# Cisco DX シリーズ アドミニストレーション ガイド、リリース 10.2(4)

初版：2015 年 06 月 23 日


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

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

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

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

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

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

- 受信アンテナの向きを変えるか、場所を移動します。
- 装置と受信機との距離を離します。
- 受信機と別の回路にあるコンセントに装置を接続します。
- 販売業者またはラジオやテレビに詳しい技術者に連絡します。

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Bluetooth の用語マークとロゴは、Bluetooth SIG, Inc. が所有する登録商標であり、かかる商標の Cisco Systems, Inc.による使用はライセンスに基づいています。

Google、Google Play、Android、その他の商標は Google Inc. の商標です。

HDMI および HDMI High-Definition Multimedia Interface の各用語、および HDMI ロゴは、HDMI Licensing LLC の米国およびその他の国における商標または登録商標です。

© 2016 Cisco Systems, Inc. All rights reserved.

# 目 次


はじめに xiv

概要 xiv

ガイドの表記法 xiv

関連資料 xvi

用語の違い xvii

マニュアルおよびテクニカル サポート xvii

シスコ製品のセキュリティの概要 xviii

技術仕様 1

物理仕様および動作環境仕様 1

ネットワーク ポートとコンピュータ ポートのピン割り当て 3

ネットワーク ポート コネクタのピン割り当て 3

コンピュータ ポート コネクタのピン割り当て 4

Cisco DX シリーズ デバイスで使用されるポート 4

ネットワーク プロトコル 6

電力要件 12

電力に関するガイドライン 12

電力削減 13

省電力モード 13

EnergyWise モード 14

LLDP での電力ネゴシエーション 15

電力に関する追加情報 15

外部デバイス 16

USB ポートと USB シリアル コンソールのデータ情報 17

USB コンソールの使用 18

ネットワーク輻輳時の動作 18
デバイスの説明 19
Cisco DX70 ハードウェア 19
Cisco DX70 のケーブルの取り付け 20
Cisco DX80 ハードウェア 21
Cisco DX80 のケーブルの取り付け 22
Cisco DX650 ハードウェア 23
Cisco DX650 ケーブルの設置 24
Wi-Fi ネットワーク設定 25
ネットワークの要件 25
ワイヤレス LAN（Wireless LAN） 26
Wi-Fi ネットワーク コンポーネント 27
AP、チャネル、規制区域の関係 27
AP の相互作用 27
アクセス ポイントとのアソシエーション 28
ワイヤレス ネットワークの QoS 28
フレキシブル DSCP のセット アップ 31
Cisco Unified Communications Manager の連携 31
WLAN 通信の 802.11 規格 31
ワールド モード（802.11d） 33
ワイヤレス変調テクノロジー 33
無線周波数範囲 34
WLAN 通信のセキュリティ 35
認証方式 35
認証キー管理 36
暗号化方式 36
AP 認証および暗号化のオプション 37
WLAN とローミング 38
展開 39
コンフィギュレーション ファイル 39
MAC アドレスの確認 40
Cisco Unified Communications Manager へのデバイスの追加方法 40

自動登録 41
自動登録と TAPS 42
Cisco Unified Communications Manager へのデバイスの追加 42
一括管理ツールの電話テンプレートを使用したデバイスの追加 43
セルフプロビジョニング 44
セルフプロビジョニングの有効化 44
Cisco Unified Communications Manager ユーザの追加 44
Cisco Unified Communications Manager へのユーザの直接追加 44
外部 LDAP ディレクトリからのユーザの追加 45
デバイス モデルの指定 46
回線の設定 46
ユーザとデバイスの関連付け 48
Survivable Remote Site Telephony 48
インストール 49
Cisco DX シリーズ デバイスの設置 49
ワイヤレス LAN のセットアップ 50
Cisco Unified Communications Manager Administration でのワイヤレス LAN のセットアップ 51
ワイヤレス LAN プロファイルのプロビジョニング 51
ワイヤレス LAN プロファイル グループのプロビジョニング 52
ネットワークの設定 52
IPv4 の設定 52
IPv4 の更新 53
IPv6 を設定する 53
IPv6 の更新 54
イーサネット Web プロキシの設定 54
管理 VLAN の設定 54
SW ポートの速度の設定 55
PC ポートの速度の設定 55
Wi-Fi ネットワークへの接続 55
非表示の Wi-Fi ネットワークへの接続 56
Wi-Fi Web プロキシの設定 56

Wi-Fi IP の設定 57
Wi-Fi の周波数帯の設定 57
Mobile and Remote Access Through Expressway（マーケティング ベータ版） 57
Expressway に対するユーザ クレデンシャルの永続性の有効化 59
Mobile and Remote Access through Expressway へのデバイスの変換 59
Expressway デバイスの VPN への変換 60
オフプレミス デバイスのオンプレミスへの変換 60
Expressway HTTP 許可リストへの問題レポート ツール サーバの追加 60
認証要求許可レートの設定 60
代替 TFTP サーバの有効化 61
TFTP サーバ 1 の設定 61
TFTP サーバ 2 の設定 62
AnyConnect VPN 62
VPN 接続プロファイルの追加 62
VPN への接続 63
VPN 経由のビデオ コール エクスペリエンスの最適化 63
Cisco Unified Communications Manager での VPN の設定 64
[VPN の設定（VPN Configuration）] の設定 65
VPN 認証 67
起動プロセス 68
起動時の TFTP サーバの手動設定 70
起動時の検証 70
**連絡先（Contacts） 71**
動作モードごとの連絡先とディレクトリ 71
ローカル連絡先 72
社内ディレクトリ 72
社内写真ディレクトリの設定 72
検索 73
検索結果の最適化 73
アプリケーション ダイヤル ルール 74
アプリケーション ダイヤル ルールの設定 74
**セルフ ケア ポータルの管理 77**

セルフ ケア ポータルの概要 77
セルフ ケア ポータルへのアクセスの設定 78
セルフ ケア ポータルの表示のカスタマイズ 78
アクセサリ 81
Bluetooth アクセサリ 81
Bluetooth デバイス プロファイル 81
ハンズフリー プロファイル 82
電話帳アクセス プロファイル 82
デバイス プロファイルの有効化 83
Bluetooth アクセサリのペアリング 83
Bluetooth の無効化 83
ケーブル ロック 84
外部カメラ 84
外部カメラの設定 84
外部カメラの設置後の確認作業 85
外部スピーカおよびマイクロフォン 85
ヘッドセット 85
Bluetooth ワイヤレス ヘッドセット 86
Bluetooth ワイヤレス ヘッドセットの追加 87
Bluetooth ヘッドセットの接続解除 88
USB ヘッドセット 88
USB ヘッドセットの有効化 88
USB ヘッドセットの無効化 89
有線ヘッドセット 89
有線ヘッドセットへの接続 89
有線ヘッドセットの無効化 89
ビデオ ディスプレイ 89
Cisco DX650 Wall-Mount キット 90
はじめる前に 90
壁面取り付けキットのコンポーネント 90
壁面への取り付け 91
セキュリティ機能 97

デバイスのセキュリティ 97
セキュリティ機能の概要 98
セキュリティ プロファイル 100
SE Android 101
アップグレードと SE Android 101
SE Android のトラブルシューティング 102
SE Android のポリシーの問題の診断 102
ADB シェルの制限 102
SE Android のログ収集 103
ローカルで有効な証明書のセットアップ 103
SHA-256 の製造元でインストールされる証明書 104
セキュアな電話コール 104
セキュアな電話コールの識別 105
セキュアな会議コールの特定 106
コール セキュリティの連携動作と制限事項 106
デバイス セキュリティ情報のリモートでの確認 108
割り込みのための暗号化 108
802.1X 認証のサポート 108
必要なネットワーク コンポーネント 109
ベスト プラクティス 109
画面ロックおよび自動ロックの設定 110
画面のロック解除/パスワードのリセットのセットアップ 111
機能とサービス 113
使用可能なテレフォニー機能 113
エージェントのグリーティング 114
エージェント グリーティングの有効化 114
すべてのコール 115
プライマリ回線でのすべてのコール 115
自動応答 115
自動ダイヤル 115
割込み 115
ビジー ランプ フィールド 116

コール転送 116
発信回線 ID 116
発信回線 ID の表記 117
Cisco エクステンション モビリティ 117
エクステンション モビリティ マルチユーザ 118
Cisco Extension Mobility の設定 118
Cisco Mobility 121
会議 121
セキュアな会議 122
転送 122
サイレント 122
ゲートウェイ録音 123
保留状態 123
保留と保留解除 123
保留音 123
無視 123
メッセージ受信インジケータ 123
ミュート 124
プラス ダイヤル 124
保護コール 124
呼出音の設定 124
呼出音 124
セキュアおよび非セキュアの通知トーン 125
サービサビリティ 125
共有回線 126
スピード ダイヤル 126
転送 126
URI ダイヤル 126
URI ダイヤル機能拡張 126
ビデオの切り替え 127
ボイス メッセージ システム 127
Visual Voicemail のセットアップ 127

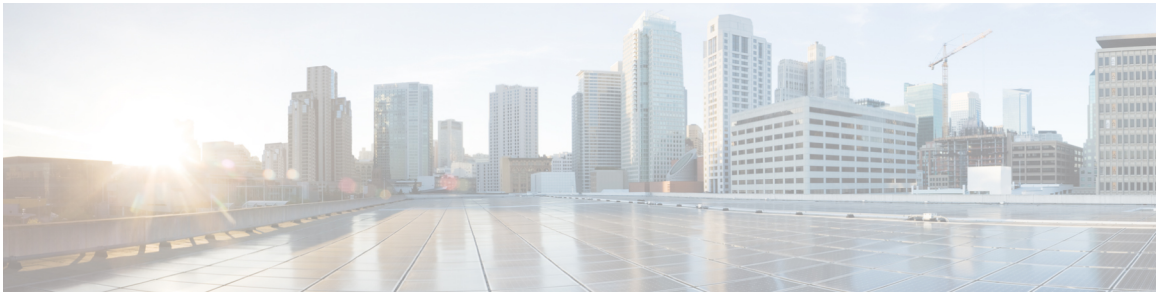
特定のユーザまたはグループに対するビジュアル ボイス メールの設定 128
機能ボタン 129
機能管理ポリシーの設定 130
機能管理ポリシーのデフォルト値 131
電話ボタン テンプレート 131
電話ボタン テンプレートの変更 132
製品固有オプションの設定 132
ビデオ送信解像度のセットアップ 147
インスタント メッセージングとプレゼンスのセットアップ 148
アプリケーションの設定 149
Cisco UCM アプリケーション クライアントの有効化 149
UCM アプリケーションにログインするエンド ユーザの作成 150
UCM アプリケーションでのユーザ登録 150
Unified Communications Manager からの Android APK ファイルのプッシュ 151
Cisco Unified Communications Manager Administration での Android サービスの追加 151
Android Phone サービスへのデバイスの登録 152
**カスタマイゼーション 155**
設定ファイルのカスタマイズおよび変更 155
ワイドバンド コーデックのセットアップ 156
動作モード 156
動作モードの設定 157
デフォルトの壁紙 158
壁紙管理の割り当て 158
デフォルトの壁紙の指定（DX70 および DX80） 158
デフォルトの壁紙の指定（DX650） 159
SSH アクセス 160
Unified Communications Manager Endpoints Locale インストーラ 160
国際コールのロギングのサポート 161
**メンテナンス 163**
デバイスのリセット 163
オプションのリセットとアップグレードのロード 165
リモート ロック 165

デバイスのリモートロック 166
リモート ワイプ 166
リモートでのデバイスのワイプ 166
Cisco DX70 の代替イメージのブート 167
Cisco DX80 の代替イメージのブート 167
Cisco DX650 の代替イメージのブート 167
データの移行 168
デバッグ ログのプロファイル 168
呼処理のデバッグ ログ プロファイルの設定 168
デバッグ ログ プロファイルのデフォルトへのリセット 169
ユーザ サポート 169
問題レポート ツール 169
カスタマー サポートのアップロード URL の設定 171
Web ブラウザからのスクリーンショットの取得 172
デバイスからのスクリーンショットの取得 172
アプリケーションのサポート 172
**モデル情報のステータスと統計情報 173**
モデル情報 173
デバイスの状態 174
ステータス メッセージ 175
イーサネット統計 180
WLAN 統計情報 181
音声コール統計 182
**リモート モニタリング 187**
Web ページへのアクセスの有効化および無効化 187
デバイスの Web ページへのアクセス 188
デバイス情報 189
ネットワークのセットアップ 191
セキュリティ情報 200
イーサネット統計 201
WLAN の設定 205
デバイス ログ 208

ストリームの統計 208

認証局信頼リスト 215

認証局信頼リスト 215



# はじめに


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


## 概要

このマニュアルでは、ネットワーク上の Cisco DX シリーズ デバイスを理解するために必要な情報とともに、これらのデバイスの設置、設定および管理に必要な情報を提供します。

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

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

## ガイドの表記法

このマニュアルでは、次の表記法を使用しています。

| 表記法 | 説明 |
|---|---|
| 太字フォント | コマンドおよびキーワードは太字で示しています。 |

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

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

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

警告は、次のように表しています。

注目 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. 警告文 1071

SAVE THESE INSTRUCTIONS

# 関連資料

### Cisco DX シリーズ

すべての Cisco DX シリーズ マニュアルは、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

ユーザ指向のマニュアルは、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-user-guide-list.html

管理者向けのマニュアルは、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-maintenance-guides-list.html

『*Cisco DX Series Wireless LAN Deployment Guide*』は、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-implementation-design-guides-list.html

翻訳された関連資料は、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-translated-end-user-guides-list.html

オープン ソースのライセンス情報は、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-licensing-information-listing.html

『Regulatory Compliance and Safety Information』は、次の URL で入手できます。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-installation-guides-list.html

### Cisco Unified Communications Manager

『*Cisco Unified Communications Manager Documentation Guide*』およびご使用の Cisco Unified Communications Manager リリースに固有の他の資料を参照してください。 次のドキュメント URL から参照してください。

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

### Cisco Business Edition 6000

『*Cisco Business Edition 6000 Documentation Guide*』およびお使いの Cisco Business Edition 6000 リリースに特化したその他の文書を参照してください。 次の URL から入手できます。

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

### シスコおよび環境

関連資料は、次の URL で入手できます。

http://www.cisco.com/go/ptrdocs

# 用語の違い

次の表に、Cisco DX シリーズ のユーザ ガイド、『*Cisco DX* シリーズ アドミニストレーション ガイド』、『*Cisco Unified Communications Manager Administration Guide*』で使用されている用語の違いをいくつか取り上げます。

**表 *1*：用語の違い**

| ユーザ ガイド | アドミニストレーション ガイド |
|---|---|
| 回線ステータス | ビジー ランプ フィールド（BLF） |
| メッセージ インジケータ | メッセージ受信インジケータ（MWI）またはメッセージ受信ランプ |
| ボイスメール システム | ボイス メッセージ システム |

# マニュアルおよびテクニカル サポート

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

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

# シスコ製品のセキュリティの概要

この製品には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。 シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。 輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。 本製品を使用するにあたっては、関係法令の順守に同意する必要があります。 米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、http://www.bis.doc.gov/policiesandregulations/ear/index.htm で参照できます。

第 1 章

# 技術仕様


- 物理仕様および動作環境仕様，1 ページ
- ネットワーク ポートとコンピュータ ポートのピン割り当て，3 ページ
- ネットワーク プロトコル，6 ページ
- 電力要件，12 ページ
- 外部デバイス，16 ページ
- USB ポートと USB シリアル コンソールのデータ情報，17 ページ
- ネットワーク輻輳時の動作，18 ページ


## 物理仕様および動作環境仕様

表 *2* : ***Cisco DX*** シリーズ デバイスの物理仕様および動作環境仕様

| 仕様 | 値または範囲 |
|---|---|
| 寸法（高さ X 幅 X 奥行） | Cisco DX70：14.84 インチ（377.1 □m）X 13.91 インチ（353.1 mm）X 2.45 インチ（62.3 mm）<br>Cisco DX80：20.2 インチ（512 mm）X 22.2 インチ（565 mm）X 3.5 インチ（89 mm）<br>Cisco DX650：8.46 インチ（215 mm）X 10.35 インチ（263 mm）X 8.19 インチ（208 mm） |
| 重量 | Cisco DX70：8.5 ポンド（3.9 kg）<br>Cisco DX80：15.65 ポンド（7.1 kg）<br>Cisco DX650：3.81 ポンド（1.73 kg） |
| 動作温度 | 0 ～ 40□（32 ～ 104°F） |

| 仕様 | 値または範囲 |
|---|---|
| 動作時の相対湿度 | 10 ～ 95%（結露しないこと） |
| 保管温度 | 14 ～ 140°F (-10 ～ 60°C) |
| 電力：Cisco DX70 | 定格：最大 12V で 3.5A<br>省電力スタンバイ モード<br>EnergyWise サポート統合 |
| 電力：Cisco DX80 | 定格：最大 60 W<br>省電力スタンバイ モード<br>EnergyWise サポート統合 |
| 電力：Cisco DX650 | IEEE 802.3af（クラス 3）または IEEE 802.3at（クラス 4）Power over Ethernet（PoE）標準がサポートされます。<br>Cisco Discovery Protocol および Link Layer Discovery Protocol Media Endpoint Discovery （LLDP-MED） PoE スイッチ ブレードの両方と互換性があります。<br>電力バジェット：802.3AF および低電力 USB サポートの場合は 13.7W（Cisco Discovery Protocol）または 15.1W（LLDP）。高電力 USB サポートには、15.4W を超える電力および 802.3AT が必要です。 |
| 接続 | 内部 2 ポート Cisco イーサネット スイッチ<br>IEEE 802.11 a/b/g/n Wi-Fi |
| オーディオ コーデック サポート | ナローバンド音声圧縮コーデック：G.711a、G.711u、G.729a、G.729ab、および Internet Low Bitrate Codec（iLBC）<br>ワイドバンド音声圧縮コーデック：G.722、Internet Speech Audio Codec（iSAC）、iLBC、および AAC-LD 音声圧縮コーデック。 |
| オペレーティング システム | Android™ 4.1.1（Jellybean） |
| プロセッサ | Cisco DX70：TI OMAP 4470 1.5GHz デュアルコア ARM Cortex-A9 プロセッサ<br>Cisco DX80：TI OMAP 4470 1.5GHz デュアルコア ARM Cortex-A9 プロセッサ<br>Cisco DX650：TI OMAP 4460 1.5GHz デュアルコア ARM Cortex-A9 プロセッサ |

| 仕様 | 値または範囲 |
|---|---|
| メモリ | 2 GB RAM。Low Power Double Data Rate Synchronous Dynamic Random-Access Memory（LPDDR2 SDRAM） |
| ストレージ | 8-GB eMMC NAND フラッシュ メモリ（マルチメディア カード内蔵、不揮発性） |

# ネットワークポートとコンピュータポートのピン割り当て

Cisco DX シリーズデバイスには、ネットワーク接続に使用するネットワーク ポートとコンピュータ（アクセス）ポートが組み込まれています。 それぞれ異なる目的で使用され、ポートのピン割り当ても異なっています。

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

## ネットワーク ポート コネクタのピン割り当て

**表 *3*: ネットワーク ポート コネクタのピン割り当て**

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

# コンピュータ ポート コネクタのピン割り当て

**表 *4*：コンピュータ（アクセス）ポート コネクタのピン割り当て**

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

# Cisco DX シリーズ デバイスで使用されるポート

次の表に、Cisco DX シリーズ デバイスで使用するポートについて説明します。詳細については、『*TCP and UDP Port Usage Guide for Cisco Unified Communications Manager*』を参照してください。

**表 *5*：*Cisco DX* シリーズ デバイス ポート**

| 送信元ポート | リモート デバイス ポート | 基本プロトコル | プロトコル/サービス | 注記 |
|---|---|---|---|---|
| 68 | 67 | - | DHCP クライアント | 動的な IP アドレスを取得する DHCP サポート |
| 49152-53248 | 53 | UDP | DNS クライアント | 名前解決のための DNS サポート |

| 送信元ポート | リモート デバイス ポート | 基本プロトコル | プロトコル/サービス | 注記 |
|---|---|---|---|---|
| 49152-53248 | 69 | UDP | TFTP クライアント | 中央サーバから各種コンフィギュレーション ファイルとイメージ ファイルを取得するには、TFTP サポートが必要です。 |
| 49152-53248 | 80 | TCP/UDP | HTTP クライアント | |
| 80 | 設定されたサーバ | TCP/UDP | HTTP サーバ | |
| 123 | 123 | UDP | NTP クライアント | タイム ゾーンを取得するためのネットワーク タイム プロトコル |
| 49152-53248 | 設定されたサーバ | TCP | HTTP クライアント | |
| 49152-53248 | 6970 | TCP | TFTP クライアント | 中央サーバから各種コンフィギュレーション ファイルとイメージ ファイルを取得するには、TFTP サポートが必要です。 |
| 49152-53248 | 5060 | TCP | SIP TCP | デフォルトは 5060 です。管理者は設定を変更できます。 |
| 49152-53248 | 5061 | TCP | SIP/TLS | デフォルトは 5061 です。管理者は設定を変更できます。 |
| 16384-32767 | 受信範囲 | UDP | RTP | 管理者は、ポート範囲を設定できます。 |
| 16384-32767 | 受信範囲 | UDP | RTCP | RTCP ポートは RTP +1 です。 |
| 4224 | PC ダイナミック レンジ | TCP | | |
| 22 | 設定されたサーバ | TCP | セキュア シェル | |
| 4051 | | TCP | | ロード アップグレード |

| 送信元ポート | リモート デバイス ポート | 基本プロトコル | プロトコル/サービス | 注記 |
|---|---|---|---|---|
| 4052 | | RDP | | ロード アップグレード |
| 4061 | | | | 特殊なデバッグ |
| 8443 | | | | 連絡先検索 |

# ネットワーク プロトコル

Cisco DX シリーズ デバイスは、音声通信に必要な複数の業界標準およびシスコのネットワーキング プロトコルに対応しています。 次の表に、デバイスでサポートされるネットワーク プロトコルの概要を示します。

**表 *6*：サポートされるネットワーク プロトコル**

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| Binary Floor Control Protocol（BFCP） | BFCP を使用すると、ユーザは進行中のビデオ会話内でプレゼンテーションを共有できます。 | BFCP は自動的に有効にされます。 |
| Bluetooth | Bluetooth は、短距離におけるデバイスの通信方法を指定する Wireless Personal Area Network（WPAN）プロトコルです。 | デバイスは Bluetooth 3.0 をサポートします。<br>デバイスはハンズフリー プロファイル（HFP）、Advanced Audio Distribution Profile（A2DP）、Human Interface Device Profile（HID）、Object Push Profile（OPP）および Phone Book Access Profile（PBAP）をサポートします。 |
| ブートストラップ プロトコル（BootP） | BootP は、特定の起動情報（IP アドレスなど）をネットワーク デバイスが検出できるようにするプロトコルです。 | — |
| Cisco Discovery Protocol（CDP） | CDP は、シスコの製造するすべての装置で動作するデバイス検出プロトコルです。<br>デバイスは、CDP を使用して自身の存在をネットワーク内の他のデバイスにアドバタイズし、他のデバイスの情報を受信することができます。 | 補助 VLAN ID、ポートごとの電源管理の詳細情報、Quality of Service（QoS）設定情報などの情報を Cisco Catalyst スイッチとやり取りするために、デバイスで CDP が使用されます。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| Cisco Peer-to-Peer Distribution Protocol（CPPDP） | CPPDPは、デバイスのピアツーピア階層を形成するために使用されるシスコ独自のプロトコルです。この階層はピア デバイスからネイバー デバイスにファームウェア ファイルを配布するために使用されます。 | ピア ファームウェア共有機能ではCPPDPが使用されます。 |
| ダイナミック ホスト コンフィギュレーションプロトコル（DHCP） | DHCPは、IPアドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。<br>DHCPを使用すると、手動でIPアドレスを割り当てたり追加のネットワーク パラメータを構成したりすることなく、デバイスをネットワークに接続するだけで、そのデバイスを運用できるようになります。 | DHCPは、デフォルトで有効になっています。無効にした場合は、各デバイスで個別にIPアドレス、サブネットマスク、ゲートウェイ、およびTFTPサーバを手動で設定する必要があります。<br>シスコでは、DHCPのカスタム オプション150を使用することを推奨します。この方法では、TFTPサーバのIPアドレスをオプション値として設定します。サポートされているその他のDHCP設定については、『*CiscoUnified Communications Manager System Guide*』の「Dynamic Host Configuration Protocol」と「Cisco TFTP」の章を参照してください。<br>（注） オプション150を使用できない場合、DHCP オプション66の使用を試みることができます。 |
| ハイパーテキスト転送プロトコル（HTTP） | HTTPは、インターネットやWeb経由で情報を転送し、ドキュメントを移送するための標準的な手段です。 | デバイスでは、XMLサービス用およびトラブルシューティング用にHTTPが使用されます。 |
| Hypertext Transfer Protocol Secure（HTTPS） | Hypertext Transfer Protocol Secure（HTTPS）は、サーバの暗号化とセキュアなIDを確保できるように、ハイパーテキスト転送プロトコルとSSL/TLSプロトコルを組み合わせたものです。 | HTTPとHTTPSの両方をサポートするWebアプリケーションには2つのURLが設定されています。HTTPSをサポートするデバイスはHTTPS URLを選択します。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| IEEE 802.1X | IEEE 802.1X 標準は、クライアント/サーバベースのアクセス コントロールと認証プロトコルを定義します。これにより、未承認のクライアントが一般にアクセス可能なポートから LAN に接続するのを制限します。<br>クライアントが認証されるまでは、802.1X アクセス コントロールによって、クライアントが接続されているポートを経由する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。認証が成功すると、通常のトラフィックがポートを通過できるようになります。 | デバイスでは、EAP-FAST および EAP-TLS 認証方式をサポートすることにより IEEE 802.1X 標準が実装されます。<br>デバイスで 802.1X 認証が有効になっている場合、PC ポートとボイス VLAN を無効にする必要があります。 |
| IEEE 802.11a/b/g/n | IEEE 802.11 標準は、ワイヤレス ローカル エリア ネットワーク（WLAN）におけるデバイスの通信方法を指定します。<br>802.11a は 5 GHz 帯域で動作し、802.11b および 802.11g は 2.4 GHz 帯域で動作します。<br>802.11.n は、2.4 GHz 帯域または 5GHz 帯域のいずれかで動作します。 | 802.11 インターフェイスは、イーサネットのケーブル接続が利用できないか望ましくない場合の展開オプションです。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| インターネット プロトコル（IP） | IPは、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。 | IP を使用して通信するには、ネットワーク デバイスに対して、IPアドレス、ドメイン名、ゲートウェイ、およびネットマスクが割り当てられている必要があります。<br>Dynamic Host Configuration Protocol（DHCP）を通じてデバイスを使用している場合、IPアドレス、サブネット、およびゲートウェイの識別情報が自動的に割り当てられます。 DHCP を使用しない場合は、各デバイスで個別にこれらのプロパティを手動で割り当てる必要があります。<br>デバイスは、IPv6アドレスをサポートします。 詳細については、『『*Features and Services Guide for Cisco Unified Communications Manager*』』の「Internet Protocol Version 6（IPv6）」の章を参照してください。 |
| Link Layer Discovery Protocol（LLDP） | LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコデバイスとサードパーティ製デバイスでサポートされています。 | デバイスは、PCポートでLLDPをサポートします。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| Link Layer Discovery Protocol - Media Endpoint Devices（LLDP-MED） | LLDP-MED は、音声製品用 LLDP 標準の拡張です。 | デバイス は、次のような情報を通信するためにSW ポート上で LLDP-MED をサポートします。<br>• ボイス VLAN の設定<br>• デバイスの検出<br>• 電源管理<br>• インベントリ管理<br>LLDP-MED サポートの詳細については、LLDP-MED および『Cisco Discovery Protocol』ホワイト ペーパーを参照してください。<br>http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml |
| リアルタイム転送プロトコル（RTP） | RTP は、インタラクティブな音声やビデオなどのリアルタイム データをデータ ネットワーク経由で転送するための標準プロトコルです。 | デバイスは RTP プロトコルを使用して、リアルタイム音声トラフィックを他の電話機やゲートウェイとやり取りします。 |
| リアルタイム制御プロトコル（RTCP） | RTCP は RTP と連動して、RTP ストリーム上で QoS データ（ジッター、遅延、ラウンドトリップ遅延など）を伝送します。<br>また、RTCP は、ビデオ エクスペリエンスが向上するように、オーディオ ストリームとビデオ ストリームを同期する際にも使用されます。 | 音声コールの RTCP は、デフォルトでは無効になっています。（ビデオコールの音声ストリームとビデオ ストリームの両方を含む）ビデオコールの RTCP は、デフォルトでは無効になっています。 Cisco Unified Communications Manager Administration から、個々のデバイスの RTCP を有効または無効にできます。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| セッション記述プロトコル（SDP） | SDP は SIP プロトコルの一部であり、2 つのエンドポイント間で接続が確立されている間に、どのパラメータを使用できるかを決定します。 会議は、会議に参加するすべてのエンドポイントがサポートする SDP 機能だけを使用して確立されます。 | コーデック タイプ、DTMF 検出、コンフォート ノイズなどの SDP 機能は通常、運用中の Cisco Unified Communications Manager またはメディア ゲートウェイでグローバルに設定されます。 SIP エンドポイントの中には、これらのパラメータをエンドポイント上で設定できるものがあります。 |
| セッション開始プロトコル（SIP） | SIP は、IP を介したマルチメディア会議のためのインターネット技術特別調査委員会（IETF）標準です。 SIP は、アプリケーション層の ASCII ベースの制御プロトコルであり（RFC 3261 で規定）、2 つ以上のエンドポイント間でコールを確立、維持、および終了するために使用できます。 | 他の VoIP プロトコルと同様に、SIP はシグナリングとセッション管理の機能をパケット テレフォニー ネットワークの内部で処理します。 シグナリングによって、ネットワーク境界を越えてコール情報を伝送することが可能になります。セッション管理とは、エンドツーエンド コールの属性を制御する機能を提供することです。 |
| Telepresence Interoperability Protocol（TIP）/Multiplex（MUX） | TIP/MUX は、メディアの受信前に、エンドポイント間で音声およびビデオのメディア オプションをネゴシエートするために使われる IP プロトコルです。 | マルチパーティ会議用に TIP/MUX が呼び出されると、コンテンツ共有が有効になります。 |
| 伝送制御プロトコル（TCP） | TCP は、コネクション型の転送プロトコルです。 | デバイスでは、Cisco Unified Communications Manager に接続したり XML サービスにアクセスしたりするために TCP が使用されます。 |
| トランスポート層セキュリティ（TLS） | TLS は、通信のセキュリティ保護と認証に使用される標準プロトコルです。 | セキュリティの実装後、デバイスは Cisco Unified Communications Manager への登録をセキュアに行う際に TLS プロトコルを使用します。 |

| ネットワーク プロトコル | 目的 | 使用方法 |
|---|---|---|
| トリビアルファイル転送プロトコル（TFTP） | TFTP を使用すると、ファイルをネットワーク経由で転送できます。<br>デバイスで TFTP を使用すると、デバイス タイプ固有の設定ファイルを取得できます。 | TFTP は DHCP サーバが自動的に識別する TFTP サーバがネットワーク内に必要です。 DHCP サーバで指定されている以外の TFTP サーバをデバイスで使用するには、デバイスの設定アプリケーションを使用して、TFTP サーバの IP アドレスを手動で割り当てる必要があります。<br>詳細については、『*Cisco Unified Communications Manager System Guide*』の「"Cisco TFTP"」の章を参照してください。 |
| ユーザ データグラム プロトコル（UDP） | UDP は、データ パケットを配信するためのコネクションレス型メッセージング プロトコルです。 | UDP は RTP ストリームにのみ使用されます。 デバイスの SIP シグナリング機能は UDP をサポートしていません。 |

# 電力要件

Cisco DX シリーズ デバイスへの電源投入には、外部電源が使用されます。 外部電源は個別の電源装置によって提供されます。

Cisco DX650 への電源投入に Power over Ethernet（PoE）を使用することもできます。 スイッチは、イーサネット ケーブルを介して PoE を提供できます。

（注） 外部電源を使用する場合、イーサネット ケーブルをデバイスに接続する前に、電源装置をデバイスに接続する必要があります。 外部電源から電力が供給されているデバイスを取り外す場合は、電源装置を取り外す前に、イーサネット ケーブルをデバイスから取り外してください。

# 電力に関するガイドライン

Cisco DX70 と Cisco DX80 に電源投入するには、付属の Lite-On PA-1600-2A-LF 電源装置または FSP075-DMAA1 を使用します。 Cisco DX650 に電源投入するには、次の表を参照してください。

表 *7*：***Cisco DX650*** 電源に関する注意事項

| 電源の種類 | ガイドライン |
|---|---|
| 外部電源：<br>CP-PWR-CUBE-4 外部電源を通じて電力を供給 | デバイスでは、CP-PWR-CUBE-4 電源を使用します。<br>（注） デバイスをワイヤレス ネットワークに配置するときは、CP-PWR-CUBE-4 を使用する必要があります。 |
| 外部電源：Cisco Unified IP Phone Power Injector 経由で供給されます。 | 任意の Cisco DX650 で Cisco Unified IP Phone Power Injector を使用できます。 インジェクタは、ミッドスパン デバイスとして機能し、接続されている電話機にインラインパワーを供給します。 Cisco Unified IP Phone Power Injector は、スイッチ ポートと電話機を接続します。また、通電されていないスイッチと電話機の間で最大 100 m のケーブル長をサポートします。 |
| PoE 電源：スイッチから、電話機に接続したイーサネット ケーブル経由で供給されます。 | Cisco DX650 は、信号ペアおよび予備のペアで IEEE 802.3af Class 3 電源をサポートします。<br>これらのデバイスは、外部アドオン デバイス用に IEEE 802.3at をサポートします。<br>電話機を無停電で運用するには、スイッチがバックアップ電源を備えている必要があります。<br>スイッチ上で実行されている CatOS または IOS のバージョンが、予定している電話機配置をサポートしていることを確認します。 オペレーティング システムのバージョンに関する情報については、スイッチのマニュアルを参照してください。<br>NG-PoE+ のサポート：デバイスは、NG-PoE+ スイッチのサポートがある限り、IEEE 802.3at よりも強力なパワーを引き出すことができます。 |

# 電力削減

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

## 省電力モード

省電力モードでは、デバイスを使用していない間、スクリーンのバックライトが消灯します。 デバイスは、ユーザがハンドセットを持ち上げるか、任意のボタンを押さない限り、スケジュールされた期間にわたって、電力節約モードのままになります。 Cisco Unified Communications Manager の [電話の設定（Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration）] 領域で、次のパラメータを設定します。

**ディスプレイ非点灯日（Days Display Not Active）**

バックライトを非アクティブのままにする日を指定します。

**ディスプレイ点灯時刻（Display on Time）**

バックライトを自動的にアクティブにする時刻をスケジュールします。

**ディスプレイ点灯継続時間（Display on Duration）**

プログラムされた時刻にバックライトがオンになった後、オン状態を保つ時間の長さを指定します。

## EnergyWise モード

電力節約モードに加えて、デバイスではCisco EnergyWise（Power Save Plus）モードもサポートされています。 ネットワークにEnergyWise（EW）コントローラが含まれている場合（たとえば、Ciscoスイッチで EnergyWise機能が有効になっている場合）、これらのデバイスをスケジュールに基づいてスリープ状態（電源オフ）およびウェイク状態（電源オン）になるように設定して、電力消費をさらに抑えることができます。

EnergyWiseは、デバイスごとに有効または無効に設定します。 EnergyWiseを有効にした場合は、他のパラメータとともに、スリープと復帰の時刻を設定します。 これらのパラメータは、デバイス設定XMLファイルの一部として電話機へ送信されます。 Cisco Unified Communications Managerの [電話の設定（Phone Configuration）] ウィンドウで、次のパラメータを設定します。

**Power Save Plus の有効化（Enable Power Save Plus）**

デバイスの電源をオフにする日のスケジュールを選択します。

**電話機をオンにする時刻（Phone On Time）**

[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択した日について、デバイスの電源を自動的にオンにする時刻を決定します。

**電話機をオフにする時刻（Phone Off Time）**

[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択した日について、デバイスの電源をオフにする時刻を決定します。

**電話機をオフにするアイドル タイムアウト（Phone Off Idle Timeout）**

デバイスの電源をオフにする前に、デバイスをアイドル状態にしておく必要がある時間の長さを決定します。

**音声によるアラートの有効化（Enable Audio Alert）**

これを有効にすると、[電話をオフにする時刻（Phone Off Time）] で指定した時刻の10分前にデバイスで音声アラートの再生が開始されます。

**EnergyWise ドメイン（EnergyWise Domain）**

そのデバイスが含まれる EnergyWise ドメインを指定します。

**EnergyWise シークレット（EnergyWise secret）**

EnergyWise ドメイン内での通信に使用するセキュリティの秘密パスワードを設定します。

**EnergyWise オーバーライドを許可（Allow EnergyWise Overrides）**

デバイスに電源レベルの更新を送信するための EnergyWise ドメイン コントローラのポリシーを許可するかどうかを決定します。

デバイスがスリープ状態のとき、Power Sourcing Equipment（PSE）はデバイスに電源/ロック ボタンを点灯するための最小限の電力を供給します。このため、スリープ中も電源/ロック ボタンを使用してデバイスを復帰させることができます。

# LLDP での電力ネゴシエーション

デバイスとスイッチは、デバイスが消費する電力のネゴシエーションを行います。 デバイスは複数の電力設定で動作し、これにより、使用可能な電力が少ないときは電力消費が低減されます。

デバイスのリブートの後、スイッチは電力ネゴシエーション用の 1 つのプロトコル（CDP または LLDP）にロックされます。 スイッチは、デバイスが送信した最初のプロトコル（電力のしきい値限度値（TLV）を含む）にロックされます。 システム管理者がデバイス上でそのプロトコルを無効にすると、スイッチがもう一方のプロトコルでの電力要求に対して応答しないため、デバイスはアクセサリの電源を投入できなくなります。

電力ネゴシエーションをサポートしているスイッチにデバイスを接続する場合は、常に電力ネゴシエーションを有効（デフォルト）にすることを推奨します。

電力ネゴシエーションを無効にした場合、スイッチがデバイスに対して電力を供給しない可能性があります。 スイッチが電力ネゴシエーションをサポートしていない場合は、アクセサリの電源を PoE+ で投入する前に、電力ネゴシエーション機能を無効にします。 電力ネゴシエーション機能を無効にすると、デバイスは IEEE 802.3af-2003 規格で許容されている最大値まで、アクセサリに電源を供給できます。

（注） CDP および電力ネゴシエーション機能を無効にすると、デバイスは 15.4 W までアクセサリに電力を供給できます。

# 電力に関する追加情報

次の表にあるドキュメントは、次のトピックに関する詳細情報を提供します。

- Cisco Unified IP Phone と連携する Cisco スイッチ

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

| ドキュメントのトピック | URL |
|---|---|
| Cisco Unified IP Phone パワー インジェクタ | http://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-power-injector/index.html |
| PoE ソリューション | http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html |
| Cisco Catalyst スイッチ | http://www.cisco.com/cisco/web/psa/default.html?mode=prod<br>http://www.cisco.com/c/en/us/products/switches/index.html |
| サービス統合型ルータ | http://www.cisco.com/c/en/us/products/routers/index.html |
| Cisco IOS ソフトウェア | http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html |

# 外部デバイス

弊社では、不要な無線周波数（RF）および可聴周波数（AF）を遮断するヘッドセット、ケーブル、コネクタなどの高品質の外部デバイスの使用を推奨しています。

（注） すべての Cisco IP Telephony 製品が外部デバイス、コードまたはケーブルをサポートしているわけではありません。 詳細については、デバイスのマニュアルを参照してください。

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

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

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

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

# USB ポートと USB シリアル コンソールのデータ情報

Cisco DX シリーズ デバイスには、USB ポートと、場合によっては micro-USB ポートが組み込まれています。 デバイスの USB ポートには最大 10 個のアクセサリを接続できます。 デバイスに接続する各アクセサリが、最大数に計上されます。 サポートされるアクセサリには、USB シリアル ケーブル、USB マウス、USB キーボード、USB 電源供給ハブ、USB メモリ スティックなどがあります。

（注）　すべての USB ハブの電源をオンにする必要があるため、1 つ以上のハブを含むキーボードをデバイスで使用することはできません（電源供給のないハブが含まれることになるためです）。

また、Android Debug Bridge（ADB）アクセスに USB 接続を使用できます。 ADB にアクセスするには、Cisco DX650 および Cisco DX70 では micro-USB ポートを使用し、Cisco DX80 では USB タイプ B ポートを使用します。 ADB 利用の詳細については、http://developer.android.com/index.html を参照してください。

USB シリアル コンソールでは、USB ポートをコンソールとして使用することで、シリアル ポートが必要でなくなります。 次の表に、USB コンソールの設定項目を示します。

**表 *8*：*USB* コンソールの設定**

| パラメータ | 設定 |
|---|---|
| ボー レート | 115200 |
| データ | 8 ビット |
| パリティ | なし |
| 停止 | 1 ビット |
| フロー制御 | なし |

（注）　デバイスにはドライバがあらかじめ組み込まれているため、シスコがサポートするケーブル タイプの数には制限があります。 IOGEAR USB シリアル アダプタを使用することをお勧めします。

# USB コンソールの使用

USB コンソール ケーブルは、一方に USB インターフェイス、そしてもう一方にシリアル インターフェイスを備えています。 USB インターフェイスは、デバイス上の USB ポートのいずれかに接続することが可能です。 シリアル インターフェイスは、PC のシリアル ポートに接続します。

Cisco DX650 では、側面または背面の USB タイプ A ポートを使用します。 Cisco DX70 および Cisco DX80 では、micro-USB ポートを使用します。

**ヒント** PC/ラップトップにシリアル ポートがない場合は、背中合わせにした 2 本の USB コンソール ケーブルを、それらの間にヌル モデム ケーブルを挟んで接続できます。

**手順**

**ステップ 1** Cisco Unified Communications Manager のデバイス ページでクレデンシャルを設定します。

**ステップ 2** ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域で、USB デバッグを有効にします。

**ステップ 3** デバイスに USB シリアル ケーブルを接続します。 デバイス コンソール出力が、端末画面に表示されます。

**ステップ 4** 出力が停止したら、Return をタップしてサインインに進みます。

**ステップ 5** $ プロンプト画面の後に、問題を診断するための debugsh などのツールを使用できます。

# ネットワーク輻輳時の動作

ネットワーク パフォーマンスの低下の原因となるものは、音声とビデオの品質にも影響を及ぼすため、場合によっては、コールがドロップする可能性があります。 ネットワーク速度低下の原因として、たとえば次のようなアクティビティがあります。

- 内部ポート スキャンやセキュリティ スキャンなどの管理タスク
- ネットワークで発生する DoS 攻撃などの攻撃

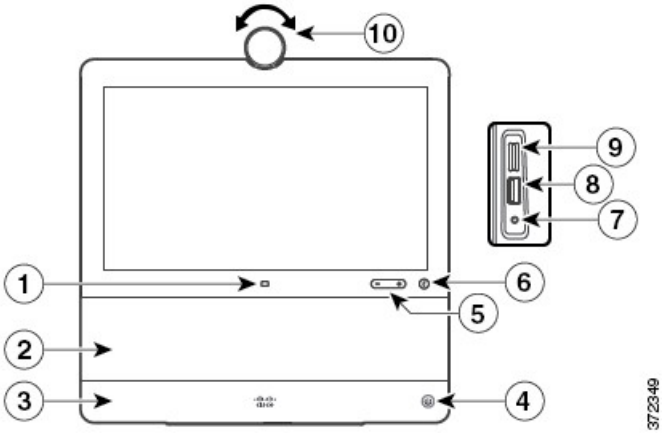
悪影響を緩和または排除するには、デバイスが使用されていない時間帯に管理ネットワーク タスクを実行するようにスケジュールするか、テストからデバイスを除外します。

第 2 章

# デバイスの説明

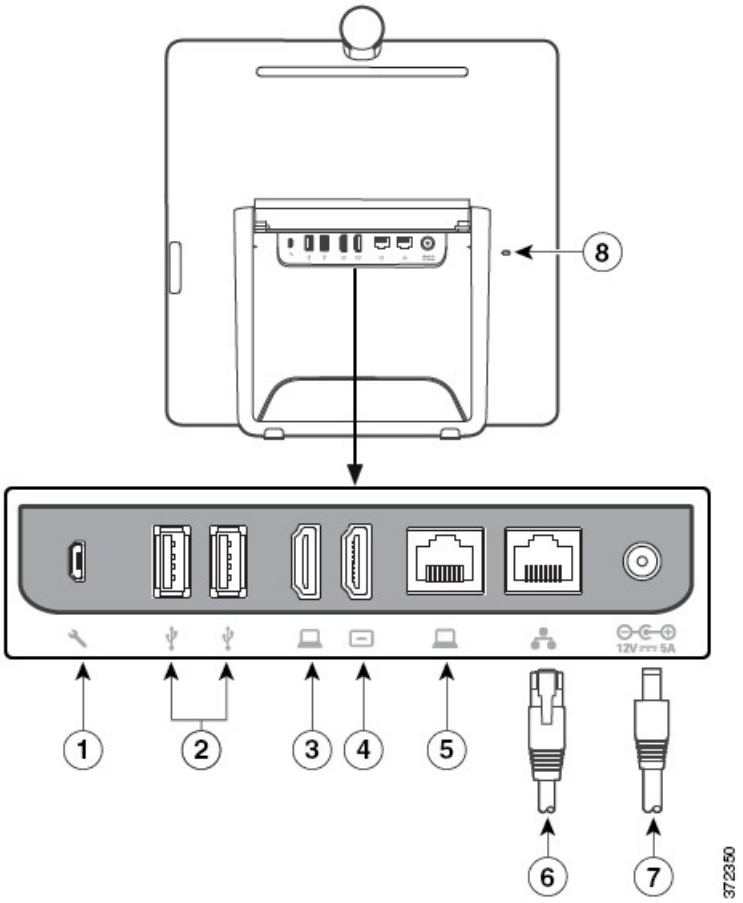

- Cisco DX70 ハードウェア，19 ページ
- Cisco DX80 ハードウェア，21 ページ
- Cisco DX650 ハードウェア，23 ページ


## Cisco DX70 ハードウェア



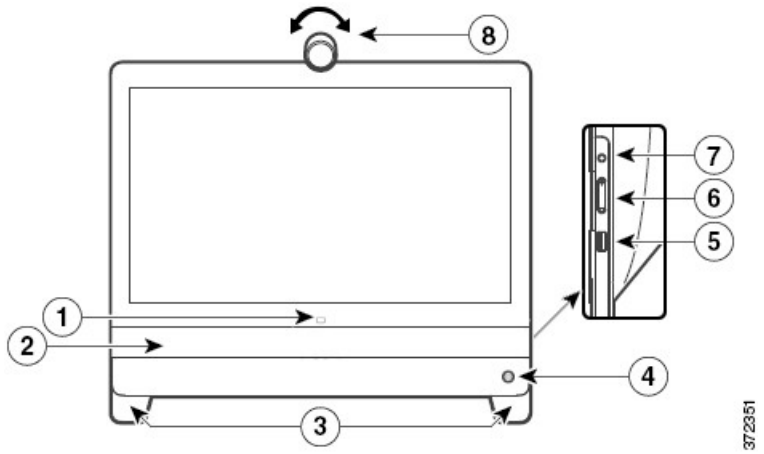

| | | | |
|---|---|---|---|
| 1 | ソース ボタン | 6 | ミュート ボタン |
| 2 | スピーカー | 7 | ミニ ジャック 3.5 mm |
| 3 | マイク | 8 | USB 充電ポート |
| 4 | 電源ボタン | 9 | microSD カード スロット |
| 5 | 音量ボタン | 10 | プライバシー シャッター付きカメラ |

# Cisco DX70 のケーブルの取り付け




| | | | |
|---|---|---|---|
| 1 | Micro B USB ポート | 5 | コンピュータ ポート |
| 2 | USB ポート | 6 | ネットワーク ポート |
| 3 | HDMI 入力 | 7 | 電源ポート |
| 4 | HDMI 出力 | | |

# Cisco DX80 ハードウェア

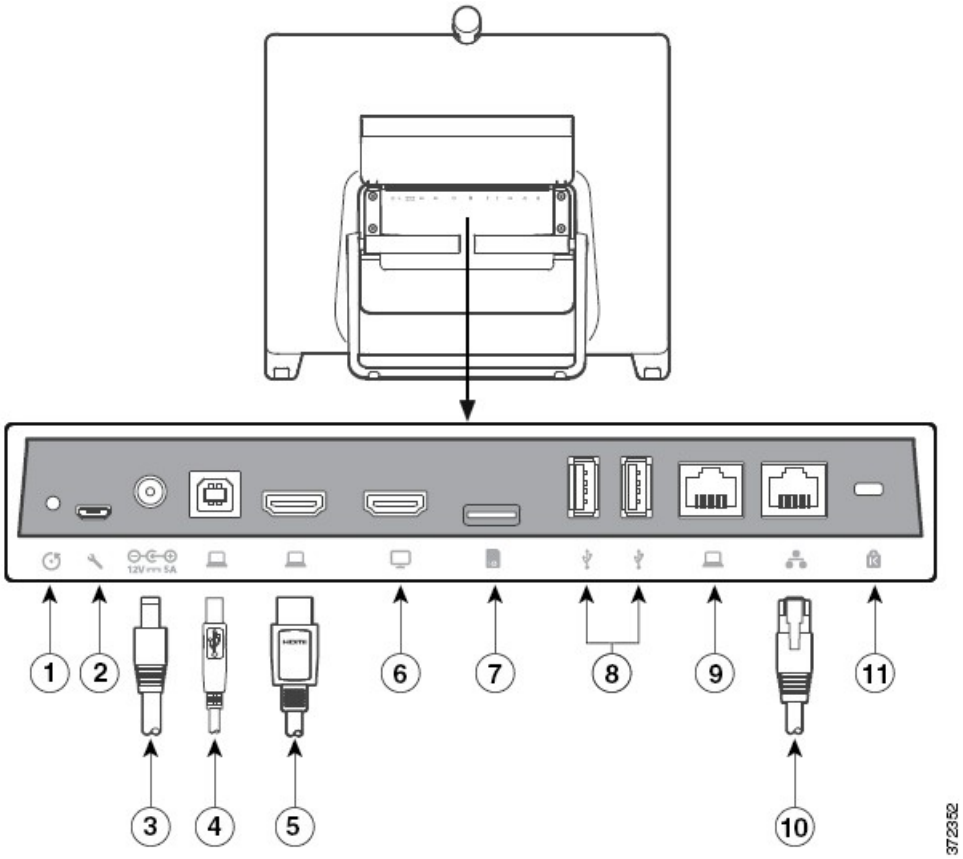



| | | | |
|---|---|---|---|
| 1 | ソース ボタン | 5 | USB ポート |
| 2 | スピーカー | 6 | 音量ボタン |
| 3 | 各脚内のマイクロフォン | 7 | ミュート ボタン |
| 4 | 電源ボタン | 8 | プライバシー シャッター付きカメラ |

Cisco DX80 には、音響エコー キャンセラ（AEC）およびラップトップ シャドウイング機能が搭載されています。 コールの相手先のユーザは、ラップトップなどの障害物がマイクの前にある場合でも、クリアな音声を体験できます。 現在のマイクが障害物によって遮られている場合、デバイスは別の脚に装備されている別のマイク アレイに自動的に切り替えます。

Cisco DX80 には、2 つのマイク アレイ ビームフォーミングも搭載されています。 ユーザがビームから移動した場合（つまり、カメラの視界から外れた場合）、相手先に送信される音声が弱くなります。 （装置前面の）ピックアップ ビーム内にない音源はすべて減衰します。

# Cisco DX80 のケーブルの取り付け

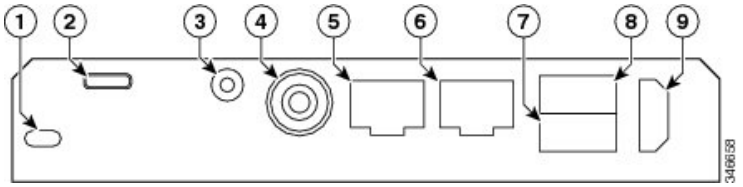



| | | | |
|---|---|---|---|
| 1 | 初期設定リセット ピンホール | 7 | microSD カード スロット |
| 2 | Micro B USB ポート | 8 | USB ポート |
| 3 | 電源ポート | 9 | コンピュータ ポート |
| 4 | USB タイプ B ポート | 10 | ネットワーク ポート |
| 5 | HDMI 入力 | 11 | ケンジントンセキュリティ スロット（K スロット） |
| 6 | HDMI 出力 | | |

# Cisco DX650 ハードウェア

| | | | |
|---|---|---|---|
| [1] | プライバシー シャッター スライド スイッチ | [10] | 会議ボタン |
| 2 | カメラ | 11 | 転送ボタン |
| 3 | タッチスクリーン | 12 | 音量ボタン |
| 4 | 12 キー ダイヤル パッド | 13 | スピーカー ボタン |
| 5 | マイクロ セキュア デジタル標準容量（HDSC）スロット | 18 | ビデオの停止ボタン |
| [6] | ロック ボタン | 15 | ヘッドセット ボタン |
| 7 | USB ポート | 16 | ミュート ボタン |
| 8 | 通話終了ボタン | 17 | ライト ストリップを備えたハンドセット |
| 9 | 保留ボタン | | |

# Cisco DX650 ケーブルの設置




| | | | |
|---|---|---|---|
| [1] | ケンジントン セキュリティ スロット (K スロット) | [6] | コンピュータ ポート |
| 2 | Micro B USB ポート | 7 | 補助ポート |
| 3 | 3.5 mm ステレオ ライン入力/出力端子 | 8 | USB 2.0 ポート |
| 4 | 電源ポート | 9 | HDMI タイプ A ポート |
| 5 | ネットワーク ポート | | |

第 3 章

# Wi-Fi ネットワーク設定


- ネットワークの要件，25 ページ
- ワイヤレス LAN（Wireless LAN），26 ページ
- Wi-Fi ネットワーク コンポーネント，27 ページ
- WLAN 通信の 802.11 規格，31 ページ
- WLAN 通信のセキュリティ，35 ページ
- WLAN とローミング，38 ページ


## ネットワークの要件

ネットワーク内でデバイスがエンドポイントとして正常に機能するためには、ネットワークが次の要件を満たしている必要があります。

- VoIP ネットワーク
  - Cisco ルータおよびゲートウェイ上で VoIP が設定されている。
  - Cisco Unified Communications Managerがネットワークにインストールされ、コール処理用に設定されている。
- IP ネットワークが DHCP をサポートしているか、IP アドレス、ゲートウェイ、およびサブネット マスクの手動割り当てをサポートしている

（注） デバイスは、Cisco Unified Communications Manager からの日時を表示します。 ユーザが設定アプリケーションで [日付と時刻の自動設定（Automatic Date & time）] をオフにした場合、日時はサーバの時刻と同期しなくなる可能性があります。

- ワイヤレス LAN

- アクセス ポイント（AP）が WLAN を介して音声とビデオをサポートするように設定されている。
- コントローラとスイッチが音声とビデオをサポートするように設定されている。
- ワイヤレス音声デバイスおよびユーザを認証するためのセキュリティが実装されている。

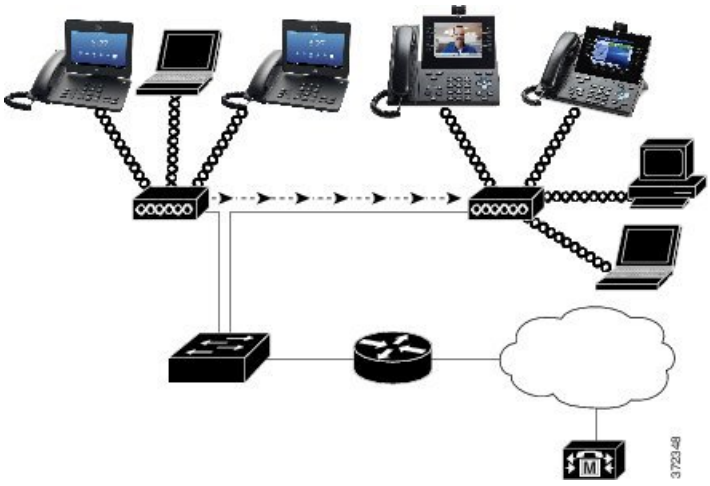
# ワイヤレス LAN（Wireless LAN）

（注） ワイヤレス Cisco DX シリーズ デバイスを配置および設定する手順については、『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

ワイヤレス機能を備えたデバイスでは、企業 WLAN 内での音声通信を行うことができます。 デバイスは、ワイヤレス音声通信を提供するために、ワイヤレス アクセス ポイント（AP）や、Cisco Unified Communications Manager Administration などの主要な Cisco IP テレフォニー コンポーネントに依存していて、これらと相互に対話します。

Cisco DX シリーズ デバイスには Wi-Fi 機能があり、802.11a、802.11b、802.11g、および 802.11n Wi-Fi を使用できます。

次の図に、ワイヤレス IP テレフォニーのワイヤレス音声伝送を可能にする典型的な WLAN トポロジを示します。



デバイスのワイヤレス アクセスがオンに設定されている場合、Cisco DX シリーズ デバイスは電源投入時に AP を検索して、AP との関連付けを行います。 記憶されているネットワークが圏外の場合は、ブロードキャストされているネットワークを選択するか、手動でネットワークを追加することができます。

AP は、有線ネットワークへの接続を使用して、スイッチとルータとの間でデータ パケットおよび音声パケットを送受信します。 音声シグナリングは、Cisco Unified Communications Manager サーバに送信され、呼処理とルーティングが行われます。

AP は、ネットワークにワイヤレス リンクまたは「ホット スポット」を提供するため、WLAN の重要なコンポーネントとなっています。 一部の WLAN では、各 AP が、LAN 上に構成された Cisco Catalyst 3750 などのイーサネット スイッチに有線接続されています。 このスイッチにより、ワイヤレス IP テレフォニーをサポートするゲートウェイや Cisco Unified Communications Manager サーバにアクセスできます。

一部のネットワークには、ワイヤレス コンポーネントをサポートする有線コンポーネントが含まれます。 そのような有線コンポーネントには、ワイヤレス機能を有効にする特別なモジュールを装備したスイッチ、ルータ、ブリッジなどがあります。

Cisco Unified Wireless Network の詳細については、http://www.cisco.com/c/en/us/products/wireless/index.html を参照してください。

# Wi-Fi ネットワーク コンポーネント

デバイスは、コールを正常に発信および受信するために、WLAN 内の複数のネットワーク コンポーネントと相互対話する必要があります。

## AP、チャネル、規制区域の関係

アクセス ポイント（AP）は、2.4 GHz または 5 GHz の周波数帯域のチャネルを使用して、RF 信号を送受信します。 安定したワイヤレス環境を提供し、チャネルの干渉を減少させるために、各 AP に重複しないチャネルを指定する必要があります。

AP、チャネル、および規制区域の関係の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』の「Designing“ ”the Wireless LAN for Voice」の項を参照してください。

## AP の相互作用

Cisco DX シリーズ デバイスはワイヤレス データ デバイスと同じ AP を使用します。 ただし、WLAN の音声トラフィックには、データ トラフィック専用の WLAN とは異なる機器の設定とレイアウトが必要です。 データ伝送では、音声伝送よりも高いレベルの RF ノイズ、パケット損失、およびチャネル コンテンションに耐えることができます。 音声伝送時のパケット損失では、不安定な音声や途切れた音声によって結果的に通話が聞き取れなくなる可能性があります。 パケット エラーにより、ビデオにブロック ノイズが発生したり、ビデオがフリーズしたりすることもあります。

デバイスはデスクトップエンドポイントであるため（モバイルエンドポイントではないため）、ローカル環境の変化により、デバイスでアクセス ポイント間のローミングが発生して、音声およびビデオのパフォーマンスに影響が出る可能性があります。 これとは対照的に、データ ユーザは一箇所に留まって、ときどき別の場所に移動します。 コールを保持しながらローミングが可能であることは、ワイヤレス音声の 1 つの利点です。そのため、RF カバレッジには、吹き抜け、エレベータ、会議室の外にある人気のない場所、通路などを含める必要があります。

優れた音声品質と最適な RF 信号カバレッジを確保するために、サイトの調査を実行する必要があります。 サイトの調査により、ワイヤレス音声に適した設定が決定されます。またサイトの調

査は、AP の位置、電力レベル、チャネル割り当てなど、WLAN の設計とレイアウトに役立ちます。

ワイヤレス音声を導入し、使用できるようにした後も、引き続き設置後のサイトの調査を実施する必要があります。 新規ユーザ グループの追加、機器の追加設置、または大量のインベントリのスタックを行うと、ワイヤレス環境が変化します。 設置後の調査で、AP のカバレッジがそれまでと同様に最適な音声通信にとって十分であるかを検証します。

（注） ローミング中にはパケット損失が発生します。しかし、セキュリティ モードおよび高速ローミングの存在により、伝送中のパケット損失数が決まります。 Cisco Centralized Key Management（CCKM）を実装して、高速ローミングを有効にすることを推奨します。

ワイヤレス ネットワークでの音声 QoS の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

# アクセス ポイントとのアソシエーション

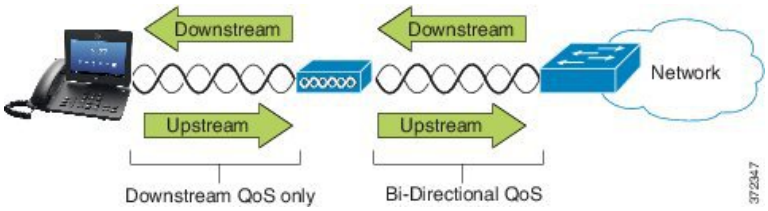
デバイスは、起動時に、認識できる SSID と暗号タイプを持つ AP をスキャンします。 デバイスにより、一連の利用可能な AP が構築、維持され、現在の設定に基づく最適な AP が選択されます。

# ワイヤレス ネットワークの QoS

ワイヤレス LAN の音声およびビデオ トラフィックは、データ トラフィックの場合と同様に、遅延、ジッター、およびパケット損失の影響を受けます。 これらの問題は、データのエンドユーザには影響しませんが、音声またはビデオ コールに重大な影響を及ぼすことがあります。 遅延やジッターを抑えて、音声およびビデオ トラフィックがタイムリーかつ確実に処理されるようにするには、Quality Of Service（QoS）を使用します。

デバイスをボイス VLAN に分離し、より高い QoS を音声パケットに割り当てることで、音声トラフィックがデータ トラフィックよりもプライオリティの高い処理を確実に受けるようにできます。その結果、パケットの遅延や損失パケットを低下させることができます。

専用帯域幅を持つ有線ネットワークとは異なり、ワイヤレス LAN では、QoA の実装時にトラフィックの方向を考慮します。 次の図に示すように、トラフィックは AP によってアップストリームまたはダウンストリームに分類されます。




Enhanced Distributed Coordination Function（EDCF）タイプの QoS には、ダウンストリーム（802.11b/g クライアント方向）QoS 用に最大 8 つのキューがあります。 キューは次のオプションに基づいて割り当てることができます。

- パケットの QoS または DiffServ コード ポイント（DSCP）設定
- レイヤ 2 またはレイヤ 3 アクセス リスト
- 特定のトラフィックの VLAN
- デバイスの動的登録

AP で最大 8 つのキューを設定できますが、可能な限り高い QoS を保障するため、それぞれ音声トラフィック、ビデオ トラフィック、およびシグナリング トラフィック用の 3 つのキューのみを使用する必要があります。 音声は音声キュー（UP6）に、ビデオはビデオ キュー（UP5）に、シグナリング（SIP）トラフィックはビデオ キュー（UP4）に、データ トラフィックはベストエフォート キュー（UP0）に入れます。 802.11b/g EDCF では音声トラフィックがデータ トラフィックから保護される保証はありませんが、このキューイング モデルを使用することで、統計的に最高の結果が得られます。

各キューは次のとおりです。

- ベスト エフォート（BE）：0、3
- バックグラウンド（BK）：1、2
- ビデオ（VI）：4、5
- ビデオ（VO）：6、7

（注） デバイスは、SIP シグナリング パケットに DSCP 値 24（CS3）をマークし、RTP パケットに DSCP 値 46（EF）をマークします。

（注） コール制御（SIP）は、UP4（VI）として送信されます。アドミッション制御必須（ACM）がビデオに対して無効になっている場合（Traffic Specification（TSpec）が無効にされている場合）、ビデオは UP5（VI）として送信されます。 ACM が音声に対して無効になっている場合（TSpec 無効）、音声は UP6（VO）として送信されます。

次の表に、音声、ビデオ、およびコール制御（SIP）のトラフィックの優先順位を指定する、AP 上の QoS プロファイルを示します。

**表 *9*：*QoS* プロファイルとインターフェイス設定**

| トラフィックのタイプ | DSCP | 802.1p | WMM UP | ポート範囲 |
|---|---|---|---|---|
| 音声 | EF（46） | 5 | 6 | UDP：16384 ～ 32767 |
| インタラクティブ ビデオ | AF41（34） | 4 | 5 | UDP：16384 ～ 32767 |
| コール制御 | CS3（24） | 3 | 4 | TCP：5060 ～ 5061 |

非決定性環境での音声伝送の信頼性を改善するため、デバイスは IEEE 802.11e 業界規格をサポートし、Wi-Fi Multimedia（WMM）に対応しています。 WMM は、音声、ビデオ、ベストエフォートデータ、およびその他のトラフィックの差別化サービスを可能にします。 これらの差別化サービスが音声パケットに十分な QoS を提供するために、一度に 1 つのチャネルで一定量の音声帯域幅だけが使用可能または許可されています。 ネットワークが予約済み帯域幅で処理可能なボイスコールが「N」個で、音声トラフィックの量がこの制限を超えた（「N+1」個のコール）場合、すべてのコールの品質が低下します。

コール品質の問題に対処するには、初期コール アドミッション制御（CAC）方式が必要です。 WLAN 上で SIP CAC が有効になっている場合、アクティブな音声コールの数が AP に設定された制限を超過しないように制限することで、ネットワークが過負荷の場合でも QoS が維持されます。 ネットワークが輻輳している間、システムは AP が「フル キャパシティ」の場合でも、ワイヤレス デバイス クライアントが隣接 AP へローミングできる程度の帯域幅の予約を維持します。 音声帯域幅の制限に達すると、チャネルの既存コールの品質に影響を与えないように、その次のコールと隣接 AP との間でロード バランシングが行われます。

（注） Cisco DX シリーズ デバイスは SIP 通信には TCP を使用し、AP がフル キャパシティの場合 Cisco Unified Communications Manager での登録が失われる可能性があります。 CAC によって承認されていないクライアントから送受信されるフレームはドロップされるため、Cisco Unified Communications Manager 登録解除の原因となることがあります。 そのため、SIP CAC を無効にすることを推奨します。

（注） ビデオ フレームの最適な伝送を行うために、DSCP、COS、および WMM UP マーキングが正しく表示されます。 デバイスでは音声とビデオの CAC がサポートされていないため、SOP CAC を実装することを推奨します。

デバイスは、ビデオが異なる種類のデバイスで再生される際の一貫性のない QoS や一貫性のない帯域幅アカウンティングを解決するために、フレキシブル DSCP やビデオ プロモーション機能を使用します。

### フレキシブル DSCP のセット アップ

**手順**

**ステップ 1** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、[システム（System）] > [サービスパラメータ（Service Parameters）] に移動します。

**ステップ 2** [クラスタ全体のパラメータ（システム：ロケーションとリージョン）（Clusterwide Parameters (System - Location and Region)）]で、[イマーシブビデオ帯域コールにビデオ帯域幅プールを使用（Use Video BandwidthPool for Immersive Video Calls）] を [いいえ（False）] に設定します。

**ステップ 3** [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)）]で、[ビデオコール QoS マーキング ポリシー（Video Call QoS Marking Policy）] を、[イマーシブにプロモートする（Promote to Immersive）] に設定します

**ステップ 4** 変更を保存します。

## Cisco Unified Communications Manager の連携

Cisco Unified Communications Manager は、電話会議やルート プランなどの機能で使用する IP テレフォニー システムのコンポーネント（エンドポイント、アクセス ゲートウェイ、およびリソース）を管理します。

Cisco DX シリーズ デバイスは、Cisco Unified Communications Manager リリース 8.5(1)、8.6(2)、9.1(2)、10.5(1) 以降でサポートされています。

Cisco Unified Communications Manager は、デバイスがデータベースで登録および設定されるまではそのデバイスを認識できません。

IP デバイスと連携するようにCisco Unified Communications Manager を設定する方法についての詳細は、『*Cisco Unified Communications Manager Administration Guide*』、『*Cisco Unified Communications Manager System Guide*』、および『*Cisco DX Series Wireless LAN Deployment Guide*』に記載されています。

# WLAN 通信の 802.11 規格

ワイヤレス LAN は、すべてのイーサネットベースのワイヤレス トラフィックの基準となるプロトコルを定義する電気電子学会（IEEE）802.11 規格に従う必要があります。 Cisco DX シリーズ デバイスでは次の標準がサポートされています。

- 802.11a：5 GHz 周波数帯を使用して OFDM テクノロジーを使用することで、より多くのチャネルを提供し、データ レートを向上させます。 Dynamic Frequency Selection（DFS）および伝送パワー制御（TPC）は、この規格をサポートしています。

- 802.11b：低データ レート（1、2、5.5、11 Mbps）でデータを送受信するために 2.4 GHz の無線周波数（RF）を指定します。
- 802.11d：アクセス ポイントが、現在サポートされている無線チャネルおよび送信電力レベルを通知できるようにします。 802.11d が有効なクライアントは、その情報を使用して使用するチャネルと電力を決定します。 デバイスは、指定の国で法的に許可されたチャネルを判別するためにワールド モード（802.11d）が必要です。 サポートされているチャネルについては、次の表を参照してください。 Cisco IOS アクセス ポイントまたは Cisco Unified Wireless LAN Controller で 802.11d が適切に設定されていることを確認してください。
- 802.11e：無線 LAN アプリケーションの一連の Quality of Service（QoS）拡張を定義します。
- 802.11g：802.11b と同じ免許不要の 2.4 GHz 周波数帯を使用します。ただし、直交周波数分割多重方式（OFDM）テクノロジーを使用することで、データ レートを高め、より高いパフォーマンスを提供します。 OFDM は、RF を使用して信号を伝送するための物理層の符号化テクノロジーです。
- 802.11h：5 GHz スペクトラムと伝送電力管理を提供します。 802.11a メディア アクセス コントロール（MAC）に、DFS と TPC を提供します。
- 802.11i：無線ネットワークにセキュリティ メカニズムを指定します。
- 802.11n：2.4 GHz または 5 GHz の無線周波数を使用してデータを送受信し、Multiple-Input Multiple-Output（MIMO）テクノロジー、チャネル ボンディング、およびペイロードの最適化を使用してデータ転送を強化します。

（注） Cisco DX シリーズ デバイスはアンテナを 1 つ装備しており、Single Input Single Output（SISO）システムを使用します。このシステムでは、MCS 0 ～ MCS 7（20 MHz チャネルで 72 Mbps、40 MHz チャネルで 150 Mbps）のデータ レートのみがサポートされます。 より高いデータ レートを利用可能な MIMO テクノロジーを 802.11n クライアントが使用している場合は、オプションとして MCS 8 ～ MCS 15 を有効にすることができます。

表 *10*：***Cisco DX*** シリーズ デバイスでサポートされているチャネル

| 帯域範囲 | 使用可能なチャネル | チャネル セット |
|---|---|---|
| 2.412～2.472 GHz | 13 | 1 ～ 13 |
| 5.180～5.240 GHz | 4 | 36、40、44、48 |
| 5.260～5.320 GHz | 4 | 52、56、60、64 |
| 5 500～5.700 GHz | 11 | 100 ～ 140 |
| 5.745～5.825 GHz | 5 | 149、153、157、161、165 |

（注） （注）チャネル 120、124、128 はアメリカ、ヨーロッパ、日本ではサポートされていませんが、他の地域ではサポートされている場合があります。

WLAN のサポートされているデータ レート、Tx Power、および受信感度については、『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

# ワールド モード（802.11d）

Cisco DX シリーズ デバイスは 802.11d を使用して、使用するチャネルと送信電力レベルを決定します。 デバイスのクライアント設定は、関連付けられたアクセス ポイントから継承されます。 デバイス をワールド モードで使用するには、アクセス ポイントのワールド モード（802.11d）を有効にします。 ワールド モードの有効化の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

（注） 周波数が 2.4 GHz で現在のアクセス ポイントがチャネル 1 ～ 11 で送信している場合は、必ずしもワールド モード（802.11d）を有効にする必要はありません。

すべての国でこれらの周波数はサポートされているため、ワールドモード（802.11d）をサポートしているかどうかに関係なくこれらのチャネルのスキャンを試行できます。2.4GHz をサポートする国については、『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

アクセス ポイントが設置されている国に応じて、ワールド モード（802.11d）を有効にします。 ワールド モードは、Cisco Unified Wireless LAN Controller に対して自動的に有効になります。

# ワイヤレス変調テクノロジー

ワイヤレス通信では、シグナリングに次の変調テクノロジーが使用されます。

### ダイレクト シーケンス スペクトラム拡散方式（DSSS）

信号を周波数範囲または帯域幅に分散することで、干渉を防止しています。 DSSS テクノロジーは、データの塊を複数の周波数上に多重化し、複数のデバイスが干渉を受けずに通信できるようにします。 各デバイスには、そのデバイスのデータ パケットを識別する特殊なコードがあり、その他のデータ パケットはすべて無視されます。 Cisco ワイヤレス 802.11b/g 製品は、WLAN 上の複数のデバイスをサポートするために DSSS テクノロジーを使用しています。

### 直交周波数分割多重方式（OFDM）

RF を使用して信号を伝送します。 OFDM は、物理層の符号化テクノロジーで、1 つの高速データ キャリアを複数のより低速なキャリアに分割し、RF スペクトラムを経由してそれらを並行して伝送します。 802.11g および 802.11a で使用した場合、OFDM は最大 54 Mbps のデータ レートをサポートします。

次の表に、データ レート、チャネル数、および変調テクノロジーを規格別に比較したものを示します。

**表 *11*：*IEEE* 規格別のデータ レート、チャネル数、および変調テクノロジー**

| 項目 | 802.11b | 802.11g | 802.11a | 802.11n |
|---|---|---|---|---|
| データ レート | 1、2、5.5、11 Mbps | 6、9、12、18、24、36、48、54 Mbps | 6、9、12、18、24、36、48、54 Mbps | • 20 MHz チャネル: 7 ～72 Mbps<br>• 40 MHz チャネル: 15～150 Mbps |
| 重複しないチャネル | 3 | 3 | 最大 24 | 最大 24 |
| ワイヤレス変調 | DSSS | OFDM | OFDM | OFDM |

# 無線周波数範囲

WLAN 通信では、次の無線周波数（RF）範囲が使用されます。

- 2.4 GHz：2.4 GHz を使用する多くのデバイスは、潜在的に 802.11b/g 接続と干渉を起こすおそれがあります。 干渉によってサービス拒否（DoS）シナリオが発生する可能性があり、正常な 802.11 伝送を妨害するおそれがあります。
- 5 GHz：この範囲は、Unlicensed National Information Infrastructure（UNII）周波数帯と呼ばれる複数の帯域に分割され、各帯域には4つのチャネルがあります。 重複しないチャネル、および 2.4 GHz よりも多くのチャネルを提供するため、各チャネルに 20 MHz ずつ割り当てられます。

# WLAN 通信のセキュリティ

通信圏内にあるすべての WLAN デバイスは他の WLAN トラフィックをすべて受信できるため、WLANにおける音声通信のセキュリティは非常に重要です。音声トラフィックが侵入者によって操作または傍受されることのないように、Cisco SAFE セキュリティ アーキテクチャは Cisco DX シリーズ デバイスと Cisco Aironet AP をサポートしています。 ネットワークでのセキュリティの詳細については、http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.htmlを参照してください。

## 認証方式

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

WLAN 認証

- WPA（802.1x 認証 + TKIP または AES 暗号化）
- WPA2（802.1x 認証 + AES または TKIP 暗号化）
- WPA-PSK（事前共有キー + TKIP 暗号化）
- WPA2-PSK（事前共有キー + AES 暗号化）
- Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling（EAP-FAST）
- Extensible Authentication Protocol – Transport Layer Security（EAP-TLS）
- PEAP（Protected Extensible Authentication Protocol）MS-CHAPv2 および GTC
- Cisco Centralized Key Management（CCKM）
- オープン（Open）

WLAN 暗号化

- AES（Advanced Encryption Scheme）
- Temporal Key Integrity Protocol/Message Integrity Check（TKIP/MIC）
- WEP（Wired Equivalent Protocol）40/64 および 104/128 ビット

（注） 802.1x 認証を使用した動的 WEP および共有キー認証はサポートされません。

認証方法の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』の「Wireless“ ”Security」の項を参照してください。

## 認証キー管理

次の認証方式では、RADIUS サーバを使用して認証キーを管理します。

- WPA/WPA2: 一意の認証キーを生成するために RADIUS サーバの情報を使用します。 これらのキーは、中央集中型の RADIUS サーバで生成されるため、WPA/WPA2 は、AP およびデバイスに格納されている WPA 事前共有キーよりも高いセキュリティを提供します。
- Cisco Centralized Key Management（CCKM）：RADIUS サーバとワイヤレス ドメイン サーバ（WDS）の情報を使用して、キーの管理および認証をします。 WDS は、高速でセキュアな再認証用に、CCKM 対応クライアント デバイスのセキュリティ クレデンシャルのキャッシュを作成します。

WPA/WPA2 および CCKM では、暗号化キーはデバイスに入力されず、AP とデバイスの間で自動的に生成されます。 ただし認証で使用する EAP ユーザ名とパスワードは、各デバイスに入力する必要があります。

## 暗号化方式

音声トラフィックの安全性を確保するため、Cisco DX シリーズ デバイスでは、暗号化方式として WEP、TKIP、および Advanced Encryption Standards（AES）をサポートします。 これらのメカニズムが暗号化に使用される場合、AP とデバイスの間で音声 Real-Time Transport Protocol（RTP）パケットが暗号化されます。

**WEP**

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

**TKIP**

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

**AES**

WPA2 認証に使用される暗号化方式。 この暗号化の国内規格は、暗号化と復号化に同じキーを持つ対称型アルゴリズムを使用します。

暗号化方法の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』の「Wireless“ ”Security」の項を参照してください。

## AP 認証および暗号化のオプション

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

（注）

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

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

**表 *12*：認証方式と暗号化方式**

| **Cisco WLAN の設定** | | | **Cisco DX シリーズ の設定** |
|---|---|---|---|
| 認証 | キー管理 | 共通の暗号化 | 認証 |
| オープン | なし | なし | なし |
| 静的 WEP | なし | WEP | WEP |
| EAP-FAST | WPA または WPA2 とオプションの CCKM | TKIP または AES | 802.1x EAP > EAP-FAST |
| PEAP-MSCHAPv2 | WPA または WPA2 とオプションの CCKM | TKIP または AES | 802.1x EAP > PEAP > MSCHAPV2 |
| PEAP-GTC | WPA または WPA2 とオプションの CCKM | TKIP または AES | 802.1x EAP > PEAP > GTC |
| EAP-TLS | WPA または WPA2 とオプションの CCKM | TKIP または AES | 802.1x EAP > TLS |

| Cisco WLAN の設定 | | | Cisco DX シリーズ の設定 |
|---|---|---|---|
| WPA/WPA2-PSK | WPA-PSK または WPA2-PSK | TKIP または AES | WPA/WPA2 PSK |

シスコの WLAN セキュリティに関する追加情報については、http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html を参照してください。

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

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

# WLAN とローミング

Cisco DX シリーズ デバイスは、Cisco Centralized Key Management（CCKM）をサポートしています。これは、ワイヤレス ドメイン サーバ（WDS）のセッション クレデンシャルでのキャッシュを提供する、集中化されたキー管理プロトコルです。

CCKM の詳細については、次の Web サイトにある『*Cisco Fast Secure Roaming Application Note*』を参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

第 4 章

# 展開


- コンフィギュレーション ファイル，39 ページ
- MAC アドレスの確認，40 ページ
- Cisco Unified Communications Manager へのデバイスの追加方法，40 ページ
- Cisco Unified Communications Manager ユーザの追加，44 ページ
- デバイス モデルの指定，46 ページ
- 回線の設定，46 ページ
- ユーザとデバイスの関連付け，48 ページ
- Survivable Remote Site Telephony，48 ページ


## コンフィギュレーション ファイル

TFTP サーバは、Cisco Unified Communications Manager への接続パラメータを定義するデバイス コンフィギュレーションファイルを保存します。通常は、デバイスのリセットが必要となる変更を Cisco Unified Communications Manager で行うたびに、その変更がデバイスのコンフィギュレーション ファイルに自動的に反映されます。

コンフィギュレーションファイルには、デバイスで実行するイメージロードに関する情報も含まれています。このイメージのロードが、デバイスに現在ロードされているイメージと異なる場合、そのデバイスは TFTP サーバと交信して、必要なロード ファイルを要求します。イメージロードのサイズのために、デバイスと TFTP サーバの間で TCP ポート 6970 が開いている必要があります。

次の条件に該当する場合、デバイスは、TFTP サーバにある XmlDefault.cnf.xml という名前のデフォルト コンフィギュレーション ファイルにアクセスします。

- 自動登録が Cisco Unified Communications Manager で有効になっている。
- デバイスをまだ Cisco Unified Communications Manager データベースに追加していない。
- 初めて登録されるデバイスである。

（注） コンフィギュレーション ファイル内のデバイス セキュリティ モードが Authenticated または Encrypted に設定されているが、デバイスで CTL ファイルや ITL ファイルをまだ受信していない場合は、安全に登録できるように、デバイスはファイルの取得を 4 回試みます。

自動登録が有効になっておらず、デバイスが Cisco Unified Communications Manager データベースにまだ追加されていない場合、登録要求は拒否されます。 この場合、デバイスの画面には [アウトオブサービス（Out of service）] と表示されます。

Cisco DX シリーズ デバイスは SEPmac_address.cnf.xml という名前のコンフィギュレーション ファイルにアクセスします（mac_address はデバイスのイーサネット MAC アドレス）。 CTL または ITL がインストールされている場合、デバイスは代わりに SEPmac_address.cnf.xml.sgn という名前のコンフィギュレーションファイルにアクセスします。デバイスが最初に設定されるとき、Cisco Unified Communications Manager Administration の [電話の設定（Phone Configuration）] ウィンドウにある [説明（Description）] フィールドには事前に値が設定されます。 MAC アドレスはデバイスを一意に識別します。

# MAC アドレスの確認

次の方法で、デバイスの MAC アドレスを確認できます。

- デバイスから、[アプリケーション（Applications）]>[設定（Settings）]>[端末について（About device）] > [ステータス（Status）] を選択し、[MAC アドレス（MAC Address）] フィールドを確認します。
- デバイスの背面にある MAC ラベルを確認します。
- デバイスの 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。

# Cisco Unified Communications Manager へのデバイスの追加方法

デバイスを設置する前に、Cisco Unified Communications Manager データベースにエンドポイントを追加する方法を選択する必要があります。

次の表に、デバイスを Cisco Unified Communications Manager データベースに追加する方法の概要を示します。

表 *13* : *Cisco Unified Communications Manager* にデバイスを追加する方法

| 方法 | MAC アドレスの必要性 | 注記 |
|---|---|---|
| 自動登録 | いいえ | 電話番号の自動割り当てが可能です。 |
| Tool for AutoRegistered Phones Support（TAPS）を使用した自動登録 | いいえ | 自動登録および一括管理ツール（BAT）が必要です。[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] とデバイスで情報を更新します。 |
| Cisco Unified Communications Managerの管理 | はい | デバイスを個別に追加する必要があります。 |
| Cisco Unified Communications Manager 一括管理ツール | はい | 複数のデバイスを同時に登録できます。 |
| セルフプロビジョニング | いいえ | ユーザが各自のデバイスをプロビジョニングできます。 |

# 自動登録

デバイスを設置する前に自動登録を有効にすると、次の操作が可能になります。

- デバイスから MAC アドレスを事前に収集せずに、デバイスを追加する。
- IP テレフォニー ネットワークにデバイスを物理的に接続するときに、Cisco Unified Communications Manager データベースをデバイスに自動的に追加する。 自動登録の実行中、Cisco Unified Communications Manager により、電話番号がその順序に従って、デバイスに順次自動的に割り当てられる。
- デバイスを Cisco Unified Communications Manager データベースに迅速に入力し、電話番号などの設定を Cisco Unified Communications Manager から変更する。
- 自動登録されたデバイスを新しい場所に移動し、電話番号を変更しないまま別のデバイスプールに割り当てる。

（注） 自動登録は、ネットワークに追加するデバイスが 100 台未満の場合に使用することを推奨します。 100 台を超えるデバイスをネットワークに追加するには、一括管理ツール（BAT）を使用します。

自動登録は、デフォルトでは無効になっています。自動登録を使用しない方がよい場合もあります。たとえば、デバイスに特定の電話番号を割り当てる場合や、『*Cisco Unified Communications Manager Security Guide*』で説明されているように、Cisco Unified Communications Manager とのセキュア接続を使用する場合です。自動登録の有効化の詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Autoregistration“ ”Setup」の項を参照してください。

# 自動登録と TAPS

自動登録と TAPS（Tool for Autoregistered Phones Support）を使用すると、デバイスから MAC アドレスを事前に収集せずに、デバイスを追加できます。

TAPS は、一括管理ツール（BAT）と連携し、Cisco Unified Communications Manager データベースにダミー MAC アドレスを使用して既に追加されている一連のデバイスを更新します。MAC アドレスを更新し、事前定義された設定をダウンロードするには、TAPS を使用します。

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

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

TAPS が機能するためには、[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）]（[システム（System）] > [Cisco Unified CM]）で自動登録が有効になっている必要があります。

（注） Cisco CTL クライアントを通じてクラスタを混合モードに設定すると、自動登録は自動的に無効になります。Cisco CTL クライアントを通じてクラスタを非セキュア モードに設定すると、自動登録は自動的には有効になりません。

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

# Cisco Unified Communications Manager へのデバイスの追加

デバイスを Cisco Unified Communications Manager データベースに個別に追加できます。追加するには、まず各デバイスの MAC アドレスを取得する必要があります。

### 手順

**ステップ 1** MAC アドレスを収集した後、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で [デバイス（Device）] > [電話（Phone） の順に選択します。

**ステップ 2** [新規追加（Add New）] をクリックします。

**ステップ 3** [電話のタイプ（Phone Type）] ドロップダウン リスト ボックスで、デイバスのタイプを選択します。

（注） Cisco Unified Communications Manager のバージョンによっては、Cisco DX シリーズ デバイスを追加するときに、ファームウェアをインストールする前に Device Enabler をインストールする必要があります。

**ステップ 4** [次へ（Next）] をクリックします。

**ステップ 5** デバイス固有の詳細なパラメータ（[デバイス プール（Device Pool）]、[デバイス セキュリティ プロファイル（Device Security Profile）] など）を入力します。

**ステップ 6** [保存（Save）]] をクリックします。
詳細については、『*Cisco Unified Communications Manager System Guide*』の「System Configuration Overview」の章を参照してください。

# 一括管理ツールの電話テンプレートを使用したデバイスの追加

Cisco Unified Communications Manager 一括管理ツール（BAT）では、複数のデバイスの登録など、バッチ操作を実行できます。

一括管理ツールの詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide*』を参照してください。

### 手順

**ステップ 1** 各デバイスの MAC アドレスを取得します。

**ステップ 2** Cisco Unified Communications Managerから、[一括管理（Bulk Administration）] > [電話（Phones）] > [電話テンプレート（Phone Template）] の順に選択します。

**ステップ 3** [新規追加（Add New）] をクリックします。

**ステップ 4** [電話のタイプ（Phone Type）] を選択し、[次へ（Next）] を選択します。

**ステップ 5** [デバイス プール（Device Pool）]、[デバイス セキュリティ プロファイル（Device Security Profile）] などのデバイス固有のパラメータの詳細を入力します。

**ステップ 6** [保存（Save）] をクリックします。

**ステップ 7** [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [電話（Phone）] > [新規追加（Add New）] の順に選択し、既存の一括管理ツール テンプレートを使用してデバイスを追加します。

# セルフプロビジョニング

セルフ プロビジョニング機能を使用すると、ユーザが自分のデバイスを設定できるため、管理者の労力が軽減されます。 セルフプロビジョニングが有効な場合、ユーザはデバイス設定時に自分のクレデンシャルを入力します。 デバイスのMACアドレスやその他の設定情報は、Cisco Unified Communications Manager サーバと共有されます。

セルフプロビジョニングには、Cisco Unified Communications Manager リリース 10.0 以降が必要です。 詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Self-Provisioning」の章を参照してください。

## セルフプロビジョニングの有効化

**手順**

**ステップ 1** [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[ユーザ管理（User Management） > [ユーザ設定（User Setting）] > [ユーザプロファイル（User Profile）] に移動します。

**ステップ 2** セルフプロビジョニングを [有効（Enabled）] に設定します。

**ステップ 3** [ユーザ管理（User Management）] > [エンド ユーザ（End User）] に移動します。

**ステップ 4** セルフ サービス ユーザ ID を設定します。

**ステップ 5** [ユーザ管理（User Management）] > [セルフプロビジョニング（Self Provisioning）] に移動し、認証モードを選択します。

# Cisco Unified Communications Manager ユーザの追加

ここでは、Cisco Unified Communications Manager にユーザを追加する手順について説明します。使用しているオペレーティング システムと、ユーザの追加方法に応じて、この項の手順のいずれかに従ってください。

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

LDAP ディレクトリを使用していない場合は、ユーザを Cisco Unified Communications Manager に直接追加することができます。

（注） LDAP が同期している場合、ユーザを Cisco Unified Communications Manager に追加することはできません。

### 手順

**ステップ 1** [ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択して、[新規追加（Add New）] 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ます。

**ステップ 2** このウィンドウの [ユーザ情報（User Information）] ペインで、次の情報を入力します。

- [ユーザ ID（User ID）]：エンド ユーザの識別名を入力します。 Cisco Unified Communications Manager では、ユーザ ID の作成後、それを変更することはできません。 使用できる特殊文字は、=、+、<、>、#、;、\、""、および空白です。
- [パスワード（Password）] および [パスワードの確認（Confirm Password）]：エンド ユーザのパスワードとして、5 文字以上の英数字または特殊文字を入力します。 使用できる特殊文字は、=、+、<、>、#、;、\、""、および空白です。
- [姓（Last Name）]：エンド ユーザの姓を入力します。 使用できる特殊文字は、=、+、<、>、#、;、\、""、および空白です。
- [電話番号（Telephone Number）]：エンド ユーザのプライマリ電話番号を入力します。 エンド ユーザは、デバイスに複数の回線を設定できます。

**ステップ 3** [Save] をクリックします。

**ステップ 4** デバイス モデルの指定, （46 ページ）に進みます。

# 外部 LDAP ディレクトリからのユーザの追加

ユーザを LDAP ディレクトリ（Cisco Unified Communications Server 以外のディレクトリ）に追加した場合は、次の手順に従うことにより、そのディレクトリを、この同じユーザとデバイスを追加している Cisco Unified Communications Manager にただちに同期化できます。

### 手順

**ステップ 1** Cisco Unified Communications Manager の管理にサインインします。

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

**ステップ 3** [検索（Find）] ボタンを使用して、対象の LDAP ディレクトリを見つけます。

**ステップ 4** LDAP ディレクトリ名をクリックします。

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

（注） LDAP ディレクトリを Cisco Unified Communications Manager に即座に同期化する必要がない場合は、[LDAP ディレクトリ（LDAP Directory）] ウィンドウの [LDAP ディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] で、次の自動同期化のスケジュールを決定します。 ただし、新規ユーザをデバイスに関連付けるには、その前に同期を完了する必要があります。

**ステップ 6** デバイス モデルの指定, （46 ページ）に進みます。

# デバイス モデルの指定

**手順**

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

**ステップ 2** [新規追加（Add New）] をクリックします。

**ステップ 3** デバイス モデルを [電話のタイプ（Phone Type）] ドロップダウン リストから選択し、[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** 回線の設定, （46 ページ）に進みます。

# 回線の設定

[電話の設定（Phone Configuration）] ウィンドウでは、ほとんどのフィールドにデフォルト値を使用できます。

**手順**

**ステップ 1** [電話の設定（Phone Configuration）] ウィンドウで、ウィンドウの左ペインにある [回線 1（Line 1）] 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 2** [電話番号（Directory Number）] フィールドに、[ユーザの設定（User Configuration）] ウィンドウの [電話番号（Telephone Number）] フィールドに表示される番号と同じ番号を入力します。

**ステップ 3** [ルート パーティション（Route Partition）] ドロップダウン リストから、電話番号が属するパーティションを選択します。 電話番号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 4** [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（[電話番号の設定（Directory Number Configuration）] ウィンドウの [電話番号の設定（Directory Number Settings）]

ペイン）から、適切なコーリング サーチ スペースを選択します。 コーリング サーチ スペースは、この電話番号からコールを発信できる番号を検索するための、パーティションのリストで構成されます。 選択した値は、この電話番号を使用するすべてのデバイスに適用されます。

**ステップ 5** [電話番号の設定（Directory Number Configuration）] ウィンドウの [コール転送の設定（Call Forward Settings）] ペインで、項目（[不在転送（Forward All）]、[話中転送（内部）（Forward Busy Internal）] など）と、それに対応するコールの転送先を選択します。

**例**：
ビジー信号を受ける着信内線コールまたは外線コールを、この回線のボイス メールに転送するには、[コール転送の設定（Call Forward Settings）] ペインの [ボイスメール（Voice Mail）] ボックスをオンにします。

**ステップ 6** [電話番号の設定（Directory Number Configuration）] ウィンドウの [デバイス（Device）] ペインの [回線 1（Line 1）] フィールドで、次の項目を設定します。

a) [表示（内線発信者 ID フィールド）（Display (Internal Caller ID field)）]：このデバイスのユーザの姓と名を入力します。入力した名前は、すべての内線コールに表示されるようになります。 このフィールドを空白にして、電話機の内線番号をシステムに表示させることもできます。

b) [外線電話番号マスク（External Phone Number Mask）]：この回線からコールを発信したときに、発信者 ID 情報の送信に使用される電話番号（マスク）を指定します。 最大 24 個の番号と文字「X」が入力することができます。 X は電話番号を表し、パターンの最後に使用する必要があります。

**例**：
たとえば、マスク 555902XXXX を指定すると、内線 6640 からの外線コールには、発信者 ID の番号として 5559026640 が表示されます。

c) [Save] をクリックします。

（注） この設定は、[共有デバイス設定の更新（Update Shared Device Settings）] をオンにして [選択対象を反映（Propagate Selected）] ボタンをクリックしない限り、現在のデバイスだけに適用されます。 （右側のチェックボックスは、この電話番号を他のデバイスと共有している場合のみ表示されます）。

**ステップ 7** このウィンドウの下部にある [エンドユーザの関連付け（Associate End Users）] をクリックして、設定している回線にユーザを関連付けます。

a) ユーザを検索するには、[検索（Search）] フィールドとともに [検索（Find）] ボタンを使用します。

b) ユーザ名の横にあるボックスをオンにして、[選択項目の追加（Add Selected）] を選択します。 [電話番号の設定（Directory Number Configuration）] ウィンドウの [回線に関連付けられているユーザ（Users Associated With Line）] ペインに、ユーザ名とユーザ ID が表示されます。

c) [Save] をクリックします。
これでユーザが、デバイスの回線 1 に関連付けられました。

**ステップ 8** デバイスに 2 番目の回線がある場合は、回線 2 を設定します。

**ステップ 9** ユーザとデバイスの関連付け，（48 ページ）に進みます。

# 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 Communications ManagerAdministration）] で、[ユーザ管理（User Management）] > [エンド ユーザ（End User）] の順に選択します。
[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが表示されます。

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

**ステップ 3** 表示されるレコードのリストで、ユーザのリンクを選択します。

**ステップ 4** [デバイスの割り当て（Device Association）] を選択します。
[ユーザ デバイス割り当て（User Device Association）] ウィンドウが表示されます。

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

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

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

**ステップ 8** [関連リンク（Related Links）] ドロップダウン リストで [ユーザの設定に戻る（Back to User）] を選択し、[検索（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。

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

# Survivable Remote Site Telephony

Survivable Remote Site Telephony（SRST）機能は、制御側 Cisco Unified Communications Manager との通信が切断されても、基本的なコール機能へのアクセスを確保します。 このシナリオでは、デバイスで進行中のコールをアクティブ状態に維持できるため、ユーザは使用可能な機能のサブセットにアクセスできます。フェールオーバーが発生すると、ユーザのデバイスにアラート メッセージが表示されます。 SRST を使用するには Cisco IOS バージョン 12.4(20) 以上が必要です。

（注） SRST は IPv6 をサポートしません。

第 5 章

# インストール


- Cisco DX シリーズ デバイスの設置，49 ページ
- ワイヤレス LAN のセットアップ，50 ページ
- ネットワークの設定，52 ページ
- 起動プロセス，68 ページ
- 起動時の検証，70 ページ


## Cisco DX シリーズ デバイスの設置

デバイスをCisco Unified Communications Manager データベースに追加したら、デバイスを設置できます。 デバイスは、管理者（またはユーザ）がユーザの作業場所に設置します。

（注） デバイスは、新品の場合でも、設置する前に最新のファームウェア イメージにアップグレードしてください。 アップグレードについては、次の URL で対象のデバイスの readme ファイルを参照してください。

http://software.cisco.com/download/release.html?mdfid=284721679&flowid=46173&softwareid=282074288

デバイスがネットワークに接続すると、デバイスの起動プロセスが開始し、デバイスがCisco Unified Communications Manager に登録されます。 デバイスの設置を完了するには、DHCP サービスを有効にするかどうかに応じて、デバイスにネットワーク設定値を設定します。

自動登録を使用した場合は、デバイス固有の設定情報を更新します。例えば、ユーザにデバイスを関連付けたり、電話番号を変更したりします。

次の手順は、Cisco DX シリーズ デバイスの設置タスクの概要およびチェックリストを示します。この手順では、推奨する順序に従ってデバイスを設置するプロセスを解説しています。 一部のタスクは、システムおよびユーザのニーズによっては省略できます。

### 手順

**ステップ 1** 電源を選択します。

- 外部電源
- [Cisco DX650 のみ] Power over Ethernet（PoE）

（注） PoE+ 802.3at により、デバイスに接続されているアクセサリ（マウスまたはキーボードなど）が電源についてネゴシエートします。 アクセサリ用に十分な電力がなければ、画面にエラー メッセージが表示されます。 デバイスを WLAN 環境で使用する場合、外部電源が必要です。

**ステップ 2** デバイスを組み立て、ネットワーク ケーブルを接続します。 WLAN 環境でデバイスを使用する場合は、ステップ 5 を参照してください。
このステップでは、デバイスの位置を決めて設置し、ネットワークに接続します。

**ステップ 3** デバイスの起動プロセスをモニタします。 このステップでは、プライマリとセカンダリの電話番号、および電話番号に関連付ける機能をデバイスに追加し、デバイスが正しく設定されていることを確認します。

**ステップ 4** ワイヤレス ネットワークにデバイスを展開する場合は、ステップ 5 に進みます。
IP ネットワーク向けのデバイスでイーサネット ネットワークを設定する場合は、DHCP を使用するか IP アドレスを手動で入力して、デバイスの IP アドレスを設定できます。

**ステップ 5** ワイヤレス ネットワーク上にデバイスを展開する場合、次を実行する必要があります。

- ワイヤレス ネットワークを設定します。
- [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] でデバイスに対しワイヤレス LAN を有効にします。
- デバイスにワイヤレス ネットワーク プロファイルを設定します。

（注） デバイスのワイヤレス LAN は、デバイスにイーサネット ケーブルが接続されているとアクティブになりません。

**ステップ 6** デバイスを使用してコールを発信し、コール アプリケーション種々の機能が正常に動作することを確認します。

**ステップ 7** デバイスの使用方法と設定方法に関する情報をエンド ユーザに提供します。

# ワイヤレス LAN のセットアップ

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

ワイヤレス ネットワーク設定の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

# Cisco Unified Communications Manager Administration でのワイヤレス LAN のセットアップ

Cisco Unified Communications Managerで、デバイスの「Wi-Fi」というパラメータを有効にする必要があります。 Cisco Unified Communications Manager Administration の次のいずれかの場所で、このパラメータを有効にすることができます。

- 特定のデバイスに関してワイヤレス LAN を有効にするには、その特定のデバイスの [プロダクト固有の設定（Product Specific Configuration Layout）] セクション（[デバイス（Device）] > [電話（Phone）]）で、[Wi-Fi] パラメータに [有効（Enable）] を選択し、[共通設定の上書き（Override Common Settings）] をオンにします。
- デバイスのグループに関してワイヤレス LAN を有効にするには、[共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウ（[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）]）で、[Wi-Fi] パラメータに [有効（Enable）] を選択し、[共通設定の上書き（Override Common Settings）] をオンにしてから、デバイス（[デバイス（Device）] > [電話（Phone）]）にその共通の電話プロファイルを関連付けます。
- ネットワークのすべての WLAN 対応デバイスに関してワイヤレス LAN を有効にするには、[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ（[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]）で、[Wi-Fi] パラメータに対して [有効（Enable）] を選択し、[共通設定の上書き（Override Common Settings）] をオンにします。

（注） MAC アドレスを設定するときには、[電話の設定（Phone Configuration）] ウィンドウ（Cisco Unified Communications Manager 管理の [デバイス（Device）] > [電話（Phone）]）で、イーサネット MAC アドレスを使用します。 Cisco Unified Communications Manager の登録にはワイヤレス MAC アドレスは使用しません。

# ワイヤレス LAN プロファイルのプロビジョニング

**手順**

**ステップ 1** [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [電話（Phone）] > [ワイヤレスLANプロファイル（Wireless LAN Profile）] を選択します。

**ステップ 2** ワイヤレス LAN プロファイルを設定し、[保存（Save）] をクリックします。

# ワイヤレス LAN プロファイル グループのプロビジョニング

**手順**

**ステップ 1** [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [電話（Phone）] > [ワイヤレスLANプロファイル グループ（Wireless LAN Profile Group）] を選択します。

**ステップ 2** ワイヤレス LAN プロファイル グループを設定し、[保存（Save）] をクリックします。

**ステップ 3** [システム（System）] > [デバイス プール（Device Pool）] を選択し、ワイヤレス LAN プロファイル グループをデバイス プールに追加し、[保存（Save）] をクリックします。 または、[デバイス（Device）] > [電話（Phone）] を選択し、ワイヤレス LAN プロファイル グループを特定のデバイスに追加して、[保存（Save）] をクリックします。

# ネットワークの設定

ネットワークでDHCPを使用していない場合、デバイスをネットワークにインストールした後に、デバイスで次のネットワーク設定を指定する必要があります。

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

必要に応じて、ドメイン名と DNS サーバ設定値も設定できます。

## IPv4 の設定

**手順**

**ステップ 1** 設定アプリケーションで、[イーサネット（Ethernet）] > [IPv4 設定（IPv4 configuration）] をタップします。

**ステップ 2** [静的 IP を使用する（Use static IP）] をオンにします。

**ステップ 3** 次のオプションを設定できます。

- IP アドレス
- ゲートウェイ

- ネットマスク
- ドメイン名

（注） デバイスに複数のドメイン名を送信するには、オプション 15 を使用できます。 各ドメイン名はスペースで区切る必要があります。 カンマなど、他の区切り文字はサポートされません。 静的 IP アドレスを使用している場合は、ドメイン名を手動で入力することもできます。 この場合も、有効な区切り文字はスペースだけです。 現在、オプション 119 はサポートされていません。

- DNS 1
- DNS 2

## IPv4 の更新

**手順**

設定アプリケーションで、[イーサネット（Ethernet）] > [IPv4 の更新（Renew IPv4）] をタップします。

# IPv6 を設定する

**手順**

**ステップ 1** 設定アプリケーションで、[イーサネット（Ethernet）] > [IPv6設定（IPv6 configuration）]をタップします。

**ステップ 2** [静的 IP を使用する（Use static IP）] をオンにします。

**ステップ 3** 次のオプションを設定できます。

- IP アドレス
- デフォルト ルータ
- プレフィックス長
- ドメイン名

（注） デバイスに複数のドメイン名を送信するには、オプション 15 を使用できます。 各ドメイン名はスペースで区切る必要があります。 カンマなど、他の区切り文字はサポートされません。 静的 IP アドレスを使用している場合は、ドメイン名を手動で入力することもできます。 この場合も、有効な区切り文字はスペースだけです。 現在、オプション 119 はサポートされていません。

- DNS 1

• DNS 2

### IPv6 の更新

**手順**

設定アプリケーションで、[イーサネット（Ethernet）] > [IPv6の更新（Renew IPv6）] をタップします。

## イーサネット Web プロキシの設定

**手順**

**ステップ 1** 設定アプリケーションで、[イーサネット（Ethernet）] > [プロキシ設定（Proxy settings）] の順にタップします。

**ステップ 2** プロキシ設定のタイプを選択します。

a) 手動プロキシを設定するには、プロキシ ホスト名、プロキシ ポート、およびプロキシ バイパス（使用している場合）を入力します。 該当する場合は[プロキシでは認証が必要です（Proxy requires authentication）] をオンにします。

b) 自動プロキシを設定するには、PAC の場所と、プロキシ バイパス（使用している場合）を入力します。 該当する場合は[プロキシでは認証が必要です（Proxy requires authentication）] をオンにします。

## 管理 VLAN の設定

**手順**

**ステップ 1** 設定アプリケーションで、[イーサネット（Ethernet）]> [管理VLAN（Admin VLAN）] をタップします。

**ステップ 2** 管理 VLAN ID 値を入力し、[OK] をタップします。

# SW ポートの速度の設定

手順

**ステップ 1** 設定アプリケーションで、[イーサネット（Ethernet）] > [SWポートの速度（SW port speed）] をタップします。

**ステップ 2** ポートの速度を選択します。
デバイスがスイッチに接続されている場合は、スイッチ上のポートをデバイスと同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。 このオプションの設定値を変更する場合は、[PC ポートの速度（PC port speed）] を同じ設定値に変更する必要があります。

# PC ポートの速度の設定

手順

**ステップ 1** 設定アプリケーションで、[イーサネット（Ethernet）]> [PCポートの速度（PC port speed）] をタップします。

**ステップ 2** ポートの速度を選択します。
デバイスがスイッチに接続されている場合は、スイッチ上のポートをデバイスと同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。 このオプションの設定値を変更する場合は、[SW ポートの速度（SW port speed）] を同じ設定値に変更する必要があります。

# Wi-Fi ネットワークへの接続

手順

**ステップ 1** 設定アプリケーションで、[Wi-Fi] をオンに切り替えます。

**ステップ 2** [Wi-Fi] をタップします。

**ステップ 3** 使用可能なネットワークのリストからワイヤレス ネットワークを選択します。

**ステップ 4** クレデンシャルを入力し、[接続（Connect）] をタップします。

# 非表示の Wi-Fi ネットワークへの接続

### 手順

**ステップ 1** 設定アプリケーションで、[Wi-Fi] をオンに切り替えます。

**ステップ 2** [Wi-Fi] をタップします。

**ステップ 3** [+] をタップします。

**ステップ 4** ネットワーク SSID を入力して、セキュリティの種類とクレデンシャルを選択します（該当する場合）。

**ステップ 5** [保存（Save）] をタップします。

# Wi-Fi Web プロキシの設定

### 手順

**ステップ 1** 設定アプリケーションで [Wi-Fi] をタップします。

**ステップ 2** 使用可能なネットワークのリストで、ワイヤレス ネットワークをタップしたままにします。

**ステップ 3** [ネットワークを変更（Modify network）] をタップします。

**ステップ 4** [詳細オプションを表示（Show advanced options）] をオンにします。

**ステップ 5** プロキシ設定のタイプを選択します。

a) 手動プロキシを設定するには、プロキシ ホスト名、プロキシ ポート、およびプロキシ バイパス（使用している場合）を入力します。 該当する場合は [プロキシでは認証が必要です（Proxy requires authentication）] をオンにします。

b) 自動プロキシを設定するには、PAC の場所と、プロキシ バイパス（使用している場合）を入力します。 該当する場合は [プロキシでは認証が必要です（Proxy requires authentication）] をオンにします。

**ステップ 6** [保存（Save）] をタップします。

# Wi-Fi IP の設定

**手順**

**ステップ 1** 設定アプリケーションで [Wi-Fi] をタップします。
**ステップ 2** 使用可能なネットワークのリストで、ワイヤレス ネットワークをタップしたままにします。
**ステップ 3** [ネットワークを変更（Modify network）] をタップします。
**ステップ 4** [詳細オプションを表示（Show advanced options）] をオンにします。
**ステップ 5** IP 設定のタイプを選択し、以下の項目を設定します。

- IP アドレス
- ゲートウェイ
- ネットワーク プレフィックス長
- DNS 1
- DNS 2
- ドメイン名

**ステップ 6** [保存（Save）] をタップします。

# Wi-Fi の周波数帯の設定

**手順**

**ステップ 1** 設定アプリケーションで [Wi-Fi] をタップします。
**ステップ 2** [...] をタップします。
**ステップ 3** [Wi-Fiの周波数帯（Wi-Fi frequency band）] をタップし、設定を選択します。

# Mobile and Remote Access Through Expressway（マーケティング ベータ版）

Mobile and Remote Access through Expressway を使用するには、Cisco Expressway 8.5.2 以降および Cisco Unified Communications Manager 10.5.2 SU2 または Cisco Unified Communications Manager 11.0 以降が必要です。

Cisco Expressway を使用すると、Cisco DX シリーズ デバイスをリモートから社内ネットワークに簡単かつ安全に接続できます。バーチャル プライベート ネットワーク（VPN）のクライアント トンネルを使用する必要はありません。 Expressway は、Transport Layer Security（TLS）を使用してネットワーク トラフィックを保護します。 DX シリーズのデバイスで Expressway 証明書を認証して TLS セッションを確立するには、DX シリーズ ファームウェアが信頼するパブリック認証局による Expressway 証明書への署名が必要です。 Expressway 証明書の認証に対して、DX シリーズ デバイスで他の CA 証明書をインストールしたり信頼したりすることはできません。 サポートされる CA 証明書の一覧については、認証局信頼リスト，（215 ページ） を参照してください。

（注） Mobile and Remote Access Through Expressway のマーケティング ベータ版は、お客様による機能テストおよび評価目的でのみ使用できます。実稼働で使用することは推奨されません。 将来のファームウェア ロードで機能が正式にリリースされるまでは、公式のシスコ TAC サポートがありません。 ご意見やご要望については、cefeedback@cisco.com まで電子メールでお送りください。

ユーザが問題レポート ツールを使用できるようにするには、Expressway HTTP サーバの許可リストに問題レポート ツールのサーバ アドレスを追加する必要があります。

Expressway にログインするときに、ユーザはサービス名、ユーザ ID、パスワードの入力を求められます。 最初の起動時、オフプレミス ユーザは、Setup Assistant を使って Expressway にログインすることを求められます。 すでにオンプレミスまたはオフプレミスに展開済みのデバイスの場合は、それらのデバイスを Expressway 用に変換する必要があります。

Cisco Unified Communications Manager で、[プロダクト固有のオプション（Product Specific Options）] に [Expressway サインインに対するユーザ クレデンシャルの永続性（User Credentials Persistent for Expressway Sign In）] パラメータを設定すると、ユーザのログイン クレデンシャルがデバイスに保存されるので、クレデンシャル情報を再入力する必要がなくなります。 デバイスに保存されたユーザ クレデンシャルは暗号化されます。

詳細については、『*Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide*』を参照してください。

### Mobile and Remote Access に関する制限事項

- Expressway を介して接続された DX シリーズのデバイスは、Web ブラウジングを実行したり、企業ネットワーク内でホストされた電子メール サービスにアクセスしたりすることはできません。
- オフフック/KPML ダイヤリング、モビリティ、DND、コール バック、および会議参加者のドロップ機能は、Expressway 8.5.2 以降でのみサポートされます。
- ビジー回線フィールド機能には、Cisco Unified Communications Manager 11.0 以降が必要です。
- Expressway を介して接続されたデバイスは、企業ネットワーク内の APK サーバから APK をダウンロードすることはできません。 ただし、アクセス可能なパブリック ネットワーク上の APK サーバから APK をダウンロードできます。
- 社内ネットワークからデバイスに SSH でアクセスすることはできません。

- 社内ネットワークからデバイスの Web ページにアクセスすることはできません。
- Expressway を介したセルフプロビジョニングはサポートされません。

### 関連トピック

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

## Expressway に対するユーザ クレデンシャルの永続性の有効化

### 手順

**ステップ 1** [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [プロダクト固有の設定（Product Specific Configuration）] を選択します。

**ステップ 2** [Expressway サインインに対するユーザ クレデンシャルの永続性（User Credentials Persistent for Expressway Sign In）] をオンにします。

## Mobile and Remote Access through Expressway へのデバイスの変換

### はじめる前に

デバイスにファームウェア 10.2(4) 以降が搭載されている必要があります。

### 手順

**ステップ 1** 設定アプリケーションで、[詳細...（More....）] をタップします。

**ステップ 2** [ネットワーク設定をリセット（Reset network settings）] をタップします。

**ステップ 3** [ローカルテレフォニーの自動検出の有効化（Enable automatic local telephony discovery）] をオフにして、[リセット（Reset）] をタップします。
ネットワーク接続がリセットされます。 デバイスが有線ネットワークに接続されている場合、デバイスは自動的に再接続します。デバイスがワイヤレス展開されている場合は、Wi-Fi ネットワークに接続する必要があります。 デバイスがネットワークに接続すると、[TFTP サーバの入力（Enter TFTP server）] 画面が表示されます。

**ステップ 4** [Expressway] をタップします。

**ステップ 5** [サービス ドメイン（Service domain）] フィールド、[ユーザ名（Username）] フィールド、および [パスワード（Password）] フィールドに入力します。

**ステップ 6** [サインイン（Sign In）] をタップします。

## Expressway デバイスの VPN への変換

手順

**ステップ 1** 設定アプリケーションで、[詳細...（More....）] をタップします。
**ステップ 2** [ネットワーク設定をリセット（Reset network settings）] をタップします。
**ステップ 3** ネットワークに接続します。
**ステップ 4** TFTP サーバの設定を入力します。
**ステップ 5** VPN プロファイルを追加し、それに接続します。

## オフプレミス デバイスのオンプレミスへの変換

手順

企業ネットワークにデバイスを接続します。
企業ネットワークが検出され、電話機が Cisco Unified Communications Manager に正常に登録されます。

## Expressway HTTP 許可リストへの問題レポート ツール サーバの追加

手順

**ステップ 1** Expressway で、[設定（Configuration）] > [Unified Communications] > [設定（Configuration）] に移動します。
**ステップ 2** [HTTP サーバ許可リスト（HTTP server allow list）]をクリックします。
**ステップ 3** 問題レポート ツールの HTTP サーバのホスト名または IP アドレスを設定します。

## 認証要求許可レートの設定

デバイスに対する Mobile & Remote Access 認証のレートはデフォルトで制御されます。 デフォルトの設定では 300 秒ごとに 3 つが認証されます。 Expressway サーバで HTTP 429 “Too Many Requests” エラーが発生する場合は、その認証レートを上げることができます。

### 手順

**ステップ 1** Expressway で、[設定（Configuration）] > [Unified Communications] > [設定（Configuration）] > [詳細設定（Advanced）] に移動します。

**ステップ 2** [認証レートの制御（Authorization Rate Control）] を設定します

# 代替 TFTP サーバの有効化

### 手順

**ステップ 1** 設定アプリケーションで、[詳細（More）] をタップします。

**ステップ 2** [TFTPサーバーの設定（TFTP Server Settings）] をタップします。

**ステップ 3** [代替TFTPサーバーの使用（Use Alternate TFTP Server）] をオンにします。

## TFTP サーバ 1 の設定

### 手順

**ステップ 1** 設定アプリケーションで、[詳細（More）] をタップします。

**ステップ 2** [TFTPサーバーの設定（TFTP Server Settings）] をタップします。

**ステップ 3** [代替TFTPサーバーの使用（Use Alternate TFTP Server）] をオンにします。

**ステップ 4** [TFTPサーバー 1（TFTP server 1）] をタップします。

**ステップ 5** TFTP サーバ アドレスを入力し、[OK] をタップします。

### TFTP サーバ 2 の設定

**手順**

**ステップ 1** 設定アプリケーションで、[詳細（More）] をタップします。
**ステップ 2** [TFTPサーバーの設定（TFTP Server Settings）] をタップします。
**ステップ 3** [代替TFTPサーバーの使用（Use Alternate TFTP Server）] をオンにします。
**ステップ 4** [TFTPサーバー 2（TFTP server 2）] をタップします。
**ステップ 5** TFTP サーバ アドレスを入力し、[OK] をタップします。

## AnyConnect VPN

AnyConnect は、ASA バージョン 8.0 以降（AnyConnect モバイル ライセンスを含む）または Adaptive Security Device Manager（ASDM）6.0 以降を実行している Cisco 5500 シリーズ ASA へのセキュアな VPN 接続をリモート ユーザに提供する VPN クライアントです。

ASA の詳細については次のサイトを参照してください： http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

### VPN 接続プロファイルの追加

**手順**

**ステップ 1** 設定アプリケーションで、[詳細（More）] をタップします。
**ステップ 2** [VPN] をタップします。
**ステップ 3** [VPNプロファイルの追加（Add VPN profile）] をタップします。
**ステップ 4** 説明とサーバ アドレスを入力します。
**ステップ 5** [保存（Save）] をタップします。

### VPN への接続

手順

**ステップ 1** 設定アプリケーションで、[詳細（More）] をタップします。

**ステップ 2** [VPN] をタップします。

**ステップ 3** VPN 接続をタップしたままにします。

**ステップ 4** 必要に応じて、適切なプロンプトへの応答として次のいずれかを行います。

- クレデンシャルを入力します。 入力を求められたら、二重認証をサポートするセカンダリ クレデンシャルも入力します。
- [証明書を取得（Get Certificate）] をタップし、次にシステム管理者により提供される証明書登録のクレデンシャルを入力します。 AnyConnect は、証明書を保存し、VPN セキュア ゲートウェイに再接続して、認証にその証明書を使用します。

**ステップ 5** [接続（Connect）] をタップします。

## VPN 経由のビデオ コール エクスペリエンスの最適化

VPN 経由のビデオ コール エクスペリエンスを最適化するために、ビデオ帯域幅の設定を調整します。 1.5 Mbps の帯域幅には 720p のビデオ解像度が必要です。 低帯域幅の設定は、低解像度につながります。

（注） スループットは、ネットワークまたは時刻で共有される他のトラフィックなどの要因によって、時間の経過とともに変化します。 このような変動はビデオ エクスペリエンスに影響する可能性があります。

手順

**ステップ 1** VPN から切断します。

**ステップ 2** デバイスの速度テストを実行し、テスト結果のアップロード速度を書き留めます。

Speed A.I. によるインターネット速度テストなどの速度テスト アプリケーションは、Google Play で入手できます。

**ステップ 3** VPN に再接続します。

**ステップ 4** 通話アプリケーションで、 をタップします。

**ステップ 5** [設定（Settings）]をタップします。

**ステップ 6** [ビデオ帯域幅（Video bandwidth）]をタップします。

**ステップ 7** 速度テスト結果のアップロード速度よりも低いビデオ帯域幅を選択します。

## Cisco Unified Communications Manager での VPN の設定

[VPN 設定（VPN Settings）] メニューでは、Secure Sockets Layer（SSL）を使用して VPN クライアント接続を有効にできます。 デバイスが信頼ネットワークの外側にある場合、あるいはデバイスと Cisco Unified Communications Manager の間のネットワーク トラフィックが非信頼ネットワークを通過しなければならない場合に、VPN 接続を使用します。

次の手順に従って VPN プロファイルを設定します。 詳細については『*Cisco Unified Communications Manager Security Guide*』および『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

### 手順

**ステップ 1** VPN ゲートウェイごとに VPN コンセントレータをセットアップします。

**ステップ 2** VPN 証明書を新しい Phone-VPN-Trust にアップロードします。

**ステップ 3** VPN ゲートウェイを設定します。

a) [拡張機能（Advanced Features）] > [VPN] > [VPN ゲートウェイ（VPN Gateway）] を選択します。

b) ゲートウェイの名前、説明、および URL を入力します。

（注） VPN ゲートウェイには最大 10 個の証明書を割り当てることができます。 各ゲートウェイには、少なくとも 1 つの証明書を割り当てます。 VPN 権限に関係付けられた証明書だけが、使用可能な VPN 証明書のリストに表示されます。

VPN ゲートウェイ URL は、ゲートウェイ内のメイン コンセントレータのためのものです。

**ステップ 4** VPN グループを設定します。 [拡張機能（Advanced Features）] > [VPN] > [VPN グループ（VPN Group）] を選択します。

（注） 1 つの VPN グループに最大 3 つの VPN ゲートウェイを追加できます。 VPN グループ内の証明書の合計数は 10 以下にする必要があります。

**ステップ 5** VPN プロファイルを設定します。 [拡張機能（Advanced Features）] > [VPN] > [VPN プロファイル（VPN Profile）] を選択します。

（注） [ネットワーク接続の自動検出の有効化（Enable Auto-Detect Network Connection）] が有効になっていると、VPN クライアントは、企業ネットワークの外にいることを検出した場合に限り動作します。

[ホスト ID チェック（Host ID Check）] が有効になっている場合、VPN ゲートウェイ証明書の一般名は、VPN クライアントの接続先の URL と一致する必要があります。

[永続的パスワードを有効化（Enable Password Persistence）] が有効な場合、ユーザ パスワードがキャッシュされます。[デバイス上に VPN パスワードを保存（Store VPN Password on Device）] も有効な場合、ログインが失敗するまでユーザ パスワードはデバイスに保存されます。

**ステップ 6** VPN 機能を設定します。 [拡張機能（Advanced Features）] > [VPN] > [VPN 機能設定（VPN Feature Configuration）] を選択します。

**ステップ 7** 共通の電話プロファイルを割り当てます。 [デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）] の順に選択します。

## [VPN の設定（VPN Configuration）] の設定

次の表に、Cisco Unified Communications Manager 上でのデバイスの VPN 設定オプションについて説明します。

**表 *14*：*VPN* 設定オプション**

| オプション | 説明 | 変更の手順 |
|---|---|---|
| 管理者がプロビジョニングした VPN ゲートウェイ（Administrator Provisioned VPN Gateway） | VPN グループ設定で有効にされる VPN。 | 表示専用。変更できません。 |

| オプション | 説明 | 変更の手順 |
| --- | --- | --- |
| ユーザ定義 VPN プロファイル（User Defined VPN Profiles） | オプションが有効になっているか無効になっているかを示します。 | [デバイス（Device）]>[デバイスの設定（Device Settings）] > [プロダクト固有の設定（Product Specific Configuration）] の順に選択します。<br>[ユーザ定義プロファイルを許可（Allow User Defined Profiles）] をオンまたはオフに設定します。<br>（注） 複数レベルの設定に使用できます。 管理者は、デバイス レベル、共通レベル、またはエンタープライズ レベルで変更できます。<br>この機能が Cisco Unified Communications Manager 上で無効にされると、ユーザ定義の VPN プロファイルがデバイス上のリストから削除され、[VPN 接続の新規追加（Add New VPN Connection）] が無効になります。 |
| 常に VPN が必要（Always Require VPN） | オプションが有効になっているか無効になっているかを示します。 | [デバイス（Device）]>[デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）] の順に選択します。<br>該当するプロファイルを選択します。<br>[常に VPN が必要（Always Require VPN）] をオンまたはオフに設定します。<br>（注） [常に VPN が必要（Always Require VPN）] の設定値は、enable と autoNetworkDetect の値を True に上書きします。 |

| オプション | 説明 | 変更の手順 |
| --- | --- | --- |
| デバイス上にVPNパスワードを保存（Store VPN Password on Device） | オプションが有効になっているか無効になっているかを示します。 | [デバイス（Device）]>[デバイスの設定（Device Settings）]>[共通の電話プロファイル（Common Phone Profile）]を選択するか、[デバイス（Device）]>[電話（Phone）]>[電話の設定（Phone Configuration）]を選択します。<br>[デバイス上にVPNパスワードを保存（Store VPN Password on Device）]をオンまたはオフに設定します。<br>（注） VPNパスワードをデバイスに保管できるのは、設定済みのVPNプロファイルでパスワード永続性が有効にされ、しかもクライアント認証方式が「ユーザーおよびパスワード」または「パスワードのみ」である場合だけです。 |

（注） ネットワーク設定を変更すると、アクティブな VPN 接続に影響を与える可能性があります。

VPN が有効になっている場合、VPN 用にプロキシが設定されたり、使用されたりすることはありません。

## VPN 認証

Cisco DX シリーズ デバイスは、次の VPN 認証方式をサポートしています。

- ユーザ名およびパスワード
- 証明書のみ
- パスワードのみ

（注） パスワードのみの認証の場合、デバイスIDがユーザ名として事前に入力されます。Cisco適応型セキュリティ アプライアンス（ASA）がユーザ名を設定します。

Cisco Unified Communications Manager 上で指定された認証は、ASA 上で設定される認証に一致している必要があります。 認証が ASA 上の認証と一致しなくてもユーザ VPN は許可されますが、パスワード持続性と自動接続の機能は適用外になります。

# 起動プロセス

ネットワークへの接続時に、Cisco DX シリーズ デバイスでは標準的な起動プロセスが実行されます。 ネットワークの設定によっては、これらの手順の一部だけがデバイスで実行される場合もあります。

1. スイッチからの電力の取得。 デバイスが外部電源を使用していない場合、デバイスに接続されているイーサネット ケーブル経由でスイッチからのインライン パワーが供給されます。 [起動しています...（Starting up...）] 画面が約 30 秒間表示されます。

   デバイスはイーサネット接続の検出を試みます。 イーサネット接続が検出されても、割り当てられた IP アドレスがない場合、ユーザは管理者に連絡するよう求められます。 イーサネット接続が見つからない場合、デバイスはワイヤレス ネットワーク接続を確立しようと試みます。

2. （ワイヤレス LAN 上のみ）アクセス ポイントをスキャンします。 デバイスは RF カバレッジ エリアをスキャンします。 デバイスはネットワーク プロファイルを検索し、Service Set Identifier（SSID）と認証タイプが一致するアクセス ポイントを見つけるためにスキャンします。 デバイスは、ネットワーク プロファイル設定に一致するアクセス ポイントとの関連付けを確立します。

3. （ワイヤレス LAN 上のみ）アクセス ポイントで認証を行います。 デバイスが認証プロセスを開始します。

4. 保存されているデバイス イメージをロードします。 デバイスには、ファームウェア イメージとユーザ定義プリファレンスの保存場所となる不揮発性のフラッシュ メモリがあります。 起動時に、デバイスはブートストラップ ローダーを実行して、フラッシュ メモリに保存されているデバイス ファームウェアをロードします。 このイメージを使用して、デバイスはソフトウェアとハードウェアを初期化します。

5. VLAN の設定。 デバイスが Cisco Catalyst スイッチに接続されると、そのスイッチは、スイッチ上に定義されているボイス VLAN をデバイスに通知します。 デバイスが Dynamic Host Configuration Protocol（DHCP）要求を使って IP アドレスを取得するには、その前に VLAN メンバーシップを把握している必要があります。

6. IPアドレスの取得。 デバイスがDHCPを使ってIPアドレスを取得する場合、デバイスはDHCPサーバに問い合わせて取得します。 ネットワークで DHCP を使用しない場合は、個々のデバイスに対してスタティック IP アドレスをローカルに割り当てる必要があります。

7 TFTP サーバへのアクセス。 DHCP サーバは、IP アドレスを割り当てることに加えて、デバイスに TFTP サーバを指定します。 デバイスの IP アドレスを静的に定義した場合は、個別のデバイスで TFTP サーバを設定する必要があります。その後、デバイスは TFTP サーバに直接アクセスします。

TFTP サーバが見つからない場合、ユーザは Expressway にサインインすることを求められます。

（注） また、DHCP で割り当てられるサーバの代わりに、別の TFTP サーバを割り当てることもできます。

8 （Expressway に接続しているデバイスでは、このステップをスキップします）。

CTL ファイルの要求TFTP サーバに、CTL ファイルが保管されています。 このファイルには、デバイスと Cisco Unified Communications Manager の間にセキュアな接続を確立するために必要な証明書が含まれています。

9 （Expressway に接続しているデバイスでは、このステップをスキップします）。

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

10 設定ファイルの要求。 TFTP サーバは設定ファイルを保持しており、これには Cisco Unified Communications Manager に接続するためのパラメータや、デバイスに関する他の情報が定義されています。

11 Cisco Unified Communications Manager にお問い合わせください。 設定ファイルは、デバイスが Cisco Unified Communications Manager と通信する方法を定義し、デバイスにロード ID を提供します。 デバイスがこのファイルを TFTP サーバから取得すると、リストで優先順位が最も高い Cisco Unified Communications Manager への接続を確立しようとします。

デバイスのセキュリティ プロファイルでセキュア シグナリング（暗号化または認証）が設定され、Cisco Unified Communications Manager がセキュア モードに設定されている場合には、デバイスが TLS 接続を実行します。 それ以外の場合は、デバイスが非セキュア TCP 接続を実行します。

デバイスがデータベースに手動で追加された場合、Cisco Unified Communications Manager はデバイスを識別します。 デバイスがデータベースに手動で追加されておらず、しかも Cisco Unified Communications Manager で自動登録が有効になっている場合、デバイスは Cisco Unified Communications Manager データベースで自動登録を試みます。

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

12 デバイスを初めて起動すると、[ようこそ（Welcome）] 画面が表示され、セットアップ アシスタントが実行されます。

# 起動時の TFTP サーバの手動設定

**手順**

**ステップ 1** 画面に [起動しています...（Starting up...）] が表示されたら、画面の左上隅を 3 回タップします。

**ステップ 2** 追加のピリオドが [起動しています...（Starting up...）] の終わりに追加され、キー シーケンスが検出されたことが示されます。

**ステップ 3** [TFTP（TFTP）] 設定画面が表示されます。 TFTP サーバ アドレスを入力し、[確認（Confirm）] をタップします。

# 起動時の検証

デバイスに電源を接続すると、デバイスは起動診断プロセスを開始し、次の手順が繰り返されます。

1. 起動中のさまざまな段階で、デバイスがハードウェアを検査している間（Cisco DX650ハードウェアの場合のみ、ハンドセットが点灯し、ミュート ボタンが赤色に点滅して、ヘッドセット ボタンおよびスピーカー ボタンが緑色に点滅し）、ロック/電源 ボタンが白色に点灯します。
2. 電話アイコンがステータス バーに表示されます。

これらの段階が正常に完了すると、デバイスは正常に起動し、ロック/電源ボタンが点灯したままになります。

第 6 章

# 連絡先（Contacts）


- 動作モードごとの連絡先とディレクトリ，71 ページ
- ローカル連絡先，72 ページ
- 社内ディレクトリ，72 ページ
- 検索，73 ページ
- アプリケーション ダイヤル ルール，74 ページ


## 動作モードごとの連絡先とディレクトリ

| 連絡先ソース | パブリック モード | 簡易モード | 拡張モード |
|---|---|---|---|
| デバイス上に作成 | はい | はい | はい |
| Bluetooth からインポート | はい | はい | はい |
| Cisco User Data Services（UDS） | はい | はい | はい |
| Jabber | いいえ | いいえ | はい |
| Exchange グローバル アドレス一覧 | いいえ | いいえ | はい |
| Google | いいえ | いいえ | はい |
| サードパーティ製アプリケーション | いいえ | いいえ | はい |

# ローカル連絡先

ローカル連絡先は、DXデバイスでユーザによって作成される連絡先です。 ローカル連絡先には、Bluetooth を介して携帯電話からインポートした連絡先も含めることができます。

拡張モードでは、Jabber、Exchange アカウント、Google アカウント、サードパーティ製アプリケーションから同期された連絡先をローカル連絡先に含めることができます。

電話番号を含むローカル連絡先は、Call アプリケーションの [連絡先（Contacts）] タブで使用できます。 People アプリケーションではすべてのローカル連絡先を使用できます。

# 社内ディレクトリ

社内ディレクトリによって、ユーザは同僚の連絡先を調べることができます。 この機能をサポートするには、社内ディレクトリを設定する必要があります。

Cisco Unified Communications Manager は Lightweight Directory Access Protocol （LDAP）ディレクトリを使用して、Cisco Unified Communications Manager のユーザに関する情報を保存し、アクティブ ディレクトリ（AD）と同期します。

Cisco DX シリーズ デバイスは Cisco User Data Services（UDS）を使用して、Cisco Unified Communications Manager に社内ディレクトリ情報を照会します。

LDAP の設定の詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

## 社内写真ディレクトリの設定

UDS を使用したユーザによる社内ディレクトリの検索時、およびローカル連絡先として追加するディレクトリ検索結果の使用時にディレクトリの写真を表示するには、このパラメータを設定します。

### 手順

**ステップ 1** Cisco Unified Communications Manager の管理で、次のいずれかのウィンドウを選択してください。

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

複数のウィンドウにパラメータを設定した場合、優先順位は次のとおりです。

1 [デバイス（Device）] > [電話（Phone）]

2 [デバイス（Device）]>[デバイスの設定（Device Settings）]>[共通の電話プロファイル（Common Phone Profile）]

3 [システム（System）] > [エンタープライズ電話（Enterprise Phone）]

**ステップ 2** [社内写真ディレクトリ（Company Photo Directory）] に http://<servername>/<path>/%%uid%%.<image file extension> を設定します。

**ステップ 3** [共通設定の上書き（Override Common Settings.）] をオンにします。

# 検索

Cisco DX シリーズユーザは、ローカルに保存された連絡先、コール履歴、および社内ディレクトリ（UDS）を検索できます。 拡張モードで DX シリーズデバイスを操作しているユーザは、Jabber 連絡先、および Exchange などの オンライン ディレクトリも検索できます。

社内ディレクトリは [ディレクトリ（Directory）] タブで検索できます。

次の項目に基づいて検索できます。

- 名（First name）
- 姓（Last name）
- 電話番号（Phone number）
- ユーザ名（Username）

検索結果には、写真（使用可能な場合）、名と姓、URI または電話番号が表示されます。 検索結果に URI と電話番号の両方が含まれている場合は、URI が表示されます。

# 検索結果の最適化

デフォルトでは、[発信（Calls）] タブでローカル連絡先を検索できますが、ディレクトリは検索できません。 [発信（Calls）] タブで検索を行う際に社内ディレクトリの結果を表示するには、以下の手順を実行します。 ディレクトリの結果は、検索結果のローカル連絡先の下に表示され、ディレクトリ タイプ別に並べ替えられます。

**手順**

**ステップ 1** をタップします。

**ステップ 2** [設定（Settings）]をタップします。

**ステップ 3** [ディレクトリ結果（Directory results）]をオンにします。

# アプリケーション ダイヤル ルール

アプリケーションダイヤルルールは、携帯電話の連絡先共有番号をネットワークでダイヤル可能な番号へ変換するために使用されます。アプリケーションダイヤルルールは、グローバル検索、連絡先、お気に入り、クイックコンタクトバッジ、およびすべてのクリックツーダイヤル機能の数字に適用されます。 アプリケーション ダイヤル ルールは、ユーザが番号をダイヤルしている時、もしくはユーザによって開始される前に番号が [編集（Edit）] フィールドに移動された場合は、適用されません。

アプリケーション ダイヤル ルールがCisco Unified Communications Managerに設定されます。 詳細については、『*Cisco Unified Communications Manager System Guide*』の「Dial Rules Overview」の章を参照してください。

# アプリケーション ダイヤル ルールの設定

## 手順

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

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

**ステップ 3** 次のフィールドを入力します。

- [名前（Name）]：ダイヤル ルールの一意の名前を入力します。名前には最長 20 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、アンダースコア（_）を任意に組み合わせて使用できます。
- [説明（Description）]：このフィールドには、ダイヤル ルールの簡単な説明を入力します。
- [開始番号（Number Begins With）]：このアプリケーション ダイヤル ルールを適用するディレクトリ番号の先頭部分の数字を入力します。
- [桁数（Number of Digits）]：この必須フィールドには、アプリケーション ダイヤル ルールを適用するディレクトリ番号の先頭部分の数字を入力します。
- [削除する合計桁数（Total Digits to be Removed）]：この必須フィールドには、ダイヤル ルールに適用する、Cisco Unified Communications Manager によってディレクトリ番号から削除する桁数を入力します。
- [プレフィックス パターン(Prefix With Pattern)]：この必須フィールドには、アプリケーション ダイヤル ルールに適用する、ディレクトリ番号に付加するパターンを入力します。
- [アプリケーション ダイヤル ルール優先順位(Application Dial Rule Priority)]：このフィールドは、[プレフィックス パターン(Prefix With Pattern)] に入力すると表示されます。 アプリケーション ダイヤル ルールの優先順位を設定することができます。

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

第 7 章

# セルフ ケア ポータルの管理


- セルフ ケア ポータルの概要，77 ページ
- セルフ ケア ポータルへのアクセスの設定，78 ページ
- セルフ ケア ポータルの表示のカスタマイズ，78 ページ


## セルフ ケア ポータルの概要

Cisco Unified Communications セルフ ケア ポータルから、電話の機能や設定をカスタマイズし、制御できます。 セルフ ケア ポータルについては、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html にある『*Cisco Unified CommunicationsSelf Care Portal User Guide*』を参照してください。

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

ユーザを Cisco Unified Communications セルフ ケア ポータルにアクセス可能にする前に、Cisco Unified Communications Manager Administration を使用して、ユーザを標準の Cisco Unified Communications Manager エンド ユーザ グループに追加する必要があります。

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

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

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

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

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

詳細については、以下を参照してください。

- 『*Cisco Unified Communications Manager Administration Guide*』の「Access“ ”Control Group Setup」の章
- 『*Cisco Unified Communications Manager Administration Guide*』の「End“ ”User Setup」の章
- 『*Cisco Unified Communications Manager Administrator Guide*』「のRole“ ”Setup」の章

# セルフ ケア ポータルへのアクセスの設定

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

**手順**

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

**ステップ 2** ユーザを検索し、ユーザ ID のリンクをクリックします。

**ステップ 3** ユーザのパスワードと PIN が設定されていることを確認します。

**ステップ 4** [保存（Save）] を選択します。

# セルフ ケア ポータルの表示のカスタマイズ

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

- 呼出音設定の表示（Show Ring Settings）
- 回線のラベル設定の表示（Show Line Label Settings）

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

### 手順

**ステップ 1** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]を 選択します。

**ステップ 2** [セルフ ケア ポータル（Self Care Portal）] 領域で、[セルフ ケア ポータルのデフォルト サーバ（Self Care Portal Default Server）] フィールドを設定します。

**ステップ 3** ポータルでユーザがアクセスできるパラメータをイネーブルまたはディセーブルにします。

**ステップ 4** [保存（Save）] を選択します。

第 8 章

# アクセサリ


- Bluetooth アクセサリ，81 ページ
- ケーブル ロック，84 ページ
- 外部カメラ，84 ページ
- 外部スピーカおよびマイクロフォン，85 ページ
- ヘッドセット，85 ページ
- ビデオ ディスプレイ，89 ページ
- Cisco DX650 Wall-Mount キット，90 ページ


## Bluetooth アクセサリ

ユーザは、ヘッドセット、キーボード、携帯電話などの Bluetooth アクセサリを DX シリーズのデバイスに組み合わせることができます。

同時に複数の Bluetooth デバイスを組み合わせることができます。ただし、同時に 1 つの Bluetooth オーディオ デバイスしか組み合わせることができない場合もあります。

Bluetooth を有効にすると、ワイヤレス ネットワーク接続がデグレードする可能性があります。 ワイヤレス ネットワークのパフォーマンスを向上させるには、使用していない Bluetooth を無効にするか、ワイヤレス ネットワーク接続に 5 GHz 帯域を使用します。

### Bluetooth デバイス プロファイル

[デバイス プロファイル設定（Device Profile Settings）] 画面には、相手側デバイスに使用できるプロファイルが表示されます。 プロファイルを無効にすると、プロファイルがオフになり、ユーザは使用することができません。

## ハンズフリー プロファイル

Cisco DX シリーズ デバイスでは、さまざまなハンズフリー プロファイル機能がサポートされています。ハンズフリー プロファイル機能により、アクセサリ（Bluetooth ワイヤレス ハンドセット、Bluetooth 対応携帯電話など）を使用して、デバイスを操作せずに特定のタスクを実行できます。 たとえば、デバイスの [リダイヤル（Redial）] をタップする代わりに、ヘッドセット製造元の説明に従って、Bluetooth ワイヤレス ヘッドセットから番号をリダイヤルできます。

次のハンズフリー機能は Bluetooth アクセサリに適用されます。

- Bluetooth HFP の接続/切断状態への対応。
- Audio Gateway（AG）での電話番号のダイヤル発信
- コールが接続または接続解除されるタイミングの指定。
- コールの受信時に、アプリケーションに通知（インバンド着信音）。
- インバンド着信音の有効化または無効化。
- 電話ステータスの報告（AG から発信者 ID、信号強度およびバッテリ レベルなど）。
- コールの応答または拒否。
- 発信者 ID でコール ウェイティング通知を受領。
- コールの保留、待機コールへの切り替え。
- AG およびコール アプリケーションでの保留と通話の切り替え。
- 音声の携帯電話への切り替え、ハンズフリー機器への再切り替え。
- 携帯電話のコール リストの取得。

各種ハンズフリーデバイスは、それぞれ機能のアクティブ化方法が異なります。デバイスのメーカーが、同じ機能を指すときに異なる用語を使用している可能性もあります。 詳細については、各メーカーのマニュアルを参照してください。

## 電話帳アクセス プロファイル

Bluetooth 電話帳アクセス プロファイル（PBAP）により、ユーザは、Cisco DX シリーズ とペアリングされた携帯電話の連絡先およびコール履歴を共有することができます。 携帯電話のペアリング時に、ユーザは手動もしくは自動操作による連絡先とコール履歴のダウンロードを選択することができ、自分のデバイスに連絡先を保存するよう選択することもできます。

### デバイス プロファイルの有効化

**手順**

**ステップ 1** [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] ページで、[デバイス（Device）] > [電話（Phone）] を選択し、変更するデバイスを見つけ、そのデバイスの [電話の設定（Phone Configuration）] ウィンドウに移動します。

**ステップ 2** [電話の設定（Phone Configuration）] ウィンドウで、Bluetooth の設定で [有効（Enable）] を選択します。

**ステップ 3** デバイス プロファイルを有効にします。

**ステップ 4** 変更を保存します。

## Bluetooth アクセサリのペアリング

**手順**

**ステップ 1** デバイスの設定アプリケーションで、[Bluetooth] をオンに切り替えます。

**ステップ 2** 使用可能なデバイスのリストから、ペアにするデバイスをタップします。

**ステップ 3** パスキーを確認し、[ペア設定する（Pair）] をタップします。

## Bluetooth の無効化

**手順**

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

**ステップ 2** [電話の検索/一覧表示（Find and List Phones）] ウィンドウで、変更するデバイスの検索条件を入力し、[検索（Find）] をクリックします。

**ステップ 3** [電話の設定（Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域で、[Bluetooth] ドロップダウン リスト ボックスから [無効（Disabled）] を選択します。

# ケーブル ロック

ラップトップ ケーブル ロックを使用して、デスクトップデバイスを固定できます。 ロックをデバイスの背面にある盗難防止用セキュリティ コネクタに接続し、ケーブルをデスクトップに固定できます。

セキュリティ スロットには最大20 mmの幅のケーブルを挿入できます。 互換性のあるラップトップ ケーブル ロックとして Kensington 製のラップトップ ケーブル ロックの他、デバイスの背面にあるセキュリティ スロットに適合するその他のメーカー製ラップトップ ケーブル ロックがあります。

# 外部カメラ

Cisco DX650は、外部カメラとして、アドオン Logitech C920-C Webcam または Logitech C930e をサポートします。

外部カメラをデバイスに接続すると、ポイントツーポイントのビデオ通話が可能になります。 外部カメラが機能するためには、ビデオ通話と USB デバイスを有効にする必要があります。

（注） Power over Ethernet で Cisco DX650 の電源がオンになる場合、外部カメラは 802.3at が必要になります。 Power over Ethernet で電話機の電源がオンにならない場合は、外部カメラに外部電源が必要です。

## 外部カメラの設定

デバイスに外部カメラを接続したら、ユーザが外部カメラの設定を制御できます。 内部カメラとは異なり、外部カメラの明るさ設定は調整できません。

# 外部カメラの設置後の確認作業

**手順**

**ステップ 1** [外部カメラが接続されました（External Camera Connected）] とメッセージが表示されるまで待ちます。

**ステップ 2** 通話アプリケーションで、 をタップします。。

**ステップ 3** [セルフビュー（Self View）]をタップします。

**ステップ 4** 視野に明るい光が入らない場所にデバイスおよび外部カメラを移動します。

**ステップ 5** ユーザが前方から照らされるようにデバイスおよび外部のカメラを移動します。

# 外部スピーカおよびマイクロフォン

外部スピーカおよびマイクロフォンは、プラグアンドプレイ式のアクセサリです。 デバイスの外部 PC タイプのマイクロフォンとパワード スピーカー（アンプ内蔵）を接続するには、回線入力/回線出力ジャックを使用できます。 外部マイクロフォンを接続すると内部マイクロフォンが無効になり、外部スピーカーを接続すると内部スピーカが無効になります。

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

# ヘッドセット

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

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

シスコでは、不要な無線周波数（RF）および可聴周波数（AF）が遮蔽された高品質のヘッドセットなどの外部デバイスの使用を推奨しています。 ヘッドセットの品質や、携帯電話および双方向ラジオなど他のデバイスとの間隔によっては、雑音やエコーが入ることもあります。 ハム音は、相手方だけに聞こえる場合もあれば、ユーザおよび相手方の両方に聞こえる場合もあります。 ハム音やブザーのような雑音は、電灯、電気モーター、大型のPCモニタなど、さまざまな外部ソースが原因となり得ます。

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

デバイスを実際に展開する場合、環境やハードウェアにより不整合が発生することがあるので、すべての環境に対して最適な唯一のヘッドセットを見出すことは不可能です。

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

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

# Bluetooth ワイヤレス ヘッドセット

デバイスは、共有キーによる認証と暗号化方式を利用して Bluetooth ヘッドセットと接続します。 デバイスは、一度に最大 5 個のヘッドセットと接続できます。 最後に接続されたヘッドセットがデフォルトとして使用されます。 通常、ペアリングはヘッドセットごとに 1 回実行されます。

デバイスのペアリング後には、デバイスとヘッドセットの両方が有効であり、相互の有効範囲内にある限り、その Bluetooth 接続は維持されます。 この接続は通常、一方のデバイスの電源が切断された後、再び電源が投入されると、自動的に接続を再確立します。 ただし、一部のヘッドセットでは、ユーザによる接続の再確立が必要です。

Bluetooth ヘッドセットのワイドバンドはサポートされません。 Bluetooth ヘッドセットを使用すると、音質が低下する可能性があります。

1 ～ 2 m（3 ～ 6 フィート）の範囲で最良の性能が得られます。 ヘッドセットは 5 個以上ペアリングできますが、最後に接続したヘッドセットだけがデフォルトとして使用されます。 ヘッドセットがデバイスから 10 m（30 フィート）を超えて離れていると、Bluetooth の接続は 15 ～ 20 秒間のタイムアウト後にドロップされます。 ペアリングされたヘッドセットがデバイスの範囲内に戻ってきたときに当該デバイスが別の Bluetooth ヘッドセットに接続していないと、範囲内にある Bluetooth ヘッドセットが自動的に再接続します。 省電力モードで動作する特定のデバイスでは、ユーザが操作ボタンをタップすると、再接続が開始され、ヘッドセットが復帰します。

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

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

Bluetooth ヘッドセットの詳細については、ヘッドセットに付属するユーザ ガイドを参照してください。

## Bluetooth ワイヤレス ヘッドセットの追加

### 手順

**ステップ 1** ヘッドセットを検出/ペアリング モードに設定します。

（注） ヘッドセットを検出/ペアリング モードに設定する手順はヘッドセットによって異なります。ペアリング手順については、ヘッドセットの製造元の説明を参照してください。

ヘッドセットとのペアリングおよび接続を正常に行うために、ヘッドセットは検出/ペアリング モードである必要があります。

**ステップ 2** デバイスの Bluetooth をオンにしていない場合は、オンに切り替えてください。
Bluetooth がオンであるかどうかを確認するには、ステータス バー上で Bluetooth アイコンを確認します。

**ステップ 3** [端末をスキャン（Scan for devices）] を選択します。
Bluetooth デバイスが特定されると、デバイス名前がウィンドウに表示されます。

デバイスは、ヘッドセットとのペアリングに PIN 0000 を自動的に使用します。ヘッドセットで別の PIN が使用されている場合は、ヘッドセット付属のユーザ ガイドに記載されている正しい PIN を入力します。

（注） ペアリングが失敗した場合、デバイスから正しい PIN の入力が求められます。

デバイスに正しい PIN が設定されると、デバイスはアクセサリへの接続を試みます。 接続できなかった場合、デバイスは失敗の原因をユーザに通知するエラーアラートを表示します。デバイスがアクセサリとの接続を試行するために 10 秒間のタイムアウトが発生します。 接続が成功しないままタイマーが時間切れになると、エラー アラートが表示されます。

アクセサリをペアリングした後では、Cisco DX シリーズ デバイスおよびヘッドセットの両方が有効であり、それぞれの範囲内にある限り、その Bluetooth 接続は維持されます。 この接続は通常、一方のデバイスの電源が切断された後、再び電源が投入されると、自動的に接続を再確立します。ただし、一部のヘッドセットでは、ユーザによる接続の再確立が必要です。

ヘッドセットがデバイスの範囲外にある場合、Bluetooth 接続は 15 ～ 20 秒のタイムアウト後にドロップされます。 ペア化されたヘッドセットがデバイスの範囲内に戻り、そのデバイスに別の Bluetooth ヘッドセットが接続していない場合、範囲内にあるその Bluetooth ヘッドセットが自動的に再接続されます。 ヘッドセットをウェイクアップし、再接続プロセスを開始するために、ユーザがヘッドセット操作ボタンをタップしなければならない場合があります。

ユーザが Bluetooth ヘッドセットを使用して通話している最中に、何らかの理由でそのヘッドセットが電源オフ、圏外、または接続解除になると、そのコールをスピーカー/ヘッドセット上で続行

するか、切断するかを尋ねるアラートが表示されます。 ユーザが 30 秒以内に何らかの操作を行わないと、通話が終了します。

### Bluetooth ヘッドセットの接続解除

**手順**

**ステップ 1** 設定アプリケーションで [Bluetooth] を選択します。
**ステップ 2** デバイス名の横にある [設定（Settings）] アイコンをタップします。
**ステップ 3** [ペアを解除（Unpair）] をタップします。

## USB ヘッドセット

有線およびワイヤレスの USB ヘッドセットがサポートされています。 USB ヘッドセット（またはワイヤレス ヘッドセットの場合はベース ステーション）を、任意の USB ポートに接続することができます。

### USB ヘッドセットの有効化

これらのパラメータは、[電話の設定（Phone Configuration）] ウィンドウ（[デバイス（Device）] > [電話（Phone）]）、[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ（[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]）、または [共通の電話プロファイル（Common Phone Profile）] ウィンドウ（[デバイス（Device）] > [デバイス設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]） で有効化または無効化できます。

**手順**

**ステップ 1** ウィンドウの [プロダクト固有の設定（Product Specific Configuration layout）] 領域で、適切な USB ポートを有効にします。
**ステップ 2** [USBクラスの有効化/無効化（Enable/Disable USB Classes）]パラメータの [オーディオクラス（Audio Class）] を選択し、[共通設定の上書き（Override Common Settings）] をオンにします。

### USB ヘッドセットの無効化

**手順**

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で有効にした USB ポート（または [オーディオクラス（Audio Class）] パラメータ）を無効にします。

## 有線ヘッドセット

Cisco DX70 およびCisco DX650 は、3.5 mm 単一プラグ ヘッドセットをサポートします。 ユーザはヘッドセットでコールを発信したり、コールに応答したりできます。

### 有線ヘッドセットへの接続

**手順**

ヘッドセットをヘッドセット ポートに接続します。

### 有線ヘッドセットの無効化

ヘッドセットを無効にするには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] を使用できます。 ヘッドセットを無効にすると、スピーカフォンも無効になります。

**手順**

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

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

# ビデオ ディスプレイ

Cisco DX650 では、HDMI ポートを介して外部ディスプレイ デバイスがサポートされます。 モニタをデバイスに接続するには、HDMI ケーブルの一端を HDMI ポートに差し込み、もう一方の一端を micro-HDMI に差し込みます。

# Cisco DX650 Wall-Mount キット

壁に Cisco DX650 を取り付けるには、Cisco DX650 壁面取り付けキットに付属している特殊なブラケットを使用します。 壁面取り付けキットは、デバイスとは別にご注文ください。

## はじめる前に

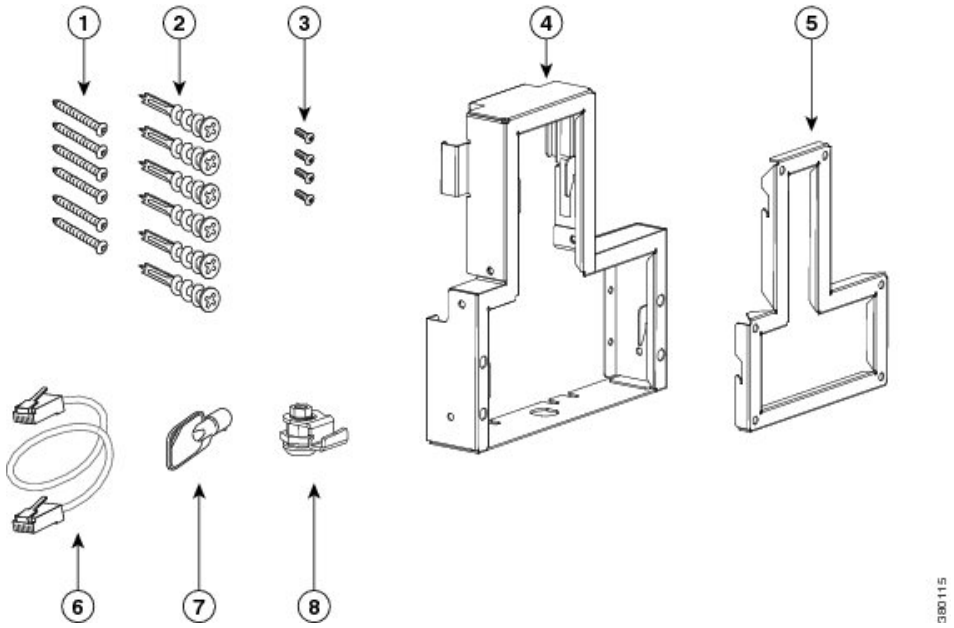
ブラケットの取り付けには、次の工具が必要です。

- No.1 と No.2 のプラス ドライバ
- 水準器

## 壁面取り付けキットのコンポーネント

（注） この壁面取り付けキットに含まれるハードウェアは乾式壁に取り付けるためのものです。 ブリックまたはコンクリートなど、他の場所に取り付けるには、独自のハードウェアを提供する必要があります。

**図 *1*：シングル電話アセンブリ用壁面取り付けキット**




| | | | |
|---|---|---|---|
| 1 | 8 ～ 18 X 1.25 インチのプラス ネジ X 6 本 | 5 | 壁面用ブラケット X 1 個 |

| | | | |
|---|---|---|---|
| 2 | アンカー 6 本 | 6 | 6 インチのイーサネット ケーブル X 1 本 |
| 3 | 3 X 6mm の小ネジ X 4 本 | 7 | ロック ダウン キー X1 個 |
| 4 | 電話機用ブラケット X 1 個 | 8 | ロック X 1 個 |

# 壁面への取り付け

**手順**

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

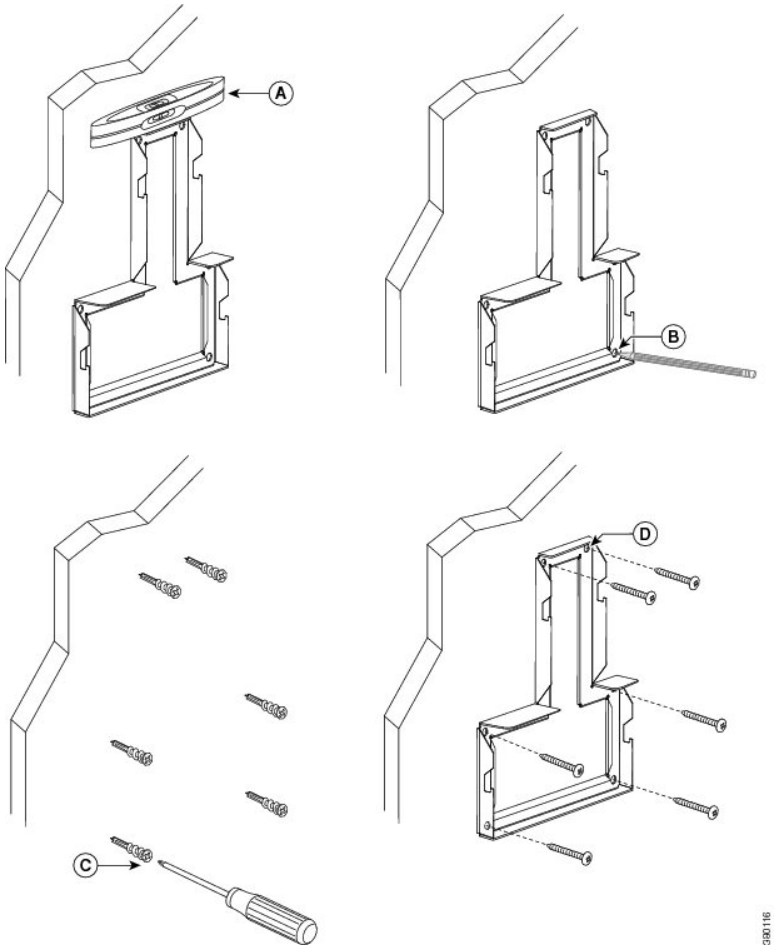
a) 水準器を使用してブラケットが水平であることを確認した後、鉛筆でネジ穴の位置に印を付けます。

b) 鉛筆で印を付けた個所に注意してアンカーの中心を合わせ、#2 のプラス ドライバーでアンカーを壁面に取り付けます。

c) アンカーを時計回りの方向に回し、壁面と平らになるまで押し込みます。

d) 付属のネジと #2 のプラス ドライバーを使用して、ブラケットを壁面に取り付けます。

**図 *2*：壁面用ブラケットの装着**




**ステップ 2** デバイスに電話機用ブラケットを装着します。

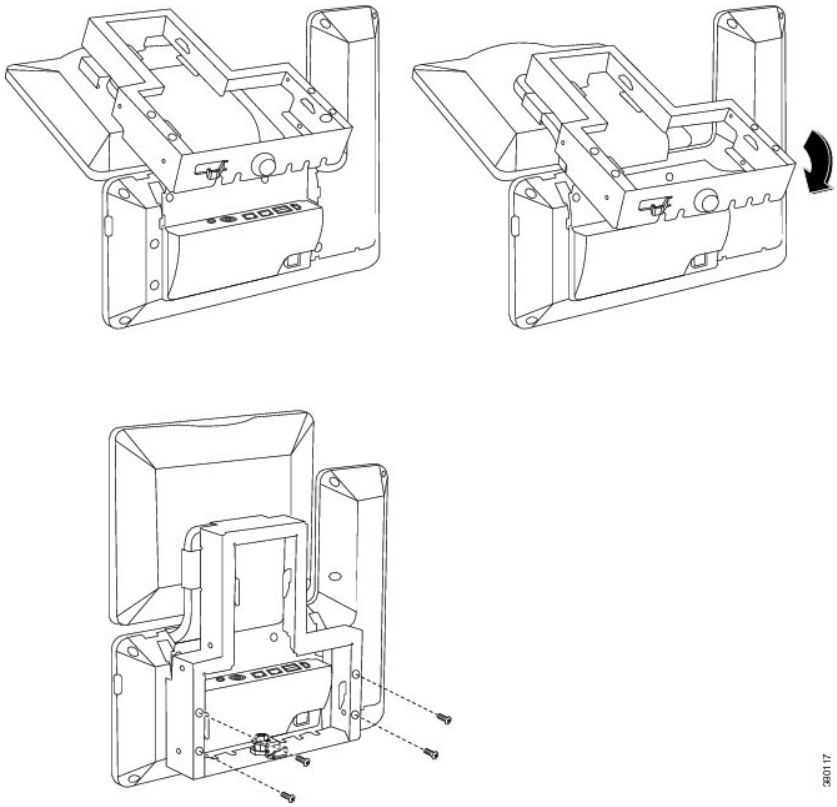
a) デバイスの底面から接続しているコードをすべて取り外します。

b) 電話機に電話機用ブラケットをスライドさせます。ブラケットの穴から、デバイスのポートにアクセスできることを確認してください

c) 小ネジを使用してデバイスに電話機用ブラケットを固定します。

d) コードを元通りに装着し、デバイス本体に付いているクリップで固定します。

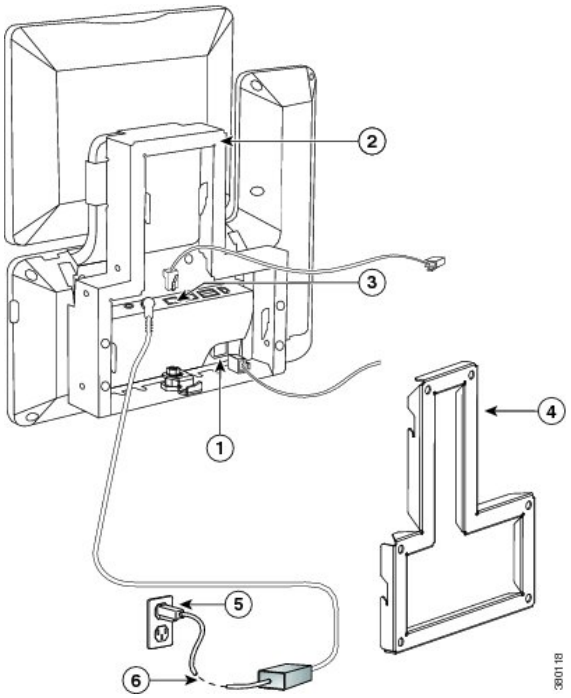
**図 *3*：電話機用ブラケットの装着**




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

外部電源を使用する場合、デバイスに電源コードを差し込みます。

**図 *4*：ケーブルの接続**

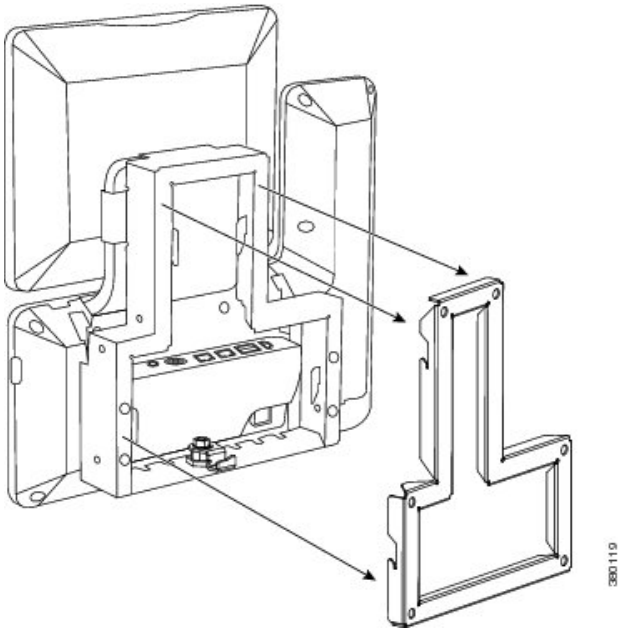



| | | | |
|---|---|---|---|
| [1] | 受話器ポート | 4 | 壁掛け用ブラケット |
| 2 | 電話機用ブラケット | 5 | AC アダプタ ポート |
| 3 | ネットワーク ポート | [6] | 電源ケーブル |

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

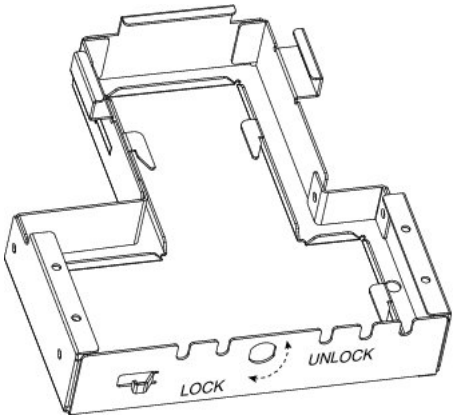
確認します。 電話機用ブラケットと壁面用ブラケットの開口部によって、複数の円形の開口部ができ、1 つの開口部に 1 本のケーブルを通すことができるようになっています。

**図 *5*** : 壁面用ブラケットへのデバイスの装着




**ステップ 5** 壁面用ブラケットにデバイスをロックするには、ロック ダウン キーを使用します。電話機用ブラケットの下部にあるキー フックにロック ダウン キーを保管できます。

**図 *6*** : キー フックのある電話機用ブラケット



第 9 章

# セキュリティ機能


- デバイスのセキュリティ，97 ページ
- 画面ロックおよび自動ロックの設定，110 ページ


## デバイスのセキュリティ

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

Cisco Unified Communications Manager Release 8.5(1) 以降にはデフォルトでセキュリティ機能が搭載されており、デバイスに次のセキュリティ機能が提供されます。CTL クライアントを実行する必要はありません。

- 設定ファイルの署名
- 設定ファイルの暗号化
- Tomcat および他の Web サービスでの HTTPS

（注） セキュアなシグナリングおよびメディア機能には、CTL ファイルが必要です。

認証局プロキシ関数（CAPF）に関連付けられた必要なタスクの実行後、ローカルで有効な証明書（LSC）がデバイスにインストールされます。 LSC は [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で設定できます。詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

また、デバイスの設定アプリケーションからLSCのインストールを開始することもできます。 この設定アプリケーションでは、LSC の更新と削除も実行できます。

# セキュリティ機能の概要

セキュリティを Cisco Unified Communications Manager システムに実装すると、デバイスや Cisco Unified Communications Manager サーバの個人情報の盗難、データの改ざん、およびコール シグナリングとメディア ストリームの改ざんを防ぐことができます。

これらの脅威を軽減するために、Cisco IP テレフォニー ネットワークはデバイスとサーバの間にセキュアな（暗号化された）通信ストリームを確立して維持します。さらにファイルをデジタル署名してからデバイスに転送し、デバイス間のメディア ストリームとコール シグナリングを暗号化します。

Cisco DX シリーズ デバイスでは、デバイスがセキュリティ保護の対象であるどうかを定義するデバイス セキュリティ プロファイルが使用されます。 デバイスにセキュリティ プロファイルを適用する方法については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Unified Communications Manager Administration でセキュリティ関連の設定値を設定すると、コンフィギュレーション ファイルに機密情報が保存されます。設定ファイルのプライバシーを確保するには、そのファイルを暗号化用に設定する必要があります。 詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Encrypted Phone Configuration Setup」の章を参照してください。

次の表に、デバイスでサポートされるセキュリティ機能の概要を示します。

**表 *15*：セキュリティ機能の概要**

| 機能 | 説明 |
|---|---|
| イメージ認証 | 署名付きバイナリ ファイル（拡張子 .sbn）と暗号化バイナリ ファイル（拡張子 .sebn）により、デバイスにロードされる前にファームウェア イメージが改ざんされないようにします。<br>イメージが改ざんされた場合、デバイスは認証プロセスに失敗し、新しいイメージを拒否します。 |
| カスタマーサイト証明書のインストール | 各デバイスには、デバイス認証用に一意の証明書が必要です。 製造元でインストールされた証明書（MIC）がデバイスに含まれていますが、追加のセキュリティとして、Certificate Authority Proxy Function（CAPF）を使って証明書をインストールするよう Cisco Unified Communications Manager Administration で指定することができます。 あるいは、デバイス上の [エンタープライズ セキュリティ（Enterprise security）] メニューからローカルで有効な証明書（LSC）をインストールします。 |
| デバイス認証 | Cisco Unified Communications Manager サーバとデバイスの間で、一方のエンティティが他方のエンティティの証明書を受け入れるときに行われます。 デバイスと Cisco Unified Communications Manager の間でセキュアな接続を確立するかどうかを指定します。必要に応じて TLS プロトコルを使用してエンティティ間のセキュアなシグナリング パスを作成します。 Cisco Unified Communications Manager は、デバイスを認証できない限り、そのデバイスを登録しません。 |

| 機能 | 説明 |
| --- | --- |
| ファイル認証 | デバイスがダウンロードするデジタル署名付きファイルを検証します。 ファイル作成後にファイルが改ざんされていないことを確認するために、デバイスは署名を検証します。 認証に失敗したファイルは、デバイスのフラッシュ メモリに書き込まれません。 デバイスはこのようなファイルを拒否し、処理を続行しません。 |
| ファイルの暗号化 | 暗号化により、デバイスに転送中のファイルから機密情報が漏れないようにします。 さらに、デバイスは署名を検証して、ファイル作成後にファイルが改ざんされていないことを確認します。 認証に失敗したファイルは、デバイスのフラッシュ メモリに書き込まれません。 デバイスはこのようなファイルを拒否し、処理を続行しません。 |
| シグナリング認証 | TLS プロトコルを使用して、シグナリング パケットが転送中に改ざんされていないことを検証します。 |
| 製造元でインストールされる証明書 | 各デバイスには、製造元でインストールされる固有の証明書（MIC）が内蔵されており、これがデバイス認証に使用されます。 MIC は、デバイスに固有の永続的な ID 証明であり、Cisco Unified Communications Manager ではこれを使ってデバイスを認証します。 |
| メディアの暗号化 | SRTP を使用して、サポートされるデバイス間のメディア ストリームがセキュアであること、および意図したデバイスのみがデータを受信し、読み取ることを保証します。 この機能には、デバイスのメディア マスターのキー ペアの作成、キーのデバイスへの配布、キーが転送される間のキー配布のセキュリティ確保などが含まれます。 |
| CAPF（Certificate Authority Proxy Function） | 証明書生成手順の中で、デバイスに過剰な処理負荷がかかる部分を代理で実装します。また、キーの生成および証明書のインストールのためにデバイスと対話します。 デバイスの代理として、顧客が指定する認証局からの証明書を要求するよう CAPF を設定できます。または、ローカルに証明書を生成するよう CAPF を設定することもできます。 |
| セキュリティ プロファイル | デバイスが無保護であるか、あるいは認証、暗号化、セキュリティ保護の対象になるかを定義します。 この表の他の項目は、セキュリティ機能について説明しています。 これらの機能の詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。 |
| 暗号化された設定ファイル | デバイスのコンフィギュレーション ファイルのプライバシーを保護できるようにします。 |
| 電話機の Web サーバの無効化（オプション） | セキュリティ上の目的で、デバイスに関する Web ページ（ここにはデバイスのさまざまな処理の統計情報が表示される）へのアクセスを防止できます。 |

| 機能 | 説明 |
| --- | --- |
| 電話機のセキュリティ強化 | 次に示す追加のセキュリティ オプションを Cisco Unified Communications Manager Administration から制御できます。<br>• PC ポートの無効化<br>• Gratuitous ARP（GARP）の無効化<br>• PC ボイス VLAN の無効化<br>• Web アプリケーションへの限定的なアクセスの提供<br>• Bluetooth アクセサリ ポートの無効化<br>• デバイスに関する Web ページへのアクセスの無効化<br>• 画面ロックが必要<br>• Google Play へのアクセス制御™<br>• 未知の提供元からのアプリケーションのインストールに対するアクセス制御 |
| 802.1X 認証（802.1X Authentication） | デバイスは802.1X認証を使用して、ネットワーク アクセスを要求および獲得することができます。 |
| SRST向けのセキュアなSIPフェールオーバー | セキュリティのために Survivable Remote Site Telephony（SRST）リファレンスを設定した後、Cisco Unified Communications Manager Administration で従属デバイスをリセットすると、TFTP サーバはデバイスの cnf.xml ファイルに SRST 証明書を追加し、そのファイルをデバイスに送信します。 その後、セキュアなデバイスは TLS 接続を使用して、SRST 対応ルータと相互に対話します。 |
| シグナリング暗号化 | デバイスと Cisco Unified Communications Manager サーバの間で送信されるすべての SIP シグナリング メッセージが暗号化されるようにします。 |
| AES 256 暗号化 | Cisco Unified Communications Manager リリース 10.5(2) 以降に接続している DX シリーズのデバイスは、シグナリングとメディア暗号化に関する TLS および SIP の AES 256 暗号化をサポートします。 これによりデバイスは、SHA-2 （Secure Hash Algorithm）標準および Federal Information Processing Standard（FIPS）に準拠する AES-256ベースの暗号を使用してTLS 1.2接続を開始し、サポートすることができます。 |

## セキュリティ プロファイル

Cisco DX シリーズデバイスでは、そのデバイスがセキュリティ保護、認証、または暗号化の対象になるかどうかを定義したセキュリティ プロファイルを使用します。 セキュリティ プロファイルの設定、およびデバイスへのセキュリティ プロファイルの適用について、詳しくは『*Cisco Unified Communications Manager Security Guide*』を参照してください。

デバイスに設定されているセキュリティモードを確認するには、設定アプリケーションの[セキュリティ（Security）]メニューを参照してください。

# SE Android

Android™ セキュリティ拡張機能（SE Android）により、デバイスのセキュリティが強化されます。SE Android は、許可されないコードや危険なコードをデバイス上で実行できないようにして、悪意のあるアプリケーションからデバイスを保護します。 SE Android には次の機能があります。

- プロセスによる権限のエスカレーションを防止できます。
- 不正使用を防止し、root などの特権付きプロセスのセキュリティが侵害された場合の損害を抑えることができます。
- ポリシーを統合的に適用して、分析可能にします。
- 隠れた脆弱性から保護します。

デバイスには、アプリケーション、プロセス、ユーザがアクセスできるデータを指定するポリシーが格納されています。 SE Android は次の 2 つのモードをサポートします。

- 許可（Permissive）
- 適用（Enforcing）

ポリシーに違反するあらゆるアクションがログに記録されます。 適用モードである場合、そのアクションは拒否されます。 ユーザや管理者がポリシーまたはモードを制御することはできません。

## アップグレードと SE Android

リリース 10.2(2) にアップグレードした時点で、Cisco DX650 は引き続き許可モードの状態になります。これは、既存のフィールドユニットを処理しなければならないためであり、強制モードを有効にするには、その前に出荷時の状態にリセットする必要があります。 許可モードでは、SE Android はエンドポイントの運用に影響を与えません。

Cisco DX650 が出荷時の状態にリセットされると、モードは自動的に強制モードに切り替わります。 この動作により、SE Android 保護が有効になり、ポリシーに違反するアクションを拒否するようになります。

デバイスが 10.2(2) より前のファームウェア リリースにダウングレードされない限り、強制モードは有効な状態を保ちます。 リリース 10.2(2) 以降にアップグレードした時点で、デバイスは許可モードに戻り、工場出荷時の状態にリセットされるまでは許可モードのままです。

Cisco DX70 およびCisco DX80 デバイスは、工場出荷時から強制モードになっています。 Cisco DX70 およびCisco DX80 デバイスを許可モードにすることはできません。

# SE Android のトラブルシューティング

ポリシーは、許可すべきアプリケーションのアクションを想定して調整されます。ただし、許可すべきアクションがポリシーによって阻止される場合があります。ポリシーエラーには、次のような症状があります。

- サードパーティ製アプリケーションや他のアプリケーションが、起動時や実行中にエラーを表示する。
- 許可モードのエンドポイント（Cisco DX650 など）で機能するアプリケーションまたは機能が、強制モードで同様に設定されたデバイスでは機能しない。
- SE Android は「常にオン」の機能であり、管理者がこれを制御することはできません。 現場の問題を診断し、不具合として報告する必要があります。

## SE Android のポリシーの問題の診断

### 手順

**ステップ 1** SE Android モードを確認します。

a) 設定アプリケーションで、[端末について（About device）] > [SELinux のステータス（SELinux status）] をタップします。

b) Debugsh から、コマンド **show selinux status** を入力します。

モードが permissive の場合、問題は SE Android に関連したものではありません。

**ステップ 2** モードが enforcing の場合は、permissive モードでデバイスを再テストします。
permissive モードで問題が再現しない場合は、その問題は SE Android に関連している可能性があります。

**ステップ 3** 問題が SE Android に関連している場合、または判別できない場合は、ログを収集して報告してください。

## ADB シェルの制限

エンドポイントが enforcing モードの場合、Android Debug Bridge（adb）シェルは制限されます。**ls** や **ps** などのコマンドでは、完全な結果が表示されないことがあります。

完全な結果を表示するには debugsh コマンドを使用します。 たとえば、シェルから **ps** の代わりに debugsh **show process** を使用します。

また enforcing モードでは、多くのディレクトリが使用禁止であるため、ファイルシステムを自由に参照することができません。

### SE Android のログ収集

問題を報告するには、次の情報を収集します。

- 問題についての簡単な説明（問題が発生した日時を含む）
- 問題のスクリーンショット（可能な場合）
- debugsh の **show selinux all** コマンドの出力
- 問題レポート ツール（PRT）の出力

# ローカルで有効な証明書のセットアップ

### はじめる前に

Cisco Unified Communications Manager と Certificate Authority Proxy Function（CAPF）のセキュリティ設定が適切に行われていることを確認します。

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

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

### 手順

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

**ステップ 2** 設定アプリケーションで、[セキュリティ（Security）] > [エンタープライズセキュリティの設定（Enterprise security settings）] を選択します。

**ステップ 3** [LSC] をタップします。
認証文字列を要求するプロンプトがデバイスに表示されます。

**ステップ 4** 認証文字列を入力し、[送信（Submit）] をタップします。
CAPF の設定に応じて、デバイスで LSC のインストール、更新、または削除が開始されます。 処理中に一連のメッセージが表示されるので、進行状況を監視できます。

（注） LSC のインストール、更新、または削除プロセスは、完了するのに長時間かかることがあります。 このプロセスは、[キャンセル（Cancel）] をタップすることでいつでも中止できます。

インストールが正常に完了すると、デバイスに [インストール済み（Installed）] と示されます。 デバイスに [未インストール（Not Installed）] と示される場合は、認証文字列が正しくないか、またはデバイスがアップグレード可能ではない可能性があります。 CAPF 操作により LSC が削除された場合、デバイスは [未インストール（Not Installed）] と表示して、操作が

成功したことを示します。 CAPF サーバで生成されるエラー メッセージを確認し、適切な処置を講じてください。

（注） LSC がインストール、アップグレード、または削除された後、デバイスは再起動します。

# SHA-256 の製造元でインストールされる証明書

Cisco DX70 と Cisco DX80 では、Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）が使用されます。この証明書の署名アルゴリズムは、SHA-256 と RSA 2048 キーを組み合わせたものです。 署名アルゴリズムには、Cisco Unified Communications Manager、Cisco Secure Access Control Server（ACS）、およびセキュア SRST サポートが必要です。

SHA-256 MIC 機能のサポート要件は次のとおりです。

- Cisco Unified Communications Manager Release 9.1(2) 以降
- ACS Release 5.2 以降。

（注） ACS 5.2 以降は、EAP-TLS 内部メソッドを使用する EAP-FAST をサポートしません。 EAP-TLS を使用するか、または EAP-TLS 内部メソッドによる EAP-FAST 対応の ISE に移行してください。

- IOS 12.4(15)T1 以降
- Cisco Identity Services Engine のリリースが 1.1 以降であること。 EAP-TLS 内部メソッドによる EAP-FAST は ISE リリース 1.2 以降でサポートされています。

別個のアプリケーションが使用されていて、それらのアプリケーションがこのシリーズの電話機の MIC を認証しなければならない場合、以下のリンクから、このシリーズの電話機の MIC を発行している Cisco 認証局を取得できます。

- http://www.cisco.com/security/pki/certs/cmca2.cer
- http://www.cisco.com/security/pki/certs/crcam2.cer

アプリケーションで Cisco DX シリーズ デバイスの MIC を認証できるようにするためには、これらの Cisco 認証局をアプリケーションにインポートする必要があります。

# セキュアな電話コール

Cisco DX シリーズ デバイスのセキュリティを実装するには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[電話の設定（Phone Configuration）] ウィンドウの [保護されたデバイス（Protected Device）] パラメータを有効にします。 セキュリティが実

装されると、コール アプリケーションにセキュア コール アイコンが表示され、セキュアな通話であることが示されます。

セキュアなコールでは、すべてのコール シグナリングとメディア ストリームが暗号化されます。セキュアなコールは高度なセキュリティを提供し、コールに保全性とプライバシーを提供します。進行中のコールが暗号化されている場合、設定アプリケーションの [エンタープライズ セキュリティ（Enterprise security）] で、[セキュリティ モード（Security Mode）] ステータスが [暗号化済み（Encrypted）] として示されます。

（注） コールが PSTN などの非 IP コール レッグを経由してルーティングされる場合、コールが IP ネットワーク内で暗号化されており、鍵のアイコンが関連付けられていても、そのコールはセキュアではないことがあります。

セキュアなコールでは、コールが暗号化され、発側と着側の両方のデバイスが保護デバイスとして設定されている場合、セキュア トーン機能が Cisco Unified Communications Manager 上で有効になっていれば、2 秒間のトーンによってユーザに通知されます。 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、発側と着側の両方のデバイスが保護されていて、なおかつ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。 コールが暗号化されていないとシステムが判断した場合、デバイスは、ノンセキュア通知トーン（6回のビープ音）を再生して、コールが無保護であることをユーザに警告します。セキュア通知トーン機能および設定要件の詳しい説明については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

（注） ビデオは非セキュアで送信されます。 したがって、発側と着側のデバイスが両方ともセキュアであっても、[暗号化済み（Encrypted）] 鍵アイコンがビデオ コールで表示されることはありません。

## セキュアな電話コールの識別

セキュアなコールは、Cisco DX シリーズ デバイスと相手側のデバイスがセキュアなコール用に設定されている場合に確立されます。 両方のデバイスは、同一のシスコ IP ネットワーク内に存在することも、IP ネットワーク外部にあるネットワークに存在することもできます。 セキュアな会議コールは、次の手順で確立されます。

1. セキュアなデバイス （暗号化セキュリティ モード）から、ユーザがコールを開始します。
2. デバイスでは、設定アプリケーションの [エンタープライズセキュリティ（Enterprise security）] に、[暗号化（Encrypted）] ステータスが示されます。 このステータスは、 セキュアなコール用にデバイスが設定されていることを示しますが、接続相手のデバイスが同様にセキュアであるとは限りません。
3. セキュアな相手側デバイスにコールが接続されると、セキュリティ トーンが再生されます。これは、会話の両側が暗号化され、セキュアであることを示しています。 そうでない場合は、非セキュア トーンが再生されます。

（注） セキュア トーンは、Cisco Unified Communications Manager で有効になっている場合にのみ再生されます。 セキュア トーンが無効になっている場合、コールがセキュアであっても、セキュア トーンは再生されません。 詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Secure and Nonsecure Indication Tone Setup」の章を参照してください。

## セキュアな会議コールの特定

セキュアな会議コールを開始し、参加者のセキュリティ レベルをモニタすることができます。セキュアな会議コールは、次の手順で確立されます。

1. ユーザがセキュアなデバイスから会議を開始します。
2. Cisco Unified Communications Manager は、セキュアな会議ブリッジをそのコールに割り当てます。
3. 参加者が追加されると、Cisco Unified Communications Manager は、各デバイスのセキュリティ モードを検証し、セキュアな会議のレベルを維持します。
4. デバイスに、電話コールのセキュリティ レベルが表示されます。

（注） 参加者デバイスのセキュリティ モードおよびセキュア 会議ブリッジの可用性に応じて、さまざまな連携動作、制約事項、および制限事項が電話会議のセキュリティ レベルに影響を与えます。 Cisco DX シリーズ デバイスでは、セキュアなオーディオ電話会議のみがサポートされます。 ビデオはセキュアになりません。

## コール セキュリティの連携動作と制限事項

Cisco Unified Communications Manager は、会議の確立時にデバイスのセキュリティ ステータスを確認し、会議のセキュリティ表示を変更するか、またはコールの確立をブロックしてシステムの整合性とセキュリティを維持します。 次の表は、割り込み機能の使用時にコールのセキュリティ レベルに適用される変更内容を示しています。

**表 *16*：割り込み機能の使用時のコール セキュリティ**

| 発信側の電話機のセキュリティ レベル | 使用する機能 | コールのセキュリティ レベル | 動作結果 |
|---|---|---|---|
| 非セキュア | 割込み | 暗号化されたコール | コールは割り込みを受け、非セキュア コールとして識別されます。 |

| 発信側の電話機のセキュリティ レベル | 使用する機能 | コールのセキュリティ レベル | 動作結果 |
|---|---|---|---|
| セキュア | 割込み | 暗号化されたコール | コールは割り込みを受け、セキュア コールとして識別されます。 |

次の表は、発信側の電話機のセキュリティ レベル、参加者のセキュリティ レベル、およびセキュアな会議ブリッジの可用性によって決定する会議のセキュリティ レベルに適用される変更内容を示しています。

**表 *17*：会議コールのセキュリティの制限事項**

| 発信側の電話機のセキュリティ レベル | 使用する機能 | 参加者のセキュリティ レベル | 動作結果 |
|---|---|---|---|
| 非セキュア | 会議 | セキュア | 非セキュアな会議ブリッジ<br>非セキュアな会議 |
| セキュア | 会議 | 少なくとも 1 台のメンバーが非セキュア。 | セキュアな会議ブリッジ<br>非セキュアな会議 |
| セキュア | 会議 | セキュア | セキュアな会議ブリッジ<br>セキュアな暗号化レベルの会議 |
| 非セキュア | ミートミー | 最小限のセキュリティ レベルが暗号化。 | 発信側は「セキュリティ レベルを満たしていません。コールを拒否します（*Does not meet Security Level, call rejected*）」というメッセージを受け取る。 |
| セキュア | ミートミー | 最小限のセキュリティ レベルは非セキュア | セキュアな会議ブリッジ<br>会議はすべてのコールを受け入れる。 |

VPN および Cisco Virtualization Experience Client（VXC）VPN を介してセキュアなビデオを使用する場合、サポートされる最大帯域幅は 320 Kpbs です。

デバイスが Cisco TelePresence をコールする場合、最大帯域幅は 320 kbps です。

## デバイス セキュリティ情報のリモートでの確認

### 手順

**ステップ 1** デバイスセキュリティ情報をリモートで確認するには、デバイスが、Cisco Unified Communications Managerサーバに登録されている必要があり、また[デバイス設定（Device Configuration）]ページで [Web アクセス（Web Access）] が有効にされている必要があります。

**ステップ 2** Web ブラウザで、デバイス セキュリティ情報を表示するには http://<device ip>/SecurityInformation に、XML 形式でデバイス セキュリティ情報を表示するには http://<device ip>/SecurityInformationX にアクセスしてください。

## 割り込みのための暗号化

デバイスに暗号化が設定されていない場合、そのデバイスを使用して暗号化されたコールに割り込むことはできません。 この場合、割り込みに失敗すると、割り込みが開始されたデバイスでリオーダー トーン（速いビジー音）が聞こえます。

割り込みの開始側のデバイスに暗号化が設定されている場合、割り込みの開始側は暗号化されたデバイスからセキュアでないコールに割り込むことができます。 割り込みが発生すると、Cisco Unified Communications Manager はそのコールを非セキュアに分類します。

割り込みの開始側のデバイスに暗号化が設定されている場合、割り込みの開始側は暗号化されたコールに割り込むことができ、デバイスはそのコールが暗号化されていることを示します。

# 802.1X 認証のサポート

Cisco DX シリーズデバイスと Cisco Catalyst スイッチは、従来から Cisco Discovery Protocol（CDP）を使用して相互を識別し、VLAN 割り当てやインライン パワー要件などのパラメータを特定していました。 CDP では、ローカルに接続されたワークステーションは識別されません。 Cisco DX シリーズ デバイスは、EAPOL パススルー メカニズムを提供します。 このメカニズムを使用すると、デバイスに接続されたワークステーションは、LAN スイッチにある 802.1X オーセンティケータに EAPOL メッセージを渡すことができます。 パススルー メカニズムにより、デバイスは、ネットワークにアクセスする前にデータ エンドポイントを認証する LAN スイッチとして動作しません。

Cisco DX シリーズデバイスまた、プロキシ EAPOL ログオフ メカニズムも提供します。 ローカルに接続された PC がデバイスから切断された場合でも、LAN スイッチとデバイス間のリンクは維持されるので、LAN スイッチは物理リンクの障害を認識しません。 ネットワークの完全性を維持するため、デバイスはダウンストリーム PC の代わりに EAPOL ログオフ メッセージをスイッチに送ります。これによって、LAN スイッチはダウンストリーム PC の認証エントリをクリアします。

Cisco DX シリーズ にはまた、802.1x サプリカントも含まれています。 このサプリカントを使用すると、ネットワーク管理者はデバイスから LAN スイッチ ポートへの接続を制御できます。 デ

バイスに含まれる 802.1X サプリカントの現在のリリースでは、ネットワーク認証に EAP-FAST オプションと EAP-TLS オプションが使用されています。

## 必要なネットワーク コンポーネント

Cisco DX シリーズ デバイスでの 802.1X 認証のサポートには、いくつかのコンポーネントが必要です。 これには次が含まれます。

- 802.1X サプリカントとして機能するデバイス。ネットワークへのアクセス要求を開始するデバイスです。
- Cisco Secure Access Control Server（ACS）（またはその他のサードパーティ サーバ）。 この認証サーバには、デバイスを認証する共有シークレットが設定されている必要があります。
- Cisco Catalyst スイッチ（またはその他のサードパーティ製スイッチ）。 スイッチは 802.1X をサポートする必要があるため、オーセンティケータとして機能して、デバイスと認証サーバとの間でメッセージを交換することができます。 この交換が完了した後、スイッチはデバイスのネットワーク アクセスを許可または拒否します。

## ベスト プラクティス

次に、802.1X 設定の要件および推奨事項について説明します。

- 802.1X 認証の有効化: 802.1X 標準を使用して Cisco DX シリーズ デバイスを認証するには、デバイスで 802.1X 認証を有効にする前に、その他のコンポーネントを正しく設定しておく必要があります。
- PC ポートの設定：802.1X 標準では VLAN の使用が考慮されないため、特定のスイッチ ポートに対してデバイスを 1 つだけ認証することを推奨します。 ただし、複数ドメインの認証をサポートしているスイッチもあります（Cisco Catalyst スイッチなど）。 スイッチの設定により、PC をデバイスの PC ポートに接続できるかどうかが決定されます。
  - 有効：複数ドメインの認証をサポートするスイッチを使用している場合、PC ポートを有効化し、そのポートに PC を接続できます。 この場合、スイッチと接続先 PC 間の認証情報の交換をモニタするために、デバイスはプロキシ EAPOL ログオフをサポートします。 Cisco Catalyst スイッチでの IEEE 802.1X サポートの詳細については、次の URL にある Cisco Catalyst スイッチのコンフィギュレーション ガイドを参照してください。

    http://www.cisco.com/c/en/us/support/switches/catalyst-6500-series-switches/tsd-products-support-series-home.html
  - 無効：スイッチで同じポート上の複数の 802.1X 準拠デバイスがサポートされていない場合は、802.1X 認証を有効にするときに PC ポートを無効にするようにしてください。 このポートを無効にしないで PC を接続しようとすると、スイッチはデバイスと PC の両方に対してネットワーク アクセスを拒否します。
- ボイス VLAN の設定：802.1X 標準では VLAN が考慮されないため、この設定をスイッチのサポートに基づいて行うようにしてください。

- 有効：複数ドメインの認証をサポートするスイッチを使用している場合は、ボイスVLANを引き続き使用できます。
- 無効：スイッチで複数ドメインの認証がサポートされていない場合は、ボイス VLANを無効にし、ポートをネイティブ VLAN に割り当てることを検討してください。

# 画面ロックおよび自動ロックの設定

画面ロック タイムアウト値は、画面がオフにされ、画面ロックが有効化される、デバイスの通常のアイドル タイムアウトを制御します。 この変数は、1 ～ 60 分の範囲内で設定できます。

自動ロック機能は、ディスプレイが暗くなる（または消灯する）までの猶予時間を制御します。デバイスが「常にオン」モードの場合、デバイスは暗くなります。 デバイスが「終夜灯」モードの場合、デバイスは完全に消灯します。 自動ロック値は、最大で 10 分まで設定可能です。 自動ロック値を設定するには、[設定（Settings）] > [セキュリティ（Security）] > [自動ロック（Automatically lock）] に移動します。

次の表は、画面ロック タイムアウト値と自動ロック値の関係を示しています。

**表 *18*：画面ロック タイムアウトと自動ロック値の関係**

| 条件 | 結果 |
|---|---|
| 画面ロック タイムアウト値が自動ロック値より低い | 画面ロック タイムアウト値に到達すると、画面は最大の明るさのままで、ロックされた画面が表示されます。 |
| 自動ロック値が画面ロック タイムアウト値より低い | 自動ロック値に到達すると、2 つの結果が考えられます。<br>• デバイスが「常にオン」モードの場合、自動ロック値に到達すると、デバイスは暗くなります。 画面ロック タイムアウト値に到達すると、デバイスはロックされ、暗い状態を維持します。<br>• デバイスが「終夜灯」モードの場合、自動ロック値に到達すると、デバイスはロックされて消灯します。 画面ロック タイムアウト値に到達しても、それ以上の変化は起こりません。 |
| 画面ロック タイムアウト値が自動ロック値と等しい | この値に到達すると、画面は最大の明るさのままで、ロックされた画面が表示されます。 |

# 画面のロック解除/パスワードのリセットのセットアップ

この機能により、ユーザは、画面のロック解除に使用されるPIN/パスワードをリセットできます。ユーザは、Cisco Unified Communications Manager または設定されている Google™ Account のクレデンシャルを使用して PIN/パスワードをリセットできます。 Cisco Unified Communications Manager を使用して PIN/パスワードをリセットするには、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 Communications ManagerAdministration）] で、[ユーザ管理（User Management）] > [エンド ユーザ（End User）] 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** 必要なユーザ情報を入力します。

**ステップ 4** [デバイス情報（Device Information）] ウィンドウで、ユーザを関連付けるデバイスを選択します。

**ステップ 5** [保存（Save）] をクリックします。

**ステップ 6** [権限情報（Permissions Information）] ウィンドウで、ユーザに Cisco Unified Communications Manager の権限を割り当てます。

**ステップ 7** [権限情報（Permissions Information）] ウィンドウで、[標準 CCM エンドユーザ（Standard CCM End Users）] を選択します。

**ステップ 8** [保存（Save）] と [設定の適用（Apply Config）] をクリックします。 デバイスが再登録した後、ユーザはそのデバイスに設定されます。

第 10 章

# 機能とサービス


- 使用可能なテレフォニー機能，113 ページ
- 機能ボタン，129 ページ
- 機能管理ポリシーの設定，130 ページ
- 電話ボタン テンプレート，131 ページ
- 製品固有オプションの設定，132 ページ
- ビデオ送信解像度のセットアップ，147 ページ
- インスタント メッセージングとプレゼンスのセットアップ，148 ページ
- アプリケーションの設定，149 ページ
- Unified Communications Manager からの Android APK ファイルのプッシュ，151 ページ


## 使用可能なテレフォニー機能

Cisco DX シリーズ デバイスには、Cisco WebEx、Cisco Unified Presence、インスタント メッセージング、電子メール、ビジュアル ボイスメール、Cisco Unified Communications Manager の音声とビデオテレフォニー機能など、コラボレーションアプリケーションの統合スイートが備わっています。 また、これらのデバイスでは Google Play のアプリケーションもサポートされます。

ネットワークに Cisco DX シリーズ デバイスをインストールして、デバイスのネットワーク設定を行い、デバイスを Cisco Unified Communications Manager に追加した後、Cisco Unified Communications Manager Administration を使用してテレフォニー機能を設定し、サービスをセットアップする必要があります。

（注） また、Cisco Unified Communications Manager には、各種のテレフォニー機能を設定するために使用できるサービス パラメータもいくつか用意されています。 サービス パラメータへのアクセスと設定方法については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。 サービスの機能の詳細については、[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、パラメータの名前または疑問符のヘルプ ボタンをクリックしてください。

# エージェントのグリーティング

エージェントが事前録音したグリーティングを作成したり更新したりできるようにします。このグリーティングは、エージェントが発信者と話しはじめる前に、顧客コールの開始時に再生されます。 エージェントは、必要に応じて 1 つまたは複数のグリーティングを事前録音できます。

詳細については、以下を参照してください。

- 『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」の章
- 『*Features and Services Guide for Cisco Unified Communications Manager*』の「Barge and Privacy」の章

## エージェント グリーティングの有効化

### 手順

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

**ステップ 2** 設定するデバイスを探します。

**ステップ 3** [デバイス情報レイアウト（Device Information Layout）] ペインまでスクロールし、[ビルトイン ブリッジ（Built In Bridge）] を [オン（On）] または [デフォルト（Default）] に設定します。

**ステップ 4** [保存（Save）] を選択します。

**ステップ 5** ブリッジの設定を確認します。

a) [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。
b) 適切なサーバおよびサービスを選択します。
c) [クラスタワイド パラメータ（デバイス - 電話）（Clusterwide Parameters (Device - Phone)）] ペインまでスクロールして、[ビルトインブリッジの有効（Builtin Bridge Enable）] を [オン（On）] に設定します。
d) [保存（Save）] を選択します。

# すべてのコール

ユーザがアクティブ コールと保留中のコールのリストを確認できるようにします。このリストは、最も古いコールから時系列順にソートされます。 ユーザは、着信コールと完了コールのリストも表示できます。このリストは、新しいコールから古いコールの順にソートされます。

# プライマリ回線でのすべてのコール

プライマリ回線で [すべてのコール（All Calls）] 機能を使用できるようにします。 プライマリ回線のコール リストにすべての着信コールが表示され、プライマリ回線でこれらのコールに応答できます。

# 自動応答

呼出音を 1 ～ 2 回鳴らした後に、着信コールを自動的に接続します。 自動応答は、スピーカーフォンとヘッドセットのどちらでも機能します。 デバイスのヘッドセットの自動応答が有効だが、ヘッドセットがデバイスに接続していない場合、デバイスはコールに自動的に応答しません。

詳細については、『『*Cisco Unified Communications Manager Administration Guide*』』の「Directory Number Configuration」の章を参照してください。

# 自動ダイヤル

ユーザが、発信履歴、着信履歴、不在履歴を含む最近のコール履歴から該当する番号を選択できます。 コールを発信するには、ユーザはすべてのコールリストから番号を選択するか、引き続き手動で番号を入力することができます。

# 割込み

ユーザが共有電話回線でプライベート コール以外のコールに参加できるようにします。割り込みにより、ユーザがコールに追加され、そのコールが会議に変換されます。 ユーザおよび他の参加者が会議機能にアクセスできるようになります。

（注） [組み込みブリッジ有効（Built In Bridge Enable）] サービス パラメータがオフに設定されている場合でも、ユーザは割り込みを使用できます。 デバイス上でユーザが割り込み機能を使用できないようにするには、デバイスの [機能管理ポリシー（Feature Control Policy）] で [割込み（Barge）] を無効にする必要があります。

詳細については、以下を参照してください。

- 『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Setup」の章
- 『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」の章
- 『*Features and Services Guide for Cisco Unified Communications Manager*』の「Barge and Privacy」の章
- 『*Cisco Unified Communications Manager Administration Guide*』の「Feature Control Policy Setup」の章

# ビジー ランプ フィールド

ユーザは、デバイス のスピードダイヤル ボタン、コール ログまたはディレクトリの一覧に関連付けられている電話番号のコール状態をモニタできます。

詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』の「IM and Presence Service」の章を参照してください。

# コール転送

ユーザは、着信コールを別の番号にリダイレクトできます。 コール転送オプションには、すべてのコールの転送、話中転送、無応答時転送、およびカバレッジなし時転送があります。

その他のオプションは次のとおりです。

- ターゲットの電話番号から発信されたコールを、転送せずに受信できるようにする。
- コール転送ループが、コール転送チェーンで最大リンク数を超えないようにする。

コール転送オプションは、回線ごとに割り当てることができます。

詳細については、以下を参照してください。

- 『『*Cisco Unified Communications Manager Administration Guide*』』の「Directory Number Setup」の章。
- 『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」の章。

# 発信回線 ID

ユーザは、発信回線 ID に対して完全な外線番号の使用を可能にすることができます。

詳細については、『*Cisco Unified Communications Manager System Guide*』の「“Cisco Unified IP Phones”」の章を参照してください。

# 発信回線 ID の表記

ユーザはケースバイケースで発信側番号の発信を有効化または制限することができます。

詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」の章を参照してください。

# Cisco エクステンション モビリティ

ユーザが、デバイスの Cisco エクステンション モビリティ サービスにログインして、共有デバイスからデバイス設定（ライン アピアランス、サービス、短縮ダイヤルなど）に一時的にアクセスできるようにします。

Cisco エクステンション モビリティは、社内の複数の場所でユーザが業務を行う場合や、作業場を同僚と共有する場合に便利です。

デバイスに対してエクステンション モビリティをオンにすると、[エクステンション モビリティ（Extension Mobility）] という新しいオプションがデバイス上に表示されます（[設定（Settings）] > [個人（Personal）] > [エクステンション モビリティ（Extension Mobility）]）。 ユーザが現在このデバイスにログインしている場合は、ロック画面に [新規ユーザとしてログイン（Sign in as New User）] と [ログアウト (Sign out)] が表示されます。

（注） ユーザがデバイスにログインするには、管理者から提供されるエクステンション モビリティのクレデンシャルを入力します。 これらのクレデンシャルは、ユーザ画面のロック PIN とは異なります。

[エクステンション モビリティ（Extension Mobility）] 画面で次のオプションがユーザに対して表示されます。

| 設定 | 説明 |
|---|---|
| ユーザ ID（User ID） | このデバイスに現在ログインしているユーザのユーザ ID です。 |
| PIN 設定（Set PIN） | エクステンション モビリティの PIN を変更するには、この設定をタップします。 （Cisco Unified Communications Manager の一部のバージョンではこの設定はサポートされていません）。 これはユーザ画面ロック PIN ではなく、ユーザ エクステンション モビリティの PIN であることに注意してください。 |
| アカウントを削除（Remove Account） | このデバイスからこのユーザのすべてのコンテンツと設定を削除するには、この設定をタップします。 |
| ログアウト（SIGN OUT） | このデバイスからサイン アウトするにはタップします。 デバイスがログアウトについて確認をします。ユーザがログアウトを確認すると、デバイスのデフォルト設定に戻るためデバイスの再起動が開始します。 |

詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』の「Extension Mobility」の章を参照してください。

## エクステンション モビリティ マルチユーザ

エクステンション モビリティ マルチユーザ機能では、エクステンション モビリティのログイン/ログアウト プロセスが使用されます。 ユーザがログインし、Cisco Unified Communications Manager サーバによりユーザ クレデンシャルが認証されるときに、サーバは、エクステンション モビリティ機能と同じメッセージング方式を使用します。

ユーザ A がデバイスに初めてログインすると、デバイスの再起動サイクルを行い、デバイス上でのユーザ A のユーザ パーティションを作成します。 デバイスは、ユーザ A にセットアップ ウィザードを表示します。 ユーザ A は個人のアプリケーションとデータのための専用領域を取得し、コール アプリケーションは他の Cisco DX シリーズデバイスの場合と同様に機能します。 最初のログインの後、ユーザ A はアプリケーション関連の設定を行います。 ユーザ A がこのデバイスからログアウトすると、ユーザ A が次回デバイスにログインしたときのためにユーザ設定が保存されます。

ユーザ A がデバイスからログアウトすると、ユーザ B がユーザ B のクレデンシャルを使用してデバイスにログインできます。 ユーザ B は同じ手順でユーザ B のパーティションを取得します。初回ログイン時に、セットアップ ウィザードでユーザ B に対し個人のアプリケーションおよびデータを設定するように指示が出されます。ユーザ B には、Cisco DX シリーズ デバイスで通常使用するコール アプリケーションもあります。

パーティションは完全に個別ものであるため、ユーザが他のユーザのデータを参照することは絶対にできません。

エクステンション モビリティのマルチユーザによりの企業でマルチユーザの利用が可能です。システム管理者は、エクステンション モビリティのマルチユーザを設定するデバイスを決定し、特定のデバイスにログインできるユーザにクレデンシャルを提供します。 適切なクレデンシャルにより、ユーザは特定デバイスだけにログインし、各自のアカウントを設定することができます（各自のアカウントの削除を含む）。 ユーザは、同一デバイス上の他のユーザのアカウントの変更はできません。

アルゴリズムにより特定のデバイスにログインできるユーザの数を制限します。 デバイスのユーザの最大数は、各ユーザの使用率によって異なります。 デバイスのフラッシュ メモリ容量が特定の割合まで低下すると、新規ユーザ用の領域を確保するために、最終ログイン日時が最も古いユーザのアカウントが削除されます。したがって、デバイスの容量不足のために新規ユーザがログインできないという事態は生じません。

## Cisco Extension Mobility の設定

Cisco Extension Mobility により、ユーザは、一時的にその他のデバイスからライン アピアランス、サービス、スピードダイヤルなどの電話機の設定にアクセスできるようになります。

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] の [デフォルトのデバイスプロファイル（Default Device Profile）] ウィンドウで、Cisco Extension Mobility に対応するように各デバイスを設定します。 これにより、特定のデバイスのユーザ デバイス プロファ

イルを持たないユーザが、そのデバイスを使用して Cisco Extension Mobility を使用することができるようになります。

（注） Extension Mobility は、通信プロトコルとして HTTP または HTTPS を使用します。 Web プロキシを使用するためにこのデバイスを設定する場合、Extension Mobility のバイパスを設定する必要があります。

次に示す順序で手順を実行し、Cisco Extension Mobility を設定します。

### 手順

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

**ステップ 2** Cisco Unified Serviceability で[ツール（Tools）] > [サービスのアクティベーション（Service Activation）] を選択して、Cisco Extension Mobility サービスをアクティブにします。

（注） どのノードでエクステンション モビリティ サービスをディセーブルにするには、最初にそのノードをサービス アクティベーション用のサービスを非アクティブにします。

（注） いずれかのノードで Cisco Extension Mobility サービスのアクティブ化または非アクティブ化の変更がなされると、サービス URL を構築するために必要な情報を使用して、データベース テーブルが更新されます。 データベース テーブルは、エクステンション モビリティ サービス パラメータが変更されると更新されます。 EMApp サービスにより、変更通知が処理されます。

**ステップ 3** Cisco Extension Mobility サービスを作成します。 要約手順は次のとおりです。

- [デバイス（Device）] > [デバイスの設定（Device Settings）] > [IP Phone サービス（Phone Services）] を選択します。
- サービス名（Extension Mobility Service または EM）を入力してください。
- 次の URL を入力してください：
  http://10.89.80.19:8080/emapp/EMAppServlet?device=#DEVICENAME#

（注） URL を間違って入力し、デバイスを誤ったサービスに登録した場合は、URL を修正して保存し、[登録の更新（Update Subscriptions）] をクリックするか、または URL を修正し、間違ったサービスが登録されている各デバイスを再び登録します。

- [サービスカテゴリ（Service Category）] および [サービスタイプ（Service Type）] の値を選択します。
  - サービス カテゴリに [XML サービス（XML Service）] を選択します。
  - サービス タイプに、[標準の IP 電話サービス（Standard IP Phone Service）] を選択します。
- [保存（Save）] をクリックします。

**ステップ 4** 管理パラメータを設定します。

**ステップ 5** Cisco Extension Mobility をサポートする各電話機タイプのデフォルトのデバイス プロファイルを作成します。

**ステップ 6** ユーザのユーザ デバイス プロファイルを作成します。 要約手順は次のとおりです。

- [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）] と選択し、[新規追加（Add New）] をクリックします。
- [デバイス タイプ（Device Type）] を入力します。
- デバイス プロファイルの名前を入力し、[保存（Save）] をクリックします。
- 電話番号（DN）と必要な情報を入力して、[保存（Save）] をクリックします。すべての DN を繰り返します。
- このデバイス プロファイルにインターコム回線をイネーブルにするには、このデバイス プロファイルのインターコムディレクトリ番号（DN）を設定します。[インターコム電話番号の設定（Intercom Directory Number Configuration）] ウィンドウでインターコム DN の設定をします。このウィンドウには、[コール ルーティング（Call Routing）] > [インターコム（Intercom）] > [インターコムの電話番号（Intercom Directory）]からもアクセス可能です。アクティブにするインターコム DN 用に、[インターコム電話番号の設定（Intercom Directory Number Settings）] ペインで[デフォルトのアクティブ デバイス（Default Activated Device）] を指定します。
- Cisco Extension Mobility にデバイス プロファイルを登録するため、[デバイス プロファイルの設定（Device Profile Configuration）] ウィンドウで、右上隅にある [関連リンク（Related Links）] ドロップダウン リスト ボックスから、[サービスの登録/登録解除（Subscribe/Unsubscribe Services）] を選択し、[検索（Go）] をクリックします。

（注） 電話番号およびデバイス プロファイルを同じエクステンション モビリティ サービスに登録します。

**ステップ 7** ユーザとユーザ デバイス プロファイルを関連付けます。 要約手順は次のとおりです。

- [ユーザ管理（User Management）] > [エンド ユーザ（End User）] の順に選択し、[新規追加（Add New）] をクリックして、ユーザ情報を入力します。
- [エクステンション モビリティの使用可能なプロファイル（Extension Mobility Available Profiles）]で、ユーザ デバイス プロファイルを選択し、下矢印をクリックしてください。これにより、[制御プロファイル（Controlled Profiles）] ボックスに選択したサービスを配置されます。
- [保存（Save）] をクリックします。

**ステップ 8** デバイスおよびユーザ デバイス プロファイルを設定し、Cisco Extension Mobility に登録します。

- [デバイス（Device）] > [電話機（Phone）] を選択し、[新規追加（Add New）] をクリックします。
- [電話の設定（Phone Configuration）] ウィンドウの [拡張情報（Extension Information）] で、[エクステンションモビリティの有効化（Enable Extension Mobility）] をオンにします。

- [ログアウトプロファイル（Log Out Profile）] ドロップダウンリストボックスで、[現在のデバイス設定を使用（Use Current Device Settings）] または仕様を設定したプロファイルを選択し、[保存（Save）] をクリックします。
- デバイスに Cisco Extension Mobility を登録するため、右上隅にある [関連リンク（Related Links）] ドロップダウンリストボックスから [サービスの登録/登録解除（Subscribe/Unsubscribe Services）] を選択してください。そして、[検索（Go）] をクリックします。

**ステップ 9** ユーザは、Cisco Extension Mobility により、デバイスのユーザ PIN を変更し、[クレデンシャルの変更（Change Credential）] 電話サービスを設定して、ユーザ、ユーザデバイスプロファイルまたはデバイスを [クレデンシャルの変更（Change Credential）] 電話サービスに関連付けることができます。

**ステップ 10** デバイスの [デバイス設定（Device Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域で、[マルチユーザ（Multi-User）] ドロップダウンリストボックスから [有効化（Enabled）] の値を選択します。

**ステップ 11** エクステンションモビリティサーバのデフォルトの URL を変更する、またはデフォルトの HTTPS URL から HTTP に変更するには、[マルチユーザ URL（Multi-User URL）] フィールドに新しいエクステンション モビリティ サーバ URL を入力します。

# Cisco Mobility

ユーザは、1 つの電話番号を使用してビジネス コールを管理したり、デスクトップ電話機および携帯電話などのリモート デバイスで、進行中のコールをピックアップしたりすることができます。 また、電話番号や時刻に応じて、発信者グループを制限できます。

Cisco Mobility for Cisco DX シリーズ デバイスには、Cisco Unified Communications Manager リリース 9.0(1) 以降が必要です。

詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』の「Cisco Mobility」の章を参照してください。

# 会議

- ユーザは複数の通話相手と同時に会話できます。このため、この機能は各参加者に個別にコールします。
- 標準（アドホック）会議では、すべての参加者が参加者を追加または削除できます。
- ユーザが、同一電話回線上にある 2 つ以上のコールを 1 つの電話会議として接続したうえで、そのコールに留まることができます。

これらの機能を有効にするには、[高度なアドホック会議（Advanced Adhoc Conference）] サービス パラメータ（Cisco Unified Communications Manager ではデフォルトで無効になっています）を使用します。

詳細については、『*Cisco Unified Communications Manager System Guide*』の「Conference Bridges」の章を参照してください。

### セキュアな会議

セキュア会議を使用すると、セキュア デバイスはセキュア会議ブリッジを使用して会議コールを発信できます。 新しい参加者が追加されても、すべての参加者がセキュアなデバイスを使用している限り、セキュア コール アイコンが表示されます。

詳細については、次の各項を参照してください。

- *Cisco Unified Communications Manager System Guide*の「Conference Bridges」の章
- 『*Cisco Unified Communications Manager Administration Guide*』の「Conference Bridge Setup」の章
- 『*Cisco Unified Communications Manager Security Guide*』

## 転送

拡張即時転送機能を有効にすると、ユーザが着信コールを自分のボイスメッセージングシステムに着信コールを直接転送できます。

ボイスメールへのコールの転送の詳細については『『*Features and Services Guide for Cisco Unified Communications Manager*』』の「Immediate Divert」の章を参照してください。

拡張即時転送機能の詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」の章を参照してください。

## サイレント

DNDをオンにすると、コールが呼び出し状態になっても呼出音が鳴らなくなります。またあらゆる種類の表示や音による通知も、一切行われません。

（注） サイレント（DND）は、911 コールには影響しません。

[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] では、次の DND 関連のパラメータを設定できます。

- [サイレント（Do Not Disturb）]：このチェックボックスを使用すると、DNDをデバイスごとに有効にすることができます。 [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [電話（Phone）] > [電話の設定（Phone Configuration）] を選択します。
- [DND 着信呼警告（DND Incoming Call Alert）]：デバイスで DND がアクティブのときに着信コールに対して発生させるアラート（存在する場合）のタイプを選択します。 このパラメー

タは、[共通の電話プロファイル（Common Phone Profile）] ウィンドウおよび [電話の設定（Phone Configuration）] ウィンドウの両方にあります （[電話の設定（Phone Configuration）] ウィンドウの値が優先されます）。

詳細については、『『*Features and Services Guide for Cisco Unified Communications Manager*』』の「Do Not Disturb」の章を参照してください。

# ゲートウェイ録音

この機能は、メディアゲートウェアに対し、コールを録音サーバに送信し、コールモニタリングを改善するように指示します。

詳細については、『『*Features and Services Guide for Cisco Unified Communications Manager*』』の「Monitoring and Recording」の章を参照してください。

# 保留状態

共有回線を持つデバイスでは、ローカル回線とリモート回線のいずれがコールを保留したのかを区別できます。

# 保留と保留解除

ユーザは、接続されたコールをアクティブな状態から保留状態に移行できます。

## 保留音

発信者が保留状態になっている間、音楽を再生します。

詳細については、『『*Features and Services Guide for Cisco Unified Communications Manager*』』の「Music On Hold」の章を参照してください。

# 無視

ユーザは、通知ウィンドウから着信コールを無視できます。

# メッセージ受信インジケータ

ハンドセットのランプの 1 つで、ユーザに対する 1 つまたは複数の新着ボイス メッセージが届いていることを示します。

詳細については、以下を参照してください。

- 『『*Cisco Unified Communications Manager Administration Guide*』』の「Message Waiting Setup」の章
- 『*Cisco Unified Communications Manager System Guide*』の「Voice Mail Connectivity to Cisco Unified Communications Manager」の章

# ミュート

デバイスのスピーカー、ハンドセット、ヘッドセットを含むすべての入力デバイスのオーディオ入力音声を消音します。

# プラス ダイヤル

ユーザは、先頭に「+」記号を付けて E.164 番号をダイヤルできます。

+ 記号をダイヤルするには、「*」キーを 1 秒以上押し続ける必要があります。 これは、オンフックかオフフックのコールで先頭桁をダイヤルするときにのみ当てはまります。

# 保護コール

2 台のデバイスの間にセキュアな（暗号化された）接続を提供します。 コールの開始時にはセキュリティ トーンが再生され、両方のデバイスが保護されていることを通知します。 保護コールを設定すると、一部の機能（会議コール、共有回線、複数ライン同時通話機能など）は使用できません。 保護されたコールは認証されません。

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

# 呼出音の設定

別のアクティブ コールがデバイスに着信したときに回線で使用される呼出音タイプを指定します。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Directory Number Setup」の章を参照してください。

# 呼出音

ユーザは、デバイスで着信コールや新しいボイス メッセージを通知する方法をカスタマイズできます。

# セキュアおよび非セキュアの通知トーン

Cisco Unified Communications Manager でセキュア（暗号化および信頼）に設定されたデバイスを、「保護された」ステータスにすることができます。 その後、必要に応じて、保護されたデバイスは、コールの初めに通知トーンを再生するように設定できます。

- 保護されたデバイス（Protected Device）：セキュアなデバイスを [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で「保護された」ステータスに変更するには、[保護されたデバイス（Protected Device）] をオンにします（[デバイス（Device）] > [電話（Phone）] > [電話の設定（Phone Configuration）]）。
- [セキュア通知トーンの再生（Play Secure Indication Tone）]：保護されたデバイスで、セキュアまたは非セキュア通知トーンの再生を有効にするには、[セキュア通知トーンの再生（Play Secure Indication Tone）] 設定を [はい（True）] に設定します。 （デフォルト設定は [いいえ（False）] です）。 このオプションは、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] の [システム（System）]> [サービス パラメータ（Service Parameters）] で設定します。 サーバを選択してから、Cisco CallManager サービスを選択します。 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、[機能 - セキュア トーン（Feature - Secure Tone）] 領域内にあるオプションを選択します。 （デフォルト設定は [いいえ（False）] です）。

セキュアまたは非セキュア通知トーンは、保護されたデバイスでのみ再生されます。 （保護されていないデバイスではトーンは聞こえません）。 コール中にコール全体のステータスが変化すると、それに従ってインディケーション トーンも変化します。そのとき、保護されたデバイスは対応するトーンを再生します。

次のような状況で、保護されたデバイスはトーンを再生する、または再生しません。

- トーンを再生するオプションを有効にした後で、[セキュア通知トーンの再生（Play Secure Indication Tone）] オプションが有効（[はい（True）]）になります。
  - エンドツーエンドのセキュア メディアが確立され、コール ステータスがセキュアになった場合、デバイスはセキュア インディケーション トーン（間に小休止を伴う 3 回の長いビープ音）を再生します。
  - エンドツーエンドの非セキュア メディアが確立され、コール ステータスが非セキュアになった場合、デバイスは非セキュア インディケーション トーンを再生します（間に短い小休止を伴う 6 回の短いビープ音）。
- [セキュア インディケーション トーンの再生（Play Secure Indication Tone）] オプションが無効になっている場合、トーンは再生されません。

# サービサビリティ

管理者は、デバイスからデバッグ情報を迅速かつ容易に収集できます。

この機能は SSH を使用して、リモートから各電話機にアクセスします。 この機能を使用するには、各 IP フォンの SSH が有効になっている必要があります。

# 共有回線

ユーザは、自分が所有する複数のデバイス間で同じ電話番号を共有したり、同僚との間で電話番号を共有したりすることができます。

詳細については、『*Cisco Unified Communications Manager System Guide*』の「Directory Numbers」の章を参照してください。

# スピード ダイヤル

ユーザは、特定の宛先電話番号にスピード ダイヤルを設定できます。

# 転送

ユーザは、接続されているコールを自分のデバイスから別の番号にリダイレクトできます。

ユーザは 2 つのコールを互いに接続できます。 ユーザは回線に留まることも、回線に留まらずにコールを転送することもできます。

# URI ダイヤル

Uniform Resource Identifier (URI) ダイヤル機能を使用すると、ユーザは英数字の URI アドレス（たとえば、bob@cisco.com）を電話番号として使ってコールを発信できます。 ユーザが連絡先を選択するには、URI アドレスを入力する必要があります。

画面には、URI コールのコール情報が表示されます。 コール ログでは、[通話履歴（Call History）] および [詳細（Details）] ページに URI コールの情報が記録されます。

詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』を参照してください。

## URI ダイヤル機能拡張

電話番号（DN）と URI の両方を使用できるコールを対象とした、デバイスの表示プリファレンスを指定できます。

URI ダイヤル表示プリファレンスが DN に設定されている場合、DN が使用可能な場合は常に DN が表示されます。 URI ダイヤル表示プリファレンスが URI に設定されている場合、URI が使用可能な場合は常に URI が表示されます。

プリファレンスを指定するには、Cisco Unified Communications Manager Administration で、Cisco CallManager サービスの [クラスタ全体のパラメータ（デバイス - 電話機）（Clusterwide Parameters

(Device - Phone)）] ペインに [URI ダイヤル表示設定（URI Dialing Display Preference）] サービス パラメータを設定します。

# ビデオの切り替え

ユーザはビデオ コール中にビデオをオフ/オンに切り替えることができます。

# ボイス メッセージ システム

コールに応答がない場合に、発信者がメッセージを残せるようにします。

詳細については、以下を参照してください。

- 『*Features and Services Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Manager System Guide*』の「Voice Mail Connectivity to Cisco Unified Communications Manager」の章

## Visual Voicemail のセットアップ

ビジュアルボイスメールは、すべてのデバイスに対して、あるいは個別のユーザまたはユーザ グループに対して、[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] から設定されます。すべてのデバイスに対してビジュアルボイスメールを設定する場合は、次の手順を使用します。

### 手順

**ステップ 1** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [デバイスの設定（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（Find）] を選択し、[標準の共通の電話プロファイル（Standard Common Phone Profile）] を選択します。

**ステップ 3** [プロダクト固有の設定（Product Specific Configuration Layout）] ウィンドウで、[ボイスメール サーバ（プライマリ）（Voicemail Server (Primary)）] フィールドに次の情報を入力します。

- Cisco Unified IP Phone スタンドアロン設定で設定する場合は、Cisco Unified IP Phone システムの完全修飾ドメイン名を入力します。
- Cisco Unified IP Phone フェールオーバー設定で設定する場合は、Cisco Unified IP Phone システムの DNS エイリアスを入力します。

**ステップ 4** 変更を保存し、[設定の適用（Apply Config）] をクリックします。

ビジュアル ボイス メールの設定方法と同期する方法の詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Voice-Mail Profile Configuration」の章を参照してください。

## 特定のユーザまたはグループに対するビジュアル ボイス メールの設定

特定のユーザまたはユーザ グループに対してビジュアルボイスメールを設定する場合は、次の手順を使用します。

### 手順

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

**ステップ 2** 検索対象のユーザに関連付けるデバイスを選択します。

**ステップ 3** [プロダクト固有の設定（Product Specific Configuration Layout）] ウィンドウで、[ボイスメール サーバ（プライマリ）（Voicemail Server (Primary)）] フィールドに次の情報を入力します。

- Cisco Unified IP Phone スタンドアロン設定で設定する場合は、Cisco Unified IP Phone システムの完全修飾ドメイン名を入力します。
- Cisco Unified IP Phone フェールオーバー設定で設定する場合は、Cisco Unified IP Phone システムの DNS エイリアスを入力します。

**ステップ 4** 変更を保存し、[設定の適用（Apply Config）] をクリックします。

**ステップ 5** [リセット（Reset）] と [リスタート（Restart）] を選択して、新しい設定をデバイスに配信します。

**ステップ 6** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] からデバイス上のセキュア メッセージを許可するには、[システム設定（System Settings）] > [API の詳細設定（Advanced API Configuration）] を選択し、[CUMIを介したセキュア メッセージ録音へのアクセスを許可する（Allow Access to Secure Message Recordings through CUMI）] と [CUMI 経由のメッセージ添付ファイルを許可する（Allow Message Attachments through CUMI）] の両方を有効にします。

**ステップ 7** ディレクトリの画像をビジュアル ボイス メールに設定するよう Cisco Unified Communications Manager を設定するには、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通デバイス設定（Common Phone Profile）] を選択し、[企業画像ディレクトリ フィールド（Company Photo Directory Field）] に企業の画像ディレクトリの URL を入力します。
ビジュアル ボイス メールの設定方法と同期する方法の詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Voice-Mail Profile Configuration」の章を参照してください。

# 機能ボタン

コール制御バーにある機能と、プログラム可能な機能ボタンとして設定する必要がある機能について次の表で説明します。 この表の「X」は、その機能が対応するボタンのタイプでサポートされることを意味します。 2 つのボタン タイプのうち、[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] での設定が必要となるのは、プログラム可能な機能ボタンだけです。

**表 *19*：機能と対応するボタン**

| 機能名 | コール制御バーのボタン | プログラム可能な機能ボタン |
|---|---|---|
| 折り返し | | X |
| コール転送 | X | |
| すべてのコールの転送 | | X |
| コール パーク | X | |
| コール ピックアップ | | X |
| Cisco Mobility | | X |
| 会議（追加） | X | |
| 転送 | | X |
| サイレント | | X |
| 終了 | X | |
| グループ ピックアップ | | X |
| 保留 | X | |
| ハント グループ | | X |
| インターコム | | X |
| 迷惑呼 ID（MCID） | | X |
| ミートミー | | X |
| プライバシー | | X |
| リダイヤル | | X |

| 機能名 | コール制御バーのボタン | プログラム可能な機能ボタン |
|---|---|---|
| 共有（DX70 および DX80 のみ） | X | |
| スピード ダイヤル | | X |
| ビデオを停止 | | X |
| 転送 | X | |

# 機能管理ポリシーの設定

機能管理ポリシー設定でテレフォニー機能を有効または無効にすることで、Cisco DX シリーズ デバイスでの一部のテレフォニー機能の表示を制限できます。 機能管理ポリシー設定で機能を無効にすると、その機能へのユーザのアクセスが制限されます。

### 手順

**ステップ 1** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [機能管理ポリシー（Feature Control Policy）] を選択します。
[機能管理ポリシーの検索と一覧表示（Find and List Feature Control Policy）] ウィンドウが表示されます。

**ステップ 2** [新規追加（Add New）] をクリックして、一連のポリシーを定義します。

**ステップ 3** 次の設定値を入力します。

- [名前（Name）]：新しい機能管理ポリシーの名前を入力します。
- [説明（Description）]：説明を入力します。
- [機能管理の選択（Feature Control Section）]：デフォルト設定を変更する機能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。

**ステップ 5** 次の設定にポリシーを含めることで、ポリシーを Cisco DX シリーズ デバイスに適用します。

- [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）]：システム内のすべての Cisco DX シリーズ デバイスに適用されます。
- [共通の電話プロファイルの設定（Common Phone Profile Configuration）]：グループ内のすべての Cisco DX シリーズ デバイスに適用されます。
- [電話の設定（Phone Configuration）]：個々の Cisco DX シリーズ デバイスに適用されます。

# 機能管理ポリシーのデフォルト値

次の表に、ユーザが設定できる機能、およびデフォルト値機能のリストを示します。

**表 *20*：機能管理ポリシーのデフォルト値**

| 機能 | デフォルト値 |
|---|---|
| 割込み | 有効 |
| 折り返し | 有効 |
| コール ピックアップ | 無効 |
| 会議リスト | 有効 |
| 転送（アラート） | 無効 |
| 転送（接続） | 無効 |
| 不在転送 | 有効 |
| グループ コール ピックアップ | 無効 |
| ミートミー | 無効 |
| モビリティ | 無効 |
| 他のコール ピックアップ | 無効 |
| パーク | 無効 |
| リダイヤル | 有効 |
| 発信者の報告 | 無効 |
| 品質の報告 | 無効 |
| スピード ダイヤル | 有効 |

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Feature Control Policy Setup」の章を参照してください。

# 電話ボタン テンプレート

電話ボタンテンプレートを使用すると、スピードダイヤルやコール処理機能をプログラム可能なボタンに割り当てることができます。

テンプレートの変更は、可能な限りデバイスをネットワークに登録する前に行ってください。 この順序に従うと、登録の実行中、カスタマイズした電話ボタン テンプレート オプションに Cisco Unified Communications Manager からアクセスできます。

# 電話ボタン テンプレートの変更

電話サービスの詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「IP Phone Services Setup」の章を参照してください。 回線ボタンの設定の詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone Setup」の章および「Configuring Speed-Dial Buttons」の項を参照してください。

### 手順

**ステップ 1** [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [電話ボタンテンプレート（Phone Button Template）] を選択します。

**ステップ 2** [検索（Find）] をクリックします。

**ステップ 3** デバイス モデルを選択します。

**ステップ 4** [コピー（Copy）] を選択し、新しいテンプレートの名前を入力して、[保存（Save）] を選択します。
[電話ボタン テンプレートの設定（Phone Button Template Configuration）] ウィンドウが表示されます。

**ステップ 5** 割り当てるボタンを確認して、機能が表示されるドロップダウン リストから、その回線に関連付ける [サービス URL（Service URL）] を選択します。

**ステップ 6** [保存（Save）] をクリックして、サービス URL を使用する新しい電話ボタン テンプレートを作成します。

**ステップ 7** [デバイス（Device）] > [電話（Phone）] を選択して、デバイスの [電話の設定（Phone Configuration）] ウィンドウを開きます。

**ステップ 8** [電話ボタン テンプレート（Phone Button Template）] ドロップダウン リストから、新しい電話ボタン テンプレートを選択します。

**ステップ 9** [保存（Save）] をクリックして変更を保存し、次に [リセット（Reset）] をクリックして変更を実装します。
これでユーザが、セルフ ケア ポータルにアクセスして、デバイスのボタンにサービスを関連付けられるようになりました。

# 製品固有オプションの設定

[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] では、次のウィンドウでデバイスに対してプロダクト固有の設定パラメータの一部を設定できます。

- [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ（[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]）
- ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 部分にある、[共通の電話プロファイル（Common Phone Profile）] ウィンドウ（[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）]）
- ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 部分にある、[デバイス電話機設定（Device Phone Configuration）] ウィンドウ（[デバイス（Device）] > [電話（Phone）] > [新規追加（Add New）] > [Cisco DX650]、[Cisco DX70]、または [Cisco DX80]）

次の表に、製品固有の設定オプションを示します。

**表 *21*：*Cisco DX* シリーズ 製品固有の設定オプション**

| 機能 | 説明 |
|---|---|
| スピーカーフォンを無効にする（Disable Speakerphone） | スピーカーフォン機能のみ無効にします。スピーカーフォン機能を無効にしても、ヘッドセットには影響しません。ハンドセットまたはヘッドセットで回線とスピード ダイヤルを使用できます。<br>デフォルト：False |
| スピーカーフォンとヘッドセットを無効にする（Disable Speakerphone and Headset） | すべてのスピーカー フォン機能およびヘッドセット マイクを無効にします。<br>デフォルト：False |
| USB の無効化（Disable USB） | デバイスで USB ポートを無効にします。<br>デフォルト：False |
| SDIO | デバイス上の SDIO デバイスが有効になっているか無効になっているかを示します。<br>デフォルト：無効 |
| Bluetooth | デバイス上の Bluetooth サービスが有効になっているか無効になっているかを示します。<br>デフォルト：有効 |
| Bluetooth 連絡先のインポートを許可（Allow Bluetooth Contacts Import） | ユーザは Bluetooth デバイスから連絡先とコール履歴をインポートし、同期できます。<br>デフォルト：有効 |

| 機能 | 説明 |
| --- | --- |
| Bluetooth モバイル ハンズフリーモードを許可（Allow Bluetooth Mobile Handsfree Mode） | ユーザはデスク電話で携帯電話回線を使用できます。<br>デフォルト：有効 |
| ディスプレイ非点灯日（Days Display Not Active） | ユーザは、バックライトをデフォルトでオフのままにする日を指定できます。<br>デフォルト：米国の企業顧客の場合、通常は土曜日と日曜日<br>（注） リストには、曜日すべてが含まれます。 土曜日と日曜日にバックライトをオフにするには、Ctrl キーを押したままにして [土曜日（Saturday）] と [日曜日（Sunday）] を選択します。 |
| ディスプレイ点灯時刻（Display On Time） | オフ スケジュールに一覧表示されている日において、ディスプレイを自動的にオンにする時刻を示します。<br>デフォルト：07:30<br>最大長：5<br>（注） 24 時間形式で入力します。00:00 は一日の始まりで、23:59 が一日の終わりを表します。 |
| ディスプレイ点灯継続時間（Display On Duration） | プログラムされた時刻にディスプレイがオンになった後、ディスプレイのアクティブな状態を保つ時間の長さを示します。<br>デフォルト：10:30<br>最大長：5<br>（注） 最大値は 24 時間です。 この値は、時間と分の形式で指定します。 たとえば、“01:30” では 1 時間 30 分にわたってディスプレイがオンになります。 |
| 着信コール時に点灯（Display On When Incoming Call） | デバイスがスクリーン セーブ モードの場合にこの機能を有効にすると、コールを着信した時点でディスプレイがオンになります。<br>デフォルト：有効 |

| 機能 | 説明 |
| --- | --- |
| Power Save Plus の有効化（Enable Power Save Plus） | Power Save Plus 機能を有効にするには、スケジュールで、デバイスの電源をオフにする日を選択します。 Ctrl キーを押しながら日をクリックすると、Power Save Plus を実行する日を複数選択できます。 Power Save Plus モードでは 1 つのキーを点灯させるだけの電力が維持されます。デバイスのその他の機能はすべてオフになります。 Power Save Plus モードは、[電話をオンにする時刻（Phone On Time）] と [電話をオフにする時刻（Phone Off Time）] フィールドで指定された期間、デバイスをオフにします。 この期間は、通常、組織の通常の運用時間外です。 点灯しているキーをユーザが押すと、デバイスが完全にオンになります。 点灯しているキーを押すと、電話機の電源が再投入され、完全に動作可能になる前に Unified CM に再登録されます。 このフィールドの日を選択すると、次の、E911 の問題を示す通知が表示されます。 Power Save Plus を有効にすることで、この通知で指定された条件に同意します。<br><br>Power Save Plus モードが有効である間は、モードに設定されたエンドポイントは、緊急コールでは無効で、インバウンド コールの受信ができません。 このモードを選択すると、次に同意したことになります。<br><br>**1** このモードが有効である間、非常発着信コールの代替手段を提供するすべての責任をお客様が負うものとします。<br><br>**2** シスコはお客様によるモードの選択に関連する責任を負わず、モードの有効化に関連するすべての責任はお客様が負うものとします。<br><br>**3** コール、発信、およびその他に対するこのモードの影響に関するすべての情報をユーザに通知します。<br><br>デフォルト：選択された日なし |
| 電話機をオンにする時刻（Phone On Time） | このフィールドでは、[Power Save Plusを有効にする（Enable Power Save Plus）] リスト ボックスで選択された日に自動的にデバイスがオンになる時刻を指定します。 時刻を 24 時間形式で入力します。00:00 は午前 0 時を表します。 たとえば、午前 7:00（0700）に電話機を自動的にオンにするには、7:00 と入力します。 午後 2 時（1400）に電話機をオンにするには、14:00 と入力します。このフィールドがブランクの場合、デバイスは 00:00 に自動的にオンになります。<br><br>デフォルト：0:00<br><br>最大長：5 |

| 機能 | 説明 |
| --- | --- |
| 電話機をオフにする時刻（Phone Off Time） | このフィールドは、[Power Save Plusを有効にする（Enable Power Save Plus）] リスト ボックスで選択された日にデバイスがオフになる時刻を指定します。時:分の形式で時間を入力します。このフィールドがブランクの場合、デバイスは午前 0 時（00:00）に自動的にオフになります。<br>（注） [電話をオンにする時刻（Phone On Time）] がブランク（または 00:00）の場合、もしくは [電話をオフにする時刻（Phone Off Time）] がブランク（または 24:00）の場合、EnergyWise でオーバーライドを送信可能にしない限り、デバイスでは実質的に Power Save Plus 機能が無効なままの状態が継続されます。<br>デフォルト：24:00<br>最大長：5 |
| 電話機をオフにするアイドルタイムアウト（Phone Off Idle Timeout） | このフィールドは、デバイスの電源をオンにデバイスが給電側機器（PSE）を要求するまでにデバイスがアイドル状態になっている必要がある分数を表します。 このフィールドの値は、次の場合に有効になります。<br>• デバイスがスケジュールどおりに Power Save Plus モードになっていたが、デバイスのユーザがキーを押したために、Power Save Plus モードが解除された場合。<br>• 接続スイッチでデバイスが再びオンになった場合<br>• [電話をオフにする時刻（Phone Off Time）] になったが、デバイスが使用中の場合。 単位は分です。 デフォルトは 60 です。 指定できる範囲は 20 ～ 1440 です。 |
| 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がオンの場合、[電話をオフにする時刻（Phone Off Time）] フィールドで指定された時刻の 10 分前に音声アラートを再生するようにデバイスに指示します。デフォルトではディセーブルになっています。 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） | このフィールドでは、デバイスが参加している EnergyWise ドメインを定義します。 EnergyWise ドメインは、Power Save Plus 機能で必要となります。 [Power Save Plus の有効化（Enable Power Save Plus）] リスト ボックスで日数を選択した場合は、EnergyWise ドメインを用意する必要があります。 デフォルトは空白です。<br>最大長：127 |

| 機能 | 説明 |
| --- | --- |
| EnergyWise Endpoint Security Secret | このフィールドは、EnergyWise ドメイン内で通信するために使用するパスワード（共有秘密）を定義します。 EnergyWise ドメインと秘密は、Power Save Plus 機能で必要となります。 [Power Save Plus の有効化（Enable Power Save Plus）] リスト ボックスで日数を選択した場合は、EnergyWise ドメインと秘密を用意する必要があります。 デフォルトは空白です。<br>最大長：127 |
| EnergyWise オーバーライドを許可（Allow EnergyWise Overrides） | このチェックボックスにより、電話機に電源レベルの更新を送信するための EnergyWise ドメイン コントローラのポリシーを許可するかどうかを決定します。 次の条件が適用されます。最初に、1 日以上、[Power Save Plus の有効化（Enable Power Save Plus）] フィールドで選択する必要があります。 [Power Save Plus を有効にする（Enable Power Save Plus）] リスト ボックスで日を選択しないと、EnergyWise からのデバイスをオフにする指示は無視されます。 第二に、Unified CM の管理での設定は、EnergyWise がオーバーライドを送信した場合でも、スケジュールどおりに有効になります。たとえば、[ディスプレイをオフにする時刻（Display Off Time）] が 22:00（午後 10 時）に設定されていると仮定すると、[ディスプレイをオンにする時刻（Display On Time）] フィールドの値は 06:00（午前 6 時）となり、[Power Save Plus の有効化（Enable Power Save Plus）] では 1 日以上が選択されています。 20:00（午後 8 時）にデバイスをオフにするように EnergyWise で指示した場合、この指示は、[電話をオンにする時刻（Phone On Time）] で設定された午前 6 時まで有効になります（ユーザによる介入が発生しないと仮定した場合）。午前 6 時になると、デバイスがオンになり、[Unified CM の管理（Unified CM Administration）] で設定された電力レベル変更の受信を再開します。 電力レベルをデバイスで再び変更するには、EnergyWise は電力レベル変更コマンドを新たに再発行する必要があります。 また、すべてのユーザ操作が有効になるため、EnergyWise によりデバイスの電源オフが指示された後でユーザがキーを押すと、その結果としてデバイスの電源がオンになります。 デフォルトでは、オフになっています。 |
| 録音トーン（Recording Tone） | 録音トーンをデバイスで有効にするか無効にするかを設定するために使用できます。<br>デフォルト：無効 |
| 録音トーンのローカル音量(Recording Tone Local Volume) | ローカル通話者が聞く録音トーンの音量を設定するために使用できます。この音量設定は再生に使用される実際のデバイス（ハンドセット、スピーカ フォン、ヘッドセット）に関係なく適用されます。 音量設定は 0% ～ 100% の範囲内でなければなりません。0% ではトーンなし、100% では現在の音量設定と同じレベルになります。 デフォルト値は 100% です。 |

| 機能 | 説明 |
| --- | --- |
| 録音トーンのリモート音量 (RecordingTone Remote Volume) | リモート通話者が聞く録音トーンの音量を設定するために使用できます。音量設定は 0% ～ 100 % の範囲内でなければなりません。0% では -66dBM 未満、100% では -4dBM です。 デフォルト値は -10dBM または 50% です。 |
| 録音トーンの長さ (Recording Tone Duration) | 録音トーンがオーディオストリームに挿入される時間をミリ秒単位で指定します。 このパラメータはデフォルトでこのフィールドのネットワーク ロケール ファイルの値に設定されます。 このパラメータの有効な値の範囲は 1 ～ 3000 ミリ秒です。 |
| G.722 コーデックと iSAC コーデックをアドバタイズする（Advertise G.722 and iSAC Codecs） | コール アプリケーションがワイドバンド コーデックを Cisco Unified Communications Manager にアドバタイズするかどうかを示します。<br>コーデックのネゴシエーションでは、次の 2 つの手順が実行されます。<br>**1** コール アプリケーションは、サポートされるコーデックを Cisco Unified Communications Manager にアドバタイズする必要があります。<br>**2** Cisco Unified Communications Manager が、コール試行に関連するすべてのデバイスからサポートされるコーデックのリストを取得すると、リージョン ペア設定などのさまざまな要因に基づいて一般にサポートされるコーデックが選択されます。<br>[システムデフォルトの使用（Use System Default）]<br>有効な値は、次のとおりです。<br>• [システム デフォルト（System Default）]：コール アプリケーションは、[G.722 コーデックと iSAC コーデックをアドバタイズする（Advertise G.722 and iSAC Codecs）] エンタープライズ パラメータで指定された設定に従います。<br>• [無効（Disabled）]：コール アプリケーションはワイドバンド コーデックを Cisco Unified Communications Manager にアドバタイズしません。<br>• [有効（Enabled）]：コールアプリケーションはワイドバンドコーデックを Cisco Unified Communications Manager にアドバタイズします。 |
| ビデオ コール（Video Calling） | 有効になっている場合、デバイスがビデオ コールに参加することを示します。<br>デフォルト：有効 |

| 機能 | 説明 |
| --- | --- |
| デバイス UI プロファイル（Device UI Profile） | デバイスのユーザ インターフェイスの特性を変更し、特定のユーザ個人（基本ビデオ発信者（簡易モード）または一般コラボレーション ユーザ（拡張モード）など）に合わせて最適化します。<br>デフォルト：シンプル（Simple） |
| Wifi | デバイス上の Wi-Fi が有効になっているか無効になっているかを示します。<br>（注） エンタープライズ設定と共通設定の場合、Wifi パラメータはデフォルト値（有効）に設定され、[共通設定の上書き（Override Common Settings）] チェックボックスがオンにされます。<br>（注） デバイス設定の場合、Wifi パラメータはデフォルト値（Enabled）のままにされますが、[共通設定の上書き（Override Common Settings）] チェックボックスはオンにされません。<br>ヒント シスコは、企業のポリシーですべてのデバイスの WiFi のデフォルトを Disabled に設定する場合を除いて、企業および一般的なレベルの導入環境のデフォルト設定が Disabled になっている場合、WiFi パラメータが Enabled に設定されているデバイスの新しい共通の電話プロファイルを作成することを推奨します。<br>デフォルト：有効 |
| PC ポート（PC Port） | PC ポートを有効にするか無効にするかを指定します。<br>デフォルト：有効 |
| PC ポートへのスパン（Span to PC Port） | PC ポートで送受信されるパケットを転送するかどうかを表示します。<br>（注） 診断目的で使用されるモニタリングと記録用のアプリケーション、ネットワーク パケットキャプチャ ツールなど、デバイス トラフィックのモニタリングを必要とするアプリケーションが PC ポート上で実行されている場合は、[有効（Enabled）] を選択します。 この機能を使用するには、PC ボイス VLAN へのアクセスを有効にする必要があります。<br>デフォルト：無効 |
| PC Voice VLAN へのアクセス（PC Voice VLAN Access） | PC ポートに接続されているデバイスがボイス VLAN へのアクセスを許可されるかどうかを示します。<br>（注） ボイス VLAN アクセスを無効にすると、接続されている PC でボイス VLAN 上のデータを送受信できなくなります。 また、デバイスで送受信されたデータを PC で受信することもできなくなります。<br>デフォルト：有効 |

| 機能 | 説明 |
| --- | --- |
| PC ポートのリモート設定（PC Port Remote Configuration） | デバイスの PC ポートの速度とデュプレックスのリモート設定を許可します。<br>デフォルト：無効 |
| スイッチポートのリモート設定（Switch Port Remote Configuration） | デバイスのスイッチポートの速度とデュプレックスのリモート設定を許可します。 これは、デバイス上での手動設定よりも優先されます。<br>デフォルト：無効 |
| Unified CM 接続障害の検出（Detect Unified CM Connection Failure） | このフィールドでは、Unified CM/SRST のバックアップへのデバイスのフェールオーバーが発生する前の最初のステップである、Cisco Unified Communications Manager（Unified CM）への接続障害を検出するための電話機の感度を決定します。 有効な値は [標準（Normal）]（Unified CM 接続障害の標準システム レートで発生の検出）または [遅延（Delayed）]（Unified CM 接続のフェールオーバーの、通常よりも約 4 倍の遅延での発生の検出）を指定します。 Unified CM 接続エラーの高速認識のためには、[標準（Normal）] を選択します。 接続を再確立できるようするためにフェールオーバーを少し遅らせる場合は、[遅延（Delayed）] を選択します。 [標準（Normal）] と [遅延（Delayed）] の接続エラー検出の正確な時間の差は、常に変化する多数の変数に応じて異なります。 これは、有線イーサネット接続にだけ適用されます。<br>デフォルト：標準（Normal） |
| Gratuitous ARP | デバイスが Gratuitous ARP 応答から MAC アドレスを学習するかどうかを示します。<br>（注） Gratuitous ARP を受信するデバイス機能を無効にすると、この仕組みを使って音声ストリームのモニタリングおよび記録を行うアプリケーションが機能しなくなります。<br>デフォルト：無効 |
| Cisco Discovery Protocol（CDP）：スイッチ ポート（Cisco Discovery Protocol (CDP): Switch Port） | 管理者は、スイッチ ポート上で CDP を有効または無効にできます。<br>警告 デバイスがシスコ以外のスイッチに接続する場合にのみ、ネットワーク ポート上で CDP を無効にします。 詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。<br>デフォルト：有効 |
| Cisco Discovery Protocol（CDP）：PC ポート（Cisco Discovery Protocol (CDP): PC Port） | CDP が PC ポートでサポートされるかどうかを示します。<br>デフォルト：有効 |

| 機能 | 説明 |
| --- | --- |
| Link Layer Discovery Protocol - Media Endpoint Discover（LLDP-MED）：スイッチポート（Link Layer Discovery Protocol - Media Endpoint Discover（LLDP-MED）：Switch Port） | 管理者は、スイッチポート上でリンク層検出プロトコル（LLDP-MED）を有効または無効にできます。<br>デフォルト：有効 |
| Link Layer Discovery Protocol（LLDP）：PC ポート（Link Layer Discovery Protocol（LLDP）：PC Port） | 管理者は、PC ポート上でリンク層検出プロトコル（LLDP）を有効または無効にできます。<br>デフォルト：有効 |
| LLDP アセット ID(LLDP Asset ID) | 管理者は、リンク層検出プロトコル用のアセット ID を設定できます。<br>最大長：32 |
| LLDP 電源優先度（LLDP Power Priority） | 管理者は、リンク層検出プロトコル用の電源優先度を設定できます。<br>デフォルト：不明 |
| 電力ネゴシエーション（Power Negotiation） | 管理者は、電力ネゴシエーションを有効または無効にできます。<br>（注） 電力ネゴシエーション機能は、電力ネゴシエーションをサポートしているスイッチにデバイスが接続されると有効になります。一方、スイッチが電力ネゴシエーションに対応していない場合は、アクセサリの電源を PoE+ で投入する前に、電力ネゴシエーション機能を無効にしてください。<br>デフォルト：有効 |
| 自動ポート同期(Automatic Port Synchronization) | 電話で PC ポートおよび SW ポートを同じ速度およびデュプレックスに同期することを有効にします。 自動ネゴシエート用に設定されたポートだけが速度を変更します。<br>デフォルト：無効 |

| 機能 | 説明 |
| --- | --- |
| 802.1X 認証（802.1x Authentication） | 802.1x 認証機能のステータスを指定します。 オプション<br>• [有効（Enabled]：デバイスは 802.1X 認証を使用してネットワーク アクセスを要求します。<br>• [無効（Disabled）]：デフォルト設定。デバイスは CDP を使用して VLAN およびネットワークにアクセスします。<br>デフォルト：ユーザ制御 |
| 常時 VPN（Always On VPN） | 常にデバイスが VPN AnyConnect クライアントを起動し、Cisco Unified Communications Manager の設定済みの VPN プロファイルで接続を確立するかどうかを示します。<br>デフォルト：False |
| デバイス上に VPN パスワードを保存（Store VPN Password on Device） | このパラメータは VPN パスワードがデバイスに保存できるかどうかを制御します。 この値はパスワード永続性が連携できるように設定されている場合にのみ使用されます。 無効の場合、ユーザの VPN パスワードはメモリに格納され、以降の接続で自動的に再送信されます。ただし、デバイスの再起動時は、VPN パスワードを再入力する必要があります。 有効の場合、ユーザの VPN パスワードはデバイスに保存され、再起動時も保持されます。<br>デフォルト：False |
| ユーザ定義 VPN プロファイルの許可（Allow User-Defined VPN Profiles） | ユーザが AnyConnect VPN クライアントを使用して VPN プロファイルを作成できるかどうかを制御します。 無効にすると、ユーザは VPN プロファイルを作成できません。<br>デフォルト：True |
| 画面ロックが必要（Require Screen Lock） | デバイス上で画面ロックが必要かどうかを示します。 オプション<br>• ユーザ制御。<br>• PIN：数字のパスワードで、少なくとも 4 桁の長さが必要です。<br>• パスワード（Password）：英数字のパスワード。4 文字以上の英数字で構成され、そのうちの 1 文字は数字以外の文字とし、さらに 1 文字は大文字にする必要があります。<br>デフォルト：PIN |

| 機能 | 説明 |
|---|---|
| 画面ロック タイムアウトの最大値（Maximum Screen Lock Timeout） | デバイスによって画面が自動的にロックされるまでの最大アイドル時間を秒単位で示します。 画面がロックされると、画面のロックを解除する際にユーザ パスワードが要求されます。<br>デフォルト：600<br>最小値：15<br>最大値：1800 |
| ディスプレイがオンの時刻に画面ロックを強制（Enforce Screen Lock During Display-On Time） | このパラメータは、Cisco Unified Communications Manager で設定された期間後もデバイスがロックされないような、ユーザが業務時間全体でこれらのデバイスを自由に使用できる、消極的なロック ポリシーを提供します。作業後、デバイスはポリシーの定義に従ってロックし、権限のないユーザがアクセスすることを防ぎます。 デバイスは、会議または昼休みのためのユーザ制御の手動ロック オプション（電源ボタン）を常にサポートしています。 デバイスは、ユーザが次の使用時にPIN/パスワードを入力するまでロックされたままとなります。 [オン（ON）] : デバイスは業務時間中またはディスプレイ点灯時刻の間はロックされます（デフォルト設定）。 [オフ（OFF）] : デバイスは、ディスプレイ消灯時刻または業務時間後のみに、上に示されている日付/時刻設定に基づいてロックされます。<br>デフォルト：True<br>（注） このパラメータを無効にすると、デバイスにインストールされているロック画面のタイムアウトに関連するサードパーティ デバイス管理ポリシーがすべてオーバーライドされます。 |
| 音声コール中のデバイスのロック（Lock Device During Audio Call） | デバイスが充電状態になり、アクティブな音声コールが行われている場合、管理者は画面ロック PIN 強制タイマーをオーバライドし、音声コール中は画面をアクティブなままにすることができます。 画面ロック タイマーは音声コールが完了し、タイマーの時間を超過すると有効になります。<br>デフォルト：無効 |
| Kerberos サーバ（Kerberos Server） | Web プロキシ Kerberos の認証サーバ。<br>最大長：256 |
| Kerberos レルム (Kerberos Realm) | Kerberos Web プロキシの認証レルム。<br>最大長：256 |
| ロード サーバ(Load Server) | デバイスが、定義されている TFTP サーバではなく、代替サーバを使用して、ファームウェア ロードとアップグレードを取得することを示します。<br>デフォルト：ローカル サーバのホスト名または IP アドレス<br>最大長：256 |

| 機能 | 説明 |
| --- | --- |
| ピア ファームウェア共有(Peer Firmware sharing) | サブネット内の 1 台のデバイスがイメージ ファームウェア ファイルを取得し、それを各ピアに配布できるようにするためのピアツーピア イメージ配信を有効または無効にします。<br>デフォルト：有効 |
| ログ サーバ(Log Server) | ログ メッセージの送信先となるリモート システムの IP アドレスとポートを指定します。<br>デフォルト：リモート システムの IP アドレス。<br>最大長：32 |
| ログのプロファイル（Log Profile） | 事前定義されたデバッグ コマンドをリモートで実行します。<br>デフォルト：プリセット |
| Web アクセス（Web Access） | デバイスが Web ブラウザまたはその他の HTTP クライアントからの接続を受け入れるかどうかを示します。<br>デフォルト：無効 |
| SSH アクセス（SSH Access） | このパラメータは、デバイスが SSH 接続を受け入れるかどうかを示します。 デバイスの SSH サーバ機能を無効にすると、デバイスへのアクセスはブロックされます。<br>デフォルト：無効 |
| Android Debug Bridge (ADB) | デバイス上で ADB を有効または無効にします。<br>[有効（Enabled）]、[無効（Disabled）]、または [ユーザ制御（User Controlled）] に設定できます。<br>デフォルト：無効 |
| マルチユーザ（Multi-User） | デバイスのマルチユーザが有効になっているか無効になっているかを示します。<br>デフォルト：無効 |
| 未知の提供元からのアプリケーションを許可（Allow Applications from Unknown Sources） | URL から、あるいは電子メール、インスタント メッセージ（IM）、または Secure Digital（SD）カード経由で受け取った Android アプリケーション パッケージ ファイル（APK）から、ユーザが Android アプリケーションをデバイス上にインストールできるかどうかを制御します。<br>[有効（Enabled）]、[無効（Disabled）]、または [ユーザ制御（User Controlled）] に設定できます。<br>デフォルト：無効 |

| 機能 | 説明 |
| --- | --- |
| Google Play からのアプリケーションを許可（Allow Applications from Google Play） | ユーザが Google Play から Android アプリケーションをインストールできるかどうかを制御します。<br>（注） Google Play にあるアプリケーションによっては、GPS または背面カメラなどの Cisco DX シリーズデバイスで利用できないハードウェア要件がある場合があります。 シスコはサードパーティのサイトからダウンロードされたアプリケーションの動作を保証しません。<br>デフォルト：False |
| Cisco UCM アプリケーションクライアントの有効化（Enable Cisco UCM App Client） | アプリケーション クライアントがデバイス上で動作するかどうかを制御します。 アプリケーション クライアントが有効になっている場合、ユーザは、Cisco Unified Communications Manager からインストールするアプリケーションを選択できます。<br>デフォルト：False |
| 背景イメージ（Background Image） | このパラメータは、デフォルトの壁紙ファイルを指定します。 このパラメータを有効にすると、管理者だけが、電話機の壁紙リストへのエンドユーザ アクセスを無効にできます。<br>最大長：64 |
| 企業画像ディレクトリ（Company Photo Directory） | デバイスがユーザを問い合わせ、そのユーザの画像を取得できる URL を指定します。<br>例：http://www.cisco.com/dir/photo/zoom/%%uid%%（uid は従業員のユーザ ID です）<br>デフォルト：画像ディレクトリ URL<br>最大長：256 |
| ボイスメールサーバ（プライマリ）（Voicemail Server (Primary)） | プライマリ ビジュアル ボイスメール サーバのホスト名または IP アドレス。<br>デフォルト：プライマリ ビジュアル ボイスメール サーバの IP アドレス。<br>最大長：256 |
| ボイスメールサーバ（バックアップ）（Voicemail Server (Backup)） | バックアップ ビジュアル ボイスメール サーバのホスト名または IP アドレス。<br>デフォルト：バックアップ ビジュアル ボイスメール サーバの IP アドレス。<br>最大長：256 |

| 機能 | 説明 |
| --- | --- |
| プレゼンスとチャットのサーバ（プライマリ）（Presence and Chat Server (Primary)） | プライマリ プレゼンス サーバのホスト名または IP アドレス。<br>デフォルト：プライマリ プレゼンス サーバの IP アドレス。<br>最大長：256 |
| プレゼンスとチャットのサーバのタイプ（Presence and Chat Server Type） | デバイスが使用するプレゼンスおよび IM のセカンダリ サーバのタイプを指定します。<br>[Cisco Unified Presence] または [Cisco WebEx Connect] に設定できます。<br>デフォルト：Cisco WebEx Connect |
| プレゼンスとチャットのシングルサインオン（SSO）ドメイン（Presence and Chat Single Sign-On (SSO) Domain） | 企業に対するシングルサインオン（SSO）認証を実施するために Cisco WebEx Connect Cloud で使用されるエンタープライズ ドメイン。<br>デフォルト：空白フィールド<br>最大長：256 |
| マルチ ユーザ URL（Multi-User URL） | このパラメータは、エクステンション モビリティ サーバの URL を指定します。<br>最大長：256 |
| Expressway サインインに対するユーザ クレデンシャルの永続性（User Credentials Persistent for Expressway Sign In） | このパラメータは、Expressway クレデンシャルをデバイスに保存できるかどうかを制御します。<br>デフォルト：無効 |
| カスタマーサポートのアップロードURL（Customer support upload URL） | ユーザがエンドポイントの「問題レポート ツール」から問題レポート ファイルを送信できる、送信先サーバ アドレスを設定します。<br>最大長：256 |

（注） 設定の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

### [共通設定の上書き（Override Common Settings）] チェックボックス

パラメータを設定した後、更新する設定ごとに [共通設定の上書き（Override Common Settings）] チェックボックスをオンにします。 このチェックボックスをオンにしないと、対応するパラメータ設定が有効になりません。 3 つの設定ウィンドウでパラメータを設定した場合、設定の優先順序は次のとおりです。

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

# ビデオ送信解像度のセットアップ

Cisco DX シリーズ デバイスは、高解像度マルチタッチ カラー LCD と内蔵カメラを介してビデオコールをサポートします。 デバイスでビデオを送受信するには、Cisco Unified Communications Manager でビデオ機能を有効にする必要があります。

（注） [ビデオ コール（Video Calls）] オプションが [オフ（Off）] に設定されていると、[ビデオの自動転送（Auto Transmit Video）] がグレー表示されます。 [通話設定（Call settings）] メニューの下にあるすべてのビデオ設定は、[プロダクト固有の設定（Product Specific Configuration Layout）] ウィンドウで [ビデオ コール（Video Calling）] が無効になっているとグレー表示されます。

**表 *22*：ビデオ送信解像度と機能**

| ビデオのタイプ | ビデオ解像度 | FPS | ビデオ ビット レート（帯域幅） | DX650 外部カメラ サポート |
|---|---|---|---|---|
| 240p | 432 X 240 | 15 | 64 ～ 149 kbps | はい。ただし、Logitech C930e では 424 x 240 の解像度を使用します。 |
| 240p | 432 X 240 | 30 | 150 ～ 299 kbps | はい。ただし、Logitech C930e では 424 x 240 の解像度を使用します。 |
| 360p | 640 X 360 | 30 | 300 ～ 599 kbps | はい |

| ビデオのタイプ | ビデオ解像度 | FPS | ビデオ ビット レート（帯域幅） | DX650 外部カメラ サポート |
|---|---|---|---|---|
| 480p | 848 X 480 | 30 | 600 ～ 799 kbps | はい。ただし、Logitech C920-C では 864 X 480 の解像度を使用します。 |
| 576p | 1024 X 576 | 30 | 800 ～ 1299 kbps | はい |
| 600p | 1024 X 600 | 30 | 800 ～ 3000 kbps | いいえ |
| 720p | 1280 X 720 | 30 | 900 ～ 1999 kbps | はい |
| 1080p | 1920 X 1080 | 30 | 2000 ～ 4000 kbps | はい |
| CIF | 352 X 288（4:3） | 30 | 64 ～ 299 kbps | はい |
| VGA | 640 X 480（4:3） | 30 | 400 ～ 1500 kbps | はい |

（注） 外部カメラは、600p などのこれらの一部の解像度をサポートしません。外部カメラが実行できる最小ビット レートは 64 kbps です。

（注） Cisco DX650 が Logitech C920-C Webcam を使ってコールを実行し、リモート デバイスがパケット化モード 0 だけをサポートする場合、最大送信解像度は 640 X 360 です。 パケット化モード 1 を使用する場合、最大送信解像度は 1920 X 1080 です。

（注） Cisco DX シリーズ デバイスの VGA での最適解像度は w360p です。400 kbps ～ 999 kbps までの帯域幅の場合、デバイスは w360p を送信します。

# インスタントメッセージングとプレゼンスのセットアップ

インスタント メッセージおよびプレゼンスを使用すると、ユーザは、時間、場所、デバイスを問わず通信できるようになります。 Cisco DX シリーズ デバイスは Cisco Unified Presence または WebEx バック エンド サーバのどちらかで Jabber IM をサポートします。 セキュリティ上の理由から、クラウドベースの IM およびプレゼンス トラフィックは、プロキシ経由でルーティングされます。

インスタントメッセージングとプレゼンスは、デバイスの[プロダクト固有の設定（Product Specific Configuration）]ウィンドウにおいてデバイス レベル、グループ レベル、またはエンタープライズ レベルで設定されます。プレゼンスと IM のサーバ（プライマリ）およびプレゼンスと IM のサーバ（バックアップ）のホスト名または IP アドレスを入力し、プレゼンスと IM のサーバのタイプを指定します。

# アプリケーションの設定

ユーザは、アプリケーションをダウンロードして、デバイスの機能をカスタマイズしたり、拡張したりできます。アプリケーションは、Google Play から入手できます。[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）]は、次のパラメータ（[プロダクト固有の設定（Product Specific Configuration）] ウィンドウ内）の設定を通じてアプリケーションへのアクセスを提供します。

- [未知の提供元からのアプリケーションを許可（Allow Applications from Unknown Sources）]：ユーザが Google Play 以外の提供元からアプリケーションをインストール可能かどうかを制御します。
- [Google Play からのアプリケーションを許可（Allow Applications from Google Play）]: Google Play からユーザがアプリケーションをインストールする機能を制御します。
- Cisco UCM アプリケーション クライアントの有効化（Enable Cisco UCM App Client）: Cisco Unified Communications Manager からアプリケーションをプッシュする管理者機能を制御します。

  UCM アプリケーションは、Cisco Unified Communications Manager で作成された Android アプリケーションの登録、または登録解除に使用できるデバイス上のクライアントです。このクライアントは、Cisco Unified Communications Manager からの Android アプリケーションの登録または登録解除と同じ機能を提供しますが、デバイスからこれを実行することができるようになります。

## Cisco UCM アプリケーション クライアントの有効化

### 手順

**ステップ 1** [デバイス設定（Device Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）]セクションで、[Cisco UCM アプリケーション クライアントの有効化（Enable Cisco UCM App Client）] 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** [設定の適用（Apply Config）] をクリックします。
この操作によって、デバイスに UCM アプリケーション クライアントをインストールします。

UCM アプリケーション クライアントがデバイスにインストールされると、デバイス ユーザは UCM アプリケーション クライアントログインするときに Cisco Unified Communications Manager に作成されるアプリケーションを登録、または登録解除できます。

# UCM アプリケーションにログインするエンド ユーザの作成

エンド ユーザが UCM アプリケーションにログインできるように、管理者は、エンド ユーザを作成してデバイスに関連付け、デバイスの所有者として割り当てる必要があります。

### 手順

**ステップ 1** エンド ユーザを作成します。（新規エンド ユーザを作成するには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[ユーザ管理（User Management）] > [エンドユーザ（End User） を選択します。）

**ステップ 2** [制御するデバイス（Controlled Devices）] でデバイスがエンドユーザに対して表示されるように、エンド ユーザとデバイスを関連付けます。

**ステップ 3** エンド ユーザに標準 CCM エンド ユーザに権限を割り当てます。

**ステップ 4** デバイスの [デバイス設定（Device Configuration）] ウィンドウで、[オーナーのユーザ ID（Owner User ID）] フィールドに、このエンド ユーザを割り当てます。

# UCM アプリケーションでのユーザ登録

デバイスのユーザは、デバイスで UCM アプリケーションを使用して、Cisco Unified Communications Manager で作成されたアプリケーションを登録および登録解除します。

### 手順

**ステップ 1** エンド ユーザ資格情報を使用して、デバイスで UCM アプリケーションにログインします。
ログイン成功時に UCM アプリケーションは、Cisco Unified Communications Manager で作成されたすべての Android アプリケーションを表示します。

**ステップ 2** アプリケーションへの登録を行うには、アプリケーション名の横にあるチェックボックスをオンにします。
この操作は、デバイスのアプリケーションのダウンロードとインストールをトリガーします。

（注） アプリケーションによっては最新の詳細情報をユーザに表示します。 チェックボックスをオンにするか、またはアプリケーションを選択すると、ユーザに2番目の画面が表示されます。 これらのアプリケーションを登録するには、2番目の画面のボックスをオンにし、[戻る（Back）]をタップします。 この操作によって、インストールが開始します。

**ステップ 3** アプリケーションの登録を解除するには、アプリケーション名の横のチェックボックスをオフにします。

# Unified Communications Manager からの Android APK ファイルのプッシュ

Cisco Unified Communications Manager から Android APK ファイルをプッシュするには、まずアプリケーションを電話機サービスとして設定し、サービスにデバイスを登録します。

### 手順

**ステップ 1** 次の apktool を使用して APK から AndroidManifest ファイルを抽出します。
http://code.google.com/p/android-apktool/

**ステップ 2** [Cisco Unified CM の管理（Cisco Unified Communications ManagerAdministration）] で Android サービスを追加します。

**ステップ 3** Android サービスにデバイスを登録します。

# Cisco Unified Communications Manager Administration での Android サービスの追加

Cisco Unified Communications Manager Administration で Android サービスを追加するには、次の手順に従います。

### はじめる前に

APK から AndroidManifest ファイルを取得した後で、この手順を使用します。

### 手順

**ステップ 1** Cisco Unified Communications Manager Administration で、[デバイス（Device）] > [デバイスの設定（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** [サービス名（Service Name）] フィールドに、APK から抽出された AndroidManifest ファイルのパッケージ名と一致する名前を入力します。

**ステップ 4** [サービスカテゴリ（Service Category）] ドロップダウン リスト ボックスで、[Android APK] を選択します。

**ステップ 5** このウィンドウのその他のフィールドは任意です。AndroidManifest ファイルに表示される情報を入力できます。

**ステップ 6** [有効（Enable）] 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。

# Android Phone サービスへのデバイスの登録

### はじめる前に

Android Phone サービスにデバイスを登録する前に、Android Phone サービスを Cisco Unified Communications Manager に追加する必要があります。

### 手順

**ステップ 1** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、[デバイス（Device）] > [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）] ウィンドウに、Android Phone サービスに登録するデバイスが表示されます。

**ステップ 3** ユーザが選択したデバイスの [デバイス名（Device Name）] エントリをクリックします。

**ステップ 4** [電話の設定（Phone Configuration）] ウィンドウで、[関連リンク（Related Links）] ドロップ ダウン リスト ボックスから、[サービスの登録/登録解除（Subscribe/Unsubscribe Services）] を選択します。
そのデバイスの [登録済みの Cisco IP Phone サービス（Subscribed Cisco IP Phone Services）] ウィンドウが表示されます。

**ステップ 5** そのデバイスの [登録済みの Cisco IP Phone サービス（Subscribed Cisco IP Phone Services）] ウィンドウで、[サービスの選択（Select a Service）] ドロップ ダウン リスト ボックスから作成したサービスを選択します。

この操作は、指定したサービスへのデバイスの登録をトリガーします。

**ステップ 6** [次へ（Next）] をクリックします。

**ステップ 7** [登録（Subscribe）] をクリックします。

第 11 章

# カスタマイゼーション


- 設定ファイルのカスタマイズおよび変更，155 ページ
- ワイドバンド コーデックのセットアップ，156 ページ
- 動作モード，156 ページ
- デフォルトの壁紙，158 ページ
- SSH アクセス，160 ページ
- Unified Communications Manager Endpoints Locale インストーラ，160 ページ
- 国際コールのロギングのサポート，161 ページ


## 設定ファイルのカスタマイズおよび変更

設定ファイルを修正して（たとえば、XML ファイルを編集して）、カスタマイズしたファイル（たとえば、独自の呼出トーンや、折返しトーン）を TFTP ディレクトリに追加することができます。 ファイルの修正、およびカスタマイズしたファイルの TFTP ディレクトリへの追加は、Cisco Unified Communications オペレーティング システムの管理ページの、TFTP サーバ ファイルのアップロード ウィンドウから実行できます。 Cisco Unified Communications Manager サーバ上の TFTP フォルダにファイルをアップロードする方法については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

システムから Ringlist.xml ファイルと List.xml ファイルのコピーを取得するには、次の管理コマンドライン インターフェイス（CLI）file コマンドを使用できます。 正確な構文については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

- admin:file
  - file list
  - file view
  - file search

- file get
- file dump
- file tail
- file delete

# ワイドバンド コーデックのセットアップ

デフォルトでは、G.722 コーデックがCisco DX シリーズ デバイスで有効になります。 Cisco Unified Communications Manager が G.722 を使用するよう設定されており、通話先エンドポイントが G.722 をサポートしている場合、G.711 の代わりに G.722 コーデックを使ってコールが接続されます。

この状態は、ユーザがワイドバンドヘッドセットまたはワイドバンドハンドセットを有効にしているかどうかを問わず発生します。ヘッドセットまたはハンドセットが有効になっている場合、ユーザはコール中の音声の感度がより高く感じられます。 感度が高いことで音声の明瞭さは増しますが、紙が擦れる音や近くの会話など、背景のノイズも通話相手によく聞こえるようになります。 ワイドバンド ヘッドセットまたはハンドセットがない場合でも、G.722 の高い感度を好むユーザもいます。 ユーザの中には G.722 の高い感度を好まないユーザもいます。

[アドバタイズ G.722 コーデック（Advertise G.722 Codec）] サービス パラメータは、この Cisco Unified Communications Manager サーバまたは特定のデバイスに登録するすべてのデバイス関してワイドバンドがサポートされるかどうかに影響を与えます。Cisco Unified Communications Manager 管理ウィンドウで次のようにパラメータを設定します。

- [アドバタイズ G.722 コーデック（Advertise G.722 Codec）] フィールド：Cisco Unified Communications Manager の管理ページで、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] を選択します。 このエンタープライズ パラメータのデフォルト値は True です。これは、この Cisco Unified Communications Manager に登録されているすべての Cisco DX シリーズ デバイスが Cisco Unified Communications Manager に G.722 をアドバタイズすることを意味します。 通話元と通話先のそれぞれの機能セットで G.722 がサポートされている場合、Cisco Unified Communications Manager は可能な限りこのコーデックを選択します。
- 特定のデバイスでG.722 コーデックをアドバタイズする：Cisco Unified Communications Manager Administration で、[デバイス（Device）] > [電話（Phone）] を選択します。 この製品固有のパラメータのデフォルト値には、エンタープライズパラメータで指定されている値を使用します。 デバイス単位でこのパラメータを上書きするには、[電話の設定（Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific configuration）] 領域にある [アドバタイズ G.722 コーデック（Advertise G.722 Codec）] パラメータで、[有効（Enabled）] または [無効（Disabled）] を選択します。

# 動作モード

Cisco DX シリーズ デバイスは、異なるモードで機能します。

- パブリック モード
- 簡易モード
- 拡張モード

デフォルトは、簡易モードです。

次の表に、各モードでユーザが使用できる機能を示します。

| 機能 | パブリック モード | 簡易モード | 拡張モード |
|---|---|---|---|
| アプリケーションの呼び出し | はい | はい | はい |
| 画面のロック | いいえ | はい | はい |
| ネットワークの設定 | いいえ | はい | はい |
| ホーム画面 | いいえ | はい | はい |
| ウィジェットとショートカットの追加または削除 | いいえ | はい | はい |
| 表示によるボイスメール | いいえ | はい | はい |
| シスコ ユーザ データ サービス | はい | はい | はい |
| Bluetooth | はい | はい | はい |
| 日付と時刻の設定 | いいえ | はい | はい |
| 最近使用したアプリケーションのリスト | いいえ | はい | はい |
| 外部ストレージ デバイス | いいえ | いいえ | はい |
| Jabber IM | いいえ | いいえ | はい |
| Android アプリケーション | いいえ | いいえ | はい |

# 動作モードの設定

### はじめる前に

簡易モードまたはパブリック モードのデバイスでは、Android Debug Bridge（ADB）を無効にすることを推奨します。 これは、簡易モードまたはパブリック モードでメール アプリケーションが無効になっているため、ユーザは Problem Report Tool を使用して管理者にログを電子メールで送信できないためです。 ログは、サービスアビリティ Web ページから収集する必要があります。

手順

**ステップ 1** Cisco Unified Communications Manager サーバーに、最新のデバイス パックをインストールします。デバイス パックのインストールの詳細については、『*Release Notes for Cisco DX Series*』を参照してください。

**ステップ 2** [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウ、[共通の電話プロファイル（Common Phone Profile）] ウィンドウ、または [電話の設定（Phone Configuration）] ウィンドウで、[デバイス UI プロファイル（Device UI Profile）] を使用するモードに設定します。

**ステップ 3** [共通設定の上書き（Override Common Settings.）] をオンにします。
拡張モードからパブリック モードまたは簡易モードに切り替えると、デバイスが再起動します。パブリック モードまたは簡易モードから拡張モードに切り替えるときも、デバイスが再起動します。 パブリック モードと簡易モード間での切替えでは、デバイスは再起動しません。

# デフォルトの壁紙

デバイスの[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] ページから、ユーザと管理者のいずれがデバイスにデフォルトの壁紙を設定できるかを制御できます。

## 壁紙管理の割り当て

デフォルトでは、ユーザがデバイスの壁紙を変更できます。

手順

**ステップ 1** [デバイス（Device）]>[デバイスの設定（Device Settings）]>[共通の電話プロファイル（Common Phone Profile）]に移動します。

**ステップ 2** 壁紙の管理を管理者に制限するためには、[ユーザの電話の壁紙画像設定へのアクセスを有効にする（Enable End User Access to Phone Background Image Settings）] をオフにします。

## デフォルトの壁紙の指定（DX70 および DX80）

Cisco DX70 および DX80 の壁紙のイメージ解像度を 2985 X 1280 にすることを推奨します。 デバイスはイメージを 2985 X 1080 にトリミングするので、2985 X 1280 のイメージの上下 100 ピクセルはデバイスに表示されません。 壁紙は 5 つの画面にまたがっており、各画面の幅は 1920 ピクセルです。

### 手順

**ステップ 1** TFTP サービスを実行しているすべてのノードの デスクトップ/1600 X 1280 X 24 フォルダに壁紙のイメージをアップロードします。

**ステップ 2** TFTP を実行しているすべてのノードで TFTP サービスを再起動します。

**ステップ 3** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] の [DX70 および DX80 の共通の電話プロファイル（DX70 and DX80 Common Phone Profile）] に移動し、次の変更を行います。

a) [背景イメージ設定へのアクセスの有効化（Enable End User Access to Phone Background Image Setting）] をオフにします。
b) [背景イメージ（Background Images）] に壁紙イメージのファイル名を入力します。
c) [共通設定の上書き（Override Common Settings）] をオンにします。

**ステップ 4** 設定を保存して、共通の電話プロファイルに適用します。

**ステップ 5** 電話デバイス ページに移動し、壁紙をロードするデバイスに設定を適用します。
大規模なエンドポイント ネットワークがある場合は、すべてのエンドポイントがイメージを取得できるように、すべてのデバイスに設定を適用するか、Cisco Unified Communications Manager サーバを再起動します。

# デフォルトの壁紙の指定（DX650）

Cisco DX650 の壁紙のイメージ解像度を 1600x1280 にすることを推奨します。 デバイスはイメージを 1600x600 にトリミングするので、1600x1280 のイメージの上下 340 ピクセルはデバイスに表示されません。 壁紙は 5 つの画面にまたがっており、各画面の幅は 1024 ピクセルです。

### 手順

**ステップ 1** TFTP サービスを実行しているすべてのノードの デスクトップ/1600x1280x24 フォルダに壁紙のイメージをアップロードします。

**ステップ 2** TFTP を実行しているすべてのノードで TFTP サービスを再起動します。

**ステップ 3** [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] の [DX650 の共通の電話プロファイルル（DX650 Common Phone Profile）] に移動し、次の変更を行います。

a) [背景イメージ設定へのアクセスの有効化（Enable End User Access to Phone Background Image Setting）] をオフにします。
b) [背景イメージ（Background Images）] に壁紙イメージのファイル名を入力します。
c) [共通設定の上書き（Override Common Settings.）] をオンにします。

**ステップ 4** 設定を保存して、共通の電話プロファイルに適用します。

**ステップ 5** 電話デバイス ページに移動し、壁紙をロードするデバイスに設定を適用します。

大規模なエンドポイント ネットワークがある場合は、すべてのエンドポイントがイメージを取得できるように、すべてのデバイスに設定を適用するか、Cisco Unified Communications Manager サーバを再起動します。

# SSH アクセス

ポート 22 を経由する SSH デーモンへのアクセスを有効または無効にすることができます。 ポート 22 を開いたままにすると、デバイスがサービス拒否（DoS）の攻撃に対して脆弱になります。 デフォルトでは、SSH ドメインは無効になっています。

SSH アクセスにより、次の順で、2 つのクレデンシャルを入力するよう要求されます。

1. Cisco Unified Communications Manager 設定の [セキュア シェル情報（Secure Shell Information）] セクション内の [セキュアシェルユーザ（Secure Shell User）] および [セキュアシェルパスワード（Secure Shell Password）]
2. デバッグのユーザ ID とパスワード

[SSH アクセス（SSH Access）] フィールドは、次のウィンドウにあります。

- [共通の電話プロファイルの設定（Common Phone Profile Configuration）]（[デバイス（Device）] >[デバイスの設定（Device Settings）]>[共通の電話プロファイル（Common Phone Profile）]）
- [電話の設定（Phone Configuration）]（[デバイス（Device）]>[電話（Phone）] ウィンドウ）

# Unified Communications Manager Endpoints Locale インストーラ

デフォルトでは、デバイスでは英語（米国）のロケールが設定されます。 それ以外のロケールでデバイスを使用するには、そのロケール固有のバージョンの Unified Communications Manager Endpoints Locale Installer を、クラスタ内の各 Cisco Unified Communications Manager サーバにインストールする必要があります。 ロケール インストーラは電話機のユーザ インターフェイス用の最新版の翻訳テキスト、ならびに国別の電話トーンをシステムにインストールして、それらをデバイスで使用できるようにします。

リリースに必要なロケール インストーラにアクセスするには、http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245 にアクセスし、お使いのデバイス モデルに移動して、Unified Communications Manager Endpoints Locale Installer リンクを選択します。

詳細については、『*Cisco Unified Communications Operating System Administration Guide*』の「Locale Installer」を参照してください。

（注） 最新のロケール インストーラがすぐに利用できるとは限らないため、Web サイトの更新を継続的に確認してください。

# 国際コールのロギングのサポート

ご使用の電話システムで国際コールのロギング（発信側の正規化）が設定されている場合、通話履歴、リダイヤル、コールディレクトリの各エントリに通話場所の国際エスケープ コードをあらわす「+」記号が表示されることがあります。 電話システムの設定によっては、「+」記号ではなく正しい国際ダイヤル コードが表示される場合があります。国際ダイヤル コードが表示されない場合は、必要に応じて、「+」記号を通話場所の国際エスケープ コードに手動で置き換えて番号を編集した後にダイヤルします。 また、コール ログやディレクトリ エントリには受信コールの完全な国際電話番号が表示され、電話機のディスプレイには国際コード（国番号）が省略された国内用の短い番号が表示される場合もあります。

第 12 章

# メンテナンス


- デバイスのリセット，163 ページ
- オプションのリセットとアップグレードのロード，165 ページ
- リモート ロック，165 ページ
- リモート ワイプ，166 ページ
- Cisco DX70 の代替イメージのブート，167 ページ
- Cisco DX80 の代替イメージのブート，167 ページ
- Cisco DX650 の代替イメージのブート，167 ページ
- データの移行，168 ページ
- デバッグ ログのプロファイル，168 ページ
- ユーザ サポート，169 ページ


## デバイスのリセット

デバイスをリセットすると、各種の設定やセキュリティ設定をリセットまたは復元したり、デバイスにエラーが発生した場合に復旧することができます。

次の手順では、実行可能なリセットのタイプについて説明します。

（注） この 3 つのどのリセット方法でも、ユーザ データがすべて削除され、デバイスのすべての設定がリセットされます。

リセットを実行すると、デバイスで次の操作が行われます。

- ユーザ設定：デフォルト値にリセットされます。
- ネットワーク設定：デフォルト値にリセットされます。

- コール履歴：消去されます。
- ロケール情報：デフォルト値にリセットされます。
- セキュリティ設定：デフォルト値にリセットされます。このリセットでは、CTLファイルが削除され、[802.1x デバイス認証（802.1x Device Authentication）] パラメータが [無効（Disabled）] に設定されます。

（注） 初期設定へのリセットプロセスが完了するまで、デバイスの電源をオフにしないでください。

### 手順

次のいずれかの操作でデバイスをリセットできます。 状況に応じて適切な操作を選択します。

- 方法 1：Cisco Unified Communications Manager Administrator Web GUI
  1. [プロダクト固有の設定（Product Specific Configuration Layout）] ウィンドウから、[デバイスのワイプ（Wipe Device）] を有効にします。
  2. デバイスの消去を行うには、管理 GUI から設定の適用、再起動、リセット コマンドを実行します。
- 方法 2：設定アプリケーション
  1. 設定アプリケーションで、[バックアップとリセット（Backup & reset）] > [データの初期化（Factory data reset）] を選択します。

     （注） デバイスに PIN またはパスワードが設定されている場合、リセットを続行する前に入力する必要があります。
- 方法 3：キー入力シーケンス

  この方法は、デバイスがPINまたはパスワードロックでセキュリティ保護されているデバイスで、PIN/パスワードを紛失した場合に使用する必要があります。

  次の手順を実行して、起動時に Cisco DX70 をリセットします。
  1. デバイスの電源をオンにし、ミュート LED が点滅するまで待ちます。
  2. ミュート ボタンが赤色に点灯するまで、音量アップ ボタンを押したままにします。
  3. 音量アップ ボタンを放し、ミュート ボタンを 3 秒間押したままにします。

  次の手順を実行して、起動時に Cisco DX80 をリセットします。
  1. 音量アップ ボタンを押したままにして、デバイスの電源をオンにします。
  2. ミュート ボタンが赤色に点灯したら、音量アップ ボタンを放し、ミュート ボタンを押します。

  次の手順を実行して、起動時に Cisco DX650 をリセットします。

1. # キーを押したまま、デバイスの電源をオンにします。
2. メッセージ受信インジケータ（MWI）が赤く点滅したら、# キーを放します

# オプションのリセットとアップグレードのロード

Cisco DX シリーズ デバイスは、設定変更を受信すると、Cisco Unified Communications Manager からアップグレードをロードします。 次の手順は、デバイスが変更要求を処理する方法を示しています。

- アクティブ コールが終了するまでの待機時間をリセットします。
- デバイス画面がオンになっている場合、変更内容とリスタートの必要性をユーザに通知するポップアップ ダイアログボックスが表示されます。 このダイアログボックスでは、次のオプションを選択できます。
  - [再起動（Restart）]：ポップアップ ダイアログボックスを終了し、デバイスを再起動します（デフォルトの処理）。
  - [スヌーズ（Snooze）]：1 時間ポップアップ ダイアログボックスを閉じた状態にします。デバイスを最大 24 時間スヌーズ状態にできます。デバイスはその時間が経過すると再起動します。

    （注） ポップアップ ダイアログボックスは、60 秒のカウントダウン タイマーを備えています。 ユーザが対応しない場合は、デフォルトのアクションが開始されます。

    デバイスをスヌーズ状態に設定した後、いつでも通知リストから手動でデバイスをリセットできます。
  - デバイス画面がオフになっている場合、アクティブなオーディオが存在すると、要求は待機し続けます。

# リモート ロック

Cisco Unified Communications Manager の [デバイス設定（Device Configuration）] ウィンドウから、この機能を使ってデバイスをロックすることができます。

リモート ロック要求を受信したデバイスは、ただちにすべてのアクティブ コードを終了して、ロックされた状態になります。 デバイスが要求時にシステムに登録されていない場合、デバイスがシステムに登録される次回にデバイスがロックされます。

（注） リモート ロック要求を発行した後に、要求をキャンセルすることはできません。

## デバイスのリモートロック

**手順**

**ステップ 1** デバイスの [電話の設定（Phone Configuration）] ウィンドウで、[ロック（Lock）] をクリックします。

**ステップ 2** [ロック（Lock）] をクリックし、ロック確認メッセージを承認します。
デバイスの [電話の設定（Phone Configuration）] ウィンドウの [デバイスのロック/ワイプのステータス（Device Lock/Wipe Status）] セクションで、ロックのステータスを確認できます。

# リモート ワイプ

Cisco Unified Communications Manager の [デバイス設定（Device Configuration）] ウィンドウから、この機能を使ってデバイス上のデータを消去することができます。

デバイスはリモート ワイプ要求を受信すると、ただちにアクティブ コールを終了し、デバイス データを消去します。 デバイスが要求時にシステムに登録されていない場合、デバイスがシステムに登録される次回にデータが消去されます。

（注） リモート ワイプ要求を発行した後に、要求をキャンセルすることはできません。

## リモートでのデバイスのワイプ

**手順**

**ステップ 1** デバイスの [電話の設定（Phone Configuration）] ウィンドウで、[ワイプ（Wipe）] をクリックします。

**ステップ 2** [ワイプ（Wipe）] をクリックし、ワイプ確認メッセージを承認します。
ワイプのステータスは、デバイスの [電話の設定（Phone Configuration）] ウィンドウの [デバイスのロック/ワイプのステータス（Device Lock/Wipe Status）] セクションで確認できます。

# Cisco DX70 の代替イメージのブート

手順

**ステップ 1** デバイスの電源をオンにし、ミュート LED が点滅するまで待ちます。
**ステップ 2** ミュート ボタンが赤色に点灯するまで、音量ダウン ボタンを押したままにします。
**ステップ 3** 音量ダウン ボタンを放し、ミュート ボタンを 3 秒間押したままにします。

# Cisco DX80 の代替イメージのブート

手順

**ステップ 1** 音量ダウン ボタンを押したままにして、デバイスの電源をオンにします。
**ステップ 2** ミュート ボタンが赤色に点灯したら、音量ダウン ボタンを放し、ミュート ボタンを押します。

# Cisco DX650 の代替イメージのブート

手順

**ステップ 1** 電源を取り外し、デバイスをオフにします。
**ステップ 2** * キーを押し、電源を接続します。
**ステップ 3** メッセージ LED が点灯するまで * キーを押したままにします。
**ステップ 4** メッセージ LED が 3 回点滅したら、* キーを放します。
デバイスは代替イメージを使用してブートします。

# データの移行

データ移行機能により、ファームウェアのアップグレードの後で既存データの非互換性がある場合、出荷時の状態へのリセットが必要とされないことが保証されます。

（注） ファームウェアをダウングレードした場合、データが失われる可能性があります。 新しいファームウェア リリースにアップグレードした場合、データを失うことなしに、以前のリリースに戻すことができない場合があります。

以前のファームウェアにダウングレードするときに、デバイスがデータを移行できない場合は、アラームを受信します。 ユーザに対しユーザ データをバック アップするように指示するか、デバイスのリモート ワイプを実行します。 デバイスが Cisco Unified Communications Manager に登録されると、デバイスは以前の初期状態へのリセットを検出し、移行をオーバーライドし、ダウングレードして再起動します。 デバイスが再起動されると、ダウングレードしたファームウェアをロードします。

# デバッグ ログのプロファイル

デバイスまたはデバイス グループ用に、デバッグ ログのプロファイルをリモートで有効にすることができます。

## 呼処理のデバッグ ログ プロファイルの設定

**手順**

**ステップ 1** 個々のデバイス設定ウィンドウまたは [共通の電話プロファイル（Common Phone Profile）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動します。

**ステップ 2** [ログのプロファイル（Log Profile）] をオンにし、[テレフォニー（Telephony）] を選択します。

**ステップ 3** 変更を保存します。

**ステップ 4** ユーザはデバッグ ロギングが通知領域で有効になっていることを通知されます。 ユーザは、詳細情報のメッセージを展開することはできますが、通知を削除することはできません。

# デバッグ ログ プロファイルのデフォルトへのリセット

**手順**

**ステップ 1** 個々のデバイス設定ウィンドウまたは[共通の電話プロファイル（Common Phone Profile）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動します。

**ステップ 2** [ログのプロファイル（Log Profile）] をオンにし、[デフォルト（Default）] を選択してすべてのデバッグをデフォルト値にリセットします。 これには、Android Debug Bridge から手動で設定されたデバッグが含まれます。

**ステップ 3** 変更を保存して適用します。

**ステップ 4** 現在のデバッグ レベルを保持するには、[プリセット（Preset）] を選択します。

**ステップ 5** 変更を保存します。

# ユーザ サポート

デバイスの一部の機能を正常に使用するには、ユーザがシステム管理者やシステム管理者のネットワーク チームから情報を入手したり、サポートを受けるためにシステム管理者に問い合わせたりできる必要があります。 支援を求める際の連絡先の担当者の名前、およびそれらの担当者に連絡する手順をエンド ユーザに提供しておく必要があります。

シスコでは、社内のサポート サイトに、ユーザにデバイスに関する重要な情報を提供するための Web ページを作成することを推奨しています。

## 問題レポート ツール

Cisco DX シリーズ デバイスでは、内蔵のレポート ツール（問題レポート ツール）により、デバイス関連の問題に対応することができます。 ツールにアクセスするには、[設定（Settings）]>[デバイスについて（About device）] > [Cisco Collaboration Problem Reporting Tool] を選択します。

（注） 問題レポート ツールのログは、Cisco TAC で Cisco DX シリーズ デバイスの問題をトラブルシューティングするときに必要になります。

これらのデバイスから通知を発行するには、ユーザが問題レポート ツールにアクセスし、次の情報を入力します。

- 問題が発生した日付（このフィールドには、ツールが起動された日付が自動入力されます）
- 問題が発見された時刻（このフィールドには、ツールが起動された時刻が自動入力されます）

- 問題のあるアプリケーション 問題のあるアプリケーションが不明な場合は、[なし（None）] を選択します。
- 問題の説明（検出された予期しない動作について、およびそれが発生する前に行った操作手順についての簡潔な説明を含む）

電子メールアドレスが設定されているが、それがリリース 10.2(3) 以降を搭載した拡張モードのデバイスでのみ機能する場合、問題レポート ツールは管理者にログを電子メールで送信します。問題レポート ツールでは、ログとデバッグ データをサーバに直接アップロードできます。これは、[デバイス UI プロファイル（Device UI Profile）] が [簡易（Simple）] モードまたは [パブリック（Public）] モードに設定され、電子メール クライアントが利用できない場合に特に役立ちます。

管理者またはエンド ユーザは、PRT 画面の [カスタマー サポートのメールアドレス（Customer support email address）] に URL 文字列を入力することで、アップロード機能を使用できます。 例：http://your-server.example.com/prt_upload_example.php

ユーザが [問題レポートを作成（Create problem report）] ボタンをタップすると、問題レポート ツールはフィールドをチェックし、それが “http://” から始まっている場合は、電子メールの代わりにアップロード機能を使用します。

エンド ユーザは PRT 画面でこの URL を直接入力できます。また、管理者は、Cisco Unified Communications Manager の個々のデバイス設定ページ、[共通の電話プロファイル（Common Phone Profile）] ページ、および [エンタープライズ電話の設定（Enterprise Phone Configuration）] ページで、[カスタマー サポート用電子メール アドレス（Email address for customer support）] フィールドに値を入力できます。

デバイスは、HTTP フォーム ベースのアップロードに類似したパラメータと共に HTTP POST 機能を使用します。 アップロードには次のパラメータが含まれます（マルチパート MIME 符号化を使用）。

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

（注） Https はサポートされません。

管理者は、問題レポート ツールのファイルを受信するためのアップロード スクリプトをサーバ（または既存のサーバを使用）に設定できます。 これらのファイルはフォルダに保持できます。また、スクリプトを複雑にして通知メカニズムを使用することにより、新しい Problem Report Tool のレポートがアップロードされたことを管理者に通知することもできます。

### サンプル スクリプト

スクリプト例を次に示します。このスクリプトは参考用の目的のみに掲載されています。シスコでは、お客様のサーバにインストールされたアップロード スクリプトをサポートしていません。

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

## カスタマー サポートのアップロード URL の設定

### 手順

**ステップ 1** 個々のデバイス設定ウィンドウ、[共通の電話プロファイル（Common Phone Profile）] ウィンドウ、または [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動します。

**ステップ 2** [カスタマー サポートのアップロード URL（Customer support upload URL）] をオンにして、デバイス管理者の電子メール アドレスを入力します。

**ステップ 3** 変更を保存します。

# Web ブラウザからのスクリーンショットの取得

### 手順

ご使用のブラウザで URL http://<Endpoint IP Address>/CGI/Screenshot に移動します。
認証を求めるプロンプトが表示されます。 対応するユーザ ID 名とパスワードを使用します。

# デバイスからのスクリーンショットの取得

### 手順

音量ダウン ボタンと 電源/ロック ボタンを 3 秒間押します。

# アプリケーションのサポート

問題がデバイス障害かアプリケーションの問題かどうかを評価します。 問題がアプリケーション関連である場合、サポート センターに直接お問い合わせください。

第 13 章

# モデル情報のステータスと統計情報


- モデル情報，173 ページ
- デバイスの状態，174 ページ


## モデル情報

モデル情報を表示するには、設定アプリケーションで[端末について（About device）]を選択します。 [モデル情報（Model Information）]画面には、次の表に示す項目があります。

**表 *23*：*Cisco DX* シリーズ デバイスのモデル情報**

| 項目 | 説明 |
|---|---|
| ステータス（Status） | デバイスに関する追加情報を提供するサブメニュー。 |
| Cisco ユーザ ガイド（Cisco user guide） | マニュアルへのリンクを提供します。 |
| 法的情報（Legal information） | オープンソースのライセンスが含まれています。 |
| モデル番号（Model Number） | モデル番号。 |
| Android バージョン（Android version） | Android のバージョンを示します。 |
| カーネル バージョン（Kernel version） | Linux カーネル番号 |
| ビルド番号（Build number） | 現在のソフトウェアビルド |
| SELinuxのステータス（SELinux status） | enforcing または permissive を示します。 |

| 項目 | 説明 |
|---|---|
| **Cisco ロード情報（Cisco load information）** | |
| アクティブ ロード（Active Load） | 現在インストールされているファームウェアのバージョン。 |
| 前回のアップグレード（Last Upgrade） | 前回ファームウェアをアップグレードした日付。 |
| （注） デバイスがアップグレード中の場合、[Cisco ロード情報（Cisco load information）] グループに [アップグレード進行中（Upgrade Progress）] メッセージが表示されます。 | |
| **Cisco Unified Communications Manager** | |
| アクティブ サーバ（Active Server） | デバイスが登録されるサーバの DNS または IP アドレス。 |
| スタンバイ サーバ（Standby Server） | スタンバイ サーバの DNS または IP アドレス。 |
| **Cisco Collaboration Problem Reporting Tool** | |
| Cisco Collaboration Problem Reporting Tool | 問題を報告するためのツール。 日付、時刻、問題となるアプリケーションの問題の説明とカスタマー サポートの電子メール アドレスをタップして、選択と入力をします。 ログ情報を収集し電子メール レポートを作成するには、[メール レポートを作成（Create email report）] をタップします。 |

ユーザがセキュアまたは認証済みサーバに接続されている場合、対応するアイコン（ロックまたは認証マーク）がホーム画面上でサーバオプションの右側に表示されます。ユーザがセキュアまたは認証済みのサーバに接続していない場合、アイコンは表示されません。

# デバイスの状態

デバイスの状態を表示するには、設定アプリケーションで[端末について（About device）>[ステータス（Status）] を選択します。

**表 *24*：デバイスの状態**

| 項目 | 説明 |
|---|---|
| ステータス メッセージ（Status Messages） | [ステータス メッセージ（Status Messages）] 画面を表示します。ここには、重要なシステム メッセージのログが示されます。 |
| MDN | デバイスの携帯電話番号が表示されます。 |

| 項目 | 説明 |
|---|---|
| IP アドレス（IP address） | デバイスの IP アドレスが表示されます。 |
| Wi-Fi MAC アドレス（Wi-Fi MAC address） | 現在の Wi-Fi 接続の MAC アドレスを示します。 |
| Ethernet MAC アドレス（Ethernet MAC address） | 現在のイーサネット接続の MAC アドレスを示します。 |
| Bluetooth アドレス（Bluetooth address） | Bluetooth チップセットの MAC アドレスを示します。 |
| DHCP 情報（DHCP information） | DHCP 情報画面を表示します。 |
| 使用可能時間（Up Time） | デバイスの実行時間。 |
| 現在のアクセス ポイント（Current Access Point） | 該当する場合、[現在のアクセス ポイント（Current Access Point）] 画面を表示します。 |
| イーサネット統計（Ethernet Statistics） | [イーサネット統計（Ethernet Statistics）] 画面を表示します。この画面には、イーサネット トラフィックの統計が表示されます。 |
| WLAN 統計（WLAN statistics） | [WLAN 統計（WLAN Statistics）] 画面を必要に応じて提供します。 |
| コール統計（オーディオ）（Call statistics (audio)） | 現在のコールの音声部分のカウンタおよび統計を表示します。 |
| コール統計（ビデオ）（Call statistics (video)） | 現在のコールのビデオ部分のカウンタおよび統計を表示します。 |
| コール統計（プレゼンテーション）（Call statistics (presentation)） | 現在のコールのプレゼンテーション部分のカウンタおよび統計を表示します。 |

# ステータス メッセージ

[ステータス メッセージ（Status Messages）] 画面には、デバイスが最近生成したステータス メッセージが 50 件表示されます。 次の表に、表示される可能性のあるステータス メッセージの説明を示します。 また、この表には、エラーの対処方法も示されています。

ステータス メッセージを表示するには、[ステータス メッセージ（Status Messages）] 画面で、[ステータス メッセージ（Status Messages）] をタップします。

現在のステータス メッセージを削除するには、[消去（Clear）] をタップします。

[ステータス メッセージ（Status Messages）] 画面を終了するには、[OK] をタップします。

**表 *25*：ステータス メッセージ**

| メッセージ | 説明 | 考えられる状況と対処方法 |
|---|---|---|
| CFG TFTP サイズ エラー（CFG TFTP Size Error） | コンフィギュレーション ファイルが、ファイル システムに対して大きすぎます。 | デバイスの電源を再投入する。 |
| チェックサム エラー（Checksum Error） | ダウンロードしたソフトウェア ファイルが破損しています。 | デバイスのファームウェアの新しいコピーを入手し、それを TFTPPath ディレクトリの中に置きます。 TFTP サーバ ソフトウェアがシャットダウンされているときにのみ、ファイルをこのディレクトリにコピーしてください。シャットダウンされていないときにコピーすると、ファイルが破損する可能性があります。 |
| DHCP タイムアウト（DHCP timeout） | DHCP サーバが応答しませんでした。 | • ネットワーク ビジー：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。<br>• DHCP サーバとデバイスとの間にネットワーク接続がない：ネットワーク接続を確認してください。<br>• DHCP サーバがダウンしている：DHCP サーバの設定を確認してください。<br>• 引き続きエラーが表示される：スタティック IP アドレスの割り当てを検討します。 |
| DNS タイムアウト（DNS timeout） | DNS サーバが応答しませんでした。 | • ネットワーク ビジー：このエラーは、ネットワーク負荷が軽減されると、自動的に解決します。<br>• DNS サーバとデバイスとの間にネットワーク接続がない：ネットワーク接続を確認してください。<br>• DNS サーバがダウンしている：DNS サーバの設定を確認してください。 |

| メッセージ | 説明 | 考えられる状況と対処方法 |
|---|---|---|
| DNS 不明ホスト（DNS unknown host） | DNS が TFTP サーバまたは Cisco Unified Communications Manager の名前を解決できませんでした。 | • TFTP サーバまたは Cisco Unified Communications Manager のホスト名が DNS に正しく設定されていることを確認してください。<br>• ホスト名ではなく IP アドレスを使用することを検討します。 |
| IP が重複しています（Duplicate IP） | 別のデバイスが、デバイスに割り当てられた IP アドレスを使用中です。 | • デバイスにスタティック IP アドレスが割り当てられている場合は、重複する IP アドレスを割り当てていないことを確認してください。<br>• DHCP を使用している場合は、DHCP サーバの設定を確認してください。 |
| ロケールの更新エラー（Error update locale） | 1 つ以上のローカリゼーションファイルが TFTPPath ディレクトリで見つからなかったか、または有効ではありませんでした。 ロケールは変更されませんでした。 | Cisco Unified Communications Manager から、次のファイルが [TFTP ファイルの管理（TFTP File Management）] のサブディレクトリ内に存在することを確認します。<br>• ネットワーク ロケールと同じ名前のサブディレクトリに存在するファイル：<br>◦ tones.xml<br>• ユーザ ロケールと同じ名前のサブディレクトリに存在するファイル：<br>◦ glyphs.xml<br>◦ dictionary.xml<br>◦ kate.xml |

| メッセージ | 説明 | 考えられる状況と対処方法 |
|---|---|---|
| ファイルが見つかりません<Cfg ファイル>（File not found <Cfg File>） | TFTP サーバで、名前ベースのデフォルトの設定ファイルが見つかりませんでした。 | デバイスが Cisco Unified Communications Manager データベースに追加されるときにコンフィギュレーション ファイルが作成されます。 デバイスが Cisco Unified Communications Manager データベースにまだ追加されていない場合、TFTP サーバは「CFG ファイルが見つかりません（CFG File Not Found）」という応答を生成します。<br>• デバイスが Cisco Unified Communications Manager に登録されていない。<br>デバイスの自動登録を許可しないように設定している場合は、手動でデバイスを Cisco Unified Communications Manager に追加する必要があります。<br>• DHCP を使用している場合は、DHCP サーバが正しい TFTP サーバを指定していることを確認してください。<br>• スタティック IP アドレスを使用している場合は、TFTP サーバの設定を確認してください。 |
| IP アドレス解放（IP address released） | デバイスはIPアドレスを解放するように設定されます。 | デバイスの電源をオフ/オンにするか、またはDHCPアドレスをリセットするまで、デバイスはアイドル状態のままです。 |
| 拒否された HC のロード（Load rejected HC） | ダウンロードされたアプリケーションには、デバイスとの互換性がありません。 | このデバイス上のハードウェア変更をサポートしないソフトウェアバージョンをデバイスにインストールしようとすると、発生します。<br>デバイスに割り当てられたロード ID を確認してください（Cisco Unified Communications Manager で、[デバイス（Device）] > [電話（Phone）] を選択)。 デバイスに表示されているロードを再入力します。 |
| デフォルト ルータがありません（No default router） | DHCP またはスタティック設定でデフォルトルータが指定されていませんでした。 | • デバイスにスタティック IP アドレスが割り当てられている場合は、デフォルト ルータが設定されていることを確認してください。<br>• DHCP を使用している場合は、DHCP サーバがデフォルト ルータを提供していません。DHCP サーバの設定を確認してください。 |

| メッセージ | 説明 | 考えられる状況と対処方法 |
|---|---|---|
| DNS サーバ IP がありません（No DNS server IP） | 名前は指定されていましたが、DHCP またはスタティック IP設定で DNS サーバのアドレスが指定されていませんでした。 | • デバイスにスタティック IP アドレスが割り当てられている場合は、DNS サーバが設定されていることを確認してください。<br>• DHCP を使用している場合は、DHCP サーバが DNS サーバを提供していません。 DHCP サーバの設定を確認してください。 |
| 信頼リストがインストールされていません（No Trust List installed） | CTL ファイルまたは ITL ファイルがデバイスにインストールされていません。 | デフォルトでセキュリティをサポートしない Cisco Unified Communications Manager で、信頼リストが設定されていません。<br>信頼リストの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。 |
| Cisco Unified Communications Manager の要求による再起動（Restart requested by Cisco Unified Communications Manager） | デバイスは、Cisco Unified Communications Manager からの要求に応じて再起動します。 | Cisco Unified Communications Manager でデバイスの設定変更が行われ、変更を有効にするために [適用（Apply）] ボタンが押された可能性があります。 |
| TFTP アクセス エラー（TFTP access error） | TFTP サーバが、存在しないディレクトリを指定しています。 | • DHCP を使用している場合は、DHCP サーバが正しい TFTP サーバを指定していることを確認してください。<br>• スタティック IP アドレスを使用している場合は、TFTP サーバの設定を確認してください。 |
| TFTP エラー（TFTP error） | デバイスが、TFTP サーバからのエラーコードを認識できません。 | Cisco Technical Assistance Center（TAC）に問い合わせてください。 |

| メッセージ | 説明 | 考えられる状況と対処方法 |
|---|---|---|
| TFTP タイムアウト（TFTP timeout） | TFTP サーバが応答しませんでした。 | • ネットワーク ビジー：このエラーは、ネットワーク負荷が軽減されると自動的に解決します。<br>• TFTP サーバとデバイスとの間にネットワーク接続がない：ネットワーク接続を確認してください。<br>• TFTP サーバがダウンしている：TFTP サーバの設定を確認してください。 |
| タイムアウト（Timed Out） | サプリカントが 802.1X トランザクションを実行しようとしましたが、オーセンティケータが存在しないためにタイムアウトになりました。 | 認証は一般的に、スイッチで 802.1x が設定されていない場合にタイムアウトします。 |
| 信頼リストの更新に失敗しました（検証失敗）（Trust List update failed, verification failure） | CTL ファイルおよび ITL ファイルの更新に失敗しました。 | エラーの場合に表示されるメッセージです。 |
| バージョン エラー（Version error） | ロードファイルの名前が不正です。 | デバイスのロードファイルが正しい名前であることを確認してください。 |
| XmlDefault.cnf.xml（またはデバイス名に対応した .cnf.xml） | 設定ファイルの名前。 | なし。このコンフィギュレーションファイルは、コンフィギュレーションファイルの名前を示す情報メッセージを提供します。 |

# イーサネット統計

[イーサネット統計（Ethernet Statistics）] 画面には、デバイスおよびネットワークのパフォーマンスに関する情報が表示されます。 次の表に、この画面に表示される情報を示します。

イーサネット統計情報を表示するには、設定アプリケーションで[端末について（About device）] > [ステータス（Status）] > [イーサネット統計（Ethernet statistics）] を選択します。

[Rx Frames]、[Tx Frames]、および [Rx Broadcasts] の統計を 0 にリセットするには、[消去（Clear）] をタップします。

[イーサネット統計（Ethernet Statistics）] 画面を終了するには、[OK] をタップします。

**表 *26*：イーサネット統計メッセージ情報**

| 項目 | 説明 |
|---|---|
| Rx フレーム（Rx Frames） | 受信パケット数 |
| Tx フレーム（Tx Frames） | 送信パケット数 |
| Rx ブロードキャスト（Rx Broadcasts） | 受信ブロードキャスト パケットの数 |
| ポート 1（Port 1） | スイッチ ポートの速度とデュプレックス |
| ポート 2（Port 2） | PC ポートの速度とデュプレックス |
| CDP ステータス（CDP status） | 現在の CDP ステータス |

# WLAN 統計情報

[WLAN 統計（WLAN Statistics）] 画面には、デバイスと WLAN に関する統計情報が表示されます。 次の表に、この画面に表示される情報を示します。

[WLAN 統計（WLAN Statistics）] 画面を表示するには、[デバイスについて（About device）] > [ステータス（Status）] > [WLAN 統計（WLAN statistics）] を選択します。

WLAN 統計画面を終了するには、[OK] をタップします。

**表 *27*：*WLAN* 統計情報**

| 項目 | 説明 |
|---|---|
| Tx バイト（tx bytes） | 送信されたバイト数 |
| Rx バイト（rx bytes） | 受信されたバイト数 |
| Tx パケット（tx packets） | 送信されたデータ パケットの数 |
| Rx パケット（rx packets） | 受信されたデータ パケットの数 |
| Tx パケット ドロップ（tx packets dropped） | ドロップされた送信データ パケットの数 |

| 項目 | 説明 |
|---|---|
| Rx パケット ドロップ（rx packets dropped） | ドロップされた受信データ パケットの数 |
| Tx パケット エラー（tx packet errors） | 送信されたデータ パケット エラー数 |
| Rx パケット エラー（rx packet errors） | 受信されたデータ パケット エラー数 |
| Tx フレーム（Tx frames） | 送信されたフレームの数 |
| Tx マルチキャスト フレーム（tx multicast frames） | ブロードキャストまたはマルチキャストとして送信されたフレームの数 |
| Tx リトライ（tx retry） | 受信デバイスの確認応答を得るために 1 回だけ再送信されたメッセージの数 |
| Tx マルチ リトライ（tx multi retry） | 成功するまでの送信リトライの回数 |
| Tx 失敗（tx failure） | 送信に失敗したフレームの数 |
| RTS 成功（rts success） | 対応する CTS を受信しました。 |
| RTS 失敗（rts failure） | 受信に失敗したフレームの数 |
| ACK 失敗（ack failure） | AP が送信に確認応答しませんでした。 |
| Rx 重複フレーム（rx duplicate frames） | 送信された重複するマルチキャスト パケットの数 |
| Rx フラグメント パケット（rx fragmented packets） | 受信されたフラグメント パケットの数 |
| ローミング カウント（roaming count） | 現在のアクセス ポイント（AP）からローミングされた回数 |

# 音声コール統計

最新コールのカウンタ、統計、および音声品質メトリックを表示するには、デバイスの [コール統計（オーディオ）（Call Statistics (audio)）] にアクセスします。

（注） ご使用の Web ブラウザから [ストリームの統計（Streaming Statistics）] Web ページにアクセスして、コール統計情報をリモートで参照できます。 この Web ページには、デバイスでは表示できない追加の RTP Control Protocol（RTCP）統計が含まれています。

単一コールに複数の音声ストリームが含まれる場合がありますが、最後の音声ストリームに関するデータだけがキャプチャされます。 音声ストリームは、2 つのエンドポイント間のパケット ストリームです。 一方のエンドポイントが保留になると、コールが引き続き接続されている場合でも、音声ストリームは停止します。 コールが再開されると、新しい音声パケットストリームが開始され、以前のコール データは新しいコール データによって上書きされます。

[コール統計（オーディオ）（Call statistics (audio)）] に最新の音声ストリームに関する情報を表示するには、[設定（Settings）] > [端末について（About device）] > [ステータス（Status）] > [コール統計（オーディオ）（Call statistics (audio)）] を選択します。

次の表に、[コール統計（オーディオ）（Call statistics (audio)）] 画面で提供される項目のリストを示します。

**表 *28*：コールの統計の項目**

| 項目 | 説明 |
|---|---|
| 受信コーデック（Rcvr Codec） | 受信した音声ストリームのタイプ（codec からの RTP ストリーミング オーディオ）：AAC-LD、G.722、iSAC、G.711 u-law、G.711 A-law、iLBC、および G.729。 |
| 送信コーデック（Sender Codec） | 送信した音声ストリームのタイプ（codec からの RTP ストリーミング オーディオ）：AAC-LD、G.722、iSAC、G.711 u-law、G.711 A-law、iLBC、および G.729。 |
| 受信サイズ（Rcvr Size） | 受信中の音声ストリーム（RTP ストリーミング オーディオ）の音声パケット サイズ（ミリ秒）。 |
| 送信サイズ（Sender Size） | 送信中の音声ストリームの音声パケット サイズ（ミリ秒）。 |
| 受信パケット（Rcvr Packets） | 音声ストリームが開始されてから受信した RTP 音声パケットの数。<br>（注） この数値は、必ずしもコールの開始以降に受信した RTP 音声パケットの数と等しいとは限りません。これは、コールが途中で保留されることがあるからです。 |
| 送信パケット（Sender Packets） | 音声ストリームの開始以降に送信された RTP 音声パケットの数。<br>（注） この数値は、必ずしもコールの開始以降に送信された RTP 音声パケットの数と等しいとは限りません。これは、コールが途中で保留されることがあるからです。 |

| 項目 | 説明 |
|---|---|
| 平均ジッター（Avg Jitter） | 受信中の音声ストリームが開始されてから測定された、RTP パケットジッタの推定平均値（パケットがネットワークを経由する際の動的な遅延。ミリ秒）。 |
| 最大ジッター（Max Jitter） | 受信中の音声ストリームが開始されてから測定された最大ジッタ（ミリ秒単位）。 |
| 受信削除（Rcvr Discarded） | 受信中の音声ストリームで廃棄された RTP パケットの数（不良パケット、過度の遅延などによる）。<br>（注） デバイスは、シスコ ゲートウェイによって生成されたペイロード タイプ 19 のコンフォート ノイズ パケットを廃棄します。これによって、このカウンタが増分されます。 |
| 受信喪失パケット（Rcvr Lost Packets） | 失われた RTP パケット（転送中に喪失）。 |
| 累積フレーム損失率（Cumulative Conceal Ratio） | 隠蔽フレームの総数を、音声ストリームの開始以降に受信された音声フレームの総数で割った値。 |
| 直近フレーム損失率（Interval Conceal Ratio） | アクティブな音声に先行する 3 秒間の間隔における、音声フレームに対する隠蔽フレームの比率。 音声アクティビティ検出（VAD）を使用する場合は、3 秒間のアクティブな音声としてより長い間隔が必要になることがあります。 |
| 最大フレーム損失率（Max Conceal Ratio） | 音声ストリームの開始以降、最も高い間隔の損失率。 |
| フレーム損失発生秒数（Conceal Secs） | 音声ストリームの開始以降、隠蔽イベント（フレーム損失）があった秒数（[深刻なフレーム損失発生秒数（Severely Conceal Secs）] の値を含む）。 |
| 深刻なフレーム損失発生秒数（Severely Conceal Secs） | 音声ストリームの開始以降、5 % を超える隠蔽イベント（フレーム損失）があった秒数。 |
| 遅延（Latency） | ネットワーク遅延の推定値（ミリ秒単位）。 ラウンドトリップ遅延の実行中の平均値を表します。これは、RTCP受信レポートブロックの受信時に測定されます。 |
| 送信の DSCP（Sender DSCP） | 送信側 SIP シグナリング パケットの DSCP 値 |

| 項目 | 説明 |
| --- | --- |
| 受信の DSCP（Receiver DSCP） | 受信側 SIP シグナリング パケットの DSCP 値 |
| 送信の RTCP DSCP（Sender RTCP DSCP） | 送信側 RTP パケットの DSCP 値 |
| 受信の RTCP DSCP（Receiver RTCP DSCP） | 受信側 RTP パケットの DSCP 値 |

第 14 章

# リモート モニタリング


- Web ページへのアクセスの有効化および無効化，187 ページ
- デバイスの Web ページへのアクセス，188 ページ
- デバイス情報，189 ページ
- ネットワークのセットアップ，191 ページ
- セキュリティ情報，200 ページ
- イーサネット統計，201 ページ
- WLAN の設定，205 ページ
- デバイス ログ，208 ページ
- ストリームの統計，208 ページ


## Web ページへのアクセスの有効化および無効化

セキュリティ上の理由から、デバイスの Web ページへのアクセスはデフォルトで無効になっています。 そのため、この章で説明している Web ページおよびセルフ ケア ポータルにアクセスできません。

手順

**ステップ 1** Cisco Unified Communications Manager から、[デバイス（Device）] > [電話（Phone）] の順に選択します。

**ステップ 2** デバイスの検索条件を指定して [検索（Find）] をクリックします。または、[検索（Find）] をクリックしてすべての電話機を表示します。

**ステップ 3** デバイス名をクリックして、そのデバイスの [電話の設定（Phone Configuration）] ウィンドウを開きます。

**ステップ 4** [プロダクト固有の設定（Product Specific Configuration）] セクションまで、下方向にスクロールします。 [Web アクセス（Web Access）] ドロップダウン リストから、Web ページ アクセスを有効にする場合は [有効（Enabled）] を選択し、Web ページ アクセスを無効にする場合は [無効（Disabled）] を選択します。

**ステップ 5** [保存（Save）] をクリックします。

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

# デバイスの Web ページへのアクセス

手順

**ステップ 1** 次のいずれかの方法でデバイスの IP アドレスを取得します。

- [デバイス（Device）] > [電話（Phone）]の順に選択して、Cisco Unified Communications Manager でデバイスを検索します。 Cisco Unified Communications Manager に登録されているデバイスの IP アドレスが、[電話の検索/一覧表示（Find and List Phones）] ウィンドウと [電話の設定（Phone Configuration）] ウィンドウの上部に表示されます。
- デバイスで、[設定（Settings）] > [端末について（About device）] > [ステータス（Status）] > [DHCP 情報（DHCP Information）] を選択して、Wi-Fi または Ethernet 用の IP アドレスを取得します。

**ステップ 2** Web ブラウザを開いて、次の URL を入力します。ここで、<IP_address> はデバイスの IP アドレスです。

```
http://<IP_address>
```

デバイスの Web ページには次のトピックが表示されます。

- [デバイス情報（Device Information）]：デバイスの設定および関連情報を提供します。
- [ネットワークのセットアップ（Network Setup）]：ネットワークの設定情報を提供します。

- [セキュリティ情報（Security Information）]：セキュリティ設定情報を提供します。
- [イーサネット統計（Ethernet Statistics）]：ネットワーク トラフィックに関する情報を提供する、次のハイパーリンクが含まれます。
  - [イーサネット情報（Ethernet Information）]：イーサネット トラフィックに関する情報を提供します。
  - [アクセス（Access）]：デバイスのネットワーク トラフィックに関する情報を提供します。
  - [ネットワーク（Network）]：デバイスのネットワーク トラフィックに関する情報を提供します。
- WLAN の設定
  - [現在の AP（Current AP）]：現在のアクセス ポイントに関する情報を提供します。
  - [WLAN 統計（WLAN Statistics）]：WLAN トラフィックに関する情報を提供します。
- [デバイス ログ（Device Logs）]：トラブルシューティングに利用できる情報を提供する次のハイパーリンクが含まれます。
  - [コンソール ログ（Console Logs）]：個々のログ ファイルへのハイパーリンクが含まれています。
  - [コア ダンプ（Core Dumps）]：個々のダンプ ファイルへのハイパーリンクが含まれています。
  - [ステータスメッセージ（Status Messages）]：デバイスに前回電源が投入されてから生成された最新のステータス メッセージが 10 件まで表示されます。
  - [デバッグの表示（Debug Display）]：トラブルシューティング時に Cisco Technical Assistance Center（TAC）のサポートが必要な場合に、役立つ可能性のあるデバッグ メッセージを表示します。
- [ストリームの統計（Streaming Statistics）]：[音声とビデオの統計（Audio and Video statistics）]、[ストリーム 1（Stream 1）]、[ストリーム 2（Stream 2）]、[ストリーム 3（Stream 3）]、[ストリーム 4（Stream 4）]、[ストリーム 5（Stream 5）]、および [ストリーム 6（Stream 6）] ハイパーリンクを含み、さまざまなストリームの統計情報が表示されます。

# デバイス情報

デバイスの Web ページにある [デバイス情報（Device Information）] 領域には、デバイスの設定および関連情報が表示されます。

表 *29* : *[*デバイス情報（*Device Information*）*]* 領域の項目

| 項目 | 説明 |
|---|---|
| イーサネット ネットワーク状態（Ethernet Network State） | イーサネット ネットワーク状態 |
| WiFi ネットワーク状態（Wifi Network State） | WiFi ネットワーク状態 |
| MAC アドレス（MAC Address） | イーサネット MAC アドレス |
| WLAN MAC アドレス（WLAN MAC Address） | Wi-Fi 接続用の IP アドレス |
| ホスト名（Host Name） | デバイスの MAC アドレスに基づいてデバイスに自動的に割り当てられる一意の固定された名前。 |
| 電話番号（Phone DN） | デバイスに割り当てられている電話番号。 |
| バージョン（Version） | デバイスで作動しているファームウェアの ID。 |
| ハードウェアのリビジョン（Hardware Revision） | デバイスのハードウェアのリビジョン値。 |
| シリアル番号（Serial Number） | デバイスの固有のシリアル番号。 |
| モデル番号（Model Number） | デバイスのモデル番号。 |
| メッセージ受信（Message Waiting） | このデバイスのプライマリ回線で受信したボイス メッセージがあるかどうかを示します。 |

| 項目 | 説明 |
|---|---|
| UDI | デバイスに関する次の Cisco Unique Device Identifier（UDI）情報を提供します。<br>• [デバイス タイプ（Device Type）]：ハードウェア タイプを示します。<br>• [デバイスの説明（Device Description）]：示されたモデル タイプに関連付けられたデバイスの名前を表示します。<br>• [シリアル番号（Serial Number）]：デバイスの一意のシリアル番号を表示します。 |
| 時刻（Time） | デバイスが属する Cisco Unified Communications Manager の日時グループから取得される時刻。 |
| タイム ゾーン（Time Zone） | デバイスが属する Cisco Unified Communications Manager の日時グループから取得されるタイムゾーン。 |
| 日付（Date） | デバイスが属する Cisco Unified Communications Manager の日時グループから取得される日付。 |

# ネットワークのセットアップ

デバイス の Web ページにある [ネットワークのセットアップ（Network Setup）] 領域には、ネットワークのセットアップ情報とその他の設定に関する情報が表示されます。 次の表に、これらの項目を示します。

これらの項目の多くは、デバイス上の設定アプリケーションから表示および設定できます。

**表 *30*：*[ネットワークのセットアップ（Network Setup）]* の項目**

| 項目 | 説明 |
|---|---|
| WiFi 情報 | |
| WiFi DHCP サーバ（Wifi DHCP Server） | デバイスの Wifi IP アドレス取得元となるダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバの IP アドレス。 |
| WiFi MAC アドレス（Wifi MAC Address） | デバイスの Wifi メディア アクセス コントロール（MAC）アドレス。 |
| WiFi ホスト名（Wifi Host Name） | DHCP サーバがデバイスに割り当てたホスト名。 |

| 項目 | 説明 |
|---|---|
| WiFi ドメイン名（Wifi Domain Name） | デバイスが属するドメイン ネーム システム（DNS）ドメインの名前。 |
| WiFi IP アドレス（Wifi IP Address） | デバイスのインターネット プロトコル（IP）アドレス。 |
| WiFi サブネット マスク（Wifi SubNet Mask） | デバイスで使用されるサブネット マスク。 |
| WiFi デフォルト ルータ（Wifi Default Router） | デバイスで使用されるデフォルト ルータ。 |
| WiFi DNS サーバ 1（Wifi DNS Server 1） | デバイスで使用されるプライマリ ドメイン システム（DNS）サーバ。 |
| WiFi DNS サーバ 2（Wifi DNS Server 2） | デバイスで使用される、オプションのバックアップ DNS サーバ。 |
| WiFi EAP 認証（Wifi EAP Authentication） | EAP 認証の設定を示します。 |
| WiFi SSID（Wifi SSID） | 現在の Wifi SSID を示します。 |
| WiFi セキュリティ モード（Wifi Security Mode） | 現在の Wifi セキュリティ モードを示します。 |
| WiFi 80211 モード（Wifi 80211 Mode） | 現在の Wifi 80211 モードを示します。 |
| イーサネット情報 | |
| イーサネット DHCP サーバ（Ethernet DHCP Server） | デバイスの IP アドレス取得元となるダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバの IP アドレス。 |
| イーサネット MAC アドレス（Ethernet MAC Address） | デバイスのメディア アクセス コントロール（MAC）アドレス。 |
| イーサネット ホスト（Ethernet Host Name） | DHCP サーバがデバイスに割り当てたホスト名。 |
| イーサネット ドメイン名（Ethernet Domain Name） | デバイスが属するドメイン ネーム システム（DNS）ドメインの名前。 |

| 項目 | 説明 |
|---|---|
| イーサネット IP アドレス（Ethernet IP Address） | デバイスのインターネット プロトコル（IP）アドレス。 |
| イーサネット サブネット マスク（Ethernet SubNet Mask） | デバイスで使用されるサブネット マスク。 |
| イーサネット DNS サーバ 1（Ethernet DNS Server 1） | デバイスで使用されるプライマリ ドメイン システム（DNS）サーバ。 |
| イーサネット DNS サーバ 2（Ethernet DNS Server 2） | デバイスで使用される、オプションのバックアップ DNS サーバ。 |
| 接続先 VLAN ID（Operational VLAN ID） | デバイスが属する、Cisco Catalyst スイッチ上に設定された補助 VLAN。 |
| 管理 VLAN ID（Admin. VLAN ID） | デバイスが属する補助 VLAN。 |
| PC VLAN | PC に送信されたパケットから 802.1P/Q タグを識別し、削除するために使用される VLAN。 |
| SW ポートの速度（SW Port Speed） | スイッチ ポートの速度とデュプレックス。次のいずれかになります。<br>• A：自動ネゴシエーション（Auto Negotiate）<br>• 10H：10BaseT/半二重<br>• 10F：10BaseT/全二重<br>• 100H：100BaseT/半二重<br>• 100F：100BaseT/全二重<br>• 1000F：1000BaseT/全二重<br>• [リンクがありません（No Link）]：スイッチ ポートへの接続がありません。 |

| 項目 | 説明 |
| --- | --- |
| PC ポートの速度（SW Port Speed） | スイッチ ポートの速度とデュプレックス。次のいずれかになります。<br>• A：自動ネゴシエーション（Auto Negotiate）<br>• 10H：10-BaseT/半二重<br>• 10F：10-BaseT/全二重<br>• 100H：100-BaseT/半二重<br>• 100F：100-BaseT/全二重<br>• 1000F：1000-BaseT/全二重<br>• [リンクがありません（No Link）]：スイッチ ポートへの接続がありません。 |
| IPv6 情報 | |
| IP アドレッシング モード（IP Addressing Mode） | IP アドレッシング モードを示します。 |
| IP 設定モード制御（IP Preference Mode Control） | IP 設定モードを示します。 |
| IPv6 自動設定（IPv6 Auto Configuration） | IPv6 自動設定が有効になっているか無効になっているかを示します。 |
| 重複アドレス検出（Duplicate Address Detection） | 重複アドレス検出が有効になっているか無効になっているかを示します。 |
| リダイレクトメッセージを承認（Accept Redirect Messages） | リダイレクト メッセージの承認機能が有効になっているか無効になっているかを示します。 |
| マルチキャストのエコー要求に応答（Reply Multicast Echo Request） | マルチキャスト エコー要求に応答する機能が有効になっているか無効になっているかを示します。 |
| IPv6 アドレス（IPv6 Address） | 電話機のインターネット プロトコル バージョン 6（IPv6）アドレスを表示します。 |
| IPv6 プレフィックス長（IPv6 Prefix Length） | IPv6 プレフィックス長を示します。 |

| 項目 | 説明 |
| --- | --- |
| IPv6 デフォルトルータ（IPv6 Default Router） | デフォルト ルータを示します。 |
| IPv6 DNS サーバ 1（IPv6 DNS Server 1） | デバイスで使用されるプライマリ DNS サーバ。 |
| IPv6 DNS サーバ 2（IPv6 DNS Server 2） | デバイスで使用される、オプションのバックアップ DNS サーバ。 |
| IPv6 代替 TFTP（IPv6 Alternate TFTP） | デバイスが代替 TFTP サーバを使用しているかどうかを示す。 |
| IPv6 TFTP サーバ 1（IPv6 TFTP Server 1） | デバイスで使用される、プライマリのトリビアル ファイル転送プロトコル（TFTP）サーバ。 |
| IPv6 TFTP サーバ 2（IPv6 TFTP Server 2） | デバイスで使用される、バックアップのトリビアル ファイル転送プロトコル（TFTP）サーバ。 |
| CUCM 設定 | |

| 項目 | 説明 |
| --- | --- |
| CUCM サーバ 1-5（DNS Server 1-5） | デバイスを登録できる Cisco Unified Communications Manager サーバのホスト名または IP アドレス（優先度順）。 限定的された Cisco Unified Communications Manager 機能を提供できる SRST ルータが使用可能な場合、項目にそのルータの IP アドレスが表示されることもあります。<br>使用可能な各サーバについて、1 つの項目に Cisco Unified Communications Manager サーバの IP アドレスと、次のいずれかの状態が示されます。<br>• [アクティブ（Active）]：デバイスがコール処理サービスを現在受信している受信元 Cisco Unified Communications Manager サーバ<br>• [スタンバイ（Standby）]：現在のサーバが使用不可になった場合にデバイスの切り替え先となる Cisco Unified Communications Manager サーバ<br>• [空白（Blank）]：現在、この Cisco Unified Communications Manager サーバへの接続はありません。<br>また、項目に Survivable Remote Site Telephony（SRST）指定を含めることもできます。これは、限定された Cisco Unified Communications Manager 機能を提供できる SRST ルータを特定します。 このルータは、他のすべての Cisco Unified Communications Manager サーバがすべて到達不能になった場合にコール処理を引き継ぎます。 SRST Cisco Unified Communications Manager はアクティブであっても、常にサーバのリストの最後尾に表示されます。 SRST ルータ アドレスは、Cisco Unified Communications Manager Administration の [デバイスプール（Device Pool）] ウィンドウで設定します。 |
| 情報 URL（Information URL） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| ディレクトリ URL（Directories URL） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| メッセージ URL（Messages URL） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| サービス URL（Services URL） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| 転送の遅延（Forwarding Delay） | リスニング ステートおよびラーニング ステートの時間。 |

| 項目 | 説明 |
|---|---|
| アイドル URL（Idle URL） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| URL のアイドル時間（Idle URL time） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| プロキシ サーバの URL（Proxy Server URL） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| 認証 URL（Authentication URL） | この機能は Cisco DX シリーズ デバイスではサポートされていません。 |
| TFTP サーバ 1（TFTP Server 2） | デバイスで使用される、プライマリのトリビアル ファイル転送プロトコル（TFTP）サーバ。 |
| TFTP サーバ 2（TFTP Server 2） | デバイスで使用される、バックアップのトリビアル ファイル転送プロトコル（TFTP）サーバ。 |
| 代替 TFTP（Alternate TFTP） | デバイスが代替 TFTP サーバを使用しているかどうかを示す。 |
| ユーザ ロケール（User Locale） | デバイスのユーザに関連付けられたユーザ ロケール。言語、フォント、日付と時刻の形式、および英数字キーボードのテキスト情報など、ユーザをサポートするための一連の詳細情報を示します。 |
| ネットワーク ロケール（Network Locale） | デバイスのユーザに関連付けられたネットワーク ロケール。デバイスが使用するトーンと断続周期の定義など、特定の場所にあるデバイスをサポートするための一連の詳細情報を示します。 |
| ユーザ ロケール バージョン（User Locale Version） | デバイス上にロードされたユーザ ロケールのバージョン。 |
| ネットワーク ロケール バージョン（Network Locale Version） | デバイス上にロードされたネットワーク ロケールのバージョン。 |
| PC ポートを無効にする（PC Port Disabled） | デバイスの PC ポートが有効になっているか無効になっているかを示します。 |
| GARP を使う（GARP Enabled） | デバイスが Gratuitous ARP 応答から MAC アドレスを取得するかどうかを示します。 |
| ビデオ機能を使う（Video Capability Enabled） | デバイスがビデオ コールに参加できるかどうかを示します。 |

| 項目 | 説明 |
| --- | --- |
| ボイスVLANアクセスを使う（Voice Vlan Access Enabled） | このデバイスが、PC ポートに接続されたデバイスに対して、ボイス VLAN へのアクセスを許可するかどうかを示します。 |
| 回線の自動選択を使う（Auto Select Line Enabled） | デバイスで回線の自動選択機能が有効になっているかどうかを示します。 |
| 通話制御の DSCP（Dscp For Call Control） | コール制御シグナリングの DSCP IP 分類。 |
| セットアップのDSCP（Dscp For Setup） | デバイス設定転送の DSCP IP 分類。 |
| サービスの DSCP（Dscp For Services） | デバイス ベースのサービスに関する DSCP IP 分類。 |
| セキュリティ モード（Security Mode） | デバイスに設定されているセキュリティ モード。 |
| Web アクセス（Web Access） | デバイスの Web アクセスが有効（[はい（Yes）]）か無効（[いいえ（No）]）かを示します。 |
| スパン PCポート（Span PC Port） | ネットワーク ポートで送受信されるパケットをアクセス ポートに転送するかどうかを表示します。 |
| PC ポートの CDP（CDP on PC Port） | PC ポートで CDP がサポートされているかどうかを示します（デフォルトでは有効）。<br>CDP が Cisco Unified Communications Manager で無効になっているときは、PC ポートで CDP を無効にすると、CVTA が動作しなくなることを示す警告が表示されます。<br>PC ポートとスイッチ ポートの CDP に関する現在の値は、設定アプリケーションに表示されます。 |

| 項目 | 説明 |
| --- | --- |
| SW ポートの CDP（CDP on SW Port） | スイッチ ポートで CDP がサポートされているかどうかを示します（デフォルトでは有効）。<br>デバイス、電力ネゴシエーション、QoS 管理、および 802.1x セキュリティに VLAN を割り当てるには、スイッチ ポートで CDP を有効にします。<br>デバイスが Cisco スイッチに接続される場合、スイッチ ポートで CDP を有効にしてください。<br>Cisco Unified Communications Manager で CDP が無効になっていると、Cisco 以外のスイッチにデバイスが接続される場合に限りスイッチ ポートで CDP を無効にする必要があることを示す警告が表示されます。<br>PC ポートとスイッチ ポートの CDP に関する現在の値は、設定アプリケーションに表示されます。 |
| LLDP-MED：SW ポート（LLDP-MED: SW Port） | スイッチ ポートで Link Layer Discovery Protocol Media Endpoint Discovery（LLDP-MED）が有効になっているかどうかを示します。 |
| LLDP PC ポート（LLDP PC Port） | リンク層検出プロトコル（LLDP）が PC ポートで有効かどうかを示します。 |
| LLDP 電源優先度（LLDP Power Priority） | デバイスの電源優先度をスイッチにアドバタイズし、スイッチが電力を適切にデバイスに供給できるようにします。 次の設定があります。<br>• 不明（Unknown）<br>• 低（Low）<br>• 大（High）<br>• クリティカル（Critical） |
| LLDP アセット ID（LLDP Asset ID） | 在庫管理のためデバイスに割り当てられているアセット ID を識別します。 |
| スイッチ ポートのリモート設定（Switch Port Remote Configuration） | 管理者は Cisco Unified Communications Manager Administration を使用してデバイステーブル ポートの速度と機能をリモートで設定できます。 |
| PC ポートのリモート設定（PC Port Remote Configuration） | 管理者は Cisco Unified Communications Manager Administration を使用してデバイステーブル ポートの速度と機能をリモートで設定できます。 |

# セキュリティ情報

デバイスの Web ページの [セキュリティ情報（Security Information）] 領域には、CTL ファイルと ITL ファイルに関する情報と、802.1X 認証に関する情報が表示されます。

**表 *31*：*[セキュリティ情報（Security Information）]* の項目**

| 項目 | 説明 |
|---|---|
| シグナリング セキュリティ モード（Signaling Security Mode） | シグナリング セキュリティ モードを示します。 |
| LSC | LSC がデバイスにインストールされているかどうかを示します。 |
| CAPF サーバの IPv4（CAPF Server (IPv4)） | IPv4 の CAPF サーバ アドレスを示します。 |
| CAPF サーバの IPv6（CAPF Server (IPv6)） | IPv6 の CAPF サーバ アドレスを表示します。 |
| CAPF ポート（CAPF Port） | CAPF ポートを示します。 |
| CTL ファイル（CTL File） | |
| CTL 署名（CTL Signature） | CTL 署名を表示します。 |
| CUCM サーバ/TFTP サーバ（CUCM Server/TFTP Server） | CUCM/TFTP サーバ アドレスを表示します。 |
| アプリケーション サーバ（Application Server） | アプリケーション サーバを示します。 |
| CAPF サーバ（CAPF Server） | CAPF サーバを示します。 |
| ITL ファイル（ITL File） | |

| 項目 | 説明 |
|---|---|
| ITL 署名（CTL Signature） | ITL 署名を表示します。 |
| CAPF サーバ（CAPF Server） | CAPF サーバを示します。 |
| TVS | TVS アドレスを示します。 |
| CUCM サーバ/TFTP サーバ（CUCM Server/TFTP Server） | CUCM/TFTP サーバ アドレスを表示します。 |
| 設定ファイル（Configuration File） | ITL コンフィギュレーション ファイルがデバイスにインストールされているかどうかを示します。 |
| 802.1X 認証（802.1X Authentication） | |
| デバイス認証（Device Authentication） | 802.1X デバイス認証が有効であるかどうかを示します。 |
| トランザクション ステータス（Transaction Status） | 802.1X トランザクション ステータスが有効であるかどうかを示します。 |
| プロトコル（Protocol） | 802.1X プロトコルを示します。 |
| デバイスID（Device ID） | デバイス ID を表示します。 |

# イーサネット統計

デバイスの Web ページに表示される次のイーサネット統計のハイパーリンクは、ネットワーク トラフィックに関する情報を提供します。 ネットワーク統計の領域を表示するには、デバイスの Web ページにアクセスします。

- [イーサネット情報（Ethernet Information）]：イーサネット トラフィックに関する情報を表示します。 最初の表に、この領域の項目を示します。
- [アクセス（Access）]領域：デバイスとの間で送受信されるネットワーク トラフィックに関する情報を提供します。 二番目の表に、この領域の項目を示します。

- [ネットワーク（Network）]領域：デバイスとの間で送受信されるネットワーク トラフィックに関する情報を提供します。 二番目の表に、この領域の項目を示します。

**表 *32*：*[イーサネット情報（Ethernet Information）]* の項目**

| 項目 | 説明 |
|---|---|
| Tx フレーム（Tx Frames） | デバイスが送信したパケットの総数 |
| Tx ブロードキャスト（Tx broadcast） | デバイスが送信したブロードキャスト パケットの総数 |
| Tx マルチキャスト（Tx multicast） | デバイスが送信したマルチキャスト パケットの総数 |
| Tx ユニキャスト（Tx unicast） | デバイスが送信したユニキャスト パケットの総数 |
| Rx フレーム（Rx Frames） | デバイスが受信したパケットの総数 |
| Rx ブロードキャスト（Rx broadcast） | デバイスが受信したブロードキャスト パケットの総数 |
| Rx マルチキャスト（Rx multicast） | デバイスが受信したマルチキャスト パケットの総数 |
| Rx ユニキャスト（Rx unicast） | デバイスが受信したユニキャスト パケットの総数 |
| Rx PacketNoDes | ダイレクト メモリ アクセス（DMA）記述子がないために廃棄されたパケットの総数 |

**表 *33*：*[アクセス（Access）]* および *[ネットワーク（Network）]* の項目**

| 項目 | 説明 |
|---|---|
| Rx totalPkt | デバイスが受信したパケットの総数 |
| Rx crcErr | CRC が失敗した、受信されたパケットの合計数 |

| 項目 | 説明 |
|---|---|
| Rx alignErr | フレーム チェック シーケンス（FCS）が無効であり、長さが 64 ～ 1522 バイトの受信されたパケットの合計数 |
| Rx マルチキャスト（Rx multicast） | デバイスが受信したマルチキャスト パケットの総数 |
| Rx ブロードキャスト（Rx broadcast） | デバイスが受信したブロードキャスト パケットの総数 |
| Rx ユニキャスト（Rx unicast） | デバイスが受信したユニキャスト パケットの総数 |
| Rx shortErr | サイズが 64 バイトより小さい、受信された FCS エラー パケットまたは Align エラー パケットの合計数 |
| Rx shortGood | サイズが 64 バイトより小さい、受信された有効なパケットの合計数 |
| Rx longGood | サイズが 1522 バイトより大きい、受信された有効なパケットの合計数 |
| Rx longErr | サイズが 1522 バイトより大きい、受信された FCS エラー パケットまたは Align エラー パケットの合計数 |
| Rx size64 | 無効なパケットを含め、サイズが 0 ～ 64 バイトまでの受信されたパケットの合計数 |
| Rx size65to127 | 無効なパケットを含め、サイズが 65 ～ 127 バイトまでの受信されたパケットの合計数 |
| Rx size128to255 | 無効なパケットを含め、サイズが 128 ～ 255 バイトまでの受信されたパケットの合計数 |
| Rx size256to511 | 無効なパケットを含め、サイズが 256 ～ 511 バイトまでの受信されたパケットの合計数 |
| Rx size512to1023 | 無効なパケットを含め、サイズが 512 ～ 1023 バイトまでの受信されたパケットの合計数 |
| Rx size1024to1518 | 無効なパケットを含め、サイズが 1024 ～ 1518 バイトまでの受信されたパケットの合計数 |
| Rx tokenDrop | リソース不足（FIFO オーバーフローなど）が原因でドロップされたパケットの合計数 |

| 項目 | 説明 |
|---|---|
| Tx excessDefer | メディアがビジーであるために送信が遅れたパケットの合計数 |
| Tx lateCollision | パケット転送の開始後 512 ビット時間過ぎてから衝突が起こった回数 |
| Tx totalGoodPkt | デバイスが受信した有効なパケット（マルチキャスト、ブロードキャスト、ユニキャスト）の総数 |
| Tx Collisions | パケットの送信中に生じた衝突の合計回数 |
| Tx excessLength | パケットの転送が 16 回試行されたために送信されなかったパケットの合計数 |
| Tx ブロードキャスト（Tx broadcast） | デバイスが送信したブロードキャスト パケットの総数 |
| Tx マルチキャスト（Tx multicast） | デバイスが送信したマルチキャスト パケットの総数 |
| LLDP FramesOutTotal | デバイスから送信された LLDP フレームの総数 |
| LLDP AgeoutsTotal | キャッシュ内でタイムアウトになった LLDP フレームの合計数 |
| LLDP FramesDiscardedTotal | 必須の TLV のいずれかが欠落しているか不正である、または文字列の長さが範囲外である場合に廃棄される、LLDP フレームの総数 |
| LLDP FramesInErrorsTotal | 検出可能な 1 つ以上のエラーとともに受信された LLDP フレームの合計数 |
| LLDP FramesInTotal | デバイスで受信された LLDP フレームの総数 |
| LLDP TLVDiscardedTotal | 破棄された LLDP TLV の総数 |
| LLDP TLVUnrecognizedTotal | デバイスで認識されなかった LLDP TLV の総数 |
| CDP ネイバー デバイス ID（CDP Neighbor Device ID） | CDP で検出された、このポートに接続されているデバイスの ID |
| CDP ネイバー IP アドレス（CDP Neighbor IP Address） | CDP で検出されたネイバー デバイスの IP アドレス |
| CDP ネイバー ポート（CDP Neighbor Port） | CDP で検出された、デバイスが接続されているネイバー デバイスのポート |

| 項目 | 説明 |
|---|---|
| LLDP ネイバー デバイス ID（LLDP Neighbor Device ID） | LLDP で検出された、このポートに接続されているデバイスの ID |
| LLDP ネイバー IP アドレス（LLDP Neighbor IP Address） | LLDP で検出されたネイバー デバイスの IP アドレス |
| LLDP ネイバー ポート（LLDP Neighbor Port） | LLDP で検出された、デバイスが接続されているネイバー デバイスのポート |
| ポート情報（Port Information） | 速度とデュプレックス情報 |

# WLAN の設定

デバイスの Web ページに表示される次の [WLAN のセットアップ（WLAN Setup）] ハイパーリングは、ワイヤレス ネットワークのセットアップ情報およびその他の設定に関する情報を提供します。

- 現在の AP
- WLAN 統計情報

**表 *34*：現在の *AP***

| 項目 | 説明 |
|---|---|
| AP 名（AP Name） | 現在のアクセス ポイントの名前を表示します。 |
| MAC アドレス（MAC Address） | アクセス ポイントの MAC アドレスを表示します。 |
| 現在のチャネル（Current Channel） | この AP で測定された最新のチャネル。 |
| 前回の RSSI（Last RSSI） | この AP で測定された最新の RSSI。 |

| 項目 | 説明 |
|---|---|
| ビーコン間隔（Beacon Interval） | ビーコン間の時間単位の数。 時間単位は 1.024 ミリ秒です。 |
| 最小レート（Min Rate） | AP で必要とする最小データ レート。 |
| 最大レート（Max Rate） | AP で必要とする最大データ レート。 |
| WMM サポート済み（WMM Supported） | Wi-Fi マルチメディア エクステンションのサポート。 |
| UAPSD サポート済み（UAPSD Supported） | AP は Unscheduled Automatic Power Save Delivery をサポートします。 WMM がサポートされている場合だけ使用可能です。 この機能は、通話時間にとっても、最大コール密度を実現するためにも重要です。 |
| ノイズ（Noise） | 現在のノイズ レベルを示します。 |
| ロード（Load） | 現在の負荷を示します。 |
| 品質（Quality） | 音声品質を示します。 |

**表 *35*：*WLAN* 統計情報**

| 項目 | 説明 |
|---|---|
| NetDevice 統計 | |
| Tx バイト（Tx Bytes） | デバイスが送信したバイトの総数。 |
| Rx バイト（Rx Bytes） | デバイスが受信したバイトの総数。 |
| Tx パケット（Tx Packets） | デバイスが送信したパケットの総数。 |
| Rx パケット（Rx Packets） | デバイスが受信したパケットの総数 |
| Tx パケット ドロップ（Tx Packets Dropped） | デバイスがドロップした送信パケットの総数。 |

| 項目 | 説明 |
|---|---|
| Rx パケット ドロップ（Rx Packets Dropped） | デバイスがドロップした受信パケットの総数。 |
| Tx パケット エラー（Tx Packets Error） | 送信されたエラー パケットの総数。 |
| Rx パケット エラー（Rx Packets Error） | 受信したエラー パケットの総数。 |
| ファームウェア統計 | |
| マルチキャスト Tx フレーム（Multicast Tx Frames） | デバイスが送信したマルチキャスト パケットの総数。 |
| 失敗しました（Failed） | 失敗したパケットの送信。 |
| 再試行（Retry） | 合計再試行数のカウンタ。 |
| 複数再試行（Multiple Retry） | 成功まで複数の再試行が必要なパケットの送信。 |
| フレーム重複（Frame Dup） | デバイスが受信した重複パケットの数。 |
| RTS 成功（RTS Success） | 対応する CTS を受信しました。 |
| RTS 失敗（RTS Failure） | 対応する CTS が受信されませんでした。 |
| ACK 失敗（ACK Failure） | AP が送信に確認応答しませんでした。 |
| Rx フラグメント（Rx Frag） | デバイスが受信したフラグメント パケットの数。 |
| マルチキャスト Rx フレーム（Multicast Rx Frame） | デバイスが受信したマルチキャスト パケットの数 |

| 項目 | 説明 |
|---|---|
| FCS エラー（FCS Error） | 受信された MPDU でフレーム チェックサム（FCS）エラーが検出されると増加します。 |
| Tx フレーム（Tx Frames） | デバイスが送信したパケット数。 |
| ローミング統計 | |
| 現在/合計（current/total） | 現在のローミング時間/合計ローミング時間（ミリ秒） |

# デバイス ログ

デバイスの Web ページにある次のデバイス ログのハイパーリンクには、デバイスのモニタとトラブルシューティングに役立つ情報が表示されます。デバイス ログ領域にアクセスするには、デバイスの Web ページにアクセスします。

- [コンソール ログ（Console Logs）]：個々のログ ファイルへのハイパーリンクが含まれます。コンソール ログ ファイルには、現在の Syslog、非アクティブ ロードのアーカイブ済みログ、最後のリブートのログ、現在のロードのアーカイブ済みログ、Problem Report Tool によって生成された圧縮済みのログ集合などがあります。
- [コア ダンプ（Core Dumps）]：個々のダンプ ファイルへのハイパーリンクが含まれます。コア ダンプ（tombstone_xx）には、アプリケーションがクラッシュしたときのデータが含まれています。 ANR ファイル（traces.txt）には、デバイスによって応答がないと判断され、ユーザが停止したアプリケーションのデータが含まれています。
- [ステータス メッセージ（Status Messages）]：デバイスに最後に電源が投入されてからデバイスが生成したステータス メッセージの中で最近のものを最大 50 件表示します。 この情報は、デバイスの [ステータス メッセージ（Status Messages）] 画面にも表示されます。
- [デバッグの表示（Debug Display）]：トラブルシューティングのサポートを依頼する際に、Cisco TAC に有用なデバッグ メッセージを提供します。

# ストリームの統計

デバイスは、コール中、または音声やデータを送受信するサービスの実行中に、情報をストリーミングします。

デバイス Web ページの [ストリームの統計（Streaming Statistics）] 領域には、ストリームに関する情報が表示されます。

[ストリームの統計（Streaming Statistics）] 領域を表示するには、デバイスの Web ページにアクセスして、 [ストリーム（Stream）] ハイパーリンクをクリックします。

次の表に、[ストリームの統計（Streaming Statistics）] 領域の項目を示します。

**表 *36*：*[*ストリームの統計（***Streaming Statistics***）*]*領域の項目**

| 項目 | 説明 |
|---|---|
| リモート アドレス（Remote Address） | ストリームの宛先の IP アドレスおよび UDP ポート。 |
| ローカル アドレス（Local Address） | デバイスの IP アドレスおよび UDP ポート。 |
| 開始時間（Start Time） | Cisco Unified Communications Manager がデバイスに対してパケットの送信開始を要求した時間を示す内部タイム スタンプ。 |
| ストリーム ステータス（Stream Status） | ストリーミングがアクティブかどうかを示します。 |
| ホスト名（Host Name） | デバイスの MAC アドレスに基づいてデバイスに自動的に割り当てられる一意の固定された名前。 |
| 送信パケット（Sender Packets） | この接続の開始以降、デバイスが送信した RTP データ パケットの総数。 接続が受信専用に設定されている場合、値は 0 です。 |
| 送信オクテット（Sender Octets） | この接続の開始以降にデバイスが RTP データ パケットで送信したペイロードオクテットの総数。 接続が受信専用に設定されている場合、値は 0 です。 |
| 送信コーデック（Sender Codec） | 送信ストリームに使用された音声符号化のタイプ。 |
| 送信した送信レポート（Sender Reports Sent）（注を参照） | RTCP 送信レポートが送信された回数。 |
| 送信した送信レポート時間（Sender Report Time Sent）（注を参照） | 最後に RTCP 送信レポートが送信された時間を示す内部タイム スタンプ。 |
| 受信喪失パケット（Receiver Lost Packets） | この接続でのデータの受信を開始してから失われた RTP データ パケットの総数。 予期されたパケット数から受信されたパケット数を差し引いた値として定義されます。受信パケット数には、遅延または重複パケットも含まれます。 接続が送信専用に設定されていた場合、値は 0 として表示されます。 |

| 項目 | 説明 |
|---|---|
| 平均ジッター（Avg Jitter） | RTP データ パケットの内部到着時間の平均偏差の推定値（ミリ秒単位）。 接続が送信専用に設定されていた場合、値は 0 として表示されます。 |
| 受信コーデック（Receiver Codec） | 受信ストリームに使用された音声符号化のタイプ。 |
| 送信した受信レポート（Receiver Reports Sent）（注を参照） | RTCP 受信レポートが送信された回数。 |
| 送信した受信レポート時間（Receiver Report Time Sent）（注を参照） | RTCP 受信レポートが送信された時間を示す内部タイム スタンプ。 |
| 受信パケット（Receiver Packets） | この接続でのデータ受信の開始以降、デバイスが受信した RTP データ パケットの総数。 マルチキャスト コールの場合は、さまざまな送信元から受信したパケットが含まれます。 接続が送信専用に設定されていた場合、値は 0 として表示されます。 |
| 受信オクテット（Receiver Octets） | この接続での受信を開始してからデバイスが RTP データ パケットで受信したペイロード オクテットの総数。 マルチキャスト コールの場合は、さまざまな送信元から受信したパケットが含まれます。 接続が送信専用に設定されていた場合、値は 0 として表示されます。 |
| 累積フレーム損失率（Cumulative Conceal Ratio） | 隠蔽フレームの総数を、音声ストリームの開始以降に受信された音声フレームの総数で割った値。 |
| 直近フレーム損失率（Interval Conceal Ratio） | アクティブな音声に先行する 3 秒間の間隔における、音声フレームに対する隠蔽フレームの比率。 音声アクティビティ検出（VAD）を使用する場合は、3 秒間のアクティブな音声としてより長い間隔が必要になることがあります。 |
| 最大フレーム損失率（Max Conceal Ratio） | 音声ストリームの開始以降、最も高い間隔の損失率。 |
| フレーム損失発生秒数（Conceal Secs） | 音声ストリームの開始以降、隠蔽イベント（フレーム損失）があった秒数（[深刻なフレーム損失発生秒数（Severely Conceal Secs）] の値を含む）。 |
| 深刻なフレーム損失発生秒数（Severely Conceal Secs） | 音声ストリームの開始以降、5% を超える隠蔽イベント（フレーム損失）があった秒数。 |

| 項目 | 説明 |
| --- | --- |
| 遅延（Latency）（注を参照） | ネットワーク遅延の推定値（ミリ秒単位）。ラウンドトリップ遅延の実行中の平均値を表します。これは、RTCP 受信レポート ブロックの受信時に測定されます。 |
| 最大ジッター（Max Jitter） | 瞬時ジッターの最大値（ミリ秒単位）。 |
| 送信サイズ（Sender Size） | 送信ストリームの RTP パケット サイズ（ミリ秒単位）。 |
| 受信した送信レポート（Sender Reports Received）（注を参照） | RTCP 送信レポートが受信された回数。 |
| 受信した送信レポート時間（Sender Report Time Received）（注を参照） | RTCP 送信レポートが最後に受信された時間。 |
| 受信サイズ（Receiver Size） | 受信ストリームの RTP パケット サイズ（ミリ秒単位）。 |
| 受信破棄（Receiver Discarded） | ネットワークから受信されたが、ジッターバッファから廃棄された RPT パケット。 |
| 受信した受信レポート（Receiver Reports Received）（注を参照） | RTCP 受信レポートが受信された回数。 |
| 受信した受信レポート時間（Receiver Report Time Received）（注を参照） | RTCP 受信レポートが最後に受信された時間。 |
| 受信暗号化（Receiver Encrypted） | 受信ストリームが暗号化されるかどうかを示します。 |
| 送信暗号化（Sender Encrypted） | 送信ストリームが暗号化されるかどうかを示します。 |
| 送信フレーム（Sender Frames） | ビデオ ストリームが開始されて以降、デバイスが送信したビデオ フレーム数。 |
| 送信部分フレーム（Sender Partial Frames） | ビデオ ストリームが開始されて以降、デバイスが送信した P フレーム数。 |
| 送信 I フレーム（Sender IFrames） | ビデオ ストリームが開始されて以降、デバイスが送信した I フレーム数。 |
| 送信フレームレート（Sender Frame Rate） | ビデオ フレームが送信されたレート（フレーム/秒）。 |

| 項目 | 説明 |
|---|---|
| 送信帯域幅（Sender Bandwidth） | 送信されたビデオ ストリームの帯域幅（kbps）。 |
| 送信解像度（Sender Resolution） | デバイスから送信されたビデオ ストリームの解像度。 |
| 受信フレーム（Receiver Frames） | ビデオ ストリームが開始されて以降、デバイスが受信したビデオ フレーム数。 |
| 受信部分フレーム（Receiver Partial Frames） | ビデオ ストリームが開始されて以降、デバイスが受信したPフレーム数。 |
| 受信 I フレーム（Receiver IFrames） | ビデオ ストリームが開始されて以降、デバイスが受信したIフレーム数。 |
| 受信 I フレーム要求（Receiver IFrames Req） | ビデオ ストリームが開始されて以降、デバイスがリモート エンドポイントに送信した IDR 要求数。 |
| 受信フレーム レート（Receiver Frame Rate） | ビデオ フレームが受信されたレート（フレーム/秒）。 |
| 受信フレーム損失（Receiver Frames Lost） | ビデオ ストリームが開始されて以降、ビデオデコーダが報告したフレーム損失数。 |
| 受信フレーム エラー（Receiver Frames Errors） | ビデオ ストリームが開始されて以降、ビデオデコーダが報告したエラー数。 |
| 受信帯域幅（Receiver Bandwidth） | 受信されたビデオ ストリームの帯域幅（kbps）。 |
| 受信解像度（Receiver Resolution） | 電話機がリモート エンドポイントから受信したビデオ ストリームの解像度。 |
| ドメイン名（Domain Name） | ドメイン名を示します。 |
| 送信参加（Sender Joins） | デバイスがストリームの送信を開始した回数。 |
| 受信参加（Receiver Joins） | デバイスがストリームの受信を開始した回数 |
| BYE（Byes） | デバイスがストリームの送信を停止した回数。 |
| 送信開始時間（Sender Start Time） | 最初の RTP パケットがネットワークに送信された時間を示すタイムスタンプ。 |
| 受信開始時刻（Receiver Start Time） | 最初の RTP パケットがネットワークから受信された時間を示すタイムスタンプ。 |

| 項目 | 説明 |
|---|---|
| 送信の DSCP（Sender DSCP） | 送信側 SIP シグナリング パケットの DSCP 値。 |
| 受信の DSCP（Receiver DSCP） | 受信側 SIP シグナリング パケットの DSCP 値。 |
| 送信の RTCP DSCP（Sender RTCP DSCP） | 送信側 RTP パケットの DSCP 値。 |
| 受信の RTCP DSCP（Receiver RTCP DSCP） | 送信側 RTP パケットの DSCP 値。 |
| ビデオ（Is Video） | ビデオ コールを示します。 |
| プレゼンテーション（Is Presentation） | プレゼンテーション コールを示します。 |
| 送信側アクティブ（Sender Active） | 送信側がアクティブであることを示します。 |
| 受信側アクティブ（Receiver Active） | 受信側がアクティブであることを示します。 |

（注） RTP 制御プロトコルが無効になっている場合、このフィールドのデータは生成されないため、0 が表示されます。

付 録 A

# 認証局信頼リスト


- 認証局信頼リスト，215 ページ


## 認証局信頼リスト

次に、デバイスに組み込まれている信頼できる認証局の一覧を示します。 Expressway 経由でモバイルおよびリモート アクセスを実行する場合は、Expressway サーバがこれらの認証局のいずれかに対して署名されている必要があります。

```
--------------------------------------------------------------------
subject=  C=NL O=Staat der Nederlanden CN=Staat der Nederlanden Root CA
--------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 3 Public Primary Certification Authority - G3
--------------------------------------------------------------------
subject=  C=HU L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock
Minositett Kozjegyzoi (Class QA) Tanusitvanykiado emailAddress=info@netlock.hu
--------------------------------------------------------------------
subject=  C=TR L=Gebze - Kocaeli O=T\xC3\xBCrkiye Bilimsel ve Teknolojik Ara\xC5\x9Ft\xC4\xB1rma
 Kurumu - T\xC3\x9CB\xC4\xB0TAK OU=Ulusal Elektronik ve Kriptoloji Ara\xC5\x9Ft\xC4\xB1rma
Enstit\xC3\xBCs\xC3\xBC - UEKAE OU=Kamu Sertifikasyon Merkezi CN=T\xC3\x9CB\xC4\xB0TAK
UEKAE K\xC3\xB6k Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1 - S\xC3\xBCr\xC3\xBCm
 3
--------------------------------------------------------------------
subject=  C=BM O=QuoVadis Limited CN=QuoVadis Root CA 3
--------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 1 Public Primary Certification Authority - G3
--------------------------------------------------------------------
subject=  C=DK O=TDC Internet OU=TDC Internet Root CA
--------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 2007 VeriSign, Inc. - For authorized
 use only CN=VeriSign Class 3 Public Primary Certification Authority - G4
--------------------------------------------------------------------
subject=  C=ZA ST=Western Cape L=Cape Town O=Thawte Consulting cc OU=Certification Services
Division CN=Thawte Server CA emailAddress=server-certs@thawte.com
--------------------------------------------------------------------
subject=  O=RSA Security Inc OU=RSA Security 2048 V3
```

認証局信頼リスト

```
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=Class 1 Public Primary Certification Authority - G2 OU=(c) 1998
VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---------------------------------------------------------------------
subject=  C=US O=The Go Daddy Group, Inc. OU=Go Daddy Class 2 Certification Authority
---------------------------------------------------------------------
subject=  C=US O=AffirmTrust CN=AffirmTrust Networking
---------------------------------------------------------------------
subject=  C=SK L=Bratislava O=Disig a.s. CN=CA Disig
---------------------------------------------------------------------
subject=  C=FR O=Certinomis OU=0002 433998903 CN=Certinomis - Autorit\xC3\xA9 Racine
---------------------------------------------------------------------
subject=  C=SE O=AddTrust AB OU=AddTrust External TTP Network CN=AddTrust External CA Root
---------------------------------------------------------------------
subject=  L=ValiCert Validation Network O=ValiCert, Inc. OU=ValiCert Class 2 Policy Validation Authority
 CN=http:  www.valicert.com  emailAddress=info@valicert.com
---------------------------------------------------------------------
subject=  C=US O=GeoTrust Inc. CN=GeoTrust Primary Certification Authority
---------------------------------------------------------------------
subject=  O=Cisco CN=ACT2 ECC SUDI CA
---------------------------------------------------------------------
subject=  C=EU O=AC Camerfirma SA CIF A82743287 OU=http:  www.chambersign.org CN=Global
Chambersign Root
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 2008 VeriSign, Inc. - For authorized
 use only CN=VeriSign Universal Root Certification Authority
---------------------------------------------------------------------
subject=  C=JP O=SECOM Trust.net OU=Security Communication RootCA1
---------------------------------------------------------------------
subject=  C=FI O=Sonera CN=Sonera Class2 CA
---------------------------------------------------------------------
subject=  C=US O=America Online Inc. CN=America Online Root Certification Authority 1
---------------------------------------------------------------------
subject=  C=US O=Equifax Secure OU=Equifax Secure eBusiness CA-2
---------------------------------------------------------------------
subject=  C=US O=GeoTrust Inc. OU=(c) 2008 GeoTrust Inc. - For authorized use only CN=GeoTrust Primary
 Certification Authority - G3
---------------------------------------------------------------------
subject=  C=US O=SecureTrust Corporation CN=Secure Global CA
---------------------------------------------------------------------
subject=  C=GB O=Trustis Limited OU=Trustis FPS Root CA
---------------------------------------------------------------------
subject=  C=JP O=Japan Certification Services, Inc. CN=SecureSign RootCA11
---------------------------------------------------------------------
subject=  C=IL O=StartCom Ltd. OU=Secure Digital Certificate Signing CN=StartCom Certification Authority
---------------------------------------------------------------------
subject=  C=US O=Digital Signature Trust OU=DST ACES CN=DST ACES CA X6
---------------------------------------------------------------------
subject=  emailAddress=pki@sk.ee C=EE O=AS Sertifitseerimiskeskus CN=Juur-SK
---------------------------------------------------------------------
subject=  C=US ST=Arizona L=Scottsdale O=GoDaddy.com, Inc. CN=Go Daddy Root Certificate Authority
 - G2
---------------------------------------------------------------------
subject=  C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http:  www.usertrust.com
CN=UTN-USERFirst-Hardware
---------------------------------------------------------------------
subject=  C=NO O=Buypass AS-983163327 CN=Buypass Class 2 Root CA
---------------------------------------------------------------------
```

subject= C=EU L=Madrid (see current address at www.camerfirma.com address) serialNumber=A82743287 O=AC Camerfirma S.A. CN=Global Chambersign Root - 2008
---
subject= C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 2006 VeriSign, Inc. - For authorized use only CN=VeriSign Class 3 Public Primary Certification Authority - G5
---
subject= O=Cisco CN=Cisco ECC Root CA
---
subject= C=DE O=T-Systems Enterprise Services GmbH OU=T-Systems Trust Center CN=T-TeleSec GlobalRoot Class 3
---
subject= C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Assured ID Root CA
---
subject= C=CH O=SwissSign AG CN=SwissSign Platinum CA - G2
---
subject= C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http: www.usertrust.com CN=UTN - DATACorp SGC
---
subject= C=CH O=WISeKey OU=Copyright (c) 2005 OU=OISTE Foundation Endorsed CN=OISTE WISeKey Global Root GA CA
---
subject= C=NL O=Staat der Nederlanden CN=Staat der Nederlanden Root CA - G2
---
subject= O=Cisco CN=Cisco Licensing Root CA
---
subject= C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http: www.usertrust.com CN=UTN-USERFirst-Network Applications
---
subject= C=ch O=Swisscom OU=Digital Certificate Services CN=Swisscom Root CA 1
---
subject= C=JP O=SECOM Trust Systems CO.,LTD. OU=Security Communication RootCA2
---
subject= C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert High Assurance EV Root CA
---
subject= C=HU L=Budapest O=NetLock Kft. OU=Tan\xC3\xBAs\xC3\xADtv\xC3\xA1nykiad\xC3\xB3k (Certification Services) CN=NetLock Arany (Class Gold) F\xC5\x91tan\xC3\xBAs\xC3\xADtv\xC3\xA1ny
---
subject= C=NO O=Buypass AS-983163327 CN=Buypass Class 3 CA 1
---
subject= C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized use only CN=VeriSign Class 2 Public Primary Certification Authority - G3
---
subject= C=PL O=Unizeto Sp. z o.o. CN=Certum CA
---
subject= C=ZA ST=Western Cape L=Cape Town O=Thawte Consulting cc OU=Certification Services Division CN=Thawte Premium Server CA emailAddress=premium-server@thawte.com
---
subject= C=TW O=Chunghwa Telecom Co., Ltd. OU=ePKI Root Certification Authority
---
subject= C=US O=VeriSign, Inc. OU=Class 2 Public Primary Certification Authority
---
subject= L=ValiCert Validation Network O=ValiCert, Inc. OU=ValiCert Class 3 Policy Validation Authority CN=http: www.valicert.com emailAddress=info@valicert.com
---
subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Universal CA CN=TC TrustCenter Universal CA I
---
subject= C=EU O=AC Camerfirma SA CIF A82743287 OU=http: www.chambersign.org CN=Chambers

認証局信頼リスト

of Commerce Root
---
subject= C=US O=VISA OU=Visa International Service Association CN=Visa eCommerce Root
---
subject= C=FR O=Certplus CN=Class 2 Primary CA
---
subject= C=US O=VeriSign, Inc. OU=Class 3 Public Primary Certification Authority
---
subject= C=FI O=Sonera CN=Sonera Class1 CA
---
subject= OU=GlobalSign Root CA - R2 O=GlobalSign CN=GlobalSign
---
subject= C=EU L=Madrid (see current address at www.camerfirma.com address) serialNumber=A82743287 O=AC Camerfirma S.A. CN=Chambers of Commerce Root - 2008
---
subject= C=PL O=Unizeto Technologies S.A. OU=Certum Certification Authority CN=Certum Trusted Network CA
---
subject= C=US O=Equifax Secure Inc. CN=Equifax Secure Global eBusiness CA-1
---
subject= C=JP O=Japanese Government OU=ApplicationCA
---
subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Class 3 CA CN=TC TrustCenter Class 3 CA II
---
subject= C=US O=VeriSign, Inc. OU=Class 3 Public Primary Certification Authority - G2 OU=(c) 1998 VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---
subject= C=DE O=Deutsche Telekom AG OU=T-TeleSec Trust Center CN=Deutsche Telekom Root CA 2
---
subject= C=US O=America Online Inc. CN=America Online Root Certification Authority 2
---
subject= C=DK O=TDC CN=TDC OCES CA
---
subject= C=US O=SecureTrust Corporation CN=SecureTrust CA
---
subject= C=HU L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock Uzleti (Class B) Tanusitvanykiado
---
subject= C=CN O=CNNIC CN=CNNIC ROOT
---
subject= CN=EBG Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1 O=EBG Bili\xC5\x9Fim Teknolojileri ve Hizmetleri A.\xC5\x9E. C=TR
---
subject= C=US O=GeoTrust Inc. OU=(c) 2007 GeoTrust Inc. - For authorized use only CN=GeoTrust Primary Certification Authority - G2
---
subject= C=US O=VeriSign, Inc. OU=Class 1 Public Primary Certification Authority
---
subject= C=US O=thawte, Inc. OU=Certification Services Division OU=(c) 2006 thawte, Inc. - For authorized use only CN=thawte Primary Root CA
---
subject= C=US ST=Arizona L=Scottsdale O=Starfield Technologies, Inc. CN=Starfield Services Root Certificate Authority - G2
---
subject= O=Cisco CN=Cisco Root CA M2
---
subject= C=US O=Wells Fargo OU=Wells Fargo Certification Authority CN=Wells Fargo Root Certificate

Authority
---
subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Universal CA CN=TC TrustCenter Universal CA III
---
subject= C=US O=GTE Corporation OU=GTE CyberTrust Solutions, Inc. CN=GTE CyberTrust Global Root
---
subject= C=US O=Entrust.net OU=www.entrust.net CPS incorp. by ref. (limits liab.) OU=(c) 1999 Entrust.net Limited CN=Entrust.net Secure Server Certification Authority
---
subject= C=CH O=SwissSign AG CN=SwissSign Silver CA - G2
---
subject= C=NO O=Buypass AS-983163327 CN=Buypass Class 2 CA 1
---
subject= C=US O=VeriSign, Inc. OU=Class 3 Public Primary Certification Authority
---
subject= C=US O=DigiCert Inc OU=www.digicert.com CN=DigiCert Global Root CA
---
subject= C=US O=thawte, Inc. OU=(c) 2007 thawte, Inc. - For authorized use only CN=thawte Primary Root CA - G2
---
subject= C=HU ST=Hungary L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado
---
subject= C=US O=Starfield Technologies, Inc. OU=Starfield Class 2 Certification Authority
---
subject= C=DE O=TC TrustCenter GmbH OU=TC TrustCenter Class 2 CA CN=TC TrustCenter Class 2 CA II
---
subject= C=ES CN=Autoridad de Certificacion Firmaprofesional CIF A62634068
---
subject= C=FR O=Dhimyotis CN=Certigna
---
subject= C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http: www.usertrust.com CN=UTN-USERFirst-Client Authentication and Email
---
subject= C=BE O=GlobalSign nv-sa OU=Root CA CN=GlobalSign Root CA
---
subject= C=US O=Entrust, Inc. OU=www.entrust.net CPS is incorporated by reference OU=(c) 2006 Entrust, Inc. CN=Entrust Root Certification Authority
---
subject= C=US O=VeriSign, Inc. OU=Class 2 Public Primary Certification Authority - G2 OU=(c) 1998 VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---
subject= C=US ST=Arizona L=Scottsdale O=Starfield Technologies, Inc. CN=Starfield Root Certificate Authority - G2
---
subject= C=US O=VeriSign, Inc. OU=Class 4 Public Primary Certification Authority - G2 OU=(c) 1998 VeriSign, Inc. - For authorized use only OU=VeriSign Trust Network
---
subject= C=US OU=www.xrampsecurity.com O=XRamp Security Services Inc CN=XRamp Global Certification Authority
---
subject= C=US O=AffirmTrust CN=AffirmTrust Premium ECC
---
subject= C=US O=VeriSign, Inc. OU=VeriSign Trust Network OU=(c) 1999 VeriSign, Inc. - For authorized use only CN=VeriSign Class 4 Public Primary Certification Authority - G3
---

認証局信頼リスト

```
subject=  C=BM O=QuoVadis Limited CN=QuoVadis Root CA 2
---------------------------------------------------------------------
subject=  C=CO O=Sociedad Cameral de Certificaci\xC3\xB3n Digital - Certic\xC3\xA1mara S.A. CN=AC
 Ra\xC3\xADz Certic\xC3\xA1mara S.A.
---------------------------------------------------------------------
subject=  C=US O=VeriSign, Inc. OU=Class 1 Public Primary Certification Authority
---------------------------------------------------------------------
subject=  C=TW O=TAIWAN-CA OU=Root CA CN=TWCA Root Certification Authority
---------------------------------------------------------------------
subject=  C=GB ST=Greater Manchester L=Salford O=Comodo CA Limited CN=AAA Certificate Services
---------------------------------------------------------------------
subject=  C=US O=Equifax OU=Equifax Secure Certificate Authority
---------------------------------------------------------------------
subject= C=AT O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU=A-Trust-nQual-03
 CN=A-Trust-nQual-03
---------------------------------------------------------------------
subject=  C=IE O=Baltimore OU=CyberTrust CN=Baltimore CyberTrust Root
---------------------------------------------------------------------
subject=  OU=GlobalSign Root CA - R3 O=GlobalSign CN=GlobalSign
---------------------------------------------------------------------
subject=  C=HK O=Hongkong Post CN=Hongkong Post Root CA 1
---------------------------------------------------------------------
subject=  C=US O=AffirmTrust CN=AffirmTrust Premium
---------------------------------------------------------------------
subject=  C=CH O=SwissSign AG CN=SwissSign Gold CA - G2
---------------------------------------------------------------------
subject=  C=US O=Equifax Secure Inc. CN=Equifax Secure eBusiness CA-1
---------------------------------------------------------------------
subject=  O=Digital Signature Trust Co. CN=DST Root CA X3
---------------------------------------------------------------------
subject=  C=NO O=Buypass AS-983163327 CN=Buypass Class 3 Root CA
---------------------------------------------------------------------
subject=  C=US O=GeoTrust Inc. CN=GeoTrust Global CA
---------------------------------------------------------------------
subject=  C=BM O=QuoVadis Limited OU=Root Certification Authority CN=QuoVadis Root Certification
Authority
---------------------------------------------------------------------
subject=  O=Cisco Systems CN=Cisco Root CA 2048
---------------------------------------------------------------------
subject=  C=US ST=UT L=Salt Lake City O=The USERTRUST Network OU=http:  www.usertrust.com
CN=UTN-USERFirst-Object
---------------------------------------------------------------------
subject=  C=HU L=Budapest O=NetLock Halozatbiztonsagi Kft. OU=Tanusitvanykiadok CN=NetLock
Expressz (Class C) Tanusitvanykiado
---------------------------------------------------------------------
subject=  O=Cisco Systems CN=Cisco Manufacturing CA
---------------------------------------------------------------------
subject=  L=ValiCert Validation Network O=ValiCert, Inc. OU=ValiCert Class 1 Policy Validation Authority
 CN=http:  www.valicert.com  emailAddress=info@valicert.com
---------------------------------------------------------------------
subject=  C=US O=Wells Fargo WellsSecure OU=Wells Fargo Bank NA CN=WellsSecure Public Root
Certificate Authority
---------------------------------------------------------------------
subject= C=US O=thawte, Inc. OU=Certification Services Division OU=(c) 2008 thawte, Inc. - For authorized
 use only CN=thawte Primary Root CA - G3
---------------------------------------------------------------------
subject=  C=IT L=Milan O=Actalis S.p.A. 03358520967 CN=Actalis Authentication Root CA
---------------------------------------------------------------------
```

```
subject=  O=Cisco CN=ACT2 SUDI CA
-----------------------------------------------------------------------
subject=  C=US O=AffirmTrust CN=AffirmTrust Commercial
-----------------------------------------------------------------------
subject=  C=RO O=certSIGN OU=certSIGN ROOT CA
-----------------------------------------------------------------------
subject=  C=GR O=Hellenic Academic and Research Institutions Cert. Authority CN=Hellenic Academic
and Research Institutions RootCA 2011
-----------------------------------------------------------------------
subject=  C=JP O=SECOM Trust Systems CO.,LTD. OU=Security Communication EV RootCA1
-----------------------------------------------------------------------
```

認証局信頼リスト