていません。これらの電話機で SIP のダイヤルプランを設定していないと、ユーザは数字が Cisco Unified Communications Manager に送信されて処理される前に、指定された時間だけ待機する必要があります。これは実際のコールの処理を遅らせます。

ディレクトリ検索ダイヤル ルールの制限

ディレクトリ検索ダイヤル ルールの制限

フィールド	制約事項
開始番号（Number Begins With）	このフィールドは、数字と文字+、*、#のみをサポートします。長さが 100 文字を超えてはなりません。

フィールド	制約事項
桁数	このフィールドは数字のみをサポートします。このフィールドの値は、パターンフィールドに指定されているパターンの長さより小さくすることはできません。
削除する合計桁数（Total Digits to be Removed）	このフィールドは数字のみをサポートします。このフィールドの値は、[桁数（Number of Digits）] フィールドの値より大きくすることはできません。
プレフィックス パターン（Prefix with Pattern）	このフィールドは、数字と文字 +、*、# のみをサポートします。長さが 100 文字を超えてはなりません。 （注） 1 つのダイヤル ルールの [削除する合計桁数（Total Digits to be Removed）] フィールドと [プレフィックスパターン（Prefix With Pattern）] フィールドの両方を空白にすることはできません。



第 25 章

クラスタ間ルックアップ サービスの設定

- クラスタ間検索サービスの概要，189 ページ
- ILS の前提条件，190 ページ
- ILS 設定のタスク フロー，190 ページ
- ILS の連携動作と制限事項，200 ページ
- ILS のトラブルシューティング，202 ページ

クラスタ間検索サービスの概要

クラスタ間検索サービス（ILS）を使用すると、リモートの Cisco Unified Communications Manager クラスタのネットワークを作成できます。複数のクラスタで ILS を設定すると、ILS ネットワークにあるリモート クラスタの現在のステータスで Cisco Unified Communications Manager が更新されます。

Cisco Unified CM の管理では、一対のクラスタで ILS を設定し、それらのクラスタを結合して ILS ネットワークを形成できます。ILS を使用すると、各クラスタ間の接続を設定することなく、ネットワークに追加クラスタを参加させることができます。

ILS ネットワークは、次のコンポーネントで構成されます。

- ハブ クラスタ
- スポーク クラスタ
- グローバル ダイヤル プランのインポート カタログ

ハブ クラスタ

ハブ クラスタは ILS ネットワークのバックボーンを形成します。ハブ クラスタは、ILS ネットワーク内の他のハブクラスタと ILS の更新情報を交換し、スポーク クラスタとの間でその情報をリレーします。

新しいハブ クラスタを既存の ILS ネットワーク内の別のハブ クラスタに登録すると、新しいハブ クラスタと ILS ネットワーク内のすべての既存ハブ クラスタ間にフル メッシュの接続が自動的に作成されます。

スポーク クラスタ

スポーク クラスタは ILS ネットワークのハブ クラスタに接続して、その他の ILS ネットワークとの間で ILS 更新プログラムをリレーします。スポーク クラスタはそれぞれのローカル ハブ クラスタにのみ接続し、他のハブ クラスタやスポーク クラスタに直接接続することはありません。

グローバル ダイヤル プランのインポート カタログ

サードパーティ システムとの URI ダイヤリングの互換性を提供するために、CSV ファイルからサードパーティのディレクトリ URI または +E.164 番号カタログを ILS ネットワークの任意のハブ クラスタに手動でインポートできます。インポートしたカタログは ILS で保持され、ネットワーク内のその他のクラスタに複製されます。ILS ネットワークの任意のサーバから、サードパーティのディレクトリ URI または +E.164 番号カタログのいずれかにダイヤルできます。

ILS の前提条件

ネットワークを理解し、ILS トポロジを設計する必要があります。

ソリューション リファレンス ネットワーク デザインの詳細については、『*Cisco Unified Communications Solution Reference Network Design*』ガイド（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html）を参照してください。

ILS 設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	クラスタ間検索サービスの有効化, （191 ページ）	クラスタ ID とリモート クラスタを設定するには、クラスタ間参照サービスをアクティベートします。
ステップ 2	クラスタ ID の設定, （192 ページ）	ILS ネットワークの各クラスタに一意の ID を提供します。
ステップ 3	リモート クラスタの設定, （193 ページ）	ILS ネットワークのリモート クラスタを設定します。

	コマンドまたはアクション	目的
ステップ 4	さまざまなクラスタで ILS クラスタをアクティベートするには、次のタスクを完了します。 • ハブ クラスタでの ILS のアクティブ化, （194 ページ） • スポーク クラスタでの ILS 有効化, （194 ページ）	ハブ クラスタの ILS と ILS ネットワークのスポーク クラスタをアクティベートします。 （注） ILS のそれぞれのクラスタを、ハブ クラスタまたはスポーク クラスタとして設定する必要があります。
ステップ 5	（オプション）クラスタとの認証を設定します。次のいずれかの手順を実行します。 • クラスタ間の TLS 認証の有効化, （195 ページ） • クラスタ間のパスワード認証を有効にする, （196 ページ） • クラスタ間の TLS パスワード認証の有効化, （197 ページ）	ILS ネットワークのクラスタ間における TLS 認証を使用します。 ILS ネットワークのリモート クラスタ間でのパスワード認証を使用します。 TLS とパスワード認証を使用して ILS ネットワークをセットアップします。このとき、クラスタ間の自己署名証明書を交換するのではなく、共通の認証局（CA）の署名がある証明書を使用します。
ステップ 6	グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする, （209 ページ）	（オプション）参加している ILS 対応のクラスタ間でダイヤル プラン情報を共有するために、グローバル ダイヤル プラン複製ための ILS サポートを有効にします。
ステップ 7	ILS ネットワークへのカタログのインポート, （198 ページ）	（オプション）サードパーティ システムに URI ダイヤリング互換性を持たせるためには、サード パーティの Directory URI または +E.164 番号カタログを、csv ファイルから ILS ネットワークのハブ クラスタに手動でインポートします。

クラスタ間検索サービスの有効化

クラスタ ID とリモート クラスタを設定するには、クラスタ間検索サービスをアクティブにする必要があります。

手順

ステップ 1 Cisco Unified Serviceability から、[ツール（Tools）] > [サービスの有効化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、シスコ クラスタ間検索サービスをアクティブ化するノードを選択し、[移動（Go）] をクリックします。

ステップ 3 [シスコ クラスタ間検索サービス（Cisco Intercluster Lookup Service）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

次の作業

クラスタ ID の設定, （192 ページ）

クラスタ ID の設定

ILS ネットワークの各クラスタの一意の ID を設定する必要があります。クラスタは、ステータスメッセージを交換する際にこの ID を使用します。

たとえば、4 つの Cisco Unified Communications Manager クラスタを含む 既存の ILS ネットワークがあり、これにクラスタを追加する場合は、新しいクラスタで ILS を設定し、そのクラスタを既存の ILS ネットワークの任意のハブ クラスタに登録できます。ILS は新しいクラスタに、既存ネットワークのすべてのクラスタについて自動的に通知します。

ILS ネットワークの各クラスタは、更新メッセージ、着信側ピア情報ベクトルを交換します。これらは、リモート クラスタにネットワークの各クラスタのステータスを通知するよう設計されています。更新メッセージには、次のような、ネットワーク内の既知のクラスタに関する情報が含まれます。

- クラスタ ID
- クラスタの説明とバージョン
- ホストの完全修飾ドメイン名（FQDN）
- ILS がアクティブ化されたクラスタ ノードの IP アドレスおよびホスト名

ネットワークの各クラスタの一意の ID を設定するには、次の手順を実行します。

はじめる前に

クラスタ間検索サービスの有効化, （191 ページ）

手順

ステップ 1 Unified Communications Manager パブリッシャ ノードにログインします。

ステップ 2 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。

ステップ 3 [エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] ウィンドウの [クラスタ ID（Cluster ID）] フィールドに、ネットワークで設定するクラスタの名前を入力します。
入力できるのは最大 50 文字です。英数字、ピリオド（.）、ハイフン（-）を入力できます。デフォルト値は StandAloneCluster です。

ステップ 4 [保存（Save）] をクリックします。

次の作業

リモート クラスタの設定, （193 ページ）

リモート クラスタの設定

ILS ネットワークのリモート クラスタを設定するには、次の手順を実行します。

はじめる前に

クラスタ ID の設定, （192 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[詳細機能（Advanced Features）] > [クラスタ ビュー（Cluster View）] を選択します。

ステップ 2 [リモート クラスタの検索と一覧表示（Find and List Remote Clusters）] ウィンドウで、以前に作成したリモート クラスタを選択します。

ステップ 3 [リモート クラスタ サービスの設定（Remote Cluster Service Configuration）] ウィンドウから、リモート クラスタの Extension Mobility Cross Cluster、TFTP、RSVP エージェントなどのサービスを設定するには、該当するチェックボックスをオンにします。

次の作業

次のいずれかの手順を実行します。

- ハブ クラスタでの ILS のアクティブ化, （194 ページ）
- スポーク クラスタでの ILS 有効化, （194 ページ）

ハブ クラスタでの ILS のアクティブ化

ハブ クラスタまたはスポーク クラスタとして、ILS ネットワークの各クラスタを設定する必要があります。各 ILS ネットワークには、少なくとも 1 つのハブ クラスタが必要です。他のハブ クラスタにハブ クラスタを接続することも、ネットワークの唯一のハブ クラスタとしてハブ クラスタを設定することもできます。また、複数のスポーク クラスタにハブ クラスタを接続することも、スポーク クラスタを使用することなくハブ クラスタを設定することもできます。

ILS ネットワークのハブ クラスタで ILS をアクティブ化するには、次の手順を実行します。

はじめる前に

リモート クラスタの設定, （193 ページ）

手順

ステップ 1 Cisco Unified Communications Manager パブリッシャ ノードにログインします。

ステップ 2 [高度な機能（Advanced Features）] > [ILS の設定（ILS Configuration）] を選択します。

ステップ 3 [ILS の設定（ILS Configuration）] ウィンドウで、[ロール（Role）] ドロップダウンリストから [ハブ クラスタ（Hub Cluster）] を選択し、[保存（Save）] をクリックします。

ステップ 4 [ILS 設定の登録（ILS Configuration Registration）] ポップアップ ウィンドウで、[登録サーバ（Registration Server）] テキスト ボックスを空欄にしたままで [OK] をクリックします。

次の作業

- スポーク クラスタでの ILS 有効化, （194 ページ）

スポーク クラスタでの ILS 有効化

スポーク クラスタは、ILS ネットワークのハブ クラスタに接続し、ILS アップデートをそのほかの ILS ネットワークとの間で双方向に中継します。ILS をスポーク クラスタで有効にするには、次の手順に従います。

はじめる前に

- クラスタ ID の設定, （192 ページ）
- リモート クラスタの設定, （193 ページ）

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM の管理で、[詳細機能（Advanced Features）] > [ILS の設定（ILS Configuration）] を選択します。

ステップ 3 [権限（Role）] ドロップダウン リストから、[スポーク クラスタ（Spoke Cluster）] を選択し、[保存（Save）] をクリックします。

ステップ 4 [ILS 設定の登録（ILS Configuration Registration）] ポップアップ ウィンドウで、[登録サーバ（Registration Server）] テキストボックスに表示された ILS ネットワークにある既存ハブ クラスタのパブリッシャノードの IP アドレス、または完全修飾ドメイン名を入力して、[OK] をクリックします。

ステップ 5 [ILS クラスタとグローバル ダイヤル プラン インポート カタログ（ILS Clusters and Global Dial Plan Imported Catalogs）] セクションでネットワークを表示して、ILS ネットワークが設定されていることを確認します。
すべてのネットワークが表示されたら、ILS ネットワークでクラスタ ディスカバリが設定されています。

次の作業

次のオプションのいずれかの手順を実行します。

- クラスタ間の TLS パスワード認証の有効化，（197 ページ）
- クラスタ間の TLS 認証の有効化，（195 ページ）
- クラスタ間のパスワード認証を有効にする，（196 ページ）
- グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする，（209 ページ）

クラスタ間の TLS 認証の有効化

（オプション）TLS 認証で、ILS ネットワークのリモート クラスタ間の通信を暗号化するには、次の手順を実行します。

はじめる前に

クラスタ間で Transport Layer Security（TLS）認証を使用するには、ILS ネットワークの各クラスタのパブリッシャ ノード間で、Tomcat 証明書を交換する必要があります。Cisco Unified Operating System Administration から、証明書の一括管理機能を使用して、以下を行います。

- ネットワークの各クラスタで、証明書をパブリッシャ ノードからセントラル ロケーションにエクスポート
- ILS ネットワークのすべてのパブリッシャ ノード サーバからエクスポートした証明書を統合

- ネットワークの各クラスタのパブリッシャ ノードに証明書をインポート

（注） クラスタ間の TLS 認証の有効化に関する詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlにある『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）] を選択します。

ステップ 3 [ILS 設定（ILS Configuration）] ウィンドウで、ILS 認証の下の [TLS 認証を使用（Use TLS Certificates）] のチェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

次の作業

これらのオプションのいずれかの手順を実行します。

- クラスタ間のパスワード認証を有効にする，（196 ページ）
- グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする，（209 ページ）

クラスタ間のパスワード認証を有効にする

（オプション）リモート クラスタ間でパスワード認証を使用するには、ILS ネットワークのクラスタ間のすべての通信にパスワードを割り当てる必要があります。

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）] を選択します。

ステップ 3 [ILS 設定（ILS Configuration）] ウィンドウで、ILS 認証の下の [パスワードを使用（Use Password）] チェックボックスをオンにします。

ステップ 4 [パスワードを使用（Use Password）] テキストボックスにパスワードを入力します。

（注） ネットワーク内の全クラスタに同じパスワードを設定する必要があります。

ステップ 5 [パスワードの確認（Confirm Password）] テキストボックスにパスワードを再入力します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

これらのオプションのいずれかの手順を実行します。

- クラスタ間の TLS 認証の有効化,（195 ページ）
- グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする,（209 ページ）

クラスタ間の TLS パスワード認証の有効化

はじめる前に

クラスタ間で証明書の交換なしに Transport Layer Security（TLS）とパスワード認証を使用するには、認証局のルート証明書を tomcat-trust にアップロードして、認証局のルート証明書の署名がある Tomcat 証明書を取得する必要があります。その証明書は同じクラスタにインポートされます。証明書がすべてのクラスタに同じパスワードでアップロードされると、クラスタは、クラスタ間検索サービス（ILS）ネットワークに接続できます。

（注） クラスタ間の TLS 認証を有効にする方法の詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM の管理で、[詳細機能（Advanced Features）] > [ILS の設定（ILS Configuration）] を選択します。

ステップ 3 [ILS の設定（ILS Configuration）] ウィンドウで、[ILS 認証（ILS Authentication）] 下にある [TLS 証明書を使用（Use TLS Certificates）] チェックボックスをオンにします。

ステップ 4 [ILS の設定（ILS Configuration）] ウィンドウで、[ILS 認証（ILS Authentication）] 下にある [パスワードを使用（Use Password）] チェックボックスをオンにします。

ステップ 5 [パスワードを使用（Use Password）] テキストボックスにパスワードを入力します。

（注） ネットワーク内の全クラスタに同じパスワードを設定する必要があります。

ステップ 6 [パスワードの確認（Confirm Password）] テキストボックスにパスワードを再入力します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

（オプション）グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする，（209 ページ）

グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする

（オプション）ローカル クラスタのグローバル ダイヤル プラン レプリケーションの ILS サポートを有効にするには、次の手順に従います。

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）] を選択します。

ステップ 3 [ILS 設定（ILS Configuration）] ウィンドウで、[グローバル ダイヤル プラン レプリケーション データとリモート クラスタの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）] のチェックボックスをオンにします。

ステップ 4 [アドバタイズルート文字列（Advertised Route String）] テキスト ボックスで、ローカル クラスタのルート文字列を入力します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

ILS ネットワークへのカタログのインポート，（198 ページ）

ILS ネットワークへのカタログのインポート

（オプション）サードパーティ システムに URI ダイヤリング互換性を持たせるためには、サードパーティの Directory URI または +E.164 番号カタログを、csv ファイルから ILS ネットワークのハブ クラスタに手動でインポートします。ILS ネットワークにカタログをインポートするには、次の手順に従ってください。

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）] > [グローバルダイヤルプラン複製（Global Dial Plan Replication）] > [イ

ンポートしたグローバルダイヤルプランカタログ（Imported Global Dial Plan Catalogs）] を選択します。

ステップ 2 [インポートしたグローバル ダイヤル プラン カタログの検索とリスト（Find and List Imported Global Dial Plan Catalogs）] ウィンドウで、[新規追加（Add New）] をクリックします。

ステップ 3 カタログの名前、説明、ルート文字列を入力して、[保存（Save）] とクリックします。

ステップ 4 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[一括管理（Bulk Administration）] > [ファイルのアップロード/ダウンロード（Upload/Download Files）] を選択します。

ステップ 5 [選択（Choose）] をクリックして、カタログ用にインポートする CSV ファイルを選択します。

ステップ 6 [ターゲットを選択（Select the Target）] ドロップダウンリストで、[インポートしたディレクトリURIとパターン（Imported Directory URIs and Patterns）] を選択します。

ステップ 7 [トランザクションタイプを選択（Select Transaction Type）] ドロップダウンリストで、[インポートしたディレクトリURIとパターンを挿入（Insert Imported Directory URIs and Patterns）] を選択します。

ステップ 8 [保存（Save）] をクリックします。

ILS の連携動作と制限事項

ILS の連携動作

表 *16*：*ILS* の連携動作

機能	データのやり取り
クラスタ検出	ILS のクラスタ検出を使用すると、管理者がそれらのクラスタ間の接続を手動で設定しなくても Cisco Unified Communications Manager はリモート クラスタの詳細を動的に学習できます。 ILS ネットワークの各クラスタは、更新メッセージ、着信側ピア情報ベクトルを交換します。これらは、リモートクラスタにネットワークの各クラスタのステータスを通知するよう設計されています。更新メッセージには、次のような、ネットワーク内の既知のクラスタに関する情報が含まれます。 • クラスタ ID • クラスタの説明とバージョン • ホストの完全修飾ドメイン名 • ILS が有効化されているクラスタ ノードの IP アドレスとホスト名 [詳細機能（Advanced Features）] > [クラスタ ビュー（Cluster View）] を選択すると、ILS クラスタ検出機能が Cisco Unified CM の管理で表示できるリモートクラスタのリストを自動的に読み込みます。このウィンドウから、リモートクラスタの Extension Mobility Cross Cluster、TFTP、RSVP エージェントなどのサービスを設定できます。 （注） [クラスタビュー（Cluster View）] に表示されるリモート クラスタの完全修飾ドメイン名には、ILS 検出で解決可能な DNS を指定する必要があります。
Global Dial Plan Replication; グローバル ダイヤル プラン レプリケーション	ILS ネットワークでグローバル ダイヤル プラン レプリケーションを有効にすると、ILS ネットワーク内のリモートクラスタは、次のようなグローバルダイヤル プラン データを共有します。 • ディレクトリ URI • 代替番号 • 代替番号パターン • ルート文字列 • PSTN フェールオーバー番号

ILS の制限事項

表 *17* : *ILS* の制限事項

制約事項	説明
ILS サービス	ILS サービスは、Unified Communications Manager のパブリッシャ ノードでのみ動作します。
クラスタ（Clusters）	ハブ クラスタは、多くのスポークを持つことができますが、スポーク クラスタは、1 つのハブ クラスタしか持つことができません。
ILS ネットワーク	ILS ネットワークに、サードパーティ コール制御システムを接続することはできません。
クラスタ インポート	ハブ クラスタにのみ、サードパーティ カタログをインポートできます。
重複した URI	既知の ILS クラスタに別のリモート クラスタから複製された URI があり、その URI がコールされると、学習されて最初にデータベースに挿入された URI のあるクラスタにコールがルーティングされます。
データベース レプリケーションのステータス	グローバル ダイヤル プラン データが ILS ネットワークで交換に成功しても、ILS を受信するクラスタは、データベース レプリケーションのステータスが完了するまで、学習した情報を書き込みません。
インポート（Import）	インポートするサードパーティのディレクトリ URI およびパターンでは、その CSV ファイル形式が、管理ウィンドウのサンプル ファイルが示すような正確なシンタックスと一致する必要があります。一致しない場合は、インポートに失敗します。

制約事項	説明
ILS ハブ	ILS ネットワークにハブ クラスタを追加するには、次の条件がプライマリ ILS ハブ ノードで満たされているかどうかを必ず確認します。 • クラスタ ID が ILS クラスタ内のすべてのハブ ノードで一意である。 • 完全修飾ドメイン名（FQDN）が設定されている。 • UDS および EM サービスが、ILS クラスタのすべてのハブ ノードで動作している。 • DNS プライマリと逆引きの名前解決が適切に機能している。 • 統合された Tomcat 証明書をすべてのハブノードからインポートする。 条件が満たされない場合は、クラスタの再起動またはエラーを修正した後でも、「バージョン」情報が、[リモート クラスタの検索と一覧表示（Find and List Remote Clusters）] ウィンドウに表示されません。これを回避するには、ハブ クラスタを ILS ネットワークから削除し、上記の条件を満たした後に、ILS ネットワークに再度追加します。

ILS のトラブルシューティング

ローカル クラスタが ILS ネットワークに接続できない

ローカル クラスタ内の接続問題をトラブルシューティングするには、RTMT を開き、そのパブリッシャ ノードに対してアラームおよび診断トレースを実行します。

クラスタ間で ILS を確立しようとしたときにエラー メッセージを受信した場合は、Cisco Unified Serviceability Administration からシスコ クラスタ間検索サービスの再起動を試行できます。

また、クラスタ間の認証の設定が不適切な場合にも接続の問題が発生する可能性があります。次の方法で認証を確認してください。

- TLS を使用している場合は、ネットワーク内のすべてのクラスタが TLS を使用していること、および通信する必要があるすべてのサーバの Tomcat 証明書が交換済みであることを確認します。

  （注） 証明書の一括エクスポート、マージ、およびインポートを使用して証明書を交換すると、TLS エラーのために ILS ハブが信頼されなくなることがあります。

- TCP パスワード認証を使用している場合は、すべての ILS クラスタが TCP パスワード認証を使用していること、およびネットワーク全体で同じ TCP パスワードが割り当てられていることを確認します。

ディレクトリ URI が ILS ネットワーク全体で複製されない

このエラーはさまざまな理由で発生する可能性があります。次の点をチェックします。

- ネットワークのすべてのクラスタがグローバル ダイヤル プラン データを交換するように設定されていることを確認します。ハブ クラスタがグローバル ダイヤル プラン データを交換するように設定されていない場合は、そのハブのどのスポーク クラスタもディレクトリ URI カタログを交換できません。
- パスに含まれるすべてのクラスタに関して（[ILS 設定（ILS Configuration）] ページで）設定された同期間隔に基づき、エンドツーエンド レプリケーションに十分な時間を与えてください。ILS ネットワーク内のすべてのクラスタは、ネットワーク内の他のどのクラスタからも 3 ホップ以内に位置します。
- CLI コマンド **utils ils showpeerinfo** を使用して、リモート クラスタの USN 値を見ながらレプリケーションの進捗状況をモニタします。
- レプリケーションの速度を上げるには、ILS Sync Throttle サービス パラメータを変更します。設定値が小さいと、システムのパフォーマンスに影響が及ぶ可能性があります。
- ILS ネットワークのすべてのクラスタに固有のクラスタ ID があること、およびクラスタ ID としてスタンドアロン クラスタが設定されていないことを確認します。クラスタ ID は、Cisco Unified CM Administration の [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] で確認できます。

グローバル ダイヤル プラン レプリケーションが設定されているのに、Unified CM がリモート ILS クラスタ内の学習ディレクトリ URI や学習番号にコールできない

この状況は、ネットワーク内のすべてのクラスタで ILS およびグローバル ダイヤル プラン レプリケーションが有効になっているが、リモート クラスタ用のルート文字列にルーティングする SIP ルート パターンが設定されていない場合に発生する可能性があります。次の手順を実行します。

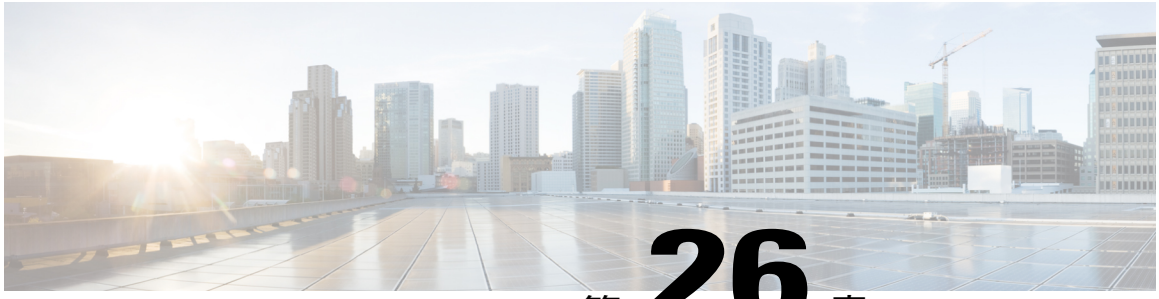
- [ILS 設定（ILS Configuration）] ウィンドウの [ILS クラスタとグローバル ダイヤル プラン インポート済みカタログ（ILS Clusters and Global Dial Plan Imported Catalogs）] ビューで、リモート クラスタのルート文字列を確認します。
- [SIPルートパターンの設定（SIP Route Pattern Configuration）] ウィンドウで、リモート クラスタ用のルート文字列にマップされるルート パターンがあることを確認します。

ILS グローバル ダイヤル プラン レプリケーション更新内容は、Cisco Unified Communications Manager データベース レプリケーションが修正されるまでキャッシュ内に保持されます。

[最後に受信した USN データ（Last USN Data Received）] の値は[最新（Current ）] で、[USN データ同期ステータス（USN Data Synchronization Status）] は [最新（Up to date）] です。ただし、学習した URI または学習したパターンは、ローカル クラスターに表示できません。

この状態は、データベースのレプリケーションが修正されないときに発生します。ILS は、データベース レプリケーションをすべてのノードのローカルクラスタに表示できない場合、リモートクラスタから学習した URI またはパターンの更新内容をキャッシュに格納します。データベース

のレプリケーションが修正された後、Cisco Unified Communications Manager はこれらの学習した URI またはパターンへのコールを発信できます。



第 26 章

グローバルダイヤルプランレプリケーションの設定

- グローバル ダイヤル プラン レプリケーションの概要，205 ページ
- グローバル ダイヤル プラン レプリケーションの前提条件，208 ページ
- グローバル ダイヤル プラン レプリケーションのタスクフロー，208 ページ

グローバル ダイヤル プラン レプリケーションの概要

グローバル ダイヤル プラン レプリケーションを使用して、クラスタ間検索サービス（ILS）ネットワーク全体のグローバル ダイヤル プランを作成します。グローバル ダイヤル プラン レプリケーションを有効にする場合、1つのクラスタにダイヤルプランのコンポーネントを設定します。設定すると、ILS によって ILS ネットワーク全体にその情報が複製されます。

グローバル ダイヤル プラン レプリケーションを有効にすると、ILS ネットワーク内の各 ILS クラスタはそれぞれのグローバル ダイヤル プラン データ（ローカルに設定されたグローバル ダイヤル プラン データ、他のクラスタから学習したデータを含む）を ILS ネットワークにアドバタイズします。グローバル ダイヤル プラン データには次のものが含まれます。

- ディレクトリ ユニバーサル リソース識別子（URI）
- 代替番号
- アドバタイズされたパターン
- PSTN フェールオーバー
- ルート文字列
- 学習したグローバル ダイヤル プラン データ
- インポートしたグローバル ダイヤル プラン データ

ディレクトリ URI

[ILS 経由でグローバルにアドバタイズ（Advertise Globally via ILS）] オプションを選択すると、ローカルに設定されたディレクトリ URI の完全なカタログが ILS によってアドバタイズされます。URI ダイヤリングの設定方法の詳細については、URI ダイヤリングの概要, （219 ページ）を参照してください。

代替番号

代替番号を使用すると、ILS ネットワーク内の任意の場所からダイヤルできる、グローバルにルーティング可能な番号を設定できます。Cisco Unified Communications Manager では、次の 2 種類の代替番号を作成できます。

- エンタープライズ代替番号
- +E.164 代替番号

アドバタイズされたパターン

アドバタイズされたパターンを使用すると、一定範囲のエンタープライズ代替番号または +E.164 代替番号の集約されたルーティング手順を作成し、そのパターンを ILS ネットワーク全体に複製できるため、ILS ネットワーク内の全クラスタがそのパターンを認識できます。アドバタイズされたパターンは、代替番号ごとに個別にルーティング情報が設定されるのを防ぎます。アドバタイズされたパターンは、そのパターンが設定されているローカル クラスタで使用されることはなく、ILS からパターンを学習するリモート クラスタでのみ使用されます。また、ILS によってアドバタイズされたパターンの公衆電話交換網（PSTN）フェールオーバー情報を設定することもできます。

PSTN フェールオーバー

Cisco Unified Communications Manager は、PSTN フェールオーバー番号を使用して、ILS から学習したパターン、代替番号、またはディレクトリ URI に発信されたコールのみ再ルーティングします。Cisco Unified Communications Manager は、ローカルに設定されたパターン、代替番号、またはディレクトリ URI に発信されたコールの場合、PSTN フェールオーバー番号にコールを再ルーティングしません。

グローバル ダイヤル プラン レプリケーションを有効にすると、学習したディレクトリ URI、学習した番号、および学習したパターンの PSTN フェールオーバー ルールを複製するように ILS を設定できます。発信コールのダイヤル文字列が学習したパターン、学習した代替番号、または学習したディレクトリ URI と一致し、Cisco Unified Communications Manager が SIP トランク経由でコールをルーティングできない場合、Cisco Unified Communications Manager は、発呼側の自動代替ルーティング（AAR）CSS を使用して、関連付けられた PSTN フェールオーバー番号にコールを再ルーティングします。

ルート文字列

ILS は ILS ネットワークにローカル ルート文字列をアドバタイズします。グローバル ダイヤル プラン データの各要素は、その要素のホーム クラスタを特定するルート文字列に関連付けられます。リモート クラスタは、ルート文字列と SIP ルート パターンを使用して、ILS ネットワーク内

のさまざまなクラスタへのルーティングを行います。リモート クラスタのユーザが ILS から学習したディレクトリ URI または代替番号をダイヤルすると、Cisco Unified Communications Manager は、関連付けられたルート文字列を SIP ルート パターンと適合して、その SIP ルート パターンで指定されているトランクにコールをルーティングします。

ユーザがクラスタにルート文字列を割り当てると、ILS は、そのルート文字列を同じクラスタ（ローカルに設定されたディレクトリ URI、代替番号、アドバタイズされたパターン、PSTN フェールオーバー情報を含む）に対してローカルである全グローバル ダイヤル プラン データに割り当てます。

（注） SIP ルート パターン名にダッシュが含まれる場合、ダッシュ間に数字が含まれていないことを確認する必要があります。ただし、ダッシュが 2 つ以上ある場合は、文字と数字または文字のみの組み合わせを使用できます。

SIP ルート パターンの良い例と悪い例は次のとおりです。

良い例：

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

悪い例：

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

学習したグローバル ダイヤル プラン データ

Cisco Unified Communications Manager は、ILS から学習したすべてのグローバル ダイヤル プラン データをローカル データベースに保存します。ILS は、ローカルに設定されたデータを複製するのに加えて、ローカル クラスタが ILS ネットワーク内の他のクラスタから学習したすべてのグローバル ダイヤル プラン データをアドバタイズします。このため、すべてのアドバタイズされたデータが ILS ネットワークの各クラスタに届きます。学習したグローバル ダイヤル プラン データには、学習したディレクトリ URI、学習した代替番号、学習したパターン、学習した PSTN フェールオーバー ルール、学習したルート文字列が含まれます。

Cisco Unified CM の管理では、次のタイプの学習したグローバル ダイヤル プラン データを確認できます。

- 学習した代替番号
- 学習したエンタープライズおよび +E.164 パターン
- 学習したディレクトリ URI

インポートしたグローバル ダイヤル プラン データ

Cisco Unified Communications Manager では、CSV ファイルのグローバル ダイヤル プラン データを ILS ネットワーク内の任意のハブ クラスタにインポートできます。ILS では ILS ネットワーク全体にインポートしたグローバル ダイヤル プラン データが複製されるため、Cisco Unified Communications Manager と Cisco TelePresence Video Communications Server またはサードパーティコール制御システムとの相互運用が可能になります。インポートしたグローバルダイヤルプランデータには、CSV ファイルから手動でインポートしたディレクトリ URI、+E.164 パターン、PSTN フェールオーバー ルールが含まれます。

（注） インポートしたデータには、Cisco Unified Communications Manager に手動でインポートしたグローバル ダイヤル プラン データのみ含まれます。インポートしたグローバル ダイヤル プラン データには、ILS から学習したデータが含まれません。

グローバル ダイヤル プラン レプリケーションの前提条件

「ILS 設定のタスク フロー, （190 ページ）」の ILS ネットワークを設定するための手順に従います。

グローバル ダイヤル プラン レプリケーションのタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする, （209 ページ）.	参加している ILS 対応のクラスタ間でダイヤル プラン情報を共有できるように、グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にします。
ステップ 2	代替番号の設定, （210 ページ）.	（オプション）クラスタ間でダイヤル可能な代替番号を設定するには、代替番号のレプリケーションを設定します。
ステップ 3	代替番号のアドバタイズ パターンの設定, （211 ページ）.	（オプション）パターンを使用して、代替番号を集約するには、アドバタイズされたパターンをセットアップして、パターンの PSTN フェイルオーバー ルールを指定します。
ステップ 4	PSTN フェールオーバーの設定, （212 ページ）.	（オプション）特定のディレクトリ URI または代替番号の PSTN フェイルオーバー番号をセットアップするには、特定の電話番号に関連付けられているす

	コマンドまたはアクション	目的
		べてのディレクトリ URI および代替番号の PSTN フェイルオーバー番号として代替番号を指定します。
ステップ 5	ルート パーティションの割り当て，（213 ページ）.	（オプション）ILS を通して、ルート パーティションをローカル クラスタが学習する代替の番号およびパターンに指定します。
ステップ 6	学習パターンのブロック，（214 ページ）.	（オプション）Cisco Unified Communications Manager のローカル クラスタで、学習した代替番号や、学習した代替番号パターンにコールをルーティングできないようにするには、ローカル ブロック ルールを設定できます。
ステップ 7	学習されたデータに対するデータベース制限の設定，（215 ページ）.	Cisco Unified Communications Manager がローカル データベースに書き込むことができる学習したオブジェクト数を判断するために、データベース制限を設定します。
ステップ 8	グローバル ダイヤル プランのデータをインポート，（216 ページ）.	（オプション）ILS ネットワークで、Cisco TelePresence Video Communication Server またはサードパーティ コール制御システムと相互運用するには、他のシステムの CSV ファイルのディレクトリ URI カタログから、ILS ネットワークのハブ クラスタにインポートします。

次の作業

クラスタ全体でディレクトリのユニバーサル リソース識別（URI）をダイアルするには、ローカル クラスタに URI ダイヤルをセットアップします。詳細については、URI ダイヤリングの概要，（219 ページ）を参照してください。

グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする

ローカル クラスタのグローバル ダイヤル プラン レプリケーションの ILS サポートを有効にするには、次の手順に従います。

手順

ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM の管理から、[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）] を選択します。

ステップ 3 [ILS 設定（ILS Configuration）] ウィンドウで、[グローバル ダイヤル プラン レプリケーション データとリモート クラスタの交換（Exchange Global Dial Plan Replication Data with Remote Clusters] のチェックボックスをオンにします。

ステップ 4 [アドバタイズルート文字列（Advertised Route String）] テキスト ボックスで、ローカル クラスタのルート文字列を入力します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

代替番号の設定, （210 ページ）.

代替番号の設定

エンタープライズ代替番号または +E.164 代替番号を作成し、電話番号と代替番号を関連付けます。代替番号をダイヤルすると、関連する電話番号に登録されている電話機の呼び出し音が鳴ります。

（注） 設定したそれぞれの代替番号は、単一の電話番号に関連付ける必要があります。ただし、その電話番号はエンタープライズ代替番号と +E.164 代替番号の両方に同時に関連付けることができます。

はじめる前に

グローバル ダイヤル プラン レプリケーションの ILS サポートを有効にする, （209 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [電話番号（Directory Number）] の順に選択します。

ステップ 2 [電話番号の検索と一覧表示（Find and List Directory Numbers）] ウィンドウから、代替番号を関連付ける電話番号を検索して選択します。

ステップ 3 [電話番号設定（Directory Number Configuration）] ウィンドウから、割り当てる代替番号のタイプに応じて次のいずれかのオプションをクリックします。

- [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）]

- [+E.164 代替番号の追加（Add +E.164 Alternate Number）]

ステップ 4 [番号マスク（Number Mask）] フィールドで、電話番号に適用する番号マスクを入力します。[代替番号（Alternate Number）] フィールドには、Cisco Unified Communications Manager が番号マスクを適用した後にどのように代替番号が表示されるかが示されます。

ステップ 5 （オプション）代替番号のローカル ルーティングを有効にするには、次の手順を実行します。

a) [ローカル ルート パーティションに追加（Add to Local Route Partition）] チェック ボックスをオンにします。

b) [ルート パーティション（Route Partition）] ドロップダウン リストから、ローカル コーリング サーチ スペースに割り当てられるルート パーティションを選択します。

ステップ 6 （オプション）番号パターンを使用してこの代替番号のクラスタ間ルーティングを設定する場合、[保存（Save）] をクリックします。

ステップ 7 （オプション）この代替番号のクラスタ間ルーティングを設定する場合、代替番号の [ILS 経由でグローバルにアドバタイズ（Advertise Globally via ILS）] チェック ボックスをオンにします。

ステップ 8 （オプション）この代替番号に PSTN フェールオーバー番号を割り当てる場合、[PSTN のフェールオーバー（PSTN failover）] ドロップダウン リストから、PSTN フェールオーバーとして番号を割り当てます。

ステップ 9 [保存（Save）] をクリックします。

次の作業

代替番号のアドバタイズ パターンの設定, （211 ページ）.

代替番号のアドバタイズ パターンの設定

代替番号の範囲を集約してクラスタ間検索サービス（ILS）ネットワークにアドバタイズするパターンを作成するには、次の手順を実行します。

はじめる前に

代替番号の設定, （210 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [グローバル ダイヤル プラン レプリケーション（Global Dial Plan Replication）] > [アドバタイズ パターン（Advertised Patterns）] の順に選択します。

ステップ 2 [アドバタイズ パターンの検索と一覧表示（Find and List Advertised Patterns）] ウィンドウから、次のタスクのいずれかを実行します。

- 既存の番号パターンの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のアドバタイズ パターンを選択します。

- 新しいアドバタイズ パターンを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [アドバタイズ パターンの設定（Advertised Pattern Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

PSTN フェールオーバーの設定, （212 ページ）.

PSTN フェールオーバーの設定

ディレクトリ URI または代替番号の PSTN フェールオーバー番号を割り当て、PSTN フェールオーバー番号を ILS ネットワークにアドバタイズするには、次の手順を実行します。リモート クラスタでは、学習ディレクトリ URI または学習代替番号へのコールに PSTN フェールオーバー番号を使用できます。

はじめる前に

代替番号のアドバタイズ パターンの設定, （211 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [電話番号（Directory Number）] の順に選択します。

ステップ 2 [電話番号の検索と一覧表示（Find and List Directory Numbers）] ウィンドウから、PSTN フェールオーバー番号を割り当てるディレクトリ URI または代替番号に関連付けられる電話番号を検索して選択します。
が表示されます。

ステップ 3 （オプション）PSTN フェールオーバーとして使用する代替番号がない場合、[電話番号の設定（Directory Number Configuration）] ウィンドウで、割り当てる代替番号のタイプに応じて次のオプションのいずれかを選択します。

- [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）]
- [+E.164 代替番号の追加（Add +E.164 Alternate Number）]

ステップ 4 [PSTN のフェールオーバー（PSTN Failover）] ドロップダウン リストで、PSTN フェールオーバーとして使用する代替番号を選択します。

ステップ 5 [保存（Save）] をクリックします。
Cisco Unified Communications Manager は、その PSTN フェールオーバー番号を電話番号に関連付けます。グローバル ダイヤル プラン レプリケーションは、電話番号に割り当てられるすべてのディ

レクトリ URI および代替番号の PSTN フェールオーバー番号として、その番号を ILS ネットワークにアドバタイズします。

次の作業

ルート パーティションの割り当て, （213 ページ）.

ルート パーティションの割り当て

学習した番号と学習したパターンをパーティションに割り当てる必要があります。パーティションを独自に定義するか、事前定義されたデフォルトのパーティションを使用できます。Cisco Unified Communications Manager では、次の、学習した代替番号と番号パターンの事前定義パーティションも同時にインストールされています。

- [学習したグローバル企業番号（Global Learned Enterprise Numbers）]
- [学習したグローバル E.164 番号（Global Learned E.164 Numbers）]
- [学習したグローバル企業パターン（Global Learned Enterprise Patterns）]
- [学習したグローバル E.164 パターン（Global Learned E.164 Patterns）]

（注） ヌルパーティションに学習した番号または学習したパターンを割り当てることはできません。

ルートパーティションを、ILS のグローバル ダイヤル プラン レプリケーション機能を介して Cisco Unified Communications Manager が学習した代替番号とパターンに割り当てるには、次の手順を実行します。

はじめる前に

PSTN フェールオーバーの設定, （212 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）]>[グローバル ダイヤル プラン レプリケーション（Global Dial Plan Replication）]>[学習した番号とパターンのパーティション（Partitions for Learned Numbers and Patterns）] を選択します。

ステップ 2 [学習した番号とパターンのパーティション（Partitions for Learned Numbers and Patterns）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

- （任意）学習パターンのブロック，（214 ページ）。
- 学習されたデータに対するデータベース制限の設定，（215 ページ）.

学習パターンのブロック

コールを学習した番号または学習したパターンにルーティングする前に、ILS はローカル ブロッキング ルールがダイヤル文字列に一致するかどうかを確認します。ブロッキング ルールに一致した場合、Cisco Unified Communications Manager はコールをルーティングしません。

ローカル クラスタがコールを特定のエンタープライズ番号および +E.164 代替番号、あるいは ILS で学習された番号パターンにルーティングしないようにするブロッキング ルールを設定するには、次の手順を実行します。

はじめる前に

ルート パーティションの割り当て，（213 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[コール ルーティング（Call Routing）] > [グローバル ダイヤル プランの複製（Global Dial Plan Replication）] > [学習した番号とパターンのブロック（Block Learned Numbers and Patterns）] を選択します。
[ブロックされた学習パターンの検索と一覧表示（Find and List Blocked Learned Patterns）] ウィンドウが表示されます。

ステップ 2 次のいずれかの作業を実行します。

- 既存の学習パターンの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のブロックされた学習パターンを選択します。
- 新しいブロックされた学習パターンを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [ブロックされた学習パターン（Blocked Learned Pattern）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

学習されたデータに対するデータベース制限の設定，（215 ページ）.

学習されたデータに対するデータベース制限の設定

データベース制限を設定します。これにより、Cisco Unified Communications Manager がローカルデータベースに書き込みできる学習されたオブジェクトの数が決定されます。

はじめる前に

- ルート パーティションの割り当て，（213 ページ）.
- （任意）学習パターンのブロック，（214 ページ）。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [サービス パラメータ（Service Parameters）] の順に選択します。
が表示されます。

ステップ 2 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、[サーバ（Server）] ドロップダウンリストから、パラメータを設定するサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウンリストから、[シスコ クラスタ間検索サービス（アクティブ）（Cisco Intercluster Lookup Service (Active)）] を選択します。
サービスがアクティブと表示されていない場合は、Cisco Unified Serviceability でサービスをアクティベートしたことを確認します。ILS をアクティベートする方法については、関連項目を参照してください。

ステップ 4 [クラスタ全体のパラメータ（Clusterwide Parameters (ILS)）] セクションで、[データベース中の学習したオブジェクトの ILS 最大数（ILS Max Number of Learned Objects in Database）] サービス パラメータを見つけます。

ヒント パラメータに関する情報については、パラメータ名をクリックするか、[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウに表示される疑問符をクリックします。

ステップ 5 [データベース中の学習したオブジェクトの ILS 最大数（ILS Max Number of Learned Objects in Database）] パラメータの上限値を設定します。
データベース サービス パラメータ中の学習したオブジェクトの ILS 最大数により、ILS を通じて学習されたデータを Cisco Unified Communications Manager がデータベースに書き込めるエントリの最大数が決定されます。サービス パラメータのデフォルト値は 100,000 で、最大値は 1,000,000 です。

（注） このサービス パラメータの値を、データベースに保存されている現在の ILS 学習エントリの数より小さくすると、Cisco Unified Communications Manager は学習した ILS オブジェクトをそれ以上データベースに書き込みません。ただし、既存のデータベース エントリはそのままです。

ステップ 6 [保存（Save）] をクリックします。

次の作業

グローバル ダイヤル プランのデータをインポート, （216 ページ）.

関連トピック

クラスタ間ルックアップ サービスの設定, （189 ページ）

グローバル ダイヤル プランのデータをインポート

次の手順を実行して、コール制御システムに対して、ディレクトリ URI、+E.164 パターン、PSTN フェールオーバー ルールを CSV ファイルから手動でインポートします。この制御システムでは、Cisco TelePresence Video Communication Server やサードパーティ コール制御などの ILS は実行していません。

はじめる前に

学習されたデータに対するデータベース制限の設定, （215 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [グローバル ダイヤル プラン レプリケーション（Global Dial Plan RepIication）] > [グローバル ダイヤル プラン レプリケーション（Imported Global Dial Plan Catalog）] を選択します。

ステップ 2 [インポートしたグローバル ダイヤル プラン カタログの検索とリスト（Find and List Imported Global Dial Plan Catalogs）] ウィンドウで、次のいずれかのタスクを実行します。

- 既存のダイヤル プラン カタログの設定を変更するには、[検索（Search）] をクリックし、結果リストから既存のカタログを選択します。
- 新しいカタログを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog Settings）] ウィンドウの [名前（Name）] フィールドに、インポートするカタログを識別する一意の名前を入力します。

ステップ 4 （オプション）[説明（Description）] フィールドに、カタログの説明を入力します。

ステップ 5 [ルート文字列（Route String）] フィールドに、カタログをインポートしているシステムのルート文字列を作成します。
ルート文字列は最大 250 文字長の英数字であり、ドットおよびダッシュを含めることができます。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[一括管理（Bulk Administration）] > [ファイルのアップロード/ダウンロード（Upload/Download Files）] を選択します。

ステップ 8 [新規追加（Add New）] をクリックします。

ステップ 9 [参照（Browse）] をクリックして、インポートするカタログの CSV ファイルを選択します。

インポートに使用する CSV ファイルが Cisco Unified Communications Manager と互換性があることを確認します。たとえば、バージョン 9.0(1) へのインポートをサポートする CSV ファイルは、バージョン 10.0(1) とは互換性がありません。

ステップ 10 [ターゲットを選択（Select the Target）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターン（Imported Directory URIs and Patterns）] を選択します。

ステップ 11 [トランザクション タイプを選択（Select Transaction Type）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターンを挿入（Insert Imported Directory URIs and Patterns）] を選択します。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[一括管理（Bulk Administration）] > [ディレクトリ URL とパターン（Directory URIs and Patterns）] > [インポートしたディレクトリ URL とパターンを挿入（Insert Imported Directory URIs and Patterns）] を選択します。

ステップ 14 [ファイル名（File Name）] ドロップダウンリストで、インポートするカタログを含む CSV ファイルを選択します。

ステップ 15 [インポートしたディレクトリ URI カタログ（Imported Directory URI Catalog）] ドロップダウンリストで、[インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog）] ウィンドウで名前を付けたカタログを選択します。

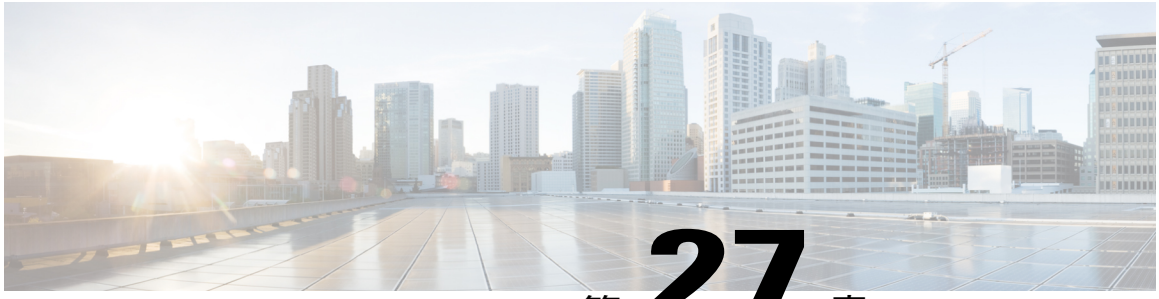
ステップ 16 [ジョブの説明（Description）] テキスト ボックスで、実行するジョブの名前を入力します。

ステップ 17 次のいずれかの手順を実行します。

- ジョブをただちに実行する場合は、[今すぐ実行（Run Immediately）] オプションを選択し、[送信（Submit）] をクリックします。
- 所定の時刻に実行するようにジョブをスケジュールするには、[後で実行（Run Later）] ラジオ ボタンをオンにして、[送信（Submit）] をクリックします。

[後で実行（Run Later）] オプションを選択した場合は、ジョブの実行時刻をスケジュールするのに、一括管理ジョブ スケジューラーを使用する必要があります。

Cisco Unified Communications Manager は、インポートしたすべての +E.164 パターンを,グローバルな学習された +E.164 パターン パーティションに保存します。



第 27 章

URI ダイヤリングの設定

- URI ダイヤリングの概要，219 ページ
- URI ダイヤリングの前提条件，220 ページ
- URI ダイヤリング設定のタスク フロー，221 ページ

URI ダイヤリングの概要

Cisco Unified Communications Manager は、コール アドレッシングにディレクトリ URI を使用するダイヤリングをサポートしています。ディレクトリ URI は Uniform Resource Identifier、つまり、ディレクトリ番号を識別するために使用できる文字列です。ディレクトリ URI の形式は電子メールアドレスと同様 username@host の形式で、ホスト部分は IPv4 アドレスまたは完全修飾ドメイン名です。ディレクトリ番号を電話に割り当てると、Cisco Unified Communications Manager は、ディレクトリ URI を使用してその電話にコールをルーティングできます。URI ダイヤリングは、ディレクトリ URI をサポートする SIP および SCCP エンドポイントで使用できます。

ディレクトリ URI 形式

ディレクトリ URI は、@ 記号で区切られたユーザとホストアドレスで構成される英数字の文字列です。

Cisco Unified Communications Manager は次のディレクトリ URI の形式をサポートしています。

- user@domain（たとえば、joe@cisco.com）
- user@ip_address（たとえば、joe@10.10.10.1）

システムはディレクトリ URI のユーザ部分（@ 記号の前の部分）では次の形式をサポートします。

- 使用可能な文字は、a-z、A-Z、0-9、!、$、%、&、*、_、+、~、-、=、\、?、\、‘、,、.、/ です。
- ユーザ部分は最大 47 文字までです。

- ディレクトリ URI がデータベースに保存されている場合、Cisco Unified Communications Manager は、次の文字にパーセント エンコーディングを自動的に適用します。

  # % ^ ` { } | \ : ” < > [ ] \ ‘ およびスペース。

（注） パーセントエンコーディングを適用すると、ディレクトリ URI の桁数が増えます。たとえば、ディレクトリ URI として joe smith#@cisco.com（20 文字）を入力した場合、Cisco Unified Communications Manager は、ディレクトリ URL を joe%20smith%23@cisco.com（24 文字）としてデータベースに保存します。データベースの制限により、[ディレクトリ URL（Directory URI）] フィールドの最大長は 254 文字となります。

Cisco Unified Communications Manager は、ディレクトリ URI のホスト部分（@ 記号の後の部分）で次の形式をサポートしています。

- IPv4 アドレスまたは完全修飾ドメイン名をサポートします。
- 使用可能な文字は、英数字、ハイフン（-）、ドット（.）です。
- ホスト部分をハイフン（-）で開始または終了することはできません。
- ホスト部分に、連続した 2 つのドットを含めることはできません。
- ホスト部分の最短の長さは 2 文字です。
- ホスト部分では、大文字と小文字は区別されません。

（注） [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] 内で、一括管理を使用して、二重引用符とカンマが埋め込まれたディレクトリ URI を含む CSV ファイルをインポートする場合は、ディレクトリ URI 全体を二重引用符（"）で囲む必要があります。

URI ダイヤリングの前提条件

URI ダイヤリングを設定する前に、ILS ネットワークを設定し、ILS ネットワークのグローバルダイヤルプラン レプリケーションを有効にする必要があります。このタスクを実行するには、次のセクションを参照してください。

- グローバル ダイヤル プラン レプリケーションのタスクフロー, （208 ページ）
- ILS 設定のタスク フロー, （190 ページ）

URI ダイヤリング設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ディレクトリ URI をネットワーク内のローカルクラスタに割り当てます。 • ユーザへのディレクトリ URI の割り当て，（222 ページ） • 電話番号とディレクトリ URI の関連付け，（222 ページ）	エンド ユーザをシステムにプロビジョニングし、ディレクトリ URI をそれらのエンド ユーザに割り当てます。また、電話番号を設定し、ディレクトリ URI をその電話番号と関連付けます。 （注） エンド ユーザの設定と電話番号の設定の両方で、一括管理を使用して、エンドユーザ、ディレクトリ URI、電話番号および電話を Cisco Unified Communications Manager にインポートすることもできます。詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。
ステップ 2	デフォルト ディレクトリ URI パーティションの割り当て，（223 ページ）	デフォルトのディレクトリ URI パーティションをコーリング サーチ スペースにある既存のパーティションに割り当てます。
ステップ 3	URI ダイヤルの SIP プロファイルの設定，（224 ページ）	SIP プロファイルを設定して、ネットワーク内のクラスタ間ダイヤリングを設定します。
ステップ 4	URI ダイヤルの SIP トランクの設定，（225 ページ）	Cisco Unified Communications Manager が、発信 SIP メッセージに対して電話番号、ディレクトリ URI、または混合アドレスを挿入するかどうかを設定します。
ステップ 5	SIP ルート パターンの設定，（226 ページ）	クラスタ間ディレクトリ URI コールをルーティングするための SIP ルート パターンを設定します。
ステップ 6	ILS ネットワーク内の全クラスタについて手順 1 ～ 5 を繰り返します。	この手順は、ILS ネットワーク内に複数のクラスタがある場合に実行します。
ステップ 7	ディレクトリ URI カタログのインポート，（227 ページ）	（オプション）ディレクトリ URI コールを Cisco TelePresence Video Communication Server またはサードパーティ コール制御システムに発信する場合は、その他のシステム用の CSV ファイルからのディレ

	コマンドまたはアクション	目的
		クトリ URI カタログを ILS ネットワーク内のハブクラスタにインポートします。

ユーザへのディレクトリ URI の割り当て

エンド ユーザにディレクトリ URI を割り当てるには、次の手順を実行します。

手順

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

ステップ 2 [ユーザの検索と一覧表示（Find and List Users）] ウィンドウで、検索条件を指定し、[検索（Find）] をクリックします。

ステップ 3 表示された一覧からユーザを選択します。[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

ステップ 4 [ディレクトリ URI（Directory URI）] フィールドで、このエンド ユーザに関連付けるディレクトリ URI を入力します。ディレクトリ URI は電子メールアドレスのように、user@host の形式に従っています。

（注） ディレクトリ URI を入力し、[プライマリ エクステンション（Primary Extension）] フィールドに電話番号も入力した場合、このディレクトリ URI は自動的に、その電話番号に関連付けられたプライマリ ディレクトリ URI になります。

ステップ 5 [保存（Save）] をクリックします。

次の作業

電話番号とディレクトリ URI の関連付け, （222 ページ）

関連トピック

ディレクトリ URI 形式, （219 ページ）

電話番号とディレクトリ URI の関連付け

電話番号とディレクトリ URI を関連付けるには、次の手順を実行します。ディレクトリ番号を電話に割り当てると、Cisco Unified Communications Manager では、ディレクトリ URI を使用してその電話にダイヤルできます。

はじめる前に

ユーザへのディレクトリ URI の割り当て, （222 ページ）

手順

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

ステップ 2 フィルタ条件を指定し、[検索（Find）] をクリックします。

ステップ 3 電話番号を関連付けるデバイスをクリックします。[電話機の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [関連付け（Association）] ペインで以下を実行します。

- 既存の電話番号をクリックします。
- 電話番号が設定されていない場合、[新しい DN を追加（Add a new DN）] をクリックします。

ステップ 5 電話番号の設定（Directory Number Configuration）] ウィンドウで、[URI] テキスト ボックスにディレクトリ URI アドレスを入力します。

ステップ 6 [パーティション（Partition）] ドロップダウン リストから、ディレクトリ URI が属するパーティションを選択します。
ユーザが入力するディレクトリ URI は、選択したパーティション内で一意であることを確認します。URI へのアクセスを制限しない場合、パーティションに対して [なし（None）] を選択します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

デフォルト ディレクトリ URI パーティションの割り当て, （223 ページ）

デフォルト ディレクトリ URI パーティションの割り当て

デフォルト ディレクトリ URI パーティションを割り当てるには、次の手順を実行します。

はじめる前に

電話番号とディレクトリ URI の関連付け, （222 ページ）

手順

ステップ 1 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。[エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウが表示されます。

ステップ 2 [エンド ユーザ パラメータ（End User Parameters）] エリアの [ディレクトリ URI エイリアス パーティション（Directory URI Alias Partition）] で、既存のコーリング サーチ スペースに含まれる既存のパーティションを選択します。

ステップ 3 [保存（Save）] をクリックします。

次の作業

URI ダイヤルの SIP プロファイルの設定, （224 ページ）

URI ダイヤルの SIP プロファイルの設定

はじめる前に

デフォルト ディレクトリ URI パーティションの割り当て, （223 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] 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。[SIPプロファイルの検索と一覧表示（Find and List SIP Profiles）] 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。既存の SIP プロファイルのリストが表示されます。

ステップ 3 表示する SIP プロファイルを選択します。[SIPプロファイルの設定（SIP Profile Configuration）] ウィンドウが表示されます。

ステップ 4 [ダイヤル文字列の解釈（Dial String Interpretation）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [常にすべてのダイヤル文字列をURIアドレスとして処理（Always treat all dial strings as URI addresses）] ： URI アドレスを着信コールのアドレスとして処理するには、このオプションを選択します。
- [電話番号は 0 ～ 9、A ～ D、*、#、+ で構成（これ以外はURIアドレスとして処理）（Phone number consists of characters 0–9, A–D, *, and + （others treated as URI addresses））] ： SIP ID ヘッダーのユーザ部分のすべての文字がこの範囲に含まれる場合は、このオプションを選択して、着信コールを電話番号として扱います。アドレスのユーザ部分で、この範囲外の文字を使用している場合は、アドレスは URI として扱われます。

- [電話番号は 0 ～ 9、*、#、+ で構成（これ以外はURIアドレスとして処理）（Phone number consists of characters 0-9, *, and +（others treated as URI addresses））] ：SIP ID ヘッダーのユーザ部分のすべての文字がこの範囲に含まれる場合は、このオプションを選択して、着信コールを電話番号として扱います。アドレスのユーザ部分で、この範囲外の文字を使用している場合は、アドレスは URI として扱われます。

ステップ 5 ネットワーク内のすべての SIP プロファイルの [SIP要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）] チェックボックスをオンにします。

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

次の作業

URI ダイヤルの SIP トランクの設定, （225 ページ）

URI ダイヤルの SIP トランクの設定

ネットワークの SIP トランクを確認して、Cisco Unified Communications Manager で電話番号、ディレクトリ URI、またはディレクトリ番号とディレクトリ URI の両方を含むアドレスが、発信 SIP メッセージの SIP ID ヘッダーに挿入されるかどうかを確認します。

はじめる前に

URI ダイヤルの SIP プロファイルの設定, （224 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）]> [トランク（Trunk）] を選択します。[トランクの検索と一覧表示（Find and List Trunks）] ウィンドウが表示されます。

ステップ 2 詳細な検索条件を入力し、[検索（Find）] をクリックします。[トランクの設定の検索と一覧表示（Find and List Trunks）] ウィンドウが表示されます。

ステップ 3 [発信コール（Outbound Calls）] 領域で、[発呼側および接続側情報形式（Calling and Connected Party Info Format）] ドロップダウン リストから、以下のいずれかを選択します。

- [接続側にのみDNを配信（Deliver DN only in connected party）] ：Cisco Unified Communications Manager は、発信 SIP メッセージで、発信者の電話番号を SIP 連絡先ヘッダー情報に挿入します。これがデフォルトの設定です。
- [接続側にのみDNを配信（使用可能な場合）（Deliver URI only in connected party, if available）] ：Cisco Unified Communications Manager は、発信 SIP メッセージで、発信者のディレクトリ URI を SIP 連絡先ヘッダーに挿入します。ディレクトリ URI が使用できない場合、Cisco Unified Communications Manager は電話番号を挿入します。
- [接続側にのみURIおよびDNを配信（使用可能な場合）（Deliver URI and DN in connected party, if available）] ：Cisco Unified Communications Manager は、発信 SIP メッセージで、発信者の

ディレクトリ URI および電話番号を SIP 連絡先ヘッダーに挿入します。ディレクトリ URI が使用できない場合、Cisco Unified Communications Manager は電話番号のみを追加します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

SIP ルート パターンの設定, （226 ページ）

SIP ルート パターンの設定

クラスタ間のディレクトリ URI コールをルーティングするには SIP ルート パターンを設定する必要があります。

SIP ルート パターンを設定するには、次の手順に従います。

はじめる前に

URI ダイヤルの SIP トランクの設定, （225 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [SIP ルート パターン（SIP Route Pattern）] を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい SIP ルート パターンを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存の SIP ルート パターンの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから SIP ルート パターンを選択します。

ステップ 3 [SIP ルート パターンの設定（SIP Route Pattern Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

（オプション） ディレクトリ URI カタログのインポート, （227 ページ）

ディレクトリ URI カタログのインポート

Cisco Unified Communications Manager により、グローバル ダイヤル プランを CSV ファイルから ILS ネットワークのハブ クラスタにインポートできます。ILS はインポートしたグローバル ダイヤル プランのデータを ILS ネットワーク全体に複製して、Cisco Unified Communications Manager が Cisco TelePresence Video Communications Server や サードパーティ コール制御システムと相互運用できるようにします。

（オプション）ディレクトリ URI カタログをインポートするには、次の手順に従ってください。

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [グローバル ダイヤル プラン レプリケーション（Global Dial Plan RepIication）] > [グローバル ダイヤル プラン レプリケーション（Imported Global Dial Plan Catalog）] を選択します。

ステップ 2 [インポートしたグローバル ダイヤル プラン カタログの検索とリスト（Find and List Imported Global Dial Plan Catalogs）] ウィンドウで、次のいずれかのタスクを実行します。

- 既存のダイヤル プラン カタログの設定を変更するには、[検索（Search）] をクリックし、結果リストから既存のカタログを選択します。
- 新しいカタログを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog Settings）] ウィンドウの [名前（Name）] フィールドに、インポートするカタログを識別する一意の名前を入力します。

ステップ 4 （オプション）[説明（Description）] フィールドに、カタログの説明を入力します。

ステップ 5 [ルート文字列（Route String）] フィールドに、カタログをインポートしているシステムのルート文字列を作成します。
ルート文字列は最大250文字長の英数字であり、ドットおよびダッシュを含めることができます。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[一括管理（Bulk Administration）] > [ファイルのアップロード/ダウンロード（Upload/Download Files）] を選択します。

ステップ 8 [新規追加（Add New）] をクリックします。

ステップ 9 [参照（Browse）] をクリックして、インポートするカタログの CSV ファイルを選択します。
インポートに使用する CSV ファイルが Cisco Unified Communications Manager と互換性があることを確認します。たとえば、バージョン 9.0(1) へのインポートをサポートする CSV ファイルは、バージョン 10.0(1) とは互換性がありません。

ステップ 10 [ターゲットを選択（Select the Target）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターン（Imported Directory URIs and Patterns）] を選択します。

ステップ 11 [トランザクション タイプを選択（Select Transaction Type）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターンを挿入（Insert Imported Directory URIs and Patterns）] を選択します。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[一括管理（Bulk Administration）] > [ディレクトリ URL とパターン（Directory URIs and Patterns）] > [インポートしたディレクトリ URL とパターンを挿入（Insert Imported Directory URIs and Patterns）] を選択します。

ステップ 14 [ファイル名（File Name）] ドロップダウンリストで、インポートするカタログを含む CSV ファイルを選択します。

ステップ 15 [インポートしたディレクトリ URI カタログ（Imported Directory URI Catalog）] ドロップダウンリストで、[インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog）] ウィンドウで名前を付けたカタログを選択します。

ステップ 16 [ジョブの説明（Description）] テキスト ボックスで、実行するジョブの名前を入力します。

ステップ 17 次のいずれかの手順を実行します。

- ジョブをただちに実行する場合は、[今すぐ実行（Run Immediately）] オプションを選択し、[送信（Submit）] をクリックします。
- 所定の時刻に実行するようにジョブをスケジュールするには、[後で実行（Run Later）] ラジオ ボタンをオンにして、[送信（Submit）] をクリックします。

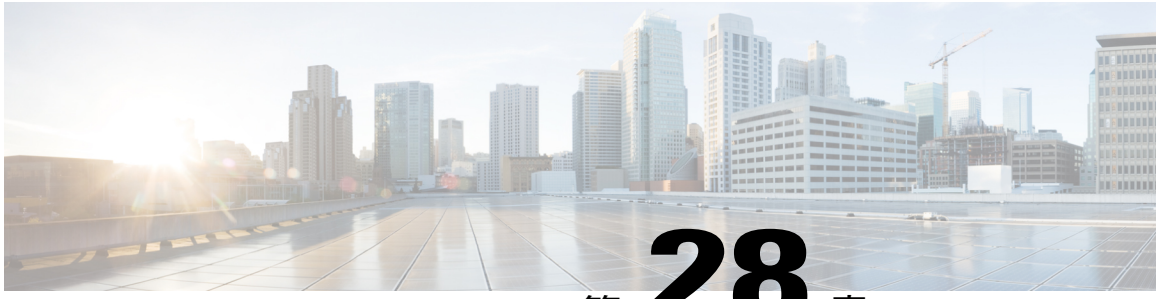
[後で実行（Run Later）] オプションを選択した場合は、ジョブの実行時刻をスケジュールするのに、一括管理ジョブ スケジューラーを使用する必要があります。

Cisco Unified Communications Manager は、インポートしたすべての +E.164 パターンを,グローバルな学習された +E.164 パターン パーティションに保存します。

第 IV 部

コール アドミッション制御の設定

- コール アドミッション制御の概要，231 ページ
- 拡張ロケーション コール アドミッション制御の設定，233 ページ
- Resource Reservation Protocol（RSVP）の設定，243 ページ



第 28 章

コール アドミッション制御の概要

- コール アドミッション制御について，231 ページ
- コール アドミッション制御の構成，231 ページ

コール アドミッション制御について

コール アドミッション制御（CAC）を使用して、WAN リンク経由の音声品質を調整できます。

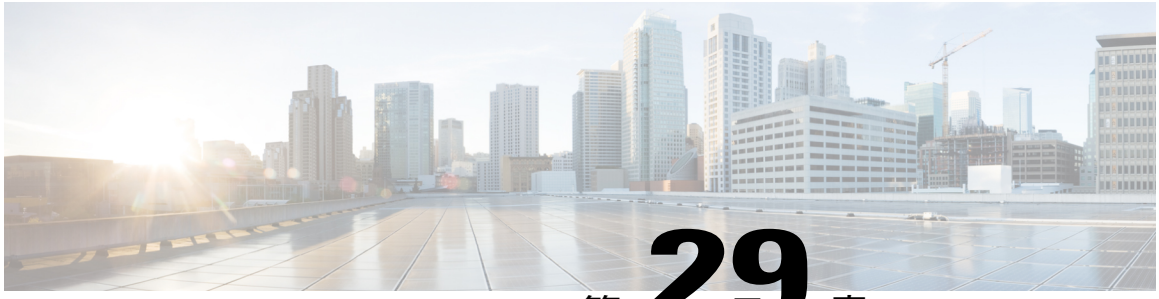
過多のアクティブ コールがリンク上に存在し、帯域幅がオーバーサブスクライブされると、音声品質が低下することがあります。コール アドミッション制御は、特定のリンク上で同時にアクティブにできるコール数を制限することで、音声品質を調整します。コール アドミッション制御は、リンク上の特定レベルの音声品質を保証するものではありませんが、リンク上のアクティブ コールが消費する帯域幅の量を調整できます。

コール アドミッション制御は、帯域幅とポリシーに基づいてコールを拒否することで動作します。コール アドミッション制御が原因でコールが拒否された場合、着信側の電話は呼び出し音が鳴らず、発信者には話中音が聞こえます。また、発信者は、電話で「帯域幅が不十分（Not enough bandwidth）」などのメッセージを受け取ります。自動代替ルーティング（AAR）を有効にすると、コール アドミッション制御は、WAN 帯域幅が使用できない場合に、自動的にコールを代替の公衆電話交換網（PSTN）ルートに転送します。

コール アドミッション制御の構成

コール アドミッション制御（CAC）を実装するには、次のいずれかのタスク フローを選択します。

タスク フロー	説明
拡張ロケーション コール アドミッション制御のタスク フロー, （235 ページ）	複数のクラスタが同じ WAN アップリンクを使用して同じ物理サイトのデバイスを管理する、分散導入環境では拡張ロケーションの CAC を使用します。拡張ロケーションの CAC により、ロケーション間のリンク上のコールに使用可能な帯域幅を制限して、音声品質を調整できます。さらに、TelePresence などのイマーシブ ビデオ コールに対してコール アドミッションを他のビデオ コールとは別に制御できます。
RSVP 設定のタスク フロー, （244 ページ）	RSVP を使用して、IP テレフォニーやビデオ会議アプリケーションを含む複雑な、複数の階層型トポロジにおいてコール アドミッション制御を実装します。RSVP でも帯域幅を動的に変更できます。



第 29 章

拡張ロケーション コール アドミッション制御の設定

- 拡張ロケーション コール アドミッション制御の概要，233 ページ
- 拡張ロケーション コール アドミッション制御の前提条件，235 ページ
- 拡張ロケーション コール アドミッション制御のタスク フロー，235 ページ
- 拡張ロケーション コール アドミッション制御の連携動作と制限事項，241 ページ

拡張ロケーション コール アドミッション制御の概要

拡張ロケーション コール アドミッション制御（CAC）は、複雑な WAN トポロジ、および複数のクラスタが同じアップリンクを使用して同じ物理サイトのデバイスを管理する分散型導入における WAN 帯域幅を制御します。拡張ロケーション CAC を使用すると、TelePresence などの実体験ビデオ コールのコール アドミッションを他のビデオコールから切り離して制御できます。

クラスタ全体で同じロケーションに割り当てられた帯域幅を予約、解放、および調整するためにクラスタの相互通信を可能にすることで、クラスタ間のロケーションを効率的に共有できます。[1]

ネットワーク モデリング

システムのメディアの処理方法を定義するには、ロケーションとリンクの概念に関するネットワーク モデルを構築します。

[1] Locations Media Resource Audio Bit Rate Policy サービス パラメータでは、トランスコーダなどのメディア リソースがメディアパスに挿入された場合やさらに複雑なシナリオの場合に、音声のみのコールに対して、当事者のロケーション内およびロケーション間で音声帯域幅プールから差し引くビット レート値を決めます。このサービス パラメータは、いずれかのコールレッグにメディアが存在しない場合、何の影響も及ぼしません。そのような場合、Location Bandwidth Manager は、そのロケーションで使用可能な帯域幅から送信元と宛先に対して設定されている最大のホップ帯域幅を差し引きます。

ロケーションはローカルエリア ネットワーク（LAN）を表します。ロケーションにはエンドポイントが含まれることがあり、ワイドエリア ネットワーク（WAN）ネットワーク モデリングのリンク間の中継場所として機能します。

リンクはロケーションを相互接続し、ロケーション間で利用可能な帯域幅を定義するために使用されます。リンクは WAN リンクを表します。

ウェイトは帯域幅パスのサイズです。ウェイトは、有効なパスへのコストを提供するためにリンク上で使用されます。ウェイトは、2 つのロケーション間に複数のパスがあるときに提供されます。

システムによってすべてロケーション間の最短パス（最小コスト）が計算されて、有効なパスが構築されます。全体的なウェイトが最小のパスが最も効率的なパスです。

システムは、ネットワーク モデルによって示される発信側ロケーションから終端側ロケーションまでのすべてのリンクの帯域幅を追跡します。

Location Bandwidth Manager; ロケーション帯域幅マネージャ

Location Bandwidth Manager（LBM）サービスは、送信元のロケーションから宛先のロケーションまでの有効なパスを計算します。このサービスは、Unified Communications Manager コール制御からの帯域幅要求の処理、クラスタ内およびクラスタ間での帯域幅情報の複製など、バックグラウンドで役立つ機能を提供します。この機能で提供される設定済みのリアルタイムの情報は、Serviceability Administration で確認できます。

Locations Media Resource Audio Bit Rate Policy サービス パラメータでは、トランスコーダなどのメディア リソースがメディア パスに挿入された場合やさらに複雑なシナリオの場合に、音声のみのコールに対して、当事者のロケーション内およびロケーション間で音声帯域幅プールから差し引くビット レート値を決めます。このサービスパラメータは、いずれかのコールレッグにメディアが存在しない場合、何の影響も及ぼしません。そのような場合、Location Bandwidth Manager は、そのロケーションで使用可能な帯域幅から送信元と宛先に対して設定されている最大のホップ帯域幅を差し引きます。

クラスタ間の拡張ロケーション コール アドミッション制御

クラスタ間の機能は、複数クラスタ間の拡張ロケーション CAC ネットワーク モデリングに拡張されます。各クラスタは、独自のネットワーク トポロジを管理します。そして、LBM クラスタ間レプリケーション ネットワークに設定されているその他のクラスタにそれぞれのトポロジを伝達します。

共有のロケーションは、LBM レプリケーション ネットワークに参加しているクラスタと同じ名前で設定されているロケーションです。

このタイプのロケーションは次の目的のために機能します。

- クラスタがそれぞれの設定済みトポロジを他のクラスタと共有可能にする
- 同じロケーションでの複数クラスタによる CAC の実行を可能にする

拡張ロケーション コール アドミッション制御の前提条件

- Unified Communications Manager およびロケーション帯域幅マネージャ（LBM）は、IP フォン、ゲートウェイ、H.323 および SIP トランク接続先を含むすべてのタイプのデバイスを対象に帯域幅を管理します。ただし、クラスタ間拡張ロケーション CAC には、他の場所へのリンクも帯域幅割り当てもない特別な場所であるシステム シャドウ ロケーションに割り当てられた SIP クラスタ間トランクが必要です。その他のタイプのデバイスはすべて、通常の（固定の）場所に割り当てられた場合のみサポートされます。
- Unified Communications Manager および LBM は、メディア リソースの帯域幅は管理しません。メディア リソースがコールの帯域幅要件を変更した場合は、最小または最大の帯域幅が予約されているかどうかを判別するグローバル パラメータの設定を変更できます。

拡張ロケーション コール アドミッション制御のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	LBM サービスのアクティブ化, （236 ページ）	シスコ ロケーション帯域幅マネージャ サービスがアクティベートされているかどうかを確認します。新しいシステムをインストールする場合、任意のノードのサービスを手動で有効にする必要があります。拡張ロケーション CAC が正常に動作するには、このサービスのインスタンスが各クラスタで実行されている必要があります。
ステップ 2	LBM グループの作成, （237 ページ）	LBM が同じノードで実行されていない場合は、LBM グループを設定し、サーバにこの LBM グループを割り当てます。LBM グループでは、ネットワークの遅延およびパフォーマンスを最適化できます。各サーバは、LBM サービスと通信して、各コールで使用可能な帯域幅を特定し、各通話時間の帯域幅を除外します。
ステップ 3	場所と場所リンクの設定, （238 ページ）	一元化されたコール処理システムで実装コール アドミッション制御を実装するロケーションを設定します。ロケーションは、ローカル エリア ネットワーク（LAN）を表しており、エンドポイントを含むか、ワイド エリア ネットワーク（WAN）のネットワーク モデリングのリンク間の中継場所として機能します。ロケーションでは、ロケーション内部だけでなく、ロケーションの内外でも帯域幅アカウンティングを使用できます。リンクでは、ロケーションとインターコネクト ロケーション間の帯域幅アカウンティングを使用できます。

	コマンドまたはアクション	目的
ステップ 4	内部ロケーションの帯域幅の割り当て，（238 ページ）	（任意） デフォルトの無制限帯域幅が不要になった場合は、内部ロケーションの帯域幅をロケーションに割り当てます。デフォルトでは、新しいロケーションを作成すると、オーディオ帯域幅が無制限、ビデオ帯域幅が 384 kbps、実体験ビデオ帯域幅は 384 kbps で、新しく追加したロケーションから Hub_None へのリンクも追加されます。この再割り当てを調整して、ネットワーク モデルに一致させることができます。
ステップ 5	外部通信の確立，（239 ページ）	ハブとして機能する LBM サーバで、リモート クラスタの LBM サーバを検索できるように、LBM ハブ グループを設定します。この手順では、このクラスタとの外部通信を確立します。LBM ハブ グループが割り当てられると、LBM サービスはハブとして機能します。LBM ハブ グループが割り当てられている LBM サービスはすべて、同じ、または重複する LBM ハブ グループが割り当てられているその他すべての LBM サーバとの通信を確立します。
ステップ 6	拡張ロケーションのコールアドミッション制御向け SIP クラスタ間トランクの設定，（240 ページ）	SIP クラスタ間トランク（ICT）をシャドウロケーションに割り当て、適切なクラスタ間オペレーションを確立します。SIP トランクが、SIP ゲートウェイなどの特定のロケーションのデバイスにリンクされている場合は、通常のロケーションに割り当てることができます。シャドウロケーションには、他の場所へのリンクを含まず、帯域幅も割り当てられていない特別なロケーションです。
ステップ 7	ビデオ コール用音声プールからオーディオ帯域幅を除外する，（241 ページ）	（任意） オーディオ帯域幅とビデオ帯域幅の除外分をビデオ コール用の別のプールに分割する場合は、次の手順を使用します。このシステムでは、ビデオ コール用ビデオ プールからオーディオ ストリームとビデオ ストリームの両方で使用するための帯域幅要件をデフォルトで除外しています。

LBM サービスのアクティブ化

シスコロケーション帯域幅マネージャ サービスがアクティベートされているかどうかを確認します。新しいシステムをインストールする場合、任意のノードのサービスを手動で有効にする必要があります。拡張ロケーション CAC が正常に動作するには、このサービスのインスタンスが各クラスタで実行されている必要があります。

手順

ステップ 1 Cisco Unified Serviceability から、[ツール（Tools）] > [サービスのアクティブ化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからサーバを選択し、[移動（Go）] をクリックします。

ステップ 3 必要に応じて、[シスコ ロケーション帯域幅マネージャ（Cisco Location Bandwidth Manager）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

次の作業

LBM グループの作成, （237 ページ）

LBM グループの作成

LBM が同じノードで実行されていない場合は、LBM グループを設定し、サーバにこの LBM グループを割り当てます。LBM グループでは、ネットワークの遅延およびパフォーマンスを最適化できます。各サーバは、LBM サービスと通信して、各コールで使用可能な帯域幅を特定し、各通話時間の帯域幅を除外します。

はじめる前に

LBM サービスのアクティブ化, （236 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [ロケーション情報（Location Info）] > [ロケーション帯域幅マネージャ グループ（Location Bandwidth Manager Group）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存の LBM グループの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存の LBM グループを選択します。
- 新しい LBM グループを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [ロケーション帯域幅マネージャ グループの設定（Location Bandwidth Manager Group Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

場所と場所リンクの設定, （238 ページ）

場所と場所リンクの設定

一元化されたコール処理システムで実装コール アドミッション制御を実装するロケーションを設定します。ロケーションは、ローカルエリア ネットワーク（LAN）を表しており、エンドポイントを含むか、ワイドエリア ネットワーク（WAN）のネットワーク モデリングのリンク間の中継場所として機能します。ロケーションでは、ロケーション内部だけでなく、ロケーションの内外でも帯域幅アカウンティングを使用できます。リンクでは、ロケーションとインターコネクト ロケーション間の帯域幅アカウンティングを使用できます。

はじめる前に

LBM グループの作成, （237 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [場所情報（Location Info）] > [場所（Location）] の順に選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存の場所の設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存の場所を選択します。
- 新しい場所を追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [場所の設定（Location Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- （オプション） 内部ロケーションの帯域幅の割り当て, （238 ページ）

内部ロケーションの帯域幅の割り当て

デフォルトの無制限帯域幅が不要になった場合は、内部ロケーションの帯域幅をロケーションに割り当てます。デフォルトでは、新しいロケーションを作成すると、オーディオ帯域幅が無制限、ビデオ帯域幅が 384 kbps、実体験ビデオ帯域幅は 384 kbps で、新しく追加したロケーションから Hub_None へのリンクも追加されます。この再割り当てを調整して、ネットワーク モデルに一致させることができます。

ヒント 音質が悪い、またはとぎれる場合は、帯域幅の設定を低くします。たとえば、ISDN では 56 kbps または 64 kbps の複数回線を使用します。

はじめる前に

場所と場所リンクの設定, （238 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [ロケーション情報（Location Info）] > [ロケーション（Location）] を選択します。

ステップ 2 検索条件を入力し、[検索（Find）] をクリックして、表示された一覧からロケーションを選択します。

ステップ 3 [詳細表示（Show Advanced）] をクリックし、内部ロケーションの帯域幅フィールドを表示します。

ステップ 4 必要に応じて、[音声の帯域幅（Audio Bandwidth）] の [kbps] オプション ボタンを選択し、テキストボックスに帯域幅の値を入力します。

ステップ 5 必要に応じて、[ビデオの帯域幅（Video Bandwidth）] の [kbps] オプション ボタンを選択し、テキストボックスに帯域幅の値を入力します。

ステップ 6 必要に応じて、[イマーシブ ビデオの帯域幅（Immersive Video Bandwidth）] の [kbps] オプション ボタンを選択し、テキストボックスに帯域幅の値を入力します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

外部通信の確立, （239 ページ）

外部通信の確立

ハブとして機能する LBM サーバで、リモート クラスタの LBM サーバを検索できるように、LBM ハブ グループを設定します。この手順では、このクラスタとの外部通信を確立します。LBM ハブ グループが割り当てられると、LBM サービスはハブとして機能します。LBM ハブ グループが割り当てられている LBM サービスはすべて、同じ、または重複する LBM ハブ グループが割り当てられているその他すべての LBM サーバとの通信を確立します。

はじめる前に

（オプション） 内部ロケーションの帯域幅の割り当て, （238 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [ロケーション情報（Location Info）] > [ロケーション帯域幅マネージャ（LBM）のクラスタ間レプリケーション グループ（Location Bandwidth Manager (LBM) Intercluster Replication Group）]を選択します。

ステップ 2 次のいずれかの作業を実行します。

- LBM のクラスタ間レプリケーション グループの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存の LBM クラスタ間レプリケーション グループを選択します。
- 新しいLBMクラスタ間レプリケーショングループを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [ロケーション帯域幅マネージャのクラスタ間レプリケーショングループの設定（Location Bandwidth Manager Intercluster Replication Group Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

拡張ロケーションのコール アドミッション制御向け SIP クラスタ間トランクの設定, （240 ページ）

拡張ロケーションのコール アドミッション制御向け SIP クラスタ間トランクの設定

SIP クラスタ間トランク（ICT）をシャドウロケーションに割り当て、適切なクラスタ間オペレーションを確立します。SIP トランクが、SIP ゲートウェイなどの特定のロケーションのデバイスにリンクされている場合は、通常のロケーションに割り当てることができます。シャドウロケーションには、他の場所へのリンクを含まず、帯域幅も割り当てられていない特別なロケーションです。

はじめる前に

- 設定された SIP クラスタ間トランク。詳細については、SIP トランクの設定タスク フロー, （107 ページ）を参照してください。
- 外部通信の確立, （239 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [トランク（Trunk）] を選択します。

ステップ 2 検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存の SIP クラスタ間トランクを選択します。

ステップ 3 [ロケーション（Location）] ドロップダウン リストから、[シャドー（Shadow）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

ビデオ コール用音声プールからオーディオ帯域幅を除外する

オーディオ帯域幅とビデオ帯域幅の除外分をビデオ コール用の別のプールに分割する場合は、次の手順を使用します。このシステムでは、ビデオコール用ビデオプールからオーディオストリームとビデオ ストリームの両方で使用するための帯域幅要件をデフォルトで除外しています。

（注） この機能を有効にする場合、CAC には、IP/UDP ネットワーク オーバーヘッドに必要な帯域幅はオーディオ帯域幅の除外分に含まれます。このオーディオ帯域幅の除外は、オーディオ ビット レートに加え、IP/UDP ネットワーク オーバーヘッドの帯域幅要件に相当します。ビデオ帯域幅は、ビデオ ビット レートのみ除外されます。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）]>[サービス パラメータ（Service Parameters）] の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからパブリッシャ ノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 4 [クラスタ全体のパラメータ（コール アドミッション制御）（Clusterwide Parameters (Call Admission Control)）] 領域で、[ビデオ コール用音声プールからオーディオ帯域幅部分を除外する（Deduct Audio Bandwidth Portion from Audio Pool for a Video Call）] サービス パラメータ値を [True] に設定します。

ステップ 5 [保存（Save）] をクリックします。

拡張ロケーション コール アドミッション制御の連携動作と制限事項

拡張ロケーション コール アドミッション制御

表 *18*：拡張ロケーション コール アドミッション制御

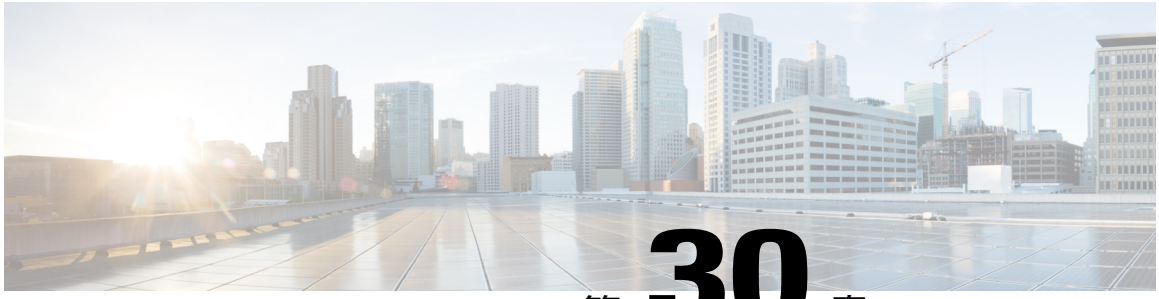
機能	データのやり取り
Bandwidth	共通のリンクまたは場所で帯域幅容量または重みの割り当てに競合がある場合、ローカル クラスタは割り当てられた値の最小値を使用します。

機能	データのやり取り
デバイス サポート	システムおよび LBM は、IP フォン、ゲートウェイ、H.323 および SIP トランク接続先を含むすべてのタイプのデバイスを対象に帯域幅を管理します。ただし、クラスタ間の拡張ロケーション CAC には、システム シャドウ ロケーションに割り当てられた SIP ICT が必要です。その他のタイプのデバイスはすべて、通常の（固定の）場所に割り当てられた場合のみサポートされます。

拡張ロケーション コール アドミッション制御の制限

表 *19*：拡張ロケーション コール アドミッション制御の制限

制約事項	説明
帯域予約パス	ネットワーク障害の状態では、Unified Communications Manager によって計算される帯域予約パスが正確にネットワークの状態を反映しないことがあります。このシナリオを考慮した申し分のない方法はモデル内にはありません。
帯域幅とビデオの機能	ビデオ機能を有効にすると、音声用の帯域幅はビデオから割り当てられます。
同期（Synchronization）	システムによって作成されたモデルは常に完全に同期されるわけではありません。保守的な帯域幅割り当てを使用して、この制約に適応できます。



第 30 章

Resource Reservation Protocol（RSVP）の設定

- RSVP コール アドミッション制御の概要，243 ページ
- RSVP コール アドミッション制御の前提条件，243 ページ
- RSVP 設定のタスク フロー，244 ページ

RSVP コール アドミッション制御の概要

Resource Reservation Protocol（RSVP）は、IP ネットワーク内のリソースを予約するためのリソース予約のトランスポートレベルのプロトコルです。拡張位置のコールアドミッション制御（CAC）の代わりに RSVP を使用できます。RSVP は、特定のセッションにリソースを予約します。セッションとは、特定の宛先アドレス、宛先ポート、およびプロトコル識別子（TCP または UDP）を持つフローです。

RSVP コール アドミッション制御の前提条件

IPv4 アドレッシングを使用する必要があります。RSVP は IPv6 アドレッシングをサポートしません。

RSVP 設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	クラスタ全体のデフォルトの RSVP ポリシーの設定, （245 ページ）	クラスタ内の全ノードについて RSVP ポリシーを設定します。
ステップ 2	ロケーション ペア RSVP ポリシーの設定, （245 ページ）	これはオプションです。場所のペアにクラスタの他とは別のポリシーを使用する場合、特定の場所のペアの RSVP ポリシーを設定できます。
ステップ 3	RSVP の再試行の設定, （246 ページ）	RSVP の再試行の頻度と番号を設定します。
ステップ 4	通話中の RSVP エラー処理の設定, （247 ページ）	コール中に RSVP が失敗したときにシステムがどのように応答するかを設定します。
ステップ 5	MLPP から RSVP へのプライオリティ マッピングの設定, （248 ページ）	これはオプションです。Multilevel Precedence and Preemption （MLPP）を使用する場合、発信者の MLPP 優先順位レベルを RSVP の優先順位にマップします。
ステップ 6	RSVP エージェントを設定します。	ゲートウェイ デバイスで次の IOS 手順を実行します。RSVP エージェントの設定方法についての情報は、デバイスのドキュメントを参照してください。
ステップ 7	アプリケーション ID の設定, （249 ページ）	RSVP アプリケーション ID を設定すると、システムは音声およびビデオ トラフィックの両方に ID を付与し、受信する ID に応じて Cisco RSVP エージェントが両方のタイプのトラフィックに別々の帯域制限を課せるようにします。
ステップ 8	DSCP マーキングの設定, （250 ページ）	DSCP マーキングを設定して、RSVP の予約が失敗した場合、システムが RSVP エージェントまたはエンドポイントデバイスに指示してメディアの差別化サービス コントロール ポイントのマーキングをベスト エフォートに変更できるようにします。DSCP マーキングを設定しない場合、EF マークされたメディアのパケットの超過分が、予約されているフローに対してもサービス品質（QoS）を劣化させます。

クラスタ全体のデフォルトの RSVP ポリシーの設定

クラスタ内の全ノードに RSVP ポリシーを設定します。

手順

ステップ 1 Cisco Unified CM の管理で、[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 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム□RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、Default interlocation RSVP Policy サービス パラメータを設定します。
このサービス パラメータを次の値に設定できます。

- 「No Reservation-No RSVP reservations」は、2 つの場所の間で適用されます。
- [オプション（ビデオが必要）（Optional（Video Desired））] : オーディオ ストリームおよびビデオ ストリームの両方の予約を取得できない場合は、ベストエフォートとして、オーディオのみのコールを継続できます。RSVP エージェントは、続けてオーディオの RSVP 予約を行い、予約が成功すると、Cisco Unified Communications Manager に通知を送信します。
- 必須：Cisco Unified Communications Manager は、オーディオ ストリームに対する（コールがビデオ コールの場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終了デバイスを呼び出しません。
- 必須（ビデオ優先）：オーディオ ストリームの予約は成功したが、ビデオ ストリームの予約に失敗する場合は、音声のみでビデオ通話を行うことができます。

次の作業

次のいずれかのオプションを選択します。

- ロケーション ペアで、残りのクラスタと異なるポリシーを使用する場合は、ロケーション ペア RSVP ポリシーの設定, （245 ページ）。
- クラスタ内の全ノードに同一の RSVP ポリシーを使用している場合は、RSVP の再試行の設定, （246 ページ）。

ロケーション ペア RSVP ポリシーの設定

クラスタの他の部分と異なるポリシーを使用するロケーションのペアがある場合は、特定のロケーション ペアに対して RSVP ポリシーを設定できます。次の手順を使用するとき、ロケーション ペアに設定する RSVP ポリシーは、クラスタに設定したポリシーをオーバーライドします。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [ロケーション（Location）] を選択します。

ステップ 2 ロケーション ペアの一方のロケーションを検索し、そのロケーションを選択します。

ステップ 3 選択したロケーションと別のロケーション間の RSVP ポリシーを変更するには、ロケーション ペアのもう一方のロケーションを選択します。

ステップ 4 [RSVP 設定（RSVP Settings）] ドロップダウン リストで、このロケーション ペアの RSVP ポリシーを選択します。
このフィールドに次の値を設定できます。

- [システム デフォルトを使用（Use System Default）] – ロケーション ペアの RSVP ポリシーが、クラスタ全体の RSVP ポリシーと一致します。
- [予約なし（No Reservation）] – 任意の 2 つのロケーション間で RSVP 予約が作られません。
- [音声優先（オプション）（Video Desired (Optional)）] – 音声およびビデオ ストリームの予約を取得できない場合、ベストエフォート、音声のみのコールとして処理されます。RSVP エージェントは、音声の RSVP の予約を引き続き試行し、予約が成功するとCisco Unified Communications Manager に通知します。オーディオ ストリームに対する（コールがビデオ コールの場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終端デバイスを呼び出しません。
- [音声優先（Video Desired）] – オーディオ ストリームの予約は成功したが、ビデオ ストリームの予約が成功しない場合、ビデオ コールは音声のみコールとして処理されます。

次の作業

RSVP の再試行の設定, （246 ページ）

RSVP の再試行の設定

RSVP の再試行の頻度および回数を設定するには、次の手順を実行します。

はじめる前に

- クラスタ全体のデフォルトの RSVP ポリシーの設定, （245 ページ）
- これはオプションです。 ロケーション ペア RSVP ポリシーの設定, （245 ページ）

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 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、指定されたサービス パラメータを設定します。
これらのサービス パラメータを次の値に設定できます。

- [RSVP 再試行タイマー（RSVP Retry Timer）]：RSVP 再試行タイマーの値を秒単位で指定します。このパラメータを 0 に設定すると、システムで RSVP の再試行が無効になります。
- [必須 RSVP ミッドコール再試行カウンタ（Mandatory RSVP Midcall Retry Counter）]：RSVP ポリシーが [必須（Mandatory）] に指定され、ミッドコール エラー処理オプションが [次の再試行カウンタを超えるとコールは失敗する（call fails following retry counter exceeds）]“ ”に設定されているときに、ミッドコール RSVP 再試行カウンタを指定します。デフォルト値は 1 回です。サービス パラメータを -1 に設定すると、予約が成功するか、コールが切断されるまで、いつまでも再試行が続行されます。

次の作業

通話中の RSVP エラー処理の設定, （247 ページ）

通話中の RSVP エラー処理の設定

通話中 RSVP エラー処理の設定には次の手順を使用します。

はじめる前に

RSVP の再試行の設定, （246 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[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 [サービス パラメータの設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、指定されたサービス パラメータを設定します。
通話中の強制 RSVP エラー処理のオプション サービス パラメータに次の値を設定できます。

- Call becomes best effort - コール中に RSVP が失敗した場合、コールはベスト エフォート型のコールになります。再試行を有効にすると、RSVP の再試行が同時に開始されます。
- Call fails following retry counter exceeded - Mandatory RSVP Mid-call Retry Counter サービス パラメータに数値「N」を指定し、コール中に RSVP が失敗した場合、RSVP の再試行を N 回実行した後に、コールは失敗します。

次の作業

ゲートウェイのデバイスに RSVP エージェントを設定します。RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。ゲートウェイで RSVP エージェントを設定した後は、Cisco Unified Communications Manager Administration に戻り、次のいずれかのオプションを選択します。

- これはオプションです。 MLPP から RSVP へのプライオリティ マッピングの設定, （248 ページ） ネットワークで Multilevel Precedence and Preemption を使用する場合。
- アプリケーション ID の設定, （249 ページ）

MLPP から RSVP へのプライオリティ マッピングの設定

これはオプションです。発信者の MLPP 優先度レベルから RSVP の優先度へのマッピングを設定するには、次のクラスタ全体の（System - RSVP）サービス パラメータを使用します。

- MLPP EXECUTIVE OVERRIDE To RSVP Priority Mapping
- MLPP FLASH OVERRIDE To RSVP Priority Mapping
- MLPP FLASH To RSVP Priority Mapping
- MLPP IMMEDIATE To RSVP Priority Mapping
- MLPP PL PRIORITY To RSVP Priority Mapping
- MLPP PL ROUTINE To RSVP Priority Mapping

これらのサービス パラメータを選択し、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 CM の管理で、[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 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータClusterwide（System - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで指定されたサービス パラメータを設定します。
これらのサービス パラメータは、次のように機能します。

- サービス パラメータ値が高いほど、優先度を上げるという設定に基づいて RSVP 予約を開始するとき、Cisco Unified Communications Manager は発信者の優先度レベルを RSVP 優先度にマップします。
- IOS ルータは RSVP 優先度に基づいてコールをプリエンプション処理します。
- RSVP エージェントは、プリエンプションの理由を含め、RSVP 予約の失敗の理由について Cisco Unified Communications Manager に通知する必要があります。
- Cisco Unified Communications Manager は既存の MLPP メカニズムを使用して、プリエンプション処理された発信側と着信側にプリエンプションを通知します。

次の作業

ゲートウェイのデバイスに RSVP エージェントを設定します。RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。ゲートウェイで RSVP のエージェントを設定した後は、Cisco Unified Communications Manager Administration と アプリケーション ID の設定, （249 ページ） に戻ります。

アプリケーション ID の設定

RSVP アプリケーション ID を設定すると、音声およびビデオ トラフィックの両方に ID が追加され、受信した ID をもとに、Cisco RSVP エージェントは、それぞれのトラフィック タイプに帯域幅の制限を設定できます。

この手順を開始する前に、ゲートウェイ デバイスで RSVP のエージェントを設定します。RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。

はじめる前に

ネットワークに RSVP アプリケーション ID を導入するには、Cisco RSVP Agent ルータで、Cisco IOS Release 12.4(6)T 以降を使用する必要があります。

手順

ステップ 1 Cisco Unified CM の管理で、[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 [サービス パラメータの設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、RSVP Audio Application ID サービス パラメータを設定します。
デフォルトは AudioStream です。

ステップ 4 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、RSVP Video Application ID を設定します。

デフォルトは VideoStream です。

次の作業

DSCP マーキングの設定, （250 ページ）

DSCP マーキングの設定

RSVP の予約が失敗すると、システムが RSVP エージェントまたはエンドポイント デバイス（RSVP エージェントの割り当てが失敗した場合）に指示して、メディアの Differentiated Services Control Point（DSCP）マーキングをベスト エフォートに変更します。変更しない場合、EF とマーキングされたメディア パケットの超過分により、予約のあるフローでもサービス品質（QoS）が低下する可能性があります。

はじめる前に

アプリケーション ID の設定, （249 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[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 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウでサーバを選択し、Cisco CallManager サービスを選択します。

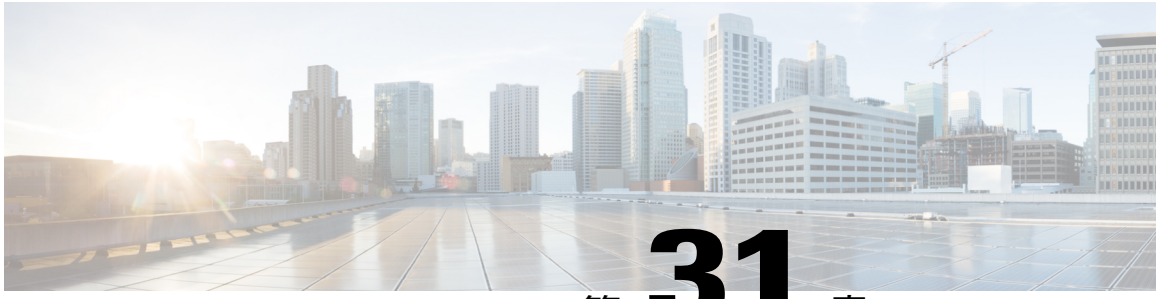
ステップ 3 [クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）] セクションで、DSCP for Audio Calls When RSVP Fails のサービス パラメータを設定します。

ステップ 4 [クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）] セクションで、DSCP for Video Calls When RSVP Fails のサービス パラメータを設定します。

第 V 部

エンド ユーザの設定

- エンド ユーザの設定の概要，253 ページ
- ユーザ アクセスの設定，257 ページ
- クレデンシャル ポリシーの設定，277 ページ
- ユーザ プロファイルの設定，281 ページ
- サービス プロファイルの設定，285 ページ
- 機能グループ テンプレートの設定，295 ページ
- LDAP ディレクトリからユーザをインポート，297 ページ
- 手動によるエンドユーザのプロビジョニング，313 ページ



第 31 章

エンド ユーザの設定の概要

- エンド ユーザの設定について，253 ページ
- End User Configuration，253 ページ

エンド ユーザの設定について

このパートの章では、システムでエンド ユーザをプロビジョニングして、設定する方法について説明します。

エンド ユーザは、Cisco Unified Communications Manager 機能の主要な使用者です。エンド ユーザは電話と電話番号に割り当てられるため、エンドユーザはシステム内の他のユーザにコールを発信してやり取りしたり、PSTN などの外部ネットワークにコールを発信したりできます。

多数のエンドユーザを一度にプロビジョニングするために、Cisco Unified Communications Manager は次の機能を提供しています。

- LDAP ディレクトリ統合：Cisco Unified Communications Manager と外部 LDAP ディレクトリを同期できるため、LDAP ディレクトリからエンドユーザ データをインポートできます。
- 一括管理ツール：一括管理ツールを使用して、多数のエンドユーザと関連付けされたユーザデータを 1 回の操作で CSV ファイルからインポートおよび設定できます。

エンドユーザがプロビジョニングされた後、電話サービス、クレデンシャル ポリシーに加え、ユーザが自身の電話をプロビジョニングできるようにユーザ プロファイルなどのユーザ設定を設定できます。

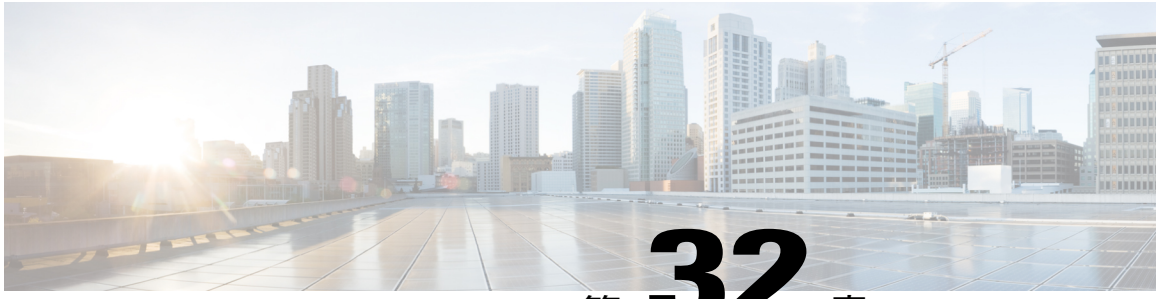
End User Configuration

次のタスク フローを実行すると、システムのエンド ユーザを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザアクセス設定のタスク フロー, （260 ページ）	エンドユーザのロールとアクセス制御グループを計画します。システム定義されたロールおよびアクセス制御グループに、導入に必要なアクセス権限を付与するかどうかに加え、新しいロールおよびアクセス制御グループを作成する必要があるかどうかを決定します。
ステップ 2	クレデンシャルポリシーの設定タスク フロー, （278 ページ）	エンド ユーザのクレデンシャル ポリシーを設定します。
ステップ 3	ユーザプロファイルの設定タスク フロー, （282 ページ）	アクセスと機能に関する同じ要件を満たすユーザのグループにユーザ プロファイルを設定します。ユーザ プロファイルは、共通の電話および電話回線設定で構成されており、ユーザプロファイルを使用するユーザ向けに新しい電話や電話回線をすばやく設定できます。このプロファイルを使用するユーザ向けにセルフプロビジョニングを有効化できます。
ステップ 4	サービスプロファイルの設定タスク フロー, （286 ページ）	ユニファイド コミュニケーション（UC）サービスの設定で、サービス プロファイルを設定します。このサービスプロファイルは、同じサービス要件が設定されているユーザのグループに適用できます。サービス プロファイルでは、このサービスプロファイルを使用するユーザ向けにプロビジョニングされている新しい電話向けに UC サービスを設定できます。
ステップ 5	機能グループテンプレートの設定, （296 ページ）	これはオプションです。機能グループテンプレートをエンドユーザに設定します。機能グループテンプレートには、共通機能設定に加え、割り当てられているユーザプロファイルおよびサービス プロファイルが含まれます。LDAP 同期ユーザの場合、LDAP 同期中に機能グループ テンプレートを割り当てられるため、ユーザプロファイル、サービスプロファイル、回線およびサービステンプレート、セルフプロビジョニング機能がユーザに割り当てられます。
ステップ 6	LDAP 同期設定のタスク フロー, （300 ページ）	会社用 LDAP ディレクトリを導入する場合は、カンパニーディレクトリ (LDAP) からエンド ユーザを Cisco Unified Communications Manager データベースに直接インポートできます。
ステップ 7	LDAP 同期設定のタスク フロー, （300 ページ）	LDAP ディレクトリからエンドユーザをインポートしていない場合は、一括管理ツールを使用して、エンド ユーザ

	コマンドまたはアクション	目的
		リストやエンドユーザ設定を CSV ファイルで Cisco Unified Communications Manager データベースにインポートできます。 一括アドミニストレーション ガイドを使用して、データベースに一括トランザクションを実行する方法については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの『*Cisco Unified Communications Manager Bulk Administration* ガイド』を参照してください。
ステップ 8	手動エンドユーザ設定のタスク フロー, (314 ページ)	これはオプションです。新しいユーザを手動でデータベースに追加します。



第 32 章

ユーザ アクセスの設定

- ユーザ アクセスの概要，257 ページ
- ユーザ アクセスの前提条件，260 ページ
- ユーザ アクセス設定のタスク フロー，260 ページ
- 標準権限とアクセス コントロール グループ，267 ページ

ユーザ アクセスの概要

Cisco Unified Communications Manager に対するユーザ アクセスは、次の項目をエンド ユーザに割り当てることで管理できます。

- ロール
- [アクセスコントロールグループ（Access Control Groups）]
- ユーザ ランク

ロール、アクセス コントロール グループ、ユーザ ランク コントロールでは、Cisco Unified Communications Manager に対する複数レベルのセキュリティを提供します。各ロールでは、Cisco Unified Communications Manager 内の特定のリソースに対する一連の権限を定義します。アクセス コントロール グループにロールを割り当て、そのアクセス コントロール グループにエンド ユーザを割り当てると、それらのエンド ユーザにそのロールで定義されているすべてのアクセス権限を付与することになります。

ユーザ ランク フレームワークはロールとアクセス コントロール グループ フレームワークをオーバーレイして、エンドユーザが使用可能なグループを決定します。エンド ユーザとアプリケーション ユーザは、それぞれのユーザ ランクで許可されるアクセス コントロール グループにのみ割り当てることができます。

ロールの概要

エンドユーザをプロビジョニングする場合、ユーザにどのようなロールを割り当てるか決定する必要があります。ロールはエンドユーザ、アプリケーションユーザ、またはアクセスコントロール グループに割り当てることができます。単独のユーザに複数のロールを割り当てることができます。

各ロールには、特定のリソースまたはアプリケーションに接続される一連の権限が含まれます。たとえば、標準CCMエンドユーザのロールは、そのロールが割り当てられているユーザに、Cisco Unified Communications セルフ ケア ポータルへのアクセス権を提供します。また、Cisco Unified Communications Manager の管理、Cisco CDR Analysis and Reporting、Dialed Number Analyzer、CTI インターフェイスなどのリソースへのアクセスを提供するロールを割り当てることもできます。特定の設定ウィンドウのようなグラフィカルユーザインターフェイスを使用する大部分のリソースでは、ロールに接続された権限によって、ユーザはそのウィンドウのデータ、または関連するウィンドウのグループ内のデータを閲覧したり更新できます。

ロールの設定と割り当て

標準ロールをユーザに割り当てるか、またはカスタム ロールを作成するかを決定する必要があります。

- 標準ロール：標準ロールとは、Cisco Unified Communications Manager に最初からインストールされている、デフォルトの事前定義のロールです。ロールの権限を編集または変更することはできません。
- カスタム ロール：カスタム ロールは自分で作成するロールです。ユーザに割り当てる権限を含む標準ロールがないときに、カスタムロールを作成できます。たとえば、標準ロールを割り当てようとしたが、権限の 1 つを変更したい場合、標準ロールの権限をカスタム ロールにコピーし、そのカスタム ロールで権限を編集できます。

権限のタイプ

各ロールには、特定のリソースに接続される一連の権限が含まれます。リソースに割り当てられる権限には 2 種類あります。

- [読み取り（Read）]：読み取り権限では、ユーザはそのリソースの設定を閲覧できますが、設定を更新することはできません。たとえば、この権限ではユーザが特定の設定ウィンドウの設定を閲覧できますが、そのアプリケーションの設定ウィンドウには更新ボタンやアイコンは表示されません。
- [更新（Update）]：更新権限では、ユーザはそのリソースの設定を変更できます。たとえば、この権限ではユーザが特定の設定ウィンドウで更新を実行できます。

エンドユーザ ロールと管理者ロール

標準 CCM エンドユーザ（Standard CCM End Users）ロールは、Cisco Unified Communications セルフ ケア ポータルへのアクセス権をエンドユーザに提供します。CTI アクセスなどの追加権限につ

いては、標準 CTI 対応（Standard CTI Enabled）ロールなどの追加ロールを割り当てる必要があります。

標準 CCM 管理ユーザ（Standard CCM Admin Users）ロールは、すべての処理タスクのベース ロールであり、認証ロールとして機能します。このロールは、Cisco Unified Communications Manager Administration のユーザ インターフェイスへの管理者アクセスを提供します。Cisco Unified CM の管理では、このロールを Cisco Unified Communications Manager Administration にログインするために必要なロールとして定義しています。

関連トピック

標準権限とアクセス コントロール グループ, （267 ページ）

アクセス コントロール グループの概要

ロールとともにアクセスコントロールグループを使用して、同様のアクセス要件のユーザ グループにネットワークへのアクセス権限をすばやく指定できます。

アクセス コントロール グループは、エンドユーザとアプリケーション ユーザのリストです。類似したアクセスの必要性を共有するエンドユーザとアプリケーションユーザに、必要な権限と役割を含むアクセス コントロール グループを指定できます。アクセス コントロール グループに割り当てられるエンドユーザやアプリケーションのユーザは、そのアクセスコントロールグループの最小ランク要件を満たす必要があります。たとえば、4 のユーザ ランクを持つユーザは、最小ランク要件が 4 ～ 10 のアクセス コントロール グループにしか割り当てることができません。

システムには、一連の事前定義された標準アクセスコントロールグループが含まれています。それぞれの標準アクセスコントロールグループには、デフォルトで割り当てられている一連のロールがあります。ユーザをそのアクセスコントロールグループに割り当てると、それらの役割もそのエンドユーザに割り当てられます。

標準アクセスコントロールグループに割り当てられたロールは編集できません。ただし、カスタマイズされたアクセスコントロールグループを作成し、選択したロールをそのカスタマイズされたアクセス コントロール グループに割り当てることができます。

関連トピック

標準権限とアクセス コントロール グループ, （267 ページ）

ユーザ ランクの概要

ユーザ ランクのアクセス コントロールでは、管理者がエンド ユーザやアプリケーション ユーザに提供できるアクセス レベルに対する一連の制御を行います。[ユーザ ランク（User Rank）] パラメータは 1 ～ 10 の整数で指定し、一番高いランクは 1 です。ユーザ ランクはユーザとアクセス コントロール グループの両方に割り当てられるため、特定のアクセス コントロール グループに割り当て可能なユーザを決定するランク階層が作成されます。

エンドユーザやアプリケーションユーザをプロビジョニングする場合、管理者は各ユーザのユーザ ランクを割り当てる必要があります。管理者は、各アクセス コントロール グループにもユーザ ランクを割り当てる必要があります。管理者は、同じランクや下のランクのアクセス コント

ロール グループにのみユーザを割り当てることができます。たとえば、あるエンドユーザのユーザ ランクが 3 の場合、3 ～ 10 のユーザ ランクが設定されているアクセス コントロール グループに割り当てることができます。そのユーザを、ユーザ ランクが 1 である必要があるアクセス コントロール グループに割り当てることはできません。

管理者は、[ユーザ ランクの設定（User Rank Configuration）] ウィンドウ内でユーザ ランクの階層をカスタマイズして、それらのランクをエンド ユーザ、アプリケーション ユーザ、アクセス コントロール グループに割り当てることができます。

ユーザ アクセスの前提条件

エンド ユーザをプロビジョニングする前に、次の手順を実行します。

- 標準権限とアクセス コントロール グループ, （267 ページ）定義済みのロールとアクセス コントロール グループのリストを確認します。カスタマイズされたロールとグループを設定する必要があるかどうかを判断します。
- ユーザとグループに割り当てるユーザ ランクを計画します。

ユーザ アクセス設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	カスタム ユーザ ランクの作成, （261 ページ）	システムのユーザのランク階層を設定します。
ステップ 2	新しいロールを作成する必要がある場合は、次のいずれかの方法を使用します。 • カスタム ロールの作成, （261 ページ） • 既存のロールのコピー, （263 ページ）	新しいロールをまったく最初から作成して設定するには、「作成（Create）」手順を実行します。新しいロールが既存のロールと同様の権限を持つ場合は、「コピー（Copy）」手順を実行します。既存のロールから新しいロールに権限をコピーしてから、新しいロールの権限を編集します。
ステップ 3	新しいアクセス コントロール グループを作成する必要があるときは、次のいずれかの方法を使用します。 • アクセス コントロール グループの作成, （264 ページ）	新しいアクセス コントロール グループをまったく最初から作成するには、「作成（Create）」手順を実行します。既存のアクセス コントロール グループに新しいアクセス コントロール グループと類似の設定があれば、「コピー（Copy）」手順を実行します。既存のアクセス コントロール グループから新しいグループに設定をコピーしてから編集できます。

	コマンドまたはアクション	目的
	• アクセス コントロール グループのコピー，（264 ページ）	
ステップ 4	アクセス コントロール グループへの権限の割り当て，（265 ページ）	新しいアクセス コントロール グループを作成したら、アクセス コントロール グループにロールを割り当てます。
ステップ 5	重複する権限ポリシーの設定，（266 ページ）	重複するアクセス権限をカバーするには、エンタープライズポリシーを設定します。これはエンドユーザやアプリケーションのユーザが複数のアクセス コントロール グループまたはロールに割り当てられ、それぞれが相反する権限設定になっている場合をカバーしています。

関連トピック

標準権限とアクセス コントロール グループ，（267 ページ）

カスタム ユーザ ランクの作成

ランク階層を目的として、カスタム ユーザ ランクを作成するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザ ランク（User Rank）] 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 ランク（User Rank）] ドロップダウン メニューから、1 ～ 10 のランク設定を選択します。最も高いランクは 1 です。

ステップ 4 [ランク名（Rank Name）] と [説明（Description）] を入力します。

ステップ 5 [保存（Save）] をクリックします。

カスタム ロールの作成

必要な権限設定を備えたシステム定義のロールがないとき、カスタム ロールを作成します。

ヒント　自分が作成する新しいロールの権限が既存のロールの権限に似ている場合、手順 既存のロールのコピー, （263 ページ） を実行して、編集可能な新しいロールに既存の権限をコピーします。

手順

ステップ 1　Cisco Unified CM の管理で、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [権限（Role）] をクリックします。

ステップ 2　[アプリケーション（Application）] ドロップダウン リスト ボックスから、この権限を関連付けるアプリケーションを選択します。
[権限の設定（Role Configuration）] ウィンドウが表示されます。

ステップ 3　[Next] をクリックします。

ステップ 4　[名前（Name）] テキストボックスに、権限の名前を入力します。
名前は、128 文字まで入力できます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。

ステップ 5　[説明（Description）] テキストボックスに、権限の説明を入力します。
説明は 128 文字以内にする必要があります。

ステップ 6　新しい権限が各リソースに対して持つ特権を次のように編集します。

- 権限がそのリソースを表示できるようにするには、[読み取り（Read）] チェックボックスをクリックします。
- 権限がそのリソースを編集できるようにするには、[更新（Update）] チェックボックスをクリックします。
- 権限がそのリソースを表示および編集できるようにするには、[読み取り（Read）] と [更新（Update）] の両方のチェックボックスをオンにします。
- 権限に、リソースへのどのようなアクセスも許可しない場合は、両方のチェックボックスをオフのままにします。

ステップ 7　この権限のページに表示されるすべてのリソースに特権を付与する場合は、[すべてにアクセス権を付与（Grant access to all）] ボタンをクリックし、すべてのリソースから特権を削除する場合は、[すべてにアクセスを許可しない（Deny access to all）] をクリックします。

（注）　リソースのリストが複数のページにわたって表示される場合、このボタンは、現在のページに表示されるリソースに限り適用されます。他のページのリストにあるリソースのアクセス権を変更するには、それらのページを表示し、表示されたページでこのボタンを使用する必要があります。

ステップ 8　[保存（Save）] をクリックします。

次の作業

アクセス コントロール グループの作成, （264 ページ）

既存のロールのコピー

[コピー（Copy）] コマンドを使用すると、既存のロール設定に基づいて、新しいロールを作成できます。Cisco Unified Communications Manager では、標準ロールを編集できません。ただし、[コピー（Copy）] コマンドで標準ロールとリソースと権限が同一の新しいロールを作成できます。そして自分が作成した新しいロールの権限を編集できます。

手順

ステップ 1 Cisco Unified CM の管理で、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [権限（Role）] をクリックします。

ステップ 2 [検索（Find）] をクリックし、コピーするリソースと特権がある権限を選択します。

ステップ 3 [コピー（Copy）] をクリックします。

ステップ 4 新しい権限の名前を入力し、[OK] をクリックします。
[権限の設定（Role Configuration）] ウィンドウに新しい権限の設定が表示されます。新しい権限の特権は、コピーした権限の特権と同じです。

ステップ 5 新しい権限のリソースのいずれかで、次のように特権を編集します。

- [読み取り（Read）]チェックボックスをオンにして、ユーザにリソースの表示を許可します。
- [更新（Update）] チェックボックスをオンにして、ユーザにリソースの編集を許可します。
- リソースへのアクセスを制限するには、両方のチェックボックスをオフにします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

次のいずれかの方法で新しいアクセス コントロール グループを作成します。

- アクセス コントロール グループの作成, （264 ページ）
- アクセス コントロール グループのコピー, （264 ページ）

関連トピック

標準権限とアクセス コントロール グループ, （267 ページ）

アクセス コントロール グループの作成

この手順では、新しいアクセスコントロールグループを作成する必要があります。システム定義アクセス コントロール グループが導入環境のニーズを満たさない場合、新しいアクセス コントロール グループを作成する必要があります。

はじめる前に

新しいロールを作成する必要がある場合は、次のいずれかの手順を実行します。

- カスタム ロールの作成, （261 ページ）
- 既存のロールのコピー, （263 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [名前（Name）] にアクセス コントロール グループの名前を入力します。

ステップ 4 [ユーザで利用できるユーザ ランク（Available for Users with User Rank as）] ドロップダウンから、このグループに割り当てる、ユーザの最低ランクを選択します。デフォルトのユーザ ランクは 1 です。

ステップ 5 [保存（Save）] をクリックします。

次の作業

アクセス コントロール グループへの権限の割り当て, （265 ページ）

アクセス コントロール グループのコピー

既存のアクセス コントロール グループから設定をコピーして、カスタム アクセス コントロール グループを作成します。既存のアクセス コントロール グループをコピーすると、システムにより、新しいアクセスコントロールグループにすべての設定（割り当てた権限やユーザを含む）がコピーされます。ただし、デフォルトのアクセス コントロール グループとは異なり、カスタム アクセス コントロール グループに割り当てられた権限は編集できます。

はじめる前に

新しい権限を作成する必要がある場合、次のステップのいずれかを実行します。

- カスタム ロールの作成, （261 ページ）
- 既存のロールのコピー, （263 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[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。

ステップ 2 [検索（Find）] をクリックして、設定をコピーする対象のアクセス コントロール グループを選択します。

ステップ 3 [コピー（Copy）] をクリックします。

ステップ 4 新しいアクセス コントロール グループの名前を入力し、[OK] をクリックします。

ステップ 5 [ユーザで利用できるユーザ ランク（Available for Users with User Rank as）] ドロップダウンから、このグループに割り当てる、ユーザの最低ランクを選択します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

アクセス コントロール グループへの権限の割り当て, （265 ページ）

関連トピック

標準権限とアクセス コントロール グループ, （267 ページ）
アクセス コントロール グループへの LDAP 同期ユーザの割り当て, （310 ページ）
アクセス コントロール グループへのエンド ユーザの割り当て, （315 ページ）

アクセス コントロール グループへの権限の割り当て

作成したすべての新しいアクセスコントロールグループに権限を割り当てます。既存のグループからアクセス コントロール グループをコピーした場合、権限の削除が必要になることもあります。

（注） デフォルトで設定されている標準アクセス コントロール グループの権限の割り当てはいずれも編集できません。

はじめる前に

新しいアクセス コントロール グループを作成するには、次のタスクのいずれかを実行します。

- アクセス コントロール グループの作成, （264 ページ）
- アクセス コントロール グループのコピー, （264 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[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。

ステップ 2 [検索（Find）] をクリックし、アクセス コントロール グループを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リスト ボックスで、[アクセス コントロール グループへの権限の割り当て（Assign Role to Access Control Group）] を選択し、[移動（Go）] をクリックします。

ステップ 4 権限を割り当てる必要がある場合は、以下の手順に従います。

a) [グループに権限を割り当て（Assign Role to Group）] をクリックします。

b) [権限の検索と一覧表示（Find and List Roles）] ウィンドウで、グループに割り当てる権限のチェックボックスをオンにします。

c) [選択項目の追加（Add Selected）] をクリックします。

ステップ 5 権限を削除する必要がある場合は、以下の手順に従います。

a) [権限（Role）] リスト ボックスで、削除する権限を強調表示します。

b) [割り当てた権限の削除（Delete Role Assignment）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

重複する権限ポリシーの設定, （266 ページ）

重複する権限ポリシーの設定

アクセス コントロール グループの割り当てで重複するユーザ権限を Cisco Unified Communications Manager がどのように処理するのかを設定します。これにより、エンド ユーザが複数のアクセス コントロール グループに割り当てられ、それぞれのロールとアクセス権限が相反する状況に対応できます。

はじめる前に

アクセス コントロール グループへの権限の割り当て, （265 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM 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 [ユーザ管理パラメータ（User Management Parameters）] で、[重複したユーザ グループとロールの実質的なアクセス権（Effective Access Privileges For Overlapping User Groups and Roles）] に次のいずれかの値を設定します。

- [最大（Maximum）] —実質的な権限は、重複したすべてのアクセス コントロール グループの最大限の権限になります。これがデフォルトのオプションです。
- [最小（Minimum）]—実質的な権限は、重複したすべてのアクセス コントロール グループの最小限の権限になります。

ステップ 3 [保存（Save）] をクリックします。

標準権限とアクセス コントロール グループ

次の表は、Cisco Unified Communications Manager にあらかじめ設定されている標準権限およびアクセス コントロール グループの概要です。標準権限が持つ特権はデフォルトで設定されています。また、標準権限に関連付けられたアクセスコントロールグループも、デフォルトで設定されています。

標準権限、および標準権限に関連付けられたアクセスコントロールグループの両方で、特権または権限の割り当てを編集できません。

表 *20*：標準権限、特権、およびアクセス コントロール グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
Standard AXL API Access	AXL データベース API へのアクセスを許可します。	標準 CCM スーパー ユーザ
標準AXL APIユーザ	AXL API を実行するログイン権限を付与します。	
標準 AXL 読み取り専用 API アクセス	AXL 読み取り専用 API（API の一覧表示、API の取得、SQL Query API の実行）の実行をデフォルトで許可します。	
標準管理Rep Tool管理	Cisco Unified Communications Manager CDR Analysis and Reporting（CAR）の表示および設定が可能になります。	標準 CAR 管理ユーザ、標準 CCM スーパー ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準監査ログ管理	監査ロギング機能の次のタスクを実行できます。 • Cisco Unified Serviceability の [監査ログ設定（Audit Log Configuration）] ウィンドウでの、監査ロギングの表示および設定 • Cisco Unified Serviceability でのトレースの表示と設定、および Real-Time Monitoring Tool の監査ログ機能向けトレースの収集 • Cisco Unified Serviceability の Cisco Audit Event Service の表示、開始、停止 • RTMT での、関連付けられたアラートの表示および更新	標準監査ユーザ
Standard CCM Admin Users	Cisco Unified Communications Manager の管理へのログイン権限を付与します。	標準CCM管理ユーザ、標準CCMゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準CCMサーバモニタリング、標準CCMスーパーユーザ、標準CCMサーバメンテナンス、標準 パケット スニファ ユーザ
[標準CCMエンドユーザ（Standard CCM End Users）]	Cisco Unified Communications セルフケアポータルにログインする権限をエンド ユーザに付与します。	[標準CCMエンドユーザ（Standard CCM End Users）]

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準 CCM 機能管理	Cisco Unified Communications Manager の管理で、次のタスクを実行できます。 • 一括管理ツールによる次の項目の表示、削除、挿入 ◦ クライアント関連のコードと強制承認コード ◦ コール ピックアップ グループ • Cisco Unified Communications Manager の管理での次の項目の表示および設定 ◦ クライアント関連のコードと強制承認コード ◦ コール パーク ◦ コール ピックアップ ◦ ミートミーの番号またはパターン ◦ メッセージ受信 ◦ Cisco Unified IP Phone サービス ◦ ボイスメール パイロット、ボイスメール ポート ウィザード、ボイスメール ポート、ボイスメール プロファイル	標準 CCM サーバ メンテナンス
標準 CCM ゲートウェイ管理	Cisco Unified Communications Manager の管理で、次のタスクを実行できます。 • 一括管理ツールによるゲートウェイ テンプレートの表示および設定 • ゲートキーパー、ゲートウェイ、およびトランクの表示および設定	標準 CCM ゲートウェイ管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準 CCM 電話管理	Cisco Unified Communications Manager の管理で、次のタスクを実行できます。 • 一括管理ツールによる電話の表示とエクスポート • 一括管理ツールによるユーザデバイスプロファイルの表示と挿入 • Cisco Unified Communications Manager の管理での次の項目の表示および設定 ◦ BLF 短縮ダイヤル ◦ CTI ルート ポイント ◦ デフォルト デバイス プロファイルまたはデフォルト プロファイル ◦ 電話番号、および回線の状態 ◦ ファームウェア ロード情報 ◦ 電話ボタンテンプレートまたはソフトキーテンプレート ◦ 電話機 ◦ [電話の設定（Phone Configuration）] ウィンドウの [ボタン項目を変更（Modify Button Items）] をクリックすることによる、特定の電話に対する電話ボタンの情報の並べ替え	標準 CCM 電話管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準 CCM ルート プラン計画管理	Cisco Unified Communications Manager の管理で、次のタスクを実行できます。 • アプリケーション ダイヤル ルールの表示および設定 • コーリング サーチ スペースおよびパーティションの表示および設定 • ダイヤル ルール パターンを含むダイヤル ルールの表示および設定 • ハントリスト、ハントパイロット、回線グループの表示および設定 • ルート フィルタ、ルート グループ、ルート ハントリスト、ルートリスト、ルートパターン、ルート プラン レポートの表示および設定 • 時間帯およびスケジュールの表示および設定 • トランスレーション パターンの表示および設定	
標準 CCM サービス管理	Cisco Unified Communications Manager の管理で、次のタスクを実行できます。 • 次の項目を表示および設定できます。 ◦ アナンシエータ、会議ブリッジ、トランスコーダ ◦ オーディオ ソースおよび MOH サーバ ◦ メディア リソース グループおよびメディア リソース グループ リスト ◦ Media Termination Point; メディア ターミネーション ポイント ◦ Cisco Unified Communications Manager Assistant ウィザード • 一括管理ツールの [マネージャの削除（Delete Managers）]、[マネージャ/アシスタントの削除（Delete Managers/Assistants）] および [マネージャ/アシスタントの挿入（Insert Managers/Assistants）] ウィンドウでの表示および設定ができます。	標準 CCM サーバ メンテナンス

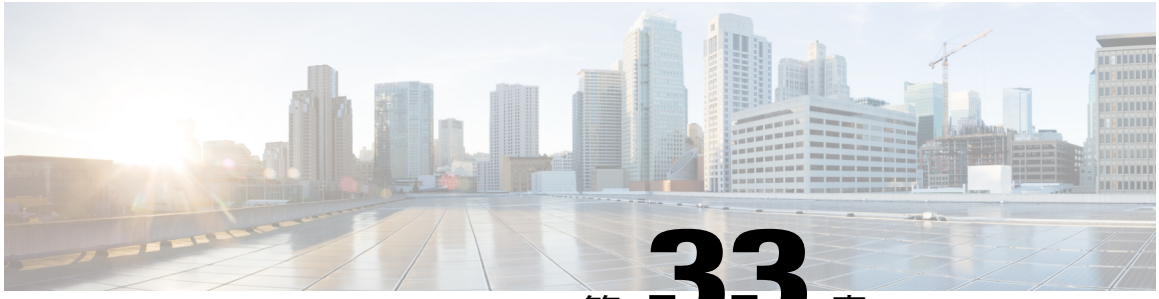
標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準 CCM システム管理	Cisco Unified Communications Manager の管理で、次のタスクを実行できます。 • 次の項目を表示および設定できます。 ◦ 代替ルーティング（AAR）グループの自動化 ◦ Cisco Unified Communications Manager（Cisco Unified CM）および Cisco Unified Communications Manager のグループ ◦ 日時グループ ◦ デバイス デフォルト ◦ デバイス プール ◦ エンタープライズ パラメータ ◦ エンタープライズ電話の設定 ◦ ロケーション（Locations） ◦ Network Time Protocol（NTP）サーバ ◦ プラグイン ◦ Skinny Call Control Protocol（SCCP）または Session Initiation Protocol（SIP）を実行する電話用のセキュリティ プロファイル、SIP トランク用のセキュリティ プロファイル ◦ Survivable Remote Site Telephony（SRST）の参照 ◦ サーバ • 一括管理ツールの、[ジョブ スケジューラ（Job Scheduler）] ウィンドウでの表示と設定	標準 CCM サーバ メンテナンス
標準 CCM ユーザ権限管理	Cisco Unified Communications Manager の管理で、アプリケーション ユーザの表示および設定ができます。	
標準 CCMADMIN 管理	CCMAdmin システムのすべての面を利用できます。	
標準 CCMADMIN 管理	Cisco Unified Communications Manager の管理および一括管理ツールのすべての項目を表示および設定できます。	標準 CCM スーパー ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準CCMADMIN管理	Dialed Number Analyzer の情報を表示および設定できます。	
標準 CCMADMIN 読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	
標準 CCMADMIN 読み取り専用	Cisco Unified Communications Manager の管理および一括管理ツールの項目を表示できます。	標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバ メンテナンス、標準 CCM サーバ モニタリング
標準 CCMADMIN 読み取り専用	Dialed Number Analyzer で、ルーティング設定の分析ができます。	
標準 CCMUSER 管理	Cisco Unified Communications セルフケアポータルへのアクセスを許可します。	[標準CCMエンドユーザ（Standard CCM End Users）]
標準 CTI 通話モニタリング許可	CTI アプリケーションまたはデバイスでコールをモニタできます。	標準 CTI 通話モニタリング許可
標準 CTI コール パーク モニタリング許可	CTI アプリケーションまたはデバイスでコールパークをモニタできます。	標準 CTI コール パーク モニタリング許可
標準 CTI 通話録音許可	CTI アプリケーション/デバイスで通話を録音できます。	標準 CTI 通話録音許可
標準 CTI 発信者番号の変更許可	CTI アプリケーションが発信者番号を通話中に変更できます。	標準 CTI 発信者番号の変更許可
標準 CTI によるすべてのデバイスの制御	CTI で制御可能なすべてのデバイスを制御できます。	標準 CTI によるすべてのデバイスの制御
標準 CTI 接続された転送と会議をサポートする電話の制御許可	接続された転送および会議をサポートするすべての CTI デバイスを制御できます。	標準 CTI 接続された転送と会議をサポートする電話の制御許可
標準 CTI ロールオーバー モードをサポートする電話の制御許可	ロールオーバー モードをサポートするすべての CTI デバイスを制御できます。	標準 CTI ロールオーバー モードをサポートする電話の制御許可

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準 CTI SRTP 重要素材の受信許可	CTI アプリケーションが、SRTP を使う重要な素材にアクセスしたり、その素材を配信したりできるようにします。	標準 CTI SRTP 重要素材の受信許可
[標準CTIを有効にする（Standard CTI Enabled）]	CTI アプリケーションの制御を可能にします。	[標準CTIを有効にする（Standard CTI Enabled）]
標準 CTI セキュア接続	Cisco Unified Communications Manager へのセキュアな CTI 接続が可能になります。	標準 CTI セキュア接続
標準CUReporting	アプリケーション ユーザが、さまざまなソースからレポートを作成できます。	
標準CUReporting	Cisco Unified Reporting での、レポートの表示、ダウンロード、作成、およびアップロードができます。	標準CCM管理ユーザ、標準CCM スーパー ユーザ
標準 EM 認証プロキシ権限	アプリケーションで使用する Cisco Extension Mobility（EM）の認証権限を管理します。この権限は、（Cisco Unified Communications Manager Assistant や Cisco Web Dialer などの）Cisco Extension Mobility と対話するすべてのアプリケーションユーザに必要です。	標準 CCM スーパー ユーザ、標準 EM 認証プロキシ権限
標準パケット スニッフィング	Cisco Unified Communications Manager の管理にアクセスし、パケット スニッフィング（キャプチャ）ができます。	標準パケット スニファ ユーザ
Standard RealtimeAndTraceCollection	Cisco Unified Serviceability および Real-Time Monitoring Tool にアクセスし、次の項目を表示および使用できます。 • Simple Object Access Protocol（SOAP）Serviceability AXL API • SOAP コール レコード API • SOAP 診断ポータル（Analysis Manager）データベース サービス • 監査ログ機能のトレースの設定 • トレース収集などの、Real-Time Monitoring Tool の設定	Standard RealtimeAndTraceCollection

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
Standard SERVICEABILITY	Cisco Unified Serviceability または Real-Time Monitoring Tool で、次のウィンドウを表示および設定できます。 • [アラーム設定およびアラーム定義（Alarm Configuration and Alarm Definitions）]（Cisco Unified Serviceability） • [監査トレース（Audit Trace）]（読み取りおよび表示のみ可能なマークが付けられています） • SNMP 関連のウィンドウ（Cisco Unified Serviceability） • [トレースの設定（Trace Configuration）] および [トレース設定のトラブルシューティング（Troubleshooting of Trace Configuration）]（Cisco Unified Serviceability） • ログ パーティションのモニタリング • [アラートの設定（Alert Configuration）]（RTMT）、[プロファイルの設定（Profile Configuration）]（RTMT）、および [トレース収集（Trace Collection）]（RTMT） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベース サービスを表示および使用できます。 SOAP コールレコード API については、RTMT Analysis Manager Call Record の権限が、このリソースを介して制御されます。 SOAP 診断ポータル データベース サービスについては、RTMT Analysis Manager Hosting Database アクセスが、このリソースを介して制御されます。	標準 CCM サーバ モニタリング、標準 CCM スーパー ユーザ
標準 SERVICEABILITY 管理	有用性の管理者は、Cisco Unified Communications Manager の管理に表示されるプラグイン ウィンドウにアクセスでき、このウィンドウからプラグインをダウンロードできます。	
標準 SERVICEABILITY 管理	Dialed Number Analyzer の有用性をすべての面で管理できます。	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセスコントロール グループ
標準 SERVICEABILITY 管理	Cisco Unified Serviceability および Real-Time Monitoring Tool のすべてのウィンドウを表示および設定できます（[監査トレース（Audit Trace）] では表示のみ可能です）。 すべての SOAP Serviceability AXL API を表示および使用できます。	
標準 SERVICEABILITY 読み取り専用	Dialed Number Analyzer のコンポーネントで使用する有用性に関するすべてのデータを表示できます。	標準 CCM 読み取り専用
標準 SERVICEABILITY 読み取り専用	Cisco Unified Serviceability および Real-Time Monitoring Tool で、設定を表示できます。（標準監査ログ管理の権限により表示される監査設定ウィンドウは除きます） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベース サービスをすべて表示できます。	
標準システム サービス管理	Cisco Unified Serviceability で、サービスを表示、アクティベート、開始、および停止できます。	
標準 SSO 設定管理	SAML SSO の設定をすべての面で管理できます。	
標準機密アクセス レベル ユーザ	すべての機密アクセス レベル ページにアクセスできます。	標準 Cisco Call Manager 管理
標準 CCMADMIN 管理	CCMAdmin システムをすべての面で管理できます。	標準 Cisco Unified CM IM およびプレゼンスの管理
標準 CCMADMIN 読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	標準 Cisco Unified CM IM およびプレゼンスの管理
標準 CUReporting	アプリケーション ユーザが、さまざまなソースからレポートを作成できます。	標準 Cisco Unified CM IM およびプレゼンスのレポーティング



第 33 章

クレデンシャル ポリシーの設定

- クレデンシャル ポリシーの概要，277 ページ
- クレデンシャル ポリシーの設定タスク フロー，278 ページ

クレデンシャル ポリシーの概要

クレデンシャル ポリシーは、Cisco Unified Communications Manager 内のリソースの認証プロセスを制御します。クレデンシャル ポリシーは、失敗したログイン試行、エンド ユーザ パスワードの有効期限とロックアウト期間、エンドユーザ PIN、アプリケーション ユーザ パスワードなどのパスワード要件とアカウントロックアウトの詳細を定義します。クレデンシャルポリシーは、すべてのエンドユーザ PIN などの特定のクレデンシャル タイプのすべてのアカウントに広く割り当てることも、特定のアプリケーションユーザやエンドユーザ用にカスタマイズすることもできます。

クレデンシャル タイプ

[クレデンシャル ポリシー設定（Credential Policy Configuration）] で、新しいクレデンシャル ポリシーを設定し、次の 3 つのクレデンシャル タイプのそれぞれのデフォルト クレデンシャル ポリシーとして新しいポリシーを適用できます。

- エンド ユーザ PIN
- エンド ユーザ パスワード
- アプリケーション ユーザ パスワード

また、特定のエンド ユーザ PIN、エンド ユーザ パスワード、またはアプリケーション ユーザ パスワードにクレデンシャル ポリシーを適用することもできます。

単純なパスワード

単純なパスワードと PIN を確認するようにシステムを設定できます。単純なパスワードとは、ABCD や 123456 といった容易に推測できるパスワードなどで、これらは簡単にハッキングできるクレデンシャルです。

単純でないパスワードは、次の要件を満たしています。

- 大文字、小文字、数字、記号の 4 種類の文字のうち 3 種類を含んでいる。
- 3 回以上連続して同じ文字や数字を使用していない。
- 繰り返しや、エイリアス、ユーザ名、内線番号を含んでいない。
- 連続する文字または数字で構成されていない。たとえば、654321 または ABCDEFG などのパスワードは許容されません。

PIN には、数字（0 ～ 9）のみを使用できます。単純でない PIN は、次の基準を満たしています。

- 3 回以上連続して同じ数字を使用していない。
- 繰り返しや、ユーザの内線番号、メールボックス、またはユーザの反転させた内線番号やメールボックスを含んでいない。
- 3 つの異なる数字を含んでいる。たとえば、121212 などの PIN は単純です。
- ユーザの姓または名の数字表現（たとえば、名前によるダイヤル）が使用されていない。
- たとえば、408408 などの複数の数字の繰り返しや、2580、159、753 などのキーパッド上で直線上にあるダイヤルのパターンを含んでいない。

クレデンシャル ポリシーの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	クレデンシャル ポリシーの設定, （279 ページ）	エンドユーザとアプリケーションユーザにクレデンシャル ポリシーを設定します。
ステップ 2	クレデンシャル ポリシーのデフォルト クレデンシャルの設定, （279 ページ）	3つのクレデンシャルタイプのいずれか（エンドユーザパスワードとアプリケーションユーザ）にデフォルトのクレデンシャル ポリシーとして設定されているクレデンシャル ポリシーを適用します。デフォルトのクレデンシャル ポリシーは、新規にプロビジョニングされたユーザのクレデンシャルタイプにデフォルトで適用されます。

関連トピック

エンドユーザへのクレデンシャル ポリシーの適用, （316 ページ）

クレデンシャル ポリシーの設定

エンドユーザの PIN またはパスワードなどの特定のクレデンシャル タイプに一致するすべてのクレデンシャルのデフォルトのクレデンシャルポリシーとして適用可能なクレデンシャルポリシーを設定します。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [クレデンシャル ポリシー（Credential Policy）] を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [検索（Find）] をクリックし、既存のクレデンシャル ポリシーを選択します。
- [新規追加（Add New）] をクリックして、新しいクレデンシャル ポリシーを作成します。

ステップ 3 [クレデンシャル ポリシーの設定（Credential Policy Configuration）] ウィンドウの各フィールドに入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

クレデンシャル ポリシーのデフォルト クレデンシャルの設定, （279 ページ）

クレデンシャル ポリシーのデフォルト クレデンシャルの設定

クレデンシャルポリシーのデフォルトクレデンシャルを設定するには、次の手順を実行します。ユーザが次のログインで変更する必要がある一時的なパスワードを割り当てるために、デフォルト クレデンシャルを割り当てることができます。

はじめる前に

クレデンシャル ポリシーの設定, （279 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザ管理（User Management）] > [クレデンシャル ポリシーのデフォルト（Credential Policy Default）] を選択します。

ステップ 2 [クレデンシャル ポリシー（Credential Policy）] ドロップダウン リスト ボックスから、このグループのクレデンシャル ポリシーを選択します。

ステップ 3 [クレデンシャルの変更（Change Credential）] と [クレデンシャルの確認（Confirm Credential）] の両方にパスワードを入力します。

ステップ 4 このクレデンシャルをユーザに変更させない場合は、[ユーザは変更不可（User Cannot Change）] チェックボックスをオンにします。

ステップ 5 ユーザが次のログイン時に変更する必要がある、一時的なクレデンシャルを設定する場合は、[次回ログイン時に変更必要（User Must Change at Next Login）] チェックボックスをオンにします。

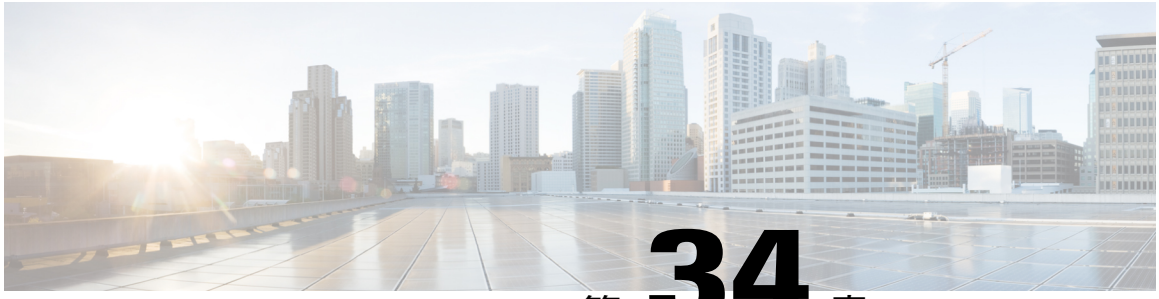
ステップ 6 クレデンシャルの期限を設定しない場合は、[有効期限なし（Does Not Expire）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

特定のエンドユーザまたは PIN にクレデンシャル ポリシーを適用する場合：

- エンドユーザへのクレデンシャル ポリシーの適用, （316 ページ）



第 34 章

ユーザ プロファイルの設定

- ユーザ プロファイルの概要，281 ページ
- ユーザ プロファイルの前提条件，282 ページ
- ユーザ プロファイルの設定タスク フロー，282 ページ

ユーザ プロファイルの概要

ユーザ プロファイルには、一般的なディレクトリ番号とデバイスの設定が含まれます。ユーザが必要とするデバイス設定と最も一般的なディレクトリ番号を含む異なるユーザ プロファイルを設定でき、その設定を必要としているユーザにそれぞれのユーザ プロファイルを割り当てることができます。ユーザのそれぞれの組に対する電話回線および電話の設定要件に応じて、会社のユーザのさまざまなグループについて異なるユーザ プロファイルを設定できます。

セルフプロビジョニングが有効になっているエンドユーザについては、ユーザプロファイルからの電話および電話回線の設定は、そのユーザがプロビジョニングする新しい電話すべてに適用されます。ユーザのセルフプロビジョニングが有効になっていないと、ユーザ プロファイルの設定は、エンドユーザに代わって管理者がプロビジョニングする新しい電話すべてに適用されます。

ユーザのプロファイルでは、エンド ユーザのプロファイルを作成するために次の電話および電話回線のテンプレートにある設定を使用します。

- ユニバーサル回線のテンプレート—ディレクトリ番号に通常割り当てられる一般的な電話回線の設定。ユニバーサル回線のテンプレートを使用すると、エンドユーザに割り当てられた新しいディレクトリ番号にすばやく電話回線を設定できます。
- ユニバーサル デバイス テンプレート—電話または他のデバイスに通常割り当てられる一般的なデバイス設定の集合。ユニバーサル デバイス テンプレートを使用すると、エンドユーザに割り当てられた新しい電話をすばやく設定できます。

ユーザ プロファイルの前提条件

ユーザ プロファイルを設定する前に、導入時にどのように電話をプロビジョニングするかの計画を立てることを確認します。セルフプロビジョニングを使用して、エンドユーザが自分の電話をプロビジョンできるようにするかどうかを決定します。

ユーザ プロファイルの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユニバーサル回線テンプレートの設定, （282 ページ）	電話番号に一般的に適用される共通設定を使用して、ユニバーサル回線テンプレートを設定します。
ステップ 2	ユニバーサルデバイステンプレートの設定, （283 ページ）	電話機やその他のデバイスに一般的に適用される共通設定を使用して、ユニバーサル デバイス テンプレートを設定します。
ステップ 3	ユーザ プロファイルの設定, （284 ページ）	ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザ プロファイルに割り当てます。

ユニバーサル回線テンプレートの設定

電話番号に通常適用される共通設定をユニバーサル回線テンプレートに設定します。1 つまたは複数のユニバーサル回線テンプレートを作成して、自分の組織で最も一般的な電話番号設定を反映した設定セットを作成できます。さらに、ユーザ プロファイルによって、ユーザにプロビジョニングする新しい電話番号にこれらの設定を適用できます。

手順

ステップ 1 Cisco Unified CM の管理で、[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル回線テンプレート（Universal Line Template）] 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 [ユニバーサル回線テンプレートの設定（Universal Line Template Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ユニバーサル デバイス テンプレートの設定, （283 ページ）

ユニバーサル デバイス テンプレートの設定

ユニバーサル デバイス テンプレートを設定します。ユニバーサル デバイス テンプレートには、通常、電話、リモート接続先プロファイル、またはエクステンションモビリティプロファイルに適用される、一連の共通設定が含まれます。組織内で最も共通するデバイス設定を反映した 1 つまたは複数のユニバーサル デバイス テンプレートを作成できます。また、ユーザ プロファイルを通じて、エンドユーザ用にプロビジョニングを行う新しいデバイスのすべてにこれらの設定を適用できます。

はじめる前に

ユニバーサル回線テンプレートの設定, （282 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル デバイス テンプレート（Universal Device Template）] 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 [ユニバーサル デバイス テンプレートの設定（Universal Device Template Configuration）] ウィンドウの各フィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ユーザ プロファイルの設定, （284 ページ）

ユーザ プロファイルの設定

プロファイルを使用するユーザに割り当てるユニバーサル回線テンプレートとユニバーサル デバイス テンプレートを含むユーザ プロファイルを設定します。このサービス プロファイルを使用するユーザに対してセルフプロビジョニングを有効にすることもできます。

はじめる前に

ユニバーサル デバイス テンプレートの設定, （283 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユーザ プロファイル（User Profile）] 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 プロファイルの [名前（Name）] および [説明（Description）] を入力します。

ステップ 4 [ユニバーサル デバイス テンプレート（Universal Device Template）] を、ユーザの [デスク フォン（Desk Phones）] 、[モバイルおよびデスクトップ デバイス（Mobile and Desktop Devices）] 、および [リモート接続先/デバイス プロファイル（Remote Destination/Device Profiles）] に割り当てます。

ステップ 5 [ユニバーサル回線テンプレート（Universal Line Template）] をこのユーザ プロファイルのユーザの電話回線に適用するために割り当てます。

ステップ 6 このユーザ プロファイルのユーザに自分の電話をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します

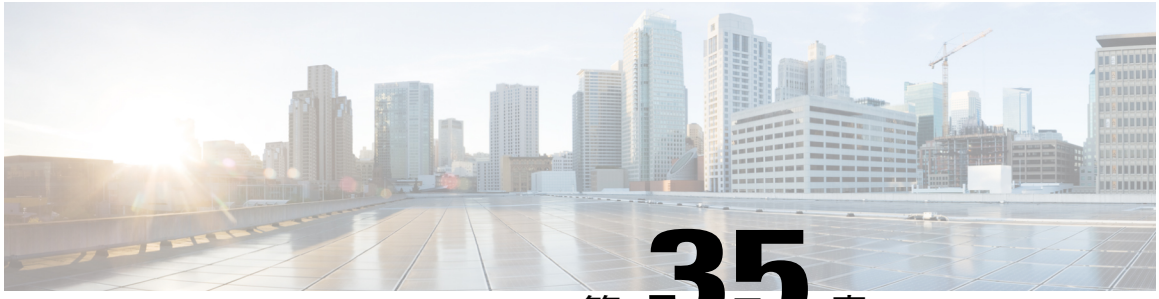
a) [自分の電話のプロビジョニングをエンドユーザに許可（Allow end user to provision their own phones）]チェックボックスをオンにします。

b) [エンド ユーザのプロビジョニングする電話数を制限（Limit Provisioning once End User has this many phones）] フィールドに、ユーザがプロビジョニングできる電話の最大数を入力します。最大値は 20 です。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

セルフプロビジョニングの設定, （619 ページ）



第 35 章

サービス プロファイルの設定

- サービス プロファイルの概要，285 ページ
- サービス プロファイルの設定タスク フロー，286 ページ

サービス プロファイルの概要

サービス プロファイルにより、Unified Communications（UC）サービスの共通設定で構成されるプロファイルを作成できます。サービス プロファイルをエンド ユーザに適用し、サービス プロファイルにある UC サービスの構成時の設定をそのエンド ユーザに割り当てることができます。企業内の異なるユーザ グループごとに異なるサービスを設定でき、その結果、各グループのユーザが、仕事に合わせて設定された適切なサービスを利用できます。

サービス プロファイルは、次の UC サービスの構成時の設定で構成されます。

- [ボイスメール（Voicemail）]
- メールストア（Mailstore）
- [会議（Conferencing）]
- [ディレクトリ（Directory）]
- [IM and Presence]
- [CTI]
- ビデオ会議サービス

エンド ユーザへのサービス プロファイルの適用

エンド ユーザにサービス プロファイルを適用するには、次の方法を使用します。

- LDAP 同期されたユーザ向け：LDAP ディレクトリからエンドユーザをインポートした場合、サービス プロファイルを機能グループ テンプレートに割り当てることができ、その機能グループ テンプレートをエンド ユーザに適用できます。

- アクティブ ローカル ユーザ（非 LDAP ユーザなど）向け：エンド ユーザの設定で、サービス プロファイルを個別のエンド ユーザに割り当てることができます。また、サービス プロファイルを多くのエンドユーザに一度に割り当てるには、一括管理ツールを利用できます。詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』を参照してください。

サービス プロファイルの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	このサービス プロファイルに割り当てる次のユニファイド コミュニケーション（UC）サービスを設定します。 • ボイスメール サービスの追加, （286 ページ） • メールストア サービスの追加, （287 ページ） • 会議サービスの追加, （288 ページ） • ディレクトリ サービスの追加, （289 ページ） • IM and Presence サービスの追加, （290 ページ） • CTI サービスの追加, （291 ページ） • ビデオ会議のスケジューリング サービスの追加, （292 ページ）	サービスプロファイル用に設定する UC サービス設定を実行します。
ステップ 2	サービス プロファイルの設定, （293 ページ）	このサービスプロファイルに適用する UC サービスを示すように、ユーザのサービスプロファイルを設定します。

ボイスメール サービスの追加

システムにボイスメールサービスを追加します。複数のボイスメールサービスを追加してから、サービス プロファイルに追加するサービスを選択できます。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）]>[ユーザ設定（User Settings）]>[UC サービス（UC Service）] 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 [UC サービス タイプ（UC Service Type）] ドロップダウン リスト ボックスから [ボイスメール（Voicemail）] を選択します。

ステップ 4 [製品タイプ（Product Type）] ドロップダウン リスト ボックスから、[Unity] または [Unity Connection] を選択します。

ステップ 5 [名前（Name）] にボイスメール サービスの名前を入力します。

ステップ 6 サービスを区別しやすくするための [説明（Description）] を入力します。

ステップ 7 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、ボイスメール サービスをホストするサーバのホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ 8 [ポート（Port）] フィールドに、ボイスメール サービスに接続するポートを入力します。デフォルト ポートは 443 です。

ステップ 9 [プロトコル（Protocol）] フィールドに、ボイス メッセージをルーティングするために使用するプロトコルを入力します。使用可能なオプションは、[HTTP] と [HTTPS] のみです。

（注） Cisco Unity サーバおよび Cisco Unity Connection サーバのボイスメール転送プロトコルには、[HTTPS] を使用することを推奨します。ネットワーク設定で [HTTPS] がサポートされない場合に限り [HTTP] に変更してください。

ステップ 10 [保存（Save）] をクリックします。

次の作業

メールストア サービスの追加, （287 ページ）

メールストア サービスの追加

システムにメールストア サービスを追加します。Cisco Jabber Clients は、ビジュアル ボイスメールの機能にメールストア サービスを使用します。

（注） Cisco Unity では、Microsoft Exchange サーバでのメッセージ保存用にサブスクライバ メールボックスが作成されます。

通常、Cisco Unity Connection はメールストア サービスを提供し、同じサーバ上でメールストア サービスをホストします。

はじめる前に

ボイスメール サービスの追加, （286 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）] 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 [UC サービスの種類（UC Service Type）] ドロップダウン リスト ボックスから、[メールストア（Mailstore）] を選択します。

ステップ 4 メールストア サービスの名前を [名前（Name）] に入力します。

ステップ 5 メールストア サービスの説明を [説明（Description）] に入力します。

ステップ 6 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、メールストアをホストするサーバの、ホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ 7 [ポート（Port）] フィールドに、メールストア サービスで利用可能なポート番号と一致する 1 ～ 65535 の範囲のポート番号を入力します。メールストアのデフォルトのポート番号は 143 です。

（注） Cisco Unity Connection を使用したセキュア ボイスメッセージングには、ポート番号 7993 を使用してください。

ステップ 8 [プロトコル（Protocol）] フィールドに、ボイスメール メッセージのルーティングに使用するプロトコル、TCP（デフォルト）、TLS、UDP、または SSL を入力します。

（注） Cisco Unity Connection を使用したセキュア メッセージングには、TLS を使用してください。

ステップ 9 [保存（Save）] をクリックします。

次の作業

会議サービスの追加, （288 ページ）

会議サービスの追加

システムに会議サービスを追加します。

はじめる前に

メールストア サービスの追加, （287 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）] 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 [UC サービス タイプ（UC Service Type）] ドロップダウン リスト ボックスから [会議（Conferencing）] を選択します。

ステップ 4 [製品タイプ（Product Type）] ドロップダウン リスト ボックスから、会議に使用する製品を選択します。

- MeetingPlace Classic
- MettingPlace Express
- WebEx

ステップ 5 [名前（Name）] に会議サービスの名前を入力します。

ステップ 6 [説明（Description）] に会議サービスの説明を入力します。

ステップ 7 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、会議サービスをホストするサーバのホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ 8 [ポート（Port）] フィールドに、会議サービスで使用可能なポートと一致するポート値を入力します。推奨される値を次に示します。

- 80（デフォルト設定）：HTTP にはこのポートを使用します。
- 443：HTTPS にはこのポートを使用します。

ステップ 9 [プロトコル（Protocol）] ドロップダウン リスト ボックスから、エンドポイントがこのサービスに連絡するときに使用するプロトコルを選択します。

- TCP（デフォルト設定）
- UDP
- SSL
- TLS

（注） Cisco Unity Connection を使用したセキュア メッセージングの場合は、TLS を使用してください。

ステップ 10 [保存（Save）] をクリックします。

次の作業

ディレクトリ サービスの追加, （289 ページ）

ディレクトリ サービスの追加

ディレクトリ検索で、Cisco Unified Communications Manager に外部の LDAP ディレクトリを参照させる場合は、ディレクトリ サービスをシステムに追加します。

はじめる前に

会議サービスの追加, （288 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）] 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 [UC サービスの種類（UC Service Type）] ドロップダウン リスト ボックスから、[ディレクトリ（Directory）] を選択します。

ステップ 4 [製品のタイプ（Product Type）] フィールドから、次のいずれかを選択します。

- [ディレクトリ（Directory）]：クライアントが UDS を使用し Cisco Unified Communications Manager データベースに接続して、ディレクトリ検索をする場合は、このオプションを選択します。
- [拡張ディレクトリ（Enhanced Directory）]：クライアントが外部の LDAP ディレクトリに接続して、ディレクトリ検索をする場合は、このオプションを選択します。

ステップ 5 ディレクトリ サービスの名前を [名前（Name）] に入力します。

ステップ 6 ディレクトリ サービスの説明を [説明（Description）] に入力します。

ステップ 7 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、クライアントがディレクトリ検索に利用するディレクトリ サービスをホストするサーバの、ホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

（注） 外部の LDAP ディレクトリをディレクトリ検索に使用している場合は、その LDAP ディレクトリのホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ 8 [ポート（Port）] フィールドに、ディレクトリ サービスで利用可能なポート番号と一致するポート番号を入力します。デフォルトのポート値は 389 です。また、ポート 636、3628、3629 は、外部の LDAP ディレクトリに接続できます。

ステップ 9 [プロトコル（Protocol）] フィールドに、ディレクトリ サービスとエンドポイント間の通信のルーティングに使用するプロトコルを入力します。次のオプションを使用できます。

- TCP（デフォルト設定）
- UDP
- TLS

ステップ 10 [保存（Save）] をクリックします。

次の作業

IM and Presence サービスの追加, （290 ページ）

IM and Presence サービスの追加

システムに IM and Presence サービスを追加します。

はじめる前に

ディレクトリ サービスの追加, （289 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）] 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 [UC サービス タイプ（UC Service Type）] ドロップダウンリスト ボックスから、IM and Presence を選択します。

ステップ 4 [製品タイプ（Product Type）] ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。

- Unified CM（IM and Presence）
- WebEx（IM and Presence）

ステップ 5 [名前（Name）] に IM and Presence サービスの名前を入力します。

ステップ 6 [説明（Description）] に IM and Presence サービスの説明を入力します。

ステップ 7 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、IM and Presence サービスをホストするサーバのホスト名、IP アドレス、または DNS SRV を入力します。

ヒント ユーザに適した IM and Presence サービスをクライアントが見つけやすい DNS SRV を推奨します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

CTI サービスの追加, （291 ページ）

CTI サービスの追加

システムに CTI サービスを追加します。

はじめる前に

IM and Presence サービスの追加, （290 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）] 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 [UC サービス タイプ（UC Service Type）] ドロップダウン リスト ボックスから [CTI] を選択します。

ステップ 4 [名前（Name）] に CTI サービスの名前を入力します。

ステップ 5 [説明（Description）] に CTI サービスの説明を入力します。

ステップ 6 [ホスト名/IP アドレス（Hostname/IP Address）] フィールドに、CTI サービスをホストするサーバのホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ 7 [ポート（Port）] フィールドに CTI サービスのポート番号を入力します。デフォルト ポートは 2748 です。

ステップ 8 [保存（Save）] をクリックします。

次の作業

ビデオ会議のスケジューリング サービスの追加, （292 ページ）

ビデオ会議のスケジューリング サービスの追加

TelePresence Management System に、ビデオ会議をスケジューリングするポータルを提供するビデオ会議スケジューリング サービスを追加します。

はじめる前に

CTI サービスの追加, （291 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）] 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 [名前（Name）] にサービスの名前を入力します。

ステップ 4 [説明（Description）] にサービスの説明を入力します。

ステップ 5 [IP アドレス/ホスト名（IP Address/Hostname）] フィールドに、ビデオ会議スケジューリング サービスをホストするサーバのホスト名、IP アドレス、または完全修飾ドメイン名を入力します。

ステップ 6 [ポート（Port）] フィールドに、ビデオ会議スケジューリング サービスで使用可能なポートと一致するポート値を入力します。利用可能なポートは次のとおりです。

- 80（デフォルト）または 8080：これらのポートは HTTP に使用します。

- 443 または 8443：これらのポートは HTTPS に使用します。

ステップ 7 [プロトコル（Protocol）] ドロップダウン リスト ボックスから、ビデオ会議スケジューリング サービスとの通信用に、次のいずれかのプロトコルを選択します。

- HTTP
- HTTPS

ステップ 8 [ポータルの URL（Portal URL）] フィールドに、TelePresence Management System を指定する URL を入力します。

ステップ 9 [保存（Save）] をクリックします。

次の作業

サービス プロファイルの設定, （293 ページ）

サービス プロファイルの設定

ユーザに割り当てられるサービス プロファイルを設定するには、次の手順を実行します。サービス プロファイルには、そのサービス用に設定されている適切なサーバが指定されています。たとえば、サービス プロファイルで、ボイスメール サービスにプライマリ サーバ、セカンダリ サーバおよび第 3 サーバ（該当する場合）を指定します。

はじめる前に

サービス プロファイルを設定する前に Unified Communications（UC）サービスを設定する必要があります。次の UC サービスのいずれかを設定できます。

- ボイスメール サービスの追加, （286 ページ）
- メールストア サービスの追加, （287 ページ）
- 会議サービスの追加, （288 ページ）
- ディレクトリ サービスの追加, （289 ページ）
- IM and Presence サービスの追加, （290 ページ）
- CTI サービスの追加, （291 ページ）
- ビデオ会議のスケジューリング サービスの追加, （292 ページ）

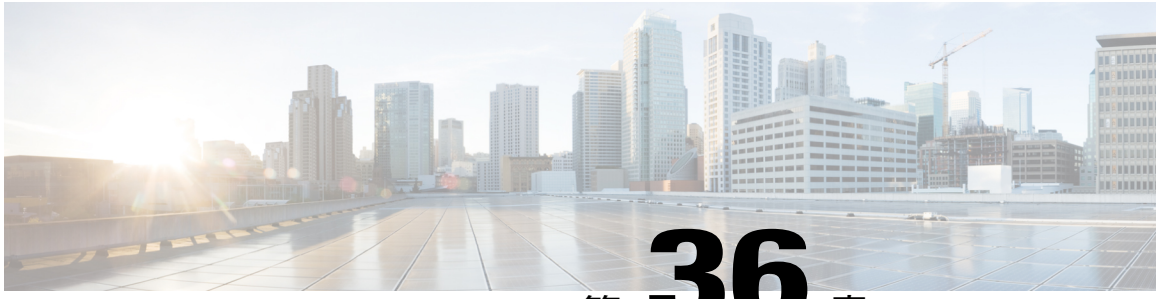
手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービス プロファイル（Service Profile）] 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 [サービス プロファイルの設定（Service Profile Configuration）] ウィンドウで各フィールドに入力します。フィールドの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。



第 36 章

機能グループ テンプレートの設定

- 機能グループ テンプレートの概要，295 ページ
- 機能グループ テンプレートの前提条件，296 ページ
- 機能グループ テンプレートの設定，296 ページ

機能グループ テンプレートの概要

機能グループテンプレートは設定済みの電話と電話回線をエンドユーザに導入するために役立ちます。機能グループテンプレートによって、機能グループテンプレートが割り当てられているすべてのユーザに、共通の電話、電話回線、サービスの設定を割り当てることができます。また、エンドユーザのセルフプロビジョニングを有効にしている場合、ユーザは機能グループ テンプレートを使用して、必要な電話、電話回線、サービスの設定で電話をすばやくプロビジョニングおよび設定できます。

機能グループテンプレート設定には、機能グループテンプレートに割り当てられる次のプロファイルが含まれます。

- ユーザ プロファイル：一連の共通の電話および電話回線の設定が含まれます。ユーザ プロファイルには、共通の電話回線設定を割り当てるユニバーサル回線テンプレートと、共通の電話設定を割り当てるユニバーサル デバイス テンプレートを設定する必要があります。これらのテンプレートは、セルフプロビジョニングするように設定されているユーザが自身の電話を設定する際に役立ちます。
- サービスプロファイル：会議やディレクトリ サービスなどのユニファイドコミュニケーション サービスにおける共通の設定グループが含まれます。

ユーザプロファイルとサービスプロファイルを含むように機能グループテンプレートを設定し、その後、その機能グループテンプレートをユーザに割り当てると、エンドユーザがプロビジョニングする新しい電話にユーザ プロファイルとサービス プロファイルが伝搬されます。

IM and Presence サービスを展開する場合は、機能グループ テンプレートを使用して、インスタント メッセージおよびプレゼンス機能で LDAP 同期ユーザを有効にできます。

機能グループ テンプレートの前提条件

機能グループ テンプレートを設定する前に、エンド ユーザのユーザ プロファイルとサービス プロファイルを設定します。

- ユーザ プロファイルの設定タスク フロー, （282 ページ）
- サービス プロファイルの設定タスク フロー, （286 ページ）

機能グループ テンプレートの設定

機能グループ テンプレートには、共通の回線、デバイス、および機能設定のセットが含まれています。新しいユーザに機能グループ テンプレートを適用すると、その回線、デバイス、および機能設定が、ユーザの電話および電話回線に適用されます。機能グループ テンプレートは、プロビジョニングされたユーザの電話、回線、および機能を非常に迅速に設定できるようにすることで、システムの導入をサポートします。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [機能グループ テンプレート（Feature Group Template）] 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 このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカル クラスタを使用する場合は、[ホーム クラスタ（Home Cluster）] チェック ボックスをオンにします。

ステップ 4 このテンプレートを使用するユーザがインスタント メッセージに IM and Presence サービスを使用できるようにする場合は、[ユーザが Unified CM IM and Presence を使用できるようにする（Enable Users for Unified CM IM and Presence）] チェック ボックスをオンにします。

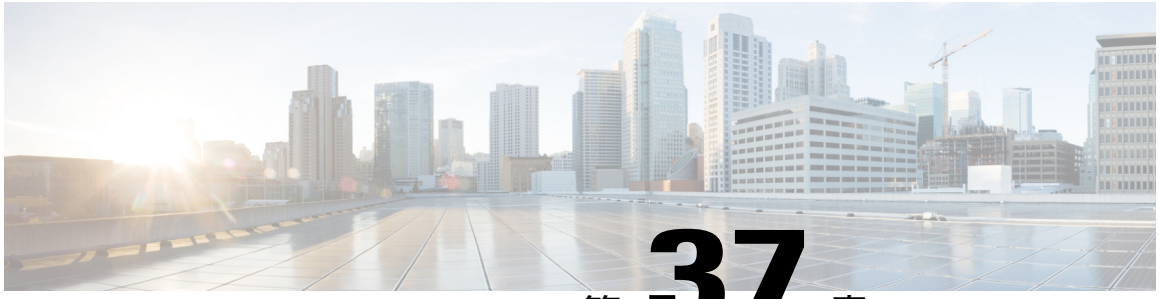
ステップ 5 ドロップダウン メニューから、[サービス プロファイル（Service Profile）] および [ユーザ プロファイル（User Profile）] を選択します。

ステップ 6 [機能グループ テンプレートの設定（Feature Group Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次の作業

機能グループ テンプレートと LDAP ディレクトリ同期を関連付け、テンプレートの設定を同期したエンド ユーザに適用します。



第 37 章

LDAPディレクトリからユーザをインポート

- LDAP 同期の概要，297 ページ
- LDAP 同期の前提条件，299 ページ
- LDAP 同期設定のタスク フロー，300 ページ

LDAP 同期の概要

Lightweight Directory Access Protocol（LDAP）の同期は、システムのエンドユーザのプロビジョニングと設定を支援します。LDAP の同期中、システムは外部 LDAP ディレクトリから Cisco Unified Communications Manager データベースにユーザのリストと関連するユーザ データをインポートします。インポートしている間に、エンドユーザを設定することもできます。また、定期的な同期スケジュールを設定すれば、従業員のデータの変更を漏らさず記録できます。

エンド ユーザのインポート

LDAP 同期を使用して、システムの初期設定時にユーザ一覧を会社の LDAP ディレクトリから Cisco Unified Communications Manager のデータベースにインポートできます。LDAP 同期プロセスは、ユーザの一覧、電話番号や電子メール アドレスなどのユーザ独自のデータをインポートし、[エンドユーザ設定（End User Configuration）] ウィンドウの対応するフィールドに保存します。

LDAP インポートを LDAP ディレクトリからのユーザのサブセットに制限するには、LDAP フィルタを LDAP 同期に設定して適用できます。

インポートしたエンド ユーザの設定

アクセス制御グループ、クレデンシャル ポリシー、機能グループのテンプレートなどの項目を設定済みの場合は、ユーザのインポート中に、インポートされたエンドユーザを設定することもできます。[LDAP ディレクトリ設定（LDAP Directory Configuration）] ウィンドウを使用して、エンドユーザの次の項目を設定できます。Cisco Unified Communications Manager では、同期中に、インポートされたエンドユーザにこれらの設定を割り当てます。たとえば、エンドユーザに次の項目を指定できます。

- エンドユーザをアクセス制御ループに指定する

- デフォルトのクレデンシャル ポリシーを指定する
- ユニバーサル回線のテンプレートをユーザのプライマリ エクステンションに指定する
- ユーザの電話に適用されるユニバーサル デバイス テンプレートを指定する
- プライマリ エクステンションを指定する
- ユーザが自分の電話機のプロビジョニングをできるようにする

エンドユーザに設定を適用するときには、LDAP フィルタを使用して、特定の要件を満たすエンドユーザにのみエンドユーザの設定が適用されることを確認します。同じ条件を満たすその他のエンドユーザ向けに、Cisco Unified Communications Manager で追加の LDAP ディレクトリの設定をセットアップできます。

スケジュールされた更新

Cisco Unified Communications Manager をスケジュールされた間隔で複数の LDAP ディレクトリと同期するように設定できます。これによって確実に、データベースが定期的に更新され、すべてのユーザ データが最新になるようにすることができます。たとえば、同期スケジュールをセットアップし、会社の LDAP ディレクトリの電話番号を更新すると、スケジュールされた次の LDAP 同期が発生したとき、その更新は自動的に Cisco Unified Communications Manager に反映されます。従業員のデータを制御し、更新する単一のリポジトリを作成することにより、同期スケジュールで企業ネットワークを継続的に管理できます。

[エンドユーザ用LDAP認証（LDAP Authentication for End Users）]

LDAP 同期を使用して、システムが Cisco Unified Communications Manager データベースではなく、LDAP ディレクトリに対してエンド ユーザ パスワードを認証するように設定できます。LDAP 認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンドユーザに割り当てることができます。この機能は、PIN またはアプリケーション ユーザ パスワードには適用されません。

Cisco Mobile およびリモート アクセス クライアントとエンドポイントのディレクトリ サーバ ユーザ検索

以前のリリースでは、Cisco Mobile とリモート アクセス クライアント（たとえば、Cisco Jabber）またはエンドポイント（たとえば、Cisco DX 80 電話）を使用しているユーザが企業ファイアウォールの外部でユーザ検索を実行した場合、結果は Cisco Unified Communications Manager に保存されたユーザ アカウントに基づいていました。データベースには、ローカルで設定されたか、または社内ディレクトリから同期されたユーザ アカウントも含まれています。

このリリースでは、Cisco Mobile およびリモート アクセス クライアントとエンドポイントは、企業ファイアウォールの外部で動作している場合でも、社内ディレクトリ サーバを検索できます。この機能を有効にすると、ユーザ データ サービス（UDS）がプロキシとして機能し、Cisco Unified Communications Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

この機能を使用して、次の結果を実現できます。

- 地理的な場所に関係なく、同じユーザ検索結果を提供する：モバイルおよびリモートアクセスクライアントとエンドポイントは、社内ディレクトリを使用してユーザ検索を実行できます。企業ファイアウォールの外部で接続されている場合でも実行可能です。
- Cisco Unified Communications Manager データベースに設定されるユーザ アカウントの数を削減する：モバイルクライアントは、社内ディレクトリ内のユーザを検索できます。以前のリリースでは、ユーザ検索結果はデータベースに設定されているユーザに基づいていました。今回のリリースでは、ユーザ検索のためだけにユーザアカウントをデータベースに設定または同期する必要がなくなりました。管理者は、クラスタによって管理されているユーザアカウントを設定すれば作業が完了します。データベース内のユーザアカウントの合計数が削減すると、データベース全体のパフォーマンスが改善される一方、ソフトウェアアップグレードの時間枠が短縮されます。

この機能を設定するには、[LDAP 検索の設定（LDAP Search Configuration）] ウィンドウで [企業ディレクトリ サーバでのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）] オプションを有効にし、LDAP ディレクトリ サーバの詳細を設定する必要があります。詳細については、エンタープライズ ディレクトリ ユーザ検索の設定, （305 ページ）の手順を参照してください。

LDAP 同期の前提条件

前提条件のタスク

LDAP ディレクトリからエンドユーザをインポートする前に、次のタスクを実行します。

- ユーザ アクセス設定のタスク フロー, （260 ページ）
- クレデンシャル ポリシーの設定タスク フロー, （278 ページ）
- 機能グループ テンプレートの設定, （296 ページ）

自分のシステムにデータを同期するユーザについて、アクティブ ディレクトリ サーバ上の電子メール ID フィールドが確実に単一エントリまたは空白になっているようにします。

サポートされる LDAP ディレクトリ

Cisco Unified Communications Manager では、次の LDAP ディレクトリとの同期をサポートしています。

- Microsoft Active Directory 2003 R1/R2（32 ビット）
- Microsoft Active Directory 2008 R1（32 ビット）/R2 （64 ビット）
- Microsoft Active Directory アプリケーション モード 2003 R1/R2（32 ビット）
- Microsoft Active Directory 2012
- Microsoft Lightweight Directory Services 2008 R1 （32 ビット）/R2（64 ビット）

- Microsoft Lightweight Directory Services 2012
- Sun ONE Directory Server 7.0
- LDAP 2.3.39 を開きます
- LDAP 2.4 を開きます
- Oracle Directory Server Enterprise Edition 11gR1
- 他の LDAPv3 対応ディレクトリ

LDAP 同期設定のタスク フロー

企業 LDAP ディレクトリと Cisco Unified Communications Manager データベースを同期するには、次のタスクを実行します。LDAP 同期により、外部 LDAP ディレクトリからユーザ リストをプルし、Cisco Unified Communications Manager のデータベースにインポートできます。このプロセスは、管理者が初めてセットアップする時にエンドユーザをプロビジョニングするのに役立ちます。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco DirSync サービスの有効化, （301 ページ）	Cisco Unified Serviceability にログインし、Cisco DirSync サービスを有効にします。
ステップ 2	LDAP ディレクトリの同期化の有効化, （302 ページ）	シスコの LDAP ディレクトリ同期を Cisco Unified Communications Manager を有効化します。
ステップ 3	LDAP フィルタの作成, （302 ページ）	これはオプションです。Cisco Unified Communications Manager に社内 LDAP ディレクトリからユーザのサブセットだけを同期するには、LDAP フィルタを作成します。たとえば、特定のアクセス制御グループに属するユーザ、または特定のユーザ プロファイルを使用するユーザだけをインポートするフィルタを作成できます。
ステップ 4	LDAP ディレクトリの同期の設定, （303 ページ）	アクセス コントロール グループ、機能グループのテンプレートとプライマリ エクステンションのフィールド設定、LDAP サーバの場所、同期スケジュール、および割り当てなどの LDAP ディレクトリ同期を設定します。
ステップ 5	エンタープライズ ディレクトリ ユーザ検索の設定, （305 ページ）	これはオプションです。エンタープライズ ディレクトリ サーバ ユーザを検索するシステムを設定します。システムの電話機とクライアントをデータベースの代わりにエンタープライズ ディレクトリ サーバに対してユーザの検索を実行するように設定するには、次の手順に従います。

	コマンドまたはアクション	目的
ステップ 6	LDAP 認証の設定, （307 ページ）	これはオプションです。エンドユーザのパスワード認証に LDAP ディレクトリを使用するには、LDAP 認証を設定します。
ステップ 7	LDAP アグリーメント サービス パラメータのカスタマイズ, （308 ページ）	これはオプションです。LDAP 同期サービス パラメータを設定します。ほとんどの導入には、デフォルト値で十分です。ただし、次の値を再設定できます。 • LDAP 同期アグリーメントの最大数 • フェールオーバーの LDAP のホスト名の最大数 • ホストの障害または hostlist の失敗の遅延タイマー • 接続タイムアウト • LDAP 同期の遅延
ステップ 8	LDAP同期済みユーザのローカル ユーザへの変換, （310 ページ）	これはオプションです。LDAP 属性と同期されるエンドユーザ設定を更新する必要があり、LDAP ディレクトリのフィールドを使用しないのであれば、LDAPユーザをローカル ユーザに変換します。

Cisco DirSync サービスの有効化

Cisco DirSync サービスをアクティブにするには、Cisco Unified Serviceability で次の手順を実行します。社内 LDAP ディレクトリでエンドユーザの設定を同期するには、このサービスをアクティブにする必要があります。

手順

ステップ 1 Cisco Unified Serviceability から、[ツール（Tools）] > [サービスの有効化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リスト ボックスからパブリッシャ ノードを選択します。

ステップ 3 [ディレクトリ サービス（Directory Services）] の下の [Cisco DirSync] オプション ボタンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

次の作業

LDAP ディレクトリの同期化の有効化, （302 ページ）

LDAP ディレクトリの同期化の有効化

エンドユーザの設定を社内 LDAP ディレクトリから同期するように Cisco Unified Communications Manager を設定するには、次の手順を実行します。

はじめる前に

Cisco DirSync サービスの有効化, （301 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [LDAP] > [LDAPシステム（LDAP System）] を選択します。

ステップ 2 Cisco Unified Communications Manager で、LDAP ディレクトリからユーザをインポートするには、[LDAPサーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] チェックボックスをオンにします。

ステップ 3 [LDAPサーバ タイプ（LDAP Server Type）] ドロップダウン リスト ボックスから、会社が使用する LDAP ディレクトリ サーバのタイプを選択します。

ステップ 4 [ユーザ ID の LDAP 属性（LDAP Attribute for User ID）] ドロップダウン リスト ボックスから、[エンドユーザ設定（End User Configuration）] の [ユーザ ID（User ID）] フィールドの値について、Cisco Unified Communications Manager を同期させる社内 LDAP ディレクトリの属性を選択します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

次のいずれかの手順を実行します。

- LDAP フィルタの作成, （302 ページ） LDAP 同期をユーザのサブセットに制限する場合
- LDAP ディレクトリの同期の設定, （303 ページ） LDAP ディレクトリの設定

LDAP フィルタの作成

LDAP フィルタを作成して LDAP 同期を LDAP ディレクトリのユーザのサブネットに制限する場合は、このオプションの手順を実行します。LDAP フィルタを LDAP ディレクトリに適用する場合、Cisco Unified Communications Manager は、フィルタに一致するユーザのみを LDAP ディレクトリからインポートします。

LDAP フィルタを設定する場合は、RFC4515 に指定されている LDAP 検索フィルタ標準に準拠する必要があります。

はじめる前に

LDAP ディレクトリの同期化の有効化, （302 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [LDAP(LDAP)] > [LDAP フィルタ（LDAP Filter）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックして、新しい LDAP フィルタを作成します。

ステップ 3 [フィルタ名（Filter Name）] テキスト ボックスに、LDAP フィルタの名前を入力します。

ステップ 4 [フィルタ（Filter）] テキスト ボックスに、フィルタを入力します。フィルタは、UTF-8 で最大 1024 文字まで入力できます。また、丸カッコ（ ()）で囲みます。

ステップ 5 [保存（Save）] をクリックします。

次の作業

LDAP ディレクトリの同期の設定, （303 ページ） に移動して、LDAP フィルタを LDAP ディレクトリに適用します。

LDAP ディレクトリの同期の設定

LDAP ディレクトリと同期するよう Cisco Unified Communications Manager を設定するには、次の手順を使用します。LDAP ディレクトリの同期により、エンドユーザのデータを外部の LDAP ディレクトリから Cisco Unified Communications Manager データベースにインポートして、[エンド ユーザの設定（End User Configuration）] ウィンドウに表示できます。定期的に LDAP ディレクトリの更新が Cisco Unified Communications Manager に伝達されるよう、同期スケジュールをセットアップできます。

また、アクセス コントロール グループ、機能グループ テンプレート、ユニバーサル回線やユニバーサル デバイス テンプレートをすでに計画済みの場合は、アクセス コントロール グループ、プライマリ内線番号、セルフプロビジョニング機能により、インポートしたエンド ユーザを即座に設定できます。

ヒント アクセス コントロール グループまたは機能グループ テンプレートを割り当てる場合は、LDAP フィルタを使用して、インポートを同じ設定要件のユーザ グループに限定できます。

はじめる前に

- LDAP ディレクトリの同期化の有効化, （302 ページ）
- LDAP フィルタの作成, （302 ページ） LDAP の同期をユーザのサブセットに限定する場合。

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [LDAP（LADP）] > [LDAP ディレクトリ（LDAP Directory）] を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [検索（Find）] をクリックし、既存の LDAP ディレクトリを選択します。
- [新規追加（Add New）] をクリックして、新しい LDAP ディレクトリを作成します。

ステップ 3 [LDAP ディレクトリの設定（LDAP Directory Configuration）] ウィンドウの各フィールドに入力します。フィールドとその説明を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 4 [LDAP 構成名（LDAP Configuration Name）] テキスト ボックスで、LDAP ディレクトリの一意の名前を指定します。

ステップ 5 [LDAP マネージャ識別名（LDAP Manager Distinguished Name）] フィールドに、LDAP ディレクトリ サーバにアクセスできるユーザ ID を入力します。

ステップ 6 パスワードの詳細を入力し、確認します。

ステップ 7 これはオプションです。インポートを特定のプロファイルに適合するユーザのサブセットにのみ限定する場合は、[LDAP カスタム フィルタ（LDAP Custom Filter）] ドロップダウン リスト ボックスから、LDAP フィルタを選択します。

ステップ 8 [LDAP ディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] フィールドに、外部 LDAP ディレクトリとデータ同期を行うために Cisco Unified Communications Manager が使用するスケジュールを作成します。

ステップ 9 [同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized）] セクションを記入します。各エンドユーザのフィールドで、それぞれ LDAP 属性を選択します。同期プロセスは LDAP 属性の値を Cisco Unified Communications Manager のエンドユーザ フィールドに割り当てます。

ステップ 10 インポートしたエンド ユーザを、インポートしたすべてのエンド ユーザに共通するアクセス コントロール グループに割り当てるには、次の手順を実行します。

a) [アクセス コントロール グループに追加（Add to Access Control Group）] をクリックします。
b) ポップアップ ウィンドウで、インポートしたユーザに割り当てるアクセスコントロール グループごとに、対応するチェックボックスをオンにします。
c) [選択項目の追加（Add Selected）] をクリックします。

ステップ 11 機能グループ テンプレートを割り当てる場合は、[機能グループ テンプレート（Feature Group Template）] ドロップダウン リスト ボックスからテンプレートを選択します。
機能グループテンプレートに関連付けられているユーザ プロファイル、サービス プロファイル、ユニバーサル回線やユニバーサル デバイス テンプレート、およびセルフプロビジョニング設定は、同期されたエンド ユーザに関連付けられます。

（注） ユーザが存在しない初回のみ、エンド ユーザは割り当てられた [機能グループ テンプレート（Feature Group Template）] と同期されます。既存の [機能グループ テンプレート（Feature Group Template）] が変更され、関連付けられた LDAP の完全同期が実行される場合、変更点は更新されません。

ステップ 12 インポートされた電話番号にマスクを適用して、プライマリ内線番号を割り当てるには、次の手順を実行します。

a) [同期された電話番号にマスクを適用して、挿入されたユーザの新しい回線を作成（Apply Mask to synced telephone numbers to create a new line for inserted users）] チェック ボックスをオンにします。

b) [マスク（Mask）] を入力します。たとえば、インポートされた電話番号が 8889945 である場合、11XX のマスクは、1145 のプライマリ内線番号を作成します。

ステップ 13 電話番号のプールからプライマリ内線番号を割り当てる場合は、次の手順を実行します。

a) [同期された LDAP 電話番号に基づいて作成されなかった場合、プール リストから新しい回線を割り当て（Assign new line from the pool list if one was not created based on a synced LDAP telephone number）] チェック ボックスをオンにします。

b) [DN プールの開始（DN Pool Start）] テキスト ボックスと [DN プールの終了（DN Pool End）] テキスト ボックスに、プライマリ内線番号を選択する電話番号の範囲を入力します。

ステップ 14 [LDAP サーバ情報（LDAP Server Information）] エリアで、LDAP サーバのホスト名または IP アドレスを入力します。

ステップ 15 SSL を使用して LDAP サーバへのセキュアな接続を作成する場合は、[SSL を使用（Use SSL）] チェック ボックスをオンにします。

ステップ 16 [保存（Save）] をクリックします。

次の作業

LDAP 認証の設定, （307 ページ）

エンタープライズ ディレクトリ ユーザ検索の設定

データベースではなくエンタープライズディレクトリ サーバに対してユーザ検索を実行するように、システムの電話機とクライアントを設定するには、次の手順を使用します。

はじめる前に

- LDAP ユーザ検索に選択するプライマリ、セカンダリ、および第 3 サーバが Cisco Unified Communications Manager のサブスクライバ ノードに到達可能なネットワークにあることを確認します。
- [システム（System）] > [LDAP] > [LDAPシステム（LDAP System）] を選択し、[LDAPシステムの設定（LDAP System Configuration）] ウィンドウの [LDAP サーバタイプ（LDAP Server Type）] ドロップダウン リスト ボックスから、LDAP サーバのタイプを設定します。

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [LDAP] > [LDAP 検索（LDAP Search）] を選択します。

ステップ 2 エンタープライズLDAPディレクトリ サーバを使用してユーザ検索を実行するには、[エンタープライズ ディレクトリ サーバのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）] チェックボックスをオンにします。
このウィンドウのフィールドはすべて有効です。

ステップ 3 [LDAP 検索の設定（LDAP Search Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

ディレクトリ サーバの UDS 検索用の LDAP 属性

次の表に、[エンタープライズディレクトリ サーバに対するユーザ検索を有効化（Enable user search to Enterprise Directory Server）] オプションが有効になっている場合に、UDS ユーザ検索要求で使用される LDAP 属性の一覧を示します。このようなタイプのディレクトリ要求の場合、UDS はプロキシとして機能して、社内ディレクトリ サーバに検索要求をリレーします。

（注） UDS ユーザの応答タグは、いずれかの LDAP 属性にマッピングされることがあります。属性のマッピングは、[LDAP サーバ タイプ（LDAP Server Type）] ドロップダウン リストから選択するオプションによって決まります。このドロップダウンリストには、[システム（System）] > [LDAP] > [LDAP システムの設定（LDAP System Configuration）] ウィンドウからアクセスします。

UDS ユーザの応答タグ	LDAP 属性
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName

UDS ユーザの応答タグ	LDAP 属性
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	メール アドレス
directoryUri	• msRTCSIP-primaryuseraddress • メール アドレス
部署	• 部署 • departmentNumber
manager	manager
タイトル	タイトル
ポケットベル	ポケットベル

LDAP 認証の設定

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンド ユーザのパスワードが認証されるようにするには、この手順を実行します。LDAP 認証により、システム管理者は会社のすべてのアプリケーションに対してエンド ユーザの 1 つのパスワードを割り当てることができます。この設定は、エンド ユーザのパスワードにのみ適用され、エンド ユーザの PIN またはアプリケーション ユーザのパスワードには適用されません。

はじめる前に

LDAP ディレクトリの同期の設定, （303 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [LDAP] > [LDAP 認証（LDAP Authentication）] を選択します。

ステップ 2 [エンドユーザ用 LDAP 認証の使用（Use LDAP Authentication for End Users）] チェックボックスをオンにして、ユーザ認証に LDAP ディレクトリを使用します。

ステップ 3 [LDAP マネージャ識別名（LDAP Manager Distinguished Name）] フィールドに、LDAP ディレクトリにアクセス権がある LDAP マネージャのユーザ ID を入力します。

ステップ 4 [パスワード（Password）] フィールドに、LDAP マネージャのパスワードを入力します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

LDAP アグリーメント サービス パラメータのカスタマイズ, （308 ページ）

LDAP アグリーメント サービス パラメータのカスタマイズ

LDAP アグリーメントのシステム レベル設定をカスタマイズするサービス パラメータを設定するには、次の手順を実行します。これらのサービス パラメータを設定しない場合、Cisco Unified Communications Manager により、LDAP ディレクトリ統合のデフォルト設定が適用されます。

サービス パラメータを使用して次の設定をカスタマイズできます。

- LDAP アグリーメントの最大数
- ホストの最大数
- ホストまたはホストリスト失敗時の再試行間隔
- 接続タイムアウト
- LDAP 同期の開始間隔

.

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [サービス パラメータ（Service Parameters）] の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リスト ボックスからパブリッシャ ノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リスト ボックスから、[Cisco DirSync] を選択します。

ステップ 4 Cisco DirSync サービス パラメータの値を設定します。サービス パラメータの説明については、「関連項目」を参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

LDAP ディレクトリ サービスのパラメータ, （309 ページ）

LDAP ディレクトリ サービスのパラメータ

サービス パラメータ	説明
Maximum Number of Agreements	自分で設定できるLDAPディレクトリの最大数。デフォルト設定は 20 です。
Maximum Number of Hosts	フェールオーバ用に設定できるLDAPホスト名の最大数。デフォルト値は 3 です。
Retry Delay on Host Failure (secs)	ホストで障害が発生した後、Cisco Unified Communications Manager が最初のLDAPサーバ（ホスト名）への接続を再試行する前の遅延秒数です。デフォルト値は 5 です。
Retry Delay on HostList Failure (mins)	ホスト リストで障害が発生した後、Cisco Unified Communications Manager が設定された各 LDAP サーバ（ホスト名）への接続を再試行する前の遅延分数です。デフォルトは 10 です。
LDAP Connection Timeout (secs)	Cisco Unified Communications Manager が LDAP 接続を確立できる秒数です。指定した時間内に接続を確立できない場合、LDAP サービス プロバイダーは接続試行を中止します。デフォルトは5です。
Delayed Sync Start Time (mins)	Cisco DirSync サービスの起動後に、Cisco Unified Communications Manager がディレクトリ同期プロセスを開始するまでの遅延分数です。デフォルトは 5 です。

LDAP同期済みユーザのローカル ユーザへの変換

LDAP ディレクトリと Cisco Unified Communications Manager を同期すると、LDAP に同期されたエンド ユーザについては、ローカル ユーザに変換しないかぎり、[エンド ユーザの設定（End User Configuration）] ウィンドウ内のフィールドは編集できません。

[エンド ユーザの設定（End User Configuration）] ウィンドウで LDAP 同期ユーザのフィールドを編集するには、そのユーザをローカル ユーザに変換します。ただし、この変換を行うと、Cisco Unified Communications Manager を LDAP ディレクトリと同期したときにエンド ユーザが更新されなくなります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[エンド ユーザ（End Users）] > [エンド ユーザ管理（End User Management）] を選択します。

ステップ 2 [検索（Find）] をクリックして、エンド ユーザを選択します。

ステップ 3 [ローカル ユーザへの変換（Convert to Local User）] ボタンをクリックします。

ステップ 4 [エンド ユーザ設定（End User Configuration）] ウィンドウでフィールドを更新します。

ステップ 5 [保存（Save）] をクリックします。

アクセス コントロール グループへの LDAP 同期ユーザの割り当て

LDAP と同期するユーザをアクセス コントロール グループに割り当てるには、次の手順を実行します。

はじめる前に

エンドユーザと外部 LDAP ディレクトリが同期されるように Cisco Unified Communications Manager を設定する必要があります。

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [LDAP（LADP）] > [LDAP ディレクトリ（LDAP Directory）] を選択します。

ステップ 2 [検索（Find）] をクリックし、設定した LDAP ディレクトリを選択します。

ステップ 3 [アクセス コントロール グループに追加（Add to Access Control Group）] ボタンをクリックします。

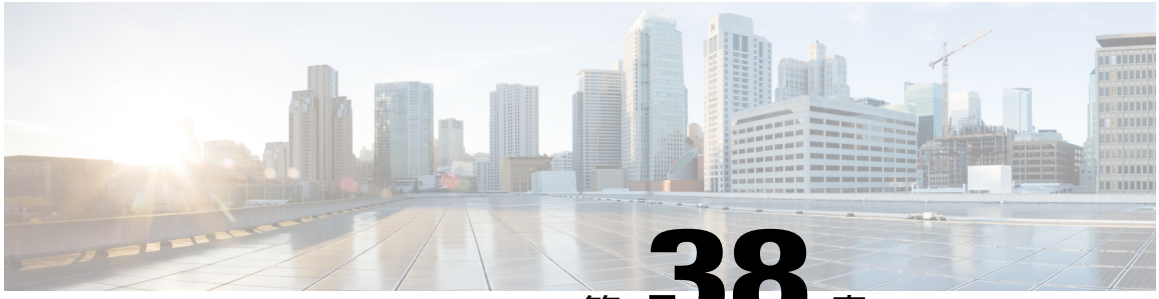
ステップ 4 この LDAP ディレクトリのエンド ユーザに適用するアクセス コントロール グループを選択します。

ステップ 5 [選択項目の追加（Add Selected）] をクリックします。

ステップ 6 [Save] をクリックします。

ステップ 7 [完全同期を実施（Perform Full Sync）] をクリックします。
Cisco Unified Communications Manager が外部 LDAP ディレクトリと同期し、同期したユーザが正しいアクセス コントロール グループに挿入されます。

（注） 同期したユーザは、アクセス コントロール グループを初めて追加した時にのみ、選択したアクセス グループに挿入されます。完全同期の実行後に LDAP に追加するグループは、同期したユーザに適用されません。



第 38 章

手動によるエンドユーザのプロビジョニング

- エンド ユーザの手動プロビジョニングの概要，313 ページ
- エンドユーザの手動プロビジョニングの前提条件，313 ページ
- 一括管理を使用したエンド ユーザのインポート，314 ページ
- 手動エンドユーザ設定のタスク フロー，314 ページ

エンド ユーザの手動プロビジョニングの概要

LDAP ディレクトリからエンドユーザをインポートしない場合は、次のいずれかの方法で、Cisco Unified Communications Manager データベースにエンド ユーザを追加できます。

- 一括管理ツールを使用したインポート
- 新しいユーザの手動での追加

エンドユーザの手動プロビジョニングの前提条件

エンドユーザをインポートする前に、エンドユーザの権限、アクセス制御グループ、クレデンシャル ポリシーを計画して設定します。

- ユーザ アクセス設定のタスク フロー，（260 ページ）
- クレデンシャル ポリシーの設定タスク フロー，（278 ページ）

一括管理を使用したエンド ユーザのインポート

一括管理ツールを使用して、多数のエンド ユーザ、電話、およびポートのインポートや更新を含め、Cisco Unified Communications Manager データベースに対する、大量のトランザクションを単一のプロセスで実行できます。一括管理ツールでは、エンド ユーザ リストおよびエンド ユーザ設定を CSV ファイルからデータベースにインポートできます。

一括管理ツールを使用してエンドユーザをインポートする方法の詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』を参照してください。

手動エンドユーザ設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	新規エンド ユーザの追加, （315 ページ）	データベースに新しいエンドユーザを手動で追加します。
ステップ 2	アクセス コントロール グループへのエンドユーザの割り当て, （315 ページ）	必要な権限を備えたアクセス コントロール グループをプロビジョニングするローカルエンドユーザを割り当てます。ローカルユーザには、手動でプロビジョニングされたエンドユーザと、一括管理ツールを使用してインポートするエンドユーザが含まれています。ローカル ユーザには、エンドユーザ設定で「アクティブ ローカル ユーザ」のユーザ ステータスがあります。
ステップ 3	エンドユーザへのクレデンシャル ポリシーの適用, （316 ページ）	これはオプションです。デフォルトのクレデンシャル ポリシーが、このエンドユーザに適用できるかどうかを確認します。適用できなければ、エンドユーザ PIN またはパスワードにクレデンシャル ポリシーを適用します。
ステップ 4	ローカルエンドユーザへの機能グループテンプレートの割り当て, （316 ページ）	エンドユーザに機能グループテンプレートを割り当てます。機能グループテンプレートを割り当てると、システムはエンドユーザにその機能グループテンプレートに関連付けられているユーザ プロファイル、サービス プロファイル、ユニバーサル回線とデバイステンプレート、セルフプロビジョニング設定を割り当てます。

新規エンド ユーザの追加

Cisco Unified Communications Manager のデータベースに新しいエンドユーザを手動で追加するには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザの管理（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 [エンド ユーザ設定（End User Configuration）] ウィンドウのフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

アクセス コントロール グループへのエンド ユーザの割り当て, （315 ページ）

アクセス コントロール グループへのエンド ユーザの割り当て

アクセス コントロール グループにユーザを割り当てるには、次の手順を使用します。LDAP 同期中にアクセス コントロール グループに割り当てた LDAP 同期ユーザに、次の手順を使用して追加のアクセス コントロール グループを割り当てることができます。この手順は、LDAP 同期設定に共通のアクセスコントロールグループがあっても、一部のユーザに権限に応じた追加のアクセス コントロール グループを割り当てる必要がある場合に便利です。

はじめる前に

新規エンド ユーザの追加, （315 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[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。

ステップ 2 [検索（Find）] をクリックし、アクセス コントロール グループを選択します。

ステップ 3 [グループにエンド ユーザを追加（Add End Users to Group）] をクリックします。

ステップ 4 [ユーザの検索と一覧表示（Find and List Users）] ポップアップで、グループに追加するエンドユーザを選択します。

ステップ 5 [選択項目の追加（Add Selected）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

ユーザ アクセスの設定, （257 ページ）

エンドユーザへのクレデンシャル ポリシーの適用

設定されたクレデンシャルポリシーを特定のエンドユーザパスワードまたはエンドユーザの暗証番号に適用します。デフォルトのクレデンシャル ポリシーから更新を行う必要がある場合に、この操作が必要になることがあります。

（注） また、アプリケーション ユーザ パスワードにクレデンシャル ポリシーを適用することもできます。詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

はじめる前に

クレデンシャル ポリシーの設定タスク フロー, （278 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 2 [検索（Find）] をクリックしてエンド ユーザを選択します。

ステップ 3 クレデンシャル ポリシーを適用するクレデンシャルに応じて、パスワードまたは暗証番号に対応する [クレデンシャルの編集（Edit Credential）] ボタンをクリックします。

ステップ 4 [認証ルール（Authentication Rule）] ドロップダウン リスト ボックスから、適用するクレデンシャル ポリシーを選択します。

ステップ 5 [クレデンシャルの設定（Credential Configuration）] ウィンドウのその他のフィールドに入力します。フィールドとその設定に関するヘルプは、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

クレデンシャル ポリシーの設定, （277 ページ）

ローカル エンドユーザへの機能グループ テンプレートの割り当て

ローカル エンドユーザに機能グループ テンプレートを割り当てます。ローカル エンドユーザとは、データベースに手動で追加された、または一括管理ツールを使用してインポートされたエンドユーザです。ローカル エンドユーザは外部 LDAP ディレクトリと同期されません。

はじめる前に

機能グループ テンプレートの設定, （296 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユーザ/電話のクイック追加（Quick User/Phone Add）] を選択します。

ステップ 2 [検索（Find）] をクリックしてエンド ユーザを選択します。

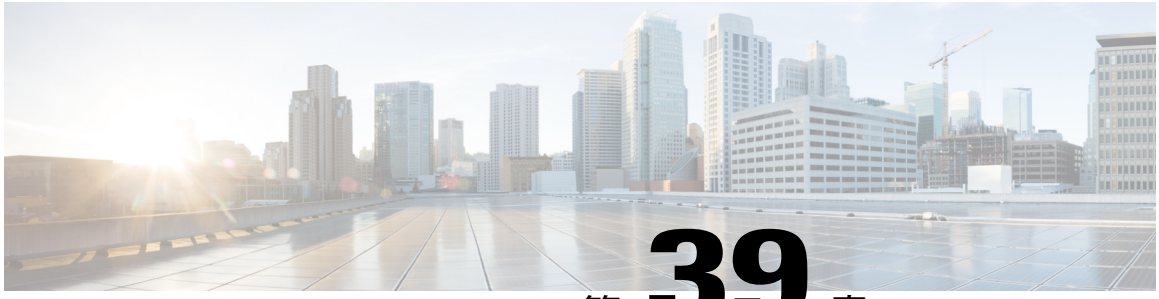
ステップ 3 [機能グループ テンプレート（Feature Group Template）] ドロップダウン リスト ボックスから、このエンドユーザに設定した機能グループのテンプレートを選択します。

ステップ 4 [保存（Save）] をクリックします。

第 VI 部

エンドポイント デバイスの設定

- エンドポイント デバイスの概要，321 ページ
- アナログ電話アダプタの設定，323 ページ
- ソフトウェアベースのエンドポイントの設定，363 ページ
- Cisco IP Phone の設定，377 ページ
- Cisco Unified IP Phone の診断とレポートの設定，407 ページ
- サードパーティ製 SIP 電話の設定，423 ページ
- サービス プロファイルとテンプレート，431 ページ
- ユーザとエンドポイントの関連付け，447 ページ



第 39 章

エンドポイント デバイスの概要

- エンドポイント デバイス設定について，321 ページ
- エンドポイント デバイス設定，321 ページ

エンドポイント デバイス設定について

このパートの章では、エンドポイント デバイスの設定方法とエンドポイントにユーザを関連付ける方法について説明します。

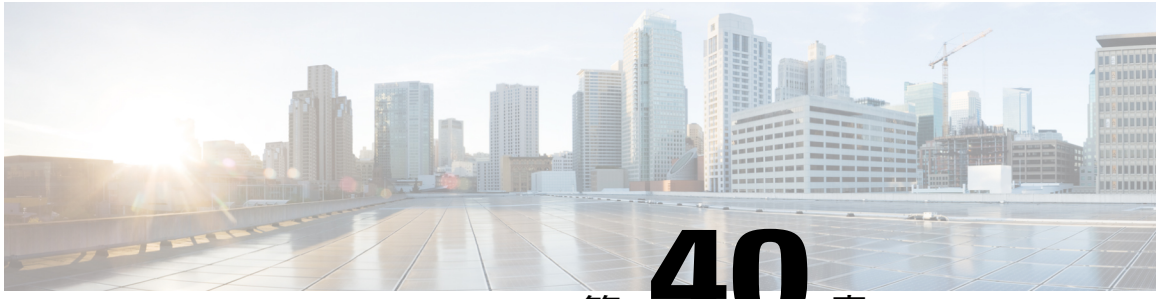
エンドポイント デバイス設定

次のタスク フローを実行すると、システムのエンド ユーザを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	アナログ電話アダプタの設定，（324 ページ）	アナログ電話と IP ベースのテレフォニー ネットワークの間のインターフェイスとして機能するアナログ電話アダプタを設定します。
ステップ 2	ソフトウェアベースのエンドポイントの設定，（363 ページ）	CTI ポート、H.323 クライアント、Cisco IP Communicator などソフトウェアベースのエンドポイントを設定します。
ステップ 3	Cisco IP Phone の設定タスク フロー，（378 ページ）	ネットワーク上で機能する Cisco IP Phones を設定します。

	コマンドまたはアクション	目的
ステップ 4	診断およびレポート設定タスク フロー, （410 ページ）	コール診断および品質レポート ツール（QRT）を使用して、Cisco IP Phones のコール品質を確保します。
ステップ 5	サードパーティ製 SIP エンドポイント設定のタスク フロー, （424 ページ）	サードパーティの SIP エンドポイントを設定します。
ステップ 6	デバイスプロファイルとテンプレートの設定タスク フロー, （432 ページ）	特定のデバイスと関連付けるサービス、機能、電話番号を定義するプロファイルおよびテンプレートを設定します。
ステップ 7	ユーザおよびデバイス設定のタスク フロー, （447 ページ）	デバイスをエンドユーザおよびアプリケーション ユーザと関連付けます。



第 40 章

アナログ電話アダプタの設定

- アナログ電話アダプタの概要，323 ページ
- アナログ電話アダプタの設定，324 ページ

アナログ電話アダプタの概要

Cisco アナログ電話アダプタ（ATA）は、通常のアナログ電話と IP ベースのテレフォニー ネットワークとのインターフェイスとなるアナログ電話アダプタとして機能します。Cisco ATA は通常のアナログ電話をインターネット電話に変換します。各アダプタは 2 個の音声ポートをサポートし、それぞれに固有の電話番号を割り当てることができます。

他の IP デバイスと同様に、Cisco ATA は TFTP サーバから自身の設定ファイルと Cisco Unified Communications Managers のリストを受信します。TFTP サーバに設定ファイルがない場合、Cisco ATA は TFTP サーバ名または IP アドレスとポート番号をプライマリ Cisco Unified Communications Manager の名前または IP アドレスとポート番号として使用します。

Cisco ATA：

- 1 個の 10 BaseT RJ-45 ポートと 2 個の RJ-11 FXS 標準アナログ電話ポートを内蔵
- G.711 A-law、G.711 μ-law、および G.723 と G.729a 音声コーデックをサポート
- Skinny Client Control Protocol（SCCP）を使用
- 音声を IP データ パケットに変換
- リダイヤル、短縮ダイヤル、コール転送、コール ウェイティング、コール保留、転送、電話会議、ボイス メッセージング、メッセージ待機インジケータ、オフフック呼び出し、発信者 ID、呼び出し先 ID、およびコール ウェイティング発信者 ID をサポート

アナログ電話アダプタの設定

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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。

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）] ドロップダウン リストから、使用しているアナログ電話アダプタモデルを選択して、[次へ（Next）] 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）] ウィンドウで各フィールドを設定します。
フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

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）] をクリックして、電話に変更を適用し、同期します。

関連トピック

アナログ電話アダプタ 186 設定フィールド, （324 ページ）
アナログ電話アダプタ 187 設定フィールド, （332 ページ）
アナログ電話アダプタ 190 設定フィールド, （347 ページ）

アナログ電話アダプタ 186 設定フィールド

表 *21*：アナログ電話アダプタ *186* 設定フィールド

フィールド	説明
MAC アドレス（MAC Address）	ATA 186 を特定する Media Access Control（MAC）アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。 次のいずれかの方法で、ATA 186 の MAC アドレスを判別できます。 • ATA 186 の背面にある MAC ラベルを確認します。 • ATA 186 の Web ページを表示し、[デバイス情報（Device Information）] ハイパーリンクをクリックします。

フィールド	説明
説明	ATA 186 の説明テキストを入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	ATA 186 を割り当てるデバイス プールを選択します。デバイス プールでは、複数の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 テンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
共通デバイス設定（Common Device Configuration）	ATA 186 を割り当てる共通デバイス設定を選択します。 共通デバイス設定を表示するには、[詳細表示（View Details）] リンクをクリックします。
[電話ボタンテンプレート（Phone Button Template）]	適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
共通の電話プロファイル（Common Phone Profile）	ドロップダウン リストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [なし（None）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
参照先	ドロップダウン リストから、デバイス プール内の電話とゲートウェイに関連付けられている場所を選択します。

フィールド	説明
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループは、帯域幅不足のためにブロックされるコールをルーティングするために使用するプレフィックス番号を提供します。Cisco Unified CM は、デバイス プールまたは回線と関連付けられている AAR グループを使用します。
ユーザ ロケール（User Locale）	ドロップダウン リストから、ATA 186 と関連付けられているユーザ ロケールを選択します。そのユーザ ロケールは、言語とフォントを含んだ、ユーザをサポートする一連の詳細情報を識別します。 ユーザ ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザ ロケールを使用します。
ネットワーク ロケール（Network Locale）	ドロップダウン リストから、ATA 186 と関連付けられているネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンとパターンの定義が含まれています。 ネットワーク ロケールを指定しない場合、Cisco Unified CM はデバイス プールと関連付けられているネットワーク ロケールを使用します。
[デバイスモビリティ モード（Device Mobility Mode）]	ドロップダウン リストから、このデバイスのデバイス モビリティ機能をオンまたはオフにします。デフォルトのデバイス モビリティ モードを使用する場合は、[デフォルト（Default）] を選択します。デフォルトの設定では、デバイスの [デバイス モビリティ モード（Device Mobility Mode）] サービス パラメータの値が使用されます。
[オーナーのユーザID（Owner User ID）]	オーナー タイプの [ユーザ（User）] または [名前非表示（パブリック/共有スペース）（Anonymous (Public/Shared Space)）] を選択します。
電話ロード名（Phone Load Name）	ドロップダウン リストから、割り当てられた電話ユーザのユーザ ID を選択します。ユーザ ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザ ID を割り当てると、そのデバイスは、ライセンスの使用状況レポートの「“未割り当てデバイス”」から「“ユーザ”」に移動します。 （注） エクステンション モビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。

フィールド	説明
[トラステッドリレーポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッドリレーポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • On：このデバイスで、TRPの使用をイネーブルにする場合にこの値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の[トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • Default：この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の [トラステッドリレーポイントを使用（Use Trusted Relay Point）] 設定を使用します。
[常にプライム回線を使用する（Always Use Prime Line）]	ドロップダウンリストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフフック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールの呼び出し音は鳴り続けます。電話のユーザは、他の回線を選択してこれらのコールに応答する必要があります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [常にプライム回線を使用する（Always Use Prime Line）] サービスパラメータの設定を使用します。

フィールド	説明
[ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Cisco Unified Communications Manager は常にボイス メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。
位置情報（GeoLocation）	ドロップダウン リストから地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、[システム（System）] > [地理位置情報の設定（Geolocation Configuration）] メニュー オプションで設定した地理位置情報も選択できます。
プレゼンテーション インジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）	コール単位でコール表示制限を設定する場合に、この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すると、Cisco Unified Communications Manager は内線コールに対して受信したすべての表示制限を無視します。 この設定は、トランスレーション パターン レベルで発信側回線 ID 表示と接続先回線 ID 表示の設定と組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
[CTIからのデバイスの制御を許可（Allow Control of Device from CTI）]	CTI に対してこのデバイスの制御と監視を許可する場合は、このチェックボックスをオンにします。 関連付けられた電話番号で共有回線が指定されている場合、CTI がサポートするデバイス タイプとプロトコルの組み合わせが少なくとも 1 つの関連付けられたデバイスで指定されている間は、このチェックボックスをオンにしておく必要があります。

フィールド	説明
ハント グループにログイン（Logged into Hunt Group）	CTI ポートをハント リストに追加したら、管理者はこのチェックボックスをオン（またはオフ）にすることによって、ユーザをログインまたはログアウトさせることができます。 ユーザは電話機のソフトキーを使用して、電話機をハント リストにログインまたはログアウトします。
リモート デバイス（Remote Device）	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、このチェックボックスはシグナルの遅延が発生している場合のみオンにしてください。
[ホットライン デバイス（Hot Line Device）]	このデバイスをホットライン デバイスにするには、このチェックボックスをオンにします。ホットラインデバイスは、他のホットラインデバイスにのみ接続できます。この機能は PLAR の拡張機能であり、電話がオフフックになると自動的に 1 つの電話番号をダイヤルするように電話を設定します。ホットラインでは、PLAR を使用するデバイスに適用できる制限を追加できます。 ホットラインを実装するには、補足サービス ソフトキーを使用せずにソフトキーテンプレートを作成して、ホットラインデバイスに適用する必要があります。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *22* : *[この電話からのコールの発信者 ID（Caller ID For Calls From This Phone）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーション CSS に、このデバイスに割り当てる発呼側トランスフォーメーション パターンが含まれていることを確認してください。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側変換 CSS を使用する場合は、この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選択しない場合、デバイスは[トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *23* : *[リモート番号（Remote Number）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リストから、このデバイスに受信したコールのリモート発信者番号に適用する、発呼側トランスフォーメーション パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換するために、このデバイスが属するデバイスプールで設定されている発呼側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 *24* : *[プロトコル固有情報（Protocol Specific Information）]*

フィールド	説明
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リストから、エンドユーザの話中ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザがモニタ可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンス グループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified CM の管理で設定されている BLF プレゼンス グループは、ドロップダウン リストにも表示されます。
デバイスのセキュリティ プロファイル（Device Security Profile）	デバイスに適用するセキュリティ プロファイルを選択します。 Cisco Unified Communications Manager の管理ページで設定されるすべてのデバイスにセキュリティ プロファイルを適用する必要があります。

フィールド	説明
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンド ユーザから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンドユーザのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified CM の管理で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリング サーチ スペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンドユーザ用に別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
不在ポート（Unattended Port）	このデバイスの不在ポートを示すには、このチェックボックスをオンにします。
[RFCC 2833 Disabled（RFCC 2833 の無効化）]	SCCP を実行しているデバイスの場合は、このチェックボックスをオンにして RFC2833 のサポートを無効にします。

表 *25*：製品固有の設定

フィールド	説明
デバイス製造元が定義するモデル固有の設定フィールド	製品固有の設定項目に関するフィールドの説明およびヘルプを表示するには、[製品固有の設定（Product Specific Configuration）] エリアで [?]“”情報アイコンをクリックして、ポップアップ ダイアログボックスにヘルプを表示します。 詳細については、ATA 186 のマニュアルを参照してください。

アナログ電話アダプタ 187 設定フィールド

表 *26*：アナログ電話アダプタ *187* 設定フィールド

フィールド	説明
MACアドレス（MAC Address）	ATA 187 を識別する Media Access Control（MAC）アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。 次のいずれかの方法で、ATA 187 の MAC アドレスを判別できます。 • ATA 187 の背面にある MAC ラベルを確認する。 • ATA 187 の Web ページを表示し、[デバイス情報（Device Information）] ハイパーリンクをクリックする。
説明	ATA 187 のテキストの説明を入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	ATA 187 を割り当てるデバイス プールを選択します。デバイス プールは、複数のデバイスに共通の特性（地域、日時グループ、ソフトキーテンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
共通デバイス設定（Common Device Configuration）	ATA 187 を割り当てる共通デバイス設定を選択します。 [共通デバイス設定（Common Device Configuration）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[電話ボタンテンプレート（Phone Button Template）]	適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
共通の電話プロファイル（Common Phone Profile）	ドロップダウン リストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。

フィールド	説明
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
ユーザ保留MOH音源（User Hold MOH Audio Source）	ドロップダウン リストから、ユーザが保留操作を開始する場合に保留音（MOH）として使用するオーディオ ソースを選択します。
参照先	ドロップダウン リストから、デバイス プール内の電話とゲートウェイに関連付けられている場所を選択します。
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループは、帯域幅不足のためにブロックされるコールをルーティングするために使用するプレフィックス番号を提供します。AAR グループが指定された場合、Cisco Unified CM はデバイス プールまたは回線に関連付けられた AAR グループを使用します。
ユーザ ロケール（User Locale）	ドロップダウン リストから、CTI ポートに関連付けられたユーザ ロケールを選択します。そのユーザ ロケールは、言語とフォントを含んだ、ユーザをサポートする一連の詳細情報を識別します。 ユーザ ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザ ロケールを使用します。
ネットワーク ロケール（Network Locale）	ドロップダウン リストから、CTI ポートに関連付けられたネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域のデバイスが使用するトーンと音調の定義が含まれます。 ネットワーク ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたネットワーク ロケールを使用します。

フィールド	説明
[ビルトインブリッジ（Built In Bridge）]	[ビルトインブリッジ（Built In Bridge）] ドロップダウン リストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 • オン • オフ（Off） • デフォルト
プライバシー（Privacy）	プライバシーについて、[プライバシー（Privacy）] ドロップダウン リストから [オン（On）] を選択します。
[デバイスモビリティモード（Device Mobility Mode）]	ドロップダウン リストから、このデバイスのデバイスモビリティ機能をオンまたはオフにします。デフォルトのデバイスモビリティ モードを使用する場合は、[デフォルト（Default）] を選択します。デフォルトの設定では、デバイスの [デバイスモビリティ モード（Device Mobility Mode）] サービス パラメータの値が使用されます。
[オーナー（Owner）]	オーナーのタイプとして、[ユーザ（User）] または [名前非表示（パブリック/共有スペース）（Anonymous (Public/Shared Space)）] を選択します。
[オーナーのユーザID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザのユーザ ID を選択します。ユーザ ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザ ID を割り当てると、[ライセンスの使用状況レポート（License Usage Report）] でデバイスが [未割り当てデバイス（Unassigned Devices）] から [ユーザ（Users）] に移動します。 （注） エクステンション モビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。
電話ロード名（Phone Load Name）	ATA 187 のカスタム ソフトウェアを入力します。

フィールド	説明
[トラステッド リレー ポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッド リレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • オン（On）：このデバイスでの TRP の使用を有効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • デフォルト（Default）：この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定を使用します。
[常にプライム回線を使用する（Always Use Prime Line）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフフック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールの呼び出し音は鳴り続けます。電話のユーザは、他の回線を選択してこれらのコールに応答する必要があります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [常にプライム回線を使用する（Always Use Prime Line）] サービス パラメータの設定を使用します。

フィールド	説明
[ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Cisco Unified Communications Manager は常にボイス メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。
位置情報（GeoLocation）	ドロップダウン リストから地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、[システム（System）] > [地理位置情報の設定（Geolocation Configuration）] メニュー オプションで設定した地理位置情報も選択できます。
プレゼンテーション インジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）	コール単位でコール表示制限を設定する場合に、この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すると、Cisco Unified Communications Manager は内線コールに対して受信したすべての表示制限を無視します。 この設定は、トランスレーション パターン レベルで発信側回線 ID 表示と接続先回線 ID 表示の設定と組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
ハント グループにログイン（Logged into Hunt Group）	ATA 187 をハント リストに追加したら、管理者はこのチェックボックスをオン（またはオフ）にすることによって、ユーザをログインまたはログアウトさせることができます。 ユーザは電話のソフトキーを使用して、電話をハント リストにログインまたはログアウトします。

フィールド	説明
リモート デバイス（Remote Device）	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。
保護されたデバイス（Protected Device）	電話を保護対象として指定するには、このチェックボックスをオンにします。コールが暗号化されており、両方の電話が保護されたデバイスとして設定されている場合に、それをユーザに通知するために、電話が 2 秒間のトーンを再生できます。このトーンは、コールが応答されたとき、発側と着側の両者に対して再生されます。このトーンは、両方の電話が保護されていて、暗号化メディア上でコールが行われたときでなければ再生されません。 このチェックボックスをオンにすると、再生するセキュア通知トーンの複数の設定要件のうち 1 つのみが表示されます。セキュア通知トーン機能と設定要件の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。 このチェックボックスがオンで、システムがコールは暗号化されていないと判断すると、電話は非セキュア通知トーンを再生して、コールが保護されていないことをユーザに通知します。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *27*：*[この電話からのコールの発信者 ID（Caller ID For Calls From This Phone）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーション CSS に、このデバイスに割り当てる発呼側トランスフォーメーションパターンが含まれていることを確認してください。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側変換 CSS を使用する場合は、この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選択しない場合、デバイスは[トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *28* : *[リモート番号（Remote Number）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リストから、このデバイスに受信したコールのリモート発信者番号に適用する、発呼側トランスフォーメーション パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換するために、このデバイスが属するデバイス プールで設定されている発呼側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 *29* : *[プロトコル固有情報（Protocol Specific Information）]*

フィールド	説明
パケット キャプチャ モード（Packet Capture Mode）	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [なし（None）] : このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。 この設定は、パケット キャプチャの完了後に行います。 • バッチ処理モード（Batch Processing Mode）：Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを 7 日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1 つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。

フィールド	説明
パケット キャプチャ時間（Packet Capture Duration）	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。 このフィールドには、1 つのパケット キャプチャ セッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は 0 で、範囲は 0 ～ 300 分です。 パケット キャプチャを開始するには、このフィールドに 0 以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リストから、エンドユーザの話中ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザがモニタ可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンス グループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified CM の管理で設定されている BLF プレゼンス グループは、ドロップダウン リストにも表示されます。
SIP ダイヤル規則	必要に応じて、適切な SIP ダイヤル ルールを選択します。SIP ダイヤル ルールは、Cisco Unified IP Phone 7940 および 7960 のローカル ダイヤル プランを提供するため、ユーザは、コールが処理される前に、キーを押したり、タイマーを待機したりする必要はありません。 SIP を実行している IP フォンにダイヤル ルールを適用しない場合は、[SIP ダイヤル ルール（SIP Dial Rules）] フィールドを [<なし>（<None>）] に設定したままにします。これは、コールが処理される前に、ユーザがダイヤル ソフトキーを使用するか、タイマーが切れるまで待つ必要があることを意味します。
MTP 優先発信コーデック（MTP Preferred Originating Codec）	メディア ターミネーション ポイントが SIP のコールに必要な場合は、ドロップダウン リストから使用するコーデックを選択します。
デバイスのセキュリティ プロファイル（Device Security Profile）	デバイスに適用するセキュリティ プロファイルを選択します。 Cisco Unified Communications Manager の管理ページで設定されるすべてのデバイスにセキュリティ プロファイルを適用する必要があります。

フィールド	説明
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	ドロップダウン リストから再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照が失敗すると、Refer Primitive は「“405 Method Not Allowed”」メッセージによって要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンド ユーザから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンド ユーザのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified CM の管理で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリング サーチ スペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザ用に別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
[SIPプロファイル（SIP Profile）]	デフォルトの SIP プロファイルまたは以前に作成された特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブ タイマー、メディア ポート、Do Not Disturb（サイレント）制御など、電話機の特定の SIP 情報を提供します。
[ダイジェストユーザ（Digest User）]	ダイジェスト認証（SIP セキュリティ）で使用されるこの設定用に、電話に関連付けるエンドユーザを選択します。 必ず、[エンド ユーザ設定（End User Configuration）] ウィンドウで指定されているとおりに、選択したユーザのダイジェスト クレデンシャルを設定してください。 電話設定を保存し、設定の更新内容を電話に適用すると、ユーザのダイジェスト クレデンシャルが電話の設定ファイルに追加されます。

フィールド	説明
メディア ターミネーション ポイントが必須（Media Termination Point Required）	このフィールドを使用して、ATA 187 がサポートしない機能（保留や転送など）を実装するために、メディア ターミネーション ポイントを使用するかどうかを指示します。 MTP を使用して機能を実装する場合は、[メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は、[メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェックボックスをオフにします。 このチェックボックスは、ATA 187 クライアントおよび H.245 Empty Capabilities セットをサポートしない ATA 187 デバイスの場合、または単一のソースを介してメディア ストリーミングを終了させる場合にのみ使用します。 このチェックボックスをオンにして、MTP を必須とし、このデバイスをビデオ コールのエンドポイントにすると、コールはオーディオのみになります。
不在ポート（Unattended Port）	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。
DTMF 受信が必要（Require DTMF Reception）	SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。 （注） Cisco Unified Mobility 機能の設定で、SIP トランク（クラスタ間トランク（ICT）またはゲートウェイ）経由で IP フォンのリモート接続先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウトオブバンドで受信できるように、このチェックボックスをオンにします。

表 *30*：認証局プロキシ機能（*CAPF*）情報（*Certification Authority Proxy Function (CAPF) Information*）

フィールド	説明
証明書の操作（Certificate Operation）	ドロップダウンリストから、次のオプションのいずれかを選択します。 • 保留中の操作なし（No Pending Operation）：証明書の操作が行われない場合に表示されます（デフォルトの設定）。 • インストール/アップグレード（Install/Upgrade）：電話に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。 • 削除（Delete）：電話に存在するローカルで有効な証明書を削除します。 • トラブルシュート（Troubleshoot）：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得し、CAPF トレースファイルで証明書クレデンシャルを表示できます。電話に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。 [トラブルシューティング（Troubleshooting）] オプションを選択して、電話に LSC または MIC が存在することを確認できます。

フィールド	説明
認証モード（Authentication Mode）	

フィールド	説明
	このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。 ドロップダウンリストから、次のオプションのいずれかを選択します。 • 認証文字列（By Authentication String）：ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 • ヌル文字列（By Null String）：ユーザの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。 • 既存証明書（LSC に優先権）（By Existing Certificate (Precedence to LSC)）：電話に製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つのみです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • 既存証明書（MIC に優先権）（By Existing Certificate (Precedence to MIC)）：電話に LSC または MIC が存在する場合に、製造元でインストールされる証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が

フィールド	説明
	存在しない場合、操作は失敗します。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
認証文字列（Authentication String）	[認証モード（Authentication Mode）] ドロップダウン リストの [認証文字列（By Authentication String）] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成（Generate String）] ボタンをクリックして、文字列を生成します。文字列が 4 ～ 10 桁であることを確認します。 ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話のユーザまたは管理者が電話に認証文字列を入力する必要があります。
キー サイズ（ビット）（Key Size (Bits)）	CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。 デフォルトの設定より大きいキーサイズを選択すると、電話機は、キーの生成に必要なエントロピーを生成するために時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中にも電話が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
操作の完了期限（Operation Completes by）	このフィールドは、証明書操作オプションの [インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシュート（Troubleshoot）] をサポートし、操作を完了する必要がある日時を指定します。 表示される値は、パブリッシャ データベース サーバに適用されます。
証明書の操作ステータス（Certificate Operation Status）	このフィールドには、証明書操作の進行状況が表示されます。たとえば、操作タイプが証明書操作オプションの [インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、または [トラブルシュート（Troubleshoot）] である場合、<operation type> について [保留（pending）]、[失敗（failed）]、または [成功（successful）] が表示されますこのフィールドに表示される情報は変更できません。

表 *31*：セキュア シェル ユーザ（*Secure Shell User*）

フィールド	説明
セキュア シェル ユーザ（Secure Shell User）	セキュア シェル ユーザのユーザ ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。 Cisco Technical Assistance Center（TAC）では、トラブルシューティングやデバッグを行うときにセキュア シェルを使用します。TAC にお問い合わせください。 Cisco Unified CM が電話に SSH クレデンシャルを平文で送信しないようにするために、暗号化電話設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。
セキュア シェル パスワード（Secure Shell Password）	セキュア シェル ユーザのパスワードを入力します。最大 200 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。TAC にお問い合わせください。 『*Cisco Unified Communications Manager Security Guide*』を参照してください

表 *32*：製品固有の設定

フィールド	説明
デバイス製造元が定義するモデル固有の設定フィールド	製品固有の設定項目のフィールドの説明とヘルプを表示するには、[製品固有の設定（Product Specific Configuration）] エリアで [?]“ ”情報アイコンをクリックし、ポップアップ ダイアログボックスでヘルプを表示します。 詳細については、ATA 187 のドキュメントを参照してください。

アナログ電話アダプタ 190 設定フィールド

表 *33*：アナログ電話アダプタ *190* 設定フィールド

フィールド	説明
MACアドレス（MAC Address）	ATA 190 を特定する Media Access Control（MAC）アドレスを入力します。値が 12 桁の 16 進文字列で構成されていることを確認します。 次のいずれかの方法で、ATA 190 の MAC アドレスを判別できます。 • ATA 190 の背面にある MAC ラベルを確認します。 • ATA 190 の Web ページを表示し、[デバイス情報（Device Information）] ハイパーリンクをクリックします。
説明	ATA 190 の説明テキストを入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	ATA 190 を割り当てるデバイス プールを選択します。デバイス プールでは、複数の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 テンプレートなど）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
共通デバイス設定（Common Device Configuration）	ATA 190 を割り当てる共通デバイス設定を選択します。 共通デバイス設定を表示するには、[詳細表示（View Details）] リンクをクリックします。
[電話ボタンテンプレート（Phone Button Template）]	適切な電話ボタンテンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
共通の電話プロファイル（Common Phone Profile）	ドロップダウン リストで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 [共通の電話プロファイル（Common Phone Profile）] の設定を表示するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。

フィールド	説明
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
ユーザ保留 MOH 音源（User Hold MOH Audio Source）	ドロップダウン リストから、ユーザが保留操作を開始する場合に保留音（MOH）として使用するオーディオ ソースを選択します。
参照先	ドロップダウン リストから、デバイス プール内の電話とゲートウェイに関連付けられている場所を選択します。
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループは、帯域幅不足のためにブロックされるコールをルーティングするために使用するプレフィックス番号を提供します。AAR グループが指定された場合、Cisco Unified CM はデバイス プールまたは回線に関連付けられた AAR グループを使用します。
ユーザ ロケール（User Locale）	ドロップダウン リストから、CTI ポートに関連付けられたユーザ ロケールを選択します。そのユーザ ロケールは、言語とフォントを含んだ、ユーザをサポートする一連の詳細情報を識別します。 ユーザ ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたユーザ ロケールを使用します。
ネットワーク ロケール（Network Locale）	ドロップダウン リストから、CTI ポートに関連付けられたネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域のデバイスが使用するトーンと音調の定義が含まれます。 ネットワーク ロケールが指定されていない場合、Cisco Unified CM はデバイス プールに関連付けられたネットワーク ロケールを使用します。

フィールド	説明
[ビルトインブリッジ（Built In Bridge）]	[ビルトインブリッジ（Built In Bridge）] ドロップダウン リストを使用して割り込み機能用の組み込み型会議ブリッジを有効または無効にします。次のいずれかを実行します。 • オン • オフ（Off） • デフォルト
プライバシー（Privacy）	プライバシーについて、[プライバシー（Privacy）] ドロップダウン リストから [オン（On）] を選択します。
[デバイスモビリティモード（Device Mobility Mode）]	ドロップダウン リストから、このデバイスのデバイス モビリティ機能をオンまたはオフにします。デフォルトのデバイス モビリティ モードを使用する場合は、[デフォルト（Default）] を選択します。デフォルトの設定では、デバイスの [デバイス モビリティ モード（Device Mobility Mode）] サービス パラメータの値が使用されます。
[オーナー（Owner）]	オーナーのタイプとして、[ユーザ（User）] または [名前非表示（パブリック/共有スペース）（Anonymous (Public/Shared Space)）] を選択します。
[オーナーのユーザID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザのユーザ ID を選択します。ユーザ ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザ ID を割り当てると、[ライセンスの使用状況レポート（License Usage Report）] でデバイスが [未割り当てデバイス（Unassigned Devices）] から [ユーザ（Users）] に移動します。 （注） エクステンション モビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。
電話ロード名（Phone Load Name）	ATA 190 のカスタム ソフトウェアを入力します。

フィールド	説明
[トラステッド リレー ポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッド リレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • オン（On）：このデバイスでの TRP の使用を有効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • デフォルト（Default）：この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定を使用します。
[常にプライム回線を使用する（Always Use Prime Line）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフ フック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールの呼び出し音は鳴り続けます。電話のユーザは、他の回線を選択してこれらのコールに応答する必要があります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [常にプライム回線を使用する（Always Use Prime Line）] サービス パラメータの設定を使用します。

フィールド	説明
[ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Cisco Unified Communications Manager は常にボイス メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。
位置情報（GeoLocation）	ドロップダウン リストから地理位置情報を選択します。 [未指定の地理位置情報（Unspecified geolocation）] を選択すると、このデバイスを地理位置情報に関連付けないように指定できます。 さらに、[システム（System）] > [地理位置情報の設定（Geolocation Configuration）] メニュー オプションで設定した地理位置情報も選択できます。
プレゼンテーション インジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）	コール単位でコール表示制限を設定する場合に、この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すると、Cisco Unified Communications Manager は内線コールに対して受信したすべての表示制限を無視します。 この設定は、トランスレーション パターン レベルで発信側回線 ID 表示と接続先回線 ID 表示の設定と組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
ハント グループにログイン（Logged into Hunt Group）	ATA 190 をハント リストに追加すると、管理者はこのチェックボックスをオン（またはオフ）にして、ユーザをログインまたはログアウトさせることができます。 ユーザは電話機のソフトキーを使用して、電話機をハント リストにログインまたはログアウトします。

フィールド	説明
リモート デバイス（Remote Device）	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、シグナリングの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。
保護されたデバイス（Protected Device）	電話を保護対象として指定するには、このチェックボックスをオンにします。コールが暗号化されており、両方の電話が保護されたデバイスとして設定されている場合に、それをユーザに通知するために、電話が 2 秒間のトーンを再生できます。このトーンは、コールが応答されたとき、発側と着側の両者に対して再生されます。このトーンは、両方の電話が保護されていて、暗号化メディア上でコールが行われたときでなければ再生されません。 このチェックボックスをオンにする操作は、セキュア通知トーンを再生するための設定要件の 1 つにすぎません。セキュア通知トーン機能および設定要件の詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。 このチェックボックスをオンにしていて、コールが暗号化されていないと判断された場合、コールが保護されていないことをユーザに通知する非セキュア通知トーンが再生されます。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *34*：*[この電話からのコールの発信者 ID（Caller ID For Calls From This Phone）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーション CSS に、このデバイスに割り当てる発呼側トランスフォーメーション パターンが含まれていることを確認してください。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイス プールに設定されている発信側変換 CSS を使用する場合は、この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選択しない場合、デバイスは[トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *35* : *[リモート番号（Remote Number）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リストから、このデバイスに受信したコールのリモート発信者番号に適用する、発呼側トランスフォーメーションパターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換するために、このデバイスが属するデバイス プールで設定されている発呼側トランスフォーメーション CSS を適用するには、このチェックボックスをオンにします。

表 *36* : *[プロトコル固有情報（Protocol Specific Information）]*

フィールド	説明
パケット キャプチャ モード（Packet Capture Mode）	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。 ドロップダウン リストから、次のいずれかのオプションを選択します。 • [なし（None）] : このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。 この設定は、パケット キャプチャの完了後に行います。 • バッチ処理モード（Batch Processing Mode）：Cisco Unified CM が、復号されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Cisco Unified CM はファイルを 7 日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Cisco Unified CM は、PktCap 仮想ディレクトリにファイルを保存します。1 つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。

フィールド	説明
パケット キャプチャ時間（Packet Capture Duration）	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。 このフィールドには、1 つのパケット キャプチャ セッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は 0 で、範囲は 0 ～ 300 分です。 パケット キャプチャを開始するには、このフィールドに 0 以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リストから、エンドユーザの話中ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンド ユーザがモニタ可能な接続先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンス グループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified CM の管理で設定されている BLF プレゼンス グループは、ドロップダウン リストにも表示されます。
SIP ダイヤル規則	必要に応じて、適切な SIP ダイヤル ルールを選択します。SIP ダイヤル ルールは、Cisco Unified IP Phone 7940 および 7960 のローカル ダイヤル プランを提供するため、ユーザは、コールが処理される前に、キーを押したり、タイマーを待機したりする必要はありません。 SIP を実行している IP フォンにダイヤル ルールを適用しない場合は、[SIP ダイヤル ルール（SIP Dial Rules）] フィールドを [<なし>（<None>）] に設定したままにします。これは、コールが処理される前に、ユーザがダイヤル ソフトキーを使用するか、タイマーが切れるまで待つ必要があることを意味します。
MTP 優先発信コーデック（MTP Preferred Originating Codec）	メディア ターミネーション ポイントが SIP のコールに必要な場合は、ドロップダウン リストから使用するコーデックを選択します。
デバイスのセキュリティ プロファイル（Device Security Profile）	デバイスに適用するセキュリティ プロファイルを選択します。 Cisco Unified Communications Manager の管理ページで設定されるすべてのデバイスにセキュリティ プロファイルを適用する必要があります。

フィールド	説明
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	ドロップダウン リストから再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照が失敗すると、Refer Primitive は「“405 Method Not Allowed”」メッセージによって要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンド ユーザから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンド ユーザのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンドユーザのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified CM の管理で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリング サーチ スペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザ用に別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [なし（None）] に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
[SIPプロファイル（SIP Profile）]	デフォルトの SIP プロファイルまたは以前に作成された特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブ タイマー、メディア ポート、Do Not Disturb（サイレント）制御など、電話機の特定の SIP 情報を提供します。

フィールド	説明
[ダイジェストユーザ（Digest User）]	ダイジェスト認証（SIP セキュリティ）で使用されるこの設定用に、電話に関連付けるエンドユーザを選択します。 必ず、[エンド ユーザ設定（End User Configuration）] ウィンドウで指定されているとおりに、選択したユーザのダイジェスト クレデンシャルを設定してください。 電話機の設定を保存し、設定の更新を電話機に適用すると、ユーザのダイジェスト クレデンシャルが電話設定ファイルに追加されます。 ダイジェスト認証の詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。
メディア ターミネーション ポイントが必須（Media Termination Point Required）	このフィールドを使用して、ATA 190 でサポートされていない機能（保留や転送など）を実装するために、メディア ターミネーション ポイントを使用するかどうかを指示します。 MTP を使用して機能を実装する場合は [メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェックボックスをオンにします。MTP を使用して機能を実装しない場合は [メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェックボックスをオフにします。 このチェックボックスは、ATA 190 クライアントおよび H.245 Empty Capabilities Set をサポートしていない ATA 190 デバイスの場合、または単一ソースを通してメディア ストリーミングを終了させる場合にのみ使用します。 このチェックボックスをオンにして MTP を必須にし、このデバイスがビデオ コールのエンドポイントになると、コールは音声のみになります。
不在ポート（Unattended Port）	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。
DTMF 受信が必要（Require DTMF Reception）	SIP と SCCP を実行しているデバイスの場合に、この電話の DTMF 受信を必須にするには、このチェックボックスをオンにします。 （注） Cisco Unified Mobility 機能の設定で、SIP トランク（クラスタ間トランク（ICT）またはゲートウェイ）経由で IP フォンのリモート接続先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に不可欠な DTMF 番号をアウト オブ バンドで受信できるように、このチェックボックスをオンにします。

表 *37*：認証局プロキシ機能（*CAPF*）情報（*Certification Authority Proxy Function (CAPF) Information*）

フィールド	説明
証明書の操作（Certificate Operation）	ドロップダウンリストから、次のオプションのいずれかを選択します。 • 保留中の操作なし（No Pending Operation）：証明書の操作が行われない場合に表示されます（デフォルトの設定）。 • インストール/アップグレード（Install/Upgrade）：電話に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。 • 削除（Delete）：電話に存在するローカルで有効な証明書を削除します。 • トラブルシュート（Troubleshoot）：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得し、CAPF トレースファイルで証明書クレデンシャルを表示できます。電話に両方の証明書タイプが存在する場合、Cisco Unified CM は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。 [トラブルシュート（Troubleshoot）] オプションを選択することで、電話機に LSC または MIC が存在することを確認できます。 認証局プロキシ機能』（CAPF）の操作の詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

フィールド	説明
認証モード（Authentication Mode）	

フィールド	説明
	このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。 ドロップダウンリストから、次のオプションのいずれかを選択します。 • 認証文字列（By Authentication String）：ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 • ヌル文字列（By Null String）：ユーザの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。 • 既存証明書（LSC に優先権）（By Existing Certificate (Precedence to LSC)）：電話に製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つのみです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • 既存証明書（MIC に優先権）（By Existing Certificate (Precedence to MIC)）：電話に LSC または MIC が存在する場合に、製造元でインストールされる証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に MIC が存在する場合、電話機に LSC が存在するかどうかに関係なく、MIC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が

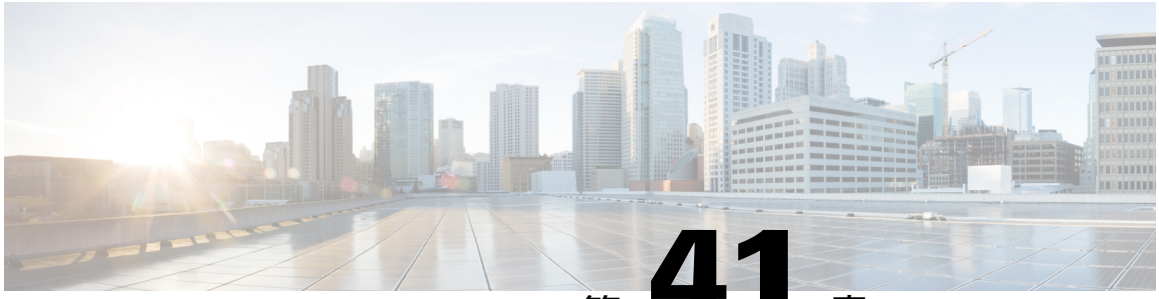
フィールド	説明
	存在しない場合、操作は失敗します。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
認証文字列（Authentication String）	[認証モード（Authentication Mode）] ドロップダウン リストの [認証文字列（By Authentication String）] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[文字列の生成（Generate String）] ボタンをクリックして、文字列を生成します。文字列が 4 ～ 10 桁であることを確認します。 ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話のユーザまたは管理者が電話に認証文字列を入力する必要があります。
キー サイズ（ビット）（Key Size (Bits)）	CAPF で使用されるこの設定では、ドロップダウン リストから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。 デフォルトの設定より大きいキー サイズを選択すると、電話機は、キーの生成に必要なエントロピーを生成するために時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中にも電話が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
操作の完了期限（Operation Completes by）	このフィールドは、証明書操作オプションの[インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、[トラブルシュート（Troubleshoot）] をサポートし、操作を完了する必要がある日時を指定します。 表示される値は、パブリッシャ データベース サーバに適用されます。
証明書の操作ステータス（Certificate Operation Status）	このフィールドには、証明書操作の進行状況が表示されます。たとえば、操作タイプが証明書操作オプションの [インストール/アップグレード（Install/Upgrade）]、[削除（Delete）]、または [トラブルシュート（Troubleshoot）] である場合、<operation type> について [保留（pending）]、[失敗（failed）]、または [成功（successful）] が表示されますこのフィールドに表示される情報は変更できません。

表 *38*：セキュア シェル ユーザ（*Secure Shell User*）

フィールド	説明
セキュア シェル ユーザ（Secure Shell User）	セキュア シェル ユーザのユーザ ID を入力します。最大 50 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。このフィールドは、設定している電話デバイスが SSH アクセスをサポートしている場合に表示されます。 Cisco Technical Assistance Center（TAC）では、トラブルシューティングやデバッグを行うときにセキュア シェルを使用します。TAC にお問い合わせください。 Cisco Unified CM が電話に SSH クレデンシャルを平文で送信しないようにするために、暗号化電話設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。
セキュア シェル パスワード（Secure Shell Password）	セキュア シェル ユーザのパスワードを入力します。最大 200 文字の英数字または特殊文字を入力できます。無効な文字は、"、%、&、<、>、\ です。TAC にお問い合わせください。 Cisco Unified CM が電話に SSH パスワードを平文で送信しないようにするために、暗号化電話設定ファイルを設定する方法については、このリリースの『*Cisco Unified Communications Manager* セキュリティ ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

表 *39*：製品固有の設定

フィールド	説明
デバイス製造元が定義するモデル固有の設定フィールド	製品固有の設定項目に関するフィールドの説明およびヘルプを表示するには、[製品固有の設定（Product Specific Configuration）] エリアで [?]“ ”情報アイコンをクリックして、ポップアップ ダイアログボックスにヘルプを表示します。 詳細については、ATA 190 のマニュアルを参照してください。



第 41 章

ソフトウェアベースのエンドポイントの設定

- ソフトウェアベースのエンドポイントの設定，363 ページ
- CTI ポートの設定，363 ページ
- H.323 クライアントを設定，374 ページ
- Cisco IP Communicator の設定，375 ページ

ソフトウェアベースのエンドポイントの設定

CTI ポート、H.323 クライアント、Cisco IP Communicator など、ソフトウェアベースのエンドポイントを設定するには、この章の手順を実行します。

CTI ポートの設定

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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。

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）] ドロップダウン リストから [CTI ポート（CTI Port）] を選択して、[次へ（Next）] 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）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

CTI Port Settings, （364 ページ）

CTI Port Settings

表 *40*：*CTI Port Settings*

フィールド	説明
デバイス名（Device Name）	所有者ユーザ ID に基づいて自動的に入力される CTI ポートの名前を指定します。 デバイス名の形式は、デフォルトで *CTIRD<OwnerUserID>* です。 このフィールドは編集できます。デバイス名は最大 15 文字で指定できます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。
説明	CTI ポートの説明文を入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	CTI ポートを割り当てるデバイスプールを選択します。デバイスプールは、複数の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など）のセットを定義します。 デバイス プール構成の設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。

フィールド	説明
共通デバイス設定（Common Device Configuration）	CTI ポートを割り当てる共通デバイス設定を選択します。 共通デバイス設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
共通の電話プロファイル（Common Phone Profile）	ドロップダウン リスト ボックスで、使用可能な共通の電話プロファイルのリストから共通の電話プロファイルを選択します。 共通の電話プロファイル設定を確認するには、[詳細の表示（View Details）] リンクをクリックします。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストを使用から、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[AARコーリングサーチスペース（AAR Calling Search Space）]	ドロップダウン リストから、自動代替ルーティング（AAR）を実行したときに使用するデバイスの適切なコーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
[メディアリソースグループリスト（Media Resource Group List）]	適切なメディア リソース グループ リストを選択します。メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループから構成されます。 [<なし>（<None>）] を選択すると、Cisco Unified CM はデバイス プールで定義されたメディア リソース グループ リストを使用します。
ユーザ保留 MOH 音源（User Hold MOH Audio Source）	ドロップダウン リストから、ユーザが保留操作を開始したときの保留音（MOH）に使用するオーディオ ソースを選択します。
ネットワーク保留 MOH 音源（Network Hold MOH Audio Source）	ドロップダウン リストから、ネットワークが保留操作を開始したときの MOH に使用するオーディオ ソースを選択します。
参照先	ドロップダウン リストから、デバイス プール内の電話とゲートウェイに関連付けられている場所を選択します。

フィールド	説明
[AARグループ（AAR Group）]	このデバイスの自動代替ルーティング（AAR）グループを選択します。AAR グループは、帯域幅不足のためにブロックされるコールをルーティングするために使用するプレフィックス番号を提供します。AAR グループが指定された場合、Cisco Unified CM はデバイス プールまたは回線に関連付けられた AAR グループを使用します。
ユーザ ロケール（User Locale）	ドロップダウン リスト ボックスから、CTI ポートに関連付けるユーザ ロケールを選択します。そのユーザ ロケールは、言語とフォントを含んだ、ユーザをサポートする一連の詳細情報を識別します。 ユーザ ロケールが指定されなかった場合、Cisco Unified CM はデバイス プールに関連付けられたユーザ ロケールを使用します。
ネットワーク ロケール（Network Locale）	ドロップダウン リスト ボックスから、CTI ポートに関連付けるネットワーク ロケールを選択します。ネットワーク ロケールには、特定の地理的領域の電話が使用するトーンと音の周期の定義が含まれます。 ネットワーク ロケールが指定されなかった場合、Cisco Unified CM はデバイス プールに関連付けられたユーザ ロケールを使用します。
プライバシー	プライバシーについては、[プライバシー（Privacy）] ドロップダウン リスト ボックスで [オン（On）] を選択します。
[オーナー（Owner）]	オーナー タイプには、[ユーザ（User）] または [匿名（Anonymous）]（パブリック/共有スペース）を選択します。
[オーナーのユーザID（Owner User ID）]	ドロップダウン リストから、割り当てられた CTI ポート ユーザのユーザ ID を選択します。ユーザ ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。デバイスにユーザ ID を割り当てると、ライセンス使用レポートの「未指定のデバイス」から「ユーザ」にデバイスが移動します。

フィールド	説明
回線をまたいで参加	ドロップダウン リスト ボックスから、このデバイスの [回線をまたいで参加（Join Across Lines）] 機能を有効または無効にするか、あるいは[デフォルト（Default）] を選択してサービス パラメータ設定を使用します。
[トラステッド リレー ポイントを使用（Use Trusted Relay Point）]	次の値のいずれかを選択します。 • [オフ（Off）]：このデバイスで、トラステッド リレー ポイント（TRP）の使用を無効にするには、この値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • On：このデバイスで、TRP の使用をイネーブルにする場合にこの値を選択します。この設定は、このデバイスに関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定よりも優先されます。 • Default：この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] 設定を使用します。

フィールド	説明
[常にプライム回線を使用する（Always Use Prime Line）]	ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態になっているときにいずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からコールに応答します。 • [オン（On）]：電話機がアイドル状態（オフ フック）になっているときにいずれかの回線でコールを受信すると、このコールにはプライマリ回線が選択されます。他の回線のコールの呼び出し音は鳴り続けます。電話のユーザは、他の回線を選択してこれらのコールに応答する必要があります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [常にプライム回線を使用する（Always Use Prime Line）] サービス パラメータの設定を使用します。

フィールド	説明
[ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）]	ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [オフ（Off）]：電話がアイドル状態の場合、電話のメッセージ ボタンを押すと、ボイス メッセージが設定されている回線からボイス メッセージ システムに自動的にダイヤルされます。Cisco Unified Communications Manager は常にボイス メッセージのある最初の回線を選択します。ボイスメッセージが設定されている回線が存在しない場合に電話のユーザが [メッセージ（Messages）] ボタンを押すと、プライマリ回線が使用されます。 • [オン（On）]：電話がアイドル状態の場合に電話のメッセージ ボタンを押すと、電話のプライマリ回線がボイス メッセージを受信するアクティブな回線になります。 • [デフォルト（Default）]：Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする [ボイスメッセージには常にプライム回線を使用する（Always Use Prime Line for Voice Message）] サービス パラメータの設定を使用します。
位置情報（GeoLocation）	ドロップダウン リスト ボックスから、地理位置情報を選択します。 このデバイスを地理位置情報に関連付けないことを指定する未指定の地理位置情報を選択できます。 さらに、[システム（System）]>[地理位置情報の設定（Geolocation Configuration）] メニュー オプションで設定した地理位置情報も選択できます。

フィールド	説明
プレゼンテーションインジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）	コール単位でコール表示制限を設定する場合に、この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すると、Cisco Unified Communications Manager は内線コールに対して受信したすべての表示制限を無視します。 この設定は、トランスレーション パターン レベルで発信側回線 ID 表示と接続先回線 ID 表示の設定と組み合わせて使用します。これらの設定を組み合わせて使用すれば、コールごとに発信側または接続先の回線表示情報を選択的に表示またはブロックするようにコール表示制限を設定できます。
ハント グループにログイン（Logged into Hunt Group）	CTI ポートをハントリストに追加したら、管理者はこのチェックボックスをオン（またはオフ）にすることによって、ユーザをログインまたはログアウトさせることができます。 ユーザは電話機のソフトキーを使用して、電話機をハントリストにログインまたはログアウトします。
リモート デバイス（Remote Device）	このチェックボックスをオンにすると、デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルします。 **ヒント** この機能はリソースを消費するため、シグナルの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。

[番号表示トランスフォーメーション（Number Presentation Transformation）]

表 *41*：*[この電話からのコールの発信者 ID（Caller ID For Calls From This Phone）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーションCSSに、このデバイスに割り当てる発呼側トランスフォーメーションパターンが含まれていることを確認してください。

フィールド	説明
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイスプールに設定されている発信側変換CSSを使用する場合は、この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選択しない場合、デバイスは [トランク設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *42* : *[リモート番号（Remote Number）]*

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	ドロップダウン リスト ボックスから、このデバイスで受信したコールのリモート着信者番号に適用する、発信側変換パターンを含むコーリング サーチ スペース（CSS）を選択します。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	リモート通話とリモート接続番号の変換するために、このデバイスが属するデバイスプールで設定されている発呼側トランスフォーメーションCSSを適用するには、このチェックボックスをオンにします。

表 *43* : *[プロトコル固有情報（Protocol Specific Information）]*

フィールド	説明
[BLFプレゼンスグループ（BLF Presence Group）]	ドロップダウン リスト ボックスから、エンドユーザのビジー ランプ フィールド（BLF）プレゼンス グループを選択します。選択したグループは、エンドユーザがモニタ可能な宛先を指定します。 BLF プレゼンス グループのデフォルト値は [標準のプレゼンス グループ（Standard Presence group）] であり、インストール時に設定されます。Cisco Unified 管理ページで設定される BLF プレゼンス グループは、ドロップダウン リスト ボックスにも表示されます。

フィールド	説明
デバイスのセキュリティ プロファイル（Device Security Profile）	デバイスに適用するセキュリティ プロファイルを選択します。 Cisco Unified Communications Manager の管理ページで設定されるすべてのデバイスにセキュリティ プロファイルを適用する必要があります。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンド ユーザから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンドユーザのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンド ユーザのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified CM の管理で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリング サーチ スペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザ用に別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは[なし（None）]に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。
不在ポート（Unattended Port）	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。

表 *44*：*[MLPP* および機密アクセス レベル情報（*MLPP and Confidential Access Level Information*）*]*

フィールド	説明
[MLPP ドメイン（MLPP Domain）]	ドロップダウン リストから、このデバイスに関連付ける Multilevel Precedence and Preemption（MLPP）ドメインを選択します。このフィールドが空欄にすると、デバイスの MLPP ドメインはデバイス プールに対して設定された値から継承されます。デバイス プールに [MLPP ドメイン（MLPP Domain）] の設定がない場合は、このデバイスの MLPP ドメインは MLPP Domain Identifier エンタープライズ パラメータの設定値から継承されます。 MLPP ドメインのデフォルト値では [なし（None）] が指定されています。
機密アクセス モード（Confidential Access Mode）	ドロップダウン リスト ボックスから、機密アクセス レベル モードとして次のいずれかのオプションを選択します。 • [固定（Fixed）]：機密アクセス レベル値はコールの完了よりも優先されます。 • [可変（Variable）]：コールの完了は CAL レベルよりも優先されます。
機密アクセス レベル（Confidential Access Level）	ドロップダウン リスト ボックスから、適切な [機密アクセス レベル（Confidential Access Level）] 値を選択します。

表 *45*：サイレント情報

フィールド	説明
[サイレント（Do Not Disturb）]	リモートデバイスのサイレント機能をイネーブルにする場合は、このチェックボックスをオンにします。
DND オプション（DND Option）	DND をイネーブルにすると、[コール拒否（Call Reject）] このオプションは、着信コール情報をユーザに提示しないようにします。[DND着信呼警告（DND Incoming Call Alert）] パラメータの設定に応じて、デバイスはビープを再生するか、コールの点滅通知を表示します。

フィールド	説明
DND 着信呼警告（DND Incoming Call Alert）	DND の [呼出音オフ（Ringer Off）] オプションまたは [コール拒否（Call Reject）] オプションを有効にした場合、このパラメータはデバイスでコールを表示する方法を指定します。 ドロップダウン リストから、次のオプションのいずれかを選択します。 • [なし（None）]：このオプションは、[共通の電話プロファイル（Common Phone Profile）] ウィンドウの [DND 着信呼警告（DND Incoming Call Alert）] 設定をこのデバイスで使用するように指定します。 • [無効（Disable）]：このオプションは、コールを通知するビープ音とフラッシュの両方を無効にしますが、DND の [呼出音オフ（Ringer Off）] オプションの場合、着信コール情報が表示されます。[DND コール拒否（DND Call Reject）] オプションの場合、コール アラートが表示されず、デバイスに情報が送信されません。 • [ビープ音のみ（Beep Only）]：着信コールの場合、このオプションによって、デバイスでビープ音のみが再生されます。 • [フラッシュのみ（Flash Only）]：このオプションを選択した場合、着信コールがあると、デバイスのフラッシュ アラートだけが表示されます。

H.323 クライアントを設定

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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。

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）] ドロップダウンリストから [H.323 Client] を選択して、[次へ（Next）] をクリックします。
[電話機の設定（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）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

H.323 クライアントの設定, （375 ページ）

H.323 クライアントの設定

Cisco IP Communicator の設定

Cisco IP Communicator は、ソフトウェア ベースのアプリケーションです。ユーザがパーソナル コンピュータを電話機として使用し、電話のコールが受信できるようにします。フル装備の Cisco Unified IP Phone と同じ機能を利用できます。Cisco IP Communicator は、Cisco Unified Communications Manager のコール処理システム上で動作し、テレフォニー機能と Voice over IP 機能を提供します。Cisco Unified CM の管理の [電話の設定（Phone Configuration）] ウィンドウで、電話デバイスとして Cisco IP Communicator を設定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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。

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）] ドロップダウン リストから、[Cisco IP Communicator] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [デバイス プロトコルの選択（Select the Device Protocol）] ドロップダウン リストから、[SCCP] または [SIP] を選択して、[次へ（Next）] 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 5 [電話の設定（Phone Configuration）] ウィンドウで次の必須フィールドを設定します。

- [デバイス名（Device Name）]：Cisco IP Communicator のデバイスを識別する名前を入力します。

- [デバイス プール（Device Pool）]：この電話機を割り当てるデバイス プールを選択します。デバイス プールは、複数のデバイスに共通の特性（地域、日時グループ、ソフトキー テンプレートなど）のセットを定義します。
- [電話ボタン テンプレート（Phone Button Template）]：該当する電話ボタン テンプレートを選択します。電話ボタンテンプレートでは、電話機上のボタンを設定し、各ボタンにどの機能（回線、スピード ダイヤルなど）を使用するかを特定します。
- [オーナーのユーザ ID（Owner User ID）]：ドロップダウン リストボックスから、割り当てられた電話ユーザのユーザ ID を選択します。
- [デバイスのセキュリティ プロファイル（Device Security Profile）]：デバイスに適用するセキュリティ プロファイルを選択します。

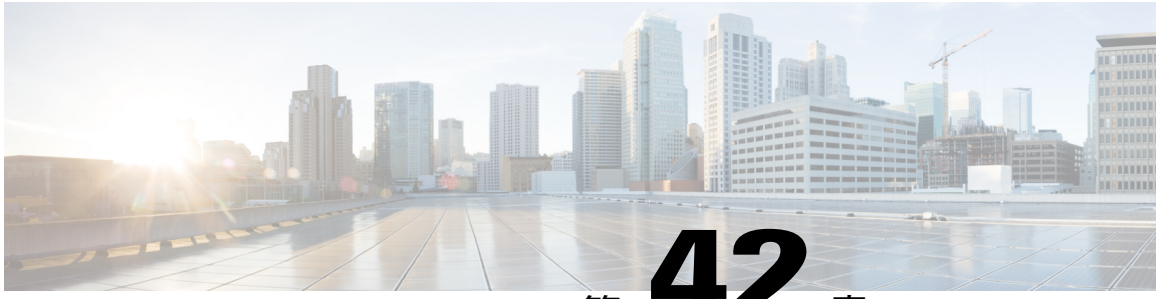
残りのフィールドにデフォルト設定を使用できます。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [関連付け（Association）] エリアで、[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] をクリックします。

ステップ 8 [電話番号（Directory Number）] フィールドに、電話機に関連付ける電話番号を入力します

ステップ 9 [保存（Save）] をクリックします。



第 42 章

Cisco IP Phone の設定

- Cisco IP Phone の概要，377 ページ
- Cisco IP Phone の設定タスク フロー，378 ページ

Cisco IP Phone の概要

Cisco Unified IP Phone は、IP ネットワークを介して音声通信を行うフル装備の電話です。この機能を提供するために、IP Phone は、他の主要な Cisco Unified IP Telephony およびネットワーク コンポーネントとやり取りしています。たとえば、Cisco Unified Communications Manager、DNS および DHCP サーバ、TFTP サーバ、メディア リソース、Cisco Power over Ethernet（PoE）などです。これらの IP Phone は、デジタル ビジネス電話と同様に機能し、コールの発信や着信のほか、ミュート、保留、転送、短縮ダイヤル、コール転送などの機能も利用できます。さらに、Cisco Unified IP Phones はデータ ネットワークに接続されるため、IP テレフォニー機能が拡張され、ネットワーク情報やサービス、およびカスタマイズ可能な機能やサービスにアクセスできるようになります。ファイル認証、デバイス認証、シグナリングの暗号化、メディアの暗号化などのセキュリティ機能もサポートします。

この章では、システムで動作するように電話を設定する方法について説明します。コール パーク、コール転送、話中ランプ フィールド（BLF）、コール ピックアップ、短縮ダイヤルなどの機能を設定するには、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Cisco IP Phone の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	電話の設定, （379 ページ）	SIP 電話または SCCP 電話を設定するには、このタスクを実行します。
ステップ 2	EnergyWise の設定, （385 ページ）	電力消費量を削減するには、自動的にオフ（スリープ）またはオン（ウェイク）するように電話を設定します。
ステップ 3	クライアント サービス フレームワーク デバイスの設定, （387 ページ）	Cisco Unified Client Services Framework デバイスを設定するには、次の手順を実行します。Cisco Unified Client Services Framework デバイスは、次のいずれかになります。 • Cisco Unified Communications Integration for Microsoft Office Communicator • Cisco Unified Communications Integration for WebEx Connect • Cisco Unified Personal Communicator（Release 8.0 以降）
ステップ 4	CTI リモート デバイスの設定, （391 ページ）	CTI リモートデバイスを設定するには、次の手順を実行します。CTI リモート デバイスは、ユーザが Cisco UC アプリケーションで使用できるオフクラスタ電話を表すデバイス タイプです。デバイス タイプには、1 つ以上の回線（電話番号）と 1 つ以上のリモート接続先が設定されます。
ステップ 5	電話データを移行, （404 ページ）	別の電話に移行し、古い電話を使用する必要がなくなった場合は、次の手順を実行します。
ステップ 6		

電話の設定

手順

	コマンドまたはアクション	目的
ステップ 1	SIP 電話を設定するには、次の手順を実行します。 • SIP 電話のセキュア ポートの設定, （380 ページ） • サービスの再起動, （380 ページ） • SIP プロファイルの設定, （381 ページ） • 電話セキュリティ プロファイルの設定, （382 ページ） • 電話の設定, （383 ページ） • Cisco Unified IP Phoneサービスの設定, （384 ページ） • VPN クライアントの設定	Session Initiation Protocol（SIP）を使用する電話機がある場合、この手順を実行します。SIP が電話機と他のネットワーク コンポーネント間のプライマリ インターフェイスとして機能します。SIP 以外に、IP アドレス割り当ての DHCP、ドメイン名のアドレス解決に DNS、イメージや設定データをダウンロードするための TFTP など他のプロトコルがさまざまな機能に使用されます。 VPN クライアントの設定に関する詳細な手順については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
ステップ 2	SCCP 電話を設定するには、次の手順を実行します。 • 電話セキュリティ プロファイルの設定, （382 ページ） • 電話の設定, （383 ページ） • Cisco Unified IP Phoneサービスの設定, （384 ページ） • VPN クライアントの設定	Skinny Client Control Protocol（SCCP）を使用する Cisco IP Phone を設定するには、次の手順を実行します。SCCP は IP デバイスと Cisco Unified Communications Manager 間の通信に Cisco 独自のメッセージを使用します。SCCP はマルチプロトコル環境で簡単に共存できます。登録時には、Cisco Unified IP Phone は Cisco Unified Communications Manager から回線と他のすべての設定を受信します。 VPN クライアントの設定に関する詳細な手順については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

次の作業

電源の供給、ネットワーク接続の検証、Cisco Unified IP Phone のネットワーク設定を実行します。ネットワーク設定の詳細は、ご使用の Cisco Unified IP Phone のモデルの『*Cisco Unified IP Phone Administration Guide*』を参照してください。

SIP 電話のセキュア ポートの設定

SIP 電話のセキュア ポートを設定するには、次の手順に従います。Cisco Unified Communications Manager は、SIP 電話からの SIP 回線登録をリッスンするためにこの TLS ポートを使用します。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [Cisco Unified CM（Cisco Unified CM）] を選択します。

ステップ 2 [このサーバの Cisco Unified Communications Manager TCP ポート設定（Cisco Unified Communications Manager TCP Port Settings for this Server）] で、[SIP 電話セキュア ポート（SIP Phone Secure Port）] フィールドにポート番号を指定するか、またはデフォルト値をそのまま使用します。デフォルト値は 5061 です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 [OK] をクリックします。

次の作業

デフォルトのポート番号を変更する場合は、次の手順を実行します。

- サービスの再起動, （380 ページ）.
- SIP 電話をリセットします。

サービスの再起動

Cisco CallManager と Cisco CTL プロバイダー サービスを再起動するには、次の手順に従います。

はじめる前に

SIP 電話のセキュア ポートの設定, （380 ページ）

手順

ステップ 1 Cisco Unified Serviceability のインターフェイスから、[ツール（Tools）] > [コントロールセンタ - 機能サービス（Control Center - Feature Services）] の順に選択します。

ステップ 2 [サーバ（Servers）] ドロップダウンリストから、[Cisco Unified Communications Manager] サーバを選択します。
CM のサービス領域で、[サービス名（Service Name）] 列の Cisco CallManager が表示されます。

ステップ 3 Cisco CallManager サービスに対応するラジオ ボタンをクリックします。

ステップ 4 [再起動（Restart）] をクリックします。
サービスが再起動し、「サービスの再起動に成功しました（`Service Successfully Restarted`）」というメッセージが表示されます。

ステップ 5 Cisco CTL プロバイダー サービスを再起動するにはステップ 3 とステップ 4 を繰り返します。

次の作業

SIP 電話をリセットします。

SIP プロファイルの設定

はじめる前に

- SIP 電話のセキュア ポートの設定, （380 ページ）
- サービスの再起動, （380 ページ）

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 [検索（Find）] をクリックします。

ステップ 3 プロファイルをコピーする場合は、[コピー（Copy）] 列のファイル アイコンをクリックします。

ステップ 4 新しいプロファイルの名前と説明を入力します。

ステップ 5 Cisco Unity Connection が Cisco Unified Communications Manager との通信に IPv6 または IPv4/IPv6 デュアル スタックを使用する場合は、[ANAT を有効化（Enable ANAT）] チェックボックスをオンにします。
この手順は、IPv6 またはデュアル スタック環境で発信者を適切に処理するために必要です。

ステップ 6 [保存（Save）] をクリックします。

次の作業

電話セキュリティ プロファイルの設定, （382 ページ）

電話セキュリティ プロファイルの設定

Cisco Unified Communications Manager は、自動登録用の事前に定義された非セキュアなセキュリティ プロファイル一式を提供します。電話のセキュリティ機能を有効にするには、新しいセキュリティプロファイルを設定し、それを電話に適用する必要があります。新しいセキュリティプロファイルを設定するには、次の手順を実行します。

はじめる前に

SIP 電話を設定する場合は、次の手順を完了します。

- SIP 電話のセキュア ポートの設定, （380 ページ）
- サービスの再起動, （380 ページ）
- SIP プロファイルの設定, （381 ページ）

SCCP 電話を設定する場合は、次の手順を開始する前に完了しておく前提条件はありません。

手順

ステップ 1 Cisco Unified CM の管理から、[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）] 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 [電話セキュリティ プロファイルのタイプ（Phone Security Profile Type）] ドロップダウン リストから、作成するプロファイルのタイプを選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 [電話セキュリティ プロファイルのプロトコルの選択（Select the phone security profile protocol）] ドロップダウン リストから、プロトコルを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Name] フィールドにプロファイルの適切な名前を入力します。

ステップ 8 プロファイルに関する簡単な説明を入力します。

ステップ 9 [保存（Save）] をクリックします。

次の作業

SIP および SCCP の両方の電話について：

サードパーティ SIP エンドポイントの追加, （427 ページ）

電話の設定

Cisco Unified Communications Manager データベースに電話を手動で追加するには、次の手順を実行します。自動登録を使用している場合は、次の手順を実行する必要はありません。自動登録を選択すると、Cisco Unified Communications Manager が自動的に電話を追加し、電話番号を割り当てます。自動登録の有効化の詳細については、「自動登録の設定タスク フロー, （606 ページ）」を参照してください。

はじめる前に

- 電話用 NTP リファレンスの追加, （52 ページ）
- 電話セキュリティ プロファイルの設定, （382 ページ）
- 日時グループの追加, （53 ページ）
- SIP ダイヤル ルールの設定, （183 ページ） （SIP 電話を設定する場合）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [電話タイプ（Phone Type）] ドロップダウンリストから、該当する Cisco IP Phone モデルを選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 [デバイス プロトコルの選択（Select the device protocol）] ドロップダウンリストから、次のいずれかを選択します。

- SCCP
- SIP

ステップ 6 [Next] をクリックします。

ステップ 7 [電話の設定（Phone Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

（注） セキュリティプロファイルで設定されている CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウに表示される Certificate Authority Proxy Function の設定に関係するものです。製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）に関連する証明書操作の CAPF 設定を設定する必要があります。電話の設定ウィンドウで更新する CAPF 設定がセキュリティプロファイルの CAPF 設定に与える影響の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』を参照してください。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [関連付け（Association）] エリアで、[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] をクリックします。

ステップ 10 [電話番号（Directory Number）] フィールドに、電話機に関連付ける電話番号を入力します

ステップ 11 [保存（Save）] をクリックします。

次の作業

SIP または SCCP 電話の場合：

Cisco Unified IP Phoneサービスの設定, （384 ページ）

Cisco Unified IP Phoneサービスの設定

Cisco Unified IP Phone に、社員名簿、ビジュアル ボイスメール、天気予報などの電話サービスを提供する場合、Cisco Unified IP Phone 用サービスを設定します。Cisco Unified Communications Manager とともに自動でインストールされるデフォルト IP Phone サービスを利用できます。また、サイトに対してカスタマイズされた Cisco Unified IP Phone サービスも作成できます。カスタマイズ サービスを Cisco Unified Communications Manager に設定するために次の手順を実行します。

はじめる前に

電話の設定, （383 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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）] をクリックします。

ステップ 3 [IP フォン サービスの設定（IP Phone Services Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

- エンタープライズ サブスクリプションとしてサービスが分類されていない場合は、データベースで電話にサービスを追加します。Bulk Administrative Tool（BAT）または Cisco Unified Communications セルフ ケア ポータルを使用して電話にサービスを追加できます。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある *Cisco Unified Communications Manager Bulk Administration* ガイド および http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/

products-user-guide-list.html にある、*Cisco Unified Communications Self Care Portal User Guide* を参照してください。

- 電話ボタンにサービスを割り当てることができます（電話モデルがこれらのボタンをサポートする場合）。サービスの割り当てについて詳細は、電話モデルの、Cisco Unified IP Phone ユーザ ガイドを参照してください。
- VPN クライアントを設定します（任意）。

EnergyWise の設定

はじめる前に

- システムにEnergyWiseコントローラが含まれることを確認します。たとえば、Cisco製スイッチは有効な EnergyWise 機能を備えています。
- 使用している電話機モデルがEnergyWise機能をサポートするかどうかを確認するには、電話機モデルのユーザ マニュアルを参照してください。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 検索条件を指定し、[検索（Find）] をクリックします。
Cisco Unified Communications Manager で設定されている電話機の一覧が表示されます。

ステップ 3 EnergyWise 機能を設定する電話を選択します。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの EnergyWise 関連フィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクションを参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

EnergyWise の設定フィールド, （386 ページ）

EnergyWise の設定フィールド

表 *46*：*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）	電話を自動的に電源オフにする日付を選択します。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、複数の日付を選択できます。 デフォルトでは、どの日も選択されていません。
電話機をオンにする時刻（Phone On Time）	24 時間形式で時間を入力します。00:00 は午前 0 時を表します。この値は、[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択した日に、電話の電源を自動的にオンにする時刻を決定します。 （注） 電話を [電話をオンにする時刻（Phone On Time）] の前に復帰させるには、電話の電源をスイッチからオンにする必要があります。詳細については、スイッチのマニュアルを参照してください。
電話機をオフにする時刻（Phone Off Time）	24 時間形式で時間を入力します。00:00 は午前 0 時を表します。この値は、[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択した日に、電話の電源を自動的にオフにする時刻を決定します。[電話をオンにする時刻（Phone On Time）] フィールドと [電話をオフにする時刻（Phone Off Time）] フィールドに同じ値が含まれている場合、電話はオフになりません。
電話機をオフにするアイドル タイムアウト（Phone Off Idle Timeout）	電話の電源をオフにする前に、電話をアイドル状態にしておく必要がある時間の長さを示します。20 ～ 1440 分の範囲の値を指定できます。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）	このチェックボックスをオンにすると、[電話をオフにする時刻（Phone Off Time）] で指定した時刻の 10 分前に電話で可聴アラートが再生されます。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）	電話が存在している EnergyWise ドメインを指定します。許容最大長は 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 シークレット パスワードを指定します。許容最大長は 127 文字です。
EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）	Power Save Plus を無効にするには、この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すると、EnergyWise ドメイン コントローラ ポリシーによって、[電源をオンにする時刻（Power On Time）] および [電源をオフにする時刻（Power Off Time）] の値がオーバーライドされます。 （注） [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のままにしておくと、Power Save Plus は無効になりません。

クライアント サービス フレームワーク デバイスの設定

クライアント サービス フレームワーク デバイスを設定するには、次の手順を実行します。Cisco Unified Client Services Framework デバイスは、次のいずれかになります。

- Cisco Unified Communications Integration for Microsoft Office Communicator
- Cisco Unified Communications Integration for WebEx Connect
- Cisco Unified Personal Communicator（リリース 8.0 以降）

手順

	コマンドまたはアクション	目的
ステップ 1	クライアント サービス フレームワーク デバイスの追加, （388 ページ）	クライアント サービス フレームワークを使用するデバイスを追加します。
ステップ 2	エンドユーザとデバイスの関連付け, （390 ページ）	クライアント サービス フレームワーク デバイスにエンド ユーザのアカウントを関連付けます。

クライアント サービス フレームワーク デバイスの追加

手順

ステップ 1 Cisco Unified CM の管理から、[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 [電話のタイプ（Phone Type）] ドロップダウン リストから、[Cisco Unified Client Services Framework] を選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 [電話の設定（Phone Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [関連付け（Association）] エリアで、[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] をクリックします。

ステップ 8 [電話番号（Directory Number）] フィールドに、クライアント サービス フレームワーク デバイスに関連付ける電話番号を入力します。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

クライアント サービス フレームワーク デバイスの設定フィールド, （389 ページ）

クライアント サービス フレームワーク デバイスの設定フィールド

表 47 : クライアント サービス フレームワーク デバイスの設定フィールド

フィールド	説明
デバイス名（Device Name）	クライアント サービス フレームワーク デバイスを識別する名前を入力します。この名前には、最長 15 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。 （注） Cisco Unified Personal Communicator のデバイス名を設定する場合は、名前が UPC で始まっていることを確認します。
説明	デバイスの簡単な説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。
[デバイスプール（Device Pool）]	このデバイスを割り当てるデバイス プールを選択します。
電話ボタンテンプレート（Phone Button Template）	[標準クライアント サービス フレームワーク（Standard Client Services Framework）] を選択します。
[オーナーのユーザID（Owner User ID）]	割り当てられたクライアント サービス フレームワーク デバイスのユーザのユーザ ID を選択します。ユーザ ID は、呼詳細レコード（CDR）で、このデバイスから発信されるすべてのコールに対して記録されます。
デバイスのセキュリティ プロファイル（Device Security Profile）	[Cisco Unified Client Services Framework：標準非セキュア プロファイル（Cisco Unified Client Services Framework - Standard SIP Non-secure Profile）] を選択します。
[SIPプロファイル（SIP Profile）]	[標準 SIP プロファイル（Standard SIP Profile）] を選択します。

エンドユーザとデバイスの関連付け

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザの管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 2 [ユーザを次の条件で検索（Find Users Where）] フィールドで適切なフィルタを指定した後、[検索（Find）] をクリックしてユーザのリストを取得します。

ステップ 3 ユーザを一覧から選択します。

ステップ 4 [デバイス情報（Device Information）] セクションを探します。

ステップ 5 [デバイスの割り当て（Device Association）] をクリックします。
[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 6 デバイスを探して選択します。

ステップ 7 関連付けを完了するには、[選択/変更の保存（Save Selected/Changes）] をクリックします。

ステップ 8 [関連リンク（Related Links）] ドロップダウン リスト ボックスで [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、割り当てたデバイスが、[制御するデバイス（Controlled Devices）] ペインに表示されます。

CTI リモート デバイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	CTI リモート デバイスの設定, （391 ページ）	CTI リモート デバイスを作成します。
ステップ 2	デバイスへの電話番号の追加, （395 ページ）	CTI リモート デバイスを登録するには、そのデバイスに電話番号を追加する必要があります。
ステップ 3	リモート接続先の設定, （396 ページ）	CTI リモートデバイスと関連付けるリモート接続先を設定します。

CTI リモート デバイスの設定

手順

ステップ 1 Cisco Unified CM の管理から、[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 [電話のタイプ（Phone Type）] ドロップダウン リストから [CTI リモート デバイス（CTI Remote Device）] を選択して、[次へ（Next）] をクリックします。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

CTI リモート デバイス設定フィールド, （391 ページ）

CTI リモート デバイス設定フィールド

CTI リモート デバイス情報

表 *48* : *[デバイス情報（Device Information）]*

フィールド	説明
登録	CTI リモート デバイスの登録ステータスを指定します。
デバイスの状態（Device Status）	デバイスがアクティブか非アクティブかを指定します。
デバイスの信頼	デバイスが信頼できるかどうかを指定します。
アクティブなリモート接続先	アクティブなリモート接続先かどうかを指定します。CTI クライアントは、任意の 1 つの時点で 1 つのリモート接続先を指定できます。着信コールと Dial via Office（DVO）コールは、アクティブなリモート接続先に転送されます。
[オーナーのユーザID（Owner User ID）]	ドロップダウン リストから、割り当てられた電話ユーザのユーザ ID を選択します。ユーザ ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。

フィールド	説明
デバイス名（Device Name）	所有者のユーザ ID に基づいて自動的に入力される CTI のリモートデバイスの名前を指定します。 デバイス名の形式は、デフォルトで CTIRD<OwnerUserID> です。 このフィールドは編集できます。デバイス名は最大 15 文字で指定できます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。
説明	CTI リモートデバイスの説明テキストを入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。
[デバイスプール（Device Pool）]	CTI のリモートデバイスの一般的な特性を定義するデバイス プールを選択します。 デバイスプールを設定する方法の詳細については、「デバイスプール設定」を参照してください。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストから、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
ユーザ保留 MOH 音源（User Hold MOH Audio Source）	ドロップダウンリストから、ユーザが保留操作を開始したときの保留音（MOH）に使用するオーディオ ソースを選択します。
ネットワーク保留 MOH 音源（Network Hold MOH Audio Source）	ドロップダウンリストから、ネットワークが保留操作を開始したときの MOH に使用するオーディオ ソースを選択します。
参照先	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーション CSS に、このデバイス プールに割り当てる発呼側トランスフォーメーションパターンが含まれていることを確認してください。
プレゼンテーションインジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）	コール単位でコール表示制限を設定する場合は、この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すると、Cisco Unified CM は内線コールに対して受信したすべての表示制限を無視します。

[コールルーティング情報（Call Routing Information）]

表 *49*：着信/発信コール情報

フィールド	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーション CSS に、このデバイスに割り当てる発呼側トランスフォーメーションパターンが含まれていることを確認してください。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイスプールに設定されている発信側変換 CSS を使用する場合は、この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場合、デバイスは [トランクの設定（Trunk Configuration）] ウィンドウで設定した発信側変換 CSS を使用します。

表 *50*：*[プロトコル固有情報（Protocol Specific Information）]*

フィールド	説明
プレゼンス グループ（Presence Group）	プレゼンス機能でこのフィールドを設定します。 このアプリケーションユーザをプレゼンス機能とともに使用していない場合は、プレゼンス グループの設定をデフォルトの[なし（None）]のままにします。 ドロップダウン リストから、アプリケーション ユーザのプレゼンス グループを選択します。選択したグループは、IPMASysUserなどのアプリケーション ユーザが監視できる宛先を指定します。
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンド ユーザから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンドユーザのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンド ユーザのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified CM の管理で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBE コーリング サーチ スペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザ用に別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは[なし（None）]に設定されます。 この目的専用の SUBSCRIBE コーリング サーチ スペースを設定するには、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定します。

フィールド	説明
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	ドロップダウンリストから、再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチスペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチスペースが原因で参照メッセージが失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージを表示して要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティングコーリングサーチスペースを使用して、リダイレクト先または転送先を検索します。

表 *51*：サイレントの情報

フィールド	説明
[サイレント（Do Not Disturb）]	リモートデバイスのサイレント機能をイネーブルにする場合は、このチェックボックスをオンにします。
DND オプション（DND Option）	電話機でDNDを有効にすると、[着信拒否（Call Reject）] オプションの指定により、着信コール情報がユーザに表示されなくなります。[DND 着信呼警告（DND Incoming Call Alert）] パラメータの設定に応じて、電話はビープを再生するか、コールの点滅通知を表示します。

デバイスへの電話番号の追加

CTI リモート デバイスを登録するには、そのデバイスに電話番号を追加する必要があります。電話番号のない CTI リモート デバイスを登録することはできません。CTI リモート デバイスには最大 5 つの電話番号を追加できます。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 フィルタ条件を指定して、電話番号を関連付ける CTI リモート デバイスをクリックします。

ステップ 3 [関連付け（Association）] ペインで、[新しい DN を追加（Add a new DN）] リンクをクリックします。

ステップ 4 [電話番号の設定（Directory Number Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

リモート接続先の設定

CTI のリモート デバイスに 1 つ以上のリモート接続先を設定できます。リモート接続先とは、リモート接続先ピックアップ（ユーザのデスクの電話機から転送を受け入れる）を実行し、Cisco Unified Mobility の着信コールを受け入れるように、設定できるモバイルなどの電話機です。CTI のリモートデバイスに関連付けられているリモート接続先では、リモートデバイスに到達するための電話番号を指定します。CTI のリモート デバイスに設定可能なリモート接続先の最大数は、オーナーのユーザ ID に設定されたリモート接続先の制限値で決まります。

リモート接続先には次のデバイスを登録できます。

- シングルモード携帯（セルラー）電話
- スマートフォン
- デュアルモード電話
- デスクの電話機と同じクラスタにないエンタープライズ IP フォン
- PSTN 内の自宅の電話番号

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] > [CTI リモート デバイス（CTI Remote Device）] > [関連付けられたリモート接続先（Associated Remote Destinations）] を選択します。

ステップ 2 フィルタ条件を指定して、リモート接続先を設定する CTI のリモート デバイスをクリックします。

ステップ 3 [関連付けられたリモート接続先（Associated Remote Destinations）] ペインで [新規リモート接続先の追加（Add a New Remote Destination）] を選択します。
あるいは、[デバイス（Device）] > [電話（Phone）] > [新規追加（Add New）] メニュー パスを使用して、リモート接続先を設定できます。

ステップ 4 [リモート接続先の設定（Remote Destination Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクションを参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

リモート接続先の設定フィールド, （397 ページ）

リモート接続先の設定フィールド

表 *52*：リモート接続先の設定フィールド

フィールド	説明
[名前（Name）]	リモート接続先の名前を入力します。
宛先番号	企業内からダイヤルする番号を入力します。外部の回線に到達するために必要な市外局番および追加するすべての桁を含めます。最大フィールド長は、24 文字で、文字には 0 ～ 9、*、#、+ の値を使用できます。リモート接続先の発信者 ID を設定することを推奨します。
[オーナーのユーザID（Owner User ID）]	ドロップダウン リストから、リモート接続先のオーナーを選択します。
[Unified Mobility 機能を有効にする（Enable Unified Mobility features）]	Unified Mobility 機能を有効にするにはチェックボックスをオンにします。
リモート宛先プロファイル	ドロップダウン リストから、設定したプロファイルを選択します。
[シングルナンバー リーチを有効にする（Enable Single Number Reach）]	リモート接続先のシングル ナンバー リーチを有効にするには、このチェックボックスをオンにします。
[携帯電話への移動を有効にする（Enable Move to Mobile）]	これはオプションのフィールドです。電話機が携帯電話の場合は、このチェックボックスをオンにします。

Cisco Spark リモート デバイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Spark リモート デバイスの設定, （398 ページ）	Cisco Spark リモート デバイスを作成します。
ステップ 2	Cisco Spark デバイスへの電話番号の追加, （403 ページ）	Cisco Spark リモート デバイスを登録するには、そのデバイスに電話番号を追加する必要があります。

Cisco Spark リモート デバイスの設定

手順

ステップ 1 Cisco Unified CM の管理から、[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 [電話のタイプ（Phone Type）] ドロップダウン リストから、[Cisco Spark リモート デバイス（Cisco Spark Remote Device）] を選択して、[次へ（Next）] をクリックします。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次の作業

関連トピック

Cisco Spark リモート デバイス設定フィールド, （398 ページ）

Cisco Spark リモート デバイス設定フィールド

表 *53* : *Cisco Spark* リモート デバイス設定フィールド

フィールド	説明
[デバイス情報（Device Information）]	
登録	Cisco Spark リモート デバイスの登録ステータスを指定します。

フィールド	説明
デバイスの状態（Device Status）	デバイスがアクティブか非アクティブかを指定します。
[デバイスの信頼性（Device Trust）]	デバイスを信頼できるか信頼できないかを指定します。
[アクティブなリモート接続先（Active Remote Destination）]	リモート接続先がアクティブであるかどうかを指定します。デフォルトでは、Cisco Spark クライアントのアクティブなリモート接続先は 1 つだけです。着信コールはすべてアクティブなリモート接続先にルーティングされます。このフィールドは、アクティブなリモート接続先に関連付けられている場合でも [なし（None）] に設定されます。
[オーナーのユーザID（Owner User ID）]	ドロップダウンリストから、割り当てられた電話ユーザのユーザ ID を選択します。ユーザ ID は、このデバイスから発信されるすべてのコールの呼詳細レコード（CDR）に記録されます。
デバイス名（Device Name）	[オーナーのユーザ ID（Owner User ID）] に基づいて自動的に入力される Cisco Spark リモートデバイスの名前を使用します。 デフォルトでは、デバイス名の形式は *SparkRD<OwnerUserID>* です。デフォルトのデバイス名 *SparkRD* は変更できません。 このフィールドは編集できます。デバイス名は最大 15 文字で指定できます。使用できる文字は、英字、数字、ダッシュ（-）、ピリオド、スペース、およびアンダースコアです。
説明	Cisco Spark リモートデバイスの説明テキストを入力します。 このフィールドには、128 文字までの値を入力できます。二重引用符（"）、山カッコ（<>）、バックスラッシュ（\）、アンパサンド（&）、パーセント記号（%）を除くすべての文字を使用できます。

フィールド	説明
[デバイスプール（Device Pool）]	Cisco Spark リモート デバイスの共通の特性を定義するデバイス プールを選択します。 デバイスプールの設定方法の詳細については、「デバイスプールの構成時の設定」を参照してください。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストから、コーリング サーチ スペースを選択するか、コーリング サーチ スペースをデフォルトの [なし（None）] のままにします。
ユーザ保留 MOH 音源（User Hold MOH Audio Source）	ドロップダウンリストから、ユーザが保留操作を開始したときの保留音（MOH）に使用するオーディオ ソースを選択します。 **注意** 現在、Cisco Spark リモート デバイスには保留/復帰機能が実装されていないため、MOH はサポートされていません。
ネットワーク保留 MOH 音源（Network Hold MOH Audio Source）	ドロップダウンリストから、ネットワークで保留操作が開始されたときの MOH に使用するオーディオ ソースを選択します。 **注意** 現在、Cisco Spark リモート デバイスには保留/復帰機能が実装されていないため、MOH はサポートされていません。
参照先	ドロップダウン リストから、デバイス プール内の電話およびゲートウェイと関連付けられている場所を選択します。
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーション CSS に、このデバイス プールに割り当てる発呼側トランスフォーメーションパターンが含まれていることを確認してください。
プレゼンテーションインジケータを無視（内線コールのみ）（Ignore Presentation Indicators (internal calls only)）	コール単位でコール表示制限を設定する場合は、この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すると、Cisco Unified CM は内線コールに対して受信したすべての表示制限を無視します。
[コールルーティング情報（Call Routing Information）]	

フィールド	説明
着信コールと発信コールの情報	
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この設定により、デバイスの発信者番号をローカライズできます。選択した発呼側トランスフォーメーションCSSに、このデバイスに割り当てる発呼側トランスフォーメーションパターンが含まれていることを確認してください。
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	このデバイスに割り当てられているデバイスプールに設定されている発呼側トランスフォーメーションCSSを使用する場合は、この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場合、デバイスは [トランクの設定（Trunk Configuration）] ウィンドウで設定した発呼側トランスフォーメーションCSSを使用します。
[プロトコル固有情報（Protocol Specific Information）]	
プレゼンス グループ（Presence Group）	プレゼンス機能でこのフィールドを設定します。 このアプリケーションユーザをプレゼンス機能とともに使用していない場合は、プレゼンスグループの設定をデフォルトの [なし（None）] のままにします。 ドロップダウンリストから、アプリケーションユーザのプレゼンスグループを選択します。選択したグループで、そのアプリケーションユーザ（IPMASysUser など）がモニタできる接続先を指定します。 **注意** 現在、プレゼンス グループは Cisco Spark リモート デバイスではサポートされていません。

フィールド	説明
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	プレゼンス機能によってサポートされるSUBSCRIBEコーリング サーチ スペースによって、Cisco Unified Communications Manager がエンド ユーザから発信されるプレゼンス要求をルーティングする方法が決まります。この設定では、エンド ユーザのプレゼンス（SUBSCRIBE）要求のコール処理サーチ スペースとは別にコーリング サーチ スペースを適用できます。 ドロップダウン リストから、エンド ユーザのプレゼンス要求に使用するSUBSCRIBEコーリング サーチ スペースを選択します。Cisco Unified CMの管理で設定するすべてのコーリング サーチ スペースが、[SUBSCRIBEコーリング サーチ スペース（SUBSCRIBE Calling Search Space）] ドロップダウン リストに表示されます。 ドロップダウン リストから、エンド ユーザ用に別のコーリング サーチ スペースを選択しない場合、SUBSCRIBEコーリング サーチ スペースのデフォルトは[なし（None）]に設定されます。 この目的専用のSUBSCRIBEコーリング サーチ スペースを設定する場合は、他のコーリング サーチ スペースと同様に新しいコーリング サーチ スペースを設定できます。 **注意** 現在、SUBSCRIBEコーリング サーチ スペースはCisco Sparkリモート デバイスではサポートされていません。

フィールド	説明
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	ドロップダウンリストから、再ルーティングに使用するコーリング サーチ スペースを選択します。 リファラーの再ルーティング コーリング サーチスペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチスペースが原因で参照メッセージが失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージを表示して要求を拒否します。 リダイレクト（3xx）プリミティブおよび転送機能も再ルーティングコーリングサーチスペースを使用して、リダイレクト先または転送先を検索します。
サイレントの情報	
[サイレント（Do Not Disturb）]	リモートデバイスのサイレント機能を有効にするには、このチェックボックスをオンにします。 **注意** DND オプションが有効になっている場合、コールは Cisco Spark クライアントにはルーティングされません。 **注意** 現在、サイレント機能は Cisco Spark リモート デバイスではサポートされていません。
DND オプション（DND Option）	電話機で DND を有効にすると、[着信拒否（Call Reject）] オプションの指定により、着信コール情報がユーザに表示されなくなります。[DND 着信呼警告（DND Incoming Call Alert）] パラメータの設定に応じて、電話はビープを再生するか、コールの点滅通知を表示します。 **注意** 現在、サイレント機能は Cisco Spark リモート デバイスではサポートされていません。

Cisco Spark デバイスへの電話番号の追加

Cisco Spark リモート デバイスを登録するには、そのデバイスに電話番号を追加します。電話番号のない Cisco Spark リモート デバイスを登録することはできません。Cisco Spark リモート デバイスには最大 5 つの電話番号を追加できます。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 フィルタの条件を指定して、電話番号を関連付ける Cisco Spark のリモートデバイスをクリックします。

ステップ 3 [関連付け（Association）] ペインで、[新規 DN を追加（Add a new DN）] リンクをクリックします。

ステップ 4 [電話番号の設定（Directory Number Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

電話データを移行

手順

	コマンドまたはアクション	目的
ステップ 1	電話テンプレートの作成, （404 ページ）	一括管理ツール（BAT）で、データを移行する電話モデルおよびプロトコルの電話テンプレートを作成します。
ステップ 2	電話データを移行, （405 ページ）	別の電話に電話データを移行します。

電話テンプレートの作成

手順

ステップ 1 Cisco Unified CM の管理から、[一括管理（Bulk Administration）] > [電話（Phones）] > [電話テンプレート（Phone Template）] 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。
[新しい電話テンプレートの追加（Add a New Phone Template）] ウィンドウが表示されます。

ステップ 3 [電話タイプ（Phone Type）] ドロップダウンリストから、テンプレートを作成する電話モデルを選択します。[Next] をクリックします。

ステップ 4 [デバイス プロトコルの選択（Select the device protocol）] ドロップダウンリストから、デバイス プロトコルを選択します。[Next] をクリックします。

[電話テンプレートの設定（Phone Template Configuration）] ウィンドウに、選択したデバイス タイプのフィールドとデフォルト エントリが表示されます。

ステップ 5 [電話テンプレートの設定（Phone Template Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

電話データを移行

はじめる前に

- 電話機をネットワークから切り離します。
- 新しい電話について、十分なデバイス ライセンス ユニットがあることを確認します。
- 電話機モデルが電話移行をサポートしていることを確認します。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 検索条件を指定して、[検索（Find）] をクリックします。

ステップ 3 移行する電話設定を選択してクリックします。

ステップ 4 [関連リンク（Related Links）] ドロップダウンリストで [電話を移行（Migrate Phone）] を選択します。
[電話の移行設定（Phone Migration Configuration）] ウィンドウが表示されます。

ステップ 5 ドロップダウン リストから、電話設定を移行する電話モデルの電話テンプレートを選択します。

ステップ 6 設定を移行する新しい Cisco Unified IP Phone の [Media Access Control（MAC）アドレス（Media Access Control (MAC) address）] を入力します。MAC アドレスは、12 桁の 16 進数文字を含んでいる必要があります。

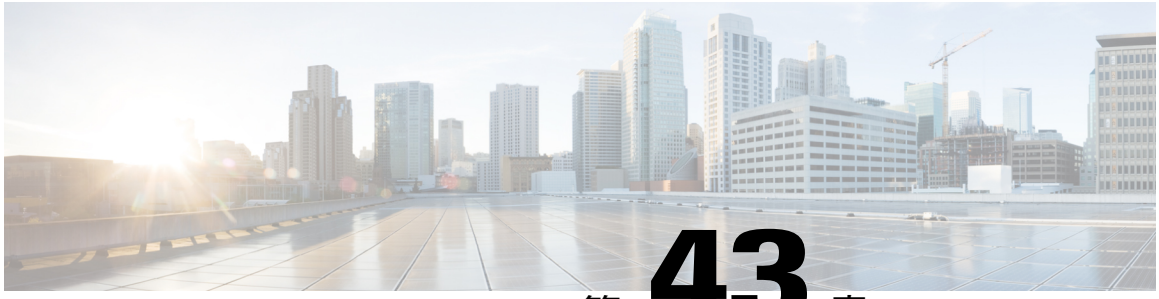
ステップ 7 （オプション）新しい電話の説明を入力します。説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 新しい電話機は機能が失われる可能性があるという警告が表示されたら、[OK] をクリックします。

次の作業

新しい電話機をネットワークに接続し、デバイスを登録します。



第 43 章

Cisco Unified IP Phone の診断とレポートの設定

- 診断およびレポートの概要，407 ページ
- 前提条件，408 ページ
- 診断およびレポート設定タスク フロー，410 ページ

診断およびレポートの概要

Cisco Unified Communications Manager には、Cisco IP Phone の通話品質を保証するためのオプションが 2 つあります。

- コール診断：コール診断には、コール管理レコード（CMR）および音声品質メトリックの生成が含まれます。
- 品質レポート ツール（QRT）：QRT は、Cisco Unified 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。このツールを使用することで、ユーザはIP フォンで生じる音声やその他の一般的な問題を簡単かつ正確に報告できます。

コール診断の概要

SCCP と SIP を実行している Cisco Unified IP Phone は、コール診断を収集するように設定できます。コール診断は、呼管理レコード（CMR）で構成され、診断レコード、音声品質メトリックとも呼ばれます。

音声品質メトリックはデフォルトで有効になっており、大半の Cisco Unified IP Phone でサポートされています。Cisco Unified IP Phone は、MOS（平均オピニオン スコア）値に基づいて、音声品質メトリックを計算します。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。

CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。CMR を生成するように、Cisco Unified Communications Manager を設定できます。この情報は、課金記録の生成やネットワーク分析などの後処理作業に役立ちます。

品質レポート ツールの概要

品質レポート ツール（QRT）は、Cisco Unified 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。このツールを使用することで、ユーザは IP フォンで生じる音声やその他の一般的な問題を簡単かつ正確に報告できます。

システム管理者は、ユーザの IP フォンに QRT ソフトキーを表示するソフトキー テンプレートを設定して割り当てることで、QRT 機能を有効化できます。QRT を使用して行うユーザ インタラクションのレベルに応じて、2 つの異なるユーザ モードを選択できます。次に、システムパラメータを設定し、Cisco Unified Serviceability ツールを設定することで、このツールの機能方法を定義します。QRT Viewer アプリケーションを使用して、電話の問題レポートを作成、カスタマイズ、および表示できます。

IP フォンに問題が発生しているユーザは、コール状態が [オンフック（On Hook）] または [接続中（Connected）] の間に、Cisco Unified IP Phone の QRT ソフトキーを押して、問題の種類や他の関連する統計情報を報告できます。ユーザは IP フォンで報告されている問題を最もよく表している理由コードを選択できます。カスタマイズされた電話の問題レポートには、具体的な情報が表示されます。

ユーザが QRT ソフトキーを押して問題の種類を選択すると、QRT はストリーミングの統計情報を収集しようとします。ストリーミングの統計情報を収集するには、QRT でコールを 5 秒以上アクティブにする必要があります。

前提条件

コール診断の前提条件

Cisco Unified IP Phone がコール診断をサポートしているかどうかを確認します。

次の表を使用して、電話がコール診断をサポートしているかどうかを判断します。コール診断のサポートの凡例は次のとおりです。

- X：SCCP と SIP の両方を実行している電話機によるサポート
- S：SCCP 機能のみ

表 *54*：コール診断のデバイスのサポート

Device	コール診断のサポート
Cisco Unified IP Phone 7906	X
Cisco Unified IP Phone 7911	X

Device	コール診断のサポート
Cisco Unified IP Phone 7921	X
Cisco Unified IP Phone 7931	X
Cisco Unified IP Phone 7940	S
Cisco Unified IP Phone 7941	X
Cisco Unified IP Phone 7942-G	X
Cisco Unified IP Phone 7942-G/GE	X
Cisco Unified IP Phone 7945	X
Cisco Unified IP Phone 7960	S
Cisco Unified IP Phone 7961	X
Cisco Unified IP Phone 7962-G	X
Cisco Unified IP Phone 7962-G/GE	X
Cisco Unified IP Phone 7965	X
Cisco Unified IP Phone 7970	X
Cisco Unified IP Phone 7971	X
Cisco Unified IP Phone 7972-G/GE	X
Cisco Unified IP Phone 7975	X

Quality Report Tool の前提条件

次の機能が含まれる Cisco IP Phone：

- ソフトキー テンプレートのサポート
- IP 電話サービスのサポート
- CTI による制御可能
- 内部 HTTP サーバを含む

詳細については、お使いの電話モデルのガイドを参照してください。

診断およびレポート設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	コール診断の設定, （411 ページ）	Cisco Unified Communications Manager が CMR を生成するように設定するには、このタスクを実行します。CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。CMR へのアクセス方法の詳細については、『*Cisco Unified Communications Manager Call Detail Records Administration Guide*』を参照してください。 音声品質メトリックはCisco IP Phone で自動的に有効になります。音声品質メトリックへのアクセス方法の詳細については、電話機モデルの『Cisco Unified IP Phone アドミニストレーション ガイド』を参照してください。
ステップ 2	品質レポート ツールの設定, （411 ページ）を行うには、次のサブタスクを実行します。 • QRT ソフトキーのソフトキー テンプレートの設定, （412 ページ） • QRT ソフトキー テンプレートと共通デバイス設定の関連付け, （414 ページ） • 電話機への QRT ソフトキー テンプレートの追加, （416 ページ） • Cisco Unified Serviceability での QRT の設定, （416 ページ） • 品質レポート ツールのサービス パラメータの設定, （420 ページ）	IP フォンで問題が発生したユーザが、QRT ソフトキーを押して、問題のタイプや他の関連統計情報を報告できるように、品質レポート ツール（QRT）を設定します。

コール診断の設定

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）]>[サービス パラメータ（Service Parameters）] の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、Cisco CallManager サービスを実行しているサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。
[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウが開きます。

ステップ 4 [クラスタ全体のパラメータ（デバイス - 全般）（Clusterwide Parameters (Device - General)）] エリアで、[コール診断有効（Call Diagnostics Enabled）] サービス パラメータを設定します。次のオプションを使用できます。

- 無効（Disabled）：CMR は生成されません。
- CDR有効フラグが True の場合のみ有効化（Enabled Only When CDR Enabled Flag is True）：[呼詳細レコード（CDR）有効化フラグ（Call Detail Records (CDR) Enabled Flag ）] サービス パラメータが True に設定されている場合のみ、CMR が生成されます。
- CDR 有効化フラグに関係なく有効化（Enabled Regardless of CDR Enabled Flag）：[CDR 有効化フラグ（CDR Enabled Flag）] サービス パラメータの値に関係なく、CMR が生成されます。

（注） [CDR有効化フラグ（CDR Enabled Flag）] サービス パラメータを有効にせずに CMR を生成すると、制御されずにディスク容量が消費される場合があります。CMR を有効にする場合は、CDR を有効にすることをお勧めします。

ステップ 5 [保存（Save）] をクリックします。

品質レポート ツールの設定

IP フォンで問題が発生したユーザが、QRT ソフトキーを押して、問題のタイプや他の関連統計情報を報告できるように、品質レポート ツール（QRT）を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	QRT ソフトキーのソフトキー テンプレートの設定, （412 ページ）	QRT ソフトキーにオンフックと接続コール状態を設定する必要があります。次のコール状態も使用可能になります。 • 接続された会議

	コマンドまたはアクション	目的
		• 接続転送（Connected Transfer）
ステップ 2	QRT ソフトキーテンプレートと共通デバイス設定の関連付け，（414 ページ）を行うには、次のサブタスクを実行します。 • 共通デバイス設定への QRT ソフトキーテンプレートの追加，（414 ページ） • 電話機と共通デバイス設定の関連付け，（415 ページ）	（任意） ソフトキーテンプレートを電話機で使用可能にするには、この手順または次の手順を実行する必要があります。システムが [共通デバイス設定（Common Device Configuration）] を使用して設定オプションを電話機に適用する場合は、この手順に従います。これは、電話機でソフトキーテンプレートを使用できるようにする際に、最も一般的に使用されている方法です。
ステップ 3	電話機への QRT ソフトキーテンプレートの追加，（416 ページ）	（任意） ソフトキーテンプレートと共通デバイス設定を関連付けるための代替手段として、または共通デバイス設定と共に、次の手順を使用します。ソフトキーテンプレートを適用して、共通デバイス設定での割り当てや、他のデフォルトのソフトキーの割り当てをオーバーライドする必要がある場合は、次の手順を共通デバイス設定と共に使用します。
ステップ 4	Cisco Unified Serviceability での QRT の設定，（416 ページ）を行うには、次のサブタスクを実行します。 • Cisco Extended Functions サービスの有効化，（417 ページ） • アラームの設定，（417 ページ） • トレースの設定，（418 ページ）	
ステップ 5	品質レポート ツールのサービス パラメータの設定，（420 ページ）	（任意）

QRT ソフトキーのソフトキー テンプレートの設定

QRT ソフトキーにオンフックと接続コール状態を設定する必要があります。次のコール状態も使用可能になります。

- 接続された会議

- 接続転送（Connected Transfer）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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 テンプレートの設定（Softkey Template Configuration）] ウィンドウが表示されます。

ステップ 2 新しいソフトキー テンプレートを作成するには、以下のステップを実行します。それ以外の場合は次のステップに進みます。

a) [新規追加（Add New）] をクリックします。
b) デフォルトのテンプレートを選択して、[コピー（Copy）] をクリックします。
c) [ソフトキー テンプレート名（Softkey Template Name）] フィールドに、テンプレートの新しい名前を入力します。
d) [保存（Save）] をクリックします。

ステップ 3 既存のテンプレートにソフトキーを追加するには、以下のステップを実行します。

a) 検索条件を入力して [検索（Find）] をクリックします。
b) 既存のテンプレートを選択します。

[ソフトキー テンプレートの設定（Softkey Template Configuration）] ウィンドウが表示されます。

ステップ 4 [デフォルト ソフトキー テンプレート（Default Softkey Template）] チェックボックスをオンにし、このソフトキー テンプレートをデフォルトのソフトキー テンプレートとして指定します。

（注） あるソフトキー テンプレートをデフォルトのソフトキー テンプレートとして指定した場合、先にデフォルトの指定を解除してからでないと、そのテンプレートは削除することができません。

ステップ 5 右上隅にある [関連リンク（Related Links）] ドロップダウン リストから [ソフトキー レイアウトの設定（Configure Softkey Layout）] を選択し、[移動（Go）] をクリックします。

ステップ 6 [設定するコール状態の選択（Select a Call State to Configure）] ドロップダウン リストから、ソフトキーに表示するコール状態を選択します。

ステップ 7 [選択されていないソフトキー（Unselected Softkeys）] リストから追加するソフトキーを選択し、右矢印をクリックして [選択されたソフトキー（Selected Softkeys）] リストにそのソフトキーを移動します。新しいソフトキーの位置を変更するには、上矢印と下矢印を使用します。

ステップ 8 追加のコール状態のソフトキーを表示するには、上記のステップを繰り返します。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- すでにデバイスに関連付けられているテンプレートを変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。
- 新しいソフトキーテンプレートを作成した場合は、そのテンプレートをデバイスに関連付けた後にデバイスを再起動します。詳細については、「次の作業」の項を参照してください。

次の作業

次のいずれかの手順を実行します。

- 共通デバイス設定への QRT ソフトキー テンプレートの追加, （414 ページ）
- 電話機への QRT ソフトキー テンプレートの追加, （416 ページ）

QRT ソフトキー テンプレートと共通デバイス設定の関連付け

これはオプションです。ソフトキー テンプレートを電話機に関連付ける方法は 2 つあります。

- ソフトキー テンプレートを [電話の設定（Phone Configuration）] に追加する。
- ソフトキー テンプレートを共通デバイス設定に追加する。

ここに示す手順は、ソフトキー テンプレートを共通デバイス設定に関連付ける方法について説明しています。システムが共通デバイス設定を使用して設定オプションを電話機に適用する場合は、この手順に従ってください。これは、電話機でソフトキー テンプレートを使用できるようにする際に、最も一般的に使用されている方法です。

別の方法を使用するには、電話機への QRT ソフトキー テンプレートの追加, （416 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	共通デバイス設定への QRT ソフトキー テンプレートの追加, （414 ページ）	
ステップ 2	電話機と共通デバイス設定の関連付け, （415 ページ）	

共通デバイス設定への *QRT* ソフトキー テンプレートの追加

はじめる前に

QRT ソフトキーのソフトキー テンプレートの設定, （412 ページ）

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）] > [共通デバイス設定（Common Device Configuration）] を選択します。
[共通デバイス設定の検索と一覧表示（Find and List Common Device Configuration）] ウィンドウが表示されます。

ステップ 2 新しい共通デバイス設定を作成し、それにソフトキー テンプレートを関連付けるには、以下の手順を実行します。それ以外の場合は、次のステップに進みます。

a) [新規追加（Add New）] をクリックします。
b) [名前（Name）] フィールドに、共通デバイス設定の名前を入力します。
c) [保存（Save）] をクリックします。

ステップ 3 既存の共通デバイス設定にソフトキー テンプレートを追加するには、以下の手順を実行します。

a) 検索条件を入力して [検索（Find）] をクリックします。
b) 既存の共通デバイス設定を選択します。

[共通デバイス設定（Common Device Configuration）] ウィンドウが表示されます。

ステップ 4 [ソフトキー テンプレート（Softkey Template）] ドロップダウン リストで、使用可能にするソフトキーが含まれているソフトキー テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 新しい共通デバイス設定を作成してその設定をデバイスに関連付けた後に、デバイスを再起動します。詳細については、「次の作業」の項を参照してください。
- すでにデバイスに関連付けられている共通デバイス設定を変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。

次の作業

電話機と共通デバイス設定の関連付け, （415 ページ）

電話機と共通デバイス設定の関連付け

はじめる前に

共通デバイス設定への QRT ソフトキー テンプレートの追加, （414 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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。

ステップ 2 ソフトキー テンプレートを追加する電話機を検索します。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ドロップダウン リストから、新しいソフトキー テンプレートが含まれている共通デバイス設定を選択します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リセット（Reset）] をクリックして、電話機の設定を更新します。

電話機への QRT ソフトキー テンプレートの追加

はじめる前に

QRT ソフトキーのソフトキー テンプレートの設定, （412 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[デバイス（Device）] > [電話（Phone）] を選択します。
[電話の検索/一覧表示（Find and List Phones）] ウィンドウが表示されます。

ステップ 2 [電話の検索/一覧表示（Find and List Phones）] ウィンドウで、[検索（Find）] をクリックします。
Cisco Unified Communications Manager で設定されている電話機の一覧が表示されます。

ステップ 3 電話ボタン テンプレートを追加する電話を選択します。
[電話機の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [電話ボタン テンプレート（Phone Button Template）] ドロップダウン リストで、新しい機能ボタンが含まれる電話ボタン テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。
電話の設定を更新するには[リセット（Reset）] を押すというメッセージ付きのダイアログ ボックスが表示されます。

Cisco Unified Serviceability での QRT の設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Extended Functions サービスの有効化, （417 ページ）	品質レポート ツール（QRT）などの音声品質機能をサポートするには、Cisco Extended Functions サービスを有効化します。
ステップ 2	アラームの設定, （417 ページ）	SysLog ビューア内のアプリケーション ログにエラーを記録するにはQRT のアラームを設定します。この機能はアラーム（アラームの説明と推奨アクション）をログに記録します。SysLog ビューアには Cisco Unified Real-Time Monitoring Tool からアクセスできます。
ステップ 3	トレースの設定, （418 ページ）	音声アプリケーションのトレース情報を記録するには QRT のトレースを設定します。QRT に対してトレースファイルに含める情報を設定したら、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central オプショ

	コマンドまたはアクション	目的
		ンを使用して、トレースファイルを収集および表示できます。

Cisco Extended Functions サービスの有効化

品質レポート ツール（QRT）などの音声品質機能をサポートするには、Cisco Extended Functions サービスを有効化します。

手順

ステップ 1 Cisco Unified Serviceability から、[ツール（Tools）] > [サービスの有効化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、Cisco Extended Functions サービスを有効にするノードを選択します。

ステップ 3 [Cisco Extended Functions] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

次の作業

アラームの設定, （417 ページ）

アラームの設定

SysLog ビューア内のアプリケーション ログにエラーを記録するには QRT のアラームを設定します。この機能はアラーム（アラームの説明と推奨アクション）をログに記録します。SysLog ビューアには Cisco Unified Real-Time Monitoring Tool からアクセスできます。

はじめる前に

Cisco Extended Functions サービスの有効化, （417 ページ）

手順

ステップ 1 Cisco Unified Serviceability から、[アラーム（Alarm）] > [設定（Configuration）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストから、アラームを設定するノードを選択します。

ステップ 3 [サービス グループ（Service Group）] ドロップダウン リストから、[CM サービス（CM Services）] を選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから、[Cisco Extended Functions（Cisco Extended Functions）] を選択します。

ステップ 5 ローカル Syslog と SDI トレースの両方に対して [アラームの有効化（Enable Alarm）] チェックボックスをオンにします。

ステップ 6 ドロップダウン リストから、次のいずれかのオプションを選択して、ローカル Syslog と SDI トレースの両方にアラーム イベント レベルを設定します。

- [緊急（Emergency）]：システムが使用できないことを示します。
- [アラート（Alert）]：ただちに対処が必要であることを示します。
- [クリティカル（Critical）]：システムがクリティカルな状態を検出しています。
- [エラー（Error）]：エラー状態が検出されたことを示します。
- [警告（Warning）]：警告状態が検出されたことを示します。
- [通知（Notice）]：異常ではないが重要な状況が検出されたことを示します。
- [情報（Informational）]：単なる情報メッセージであることを示します。
- [デバッグ（Debug）]：このレベルは、Cisco テクニカル アシスタンス センター（TAC）のエンジニアがデバッグに使用する詳細イベント情報を示します。

デフォルト値は [エラー（Error）] です。

ステップ 7 [保存（Save）] をクリックします。

次の作業

トレースの設定, （418 ページ）

トレースの設定

音声アプリケーションのトレース情報を記録するには QRT のトレースを設定します。QRT に対してトレース ファイルに含める情報を設定したら、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central オプションを使用して、トレース ファイルを収集および表示できます。

はじめる前に

アラームの設定, （417 ページ）

手順

ステップ 1 Cisco Unified Serviceability で、[トレース（Trace）] > [設定（Configuration）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウンリストから、トレースを設定するノードを選択します。

ステップ 3 [サービス グループ（Service Group）] ドロップダウンリストから、[CM サービス（CM Services）] を選択します。

ステップ 4 [サービス（Service）] ドロップダウンリストから、[Cisco 拡張機能（Cisco Extended Functions）] を選択します。

ステップ 5 [トレース オン（Trace On）] チェックボックスをオンにします。

ステップ 6 [トレース レベルのデバッグ（Debug Trace Level）] ドロップダウンリストから、次のいずれかのオプションを選択します。

- [エラー（Error）]：すべてのエラー状態、プロセス、デバイス初期化メッセージをトレースします。
- [特殊（Special）]：通常運用時に発生するすべての特殊状態とサブシステムの状態遷移をトレースします。コール処理イベントをトレースします。
- [状態遷移（State Transition）]：通常運用時に発生するすべての状態遷移の状態とメディア レイヤ イベントをトレースします。
- [重要（Significant）]：すべての重要な状態と、ルーチンの開始および終了ポイントをトレースします。すべてのサービスがこのトレース レベルを使用するわけではありません。
- [開始_終了（Entry_exit）]：すべての開始および終了状態と、詳細なデバッグ情報をトレースします。
- [任意（Arbitrary）]：すべての任意の状態と、詳細なデバッグ情報をトレースします。
- [詳細（Detailed）]：アラームの状態およびイベントをトレースします。異常なパスで生成されたすべてのトレースに使用します。最小の CPU サイクル数を使用します。

デフォルト値は Error です。

ヒント トラブルシューティングを実行するため、このセクションのすべてのチェック ボックスをオンにすることを推奨します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

（オプション） 品質レポート ツールのサービス パラメータの設定, （420 ページ）

品質レポート ツールのサービス パラメータの設定

注意 Cisco Technical Assistance Center（TAC）から指示がある場合を除き、デフォルトのサービス パラメータ設定を使用することを推奨します。

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 QRT アプリケーションが存在するノードを選択します。

ステップ 3 [Cisco Extended Functions] サービスを選択します。

ステップ 4 サービス パラメータを設定します。サービス パラメータとその設定オプションの詳細については、「関連項目」セクションを参照してください。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

品質レポート ツールのサービス パラメータ, （420 ページ）

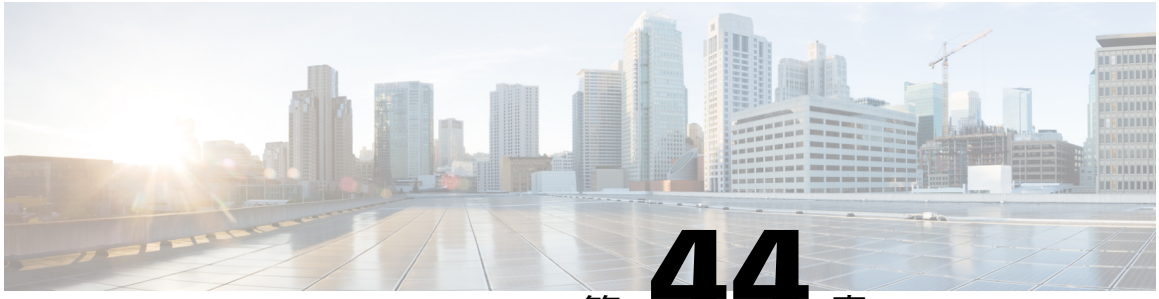
品質レポート ツールのサービス パラメータ

表 *55*：品質レポート ツールのサービス パラメータ

パラメータ	説明
拡張 QRT メニューの選択肢を表示します。	拡張メニューの選択肢がユーザに表示されるかどうかを決定します。次のいずれかの設定オプションを選択できます。 • 拡張メニューの選択肢を表示する（インタビュー モード）には、このフィールドを True に設定します。 • 拡張メニューの選択肢を表示する（サイレント モード）には、このフィールドを False に設定します。 • 推奨されるデフォルト値は False（サイレント モード）です。

パラメータ	説明
ストリーミング統計のポーリング期間	ストリーミング統計のポーリングに使用する期間を決定します。次のいずれかの設定オプションを選択できます。 • コールが終了するまでポーリングするには、このフィールドを -1 に設定します。 • ポーリングを一切行わない場合は、このフィールドを 0 に設定します。 • 任意の秒数の間ポーリングするには、任意の正の値を設定します。コールが終了するとポーリングが停止します。 • 推奨されるデフォルト値は-1（コールが終了するまでポーリングする）です。
ストリーミング統計のポーリング頻度（秒）	各ポーリングの間で待機する秒数を入力します。 値の範囲は 30 ～ 3600 です。推奨デフォルト値は 30 です。
Maximum No. of Files	ファイルのカウントが再起動し、古いファイルを上書きするまでのファイルの最大数を入力します。 有効な値は、1 ～ 10000 です。推奨デフォルト値は 250 です。
Maximum No. of Lines per File	次のファイルを開始する前の各ファイルの最大回線数を入力します。 • 値の範囲は 100 ～ 2000 です。 • 推奨デフォルト値は 2000 です。

パラメータ	説明
CAPF Profile Instance Id for Secure Connection to CTI Manager	CTI マネージャへのセキュアな接続を開くために Cisco Extended Function サービスが使用する、アプリケーション ユーザ CCMQRTSysUser の CAPF アプリケーション プロファイルのインスタンス ID を入力します。CTI Manager Connection Security Flag パラメータが有効な場合、このパラメータを設定する必要があります。 （注） CTI Manager Connection Security Flag サービス パラメータを有効にすることで、セキュリティをオンにします。変更を有効にするためには、Cisco Extended Functions サービスを再起動する必要があります。
CTI Manager Connection Security Flag	Cisco Extended Functions サービスの CTI Manager 接続のセキュリティを有効にするか、または無効にするかを選択します。有効にすると、Cisco Extended Functions はアプリケーション ユーザ CCMQRTSysUser のインスタンス ID に設定された CAPF アプリケーション プロファイルを使用して、CTI マネージャへのセキュアな接続を開きます。 値は True または False を選択します。CTI へのセキュアな接続を有効にするには、True を選択する必要があります。



第 44 章

サードパーティ製 SIP 電話の設定

- サードパーティ製 SIP エンドポイントの概要，423 ページ
- サードパーティ製 SIP エンドポイント設定のタスク フロー，424 ページ

サードパーティ製 SIP エンドポイントの概要

SIP を実行する Cisco Unified IP Phone に加え、Cisco Unified Communications Manager は、さまざまなサードパーティ製 SIP エンドポイントをサポートしています。Cisco Unified Communications Manager の管理ページで、次のサードパーティ製 SIP エンドポイントを設定できます。

- サードパーティ製 SIP デバイス（拡張）：この 8 回線 SIP デバイスは、SIP を実行している、RFC3261 準拠のサードパーティ製電話機です。
- サードパーティ製 SIP デバイス（基本）：この 1 回線 SIP デバイスは、SIP を実行している、RFC3261 準拠のサードパーティ製電話機です。
- サードパーティ製 AS-SIP デバイス：Assured Services SIP（AS-SIP）エンドポイントは、MLPP、DSCP、TLS/SRTP、および IPv6 要件に準拠した SIP エンドポイントです。AS-SIP は、Unified Communications Manager に複数のエンドポイント インターフェイスを提供します。
- Generic Desktop Video Endpoint：この SIP デバイスは、ビデオ、セキュリティ、設定可能な信頼性、および Cisco の拡張機能をサポートします。このデバイスは、8 回線をサポートします。各回線のコールとビジー トリガーの最大数は、それぞれ 4 と 2 です。
- Generic Single Screen Room System：この SIP デバイスは、1 画面のテレプレゼンス（ルーム システム）、ビデオ、セキュリティ、設定可能な信頼性、および Cisco の拡張機能をサポートします。このデバイスは、8 回線をサポートします。各回線のコールとビジー トリガーの最大数は、それぞれ 4 と 2 です。
- Generic Multiple Screen Room System：この SIP デバイスは、複数画面のテレプレゼンス（ルーム システム）、ビデオ、セキュリティ、設定可能な信頼性、および Cisco の拡張機能をサポートします。このデバイスは、8 回線をサポートします。各回線のコールとビジー トリガーの最大数は、それぞれ 4 と 2 です。

サードパーティ製 SIP エンドポイント設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ダイジェスト ユーザの設定, （425 ページ）	ダイジェスト認証を有効にするには、ダイジェストユーザとなるエンド ユーザを設定します。Cisco Unified Communications Manager は、[エンドユーザの設定（End User Configuration）] ウィンドウで指定されたダイジェスト クレデンシャルを使用して、SIP トランクとのチャレンジの間、SIP ユーザ エージェントの応答を検証します。 サードパーティ製 SIP 電話がダイジェスト ユーザをサポートしていない場合は、サードパーティ製 SIP 電話の電話番号に一致するユーザ ID でユーザを作成します。たとえば、1000 という名前のエンド ユーザを作成し、電話の電話番号として 1000 を作成します。このユーザを電話に割り当てます。
ステップ 2	SIP プロファイルの設定, （381 ページ）	SIP トランクに関連付けられている一連の SIP 属性を提供します。
ステップ 3	電話セキュリティ プロファイルの設定, （382 ページ）	ダイジェスト認証を使用するには、新しい電話セキュリティ プロファイルを設定する必要があります。自動登録用に提供されている標準の非セキュア SIP プロファイルのいずれかを使用している場合、ダイジェスト認証を有効にすることはできません。
ステップ 4	サードパーティ SIP エンドポイントの追加, （427 ページ）	サード パーティ製エンドポイントを設定します。
ステップ 5	エンドユーザとデバイスの関連付け, （390 ページ）	サード パーティ製エンドポイントをエンドユーザと関連付けます。

次の作業

電源を投入し、ネットワーク接続を確認して、サードパーティ製SIPエンドポイントのネットワーク設定を行います。ネットワーク設定の詳細については、サードパーティ製 SIP エンドポイントのユーザ ガイドを参照してください。

ダイジェスト ユーザの設定

ダイジェストユーザとして、エンドユーザを設定するには、次の手順を実行します。ダイジェスト認証によって、Cisco Unified Communications Manager は接続してくるデバイスが正当なものかどうかを確認できます。確認するとき、デバイスはユーザ名とパスワードに類似したダイジェスト クレデンシャルを検証用に Cisco Unified Communications Manager に送ります。送られたクレデンシャルがデータベース内に設定されたそのデバイスに対するクレデンシャルと一致した場合、ダイジェスト認証は成功となり、Cisco Unified Communications Manager によって SIP リクエストが処理されます。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（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 ID（User ID）] を入力します。

ステップ 4 [姓（Last Name）] に入力します。

ステップ 5 [ダイジェスト クレデンシャル（Digest Credentials）] を入力します。ダイジェスト クレデンシャルは英数文字列です。

ステップ 6 [エンドユーザの設定（End User Configuration）] ウィンドウでその他のフィールドに入力します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次の作業

SIP プロファイルの設定, （381 ページ）

SIP プロファイルの設定

はじめる前に

- SIP 電話のセキュア ポートの設定, （380 ページ）
- サービスの再起動, （380 ページ）

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 [検索（Find）] をクリックします。

ステップ 3 プロファイルをコピーする場合は、[コピー（Copy）] 列のファイル アイコンをクリックします。

ステップ 4 新しいプロファイルの名前と説明を入力します。

ステップ 5 Cisco Unity Connection が Cisco Unified Communications Manager との通信に IPv6 または IPv4/IPv6 デュアル スタックを使用する場合は、[ANAT を有効化（Enable ANAT）] チェックボックスをオンにします。
この手順は、IPv6 またはデュアル スタック環境で発信者を適切に処理するために必要です。

ステップ 6 [保存（Save）] をクリックします。

次の作業

電話セキュリティ プロファイルの設定, （382 ページ）

電話セキュリティ プロファイルの設定

Cisco Unified Communications Manager は、自動登録用の事前に定義された非セキュアなセキュリティ プロファイル一式を提供します。電話のセキュリティ機能を有効にするには、新しいセキュリティプロファイルを設定し、それを電話に適用する必要があります。新しいセキュリティプロファイルを設定するには、次の手順を実行します。

はじめる前に

SIP 電話を設定する場合は、次の手順を完了します。

- SIP 電話のセキュア ポートの設定, （380 ページ）
- サービスの再起動, （380 ページ）
- SIP プロファイルの設定, （381 ページ）

SCCP 電話を設定する場合は、次の手順を開始する前に完了しておく前提条件はありません。

手順

ステップ 1 Cisco Unified CM の管理から、[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）] 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 [電話セキュリティ プロファイルのタイプ（Phone Security Profile Type）] ドロップダウン リストから、作成するプロファイルのタイプを選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 [電話セキュリティ プロファイルのプロトコルの選択（Select the phone security profile protocol）] ドロップダウン リストから、プロトコルを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Name] フィールドにプロファイルの適切な名前を入力します。

ステップ 8 プロファイルに関する簡単な説明を入力します。

ステップ 9 [保存（Save）] をクリックします。

次の作業

SIP および SCCP の両方の電話について：

サードパーティ SIP エンドポイントの追加, （427 ページ）

サードパーティ SIP エンドポイントの追加

はじめる前に

ダイジェスト ユーザの設定, （425 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [電話タイプ（Phone Type）] ドロップダウン リストから、次のいずれかを選択します。

- サードパーティ SIP デバイス（基本）
- サードパーティ SIP デバイス（拡張）
- サードパーティ AS-SIP デバイス
- Generic Desktop Video Endpoint
- Generic Single Screen Room System

- Generic Multiple Screen Room System

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 サードパーティのエンドポイントの電話番号を設定するには、ウィンドウの左側にある [関連付け情報（Association Information）] エリアに表示される、[新しい DN を追加（Add a New DN）] リンクをクリックします。
[電話番号の設定（Directory Number Configuration）] ウィンドウが表示されます。詳細については、電話番号の追加と設定に関するトピックを参照してください。

次の作業

エンドユーザとデバイスの関連付け, （390 ページ）

エンドユーザとデバイスの関連付け

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[ユーザの管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 2 [ユーザを次の条件で検索（Find Users Where）] フィールドで適切なフィルタを指定した後、[検索（Find）] をクリックしてユーザのリストを取得します。

ステップ 3 ユーザを一覧から選択します。

ステップ 4 [デバイス情報（Device Information）] セクションを探します。

ステップ 5 [デバイスの割り当て（Device Association）] をクリックします。
[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 6 デバイスを探して選択します。

ステップ 7 関連付けを完了するには、[選択/変更の保存（Save Selected/Changes）] をクリックします。

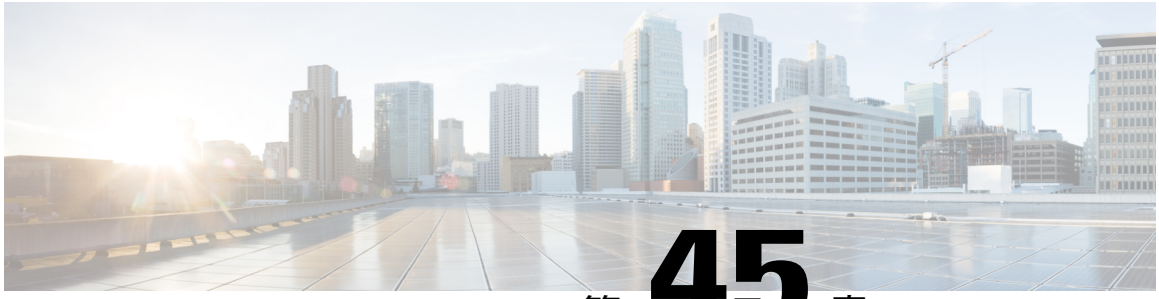
ステップ 8 [関連リンク（Related Links）] ドロップダウン リスト ボックスで [ユーザの設定に戻る（Back to User）] を選択し、[移動（Go）] をクリックします。
[エンド ユーザの設定（End User Configuration）] ウィンドウが表示され、選択し、割り当てたデバイスが、[制御するデバイス（Controlled Devices）] ペインに表示されます。

サードパーティのインタラクションと制限事項

サードパーティの制限事項

表 *56* : サードパーティ製 *SIP* エンドポイントの制限事項

制約事項	説明
Cisco Video Communication Server（VCS）のリングバック トーンの制限は、サードパーティ製 SIP エンドポイントに登録されています。	Cisco Unified Communications Manager に登録された VCS エンドポイント上で発生する転送を要求するためのブラインド転送やスイッチには、リングバック トーンはありません。監視転送を行う場合、保留音（MOH）は割り当てますが、リングバック トーンは割り当てません。



第 45 章

サービス プロファイルとテンプレート

- デバイス プロファイルとテンプレートの概要，431 ページ
- デバイス プロファイルとテンプレートの設定タスク フロー，432 ページ

デバイス プロファイルとテンプレートの概要

この章では、デバイス プロファイルとテンプレートの設定方法について説明します。特定の機能を設定する方法の詳細については、『*Features and Services Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

デバイス プロファイル

デバイス プロファイルは、特定のデバイスに関連付けられるサービス、機能、および電話番号を定義します。デバイス プロファイルを設定後、ユーザ デバイス プロファイルをユーザに割り当てることができます。それによって、ユーザは、デバイスにログインしたときに、それらの機能とサービスをそのデバイスで使用できます。

エンドポイントの SIP プロファイル

SIP プロファイルは、SIP エンドポイントに関連付けられている一連の SIP 属性で構成されています。SIP プロファイルには、名前、説明、タイミング、再試行、コール ピックアップ URI などが含まれます。プロファイルに含まれる一部の標準エントリは、削除または変更ができません。

サービス プロファイルとテンプレート

Cisco Unified Communications Manager は、デフォルトのデバイス プロファイルもサポートします。Cisco Unified Communications Manager は、ユーザ デバイス プロファイルがない電話機モデルにユーザがログインするたびに、デフォルトのデバイス プロファイルを使用します。

ピアツーピア イメージの分配

ピア ファームウェア共有機能を使用すると、高速キャンパス LAN 設定において次の利点が得られます。

- 中央集中型 TFTP サーバへの TFTP 転送における輻輳が制限されます。
- ファームウェアのアップグレードを手動で制御する必要がなくなります。
- アップグレード時に多数のデバイスが同時にリセットされた場合の電話機のダウンタイムが削減されます。

ほとんど条件で、ピア ファームウェア共有機能は、帯域幅が制限された WAN リンク上のブランチ導入シナリオでのファームウェア アップグレードを最適化します。

この機能が有効の場合、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、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。

デバイス プロファイルとテンプレートの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	デフォルト デバイス プロファイルでのソフトキーテンプレートの設定, （434 ページ）	デフォルト デバイス プロファイルをソフトキー テンプレートに追加します。
ステップ 2	共通デバイス設定とソフトキーテンプレートの関連付け, （435 ページ）：	これはオプションです。ソフトキー テンプレートを電話で利用できるようにするには、テンプレートを共通デバイス設定または電話に直接に関連付ける必要があります。システムで共通デバイス設定を使用して設定オプションを電話に適用する場合、このステップを実行します（これは電話でソフトキー テンプレートを使用できるようにする最も一般的な使用方法です）。 （注） Bulk Administration Tool を使用して複数の電話の共通デバイス設定を関連付ける方法の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある *Cisco Unified Communications Manager Bulk Administration* ガイド を参照してください。

	コマンドまたはアクション	目的
ステップ 3	電話機とソフトキーテンプレートの関連付け, （437 ページ）	これはオプションです。ソフトキー テンプレートと共通デバイス設定を関連付けるための代替手段として、または共通デバイス設定と共に、次の手順を使用します。ソフトキー テンプレートを適用して、共通デバイス設定での割り当てや、他のデフォルトのソフトキーの割り当てをオーバーライドする必要がある場合は、次の手順を共通デバイス設定と共に使用します。
ステップ 4	機能管理ポリシーの設定, （437 ページ）	これはオプションです。ソフトキー テンプレートを設定する代替手段として次の手順を使用します。機能管理ポリシーを設定して、特定の機能を有効/無効にして、電話機でのソフトキーの表示を制御できます。機能の共通セットを使用するユーザ グループに機能管理ポリシーを作成できます。たとえば、コール パークおよびコール ピックアップ機能を販売グループの従業員はよく使用しますが、社内の全従業員が使用するわけではありません。これらの 2 つの機能だけを有効にした機能管理ポリシーを作成し、販売グループにそのポリシーを割り当てることができます。機能管理ポリシーを作成したら、そのポリシーを各電話機、電話機のグループ、またはシステム内のすべての電話機に関連付けることができます。
ステップ 5	電話ボタンテンプレートの設定, （441 ページ） • 電話機とボタン テンプレートの関連付け, （442 ページ）	各 Cisco Unified IP Phone モデルのデフォルト テンプレートを導入するには、次の手順を使用します。電話機を追加する場合、これらのテンプレートの 1 つを割り当てることも、独自のテンプレートを作成することもできます。
ステップ 6	デバイス プロファイルの設定, （443 ページ）	SIP または SCCP をサポートする任意の電話モデル用デバイス プロファイルを設定します。
ステップ 7	エンドポイントの SIP プロファイルの設定, （444 ページ）	電話の新しい SIP プロファイルを設定します。
ステップ 8	デフォルトのデバイス プロファイルの設定, （444 ページ）	SIP または SCCP をサポートする任意の電話モデル用のデフォルト デバイス プロファイルを設定します。

デフォルト デバイス プロファイルでのソフトキー テンプレートの設定

Cisco Unified Communications Manager にはコール処理とアプリケーション用の標準ソフトキー テンプレートが含まれます。カスタム ソフトキーテンプレートを作成するときは、標準テンプレートをコピーして、必要に応じて変更します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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 テンプレートの設定（Softkey Template Configuration）] ウィンドウが表示されます。

ステップ 2 新しいソフトキー テンプレートを作成するには、以下のステップを実行します。それ以外の場合は次のステップに進みます。

a) [新規追加（Add New）] をクリックします。
b) デフォルトのテンプレートを選択して、[コピー（Copy）] をクリックします。
c) [ソフトキー テンプレート名（Softkey Template Name）] フィールドに、テンプレートの新しい名前を入力します。
d) [保存（Save）] をクリックします。

ステップ 3 既存のテンプレートにソフトキーを追加するには、以下のステップを実行します。

a) 検索条件を入力して [検索（Find）] をクリックします。
b) 既存のテンプレートを選択します。

[ソフトキー テンプレートの設定（Softkey Template Configuration）] ウィンドウが表示されます。

ステップ 4 [デフォルト ソフトキーテンプレート（Default Softkey Template）]チェックボックスをオンにし、このソフトキー テンプレートをデフォルトのソフトキー テンプレートとして指定します。

（注） あるソフトキー テンプレートをデフォルトのソフトキー テンプレートとして指定した場合、先にデフォルトの指定を解除してからでないと、そのテンプレートは削除することができません。

ステップ 5 右上隅にある [関連リンク（Related Links）] ドロップダウン リストから [ソフトキー レイアウトの設定（Configure Softkey Layout）] を選択し、[移動（Go）] をクリックします。

ステップ 6 [設定するコール状態の選択（Select a Call State to Configure）] ドロップダウン リストから、ソフトキーに表示するコール状態を選択します。

ステップ 7 [選択されていないソフトキー（Unselected Softkeys）] リストから追加するソフトキーを選択し、右矢印をクリックして [選択されたソフトキー（Selected Softkeys）] リストにそのソフトキーを移動します。新しいソフトキーの位置を変更するには、上矢印と下矢印を使用します。

ステップ 8 追加のコール状態のソフトキーを表示するには、上記のステップを繰り返します。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- すでにデバイスに関連付けられているテンプレートを変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。

- 新しいソフトキーテンプレートを作成した場合は、そのテンプレートをデバイスに関連付けた後にデバイスを再起動します。詳細については、「次の作業」の項を参照してください。

次の作業

次のいずれかの手順を実行します。

- 共通デバイス設定へのソフトキー テンプレートの追加, （435 ページ）
- 電話機とソフトキー テンプレートの関連付け, （437 ページ）

共通デバイス設定とソフトキー テンプレートの関連付け

これはオプションです。ソフトキー テンプレートを電話機に関連付ける方法は 2 つあります。

- ソフトキー テンプレートを [電話の設定（Phone Configuration）] に追加する。
- ソフトキー テンプレートを**共通デバイス設定**に追加する。

ここに示す手順では、ソフトキー テンプレートを**共通デバイス設定**に関連付ける方法について説明します。システムが**共通デバイス設定**を使用して設定オプションを電話機に適用する場合は、この手順に従ってください。これは、電話機でソフトキー テンプレートを使用できるようにする際に、最も一般的に使用されている方法です。

別の方法を使用するには、電話機とソフトキーテンプレートの関連付け, （437ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	共通デバイス設定へのソフトキーテンプレートの追加, （435 ページ）	
ステップ 2	電話機と共通デバイス設定の関連付け, （436 ページ）	

共通デバイス設定へのソフトキー テンプレートの追加

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）] > [共通デバイス設定（Common Device Configuration）] を選択します。

[共通デバイス設定の検索と一覧表示（Find and List Common Device Configuration）] ウィンドウが表示されます。

ステップ 2 新しい共通デバイス設定を作成し、それにソフトキー テンプレートを関連付けるには、以下の手順を実行します。それ以外の場合は、次のステップに進みます。

a) [新規追加（Add New）] をクリックします。

b) [名前（Name）] フィールドに、共通デバイス設定の名前を入力します。

c) [保存（Save）] をクリックします。

ステップ 3 既存の共通デバイス設定にソフトキー テンプレートを追加するには、以下の手順を実行します。

a) 検索条件を入力して [検索（Find）] をクリックします。

b) 既存の共通デバイス設定を選択します。

[共通デバイス設定（Common Device Configuration）] ウィンドウが表示されます。

ステップ 4 [ソフトキー テンプレート（Softkey Template）] ドロップダウン リストで、使用可能にするソフトキーが含まれているソフトキー テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- 新しい共通デバイス設定を作成してその設定をデバイスに関連付けた後に、デバイスを再起動します。詳細については、「次の作業」の項を参照してください。
- すでにデバイスに関連付けられている共通デバイス設定を変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。

次の作業

電話機と共通デバイス設定の関連付け, （436 ページ）

電話機と共通デバイス設定の関連付け

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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。

ステップ 2 ソフトキー テンプレートを追加する電話機を検索します。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ドロップダウン リストから、新しいソフトキー テンプレートが含まれている共通デバイス設定を選択します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リセット（Reset）] をクリックして、電話機の設定を更新します。

電話機とソフトキー テンプレートの関連付け

この手順は任意です。この手順を代わりに使用して、ソフトキー テンプレートを共通デバイス設定と関連付けることができます。また、この手順は共通デバイス設定とも連動しています。ソフトキー テンプレートを適用して、共通デバイス設定での割り当てや、他のデフォルトのソフトキーの割り当てを上書きする必要がある場合に使用します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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。

ステップ 2 ソフトキー テンプレートを追加する電話機を選択します。
[電話機の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 3 [ソフトキー テンプレート（Softkey Template）] ドロップダウン リストから、新しいソフトキーが含まれているテンプレートを選択します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リセット（Reset）] を押して、電話機の設定を更新します。

機能管理ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	電話機能一覧の生成, （438 ページ）	Cisco Unified Reporting にログインし、電話機能リスト レポートを実行して、機能管理ポリシーをサポートする電話を決定します。
ステップ 2	機能管理ポリシーの作成, （438 ページ）	Cisco Unified IP Phones の機能管理ポリシーを作成します。
ステップ 3	次のいずれかの作業を実行します。 • 電話への機能管理ポリシーの適用, （440 ページ） • 共通の電話プロファイルへの機能管理ポリシーの適用, （440 ページ）	機能管理ポリシーを設定したら、そのポリシーを各電話機、電話機のグループ、またはシステム内のすべての電話機に関連付ける必要があります。各電話の機能管理ポリシーは、クラスタ全体の機能管理ポリシーより優先されます。

	コマンドまたはアクション	目的
	• すべての電話への機能管理ポリシーの適用, （441 ページ）	（注） 一括管理ツールを使用して複数の電話に機能管理ポリシーを適用する方法については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』を参照してください。

電話機能一覧の生成

電話機能一覧のレポートを生成し、設定したい機能をどのデバイスがサポートしているのか判別します。

手順

ステップ 1 [Cisco Unified Reporting の管理（Cisco Unified Reporting Administration）] から [System Reports] を選択してください。

ステップ 2 レポートのリストから、[Unified CM 電話機能一覧（Unified CM Phone Feature List）] をクリックします。

ステップ 3 次のいずれかの手順を実行します。

- [レポートの新規生成（Generate New Report）] （棒グラフのアイコン）を選択し、新しいレポートを生成します。
- レポートがすでにできていれば、[Unified CM 電話機能一覧（Unified CM Phone Feature List）] を選択します。

ステップ 4 [製品（Product）] ドロップダウン リストから、[All] を選択します。

ステップ 5 設定の対象となる機能の名前をクリックします。

ステップ 6 [送信（Submit）] をクリックします。
レポートが生成されます。

機能管理ポリシーの作成

機能管理ポリシーを作成するには、次の手順に従います。Cisco Unified Communications Manager で複数の機能管理ポリシーを設定できます。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [機能管理ポリシー（Feature Control Policy）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のポリシーの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストからポリシーを選択します。
- 新しいポリシーを追加するには、[新規追加（Add New）] をクリックします。

[機能管理ポリシーの設定（Feature Control Policy Configuration）] ウィンドウが表示されます。

ステップ 3 [名前（Name）] フィールドに機能管理ポリシーの名前を入力します。この名前には、最長 50 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。各機能管理ポリシー名がシステムに固有の名前であることを確認します。

ステップ 4 [説明（Description）] フィールドに、この機能管理ポリシーの説明を入力します。この説明には、最長 50 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

ステップ 5 [機能管理セクション（Feature Control Section）] でリストされている各機能に対して、システムデフォルトをオーバーライドするか、次の設定を有効/無効にするかを選択します。

- デフォルトで有効な機能の設定を無効にする場合は、[デフォルトをオーバーライド（Override Default）] チェックボックスをオンにして、[設定を有効にする（Enable Setting）] チェックボックスをオフにします。
- デフォルトで無効な機能の設定を有効にする場合は、[デフォルトをオーバーライド（Override Default）] チェックボックスをオンにして、[設定を有効にする（Enable Setting）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

次のいずれかを実行します。

- 電話への機能管理ポリシーの適用, （440 ページ）
- 共通の電話プロファイルへの機能管理ポリシーの適用, （440 ページ）
- すべての電話への機能管理ポリシーの適用, （441 ページ）

電話への機能管理ポリシーの適用

はじめる前に

- 電話モデルが機能管理ポリシーをサポートしていることを確認します。詳細については、電話機能一覧の生成, （438 ページ）を参照してください。
- 機能管理ポリシーの作成, （438 ページ）

手順

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

ステップ 2 検索条件を入力し、[検索（Find）] をクリックします。
Cisco Unified Communications Manager で設定されている電話機の一覧が表示されます。

ステップ 3 機能管理ポリシーを適用する電話を選択します。

ステップ 4 [機能管理ポリシー（Feature Control Policy）] ドロップダウン リストから、必要な機能管理ポリシーを選択します。

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。

ステップ 7 [OK] をクリックします。

共通の電話プロファイルへの機能管理ポリシーの適用

共通の電話プロファイルを使用すると、機能管理ポリシーを設定し、そのプロファイルを使用するネットワーク内のすべての電話にこれらの設定を適用できます。

はじめる前に

機能管理ポリシーの作成, （438 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 検索条件を入力し、[検索（Find）] をクリックします。

ステップ 3 機能管理ポリシーを適用する共通の電話プロファイルを選択します。

ステップ 4 [機能管理ポリシー（Feature Control Policy）] ドロップダウン リストから、必要な機能管理ポリシーを選択します。

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。

ステップ 7 [OK] をクリックします。

すべての電話への機能管理ポリシーの適用

はじめる前に

機能管理ポリシーの作成, （438 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] の順に選択します。

ステップ 2 [機能管理ポリシー（Feature Control Policy）] ドロップダウン リストから、必要な機能管理ポリシーを選択します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 [OK] をクリックします。

電話ボタン テンプレートの設定

手順

ステップ 1 Cisco Unified CM の管理から、[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）] を選択します。

[電話ボタン テンプレートの検索と一覧表示（Find and List Phone Button Templates）] ウィンドウが表示されます。

ステップ 2 [検索（Find）] をクリックします。
ウィンドウにサポートする電話のテンプレートのリストが表示されます。

ステップ 3 新しい電話ボタン テンプレートを作成するには、以下のステップを実行します。それ以外の場合は次のステップに進みます。

a) 電話機モデルのデフォルトのテンプレートを選択し、[コピー（Copy）] をクリックします。
b) [電話ボタン テンプレート情報（Phone Button Templates Information）] フィールドに、テンプレートの新しい名前を入力します。
c) [保存（Save）] をクリックします。

ステップ 4 既存のテンプレートにダイヤル ボタンを追加するには、この手順を実行します。

a) 検索条件を入力して [検索（Find）] をクリックします。
b) 既存のテンプレートを選択します。

[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 [回線（Line）] ドロップダウン リストから、テンプレートに追加する機能を選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 次のいずれかの作業を実行します。

- すでにデバイスに関連付けられているテンプレートを変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。
- 新しいソフトキーテンプレートを作成した場合は、そのテンプレートをデバイスに関連付けた後にデバイスを再起動します。詳細については、「次の作業」の項を参照してください。

次の作業

電話機とボタン テンプレートの関連付け, （442 ページ）

電話機とボタン テンプレートの関連付け

はじめる前に

電話ボタン テンプレートの設定, （441 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[デバイス（Device）] > [電話（Phone）] を選択します。
[電話の検索/一覧表示（Find and List Phones）] ウィンドウが表示されます。

ステップ 2 [電話の検索/一覧表示（Find and List Phones）] ウィンドウで、[検索（Find）] をクリックします。

Cisco Unified Communications Manager で設定されている電話機の一覧が表示されます。

ステップ 3 電話ボタン テンプレートを追加する電話を選択します。
[電話機の設定（Phone Configuration）] ウィンドウが表示されます。

ステップ 4 [電話ボタン テンプレート（Phone Button Template）] ドロップダウン リストで、新しい機能ボタンが含まれる電話ボタン テンプレートを選択します。

ステップ 5 [保存（Save）] をクリックします。
電話の設定を更新するには [リセット（Reset）] を押すというメッセージ付きのダイアログ ボックスが表示されます。

デバイス プロファイルの設定

デバイス プロファイルは特定のデバイスに関連付ける属性セットで構成されます。

はじめる前に

次のいずれかの手順を実行します。

- デフォルト デバイス プロファイルでのソフトキー テンプレートの設定, （434 ページ）
- 電話ボタン テンプレートの設定, （441 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] ウィンドウで、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイス プロファイル（Devicec Profile）] を選択します。

ステップ 2 [デバイス プロファイルの設定（Device Profile Configuration）] ウィンドウで、[デバイス プロファイル タイプ（Device Profile Type）] ドロップダウン リストから、該当する Cisco Unified IP Phone を選択します。

ステップ 3 [Next] をクリックします。

ステップ 4 [デバイスプロトコル（Device Protocol）] ドロップダウン リストから、適切なプロトコルを選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [デバイス プロファイルの設定（Device Profile Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

エンドポイントの SIP プロファイルの設定

Cisco Unified Communications Manager は、SIP プロファイルを使用して、SIP トランクおよび Cisco Unified IP Phone に関連付けられている SIP 属性を定義します。

手順

ステップ 1 [Cisco Unified CM の管理（**Cisco Unified CM Administration**）] ウィンドウで、[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 新しい SIP プロファイルを追加するには、[新規追加（Add New）] ボタンをクリックします。

ステップ 3 [SIPプロファイルの設定（SIP Profile Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

デフォルトのデバイス プロファイルの設定

ユーザがユーザデバイスプロファイルを持たない電話機にログインするたびに、電話機がデフォルトのデバイス プロファイルを取得します。

デフォルトのデバイス プロファイルには、デバイス タイプ（電話）、ユーザ ロケール、電話ボタン テンプレート、ソフトキー テンプレート、Multilevel Precedence and Preemption（MLPP）情報が含まれます。

はじめる前に

次のいずれかの手順を実行します。

- デフォルト デバイス プロファイルでのソフトキー テンプレートの設定, （434 ページ）
- 電話ボタン テンプレートの設定, （441 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] ウィンドウで、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デフォルトのデバイス プロファイル（Default Device Profile）] を選択します。

ステップ 2 [デフォルトのデバイスプロファイルの設定（Default Device Profile Configuration）] ウィンドウで、[デバイスプロファイルタイプ（Device Profile Type）] ドロップダウンリストから、該当する Cisco Unified IP Phone を選択します。

ステップ 3 [Next] をクリックします。

ステップ 4 [デバイスプロトコル（Device Protocol）] ドロップダウン リストから、適切なプロトコルを選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [デフォルトのデバイス プロファイルの設定（Default Device Profile Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

電話のピアツーピア イメージの配信機能の設定

手順

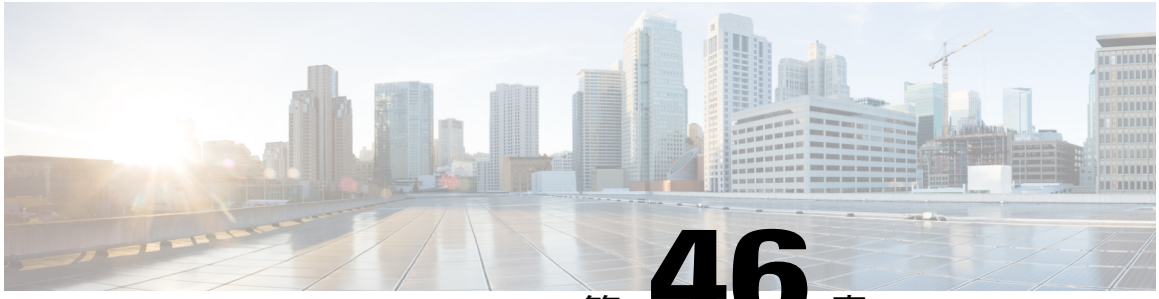
ステップ 1 Cisco Unified Communications Manager の管理ページで、[デバイス（Device）] > [電話（Phone）] を選択します。

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、電話を選択するには、[電話を次の条件で検索（Find Phone where）] フィールドで[検索（Find）] をクリックして電話のリストを取得し、そのリストから電話を選択します。

ステップ 3 [電話機の設定（Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] ペインの [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、次のいずれかのオプションを選択します。

- [有効（Enabled）　（デフォルト）] : 電話がピアツーピア イメージの配信（PPID）をサポートしていることを示します。
- [無効（Disabled）] ：電話がピアツーピア イメージの配信（PPID）をサポートしていないことを示します。

ステップ 4 [設定の適用（Apply Config）] をクリックします。



第 46 章

ユーザとエンドポイントの関連付け

- ユーザとエンドポイントの関連付けの概要，447 ページ
- ユーザとエンドポイントの関連付けに関する前提条件，447 ページ
- ユーザおよびデバイス設定のタスク フロー，447 ページ
- ユーザとエンドポイントの関連付けに関する連携動作と制約事項，452 ページ

ユーザとエンドポイントの関連付けの概要

この章では、エンドユーザとアプリケーションユーザをデバイスに関連付ける方法について説明します。エンド ユーザは、自身に関連付けられるデバイスを制御できます。ユーザとして特定されたアプリケーションは、電話やコンピュータ テレフォニー インテグレーション（CTI）ポートなどのデバイスを制御できます。

ユーザとエンドポイントの関連付けに関する前提条件

エンドポイントと関連付ける前に、エンドユーザとアプリケーション ユーザを設定します。エンド ユーザとデバイスの関連付け，（448 ページ）およびアプリケーション ユーザとデバイスの関連付け，（451 ページ）を参照してください。

ユーザおよびデバイス設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	エンド ユーザとデバイスの関連付け，（448 ページ）.	エンドユーザをデバイスと関連付けます。

	コマンドまたはアクション	目的
ステップ 2	アプリケーション ユーザとデバイスの関連付け，（451 ページ）.	アプリケーションユーザをデバイスと関連付けます。

エンド ユーザとデバイスの関連付け

Cisco Unified Communications Manager では、エンド ユーザ ID の重複は許可されていません。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 2 [アプリケーションユーザの検索/一覧表示（Find and List Application Users）] ウィンドウで、[検索（Find）] をクリックします。

ステップ 3 エンドユーザのリストを表示するウィンドウで、該当するエンドユーザのリンクをクリックします。

ステップ 4 [エンドユーザの設定（End User Configuration）] ウィンドウで、[デバイス情報（Device Information）] 領域までスクロール ダウンし、エンド ユーザに関連付けるデバイスを選択します。[利用可能なデバイス（Available Devices）] ボックスで、アプリケーション ユーザに関連付けるデバイスを選択し、ボックスの下にある下矢印をクリックします。

（注） [デバイス情報（Device Information）] 領域にデバイスがない場合は、[デバイスの割り当て（Device Associations）] ボタンをクリックして、[ユーザとデバイスの関連付け（User Device Association）] ウィンドウを開きます。1 つまたは複数のデバイスを選択し、[選択/変更を保存（Save Selected/Changes）] ボタンをクリックします。選択したデバイスは、[デバイス情報（Device Information）] 領域の [制御されたデバイス（Controlled Devices）] リスト ボックスに表示されます。次に、ステップ 1 ～ 4 に従ってデバイスを関連付けます。

ステップ 5 （任意）ライン アピアランスをプレゼンスのエンド ユーザに関連付けるには、またこのライン アピアランスがオフフックの場合に、IM and Presence のクライアントに対して通話中のステータス情報を有効にするには、[ライン アピアランスのプレゼンスからの関連付け（Line Appearance Association from Presence）] ボタンをクリックします。[ライン アピアランスのプレゼンスとの関連付け（Line Appearance Association for Presence）] ウィンドウが表示され、ここで製品タイプ、デバイス名、ディレクトリ、パーティション、または説明を選択できます。このウィンドウで利用できる選択肢は、制御されたデバイスと関連付けられた回線によって異なります。[保存（Save）] をクリックします。

ステップ 6 [エンドユーザの設定（End User Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクションを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次の作業

アプリケーション ユーザとデバイスの関連付け, （451 ページ）.

関連トピック

エンド ユーザおよびデバイス構成時の設定, （449 ページ）

エンド ユーザおよびデバイス構成時の設定

表 *57* : ユーザ情報

フィールド	説明
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。
[パスワード（Password）]	英数字または特殊文字を使用して、5 文字以上のエンドユーザのパスワードを入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、“”、および空白です。
[PIN]	パーソナル ID 番号として 5 桁以上の数字を入力します。
姓	エンドユーザの姓を入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、“”、および空白です。
ミドル ネーム（Middle Name）	エンド ユーザのミドル ネームを入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、“”、および空白です。
名	エンドユーザの名を入力します。使用できる特殊文字は、=、+、<、>、#、;、\、,、“”、および空白です。

表 *58* : デバイスの割り当て

フィールド	説明
[製品のタイプ（Product Type）]	ドロップダウン リストから、このエンド ユーザに関連付けるデバイスの種類を選択します。

フィールド	説明
MAC アドレス	新規ユーザに関連付けている新しいデバイスに対する一意の MAC アドレスを入力します。MAC アドレスは、正確に 12 桁の 16 進数（0 ～ 9、A ～ F）で構成されます。
コーリングサーチスペース DN	ドロップダウン リストから、このユーザとデバイスを関連付けているディレクトリ番号の発信コーリング サーチ スペースを選択します。
コーリング サーチ スペース電話	ドロップダウン リストから、このユーザとデバイスに関連付けている電話のコーリング サーチ スペースを選択します。
[外線電話番号マスク（External Phone Number Mask）]	関連付けられたデバイスからの外部発信（アウトバウンドの）コールの発信者 ID 情報のフォーマットに使用するマスクを指定します。 • マスクには最大 24 文字を含めることができます。有効な文字として、0 ～ 9、*、#、および X を指定します。 • 発信者 ID 情報として表示するリテラル文字を入力し、X を使用して関連付けられたデバイスのディレクトリ番号を表します。 • マスクとして 972813XXXX を指定する場合、外線通話に使用されるルート パターンで外部電話番号マスク オプションがオンになっていると、内線番号 1234 からの外部コールで発信者 ID 番号として 9728131234 が表示されます。主なアテンダント番号を表すために 9728135000 のようなリテラル文字のマスクを指定すると、そのリテラル番号（9728135000）が、関連付けられたデバイスからの外部コールの発信者 ID として表示されます。
内線番号	新しいユーザおよび電話の内線番号を入力します。使用できる文字は、0 ～ 9、?、[,]、+、-、*、^、#、！です。 このフィールドは、エンドユーザのプライマリ電話番号を表します。エンドユーザは、電話機に複数の回線を接続できます。

フィールド	説明
[ルートパターン（Route Pattern）]	ドロップダウンリストから、拡張フィールドで指定したディレクトリ番号のパーティションを選択します。
ボイス メール プロファイル（Voice Mail Profile）	ドロップダウンリストから、ディレクトリ番号のボイス メール プロファイルを選択します。 システム デフォルトを使用には、[なし（None）] を選択します。
[エクステンションモビリティの有効化（Enable Extension Mobility）]	エクステンション モビリティを有効にするには、このチェック ボックスをオンにします。 新しいユーザを追加すると、ユーザ管理> エンド ユーザ メニュー オプションを使用して、エクステンション モビリティ プロファイルを選択できます。

アプリケーション ユーザとデバイスの関連付け

アプリケーション ユーザが制御できるデバイスを関連付けることができます。アプリケーション ユーザは、電話などのデバイスを制御できます。ユーザとして特定されたアプリケーションは、CTI ポートなどの他のデバイスを制御できます。アプリケーション ユーザが電話を制御できる場合、短縮ダイヤル、コール転送など、その電話機の特定の設定を制御できます。

はじめる前に

エンド ユーザとデバイスの関連付け，（448 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）] を選択します。
が表示されます。

ステップ 2 [アプリケーションユーザの検索/一覧表示（Find and List Application Users）] ウィンドウで、[検索（Find）] をクリックします。

ステップ 3 アプリケーション ユーザのリストから、該当するアプリケーションのユーザのリンクをクリックします。

ステップ 4 [アプリケーション ユーザの設定（Application User Configuration） ウィンドウから、[デバイス情報（Device Information）]エリアまでスクロールします。[使用可能なデバイス（Available Devices）] ボックスで、アプリケーション ユーザに関連付けするデバイスを選択し、ボックスの下にある下向き矢印をクリックします。

デバイスが [制御デバイス（Controlled Devices）] ボックスに移動します。

ステップ 5 使用可能なデバイスのリストに追加するには、次のボタンのいずれかをクリックします。

- [別の電話を検索（Find more Phones）]：このアプリケーション ユーザに関連付ける別の電話機を検索します。
- [別のルート ポイントを検索（Find more Route Points）]：このアプリケーション ユーザに関連付ける CTI ルート ポイントを検索します。
- [別のパイロット ポイントを検索（Find more Pilot Points）]：このアプリケーション ユーザに関連付けるパイロット ポイントを検索します。

ステップ 6 アプリケーション ユーザに割り当てるデバイスごとに、ステップ 5 を繰り返します。

ステップ 7 [保存（Save）] をクリックします。

ユーザとエンドポイントの関連付けに関する連携動作と制約事項

ユーザとエンドポイントの関連付けに関する連携動作

表 *59*：ユーザとエンドポイントの関連付けの連携動作

機能	データのやり取り
CTI 制御不可のデバイス	H.323 デバイスなど CTI 制御が不可能なデバイスの場合は、使用可能なデバイス リストのデバイス アイコンの横にアスタリスク（*）が表示されます。
Cisco エクステンション モビリティ	Cisco Extension Mobility 機能を使用して、Cisco Unified IP Phone を一時的にエンドユーザの電話として表示するように設定できます。エンドユーザは電話にサインインでき、そのエンドユーザの Extension Mobility プロファイル（回線、短縮ダイヤル番号を含む）が電話に配置されます。この機能は主に、エンドユーザが物理的な電話に永続的に割り当てられない環境に適用されます。
IM and Presence Service	Cisco Unified Communications Manager の管理を使用して、エンド ユーザを IM およびプレゼンス サービス サーバ ノードとエンド ユーザのクラスタに割り当てると、IM およびプレゼンス サービスの可用性およびインスタント メッセージング サービスを受けることができます。

ユーザとエンドポイントの関連付けに関する制約事項

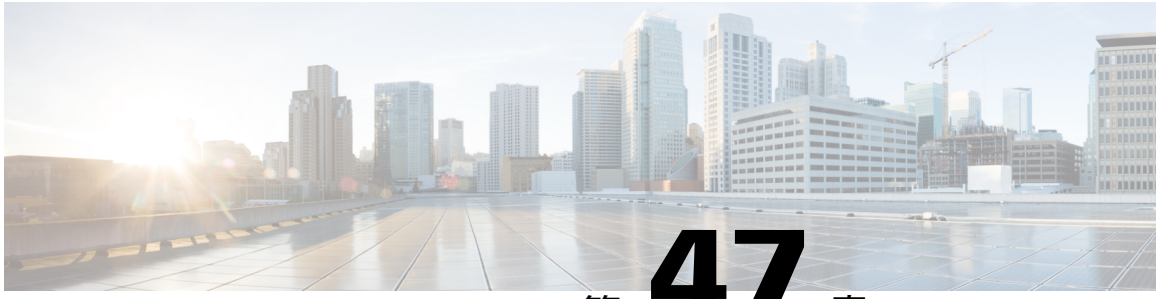
表 *60*：エンドポイントが関連付けられたユーザの制約事項

制約事項	説明
エンドユーザ情報の変更	エンドユーザの情報は、LDAP サーバとの同期が有効になっているときのみ変更できます。LDAP サーバとの同期が有効になっているかどうかを確認するには、[システム（System）] > [LDAP] > [LDAP システム（LDAP System）] を選択します。

第 VII 部

アプリケーションの統合

- アプリケーションの統合の概要，457 ページ
- アプリケーション サーバの設定，461 ページ
- プラグインのインストール，465 ページ
- プレゼンス冗長グループの設定，469 ページ
- ボイスメールおよびメッセージング向けの Cisco Unity Connection の設定，477 ページ
- Cisco Unified Contact Center Enterprise の設定，481 ページ
- Cisco Unified Contact Center Express の設定，483 ページ
- CTI アプリケーションの設定，485 ページ
- Cisco TelePresence の設定，499 ページ
- Cisco Jabber の設定，501 ページ



第 47 章

アプリケーションの統合の概要

- アプリケーションの統合，457 ページ
- アプリケーションの統合，457 ページ

アプリケーションの統合

章のこの部分では、アプリケーションを統合してシステムの機能を拡張する方法について説明します。ボイスメール、コンタクト センターの機能、表現力豊かな会議、システムの健全性を監視する機能などのさまざまな機能を追加できます。Cisco Unified Real-Time Monitoring Tool など、一部のアプリケーションはシステムに組み込まれ管理インターフェイスからダウンロードできます。Cisco Jabber や Cisco Unified Contact Center Express などの他のアプリケーションは、外部システムであり、Cisco Unified Communications Manager と相互運用するように設定できます。

アプリケーションの統合

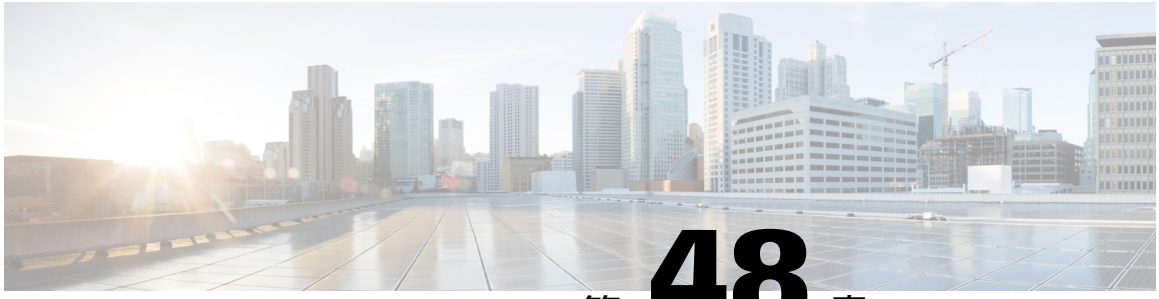
次のタスク フローを実行すると、システムの統合アプリケーションを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーションサーバのタスク フロー，（461 ページ）	アプリケーション サーバを設定して他の製品サーバをクラスタに追加し、その間のセキュアな動作を確立します。
ステップ 2	プラグインのインストールのタスク フロー，（466 ページ）	システムの機能を拡張するには、アプリケーションプラグインを使用します。

	コマンドまたはアクション	目的
ステップ 3	プレゼンス冗長グループのタスク フロー, （470 ページ）	同じクラスタからの 2 つの IM and Presence Service ノードで設定されているプレゼンス冗長グループを設定します。このグループは、IM and Presence Service クライアントとアプリケーションの冗長性とリカバリの両方を提供します。
ステップ 4	Cisco Unity Connection, （477 ページ）	ユーザにボイスメールとメッセージング機能を提供できるように、システムに Cisco Unity Connection を統合します。
ステップ 5	Cisco Unified Contact Center Enterprise, （481 ページ）	高度な分散コンタクト センターを導入するように Cisco Unified Contact Center Enterprise（Unified CCE）を設定します。Unified CCE は、インテリジェント コール ルーティング、ネットワーク対デスクトップのコンピュータ テレフォニー インテグレーション（CTI）、マルチチャネル コンタクト管理を、IP ネットワークを介してコンタクト センターのエージェントに提供します。
ステップ 6	Cisco Unified Contact Center Express, （483 ページ）	Cisco Unified Contact Center Express（Unified CCX）を設定して、単一またはデュアル サーバ導入にパッケージされた大規模なコンタクト センターの機能を提供します。
ステップ 7	CTI アプリケーションの設定タスク フロー, （487 ページ）	コンピュータ テレフォニー インテグレーション（CTI）を使用して、電話の発信、受信、管理をすると同時に、コンピュータ処理機能を活用します。CTI アプリケーションを使用すると、発信者 ID に基づいてデータベースから顧客情報を取得したり、顧客の発信を適切なカスタマー サービス担当者に顧客情報と併せて渡すために自動音声応答（IVR）システムによって収集された情報を操作したりといったタスクを実行できます。
ステップ 8	Cisco TelePresence, （499 ページ）	システムに TelePresence 機能を統合します。Unified Communications Manager が主なコール処理エージェントである場合は、Cisco Video Communications Server（VCS）を追加すると、H.323 のエンドポイントとのフル機能の相互運用性、サードパーティ製ビデオ エンドポイントとの SIP 統合インターワーキング、会議の代替ソリューションを提供できます。使用しているシステムまたは Cisco VCS と関連して動作する Cisco TelePresence Conductor を追加して、会議とマルチポイント デバイスを簡素化することもできます。TelePresence Conductor は、アドホック、ランデブー、スケジュールの複数の会議ブリッジ（Cisco MCU および TelePresence サーバ）を管理できます。
ステップ 9	Cisco Jabber の設定, （501 ページ）	ユニファイド コミュニケーション アプリケーションのスイートである Cisco Jabber を設定すると、ユーザは、どこ

	コマンドまたはアクション	目的
		からでも担当者とシームレスに対話できます。このスイートは、さまざまなプラットフォームで IM、応答可能性、オーディオとビデオ発信、ボイスメールと会議を行えるようにします。



第 48 章

アプリケーション サーバの設定

- アプリケーション サーバの概要，461 ページ
- アプリケーション サーバの前提条件，461 ページ
- アプリケーション サーバのタスク フロー，461 ページ

アプリケーション サーバの概要

アプリケーション サーバの機能を使用して、Cisco Unified Communications Manager とオフクラスタ、Cisco Unity Connection や Cisco Emergency Responder などの外部アプリケーション間の関連付けを維持します。アプリケーション サーバは、Cisco Unified Communications Manager と Cisco WebDialer などのアプリケーション間の情報も同期します。

アプリケーション サーバの前提条件

Cisco Unity と Cisco Unity Connection については、AXL Web サービスが Cisco Unity と Cisco Unity Connection サーバと通信するように設定されている Cisco Unified Communications Manager ノードで実行されていることを確認します。

アプリケーション サーバのタスク フロー

設定するアプリケーション サーバの種類に応じて、次のいずれかのタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーション サーバの設定, （462 ページ）	安全に参加し、相互運用し、クラスタ内で情報を共有するために使用するアプリケーション サーバを設定します。
ステップ 2	Cisco WebDialer サーバの設定, （463 ページ）	ユーザが入力できる文字数が制限される [WebDialers のリスト（List of WebDialers）] サービスの代替手段として、Cisco WebDialer アプリケーション サーバを設定します。[アプリケーション サーバの設定（Application Server Configuration）] ウィンドウで Cisco WebDialer アプリケーション サーバを追加したら、Cisco WebDialer Web サービスの [サービス パラメータの設定（Service Parameter Configuration）] ウィンドウの [WebDialers のリスト（List of WebDialers）] フィールドにこのサーバが表示されます。Cisco WebDialer の設定に関する詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

アプリケーション サーバの設定

安全に参加し、相互運用し、クラスタ内で情報を共有するために使用するアプリケーション サーバを設定します。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [アプリケーション サーバ（Application Server）] 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 [アプリケーション サーバ タイプ（Application Server Type）] ドロップダウン リストから、次のいずれかのサーバ オプションを選択します。

- Cisco Unity Voice Mail 4.x 以降
- Cisco Unity Connection
- CUMA プロビジョニング サーバ
- CER ロケーション管理

- リモート システム ログ サーバ

ステップ 4 [Next] をクリックします。

ステップ 5 [アプリケーション サーバの設定（Application Server Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

Cisco WebDialer サーバの設定

ユーザが入力できる文字数が制限される [WebDialers のリスト（List of WebDialers）] サービスの代替手段として、Cisco WebDialer アプリケーション サーバを設定します。[アプリケーション サーバの設定（Application Server Configuration）] ウィンドウで Cisco WebDialer アプリケーション サーバを追加したら、Cisco WebDialer Web サービスの [サービス パラメータの設定（Service Parameter Configuration）] ウィンドウの [WebDialers のリスト（List of WebDialers）] フィールドにこのサーバが表示されます。Cisco WebDialer の設定に関する詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [アプリケーション サーバ（Application Server）] 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 [アプリケーション サーバ タイプ（Application Server Type）] ドロップダウン リストから、[Cisco Web Dialer] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [ホスト名/IP アドレス（Host name/IP Address）] フィールドに、WebDialer サーバのホスト名または IP アドレスを入力します。

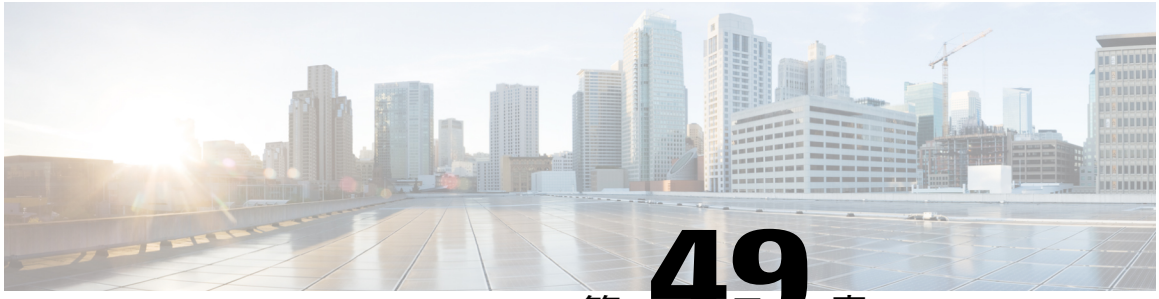
ステップ 5 [リダイレクタ ノード（Redirector Node）] ドロップダウン リストから、[<なし>（<None>）] か、特定の Unified Communications Manager ノードを選択します。
[<なし>（< None >）] の場合は、WebDialer サーバがすべてのノードを対象にすることを示します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 Cisco Unified Serviceability で [ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] を選択します。

ステップ 8 [Cisco WebDialer Web サービス（Cisco WebDialer Web Service）] オプション ボタンをクリックします。

ステップ 9 [再起動（Restart）] をクリックします。



第 49 章

プラグインのインストール

- プラグインの概要，465 ページ
- プラグインのインストールのタスク フロー，466 ページ

プラグインの概要

アプリケーション プラグインは、システムの機能を拡張します。

次のプラグインは、[アプリケーション（Application）] > [プラグイン（Plugins）] メニューから使用できます。

- Cisco AXL ツールキット：開発者は、パブリッシャ ノードでプロビジョニング オブジェクトを作成、読み取り、更新、および削除するアプリケーションを作成できます。ZIP ファイルには、SOAP over HTTP/HTTPS を使用して、AXL の要求と応答を送受信するための Java ベースのライブラリが含まれています。
- Cisco CTL クライアント：TFTP サーバに保存される証明書をデジタル署名します。このクライアントは Cisco TFTP サーバから CTL ファイルを取得し、セキュリティ トークンを使用して CTL ファイルをデジタル署名し、Cisco TFTP サーバのファイルを更新します。
- Cisco IP Phone Address Book Synchronizer：Microsoft Windows Address Book とシスコの個人用アドレス帳を同期させます。
- Cisco JTAPI クライアント：Java プログラミング言語で作成されている通信対応アプリケーション向けの標準プログラミング インターフェイスを提供します。
- Cisco TAPI クライアント：Microsoft Windows で実行中の通信対応アプリケーション向けの標準プログラミング インターフェイスを提供します。
- Cisco Tool for Auto-Registered Phone Support（TAPS）：ユーザは事前設定済みの電話の設定をリモートにダウンロードして、デバイスをプロビジョニングできます。
- Cisco Unified CM Assistant Console：アシスタントは自分のマネージャのコールをより効率的に処理できます。Assistant Console は、ログインおよびディレクトリ サービスのために、Cisco Unified Communications Manager IP Manager Assistant（IPMA）サービスに接続します。

- Cisco Unified Real-Time Monitoring Tool：クラスタで実行中のデバイスのステータス、システムパフォーマンス、デバイス検出、およびCTIアプリケーションをリアルタイムでモニタします。また、RTMT はトラブルシューティングのためにデバイスに直接接続します。

プラグインのインストールのタスク フロー

必要に応じて、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	プラグインのダウンロード, （466 ページ）	プラグインをダウンロードし、実行可能ファイルまたは ZIP ファイルからのインストール手順に従います。システムをアップグレードした後、すべてのプラグインを再インストールする必要があります。
ステップ 2	プラグイン URL の更新, （467 ページ）	（任意） ドメイン ネーム サーバ（DNS）が変更された場合は、プラグイン URL を更新します。システムのインストール時に、DNS はプラグイン URL の基礎を提供します。DNS が変更されても、URL は自動更新されません。

プラグインのダウンロード

プラグインをダウンロードし、実行可能ファイルまたは ZIP ファイルからのインストール手順に従います。システムをアップグレードした後、すべてのプラグインを再インストールする必要があります。

はじめる前に

プラグインのインストール先となるサーバで実行されている、侵入検知やウイルス対策などのサービスを一時的にすべて無効にしてください。

手順

ステップ 1 Cisco Unified CM の管理から、[アプリケーション（Application）] > [プラグイン（Plugins）] の順に選択します。

ステップ 2 検索条件を入力するか、またはダイアログボックスを空欄にして、[検索（Find）] をクリックします。
表示されたウィンドウには、アプリケーションのプラグインに関する詳細情報が含まれています。

ステップ 3 ダウンロードおよびインストールするプラグインの [ダウンロード（Download）] をクリックします。
また、[ダウンロード（Download）] を右クリックし、[名前を付けて保存（Save As）] をクリックしてフォルダを選択すると、検索が簡単です。

ステップ 4 （任意） プラグインが ZIP ファイルの場合、組み込みまたはサードパーティの ZIP プログラムを使用してファイルを解凍します。

ステップ 5 実行可能ファイルを実行するか、または必要に応じて、ZIP ファイルに格納された readme ファイルを参照します。

次の作業

実行可能ファイルの説明を参照して、プラグインをインストールしてください。

プラグイン URL の更新

ドメイン ネーム サーバ（DNS）が変更された場合は、プラグイン URL を更新します。システムのインストール時に、DNS はプラグイン URL の基礎を提供します。DNS が変更されても、URL は自動更新されません。

手順

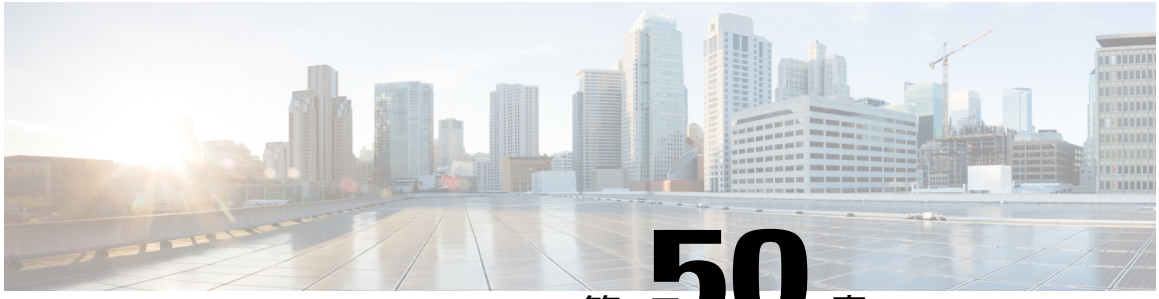
ステップ 1 Cisco Unified CM の管理から、[アプリケーション（Application）] > [プラグイン（Plugins）] の順に選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 更新するプラグイン名をクリックします。

ステップ 4 [カスタム URL（Custom URL）] フィールドに、プラグインの更新された URL を入力します。

ステップ 5 [保存（Save）] をクリックします。



第 50 章

プレゼンス冗長グループの設定

- プレゼンス冗長グループの概要，469 ページ
- プレゼンス冗長グループの前提条件，470 ページ
- プレゼンス冗長グループのタスク フロー，470 ページ
- 冗長性の連携動作と制約事項，476 ページ

プレゼンス冗長グループの概要

プレゼンス冗長グループは、同じクラスタからの 2 つの IM and Presence Service ノードで設定されています。プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。IM and Presence Service クライアントおよびアプリケーションで冗長性と回復性の両方を実現するようにプレゼンス冗長グループを設定できます。

- フェールオーバー：プレゼンス冗長グループ内の IM and Presence サービス ノード上で 1 つ以上の重要なサービスが失敗した場合、またはグループ内のノードが失敗した場合に、そのプレゼンス冗長グループ内で行われます。クライアントは、そのグループ内のもう 1 つの IM and Presence サービス ノードに自動で接続します。
- フォールバック：以下のいずれかの状況で、フォールバック コマンドが CLI または Cisco Unified Communications Manager から発行されると行われます。
  - 失敗した IM and Presence サービス ノードがサービスを再開し、すべての重要なサービスが動作している場合。そのグループのフェールオーバーが発生したクライアントは、使用可能になると回復したノードと再接続します。
  - 重要なサービスの不具合のために、アクティブ化されていたバックアップ IM and Presence サービス ノードが失敗し、ピア ノードがフェールオーバー状態であり、自動回復フォールバックをサポートしている場合。

たとえば、プレゼンス冗長グループを使用していると、ローカルの IM and Presence サービス ノードのサービスまたはハードウェアで障害が発生した場合、Cisco Jabber クライアントはバックアップ用 IM and Presence サービス ノードにフェールオーバーします。障害の発生したノードがオンラ

インに戻ると、自動フォールバックを設定している場合、クライアントはローカルのIM and Presence サービス ノードに自動的に再接続します。自動フォールバックを設定していない場合、障害の発生したノードがオンラインに戻ったらフォールバックを手動で開始できます。

冗長性と回復性に加え、プレゼンス冗長グループでは、クラスタのハイ アベイラビリティを設定することもできます。

高可用性

IM and Presence Service は複数ノードのハイ アベイラビリティ展開をサポートします。

プレゼンス冗長グループを構成した後、グループのハイ アベイラビリティを有効にできます。高可用性には、ペアのノードが必要です。各ノードには、独立型のデータベースと一連のユーザが存在し、これらは、共通のユーザをサポートできる共有アベイラビリティ データベースとともに運用されます。

すべての IM and Presence Service ノードが、プレゼンス冗長グループに属している必要があります。このグループは、単一の IM and Presence Service ノード、またはペアの IM and Presence Service ノードで構成されている場合があります。

2 つの異なるモードを使用してハイ アベイラビリティを構成できます。

- バランス モード：このモードでは、コンポーネントの障害や停電が原因で 1 つのノードが停止するイベント時に自動ユーザ ロード バランシングとユーザ フェールオーバーを含む冗長ハイ アベイラビリティを提供します。
- アクティブ/スタンバイモード：アクティブ ノードが停止すると、スタンバイ ノードはアクティブ ノードを自動的に引き継ぎます。自動ロード バランシングは行いません。

IM and Presence Service の展開をハイ アベイラビリティ展開として設定することを推奨します。シングル展開では、ハイアベイラビリティと非ハイアベイラビリティの両方を、プレゼンス冗長グループに設定しておくことが許可されますが、この設定は推奨されません。

プレゼンス冗長グループの前提条件

WAN 経由での導入では、IM およびプレゼンス クラスタごとに少なくとも 10 Mbps の専用の帯域幅が必要であり、往復遅延は 80 ミリ秒を超えないことが必要です。帯域幅がこの推奨事項未満の場合、パフォーマンスに悪影響を及ぼす場合があります。

プレゼンス冗長グループのタスク フロー

1 つの IM and Presence Service ノードは、1 つのプレゼンス冗長グループのみに割り当てることができます。高可用性を実現するには、同じクラスタから 2 つのノードをプレゼンス冗長グループに割り当て、グループの高可用性を確保する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	データベース レプリケーションの確認，（471 ページ）	データベース レプリケーションが IM and Presence サービス クラスタで設定されていることを確認します。
ステップ 2	確認サービス，（472 ページ）	重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。
ステップ 3	プレゼンス冗長グループの設定，（473 ページ）	IM and Presence Service クライアントとアプリケーションの冗長性とリカバリを提供します。
ステップ 4	障害検出パラメータの設定，（474 ページ）	これはオプションです。プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。ノードが自身のピアを監視する間隔を設定できます。
ステップ 5	高可用性を有効にする，（475 ページ）	これはオプションです。プレゼンス冗長グループを設定した際にハイ アベイラビリティを有効にしなかった場合、この手順を実行します。
ステップ 6	ユーザ割り当てモードの設定，（475 ページ）	Sync Agent が IM and Presence サービス クラスタのさまざまなノード全体にユーザを分散する方法を設定します。この設定は、システムがフェールオーバーとロード バランシングを処理する方法に影響します。

データベース レプリケーションの確認

プレゼンス冗長グループのハイ アベイラビリティを有効にする前に、データベース レプリケーションが IM and Presence サービス クラスタでセットアップされるようにします。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。SSH クライアントで、ssh *adminname@hostname* およびパスワードを入力します。

- シリアルポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils dbreplication status** コマンドを実行して、データベース テーブルのエラーまたは誤りを確認します。

ステップ 3 **utils dbreplication runtimestate** コマンドを実行して、データベース レプリケーションがノードでアクティブであることを確認します。
出力にはすべてのノードが一覧表示されます。データベース レプリケーションがセットアップされて正常であれば、各ノードの **replication setup** の値は **2** になります。

2 以外の値が返される場合は、アップグレードに進む前にエラーを解決する必要があります。

次の作業

確認サービス, （472 ページ）

確認サービス

重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。ハイ アベイラビリティをオンにする前に、重要なサービスを実行する必要があります。重要なサービスがいずれのノードでも動作していない場合、障害状態に高可用性をオンにするとプレゼンス冗長グループは Failed 状態になります。重要なサービスが 1 つのノードで実行されていない場合、高可用性をオンにすると、そのノードが他のノードにフェールオーバーします。

はじめる前に

データベース レプリケーションの確認, （471 ページ）

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、[ツール（Tools）] > [コントロールセンタ-ネットワークサービス（Control Center - Network Services）] を選択します。

ステップ 2 [サーバ（Server）] リストから、サービスを再アクティブ化するノードを選択し、[移動（Go）] をクリックします。

ステップ 3 [IM and Presenceサービス（IM and Presence Services）] で、次のサービスを有効にします。

- Cisco Client Profile Agent
- Cisco Sync Agent

- Cisco XCP Router

ステップ 4 [関連リンク（Related Links）] ドロップダウン リストから [サービスのアクティブ化（Service Activation）] を選択し、[移動（Go）] をクリックします。

ステップ 5 [IM and Presenceサービス（IM and Presence Services）] で、次のサービスを有効にします。

- Cisco SIP Proxy
- Cisco Presence Engine

次の作業

プレゼンス冗長グループの設定, （473 ページ）

プレゼンス冗長グループの設定

Cisco Unified Communications Manager を使用して、IM and Presence サービス ノードの冗長性を設定します。

各プレゼンス冗長グループには、IM and Presence サービスの 2 つのノードを含めることができます。各ノードを割り当てることができるプレゼンス冗長グループは 1 つだけです。プレゼンス冗長グループのノードはどちらも同じクラスタ上にあり、同じ IM and Presence サービス データベース パブリッシャ ノードを持つ必要があります。

はじめる前に

- 確認サービス, （472 ページ）
- プレゼンス 冗長グループに追加する IM and Presence サービス ノードが同じソフトウェア バージョンを実行していることを確認します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）] 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 プレゼンス冗長グループの一意の名前を入力します。
アンダースコア（_）およびダッシュ（-）を含む最大 128 文字の英数字を入力できます。

ステップ 4 グループの説明を入力します。
最大 128 文字の英数字と記号を入力できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 IM and Presence Serviceの 2 つの異なるノードを [プレゼンス サーバ（Presence Server）] フィールドで選択し、グループに割り当てます。

ステップ 6 （任意） [高可用性を有効にする（Enable High Availability）] チェックボックスをオンにして、プレゼンス冗長グループの高可用性を有効にします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

障害検出パラメータの設定, （474 ページ）

障害検出パラメータの設定

IM and Presence サービスは、プレゼンス冗長グループの自動障害検出メカニズムを提供します。プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。ノードが自身のピアを監視する間隔を設定できます。

はじめる前に

プレゼンス冗長グループの設定, （473 ページ）

手順

ステップ 1 Cisco Unified CM IM and Presence の管理で、[システム（System）] > [サービスパラメータ（Service Parameters）] > [Server Recovery Manager（サービス）（Server Recovery Manager (service)）] を選択します。

ステップ 2 [一般的な Server Recovery Manager パラメータ（General Server Recovery Manager Parameters）]（クラスタ全体）で、次のパラメータを設定します。

- [ハートビート間隔（Heart Beat Interval）]：このパラメータは、Server Recovery Manager が同じ冗長グループのピア Server Recovery Manager にハートビート メッセージを送信する間隔を秒単位で指定します。ハートビートは、ネットワークのアベイラビリティを判断するために使用されます。デフォルト値は 60 秒です。
- [接続タイムアウト（Connect Timeout）]：このパラメータは、Server Recovery Manager がピア Server Recovery Manager への接続要求から応答を受信するために待つ時間を秒単位で指定します。デフォルト値は 30 秒です。

（注） シスコは、これらのパラメータにデフォルト値を設定することを推奨します。

次の作業

プレゼンス冗長グループを設定した際にハイ アベイラビリティを有効にしていない場合は、高可用性を有効にする, （475 ページ）

高可用性を有効にする

注意 IM and Presence Service クラスタのレプリケーションのセットアップに失敗したが、すべての重要なサービスが実行されている場合、現在の冗長グループで有効な場合は、すぐにフェールオーバーする場合があります。

はじめる前に

- プレゼンス冗長グループの設定, （473 ページ）
- IM and Presence Service クラスタでレプリケーションがセットアップされていることを確認します。
- すべての重要なサービスが動作していることを確認します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）] を選択します。

ステップ 2 検索情報を指定し、[検索（Find）] をクリックします。

ステップ 3 設定したプレゼンス冗長グループを選択します。

ステップ 4 ハイ アベイラビリティを有効にするには、[ハイ アベイラビリティを有効にする（Enable High Availability）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

ユーザ割り当てモードの設定

この手順を使用すると、Sync Agent がクラスタ内のノードにユーザを分散させる方法を設定できます。この設定により、フェール オーバーおよびロード バランシングを管理できます。

手順

ステップ 1 Cisco Unified CM の管理から、[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。

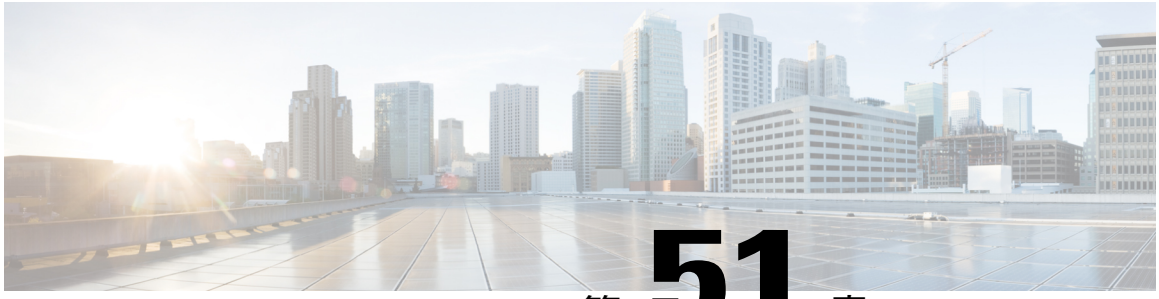
ステップ 2 [ユーザ管理パラメータ（User Management Parameters）] 領域で、[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] パラメータに次のいずれかのオプションを選択します。

- [バランス（Balanced）]：このモード（デフォルト）では、ユーザを各サブクラスタのそれぞれのノードに均等に割り当て、各ノードにユーザの合計数が均等に分散するようにします。これがデフォルトのオプションです。
- [アクティブスタンバイ（Active-Standby）]：このモードでは、サブクラスタの最初のノードにすべてのユーザを割り当て、セカンダリ サーバをバックアップのままにします。
- [なし（None）]：このモードでは、Sync Agent でクラスタのノードにユーザが割り当てられません。

ステップ 3 [保存（Save）] をクリックします。

冗長性の連携動作と制約事項

機能	データのやり取り
Multiple Device Messaging	Multiple Device Messaging 機能を使用すると、フェールオーバー時に IM and Presence サービスでサーバのリカバリに遅延が発生します。Multiple Device Messaging が設定されているシステムでサーバのフェール オーバーが発生すると、通常、[Cisco Server Recovery Manager] サービス パラメータで指定された時間の 2 倍かかります。



第 51 章

ボイスメールおよびメッセージング向けの Cisco Unity Connection の設定

- Cisco Unity Connection, 477 ページ
- Cisco Unity Connection のボイスメールとメッセージング設定タスク フロー, 479 ページ

Cisco Unity Connection

ボイスメールとメッセージングのシステムを設定する時には、ユーザの追加、機能の有効化、Cisco Unified Communications Manager と Cisco Unity Connection との統合の各オプションに注意します。

Cisco Unified Communications Manager に統合された Cisco Unity Connection（ボイスメールとメッセージングのシステム）は、AXL サービスまたは LDAP 統合を介して、手動で設定したユーザにボイスメッセージング機能を提供します。ユーザが、メールボックスでボイスメッセージを受信すると、ユーザの電話機のメッセージ待機ランプが点灯します。ユーザは、内部または外部コールでボイスメッセージングシステムにアクセスして、メッセージの取得、再生、応答、転送、削除ができます。

このシステムは直接接続とゲートウェイベースの両方をサポートするメッセージングシステムです。直接接続のボイスメッセージングシステムは、パケットプロトコルを使用して Cisco Unified Communications Manager と通信します。ゲートウェイベースのボイスメッセージングシステムは、アナログまたはデジタルトランク経由で Cisco ゲートウェイに接続することにより Cisco Unified Communications Manager に接続します。

Unified Communications Manager と Cisco Unity Connection を統合すると、ユーザに次の機能を設定できます：

- パーソナルグリーティングへの自動転送
- 通話中グリーティングへの自動転送
- 発信者 ID

- 容易なメッセージ アクセス（ユーザは、ID を入力しなくてもメッセージを取得できます。Cisco Unity Connection は、コール発信元の内線番号に基づいてユーザを識別します。パスワードが必要になる場合があります）。
- 識別されているユーザのメッセージング（Cisco Unity Connection は、転送された内線コール中にメッセージを残したユーザを、コール発信元の内線番号に基づいて自動的に識別します）。
- メッセージ待機インジケータ（MWI）

Cisco Unified Communications Manager と Cisco Unity Connection は次のいずれかのインターフェイスを介して連携します：

- SIP トランク：SIP を使用して Cisco Unity Connection と Unified Communications Manager を統合できます。従来の統合に必要な複数の SCCP ポートの代わりに、SIP は、各 Unity Connection サーバに 1 つのトランクを使用します。SIP の統合により、ボイスメール ポートとボイスメール メッセージ待機インジケータ（MWI）に電話番号を設定する必要がなくなります。
- SCCP プロトコル：ボイスメール ポートを作成して、直接接続するボイス メッセージング システムとのインターフェイスを設定します。この方法により、Unified Communications Manager と Cisco Unity Connection との間のリンクが確立します。

  ボイス メッセージング システムに複数かつ同時に接続するコールを処理するためには、複数のボイスメール ポートを作成して、そのポートを、回線グループおよびルート/ハント リスト内の回線グループに設定します。

  Cisco Unified Communications Manager は、SCCP メッセージを生成します。 Cisco Unity Connection がそのメッセージを変換します。ボイスメール システムは、メッセージ待機ランプの点滅設定のある番号をコールして、メッセージ待機インジケータ（MWI）を送信します。

  ボイスメール ポートおよび Cisco Unity SCCP デバイスのセキュリティ設定を行うと、各デバイスが他のデバイスの証明書を受け入れた後、認証済みのデバイス間で TLS 接続（ハンドシェイク）が開始されます。また、システムは、デバイス間で SRTP ストリームを送受信できるようにします。これは、デバイスに暗号化設定を行った場合の動作です。

  デバイスのセキュリティ モードに認証または暗号化を設定すると、Cisco Unity TSP は Cisco Unified Communications Manager の TLS ポートを介して Unified Communications Manager に接続します。セキュリティ モードが非セキュアの場合、Cisco Unity TSP は Cisco Unified Communications Manager の SCCP ポートを介して Unified Communications Manager に接続します。

システムに Cisco Unity Connection を統合する設定の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html で、『*Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection*』または『*Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection*』を参照してください。

Cisco Unity Connection のボイスメールとメッセージング設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unity Connection で、ボイスメールとメッセージングを設定します。	Cisco Unity Connection を設定するには、Cisco Unity Connection 向け『*Cisco Unified Communications Manager SCCP Integration Guide*』または『*Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection*』を参照してください。 http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html
ステップ 2	PIN 同期の有効化, （479 ページ）	これはオプションです。共通の PIN 同期を有効にするには、次の手順を使用します。

PIN 同期の有効化

PIN 同期を有効にし、エンド ユーザが、エクステンション モビリティ、開催中の会議、モバイル コネクト、および Cisco Unity Connection ボイスメールに同じ PIN を使用してログインできるようにするには、次の手順を実行します。

（注） Cisco Unified Communications Manager パブリッシュ データベース サーバが稼働し、そのデータベースのレプリケーションが完了した場合のみ、Cisco Unity Connection と Cisco Unified Communications Manager 間の PIN の同期に成功します。Cisco Unity Connection で PIN の同期に失敗すると、次のエラー メッセージが表示されます。`Failed to update PIN on CUCM.Reason: Error getting the pin.`

（注） PIN の同期が有効で、エンド ユーザが PIN を変更した場合は、Cisco Unified Communications Manager で PIN が更新されます。これは、設定済みの Unity Connection アプリケーション サーバの 1 台以上で PIN の更新に成功した場合のみです。

はじめる前に

この手順は、アプリケーション サーバを Cisco Unity Connection の設定にすでに接続していることを前提としています。接続していない場合は、新しいアプリケーション サーバの追加方法の詳細について、以下の「関連項目」のセクションを参照してください。

PIN 同期の機能を有効にするには、最初に、Cisco Unity Server に接続するための有効な証明書を Cisco Unified OS の管理ページから Cisco Unified Communications Manager の tomcat-trust にアップロードする必要があります。証明書をアップロードする方法の詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「"Manage Security Certificates"」の章を参照してください。 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Cisco Unity Connection サーバのユーザ ID は、Cisco Unified Communications Manager のユーザ ID と一致する必要があります。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [アプリケーション サーバ（Application Servers）] の順に選択します。

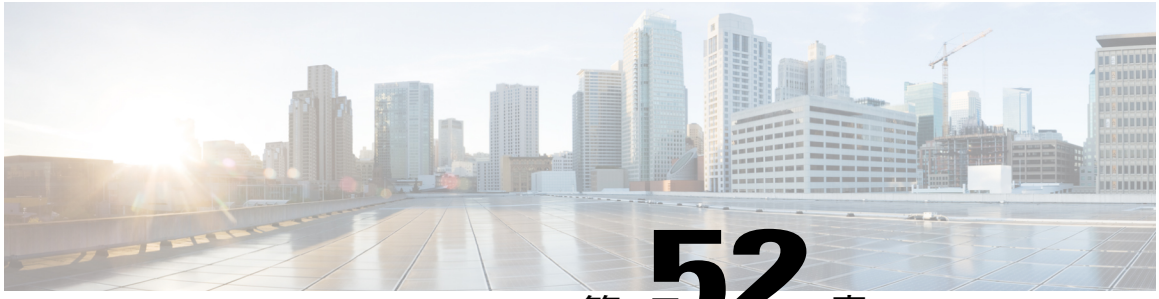
ステップ 2 Cisco Unity Connection の設定を行うアプリケーション サーバを選択します。

ステップ 3 [エンド ユーザの PIN 同期（Enable End User PIN Synchronization）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

アプリケーション サーバの設定, （462 ページ）



第 52 章

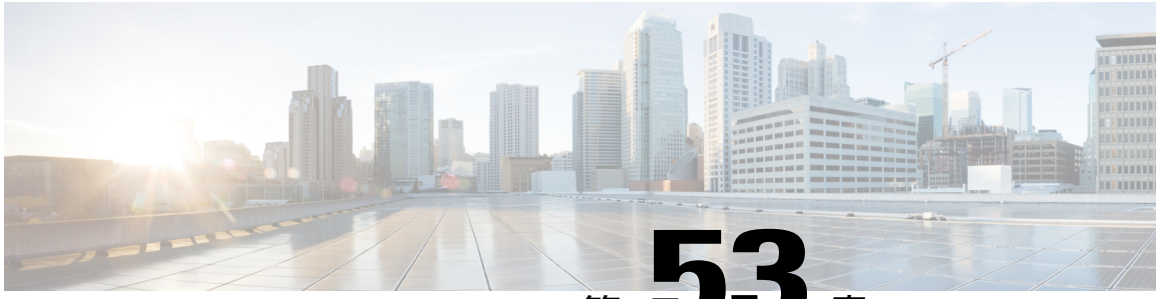
Cisco Unified Contact Center Enterprise の設定

- Cisco Unified Contact Center Enterprise, 481 ページ

Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise（Unified CCE）を使用して、インテリジェント コール ルーティング、ネットワーク対デスクトップのコンピュータテレフォニーインテグレーション（CTI）、マルチチャネルコンタクト管理を、IP ネットワークを介してコンタクトセンターのエージェントに統合できます。Unified CCE は、ソフトウェア IP 自動着信呼分配（ACD）と Cisco Unified Communications を統合して、高度な分散型コンタクト センターの迅速な展開を可能にします。

Unified CCE をシステムに統合するための設定方法の詳細については、『*Cisco Unified Contact Center Enterprise* インストレーションおよびアップグレード ガイド』（http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html）を参照してください。



第 53 章

Cisco Unified Contact Center Express の設定

- Cisco Unified Contact Center Express, 483 ページ

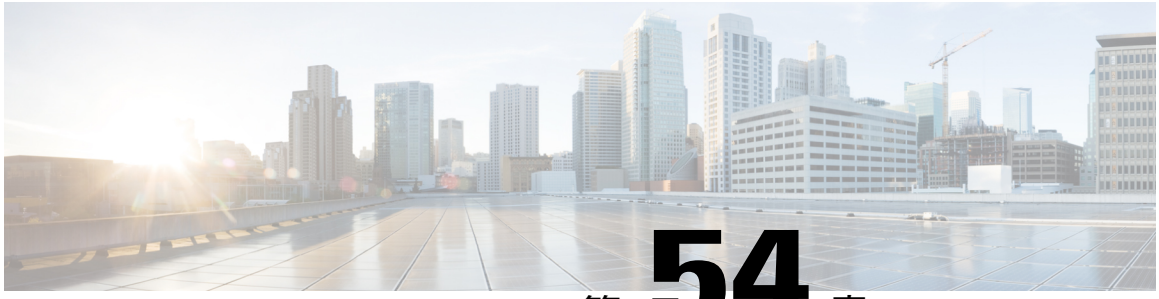
Cisco Unified Contact Center Express

Cisco Unified Contact Center Express（Unified CCX）は、シングルまたはデュアル サーバの導入において、パッケージ化された大規模なコンタクトセンターの機能をシステムに提供します。Unified CCX は、最大 400 人の同時エージェント、42 人のスーパバイザ、150 のエージェント グループ、および 150 のスキル グループに対応するように拡張できます。また、電子メール、チャット、発信コール、着信コール、ワークフォース最適化、およびレポート機能が含まれています。

Unified CCX は、Unified CCX に代わってすべてのコンタクトセンターのコールを管理する Unified Communications Manager と連携します。ヘルプ デスクに電話がかかってくると、コール システムは、それが Unified CCX アプリケーション サーバ宛の番号であることを認識します。この設定では、Unified CCX は着信コールを受信して、ダイヤルされた内線番号に基づいて要求を処理します。スクリプトでプロンプトが再生されて電話番号が収集され、必要に応じて、発信者からの情報を使用して適切なエージェントが選択されます。割り当てられたエージェントが空いていない場合、コールは適切なキューに入り、録音メッセージや音楽が発信者に流されます。エージェントが対応可能になるとすぐに、Unified CCX はそのエージェントの電話を鳴らすように Unified Communications Manager に指示します。

エージェントが電話に出ると、関連するコール コンテキストがそのエージェントのデスクトップ アプリケーションに提供されます。この手順により、お客様をサポートするための適切な情報がエージェントの目の前に表示されます。

Unified CCE をシステムに統合するための設定方法の詳細については、『*Cisco Unified CCX* アドミニストレーション ガイド』（http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-and-configuration-guides-list.html）を参照してください。



第 54 章

CTI アプリケーションの設定

- CTI アプリケーションの概要，485 ページ
- CTI アプリケーションの前提条件，487 ページ
- CTI アプリケーションの設定タスク フロー，487 ページ

CTI アプリケーションの概要

コンピュータ テレフォニー インテグレーション（CTI）を使用すると、コールを発信、受信、および管理しながらコンピュータ処理機能を利用できます。CTI アプリケーションでは、発信者 ID を使用してデータベースから顧客情報を取得するなどのタスクを実行する、または自動音声応答（IVR）システムによって収集された情報を使用して、顧客のコールを顧客情報とともに、適切なカスタマー サービス担当者にルーティングできます。

コールのメディアをルート ポイントで終端させたいアプリケーションでは、コールのメディアとポートをコール単位で指定する必要があります。CTI アプリケーションは、スタティックまたはダイナミック IP アドレスおよびポート番号を使用して、CTI ポートと CTI ルート上でメディアを終端させることができます。

この章では、CTI アプリケーションと連携させるための Cisco Unified Communications Manager の設定方法について説明します。特定のアプリケーションの設定方法の詳細については、Cisco Unified Communications Manager の機能設定ガイド [英語] を参照してください。

次に、利用可能な Cisco CTI アプリケーションをいくつか示します。

- Cisco IP Communicator：コンピュータをフル機能の電話機に変えるデスクトップ アプリケーションです。コール トラッキング、デスクトップ コラボレーション、およびオンライン電話帳からのワンクリック ダイヤルなどの機能が追加されています。
- Cisco Unified Communications Manager Auto-Attendant：Cisco Unified Communications Manager と連動して、特定の内線電話番号に対するコールを受信し、発信者が適切な内線番号を選択できるようにします。
- Cisco Web Dialer：Cisco Unified IP Phone ユーザが Web アプリケーションやデスクトップ アプリケーションからコールを発信できるようにします。

- Cisco Unified Communications Manager Assistant：マネージャとアシスタントがより効率的に連携できるようにします。この機能は、コールルーティングサービス、マネージャとアシスタントに対する電話機能の機能拡張、主にアシスタントによって使用される Assistant Console インターフェイスで構成されています。

（注） SIP IP フォンをサポートする Cisco Unified Communications Manager CTI アプリケーションについては、アプリケーション固有のマニュアルを参照してください。

CTI ルート ポイントの概要

CTI ルート ポイント仮想デバイスは、アプリケーション制御のリダイレクションに対する多重同時コールを受信できます。CTI ルート ポイントには、ユーザがアプリケーションにアクセスするためにコールできる回線を 1 つ以上設定できます。アプリケーションはルート ポイントでコールに応答でき、CTI ポートや IP フォンにコールをリダイレクトすることもできます。CTI アプリケーションがリダイレクト API を使用してコールのリダイレクトを要求すると、Cisco Unified Communications Manager はリダイレクトされた側の回線/デバイス コーリング サーチ スペースの設定を使用します。

CTI ルート ポイントでは次のことができます。

- コールへの応答
- 複数のアクティブ コールの発信と受信
- コールのリダイレクト
- コールを保留にする
- コールの保留解除
- コールのドロップ

Cisco Unified Communications Manager の CTI 冗長性

クラスタ内の Cisco Unified Communications Manager ノードで障害が発生すると、CTIManager は、該当デバイスを別の Cisco Unified Communications Manager ノード上で再度開くことで影響を受けた CTI ポートとルート ポイントを復旧します。アプリケーションに開かれている電話デバイスがある場合、その電話が別の Cisco Unified Communications Manager にフェールオーバーすると、CTIManager はその電話も再度開きます。Cisco Unified IP Phone が別の Cisco Unified Communications Manager にフェールオーバーされない場合、CTIManager はその電話またはその電話の回線を開くことができません。CTIManager はデバイス プールに割り当てられている Cisco Unified Communications Manager グループを使用して、アプリケーションが開いた CTI デバイスと電話を復旧するために使用する Cisco Unified Communications Manager を決定します。

CTIManager の CTI 冗長性

CTIManager で障害が発生すると、その CTIManager に接続されているアプリケーションは、別の CTIManager で該当デバイスを再度開くことで影響を受けたリソースを回復できます。アプリケーションは、アプリケーションの設定時にプライマリおよびバックアップとして定義した CTIManager に基づき使用する CTIManager を決定します（そのアプリケーションでサポートされている場合）。アプリケーションは、新しい CTIManager に接続すると、以前開かれていたデバイスと回線を再度開くことができます。アプリケーションは、Cisco Unified IP Phone が新しい Cisco Unified Communications Manager に再ホーム化される前にその電話を開くことができますが、再ホーム化が完了しないとその電話を制御できません。

（注） アプリケーションは、稼働状態に戻るとプライマリ CTIManager に再ホーム化されません。アプリケーションを再起動するか、バックアップ CTIManager で障害が発生すると、アプリケーションはプライマリ CTIManager にフェールバックします。

アプリケーションの障害に対する CTI の冗長性

アプリケーション（TAPI/JTAPI または CTIManager に直接接続するアプリケーション）が失敗すると、CTIManager はアプリケーションを終了し、CTI ポートとルート ポイントにある未完了のコールを設定された障害時転送（CFOF）番号にリダイレクトします。また、アプリケーションが回復してこれらのデバイスを再登録するまで、CTIManager は、これらの CTI ポートとルート ポイントへの後続のコールを、設定された無応答時転送（CFNA）番号に回します。

CTI アプリケーションの前提条件

Cisco Unified Communications Manager を CTI アプリケーションに対応するように設定する前に、事前にデバイス プールを設定しておく必要があります。

CTI アプリケーションごとに IP フォンを追加して設定します。IP フォンを追加して設定する方法の詳細については、Cisco Unified IP Phone を参照してください。

CTI アプリケーションを使用するエンド ユーザとアプリケーション ユーザを設定します。

Computer Telephony Integration（CTI）は、IPv4 アドレスと IPv6 アドレスをサポートできる JTAPI および TAPI インターフェイスを介して IP アドレス情報を提供します。IPv6 アドレスをサポートする場合は、アプリケーションが IPv6 をサポートする JTAPI/TAPI クライアント インターフェイス バージョンを使用していることを確認します。

CTI アプリケーションの設定タスク フロー

CTI アプリケーション向けに Cisco Unified Communications Manager を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	CTIManager サービスの有効化, （489 ページ）	アクティブになっていない場合、適切なサーバで CTIManager サービスをアクティブにします。
ステップ 2	CTIManager および Cisco Unified Communications Manager のサービス パラメータの設定, （489 ページ）	CTI のスーパープロバイダー機能と連携して使用される CTIManager のクラスタ全体の高度サービス パラメータを設定します。
ステップ 3	CTI ルートポイントを設定するには、次の手順を実行します。 • CTI ルート ポイントの設定, （491 ページ） • 新しいコール受け入れタイマーの設定, （491 ページ） • アクティブな多重同時コールの設定, （492 ページ） • CTI ルート ポイントの同期, （493 ページ）	アプリケーション制御のリダイレクションに複数の同時コールを受信できる 1 つ以上の CTI ルート ポイントの仮想デバイスを設定します。
ステップ 4	CTI デバイスの電話番号の設定, （493 ページ）	CTI デバイスの電話番号を設定します。
ステップ 5	デバイスとグループの関連付け, （494 ページ）	アプリケーション ユーザとエンド ユーザがアプリケーションで使用するすべてのデバイスを、適切な Cisco Unified Communications Manager グループに関連付けます（デバイス プール経由）。
ステップ 6	エンド ユーザとアプリケーション ユーザの追加, （494 ページ）	Cisco Unified Communications Manager システムで Standard CTI Enabled ユーザ グループにエンド ユーザとアプリケーション ユーザを追加することで設定されている CTI 制御可能なデバイスを CTI アプリケーションが制御できます。
ステップ 7	（オプション） アプリケーション障害時の CTI 冗長性の設定, （496 ページ）	CTIManager が、連続する 2 回の間隔でアプリケーションからメッセージを受信するまで待機する間隔を定義します。

CTIManager サービスの有効化

手順

ステップ 1 Cisco Unified Serviceability で、[ツール（Tools）] > [サービスの有効化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからノードを選択します。

ステップ 3 [CM サービス（CM Services）] セクションで、[Cisco CTIManager] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

次の作業

CTIManager および Cisco Unified Communications Manager のサービス パラメータの設定, （489 ページ）

CTIManager および Cisco Unified Communications Manager のサービス パラメータの設定

CTI のスーパー プロバイダー機能と連携して使用される CTIManager のクラスタ全体の高度サービス パラメータを設定します。

（注） 設定された制限を超えると、CTI はアラームを生成しますが、アプリケーションは、他のデバイスで動作し続けます。

はじめる前に

CTIManager サービスの有効化, （489 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）]>[サービスパラメータ（Service Parameters）] の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから [Cisco CTIManager（アクティブ）（Cisco CTIManager（Active））] を選択します。

ステップ 4 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、[詳細（Advanced）] をクリックします。

ステップ 5 [プロバイダーあたりの最大デバイス数（Maximum Devices Per Provider）] フィールドに、CTI アプリケーションで一度に開くことのできる最大デバイス数を入力します。デフォルトのデバイス数は 2000 です。

ステップ 6 [ノードあたりの最大デバイス数（Maximum Devices Per Node field）] フィールドに、すべての CTI アプリケーションで、Cisco Unified Communications Manager システムの CTIManager ノードに開くことができる最大デバイス数を入力します。デバイスのデフォルト数は 800 です。

ステップ 7 [保存（Save）] をクリックします。

次の作業

CTI ルート ポイントの設定, （491 ページ）

CTI ルート ポイントの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	CTI ルート ポイントの設定, （491 ページ）	新規の CTI ルート ポイントを追加するか、既存のポイントを変更します。
ステップ 2	新しいコール受け入れタイマーの設定, （491 ページ）	コールがルートポイントに到着したとき、アプリケーションが指定時間内に処理（受信、応答、リダイレクト）するように新しいコール受け入れタイマーを設定します。
ステップ 3	アクティブな多重同時コールの設定, （492 ページ）	ルート ポイントの同時アクティブ コール数を設定します。
ステップ 4	（オプション） CTI ルート ポイントの同期, （493 ページ）	同期して、CTI ルート ポイントに最新の設定変更を反映させます。割り込みを最小限に抑えて、適用されていない設定を適用します（たとえば、影響を受けるデバイスの一部でリセットまたは再起動を行う必要がない場合があります）。

	コマンドまたはアクション	目的

CTI ルート ポイントの設定

新規の CTI ルート ポイントを追加するか、既存のポイントを変更します。

はじめる前に

CTIManager および Cisco Unified Communications Manager のサービス パラメータの設定, （489 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [CTI ルート ポイント（CTI Route Point）] をクリックします。

ステップ 2 次のいずれかの作業を実行します。

- 既存の CTI ルート ポイントの設定を変更し、検索条件を入力し、[検索（Search）] をクリックして、結果リストから CTI ルート ポイントを選択します。
- 新しいゲートウェイを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [CTI ルート ポイント設定 （CTI Route Point Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

新しいコール受け入れタイマーの設定, （491 ページ）

新しいコール受け入れタイマーの設定

コールがルート ポイントに到着したとき、アプリケーションが指定時間内に処理（受信、応答、リダイレクト）するように新しいコール受け入れタイマーを設定します。

はじめる前に

CTI ルート ポイントの設定, （491 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [サーバ（Server）] ドロップダウン リストからノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから [Cisco CallManager（アクティブ）（Cisco CallManager (Active)）] を選択します。

ステップ 4 [CTI の新しいコール受け入れタイマー（CTI New Call Accept Timer）] フィールドで、コールに応答するまでの猶予時間を指定します。デフォルト値は 4 です。

ステップ 5 [保存（Save）] をクリックします。

次の作業

アクティブな多重同時コールの設定, （492 ページ）

アクティブな多重同時コールの設定

ルート ポイントの同時アクティブ コール数を設定します。

（注） Cisco CallManager Telephony Service Provider（TSP）を使用して、CTI ポート デバイスを制御するために TAPI アプリケーションを使用する予定がある場合、CTI ポート デバイスごとに 1 つの回線のみ設定できます。

はじめる前に

新しいコール受け入れタイマーの設定, （491 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）]>[電話番号（Directory Number）] をクリックします。

ステップ 2 [電話番号の設定（Directory Number Configuration）] ウィンドウで、[新規追加（Add New）] をクリックします。

ステップ 3 必須フィールドに入力します。

ステップ 4 [保存（Save）] をクリックします。

CTI ルート ポイントの同期

同期して、CTI ルート ポイントに最新の設定変更を反映させます。割り込みを最小限に抑えて、適用されていない設定を適用します（たとえば、影響を受けるデバイスの一部でリセットまたは再起動を行う必要がない場合があります）。

手順

ステップ 1 Cisco Unified CM の管理から [デバイス（Device）] > [CTI ルート ポイント（CTI Route Point）] の順にクリックします。

ステップ 2 [CTI ルート ポイントの検索と一覧表示（Find and List CTI Route Points）] ウィンドウで、[検索（Find）] をクリックして CTI ルート ポイントのリストを表示します。

ステップ 3 同期する CTI ルート ポイントの横にあるチェック ボックスをオンにします。ウィンドウ内のすべての CTI ルート ポイントを選択するには、一致するレコードのタイトル バーのチェック ボックスをオンにします。

ステップ 4 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。

ステップ 5 [OK] をクリックします。

CTI デバイスの電話番号の設定

CTI デバイスの電話番号を設定します。

はじめる前に

アクティブな多重同時コールの設定, （492 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [電話番号の検索と一覧表示（Find and List Directory Numbers）] ウィンドウで [新規追加（Add New）] をクリックします。

ステップ 3 [電話番号の設定（Directory Number Configuration）] ウィンドウで、必須フィールドに入力します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

デバイスとグループの関連付け, （494 ページ）

デバイスとグループの関連付け

アプリケーションユーザとエンドユーザがアプリケーションで使用するすべてのデバイスを、適切な Cisco Unified Communications Manager グループに関連付けます（デバイス プール経由）。

はじめる前に

CTI デバイスの電話番号の設定, （493 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）] をクリックします。

ステップ 2 [アプリケーション ユーザの検索および一覧表示（Find and List Application Users）] ページで、[新規追加（Add New）] をクリックします。[アプリケーション ユーザの設定（Application User Configuration）] ウィンドウが表示されます。

ステップ 3 [デバイス情報（Device Information）] ペインで、[使用可能なデバイス（Available Devices）] リストから [制御するデバイス（Controlled Devices）] リストに移動して、デバイスを関連付けます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 エンド ユーザのデバイスを関連付けるには、 [ユーザの管理（User Management）] > [エンド ユーザ（End User）] をクリックします。

ステップ 6 ステップ 2 ～ 4 を繰り返します。

次の作業

エンド ユーザとアプリケーション ユーザの追加, （494 ページ）

エンド ユーザとアプリケーション ユーザの追加

Cisco Unified Communications Manager システムで Standard CTI Enabled ユーザ グループにエンド ユーザとアプリケーション ユーザを追加することで設定されている CTI 制御可能なデバイスを CTI アプリケーションが制御できます。

はじめる前に

デバイスとグループの関連付け, （494 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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）] をクリックします。

ステップ 2 [アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）] ウィンドウで、[検索（Find）] をクリックして、現在のアクセス コントロール グループの一覧を表示します。

ステップ 3 [標準 CTI を有効にする（Standard CTI Enabled）] をクリックすると、このグループの [アクセス コントロール グループの設定（Access Control Group Configuration）] ウィンドウが表示されます。すべての CTI ユーザが [標準 CTI を有効にする（Standard CTI Enabled）] ユーザ グループに含まれることを確認します。使用可能なグループとその機能の完全な一覧については、「アクセス コントロール グループ設定のオプション」を参照してください。

ステップ 4 エンド ユーザを追加する場合は、[グループにエンド ユーザを追加（Add End Users to Group）] をクリックします。アプリケーションユーザを追加する場合は、[アプリケーションユーザをグループに追加（Add App Users to Group）] をクリックします。

ステップ 5 [Find（検索）] をクリックして現在のユーザの一覧を表示します。

ステップ 6 [標準 CTI を有効にする（Standard CTI Enabled）] ユーザ グループに割り当てるユーザのチェックボックスをオンにします。

ステップ 7 [選択項目の追加（Add Selected）] をクリックします。

次の作業

アプリケーション障害時の CTI 冗長性の設定, （496 ページ）

アクセス コントロール グループの設定オプション

（注） CTI アプリケーションは、割り当てられた指定ユーザ グループをサポートする必要があります。

（注） シスコでは、標準 CTI によるすべてのデバイスの制御に関連付けられているユーザは、標準 CTI のセキュアな接続のユーザ グループにも関連付けられていることを推奨します。

フィールド	説明
Standard CTI Allow Call Monitoring	このユーザ グループでは、アプリケーションがコールをモニタできます。

フィールド	説明
Standard CTI Allow Call Park Monitoring	このユーザ グループでは、コールがすべてのコールパークディレクトリの番号にパーク/パーク解除されるとき、アプリケーションが通知を受信できます。
Standard CTI Allow Call Recording	このユーザグループでは、アプリケーションがコールを記録できます。
Standard CTI Allow 発信者番号の変更	このユーザグループでは、サポートされているCTIアプリケーションの発信側番号をアプリケーションが変更できます。
Standard CTI Allow Control of All Devices	このユーザ グループでは、システムのCTI制御可能なデバイスをアプリケーションが制御またはモニタできます。
SRTP キー材料の Standard CTI Allow の受け取り	このユーザグループでは、暗号化されたメディアのストリームの復号に必要な情報をアプリケーションが受け取ることができます。このグループは通常、録音とモニタリングの目的で使用されます。
[標準CTIを有効にする（Standard CTI Enabled）]	すべての CTI アプリケーションに必要なこのユーザグループでは、アプリケーションがCisco Unified Communications Manager に接続し、CTI の機能を利用できます。
Standard CTI Secure Connection	このグループに入るためには、アプリケーションが Cisco Unified Communications Manager にセキュア（TLS）な CTI 接続が可能で、Cisco Unified Communications Manager のクラスタのセキュリティが有効になっていることが必要です。

アプリケーション障害時の CTI 冗長性の設定

CTIManager が、連続する 2 回の間隔でアプリケーションからメッセージを受信するまで待機する間隔を定義します。

はじめる前に

エンド ユーザとアプリケーション ユーザの追加, （494 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [サーバ（Server）] ドロップダウン リストからノードを選択します。

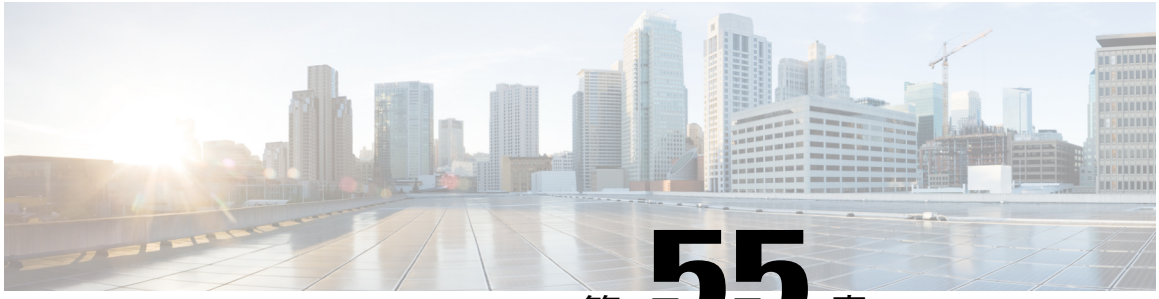
ステップ 3 [サービス（Service）] ドロップダウン リストから [Cisco CTIManager（アクティブ）（Cisco CTIManager (Active)）] を選択します。

ステップ 4 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、[詳細（Advanced）] をクリックします。

ステップ 5 [アプリケーション ハートビート最小間隔（Application Heartbeat Minimum Interval）] フィールドで、最小間隔の時間を入力します。デフォルトは 5 です。

ステップ 6 [アプリケーション ハートビート最大間隔（Application Heartbeat Maximum Interval）] フィールドで、最大間隔の時間を入力します。デフォルトは 3600 です。

ステップ 7 [保存（Save）] をクリックします。



第 55 章

Cisco TelePresence の設定

- Cisco TelePresence, 499 ページ

Cisco TelePresence

Cisco TelePresence Conductor

Cisco TelePresence Conductor によって、マルチパーティのビデオ通信が容易になります。Cisco TelePresence Conductor は、ビデオ通信ネットワーク内に配置され、1 つ以上の会議ブリッジと 1 つ以上のコール制御デバイス（Cisco TelePresence Video Communication Server（Cisco VCS）または Unified Communications Manager）と連動して機能します。自発的な会議やランデブー会議を簡単にプロビジョニング、開始、アクセス、および管理できるようにビデオ ネットワークを設定できます。

アドホック会議の場合、Unified Communications Manager と TelePresence Conductor 間で SIP トランクが使用されます。Unified Communications Manager の SIP トランクの宛先として、関連する TelePresence Conductor のロケーションのアドホック IP アドレスを設定します。このロケーションのアドホック コールは、その SIP トランクにルーティングできます。

ランデブー会議の場合、Unified Communications Manager と TelePresence Conductor 間で別の SIP トランクが使用されます。Unified Communications Manager の SIP トランクの宛先として、関連する TelePresence Conductor のロケーションのランデブー IP アドレスを設定します。このロケーションのランデブー コールは、その SIP トランクにルーティングできます。

Cisco TelePresence Conductor とともにシステムを設定する方法の詳細については、導入ガイド（http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html）を参照してください。

Cisco TelePresence 会議ブリッジ

Cisco TelePresence Server は、Cisco Unified Communications Manager と連携してユニファイド コミュニケーションの導入環境にマルチパーティ ビデオ機能を提供するスケーラブルなビデオ会議ブ

リッジです。マルチパーティ ビデオ会議に、柔軟なビデオ、音声、およびコンテンツ共有機能を提供します。標準ベースのビデオ エンドポイント、モバイル デバイス、Cisco WebEx クライアント、およびサードパーティ ビデオエンドポイントを使用して、会議の作成、開始、および参加を簡単に行うことができます。

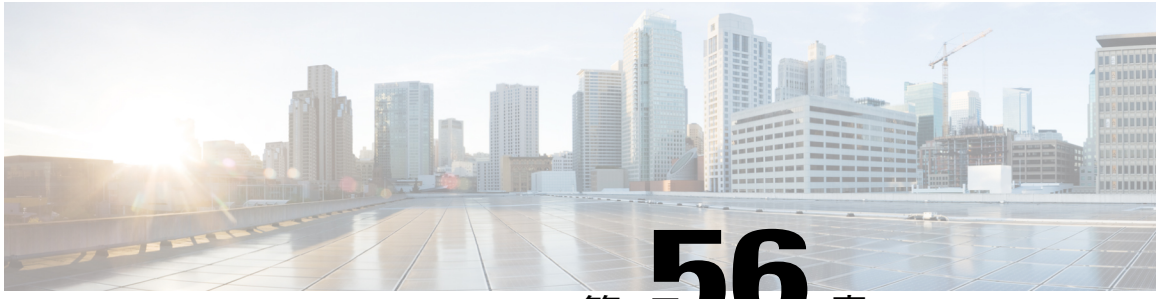
Cisco TelePresence Multipoint Control Unit（MCU）は、高画質のマルチポイント ビデオ会議ブリッジです。最大で毎秒 1080 p/30 フレーム、すべての会議の完全な連続表示、フル トランスコーディングを提供し、高解像度エンドポイントが混在した環境を設定する場合に適しています。Cisco TelePresence MCU は、シグナリング コール制御プロトコルとして SIP をサポートしています。組み込みの Web サーバがあり、システムおよび会議の完全な設定、制御、モニタリングが可能です。

Cisco TelePresence Server は、主に Cisco TelePresence Conductor によって制御されます。システム内でのこれらの会議ブリッジの設定方法の詳細については、導入ガイド（http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html）を参照してください。

Cisco TelePresence Video Communication Server

Cisco TelePresence Video Communication Server（VCS）は、テレプレゼンス会議のセッション管理と制御を簡素化します。VCS は、Cisco TelePresence Management Suite（Cisco TMS）と連携して、セキュアな通信、簡素化された大規模プロビジョニング、ネットワーク管理を実現します。VCS は Cisco Unified Communications Manager（Unified Communications Manager）と相互に作用して、システムに多彩なテレプレゼンス サービスを提供します。

Cisco TelePresence VCS をシステムと統合するための設定方法の詳細については、導入ガイド（http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html）を参照してください。



第 56 章

Cisco Jabber の設定

- Cisco Jabber の設定，501 ページ
- Cisco Jabber のインタラクションと制限事項，502 ページ

Cisco Jabber の設定

Cisco Jabber は、あらゆる場所から連絡先とのシームレスな対話を実現する Unified Communications アプリケーション スイートです。Cisco Jabber は、IM、プレゼンス、音声およびビデオ通話、ボイスメール、および会議を提供します。

Cisco Jabber 製品ファミリには、次のようなアプリケーションが含まれています。

- Cisco Jabber for Android
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Mac
- Cisco Jabber for Windows

Cisco Jabber 製品スイートの詳細については、https://www.cisco.com/go/jabber を参照してください。

Cisco Jabber と連携するようにシステムを設定する方法の詳細については、『*Cisco Jabber* 導入およびインストレーション ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html）を参照してください。

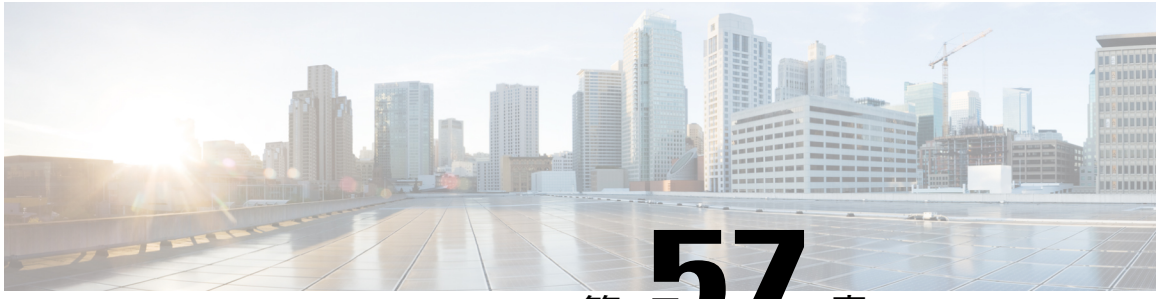
Cisco Jabber のインタラクションと制限事項

機能	インタラクション
グレースフル登録	グレースフル登録は、（オフィスのラップトップとホーム オフィスのラップトップの両方で Jabber を実行している場合など）デバイス名が同じ 2 つの Cisco Jabber クライアントからの二重登録に対応しています。この機能では、最初の登録が自動的に登録解除されるため、2 番目の登録を続けることができます。登録が解除された Jabber クライアントは再登録されません。 グレースフル登録は、Jabber がモバイルおよびリモート アクセス（MRA）環境に導入されている場合を除き、Cisco Jabber では自動的にサポートされます。MRA 環境では、登録解除された Jabber クライアントは再登録を試みます。 MRA 環境では、デバイス名が同じ 2 台のデバイス上で Cisco Jabber を実行している場合は、1 台のデバイスから Jabber をログアウトしてからもう 1 台のデバイスを使用してください。

第 VIII 部

メディア リソースの設定

- メディア リソースの概要，505 ページ
- メディア リソースの定義，507 ページ
- トラステッド リレー ポイントの設定，515 ページ
- アナンシエータの設定，525 ページ
- 自動音声応答の設定，535 ページ
- Video On Hold サーバの設定，543 ページ
- アナウンスの設定，547 ページ
- 会議ブリッジの設定，553 ページ
- フレキシブル DSCP マーキングおよびビデオ プロモーションの設定，563 ページ
- トランスコーダおよびメディア ターミネーション ポイントの設定，573 ページ



第 57 章

メディア リソースの概要

- メディア リソースについて，505 ページ
- メディア リソースの設定，505 ページ

メディア リソースについて

Cisco Unified Communications Manager の機能では、メディア リソースが使用されます。メディア リソースにより、アナンシエータ、自動音声応答（IVR）、トランスコーディング、会議、保留音、メディア ターミネーションなどのサービスが提供されます。

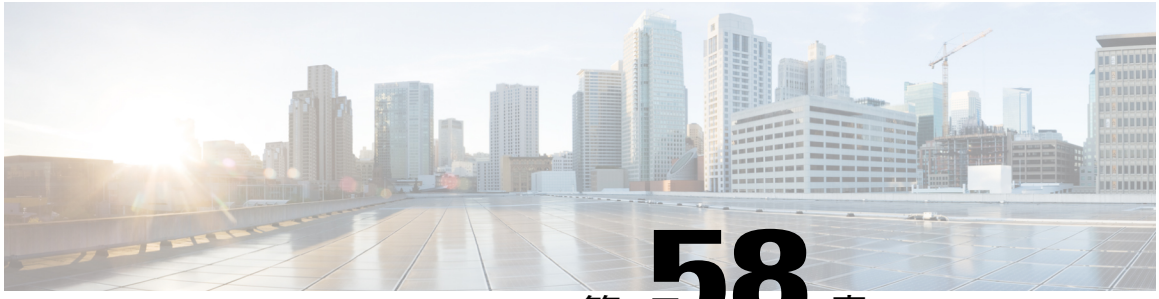
メディア リソースの設定

次のタスク フローを実行すると、システムのメディア リソースを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	メディア リソース グループのタスク フロー，（508 ページ）	この章の手順を使用して、メディア サーバの論理グループを定義します。
ステップ 2	トラステッド リレー ポイントのタスク フロー，（516 ページ）	トラステッド リレー ポイントをメディア ストリームに挿入し、そのストリームのコントロール ポイントとして機能させます。このデバイスを使用すると、そのストリームにさらに処理を加えることができます。また、ストリームが確実に特定のパスを辿るようにする手段として使用することもできます。
ステップ 3	アナンシエータ設定タスク フロー，（528 ページ）	Cisco Unified Communications Manager が事前に録音されたアナウンス（.wav ファイル）を再生したり、Cisco

	コマンドまたはアクション	目的
		Unified IP Phone やシスコの Multilevel Precedence and Preemption 対応として設定されているゲートウェイなどのデバイスにトーンを送信したりできるように、アナンシエータを設定します。
ステップ 4	自動音声応答の設定のタスク フロー, （537 ページ）	自動音声応答（IVR）デバイスを使用して、Cisco Unified IP Phone やゲートウェイなどのデバイスに対して事前に録音された機能アナウンスメント（.wav ファイル）を再生できます。これらのアナウンスは、開催中の会議などの、IVR アナウンスが必要な機能を使用するデバイスで再生されます。
ステップ 5	保留ビデオ設定のタスク フロー, （544 ページ）	ビデオ コンタクト センターにコールを発信する顧客が、コンタクトセンターでのエージェントとの最初のコンサルティングの後に、特定のビデオを視聴できるように、ビデオ コンタクト センターに Video On Hold を設定します。
ステップ 6	アナウンスの設定タスク フロー, （548 ページ）	この章の手順を使用して、事前定義済みのアナウンスを使用するか、またはカスタム アナウンスをアップロードできます。
ステップ 7	会議ブリッジの設定タスク フロー, （561 ページ）	アドホック/ミートミー ビデオ会議およびビデオ会議を可能にするソフトウェアとハードウェアのアプリケーションを設定します。
ステップ 8	DSCP の設定構成のタスク フロー, （565 ページ）	フレキシブル DSCP マーキングおよびビデオ プロモーションを使用して、コールアドミッション制御（CAC）と Quality of Service（QoS）の処理でどのアプリケーションを最も優先するかを指定するポリシーを設定できます。
ステップ 9	トランスコーダと MTP 設定のタスク フロー, （579 ページ）	1 つのコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換するために、トランスコーダを設定します。



第 58 章

メディア リソースの定義

- メディア リソース グループの概要，507 ページ
- [メディアリソースグループリスト（Media Resource Group List）]，508 ページ
- メディア リソース グループの前提条件，508 ページ
- メディア リソース グループのタスク フロー，508 ページ
- メディア リソース グループの連携動作と制約事項，513 ページ

メディア リソース グループの概要

メディア リソース グループは、メディア サーバの論理グループを定義します。必要に応じて、メディアリソースグループを地理的な場所またはサイトと関連付けることができます。さらに、サーバの使用または必要なサービスの種類（ユニキャストまたはマルチキャスト）を制御するメディア リソース グループを形成することもできます。

システムにはメディア リソースを管理する 2 層構造のアプローチがあります。

- メディア リソース グループ：メディア サーバの論理グループ。
- メディア リソース グループ リスト：メディア リソース グループの優先順位を付けたリスト。アプリケーションは、[メディアリソースグループリスト（Media Resource Group List）] で定義された優先順位に従って、使用可能なメディア リソースから必要なメディア リソース（保留音サーバなど）を選択します。デバイス関連付けられるメディア リソース グループ リストは、メディア リソース グループの冗長性を提供します。

次のタイプのデバイスをグループ化して、メディア リソース グループを作成できます。

- 会議ブリッジ（CFB）
- メディア ターミネーション ポイント（MTP）
- 保留音サーバ（MOH）
- トランスコーダ（XCODE）

- アナンシエータ（ANN）

（注） メディア リソースを設定した後に、メディア リソース グループを定義していない場合、すべてのメディア リソースはデフォルト グループに属し、すべてのメディア リソースが、特定のクラスタにあるすべての Cisco Unified Communications Manager で使用可能になります。

[メディアリソースグループリスト（Media Resource Group List）]

メディア リソース グループ リストは、優先順位順に並べられたメディア リソース グループを提供します。アプリケーションは、[メディア リソース グループ リスト（Media Resource Group List）] で定義された優先順位に従って、使用可能なメディア リソースから必要なメディア リソース（保留音サーバなど）を選択します。デバイスまたはデバイス プールに関連付けられるメディア リソース グループ リストは、メディア リソース グループの冗長性を提供します。

メディア リソース グループの前提条件

Cisco Unified Communications Manager に、アナンシエータ、トランスコーディング、会議、保留音、およびメディアターミネーションなどのサービスを提供するためのメディア リソースが存在することを確認します。

メディア リソース グループのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	メディア リソース グループの設定，（509 ページ）.	メディア リソース グループを設定し、メディア サーバの論理グループを定義します。
ステップ 2	メディア リソース グループへのデバイスの割り当て，（510 ページ）.	メディア リソース グループにデバイスを割り当てます。 （注） デバイスの割り当て順序は重要ではありません。
ステップ 3	メディア リソース グループ リストの作成，（510 ページ）.	メディア リソース グループ リストを作成し、優先順位付けされたメディア リソース グループのリストを指定します。デバイスまたはデバイス プールに関連付けられたメディア リソース グループによって、メディア リソース グループの冗長性が提供されます。

	コマンドまたはアクション	目的
		（注） デバイスの割り当て順序は重要です。
ステップ 4	メディア リソース グループ リストへのメディア リソース グループの割り当て，（511 ページ）．	新しく作成したメディア リソース グループをメディア リソース グループ リストに割り当てます。
ステップ 5	デバイスまたはデバイス プールへのメディア リソース グループ リストの割り当て，（512 ページ）．	既存または新しく作成したメディア リソース グループ リストをデバイスまたはデバイス プールに割り当てます。
ステップ 6	（任意）メディア リソース冗長性の設定，（513 ページ）。	メディア リソースに障害が発生した場合のメディア リソースの冗長性を確認します。

メディア リソース グループの設定

メディア リソース グループは、メディア リソース グループ リストのメンバーとして設定されています。メディア リソース グループと、電話などデバイスを関連付けることができます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[メディア リソース（Media Resources）] > [メディア リソース グループ（Media Resource Group）] を選択します。

ステップ 2 既存のメディア リソース グループを設定するには、[メディア リソース グループの検索と一覧表示（Find and List Media Resource Group）] ウィンドウから、該当するフィルタを指定し、[検索（Find）] をクリックします。

ステップ 3 新しいメディア リソース グループを設定するには、[新規追加（Add New）] をクリックします。

ステップ 4 [メディア リソース グループの設定（Media Resource Group Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [名前（Name）] フィールドに、メディア リソース グループの名前を入力します。

ステップ 6 （オプション）保留音の音声用にマルチキャストを使用するには、[MOHの音声にマルチキャストを使用（Use Multi-cast for MOH Audio）]チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

メディア リソース グループへのデバイスの割り当て，（510 ページ）．

メディア リソース グループへのデバイスの割り当て

アナンシエータ（ANN）、音声自動応答（IVR）、会議ブリッジ（CFB）、メディア ターミネーション ポイント（MTP）、保留音（MOH）サーバ、およびトランスコーダなどのデバイスをメディアリソースグループへ割り当てることができます。デバイスを割り当てる順番は重要ではありません。

はじめる前に

メディア リソース グループの設定, （509 ページ）.

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[メディア リソース（Media Resources）] > [メディア リソース グループ（Media Resource Group List）] を選択します。

ステップ 2 既存のメディア リソース グループを設定するには、[メディア リソース グループの検索と一覧表示（Find and List Media Resource Group）] ウィンドウで、適切なフィルタを指定して [検索（Find）] をクリックします。

ステップ 3 新しいメディア リソース グループを設定する場合、[新規追加（Add New）] をクリックします。

ステップ 4 [使用可能なメディア リソース（Available Media Resources）] フィールドで、1 つまたは複数のデバイスを選択し、下矢印キーをクリックします。
選択したデバイスが [選択されたメディア リソース（Selected Media Resources）] フィールドに表示されます。

ステップ 5 [保存（Save）] をクリックします。

次の作業

メディア リソース グループ リストの作成, （510 ページ）.

メディア リソース グループ リストの作成

はじめる前に

メディア リソース グループへのデバイスの割り当て, （510 ページ）.

手順

ステップ 1 Cisco Unified CM の管理で、[メディア リソース（Media Resources）] > [メディア リソース グループ リスト（Media Resource Group List）] を選択します。

ステップ 2 既存のメディア リソース グループ リストを設定するには、検索パラメータを入力してメディア リソース グループ リストを見つけます。

すべての条件に一致したレコードが [メディア リソース グループ リストの設定（Media Resource Group List Configuration）] ウィンドウに表示されます。

ステップ 3 新しいメディア リソース グループ リストを設定するには、[新規追加（Add New）] をクリックします。

ステップ 4 [メディア リソース グループ リストの設定（Media Resource Group List Configuration）] ウィンドウで次のフィールドを設定します。

- [名前（Name）]：メディア リソース グループ リストの名前を入力します。
- [使用可能なメディア リソース（Available Media Resources）]：このリストから、1 つまたは複数のメディア リソースを選択します。
- [選択されたメディア リソース（Selected Media Resources）]：矢印キーを使用して、マルチキャストに使用する 1 つまたは複数のメディア リソースを選択します。

ステップ 5 [メディア リソース グループ リストの設定（Media Resource Group List Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。
メディア リソース グループ リストが作成されます。Cisco Unified Communications Manager はこのリストを使用して保留音のリソースを割り当てます。

次の作業

メディア リソース グループ リストへのメディア リソース グループの割り当て, （511 ページ）.

メディア リソース グループ リストへのメディア リソース グループの割り当て

はじめる前に

メディア リソース グループ リストの作成, （510 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[メディア リソース（Media Resources）] > [メディア リソース グループ（Media Resource Group）] の順に選択します。

ステップ 2 既存のメディア リソース グループを設定するには、[メディア リソース グループの検索と一覧表示（Find and List Media Resource Group）] ウィンドウから、適切なフィルタを指定して [検索（Find）] をクリックします。

ステップ 3 [使用可能なメディア リソース（Available Media Resources）] リストから、1 つまたは複数のメディア リソースを選択して、下矢印キーをクリックします。

選択されたメディア リソースが [選択されたメディア リソース（Selected Media Resources）] リストに表示されます。

ステップ 4 [保存（Save）] をクリックします。

次の作業

デバイスまたはデバイス プールへのメディア リソース グループ リストの割り当て，（512 ページ）.

デバイスまたはデバイス プールへのメディア リソース グループ リストの割り当て

はじめる前に

メディア リソース グループ リストへのメディア リソース グループの割り当て，（511 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] の順に選択します。

ステップ 2 メディア リソース グループ リストを検索してデバイスまたはデバイス プールに割り当てるには、[電話の検索と一覧表示（Find and List Phones）] ウィンドウから、適切なフィルタを指定して [検索（Find）] をクリックします。

ステップ 3 使用可能なリストから 1 つまたは複数のデバイスまたはデバイス プール選択します。

ステップ 4 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。
デバイス名および適切な設定変更を示した [設定の適用（Apply Configuration）] ウィンドウが表示されます。

ステップ 5 メディア リソース グループ リストをデバイスに割り当てるには、デバイスのリンクをクリックします。

ステップ 6 [電話の設定（Phone Configuration）] ウィンドウの [デバイス情報（Device Information）] セクションで、[メディア リソース グループ リスト（Media Resource Group List）] ドロップダウン リストから値を選択します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。
デバイス名および適切な設定変更を示した [設定の適用（Apply Configuration）] ウィンドウが表示されます。

ステップ 9 [OK] をクリックします。

次の作業

（任意）メディア リソース冗長性の設定，（513 ページ）。

メディア リソース冗長性の設定

メディア リソース グループ リストでは、メディア リソース グループの優先リストを指定して、メディア リソースの冗長性を確保します。アプリケーションは、メディア リソース リストで定義されている優先順位に従って、使用できる対象から必要なメディア リソースを選択できます。

メディア リソース グループおよびメディア リソース リストに冗長性を設定するには、「メディア リソース グループの設定, （509 ページ）」と「[メディアリソースグループリスト（Media Resource Group List）], （508 ページ）」の手順を実行します。

メディア リソース グループの連携動作と制約事項

メディア リソース グループの連携動作

表 *61*：メディア リソース グループの連携動作

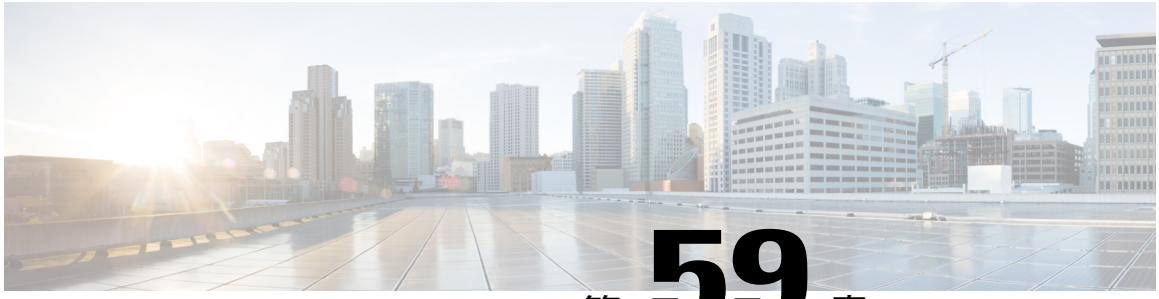
機能	データのやり取り
呼処理	メディア リソース グループ リストを選択している場合、コール処理では、デバイス レベルでメディア リソース グループ リストが使用されます。リソースが見つからない場合、コール処理はデフォルトの割り当てからリソースを取得できます。 コール処理は、デバイス レベルでメディア リソース グループ リストが選択されていない場合のみ、デバイス プール内のメディア リソース グループ リストを使用します。リソースが見つからない場合、コール処理はデフォルトの割り当てからリソースを取得できます。
アナンシエータ リソースのサポート	Cisco Unified Communications Manager は、アナンシエータを含むメディア リソース グループ リストが会議ブリッジの存在するデバイスプールに割り当てられている場合に、会議ブリッジにアナンシエータ リソースのサポートを提供します。 Cisco Unified Communications Manager は、メディア リソース グループ リストが電話会議を制御するデバイスに直接割り当てられている場合には、会議ブリッジ向けにアナンシエータ リソースのサポートを提供しません。

機能	データのやり取り
ビデオ会議	ユーザがビデオ会議の開催を望む場合にのみビデオ会議ブリッジが使用されるようにするには、ビデオ会議ブリッジをメディア リソース グループに追加します。メディア リソース グループをメディア リソース グループ リストに追加し、ビデオ会議ブリッジを使用するデバイスまたはデバイス プールにメディア リソース グループ リストを割り当てます。

メディア リソース グループの制約事項

表 *62* : メディア リソース グループの制約事項

制約事項	説明
メディア リソース グループの削除	メディア リソース グループ リストに割り当てられたメディア リソース グループを削除することはできません。
トランスコーダの削除	メディア リソース グループに割り当てられたトランスコーダは削除できません。
メディア リソースの削除	メディア リソース グループから最初にリソースを削除するか、またはメディア リソースを含むメディア リソース グループを削除しない限り、会議ブリッジなどのメディア リソース グループに属するメディア リソースを削除することはできません。



第 59 章

トラステッド リレー ポイントの設定

- トラステッド リレー ポイントの概要，515 ページ
- トラステッド リレー ポイントのタスク フロー，516 ページ
- トラステッド リレー ポイントの連携動作と制約事項，521 ページ

トラステッド リレー ポイントの概要

トラステッドリレーポイント（TRP）はメディアストリームに挿入可能なデバイスで、そのストリームのコントロール ポイントとして機能します。TRP を使用すると、そのストリームにさらに処理を加えることができます。また、ストリームが特定のパスを通るようにする手段として TRP を使用することも可能です。TRP の機能には 2 つのコンポーネントがあります。

- Cisco Unified Communications Manager が TRP を呼び出すために使用するロジック。
- コールのアンカー ポイントとして呼び出される実際のデバイス。たとえば、メディア ターミネーション ポイント（MTP）デバイスは、そのようなアンカー ポイントとして機能できます。

Cisco Unified Communications Manager は、個々の電話デバイスに設定パラメータを提供します。このパラメータにより、その電話機から発信される、または電話機に着信するすべてのコールで TRP が呼び出されます。TRP リソースの管理には、メディア リソース プール メカニズムが利用されます。その電話機のメディア リソース プールには、TRP として呼び出し可能なデバイスが含まれている必要があります。

トラステッド リレー ポイントのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスのトラステッドリレーポイントの設定, （516 ページ）.	メディアが終端する1つ以上のデバイスにトラステッド リレー ポイント（TRP）を設定し、TRP を Cisco Unified Communications Manager に挿入します。
ステップ 2	メディア ターミネーション ポイントのトラステッド リレー ポイントの設定, （517 ページ）.	デバイスをトラステッドリレー ポイントとして使用できるように、メディア ターミネーション ポイント（MTP）を設定します。 （注） Cisco Unified Communications Manager に TRP として設定されているデバイスが、TRP とコールに関与するエンドポイントとの間に適切なネットワーク接続と設定を保持していることを確認します。
ステップ 3	トランスコーダに対するトラステッド リレー ポイントの設定, （518 ページ）.	デバイスをトラステッドリレー ポイントとして使用できるように、トランスコーダを設定します。 （注） Cisco Unified Communications Manager に TRP として設定されているデバイスが、TRP とコールに関与するエンドポイントとの間に適切なネットワーク接続と設定を保持していることを確認します。
ステップ 4	トラステッド リレー ポイントのサービス パラメータの有効化, （519 ページ）.	TRP リソースが使用できない場合に、TRP を必要とするコールのさらなる処理を許可するかどうかを決定するには、TRP サービス パラメータを有効にします。

デバイスのトラステッド リレー ポイントの設定

メディアの終端である 1 つまたは複数のデバイスのトラステッド リレー ポイント（TRP）を設定したり、Cisco Unified Communications Manager に TRP を挿入できます。デバイスの TRP を設定することによって、デバイスは、そのストリームでさらに処理を実行したり、ストリームが特定のパスをたどっていることを確認できます。

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通デバイス設定（Common Device Configuration）] の順に選択します。

ステップ 2 既存デバイスのトラステッド リレー ポイントを設定するには、[共通デバイス設定の検索と一覧表示（Find and List Common Device Configurations）] ウィンドウから、適切なフィルタを指定して [検索（Find）] をクリックします。

ステップ 3 新規デバイスのトラステッド リレー ポイントを設定するには、[共通デバイス設定（Common Device Configuration）] ウィンドウから、[新規追加（Add New）] をクリックします。

ステップ 4 [共通デバイス設定（Common Device Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [共通デバイス設定情報（Common Device Configuration Information）] セクションで、[トラステッド リレー ポイントを使用（Use Trusted Relay Point）] チェック ボックスをクリックします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

メディア ターミネーション ポイントのトラステッド リレー ポイントの設定, （517 ページ）.

メディア ターミネーション ポイントのトラステッド リレー ポイントの設定

デバイスをトラステッド リレー ポイント（TRP）として利用できるようにメディア ターミネーション ポイント（MTP）を設定できます。

はじめる前に

デバイスのトラステッド リレー ポイントの設定, （516 ページ）.

手順

ステップ 1 Cisco Unified CM の管理で、[メディア リソース（Media Resources）] > [メディア ターミネーション ポイント（Media Termination Point）] を選択します。

ステップ 2 既存のメディア ターミネーション ポイントに TRP を設定するには、[メディアターミネーション ポイントの検索と一覧表示（Find and List Media Termination Points）] ウィンドウから、該当するフィルタを指定し、[検索（Find）] をクリックします。

ステップ 3 新しいメディア ターミネーション ポイントに TRP を設定するには、[新規追加（Add New）] をクリックします。

ステップ 4 [メディア ターミネーション ポイントの設定（Media Termination Point Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 5 [メディア ターミネーション ポイント情報（Media Termination Point Information）] セクションで、[トラステッド リレー ポイントを使用（Use Trusted Relay Point）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

トランスコーダに対するトラステッド リレー ポイントの設定, （518 ページ）.

トランスコーダに対するトラステッド リレー ポイントの設定

トラステッド リレー ポイント（TRP）としてデバイスを使用できるようにトランスコーダを設定できます。

はじめる前に

メディア ターミネーション ポイントのトラステッド リレー ポイントの設定, （517 ページ）.

手順

ステップ 1 Cisco Unified CM の管理で、[メディア リソース（Media Resources）] > [トランスコーダ（Transcoder）] の順に選択します。

ステップ 2 既存のトランスコーダに対する TRP を設定するには、[トランスコーダの検索と一覧表示（Find and List Trancoder）] ウィンドウから、該当するフィルタを指定し、[検索（Find）] をクリックします。

ステップ 3 新しいトランスコーダに対して TRP を設定するには、[新規追加（Add New）] をクリックします。

ステップ 4 [トランスコーダの設定（Transcoder Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [メディア サーバ トランスコーダ情報（Media Server Transcoder Info）] セクションで、[トラステッド リレーポイントを使用（Use Trusted Relay Point）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

次の作業

トラステッド リレー ポイントのサービス パラメータの有効化, （519 ページ）.

トラステッド リレー ポイントのサービス パラメータの有効化

TRP サービス パラメータを有効にすると、TRP リソースが使用できない場合に、TRP を必要とするコールの続行を許可するかどうかを決定できます。

はじめる前に

トランスコーダに対するトラステッド リレー ポイントの設定, （518 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）]>[サービス パラメータ（Service Parameters）] の順に選択します。
[サーバ（Server）] ドロップダウン リストのみが表示されます。

ステップ 2 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、[サーバ（Server）] ドロップダウン リストからサーバを選択します。
[サービス（Service）] ドロップダウン リストが表示されます。

ステップ 3 [サーバ（Server）] ドロップダウン リストから、Cisco Unified Communications Manager サーバを選択します。
選択されたサーバおよびサービスに基づいて、サービス パラメータが表示されます。

ステップ 4 [クラスタ全体のパラメータ（デバイス - 全般）（Clusterwide Parameters (Device - General)）] セクションから、[トラステッド リレー ポイントの割り当てが失敗するとコールは失敗する（Fail Call

If Trusted Relay Point Allocation Fails）] ドロップダウン リストの [True（True）] を選択します。フィールドとその設定オプションについては、「関連項目」の項を参照してください。

ステップ 5 [クラスタ全体のパラメータ（デバイス - H323）（Clusterwide Parameters (Device - H323)）] セクションから、[MTP の割り当てが失敗するとコールは失敗する（Fail Call If MTP Allocation Fails）] ドロップダウン リストの [True（True）] を選択します。フィールドとその設定オプションについては、「関連項目」の項を参照してください。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

MTP および TRP サービス パラメータを選択したときのコール ステータス, （520 ページ）
MTP と TRP サービス パラメータが選択されない場合のコール ステータス, （521 ページ）

MTP および TRP サービス パラメータを選択したときのコール ステータス

エンドポイントの [メディア ターミネーション ポイントが必要（Media Termination Point Required）] および [信頼されるリレー ポイントを使用（Use Trusted Relay Point）] の両方のチェックボックスをオンにすると、Cisco Unified Communications Manager は、トラステッド リレー ポイント（TRP）でもあるメディア ターミネーション ポイント（MTP）を割り当てます。管理者がこのような MTP または TRP の割り当てに失敗すると、コール ステータスが表示されます。

次の表は、コールが失敗したときに [トラステッド リレー ポイントの割り当て失敗時にコールが失敗（Fail Call If Trusted Relay Point Allocation Fails）] および [MTP の割り当て失敗時にコールが失敗（Fail Call if MTP Allocation Fails）] のサービス パラメータ値を備えたコール ステータスを示します。

[TRP の割り当て失敗時にコール失敗（Fail Call If TRP Allocation Fails）]	**[MTP の割り当て失敗時にコール失敗（Fail Call If MTP Allocation Fails）]**	**コール失敗?**
[はい（True）]	[はい（True）]	○
[はい（True）]	いいえ（False）	○
いいえ（False）	[はい（True）]	[MTP が H.323 エンドポイントで必要な場合、はい（Yes, if MTP is required for H.323 endpoint）][MTP が SIP エンドポイントで必要な場合、いいえ（No, if MTP is required for SIP endpoint）]
いいえ（False）	いいえ（False）	なし

MTP と TRP サービス パラメータが選択されない場合のコール ステータス

[トラステッド リレー ポイントの割り当てに失敗した場合コールを失敗させる（Fail Call If Trusted Relay Point Allocation Fails）] サービス パラメータ、および [MTP の割り当てに失敗した場合コールを失敗させる（Fail Call If MTP Allocation Fails）] サービス パラメータの両方が、False に設定されている場合に、MTP が必要かどうか、[トラステッド リレー ポイントを使用（Use Trusted Relay Point）] の設定、およびリソースの割り当て状況に関係するコールの動作を、次の表に示します。

MTP が必要かどうか	TRP の使用	リソースの割り当て状況	コールの動作
Y	Y	TRP の割り当てあり	パススルー サポートがないため音声通話のみです。
Y	[Y] または [N]	MTP のみ	音声通話のみです。TRP のサポートはありません。
Y	[Y] または [N]	割り当てなし	H.323 エンドポイントで MTP を必要とする設定にしている場合、補足サービスは無効になります。
N	Y	TRP の割り当てあり	エンドポイントの機能、またはコール アドミッション制御（CAC）に応じて、音声またはビデオ通話のどちらかになります。補足サービスは動作します。
N	Y	割り当てなし	音声またはビデオ通話。補足サービスは動作しますが、TRP のサポートはありません。

トラステッド リレー ポイントの連携動作と制約事項

トラステッド リレー ポイントの連携動作

機能	データのやり取り
リソース予約プロトコル（RSVP）	RSVP がコールに対して有効な場合、Cisco Unified Communications Manager は最初に TRP としてもラベル付けされている RSVPAgent の割り当てを試みます。それ以外の場合は、別の TRP デバイスが RSVPAgent とエンドポイントの間に挿入されます。

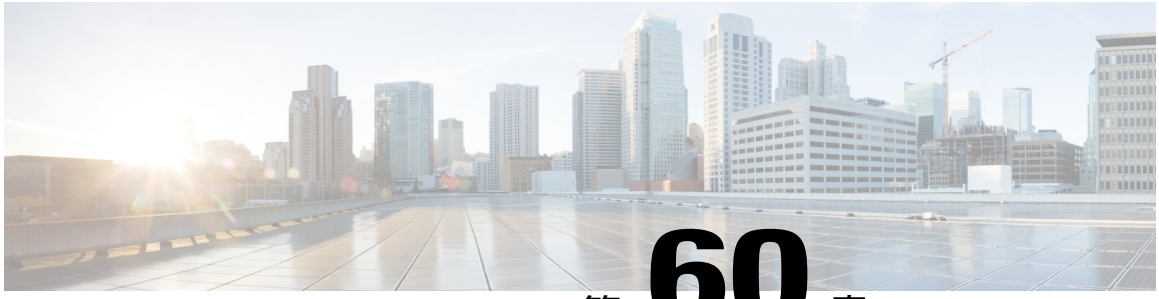
機能	データのやり取り
コール用のトランスコーダ	コールにトランスコーダが必要で、TRP を必要とするエンドポイントと同じ側にトランスコードを割り当てる必要がある場合、Cisco Unified Communications Manager は最初に TRP としてもラベル付けされたトランスコードの割り当てを試みます。それ以外の場合は、別の TRP デバイスがトランスコーダとエンドポイントの間に挿入されます。

トラステッド リレー ポイントの制限事項

表 *63*：トラステッド リレー ポイントの制限事項

制約事項	説明
エンドポイント向けトラステッド リレー ポイントの挿入	エンドポイントまたはデバイスに関連付けられているデバイス プールのいずれかで、[トラステッド リレー ポイントを使用（Use Trusted Relay Point）] チェックボックスをオンにした場合、Cisco Unified Communications Manager はそのエンドポイント向けに TRP を挿入する必要があります。[トラステッドリレーポイントの割り当てに失敗した場合コールを失敗させる（Fail Call If Trusted Relay Point Allocation Fails）] サービス パラメータが、True に設定されている場合、Cisco Unified Communications Manager が TRP の割り当てに失敗すると、コールが失敗することがあります。
エンドポイント向けメディア ターミネーション ポイントの割り当て	エンドポイント向けに、[メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェックボックスおよび[トラステッド リレー ポイントを使用（Use Trusted Relay Point）] チェックボックスをオンにすると、Cisco Unified Communications Manager は、TRP を兼ねる MTP を割り当てます。管理者がそのような MTP または TRP の割り当てに失敗すると、コールの状態が表示されます。

制約事項	説明
トラステッド リレー ポイントの割り当て	ほとんどのインスタンスでは、ユーザがコールに応答した後に、TRP が割り当てられるため、TRP の割り当ての失敗によりコールが失敗する場合、ユーザがコールに応答すると短い間隔の話中音を受信する可能性があります（MTP が必要な SIP アウトバウンド レッグ、つまり H.323 アウトバウンド FastStart は例外です）。



第 60 章

アナンシエータの設定

- アナンシエータの概要，525 ページ
- アナンシエータ設定タスク フロー，528 ページ

アナンシエータの概要

アナンシエータを使用すると、Cisco Unified Communications Manager は、事前に録音されたアナウンス（.wav ファイル）を再生し、Cisco Unified IP Phone やゲートウェイなどのデバイスにトーンを送信できます。アナウンスは、Cisco Multilevel Precedence and Preemption 用に設定されているデバイスに対して再生されます。

ノードを追加すると、アナンシエータ デバイスがそのノードに自動で追加されます。アナンシエータは、Cisco IP Voice Media Streaming Application サービスが同じノードでアクティブになるまで非アクティブの状態が続きます。

注意 コール処理の負荷が高い Cisco Unified Communications Manager ノードでは、アナンシエータをアクティブにしないことを推奨します。

デフォルトでは、アナンシエータは 48 の同時メディア ストリームをサポートします。アナンシエータ メディア ストリームのデフォルト数は、アナンシエータ サービス パラメータを使用して変更できますが、1 つのノードに対して 48 を超えるアナンシエータ ストリームを設定しないことを推奨します。

Cisco Unified Communications Manager サービスが実行されていない専用のサブスクライバ ノードでアナンシエータが実行されている場合、アナンシエータは最大 255 の同時アナウンス ストリームをサポートできます。専用のサブスクライバ ノードが 10,000 ユーザに対応する OVA 仮想マシンの設定を満たしている場合、アナンシエータは最大 400 の同時アナウンス ストリームをサポートできます。

ノードで IPv6 を使用している場合、アナンシエータは IPv4 と IPv6 の両方のオーディオ メディア接続をサポートし、自動的にデュアル モードで設定されます。IPv6 を使用していない場合、アナンシエータは IPv4 専用モードとして自動的に設定されます。

Secure Real-Time Protocol（SRTP）が有効になっている Cisco Unified Communications Manager ノードの場合、アナンシエータはセキュアな SRTP デバイスとして自動的に登録されます。状況に応じて、アナンシエータがセキュア モードで稼働している場合は、アナウンスとトーンを暗号化しないことを選択できます。

メディア リソースを管理するために、メディア リソース グループとリストにアナンシエータを追加できます。アナンシエータは、Serviceability のパフォーマンス カウンタもサポートします。たとえば、使用されているストリームの数、現在アクティブなストリーム、使用可能なストリームの総数、失敗したアナンシエータ ストリームの数をモニタできます。また、Real-Time Monitoring Tool（RTMT）を使用して、Cisco IP Voice Media Streaming Application のトレースを取得して、アナンシエータのパフォーマンスをトラブルシューティングすることもできます。

メディア ストリームのアクティビティとステータスのモニタリングの詳細については、『*Cisco Unified Serviceability* アドミニストレーション ガイド』および『*Cisco Unified Real-Time Monitoring Tool* アドミニストレーション ガイド』を参照してください。

デフォルトのアナウンスとトーン

Cisco Unified Communications Manager は、Cisco IP メディア ストリーミング アプリケーション サービスが有効化されたときに、一連の事前に録音されたアナンシエータ アナウンスを自動的に提供します。アナウンスまたはトーンは、次の条件で再生されます。

- アナウンス：シスコの Multilevel Precedence and Preemption 用に設定されたデバイスの場合に再生されます。
- 割り込みトーン：参加者がアドホック会議に参加する前に流れます。
- リング バック トーン：コールがアクティブな場合、ゲートウェイはトーンを再生できないため、IOS ゲートウェイ経由で PSTN を介してコールを転送する場合は、アナンシエータがトーンを再生します。
- リング バック トーン：H.323 クラスタ間トランクを介してコールを転送する場合は、トーンが再生されます。
- リング バック トーン：SCCP を実行している電話から SIP クライアントにコールを転送する場合は、トーンが再生されます。

デフォルトの事前に録音されたアナンシエータ アナウンスを変更したり、アナウンスを追加したりすることはできません。Cisco Unified Communications Manager ロケール インストーラがインストールされており、Cisco Unified IP Phone またはデバイス プールにロケールが設定されている場合は、アナウンスのローカリゼーションがサポートされます。ロケール インストーラとユーザおよび（対応する）ネットワーク ロケール用にインストールするファイルの詳細については、『*Installing Cisco Unified Communications Manager*』を参照してください。ロケール インストーラをダウンロードするには、www.cisco.com のサポート ページを参照してください。

表 *64*：事前に録音されたアナンシエータ アナウンス

条件	アナウンス
優先順位が同じか高いコールが処理されます。	優先順位アクセス制限のため、コールを完了できません。（Precedence access limitation has prevented the completion of your call.）電話を切り、もう一度かけ直してください。（Please hang up and try again.）これは録音です。（This is a recording.）
優先順位アクセス制限が存在します。（A precedence access limitation exists.）	優先順位アクセス制限のため、コールを完了できません。（Precedence access limitation has prevented the completion of your call.）電話を切り、もう一度かけ直してください。（Please hang up and try again.）これは録音です。（This is a recording.）
誰かが許可されていない優先順位レベルを試行しました。（Someone attempted an unauthorized precedence level.）	使用した優先順位は、回線で許可されていません。（The precedence used is not authorized for your line.）許可された優先順位を使用するか、オペレータにお問い合わせください。（Please use an authorized precedence or ask your operator for assistance.）これは録音です。（This is a recording.）
コールが話中であるか、管理者がコール ウェイティングまたはプリエンプションの電話番号を設定していません。（The call appears busy, or the administrator did not configure the directory number for call waiting or preemption.）	ダイヤルした番号は通話中で、コール待機またはプリエンプションに対応していません。（The number you have dialed is busy and not equipped for call waiting or preemption.）電話を切り、もう一度かけ直してください。（Please hang up and try again.）これは録音です。（This is a recording.）
システムがコールを完了できません。（The system cannot complete the call.）	ダイヤルしたコールを完了できません。（Your call cannot be completed as dialed.）ディレクトリを調べてかけ直すか、オペレータに連絡してください。（Please consult your directory and call again or ask your operator for assistance.）これは録音です。（This is a recording.）
サービスに割り込みが発生しました。（A service interruption occurred.）	サービスが中断されたため、コールを完了できません。（A service disruption has prevented the completion of your call.）緊急の場合は、オペレータに電話してください。（In case of emergency call your operator.）これは録音です。（This is a recording.）

次の表に、アナンシエータでサポートされるトーンを示します。

表 *65*：トーンの説明

タイプ（Type）	説明
話中音	話中音は、着信番号が話中の場合に聞こえます。
割り込みトーン	会議割り込みトーンは、参加者がアドホック会議に参加する前に聞こえます。
リング バック トーン	アラート トーンは、次のシナリオの場合に聞こえます。 • IOS ゲートウェイ経由で PSTN を介してコールを転送する場合。 • H.323 クラスタ間トランクを介してコールを転送する場合。 • SCCP 電話から SIP クライアントにコールを転送する場合。

会議ブリッジでのアナンシエータの使用

次の条件を満たす場合に、アナンシエータを会議ブリッジで使用できます。

- アナンシエータを含むメディア リソース グループ リストが、会議ブリッジが存在するデバイス プールに割り当てられている場合。
- アナンシエータがデフォルト メディア リソースとして設定されている場合。

メディア リソース グループ リストが会議を制御するデバイスに直接割り当てられている場合は、会議ブリッジでアナンシエータを使用できません。

電話会議ごとに 1 つのアナウンスのみがサポートされます。現在のアナウンスの再生中に、システムが別のアナウンスを要求した場合は、新しいアナウンスによって再生中のアナウンスがプリエンプション処理されます。

関連トピック

メディア リソース グループの概要

アナンシエータ設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	アナンシエータのアクティブ化，（529 ページ）	アナンシエータをアクティブ化するノードで、Cisco IP Voice Media Streaming Application サービスをアクティブ化します。クラスタの各アナンシエータ デバイスで、Cisco IP Voice Media Streaming Application サービスを 1 つだけアクティブ化します。

	コマンドまたはアクション	目的
ステップ 2	メディア リソース グループのタスク フロー, （508 ページ）	Cisco Unified Communications Manager の管理を使用して、アナンシエータをメディア リソース グループおよびリストに追加し、メディア リソースを管理します。[依存関係レコード要約（Dependency Records Summary）] ウィンドウで、どのメディア リソース グループにアナンシエータがあるかを確認できます。
ステップ 3	基本的なデバイス プールの設定, （56 ページ）	Cisco Unified Communications Manager の管理を使用して、アナンシエータを含むメディア リソース グループをデバイス プールに追加します。各アナンシエータに対して、この手順を繰り返します。各アナンシエータは、デバイス プールに含まれる必要があります。
ステップ 4	メディア ストリームのデフォルトの番号の変更, （530 ページ）	（任意） アナンシエータ向けメディア ストリームのデフォルト番号は変更可能です。
ステップ 5	アナンシエータのセキュリティ モードを上書き, （531 ページ）	（任意） Cisco Unified Communications Manager がセキュアに展開されている場合、アナンシエータとセキュリティが有効なデバイスとの間のメディア ストリーミングは Secure Real-Time Protocol（SRTP）で自動的に暗号化されます。アナンシエータのセキュリティ設定を上書きし、セキュアなアナンシエータから配信されたストリーム メディアが暗号化されないようにすることができます。
ステップ 6	アナンシエータがあるメディア リソース グループ リストを表示, （532 ページ）	（任意） どのメディア リソース グループがアナンシエータ デバイスを使用するかを確認できます。
ステップ 7	会議ブリッジのアナンシエータの設定, （532 ページ）	（任意） アナンシエータと会議ブリッジが同じデバイス プールに属している時は、会議ブリッジでアナンシエータを使用できます。

アナンシエータのアクティブ化

クラスタ内の各アナンシエータ デバイスで、Cisco IP Voice Media Streaming Application サービスを 1 つだけアクティブにします。

⚠

注意 コール処理負荷が高い Cisco Unified Communications Manage ノードでは、アナンシエータをアクティブにしないことをお勧めします。

手順

ステップ 1 Serviceability GUI から、[ツール（Tools）] > [アクティブ化（Activation）] を選択します。[サービスのアクティブ化（Service Activation）] ウィンドウが表示されます。

ステップ 2 [サーバ（Server）] フィールドのノードを選択し、[移動（Go）] をクリックします。

ステップ 3 [Cisco IP Voice Media Streaming Application] をオンにし、[保存（Save）] をクリックします。

次の作業

メディア リソース グループの設定およびデバイス プールへの割り当てをまだ行っていない場合、メディア リソースの設定, （505 ページ）に進みます。

それ以外の場合は、メディア ストリームのデフォルトの番号の変更, （530ページ）に進みます。

メディア ストリームのデフォルトの番号の変更

デフォルトでは、アナンシエータは 48 のメディア ストリームを同時にサポートするように設定されています。デフォルトのメディアストリーム数は、アナンシエータのサービスパラメータを使用して変更できます。ただし、ノードのアナンシエータ ストリームは 48 以下にすることを推奨します。

はじめる前に

アナンシエータのアクティブ化, （529 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM 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 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco IP Voice Media Streaming Application という名前のサービスを選択します。

ステップ 3 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウの [アナンシエータ (ANN) パラメータ] セクションの [コール カウント（Call Count）] フィールドに、多重同時メディア ストリーム数を入力し、[保存（Save）] をクリックします。
アナンシエータを更新した場合、変更内容は、アナンシエータがアイドル状態になり、アクティブなアナウンスが再生されていないときに自動的に変更されます。

次の作業

アナンシエータのセキュリティ モードを上書き, （531 ページ）

アナンシエータのセキュリティ モードを上書き

Cluster セキュリティ モードと呼ばれるエンタープライズ パラメータが 1（混合モード）に設定されると、アナになります。アナンシエータは、Secure Real-Time Protocol （SRTP）を有効にした Cisco Unified Communications Manager で、セキュアな SRTP デバイスとして登録されます。ロックされたアイコンは、SRTP 対応デバイスに表示されます。セキュアなアナンシエータからのアナウンスは、受信側デバイスも SRTP 対応であれば暗号化されます。SRTP 対応ではない場合は、保護されていないアナウンスとトーンが送信されます。

Make Annunciator Non-secure when Cluster Security is Mixed（クラスタのセキュリティが混在している場合はアナンシエータを非セキュアに設定）というサービス パラメータを使用して、アナンシエータのセキュリティ モードをオーバーライドできます。アナンシエータのセキュリティモードが上書きされると、受信側デバイスで SRTP が有効でも暗号化されていないアナウンスが再生されます。

はじめる前に

メディア ストリームのデフォルトの番号の変更, （530 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[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 [サーバ（Server）] フィールドのノードを選択します。

ステップ 3 [サービス（Service）] フィールドの [シスコ統合 IP ボイス メディア ストリーミング アプリケーション（Cisco Unified IP Voice Media Streaming Application）] を選択します。

ステップ 4 [クラスタのセキュリティが混在している場合はアナンシエータを非セキュアに設定（Make Annunciator Non-secure when Cluster Security is Mixed）] を「True」に設定して、[保存（Save）] をクリックします。

ヒント [クラスタのセキュリティが混在している場合はアナンシエータを非セキュアに設定（Make Annunciator Non-secure when Cluster Security is Mixed）] パラメータが表示されていないときは、[詳細機能（Advanced）] をクリックします。

次の作業

アナンシエータがあるメディア リソース グループ リストを表示, （532 ページ）

アナンシエータがあるメディア リソース グループ リストを表示

どのメディア リソース グループがアナンシエータ デバイスを使用するかを確認するには、[依存レコード サマリー（Dependency Records Summary）] ウィンドウを表示します。

はじめる前に

アナンシエータのセキュリティ モードを上書き, （531 ページ）

手順

ステップ 1 Cisco Unified CM の管理で [メディア リソース（Media Resources）] > [アナンシエータ（Annunciator）] を選択します。

ステップ 2 システム用に設定されているアナンシエータを選択します。

ステップ 3 [関連リンク（Related Links）] ドロップダウン リスト ボックスで、[依存レコード （Dependency Records）] を選択し、[移動（Go）] をクリックします。
[依存レコード サマリー（Dependency Records Summary）] ウィンドウは、アナンシエータ デバイスを使用するメディア リソース グループを表示します。

次の作業

会議ブリッジのアナンシエータの設定, （532 ページ）

会議ブリッジのアナンシエータの設定

会議ブリッジでアナンシエータを使用できます。

はじめる前に

アナンシエータがあるメディア リソース グループ リストを表示, （532 ページ）

手順

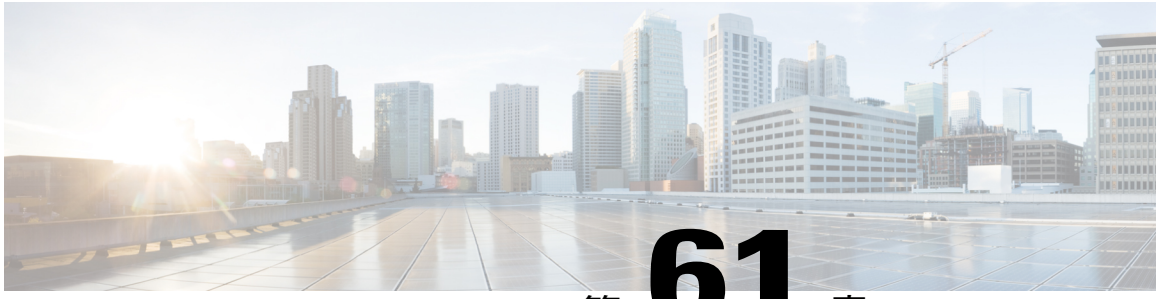
ステップ 1 メディア リソース グループ リストにアナンシエータを追加します。

ステップ 2 クラスタ内の全デバイスでアナンシエータを使用できるようにするには、アナンシエータを含むメディア リソース グループ リストを会議ブリッジのデバイス プールに割り当てます。

関連トピック

メディア リソース グループの概要
メディア リソース グループのタスク フロー, （508 ページ）
Device Pools, （51 ページ）

基本的なデバイス プールの設定, （56 ページ）



第 61 章

自動音声応答の設定

- 自動音声応答の概要，535 ページ
- デフォルトのアナウンスとトーン，535 ページ
- 自動音声応答の制限，537 ページ
- 自動音声応答の設定のタスク フロー，537 ページ

自動音声応答の概要

自動音声応答（IVR）デバイスによって、Cisco Unified Communications Manager は Cisco Unified IP Phone やゲートウェイなどのデバイスに対して事前に録音された機能アナウンス（.wav ファイル）を再生できます。これらのアナウンスは、開催中の会議のように IVR アナウンスを必要とする機能を使用しているデバイスで再生されます。

ノードを追加すると、IVR デバイスは自動的にそのノードに追加されます。IVR デバイスは、Cisco IP Voice Media Streaming Application サービスがそのノード上で有効化されるまで、非アクティブなままです。

IVR は、デフォルトでは、48 人の同時発信者をサポートします。Cisco IP Voice Media Streaming Application サービス パラメータを使用して、IVR 発信者の数を変更できます。ただし、1 つのノードの IVR 発信者は 48 人以下にすることを推奨します。IVR の発信者数は、開催中の会議への参加を目的とする IVR への同時コールの予期される数に基づいて設定できます。

注意 コール処理負荷の高い Cisco Unified Communications Manager ノードでは IVR デバイスを有効化しないでください。

デフォルトのアナウンスとトーン

Cisco Unified Communications Manager は、Cisco IP メディア ストリーミング アプリケーション サービスが有効化されたときに、一連の事前に録音された自動音声応答（IVR）アナウンスを自動的

に提供します。デフォルトの事前に録音された IVR アナウンスは置き換えることができます。アナウンスは、次の条件で再生されます。

表 *66*：事前に録音された *IVR* アナウンス

アナウンス	条件
ConferenceNowAccessCodeFailed アナウンス	参加者が開催中の会議に参加するための最大試行回数を超えた後に、さらに間違ったアクセスコードを入力すると再生されます。
ConferenceNowAccessCodeInvalid アナウンス	参加者が間違ったアクセスコードを入力すると再生されます。
ConferenceNowCFBFailed アナウンス	開催中の会議を開始する際に、会議ブリッジ容量の制限を超えている場合に再生されます。
ConferenceNowEnterAccessCode アナウンス	参加者が開催中の会議に参加し、主催者が参加者のアクセス コードを設定すると再生されます。
ConferenceNowEnterPIN アナウンス	主催者または参加者が会議への参加を試みると再生されます。
ConferenceNowFailedPIN アナウンス	主催者が正しい PIN を入力するための最大試行回数を超えた後に再生されます。
ConferenceNowGreeting アナウンス	開催中の会議のグリーティングプロンプトが再生されます。
ConferenceNowInvalidPIN アナウンス	主催者が間違った PIN を入力すると再生されます。
ConferenceNowNumberFailed アナウンス	主催者または参加者が、最大試行回数を超えた後に、さらに間違った会議番号を入力すると再生されます。
ConferenceNowNumberInvalid アナウンス	主催者または参加者が間違った会議番号を入力すると再生されます。

自動音声応答の制限

機能	制約事項
IVR	自動音声応答（IVR）は、共通のメディアデバイス ドライバを介して Real-Time Protocol（RTP）ストリームを使用します。このデバイス ドライバは、保留音（MOH）、ソフトウェア メディア ターミネーション ポイント（MTP）、ソフトウェア会議ブリッジ（CFB）、アナンシエータなどの Cisco IP Voice Media Streaming Application サービスによって提供されている他のソフトウェア メディア デバイスによっても使用されます。 デバイスに設定するコール数が多いと、システム パフォーマンスに影響します。CallManager サービスが同じサーバ ノードでアクティブな場合には、これはコール処理にも影響します。
IVR	IVR はアウトオブバンド（OOB）DTMF 桁収集方式のみをサポートします。発信側デバイスと IVR の間で DTMF 機能に不一致がある場合は、MTP が割り当てられます。
IVR	IVR は、G.711（A-law および μ-law）、G.729、およびワイドバンド 256K をサポートします。発信側デバイスと IVR の間でコーデックに不一致がある場合は、トランスコーダが割り当てられます。

自動音声応答の設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	自動音声応答装置のアクティブ化, （538 ページ）	ノードの IVR を有効化するには、そのノードで Cisco IP Voice Media Streaming Application サービスを有効化します。クラスタ内の IVR デバイスごとに 1 つの Cisco IP Voice Media Streaming Application サービスのみを有効化します。

	コマンドまたはアクション	目的
ステップ 2	IVR を保持するメディア リソース グループのリストの表示, （538 ページ）	Cisco Unified Communications Manager の管理を使用してメディア リソースを管理するには、メディア リソース グループとリストに IVR を追加します。
ステップ 3	メディア ストリームのデフォルトの番号の変更, （530 ページ）	（任意） IVR のメディア ストリームのデフォルトの数を変更できます。

自動音声応答装置のアクティブ化

クラスタに自動音声応答装置（IVR）デバイスを登録するには、各ノードで 1 つ以上の Cisco IP Voice Media Streaming Application サービスをアクティブにします。

注意 コール処理負荷が高い Cisco Unified Communications Manage ノードでは、IVR をアクティブにしないでください。

手順

ステップ 1 Cisco Unified Serviceability GUI から、[ツール（Tools）] > [アクティブ化（Activation）] を選択します。[サービスのアクティブ化（Service Activation）] ウィンドウが表示されます。

ステップ 2 [サーバ（Server）] フィールドのノードを選択し、[移動（Go）] をクリックします。

ステップ 3 [Cisco IP Voice Media Streaming Application] チェックボックスをオンにし、[保存（Save）] をクリックします。

IVR を保持するメディア リソース グループのリストの表示

手順

ステップ 1 Cisco Unified CM の管理から、[メディア リソース（Media Resources）] > [自動音声応答（IVR）（Interactive Voice Response (IVR)）] を選択します。
[自動音声応答（IVR）の検索と一覧表示（Find and List Interactive Voice Response (IVR)）] ウィンドウが表示されます。

ステップ 2 [自動音声応答（IVR）の検索と一覧表示（Find and List Interactive Voice Response (IVR)] ウィンドウから、[検索（Find）] をクリックします。

Cisco Unified Communications Manager で使用可能な IVR のリストが表示されます。

ステップ 3 メディア リソース グループの関連付けリストを表示する IVR を選択します。

ステップ 4 [関連リンク（Related Links）] ドロップダウン リストから [依存関係レコード（Dependency Records）] ノードを選択し、[移動（Go）] をクリックします。
システムで依存関係レコードが有効でない場合、[依存関係レコード要約（Dependency Records Summary）] ウィンドウにメッセージが表示されます。

IVR 設定

フィールド	説明
サーバ	システムは、自動的に事前に設定されたサーバを表示します（サーバはインストール時に追加されます）。
[名前（Name）]	このフィールドは、デバイスが Cisco Unified Communications Manager に登録するときに使用される名前を指定します。最長 15 文字の英数字（ピリオド、ダッシュ、下線は使用可）の名前を入力します。
説明	最長 128 文字の英数字（ピリオド、ダッシュ、下線は使用可）の説明を入力します。デフォルトでは、プレフィックス IVR_ を含むサーバ名を使用します。
[デバイスプール（Device Pool）]	デフォルトを選択するか、設定済みのデバイス プールのドロップダウン リストからデバイス プールを選択します。

フィールド	説明
参照先	ロケーションを使用して、一元化されたコール処理システムでコールアドミッション制御（CAC）を実装します。CACでは、ロケーション間のリンクを経由する音声コールとビデオコールで使用可能な帯域幅を制限することで、音声品質とビデオの可用性を調整できます。ロケーションは、このロケーションとの間で送受信されるコールで使用可能な帯域幅の合計を指定します。 ドロップダウンリストから、このIVRに適したロケーションを選択します。 ロケーション設定値の [ハブなし（Hub_None）] は、この IVR で使用される帯域幅がロケーション機能によって追跡されないことを意味します。ファントムのロケーション設定は、H.323 プロトコルまたは SIP を使用するクラスタ間トランクを対象に正常な CAC を有効にするロケーションを指定します。 新しいロケーションを設定するには、[システム（System）] > [ロケーション（Location）] メニューオプションを使用します。 クラスタ間トランク経由のロケーション ベースの CAC のセットアップ方法については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

フィールド	説明
[トラステッド リレー ポイントを使用（Use Trusted Relay Point）]	Cisco Unified Communications Manager によってこのメディア エンドポイントとともにトラステッドリレーポイント（TRP）デバイスを挿入するかどうかを、ドロップダウン リストから選択します。次の値のいずれかを選択します。 • オフ（Off）：このデバイスで TRP の使用を無効にするには、この値を選択します。 • オン（On）：このデバイスでの TRP の使用を有効にするには、この値を選択します。 トラステッドリレーポイント（TRP）デバイスはトラステッド リレー ポイントとしてラベル付けされている MTP またはトランスコーダ デバイスを指定します。 複数のリソースがエンドポイントに必要な場合（たとえばトランスコーダや RSVPAgent）、Cisco Unified Communications Manager は関連付けられたエンドポイント デバイスに最も近い TRP を選択します。 TRP と MTP の両方がエンドポイントに必要な場合は、TRP が必須の MTP として使用されます。 TRP と RSVPAgent の両方がエンドポイントに必要な場合、Cisco Unified Communications Manager は、TRP としても使用可能な RSVPAgent を検索します。 TRP とトランスコーダの両方がエンドポイントに必要な場合、Cisco Unified Communications Manager は、TRP としても指定可能なトランスコーダを検索します。

IVR パラメータの変更

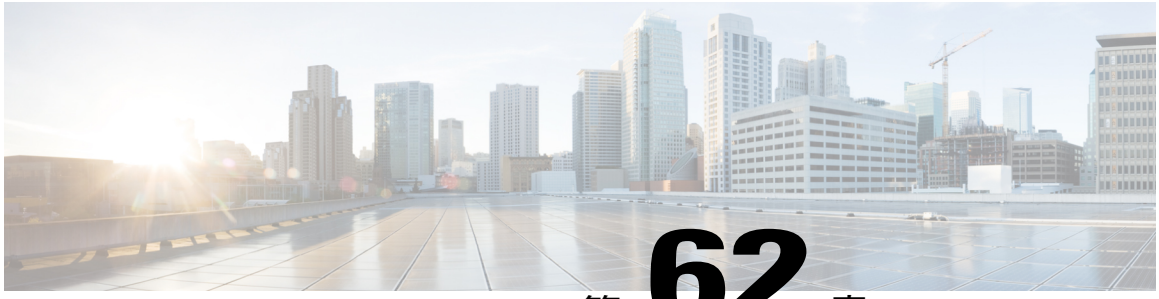
手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [サービス パラメータ（Service Parameters）]を選択します。[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウが表示されます。

ステップ 2 サーバを選択し、Cisco IP Voice Media Streaming App と呼ばれるサービスを選択します。[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウが表示されます。

ステップ 3 [音声自動応答（IVR）（Interactive Voice Response (IVR)）] セクションの [コール カウント（Call Count）] フィールドに、多重同時メディア ストリーム数を入力し、[保存（Save）] をクリックします。

IVR を更新した場合、その内容は、IVR がアイドル状態になり、アクティブなアナウンスが再生されていないときに自動的に変更されます。



第 62 章

Video On Hold サーバの設定

- 保留中ビデオの概要，543 ページ
- 保留ビデオ設定のタスク フロー，544 ページ
- 保留中ビデオの制限事項，546 ページ

保留中ビデオの概要

保留中ビデオは、ビデオコンタクトセンター向けの機能です。この機能により、顧客は、ビデオコンタクト センターをコールしてエージェントに最初の相談を行った後に、特定のビデオを見ることができます。この場合、エージェントが、保留中の顧客向けに再生するこのビデオ ストリームを選択します。

保留中ビデオ サーバは、メディア コンテンツ サーバとして、Cisco Unified Communications Manager の指示により、音声およびビデオ コンテンツのストリーム配信を行うことができます。メディア コンテンツ サーバは、信号プロトコルに SIP を使用する Unified Communications Manager に制御され、音声とビデオの保存およびストリーム配信ができる外部デバイスです。1080p、720p の高解像度、または 360p などの低い解像度のビデオ コンテンツを提供できます。メディア コンテンツ サーバには Cisco MediaSense を使用します。

ビデオコンタクトセンターに加えて、一般的な保留中ビデオの機能が必要な企業内にも、保留中ビデオを導入できます。保留中ビデオ サーバの [デフォルトのビデオ コンテンツ識別子（Default Video Content Identifier）] を設定して、保留中のユーザ向けに再生するビデオ ストリームを識別できます。

（注） Customer Voice Portal（CVP）による発信者情報の転送を導入するユニファイド コンタクト センターで、保留中ビデオの機能を利用するには、Cisco Unified Communications Manager と CVP 間の SIP トランクに保留中ビデオのリソースを割り当てる必要があります。

保留ビデオ設定のタスク フロー

はじめる前に

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco MediaSense サーバへの SIP トランクの作成, （544 ページ）	Cisco MediaSense クラスタへの SIP トランクを設定します。
ステップ 2	保留ビデオ サーバの設定, （545 ページ）	MediaSense サーバに保存されているビデオ コンテンツを特定する保留ビデオ サーバを Cisco Unified Communications Manager で設定します。

Cisco MediaSense サーバへの SIP トランクの作成

Unified Communications Manager には、Cisco MediaSense クラスタへの SIP トランクを設定する必要があります。Cisco MediaSense サーバへの SIP トランクには、Cisco MediaSense ノードの IP アドレスが含まれています。Unified Communications Manager SIP トランクは、最大 16 の宛先 IP アドレスをサポートします。

（注） Cisco MediaSense クラスタには、冗長性と拡張性のために 2 個以上のノードが必要です。

SIP トランクにデフォルト設定を設定します。SIP トランク上では、Video on Hold 機能に対応したその他の設定はサポートされていません。

手順

ステップ 1 Cisco Unified CM の管理で、[デバイス（Device）] > [トランク（Trunk）]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 [トランク タイプ（Trunk Type）] ドロップダウンリストから [SIP トランク（SIP Trunk）] を選択します。

ステップ 4 [デバイス プロトコル（Device Protocol）] ドロップダウン リストから、プロトコルとして [SIP] が入力されていることを確認し、[次へ（Next）] をクリックします。

ステップ 5 [デバイス情報（Device Information）] エリアで、次のフィールドに入力します。

- デバイス名（Device Name）：トランクの名前を入力します。
- 説明（Description）：トランクの説明を入力します。

- デバイス プール（Device Pool）：SIP トランクの適切なデバイス プールを選択します。
- ロケーション（Location）：このトランクの適切なロケーションを選択します。

ステップ 6 [SIP 情報（SIP Information）] エリアで、次のフィールドに入力します。

- 宛先アドレス（Destination Address）：Cisco MediaSense サーバの IP アドレスを入力します。複数の IP アドレスを指定できます。
- 宛先ポート（Destination Port）：ポート番号を入力します。デフォルトのポート番号 5060 を受け入れることを推奨します。複数のポートを指定できます。
- SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）：ドロップダウン リストから SIP トランク セキュリティ プロファイルを選択します。
- SIPプロファイル（SIP Profile）：ドロップダウン リストから SIP プロファイルを選択します。オプションの ping が設定されている SIP プロファイルを選択します。存在しない場合は、それを作成します。これは必須ではありませんが、ユーザエクスペリエンスが改善されます。

ステップ 7 [保存（Save）] をクリックします。

次の作業

保留ビデオ サーバの設定, （545 ページ）

保留ビデオ サーバの設定

保留ビデオ サーバの SIP トランクは Cisco MediaSense サーバを指し、デフォルトのコンテンツ ID は MediaSense サーバに存在するストリーム ID を指します。コンテンツ ID は任意の英数文字列です。

はじめる前に

Cisco MediaSense サーバへの SIP トランクの作成, （544 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CManager Administration）] で、[メディア リソース（Media Resources）] > [保留ビデオ サーバ（Video On Hold Server）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックして、新しい保留ビデオ サーバをセットアップします。

ステップ 3 保留ビデオ サーバの名前を入力します。

ステップ 4 サーバについての説明を入力します。

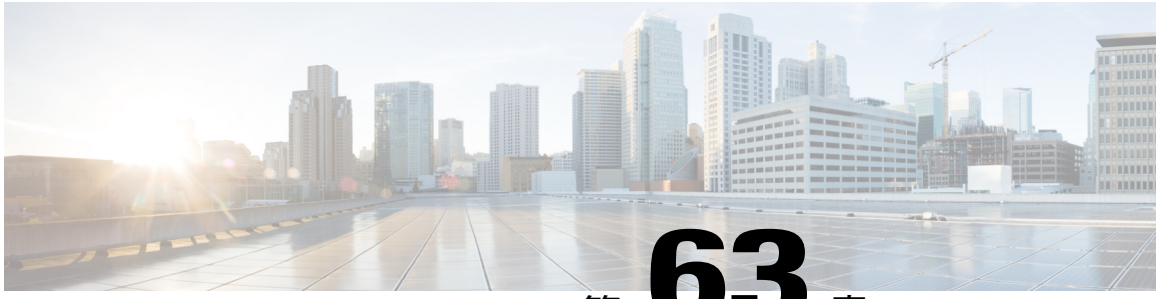
ステップ 5 [デフォルトのビデオ コンテンツ ID（Default Video Content Identifier）] に英数文字列を入力します。

ステップ 6 ドロップダウン リストから使用する SIP トランクを選択します。新しい SIP トランクを作成する必要がある場合、[SIP トランクの作成（Create SIP Trunk）] ボタンをクリックします。

ステップ 7 [保存（Save）] をクリックします。

保留中ビデオの制限事項

拡張位置のコール アドミッション制御の機能を使用するために、Cisco MediaSense サーバを、Unified Communications Manager のクラスタに配置できます（MediaSense のクラスタは、保留中のパーティが登録されているクラスタに直接接続します）。その場合、Unified Communications Manager クラスタは、保留中のパーティが位置する場所と Cisco MediaSense が位置する場所との間の帯域幅を縮小する役割を担います。保留中ビデオの連携動作は、720p または 1080p のビデオ ストリームを使用するため、既存のセッションのビデオ品質を維持するために、新規のセッションを可能にする前に帯域幅の使用を考慮することが重要です。



第 63 章

アナウンスの設定

- アナウンス設定の概要，547 ページ
- アナウンスの設定タスク フロー，548 ページ

アナウンス設定の概要

事前に定義されたアナウンスを使用するか、カスタム アナウンスをアップロードして、ユーザに情報を提供できます。

Cisco Unified Communications Manager には、次のアナウンスが含まれています。

- システム アナウンス：これらのアナウンスは、通常のコール処理で使用される事前定義されたアナウンスです。また、機能アナウンスのサンプルとして提供されているものもあります。
- 機能アナウンス：これらのアナウンスは、ハント パイロット コール キューイングまたは外部コール制御とともに、保留音（MOH）などの機能によって使用されます。

[アナウンスの設定（Announcement Configuration）] ウィンドウで [新規追加（Add New）] ボタンをクリックすると、最大50の機能アナウンスを使用できます。これらのアナウンスは、シスコが提供するオーディオファイルの場合もあれば、アップロードされたカスタム.wavファイルの場合もあります。すべてのカスタムアナウンス.wavファイルをクラスタ内のすべてのサーバにアップロードします。

デフォルトのアナウンス

カスタム アナウンスの WAV ファイルをアップロード、または Cisco が提供するファイルを変更できます。ただし、アナウンス ID は変更できません。たとえば、システム アナウンス（VCA_00121）は、発信者が無効な番号にダイヤルすると再生されます。これは一般に空きのコール アナウンスと呼ばれます。

表 *67* : *[*アナウンスの検索と一覧表示（***Find and List Announcements***）*]* ウィンドウに表示されるアナウンス

[アナウンス ID（Announcement Identifier）]	説明
Gone_00126	システム：現在使用されていない
MLPP-BNEA_00123	システム：MLPP ビジーが備わっていない
MLPP-BPA_00122	システム：MLPP 以上の優先レベル
MLPP-ICA_00120	システム：MLPP サービス障害
MLPP-PALA_00119	システム：MLPP 優先順位のアクセス制限
MLPP-UPA_00124	システム：MLPP で許可されていない優先レベル
Mobility_VMA	接続するには 1 を押してください
MonitoringWarning_00055	システム：モニタリングまたは録音中
RecordingWarning_00038	システム：録音中
TemporaryUnavailable_00125	システム：一時的に使用不可
VCA_00121	システム：欠番/無効な番号がダイヤルされた
Wait_In_Queue_Sample	組み込み：キューに入った発信者用の定期的なアナウンス（サンプル）
Welcome_Greeting_Sample	組み込み：発信者へのグリーティング（サンプル）

アナウンスの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	アナウンスの設定，（549 ページ）．	ハント パイロット コール キューイングまたは外部コール制御と連動する保留音（MOH）などの機能と使用できるアナウンスを設定します。

	コマンドまたはアクション	目的
ステップ 2	カスタマイズされたアナウンスのアップロード, （550 ページ）.	カスタム アナウンスの .wav ファイルをアップロードするか、シスコから提供されるシステム アナウンス用のファイルを変更します。ただし、アナウンスの識別子は変更できません。カスタマイズされたアナウンスにはハイパーリンクの下線が引かれ、Cisco Unified Communications Manager の [アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウに表示されます。

アナウンスの設定

システム アナウンスとして、または機能アナウンスとして使用できるアナウンスを設定できます。システム アナウンスは、コール処理に使用されます。また、機能アナウンスのサンプルとして使用されることもあります。一方、機能アナウンスは、ハント パイロット コール キューイングまたは外部コール制御に関連する保留音（MOH）などの特定の機能に使用されます。

Cisco Unified Communications Manager で既存のアナウンスを変更することも、新しいアナウンスを設定することもできます。

手順

ステップ 1 Cisco Unified CM の管理から、[メディア リソース（Media Resources）] > [アナウンス（Announcement）] を選択します。

ステップ 2 [アナウンスの検索と一覧表示（Find and List Announcement）] ウィンドウで、次のタスクのいずれかを実行します。

- 既存のアナウンスのフィールドを変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストからアナウンスを選択します。
- 新しいアナウンスを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [アナウンスの設定（Announcement Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

カスタマイズされたアナウンスのアップロード, （550 ページ）.

カスタマイズされたアナウンスのアップロード

アップロードされたカスタム.wavファイルを使用して、デフォルトのアナウンスを別のアナウンスに変更できます。オーディオ ソース ファイルをインポートする場合は、Cisco Unified Communications Managerがファイルを処理し、保留音（MOH）サーバが使用するために適した形式にファイルを変換します。

（注） アナウンスはロケール（言語）固有です。インストールが複数の言語ロケールを使用している場合は、個別の.wavファイルとして言語ごとに各カスタムアナウンスを録音し、正しいロケール割り当てでアップロードする必要があります。このタスクでは、米国英語以外の言語のカスタム アナウンス.wavファイルをアップロードする前に、各サーバに正しいロケール パッケージがインストールされている必要があります。

MOHオーディオ ソースファイルと同様、アナウンスの推奨形式には次の仕様が含まれます。

- 16 ビット PCM .wav ファイル
- ステレオまたはモノラル
- 48 kHz、44.1 kHz、32 kHz、16 kHz、または 8 kHz のサンプル レート

（注） Cisco Unified Communications Manager 内の [アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウでハイパーリンクされていないアナウンスは更新できません。このウィンドウでハイパーリンクされた下線付きのシスコ提供のアナウンスの場合は、カスタマイズされたアナウンスを追加できます。たとえば、MLPP-ICA_00120 と MonitoringWarning_00055 があります。

はじめる前に

アナウンスの設定, （549 ページ）.

手順

ステップ 1 Cisco Unified CM の管理から、[メディア リソース（Media Resources）] > [アナウンス（Announcement）] を選択します。

ステップ 2 [アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウで、検索条件を入力して、[検索（Find）] をクリックし、結果リストからアナウンスのハイパーリンクをクリックします。

ステップ 3 [アナウンスの設定（Announcement Configuration）] ウィンドウで、[ファイルのアップロード（Upload File）] をクリックします。

ステップ 4 [ファイルのアップロード（Upload Files）] ポップアップ ウィンドウから、ロケールを選択し、ファイル名を入力して参照し、.wavファイルを選択して、[ファイルのアップロード（Upload File）] をクリックします。

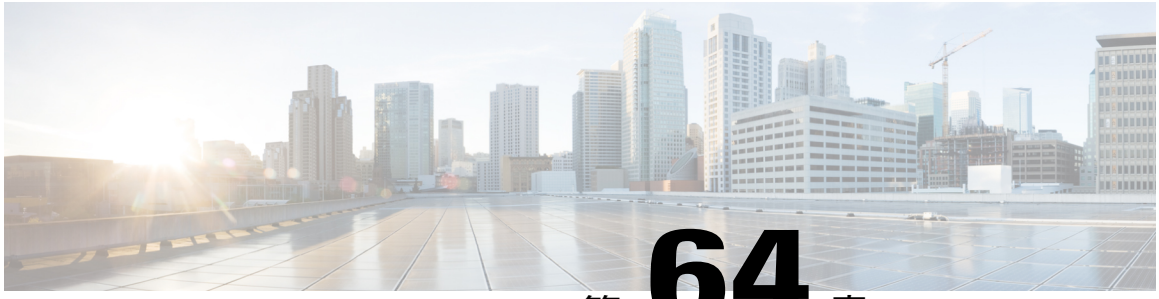
アップロードプロセスが始まり、処理が完了した後にステータスが更新されます。[閉じる（Close）] を選択して [ファイルのアップロード（Upload File）] ウィンドウを閉じます。

ステップ 5 （オプション）Cisco Unified Communications Manager に、シスコ提供のアナウンスを再生させるのではなく、カスタマイズされたアナウンスを再生させるには、[アナウンスの設定（Announcements Configuration）] ウィンドウの [ロケール別アナウンス（Announcement by Locale）] ペインに表示される [有効（Enable）] チェックボックスをオンにします。
[有効（Enable）] チェックボックスをオフにすると、Cisco Unified Communications Manager はシスコ提供のアナウンスを再生します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

クラスタ内のサーバ間ではアナウンス ファイルが伝搬されないため、クラスタ内の各ノードにアナウンスをアップロードします。クラスタ内の各サーバで Cisco Unified Communications Manager の管理を参照し、アップロード プロセスを繰り返します。



第 64 章

会議ブリッジの設定

- 会議ブリッジの概要，553 ページ
- 会議ブリッジ タイプ，553 ページ
- コール保持，558 ページ
- コール保持のシナリオ，559 ページ
- 会議ブリッジの設定タスク フロー，561 ページ

会議ブリッジの概要

Cisco Unified Communications Manager 対応の会議ブリッジは、アドホック会議とミートミー音声会議の両方に対応するように設計されたソフトウェアまたはハードウェアのアプリケーションです。その他の会議ブリッジ タイプがビデオ会議を含む他のタイプの電話会議をサポートします。各会議ブリッジは複数のマルチパーティ会議を同時にホストできます。ハードウェアとソフトウェアの両方の会議ブリッジを同時にアクティブにできます。ソフトウェアとハードウェアの会議ブリッジはストリーム数とサポートするコーデックのタイプが異なります。新しいサーバを追加すると、システムは自動的にソフトウェア会議ブリッジを追加します。

（注） Cisco Unified Communications Manager サーバが作成されると、会議ブリッジ ソフトウェアも自動的に作成されるため、作成できません。Cisco Unified Communications Manager の管理ページに会議ブリッジ ソフトウェアを追加できません。

会議ブリッジ タイプ

Cisco Unified Communications Manager の管理では、次の会議ブリッジ タイプを使用できます。

表 *68*：会議ブリッジタイプ

会議ブリッジタイプ	説明
シスコ会議ブリッジのハードウェア	このタイプは、Cisco Catalyst 4000 および 6000 音声ゲートウェイ モジュールと次の数の会議セッションをサポートします。 **Cisco Catalyst 6000** • G.711 または G.729a 電話会議：ポートあたり 32 人の参加者、電話会議あたり最大 6 人の参加者、モジュールあたり合計 256 人の参加者、3 人の参加者の 10 のブリッジ。 • GSM：ポートあたり 24 人の参加者、会議あたり最大 6 人の参加者、モジュールあたり合計 192 人の参加者。 **Cisco Catalyst 4000** G.711 電話会議のみ：電話会議あたり 24 人の会議参加者、各 6 人の参加者で最大 4 会議。
シスコ会議ブリッジのソフトウェア	ソフトウェア電話会議デバイスはデフォルトで G.711 コーデックをサポートします。 このタイプの発信者の最大数は 256 です。256 に設定すると、ソフトウェア会議ブリッジは 4 人それぞれで 64 の会議セッションをサポートできます。会議セッションの発信者の最大数は、[最大アドホック会議（Maximum Ad Hoc Conference）] および [最大ミートミー会議ユニキャスト（Maximum MeetMe Conference Unicast）] のサービス パラメータを介して指定します。 **注意** このタイプの会議ブリッジ（SW 会議ブリッジ）は、実装が簡単です。サイレントな両当事者を特定せず、簡単な加算アルゴリズムを使用するため、多くの参加者がいる会議の音声品質と音量レベルが低下する可能性があります。

会議ブリッジ タイプ	説明
Cisco IOS Conference Bridge	• NM-HDV または NM-HDV-FARM ネットワーク モジュールを使用します。 • G.711 A/μ-law、G.729、G.729a、G.729b、G.729ab の参加者は単一の電話会議に参加できます。 • 最大 6 人が単一の電話会議に参加できます。 Cisco Unified Communications Manager は、コールに対して会議リソースを動的に割り当てます。 Cisco IOS Conferencing and Transcoding for Voice Gateway Router の詳細については、この製品に付属の Cisco IOS のドキュメントを参照してください。
Cisco IOS Enhanced Bridge	• Cisco 2800 および 3800 シリーズ音声ゲートウェイ ルータ上のオンボード Cisco Packet Voice/Fax デジタル シグナル プロセッサ モジュール（PVDM2）を使用するか、NM-HD または NM-HDV2 ネットワーク モジュールを使用します。 • G.711 A-law/μ-law、G.729、G.729a、G.729b、G.729ab、GSM FR、GSM EFR の参加者は単一の電話会議に参加できます。 • 最大 8 人が単一のコールに参加できます。 （注） ISR4000 ルータおよび SM-X-PVDM-3000/SM-X-PVDM-2000/SM-X-PVDM-1000/SM-X-PVDM-500 では、Unified Communications Manager の最大ストリームは 4096 に制限されているため、各会議ブリッジ プロファイルで最大 512 のセッションを登録できます。 Cisco Unified Communications Manager は、コールに対して会議リソースを動的に割り当てます。 Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Router の詳細については、この製品に付属の Cisco IOS のドキュメントを参照してください。 この会議ブリッジ タイプは、ISR 4000 シリーズ ゲートウェイが導入されたサポート対象の SIP 電話向けに AES_CM_128_HMAC_SHA1_80 を使用した SRTP メディア暗号化をサポートします。SCCP 電話とサポート対象外の SIP 電話は、AES_CM_128_HMAC_SHA1_32 暗号化へフォールバックされます。 （注） ゲートウェイの負荷が暗号をサポートしていることを確認してください。サポートの詳細については、ゲートウェイのドキュメントを参照してください。

会議ブリッジ タイプ	説明
Cisco Conference Bridge（WS-SVC-CMM）	この会議ブリッジ タイプは、Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズ通信メディア モジュール（CMM）をサポートしています。 会議あたり最大 8 人の参加者とポート アダプタあたり最大 64 の会議をサポートします。この会議ブリッジ タイプは次のコーデックをサポートし、アドホック会議もサポートします。 • G.711 A-law/μ-law • G.729 annex A および annex B • G.723.1
Cisco Video Conference Bridge（IPVC-35xx）	Cisco Video Conference Bridge は、Cisco IP Video Phone、H.323 エンドポイントおよび音声専用 Cisco Unified IP Phone 対応の音声およびビデオ会議機能を提供します。Cisco Video Conference Bridge はビデオ用に H.261、H.263、H.264 コーデックをサポートします。

会議ブリッジ タイプ	説明
Cisco TelePresence MCU	Cisco TelePresence MCU は、Cisco Unified Communications Manager のハードウェア会議ブリッジ セットです。 Cisco TelePresence MCU は、高解像度（HD）マルチポイント ビデオ会議ブリッジです。1 秒あたり 30 フレームで 1080p、すべての会議でフル連続表示、フル トランスコーディングを実現し、混合 HD エンドポイント環境にとって理想的です。 Cisco TelePresence MCU は、シグナリング コール制御プロトコルとして SIP をサポートします。システムと電話会議を完全に設定、制御、モニタリングできる Web サーバが組み込まれています。Cisco TelePresence MCU は HTTP を介した XML 管理 API を提供しています。 Cisco TelePresence MCU は、アドホックとミートミーの両方の音声およびビデオ会議に対応しています。各会議ブリッジは複数のマルチパーティ会議を同時にホストできます。 Cisco Unified Communications Manager は、Unified Communications Manager と Cisco TelePresence MCU との間での Binary Floor Control Protocol（BFCP）を使用したプレゼンテーション共有をサポートしています。 Cisco TelePresence MCU はポート予約モードで設定する必要があります。詳細については、『*Cisco TelePresence MCU Configuration Guide*』を参照してください。 （注） Cisco TelePresence MCU は、一般のアウトオブバンド DTMF 方式をサポートしていません。デフォルト設定では、Cisco Unified Communications Manager には、メディア ターミネーション ポイント（MTP）は必要ありません。ただし、[メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェックボックスがオンの場合は、Cisco Unified Communications Manager が MTP を割り当て、SIP トランクは RFC 2833 に従って DTMF をネゴシエートします。

会議ブリッジ タイプ	説明
Cisco TelePresence Conductor	Cisco TelePresence Conductor は、インテリジェントな会議管理制御を提供しています。MCU および複数のデバイスの可用性に基づいてロードバランシングを行うデバイス クラスタリングをサポートしており、スケーラブルです。管理者は、アプライアンス、または Cisco Unified Computing System（Cisco UCS）プラットフォームやサードパーティベースのプラットフォームをサポートする VMware 上の仮想化アプリケーションのいずれかとして、Cisco TelePresence Conductor を実装できます。 Cisco TelePresence Conductor はそれぞれの新しい電話会議用に最適な Cisco TelePresence リソースを動的に選択します。アドホック、“ミートミー”、およびスケジュール済みの音声およびビデオ会議を、個々の MCU の容量を超えて動的に拡張できます。最大 3 つの Cisco TelePresence Conductor アプライアンスまたは仮想化アプリケーションをクラスタ化して、復元力を強化できます。1 つの Cisco TelePresence Conductor アプライアンスまたは Cisco TelePresence Conductor クラスタには、30 の MCU または 2400 の MCU ポートのシステム容量があります。

コール保持

Cisco Unified Communications Manager のコール保持機能は、Cisco Unified Communications Manager で障害が発生した場合やデバイスとコールをセットアップした Cisco Unified Communications Manager 間の通信で障害が発生した場合にアクティブ コールが中断されないことを保証します。

Cisco Unified Communications Manager は広範な Cisco Unified Communications デバイスでのコール保持を完全にサポートします。このサポートには、Cisco Unified IP Phone、および Foreign Exchange Office（FXO）（非ループ開始トランク）と Foreign Exchange Station（FXS）インターフェイスをサポートする Media Gateway Control Protocol（MGCP）ゲートウェイ、それよりも規模は小さくなりますが、会議ブリッジ、MTP、およびトランスコーディング リソース デバイス間のコール保持が含まれます。

高度なサービス パラメータ Allow Peer to Preserve H.323 Calls を True に設定することにより、H.323 コール保持を有効にします。

次のデバイスおよびアプリケーションはコール保持をサポートします。両端が次のデバイスのいずれかを経由して接続している場合、Cisco Unified Communications Manager はコール保持を維持します。

- Cisco Unified IP Phone
- SIP トランク
- ソフトウェア会議ブリッジ
- ソフトウェア MTP

- ハードウェア会議ブリッジ（Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module、Cisco Catalyst 4000 Access Gateway Module）
- トランスコーダ（Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module、Cisco Catalyst 4000 Access Gateway Module）
- 非 IOS MGCP ゲートウェイ（Catalyst 6000 24 Port FXS Analog Interface Module、Cisco DT24+、Cisco DE30+、Cisco VG200）
- Cisco IOS H.323 ゲートウェイ（Cisco 2800 シリーズ、Cisco 3800 シリーズなど）
- Cisco IOS MGCP ゲートウェイ（Cisco VG200、Catalyst 4000 Access Gateway Module、Cisco 2620、Cisco 3620、Cisco 3640、Cisco 3660、Cisco 3810）
- Cisco VG248 Analog Phone ゲートウェイ

次のデバイスおよびアプリケーションはコール保持をサポートしません。

- アナンシエータ
- NetMeeting またはサードパーティ製 H.323 エンドポイントなどの H.323 エンドポイント
- CTI アプリケーション
- TAPI アプリケーション
- JTAPI アプリケーション

コール保持のシナリオ

次の表で、さまざまなシナリオでのコール保持の処理方法について説明します。

表 *69*：コール保持のシナリオ

シナリオ	コール保持の処理
Cisco Unified Communications Manager に障害が発生しました。	Cisco Unified Communications Manager の障害によって、その Cisco Unified Communications Manager を介して設定されたすべてのコールの呼処理機能が失われます。 Cisco Unified Communications Manager は、エンドユーザが受話器を置くまで、またはメディア接続が解放されたことをデバイスが判別するまで、影響を受けるアクティブ コールを保持します。ユーザは、この障害の結果として保持されるコールの呼処理機能を呼び出すことはできません。

シナリオ	コール保持の処理
Cisco Unified Communications Manager とデバイス間に通信障害が発生しました。	デバイスとそれを制御する Cisco Unified Communications Manager 間の通信に障害が発生すると、デバイスは障害を認識し、アクティブな接続を維持します。Cisco Unified Communications Manager は通信障害を認識し、通信が失われたデバイスのコールに関連付けられている呼処理エンティティを消去します。 Cisco Unified Communications Manager は影響を受けるコールに関連付けられている動作中のデバイスの制御を引き続き維持します。Cisco Unified Communications Manager は、エンドユーザが受話器を置くまで、またはメディア接続が解放されたことをデバイスが判別するまで、影響を受けるアクティブ コールを保持します。ユーザは、この障害の結果として保持されるコールの呼処理機能を呼び出すことはできません。 （注） 電話またはデバイスはコール保持モードになり、会議ブリッジプロファイル ゲートウェイは、ユーザが受話器を置くことによって接続を切るまでコールエントリを保持します。接続がオンラインに戻ると、会議ブリッジプロファイル ゲートウェイは、ゲートウェイの [sccp] 設定の下に設定された [Switchback Guard time] に応じて、CUCM に登録します。
デバイスの障害 （電話、ゲートウェイ、会議ブリッジ、トランスコーダ、MTP）	デバイスに障害が発生した場合、デバイスを介して存在している接続は、ストリーミング メディアを停止します。アクティブな Cisco Unified Communications Manager はデバイスの障害を認識し、障害が発生したデバイスのコールに関連付けられている呼処理エンティティを消去します。 Cisco Unified Communications Manager は影響を受けるコールに関連付けられている動作中のデバイスの制御を維持します。Cisco Unified Communications Manager は、存続しているエンド ユーザが受話器を置くまで、またはメディア接続が解放されたことを動作中のデバイスが判別するまで、動作中のデバイスに関連付けられたアクティブな接続（コール）を保持します。

会議ブリッジの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	会議ブリッジの設定, （561 ページ）	アドホックおよびミートミー音声会議を使用できるように、ハードウェアまたはソフトウェアの会議ブリッジを設定します。
ステップ 2	会議ブリッジのサービス パラメータの設定, （561 ページ）	ネットワークに、Cisco IOS 会議ブリッジと Cisco IOS 拡張会議ブリッジがいずれも存在する場合は、次の手順を実行します。

会議ブリッジの設定

アドホックおよびミートミー音声会議を許可するように、ハードウェアまたはソフトウェア会議ブリッジを設定する必要があります。

手順

ステップ 1 Cisco Unified CM の管理から、[メディア リソース（Media Resources）]>[会議ブリッジ（Conference Bridge）] 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 [会議ブリッジの設定（Conference Bridge Configuration）] ウィンドウで各フィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ネットワークに Cisco IOS 会議ブリッジおよび Cisco IOS の拡張会議ブリッジが含まれる場合、会議ブリッジのサービス パラメータの設定, （561 ページ）を実行します。

会議ブリッジのサービス パラメータの設定

ネットワークに Cisco IOS Conference Bridge と Cisco IOS Enhanced Conference Bridge の両方が含まれる場合は、次の手順を実行します。

手順

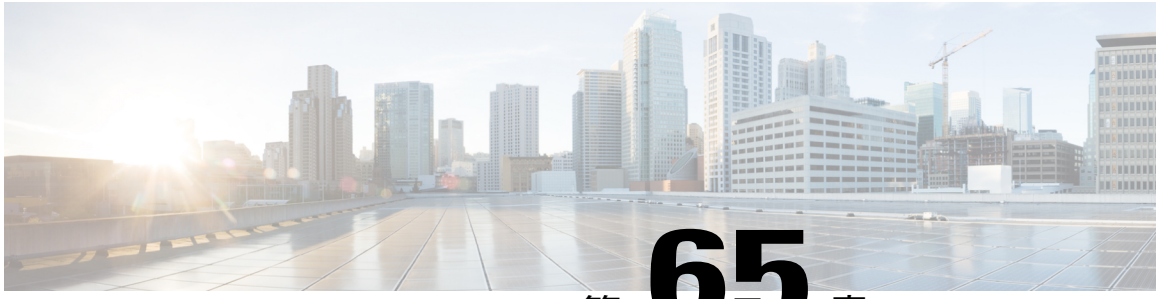
ステップ 1 Cisco Unified CM の管理から、[システム（System）]> [サービス パラメータ（Service Parameters）] の順に選択します。

ステップ 2 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（機能 - 会議）（Clusterwide Parameters (Features - Conference)）] セクションで、次のパラメータを 6 に設定します。

- [アドホック会議の最大参加者数（Maximum Ad Hoc Conference）]
- Maximum MeetMe Conference Unicast

ステップ 4 [保存（Save）] をクリックします。



第 65 章

フレキシブル DSCP マーキングおよびビデオ プロモーションの設定

- フレキシブル DSCP マーキングおよびビデオ プロモーションの概要，563 ページ
- ユーザに対するカスタム QoS の設定，564 ページ
- トラフィック クラスのラベル，565 ページ
- DSCP の設定構成のタスク フロー，565 ページ
- フレキシブル DSCP マーキングおよびビデオ プロモーションのインタラクションと制約事項，571 ページ

フレキシブル DSCP マーキングおよびビデオ プロモーションの概要

デバイスおよびアプリケーションは、Differentiated Services Code Point（DSCP; DiffServ コード ポイント）マーキングを使用して、IP コミュニケーションのサービス品質（QoS）を示します。たとえば、デスクトップ ビデオ エンドポイントはビデオ メディア ストリーム用にマルチメディア会議 AF41 マーキングを使用できますが、一方で高画質ビデオ ルーム システムはリアルタイム インタラクティブ CS4 マーキングを使用できます。アプリケーションが同じタイプのアプリケーションとの間で IP コミュニケーションを送受信している場合、DSCP マーキングは対称的であり、各アプリケーションが送受信する IP コミュニケーションの QoS 処理は同一です。ただし、アプリケーションが異なるタイプのアプリケーションとの間でメディアを送受信すると、DSCP マーキングは非対称となり、各アプリケーションが送受信する IP コミュニケーションの QoS 処理において一貫性が失われる場合があります。たとえば、ビデオ ルーム システムがデスクトップ ビデオ エンドポイントから受信するビデオ メディア ストリームの QoS 処理が、ビデオ ルーム システムの期待される品質をサポートするには不十分な場合があります。

デバイスおよびアプリケーションは、確立されたセッションの間、十分な帯域幅が使用できるようにするため、コール アドミッション制御（CAC）に従います。確立されたセッションによって使用されている帯域幅は、セッションの開始と終了の時点で更新されます。使用可能な帯域幅を超えた新しいセッションの確立試行はブロックされます。異なるタイプのデバイスおよびアプリケーションの場合、使用可能な帯域幅の量は独立して追跡できます。たとえば、帯域幅の独立ト

ラッキングは、デスクトップ ビデオ エンドポイントと高画質ビデオ ルーム システムがビデオ メディア ストリームを送受信するために使用できます。

同じタイプのデバイスとアプリケーションが通信を送受信している場合は、各方向で同じタイプの帯域幅控除が実行されます。ただし、異なるタイプのデバイスやアプリケーションが通信を送受信している場合は、各方向で異なるタイプの帯域幅控除が実行されます。さらに、帯域幅控除は通常、量は対称で、設計によって IP ネットワークの通常の動作を反映します。その結果、異なるタイプのデバイスとアプリケーションが通信を送受信している場合、総帯域幅控除は最大で実際に使用されているネットワーク帯域幅量の 2 倍に達することがあります。帯域幅アカウンティングにおけるこの不一致によって、新しいセッションの確立試行が不必要にブロックされる場合があります。

フレキシブル DSCP マーキングおよびビデオ プロモーション機能を使用すると、より有利な CAC および QoS 処理を受けるアプリケーションを優先するように帯域幅アカウンティングの不一致を調整するビデオ プロモーション ポリシーを設定できます。たとえば、デスクトップ ビデオ エンドポイントと高画質ビデオ ルーム システム間のセッションがビデオ ルーム システムを優先するように調整された場合、その後、調整はデスクトップ ビデオエンドポイントのプロモーションと見なされます。

調整が異なるタイプのデバイスとアプリケーションの間で有効になると、帯域幅は調整によって優先されるアプリケーション タイプの分のみ控除されます。このタイプのセッションを許容するために十分な帯域幅が使用可能な場合、調整によって優先されないタイプのデバイスまたはアプリケーションは、使用している DSCP マーキングを、調整によって優先されるタイプのデバイスまたはアプリケーションで使用される DSCP マーキングに変更するように指示されます。たとえば、デスクトップ ビデオ エンドポイントが高画質ビデオ ルーム システムとのセッションでプロモートされると、帯域幅アカウンティングは、デスクトップ ビデオエンドポイントがビデオルーム システムと同じタイプのアプリケーションであるかのように動作します。デスクトップ ビデオ エンドポイントは、DSCP マーキングを、ビデオ ルーム システムが使用している DSCP マーキングに変更するように指示されます。QoS 処理は双方向で一貫しており、帯域幅はビデオルーム システムと同じタイプのデバイスとアプリケーション間のセッション分が控除されます。デスクトップ ビデオエンドポイントと同じタイプのデバイスとアプリケーション間のセッション分の帯域幅は控除されません。

フレキシブル DSCP マーキングおよびビデオ プロモーション機能を有効にすると、Unified Communications Manager は動的にデスクトップ ビデオ デバイスに、それぞれのネゴシエートされたメディア ストリームの DSCP マーキングを示すトラフィック クラス ラベルを通知します。

ユーザに対するカスタム QoS の設定

リリース 11.0(1) を使用すると、SIP プロファイル内のサービス品質（QoS）の設定をカスタマイズし、ユーザに適用できます。[SIP プロファイル設定（SIP Profile Configuration）] ウィンドウは、次の QoS 設定で拡張されています。

- オーディオとビデオ ストリームのカスタム DSCP 値
- オーディオとビデオ ストリームのカスタム UDP ポート範囲

オーディオとビデオのカスタム DSCP 値

SIP プロファイル内のオーディオとビデオ コール用 DSCP 値を設定し、そのプロファイルを使用する SIP 電話に適用できます。[SIP プロファイル設定（SIP Profile Configuration）] ウィンドウには、次のタイプのコール用にカスタム DSCP の設定が含まれています。

- 音声通話
- ビデオ コール
- ビデオ コールの音声部分
- TelePresence コール
- TelePresence コールの音声部分

営業チームや CEO など、大半の従業員よりも QoS の優先順位の高い設定を必要とする一団が社内にいる場合、SIP プロファイル設定を使用して、これらのユーザのカスタム DSCP 値を設定できます。SIP プロファイル内の設定は、対応するクラス全体のサービス パラメータ設定を上書きします。

オーディオとビデオのカスタム UDP ポート範囲

SIP コールのオーディオ ストリームとビデオ ストリームに対して、個々に UDP ポート範囲を設定できます。通常、ビデオにはオーディオよりもかなり多くの帯域幅が必要であるため、メディアのタイプごとに専用のポート範囲を使用することで、ネットワーク帯域幅の管理を簡素化できます。また、オーディオ ストリームが広帯域幅のビデオ ストリームから分離された専用チャネルを持つことを保証することにより、オーディオ ストリームの劣化を防ぐことができます。

SIP ファイルの [メディア ポート範囲（Media Port Ranges）] フィールドを設定すれば、この設定を [オーディオとビデオに個別のポート範囲（Separate Port Ranges for Audio and Video）] に適用できます。SIP プロファイルを電話に関連付けて、設定を電話に適用できます。

トラフィック クラスのラベル

柔軟な DSCP とビデオ プロモーション機能では、設定するビデオ プロモーション ポリシーに基づいて、コールごとにその DSCP をマークするために、トラフィック クラス ラベル（TCL）を使用して動的に SIP エンドポイントに指示します。TCL はメディアごとに定義された SIP Session Description Protocol（SDP）属性であるため、TCL と 関連する DSCP マーキングは、ビデオ コールのオーディオ メディア回線とビデオ メディア回線とによって異なります。ビデオ コールのオーディオ ストリームとビデオ ストリームに対して、さまざまな DSCP マーキングを選択できます。

DSCP の設定構成のタスク フロー

ネットワークの DSCP 値とビデオ プロモーション ポリシーを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	フレキシブル DSCP マーキングおよびビデオプロモーション ポリシーの設定, （566 ページ）	異なるタイプのビデオを処理するビデオ プロモーション ポリシーを設定します。
ステップ 2	ユーザのカスタム QoS ポリシーの設定, （568 ページ）	社内の他のユーザよりも高いプライオリティを必要とするユーザがあれば、オーディオおよびビデオストリームのカスタム DSCP 値が含まれている SIP プロファイルを設定します。たとえば、社内に高い優先度を必要とする電話営業チームや CEO がいれば、そのユーザの電話にカスタマイズした SIP プロファイルを適用できます。

フレキシブル DSCP マーキングおよびビデオ プロモーション ポリシーの設定

異なるビデオのタイプを処理するようにビデオ プロモーションのポリシーを設定するには、次の手順に従います。

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 [サーバ（Server）] ドロップダウン リストから、パラメータを設定するサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リスト から、[Cisco CallManager（アクティブ）（Cisco CallManager（Active））] サービスを選択します。
サービスがアクティブとして表示されない場合、サービスが Cisco Unified Serviceability でアクティブ化されていることを確認します。

ステップ 4 デスクトップ ビデオ エンドポイントをイマーシブなビデオ エンドポイントにレベルを上げるビデオ プロモーション ポリシーを設定するには、[イマーシブ ビデオ コールにビデオ帯域プールを使用（Use Video BandwidthPool for Immersive Video Calls）] パラメータに [False（False）] を、[ビデオ コール QoS マーキング ポリシー（Video Call QoS Marking Policy）] パラメータに [イマーシブにレベルアップ（Promote to Immersive）] を設定します。

ステップ 5 その他のパラメータを設定するには、[サービス パラメータの設定（Service Parameter Configuration）] ウィンドウの適切なエリアにスクロールして、パラメータ値を更新します。サービス パラメータとその設定オプションの詳細については、「関連項目」のセクションを参照してください。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

フレキシブル DSCP マーキングおよびビデオ プロモーション サービス パラメータ, （567 ページ）

フレキシブル DSCP マーキングおよびビデオ プロモーション サービス パラメータ

（注） サービス パラメータの詳細については、パラメータ名をクリックするか、[サービス パラメータの設定（Service Parameter Configuration）] ウィンドウに表示されている疑問符（?）アイコンをクリックしてください。

表 *70*：フレキシブル *DSCP* マーキングおよびビデオ プロモーション サービス パラメータ

パラメータ	説明
クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）	サービスパラメータのこのセクションには、音声通話、ビデオ コール、ビデオ コールの音声部分、テレプレゼンス コール、テレプレゼンス コールの音声部分の DSCP を含め、広範な音声およびビデオ コール タイプのクラスタ全体の DSCP 値が含まれます。 シスコのサポートエンジニアから指示がないかぎり、これらのパラメータはデフォルト値のままにしておくことを強くお勧めします。
クラスタ全体のパラメータ（コール アドミッション制御）（Clusterwide Parameters (Call Admission Control)）	
ビデオ コール QoS マーキング ポリシー（Video Call QoS Marking Policy）	このパラメータでは、デスクトップ ビデオ エンドポイントと Cisco TelePresence イマーシブ ビデオエンドポイント間の帯域幅割り当ての不一致を調整し、イマーシブ エンドポイントを優先する [イマーシブにプロモートする（Promote to Immersive）] ポリシーを設定できます。プロモーションが実行されると、音声およびビデオの帯域幅はイマーシブ帯域幅ポート割り当てから予約されます。[イマーシブにプロモートする（Promote to Immersive）] ポリシーは、イマーシブ ビデオデバイスとフレキシブル DSCP マーキングをサポートするデスクトップ ビデオ デバイス間のコールに対してのみ有効です。

パラメータ	説明
クラスタ全体のパラメータ（システム - 場所と地域）（Clusterwide Parameters (System - Location and Region)）	
地域内のデフォルトの最大イマーシブ ビデオ コール ビット レート（オーディオ含む）（Default Intraregion Max Immersive Video Call Bit Rate (Includes Audio)）	このパラメータは、地域自体の地域との関係について、[地域の設定（Region Configuration）] ウィンドウで [システム デフォルトを使用する（Use System Default）] オプションが [最大イマーシブ ビデオ コール ビット レート（Max Immersive Video Call Bit Rate）] として選択されている場合に、特定地域内の各イマーシブ ビデオ コールのデフォルトの最大合計ビット レートを指定します。
リージョン間のデフォルトの最大イマーシブ ビデオ コール ビット レート（オーディオ含む）（Default Interregion Max Video Call Bit Rate (Includes Audio)）	このパラメータは、地域と他の地域との関係について、[地域の設定（Region Configuration）] ウィンドウで [システム デフォルトを使用する（Use System Default）] オプションが [最大イマーシブ ビデオ コール ビット レート（Max Immersive Video Call Bit Rate）] として選択されている場合に、特定地域と別の地域間での各イマーシブ ビデオ コールのデフォルトの最大合計ビット レートを指定します。
イマーシブ ビデオ コールにビデオ帯域幅プールを使用する（Use Video BandwidthPool for Immersive Video Calls）	このパラメータは、Unified Communications Manager がイマーシブ ビデオ コール用にデスクトップ ビデオ帯域幅プールからの帯域幅を予約するかどうかを指定します。

ユーザのカスタム QoS ポリシーの設定

ユーザの Quality of Service（QoS）ポリシーをセットアップするには、次のタスクを実行します。社内の一部ユーザに、他のユーザと異なる QoS 要件を使用する場合、カスタム ポリシーを適用する場合があります。たとえば、電話営業担当者または CEO です。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイルのカスタム QoS の設定, （569 ページ）	オーディオ ストリームおよびビデオ ストリーム向けにカスタマイズされた DSCP 値と UDP ポー

	コマンドまたはアクション	目的
		ト範囲を使用して SIP プロファイルを設定します。
ステップ 2	電話機へのカスタム QoS ポリシーの適用，（570 ページ）	電話に SIP プロファイルを適用します。SIP プロファイルの DSCP 設定は、DSCP のクラスタ全体のサービスパラメータ設定よりも優先されます。

SIP プロファイルのカスタム QoS の設定

この SIP プロファイルを使用する電話のカスタム DSCP 値と UDP ポート範囲を設定します。次の設定を使用して、ネットワーク内の特定の電話およびユーザに適用できるカスタマイズ QoS ポリシーを設定できます。従業員や CEO などの企業内の特定のユーザに、特定の QoS 設定を適用するには、次のように行います。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [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 次のいずれかの手順を実行します。

- [検索（Find）] をクリックし、既存の SIP プロファイルを選択します。
- [新規追加（Add New）] をクリックして、新しい SIP プロファイルを作成します。

ステップ 3 [メディア ポートの範囲（Media Port Ranges）] フィールドで、オーディオ メディアおよびビデオ メディアの両方に対応する単一の UDP ポート範囲、またはオーディオ ストリームおよびビデオ ストリームそれぞれに対応するポート範囲のどちらを割り当てるかを選択します。

- オーディオメディアおよびビデオメディアに1つのポート範囲を設定するには、[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）] フィールドにポート範囲を入力します。有効なポートは 2048 ～ 65535 です。
- オーディオ ストリームおよびビデオ ストリームにそれぞれポート範囲を設定する場合は、[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）] フィールドを使用して、オーディオポートの範囲を入力します。[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）] フィールドを使用して、ビデオ ポートの範囲を入力します。各ポートの有効な値は、 2048 ～ 65535 です。2 つのポート範囲を重複させることはできません。

ステップ 4 次のフィールドで、オーディオストリームおよびビデオストリーム用にカスタマイズされたDSCP値を設定します。

- 音声コールの DSCP（DSCP for Audio Calls）

- ビデオ コールの DSCP（DSCP for Audio Calls）
- ビデオコールのオーディオ部分の DSCP（DSCP for Audio Portion of Video Calls）
- TelePresence コールの DSCP（DSCP for TelePresence Calls）
- TelePresence コールのオーディオ部分の DSCP（DSCP for Audio Portion of TelePresence Calls）

（注） デフォルトでは、上記の各フィールドは、対応するサービス パラメータの値を使用するように設定されています。新しい値を割り当てると、サービス パラメータ設定は新しい値に上書きされます。

ステップ 5 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

次の作業

電話機へのカスタム QoS ポリシーの適用, （570 ページ）

電話機へのカスタム QoS ポリシーの適用

DSCP 値や、音声およびビデオ メディアの UDP ポート範囲などのカスタマイズされた QoS 設定を含む SIP プロファイルを適用するには、次の手順を使用します。この SIP プロファイルを電話機に適用すると、電話機は SIP プロファイルのカスタム設定を使用します。

はじめる前に

SIP プロファイルのカスタム QoS の設定, （569 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [検索（Find）] をクリックして既存の電話機を選択します。
- [新規追加（Add New）] をクリックして新しい電話機を作成します。

ステップ 3 [SIP プロファイル（SIP Profile）] ドロップダウン リストから、カスタム DSCP 値と UDP ポート範囲の値を設定する SIP プロファイルを選択します。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

フレキシブル DSCP マーキングおよびビデオ プロモーションのインタラクションと制約事項

フレキシブル DSCP マーキングおよびビデオ プロモーションの連携動作

表 *71*：フレキシブル *DSCP* マーキングおよびビデオ プロモーションの連携動作

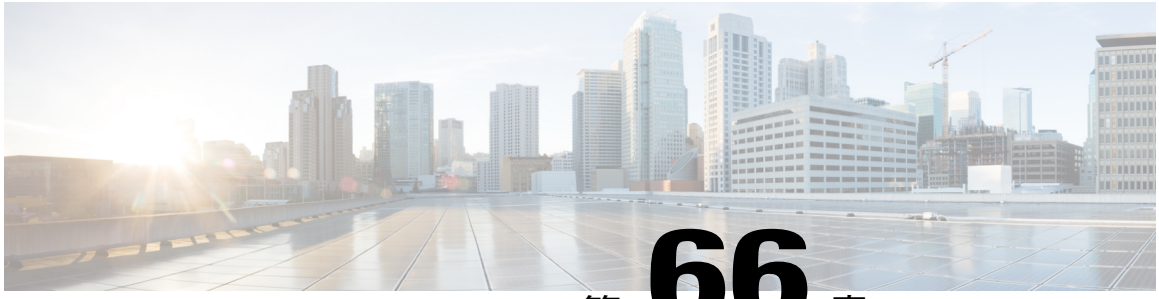
Device	データのやり取り
SIP クラスタ間トランク	フレキシブル DSCP マーキングおよびビデオプロモーション機能は、SIP クラスタ間トランクを介してサポートされます。
Skinny Client Control Protocol（SCCP）デバイス	フレキシブル DSCP マーキングおよびビデオプロモーション機能は、SCCP デバイス向けにサポートされています。
パススルー MTP	パススルー MTP がコールに挿入されている場合、Unified Communications Manager は、最初にビデオストリーム用にパケットを出力したエンドポイントデバイスから予期される DSCP マーキングでパケットをマークするように、MTP に通知します。コールの 2 つのエンドポイントが異なる DSCP マーキング（Cisco TelePresence イマーシブ ビデオ エンドポイントとビデオ プロモーションのないデスクトップ ビデオ エンドポイント）を使用する場合、MTP は各ストリーム方向で DSCP マーキングを維持します。

フレキシブル DSCP マーキングおよびビデオ プロモーションの制約事項

表 *72*：フレキシブル *DSCP* マーキングおよびビデオ プロモーションの制約事項

制約事項	説明
トランクおよびゲートウェイ	フレキシブル DSCP マーキングおよびビデオプロモーション機能は、H.323 トランクおよび Media Gateway Control Protocol（MGCP）ゲートウェイではサポートされません。

制約事項	説明
Multilevel Precedence and Preemption	シスコはフレキシブルDSCPマーキングおよびビデオ プロモーション機能を Multilevel Precedence and Preemption（MLPP）サービスコールと一緒に使用することは推奨しません。MLPPサービス機能が必要な場合、[実体験ビデオ通話（Immersive Video Calls）] サービス パラメータで、[ビデオ通話QoSマーキング ポリシー（Video Call QoS Marking Policy）] と [ビデオ帯域幅プールを使用（Use Video BandwidthPool）] をそれぞれのデフォルト値に設定することをお勧めします。[実体験ビデオ通話（Immersive Video Calls）] サービス パラメータで、[ビデオ通話 QoS マーキング ポリシー（Video Call QoS Marking Policy）] と [ビデオ帯域幅プールを使用（Use Video BandwidthPool）] をデフォルト値に設定すると、Unified Communications Manager とエンドポイントがメディア パケットに対して MLPP DSCP マーキングを使用します。
SIP ビデオ エンドポイント	フレキシブルDSCPマーキングおよびビデオプロモーション機能は、デスクトップ SIP ビデオエンドポイントのサポートによって異なります。現在、Cisco DX650 シリーズの SIP 電話のみが、必要なエンドポイントのサポートを提供しています。



第 66 章

トランスコーダおよびメディア ターミネーション ポイントの設定

- トランスコーダとメディア ターミネーション ポイントの概要，573 ページ
- トランスコーダと MTP 設定のタスク フロー，579 ページ
- トランスコーダと MTP の連携動作と制約事項，584 ページ

トランスコーダとメディア ターミネーション ポイントの概要

トランスコーダ

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換するデバイスです。たとえば、G.711 コーデックのストリームを取得して、リアルタイムで G.729 ストリームに変換できます。トランスコーダは、コーデックの変換に加えて、メディア ターミネーション ポイント（MTP）と同じ機能も実行できます。トランスコーダ機能と MTP 機能の両方が必要な場合、トランスコーダがシステムによって割り当てられます。MTP 機能が必要な場合、システムはトランスコーダまたは MTP をリソース プールから割り当てます。リソースの選択はメディア リソース グループによって決まります。

（注） トランスコーダは、G.711 コーデックとすべてのコーデック（MTP/TRP の機能を提供するときにトランスコーダとして機能する G.711 を含む）間のトランスコーディングをサポートしています。

2 台のデバイスが異なる音声コーデックを使用しており、通常であれば通信できない場合、Cisco Unified Communications Manager がエンドポイント デバイスに代わってトランスコーダを呼び出します。コールに挿入されると、トランスコーダは互換性のない 2 つのコーデック間でデータ ストリームを変換し、コーデック間の通信を可能にします。トランスコーダは、そのコールに関係するユーザやエンドポイントには表示されません。

トランスコーダおよびメディア リソース マネージャ

すべての Cisco Unified Communications Manager ノードは、メディア リソース マネージャ（MRM）を介してトランスコーダにアクセスできます。MRM はトランスコーダへのアクセスを制御します。

また、MRM は Cisco Unified Communications Manager のメディア リソース グループおよびメディア リソース グループ リストを使用します。メディア リソース グループ リストにより、トランスコーダは、メディア リソース グループ リストに割り当てられたほかのデバイスと通信できるようになります。それに続き、クラスタ内のリソース管理が可能になります。

トランスコーダ制御プロセスは、データベースで定義されたトランスコーダ デバイスごとに作成されます。MRM は、トランスコーダのリソースを追跡し、その可用性をクラスタ全体にアドバタイズします。

メディア ターミネーション ポイントとしてのトランスコーダ

ハードウェアベースのトランスコーダのリソースも、メディア ターミネーション ポイント（MTP）とトラステッド リレー ポイント（TRP）の両方またはいずれか一方の機能をサポートします。この機能で、Cisco Unified Communications Manager は、コール中のエンドポイントに MTP または TRP が必要と判断すると、トランスコーダ リソースを配分し、コールに挿入します。その場合、このリソースが MTP トランスコーダのように動作します。

Cisco Unified Communications Manager は、MTP と TRP とトランスコーディング機能を同時にサポートします。たとえば、（G.723 の地域に位置する）Cisco Unified IP Phone から（G.711 の地域に位置する）NetMeeting へのコールが発生すると、1 つのトランスコーダ リソースが MTP とトランスコーディング機能を同時にサポートします。

必要なソフトウェア MTP リソースが利用できない場合、コールは MTP リソースおよび MTP/TRP サービスを使用せずに接続を試みます。ハードウェア トランスコーダ機能が、（コーデックを別のコーデックに変換する上で）必要な時に利用できない場合、コールは失敗します。

（注） トランスコーダは、トランスコーダとして機能している時、および MTP/TRP 機能を提供している時に、G.711 と、G.711 を含むすべてのコーデックとの間のトランスコーディングをサポートします。

トランスコーダ タイプ

Cisco Unified Communications Manager Administration のトランスコーダの種類は、次の表にリストされています。

（注） トランスコーダは、G.711 と、（トランスコーダとして機能しているときと MTP/TRP 機能を提供しているとき）G.711 を含むすべてのコーデックとの間のトランスコーディングをサポートしています。

表 *73*：トランスコーダ タイプ

トランスコーダ タイプ（**Transcoder Type**）	説明
Cisco Media Termination Point のハードウェア	このタイプは、Cisco Catalyst 4000 WS-X4604-GWY と Cisco Catalyst 6000 WS-6608-T1 または WS-6608-E1 をサポートしており、次のトランスコーディング セッション数をサポートしています。 Cisco Catalyst 4000 WS-X4604-GWY について • G.711-16 MTP transcoding セッションへのトランスコーディングについて Cisco Catalyst 6000 WS-6608-T1 または WS-6608-E1 について • G.723 から G.711 へのトランスコーディングについて/G.729 から G.711-24 への物理ポートごとの MTP トランスコーディング セッション。モジュールごとに 192 セッション
Cisco IOS メディア ターミネーション ポイント（ハードウェア）	このタイプは Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745、Cisco 3660、Cisco 3640、Cisco 3620、Cisco 2600、Cisco VG200 ゲートウェイをサポートしており、トランスコーディング セッション数は次のとおりです。 NM-HDV ごと • G.711 から G.729-60 にトランスコーディング • G.711 から GSM FR/GSM EFR- 45 へのトランスコーディング

トランスコーダ タイプ（**Transcoder Type**）	説明
Cisco IOS 拡張メディア ターミネーション ポイント（ハードウェア）	NM-HD ごと Cisco 2600XM、Cisco 2691、Cisco 3660、Cisco 3725、Cisco 3745、Cisco 3660 アクセス ルータをサポートするこのタイプのトランスコーディング セッション数は次のとおりです。 • G.711 から G.729a/G.729ab/GSMFR-24 にトランスコーディング • G.711 から G.729/G.729b/GSM EFR-18 にトランスコーディング NM-HDV2 ごと Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745、Cisco 3660 アクセス ルータをサポートするこのタイプのトランスコーディング数は次のとおりです。 • G.711 から G.729a/G.729ab/GSMFR-128 にトランスコーディング • G.711 から G.729/G.729b/GSM EFR-96 にトランスコーディング
Cisco Media Termination Point（WS-SVC-CMM）	このタイプは、実装されたドーターカードあたり 64 のトランスコーディング セッションを提供します。1 枚のドーター カードで 64 のトランスコーディング セッション、2 枚のドーター カードで 128 のトランスコーディング セッション、3 枚のドーターカードで 192 のトランスコーディング セッション、4 枚のドーター カード（最大）で 256 のトランスコーディング セッション。 このタイプは、次のコーデックのすべての組み合わせの間でトランスコーディングを提供します。 • G.711 a-law と G.711 mu-law • G.729 annex A と annex B • G.723.1 • GSM （FR） • GSM （EFR）

トランスコーダのフェールオーバーおよびフォールバック

次の項目では、トランスコーダが非アクティブになったCisco Unified Communications Managerノードに登録されている場合のトランスコーダ デバイスのリカバリ方法を説明しています。

- プライマリ Cisco Unified Communications Manager ノードで障害が生じた場合、トランスコーダは、トランスコーダが属するデバイス プールに指定された Cisco Unified Communications Manager グループ内で次に使用可能なノードへの登録を試みます。
- プライマリ Cisco Unified Communications Manager ノードが使用可能になるとすぐに、トランスコーダ デバイスはそれに登録します。
- トランスコーダ デバイスは到達不能になった Cisco Unified Communications Manager ノードから登録を解除します。そのノード上にあったコールは、リスト内の次の Cisco Unified Communications Manager ノードに登録されます。
- トランスコーダが新しい Cisco Unified Communications Manager ノードへの登録を試みても、登録確認応答が受信されない場合、トランスコーダはリスト内の次のノードに登録します。

トランスコーダ デバイスは、ハード リセットまたはソフト リセットの後に登録解除され、切断されます。リセットが完了すると、デバイスはプライマリ Cisco Unified Communications Manager ノードに再登録します。

メディア ターミネーション ポイント

メディア ターミネーション ポイント（MTP）により、Cisco Unified Communications Manager は、SIP または H.323 のエンドポイント、またはゲートウェイ経由でルーティングされたコールを中継できます。メディア ターミネーション ポイントは、H.323 エンドポイント経由でコールがルーティングされた場合は通常利用できない補足サービス（コール保留、コール転送、コール パーク、会議など）を拡張します。H.323 の補足サービスの利用には、Empty Capability Set（ECS）または FastStart をサポートしないエンドポイントにのみ MTP が必要です。ECS および FastStart をサポートする、Cisco のすべてのエンドポイントおよびサードパーティのエンドポイントには MTP は必要ありません。

Cisco Unified Communications Manager が利用できる場合、MTP デバイスは、プライマリ Cisco Unified Communications Manager に登録され、サポートする MTP リソースの数を Cisco Unified Communications Manager に通知します。同じ Cisco Unified Communications Manager に複数の MTP を登録できます。複数の MTP が Cisco Unified Communications Manager に登録される場合、その Cisco Unified Communications Manager が、各 MTP の一連のリソースを制御します。

たとえば、MTP サーバ 1 が 48 の MTP リソース向けに設定され、MTP サーバ 2 が 24 の MTP リソース向けに設定されているとします。両方の MTP が、同じ Cisco Unified Communications Manager に登録される場合、その Cisco Unified Communications Manager が、両方の一連のリソースである合計 72 の登録されたリソースを保持します。

Cisco Unified Communications Manager は、コール エンドポイントが MTP を必要とすると判断すると、最小のアクティブ ストリームを持つ MTP から MTP リソースを割り当てます。その MTP リソースが、エンドポイントのためにコールに挿入されます。システムのユーザ、およびリソースが挿入されたエンドポイントの両方が MTP リソースの利用を意識することはありません。必要な

MTP リソースが利用できない場合、コールは MTP リソースを使わずに接続し、補足サービスを利用しません。

MTP フェールオーバーおよびフォールバック

ここでは、MTP デバイスが登録している Cisco Unified Communications Manager に到達できなくなったときに、フェールオーバーとフォールバックがどのように発生するかを説明します。

- プライマリ Cisco Unified Communications Manager で障害が発生した場合、MTP は、MTP が属するデバイス プールに指定された Cisco Unified Communications Manager グループ内で、次に利用可能な Cisco Unified Communications Manager への登録を試みます。
- MTP デバイスは、障害が発生し、現在使用されていないプライマリ Cisco Unified Communications Manager が使用可能になるとすぐに再登録します。
- システムは、すべての参加者が切断されるまで、コール保留モードでアクティブであったコールまたは会議を維持します。システムが補足サービスを利用できるようにすることはありません。
- MTP が新しい Cisco Unified Communications Manager への登録を試み、登録の確認応答が受信されなかった場合、MTP は次の Cisco Unified Communications Manager に登録されます。

MTP デバイスは、ハード リセットまたはソフト リセット後に登録を解除し、その後接続を解除します。リセットが完了すると、デバイスは Cisco Unified Communications Manager に再登録されます。

ソフトウェア メディア ターミネーション ポイントの種類

Cisco Unified Communications Manager Administration のソフトウェア メディア ターミネーション ポイントの種類を次の表で示します。

ソフトウェア MTP の種類	説明
Cisco メディア ターミネーション ポイント ソフトウェア	1 つの MTP は、ネットワークの速度およびネットワーク インターフェイス カード（NIC）に応じて、デフォルトで 48 の MTP（ユーザが設定可能）リソースを提供します。たとえば、100 MB のネットワークまたは NIC カードの場合、48 の MTP リソースをサポートできますが、10 MB の NIC カードではサポートできません。 10 MB のネットワークまたは NIC カードでは、約 24 の MTP リソースを指定できます。ただし、使用可能な MTP リソースの正確な数は、その PC の他のアプリケーションが消費するリソース、プロセッサの速度、ネットワーク負荷などのさまざまな要因によって異なります。

トランスコーダと MTP 設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	トランスコーダの設定, （579 ページ）を行うには、次のサブタスクを完了します。 • トランスコーダの追加, （580 ページ） • メディア リソース グループへのトランスコーダの追加, （580 ページ）	トランスコーダを設定する必要がある場合は、次の手順に従います。トランスコーダは、1 つのコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換します。
ステップ 2	ソフトウェア MTP の設定, （582 ページ）を行うには、次のサブ タスクを完了します。 • ソフトウェア MTP の追加, （582 ページ） • メディア リソース グループへのソフトウェア MTP の追加, （583 ページ）	ソフトウェア MTP を設定する必要がある場合は、次の手順に従います。ソフトウェア MTP によって、Cisco Unified Communications Manager は、SIP または H.323 エンドポイントまたはゲートウェイ経由でルーティングされたコールをリレーできます。

トランスコーダの設定

手順

	コマンドまたはアクション	目的
ステップ 1	必要なトランスコーダ リソースの数とリソースの提供に必要なトランスコーダ デバイスの数を決定します。	マルチサイト配置の場合は、トランスコーダを必要な各サイトにローカルに配置することを推奨します。複数のコーデックが必要な場合は、すべてのコーデックをサポートしないエンドポイントの数、これらのエンドポイントを配置する場所、これらのリソースにアクセスする他のグループ、これらのデバイスがサポートする同時コールの最大数、およびネットワーク上でこれらのリソースを配置する場所を検討する必要があります。

	コマンドまたはアクション	目的
ステップ 2	トランスコーダの追加, （580 ページ）	あるコーデックからの入力ストリームを別のコーデックを使用する出力ストリームに変換するようにトランスコーダを設定します。
ステップ 3	メディア リソース グループへのトランスコーダの追加, （580 ページ）	適切なメディア リソース グループに新しいトランスコーダを追加します。
ステップ 4	トランスコーダデバイスを再起動します。	詳細については、トランスコーダのマニュアルを参照してください。

トランスコーダの追加

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換するデバイスです。

はじめる前に

必要なトランスコーダのリソース数を決定し、これらのリソースを提供するうえで必要なトランスコーダのデバイス数を決定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] にログインし、[メディア リソース（Media Resources）] > [トランスコーダ（Transcoder）].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 [トランスコーダの設定（Transcoder Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

メディア リソース グループへのトランスコーダの追加, （580 ページ）

メディア リソース グループへのトランスコーダの追加

はじめる前に

トランスコーダの追加, （580 ページ）

手順

ステップ 1 [メディア リソース（Media Resources）] > [メディア リソース グループ（Media Resource Group）] を選択します。

ステップ 2 [検索（Find）] をクリックして設定されたメディア リソース グループのリストを表示します。

ステップ 3 必要なメディア リソース グループをクリックします。
[メディア リソース グループの設定(Media Resource Group Configuration)] ウィンドウが表示されます。

ステップ 4 トランスコーダを [利用可能なメディア リソース（Available Media Resources）] のリストから選択し、[選択されたメディア リソース（Selected Media Resources）] のリストに追加します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [メディア リソース（Media Resources）] > [メディア リソース グループ（Media Resource Group）] に移動します。

ステップ 7 [トランスコーダの検索と一覧表示（Find and List Transcoders）] ウィンドウで、同期させるトランスコーダの隣にあるチェックボックスをオンにします。ウィンドウ内のすべてのトランスコーダを選択するには、一致するレコードのタイトル バーのチェックボックスをオンにします。

ステップ 8 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。
[設定情報の適用（Apply Configuration Information）] ダイアログ ボックスが表示されます。

ステップ 9 [OK] をクリックします。

次の作業

トランスコーダ デバイスを再起動します。

トランスコーダの同期

トランスコーダを最新の設定変更と同期するには、次の手順を実行します。この手順は、最小限の割り込みで未適用の設定を適用します（たとえば、影響を受けるデバイスでのリセットや再起動が不要です）。

手順

ステップ 1 [メディア リソース（Media Resources）] > [トランスコーダ（Transcoder）] の順に選択します。
[トランスコーダの検索と一覧表示（Find and List Transcoders）] ウィンドウが表示されます。

ステップ 2 使用する検索条件を選択します。

ステップ 3 [検索（Find）] をクリックします。
検索条件に一致するトランスコーダのリストがウィンドウに表示されます。

ステップ 4 同期するトランスコーダの横にあるチェック ボックスをオンにします。ウィンドウ内のすべてのトランスコーダを選択するには、一致するレコードのタイトルバーのチェック ボックスをオンにします。

ステップ 5 [選択項目への設定の適用（Apply Config to Selected）] をクリックします。
[設定情報の適用（Apply Configuration Information）] ダイアログ ボックスが表示されます。

ステップ 6 [OK] をクリックします。

ソフトウェア MTP の設定

ここでは、ソフトウェア MTP の設定手順を説明します。ハードウェア MTP の設定については、トランスコーダの設定, （579 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	ソフトウェア MTP の追加, （582 ページ）	SIP エンドポイントまたはゲートウェイを介してルーティングされるコールをリレーするように、メディア ターミネーション ポイントを設定します。
ステップ 2	メディア リソース グループへのソフトウェア MTP の追加, （583 ページ）	適切なメディア リソース グループに新しいメディア ターミネーション ポイントを追加します。
ステップ 3	メディア ターミネーション ポイントのデバイスを再起動します。	

ソフトウェア MTP の追加

はじめる前に

必要な MTP リソースの数と、これらのリソースに必要な MTP デバイスの数を決定します。

手順

ステップ 1 Cisco Unified CM の管理から、[メディア リソース（Media Resources）] > [Media Termination Point（メディア ターミネーション ポイント）] 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 [Media Termination Point（メディア ターミネーション ポイント）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

メディア リソース グループへのソフトウェア MTP の追加, （583 ページ）

メディア リソース グループへのソフトウェア MTP の追加

はじめる前に

ソフトウェア MTP の追加, （582 ページ）

手順

ステップ 1 [メディア リソース（Media Resources）] > [メディア リソース グループ（Media Resource Group）] を選択します。

ステップ 2 [検索（Find）] をクリックして設定されたメディア リソース グループのリストを表示します。

ステップ 3 必要なメディア リソース グループをクリックします。
[メディア リソース グループの設定(Media Resource Group Configuration)] ウィンドウが表示されます。

ステップ 4 トランスコーダを [利用可能なメディア リソース（Available Media Resources）] のリストから選択し、[選択されたメディア リソース（Selected Media Resources）] のリストに追加します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

メディア ターミネーション ポイントのデバイスを再起動します。

トランスコーダと MTP の連携動作と制約事項

トランスコーダの制限

トランスコーダの制限

制約事項	説明
トランスコーダの削除	メディア リソース グループに割り当てられたトランスコーダは削除できません。トランスコーダを使用しているメディアリソースグループを検索するには、[トランスコーダの設定（Transcoder Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウン リストボックスで[依存関係レコード（Dependency Records）] を選択し、[Go] をクリックします。[依存関係レコード サマリー（Dependency Records Summary）] ウィンドウにトランスコーダを使用しているメディア リソース グループに関する情報が表示されます。メディアリソース グループに関する詳細を検索するには、メディア リソース グループをクリックして、[依存関係レコードの詳細（Dependency Records Details）] ウィンドウを表示します。システムで依存関係レコードが有効でない場合、[依存関係レコード サマリー（Dependency Records Summary）] ウィンドウにメッセージが表示されます。使用中のトランスコーダの削除を試みると、Cisco Unified Communications Manager がメッセージを表示します。現在使用中のトランスコーダを削除する前に、トランスコーダが割り当てられているメディア リソース グループからトランスコーダを削除する必要があります。

メディア ターミネーション ポイントの制限

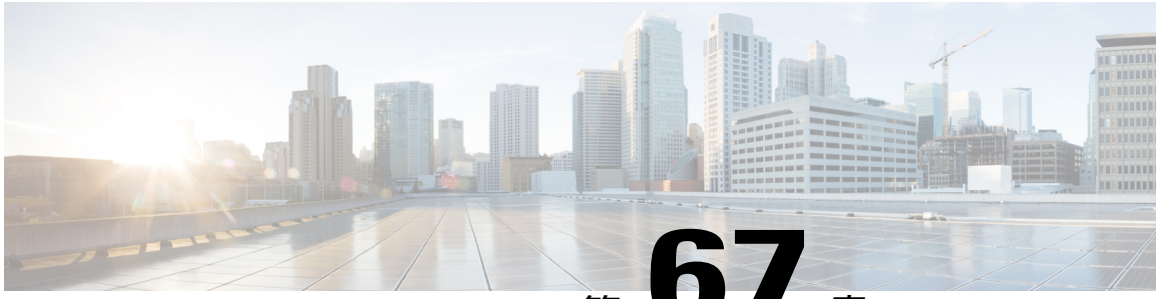
表 *74* : メディア ターミネーション ポイントの制限

制約事項	説明
Cisco IP Voice Media Streaming Application	サーバごとにアクティブ化できる Cisco IP Voice Streaming Application は 1 つのみです。より多くの MTP リソースを提供するには、追加のネットワーク接続されたサーバで Cisco IP Voice Streaming Application をアクティブ化します。 Cisco Unified Communications Manage のパフォーマンスに悪影響が及ぶ可能性があるため、コール処理の負荷が大きい Cisco Unified Communications Manager では Cisco IP Voice Streaming Media Application をアクティブ化しないことを強くお勧めします。
Cisco Unified Communications Manager への登録	各 MTP は、一度に 1 つの Cisco Unified Communications Manager のみに登録できます。システムの設定方法に応じて、システムに複数の MTP があり、それぞれがいずれかの Cisco Unified Communications Manager に登録されている場合があります。

第 IX 部

登録デバイス

- 登録デバイスの概要，589 ページ
- TFTP サーバの設定，591 ページ
- デバイスのデフォルトの更新，601 ページ
- 自動登録の設定，605 ページ
- 電話機の手動登録，615 ページ
- セルフプロビジョニングの設定，619 ページ



第 67 章

登録デバイスの概要

- デバイスの登録について，589 ページ
- デバイスの登録，589 ページ

デバイスの登録について

この項では、新しいエンドポイント デバイスの登録、エンドポイント デバイスとゲートウェイ デバイス用のプロキシ TFTP サーバの設定で実行する作業について説明します。

新しい電話機を手動で登録するか、または自動登録を使用することを選択できます。100 台を超える電話機を登録するには、一括管理ツール（BAT）を使用します。詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

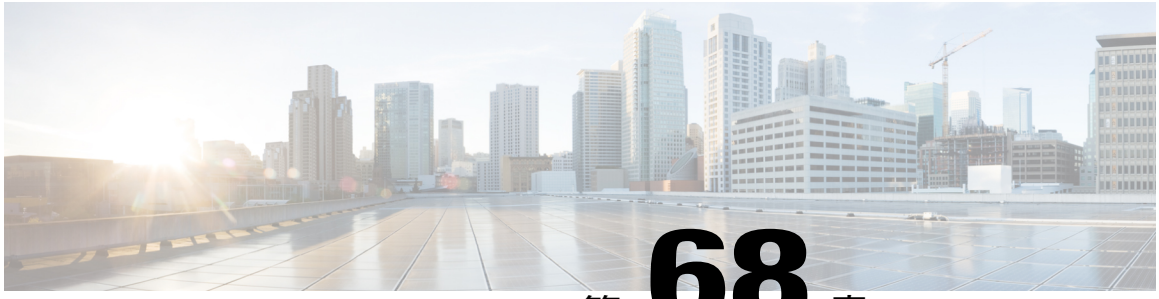
（注） BAT を使用して新しい設定を作成することはできませんが、BAT を使用して電話機を登録する場合は電話パラメータを設定できます。デバイス プール、ロケーション、コーリング サーチ スペース、ボタン テンプレート、ソフトキー テンプレートなどの電話の設定が、Cisco Unified CM の管理を使用して設定済みであることを確認します。

デバイスの登録

次のタスク フローを実行すると、システムのデバイスを登録できます。

手順

	コマンドまたはアクション	目的
ステップ 1	TFTP サーバの設定タスク フロー, （593 ページ）	ネットワークのエンドポイントの設定ファイルを提供するプロキシ Trivial File Transfer Protocol（TFTP）サーバを設定します。
ステップ 2	デバイスのデフォルトの更新タスク フロー, （601 ページ）	（任意） 登録時にエンドポイントに適用された、デバイスロード、デバイスプール、電話ボタンテンプレートの各値を変更します。
ステップ 3	自動登録の設定タスク フロー, （606 ページ）	ネットワークの自動登録を有効にします。デバイスがネットワークに自動で登録されることを許可すること自体にセキュリティリスクがあるので、新しいエンドポイントが登録でき次第、自動登録を無効にすることをお勧めします。
ステップ 4	手動によるデバイス登録タスク フロー, （615 ページ）	手動で IP フォンを登録し、新しいディレクトリ番号を割り当てます。
ステップ 5	セルフプロビジョニングの設定タスク フロー, （621 ページ）	これはオプションです。エンドユーザが、管理者を使わずに自社の電話機をプロビジョニングできるようにするのなら、セルフプロビジョニングを設定します。



第 68 章

TFTP サーバの設定

- プロキシ TFTP 導入の概要，591 ページ
- TFTP サーバの設定タスク フロー，593 ページ

プロキシ TFTP 導入の概要

ネットワークのエンドポイントが必要とするダイヤル計画、呼出音ファイル、デバイス設定ファイルなどを提供するために、プロキシ Trivial File Transfer Protocol（TFTP）サーバを使用します。TFTP サーバは、導入する任意のクラスタに設置でき、複数のクラスタのエンドポイントから要求を処理できます。DHCP スコープでは、設定ファイルを取得するためにプロキシ TFTP サーバの IP アドレスを指定します。

冗長とピア プロキシ TFTP サーバ

単一クラスタ導入では、クラスタは、少なくとも 1 つのプロキシ TFTP サーバが必要です。別のプロキシ TFTP サーバを冗長性のためのクラスタに追加できます。2 番目のプロキシ TFTP サーバは、IPv4 のオプション 150 に追加されます。IPv6 では、DHCP スコープの TFTP サーバ アドレスのサブオプションのタイプ 1 に 2 番目のプロキシ TFTP サーバを追加します。

複数のクラスタを導入する場合、プライマリ プロキシ TFTP サーバのピア クラスタとして、最大 3 台のリモート プロキシ TFTP サーバを指定できます。これは、多数の DHCP スコープに対してプロキシ TFTP サーバを 1 台だけ設定する場合に便利です。プライマリ プロキシ TFTP サーバは、ネットワークのすべての電話やデバイスに設定ファイルを提供します。

それぞれのリモート プロキシ TFTP サーバとプライマリ プロキシ TFTP サーバとの間のピア関係を作成する必要があります。

ヒント　ネットワークのリモートプロキシTFTPサーバ間のピア関係を設定する際、階層的な関係を保つようにします。ループを回避するために、リモート クラスタのピア プロキシ TFTP サーバが相互に指しあわないことを確認します。たとえば、プライマリ ノードAが、ノードB、ノードCとピア関係にあると、ノードBとノードCの間のピア関係を作成してはいけません。作成すると、ループ関係ができます。

IPv4 および IPv6 デバイスの TFTP サポート

TFTP サーバの IP アドレスを検出するために、IPv4 電話とゲートウェイの DHCP カスタム オプション 150 の使用を有効にすることをお勧めします。ゲートウェイと電話はオプション 150 を使用して TFTP サーバの IP アドレスを検出します。詳細については、デバイスに付属のドキュメントを参照してください。

IPv6 ネットワークでは、シスコ ベンダー固有の DHCPv6 情報を使用して、TFTP サーバの IPv6 アドレスをエンドポイントに渡すことをお勧めします。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。

IPv4 を使用するエンドポイントと IPv6 を使用するエンドポイントがある場合は、IPv4 用に DHCP カスタム オプション 150 を使用し、IPv6 用にシスコ ベンダー固有の情報オプションである TFTP サーバアドレス サブオプション タイプ 1 を使用することをお勧めします。エンドポイントが IPv6 アドレスを取得して TFTP サーバに要求を送信する一方、TFTP サーバが IPv4 を使用して要求を処理している場合、TFTP サーバは IPv6 スタック上で要求をリスニングしていないため、要求を受信しません。この場合、エンドポイントは、Cisco Unified Communications Manager に登録できません。

TFTP サーバの IP アドレスを検出するために、IPv4 および IPv6 デバイスで使用できる代替手段があります。たとえば、IPv4 デバイスでは DHCP オプション 066 または CiscoCM1 を使用できます。IPv6 デバイスでは、その他の方法として、TFTP サービス サブオプション タイプ 2 の使用や、エンドポイントでの TFTP サーバの IP アドレスの設定が含まれます。これらの代替手段は推奨されません。代替手段を使用する前に、シスコのサービス プロバイダーに問い合わせてください。

TFTP 導入でのエンドポイントと設定ファイル

SCCP 電話、SIP 電話、ゲートウェイは、初期化時に設定ファイルが必要です。デバイス設定を変更すると常に、更新された設定ファイルがエンドポイントに送信されます。

設定ファイルには、Cisco Unified Communications Manager ノードの優先順位付けされたリスト、それらのノードに接続するために使用された TCP ポート、その他の実行可能ファイルなどの情報が含まれます。一部のエンドポイントでは、設定ファイルにメッセージ、ディレクトリ、サービス、情報などの電話ボタンのロケール情報と URL も含まれます。ゲートウェイの設定ファイルには、デバイスが必要なすべての設定情報が含まれています。

TFTP のセキュリティに関する考慮事項

シスコ プロキシ TFTP サーバは、署名付き要求と署名なし要求の両方を処理し、非セキュア モードまたは混合モードのいずれかで動作できます。プロキシ TFTP サーバは、ファイルをエンドポイントに送信する前に、独自の TFTP 秘密キーでファイルに署名します。

プロキシ TFTP サーバがエンドポイントのホーム クラスタに存在する単一クラスタ導入では、エンドポイントが自動的に署名付き設定ファイルを信頼します。

プロキシ TFTP 導入にリモート クラスタが含まれる場合は、プロキシ TFTP サーバをすべてのリモート エンドポイントの信頼検証リスト（TVL）に追加する必要があります。追加しないと、エンドポイントは、リモート プロキシ TFTP サーバからの書名付きファイルを拒否します。手順については、エンドポイント デバイスをサポートするドキュメントを参照してください。

混合モードで動作しているリモート クラスタ上のすべての TFTP サーバに、プライマリ クラスタ TFTP サーバまたはクラスタ外 CTL ファイルに追加された IP アドレスが存在している必要があります。存在していない場合は、セキュリティが有効なクラスタに登録するエンドポイントが必要なファイルをダウンロードできません。

TFTP サーバの設定タスク フロー

Extension Mobility Cross Cluster（EMCC）をクラスタ用に設定している場合、システムでプロキシ TFTP サーバを動的に設定できます。EMCC を設定していない場合は、TFTP サーバを設定して、手動でセキュリティ モードを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	次の方法のいずれかを使用して、TFTPサーバを設定します。 • TFTP サーバの動的設定, （594 ページ） • TFTP サーバの手動設定, （595 ページ）	Extension Mobility Cross Cluster（EMCC）を設定している場合、TFTP サーバを動的に設定できます。 EMCC を設定していない場合は、手動で TFTP サーバを設定します。クラスタがセキュアか非セキュアかを示す必要があります。デフォルトでは、クラスタは非セキュアとして処理されます。
ステップ 2	TFTP サーバ ピア関係を追加, （596 ページ）	（任意） プライマリ プロキシ TFTP サーバとのピア関係を設定して、リモート プロキシ TFTP サーバを追加します。
ステップ 3	TFTP サーバの CTL ファイルの更新, （597 ページ）	（任意） CTL クライアント プラグインをインストールして、混合モードで動作するすべてのリモート クラスタ内にあるすべてのプロキシ TFTP サーバの Cisco

	コマンドまたはアクション	目的
		Certificate Trust List（CTL）ファイルにプライマリ TFTP サーバを追加します。
ステップ 4	エンドポイントデバイスに対応するドキュメントを参照してください。	（任意） プロキシ TFTP の導入にリモート クラスタが含まれている場合、プロキシ TFTP サーバをすべてのリモート エンドポイントの信頼検証リスト（TVL）に追加します。
ステップ 5	TFTP サーバの非設定ファイルの変更，（597 ページ）	（任意） エンド ポイントがプロキシ TFTP サーバから要求する非設定ファイルを変更できます。
ステップ 6	TFTP サービスの停止および開始，（598 ページ）	（任意） エンドポイントの変更済み非設定ファイルをアップロードした場合、プロキシ TFTP ノードの TFTP サービスを停止および再起動します。
ステップ 7	DHCP サーバに対応するドキュメントを参照してください。	（任意） 複数のクラスタを導入する場合、プライマリ プロキシ TFTP サーバの IP アドレスを含むように個々のリモート ノードの DHCP 範囲を変更します。

TFTP サーバの動的設定

ネットワークに Cisco Extension Mobility Cross Cluster（EMCC） が設定されている場合は、Cisco Proxy TFTP Server を動的に設定できます。

はじめる前に

ネットワークの EMCC を設定します。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager* 機能およびサービス ガイド』を参照してください。

手順

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[詳細機能（Advanced Features）] > [クラスタ ビュー（Cluster View）] > [今すぐリモート クラスタを更新（Update Remote Cluster Now）] を選択します。TFTP サーバは、自動的に該当クラスタ向けに設定されます。

次の作業

リモート プロキシの TFTP サーバをエンドポイントの信頼検証リスト（TVL）に追加する必要があります。追加しない場合、リモート クラスタ上にあるプロキシの TFTP サーバの設定ファイルは承認されません。手順については、エンドポイント デバイスに対応しているマニュアルを参照してください。

TFTP サーバの手動設定

EMCC が設定されていない場合にネットワークで TFTP を設定するには、手動の手順を実行する必要があります。

[クラスタ ビュー（Cluster View）] で、プライマリ プロキシ TFTP サーバとその他の TFTP サーバ間のピア関係をセットアップします。最大 3 台のピア TFTP サーバを追加できます。

プロキシ TFTP 導入環境の各リモート TFTP サーバには、プライマリ プロキシ TFTP サーバとのピア関係が含まれる必要があります。ループの作成を回避するため、リモート クラスタのピア TFTP サーバが互いを指し示していないことを確認します。

手順

ステップ 1 リモート クラスタを作成します。次の操作を実行します。

a) [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] で、[高度な機能（Advanced Features）] > [クラスタ ビュー（Cluster View）]. を選択します。

b) [新規追加（Add New）] をクリックします。[リモート クラスタの設定（Remote Cluster Configuration）] ウィンドウが表示されます。

c) TFTP サーバの最大 50 文字のクラスタ ID と完全修飾ドメイン名（FQDN）を入力し、[保存（Save）] をクリックします。
クラスタ ID の有効な値には、英数字、ピリオド（.）、ハイフン（-）が含まれます。FQDN の有効な値には、英数字、ピリオド（.）、ハイフン（-）、アスタリスク（*）、およびスペースが含まれます。

d) （任意） [リモート クラスタ サービスの設定（Remote Cluster Service Configuration）] ウィンドウで、リモート クラスタの最大 128 文字の説明を入力します。
二重引用符（“）、山カッコ（> <）、バックスラッシュ（\）、ハイフン（-）、アンパサンド（&）、またはパーセント記号（%）は使用しないでください。

ステップ 2 リモート クラスタの TFTP を有効にするには、[TFTP] チェック ボックスをオンにします。

ステップ 3 [TFTP] をクリックします。

ステップ 4 [リモート クラスタ サービスの手動上書き設定（Remote Cluster Service Manually Override Configuration）] ウィンドウで、[リモート サービス アドレスの手動設定（Manually configure remote service addresses）] を選択します。

ステップ 5 これらの TFTP サーバとピア関係を作成するには、TFTP サーバの IP アドレスを入力します。TFTP サーバの IP アドレスは 3 つまで入力できます。

ステップ 6 （任意） プロキシ TFTP サーバがセキュアなクラスタに展開されている場合は、[クラスタは安全です（Cluster is Secure）] チェック ボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

エンドポイントの Trust Verification List（TVL）に、すべてのリモート TFTP サーバを追加する必要があります。追加しないと、エンドポイントがリモート クラスタにあるプロキシ TFTP サーバからの設定ファイルの受け入れが拒否されます。詳細については、お使いのエンドポイント デバイスをサポートするマニュアルを参照してください。

TFTP サーバ ピア関係を追加

プライマリ プロキシ TFTP サーバは、ネットワークで他のプロキシ TFTP サーバとのピア関係を使用して、自身のデータベースで見つからない設定ファイルの場所を探し出します。プライマリ TFTP サーバは、ネットワークのすべての電話やデバイスにこれらのリモート プロキシ TFTP サーバの設定ファイルを提供します。

導入時の各リモート プロキシ TFTP サーバは、プライマリ プロキシ TFTP サーバとピア関係が必要です。クラスタ ビューからピア関係をセットアップします。ループを作成するのを避けるには、リモート クラスタのピア プロキシ TFTP サーバが相互に指さないことを確認します。

手順

ステップ 1 Cisco Unified CM の管理で、[詳細機能（Advanced Features）] > [クラスタ ビュー（Cluster View）] を選択します。

ステップ 2 [Cluster View（クラスタ ビュー）] ウィンドウで、プライマリ プロキシ TFTP サーバのあるクラスタを選択します。

ステップ 3 [リモート クラスタ サービス設定（Remote Cluster Service Configuration）] ウィンドウで、[TFTP] をクリックします。

ステップ 4 [リモート クラスタ サービス設定（Remote Cluster Service Manually Override Configuration）] ウィンドウで、[リモート サービス アドレスを手動で設定（Manually configure remote service addresses）] を選択します。

ステップ 5 これらの TFTP サーバとピア関係を作成するには、TFTP サーバの IP アドレスを入力します。最大 3 つの TFTP サーバの IP アドレスを入力できます。

ステップ 6 （任意） プロキシ TFTP サーバがセキュア クラスタに導入されている場合は [クラスタはセキュア（Cluster is Secure）] チェックボックスをオンにして、[保存（Save）] をクリックします。

次の作業

エンドポイントの Trust Verification Lists（TVL）にリモート プロキシ TFTP サーバを追加する必要があります。そうでない場合、リモート クラスタにあるプロキシ TFTP サーバの設定ファイルを

受け入れません。手順については、エンドポイント デバイスに対応しているマニュアルを参照してください。

TFTP サーバの CTL ファイルの更新

混合モードで動作しているリモート クラスタ内にあるすべての TFTP サーバに対する Cisco 証明書信頼リスト（CTL）ファイルにプライマリ TFTP サーバの IP アドレスを追加する必要があります。これは、セキュリティ対応クラスタのエンドポイントが設定ファイルを正常にダウンロードするために必要です。

プロキシ TFTP サーバに CTL クライアント プラグインをダウンロードしてインストールする必要があります。CTL クライアントは、プロキシ TFTP サーバから CTL ファイルを取得し、セキュリティ トークンを使用して CTL ファイルにデジタル署名を追加して、プロキシ TFTP サーバのファイルを更新します。

（注） セキュリティ トークンなしの CLI はサポートされていません。

セキュリティと Cisco CTL クライアントを使用する方法の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある *Cisco Unified Communications Manager* セキュリティ ガイド を参照してください。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[アプリケーション（Application）] > [プラグイン（Plugins）] を選択して、[プラグインの検索と一覧表示（Find and List Plugins）] ウィンドウで [検索（Find）] をクリックします。
インストールできるすべてのプラグインが一覧表示されます。

ステップ 2 Cisco CTL クライアントの [ダウンロード（Download）] リンクをクリックします。
TFTP サーバにある証明書にデジタル署名するクライアントをインストールします。

ステップ 3 TFTP サーバをリブートします。

TFTP サーバの非設定ファイルの変更

エンドポイントがプロキシ TFTP サーバから要求する、ロード ファイルや RingList.xml などの非設定ファイルを健康できます。この手順を完了すると、変更したファイルをプロキシ TFTP サーバの TFTP ディレクトリにアップロードします。

手順

ステップ 1 Cisco Unified Communications Operating System Administration で、[ソフトウェア アップグレード（Software Upgrades）] > [TFTP ファイル管理（TFTP File Management）] を選択します。
[TFTP ファイル管理（TFTP File Management）] ウィンドウが表示されます。

ステップ 2 [ファイルのアップロード（Upload File）] をクリックします。
[ファイルのアップロード（Upload File）] ポップアップが表示されます。

ステップ 3 次のいずれかの操作を実行します。

- アップロードするファイルのディレクトリの場所を参照するには、[参照（Browse）]をクリックしてください。
- [ディレクトリ（Directory）] フィールドに更新されるファイルの完全なディレクトリ パスを貼り付けます。

ステップ 4 [ファイルのアップロード（Upload File）]をクリックするか、ファイルをアップロードせずに終了するには、[閉じる（Close）] をクリックします。

次の作業

Cisco Unified Serviceability 管理を使用して、プロキシ TFTP ノード上の Cisco TFTP サービスを停止するか、または再起動します。

関連トピック

TFTP サービスの停止および開始, （598 ページ）

TFTP サービスの停止および開始

プロキシ TFTP ノードで TFTP サービスを停止および再起動するには、次の手順を使用します。

サービスの有効化、無効化、および再起動についての詳細は、『*Cisco Unified Serviceability Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

手順

ステップ 1 Cisco Unified Serviceability で、[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。

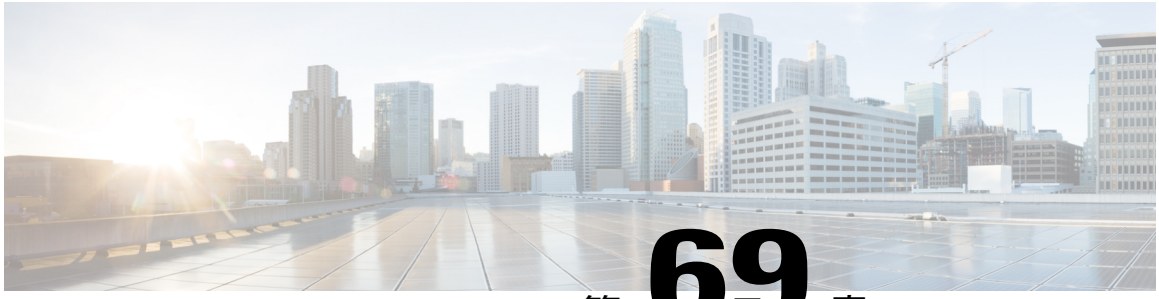
ステップ 2 [コントロール センター - 機能サービス（Control Center - Feature Services）] ウィンドウで、[サーバ（Server）] ドロップダウン リストからプロキシ TFTP ノードを選択します。

ステップ 3 [CM サービス（CM Services）] 領域で TFTP サービスを選択し、[停止（Stop）] をクリックします。

ステータスが変化し、更新されたステータスが反映されます。

ヒント サービスの最新ステータスを表示するには、[更新（Refresh）] をクリックします。

ステップ 4 [CM サービス（CM Services）] 領域で TFTP サービスを選択し、[開始（Start）] をクリックします。
ステータスが変化し、更新されたステータスが反映されます。



第 69 章

デバイスのデフォルトの更新

- デバイスのデフォルトの概要，601 ページ
- デバイスのデフォルトの更新タスク フロー，601 ページ

デバイスのデフォルトの概要

Cisco Unified Communications Manager ノードに登録されている各デバイスには、そのタイプのデバイスのデフォルトが設定されています。デバイスのデフォルトは、クラスタ内のすべての自動登録デバイスに適用されます。登録後に、デバイスの設定を変更できます。

新しいデバイスのデフォルトを作成したり、既存のデフォルトを削除したりすることはできませんが、自動登録されるデバイスに適用されるデフォルト設定を変更することはできます。

変更できるデバイスのデフォルト設定は、次のとおりです。

- デバイスの負荷（Device Load）
- デバイス プール（Device Pool）
- 電話ボタン テンプレート（Phone button template）

Cisco Unified Communications Manager をインストールすると、デバイスのデフォルトが自動的に設定されます。

デバイスのデフォルトの更新タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスのデフォルト設定の更新，（602 ページ）	Cisco Unified Communications Manager ノードに自動登録するデバイスに適用されるデフォルト設定

	コマンドまたはアクション	目的
		を変更できます。デバイスのタイプごとに固有のデフォルト設定があります。

デバイスのデフォルト設定の更新

はじめる前に

デバイスのデフォルト設定を更新する前に、システムに適用する次のタスクを実行します。

- TFTP サーバにデバイスの新しいファームウェア ファイルを追加します。
- デバイスのデフォルトを使用して、ディレクトリに存在しないファームウェア ロードを割り当てると、それらのデバイスは割り当てられたファームウェアをロードできません。
- 新しいデバイスプールを設定します。デバイスが電話の場合は、新しい電話テンプレートを設定します。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）] を選択します。

ステップ 2 [デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウで、更新するデバイス タイプに適用可能な設定を変更し、[保存（Save）]をクリックします。フィールドの説明については、オンライン ヘルプを参照してください。

- ロード情報（Load Information）
- [デバイスプール（Device Pool）]
- 電話機テンプレート

ステップ 3 そのタイプのすべてのデバイスをリセットして、クラスタ内の全ノードにある該当するタイプのすべてのデバイスに新しいデフォルトをロードするには、デバイス名の左側にある [リセット（Reset）] アイコンをクリックします。
すべてのデバイスをリセットしない場合は、ノードに自動登録された新しいデバイスにだけ、更新されたデフォルト値が設定されます。

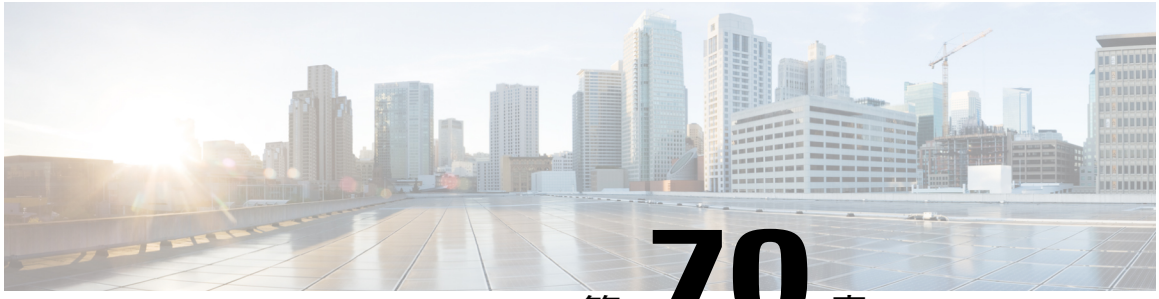
関連トピック

基本的なデバイス プールの設定, （56 ページ）
デバイス プロファイルとテンプレートの設定タスク フロー, （432 ページ）

デバイスのデフォルト設定

表 *75*：デバイスのデフォルト設定

フィールド名	説明
デバイスタイプ（Device Type）	このフィールドには、デフォルトを適用するデバイス タイプが表示されます。
プロトコル	このフィールドには、このデバイス タイプで使用されるプロトコルが表示されます。
ロード情報（Load Information）	ハードウェアデバイスの特定のタイプで使用されるファームウェア ロードの ID 番号を入力します。アップグレードまたはパッチ ロードをインストールする場合は、新しいロードを使用するデバイス タイプごとにロード情報を更新する必要があります。
[デバイスプール（Device Pool）]	各デバイス タイプに関連付けるデバイス プールを選択します。デバイス プールは、プール内の全デバイスに共通する特性を定義します。
電話機テンプレート	Cisco Unified IP Phone の各タイプが使用する電話ボタン テンプレートを選択します。テンプレートは、電話のキーの機能を定義します。



第 70 章

自動登録の設定

- 自動登録の概要，605 ページ
- 自動登録の設定タスク フロー，606 ページ

自動登録の概要

自動登録によって、新しい電話がネットワークにプラグインされたときに、Cisco Unified Communications Manager によりそれらの電話に自動で電話番号を割り当てることができます。

現在、自動登録はセキュア モードで有効になっています。この拡張機能によって、新しい電話のプロビジョニング中にクラスタを保護できるため、システムのセキュリティが強化されます。また、新しい電話を登録する際にクラスタ セキュリティを無効にする必要がないため、登録プロセスが簡素化されるメリットもあります。

911（緊急）および0（オペレータ）コールのみを許可するデバイスプールを作成しておくと、自動登録が有効になっている場合に許可されていないエンドポイントがネットワークに接続するのを防ぐために使用できます。新しいエンドポイントはこのプールに登録できますが、アクセスは制限されます。連続して起動しネットワークへの登録を試みる不正なデバイスによる不正アクセスは阻止されます。電話番号に影響を与えることなく、自動登録された電話を新しい場所に移動し、別のデバイス プールに割り当てることができます。

システムは、自動登録している新しい電話が SIP または SCCP を実行しているかどうかを認識しません。自動登録を有効にしている場合は、実行している方を指定する必要があります。SIP と SCCP の両方をサポートするデバイス（Cisco Unified IP Phone 7911、7940、7941、7960、7961、7970、7971 など）は、Auto Registration Phone Protocol と呼ばれるエンタープライズ パラメータで指定されたプロトコルとともに自動登録されます。

単一のプロトコルのみサポートするデバイスは、そのプロトコルとともに自動登録されます。Auto Registration Phone Protocol 設定は無視されます。たとえば、SCCP のみをサポートする Cisco Unified IP Phone は、Auto Registration Phone Protocol パラメータが SIP に設定されている場合でも SCCP とともに自動登録されます。

自動登録は、ネットワークに追加する電話が100台未満の場合に使用することを推奨します。100台を超える電話を追加するには、一括管理ツール（BAT）を使用します。詳細については、『*Cisco*

Unified Communications Manager Bulk Administration ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

自動登録の設定タスク フロー

自動登録を有効にすると、セキュリティ リスクが生まれます。ネットワークに新しいエンドポイントを追加するときに、短時間だけ自動登録を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	自動登録用パーティションの設定，（607 ページ）	自動登録電話を内線専用に制限するには、自動登録専用のルート パーティションを設定します。
ステップ 2	自動登録用コーリング サーチ スペースの設定，（608 ページ）	自動登録電話を内線専用に制限するには、自動登録専用のコーリング サーチ スペースを設定します。
ステップ 3	自動登録のデバイス プールの設定，（609 ページ）	自動登録用に設定したコーリング サーチ スペースを使用するデバイス プールを作成します。
ステップ 4	自動登録のデバイス プロトコル タイプの設定，（610 ページ）	自動登録している電話機のタイプを SCCP または SIP プロトコルに合わせて設定するには、次の手順を使用します。
ステップ 5	自動登録を有効にする，（610 ページ）	自動登録で使用する Cisco Unified Communications Manager グループに対して自動登録を有効にするには、自動登録用ノードで自動登録を有効にして、[自動登録 Cisco Unified Communications Manager グループ（Auto-registration Cisco Unified Communications Manager Group）] パラメータを設定します。
ステップ 6	自動登録の無効化，（613 ページ）	新しいデバイスの登録が完了したらすぐに、ノードで自動登録を無効にします。
ステップ 7	再利用の自動登録の数，（613 ページ）	これはオプションです。無効になった、デバイスの自動登録番号は再利用できます。自動登録用の電話番号の範囲をリセットするとき、最初の番号から再度検索をシステムで実行します。使用可能な電話番号は再利用されます。

自動登録用パーティションの設定

自動登録電話を内線専用に制限するには、自動登録専用のルート パーティションを設定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックして新しいパーティションを作成します。

ステップ 3 [パーティション名、説明（Partition Name, Description）] フィールドに、ルート プランに固有のパーティション名を入力します。
パーティション名には、英数字とスペースの他にハイフン（-）とアンダースコア（_）を使用できます。パーティション名に関するガイドラインについては、オンライン ヘルプを参照してください。

ステップ 4 パーティション名の後にカンマ（,）を入力し、パーティションの説明を同じ行に入力します。
説明には、任意の言語で最大50文字を使用できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）、角括弧（[]）は使用できません。説明を入力しなかった場合は、Cisco Unified Communications Manager が、このフィールドに自動的にパーティション名を入力します。

ステップ 5 複数のパーティションを作成するには、各パーティション エントリごとに 1 行を使います。

ステップ 6 [スケジュール（Time Schedule）] ドロップダウン リストから、このパーティションに関連付けるスケジュールを選択します。
スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）] を選択した場合は、パーティションが常にアクティブになります。

ステップ 7 次のオプション ボタンのいずれかを選択して、[タイム ゾーン（Time Zone）] を設定します。

- [発信側デバイス（Originating Device）]：このオプション ボタンを選択すると、発信側デバイスのタイムゾーンと [スケジュール（Time Schedule）] が比較され、パーティションが着信コールの受信に使用できるかどうかが判断されます。
- [特定のタイム ゾーン（Specific Time Zone）]：このオプション ボタンを選択した後、ドロップダウン リストからタイム ゾーンを選択します。選択されたタイム ゾーンと [スケジュール（Time Schedule）] が比較され、着信コールの受信にパーティションが使用できるかどうかが判断されます。

ステップ 8 [保存（Save）] をクリックします。

次の作業

自動登録用コーリング サーチ スペースの設定, （608 ページ）

自動登録用コーリング サーチ スペースの設定

自動登録電話機を内線通話のみに制限するには、コーリング サーチ スペースを自動登録専用に設定します。

はじめる前に

自動登録用パーティションの設定, （607 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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 [名前（Name）] フィールドに、名前を入力します。
各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

ステップ 4 [説明（Description）] フィールドに、説明を入力します
説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 [使用可能なパーティション（Available Partitions）] ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。
- パーティションが複数ある場合は、コントロール（Ctrl）キーを押したまま、適切なパーティションを選択します。

ステップ 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）] フィールドにパーティションを移動させます。

ステップ 7 （任意） [選択されたパーティション（Selected Partitions）] ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

自動登録のデバイス プールの設定, （609 ページ）

関連トピック

サービス クラス, （131 ページ）

自動登録のデバイス プールの設定

SCCP および SIP デバイスで自動登録を使用できるように、自動登録用デフォルト デバイス プールを使用するか、または別のデバイス プールを設定できます。

自動登録用デフォルト デバイス プールを設定するには、デフォルトの Cisco Unified Communications Manager グループと自動登録のコーリング サーチ スペース（CSS）をデフォルト デバイス プールを割り当てます。SCCP および SIP デバイス用の個別のデフォルト デバイス プールを設定する場合は、デバイス プールのデフォルト値を使用します。

はじめる前に

自動登録用コーリング サーチ スペースの設定, （608 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [デバイス プール（Device Pool）] を選択します。

ステップ 2 自動登録用デフォルト デバイス プールを変更するには、次の操作を実行します。

a) [検索（Find）] をクリックし、デバイス プールのリストから [デフォルト（Default）] を選択します。

b) [デバイス プールの設定（Device Pool Configuration）] ウィンドウで、[自動登録用コーリング サーチ スペース（Calling Search Space for Auto-registration）] フィールドで、自動登録に使用する CSS を選択し、[保存（Save）] をクリックします。

ステップ 3 自動登録用の新しいデバイス プールを作成するには、次の操作を実行します。

a) [新規追加（Add New）] をクリックします。

b) [デバイス プールの設定（Device Pool Configuration）] ウィンドウで、デバイス プールの一意の名前を入力します。
英数字、ピリオド（.）、ハイフン（-）、アンダースコア（_）、スペースを含む、最大 50 文字を入力できます。

c) デフォルトのデバイス プールに一致するように、次のフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

- [Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）] で、[デフォルト（Default）] を選択します。
- [日時グループ（Date/Time Group）] で、[CMLocal（CMLocal）] を選択します。
- [リージョン（Region）] で、[デフォルト（Default）] を選択します。

d) [自動登録用コーリング サーチ スペース（Calling Search Space for Auto-registration）] フィールドで自動登録に使用する CSS を選択し、[保存（Save）] をクリックします。

次の作業

自動登録のデバイス プロトコル タイプの設定, （610 ページ）

自動登録のデバイス プロトコル タイプの設定

SIP および SCCP デバイスを自動登録するには、まず、自動登録電話プロトコル パラメータを SCCP に設定し、SCCP を実行しているすべてのデバイスをインストールする必要があります。その後、自動登録電話プロトコル パラメータを SIP に変更して、SIP を実行しているすべてのデバイスを自動登録します。

はじめる前に

自動登録のデバイス プールの設定, （609 ページ）

手順

ステップ 1 Cisco Unified Communications Manager の管理で、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] の順に選択します。

ステップ 2 [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウで、[自動登録電話プロトコル（Auto Registration Phone Protocol）] ドロップダウン リストから [SCCP（SCCP）] または [SIP（SIP）] のいずれかを選択し、[保存（Save）] をクリックします。

次の作業

自動登録を有効にする, （610 ページ）

自動登録を有効にする

自動登録が有効の場合は、ネットワークに接続する際に新しいエンドポイントに割り当てられる電話番号の範囲を指定する必要があります。新しいエンドポイントが接続される度に、次の使用可能な電話番号が割り当てられます。自動登録に使用できる電話番号がなくなった場合、エンドポイントを自動登録することはできません。

新しいエンドポイントは、[自動登録 Cisco Unified CM グループ（Auto-Registration Cisco Unified Communications Manager Group）] 設定が有効になっているグループの最初の [Cisco Unified Communications Manager] ノードを使用して自動登録されます。その後、デバイス タイプに基づき、自動登録された各エンドポイントがデフォルトのデバイス プールに自動で割り当てられます。

はじめる前に

自動登録のデバイス プロトコル タイプの設定, （610 ページ）

- デバイス プール、コーリング サーチ スペース、および内線発信のみ許可するように自動登録するデバイスのアクセスを制限するルート パーティションを作成します。

- 電話番号が自動登録範囲で利用できることを確認します。
- 新しい電話を登録するために利用できるライセンス ポイントが十分にあることを確認します。
- [デバイスのデフォルト設定（Device Defaults Configuration）] ウィンドウに、SIP および SCCP の電話イメージ名が正しく表示されていることを確認します。共通デバイス設定ファイルのほとんどは TFTP サーバ上で利用できますが、デバイスの設定ファイルが存在することを確認します。
- Cisco Proxy の TFTP サーバが起動して実行中であることと、TFTP の DHCP オプションで適切なサーバが指定されていることを確認します。

手順

ステップ 1 [Cisco Unified Communications Manager Administration] で、[システム（System）] > [Cisco Unified CM] を選択し、[Find and List Cisco Unified Communications Managers] ウィンドウの [検索（Find）] をクリックします。

ステップ 2 自動登録を使用するには、クラスタの [Cisco Unified Communications Manager] を選択します。
が表示されます。

ステップ 3 [Cisco Unified CM Configuration（Cisco Unified CM Configuration）] ウィンドウで、[自動登録情報（Auto-registration Information）]セクションのノードの自動登録パラメータを設定し、[保存（Save）] をクリックします。フィールドの説明については、オンライン ヘルプを参照してください。

a) ユニバーサル デバイス テンプレートを選択して、ドロップダウン リストから自動登録を使用します。
自動登録用に作成されているユニバーサル デバイス テンプレートがない場合は、[デフォルトのユニバーサル デバイス テンプレート（Default Universal Device Template）] を選択します。選択したテンプレートで、デバイス プールが指定されていることを確認します。これは、[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル デバイス テンプレート（Universal Device Template）] の自動登録で使用されます。

b) ドロップダウン リストからの自動登録に使用するユニバーサル ライン テンプレートを選択します。
自動登録用に作成されているユニバーサル ライン テンプレートがない場合は、[デフォルトのユニバーサル ライン テンプレート（Default Universal Line Template）] を選択します。選択したテンプレートで、コーリング サーチ スペースおよびルート パーティションが指定されていることを確認します。これは、[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル ライン テンプレート（Universal Line Template）] の自動登録で使用されます。

c) 電話番号の最初と最後を [開始電話番号（Starting Directory Number）] および [終了電話番号（Ending Directory Number）] フィールドに入力します。
電話番号の最初と最後を同じ値に設定すると、自動登録は無効になります。

d) [このCisco Unified CM では自動登録は無効にする（Auto-registration Disabled on this Cisco Unified Communications Manager）] のチェックボックスをオフにして、このノードの自動登録を有効にします。

選択した Cisco Unified Communications Manager ノードでのみ自動登録を常に有効または無効にします。 自動登録機能をクラスタ内の他のノードに切り替える場合は、Cisco Unified Communications Manager ノード、デフォルトの Cisco Unified Communications Manager グループ、デフォルトのデバイス プールを再設定する必要があります。

ステップ 4 [システム（System）] > [Cisco Unified CM Group]を選択し、[Cisco Unified CMグループの検索と一覧表示（Find and List Cisco Unified Communications Manager Groups）] ウィンドウの [検索（Find）] をクリックします。

ステップ 5 Cisco Unified Communications Manager グループを選択して、自動登録を有効にします。
このグループ名は、ほとんどの場合 [デフォルト（Default）] になります。別の Cisco Unified Communications Manager グループを選択することもできます。このグループでは、最低 1 つのノードを選択する必要があります。

ステップ 6 このグループの [Cisco Unified CM Group Configuration] ウィンドウにおいて、 [自動登録（Auto-registration）] [Cisco Unified Communications Manager][グループ（Group）] を選択して、グループの自動登録を有効にし、[保存（Save）] をクリックします。

ヒント [選択済 Cisco Unified CM（Selected Cisco Unified Communications Managers）] のリストに、自動登録用に設定したノードが含まれていることを確認します。矢印を使用して、リストに表示するノードを移動します。表示されている順で、Cisco Unified Communications Manager ノードが選択されます。変更を [保存（Save）] します。

ステップ 7 自動登録するデバイスをインストールします。

（注） 自動登録された電話を再設定し、その電話を永続的なデバイス プールに割り当てます。電話のロケーションを変更しても、電話に割り当てられている電話番号は変更されません。

（注） 別の種類の電話を登録するには、デバイスのプロトコル タイプを変更し、そのデバイスを取り付けてから自動登録を無効にします。

次の作業

新しい電話の登録が完了したら、自動登録の無効化, （613 ページ）。

関連トピック

自動登録のデバイス プロトコル タイプの設定, （610 ページ）
自動登録の無効化, （613 ページ）
ユニバーサル デバイス テンプレートの設定, （283 ページ）
ユニバーサル回線テンプレートの設定, （282 ページ）
TFTP サーバの設定タスク フロー, （593 ページ）

自動登録の無効化

新しいデバイスの登録が完了したらすぐに、ノードの自動登録を無効にします。

はじめる前に

自動登録を有効にする，（610 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[システム（System）] > [Cisco Unified CM]を選択し、[Cisco Unified CM グループの検索と一覧表示（Find and List Cisco Unified Communications Manager Groups）] ウィンドウの [検索（Find）] をクリックします。

ステップ 2 ノードのリストから、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] を選択します。

ステップ 3 選択したノードの [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] ウィンドウで、[このCisco Unified CM では自動登録は無効にする（Auto-registration Disabled on this Cisco Unified Communications Manager）] チェックボックスをオンにし、このノードの自動登録を無効にします。その後、[保存（Save）] をクリックします。

ヒント [開始電話番号(Starting Directory Number)] フィールドと [終了電話番号(Ending Directory Number)] フィールドに同一値を設定して、自動登録を無効にすることもできます。

次の作業

これはオプションです。自動登録済みデバイスの電話番号を手動変更したか、そのデバイスをデータベースから削除した場合は、該当する電話番号を再利用できます。詳細は、再利用の自動登録の数，（613 ページ）を参照してください。

再利用の自動登録の数

ネットワークに新しいデバイスを接続すると、システムはそのデバイスに利用可能な次の自動登録ディレクトリ番号を割り当てます。手動で自動登録済みデバイスのディレクトリ番号を変更するか、データベースからそのデバイスを削除すると、そのデバイスの自動登録ディレクトリ番号は再利用できます。

デバイスが自動登録を試みると、システムは指定した自動登録番号の範囲を検索し、そのデバイスに割り当てるための、次に使用可能なディレクトリ番号を検索します。割り当てられた最後の番号の後、次のディレクトリ番号から順に検索を開始します。範囲内の最後のディレクトリ番号に達すると、システムは範囲の開始ディレクトリ番号から検索し続けます。

自動登録のディレクトリ番号の範囲をリセットし、システムがその範囲の開始番号から検索するようにすることができます。

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [シスコ統合コミュニケーション マネージャ（Cisco Unified Communications Manager）] を選択します。

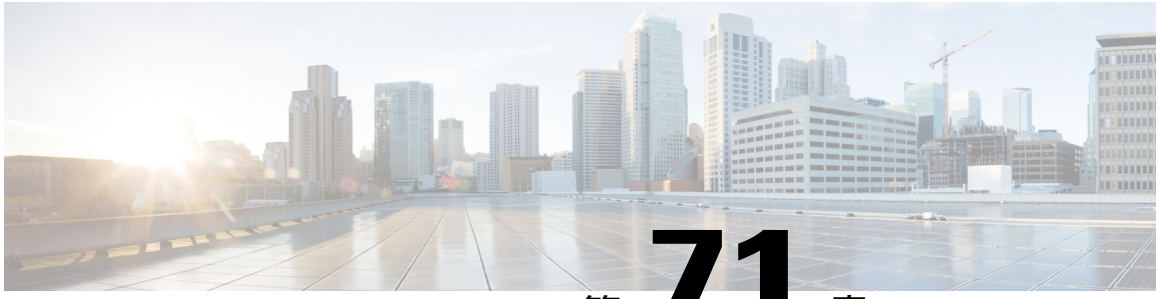
ステップ 2 自動登録をリセットするには、[シスコ統合コミュニケーション マネージャ（Cisco Unified Communications Manager）] を選択します。

ステップ 3 現在の設定を [開始のディレクトリ番号（Starting Directory Number）] と [最後のディレクトリ番号（Ending Directory Number）] フィールドに書き留めます。

ステップ 4 [この Cisco Unified Communications Manager で自動登録を無効化（Auto-registration Disabled on this Cisco Unified Communications Manager）] をクリックしてから、[保存（Save）] をクリックします。自動登録が無効の間、新しい電話は自動登録できません。

ステップ 5 [開始ディレクトリ番号（Starting Directory Number）] と [最後のディレクトリ番号（Ending Directory Number）] フィールドを以前の値に設定してから、[保存（Save）] をクリックします。

ヒント フィールドに新しい値を設定できます。



第 71 章

電話機の手動登録

- 電話の手動登録の概要，615 ページ
- 手動によるデバイス登録タスク フロー，615 ページ

電話の手動登録の概要

新しい Cisco IP Phone を手動で登録するには、Cisco Unified Communications Manager の管理 を使用して、Cisco Unified Communications Manager に電話を追加してから、電話の電話番号を設定する必要があります。

新しい電話が Cisco Unified Communications Manager ノードを見つける方法を認識できるように、事前にプロキシ TFTP サーバの IP アドレスを新しい電話に設定しておく必要があります。手順については、エンドポイント デバイスをサポートするドキュメントを参照してください。

関連トピック

プロキシ TFTP 導入の概要，（591 ページ）

手動によるデバイス登録タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	エンドポイント デバイスに対応するマニュアルを参照してください。	新しい電話に Cisco Unified Communications Manager ノードの特定方法が分かるように、プロキシ TFTP サーバ IP アドレスに新しい電話を設定します。
ステップ 2	システムへの電話機の手動での追加，（616 ページ）	Cisco Unified Communications Manager ノードに電話を追加します。

	コマンドまたはアクション	目的
ステップ 3	電話機に対する電話番号の手動設定, （616 ページ）	電話機の電話番号を追加し、電話番号のある基本設定を行います。

システムへの電話機の手動での追加

新しい電話機を手動で Cisco Unified Communications Manager ノードに追加します。

手順

ステップ 1 Cisco Unified Communications Manager の管理で、[デバイス（Device）] > [電話（Phone）] の順に選択し、[新規追加（Add New）] をクリックします。

ステップ 2 [新しい電話機の追加（Add a New Phone）] ウィンドウで、[電話のタイプ（Phone Type）] フィールドの電話モデルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [電話の設定（Phone Configuration）] ウィンドウで、[デバイス プロトコルの選択（Select the device protocol）] フィールドからデバイスのプロトコル タイプを選択し、[次へ（Next）] をクリックします。

ステップ 4 [デバイス情報（Device Information）] 領域で、次の操作を実行します。

a) [デバイス名（Device Name）] フィールドに名前を入力します。
ここに入力する名前は、電話機で設定したデバイス名と同じにする必要があります。詳細については、エンドポイント デバイスに対応するドキュメントを参照してください。

b) デバイス プールのリストから電話機のデバイス プールを選択します。

c) 電話ボタン テンプレートのリストから、使用する電話ボタン テンプレートを選択します。

ステップ 5 [プロトコル固有情報（Protocol Specific Information）] 領域で、[デバイスのセキュリティ プロファイル（Device Security Profile）] フィールドから電話機のタイプの非セキュア プロファイルを選択します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

電話機に対する電話番号の手動設定, （616 ページ）

電話機に対する電話番号の手動設定

Cisco Unified Communications Manager Administration を使用して、電話番号（DN）を手動で追加し、設定するには複数の方法があります。

- [コール ルーティング（Call Routing）] > [電話番号（Directory Number）] を使用して表示された、[電話番号の設定（Directory Number Configuration）] ウィンドウから設定。
- [デバイス（Device）] > [電話（Phone）] を使用して表示された、[電話の設定（Phone Configuration）] ウィンドウから、[割り当て情報（Association Information）] 領域で、[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] または [回線 [2] - 新規 DN を追加（Line [2] - Add a new DN）] リンクを選択して設定。
- 電話機をコール ルーティングに追加した後で、[コール ルーティング（Call Routing）] > [電話（Phone）] を使用して表示された、[電話の設定（Phone Configuration）] ウィンドウから設定。
- [デバイス（Device）] > [CTI ルート ポイント（CTI Route Point）] を使用して表示された[CTI ルート ポイントの設定（CTI Route Point Configuration）] ウィンドウから設定。

新しい電話を Cisco Unified Communications Manager ノードに追加した後に、表示された [電話の設定（Phone Configuration）] ウィンドウを使用して新しい電話の DN を設定していることをこの手順では前提にしています。

このメソッドを使用して、電話機モデルに適用した設定のみが表示されます。

ヒント　電話に新しい DN を追加すると同時に、電話機能を設定できます。使用可能なすべての DN の設定を表示するには、ユーザ インターフェイスのコール ルーティングから [電話番号の設定（Directory Number Configuration）]ウィンドウにアクセスする必要があります。

はじめる前に

電話機をノードに追加します。登録している新しい電話機に対する [電話の設定（Phone Configuration）] ウィンドウを表示したままにします。

システムでパーティションを使用する場合、ルート パーティションとコーリング サーチ スペースを特定し、新しい電話に対して使用します。

手順

ステップ 1　[電話の設定（Phone Configuration）] ウィンドウの [関連付け（Association）]領域で [回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] をクリックします。

ヒント　[電話の設定（Phone Configuration）] ウィンドウが表示されていない場合は、[デバイス（Device）] > [電話（Phone）] を選択し、[検索（Find）] をクリックしてから、電話機のリストから電話を選択します。

ステップ 2 [電話番号の設定（Directory Number Configuration）] ウィンドウで、[電話番号（Directory Number）] フィールドにダイヤル可能な電話番号を入力します。

ステップ 3 （任意） [ルート パーティション（Route Partition）] フィールドでパーティションを選択します。

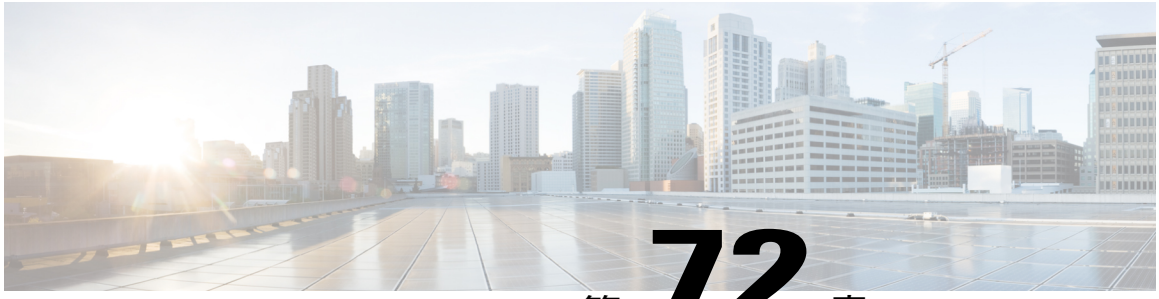
ステップ 4 （任意） [電話番号の設定（Directory Number Settings）]エリアの [コーリング サーチ スペース（Calling Search Space）] フィールドでコーリング サーチ スペースを選択します。

ステップ 5 （任意） 新しい電話機に適用できる他の電話番号機能を設定し、[保存（Save）] をクリックします。

たとえば、すでに新しい電話のユーザ名を知っている場合は、[表示（発信者 ID）（Display (Caller ID)）] フィールドにその名前を入力できます。フィールドの説明については、オンライン ヘルプを参照してください。

関連トピック

サービス クラス, （131 ページ）



第 72 章

セルフプロビジョニングの設定

- セルフプロビジョニングの概要，619 ページ
- セルフプロビジョニングの前提条件，620 ページ
- セルフプロビジョニングの設定タスク フロー，621 ページ

セルフプロビジョニングの概要

セルフプロビジョニング機能により、エンドユーザが管理者に連絡せずに自社の電話機をプロビジョニングできるようにすることで、電話機を自社のネットワークにプロビジョニングします。システムがセルフプロビジョニング用に設定されていて、個々のエンドユーザがセルフプロビジョニング可能になっていると、そのエンドユーザは電話機をネットワークに接続していくつかの指示に従うことにより、新しい電話をプロビジョニングできます。Cisco Unified Communications Manager は、事前に設定されたテンプレートを適用して、電話回線および電話を設定します。

セルフプロビジョニングは、管理者がエンドユーザに代わって電話のプロビジョニングに使用するか、またはエンドユーザがセルフプロビジョニングを使って自社の電話機のプロビジョニングを行うかの、いずれにも使用できます。

クラスタのセキュリティ設定が非セキュアでも、混合モードでも、セルフプロビジョニングはサポートされています。

セキュリティ モード

次の 2 つのモードのいずれかで、セルフプロビジョニングを設定できます。

- セキュア モード—セキュア モードでは、ユーザまたは管理者は、セルフプロビジョニングにアクセスするためには認証されている必要があります。エンドユーザは、自分のパスワードまたは PIN に対して認証されることができます。管理者は、事前設定された認証コードを入力できます。
- 非セキュア モード—非セキュア モードでは、ユーザまたは管理者は、自分のユーザ ID、またはセルフプロビジョニング ID を入力して電話とユーザ アカウントを関連付けることができます。非セキュア モードは日々の使用には推奨されません。

ユニバーサル回線とデバイス テンプレートによる設定

セルフプロビジョニングでは、エンドユーザにプロビジョニングされた電話および電話回線を設定するために、ユニバーサル回線テンプレートとユニバーサルデバイステンプレートの設定を使用します。ユーザが自分の電話をプロビジョニングすると、システムはそのユーザのユーザ プロファイルを参照し、関連付けられているユニバーサル回線のテンプレートをプロビジョニングされた電話回線に、ユニバーサルデバイステンプレートをプロビジョンされた電話に適用します。

セルフプロビジョニング電話

機能が設定されると、次の操作を実行して電話をプロビジョニングできます。

- 電話をネットワークに接続します。
- セルフプロビジョニング IVR 内線番号をダイヤルします。
- 指示に従って電話を設定し、エンドユーザに電話を関連付けます。セルフプロビジョニングをどのように設定したかによって、エンドユーザはユーザ パスワード、暗証番号、PIN、または管理用の認証コードを入力します。

ヒント エンドユーザに代わって多数の電話をプロビジョニングしている場合、セルフプロビジョニング IVR 拡張に転送するユニバーサル デバイス テンプレートに短縮ダイヤルを設定します。

セルフプロビジョニングの前提条件

セルフプロビジョニングを使用するためには、エンドユーザは次の項目を設定します。

- エンドユーザには、プライマリ内線番号が必要です。
- エンドユーザは、ユニバーサル回線のテンプレート、ユニバーサル デバイス テンプレートを含む、ユーザ プロファイルまたは機能グループ テンプレートに関連付けられる必要があります。ユーザ プロファイルは、セルフプロビジョニング用に有効にする必要があります。詳細は、ユーザ プロファイルの設定タスク フロー, （282 ページ）を参照してください。

関連トピック

エンド ユーザの設定, （251 ページ）

セルフプロビジョニングの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	セルフプロビジョニングのサービスの有効化, （621 ページ）	Cisco Unified Serviceability で、[セルフプロビジョニング IVR（Self-Provisioning IVR）] サービスと [CTI Manager（CTI Manager）] サービスを有効にします。
ステップ 2	セルフプロビジョニング用自動登録の有効化, （622 ページ）	セルフプロビジョニングの自動登録パラメータを有効にします。
ステップ 3	CTI ルート ポイントの設定, （623 ページ）	セルフプロビジョニング IVR サービスを処理するように CTI ルート ポイントを設定します。
ステップ 4	CTI ルート ポイントへの電話番号の割り当て, （623 ページ）	ユーザがセルフプロビジョニング IVR にアクセスする場合にダイヤルする内線番号を設定し、その内線番号を CTI ルート ポイントに関連付けます。
ステップ 5	セルフプロビジョニング用アプリケーション ユーザの設定, （624 ページ）	セルフプロビジョニング IVR のアプリケーション ユーザを設定します。CTI ルート ポイントをアプリケーション ユーザに関連付けます。
ステップ 6	システムのセルフプロビジョニング設定, （625 ページ）	アプリケーション ユーザや CTI ルート ポイントをセルフプロビジョニング IVR に関連付けるなど、システムのセルフプロビジョニング設定を実行します。

セルフプロビジョニングのサービスの有効化

セルフプロビジョニング機能をサポートするサービスをアクティブにするには、次の手順を使用します。セルフプロビジョニング IVR および Cisco CTI Manager サービスの両方が実行されている必要があります。

手順

ステップ 1 Cisco Unified Serviceability から、[ツール（Tools）] > [サービスの有効化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リスト ボックスからパブリッシャ ノードを選択し、[移動（Go）] をクリックします。

ステップ 3 [CM サービス（CM Services）] で、[Cisco CTI Manager] をオンにします。

ステップ 4 [CTI サービス（CTI Services）] で、[Self Provisioning IVR] をオンにします。

ステップ 5 [保存（Save）] をクリックします。

次の作業

セルフプロビジョニング用自動登録の有効化, （622 ページ）

セルフプロビジョニング用自動登録の有効化

セルフプロビジョニングを使用するには、パブリッシャで自動登録パラメータを設定する必要があります。

はじめる前に

セルフプロビジョニングのサービスの有効化, （621 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[システム（System）] > [Cisco Unified CM（Cisco Unified CM）] を選択します。

ステップ 2 パブリッシャ ノードをクリックします。

ステップ 3 プロビジョニングされる電話機に適用する [ユニバーサルデバイス テンプレート（Universal Device Template）] を選択します。

ステップ 4 プロビジョニングされる電話機の電話回線に適用する [ユニバーサル回線テンプレート（Universal Line Template）] を選択します。

ステップ 5 [開始電話番号（Starting Directory Number）] と [終了電話番号（Ending Directory Number）] フィールドにプロビジョニングする電話に適用する電話番号の範囲を入力します。

ステップ 6 [この Cisco Unified CM では自動登録は無効にする（Auto-registration Disabled on the Cisco Unified Communications Manager）] チェックボックスをオフにします。

ステップ 7 [保存（Save）] をクリックします。

次の作業

CTI ルート ポイントの設定, （623 ページ）

CTI ルート ポイントの設定

セルフプロビジョニング IVR 向けの CTI ルート ポイントを設定する必要があります。

はじめる前に

セルフプロビジョニング用自動登録の有効化, （622 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [CTI ルート ポイント（CTI Route Point）] を選択します。

ステップ 2 次のいずれかの手順を実行します。

a) [検索（Find）] をクリックし、既存の CTI ルート ポイントを選択します。

b) [新規追加（Add New）] をクリックして、新しい CTI ルート ポイントを作成します。

ステップ 3 [デバイス名（Device Name）] フィールドに、ルート ポイントを識別する一意の名前を入力します。

ステップ 4 [デバイス プール（Device Pool）] ドロップダウン リストボックスから、このデバイスにプロパティを指定するデバイス プールを選択します。

ステップ 5 [ロケーション（Location）] ドロップダウン リスト ボックスから、この CTI ルート ポイントに適切な場所を選択します。

ステップ 6 [トラステッド リレー ポイントを使用（Use Trusted Relay Point）] ドロップダウン リスト ボックスで、Cisco Unified Communications Manager がこのメディア エンドポイントにトラステッド リレー ポイント（TRP）デバイスを挿入するかどうかを選択します。デフォルト設定はこのデバイスに関連付けられた共通デバイス設定を使用します。

ステップ 7 [CTI ルート ポイントの設定（CTI Route Point Configuration）] ウィンドウでその他のフィールドに入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 8 [保存（Save）] をクリックします。

次の作業

CTI ルート ポイントへの電話番号の割り当て, （623 ページ）

CTI ルート ポイントへの電話番号の割り当て

セルフプロビジョニング IVR の利用のためにユーザがダイヤルする内線番号を設定するには、次の手順を使用します。その内線番号をセルフプロビジョニングに使用する CTI ルート ポイントに関連付ける必要があります。

はじめる前に

CTI ルート ポイントの設定, （623 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [CTI ルート ポイント（CTI Route Point）] を選択します。

ステップ 2 [検索（Find）] をクリックし、セルフプロビジョニングを設定する CTI ルート ポイントを選択します。

ステップ 3 [関連付け（Association）] の下にある [回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）] をクリックします。
[電話番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 4 [電話番号（Directory Number）] フィールドに、ユーザがセルフプロビジョニング IVR サービスを利用するためにダイヤルする内線番号を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [電話番号の設定（Directory Number Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次の作業

セルフプロビジョニング用アプリケーション ユーザの設定, （624 ページ）

セルフプロビジョニング用アプリケーション ユーザの設定

セルフプロビジョニング IVR 用にアプリケーション ユーザを設定し、アプリケーション ユーザに作成した CTI ルーティング ポイントを関連付ける必要があります。

はじめる前に

CTI ルート ポイントへの電話番号の割り当て, （623 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザ（User）] > [アプリケーション ユーザ（Application User）] を選択します。

ステップ 2 次のいずれかの手順を実行します。

a) 既存のアプリケーション ユーザを選択するには、[検索（Find）] をクリックして、アプリケーション ユーザを選択します。

b) 新しいアプリケーションユーザを作成するには、[新規追加（Add New）] をクリックします。

ステップ 3 [ユーザ ID（User ID）] テキスト ボックスに、アプリケーション ユーザの一意の名前を入力します。

ステップ 4 アプリケーション ユーザの [BLF プレゼンス グループ（BLF Presence Group）] を選択します。

ステップ 5 アプリケーションユーザに作成した CTI ルーティング ポイントを関連付けるには、次の手順を実行します。

a) 作成した CTI ルーティング ポイントが、[使用可能なデバイス（Available Devices）] リスト ボックスに表示されない場合は、[別のルート ポイントを検索（Find More Route Points）] をクリックします。
作成した CTI ルーティング ポイントが、利用可能なデバイスとして表示されます。

b) [使用可能なデバイス（Available Devices）] リスト ボックスで、セルフプロビジョニング用に作成した CTI ルーティング ポイントを選択し、下矢印をクリックします。
[制御するデバイス（Controlled Devices）] リスト ボックスに、[CTI ルート ポイント（CTI Route Point）] が表示されます。

ステップ 6 [アプリケーション ユーザの設定（Application User Configuration）] ウィンドウの他のフィールドを設定します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 7 [保存（Save）] をクリックします。

次の作業

システムのセルフプロビジョニング設定, （625 ページ）

システムのセルフプロビジョニング設定

システムをセルフプロビジョニング対応に設定するには、次の手順を実行します。セルフプロビジョニングにより、ユーザは IVR システムを介して、管理者に連絡することなく、ネットワークに自分のデスクの電話機やソフト クライアントを追加できます。

（注） セルフプロビジョニング機能を使用するには、エンド ユーザのユーザ プロファイルでも該当機能を有効にする必要があります。

手順

ステップ 1 Cisco Unified CM の管理から、[ユーザ管理（User Management）] > [セルフプロビジョニング（Self-Provisioning）] を選択します。

ステップ 2 セルフプロビジョニング IVR でエンドユーザを認証するかどうかを設定するには、次のオプション ボタンのいずれかをクリックします。

- [認証が必要（Require Authentication）]：セルフプロビジョニング IVR を使用するには、エンドユーザが自分のパスワード、PIN、またはシステム認証コードを入力する必要があります。

- [認証は必要なし（No Authentication Required）] : エンド ユーザは認証なしでセルフプロビジョニング IVR にアクセスできます。

ステップ 3 セルフプロビジョニング IVR で認証を要求するように設定されている場合、次のオプション ボタンのいずれかをクリックして、IVR がエンド ユーザを認証する方法を設定します。

- [エンド ユーザのみを認証（Allow authentication for end users only）] : エンド ユーザは自分のパスワードまたは PIN を入力する必要があります。
- [ユーザ（Password/PIN の入力）および管理者（認証コードの入力）を認証（Allow authentication for users (via Password/PIN) and Administrators (via Authentication Code)）] : エンド ユーザは認証コードを入力する必要があります。このオプションを選択した場合、認証コードとして、0 から 20 桁までの整数を [認証コード（Authentication Code）] テキストボックスに入力します。

ステップ 4 [IVR 設定（IVR Settings）] のリストボックスから、矢印を使用して IVR プロンプトで使用する言語を選択します。使用可能な言語は、システムにインストールした言語パックによって異なります。追加の言語パックをダウンロードするには、cisco.com のダウンロードセクションを参照してください。

ステップ 5 [CTI ルート ポイント（CTI Route Points）] ドロップダウン リスト ボックスから、セルフプロビジョニング IVR に設定した CTI ルート ポイントを選択します。

ステップ 6 [アプリケーション ユーザ（Application User）] ドロップダウン リストボックスから、セルフプロビジョニング用に設定したアプリケーション ユーザを選択します。

ステップ 7 [保存（Save）] をクリックします。

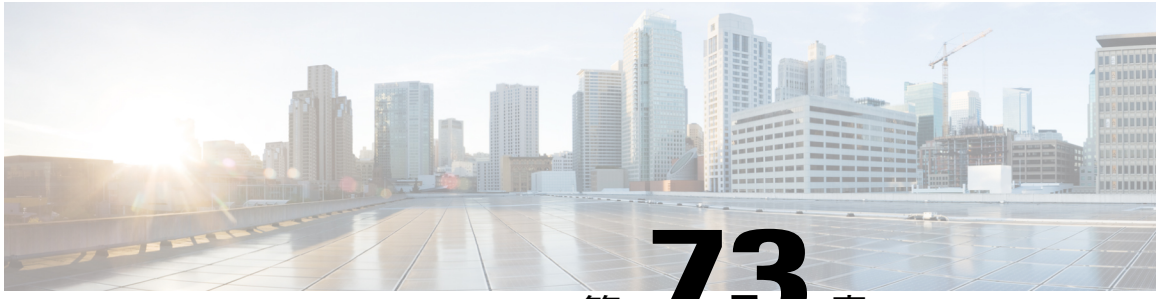
関連トピック

ユーザ プロファイルの設定, （284 ページ）

第 X 部

応用的なコール処理の設定

- 応用的なコール処理の概要，629 ページ
- APIC-EM コントローラによる QoS の設定，633 ページ
- コール制御検出の設定，641 ページ
- 外部コール制御の設定，653 ページ
- コール キューイングの設定，667 ページ
- コール スロットリングの設定，683 ページ
- 発信側の正規化，687 ページ
- 論理パーティション分割の設定，699 ページ
- 地理位置情報とロケーション伝達の設定，713 ページ
- ロケーション認識の設定，721 ページ
- 自動代替ルーティングの設定，729 ページ
- マルチレベルの優先とプリエンプション，733 ページ



第 73 章

応用的なコール処理の概要

- 応用的なコール処理について，629 ページ
- 応用的なコール処理の設定，629 ページ

応用的なコール処理について

このパートの章では、システムで応用的なコール処理を設定するためのさまざまな方法について説明します。このパートで概説する機能を使用して、システムがコール フローの任意の時点でコールを処理する方法を、コール転送などの基本的なコール処理機能よりきめ細かいレベルで設定できます。このパートのタスク フローでは、各コール処理機能を一覧して、その設定目的を説明し、さらに詳細に説明している適切な章へのリンクを示します。

応用的なコール処理の設定

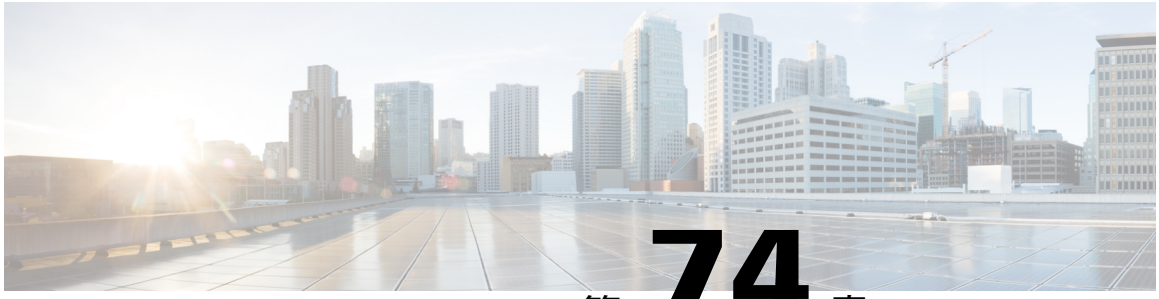
次のタスク フローを実行すると、システムの応用的なコール処理を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	APIC-EM コントローラ設定タスク フロー，（634 ページ）	SIP コールのネットワークサービス品質（QoS）を管理するには、Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）を導入します。APIC-EM は、Cisco Unified Communications Manager で管理された SIP エンドポイントおよびトランク間の通信セッションで作成されたメディア フローに DSCP マーキングを適用します。DSCP マーキングをメディア フローに適用すると、音声およびビデオ メディアが、電子メール、印刷ジョブ、ソフトウェアのダウンロードなどの優先順位の低

	コマンドまたはアクション	目的
		い他のネットワーク トラフィックによってブロックされなくなります。
ステップ 2	コール制御検出の設定タスク フロー, （642 ページ）	Service Advertisement Framework（SAF）ネットワークを使用する他のコール制御エンティティに Cisco Unified Communications Manager をアドバタイズするには、コール制御検出を設定します。これらのコール制御エンティティは、アドバタイズされた情報を使用して、コールのルーティング操作を動的に設定できます。
ステップ 3	外部コール制御の設定タスク フロー, （654 ページ）	付加ルート サーバでシステムのコールルーティングを決定できるようにするには、外部コール制御を設定します。Unified Communications Manager は、付加ルート サーバにルート要求を発行し、コールのルーティング方法と、適用する追加のコール処理について指示します。
ステップ 4	コール キューイング タスク フロー, （669 ページ）	ハント メンバーが応答可能になるまで発信者をキューに入れておくには、コール キューイングを設定します。
ステップ 5	コール スロットリングの設定, （684 ページ）	システムの状態により、オフフックになってからダイヤルトーンを受信するまでの間隔に遅延が生じる可能性があるとき、新しいコール試行を自動的に制限または拒否するには、コール スロットリングを設定します。コール スロットリングのパラメータは、シスコカスタマーサポートに指示された場合を除き、変更しないことを推奨します。
ステップ 6	発信側の正規化の設定タスク フロー, （689 ページ）	着信電話番号のフォーマットを変更して、グローバル化またはローカライズされた電話番号として受信者の電話機に表示するには、発信側の正規化を設定します。この機能を使用すれば、コールが複数の場所にルーティングされる際のコールバック機能を改善できます。また、電話機のコール ログ ディレクトリのディレクトリ番号を変更することなく電話機がコールバックできるよう、グローバル発信者番号をローカライズされた番号にマッピングできます。
ステップ 7	論理パーティション設定タスク フロー, （699 ページ）	トールバイパスが禁止されている市場で規制要件を満たすには、論理パーティショニングを設定します。たとえば、会議の参加やリダイレクトなどの通話中機能を使用して、ユーザが制限されたコールを開始できないようにするポリシーを設定できます。
ステップ 8	地理位置情報とロケーションの配信タスク フロー, （713 ページ）	すべてのデバイスの地理位置を特定し、クラスタ全体に地理位置情報を伝達します。地理位置情報がデバイスに民間

	コマンドまたはアクション	目的
		アドレスを割り当てることで、特定の国の法的要件に基づいてデバイス間の通信を制御できます。
ステップ 9	Location Awareness の設定タスク フロー, （723 ページ）	ロケーション認識によって、管理者は企業ネットワークに接続している電話の接続元となる物理的な場所を決定できます。
ステップ 10	AAR 設定タスク フロー, （729 ページ）	場所の帯域幅不足のためシステムがコールをブロックする場合、PSTN またはその他のネットワークを通じてコールを自動的に再ルーティングするようシステムを設定します。自動代替ルーティングにより、発信者が通話を終了して着信側にリダイヤルする必要はなくなります。
ステップ 11	Multilevel Precedence and Preemption Precendence のタスク フロー, （733 ページ）	検証済みのユーザにプライオリティ コールの発信を許可するには、Multilevel Precedence and Preemption（MLPP）を設定します。これらのユーザは、必要に応じて優先順位の低いコールをプリエンプション処理できます。



第 74 章

APIC-EM コントローラによる QoS の設定

- APIC-EM コントローラの概要，633 ページ
- APIC-EM コントローラの前提条件，634 ページ
- APIC-EM コントローラ設定タスク フロー，634 ページ

APIC-EM コントローラの概要

APIC-EM コントローラでは、一元化されたシステムによりネットワーク トラフィックを管理します。輻輳したネットワークにおいても、通信を維持するための帯域幅を常に確保できます。Cisco Unified Communications Manager は、SIP メディア フローの管理に APIC-EM コントローラを使用するように設定できるため、次の利点が得られます。

- QoS 管理の一元化により、DSCP 値を割り当てるためのエンドポイントが不要になります。
- メディア フローごとに異なる QoS 処理を適用できます。たとえば、ネットワーク帯域幅が低い場合でも、基本的な音声通信が常に維持されるように、音声をビデオより優先させることができます。
- SIP プロファイルの外部 QoS の設定により、ユーザが APIC-EM を使用する対象を設定できます。たとえば、Cisco Jabber ユーザは APIC-EM を使用してメディア フローを管理し、一方で Cisco Unified IP Phone ユーザは Cisco Unified Communications Manager の DSCP の設定を使用できます。

SIP メディア フローの管理

APIC-EM を使用する SIP コールの場合、Cisco Unified Communications Manger はコールの始めに APIC-EM コントローラにポリシー要求を送信して、メディア フローの APIC-EM がセットアップ中であることを通知します。ポリシー要求にはコールに関する情報（送信元デバイスと宛先デバイスの IP アドレスとポート、フローのメディア タイプ、プロトコルなど）が含まれています。

APIC-EM は、関連付けられているメディア フローの DSCP 値をコール フローの先頭でスイッチに通知します。スイッチは、それらの DSCP 値を個別のメディア パケットに挿入して、エンドポイントで挿入される値を上書きします。コール フロー内のゲートウェイで輻輳が発生すると、そ

のゲートウェイでは DSCP 値が高い方のパケットが先に送信されます。そのため、優先順位が高い音声ストリームやビデオストリームが、電子メール、印刷ジョブ、ソフトウェア ダウンロードなどの優先順位の低いネットワーク トラフィックによってブロックされません。コールが終了すると、Cisco Unified Communications Manager は APIC-EM に通知し、APIC-EM はフローの削除をスイッチに通知します。

外部 QoS のサポート

Cisco Unified Communications Manager で APIC-EM を使用してメディア フローを管理するためには、外部 QoS パラメータを、クラスタ全体のサービス パラメータを使用して両方のシステム レベルで有効にし、SIP プロファイルを使用してデバイス レベルで有効にする必要があります。

APIC-EM コントローラの前提条件

APIC-EM を使用する前に、次の手順を実行する必要があります。

- Cisco Unified Communications Manager の異なる SIP メディア フローの DSCP プライオリティを設定します。詳細は、DSCP の設定構成のタスク フロー, （565 ページ）を参照してください。
- ネットワーク内の APIC-EM コントローラ ハードウェアを設定します。詳細については、APIC-EM コントローラ付属のハードウェア ドキュメンテーションを参照してください。

APIC-EM コントローラ設定タスク フロー

APIC-EM コントローラが SIP メディア フローを制御できるようにするには、Cisco Unified Communications Manager で次のタスクを実行します。

はじめる前に

- APIC-EM コントローラの前提条件, （634 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	APIC-EM コントローラ証明書のアップロード, （636 ページ）	APIC-EM 証明書を Cisco Unified OS の管理にアップロードします。
ステップ 2	APIC-EM コントローラへの HTTPS 接続の設定, （637 ページ）	APIC-EM サービスを指定する HTTP サービス プロファイルを設定します。

	コマンドまたはアクション	目的
ステップ 3	システム向けに外部の QoS サービスを有効にする，（637 ページ）	[外部 QoS 有効（External QoS Enable）] サービス パラメータを有効にして、システムが APIC-EM を使用してメディア フローを制御するように設定します。デバイスが SIP メディア フローの管理に APIC-EM を使用できるようにするには、このサービス パラメータを有効にする必要があります。 （注） また、SIP メディア フローの管理に APIC-EM を使用するデバイスでは、SIP プロファイル内の外部 QoS も有効にする必要があります。
ステップ 4	SIP プロファイル レベルの外部 QoS サービスの設定，（638 ページ）	SIP プロファイル内の外部 QoS を有効にします。この SIP プロファイルを使用するすべてのデバイスは、SIP メディア フローを管理するために APIC-EM を使用できるようになります。 SIP プロファイル設定を使用すると、APIC-EM にメディア フローを管理させるデバイスやデバイス タイプを設定できます。
ステップ 5	電話機への SIP プロファイルの割り当て，（639 ページ）	外部 QoS 対応 SIP プロファイルを電話機に関連付けます。

APIC-EM コントローラの設定

ユーザとして Cisco Unified Communications Manager を追加するには、APIC-EM コントローラで次の手順を使用します。APIC-EM のロールベース アクセス コントロール機能により、Cisco Unified Communications Manager で APIC-EM リソースの利用が可能になります。

手順

ステップ 1 APIC-EM コントローラで、[設定（Settings）] > [内部ユーザ（Internal Users）] を選択します。

ステップ 2 次の権限で新しいユーザを作成します。[ROLE_POLICY_ADMIN]Cisco Unified Communications Manager の [HTTP プロファイル（HTTP Profile）] ウィンドウで同一のクレデンシャルを入力する必要があるため、入力するユーザ名とパスワードを記録しておきます。

ステップ 3 [ディスカバリ（Discovery）] タブに移動し、CDP による検出、または使用可能なデバイスの IP アドレスの範囲を追加します。

ステップ 4 [デバイス インベントリ（Device Inventory）] タブを選択し、到達可能なデバイスを選択します。

ステップ 5 [ポリシー タグの設定（Set Policy Tag）] をクリックします。

ステップ 6 ポリシー タグを作成し、そのタグをデバイスに設定します。

ステップ 7 [EasyQoS] タブで、作成したポリシーを選択し、[DynamicQoS] を有効にします。

次の作業

APIC-EM コントローラ証明書のアップロード, （636 ページ）

APIC-EM コントローラ証明書のアップロード

APIC-EM コントローラ証明書を Cisco Unified Communications Manager にアップロードするには、次の手順を使用します。

手順

ステップ 1 Cisco Unified OS の管理から、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ポップアップ ウィンドウが表示されます。

ステップ 3 [証明書目的（Certificate Purpose）] ドロップダウンリストで、[CallManager 信頼（CallManager-trust）] を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。

ステップ 5 [参照（Browse）] をクリックし、証明書を検索して選択します。

ステップ 6 [アップロード（Upload）] をクリックします。

次の作業

APIC-EM コントローラへの HTTPS 接続の設定, （637 ページ）

APIC-EM コントローラへの HTTPS 接続の設定

Cisco Unified Communications Manager を APIC-EM コントローラに接続するように HTTP プロファイルを設定するには、次の手順を使用します。この接続では、Cisco Unified Communications Manager は HTTP ユーザとして機能し、APIC-EM は HTTP サーバとして機能します。

はじめる前に

APIC-EM コントローラ証明書のアップロード, （636 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）]>[HTTP プロファイル（HTTP Profile）] を選択します。

ステップ 2 [名前（Name）] にサービスの名前を入力します。

ステップ 3 この HTTP 接続の [ユーザ名（User Name）] と [パスワード（Password）] を入力します。ユーザ名を Cisco Unified Communications Manager で設定済みのエンドユーザとする必要はありませんですが、ユーザ名とパスワードは、APIC-EM コントローラに設定された値に一致する必要があります。

ステップ 4 [Web サービスのルート URI（Web Service Root URI）] テキスト ボックスで、APIC-EM サービスの IP アドレスまたは完全修飾ドメイン名を入力します。

ステップ 5 [HTTP プロファイル（HTTP Profile）] ウィンドウの残りのフィールドを設定します。フィールドとそのオプションに関するヘルプは、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

次の作業

システム向けに外部の QoS サービスを有効にする, （637 ページ）

システム向けに外部の QoS サービスを有効にする

QoS 管理の外部サービスを使用できるように、Cisco Unified Communications Manager を設定するには、次の手順を実行します。QoS の APIC-EM コントローラを使用するために、このサービスパラメータを有効にする必要があります。

はじめる前に

APIC-EM コントローラへの HTTPS 接続の設定, （637 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）]>[サービス パラメータ（Service Parameters）] の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからパブリッシャ ノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 4 [外部 QoS 機能を有効にする（External QoS Enabled）] サービス パラメータの値を [True] に設定します。

ステップ 5 [保存（Save）] をクリックします。

（注） APIC-EM を使用してデバイスのコール フローを管理するには、デバイスの SIP プロファイル内の外部 QoS を有効にする必要があります。

次の作業

SIP プロファイル レベルの外部 QoS サービスの設定, （638 ページ）

SIP プロファイル レベルの外部 QoS サービスの設定

クラスタ全体のサービス パラメータである [外部 QoS 有効（External QoS Enabled）] を有効にした場合、次の手順を使用して、この SIP プロファイルを使用する SIP デバイスの外部 QoS を有効にします。

（注） 外部 QoS は、APIC-EM を使用して QoS を管理するためにシステム レベルと SIP プロファイルの両方で有効にする必要があります。

はじめる前に

システム向けに外部の QoS サービスを有効にする, （637 ページ）

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 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存の SIP プロファイルを選択します。

- [新規追加（Add New）] をクリックして、新しい SIP プロファイルを作成します。

ステップ 3 [外部 QoS の有効化（Enable External QoS）] チェックボックスをオンにします。この SIP プロファイルを使用して APIC-EM コントローラで QoS を管理する電話の場合、このチェックボックスをオンにする必要があります。

ステップ 4 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

次の作業

電話機への SIP プロファイルの割り当て, （639 ページ）

電話機への SIP プロファイルの割り当て

作成した外部 QoS 対応 SIP プロファイルを電話機に割り当てるには、次の手順を使用します。

ヒント 多数の電話機を選択した SIP プロファイルの更新を一度の操作で行うには、一括管理ツールを使用します。詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』を参照してください。

はじめる前に

電話機への SIP プロファイルの割り当て, （639 ページ）

手順

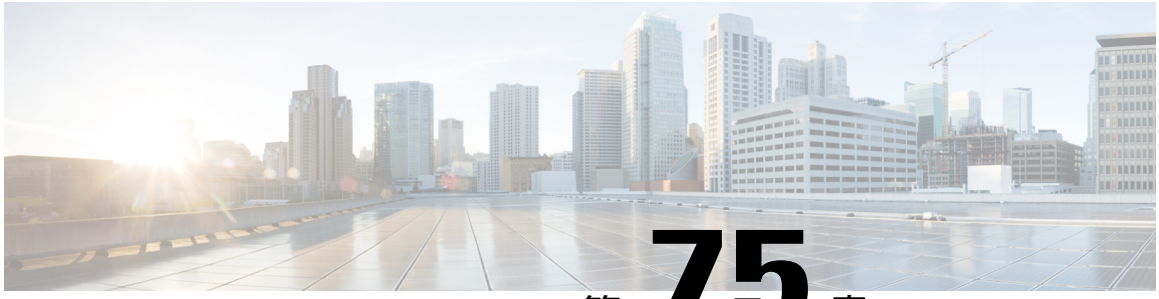
ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 [検索（Find）] をクリックし、既存の電話機を選択します。

ステップ 3 [SIP プロファイル（SIP Profile）] ドロップダウン リスト ボックスから、トラフィック管理に APIC-EM コントローラを使用する電話機向けに更新した SIP プロファイルを選択します。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウの残りのフィールドをすべて入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。



第 75 章

コール制御検出の設定

- コール制御検出の概要，641 ページ
- コール制御検出の前提条件，641 ページ
- コール制御検出の設定タスク フロー，642 ページ
- コール制御検出の連携動作と制限事項，650 ページ

コール制御検出の概要

コール制御検出（CCD）を使用して、電話番号パターンなどのその他の主要な属性とともにCisco Unified Communications Manager 情報をアドバタイズできます。Service Advertisement Framework（SAF）ネットワークを使用するその他のコール制御エンティティは、アドバタイズされた情報を使用して、動的にルーティング動作を設定し、適応させることができます。SAF を使用するすべてのエンティティが、他の主要な情報とともに電話番号パターンをアドバタイズします。その他のリモート コール制御エンティティは、このブロードキャストから情報を習得し、コールのルーティング動作を適合させることができます。

コール制御検出の前提条件

- SAF 対応の SIP または H.323 クラスタ間（ゲートキーパー非制御）トランク
- SAF ネットワークをサポートおよび使用しているリモート コール制御エンティティ。たとえば、その他の Cisco Unified Communications Manager、または Cisco Unified Communications Manager Express サーバ
- SAF フォワーダとして設定されている Cisco IOS ルータ

コール制御検出の設定タスク フロー

はじめる前に

- コール制御検出の前提条件, （641 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco IOS ルータをサポートするドキュメントを参照してください。Cisco Feature Navigator（http://www.cisco.com/go/cfn）を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。	Cisco IOS ルータを SAF フォワーダとして設定します。
ステップ 2	SAF セキュリティ プロファイルの設定, （644 ページ）	SAF フォワーダと Cisco Unified Communications Manager の間にセキュアな接続を確立するために、SAF フォワーダ向けに SAF セキュリティ プロファイルを設定します。
ステップ 3	SAF フォワーダの設定, （644 ページ）	SAF フォワーダを設定します。これは、SAF 向けに設定された Cisco IOS ルータです。SAF フォワーダは、リモート呼制御エンティティがホスト DN パターンをアドバタイズすると、ローカル クラスタに通知します。さらに、それぞれ設定されているローカル クラスタからのパブリッシング要求や、設定されている登録トランクが SAF フォワーダに送信されます。パブリッシング要求には、Cisco Unified Communications Manager の DN パターン、PSTN フェールオーバー設定、トランク、SIP トランクのリスニング ポートに加え、トランクの URI を含む SIP ルート ヘッダー フィールドが含まれます。
ステップ 4	SIP トランクと H.323 クラスタ間トランクの設定, （645 ページ）	SAF をサポートするには、SIP または H.323 クラスタ間（ゲートキーパー非制御）トランクを設定します。ローカル クラスタは、CCD 要求サービスに割り当てられている SAF 対応のトランクを使用して、SAF ネットワークを使用するリモートの呼制御に発信コールをルーティングします。

	コマンドまたはアクション	目的
ステップ 5	ホスト DN グループの設定,（646 ページ）	ホスト DN グループを設定します。これは、ホスト DN パターンのコレクションです。ホスト DN グループを CCD アドバタイジング サービスに割り当てると、CCD アドバタイジング サービスは、ホスト DN グループに含まれているすべてのホスト DN パターンをアドバタイズします。1 つの CCD アドバタイジング サービスに割り当てられるホスト DN グループは 1 つのみです。
ステップ 6	ホスト DN パターンの設定,（646 ページ）	ホスト DN パターンを設定します。これは、Cisco Unified Communications Manager に属する電話番号パターンです。CCD アドバタイジング サービスは、SAF ネットワークを使用する他のリモート呼制御エンティティにこのパターンをアドバタイズします。このパターンをホスト DN グループに関連付けます。関連付けることで、複数のパターンを かんたんに CCD アドバタイジング サービスに関連付けることができます。
ステップ 7	アドバタイジング サービスの設定,（647 ページ）	コール制御検出アドバタイジング サービスを設定します。これにより、Cisco Unified Communications Manager で、クラスタのホスト DN と PSTN フェイルオーバー設定を、SAF ネットワークを使用するリモート コール制御エンティティにアドバタイズします。
ステップ 8	コール制御検出のパーティションの設定,（648 ページ）	コール制御検出パーティションを確認して、学習パターンがこのパーティションの番号分析に挿入されていることを確認します。
ステップ 9	要求サービスの設定,（648 ページ）	ローカル クラスタから、SAF ネットワークのアドバタイズメントを検出できるようにするには、コール制御検出の要求サービスのいずれかを設定して、SAF ネットワークを使用するリモートコール制御のアドバタイズメントをリッスンします。また、CCD 要求サービスは、学習パターンが番号分析に挿入されていることを確認します。
ステップ 10	学習パターンのブロック,（649 ページ）	リモート コール制御エンティティからローカル Cisco Unified Communications Manager に送信される学習パターンをブロックします。今後使用しない学習パターンについては、次の手順を実行します。

SAF セキュリティ プロファイルの設定

SAF フォワーダと Cisco Unified Communications Manager の間にセキュアな接続を確立するために、SAF フォワーダ向けに SAF セキュリティ プロファイルを設定します。

ヒント　ルータ（SAF フォワーダ）で入力したものと同じユーザ名とパスワードを使用します。

はじめる前に

SAF フォワーダとして Cisco IOS ルータを設定します。（http://www.cisco.com/go/cfn にある Cisco Feature Navigator を参照してください）

手順

ステップ 1　Cisco Unified CM の管理から、[詳細機能（Advanced Features）] > [SAF] > [SAF セキュリティ プロファイル（SAF Security Profile）] を選択します。

ステップ 2　[SAF セキュリティ プロファイルの設定（SAF Security Profile Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3　[保存（Save）] をクリックします。

次の作業

SAF フォワーダの設定, （644 ページ）

SAF フォワーダの設定

SAF フォワーダを設定します。これは、SAF 向けに設定された Cisco IOS ルータです。SAF フォワーダは、リモート呼制御エンティティがホスト DN パターンをアドバタイズすると、ローカル クラスタに通知します。さらに、それぞれ設定されているローカル クラスタからのパブリッシング要求や、設定されている登録トランクが SAF フォワーダに送信されます。パブリッシング要求には、Cisco Unified Communications Manager の DN パターン、PSTN フェールオーバー設定、トランク、SIP トランクのリスニング ポートに加え、トランクの URI を含む SIP ルート ヘッダー フィールドが含まれます。

ヒント　[選択された Cisco Unified Communications Manager（Selected Cisco Unified Communications Managers）] ペインに複数のノードが表示される場合、「@」がクライアント ラベル値に付加されます。各ノードが SAF フォワーダの登録に同じクライアント ラベルを使用した場合にエラーが発生することがあるからです。

はじめる前に

SAF セキュリティ プロファイルの設定, （644 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[詳細機能（Advanced Features）] > [SAF（SAF）] > [SAF フォワーダ（SAF Forwarder）] を選択します。

ステップ 2 [SAF フォワーダの設定（SAF Forwarder Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

SIP トランクと H.323 クラスタ間トランクの設定, （645 ページ）

SIP トランクと H.323 クラスタ間トランクの設定

SAF をサポートするには、SIP または H.323 クラスタ間（ゲートキーパー非制御）トランクを設定します。ローカル クラスタは、CCD 要求サービスに割り当てられている SAF 対応のトランクを使用して、SAF ネットワークを使用するリモートの呼制御に発信コールをルーティングします。

はじめる前に

SAF フォワーダの設定, （644 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、[デバイス（Device）]>[トランク（Trunk）] 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 次のいずれかの作業を実行します。

- SIP トランクの場合：
  1. [トランク サービス タイプ（Trunk Service Type）] ドロップダウン リストから、[コール制御検出（Call Control Discovery）] を選択します。ドロップダウン リストから選択した後は、トランク サービス タイプを変更できません。
  2. [Next] をクリックします。
  3. [トランクの設定（Trunk Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。
- クラスタ間（ゲートキーパー制御なし）トランクの場合：
  1. [Next] をクリックします。

2 [SAF を有効にする（Enable SAF）] チェックボックスをオンにします。

3 [トランクの設定（Trunk Configuration）] ウィンドウで他のフィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ホスト DN グループの設定, （646 ページ）

ホスト DN グループの設定

ホスト DN グループを設定します。これは、ホスト DN パターンのコレクションです。ホスト DN グループを CCD アドバタイジング サービスに割り当てると、CCD アドバタイジング サービスは、ホスト DN グループに含まれているすべてのホスト DN パターンをアドバタイズします。1 つの CCD アドバタイジング サービスに割り当てられるホスト DN グループは 1 つのみです。

はじめる前に

SIP トランクと H.323 クラスタ間トランクの設定, （645 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [コール制御検出（Call Control Discovery）] > [ホスト DN グループ（Hosted DN Group）] を選択します。

ステップ 2 [ホスト DN グループの設定（Hosted DN Groups Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

ホスト DN パターンの設定, （646 ページ）

ホスト DN パターンの設定

ホスト DN パターンを設定します。これは、Cisco Unified Communications Manager に属する電話番号パターンです。CCD アドバタイジング サービスは、SAF ネットワークを使用する他のリモート呼制御エンティティにこのパターンをアドバタイズします。このパターンをホスト DN グループに関連付けます。関連付けることで、複数のパターンを かんたんに CCD アドバタイジング サービスに関連付けることができます。

はじめる前に

ホスト DN グループの設定, （646 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [コール制御検出（Call Control Discovery）] > [ホスト DN パターン（Hosted DN Patterns）] を選択します。

ステップ 2 [ホスト DN パターンの設定（Hosted DN Patterns Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

アドバタイジング サービスの設定, （647 ページ）

アドバタイジング サービスの設定

コール制御検出アドバタイジング サービスを設定します。これにより、Cisco Unified Communications Manager で、クラスタのホスト DN と PSTN フェイルオーバー設定を、SAF ネットワークを使用するリモート コール制御エンティティにアドバタイズします。

はじめる前に

ホスト DN パターンの設定, （646 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [コール制御ディスカバリ（Call Control Discovery）] > [アドバタイジング サービス（Advertising Service）] を選択します。

ステップ 2 [アドバタイジング サービスの設定（Advertising Service Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

コール制御検出のパーティションの設定, （648 ページ）

コール制御検出のパーティションの設定

コール制御検出パーティションを確認して、学習パターンがこのパーティションの番号分析に挿入されていることを確認します。

（注） [Cisco Unified CM の管理（Cisco Unified CM Administration）] 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）] > [パーティション（Partition）] を選択して表示されるウィンドウに CCD のパーティションは表示されません。

はじめる前に

アドバタイジング サービスの設定, （647 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [コール制御検出（Call Control Discovery）] > [アドバタイジング サービス（Advertising Service）] を選択します。

ステップ 2 [コール制御検出パーティションの設定（Call Control Discovery Partition Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

要求サービスの設定, （648 ページ）

要求サービスの設定

注意 [学習されたパターンのプレフィックス（Learned Pattern Prefix）] フィールドまたは [ルート パーティション（Route Partition）] フィールドの更新は、システム パフォーマンスに影響を与える可能性があります。システム パフォーマンスの問題を回避するため、これらのフィールドはオフピークの時間帯に更新することを推奨します。

ローカル クラスタから、SAF ネットワークのアドバタイズメントを検出できるようにするには、コール制御検出の要求サービスのいずれかを設定して、SAF ネットワークを使用するリモート コール制御のアドバタイズメントをリッスンします。また、CCD 要求サービスは、学習パターンが番号分析に挿入されていることを確認します。

はじめる前に

コール制御検出のパーティションの設定, （648 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [コール制御検出（Call Control Discovery）] > [要求サービス（Requesting Service）].を選択します。

ステップ 2 [要求サービスの設定（Requesting Service Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

- SAF ネットワークを使用するには、リモート コール制御エンティティを設定します。（リモート コール制御エンティティのマニュアルを参照してください）。
- 学習パターンのブロック，（649 ページ）

学習パターンのブロック

リモート コール制御エンティティからローカル Cisco Unified Communications Manager に送信される学習パターンをブロックします。今後使用しない学習パターンについては、次の手順を実行します。

はじめる前に

SAF ネットワークを使用するには、リモート コール制御デバイスを設定します。お使いのリモート コール制御デバイスに対応するマニュアルを参照してください。

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [コール制御ディスカバリ（Call Control Discovery）] > [学習パターンのブロック（Block Learned Patterns）] を選択してください。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 次のいずれかのフィールドを設定します。

- [学習パターン（Learned Pattern）] フィールドで、ブロックする学習パターンを正確に入力します。Cisco Unified Communications Manager にブロックさせるパターンを正確に入力する必要があります。
- [学習パターンのプレフィックス（Learned Pattern Prefix）] フィールドに、パターンの先頭に付加されているプレフィックスに基づいて学習パターンをブロックするプレフィックスを入力します。

例：
[学習パターン（Learned Pattern）] では、235XX パターンをブロックするには 235XX を入力します。

例：
[学習パターン プレフィックス（Learned Pattern Prefix）] では、+1 を使用するパターンをブロックするには +1 を入力します。

ステップ 4 [リモート コール制御デバイス（Remote Call Control Entity）] フィールドに、ブロックするパターンをアドバタイズするリモート コール制御デバイスの名前を入力します。

ステップ 5 [リモート IP（Remote IP）] フィールドに、学習パターンをブロックするリモート コール制御デバイスの IP アドレスを入力します。

ステップ 6 [保存（Save）] をクリックします。

コール制御検出の連携動作と制限事項

コール制御検出の連携動作

表 *76*：コール制御検出の連携動作

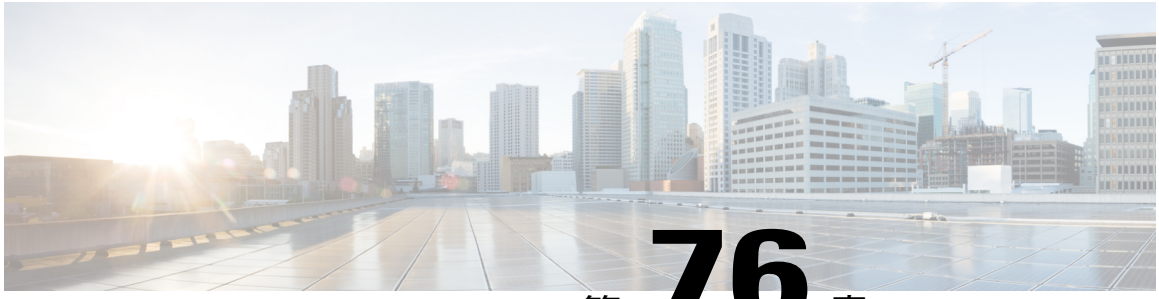
機能	データのやり取り
アラーム	Cisco Unified Serviceability は、コール制御検出機能をサポートするためのアラームを提供しています。アラームの設定方法の詳細については、『*Cisco Unified Serviceability Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。
BLF サブスクリプション	ユーザが SAF 学習パターンの BLF ステータスを登録すると、Cisco Unified Communications Manager は、SIP トランクを介して SIP 登録メッセージをリモート クラスタに送信します。 この機能は、SAF 対応の SIP トランクでのみサポートされます。
一括管理ツール	一括管理ツールでは、SAF セキュリティ プロファイル、SAF フォワーダ、CCD アドバタイジング サービス、CCD 要求サービス、ホステッド DN グループおよびホステッド DN パターンの設定をインポートおよびエクスポートできます。

機能	データのやり取り
コール詳細レコード	Cisco Unified Communications Manager は、リダイレクション理由を SS_RFR_SAF_CCD_PSTNFAILOVER とした、onBehalfOf の SAFCCDRequestingService としてのリダイレクトをサポートしています。これは、コールが PSTN フェールオーバー番号にリダイレクトされることを示しています。
[着信の着呼側設定（Incoming Called Party Settings）]	H.323 プロトコルは、国際番号用エスケープ文字 + をサポートしていません。H.323 ゲートウェイまたはトランク経由の着信コールに対する SAF およびコール制御検出で正しい DN パターンが使用されるようにするには、サービス パラメータ、デバイス プール、H.323 ゲートウェイ、または H.323 トランク ウィンドウの着信の着呼側を設定する必要があります。つまり、H.323 ゲートウェイまたはトランクからコールが着信した場合に、Cisco Unified Communications Manager が着信者番号をトランクまたはゲートウェイ経由で送信された元の値に変換するように設定します。 たとえば、発信者は Cisco Unified Communications Manager A 宛てへ +19721230000 に発信します。 Cisco Unified Communications Manager A は +19721230000 を受信し、H.323 トランクにコールを送信する前に、その番号を 55519721230000 に変換します。この場合、設定は、国際番号用エスケープ文字 + が取り除かれ、555 が国際番号タイプのコールの前に付加されることを示しています。 トランクからのこの着信コールの場合、番号分析が発信者によって送信された値を使用できるように、Cisco Unified Communications Manager B は 55519721230000 を受信すると、その番号を +19721230000 に変換し直します。この場合、着信の着呼側の設定は、555 を取り除き、国際番号タイプの着信者番号の前に +1 を付加することを示しています。
ダイジェスト認証	Cisco Unified Communications Manager は、ダイジェスト認証（TLS なし）を使用して、SAF フォワーダを認証します。Cisco Unified Communications Manager が SAF フォワーダにメッセージを送信すると、Cisco Unified Communications Manager は SHA1 チェックサムを計算し、それをメッセージの MESSAGE-INTEGRITY フィールドに含めます。

機能	データのやり取り
QSIG	[H.323 の設定（H.323 Configuration）] ウィンドウの [QSIG バリエーション（QSIG Variant）] および [ASN.1 ROSE OID エンコーディング（ASN.1 ROSE OID Encoding）] 設定は、CCD アドバタイジング サービスによってアドバタイズされます。これらの設定は、着信トンネル化コールの QSIG メッセージの復号に影響します。コール制御検出の場合、発信コールには影響しません。 リモート呼制御エンティティが、H.323 トランク経由の発信コールに QSIG トンネリングが必要かどうかを判別します。リモート呼制御エンティティによって QSIG トンネリングが必要であるとアドバタイズされると、Cisco Unified CM の管理の [H.323 の設定（H.323 Configuration）] ウィンドウで QSIG サポートが必要ないことが示されている場合でも、発信コールのメッセージ内に QSIG メッセージがトンネル化されます。

コール制御検出の制限

すべてのクラスタが、同じ自律システム（AS）内のアドバタイズされたルートまたは学習されたルートに制限されます。



第 76 章

外部コール制御の設定

- 外部コール制御の概要，653 ページ
- 外部コール制御の前提条件，654 ページ
- 外部コール制御の設定タスク フロー，654 ページ
- 外部コール制御の連携動作と制限事項，662 ページ

外部コール制御の概要

外部コール制御によって、付加ルート サーバは、Cisco Unified ルーティング ルール インターフェイスを使用して、Cisco Unified Communications Manager のコール ルーティングを決定できます。外部コール制御を設定すると、Cisco Unified Communications Manager は、発信側および着信側の情報を含むルート要求を付加ルート サーバに発行します。サーバは要求を受信すると、適切なビジネス ロジックを適用し、コールのルーティング方法と適用する追加のコール処理をシステムに指示するルート応答を返します。

付加ルータは、システムが、コールの許可/転送/拒否、発信側および着信側の情報の変更、発信者へのアナウンスの再生、付加ボイスメール サーバと IVR サーバが発信側/着信側の情報を適切に解釈できるようにするためのコール履歴のリセット、コールが転送または拒否された理由を示す理由コードの記録を実行する方法に影響します。

外部コール制御は、次の機能を提供します。

- 最高品質の音声ルーティング：すべてのコール参加者に最高の音声品質を提供する音声ゲートウェイを介してコールがルーティングされるように、付加ルート サーバはネットワーク リンクの可用性、帯域幅の使用、遅延、ジッタ、MOS 値をモニタします。
- 最小コスト ルーティング：コールがコスト効率の最も高いリンクを経由してルーティングされるように、付加ルート サーバは Local Access and Transport Area（LATA）および LATA 間の料金プラン、トランキング コスト、バースト使用コストなどのキャリアとの契約情報を使用して設定されます。
- 論理的境界：付加ルート サーバには、到達可能性、たとえば、ユーザ 1 にユーザ 2 へのコール発信を許可するかどうかを決定する企業ポリシーが設定されます。

外部コール制御の前提条件

この機能には、システムにコールの処理方法を指示する Cisco Unified ルーティング ルール XML インターフェイスが必要です。

詳細については、『*Cisco Unified Routing Rules Interface Developers Guide*』（CURRI のドキュメント）（https://developer.cisco.com）を参照してください。

外部コール制御の設定タスク フロー

はじめる前に

- 外部コール制御の前提条件,（654 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	外部コール制御用コーリング サーチ スペースの設定,（655 ページ）	ルート サーバが転送オブリゲーションを送信する際に使用するシステムのコーリング サーチ スペースを設定します。コーリング サーチ スペースは、デバイスに割り当てられるルートパーティションの番号付きリストから構成されます。コーリング サーチ スペースでは、発信側デバイスが電話を終了しようとする際に検索するパーティションが決定されます。
ステップ 2	外部コール制御プロファイルの設定,（656 ページ）	外部のコール制御プロファイルで、付加ルート サーバの URI、電話の転送に使用するコーリング サーチ スペース、付加ルート サーバからのシステムの応答待機時間を示すタイマーなどを設定します。
ステップ 3	トランスレーション パターンへのプロファイルの割り当て,（657 ページ）	外部コール制御で使用する変換パターンの場合、外部コール制御プロファイルをパターンに割り当てます。変換パターンに一致するコールが発生すると、システムはコール ルーティング クエリを付加ルート サーバに送信し、付加ルート サーバは、システムにコールの対処方法を指示します。
ステップ 4	ルーティング サーバの証明書のトラステッド ストアへのインポート,（658 ページ）	（任意） ルーティング サーバでHTTPSが使用されている場合、ルーティング サーバの証明書は、システム ノードの信頼ストアにインポートされます。このタスクは、クラスタの各ノードで実行する必要があります。ルーティング クエリはルーティング サーバに送信できます。外部コール制御プロファイルのプライマリまたはセカンダリの Web サービス URI に

	コマンドまたはアクション	目的
		HTTPS を使用している場合、システムでは、証明書を使用して、設定済みの付加ルーティング サーバに TLS 接続で相互認証します。
ステップ 5	自己署名証明書をルーティング サーバにエクスポートする, （659 ページ）	（任意） ルーティング サーバで HTTPS が使用されている場合は、Cisco Unified Communications Manager の自己署名証明書をルーティング サーバにエクスポートします。クラスタの各ノードでこのタスクを実行する必要があります。これにより、ルーティング クエリをルーティング サーバに送信できます。プライマリ サーバおよび冗長ルート サーバが、Cisco Unified Communications Manager を使用して HTTPS 経由で認証できることを確認するには、システムに命令を送信する各付加ルート サーバにインポートできる自己署名証明書を生成する必要があります。 クラスタの各ノードでこの手順を実行します。これにより、プライマリ サーバおよび冗長付加ルート サーバと通信できるようになります。
ステップ 6	監察機能の設定, （659 ページ）	（任意） 監察者はコールをモニタするか、録音する必要があることをルートをルーティングのサーバのステータスから規定する権限の機能を設定します。監察者はコールの会社のポリシーを示し、コールをモニタおよび録音、選択した電話ユーザです。
ステップ 7	カスタマイズされたアナウンスの設定, （661 ページ）	（任意） ルーティング ルールで、一部のコールでアナウンスを再生する必要があり、シスコ提供のアナウンスを使用しない場合には、この手順に従います。

外部コール制御用コーリング サーチ スペースの設定

ルート サーバが転送オブリゲーションを送信する際に使用するシステムのコーリング サーチ スペースを設定します。コーリング サーチ スペースは、デバイスに割り当てられるルート パーティションの番号付きリストから構成されます。コーリング サーチ スペースでは、発信側デバイスが電話を終了しようとする際に検索するパーティションが決定されます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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 [名前（Name）] フィールドに、名前を入力します。
各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

ステップ 4 [説明（Description）] フィールドに、説明を入力します
説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 [使用可能なパーティション（Available Partitions）] ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。
- パーティションが複数ある場合は、コントロール（Ctrl）キーを押したまま、適切なパーティションを選択します。

ステップ 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）] フィールドにパーティションを移動させます。

ステップ 7 （任意） [選択されたパーティション（Selected Partitions）] ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

外部コール制御プロファイルの設定, （656 ページ）

外部コール制御プロファイルの設定

外部のコール制御プロファイルで、付加ルート サーバの URI、電話の転送に使用するコーリング サーチ スペース、付加ルート サーバからのシステムの応答待機時間を示すタイマーなどを設定します。

はじめる前に

外部コール制御用コーリング サーチ スペースの設定, （655 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [外部コール制御プロファイル（External Call Control Profile）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存の外部コール制御プロファイルの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存の外部コール制御プロファイルを選択します。
- 新しい外部コール制御プロファイルを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [外部コール制御プロファイルの設定（External Call Control Profile Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

トランスレーション パターンへのプロファイルの割り当て, （657 ページ）

トランスレーション パターンへのプロファイルの割り当て

外部のコール制御プロファイルで、付加ルート サーバの URI、電話の転送に使用するコーリング サーチスペース、付加ルートサーバからのシステムの応答待機時間を示すタイマーなどを設定します。

はじめる前に

外部コール制御プロファイルの設定, （656 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [トランスレーション パターン（Translation Pattern）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のトランスレーションパターンの設定を変更するには、検索条件を入力して[検索（Find）] をクリックし、結果のリストから既存のトランスレーション パターンを選択します。

- 新しいトランスレーション パターンを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [外部コール制御プロファイル（External Call Control Profile）] ドロップダウン リストから、パターンに割り当てる外部コール制御プロファイルを選択します。

ステップ 4 [トランスレーションパターンの設定（Translation Pattern Configuration）] ウィンドウ内の他のフィールドを必要に応じて設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

次の作業

（オプション） ルーティング サーバの証明書のトラステッド ストアへのインポート，（658 ページ）

ルーティング サーバの証明書のトラステッド ストアへのインポート

ルーティング サーバで HTTPS が使用されている場合、ルーティング サーバの証明書は、システム ノードの信頼ストアにインポートされます。このタスクは、クラスタの各ノードで実行する必要があります。ルーティングクエリはルーティングサーバに送信できます。外部コール制御プロファイルのプライマリまたはセカンダリの Web サービス URI に HTTPS を使用している場合、システムでは、証明書を使用して、設定済みの付加ルーティング サーバに TLS 接続で相互認証します。

はじめる前に

トランスレーション パターンへのプロファイルの割り当て，（657 ページ）

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] で、[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 3 [証明書のアップロード（Upload Certificate）] ポップアップ ウィンドウで、[証明書名（Certificate Name）] ドロップダウンリストから [CallManager-trust] をクリックして、付加ルート サーバの証明書を参照します。

ステップ 4 [ファイルのアップロード（Upload File）] フィールドに証明書が表示されたら、[アップロード（Upload）] をクリックします。

ステップ 5 （任意） システムが冗長性付加ルート サーバに連絡できたら、次の手順を再度実行します。

次の作業

自己署名証明書をルーティング サーバにエクスポートする, （659 ページ）

自己署名証明書をルーティング サーバにエクスポートする

ルーティング サーバで HTTPS が使用されている場合は、Cisco Unified Communications Manager の自己署名証明書をルーティング サーバにエクスポートします。クラスタの各ノードでこのタスクを実行する必要があります。これにより、ルーティングクエリをルーティングサーバに送信できます。プライマリ サーバおよび冗長ルート サーバが、Cisco Unified Communications Manager を使用して HTTPS 経由で認証できることを確認するには、システムに命令を送信する各付加ルート サーバにインポートできる自己署名証明書を生成する必要があります。

クラスタの各ノードでこの手順を実行します。これにより、プライマリ サーバおよび冗長付加ルート サーバと通信できるようになります。

はじめる前に

ルーティング サーバの証明書のトラステッド ストアへのインポート, （658 ページ）

手順

ステップ 1 [Cisco Unified Operating Administration] で、[セキュリティ（Security）]>[証明書の管理（Certificate Management）] を選択します。

ステップ 2 [証明書リスト（Certificate List）] ウィンドウで、[新規作成（Generate New）] をクリックします。

ステップ 3 [証明書の名前（Certificate Name）] ドロップダウン リストで、[CallManager] を選択します。

ステップ 4 [新規作成（Generate New）] をクリックします。

ステップ 5 [証明書の検索と一覧表示（Find and List Certificates）] ウィンドウで、作成した [CallManager.pem] の証明書を選択します。

ステップ 6 証明書のファイル データが表示されたら、[ダウンロード（Download）] をクリックして、付加ルート サーバへ証明書をエクスポートするために使用するロケーションに証明書をダウンロードします。

ステップ 7 命令を送信する各付加ルート サーバに証明書をエクスポートします。

次の作業

（オプション） 監察機能の設定, （659 ページ）

監察機能の設定

監察者はコールをモニタするか、録音する必要があることをルートをルーティングのサーバのステータスから規定する権限の機能を設定します。監察者はコールの会社のポリシーを示し、コールをモニタおよび録音、選択した電話ユーザです。

Cisco Unified Communications Manager では次の機能により、付加ルート サーバのダイレクトのような監察機能をサポートします。

- 監察者、ハント グループ、監察者リストに着信コールをリダイレクトします。
- 監察者はコールを記録できます。

監察者が発信者に接続するか、または監察対象の会議が確立されると、コールの録音を開始できるように、[録音（Record）] ソフトキーまたはプログラム可能なライン キー（PLK）（電話モデル固有）が電話機でアクティブになります。コールの録音は現在のコールに対してのみ実行され、現在のコールが終了すると、録音が停止します。監察者が録音ソフトキーまたはPLK を押すと、録音ステータスを示すメッセージが電話機に表示されることがあります。

はじめる前に

（オプション） 自己署名証明書をルーティング サーバにエクスポートする，（659 ページ）

手順

ステップ 1 電話で録音を有効にするには、[電話の設定（Phone Configuration）] ウィンドウで [ビルトインブリッジ（Built-in Bridge）] を [オン（On）] に設定します。

ステップ 2 次のとおり録音プロファイルを作成します。

a) [デバイス（Device）] > [デバイスの設定（Device Settings）] > [録音プロファイル（Recording Profile）] の順に選択します。

b) 監察対象の会議を録音できる電話機に対してコール録音プロファイルを作成します。

ステップ 3 ライン アピアランスに録音プロファイルを適用します。

ステップ 4 レコーダーのポイントに SIP トランクを追加します。

ステップ 5 SIP トランクを指すルート パターンを作成します。

ステップ 6 次のサービス パラメータを設定します。

a) [監察ターゲットで録音通知トーンを再生する（Play Recording Notification Tone to Observed Target）]

b) [接続済み監察ターゲットで録音通知トーンを再生する（Play Recording Notification Tone to Observed Connected Target）]

ステップ 7 監察者が使用している電話機で標準監察用電話ソフトキー テンプレートを割り当てます。

ステップ 8 新しい電話機に対しては、[コール ルーティング（Call Routing）]>[電話番号（Directory Number）] を、または電話機がすでに設定されている場合は、[デバイス（Device）] > [電話（Phone）] から次の手順を実行します。

a) 監察者の電話機で電話番号（DN）を 1 つだけ設定します。

b) 監察者の電話機の DN に、[録音オプション（Recording Options）] ドロップダウン リストから [コールの録音をデバイスが開始する（Device Invoked Call Recording Enabled）] を選択します。

c) 監察者の電話機の DN に、[コールの最大数（Maximum Number of Calls）] 設定に 2 を入力し、[ビジー トリガー（Busy Trigger）] 設定に 1 を入力します。

ステップ 9 [録音（Record）] ソフトキーをサポートする Cisco Unified IP Phone の場合、標準監察用電話ソフトキー テンプレートを設定して、[会議（Conference）]、[録音（Record）]、[コール終了（End Call）] ソフトキーだけが接続状態の電話機に表示されるようにします。

ステップ 10 録音用プログラム可能なライン キー（PLK）をサポートする Cisco Unified IP Phone の場合、[電話ボタン テンプレートの設定（Phone Button Template Configuration）] ウィンドウで PLK を設定します。

ステップ 11 （任意） クラスタに複数の監察者がいる場合、監察ハント リストに割り当てる予定である監察者回線グループに監察者の DN を追加します。
この手順により、利用可能な監察者が必ず通話をモニタできます。

次の作業

（オプション） カスタマイズされたアナウンスの設定, （661 ページ）

カスタマイズされたアナウンスの設定

ルーティング ルールで、一部のコールでアナウンスを再生する必要があり、シスコ提供のアナウンスを使用しない場合には、この手順に従います。

ヒント アナウンス ID にスペースを使用しないでください。

他言語ロケールがインストールされている場合、アナウンス用に、それらのロケールと共に使用する他の .wav ファイルをアップロードできます。

手順

ステップ 1 Cisco Unified CM の管理から、[メディア リソース（Media Resources）] > [アナウンス（Announcement）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 新しいアナウンスを追加するには、次の手順を実行します。

a) [新規追加（Add New）] をクリックします。
b) [アナウンス ID（Announcement Identifier）] フィールドに、アナウンス ID を入力します。
c) [説明（Description）] フィールドに、アナウンスの説明を入力します。
d) [デフォルトのアナウンス（Default Announcement）] ドロップダウン リストから、必要に応じて、シスコが提供するデフォルトのアナウンスを選択します。
e) [保存（Save）] をクリックします。

- アナウンスにカスタム .wav ファイルをアップロードするには、次の手順を実行します。

a) [ファイルのアップロード（Upload File）] をクリックします。
b) [ロケール（Locale）] ドロップダウン リストから、そのアナウンス用のロケール言語を選択します。
c) [ファイルの選択（Choose File）] をクリックし、アップロードする .wav ファイルを選択します。
d) [ファイルのアップロード（Upload File）] をクリックします。
e) アップロードが終わったら、[閉じる（Close）] をクリックしてウィンドウを更新し、アップロードされたアナウンスを表示します。

外部コール制御の連携動作と制限事項

外部コール制御の連携動作

表 *77*：外部コール制御の連携動作

機能	データのやり取り
最適なコール品質のルーティング	コールに使用するゲートウェイを決定する付加ルート サーバにルーティング ルールを設定して、音声品質を考慮させることができます。たとえば、ゲートウェイ A が最適な音声品質を提供しているため、コールにはそれが使用されます。この場合、すべてのコール参加者に最高の音声品質を提供する音声ゲートウェイを介してコールがルーティングされるように、付加ルート サーバはネットワーク リンクの可用性、帯域幅の使用、遅延、ジッタ、平均オピニオン評点（MOS）値をモニタします。
コール詳細レコード	外部コール制御機能は、コール詳細レコードで表示できます。たとえば、コール詳細レコードは付加ルート サーバがコールを許可または拒否するかどうかを示すことができます。また、コール詳細レコードは、Cisco Unified Communications Manager が付加ルート サーバからの決定を受信しなかった期間にコールをブロックするか、または許可するかを示すこともできます。

機能	データのやり取り
コール転送	外部コール制御はトランスレーション パターン レベルでコールをインターセプトし、コール転送は電話番号レベルでコールをインターセプトします。外部コール制御はコール転送より高い優先順位を保持しています。外部コール制御プロファイルにトランスレーション パターンが割り当てられている場合、コール転送を呼び出すコールに関して、Cisco Unified Communications Manager は、ルーティング クエリを付加ルート サーバに送信します。コール転送は、付加ルート サーバが続行義務付きの許可決定を Cisco Unified Communications Manager に送信した場合にのみトリガーされます。 （注） 外部コール制御をサポートする [コール転送ホップ カウント（Call Diversion Hop Count）] サービス パラメータと、コール転送をサポートする [コール転送コール ホップ カウント（Call Forward Call Hop Count）] サービス パラメータは互いに独立しています。
コール ピックアップ（Call Pickup）	電話ユーザがコール ピックアップ機能を使用してコールのピックアップを試みた場合、外部コール制御は呼び出されません。Cisco Unified Communications Manager は、コールのその部分に関するルーティング クエリを付加ルート サーバに送信しません。
監察者（Chaperone）	監察者は、必要に応じて、コールへの会社のポリシーの通知、コールのモニタ、コールの録音を実行できる指名された電話ユーザです。コールに関与する参加者が監察者の存在なく通話できないように、監察者による制限が存在します。
Cisco Unified Mobility	Cisco Unified Communications Manager によって、次の Cisco Unified Mobility 機能に関する付加ルート サーバからのルート決定が許可されます。 • モバイル ボイス アクセス • エンタープライズ機能アクセス • Dial-via-Office リバース コールバック Cisco Unified Communications Manager は、次の Cisco Unified Mobility 機能について、ルーティング クエリを送信しません。 • 携帯電話ピックアップ • デスク ピックアップ • セッション ハンドオフ
電話会議	電話ユーザが電話会議を作成すると、プライマリ コールとコンサルタティブ コールに対して外部コール制御が呼び出されます。

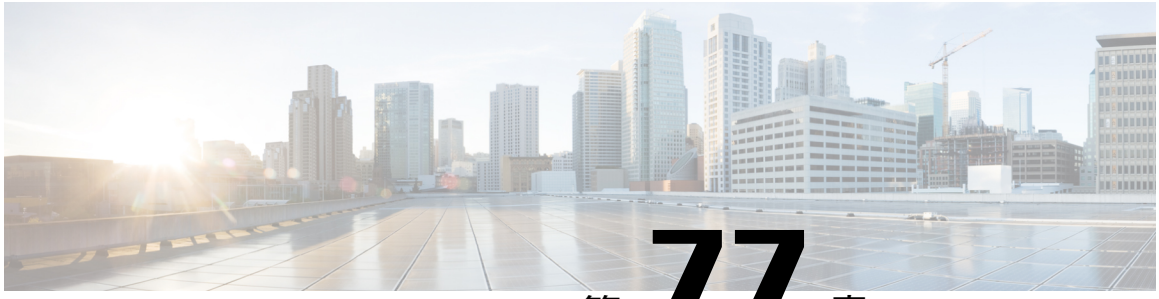
機能	データのやり取り
電話番号（Directory Numbers）	電話番号を 4 桁または 5 桁の内線番号（企業内線番号）として設定し、オンネット ダイヤリングが 4 または 5 桁をサポートしている場合は、2 つのトランスレーション パターンを設定する必要があります。1 番目のトランスレーション パターンは発信者番号と着信者番号のグローバル化をサポートし、2 番目のトランスレーション パターンは発信者番号と着信者番号のローカライズをサポートします。
サイレント	デフォルトでは、付加ルート サーバのユーザ ルールが、付加ルート サーバが続行義務を送信することを示している場合に、ユーザの DND 設定が有効となります。たとえば、付加ルート サーバが続行義務を送信せず、ユーザが DND-R を有効にした場合、Cisco Unified Communications Manager はコールを拒否します。
緊急通報の処理	**注意** 緊急通報の処理方法の手順をルート サーバに問い合わせる必要なく、コールが適切な接続先（たとえば、Cisco Emergency Responder またはゲートウェイ）にルーティングされるように、緊急通報については非常に明示的なパターン セット（たとえば、911 や 9.11）を設定することを強く推奨します。
転送	電話ユーザがコールを転送すると、外部コール制御がプライマリ コールとコンサルタティブ コールの両方に対して呼び出されることがあります。ただし、Cisco Unified Communications Manager は、転送元と転送先の間に、付加ルート サーバからのルーティング ルールを適用できません。

外線コール制御の制限事項

表 *78*：外線コール制御の制限事項

制約事項	説明
通話者の追加	監察者は、会議が始まった後に電話を使用して会議に参加者を追加することはできません。監察者が参加者を追加するには、コールを保留にする必要があるためです。 会議の他の通話者は、会議に通話者を追加できます。Cisco CallManager サービスをサポートする [高度なアドホック会議が有効（Advanced Ad Hoc Conference Enabled）] サービス パラメータの設定は、他の通話者が会議に参加者を追加できるかどうかを決定します。サービス パラメータを True に設定すると、他の通話者は会議に参加者を追加できます。
コール転送	監察者は電話を使用して他の通話者に会議コールを転送することはできません。

制約事項	説明
会議ログアウト	監察者が会議を出ると、会議自体が終了します。
会議のソフトキー	監察者が会議を作成すると、[会議（Conference）] ソフトキー（利用可能な場合）は電話機で無効になります。
保留	監察者は電話を使用して会議コールを保留にすることはできません。
録音（Recording）	この機能が会議に参加する通話者に相談コールを行う前に監察者が録音を開始した場合、Cisco Unified Communications Manager は監察者が相談コールを行う間録音を一時停止し、会議の確立後に録音を再開します。



第 77 章

コール キューイングの設定

- コール キューイングの概要，667 ページ
- コール キューイングの前提条件，669 ページ
- コール キューイング タスク フロー，669 ページ
- コール キューイングの連携動作と制限，679 ページ

コール キューイングの概要

Cisco Unified Communications Manager は、ハント メンバーが発信者に応答可能になるまで、発信者をキューに入れるためのコール キューイングを備えています。管理者は、コールがエージェントに接続される前に発信者が初期グリーティング アナウンスを受信するようにデフォルトを設定することも、発信者がキューに入った後にのみ初期アナウンスを再生し、続いて保留音または保留トーンが流れるようにデフォルトを変更することもできます。発信者が一定期間キューに残る場合、コールが応答されるか最長待機タイマーが期限切れになるまで、設定済みの間隔でセカンダリ アナウンスが再生され続けます。

着信コールがハント パイロットに到達すると、次の機能が提供されます。

- 発信者は、次の段階に進む前にカスタマイズ可能な初期グリーティング アナウンスに接続される場合があります。
- 1 つ以上の回線メンバーがハント パイロットにログインしており、アイドル状態でコールがキューに入れられていない場合、コールはアイドル状態が最長の回線メンバーに接続されます。
- 回線メンバーがコールに応答しない場合、発信者はキューには入りません。コールは、ハント メンバーが応答しない場合の設定（ログインまたは登録）に基づいて、新しい接続先にルーティングされるか、切断されます。
- キューが有効なコールに回線メンバーが応答しない場合、[回線グループ（Line Group）] 設定ウィンドウで [無応答時にハント メンバーを自動的にログアウト(Automatically Logout Hunt Member on No Answer)] が選択されているときのみ、回線メンバーはハント グループからログオフされます。

- コールは、すべてのメンバーが話中の場合のみキューに入れられます。
- キューで待機している発信者には、保留音が流され、（カスタマイズ可能で）定期的なアナウンスが繰り返される場合があります。
- 回線メンバーがアイドル状態になった後、複数のハント グループで待機時間が最長の発信者がアイドル状態の回線メンバーに接続されます。アイドル状態の回線メンバーがコールに応答しない場合、発信者はキュー内の以前の位置に戻されます。
- キューに入っているコールが最長待機時間を超過するか、またはキューで許容される最大発信者数を超えると、コールは、ハント パイロットの設定方法に応じて、代替番号にルーティングされるか、切断されます。代替番号は、次のいずれかになります。
  - キューイングが有効または無効のいずれかのハント パイロット DN
  - ボイスメール DN
  - 回線 DN
  - 共有 DN
- 回線メンバーは、キューが有効なハント パイロットのキュー ステータスを表示できます。キュー ステータス表示には、次のタイプの情報が含まれます。
  - ハント パイロット パターン
  - 各ハント パイロットのキューに入っている発信者数
  - 最長待機時間

コール キューイングは既存のハント パイロットと連携して動作しますが、ハント パイロットのキューイング機能の有無に関係なく、ハント操作の動作は同じです。コール キューイングが有効なハント パイロットは、次の機能を提供します。

- キューイングが有効なハント パイロットのコールの場合、回線メンバーは一度に 1 コールしか受信できません。キューイングが有効なハント パイロットの 2 つのコールを 1 つの回線メンバーに提供することはできません。回線メンバーは、DN への直接コール、またはキューイング機能のないハント パイロットからのコールを受信できます。
- ハント パイロットによってルーティングされたコールに応答しない回線メンバーは、自動的にログアウトされます。回線メンバーが、キューイングが有効なハント パイロットのコールを受信し、タイムアウトになる前にコールに応答しない場合、回線メンバーは自動的にデバイスからログアウトされます。共有回線を導入している場合は、同じ共有回線に設定されているすべてのデバイスがログアウトされます。この動作は、[回線グループ（Line Group）] 設定ウィンドウで、[無応答時にハント メンバーを自動的にログアウト(Automatically Logout Hunt Member on No Answer)] を選択することで、設定できます。回線メンバーは、このチェックボックスがオンの場合のみ、ログアウトされます。

コール キューイングのモニタリングとアナウンスのモニタリングの詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

着信コールが、キューイングが有効なハントパイロットのハントメンバーに接続されている間、キューイング アナウンスを再生する前に、そのコールの状態を接続済みに変更するように設定できます。

コール キューイングの前提条件

- クラスタ内の 1 つ以上のノードでアクティブ化されている Cisco IP Voice Media Streaming（IPVMS）Application
- クラスタ内の 1 つ以上のサーバで実行されている Cisco CallManager サービス
- Cisco CallManager サービスと同じサーバで実行されている Cisco RIS Data Collector サービス
- Cisco Unified Communications Manager ロケール インストーラ（英語以外の電話ロケールまたは国独自のトーンを使用する場合）。

コール キューイング タスク フロー

はじめる前に

アナウンスの設定

Cisco Unified Communications Manager により次の操作を実行できます。

- Cisco が提供する既存のアナウンスを使用する。
- 再生するアナウンスでメッセージやトーンを変更する。
- カスタム アナウンスの .wav ファイルを導入する。
- アナウンスのロケールを割り当てる。
- アナウンスの説明を変更する。
- 再生するアナウンスでメッセージやトーンを変更する。

機能アナウンスは、ハント パイロット コール キューイングや外部コール制御と連携した保留音（MOH）などの特定機能で使用されます。

最大 50 の機能アナウンスが利用できます。これらのアナウンスは、Cisco が提供するオーディオファイルまたはカスタム .wav ファイルをアップロードしたものです。

すべてのカスタム アナウンス .wav ファイルは、クラスタ内のすべてのサーバにアップロードする必要があります。

手順

ステップ 1 Cisco Unified Communications Manager で、[メディア リソース（Media Resource）] > [アナウンス（Announcements）] を選択します。
[アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウが表示されます。

ステップ 2 使用するアナウンスに対するハイパーリンクを選択します。

例：
ハイパーリンク：Wait_In_Queue_Sample
アナウンスの説明を編集する、またはアップロードした場合はカスタマイズしたアナウンスを選択できます。

ステップ 3 カスタム アナウンスとして使用するために .wav ファイルをアップロードするには、[ファイルのアップロード（Upload File）] をクリックします。
[ファイルのアップロード（Upload File）] ウィンドウが表示されます。

ステップ 4 [ファイルのアップロード（Upload File）] ウィンドウで、ロケールを選択し、ファイル名を入力するか、.wav ファイルを参照して選択してから[ファイルのアップロード（Upload File）] をクリックします。
アップロード プロセスが開始します。サイズによっては数分かかることがあります。処理が完了するとステータスが更新されます。

ステップ 5 [閉じる（Close）] をクリックして、アップロード ウィンドウを閉じます。
[アナウンスの設定（Announcement Configuration）] ウィンドウで、アップロードされたファイルのステータスが更新されます。

ステップ 6 カスタマイズされたアナウンスを再生するには、[アナウンスの設定（Announcement Configuration）] ウィンドウの [ロケールごとのアナウンス（Announcement by Locale）] ペインで [有効（Enable）] チェックボックスがオンであることを確認します。

ステップ 7 [アナウンスの設定（Announcement Configuration）] ウィンドウで変更を行った後、[保存（Save）] をクリックします。

次の作業

アナウンス ファイルはクラスタ内のサーバ間で反映されないため、クラスタ内の各ノードにアナウンスをアップロードする必要があります。クラスタ内の各サーバで [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] を開き、同じアップロード処理を実行します。

保留音の設定

保留音（MOH）を設定して、初めて保留したときにオプションで初期グリーティング アナウンスを再生したり、アナウンスを一定間隔で繰り返したりすることができます。これらのアナウンスにはシスコが提供するオーディオ ファイルまたはシステムにアップロードしたファイルのいずれかを使用できます。

保留音のオーディオ ソースを追加または更新する、既存のオーディオ ソースをオーディオ ストリーム番号に関連付ける、新しいカスタム オーディオ ソースをアップロードするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager で、[メディア リソース（Media Resources）]>[保留音のオーディオ ソース（Music On Hold Audio Source）] を選択します。
[保留音のオーディオ ソースの検索と一覧表示（Find and List Music On Hold Audio Sources）] ウィンドウが表示されます。

ステップ 2 新しい保留音のオーディオ ソースを追加するには、[新規追加（Add New）] をクリックします。
保留音のオーディオ ソースを更新するには、対象の保留音のオーディオ ソースを見つけます。指定した検索条件に基づいて、すべての条件に一致するものが検索結果として表示されます。

ステップ 3 保留音のオーディオ ソース フィールド, （671 ページ） の説明に従って、適切な設定を入力します。

ステップ 4 [保存（Save）] をクリックします。
ウィンドウ下部のリスト ボックスに新しい保留音のオーディオ ソースが表示されます。[MOH オーディオ ソース ファイル ステータス（MOH Audio Source File Status）] ペインに、追加されたソースに対する MOH オーディオ トランスレーション ステータスが表示されます。

保留音のオーディオ ソース フィールド

表 *79*：保留音のオーディオ ソース情報

フィールド	説明
[MOH オーディオ ストリーム番号（MOH Audio Stream Number）]	この MOH オーディオ ソースのストリーム番号を選択するには、このフィールドを使用します。ドロップダウン矢印をクリックし、リストから値を選択します。既存の MOH オーディオ ソースの場合、値は MOH オーディオ ソースのタイトルで表示されます。
[MOH オーディオ ソース ファイル（MOH Audio Source File）]	この MOH オーディオ ソースのファイルを選択するには、このフィールドを使用します。ドロップダウン矢印をクリックし、リストから値を選択します。
[MOH オーディオ ソース名（MOH Audio Source Name）]	MOH オーディオ ソースの一意の名前を、このフィールドに入力します。この名前には、文字、数字、スペース、ダッシュ、ドット（ピリオド）およびアンダースコアを含む、最大で 50 の有効な文字を使用できます。

フィールド	説明
[マルチキャストを許可（Allow Multicasting）]	選択したMOHオーディオ ソースのマルチキャストを許可するには、このチェックボックスをオンにします。
[MOH オーディオ ソース ファイル ステータス（MOH Audio Source File Status）]	このペインには、選択したMOHオーディオ ソースのファイルに関して、次の情報が表示されます。 • [InputFileName] • [ErrorCode] • [ErrorText] • [DurationSeconds] • [DiskSpaceKB] • [LowDateTime] • [HighDateTime] • [OutputFileList] • [MOH オーディオ変換の完了日（MOH Audio Translation completion date）] （注） [OutputFileList] には ULAW、ALAW、G.729 およびワイドバンド wav ファイルと、ステータス オプションについての情報が含まれます。

表 *80*：アナウンスの設定

フィールド	説明
[最初のアナウンス（Initial Announcement）]	ドロップダウン リストから最初のアナウンスを選択します。 （注） 最初のアナウンスを持たない MoH を選択するには、[選択なし（Not Selected）] オプションを選択します。 [詳細表示（View Details）] リンクをクリックすると、次のような最初のアナウンスの情報を参照できます。 • [アナウンス ID（Announcement Identifier）] • 説明 • [デフォルトのアナウンス（Default Announcement）] （注） • オーディオ ソースの [マルチキャストを許可（Allow Multi-casting）]“ ”のチェックがオフで、[再生される最初のアナウンス（Initial Announcement Played）]“ ”が [キューされたコールのみ（Only for queued calls）] に設定されている場合だけ、MOH サーバによって再生されます。 • [マルチキャストを許可（Allow Multi-casting）]“ ”のチェックがオンか、[再生される最初のアナウンス（Initial Announcement Played）]“ ”が [常時（Always）] に設定されている場合、ANN によって再生されます。
[再生される最初のアナウンス（Initial Announcement Played）]	次のうち 1 つを選択して、最初のアナウンスをいつ再生するかを決定します。 • [ハント メンバへのルーティング前にアナウンスを再生（Play announcement before routing to Hunt Member）] • [コールがキューに入る場合アナウンスを再生（Play announcement if call is queued）]

フィールド	説明
[定期アナウンス（Periodic Announcement）]	定期アナウンスをドロップダウン リストから選択します。 （注） 定期アナウンスを持たない MoH を選択するには、[選択なし（Not Selected）] オプションを選択します。 [詳細表示（View Details）] リンクをクリックすると、次のような定期アナウンスの情報を参照できます。 • [アナウンス ID（Announcement Identifier）] • 説明 • [デフォルトのアナウンス（Default Announcement）] （注） MOH サーバは、他の設定に関係なく常に定期アナウンスを再生します。
[定期アナウンスの間隔（Periodic Announcement Interval）]	定期アナウンスの間隔を指定する値（秒単位）を入力します。有効な値は 10 ～ 300 です。デフォルト値は 30 です。
[アナウンスのロケール（Locale Announcement）]	[アナウンスのロケール（Locale Announcement）] は、インストールされたロケール インストール パッケージによって異なります。 （注） • MoH が再生する音声ガイダンスは、[アナウンスのロケール（Locale Announcement）] の設定を使用します。 • ANN が再生する音声ガイダンスは、発信者側のユーザ ロケールを使用します。

表 *81*：保留音のオーディオ ソース

フィールド	説明
（MOHオーディオ ソースのリスト）	このリスト ボックスには、追加するMOHオーディオ ソースが表示されます。MOH オーディオ ソースを設定するには、その MOH オーディオ ソースのオーディオ ストリーム番号を選択します。 オーディオ ソース ID は、保留音サーバ内のオーディオ ソースを示す ID です。このオーディオ ソースには、ディスク上のファイルか、ソース ストリーム保留音サーバがストリーミング データを取得する固定デバイスのどちらかを含めることができます。MOH サーバは、最大で 51 のオーディオ ソース ID をサポートします。オーディオ ソース ID が示す各オーディオ ソースは、必要に応じてユニキャストおよびマルチキャスト モードでストリームできます。 （注） [<なし>（<None>）] を選択すると、MOH オーディオ ソースにはシステムのデフォルトである MOH オーディオ ソース サービス パラメータ（[デフォルトのネットワーク保留MoHオーディオソースID（Default Network Hold MoH Audio Source ID）]）が使用されます。

フィールド	説明
ファイルのアップロード（Upload File）	ドロップダウン リストに表示されていないMOHオーディオ ソース ファイルをアップロードするには、[ファイルのアップロード（Upload file）] をクリックします。[ファイルのアップロード（Upload File）] ウィンドウで、オーディオ ソース ファイルのパスを入力するか、[参照（Browse）] をクリックしてファイルを指定します。オーディオ ソース ファイルを指定した後、[ファイルのアップロード（Upload File）] をクリックしてアップロードを完了します。オーディオ ファイルがアップロードされた後、[アップロード結果（Upload Result）] ウィンドウにアップロードの結果が表示されます。[閉じる（Close）] をクリックして、このウィンドウを閉じます。 （注） ファイルをアップロードする際、ファイルは Cisco Unified Communications Manager サーバにアップロードされ、オーディオ変換が実行されて、MoHのための指定コーデックのオーディオ ファイルが作成されます。元のファイル サイズによっては、処理が完了するまで数分かかることがあります。 （注） MOHサーバにオーディオ ソース ファイルをアップロードする場合、ファイルは1つのMOHサーバのみにアップロードされます。各サーバの Cisco Unified CM の管理を使用して、クラスタ内の各 MOH サーバにオーディオ ソース ファイルをアップロードする必要があります。MOHオーディオ ソース ファイルは、クラスタ内の他の MOH サーバには自動で反映されません。

ハント パイロット キューイングの設定

ハントメンバーが一定時間で処理できるより多くのコールが、ハントパイロットに、コール分配機能を介して届いた場合、応答可能になるまで、キュー内のコールは、コール キューイングにより保留されます。

キューイングを有効にすると、[無応答時ハント転送（Forward Hunt No Answer）] と [話中ハント転送（Forward Hunt Busy）] の両方が自動的に無効になります。逆に、[無応答時ハント転送（Forward Hunt No Answer）] または [話中ハント転送（Forward Hunt Busy）] を有効にすると、キューイングが自動的に無効になります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM 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）] を選択し、ハント パイロットを設定します。

ステップ 2 キューイングに設定する必要があるハント パイロットを選択します。

ステップ 3 [ハント パイロットの設定（Hunt Pilot Configuration）] ウィンドウの [キューイング（Queuing）] セクションに移動します。

ステップ 4 キューイングを有効にするには、[コールのキューイング（Queue Calls）] チェックボックスをオンにします。

ステップ 5 アナウンスの再生とキューの保留処理のために使用されるドロップダウン リストボックスから保留音（MoH）ソースを選択します。
MOH ソースはユニキャストまたはマルチキャストとして設定できます。発信者側のメディア リソース グループ リスト（MRGL）では、マルチキャスト、ユニキャストに優先順位を設定します。

ソースを選択しない場合、デフォルトのネットワークによる保留 MoH/MoH ソースとアナウンスが使用されます。

MoH ソース アナウンス ロケールはアナウンスに使用する言語を判別するために使用されます。1 つのハント パイロットで再生できるのは、1 つの言語アナウンス タイプだけです。

ステップ 6 [キューに入れられる発信者の最大数（Maximum Number of Callers Allowed in Queue）] フィールドに、このハント パイロットでキューに入れられる発信者の最大数を整数で入力します。
デフォルト値は 32 です。値の範囲は 1 ～ 100 です。

ステップ 7 キューの発信者が最大数に達したとき、次のいずれかのオプションを選択します。

- 後につづくコールを切断する場合は、[コールを切断（Disconnect the call）] を選択します。
- 後につづくコールを 2 番目の接続先にルーティングする場合は、[コールをこの接続先にルーティングする（Route the call to this destination）] を選択します。特定のデバイス DN、共有回線 DN、または別のハント パイロット DN を入力します。
- （オプション）ドロップダウン リストから、[コーリング サーチ スペースの完全キュー（Full Queue Calling Search Space）] を選択できます。コールを完了するように試みるとき、検索するパーティションを判別するために使用されます。

ステップ 8 [キューの最大待機時間（Maximum Wait Time in Queue）] フィールドで、キューの最大待機時間を秒単位の整数値を入力します。
デフォルト値は 900 秒です。有効な範囲は 10 ～ 3600 秒です。

ステップ 9 最大待機時間に達したとき、次のいずれかのオプションを選択します。

- コールを切断する場合は、[コールを切断（Disconnect the call）] を選択します。
- コールを 2 番目の接続先にルーティングする場合は、[コールをこの接続先にルーティングする（Route the call to this destination）] を選択します。特定のデバイス DN、共有回線 DN、または別のハント パイロット DN を入力します。

- （オプション）ドロップダウン リストから、[コーリング サーチ スペースの最大待機時間（Maximum Wait Time Calling Search Space）] も選択できます。コールを完了するように試みるとき、検索するパーティションを判別するために使用されます。

ステップ 10 回線メンバーがログ インしていない、または着信コール時に登録されていないとき、次のオプションのいずれかを選択します。

- コールを切断する必要がある場合は、[コールを切断（Disconnect the call）] を選択します。
- コールを 2 番目の接続先にルーティングする必要がある場合は、[コールをこの接続先にルーティングする（Route the call to this destination）] を選択します。特定のデバイス DN、共有回線 DN、または別のハント パイロット DN を入力します。
- （オプション）ドロップダウン リストから [ハント メンバーがコーリング サーチ スペースに登録またはログ インしていない（No hunt members logged in or registered Calling Search Space）] を選択することもできます。コールを完了するように試みるとき、検索するパーティションを判別するために使用されます。

ステップ 11 [保存（Save）] をクリックします。

無応答時のハント メンバーの自動ログアウト

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [回線グループ（Line Group）] を選択し、回線グループを設定します。

ステップ 2 設定する必要がある回線グループを [回線グループの検索と一覧表示（Find and List Line Group）] ウィンドウから選択します。

ステップ 3 [回線グループの設定（Line Group Configuration）] ウィンドウの [ハント オプション（Hunt Options）] セクションに移動します。

ステップ 4 [無応答時にハント メンバー自動的にログアウトする（Automatically Logout Hunt Member on No Answer）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

コール キューイングの連携動作と制限

コール キューイングの連携動作

機能	データのやり取り
[SIP Rel1XX オプション（SIP Rel1XX Options）]	コールが SIP ICT を通じてキューイング対応ハント パイロットにルーティングされる場合、SIP ICT は、SIP Rel1XX オプションが [1XX に SDP が含まれる場合 PRACK を送信（Send PRACK if 1XX contains SDP）] に設定されている SIP プロファイルを使用します。その結果、コールが回線メンバに接続される前に、コールごとに最初の通知が再生されます。 SIP ICT に対する上記のインタラクションは、Cisco Unified CM Administration で [デバイス（Device）] [デバイス設定（Device Settings）] [SIPプロファイル（SIP Profile）] > [トランク固有の設定（Trunk Specific Configuration）] で [キューイング通知を再生する前に着信コールを接続（Connect Inbound Call before Playing Queuing Announcement）] チェックボックスがオンの場合には適用されません。 [キューイング通知を再生する前に着信コールを接続（Connect Inbound Call before Playing Queuing Announcement）] チェックボックスがオフである場合でも、SIP ICT のインタラクションは変わりません。ただし、PSTN 側の発信者向けに最初の通知が必ず再生されることは保証されません。PSTNプロバイダーがコール時に接続メッセージを受信するまで音声パスを開かない場合、最初の通知が PSTN 側の発信者向けに再生されることはありません。

機能	データのやり取り
ハント パイロットおよびハント グループ	• ハント グループのログオフ通知機能は、コール キューイングがハント パイロットでイネーブルになったときに変化します。コール キューイングがハント パイロットでイネーブルになると、ユーザがハント グループをログアウトまたはログオフしても、ハント グループのログオフ通知は再生されません。これは、キュー内で順番を失ったためです。 • ハント リストに複数の回線グループがある場合、これらの回線グループは [無応答時にハント メンバを自動的にログアウト（Automatically Logout Hunt Member on No Answer）] が同じ設定である必要があります。 • すべてのハント オプションは、[次のメンバへ、その後ハントリスト内の次のグループへ（Try Next Member; Then, Try Next Group in Hunt List）] に設定する必要があります。

コール キューイングの制約事項

次の一般的な制限は、発信のキューイングに適用されます:

- H.323 Fast Start は発信のキューイングをサポートしません。
- キューのステータス PLK がサポートされているのは、SCCP および SIP の両方で次の LCD 表示の電話だけです：6921、6941、6945、6961、7911G、7931G、7942G、7945G、7962G、7965G、7975G、8961、8945、8941、9951、9971。
- ハント グループ（HLog）からのログアウトは、Cisco Extension Mobility Cross Cluster（EMCC）とは互換性がありません。コール キューイングは EMCC とともに導入することはできません。
- Cisco Unified Communications Manager は、コール キューイングの Unified Mobility をサポートしていません。
- H323 から SIP へのインターワーキング シナリオでは、インターワーキング遅延のために、ユーザがネイティブ コール キューイング フローで初期アナウンスメント、MoH、定期アナウンスを聞いたり、コール失敗を見ることがないことがあります。このようなシナリオでは、SIP プロトコルだけを使用することを勧めします。

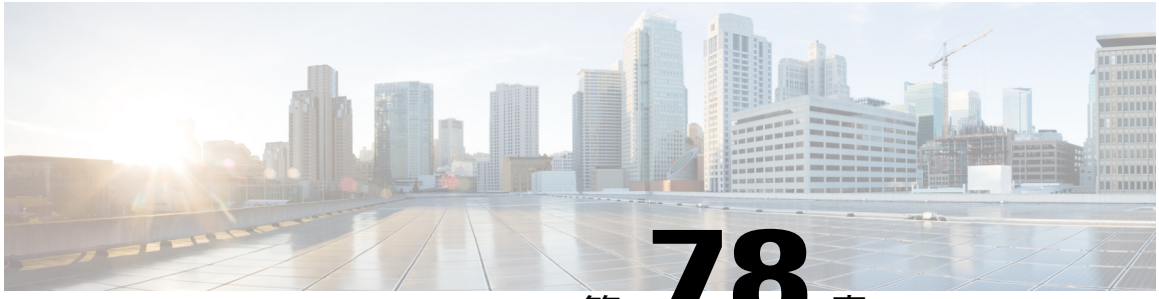
コール キューイングが有効なハント パイロットのパフォーマンスと拡張性

次のパフォーマンスと拡張性の制限事項が適用されます。

- 単一の Unified CM クラスタは、最大 15,000 のハント リスト デバイスをサポートします。
- 単一の Unified CM サブスクライバは、コール キューイングが有効になっている状態でノードごとに最大 100 のハント パイロットをサポートします。
- ハント リスト デバイスは、各ハント リストに 10 台の IP フォンを含む 1500 のハント リスト、各ハント リストに 20 台の IP フォンを含む 750 のハント リストの組み合わせ、または同様の組み合わせにすることができます。

（注） コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハント リスト デバイスの数は、Busy Hour Call Attempts（BHCA）の数によって制限されます。ブロードキャスト アルゴリズムを使用して、10 台の電話機を含むハント リストまたはハント グループを指すハント パイロットに対して 10 回の BHCA を行うことは、10 回の BHCA を行う 10 台の電話機と同じです。

- 各ハント パイロットのキューに設定できる同時発信者の最大数は 1 ～ 100 です（デフォルトは 32）。
- 各ハント パイロットのキューに設定できる最大待機時間は 0 ～ 3600 秒です（デフォルトは 900）。ハント リストの数が増えると、Unified Communications Manager のサービス パラメータで指定するダイヤル プラン初期化タイマーの値を大きくする必要があります。1500 のハント リストを設定している場合は、ダイヤル プラン初期化タイマーを 600 秒に設定することを推奨します。
- コール キューイングとともにブロードキャスト アルゴリズムを使用している場合は、単一の回線グループに対して 35 を超える電話番号を設定しないでください。また、ブロードキャスト回線グループの数は、Busy Hour Call Completion（BHCC）レートによって異なります。Unified CM システム内に複数のブロードキャスト回線グループがある場合、1 回線グループの電話番号の最大数は 35 未満にする必要があります。すべてのブロードキャスト回線グループの最繁時呼数（BHCA）の数が、1 秒あたり 35 コール セットアップを超えないようにします。



第 78 章

コール スロットリングの設定

- コール スロットリングの概要，683 ページ
- コール スロットリングの設定，684 ページ

コール スロットリングの概要

コール スロットリングによって、システムは新しいコール試行を自動的にスロットルまたは拒否できます。このアクションは、ユーザがオフフックからダイヤル トーンを聴取するまでに遅延を認識するようになる状況で実行されます。

この遅延を引き起こす可能性があるいくつかの要因は、次のとおりです。

- 過度なコール アクティビティ
- 低い CPU の可用性
- ルーティング ループ
- ディスク I/O の制限
- ディスク フラグメンテーション

システムはコール スロットリング パラメータに指定された値を使用して、ダイヤル トーンに遅延が生じている可能性があるかどうかを判別し、状況に応じてそれ以上コール スロットリングが必要なくなるタイミングも判別します。

ダイヤル トーンの過度な遅延を防ぐためにスロットリングが必要な場合、システムはCode Yellow状態に切り替わり、新しいコール試行をスロットル（拒否）します。

コール スロットリング サービス パラメータに設定されたしきい値を超えたために、システムがダイヤルトーンの遅延を計算すると、Cisco Unified Communications Manager は新しいコールを拒否します。コール スロットリングを有効化すると、新しいコールを試みたユーザはリオーダー音を受信します。電話のモデルに応じて、電話機のディスプレイにプロンプトが表示される場合もあります。

コール スロットリングは、ユーザがシステム管理者に不満を言ったり、システムのダウンや電話の破損ではないかと疑問を抱かせたりすることのある過度な遅延のタイプを効果的に防ぎます。このような遅延が発生するタイミングを予測するため、システムは常にシステムをモニタしています。

ダイヤル トーンの遅延がコール スロットリング サービス パラメータのガイドライン内である場合、Cisco Unified Communications Manager は、Code Yellow 状態を終了することでコールのスロットルを停止し、新しいコールは再び許可されます。

コール スロットリングの設定

注意 コール スロットリング パラメータは、カスタマー サポートに指示された場合を除き、変更しないことを推奨します。

コールスロットリングは、システムが過負荷なコールアクティビティ、低いCPUの可用性、ディスク フラグメンテーションなどの状況を検出すると自動的に発生します。これらの状況が修正されると、システムはスロットリングを自動的に終了します。

関連トピック

コール スロットリング サービス パラメータ, （684 ページ）

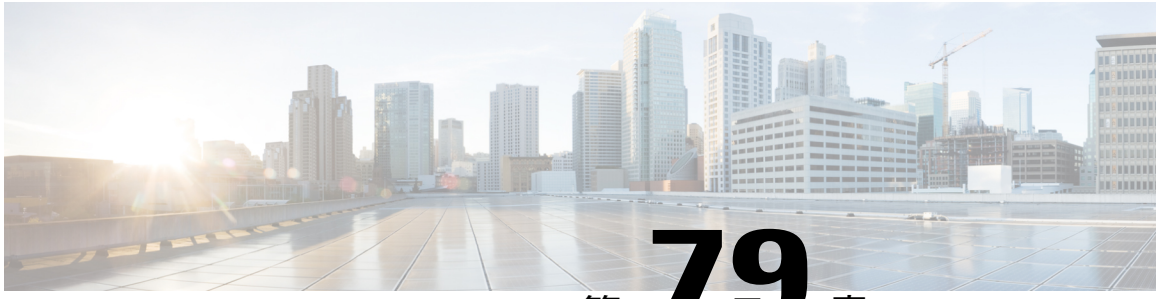
コール スロットリング サービス パラメータ

表 *82* : コール スロットリング サービス パラメータ

サービス パラメータ	説明
Code Yellow Entry Latency	システム内のさまざまなデバイスによって Cisco Unified Communications Manager に送信されるシステム診断レイヤー（SDL）メッセージを処理するための最大許容遅延（ミリ秒単位）を定義します。この最大値は、キープアライブ インターバルや変更通知などのさまざまなアクティビティに関して Cisco Unified Communications Manager によって送受信される内部メッセージにも適用されます。計算された平均予測遅延がこのサービス パラメータで指定した値を超えた場合、システムは Code Yellow 状態に切り替わり、コール スロットリングを開始して新しいコールの受け入れを停止します。

サービス パラメータ	説明
Code Yellow Exit Latency Calculation	Cisco Unified Communications Manager がコール スロットリングを開始した後に Code Yellow 状態（コール スロットリング）を離脱する終了基準を指定するため、Code Yellow Entry Latency の許容可能なパーセンテージを決定します。 このパラメータに指定する値は、Code Yellow Entry Latency パラメータ（ミリ秒単位で測定された遅延）の値を使用する式から導き出されます。 パーセンテージを求めるには、次の式を使用します。 Code Yellow Entry Latency 値に、Code Yellow Exit Latency 値を乗算します。 次に例を示します。 • Code Yellow Entry Latency サービス パラメータ値：20 ミリ秒 • Code Yellow Exit Latency サービス パラメータ値：40% • Code Yellow Exit Latency 値 = 20 X 0.4 = 8 ミリ秒。つまり、Cisco Unified Communications Manager は、計算されたメッセージ遅延が 8 ミリ秒以下になると、Code Yellow 状態を終了します。 Code Yellow 状態を終了するため、Cisco Unified Communications Manager は平均予測遅延が Code Yellow Exit Latency の値を下回っていることを確認します。
Code Yellow Duration	Cisco Unified Communications Manager システムが Code Yellow 状態（コール スロットリング）を持続できる分数を指定します。 この期間が経過しても、システムが引き続き Code Yellow 状態の場合、Cisco Unified Communications Manager は Code Red 状態に切り替わり、Cisco Unified Communications Manager が Code Yellow 状態のままである期間が延長され、回復できないことを示します。 Cisco Unified Communications Manager が Code Red 状態になると、Communications Manager サービスが再起動し、メモリ ダンプも生成されるため、障害の分析に役立つことがあります。

サービス パラメータ	説明
System Throttle Sample Size	Cisco Unified Communications Manager が SDL メッセージを処理するための平均予測遅延の計算に使用されるサンプルサイズ（秒単位）を示します。 たとえば、サンプル サイズ 10 は、Cisco Unified Communications Manager が、平均予測遅延を計算して、それを CodeYellow Entry Latency パラメータの値と比較する前に、連続する 10 秒間にゼロ以外の遅延値を計算する必要があることを示しています。 このパラメータを使用してコール スロットリングを無効化できます。



第 79 章

発信側の正規化

この章では、発信側の正規化機能について説明します。発信側の正規化によって、発信者番号の表示を国際標準化国番号などのプレフィックスを含むグローバル化されたバージョンに再形式化したり、発信者番号を着信側の電話に表示するローカライズ版にローカライズしたりできます。

- 発信側の正規化の概要，687 ページ
- 発信側の正規化の前提条件，688 ページ
- 発信側の正規化の設定タスク フロー，689 ページ
- 発信側の正規化の連携動作と制約事項，694 ページ

発信側の正規化の概要

発信側の正規化によって、電話番号のグローバル化とローカライズが可能になるため、電話に適切な表現で発信側が表示されます。発信側の正規化は、一部の電話のダイヤル機能を拡張し、コールが複数の地理的場所にルーティングされたときのコールバック機能を改善します。この機能によって、グローバル発信者番号をローカライズされた番号にマッピングできるため、電話は電話の通話履歴ディレクトリ内の電話番号を変更することなく、コールバックできます。

発信者番号のグローバリゼーション

Cisco Unified CM の管理で [発信者番号タイプ（Calling Party Number Type）] とプレフィックスを設定することで、着信側の電話に表示する発信者電話番号を、（国際国番号などのプレフィックスを含むグローバル化バージョンに）再フォーマットするように Cisco Unified Communications Manager を設定できます。それによって、世界中のどこからでもその番号をダイヤルできます。

Cisco Unified Communications Manager は、[発信者番号タイプ（Calling Party Number Type）] の値とともにルートパターンやトランスレーションパターンなどのさまざまな番号パターンを使用して、電話番号をグローバル化できます。たとえば、Cisco Unified Communications Manager は、サブスクライバ発信者番号タイプのローカライズされたドイツの電話番号 069XXXXXXX を、ドイツの国番号と都市コードを含む +49 40 69XXXXXXX にグローバル化するように設定できます。

複数の地理的場所にルーティングされるコールの場合、各ルーティング パスに適用される異なるトランスレーション設定によって、発信者番号は各コール パスで一意にグローバル化できます。Cisco Unified Communications Manager では、電話でローカライズされた発信者番号を電話画面に表示し、グローバル化された番号を電話の通話履歴ディレクトリに表示するように設定することもできます。電話ユーザがコールを発信する前に、電話の通話履歴ディレクトリのエントリを編集する必要がないようにするため、グローバル発信者番号をそのローカル バージョンにマッピングします。

発信者番号のローカリゼーション

発信者番号の最終表示用に、発信者番号タイプ（国内、国際、サブスクライバ、不明）ごとに発信側トランスフォーメーション パターンを設定し、そのコールの発信者番号タイプに固有のストリップ桁数とプレフィックスの手順を適用できます。これによって、Cisco Unified Communications Manager は、着信側の電話に表示される発信者番号が不要な国コードや国際アクセス コードを含まないローカライズされた番号となるように、発信者番号を再フォーマットできます。

たとえば、PSTN から到着した着信番号が、グローバル化された番号 +49 40 69XXXXXXX で（+49 が国番号、40 が都市コードを表す）、発信者番号タイプがサブスクライバであるとします。Cisco Unified Communications Manager には、国番号、都市コードを取り除き、プレフィックス 0 を追加する手順とともに、発信側のトランスフォーメーション パターンを設定できます。手順が適用された後、発信者番号はダイヤルされた電話に 069XXXXXXX として表示されます。

グローバル化された発信者番号のローカライズ バージョンへのマッピング

電話ユーザがコールを発信する前に、電話の通話履歴ディレクトリのエントリを編集する必要がないようにするため、ルートパターンと着信側トランスフォーメーションパターンを使用して、グローバル発信者番号をローカライズされたバージョンにマッピングできます。これによって、着信側がコールを返す場合に、Cisco Unified Communications Manager は確実に正しいゲートウェイにコールをルーティングできます。

グローバル発信者番号のマッピングによって、コールバック機能が改善され、着信側は電話の通話履歴ディレクトリ内の電話番号を変更する必要なく、コールバックできます。

発信側の正規化の前提条件

発信側の標準化を設定する前に、Cisco Unified Serviceability で Cisco CallManager サービスをアクティブにしてください。詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Cisco Unified Communications Manager に発信者番号タイプを判別させるには、想定するコールに一致する [発信者番号タイプ（Calling Party Number Type）] 値を割り当てるパターンを設定します。次の設定ウィンドウでパターンを作成して適用できます。

- ルート パターン
- ハント パイロット
- トランスレーション パターン

- 発信者番号のトランスレーション パターン

（注） 発信者番号のトランスレーションは、元の発信者を使用する場合のみ機能します。転送番号への変更は、転送ヘッダーにのみ影響を及ぼします。SIP トランクの章の設定を確認し、SIP トランク自体に転送ヘッダーを追加します。

発信側の正規化の設定タスク フロー

発信側の正規化のプレフィックスおよび削除桁数ルールは、Cisco Unified Communications Manager でさまざまな方法で適用できます。たとえば、デバイスプール、ルートパターン、トランスレーションパターン、ハントパイロット、ゲートウェイ、およびトランクに桁数の変換を適用できます。桁数の変換を適用する方法は、ダイヤル プラン、デバイス、およびトランクの導入方法に応じて変わります。詳細については、ダイヤル プラン、ルート パターン、トランスレーション パターン、およびトランスフォーメーション パターンに関連するトピックを参照してください。

はじめる前に

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Communications Manager で発信者番号タイプを決定する場合は、パターンを作成して、予測されるコールと一致する発信者番号タイプを設定します。次の設定ウィンドウで、パターンを作成して適用できます。 • ルート パターン • ハント パイロット • トランスレーション パターン • 発信者番号トランスフォーメーション パターン	
ステップ 2	発信側番号のグローバル化, （690 ページ）	PSTN を介した着信コールについては、発信者番号をグローバル化する設定を実行します。
ステップ 3	コーリング サーチ スペースの設定, （691 ページ）	パーティションとコーリング サーチ スペースを設定します。

	コマンドまたはアクション	目的
ステップ 4	発信側トランスフォーメーション パターンの作成, （691 ページ）	発信者番号をグローバル化またはローカライズされたバージョンに変換して各パターンをパーティションに割り当てる、発呼側トランスフォーメーション パターンを作成します。
ステップ 5	コーリング サーチ スペースへの発信側トランスフォーメーション パターンの適用, （692 ページ）	デバイス プール、ゲートウェイ、トランクなどのデバイスに発着信側トランスフォーメーション CSS を適用します。

発信側番号のグローバル化

PSTN 経由で到達する着信コールの場合は、発信者番号をグローバル化する設定を行います。発信者番号をグローバル化し、それをデバイス プールまたは個々のデバイスに適用する設定できます。また、クラスタ全体に、発信者番号の正規化設定を適用するサービス パラメータを設定できます。

発信者番号をグローバル化するには、次の手順を実行します。

手順

ステップ 1 発信者番号の正規化設定を特定のデバイスに適用するには、次の手順を実行します。

a) 設定を適用するデバイスの設定ウィンドウを開きます。たとえば、デバイス プール、ゲートウェイ、電話、トランクです。

b) 設定ウィンドウの着信発呼者設定セクションで、各発信者番号タイプのプレフィックスおよび strip digit の指示を適用します。

（注） Cisco Unified Communications Manager には、コール転送、コール パーク、ボイス メッセージング、CDR データなどの補足サービスのような、すべての追加アクションの発信者番号フィールドにプレフィックスが含まれます。

ステップ 2 サービス パラメータを使用して、クラスタ全体のすべてのデバイスの発信者番号をグローバル化する場合には、次の手順を実行します。

a) Cisco Unified CM の管理から、[システム（System）] > [サービス パラメータ（Service Parameters）] の順に選択します。

b) [サーバ（Server）] ドロップダウン リストから、サービスを実行するサーバを選択します。

c) [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

d) [詳細設定（Advanced）] をクリックします。

e) 以下のパラメータの値を設定します。この値は、クラスタ全体から電話、MGCP ゲートウェイ、H.323 ゲートウェイに適用できます。

- [着信発呼者の国内番号プレフィックス（Incoming Calling Party National Number Prefix）]
- [着信発呼者の国際番号プレフィックス（Incoming Calling Party International Number Prefix）]
- [発呼側の不明な着信番号プレフィックス（Incoming Calling Party Unknown Number Prefix）]
- [着信発呼者の加入者番号プレフィックス（Incoming Calling Party Subscriber Number Prefix）]

（注） Cisco Unified Communications Manager で、特定の電話のクラスタ全体のサービス パラメータ設定を適用するには、デバイスとデバイス プール レベルの両方で、その電話のプリフィックス設定をデフォルト オプションに設定する必要があります。

次の作業

コーリング サーチ スペースの設定, （691 ページ）

コーリング サーチ スペースの設定

コーリング サーチ スペースを設定して発信側の正規化機能を処理する場合は、次の手順を使用します。

はじめる前に

発信側番号のグローバル化, （690 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partitions）] の順に選択します。

ステップ 2 ネットワークのパーティションを作成します。

ステップ 3 Cisco Unified CM の管理で、[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）] の順に選択します。

ステップ 4 発呼側トランスフォーメーション パターンのコーリング サーチ スペースを作成します。

ステップ 5 コーリング サーチ スペースごとに、パーティションをコーリング サーチ スペースに割り当てます。

次の作業

発信側トランスフォーメーション パターンの作成, （691 ページ）

発信側トランスフォーメーション パターンの作成

発信側の正規化機能を処理するために発信側トランスフォーメーション パターンを設定している場合、次の手順を使用します。

はじめる前に

コーリング サーチ スペースの設定, （691 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、[コール ルーティング（Call Routing）] > [トランスフォーメーション パターン（Transformation Pattern）] > [発信側トランスフォーメーション パターン（Calling Party Transformation Pattern）] を選択します。

ステップ 2 トランスフォーメーション パターンを作成します。

ステップ 3 作成する発信側トランスフォーメーション パターンそれぞれには、発信側番号を国際対応または国内対応するために、先頭に付加または除外している番号コマンドを割り当てます。

ステップ 4 それぞれの発信側トランスフォーメーション パターンには、コーリング サーチ スペースの 1 つに関連付けられているパーティションを割り当てます。

次の作業

コーリング サーチ スペースへの発信側トランスフォーメーション パターンの適用, （692 ページ）

コーリング サーチ スペースへの発信側トランスフォーメーション パターンの適用

デバイス プール、ゲートウェイ、トランクなどのデバイスに、着信する発信側トランスフォーメーション CSS を割り当てます。

はじめる前に

発信側トランスフォーメーション パターンの作成, （691 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、発信側トランスフォーメーションを適用するデバイスに該当する設定ウィンドウを選択します。

- ゲートウェイ
- トランク
- Device Pools

ステップ 2 発信者番号をローカライズするには、[コーリング サーチ スペース（Calling Search Space）] ドロップダウン リスト ボックスで、適用する発信側トランスレーション パターンを含む CSS を選択します。

（注） デバイス プールに対して CSS を設定する場合、電話機にもそのデバイス プールを適用する必要があります。

ステップ 3 発信者番号をグローバル化するには、[着信の発信者番号設定（Incoming Calling Party Settings）] セクションで、適用する発信側トランスレーション パターンを含むコーリング サーチ スペースを選択します。

発信側の正規化サービス パラメータの例

次のサービス パラメータは、電話、MGCP ゲートウェイ、または H.323 ゲートウェイの基盤となるクラスタ全体に適用できます。特定のデバイスでクラスタ全体のパラメータが使用されるようにするには、デバイス設定のプレフィックスをデフォルトの : に設定する必要があります。

- 着信発呼者の国内番号プレフィックス（Incoming Calling Party National Number Prefix）
- [着信発呼者の国際番号プレフィックス（Incoming Calling Party International Number Prefix）]
- [発呼側の不明な着信番号プレフィックス（Incoming Calling Party Unknown Number Prefix）]
- 着信発呼者のサブスクライバ番号プレフィックス（Incoming Calling Party Subscriber Number Prefix）

次の表に、プレフィックスとストリップの桁数の設定例と、発信者番号の表示を変換するためにこれらの値をどのように使用できるかを示します。サービス パラメータの設定では、コロンの後の番号が発信者番号の先頭から取り除く桁数を表し、コロンの前の数字は発信者番号の先頭に追加されるプレフィックスを表します。

表 *83* : 発信側番号の正規化サービス パラメータの例

元の発信者番号	[サービスパラメータ値（**Service Parameter Value**）]	説明	最終的な発信者番号
04423452345	+:1	先頭 1 桁を取り除き、プレフィックスとして + を追加します	+4423452345
04423452345	:2	先頭 2 桁を取り除きます	423452345
552345	+1:6	先頭 6 桁を取り除き、プレフィックスとして +1 を追加します	+1
552345	+1:8	使用可能な桁数より多くの桁数が取り除かれるため、最終的な番号は空白になります	

元の発信者番号	[サービスパラメータ値（Service Parameter Value）]	説明	最終的な発信者番号
552345	123	プレフィックスとして 123 を追加します	123552345
空白	+1:2	発信者番号が空白の場合、プレフィックスは適用されません	空白
0442345	:26	発信者番号の正規化で取り除くことができる桁数は、24 桁のみです	Cisco Unified Communications Manager では、この設定は許可されません

発信側の正規化の連携動作と制約事項

発信側の正規化の連携動作

次の表は、発信側の正規化機能と連携動作する機能について説明しています。

機能	データのやり取り
転送コール（Transferred Calls）	転送機能がミッドコール更新に依存しており、発信側の正規化は各コール ホップの初期コール セットアップ時に実行されるため、一部の転送されたコールのシナリオでは発信側の正規化がサポートされていない場合があります。以下に、発信側の正規化が転送のためにどのように動作するかについて、一例を示します。 内線番号が 12345 で電話番号が 972 500 2345 の電話 A が、内線番号が 54321 で電話番号が 972 500 4321 の電話 B にコールを発信します。電話 B では、発信者番号 12345 が表示されますが、電話 B はそのコールをサンノゼのゲートウェイ経由で電話 C に転送します。初期転送時に、電話 C には発信者番号 972 500 4321 が表示されますが、転送の完了後は、電話 C には 12345 として電話 A の発信者番号が表示されます。

機能	データのやり取り
転送されたコール	転送されたコールは、発信者番号のグローバリゼーションとローカリゼーションをサポートします。たとえば、電話 F の発信者が PSTN 経由でダラスの電話 G にコールを発信しますが、電話 G はサンノゼの電話 H にコールを転送します。着信したダラスのゲートウェイでは、555-5555/Subscriber として発信者番号が表示されますが、コールはサンノゼのゲートウェイに転送されます。ダラスからの発信コールは、972 555 5555 として表示されます。着信したサンノゼのゲートウェイでは、+1 がプレフィックスとして付加され、電話 F には発信者番号として +1 972 555 5555 が表示されます。
コール詳細レコード	発信側の正規化が CDR レコードと連携動作する方法の詳細については、『*Cisco Unified Communications Manager Call Detail Records Administration Guide*』を参照してください。
Cisco Unified Communications Manager Assistant	発信側の正規化機能が設定されている場合、Cisco Unified Communications Manager Assistant はローカライズされたコールとグローバル化されたコールを自動的にサポートします。Cisco Unified Communications Manager Assistant は、ユーザインターフェイスにローカライズされた発信者番号を表示できます。また、マネージャ宛ての着信コールでは、フィルタパターンに一致する場合に、Cisco Unified Communications Manager Assistant はローカライズされた発信者番号とグローバル化された発信者番号を表示できます。Cisco Unified Communications Manager Assistant の設定方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

機能	データのやり取り
Cisco Unity Connection	Cisco Unity Connection は、国際番号用エスケープ文字（+）をサポートしていません。そのため、ボイス メッセージング機能が予期したとおり動作するように、Cisco Unity Connection へのコールに + が含まれていないことを確認する必要があります。 Cisco Unity Connection を予期したとおりに動作させるために、このアプリケーションをデバイスとして扱い、+がこのボイスメッセージングアプリケーションに送信されないようにする発信側トランスフォーメーションを設定します。Cisco Unity Connection サーバが北米ベースのダイヤル プランを使用する場合は、Cisco Unity Connection が発信者番号を受信する前に、発信者番号を NANP 形式にローカライズします。発信側トランスフォーメーション オプションは、ボイス メッセージング ポートの Cisco Unified Communications Manager の管理には存在しないため、必ず、ボイスメッセージング ポートに関連付けられたデバイス プールに発信者番号トランスフォーメーションを設定してください。発信者番号をローカライズするには、ボイスメッセージング アプリケーションが、ライブ応答などの特定の機能の番号を簡単にリダイヤルできるように、アクセス コードのプレフィックスを追加することも検討します。たとえば、+12225551234 を 912225551234 に変換できます。さらに、国際番号 +4423453456 を国際番号用エスケープ コードを含めて 90114423453456 に変換できます。
デバイス モビリティ	ローミング デバイス プールの発信側トランスフォーメーション CSS は、電話の設定ウィンドウの[デバイスプールの発信側トランスフォーメーション CSS を使用（Use Device Pool Calling Party Transformation CSS）]チェックボックスがオフのままの場合でも、同じデバイス モビリティ グループ内でローミングしている電話のデバイスレベルの設定をオーバーライドします。 次の例は、発信側の正規化が、現在サンノゼ内でローミングしており、ダラスをホームの場所としている電話のデバイス モビリティとどのように連携動作するかを示しています。 電話がサンノゼ内でローミングしている場合、コールはダラス内の 972 500 1212 <National> から PSTN を経由します。着信したサンノゼのゲートウェイで、発信者番号はグローバル形式の + 1 408 500 1212 に変換されます。現在サンノゼ内にある電話では、発信者番号は 1 972 500 1212 として表示されます。 電話がサンノゼ内でローミングしている場合、コールはサンノゼの 7 桁のダイヤリング エリアの 500 1212 <Subscriber> から PSTN を経由します。着信したサンノゼのゲートウェイで、発信者番号はグローバル形式の + 1 408 500 1212 に変換されます。現在サンノゼ内にある電話では、発信者番号が 9 500 1212 として表示されます。

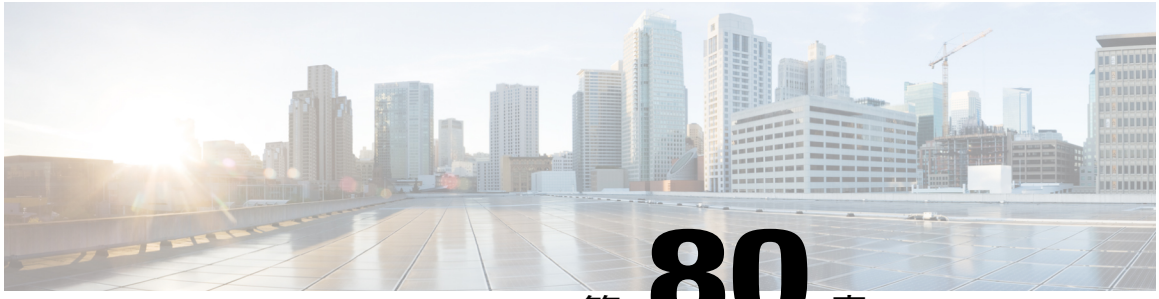
発信側の正規化の制約事項

次の表に、Calling Party Normalization 機能が特定の機能に持つ制約事項と、Cisco Unified Communications Manager のシステム コンポーネントを示します。

表 *84*：***Calling Party Normalization*** の制約事項

機能	制約事項
共有回線	共有回線を表示する発信側番号は、Cisco Unified Communications Manager のコール制御イベントのシーケンスに依存します。共有回線上で不適切にローカライズされた発信者番号が表示されることを避けるには、特に共有回線が地理的に異なる場所で発生する場合、同じ回線を共有するさまざまなデバイスで同じ発呼側トランスフォーメーション CSS を設定してください。
SIP トランクと MGCP ゲートウェイ	SIP トランクと MGCP ゲートウェイは、コールへの国際エスケープ文字（+）の送信をサポートします。H.323 ゲートウェイは + をサポートしていません。QSIG トランクは、+ の送信を試みません。+ をサポートするゲートウェイを通じた発信コールでは、Cisco Unified Communications Manager が + とダイヤル番号をゲートウェイに送信できます。+ をサポートしないゲートウェイからの発信コールでは、Cisco Unified Communications Manager がコール情報をゲートウェイに送信したときに、国際エスケープ文字 + は削除されます。
SIP	SIP は番号タイプをサポートしないため、SIP トランク経由のコールは、発信側番号の種類が不明（Unknown）である [着信番号（Incoming Number）] 設定のみをサポートします。
QSIG	QSIG 設定は通常、同一のダイヤル プランをサポートします。QSIG を使用している場合、番号やプレフィックスの変換は、機能のインタラクションの問題を引き起こす可能性があります。
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	発信者番号をローカライズするには、デバイスは番号分析を使用してトランスフォーメーションを適用する必要があります。[発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）] を [なし（None）] に設定した場合、変換は一致せず、適用されません。[発呼側トランスフォーメーションパターン（Calling Party Transformation Pattern）] は、必ず、ルーティングに使用されていない Null 以外のパーティションに設定してください。

機能	制約事項
T1-CAS ポートと FXO ポート	発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）設定は、ゲートウェイ上の T1-CAS と FXO ポートには適用されません。
Cisco Unity Connection	Cisco Unity Connection は、国際エスケープ文字（+）をサポートしていません。従って、ボイスメッセージング機能が期待どおりに動作するように、Cisco Unity Connection へのコールに + が含まれていないことを確認する必要があります。 Cisco Unity Connection の詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unity-connection/index.html をご覧ください。



第 80 章

論理パーティション分割の設定

- 論理パーティション分割の概要，699 ページ
- 論理パーティション設定タスク フロー，699 ページ
- 論理的なパーティション分割の連携動作と制約事項，709 ページ

論理パーティション分割の概要

論理パーティション分割を行うことで、発信の分離に関する規制上の要件を満たしながら、単一のシステムで PSTN コールと VoIP コールをサポートできます。たとえば、インドの規制上の制約の下では、外部の電話で送受信されるコールはすべて、ローカルまたは長距離のサービス プロバイダーに渡し、適切な電話料金で完全な接続を介して伝送される必要があります。発信者の場所や呼び出されている電話番号に応じて、コールを PSTN または VoIP ネットワークに適切にルーティングする単一の Unified Communications Manager クラスタを作成できます。

論理パーティション分割では、互いに通信可能な一連の VoIP デバイスを定義します。ユーザが PSTN に使用する回線や VoIP に使用する回線を覚えておく必要はありません。オフネット コールを行う電話のみ、PSTN ゲートウェイと通信できます。これは、2 倍のインフラストラクチャ コストをかけずに、2 つのネットワークで VoIP コールと PSTN コールを個別に処理しているのと同じです。

論理パーティション設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	Enable Logical Partitioning, （701 ページ）	

	コマンドまたはアクション	目的
ステップ 2	地理位置情報の設定，（701 ページ）を行うには、次のサブタスクを実行します。 • 地理位置情報の定義，（702 ページ） • 地理位置情報の割り当て，（702 ページ） • デフォルトの地理位置情報の設定，（703 ページ）	地理位置情報を設定するのは、場所の定義とそのデバイスへの割り当ての 2 段階のプロセスです。また、クラスタ内の全デバイスが使用するデフォルトの場所を設定できます。
ステップ 3	論理パーティション分割のデフォルト ポリシーの設定，（704 ページ）	地理位置情報または地理位置情報フィルタと関連付けられていないデバイスのデフォルトのポリシーを設定します。このポリシーを使用すると、これらのデバイス間の PSTN コールを許可または拒否できます。
ステップ 4	論理パーティショニング チェックを回避するためのデバイス設定，（704 ページ）	デバイスとデバイスプールをパーティショニング チェックから特に除外できます。
ステップ 5	地理位置情報フィルタの設定，（705 ページ）を行うには、次のサブタスクを実行します。 • フィルタ ルールの定義，（706 ページ） • 地理位置情報フィルタの割り当て，（706 ページ） • デフォルトの地理位置情報フィルタの設定，（707 ページ）	論理パーティショニングでは、場所に基づいて、各デバイスに一意の ID を割り当てます。1 つのデバイスが別のデバイスをコールすると、コールを許可するかどうかと、ルートが適切であるかを判別するために、これらの ID を使用します。どのフィールドを使用してこの ID を作成するかを選択できます。たとえば、ビルディング内の部屋またはフロアに応じて異なるポリシーを適用できます。
ステップ 6	論理パーティション ポリシー レコードの定義，（708 ページ）	地理位置情報中のコールを許可または拒否するための論理的なパーティショニング ポリシーのセットを定義します。地理位置情報間のコールの続行が許可される前に、システムはこれらのポリシーに基づいて指定された地理位置情報間でコールが許可されていることを確認します。

	コマンドまたはアクション	目的
ステップ 7	ロケーション伝達の有効化, （708 ページ）	（任意） クラスタ間でデバイスに関する地理位置情報を通信するには、ロケーション配信を設定します。

Enable Logical Partitioning

手順

ステップ 1 Cisco Unified CM の管理から、[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 [論理パーティションを有効にする（Enable Logical Parititioning）] エンタープライズ パラメータのドロップダウン リストから [True] を選択します。

ステップ 3 [保存（Save）] をクリックします。

次の作業

地理位置情報の定義, （702 ページ）

地理位置情報の設定

地理位置情報を設定するのは、場所の定義とそのデバイスへの割り当ての2段階のプロセスです。また、クラスタ内の全デバイスが使用するデフォルトの場所を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報の定義, （702 ページ）	地理位置情報を指定するには、地理的なロケーションを設定します。この情報は、デバイスを論理パーティション設定などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。
ステップ 2	地理位置情報の割り当て, （702 ページ）	デバイスまたはデバイス プールに地理位置情報を割り当てます。

	コマンドまたはアクション	目的
ステップ 3	デフォルトの地理位置情報の設定, （703 ページ）	このクラスタ内の全デバイスとデバイス プールにデフォルトの地理位置情報を指定します。

地理位置情報の定義

地理位置情報を指定するには、地理的なロケーションを設定します。この情報は、デバイスを論理パーティション設定などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。

はじめる前に

Enable Logical Partitioning, （701 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [地理位置情報の設定（Geolocation Configuration）] 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 [地理位置情報の設定（Geolocation Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

地理位置情報の割り当て, （702 ページ）

地理位置情報の割り当て

デバイスまたはデバイス プールに地理位置情報を割り当てます。

はじめる前に

地理位置情報の定義, （702 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、次のいずれかのメニュー項目を選択します。

- [デバイス（Device）] > [電話（Phone）]
- [デバイス（Device）] > [トランク（Trunk）]

- [デバイス（Device）] > [ゲートウェイ（Gateway）]
- [システム（System）] > [デバイス プール（Device Pool）]

ステップ 2 次のいずれかの作業を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のデバイスまたはデバイス プールを選択します。
- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスでは、必要に応じてデバイスタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [地理位置情報（Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

デフォルトの地理位置情報の設定, （703 ページ）

デフォルトの地理位置情報の設定

このクラスタ内の全デバイスとデバイス プールにデフォルトの地理位置情報を指定します。

はじめる前に

地理位置情報の割り当て, （702 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに値を入力し、[保存（Save）] をクリックします。

次の作業

論理パーティション分割のデフォルト ポリシーの設定, （704 ページ）

論理パーティション分割のデフォルト ポリシーの設定

地理位置情報または地理位置情報フィルタと関連付けられていないデバイスのデフォルトのポリシーを設定します。このポリシーを使用すると、これらのデバイス間の PSTN コールを許可または拒否できます。

はじめる前に

デフォルトの地理位置情報の設定, （703 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [論理パーティション分割ポリシーの設定（Logical Partitioning Policy Configuration）] 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 [論理パーティション分割ポリシーの設定（Logical Partitioning Policy Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

（注） 値の [許可（Allow）] が含まれていたポリシーの値が、後で [拒否（Deny）] に変更された場合、そのポリシーは [拒否（Deny）] のままになります。逆も同様です。前に [拒否（Deny）] に設定されていて、後で [許可（Allow）] に変更されたポリシーは、[許可（Allow）] になります。[Cisco 統合レポート（Cisco Unified Reporting）] > [地理位置情報ポリシー レポート（Geolocation Policy Report）] を利用して重複するポリシーを特定できます。

次の作業

論理パーティショニング チェックを回避するためのデバイス設定, （704 ページ）

論理パーティショニング チェックを回避するためのデバイス設定

デバイスとデバイスプールをパーティショニング チェックから特に除外できます。

はじめる前に

論理パーティション分割のデフォルト ポリシーの設定, （704 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、次のいずれかのメニュー項目を選択します。

- [デバイス（Device）] > [電話（Phone）]
- [デバイス（Device）] > [トランク（Trunk）]

- [デバイス（Device）] > [ゲートウェイ（Gateway）]
- [システム（System）] > [デバイス プール（Device Pool）]

ステップ 2 次のいずれかの作業を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のデバイスまたはデバイス プールを選択します。
- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスについては、必要に応じてデバイスのタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [地理位置情報（Geolocation）] ドロップダウンリストから、[未指定（Unspecified）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

フィルタ ルールの定義, （706 ページ）

地理位置情報フィルタの設定

論理パーティショニングでは、場所に基づいて、各デバイスに一意の ID を割り当てます。1 つのデバイスが別のデバイスをコールすると、コールを許可するかどうかと、ルートが適切であるかを判別するために、これらの ID を使用します。どのフィールドを使用してこの ID を作成するかを選択できます。たとえば、ビルディング内の部屋またはフロアに応じて異なるポリシーを適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	フィルタ ルールの定義, （706 ページ）	地理位置情報フィルタでは、地理位置情報の識別子を作成するためにどのフィールドを使用するかを指定できます。この機能を使用して、地理位置情報オブジェクトのサブセットでポリシーを決定します。
ステップ 2	地理位置情報フィルタの割り当て, （706 ページ）	
ステップ 3	デフォルトの地理位置情報フィルタの設定, （707 ページ）	クラスタのデフォルトの地理位置情報フィルタを指定するには、デフォルトの地理位置情報フィルタのエンタープライズ パラメータを設定します。このパラメータが、地理位置情報フィルタと関連付けられていないすべてのデバイスおよびデバイス プールの

	コマンドまたはアクション	目的
		デフォルトの地理位置情報フィルタの設定を決定します。

フィルタ ルールの定義

地理位置情報フィルタでは、地理位置情報の識別子を作成するためにどのフィールドを使用するかを指定できます。この機能を使用して、地理位置情報オブジェクトのサブセットでポリシーを決定します。

はじめる前に

論理パーティショニング チェックを回避するためのデバイス設定, （704 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [地理位置情報フィルタ（Geolocation Filter）] 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 [地理位置情報フィルタの設定（Geolocation Filter Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

地理位置情報フィルタの割り当て, （706 ページ）

地理位置情報フィルタの割り当て

はじめる前に

フィルタ ルールの定義, （706 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、次のいずれかのメニュー項目を選択します。

- [デバイス（Device）] > [電話（Phone）]
- [デバイス（Device）] > [トランク（Trunk）]

- [デバイス（Device）] > [ゲートウェイ（Gateway）]
- [システム（System）] > [デバイス プール（Device Pool）]

ステップ 2 次のいずれかの作業を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のデバイスまたはデバイス プールを選択します。
- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスでは、必要に応じてデバイスタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [地理位置情報フィルタ（Geolocation Filter）] ドロップダウン リストから、設定した地理位置情報フィルタを選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

デフォルトの地理位置情報フィルタの設定, （707 ページ）

デフォルトの地理位置情報フィルタの設定

はじめる前に

地理位置情報フィルタの割り当て, （706 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに地理位置情報フィルタのデフォルト値を入力し、[保存（Save）] をクリックします。

次の作業

論理パーティション ポリシー レコードの定義, （708 ページ）

論理パーティション ポリシー レコードの定義

地理位置情報中のコールを許可または拒否するための論理的なパーティショニング ポリシーのセットを定義します。地理位置情報間のコールの続行が許可される前に、システムはこれらのポリシーに基づいて指定された地理位置情報間でコールが許可されていることを確認します。

はじめる前に

地理位置情報フィルタの設定, （705 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[コール ルーティング（Call Routing）] > [論理パーティション ポリシーの設定（Logical Partitioning Policy Configuration）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存の論理パーティションポリシーの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のパーティション ポリシーを選択します。
- 新しい論理パーティション ポリシーを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [論理パーティション ポリシーの設定（Logical Partitioning Policy Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ロケーション伝達の有効化, （708 ページ）

ロケーション伝達の有効化

クラスタ間でデバイスに関する地理位置情報を通信するには、ロケーション配信を設定します。

はじめる前に

論理パーティション ポリシー レコードの定義, （708 ページ）

手順

ステップ 1 クラスタ間トランク（ICT）またはローカルクラスタの SIP トランクで [地理位置情報の送信（Send Geolocation Information）] チェックボックスをオンにします。

ステップ 2 [保存（Save）] をクリックします。

ステップ 3 ICT またはリモートクラスタの SIP トランクで [地理位置情報の送信（Send Geolocation Information）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

論理的なパーティション分割の連携動作と制約事項

論理パーティショニングの連携動作

表 *85*：論理パーティショニングの連携動作

機能	データのやり取り
アドホック会議、参加、複数ライン同時通話機能、コール転送、コール転送	論理パーティションの処理は、次の状況で起こりません: • すべての参加者は VoIP 電話です。 • 地理位置情報または地理位置情報フィルタ処理がデバイスに関連付けされていないとき。
割り込み、c割り込みおよびリモート再開	論理パーティションの処理は、次の状況で起こりません: • 発信者と呼び出される者の両方のデバイスが VoIP 電話のとき、論理パーティション分割ポリシーの確認は無視されます。 • 割り込み/c割り込みの参加者に対して、論理パーティション分割ポリシーの確認はなく、論理パーティション分割拒否シナリオを防ぐことはできません。
Cisco Unified Mobility	論理パーティションの処理は、次の状況で起こりません: • 地理位置情報または地理位置情報フィルタ処理は、含まれるデバイスに関連付けられません。 • デュアルモードの電話機を使用するとき、論理パーティション分割サポートはありません。

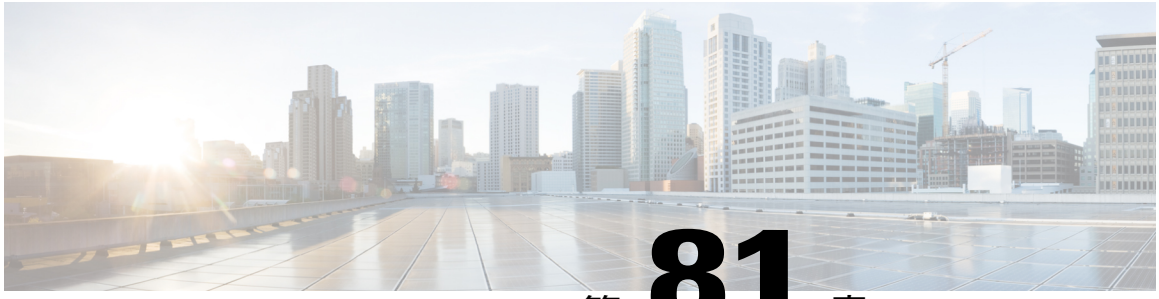
機能	データのやり取り
CTI の処理	論理パーティションの処理は、次の状況で起こりません: • 地理位置情報または地理位置情報フィルタ処理がどのデバイスにも関連付けられていないとき、処理は発生しません。 • 含まれるすべてのデバイスで VoIP 電話が指定されると、処理は発生しません。
エクステンション モビリティ（Extension Mobility）	論理パーティションの処理は、次の状況で起こりません: • 地理位置情報または地理位置情報フィルタ処理は、Cisco Extension Mobility にログインしている VoIP 電話とは関連付けられません。 • Cisco Extension Mobility にログインしている VoIP 電話は、VoIP 電話にコールを発信するか、または VoIP 電話からのコールを受信します。
ミートミー会議	論理パーティションの処理は、次の状況で起こりません: • すべての参加者が VoIP 電話のとき、処理は発生しません。 • 地理位置情報または地理位置情報フィルタ処理がデバイスと関連しないとき、そのデバイスではポリシー チェックは起こりません。
ルート リストとハント パイロット	論理パーティションの処理は、次の状況で起こりません: • 発信元と着信側デバイスが VoIP 電話のときに処理は発生しません。 • すべてのデバイスは、地理位置情報と地理位置情報フィルタ処理の両方に関連付けられている必要があります。どのデバイスも地理位置情報と地理位置情報フィルタ処理に関連付けられていない場合、処理は発生しません。
共有回線	論理パーティションの処理は、次の状況で起こりません: • 発信者と呼び出される者の両方のデバイスが VoIP 電話のとき、処理は発生しません。 • 地理位置情報または地理位置情報フィルタ処理がどのデバイスにも関連付けられていないと、処理は発生しません。

論理パーティショニングの制約事項

表 *86*：論理パーティショニングの制約事項

制約事項	説明
割り込み/c 割り込み	割り込み/c 割り込みは発生せず、コール インスタンスはドロップされます。 c 割り込み/割り込みの参加者に対しては、論理パーティション分割ポリシーのチェックは行われず、論理パーティション分割が拒否されるシナリオを防ぐことはできません。
BLF プレゼンス	論理パーティション分割ポリシーではBLFプレゼンス通知はチェックされません。
Cisco エクステンション モビリティ	Cisco Extension Mobility が異なる地理位置情報の電話にログインすると、ローカル ルート グループの設定時に PSTN 発信コールが行われる場合があります。PSTN 着信コールは電話では受信されませんが、リオーダー音が聞こえます。
Cisco Unified MeetingPlace	このシステムでは、Cisco Unified MeetingPlace または Cisco Unified MeetingPlace Express が関与するコールに対する論理パーティショニング機能はサポートされません。
会議	論理パーティション分割チェックは、会議チェーン内の会議全体の参加者ではサポートされません。 たとえば、ミートミー会議およびアドホック チェーン会議には、論理パーティション分割が拒否された参加者が参加できます。
H.225 ゲートキーパー制御のトランク	Cisco Unified Communications Manager が H.225 ゲートキーパー制御トランク経由で地理位置情報を伝えることはありません。
H.323 および MGCP ゲートウェイ	Cisco Unified Communications Manager が H.323 または MGCP ゲートウェイに地理位置情報を伝えることはありません。 SIP ゲートウェイへの通信は、SIP トランクのチェックボックスを介して無効にすることもできます。
モビリティ携帯電話ピックアップ	コールが携帯電話で応答された後で論理パーティション分割の否定処理が行われます。 論理パーティション分割ポリシーのチェックは、携帯電話にコールが発信される前には行われません（基本 SNR コールで実行されるため）。携帯電話がコールに応答した後で、システムが論理パーティション分割ポリシーをチェックします。

制約事項	説明
Q.SIG クラスタ間トランク	Q.SIGプロトコルを持つクラスタ間トランク（ICT）が、発信側または受信側デバイスの地理位置情報を伝えることは許可されていません。“地理位置情報の送信”のための ICT 設定は、Q.SIG トンネル プロトコルが選択されていると無効になります。
リオーダー音	論理パーティション分割ポリシーにより、接続コールがリリースされても IOS H.323 および SIP ゲートウェイではリオーダー音（ファスト ビジー音）は鳴りません。
共有回線のアクティブ コール	制限された論理パーティション分割シナリオでは、機能によって共有回線コールを許可されたカテゴリに移動された場合でも、共有回線はコールの期間中はアクティブ コール情報をドロップします。
User Agent Server（ユーザ エージェント サーバ）	この地理位置情報を受け取る論理パーティション分割認識クラスタ内の論理パーティション分割ポリシー チェックは、ポリシーが拒否された場合にコールをキャンセルする可能性があります。



第 81 章

地理位置情報とロケーション伝達の設定

- 地理位置情報とロケーション伝達の概要，713 ページ
- 地理位置情報とロケーションの配信タスク フロー，713 ページ

地理位置情報とロケーション伝達の概要

地理位置情報を使用して、ポリシーの決定（ある電話機から別の電話機へのコールを許可するかどうかなど）で使用されるデバイスの地理的場所（または都市の住所）を定義します。Request For Comments（RFC）4119 規格には、地理位置情報の基本が記載されています。

ロケーション伝達を使用すると、コールが確立されるとそのコールの間、あるクラスタから別のクラスタに地理位置情報を伝達できます。

地理位置情報とロケーションの配信タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報の設定，（714 ページ）を行うには、次のサブタスクを実行します。 • 地理位置情報の設定，（715 ページ） • 地理位置情報の割り当て，（715 ページ） • デフォルトの地理位置情報の設定，（716 ページ）	地理位置情報を指定するには、地理的なロケーションを設定します。この情報は、デバイスを論理パーティション設定などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。

	コマンドまたはアクション	目的
	• ロケーション配信の設定，（716 ページ）	
ステップ 2	地理位置情報フィルタの設定，（717 ページ）を行うには、次のサブタスクを実行します。 • 地理位置情報フィルタの設定，（718 ページ） • 地理位置情報フィルタの割り当て，（718 ページ） • デフォルトの地理位置情報フィルタの設定，（719 ページ）	地理位置情報フィルタを設定して、地理位置情報の識別子を作成するために使用するフィールドを選択します。この機能は、地理位置情報オブジェクトのサブセットで、ポリシー決定を行うために使用されます。地理位置情報フィルタでは、異なるデバイスの地理位置情報を比較するときに使用する地理位置情報のオブジェクトを定義します。たとえば、電話機のグループには、それらの電話機が置かれている部屋やフロアを除いて、同じジオロケーションが割り当てられる可能性があります。各電話の実際のジオロケーションは異なりますが、フィルタ処理されたジオロケーションは同じになります。

地理位置情報の設定

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報の設定，（715 ページ）	地理位置情報を指定するには、地理的なロケーションを設定します。この情報は、デバイスを論理パーティション設定などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。
ステップ 2	地理位置情報の割り当て，（715 ページ）	デバイスまたはデバイスプールに地理位置情報を割り当てます。
ステップ 3	デフォルトの地理位置情報の設定，（716 ページ）	このクラスタ内の全デバイスとデバイスプールにデフォルトの地理位置情報を指定します。
ステップ 4	ロケーション配信の設定，（716 ページ）	（任意） クラスタ間でデバイスに関する地理位置情報を通信するには、ロケーション配信を設定します。

地理位置情報の設定

地理位置情報を指定するには、地理的なロケーションを設定します。この情報は、デバイスを論理パーティション設定などの規制機能と関連付けるために使用されます。地理位置情報は、国内の規制など、ポリシーの判断で使用されます。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [地理位置情報の設定（Geolocation Configuration）] 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 [地理位置情報の設定（Geolocation Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

地理位置情報の割り当て, （715 ページ）

地理位置情報の割り当て

デバイスまたはデバイス プールに地理位置情報を割り当てます。

はじめる前に

地理位置情報の設定, （715 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、次のいずれかのメニュー項目を選択します。

- [デバイス（Device）] > [電話（Phone）]
- [デバイス（Device）] > [トランク（Trunk）]
- [デバイス（Device）] > [ゲートウェイ（Gateway）]
- [システム（System）] > [デバイス プール（Device Pool）]

ステップ 2 次のいずれかの作業を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のデバイスまたはデバイス プールを選択します。

- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスでは、必要に応じてデバイス タイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [地理位置情報（Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

デフォルトの地理位置情報の設定, （716 ページ）

デフォルトの地理位置情報の設定

このクラスタ内の全デバイスとデバイス プールにデフォルトの地理位置情報を指定します。

はじめる前に

地理位置情報の割り当て, （715 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[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 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに値を入力し、[保存（Save）] をクリックします。

次の作業

- （オプション） ロケーション配信の設定, （716 ページ）
- 地理位置情報フィルタの設定, （717 ページ）

ロケーション配信の設定

クラスタ間でデバイスに関する地理位置情報を通信するには、ロケーション配信を設定します。

はじめる前に

- 地理位置情報の設定, （715 ページ）

- 地理位置情報の割り当て，（715 ページ）
- デフォルトの地理位置情報の設定，（716 ページ）

手順

ステップ 1 クラスタ間トランク（ICT）またはローカルクラスタの SIP トランクで [地理位置情報の送信（Send Geolocation Information）] チェックボックスをオンにします。

ステップ 2 [保存（Save）] をクリックします。

ステップ 3 ICT またはリモートクラスタの SIP トランクで [地理位置情報の送信（Send Geolocation Information）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

地理位置情報フィルタの設定

地理位置情報フィルタを設定して、地理位置情報の識別子を作成するために使用するフィールドを選択します。この機能は、地理位置情報オブジェクトのサブセットで、ポリシー決定を行うために使用されます。地理位置情報フィルタでは、異なるデバイスの地理位置情報を比較するときに使用する地理位置情報のオブジェクトを定義します。たとえば、電話機のグループには、それらの電話機が置かれている部屋やフロアを除いて、同じジオロケーションが割り当てられる可能性があります。各電話の実際のジオロケーションは異なりますが、フィルタ処理されたジオロケーションは同じになります。

手順

	コマンドまたはアクション	目的
ステップ 1	地理位置情報フィルタの設定，（718 ページ）	地理位置情報フィルタでは、地理位置情報の識別子を作成するためにどのフィールドを使用するかを指定できます。この機能を使用して、地理位置情報オブジェクトのサブセットでポリシーを決定します。
ステップ 2	地理位置情報フィルタの割り当て，（718 ページ）	
ステップ 3	デフォルトの地理位置情報フィルタの設定，（719 ページ）	クラスタのデフォルトの地理位置情報フィルタを指定するには、デフォルトの地理位置情報フィルタのエンタープライズパラメータを設定します。このパラメータが、地理位置情報フィルタと関連付けられていないすべてのデバイスおよびデバイスプールのデフォルトの地理位置情報フィルタの設定を決定します。

地理位置情報フィルタの設定

地理位置情報フィルタでは、地理位置情報の識別子を作成するためにどのフィールドを使用するかを指定できます。この機能を使用して、地理位置情報オブジェクトのサブセットでポリシーを決定します。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [地理位置情報フィルタ（Geolocation Filter）] 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 [地理位置情報フィルタの設定（Geolocation Filter Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

地理位置情報フィルタの割り当て, （718 ページ）

地理位置情報フィルタの割り当て

はじめる前に

地理位置情報フィルタの設定, （718 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、次のいずれかのメニュー項目を選択します。

- [デバイス（Device）] > [電話（Phone）]
- [デバイス（Device）] > [トランク（Trunk）]
- [デバイス（Device）] > [ゲートウェイ（Gateway）]
- [システム（System）] > [デバイス プール（Device Pool）]

ステップ 2 次のいずれかの作業を実行します。

- 既存のデバイスまたはデバイス プールの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストから既存のデバイスまたはデバイス プールを選択します。

- 新しいデバイスまたはデバイス プールを追加するには、[新規追加（Add New）] をクリックします。デバイスでは、必要に応じてデバイスタイプとプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [地理位置情報フィルタ（Geolocation Filter）] ドロップダウン リストから、設定した地理位置情報フィルタを選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

デフォルトの地理位置情報フィルタの設定, （719 ページ）

デフォルトの地理位置情報フィルタの設定

クラスタのデフォルトの地理位置情報フィルタを指定するには、デフォルトの地理位置情報フィルタのエンタープライズ パラメータを設定します。このパラメータが、地理位置情報フィルタと関連付けられていないすべてのデバイスおよびデバイス プールのデフォルトの地理位置情報フィルタの設定を決定します。

はじめる前に

地理位置情報フィルタの割り当て, （718 ページ）

手順

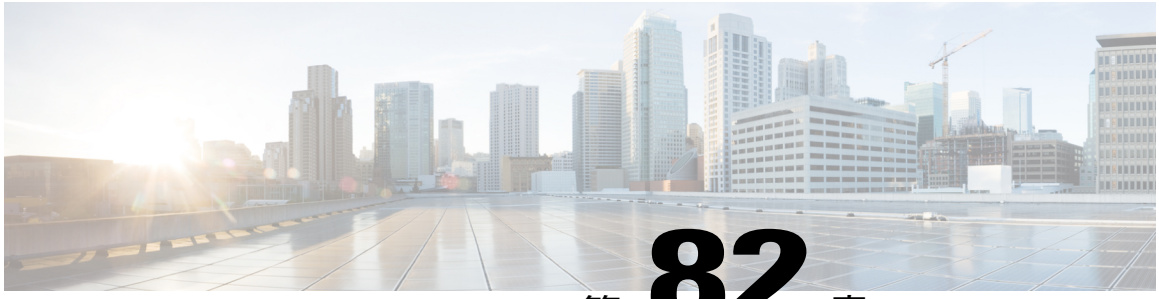
ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] を選択します。

ステップ 2 [デフォルトの地理位置情報（Default Geolocation）] ドロップダウン リストから、設定した地理位置情報を選択します。デフォルト値は、[未指定（Unspecified）] です。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [設定の適用（Apply Config）] をクリックします。

ステップ 5 （任意） 特定のデバイスまたはデバイス プールでこのデフォルトをオーバーライドする必要がある場合は、[デバイス設定（Device Configuration）] または [デバイス プール設定（Device Pool Configuration）] ウィンドウのいずれかに地理位置情報フィルタのデフォルト値を入力し、[保存（Save）] をクリックします。



第 82 章

ロケーション認識の設定

- ロケーション認識の概要，721 ページ
- 場所の認識の前提条件，723 ページ
- Location Awareness の設定タスク フロー，723 ページ

ロケーション認識の概要

ロケーション認識によって、管理者は企業ネットワークに接続している電話の接続元となる物理的な場所を決定できます。ワイヤレス ネットワークでは、ワイヤレス アクセスポイント インフラストラクチャを表示し、どのモバイル デバイスが現在それらのアクセスポイントに関連付けられているかを確認できます。有線ネットワークでは、イーサネット スイッチ インフラストラクチャを表示し、どのデバイスが現在それらのスイッチに接続しているかを確認できます。これによって、コールが発信されたビル、フロア、およびキューブを判別できます。

Cisco Unified Communications Manager の [スイッチとアクセス ポイントの検索と一覧表示（Find and List Switches and Access Points）] ウィンドウでネットワーク インフラストラクチャを表示できます。

この機能は、次の情報で Cisco Unified Communications Manager データベースを動的に更新します。

- 各インフラストラクチャ デバイスの IP アドレス、ホスト名、BSSID 情報（適用可能な場合）を含む、スイッチやワイヤレスアクセスポイントなどのネットワーク インフラストラクチャ デバイス。
- 次を含む、各インフラストラクチャ デバイスに関連付けられたエンドポイント。
  - ワイヤレス ネットワークでは、現在ワイヤレス アクセスポイントに関連付けられているデバイスのリスト。
  - 有線ネットワークでは、現在イーサネット スイッチに接続されているデバイスとデバイス タイプのリスト。

Cisco Emergency Responder の統合

ロケーション認識は、緊急通報を発信するユーザの物理的な場所を判別する Cisco Emergency Responder などの統合アプリケーションで役立ちます。ロケーション認識を有効にすると、Cisco Emergency Responder は、モバイル デバイスが新しいワイヤレス アクセスポイントに関連付けられた後、またはデスクトップ電話が新しいイーサネット スイッチに接続された後、数分以内にデバイスとインフラストラクチャの新しい関連付けを学習します。

Cisco Emergency Responder は、初回起動時に、デバイスとネットワーク インフラストラクチャの現在の関連付けを Cisco Unified Communications Manager データベースにクエリします。以降 2 分ごとに、Cisco Emergency Responder は既存の関連付けへの更新をチェックします。その結果、モバイル発信者がローミング状態で緊急通報を発信した場合でも、Cisco Emergency Responder はすぐに発信者の物理的な場所を判別し、適切なビル、フロア、またはキューブに緊急サービスを手配します。

ワイヤレス ネットワークの更新

無線インフラストラクチャで、Location Awareness を有効にするには、Cisco Unified Communications Manager がシスコ ワイヤレス LAN コントローラと同期するように設定します。Cisco Unified Communications Manager は、最大 50 のコントローラと同期できます。同期の過程で、コントローラが管理するアクセス ポイント インフラストラクチャの情報により、データベースを更新します。Cisco Unified CM Manager の管理では、各アクセス ポイントに関連付けられているモバイル クライアントのリストを含む、ワイヤレス アクセス ポイントのステータスを表示できます。

モバイル クライアントがアクセス ポイント間でローミングすると、エンドポイントからの SIP および SCCP シグナリングが、新しいデバイスとアクセス ポイントとの関連付けを、Cisco Unified Communications Manager に伝え、Cisco Unified Communications Manager はデータベースを更新します。また、Cisco Emergency Responder は、Cisco Unified Communications Manager のデータベースに数分ごとに問い合わせて、関連付けが変更された新しいエンドポイントの情報として、その新しい関連付けを取得します。その結果、モバイル クライアントが緊急通報の電話をかけると、Cisco Emergency Responder に、電話をかけたユーザがいる物理的な場所の正確な情報が残ります。

ワイヤレス アクセス ポイント コントローラの定期的な同期スケジュールがあれば、Cisco Unified Communications Manager は、同期の終わったデータベースから取得したアクセス ポイントを動的に追加および更新します。

一括管理を使用したアクセス ポイントの挿入

サードパーティのワイヤレス アクセス ポイント コントローラを使用している場合、または Cisco Prime Infrastructure からアクセス ポイントをエクスポートする場合は、一括管理ツールにより、ワイヤレス アクセス ポイント インフラストラクチャを CSV ファイルから Cisco Unified Communications Manager データベースに一括挿入できます。一括挿入の後に発生するモバイル デバイスの場所の更新により、アクセス ポイントの現在の関連付けでデータベースが更新されます。

ただし、一括管理では、新しいアクセス ポイントがワイヤレス ネットワークに追加される際に、アクセス ポイント インフラストラクチャを動的に更新することはできません。一括挿入の後に追加されたアクセス ポイントを通じて携帯電話から発信があると、データベースにそのアクセス ポイントのレコードがないため、Cisco Unified Communications Manager は、新しいアクセス ポイン

トのBSSIDを一致させることができず、その携帯電話のインフラストラクチャをUNIDENTIFIED AP としてマークします。

一括管理ツールの詳細については、『*Cisco Unified Communications Manager Bulk Administration* ガイド』の「Manage Infrastructure Devices」の章を参照してください。

有線ネットワークの更新

有線インフラストラクチャについて場所の認識を有効にするために何も設定する必要はありません。機能は自動的に有効になります。

有線電話を登録する際、電話機と Cisco Unified Communications Manager の間のシグナリングによって、スイッチ インフラストラクチャでデータベースが動的に更新されます。Cisco Unified CM Administration での会社のスイッチインフラストラクチャに関する詳細を、特定のスイッチに接続されている電話機のリストも含め表示できます。

モバイル デバイスと異なり、有線デバイスは、通常、1 つのスイッチから別のスイッチにローミングしません。会社内で従業員が席を替わったときなどに起こり得る、電話機が移動しない場合は、電話機が新しい場所から再登録されると、新しいスイッチ情報でデータベースが更新されます。Cisco Unified Communications Manager で、新しいスイッチは移動された電話を接続されたエンドポイントとして表示されます。

スイッチが廃止され、ネットワーク インフラストラクチャから削除される場合、そのスイッチは、Cisco Unified Communications Manager 内で見えたままです。インフラストラクチャのビューから古いスイッチを削除するには、[アクセス ポイントとスイッチの設定（Access Point and Switch Configuration）] ウィンドウで非アクティブ化する必要があります。

場所の認識の前提条件

この機能を使用すると、Cisco Unified Communications Manager を複数のシスコ ワイヤレス LAN コントローラと同期できます。また、シスコ ワイヤレス LAN コントローラのハードウェアとアクセス ポイントのインフラストラクチャをセットアップする必要があります。詳細については、コントローラのドキュメンテーションを参照してください。

Location Awareness の設定タスク フロー

Cisco Unified Communications Manager で Location Awareness をセットアップするには、次のタスクを実行します。

はじめる前に

- 場所の認識の前提条件, （723 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	無線インフラストラクチャ同期のサービスの開始, （724 ページ）	Cisco Unified Serviceability で、Location Awareness 機能をサポートするサービスを開始します。
ステップ 2	ワイヤレス アクセス ポイント コントローラの設定, （725 ページ）	データベースとワイヤレス アクセス ポイント コントローラを同期します。同期すると、無線インフラストラクチャがデータベースにインポートされます。 ヒント　自動更新の同期スケジュールをセットアップします。
ステップ 3	インフラストラクチャデバイスの挿入, （726 ページ）	これはオプションです。Cisco Prime Infrastructure の無線インフラストラクチャを追加するか、またはサードパーティのワイヤレス LAN コントローラを使用している場合は、一括管理を使用して、CSV ファイルでデータベースを更新します。 （注）　このメソッドを使用して、自動更新をセットアップすることはできません。
ステップ 4	インフラストラクチャデバイストラッキングの非アクティブ化, （727 ページ）	これはオプションです。同期内容に追跡を望まないアクセスポイントが含まれている場合（たとえば、同期することでラボのアクセスポイントが制御される場合）は、アクセスポイントを非アクティブにできるため、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] でアクセス ポイントの更新が追跡されることはありません。

無線インフラストラクチャ同期のサービスの開始

場所認識機能に対応するシスコ ワイヤレス LAN コントローラとの同期をサポートする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 Serviceability にログインし、[ツール（Tools）] > [サービスの有効化（Service Activation）] の順に選択します。

ステップ 2　[サーバ（Server）] ドロップダウン リスト ボックスからパブリッシャ ノードを選択します。

ステップ 3　次のサービスがオンになっていることを確認します。

- Cisco CallManager

- Cisco AXL Web Service
- Cisco Wireless Controller Synchronization サービス

ステップ 4 これはオプションです。一括管理を使用して CSV ファイルからネットワーク インフラストラクチャをインポートする場合、[一括プロビジョニング サービス（Bulk Provisioning Service）] がオンになっていることを確認します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

ワイヤレス アクセス ポイント コントローラの設定, （725 ページ）

ワイヤレス アクセス ポイント コントローラの設定

シスコのワイヤレス アクセス ポイント コントローラとデータベースを同期するには、次の手順を使用します。同期中、Cisco Unified Communications Manager は、コントローラが管理するワイヤレス アクセスポイントのインフラストラクチャを使用して、データベースを更新します。最大 50 のワイヤレス アクセスポイント コントローラを追加できます。

はじめる前に

無線インフラストラクチャ同期のサービスの開始, （724 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[詳細機能（Advanced Features）] > [デバイス ロケーション追跡サービス（Device Location Tracking Services）] > [ワイヤレス アクセス ポイント コントローラ（Wireless Access Point Controllers）] を選択します。

ステップ 2 設定するコントローラを選択します。

- 既存のコントローラを編集するには、[検索（Find）] をクリックし、コントローラを選択します。
- 新しいコントローラを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、コントローラの IP アドレスまたはホスト名を入力します。

ステップ 4 コントローラの [説明（Description）] を入力します。

ステップ 5 コントローラに SNMP メッセージを送信するために使用する SNMP 設定を行います。

a) [SNMP バージョン（SNMP Version）] ドロップダウン リスト ボックスから、コントローラで使用する SNMP バージョン プロトコルを選択します。

b) その他の SNMP 認証フィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

c) [SNMP 設定のテスト（Test SNMP Settings）] ボタンをクリックし、入力した SNMP 設定が有効であることを確認します。

ステップ 6 スケジュール同期を設定して、データベースを定期的に更新する場合：

a) [インフラストラクチャ デバイスを検出するためにスケジュール同期を有効にする（Enable scheduled synchronization to discover Infrastructure Devices）] チェックボックスをオンにします。

b) [再同期の実行間隔（Perform a Re-sync Every）] フィールドで、同期スケジュールを作成します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 これはオプションです。データベースを今すぐ更新するには、[同期（Synchronize）] をクリックします。

次の作業

これはオプションです。同期内容に、追跡を行わないアクセス ポイント（たとえば、研究室用の機器または使用していないアクセスポイント）が含まれる場合は、アクセスポイントを追跡の対象から外すことができます。

- インフラストラクチャ デバイス トラッキングの非アクティブ化, （727 ページ）

インフラストラクチャ デバイスの挿入

CSV ファイルから Cisco Unified Communications Manager データベースへのワイヤレス アクセス ポイント インフラストラクチャの一括インポートを行うには、次の手順を実行します。この手順を使用して、Cisco Prime Infrastructure からエクスポートされた CSV ファイルをインポートすることや、サードパーティのワイヤレス アクセス ポイント コントローラからアクセス ポイントをインポートすることも可能です。

はじめる前に

データ ファイルは、次のように区別された列を含む、カンマ区切り値（CSV）形式にしてしておく必要があります。

- アクセス ポイントまたはスイッチの名前
- IPv4 アドレス（IPv4 Address）
- IPv6 アドレス（IPv6 Address）
- BSSID：ワイヤレス アクセス プロトコル（WAP）のインフラストラクチャ デバイスに必須
- 説明：場所の識別子、スイッチ タイプと場所の組み合わせ、または別の有効な識別子

（注） IPv4 アドレスと IPv6 アドレスの両方を定義することも、そのいずれかを定義することもできます。

（注） BSSID 値には、アクセス ポイントの個別のチャネルの BSSID とは異なり、アクセス ポイントを一意に識別する、0 で終わる BSSID マスクを入力します。

手順

ステップ 1 [一括管理（Bulk Administration）]>[インフラストラクチャ デバイス（Infrastructure Device）]>[インフラストラクチャ デバイスの挿入（Insert Infrastructure Device）].を選択します。
[インフラストラクチャ デバイスの挿入の設定（Insert Infrastructure Device Configuration）] ウィンドウが表示されます。

ステップ 2 [ファイル名（File Name）] フィールドで、このトランザクション用に作成した CSV データ ファイルを選択します。

ステップ 3 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。
デフォルトの説明は、[インフラストラクチャ デバイスの挿入（Insert Infrastructure Device）] です。

ステップ 4 ジョブを実行するタイミングを選択します。

- ジョブをただちに実行する場合は、[ただちに実行（Run Immediately）] オプション ボタンを選択します。
- ジョブを改めてスケジュールする場合は、[後で実行（Run Later）] オプション ボタンを選択します。

ステップ 5 [送信（Submit）] をクリックします。
ジョブをただちに実行することを選択した場合は、ジョブが実行されます。

ステップ 6 ジョブを後で実行することを選択した場合は、ジョブを実行するスケジュールを設定します。

a) [一括管理（Bulk Administration）] > [ジョブ スケジューラ（Job Scheduler）] を選択します。
b) [検索（Find）] をクリックし、作成したジョブを選択します。
c) [ジョブ スケジューラ（Job Scheduler）] ウィンドウで、ジョブを実行するスケジュールを設定します。
d) [保存（Save）] をクリックします。
スケジュールされた時間にジョブが実行されます。

インフラストラクチャ デバイス トラッキングの非アクティブ化

同期の対象に、トラッキングを避けたいスイッチまたはアクセス ポイント（たとえば、ラボの機器や使用されていないアクセスポイントなど）が含まれている場合、そのアクセスポイントまたはスイッチへのトラッキングを非アクティブ化できます。Cisco Unified Communications Manager は、そのアクセス ポイントまたはスイッチのステータスを更新しなくなります。

手順

ステップ 1 Cisco Unified CM の管理で、[詳細機能（Advanced Features）] > [デバイスの位置のトラッキングサービス（Device Location Tracking Services）] > [スイッチとアクセス ポイント（Switches and Access Points）] を選択します。

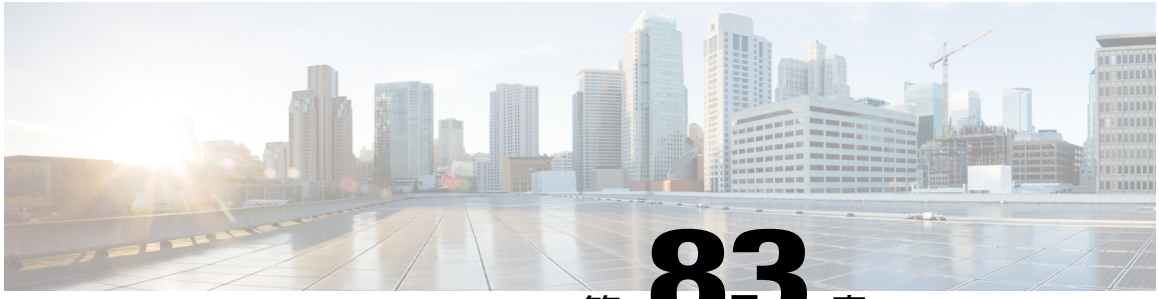
ステップ 2 [検索（Find）] をクリックして、追跡を停止するスイッチまたはアクセスポイント選択します。

ステップ 3 [選択項目の非アクティブ化（Deactivate Selected）] をクリックします。

関連資料

システム設定が完了し、システムが稼働したら、次の章のタスクを使用して、インフラストラクチャを継続的に管理できます。

Cisco Unified Communications Manager および IM and Presence サービスのアドミニストレーションガイド の「インフラストラクチャの管理」を参照。



第 83 章

自動代替ルーティングの設定

- 自動代替ルーティングの概要，729 ページ
- AAR 設定タスク フロー，729 ページ

自動代替ルーティングの概要

ロケーション帯域幅の不足により、コールがブロックされている場合、PSTN または他のネットワーク経由でコールを自動的に再ルーティングするための自動代替ルーティング（AAR）を設定します。自動代替ルーティングにより、発信者は通話を終了して着信側にリダイヤルする必要がなくなります。

AAR 設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	クラスタ全体の AAR を有効にする，（730 ページ）	クラスタで自動代替ルーティングを有効にします。
ステップ 2	自動代替ルーティングの設定，（730 ページ）	自動代替ルーティング（AAR）を設定し、その場所の帯域幅が不十分だったことが原因で Cisco Unified CM がコールをブロックした場合に、代替番号を使用することによって、PSTN またはその他のネットワークを通じてコールを再ルーティングします。

クラスタ全体の AAR を有効にする

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 [サーバー（Server）] ドロップダウン ボックスのノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco Call Manager] を選択します。

ステップ 4 クラスタ全体のパラメータ（システム□CCM 自動代替ルーティング）領域で、[自動代替ルーティングの有効化（Automated Alternate Routing Enable）] パラメータを [True] に設定します。

次の作業

自動代替ルーティングの設定, （730 ページ）

自動代替ルーティングの設定

場所の帯域幅不足のため Cisco Unified Communications Manager がコールをブロックした場合に、代替番号を使用して、PSTN またはその他のネットワークを通じてコールを再ルーティングする自動代替ルーティング（AAR）を設定します。

はじめる前に

クラスタ全体の AAR を有効にする, （730 ページ）

手順

ステップ 1 [コール ルーティング（Call Routing）] > [AAR グループ（AAR Group）].を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい AAR グループを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存の AAR グループの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果の一覧から AAR グループを選択します。

[AAR グループの設定（AAR Group Configuration）] ウィンドウが表示されます。

ステップ 3 [名前（Name）] フィールドに、新しい AAR グループに割り当てる名前を入力します。
この名前には、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（-）、および下線文字（_）を任意に組み合わせることが可能です。

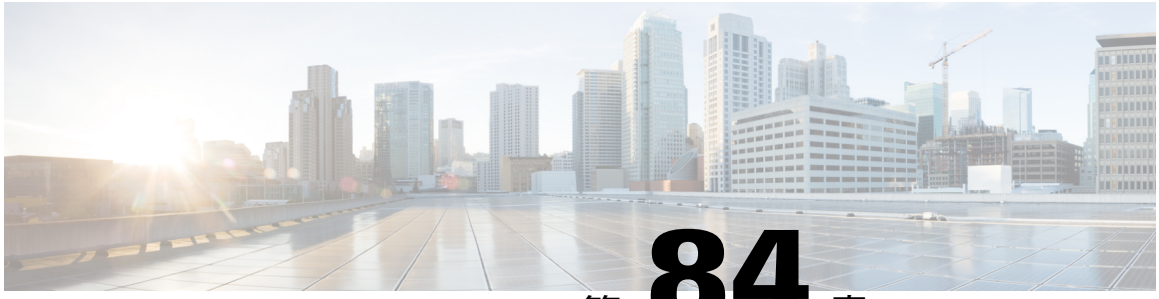
ウィンドウが更新され、その他のフィールドが表示されます。

ステップ 4 [AAR グループの設定（AAR Group Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

次の作業

これはオプションです。AAR をハントパイロットと連動させる方法については、次のセクションを参照してください。 ハント パイロットの設定タスク フロー, （166 ページ）



第 84 章

マルチレベルの優先とプリエンプション

- Multilevel Precedence and Preemption の概要，733 ページ
- Multilevel Precedence and Preemption の前提条件，733 ページ
- Multilevel Precedence and Preemption Precendence のタスク フロー，733 ページ
- Multilevel Precedence and Preemption の連携動作と制限事項，755 ページ

Multilevel Precedence and Preemption の概要

Multilevel Precedence and Preemption（MLPP）サービスを使用すると、コールに優先順位を付けることができます。適切に検証されたユーザは、優先順位が低いコールと優先順位が高いコールをプリエンプション処理できます。認証されたユーザは、対象のステーション向けに、または完全にサブクライブされた TDM トランクを介してコールをプリエンプション処理できます。この機能により、国家の非常事態やネットワークの機能低下など、ネットワークに負荷がかかっている場合に、優先順位の高いユーザが重要な組織や担当者への通信を確実に行うことができます。

Multilevel Precedence and Preemption の前提条件

サポートされる SCCP または SIP フォン。Cisco IP フォンのサポート情報については、関連する電話管理ガイドおよびユーザ ガイドを参照してください。

Multilevel Precedence and Preemption Precendence のタスク フロー

はじめる前に

- Multilevel Precedence and Preemption の前提条件，（733 ページ）を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	ドメインおよびドメイン リストの設定, （736 ページ）を行うには、次のサブタスクを実行します。 • Multilevel Precedence and Preemption ドメインの設定, （737 ページ） • リソース プライオリティ ネームスペース ネットワーク ドメインの設定, （737 ページ） • リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定, （738 ページ）	MLPP サブスクライバに関連付けられるリソースのデバイスを指定するには、MLPP ドメインを設定します。
ステップ 2	共通デバイス設定での Multilevel Precedence and Preemption 設定, （739 ページ）	一般的なデバイス設定には、複数のユーザとそのデバイスに適用できる MLPP 関連の情報が含まれています。各デバイスは一般的なデバイス設定に関連付けられていることを確認します。これらの設定は、エンタープライズ パラメータの設定を上書きします。
ステップ 3	Multilevel Precedence and Preemption のエンタープライズ パラメータの設定, （740 ページ）	MLPP の通知とプリエンプションを有効にするには、エンタープライズ パラメータを設定します。個々のデバイスや一般的なデバイス設定のデバイスがデフォルトの MLPP 設定になっていると、MLLP 関連のエンタープライズ パラメータは、これらのデバイス、および一般的なデバイス設定に適用されます。
ステップ 4	Multilevel Precedence and Preemption のパーティションの設定, （742 ページ）	パーティションを設定して、電話番号（DN）の論理グループと、到達可能性の特徴が類似したルートパターンを作成します。パーティションに通常、配置されるデバイスは、DNs とルート パターンを含みます。これらのエンティティは、ユーザがダイヤルする DNs に関連付けられます。わかりやすくするために、パーティション名は通常、その特性を反映しています。

	コマンドまたはアクション	目的
ステップ 5	Multilevel Precedence and Preemption のコーリング サーチ スペースの設定, （744 ページ）	コーリング サーチ スペースは、パーティションの番号付きリストです。コーリング サーチ スペースは、IP フォン、ソフトフォン、ゲートウェイなどのコーリング デバイスがコールを完了しようとしたときに検索できるパーティションを決めます。
ステップ 6	Multilevel Precedence and Preemption（MLPP）のルート パターンの設定, （745 ページ）	内部および外部コールの両方をルーティングまたはブロックするためにルート パターンを設定します。
ステップ 7	Multilevel Precedence and Preemption のトランスレーション パターンの設定, （747 ページ）	コールされてからコールをルーティングされる方法を指定するには、トランスレーション パターンを設定します。トランスレーション パターンを設定すると、システムで必要に応じて発信と発信された数字を処理できます。パターン一致が発生していることを確認すると、システムは後続の一致を実行するためにトランスレーション パターン用に設定されたコーリング サーチ スペースを使用します。
ステップ 8	ゲートウェイの Multilevel Precedence and Preemption の設定, （748 ページ）	非 IP 通信デバイスと通信するように Cisco Unified Communications Manager を設定します。
ステップ 9	電話機のMultilevel Precedence and Preemption の設定, （749 ページ）	
ステップ 10	Multilevel Precedence and Preemption コールの電話番号の設定, （752 ページ）	デバイスを設定した後、更新された [デバイス設定（Device Configuration）] ウィンドウから回線（ディレクトリ番号）を追加できます。
ステップ 11	Multilevel Precedence and Preemption のユーザ デバイス プロファイルの設定, （752ページ）	ユーザプロファイルが電話機に割り当てられると、その電話は、ユーザに関連付けられている CSS を含む割り当てられたユーザの設定を継承します。しかし、電話の CSS は、ユーザ プロファイルを上書きします。パターン一致が発生すると、Cisco Unified Communications Manager は、そのコールへのダイヤル パターンに関連付けられる優先度レベルを割り当てます。システムは、割り当てられた優先度レベルで優先度の高いコールとしてコール要求を設定します。
ステップ 12	Multilevel Precedence and Preemption のデフォルトのデバイス プロファイルの設定, （754ページ）	ユーザがユーザ デバイス プロファイルがない電話機モデルにログインするたびに、デフォルト デバイス プロファイルを使用します。デフォルトのデ

	コマンドまたはアクション	目的
		バイス プロファイルは、特定のデバイスに関連付けられている機能とサービスで構成されています。

ドメインおよびドメイン リストの設定

MLPP サブスクライバに関連付けられるリソースのデバイスを指定するには、MLPP ドメインを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Multilevel Precedence and Preemption ドメインの設定, （737 ページ）	デバイスおよびリソースをMLPPサブスクライバと関連付けます。特定のドメインに属しているMLPPサブスクライバが、同じドメインに属している別のMLPPサブスクライバに優先度の高いコールを発信する場合、MLPPサービスでは、着信側MLPPサブスクライバが対応中の既存のコールを優先度の高いコールにプリエンプション処理できます。MLPPサービスは、異なるドメイン間では利用できません。 発信側ユーザの MLPP ドメイン サブスクリプションにより、コールとその接続のドメインが決定されます。1 つのドメインの優先度の高いコールのみ、同じドメインのコールが使用している接続をプリエンプション処理できます。
ステップ 2	リソース プライオリティ ネームスペース ネットワーク ドメインの設定, （737 ページ）	SIP トランクを使用する Voice over Secured IP（VoSIP）ネットワークの名前空間ドメインを設定します。システムでは SIP シグナル リソースを優先することで、緊急時や電話回線、IP 帯域幅、およびゲートウェイの輻輳時にこれらのリソースを最も効率的に使用できるようにしています。エンドポイントは、優先順位およびプリエンプション情報を受信します。
ステップ 3	リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定, （738 ページ）	許容できるネットワーク ドメインの一覧を設定します。着信コールが一覧と照合され、許容できるネットワーク ドメインが一覧にある場合は処理されます。

Multilevel Precedence and Preemption ドメインの設定

デバイスおよびリソースを MLPP サブスクライバと関連付けます。特定のドメインに属している MLPP サブスクライバが、同じドメインに属している別の MLPP サブスクライバに優先度の高いコールを発信する場合、MLPP サービスでは、着信側 MLPP サブスクライバが対応中の既存のコールを優先度の高いコールにプリエンプション処理できます。MLPP サービスは、異なるドメイン間では利用できません。

発信側ユーザの MLPP ドメイン サブスクリプションにより、コールとその接続のドメインが決定されます。1 つのドメインの優先度の高いコールのみ、同じドメインのコールが使用している接続をプリエンプション処理できます。

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [MLPP] > [ドメイン（Domain）] > [MLPP ドメイン（MLPP Domain）] 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 [ドメイン名（Domain Name）] フィールドに、新しい MLPP ドメインに割り当てる名前を入力します。
最長 50 文字の英数字を入力でき、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて使用することが可能です。

ステップ 4 [ドメイン ID（Domain ID）] フィールドに、MLPP ドメイン ID として一意の 6 文字の 16 進数を入力します。
ドメイン ID は 000001 と FFFFFF の範囲で指定する必要があります。（000000 は、デフォルトの MLPP ドメイン ID に予約されています）

ステップ 5 [保存（Save）] をクリックします。

次の作業

リソース プライオリティ ネームスペース ネットワーク ドメインの設定, （737 ページ）

リソース プライオリティ ネームスペース ネットワーク ドメインの設定

SIP トランクを使用する Voice over Secured IP（VoSIP）ネットワークの名前空間ドメインを設定します。システムでは SIP シグナル リソースを優先することで、緊急時や電話回線、IP 帯域幅、およびゲートウェイの輻輳時にこれらのリソースを最も効率的に使用できるようにしています。エンドポイントは、優先順位およびプリエンプション情報を受信します。

はじめる前に

Multilevel Precedence and Preemption ドメインの設定, （737 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [MLPP（MLPP）] > [ネームスペース（Namespace）] > [リソース プライオリティ ネームスペース ネットワーク ドメイン（Resource Priority Namespace Network Domain）] を選択します。

ステップ 2 [情報（Information）] セクションで [リソース プライオリティ ネームスペース ネットワーク ドメイン（Resource Priority Namespace Network Domain）] の名前を入力します。ドメイン名の最大文字数は 100 です。

ステップ 3 ドメイン名についての説明を入力します。
説明には、任意の言語で最大 50 文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、山カッコ（<>）は使用できません。

ステップ 4 ドメイン名をデフォルトにする場合は、[このリソースプライオリティネームスペースネットワーク ドメインをデフォルトにする（Make this the Default Resource Priority Namespace Network Domain）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

次の作業

リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定, （738 ページ）

リソース プライオリティ ネームスペース ネットワーク ドメイン リストの設定

許容できるネットワーク ドメインの一覧を設定します。着信コールが一覧と照合され、許容できるネットワーク ドメインが一覧にある場合は処理されます。

はじめる前に

リソース プライオリティ ネームスペース ネットワーク ドメインの設定, （737 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[システム（System）] > [MLPP] > [ネームスペース（Namespace）] > [リソース プライオリティ ネームスペース リスト（Resource Priority Namespace List）] を選択します。

ステップ 2 リソース プライオリティ ネームスペース リストの名前を入力します。最大文字数は 50 です。

ステップ 3 リストの説明を入力します。説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 4 上矢印と下矢印で、リソース プライオリティ ネームスペース ネットワーク ドメインを [選択されたリソース プライオリティ ネームスペース（Selected Resource Priority Namespaces）] フィールドに移動します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

共通デバイス設定での Multilevel Precedence and Preemption 設定, （739 ページ）

共通デバイス設定での Multilevel Precedence and Preemption 設定

一般的なデバイス設定には、複数のユーザとそのデバイスに適用できる MLPP 関連の情報が含まれています。各デバイスは一般的なデバイス設定に関連付けられていることを確認します。これらの設定は、エンタープライズ パラメータの設定を上書きします。

はじめる前に

ドメインおよびドメイン リストの設定, （736 ページ）

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）] > [共通デバイス設定（Common Device Configuration）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存の共通デバイス設定を変更するには、検索条件を入力して [Find（検索）] をクリックし、結果のリストから共通デバイス設定を選択します。
- 新しい共通デバイス設定を追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ウィンドウの各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

Multilevel Precedence and Preemption のエンタープライズ パラメータの設定, （740 ページ）

Multilevel Precedence and Preemption のエンタープライズ パラメータの設定

MLPPの通知とプリエンプションを有効にするには、エンタープライズパラメータを設定します。個々のデバイスや一般的なデバイス設定のデバイスがデフォルトの MLPP 設定になっていると、MLLP 関連のエンタープライズ パラメータは、これらのデバイス、および一般的なデバイス設定に適用されます。

はじめる前に

共通デバイス設定での Multilevel Precedence and Preemption 設定, （739 ページ）

手順

ステップ 1 [システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] と選択します。

ステップ 2 [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウで MLPP エンタープライズ パラメータを設定します。パラメータとその設定オプションの詳細については、「関連項目」セクションを参照してください。

ステップ 3 [保存（Save）] をクリックします。

次の作業

Multilevel Precedence and Preemption のパーティションの設定, （742 ページ）

関連トピック

Multilevel Precedence and Preemption のエンタープライズ パラメータ, （741 ページ）

Multilevel Precedence and Preemption のエンタープライズ パラメータ

表 *87*：*Multilevel Precedence and Preemption* のエンタープライズ パラメータ

パラメータ	説明
MLPP Domain Identifier	ドメインを定義するには、このパラメータを設定します。MLPP サービスはドメインに適用されるため、Cisco Unified Communications Manager は、優先度レベルを備えた特定のドメインでの MLPP ユーザからのコールに属する接続およびリソースのみをマーキングします。Cisco Unified Communications Manager は、同じドメインの MLPP ユーザからの低優先コールのみをプリエンプション処理できます。 デフォルトは 000000 です。
MLPP 表示ステータス（MLPP Indication Status）	このパラメータは、MLPP 優先コールを通知するために、デバイスが MLPP トーンおよび特別なディスプレイを使用するかどうかを指定します。企業全体で MLPP 通知を有効にするには、このパラメータで MLPP 通知をオンに設定します。 デフォルトは [MLPP 通知がオフ（MLPP Indication turned off）] です。
MLPP Preemption Setting	このパラメータは、優先度の高いコールに対応するため、デバイスが（プリエンプション トーンなどの）プリエンプションやプリエンプション シグナリングを適用する必要があるかどうかを決定します。企業全体で MLPP プリエンプションを有効にするには、このパラメータを [強制プリエンプション（Forceful Preemption）] に設定します。 デフォルトは、[プリエンプションを許可しない（No preemption allowed）] です。
Precedence Alternate Party Timeout	優先コールでは、着信側が別の相手への転送を登録している場合、このタイマーは、着信側がプリエンプションを承認しないまたは優先コールに応答しなかった場合に、Cisco Unified Communications Manager がコールを別の相手に転送するまでの秒数を示します。 デフォルトは 30 秒です。

パラメータ	説明
Use Standard VM Handling for Precedence Calls	このパラメータは、優先コールをボイスメッセージング システムに転送するかどうかを決定します。 このパラメータが False に設定される場合は、優先順位が高いコールがボイスメッセージング システムに転送されません。このパラメータが True に設定される場合は、優先順位が高いコールがボイスメッセージング システムに転送されます。 MLPP では、このパラメータの推奨設定は False です。これは、ボイス メッセージング システムではなくユーザが優先コールに常に応答できるようにするためです。 デフォルトは False です。

Multilevel Precedence and Preemption のパーティションの設定

パーティションを設定して、電話番号（DN）の論理グループと、到達可能性の特徴が類似したルートパターンを作成します。パーティションに通常、配置されるデバイスは、DNs とルートパターンを含みます。これらのエンティティは、ユーザがダイヤルする DNs に関連付けられます。わかりやすくするために、パーティション名は通常、その特性を反映しています。

はじめる前に

Multilevel Precedence and Preemption のエンタープライズ パラメータの設定, （740 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックして新しいパーティションを作成します。

ステップ 3 [パーティション名、説明（Partition Name, Description）] フィールドに、ルート プランに固有のパーティション名を入力します。
パーティション名には、英数字とスペースの他にハイフン（-）とアンダースコア（_）を使用できます。パーティション名に関するガイドラインについては、オンライン ヘルプを参照してください。

ステップ 4 パーティション名の後にカンマ（,）を入力し、パーティションの説明を同じ行に入力します。
説明には、任意の言語で最大 50 文字を使用できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）、角括弧（[]）は使用できません。

説明を入力しなかった場合は、Cisco Unified Communications Manager が、このフィールドに自動的にパーティション名を入力します。

ステップ 5 複数のパーティションを作成するには、各パーティション エントリごとに 1 行を使います。

ステップ 6 [スケジュール（Time Schedule）] ドロップダウン リストから、このパーティションに関連付けるスケジュールを選択します。
スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）] を選択した場合は、パーティションが常にアクティブになります。

ステップ 7 次のオプション ボタンのいずれかを選択して、[タイム ゾーン（Time Zone）] を設定します。

- [発信側デバイス（Originating Device）]：このオプション ボタンを選択すると、発信側デバイスのタイムゾーンと [スケジュール（Time Schedule）] が比較され、パーティションが着信コールの受信に使用できるかどうかが判断されます。
- [特定のタイム ゾーン（Specific Time Zone）]：このオプション ボタンを選択した後、ドロップダウン リストからタイム ゾーンを選択します。選択されたタイム ゾーンと [スケジュール（Time Schedule）] が比較され、着信コールの受信にパーティションが使用できるかどうかが判断されます。

ステップ 8 [保存（Save）] をクリックします。

次の作業

Multilevel Precedence and Preemption のコーリング サーチ スペースの設定, （744 ページ）

関連トピック

パーティション名のガイドライン, （743 ページ）

パーティション名のガイドライン

コーリング サーチ スペースのパーティションのリストは最大 1024 文字に制限されています。つまり、CSS 内のパーティションの最大数は、パーティション名の長さによって異なります。次の表を使用して、パーティション名が固定長である場合のコーリングサーチスペースに追加できるパーティションの最大数を決定します。

表 *88*：パーティション名のガイドライン

パーティション名の長さ	パーティションの最大数
2 文字	340
3 文字	256
4 文字	204
5 文字	172

パーティション名の長さ	パーティションの最大数
。 ..	...
10 文字	92
15 文字	64

Multilevel Precedence and Preemption のコーリング サーチ スペースの設定

コーリング サーチ スペースは、パーティションの番号付きリストです。コーリング サーチ スペースは、IP フォン、ソフトフォン、ゲートウェイなどのコーリング デバイスがコールを完了しようとしたときに検索できるパーティションを決めます。

はじめる前に

Multilevel Precedence and Preemption のパーティションの設定, （742 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[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 [名前（Name）] フィールドに、名前を入力します。
各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

ステップ 4 [説明（Description）] フィールドに、説明を入力します
説明には、任意の言語で最大50文字を指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 [使用可能なパーティション（Available Partitions）] ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。

- パーティションが複数ある場合は、コントロール（Ctrl）キーを押したまま、適切なパーティションを選択します。

ステップ 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）] フィールドにパーティションを移動させます。

ステップ 7 （任意） [選択されたパーティション（Selected Partitions）] ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

ステップ 8 [保存（Save）] をクリックします。

次の作業

Multilevel Precedence and Preemption（MLPP）のルート パターンの設定, （745 ページ）

Multilevel Precedence and Preemption（MLPP）のルート パターンの設定

内部および外部コールの両方をルーティングまたはブロックするためにルート パターンを設定します。

はじめる前に

Multilevel Precedence and Preemption のコーリング サーチ スペースの設定, （744 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、[コール ルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルート パターン（Route Pattern）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のルート パターンの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果の一覧から既存のルート パターンを選択します。
- 新しいルート パターンを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [ルート パターンの設定（Route Pattern Configuration）] ウィンドウ内の各フィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクションを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

Multilevel Precedence and Preemption のトランスレーション パターンの設定, （747 ページ）

関連トピック

Multilevel Precedence and Preemption のルート パターン設定フィールド, （746 ページ）

Multilevel Precedence and Preemption のルート パターン設定フィールド

表 *89*：*Multilevel Precedence and Preemption* のルート パターン設定フィールド

フィールド	説明
ルート パターン	スペースを除き、数字とワイルドカードを含むルート パターンを入力します。たとえば、NANP の場合、一般的なローカル アクセスには 9.@、一般的なプライベート ネットワークの番号計画には 8XXX を入力します。有効な文字には、大文字の A、B、C、D と、国際的なエスケープ文字 + を表す \+ などがあります。
[MLPP優先度（MLPP Precedence）]	ドロップダウン リストから、このルート パターンに関する MLPP 優先設定を選択します。 • [エグゼクティブ オーバーライド（Executive Override）]：MLPP コールに関する最高優先設定。 • [フラッシュ オーバーライド（Flash Override）]：MLPP コールに関する 2 番目に高い優先設定。 • [フラッシュ（Flash）]：MLPP コールに関する 3 番目に高い優先設定。 • [即時（Immediate）]：MLPP コールに関する 4 番目に高い優先設定。 • [優先順位（Priority）]：MLPP コールに関する 5 番目に高い優先設定。 • [ルーチン（Routine）]：MLPP コールに関する最低優先設定。 • [デフォルト（Default）]：入力優先レベルをオーバーライドせずに、そのまま通過させます。
[ブロックコール率の適用（Apply Call Blocking Percentage）]	宛先コード制御（DCC）機能を有効にするには、このチェックボックスをオンにします。DCC を有効にすることにより、接続先に対して行われたフラッシュ コールおよび高優先コール以外のすべてのコールはフィルタ処理され、接続先に設定されているブロックコール率のクォータに基づいて許可または拒否されます。フラッシュ コールおよび高優先コールは必ず許可されます。DCC はデフォルトでディセーブルになっています。 [ブロックコール率の適用（Apply Call Blocking Percentage）] フィールドは、MLPP レベルが即時、優先順位、ルーチンまたはデフォルトである場合のみ有効になります。

フィールド	説明
ブロックコール率（%）	この宛先に関してブロックされるコールの割合を数値で入力します。この値は、この接続先に対して実行され、ルートパターンによってブロックされる低優先コールの割合を示します。この割合は低優先コールのみを制限し、この接続先にに行われたフラッシュ コルと高優先コールは常に許可されます。 [ブロックコール率（%）（Blocked Call Percentage (%)）] フィールドは、[ブロックコール率の適用（Apply Call Blocking Percentage）] チェックボックスがオンになっている場合にのみ有効になります。
[リソースプライオリティネームスペースネットワークドメイン（Resource Priority Namespace Network Domain）]	ドロップダウン リストボックスからリソースプライオリティ ネームスペース ネットワーク ドメインを選択します。[リソース プライオリティ ネームスペース ネットワーク ドメイン（Resource Priority Namespace Network Domains）] を設定するには、[システム（System）] > [MLPP] >[名前空間（Namespace）] > [リソースのプライオリティの名前空間のネットワークドメイン（Resource Priority Namespace Network Domain）] を選択します。

Multilevel Precedence and Preemption のトランスレーション パターンの設定

コールされてからコールをルーティングされる方法を指定するには、トランスレーション パターンを設定します。トランスレーション パターンを設定すると、システムで必要に応じて発信と発信された数字を処理できます。パターン一致が発生していることを確認すると、システムは後続の一致を実行するためにトランスレーション パターン用に設定されたコーリング サーチ スペースを使用します。

はじめる前に

Multilevel Precedence and Preemption（MLPP）のルート パターンの設定, （745 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[コール ルーティング（Call Routing）] > [トランスレーション パターン（Translation Pattern）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のトランスレーションパターンの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存のトランスレーション パターンを選択します。
- 新しいトランスレーション パターンを追加するには、[新規追加（Add New）] をクリックします。

ステップ 3 [MLPP 優先設定（MLPP Precedence）] ドロップダウン リストから、トランスレーション パターンに次のいずれかの設定を選択します。

- [エグゼクティブ オーバーライド（Executive Override）]：MLPP コールに関する最高優先設定。
- [フラッシュ オーバーライド（Flash Override）]：MLPP コールに関する 2 番目に高い優先設定。
- [フラッシュ（Flash）]：MLPP コールに関する 3 番目に高い優先設定。
- [イミディエート（Immediate）]：MLPP コールに関する 4 番目に高い優先設定。
- [プライオリティ（Priority）]：MLPP コールに関する 5 番目に高い優先設定。
- [ルーチン（Routine）]：MLPP コールに関する最低優先設定。
- [デフォルト（Default）]：入力優先レベルをオーバーライドせずに、そのまま通過させます。

ステップ 4 [リソース プライオリティ ネームスペース ネットワーク ドメイン（Resource Priority Namespace Network Domain）] ドロップダウン リストから、設定したリソース プライオリティ ネームスペース ネットワーク ドメインを選択します。

ステップ 5 [コーリング サーチ スペース（Calling Search Space）] ドロップダウン リストから、設定したコーリング サーチ スペースを選択します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

ゲートウェイの Multilevel Precedence and Preemption の設定, （748 ページ）

ゲートウェイの Multilevel Precedence and Preemption の設定

非 IP 通信デバイスと通信するように Cisco Unified Communications Manager を設定します。

はじめる前に

- 次のいずれかのゲートウェイを設定します。
  - Cisco Catalyst 6000 24 port FXS Gateway
  - Cisco Catalyst 6000 E1 VoIP Gateway
  - Cisco Catalyst 6000 T1 VoIP Gateway
  - Cisco DE-30+ Gateway
  - Cisco DT-24+ Gateway
  - H.323 ゲートウェイ

  ゲートウェイ設定の詳細については、ゲートウェイの設定タスク フロー, （67 ページ）を参照してください。
- Multilevel Precedence and Preemption のトランスレーション パターンの設定, （747 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）]>[ゲートウェイ（Gateway）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のゲートウェイの設定を変更するには、検索条件を入力して [検索（Find）] をクリックし、結果のリストからゲートウェイを選択します。
- 新しいゲートウェイを追加するには、次の手順を実行します。
  1. [新規追加（Add New）] をクリックします。
  2. [ゲートウェイ タイプ（Gateway Type）] ドロップダウン リストから、サポート ゲートウェイ モデルのいずれかを選択します。
  3. [Next] をクリックします。

ステップ 3 [ゲートウェイの設定（Gateway Configuration）] ウィンドウで MLPP のフィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクションを参照してください。

ステップ 4 [保存（Save）] をクリックします。

次の作業

電話機のMultilevel Precedence and Preemption の設定, （749 ページ）

関連トピック

ゲートウェイの Multilevel Precedence and Preemption 設定

電話機のMultilevel Precedence and Preemption の設定

注意 デバイスに対して、[MLPP 通知（MLPP Indication）] を [オフ（Off）] または [デフォルト（Default）]（デフォルトがオフの場合）に設定したとき、[MLPP プリエンプション（MLPP Preemption）] を [強制（Forceful）] に設定しないでください。

はじめる前に

- IP フォンを設定します。詳細については、エンドポイント デバイス設定, （321 ページ）を参照してください。
- ゲートウェイの Multilevel Precedence and Preemption の設定, （748 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [電話（Phone）] を選択します。

ステップ 2 検索条件を入力します。

ステップ 3 [検索（Find）] をクリックして、結果リストから電話を選択します。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウで MLPP のフィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクションを参照してください。

次の作業

Multilevel Precedence and Preemption コールの電話番号の設定, （752 ページ）

電話の Multilevel Precedence and Preemption 設定

表 *90*：電話の *Multilevel Precedence and Preemption* 設定

電話の MLPP 設定フィールド	説明
共通デバイス設定（Common Device Configuration）	設定した共通デバイス設定を選択します。共通デバイス設定には、特定のユーザに関連付けられた属性（サービスまたは機能）が含まれています。
[コーリングサーチスペース（Calling Search Space）]	ドロップダウン リストから、設定したコーリング サーチ スペース（CSS）を選択します。コーリング サーチ スペースは、検索対象のパーティションのコレクションで構成され、ダイヤル番号のルーティング方法を決めるために使用されます。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。
[MLPP ドメイン（MLPP Domain）]	MLPP ドメインのドロップダウン リストから、このデバイスに関連付けられる MLPP ドメインを選択します。[なし（None）] 値のままにした場合、このデバイスは共通デバイス設定で設定された値から、その MLPP ドメインを継承します。共通デバイス設定に [MLPP ドメイン（MLPP Domain）] の設定がない場合は、このデバイスの MLPP ドメインは MLPP Domain Identifier エンタープライズ パラメータの設定値から継承されます。

電話の **MLPP** 設定 フィールド	説明
[MLPP 通知（MLPP Indication）]	該当する場合、この設定は、優先トーンを再生可能なデバイスが MLPP 優先コールを発信するときにこの機能を使用するかどうかを指定します。 ドロップダウン リストで、次のオプションの中からこのデバイスに割り当てる設定を選択します。 • [デフォルト（Default）] : このデバイスは共通デバイス設定からその MLPP 通知設定を継承します。 • [オフ（Off）] : このデバイスは MLPP 優先コールの通知に対処して処理を行うことはありません。 • [オン（On）] : このデバイスは MLPP 優先コールの通知に対処して処理を行います。 （注） 次の設定の組み合わせを使ってデバイスを設定しないでください。[MLPP 通知（MLPP Indication）] を [オフ（Off）] または [デフォルト（Default）]（デフォルトがオフの場合）に設定し、[MLPPプリエンプション（MLPP Preemption）] を [強制（Forceful）] に設定。 MLPP通知をオンにすると（エンタープライズパラメータまたはデバイス レベルで）、MLPP通知がデバイスでオフになっている（オーバーライドされている）場合を除き、デバイスの回線の通常の呼び出し音設定の動作が無効になります。
[MLPP プリエンプション（MLPP Preemption）]	この設定は、すべてのデバイスで使用できる訳ではないことに留意してください。使用できる場合、この設定は、進行中のコールをプリエンプション処理可能なデバイスが MLPP 優先コールを発信するときにこの機能を使用するかどうかを指定します。 ドロップダウン リストで、次のオプションの中からこのデバイスに割り当てる設定を選択します。 • [デフォルト（Default）] : このデバイスは共通デバイス設定からその MLPP プリエンプション設定を継承します。 • [無効（Disabled）] : このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可しません。 • [強制（Forceful）] : このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可します。

Multilevel Precedence and Preemption コールの電話番号の設定

デバイスを設定した後、更新された [デバイス設定（Device Configuration）] ウィンドウから回線（ディレクトリ番号）を追加できます。

はじめる前に

電話機のMultilevel Precedence and Preemption の設定, （749 ページ）

手順

ステップ 1 Cisco Unified CM の管理の [デバイスの設定（Device Configuration）] ウィンドウで、該当する行の [新規 DN を追加（Add a new DN）] をクリックします。

ステップ 2 [ターゲット（接続先）（Target (Destination)）] フィールドに、この電話番号が優先コールを受信し、この番号とそのコール転送先の両方が優先コールに応答しない場合に、MLPP 優先コールを転送する番号を入力します。
値には、数字、シャープ（#）およびアスタリスク（*）を使用できます。

ステップ 3 [MLPP コーリング サーチ スペース（MLPP Calling Search Space）] ドロップダウン リストから、MLPP 代替パーティのターゲット（接続先）番号に関連付けるコーリング サーチ スペースを選択します。

ステップ 4 [MLPP 無応答時の着信転送までの時間（秒）（MLPP No Answer Ring Duration (seconds)）] で、この電話番号とそのコール転送先が優先コールに応答しない場合に、MLPP 優先コールをこの電話番号の代替パーティに転送するまでに待機する秒数（4 ～ 60）を入力します。
[優先代替パーティ タイムアウト（Precedence Alternate Party Timeout）] エンタープライズ パラメータで設定した値を使用するには、この設定を空白のままにします。

ステップ 5 [保存（Save）] をクリックします。

次の作業

Multilevel Precedence and Preemption のユーザ デバイス プロファイルの設定, （752 ページ）

Multilevel Precedence and Preemption のユーザ デバイス プロファイルの設定

ユーザ プロファイルが電話機に割り当てられると、その電話は、ユーザに関連付けられている CSS を含む割り当てられたユーザの設定を継承します。しかし、電話の CSS は、ユーザ プロファイルを上書きします。パターン一致が発生すると、Cisco Unified Communications Manager は、そのコールへのダイヤル パターンに関連付けられる優先度レベルを割り当てます。システムは、割り当てられた優先度レベルで優先度の高いコールとしてコール要求を設定します。

はじめる前に

Multilevel Precedence and Preemption コールの電話番号の設定, （752 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、[デバイス（Device）] > [デバイス設定（Device Settings）] > [デバイス プロファイル（Device Profile）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のデバイス プロファイルの設定を変更するには、検索条件を入力し、[検索（Find）] をクリックし、結果リストから既存のデバイス プロファイルを選択します。
- 新しいデバイス プロファイルを追加する手順は次のとおりです。
  - [新規追加（Add New）] をクリックします。
  - [デバイス プロファイル タイプ（Device Profile Type）] ドロップダウン リストから、デバイス タイプを選択します。
  - [Next] をクリックします。
  - [デバイス プロトコル（Device Protocol）] ドロップダウン リストから、[SIP（SIP）] か [SCCP（SCCP）] を選択します

ステップ 3 [Next] をクリックします。

ステップ 4 [MLPP ドメイン（MLPP Domain）] ドロップダウンリストから、設定した MLLP ドメインを選択します。

ステップ 5 MLPP 優先コールを発信するとき、優先トーンを再生できるデバイスがこの機能を使用するかどうかを指定するには、[MLPP 通知（MLPP Indication）] ドロップダウン リストから、次の設定のいずれかを選択します。

-
  - [デフォルト（Default）]：このデバイスは、デバイス プールから MLPP 設定を継承します。
  - [オフ（Off）]：このデバイスは、MLPP 優先コールの通知を処理しません。
  - [オン（On）]：このデバイスは、MLPP 優先コールの通知を処理します。

ステップ 6 [MLPPプリエンプション（MLPP Preemption）] リストから、以下のいずれかの設定を選択して、MLPP優先コールがあったときに進行中のコールをプリエンプション可能かどうかを指定します。

-
  - [デフォルト（Default）]：このデバイスは、デバイスプールからMLPPプリエンプションを継承します。
  - [無効（Disabled）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可しません。

- [強制（Forceful）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可します。

ステップ 7 [保存（Save）] をクリックします。

次の作業

Multilevel Precedence and Preemption のデフォルトのデバイス プロファイルの設定, （754 ページ）

Multilevel Precedence and Preemption のデフォルトのデバイス プロファイルの設定

ユーザがユーザ デバイス プロファイルがない電話機モデルにログインするたびに、デフォルトデバイスプロファイルを使用します。デフォルトのデバイスプロファイルは、特定のデバイスに関連付けられている機能とサービスで構成されています。

注意 次の設定の組み合わせを使って、デフォルトのデバイス プロファイルを設定しないでください。[MLPP 通知（MLPP Indication）] を [オフ（Off）] または [デフォルト（Default）]（デフォルトがオフの場合）に設定し、[MLPP プリエンプション（MLPP Preemption）] を [強制（Forceful）] に設定。

はじめる前に

Multilevel Precedence and Preemption のユーザ デバイス プロファイルの設定, （752 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、[デバイス（Device）] > [デバイス設定（Device Settings）] > [デフォルトのデバイス プロファイル（Default Device Profile）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のデフォルトのデバイス プロファイルの設定を変更するには、[デバイス プロファイルのデフォルト（Device Profile Defaults）] セクションから既存のデフォルトのデバイス プロファイルを選択します。

- 新しいデフォルトのデバイス プロファイルを追加するには、ドロップダウン リストからデバイスプロファイルの種類を選択後、[次へ（Next）] をクリックしてデバイスプロトコルを選択し、[次へ（Next）] をクリックします。

ステップ 3 [MLPP Domain（MLPP ドメイン）] ドロップダウン リストから、デバイスに関連付けるために設定した MLPP ドメインを選択します。

ステップ 4 [MLPP 通知（MLPP Indication）] ドロップダウン リストから、以下のいずれかの設定を選択して、MLPP 優先コールがあったときに優先トーンを再生できるデバイスで機能を使用するかどうかを指定します。

- [デフォルト（Default）]：このデバイスは、デバイス プールから MLPP 設定を継承します。
- [オフ（Off）]：このデバイスは、MLPP 優先コールの通知を処理しません。
- [オン（On）]：このデバイスは、MLPP 優先コールの通知を処理します。

ステップ 5 [MLPPプリエンプション（MLPP Preemption）] リストから、以下のいずれかの設定を選択して、MLPP優先コールがあったときに進行中のコールをプリエンプション可能かどうかを指定します。

- [デフォルト（Default）]：このデバイスは、デバイス プールから MLPP プリエンプションを継承します。
- [無効（Disabled）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可しません。
- [強制（Forceful）]：このデバイスは、高優先コールの実行が必要なときに、低優先コールのプリエンプションの実行を許可します。

ステップ 6 [保存（Save）] をクリックします。

Multilevel Precedence and Preemption の連携動作と制限事項

Multilevel Precedence and Preemption（MLPP）

表 *91*：***Multilevel Precedence and Preemption（MLPP）***

機能	データのやり取り
729 Annex A	729 Annex A がサポートされています。

機能	データのやり取り
Cisco エクステンション モビリティ	ユーザが Extension Mobility を使用してデバイスにログインしている場合、MLPP サービス ドメインはユーザ デバイス プロファイルに関連付けられたままになります。MLPP の表示とプリエンプションの設定も、Extension Mobility によって伝搬されます。デバイスまたはデバイス プロファイルのいずれかが MLPP をサポートしていない場合、これらの設定は伝搬されません。
Cisco Unified Communications Manager Assistant	MLPP は次のように Cisco Unified Communications Manager Assistant とやり取りします。 • Cisco Unified Communications Manager Assistant が MLPP 優先コールを処理する場合、Cisco Unified Communications Manager Assistant はコールの優先順位に従います。 • Cisco Unified Communications Manager Assistant は、他のすべてのコールをフィルタする場合と同じ方法で、MLPP 優先コールをフィルタします。コールの優先順位は、コールがフィルタ処理されるかどうかには影響しません。 • Cisco Unified Communications Manager Assistant は、コールの優先順位を登録しないため、Assistant Console でコールの優先順位を追加で表示することはありません。
即時転送	即時転送は、コールのタイプ（たとえば、優先コール）に関係なく、コールをボイスメッセージング メールボックスに転送します。代替パーティ転送（コールの優先順位）が有効化されると、無応答時転送（CFNA）は非アクティブ化されます。
リソース予約プロトコル（RSVP）	RSVP は本質的に MLPP をサポートします。『Cisco Unified Communications Manager System Guide』に、RSVP が有効化された場合に MLPP がどのように機能するかについて説明されています。
捕足サービス（Supplementary Services）	MLPP は、各サービスの連携動作について説明するサブセクションに記載されているとおりに、複数のラインアピアランス、コール転送、コール転送（フォワーディング）、3 ウェイ コール、コール ピックアップ、およびハント パイロットと連携動作します。

Multilevel Precedence and Preemption の制約事項

表 *92*：*Multilevel Precedence and Preemption* の制約事項

制約事項	説明
Bandwidth	Cisco Unified Communications Manager は、優先度の高いコール用にビデオ帯域幅を調整するときに、低優先コールをプリエンプション処理します。帯域幅がプリエンプション処理十分でない場合、Cisco Unified Communications Manager は、以前に予約した低ビデオ帯域幅を使用するようにエンドポイントに指示します。Cisco Unified Communications Manager がビデオ コールをプリエンプション処理するとき、プリエンプション処理される相手はプリエンプション トーンを受信し、コールがクリアされます。
コール詳細レコード	DRSN では、CDR は値 0、1、2、3、4 によって優先レベルを表します。ここで、DSN で使用される場合のように、0 はエクゼクティブ オーバーライドを指定し、4 は ルーチンを指定します。そのため、CDR は DRSN 形式を使用しません。
一般的なネットワーク機能のプリエンプション	一般的なネットワーク機能のプリエンプションサポートは、Cisco Unified Communications Manager が MGCP プロトコルを使用して制御し、MLPP プリエンプションを有効に設定された、標的型の Voice over IP ゲートウェイの T1-CAS および T1-PRI（北米）インターフェイスでのみ存在します。
クラスタ間トランク	クラスタ間トランク MLPP はダイヤル番号を介して優先情報を伝えます。ドメイン情報は保持されないため、着信コールのトランクごとに設定する必要があります。

制約事項	説明
[回線グループ（Line Groups）]	MLPP 対応デバイスは回線グループではサポートされません。次のガイドラインを推奨します。 • MLPP 対応デバイスは回線グループで設定しないでください。ただし、ルート グループはサポートされます。トランクの選択とハント方法の両方がサポートされます。 • MLPP 対応デバイスが回線グループまたはルート グループで設定されると、プリエンプション処理が行われたときに、ルート リストがデバイスをロックしない場合、プリエンプション処理されたコールは、ルート/ハント リスト内の他のデバイスに再ルーティングされ、コールを受け取ることができるデバイスがなくなった後でのみ、プリエンプションの通知を返すことができます。 • ルート リストは、優先コールのためにトランク選択とハンティングの 2 つのアルゴリズムのいずれかをサポートするように設定できます。方法 1 では、優先検索を直接実行します。方法 2 では、最初にフレンドリ検索を実行します。この検索が成功しないと、優先検索を実行します。方法 2 ではルート リストのデバイスを介した 2 つの反復が必要です。ルート リストが方法 2 に設定されると、回線グループを含む特定のシナリオでは、ルート リストが優先コールのためにデバイスを介して 2 回反復するように見える場合があります。
Look Ahead For Busy	Cisco Unified Communications Manager は Look Ahead For Busy（LFB）オプションをサポートしていません。
MLPP 通知	MLPP 通知対応デバイスのみが、トーンや呼出音のような MLPP 関連通知を生成します。優先コールが MLPP 通知対応でないデバイスで終了すると、優先呼び出し音は適用されません。優先コールが MLPP 通知対応でないデバイスから発信されると、優先折り返し音は適用されません。MLPP 通知対応でないデバイスがプリエンプト処理されたコール（つまり、コールが開始したプリエンプションの相手側）に関与する場合、プリエンプション トーンはデバイスに適用されません。
電話とトランク	電話では、MLPP 通知が無効化された（つまり、MLPP 通知がオフに設定されている）デバイスではプリエンプション処理ができません。トランクでは、MLPP 通知とプリエンプションは個別に機能します。

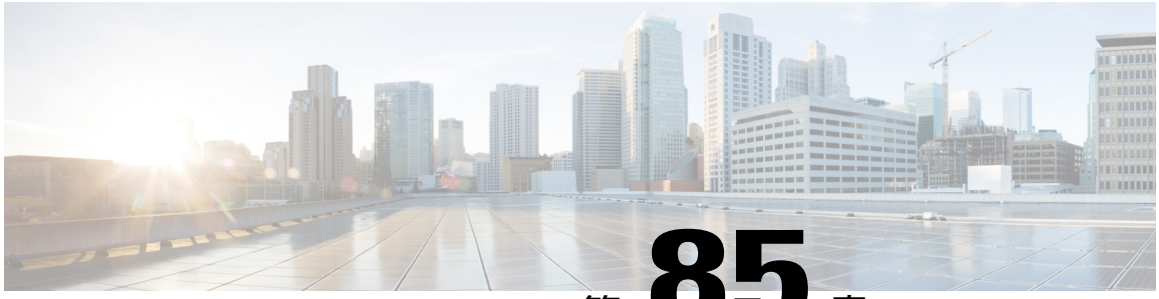
制約事項	説明
呼び出し音設定の動作	MLPP 通知をオンにすると（エンタープライズ パラメータ、共通デバイス設定、またはデバイス レベルで）、MLPP 通知がデバイスでオフになっている（オーバーライドされている）場合を除き、デバイスの回線の通常の呼び出し音設定の動作が無効になります。
SCCP	IOS ゲートウェイは、Cisco Unified Communications Manager への SCCP インターフェイスをサポートします。これらは BRI およびアナログ電話をサポートし、Cisco Unified Communications Manager でサポート対象の電話モデルとして表示されます。SCCP 電話は MLPP 機能をサポートし、特定の SIP ロードを持つ一部の電話も同様です。Cisco IP フォンのサポート情報については、関連する電話管理ガイドおよびユーザ ガイドを参照してください。

制約事項	説明
捕足サービス（Supplementary Services）	補足サービスのMLPPサポートは、次の制約事項を指定します。 • MLPP は基本的なコール ピックアップ機能およびグループ コール ピックアップ機能のみをサポートし、その他のグループ ピックアップはサポートしません。 • 着信MLPPコールの不在転送（CFA）サポートにより、MLPP代替パーティ（MAP）ターゲットが設定されている場合には、着信側の MAP ターゲットにコールが常に転送されます。設定が誤っている場合（MAP ターゲットが指定されていない場合）、コールは拒否され、発信側にリオーダー音が聞こえます。 • 着信 MLPP コールの無応答時転送（CFNA）サポートにより、コールは CFNA ターゲットに 1 回転送されます。MAP ターゲットが設定されている場合、最初のホップの後にコールに対する応答がないと、コールは元の着信側のMAPターゲットに転送されます。設定が誤っている場合（MAP ターゲットが指定されていない場合）、コールは拒否され、発信側にリオーダー音が聞こえます。 • 着信 MLPP コールの話中転送（CFB）サポートにより、設定されている転送ホップの最大数までコールが転送されます。MAP ターゲットが設定されている場合、最大ホップ数に達すると、コールは元の着信側のMAPターゲットに転送されます。設定が誤っている場合（MAP ターゲットが指定されていない場合）、コールは拒否され、発信側にリオーダー音が聞こえます。 • ハント パイロット サポートについては、ハント グループのアルゴリズムは [最長アイドル時間（Longest Idle Time）]、[トップダウン方式（Top Down）]、または [サーキュラー（Circular）] を指定する必要があります。取り込み中の処理、無応答処理、および登録解除時の処理に関するハント グループのオプションが、[次のメンバへ、ただし次のグループへは行かない（Try next member, but do not go to next group）] に設定されていることを確認します。プリエンプションは単独のハント グループでのみ行われます。
ユーザ アクセス チャネル	ユーザ アクセス チャネルは、MLPP プリエンプションが有効として設定されている必要がある、次の Cisco Unified IP Phone モデルでのみサポートされます。 • Cisco Unified IP Phone 7960、7962、7965 • Cisco Unified IP Phone 7940、7942、7945

第 XI 部

参考情報

- Cisco Unified Communications Manager での TCP および UDP ポートの使用，765 ページ
- IM and Presence Service のポート使用状況の情報，787 ページ



第 85 章

Cisco Unified Communications Manager での TCP および UDP ポートの使用

この章では、Cisco Unified Communications Manager がクラスタ内接続および外部アプリケーションまたはデバイスとの通信に使用する TCP ポートと UDP ポートの一覧を示します。また、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセス コントロール リスト（ACL）、および Quality of Service（QoS）を設定するために重要な情報も記載されています。

- Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要，765 ページ
- ポートの説明，767 ページ
- ポート参照，784 ページ

Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要

Cisco Unified Communications Manager の TCP および UDP ポートは、次のカテゴリに整理されます。

- Cisco Unified Communications Manager サーバの間のクラスタ内ポート
- 共通サービス ポート
- Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート
- CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求
- Cisco Unified Communications Manager から電話機への Web 要求
- 電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

- ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信
- アプリケーションと Cisco Unified Communications Manager との間の通信
- CTL クライアントとファイアウォールとの通信
- HP サーバ上の特殊なポート

上記のそれぞれのカテゴリのポートの詳細については、「“ポートの説明”」を参照してください。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

ポートの参照は、特に Cisco Unified Communications Manager に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、インストールされている Cisco Unified Communications Manager のバージョンに一致するバージョンのマニュアルを使用していることを確認してください。

ほとんどすべてのプロトコルは双方向ですが、セッション送信元からみた方向性は想定されています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベスト プラクティスとしてこのような変更は推奨しません。Cisco Unified Communications Manager が内部使用に限って複数のポートを開くことに注意してください。

Cisco Unified Communications Manager ソフトウェアをインストールすると、デフォルトではサービスアビリティ用に次のネットワーク サービスが自動的にインストールされてアクティブになります。詳細については、「“Cisco Unified Communications Manager サーバの間のクラスタ内ポート”」を参照してください。

- Cisco Log Partition Monitoring（共通パーティションを監視および消去します。このサービスは、カスタム共通ポートを使用しません）
- Cisco Trace Collection Service（TCTS ポート使用）
- Cisco RIS Data Collector（RIS サーバ ポート使用）
- Cisco AMC Service（AMC ポート使用）

ファイアウォール、ACL、または QoS の設定は、トポロジ、テレフォニー デバイスおよびテレフォニー サービスの配置とネットワーク セキュリティ デバイスの配置との関係、および使用中のアプリケーションとテレフォニー拡張機能によって異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

（注） Cisco Unified Communications Manager でマルチキャスト保留音（MoH）ポートを設定することもできます。管理者が実際のポート値を指定するため、マルチキャスト MOH のポート値は提供されません。

（注） システムのエフェメラル ポート範囲は 32768 ～ 61000 です。詳細については、http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.htmlを参照してください。

ポートの説明

Cisco Unified Communications Manager サーバがクラスタ間で使用するポート

表 *93*：*Cisco Unified Communications Manager* サーバがクラスタ間で使用するポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	RTMT	1090、1099 / TCP	RTMT パフォーマンスモニタ、データ収集、ロギング、およびアラート向けの Cisco AMC Service
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1500、1501 / TCP	データベース接続（1501 / TCP はセカンダリ接続）
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1510 / TCP	CAR IDS DB。CAR IDS エンジンが、クライアントからの接続要求を監視します。
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1511 / TCP	CAR IDS DB。アップグレード時に、CAR IDS のインスタンスをもう 1 つ開始するために使用される代替ポート。
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1515 / TCP	インストール時のノード間でのデータベースレプリケーション

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Cisco Extended Functions（QRT）	Unified Communications Manager（DB）	2552 / TCP	Cisco Unified Communications Manager データベース変更通知をサブスクライバが受信できるようにします。
Unified Communications Manager	Unified Communications Manager	2551 / TCP	アクティブ/バックアップ判別のための Cisco Extended Services 間のクラスタ間通信
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	2555 / TCP	Real-time Information Services（RIS）データベース サーバ
Unified Communications Manager（RTMT、AMC、またはSOAP）	Unified Communications Manager（RIS）	2556 / TCP	Cisco RIS 向け Real-time Information Services（RIS）データベースクライアント
Unified Communications Manager（DRS）	Unified Communications Manager（DRS）	4040 / TCP	DRS マスターエージェント
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5001 / TCP	このポートは、SOAP モニタがリアルタイムモニタリングサービスに使用します。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5002 / TCP	このポートは、SOAP モニタがパフォーマンスモニタ サービスに使用します。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5003 / TCP	このポートは、SOAP モニタがコントロールセンターサービスに使用します。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5004 / TCP	このポートは、SOAP モニタがログ コレクションサービスに使用します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5007 / TCP	SOAP モニタ
Unified Communications Manager（RTMT）	Unified Communications Manager（TCTS）	エフェメラル / TCP	Cisco Trace Collection Tool Service（TCTS）：RTMT Trace and Log Central（TLC）向けのバックエンドサービス
Unified Communications Manager（Tomcat）	Unified Communications Manager（TCTS）	7000、7001、7002 / TCP	このポートは、Cisco Trace Collection Tool Service と Cisco Trace Collection Servlet との通信に使用されます。
Unified Communications Manager（DB）	Unified Communications Manager（CDLM）	8001 / TCP	クライアント データベース変更通知
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8002 / TCP	クラスタ間通信サービス
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8003 / TCP	クラスタ間通信サービス（CTI 対象）
Unified Communications Manager	CMI マネージャ	8004 / TCP	Cisco Unified Communications Manager と CMI マネージャとのクラスタ間通信
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8005 / TCP	Tomcat シャットダウンスクリプトで使用される内部リスニング ポート
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8080 / TCP	診断テストのためのサーバ間の通信
ゲートウェイ	Unified Communications Manager	8090	CUCM と GW（Cayuga インターフェイス）が Gateway Recording 機能のための通信に使用する HTTP ポート
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager（IPSec）	Unified Communications Manager（IPSec）	8500 / TCP および UDP	IPSec クラスタ マネージャによるシステムデータのクラスタ間複製
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	8888 ～ 8889 / TCP	RIS サービス マネージャのステータス要求と応答
Location Bandwidth Manager（LBM）	Location Bandwidth Manager（LBM）	9004 / TCP	LBM 間のクラスタ間通信

共通サービス ポート

表 *94*：共通サービス ポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
エンドポイント（Endpoint）	Unified Communications Manager	7	Internet Control Message Protocol（ICMP）。このプロトコル番号がエコー関連のトラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
Unified Communications Manager	エンドポイント（Endpoint）		
Unified Communications Manager（DRS、CDR）	SFTP サーバ	22 / TCP	SFTP サーバにバックアップデータを送信します。（DRS ローカル エージェント） SFTP サーバに CDR データを送信します。
エンドポイント（Endpoint）	Unified Communications Manager（DHCP サーバ）	67 / UDP	DHCP サーバとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP サーバを実行することは推奨しません。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	DHCP サーバ（DHCP Server）	68 / UDP	DHCP クライアントとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP クライアントを実行することは推奨しません。その代わりに、Cisco Unified Communications Manager には固定 IP アドレスを設定します。
エンドポイントまたはゲートウェイ	Unified Communications Manager	69、6969、次にエフェメラル / UDP	電話機およびゲートウェイに対する Trivial File Transfer Protocol（TFTP）サービス
エンドポイントまたはゲートウェイ	Unified Communications Manager	6970 / TCP	マスター サーバとプロキシ サーバ間の Trivial File Transfer Protocol（TFTP） 電話機とゲートウェイに対する TFTP サーバの HTTP サービス
Unified Communications Manager	NTP サーバ（NTP Server）	123 / UDP	ネットワーク タイム プロトコル（NTP）
SNMP サーバ	Unified Communications Manager	161 / UDP	SNMP サービス応答（管理アプリケーションからの要求）
CUCM サーバ SNMP マスター エージェント アプリケーション	SNMP トラップの宛先	162 / UDP	SNMP トラップ
SNMP サーバ	Unified Communications Manager	199 / TCP	SMUX サポートのためのネイティブ SNMP エージェント リスニング ポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	DHCP サーバ（DHCP Server）	546 / UDP	DHCPv6。IPv6 用の DHCP ポート。
Unified Communications Manager Serviceability	Location Bandwidth Manager（LBM）	5546 / TCP	Enhanced Location CAC Serviceability
Unified Communications Manager	Location Bandwidth Manager（LBM）	5547 / TCP	コールアドミッションの要求および帯域幅の縮小
Unified Communications Manager	Unified Communications Manager	6161 / UDP	ネイティブエージェントMIB要求を処理するために、マスターエージェントとネイティブエージェントとの通信に使用されます。
Unified Communications Manager	Unified Communications Manager	6162 / UDP	ネイティブエージェントから生成された通知を転送するために、マスターエージェントとネイティブエージェントとの通信に使用されます。
中央集中型 TFTP	代替 TFTP（Alternate TFTP）	6970 / TCP	中央集中型 TFTP ファイル ロケータ サービス
Unified Communications Manager	Unified Communications Manager	7161 / TCP	SNMPマスターエージェントとサブエージェントとの通信に使用されます。
SNMP サーバ	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol（CDP）エージェントが、CDP実行可能機器と通信します。
エンドポイント（Endpoint）	Unified Communications Manager	443、8443/TCP	Cisco ユーザ データ サービス（UDS）の要求に使用されます。
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Cisco Unified Communications Manager にある TAPS を利用してCRS要求を処理します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager アプリケーションが、UDP でこのポートにアラームを送信します。Cisco Unified Communications Manager MIB エージェントが、Cisco Unified Communications Manager MIB 定義に従って、このポートを監視し、SNMP トラップを生成します。
Unified Communications Manager	Unified Communications Manager	5060、5061 / TCP	トランクベースの SIP サービスを提供します。
Unified Communications Manager	Unified Communications Manager	7501	クラスタ間検索サービス（ILS）の証明書ベースの認証に使用されます。
Unified Communications Manager	Unified Communications Manager	7502	ILS のパスワード ベース認証に使用されます。

Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート

表 *95*：*Cisco Unified Communications Manager* と *LDAP* ディレクトリとの間のポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	外部ディレクトリ	389、636、3268、3269 / TCP	外部ディレクトリ（Active Directory、Netscape Directory）への Lightweight Directory Access Protocol（LDAP）クエリ
外部ディレクトリ	Unified Communications Manager	エフェメラル	

CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求

表 *96*：*CCMAdmin* または *CCMUser* から *Cisco Unified Communications Manager* への *Web* 要求

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ブラウザ	Unified Communications Manager	80、8080 / TCP	ハイパーテキスト転送プロトコル（HTTP）
ブラウザ	Unified Communications Manager	443、8443 / TCP	Hypertext Transport Protocol over SSL（HTTPS）

Cisco Unified Communications Manager から電話機への Web 要求

表 *97*：*Cisco Unified Communications Manager* から電話機への *Web* 要求

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager • QRT • RTMT • [電話の検索と一覧表示（Find and List Phones）] ページ • [電話の設定（Phone Configuration）] ページ	電話	80/TCP	ハイパーテキスト転送プロトコル（HTTP）

電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

表 *98*：電話機と *Cisco Unified Communications Manager* との間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
電話	Unified Communications Manager	53 / TCP	Session Initiation Protocol（SIP）電話機が、ドメイン ネーム システム（DNS）を使用して、完全修飾ドメイン名（FQDN）を解決します。 （注） デフォルトでは、一部のワイヤレス アクセス ポイントは TCP の 53 番ポートをブロックし、FQDN を使用しながら CUCM を設定しているときに、ワイヤレス SIP 電話機が登録されないようにします。
電話	Unified Communications Manager（TFTP）	69、次にエフェメラル / UDP	ファームウェアおよび設定ファイルのダウンロードに使用される Trivial File Transfer Protocol（TFTP）
電話	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol（SCCP）
電話	Unified Communications Manager	2443 / TCP	Secure Skinny Client Control Protocol（SCCPS）

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
電話	Unified Communications Manager	2445 / TCP	エンドポイントに信頼検証サービスを提供します。
電話	Unified Communications Manager（CAPF）	3804 / TCP	ローカルで有効な証明書（LSC）を IP Phone に発行するための認証局プロキシ機能（CAPF）リスニングポート
電話	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol（SIP）電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager	5061 TCP	Secure Session Initiation Protocol（SIPS）電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager（TFTP）	6970 TCP	ファームウェアおよび設定ファイルの HTTP ベースのダウンロード
電話	Unified Communications Manager（TFTP）	6971、6972 / TCP	TFTP への HTTPS インターフェイス。電話機が、TFTP からセキュアな設定ファイルをダウンロードするためにこのポートを使用します。
電話	Unified Communications Manager	8080 / TCP	XML アプリケーション、認証、ディレクトリ、サービスなどで電話機が使用する URL。サービスごとにこれらのポートを設定できます。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
電話	Unified Communications Manager	9443 / TCP	電話機が、認証された連絡先検索にこのポートを使用します。
IP VMS	電話	16384 ～ 32767 / UDP	Real-Time Protocol（RTP）、Secure Real-Time Protocol（SRTP） （注） 他のデバイスは全範囲を使用しますが、Cisco Unified Communications Manager は 24576 ～ 32767 だけを使用します。
電話	IP VMS		

ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

表 *99*：ゲートウェイと *Cisco Unified Communications Manager* との間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ゲートウェイ	Unified Communications Manager	47、50、51	Generic Routing Encapsulation（GRE）、Encapsulating Security Payload（ESP）、認証ヘッダー（AH）。これらのプロトコル番号は、暗号化された IPSec トラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ゲートウェイ	Unified Communications Manager	500 / UDP	IP Security（IPSec）プロトコル確立のためのインターネットキーエクスチェンジ（IKE）
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager（TFTP）	69、次にエフェメラル / UDP	トリビアルファイル転送プロトコル（TFTP）
Cisco Intercompany Media Engine（CIME）トランクを使用した Unified Communications Manager	CIME ASA	1024 ～ 65535 / TCP	ポートマッピングサービス。CIME オフパス導入モデルでのみ使用します。
Gatekeeper	Unified Communications Manager	1719 / UDP	ゲートキーパー（H.225）RAS
ゲートウェイ	Unified Communications Manager	1720 / TCP	H.323 ゲートウェイおよびクラスタ間トランク（ICT）向けの H.225 シグナリングサービス
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	ゲートキーパー制御トランク上の H.225 シグナリング サービス
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	音声、ビデオ、およびデータを確立するための H.245 シグナリングサービス （注） ゲートウェイの種類によって異なる、リモート システムで使用される H.245 ポート。 IOS ゲートウェイでの H.245 ポート範囲は、11000 ～ 65535 です。
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol（SCCP）
ゲートウェイ	Unified Communications Manager	2001 / TCP	Cisco Unified Communications Manager の導入で使用する 6608 ゲートウェイ用アップグレードポート
ゲートウェイ	Unified Communications Manager	2002 / TCP	Cisco Unified Communications Manager の導入で使用する 6624 ゲートウェイ用アップグレードポート
ゲートウェイ	Unified Communications Manager	2427 / UDP	Media Gateway Control Protocol（MGCP）ゲートウェイ コントロール
ゲートウェイ	Unified Communications Manager	2428 / TCP	Media Gateway Control Protocol（MGCP）バックホール

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
--	--	4000 ～ 4005 / TCP	Cisco Unified Communications Manager に音声、ビデオ、およびDチャネルのポートがないときには、これらのポートがこのようなメディアのファントム Real-Time Transport Protocol（RTP）ポートおよび Real-Time Transport Control Protocol（RTCP）ポートとして使用されます。
ゲートウェイ	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol（SIP）ゲートウェイおよびクラスタ間トランク（ICT）
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	5061 / TCP	Secure Session Initiation Protocol（SIPS）ゲートウェイおよびクラスタ間トランク（ICT）
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	16384 ～ 32767 / UDP	Real-Time Protocol（RTP）、Secure Real-Time Protocol（SRTP） （注） 他のデバイスは全範囲を使用しますが、Cisco Unified Communications Manager は 24576 ～ 32767 だけを使用します。
Unified Communications Manager	ゲートウェイ		

アプリケーションと Cisco Unified Communications Manager との間の通信

表 *100*：アプリケーションと *Cisco Unified Communications Manager* との間の通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
CTL クライアント	Unified Communications Manager CTL プロバイダー	2444 / TCP	Cisco Unified Communications Manager の証明書信頼リスト（CTL）プロバイダーリスニングサービス
Cisco Unified Communications アプリケーション	Unified Communications Manager	2748 / TCP	CTI アプリケーションサーバ
Cisco Unified Communications アプリケーション	Unified Communications Manager	2749 / TCP	CTI アプリケーション（JTAPI/TSP）と CTI Manager 間の TLS 接続
Cisco Unified Communications アプリケーション	Unified Communications Manager	2789 / TCP	JTAPI アプリケーション サーバ
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Communications Manager Assistant サーバ（以前の IPMA）
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 ～ 1129 / TCP	Cisco Unified Communications Manager Attendant Console（AC）JAVA RMI レジストリ サーバ
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI サーバは、RMI コールバック メッセージをこれらのポートを使用するクライアントに送信します。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console（AC）RMI サーバ バインド ポート：RMI サーバは、これらのポートにRMI メッセージを送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Communications Manager Attendant Console（AC）サーバ回線状態ポートは、Attendant Console サーバから ping および登録メッセージを受信し、Attendant Console サーバに回線状態を送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Communications Manager Attendant Console（AC）クライアントは、回線状態情報およびデバイス状態情報のために AC サーバに登録されます。
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Communications Manager Attendant Console（AC）クライアントは、コール制御のために AC サーバに登録されます。
SAF/CCD を使用する Unified Communications Manager	SAF イメージを実行する IOS ルータ	5050 / TCP	EIGRP/SAF プロトコルを実行するマルチサービス IOS ルータ。

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
Unified Communications Manager	Cisco Intercompany Media Engine（IME）サーバ	5620 / TCP このポートでは、ポート番号5620の使用を推奨しますが、CLI コマンドの add ime vapserver または set ime vapserver port を Cisco IME サーバで実行することにより、値を変更できます。	VAP プロトコルは、Cisco Intercompany Media Engine サーバとの通信に使用されます。
Cisco Unified Communications アプリケーション	Unified Communications Manager	8443 / TCP	課金アプリケーションまたはテレフォニー管理アプリケーションなどのサードパーティが、Cisco Unified Communications Manager データベースに対してプログラムで読み書きするために使用する AXL/SOAP API。

CTL クライアントとファイアウォールとの通信

表 *101*：*CTL* クライアントとファイアウォールとの通信

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
CTL クライアント	TLS プロキシ サーバ	2444 / TCP	ASA ファイアウォールの証明書信頼リスト（CTL）プロバイダー リスニング サービス

HP サーバ上の特殊なポート

表 *102*：*HP* サーバ上の特殊なポート

送信元（送信者）	送信先（リスナー）	接続先ポート	目的
エンドポイント（Endpoint）	HP SIM	2301 / TCP	HP エージェントへの HTTP ポート
エンドポイント（Endpoint）	HP SIM	2381 / TCP	HP エージェントへの HTTPS ポート
エンドポイント（Endpoint）	Compaq 管理エージェント	25375、25376、25393 / UDP	COMPAQ 管理エージェント拡張（cmaX）
エンドポイント（Endpoint）	HP SIM	50000 ～ 50004 / TCP	HP SIM への HTTPS ポート

ポート参照

ファイアウォール アプリケーション インスペクション ガイド

ASA シリーズ参考情報

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

『PIX Application Inspection Configuration Guide』

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

『FWSM 3.1 Application Inspection Configuration Guide』

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF TCP/UDP ポート割り当てリスト

Internet Assigned Numbers Authority（IANA）IETF 割り当てポート リスト

http://www.iana.org/assignments/port-numbers

IP テレフォニー設定とポート使用に関するマニュアル

『Cisco CRS 4.0 (IP IVR and IPCC Express) Port Utilization Guide』

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

『Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions』

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

『Cisco Unified Communications Manager Express Security Guide to Best Practices』

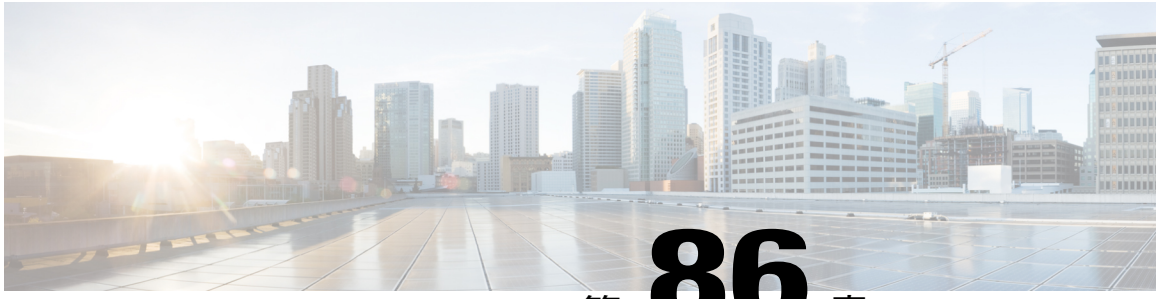
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

『Cisco Unity Express Security Guide to Best Practices』

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware ポート割り当てリスト

vCenter Server、ESX ホストおよびその他のネットワーク コンポーネント管理アクセス用の TCP および UDP ポート



第 86 章

IM and Presence Service のポート使用状況の情報

- IM and Presence サービス ポートの使用方法の概要，787 ページ
- テーブルで照合する情報，788 ページ
- IM and Presence サービス ポート リスト，788 ページ

IM and Presence サービス ポートの使用方法の概要

このマニュアルには、IM and Presence Service が、クラスタ内接続用および、外部アプリケーションまたは外部デバイスとの通信用に使用する TCP および UDP ポートの一覧を示します。これは、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセス コントロール リスト（ACL）、および Quality of Service（QoS）を設定するうえで重要な情報となります。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

事実上すべてのプロトコルが双方向で行われますが、このマニュアルではセッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベスト プラクティスとしてこのような変更は推奨しません。IM and Presence Service が内部使用に限って複数のポートを開くことに注意してください。

このドキュメントのポートは、IM and Presence サービスに特別に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、インストールされている IM and Presence Service のバージョンに一致する正しいバージョンのマニュアルを使用していることを確認してください。

ファイアウォール、ACL、または QoS の設定内容は、トポロジ、ネットワーク セキュリティ デバイスの配置に対するデバイスとサービスの配置、および使用するアプリケーションとテレフォ

ニー拡張機能の種類に応じて異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

テーブルで照合する情報

この表では、このドキュメントの表のそれぞれに照合する情報を定義します。

表 *103*：表の内容

表の項目	説明
送信元（From）	ポートに要求を送信するクライアント
移行後	ポートで要求を受信するクライアント
[役割（Role）]	クライアントまたはサーバのアプリケーションまたはプロセス
プロトコル	通信の確立と終了に使用されるセッション層プロトコル、またはトランザクションの要求と応答に使用されるアプリケーション層プロトコルのどちらか。
トランスポートプロトコル（Transport Protocol）	コネクション型（TCP）またはコネクションレス型（UDP）のトランスポート層プロトコル
宛先/リスナー	要求の受信に使用されるポート
ソース/送信元	要求の送信に使用されるポート

IM and Presence サービス ポート リスト

次のテーブルは、IM and Presence サービスがクラスタ内とクラスタ間のトラフィックに使用するポートを示します。

表 *104*：*IM and Presence* サービス ポート：*SIP* プロキシの要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
SIP ゲートウェイ ---------- [IM and Presence]	[IM and Presence] ---------- SIP ゲートウェイ	SIP	TCP/UDP	[5060]	エフェメラル	デフォルトの SIP プロキシの UDP および TCP リスナー
SIP ゲートウェイ	[IM and Presence]	SIP	TLS	5061	エフェメラル	TLS サーバ認証のリスナー ポート
[IM and Presence]	[IM and Presence]	SIP	TLS	5062	エフェメラル	TLS 相互認証のリスナー ポート
[IM and Presence]	[IM and Presence]	SIP	UDP/TCP	5049	エフェメラル	内部ポート。ローカルホストトラフィック専用。
[IM and Presence]	[IM and Presence]	HTTP	[TCP]	8081	エフェメラル	設定の変更を示す設定のエージェントからの HTTP 要求に使用されます。
サードパーティ製クライアント	[IM and Presence]	HTTP	[TCP]	8082	エフェメラル	デフォルトの IM and Presence HTTPのリスナー。サードパーティ製クライアントからの接続に使用されます。
サードパーティ製クライアント	[IM and Presence]	HTTPS	TLS/TCP	8083	エフェメラル	デフォルトの IM and Presence HTTPS リスナー。サードパーティ製クライアントからの接続に使用されます。

表 *105*：*IM and Presence* サービス ポート：*Presence* エンジンの要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（**Transport Protocol**）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	IM and Presence（Presence Engine）	SIP	UDP/TCP	5080	エフェメラル	デフォルトの SIP UDP/TCP リスナー ポート
IM and Presence（Presence Engine）	IM and Presence（Presence Engine）	Livebus	UDP	50000	エフェメラル	内部ポート。ローカル ホスト トラフィック専用。LiveBus メッセージング ポート。IM and Presence サービスは、このポートをクラスタ通信に使用します。

表 *106*：*IM and Presence* サービス ポート：シスコの *Tomcat WebRequests*

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（**Transport Protocol**）	宛先/リスナー	ソース/送信元	備考
ブラウザ	[IM and Presence]	HTTPS	[TCP]	8080	エフェメラル	Web アクセスに使用されます。
ブラウザ	[IM and Presence]	AXL/HTTPS	TLS/TCP	8443	エフェメラル	SOAP によりデータベースおよびサービス アビリティへのアクセスを提供します。
ブラウザ	[IM and Presence]	HTTPS	TLS/TCP	8443	エフェメラル	Web 管理へのアクセスを提供します。
ブラウザ	[IM and Presence]	HTTPS	TLS/TCP	8443	エフェメラル	ユーザ オプション ページへのアクセスを提供します。

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
ブラウザ	[IM and Presence]	SOAP	TLS/TCP	8443	エフェメラル	SOAP により Cisco Unified Personal Communicator、Cisco Unified Mobility Advantage、およびサードパーティ製の API クライアントへのアクセスを提供します。

表 *107*：*IM and Presence* サービス ポート：外部社内ディレクトリ要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence] ---------- 外部社内ディレクトリ	外部社内ディレクトリ ---------- [IM and Presence]	LDAP	[TCP]	389 / 3268	エフェメラル	ディレクトリプロトコルを外部社内ディレクトリと統合できるようにします。この LDAP ポートは、統合される社内ディレクトリによって異なります（デフォルトは 389）。Netscape Directory の場合は、別のポートで LDAP トラフィックを受信するよう設定できます。 認証用に IM&P と LDAP サーバ間の通信を LDAP に許可します。

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	外部社内ディレクトリ	LDAPS	[TCP]	636	エフェメラル	ディレクトリプロトコルを外部社内ディレクトリと統合できるようにします。このLDAPポートは、統合される社内ディレクトリによって異なります（デフォルトは636）。

表 *108*：*IM and Presence* サービス ポート：リクエストの設定

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（設定エージェント）	IM and Presence（設定エージェント）	[TCP]	[TCP]	8600	エフェメラル	設定エージェントのハートビート ポート

表 *109*：*IM and Presence* サービス ポート：*Certificate Manager* の要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	証明書マネージャ	[TCP]	[TCP]	7070	エフェメラル	内部ポート。ローカルホストトラフィック専用。

表 *110*：*IM and Presence* サービス ポート：*IDS*データベースの要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（データベース）	IM and Presence（データベース）	[TCP]	[TCP]	1500	エフェメラル	データベースクライアント用の内部IDSポート。ローカルホストトラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	[TCP]	[TCP]	1501	エフェメラル	内部ポート：アップグレード中にIDSの2次インスタンスを始動するための代替ポートです。ローカルホストトラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	XML	[TCP]	1515	エフェメラル	内部ポート。ローカルホストトラフィック専用。DB レプリケーション ポート。

表 *111*：*IM and Presence* サービス ポート：*IPSec*マネージャからの要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（IPSec）	IM and Presence（IPSec）	専用	UDP/TCP	8500	8500	内部ポート：ipsec_mgrデーモンがプラットフォームデータ（ホスト）の証明書のクラスタ レプリケーションに使用するクラスタ マネージャ ポートです。

表 *112*：*IM and Presence* サービス ポート：*DRF*にマスター エージェント サーバ要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（DRF）	IM and Presence（DRF）	[TCP]	[TCP]	4040	エフェメラル	DRF Master Agent サーバ ポート。Local Agent、GUI、および CLI からの接続を受け入れます。

表 *113*：*IM and Presence* サービス ポート：*RISDC* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	[TCP]	[TCP]	2555	エフェメラル	Real-time Information Services（RIS）データベースサーバ。クラスタ内の他の RISDC サービスに接続し、クラスタ全体のリアルタイム情報を提供します。
IM and Presence（RIMT/AMC/SOAP）	IM and Presence（RIS）	[TCP]	[TCP]	2556	エフェメラル	Cisco RIS の Real-time Information Services（RIS）データベースクライアント。RIS クライアント接続で、リアルタイム情報を取得できるようにする

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	[TCP]	[TCP]	8889	8888	内部ポート。ローカルホストトラフィック専用。サービスステータスの要求および応答用として、RISDC（システム アクセス）が TCP で servM にリンクするために使用します。

表 *114*：*IM and Presence* サービス ポート：*SNMP* の要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
SNMP サーバ	[IM and Presence]	SNMP	UDP	161、8161	エフェメラル	SNMP ベースの管理アプリケーションにサービスを提供
[IM and Presence]	[IM and Presence]	SNMP	UDP	6162	エフェメラル	SNMP マスター エージェントから転送される要求を受信するネイティブ SNMP エージェント。
[IM and Presence]	[IM and Presence]	SNMP	UDP	6161	エフェメラル	ネイティブ SNMP エージェントからのトラップ情報を受信し、管理アプリケーションに転送する SNMP マスターエージェント。
SNMP サーバ	[IM and Presence]	[TCP]	[TCP]	7999	エフェメラル	CDP Agent が CDP バイナリと通信するためにソケットとして使用します。

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	[TCP]	[TCP]	7161	エフェメラル	SNMP マスター エージェントとサブエージェントの間の通信に使用します。
[IM and Presence]	SNMP トラップ モニタ	SNMP	UDP	162	エフェメラル	SNMP トラップを管理アプリケーションに送信します。
[IM and Presence]	[IM and Presence]	SNMP	UDP	設定可能	61441	内部 SNMP トラップ レシーバ

表 *115*：*IM and Presence* サービス ポート：*Racoon* サーバ要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[ゲートウェイ（Gateway）] ---------- [IM and Presence]	[IM and Presence] ---------- [ゲートウェイ（Gateway）]	Ipsec	UDP	500	エフェメラル	Internet Security Association and the Key Management Protocol（ISAKMP）を有効にします。

表 *116*：*IM and Presence* サービス ポート：システム サービス要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	XML	[TCP]	8888 および 8889	エフェメラル	内部ポート。ローカルホストトラフィック専用。RIS サービス マネージャ（servM）と通信するクライアントを受信するために使用します。

表 *117*：*IM and Presence* サービス ポート：*DNS* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	DNS サーバ	DNS	UDP	53	エフェメラル	DNS サーバが IM and Presence DNS 照会を受信するポート。 宛先:DNS サーバ|送信元:IM and Presence

表 *118*：*IM and Presence* サービス ポート：*SSH/SFTP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	エンドポイント（Endpoint）	SSH/SFTP	[TCP]	22	エフェメラル	多くのアプリケーションが、サーバへのコマンドラインアクセスを行うために使用します。ノード間で証明書などのファイル交換（sftp）にも使用されます。

表 *119*：*IM and Presence* サービス ポート：*ICMP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence] ---------- Cisco Unified Communications Manager	Cisco Unified Communications Manager ---------- [IM and Presence]	ICMP	IP	N/A	エフェメラル	インターネット制御メッセージプロトコル（ICMP）。Cisco Unified Communications Manager サーバとの通信に使用されます。

表 *120*：*IM and Presence* サービス ポート：*NTP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	NTP サーバ（NTP Server）	NTP	UDP	123	エフェメラル	Cisco Unified Communications Manager は NTP サーバとして動作します。サブスクライバ ノードが、パブリッシャ ノードと時刻を同期するために使用されます。

表 *121*：*IM and Presence* サービス ポート：*Microsoft Exchange* 通知要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
Microsoft Exchange	[IM and Presence]	HTTP（HTTPu）	) WebDAV：HTTP /UDP/IP 通知 2) EWS - HTTP/TCP/IP SOAP 通知	IM and Presence サーバ ポート（デフォルト 50020）	エフェメラル	Microsoft Exchange は、このポートを使用してカレンダーイベントの特定のサブスクリプション識別子に対する変更を示す通知（NOTIFY メッセージによって示される）を送信します。ネットワーク構成内にある Exchange サーバと統合する場合に使用されます。どちらのポートも作成されます。送信されるメッセージの種類は、設定するカレンダー プレゼンス バックエンドゲートウェイのタイプによって異なります。

表 *122*：*IM and Presence* サービス ポート：*SOAP* サービス リクエスト

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
IM and Presence（Tomcat）	IM and Presence（SOAP）	[TCP]	[TCP]	5007	エフェメラル	SOAP モニタ ポート

表 *123*：*IM and Presence* サービス ポート：*AMC RMI* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	RTMT	[TCP]	[TCP]	1090	エフェメラル	AMC RMI オブジェクト ポートRTMT パフォーマンスモニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。
[IM and Presence]	RTMT	[TCP]	[TCP]	1099	エフェメラル	AMC RMI レジストリ ポートRTMT パフォーマンスモニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

表 *124*：*IM and Presence* サービス ポート：*XCP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
XMPP クライアント	[IM and Presence]	[TCP]	[TCP]	5222	エフェメラル	クライアントアクセスポート
[IM and Presence]	[IM and Presence]	[TCP]	[TCP]	5269	エフェメラル	サーバ間接続（S2S）ポート
サードパーティ製 BOSH クライアント	[IM and Presence]	[TCP]	[TCP]	7335	エフェメラル	XCP Web Connection Manager が、BOSH を使用するサードパーティ製 API との接続に使用する HTTP リスニング ポート
IM and Presence（XCP サービス）	IM and Presence（XCP ルータ	[TCP]	[TCP]	7400	エフェメラル	XCP ルータ マスターアクセスポート。オープン ポート設定からルータに接続する XCP サービス（XCP 認証コンポーネントサービスなど）は、通常このポートを使用して接続します。
IM and Presence（XCP ルータ	IM and Presence（XCP ルータ	UDP	UDP	5353	エフェメラル	MDNS ポート。クラスタ内の XCP ルータはこのポートを使用してお互いを検出します。

表 *125*：*IM and Presence* サービス ポート：外部データベース（*PostgreSQL*）要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（**Transport Protocol**）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	PostgreSQL データベース	[TCP]	[TCP]	5432 [2]	エフェメラル	PostgreSQL データベース リスニング ポート

2 これがデフォルトのポートですが、任意のポートで受信するよう PostgreSQL データベースを設定できます。

表 *126*：*IM and Presence* サービス ポート：高可用性の要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（**Transport Protocol**）	宛先/リスナー	ソース/送信元	備考
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	[TCP]	[TCP]	20075	エフェメラル	Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポート。
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	UDP	UDP	22001	エフェメラル	Cisco Server Recovery Manager がピアとの通信に使用するポート。

表 *127*：*IM and Presence* サービス ポート：*In Memory* データベース レプリケーションのメッセージ

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（**Transport Protocol**）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6603*	エフェメラル	Cisco Presence Datastore

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6604*	エフェメラル	Cisco Login Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	6605*	エフェメラル	Cisco SIP Registration Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	9003	エフェメラル	Cisco Presence Datastore デュアル ノード プレゼンス冗長グループの複製。
[IM and Presence]	[IM and Presence]	専用	[TCP]	9004	エフェメラル	Cisco Login Datastore デュアル ノード プレゼンス冗長グループの複製。
[IM and Presence]	[IM and Presence]	専用	[TCP]	9005	エフェメラル	Cisco SIP Registration Datastore デュアル ノードプレゼンス冗長グループの複製。

* 管理 CLI 診断ユーティリティを実行するには、`utils imdb_replication status` コマンドを使用します。これらのポートは、クラスタの IM and Presence Service ノード間で設定されているすべてのファイアウォールでオープンである必要があります。このセットアップは、通常の運用では必要ありません。

表 *128*：*IM and Presence* サービス ポート：*In Memory* データベース *SQL* メッセージ

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6603	エフェメラル	Cisco Presence Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6604	エフェメラル	Cisco Login Datastore SQL クエリ。

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6605	エフェメラル	Cisco SIP Registration Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6606	エフェメラル	Cisco Route Datastore SQL クエリ。

表 *129*：*IM and Presence* サービス ポート：*In Memory* データベースの通知メッセージ

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポート プロトコル（Transport Protocol）	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6607	エフェメラル	Cisco Presence Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6608	エフェメラル	Cisco Login Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6609	エフェメラル	Cisco SIP Registration Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6610	エフェメラル	Cisco Route Datastore XML ベースの変更通知。

SNMP については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。