Cisco DX シリーズ管理ガイド、リリース 10.2(5)

初版：2015 年 12 月 9 日

最終更新：2020 年 7 月 13 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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

【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。

【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。

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

目 次

はじめに

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 デバイスを理解し、インストール、構成、および管理するため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、ユーザーを対象にしていないネットワーク設定値の構成が含まれます。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、以下の表記法を使用しています。

表記法	説明
▿太字▵	コマンドおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で表記されています。
[]	角カッコの中の要素は、省略可能です。

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

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

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

警告は、次のように表しています。

注目 安全上の重要事項

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

これらの注意事項を保管しておいてください。

Related Documentation

Cisco DX シリーズ

All Cisco DX シリーズ documentation is available at the following URL:

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

User-oriented documents are available at the following URL:

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

Administrator-oriented documentation is available at the following URL:

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

The 『*Cisco DX Series Wireless LAN Deployment Guide*』 is available at the following URL:

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

Translated publications are available at the following URL:

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

Open Source license information is available as the following URL:

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 is available at the following URL:

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

Cisco Unified Communications Manager

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

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

Cisco Business Edition 6000

Refer to the *Cisco Business Edition 6000 Documentation Guide* and other publications that are specific to your Cisco Business Edition 6000 release. Navigate from the following URL:

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

Cisco and the Environment

Related publications are available at the following URL:

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

用語の違い

次の表に、『Cisco DX シリーズ ユーザー ガイド』、『*Cisco DX* シリーズ 管理ガイド』、『『*Cisco Unified Communications Manager Administration Guide*』』で使用される用語の違いをいくつか説明します。

表 *1*: 用語の違い

ユーザ ガイド	管理ガイド
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、サポート、およびセキュリティ ガイドライン

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

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

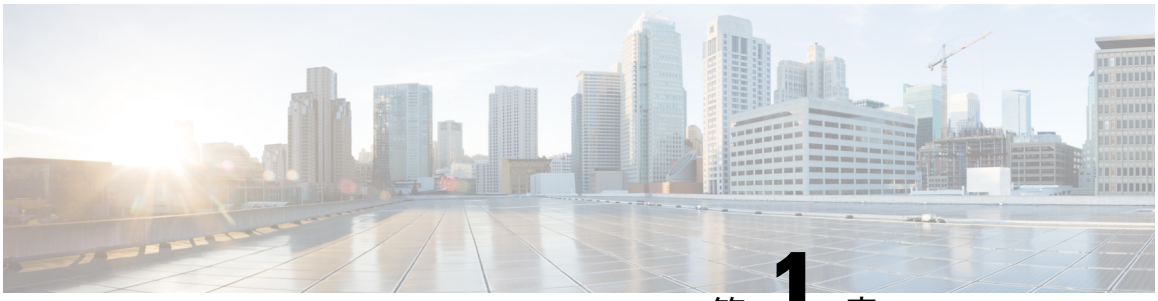
『*What's New in Cisco Product Documentation*』はRSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。Cisco は現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティの概要

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

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

はじめに

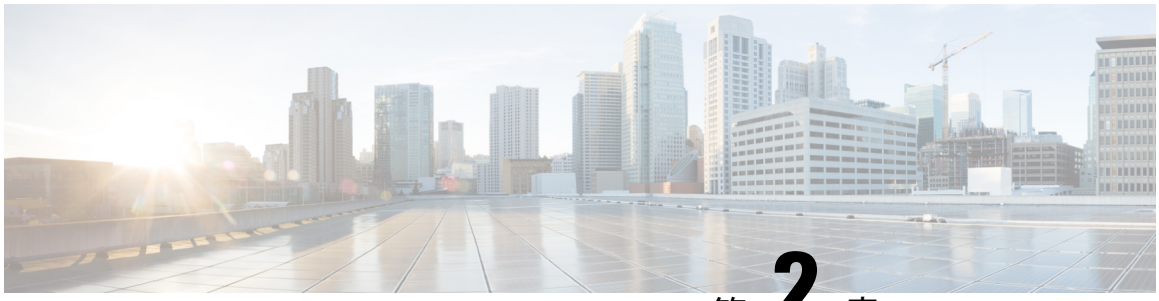


第 1 章

新機能および変更された機能に関する情報

リリース 10.2(5) の新機能および変更

新しいコンテンツおよび変更されたコンテンツ	セクション
無線ハードウェアの追加なし	No Radio ハードウェア （24 ページ）
代理電話帳サービスを追加	代替電話帳サーバーの設定 （70 ページ）
FIPS モードの追加	製品固有オプションの構成 （125 ページ）
Cisco DX650 のデフォルトの壁紙の寸法とフォルダを更新	デフォルトの壁紙指定（DX650） （148 ページ）
連絡先検索の更新	連絡先検索 （71 ページ）
自動問題レポート アップロードを追加	製品固有オプションの構成 （125 ページ）
設定に管理者パスワードを追加	設定での管理者パスワードの設定 （107 ページ）



第 2 章

技術仕様

物理環境および動作環境に関する仕様

表 *2 : Cisco DX* シリーズ デバイスの物理仕様と動作仕様

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 mm）X 13.91 インチ（353.1 mm）X 2.45 インチ（62.3 mm） Cisco DX80：20.2 インチ（51 2 mm）X 22.2 インチ（565 mm）X 3.5 インチ（89 mm） 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）
ウェイト（Weight）	Cisco DX70：8.5 ポンド（3.9 kg） Cisco DX80：15.65 ポンド（7.1 kg） Cisco DX650：3.81 ポンド（1.73 kg）
動作温度	0 ～ 40°C（32 ～ 104°F）
動作相対湿度	10 ～ 95 %（結露しないこと）
保管温度	-10 ～ 60 °C（14 ～ 140 °F）

仕様	値または範囲
電力、Cisco DX70	定格：12 V（最大）で 3.5 A 低電力スタンバイ モード 統合型 EnergyWise サポート
電力、Cisco DX80	定格：最大 60 W 低電力スタンバイ モード 統合型 EnergyWise サポート
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。 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。 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	2 ポート Cisco イーサネット スイッチ内蔵 IEEE 802.11 a/b/g/n Wi-Fi
音声コーデックのサポート	ナローバンド音声圧縮コーデック：G.711a、G.711u、G.729a、G.729ab、Internet Low Bitrate Codec（iLBC） ワイドバンド音声圧縮コーデック：G.722、Internet Speech Audio Codec（iSAC）、iLBC、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 Cisco DX80：TI OMAP 4470 1.5GHz デュアル コア ARM Cortex-A9 プロセッサ Cisco DX650：TI OMAP 4460 1.5 GHz デュアル コア ARM Cortex-A9 プロセッサ
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されるネットワーク ポートとコンピュータ（アクセス）ポートが含まれます。これらは異なる目的で使用され、ポートのピン割り当ても異なります。

- ネットワーク ポートは 110/100/1000 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+

ピン番号	機能
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

以下の表では、Cisco DX シリーズデバイスが使用するポートを説明します。詳細については、『*Cisco Unified Communications Manager* の *TCP* および *UDP* ポート使用ガイド』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	基盤となるプロトコル	プロトコル/サービス	注記
68	67	-	DHCP クライアント	ダイナミック IP アドレスを取得するための DHCP サポート
49152-53248	53	UDP	DNS クライアント	名前解決の DNS サポート
49152-53248	69	UDP	TFTP クライアント	中央サーバからさまざまなコンフィギュレーションファイルや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	サーバーの構成	TCP/UDP	HTTP サーバ	
123	123	UDP	NTP クライアント	時刻を取得する Network Time Protocol
49152-53248	サーバーの構成	TCP	HTTP クライアント	

送信元ポート	リモート デバイス ポート	基盤となるプロトコル	プロトコル/サービス	注記
49152-53248	6970	TCP	TFTP クライアント	中央サーバーからさまざまな構成ファイルや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。管理者は変更できます。
16384- 32767	受信範囲	UDP	RTP	管理者はポート範囲を構成できます。
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	サーバーの構成	TCP	セキュア シェル	
4051		TCP		アップグレードのロード
4052		RDP		アップグレードのロード
4061				特殊なデバッグ
8443				連絡先検索

Network Protocols

Cisco DX シリーズ devices support several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the devices support.

Table 6: Supported Network Protocols

Network Protocol	Purpose	Usage Notes
Binary Floor Control Protocol (BFCP)	BFCP allows users to share a presentation within an ongoing video conversation.	BFCP is autom

Network Protocol	Purpose	Usage Notes
Bluetooth	Bluetooth is a wireless personal area network (WPAN) protocol that specifies how devices communicate over short distances.	The devices suppo The devices suppor Advanced Audio D Human Interface D Push Profile (OPP Profile (PBAP).
Bootstrap Protocol (BootP)	BootP enables a network device to discover certain startup information, such as the IP address.	—
Cisco Discovery Protocol (CDP)	CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment. Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.	The device uses C information, such per-port power ma Quality of Service information, with
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is a Cisco proprietary protocol that is used to form a peer-to-peer hierarchy of devices. This hierarchy is used to distribute firmware files from peer devices to their neighboring devices.	The Peer Firmwar CPPDP.
Dynamic Host Configuration Protocol (DHCP)	DHCP dynamically allocates and assigns an IP address to network devices. DHCP enables you to connect a device into the network and for that device to become operational without the need to manually assign an IP address or to configure additional network parameters.	DHCP is enabled b you must manually subnet mask, gatev each device locally Cisco recommends option 150. With t the TFTP server IP For additional supp see the “Dynamic Protocol” chapter a in the *Cisco Unifi Manager System C* **Note** If you cann try using D
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Devices use HTTP troubleshooting pu
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	Web applications w support have two U that support HTTP

Network Protocol	Purpose	Usage Notes
IEEE 802.1X	The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication succeeds, normal traffic can pass through the port.	Devices implem by providing su authentication EAP-TLS. When 802.1X a device, you sho voice VLAN.
IEEE 802.11a/b/g/n	The IEEE 802.11 standard specifies how devices communication over a wireless local area network (WLAN). 802.11a operates at the 5 GHz band, and 802.11b and 802.11g operate at the 2.4 GHz band. 802.11.n operates in either 2.4 GHz or 5Ghz band.	The 802.11 int for cases when or undesirable.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communica must have an a name, gateway IP addresses, s identifications you are using t Configuration using DHCP, y properties to ea The device sup information, se *Guide for Cisc* *Manager*』, "I (IPv6)" chapte
Link Layer Discovery Protocol (LLDP)	LLDP is a standardized network discovery protocol (similar to CDP) that is supported on some Cisco and third-party devices.	The device sup
Link Layer Discovery Protocol - Media Endpoint Devices (LLDP-MED)	LLDP-MED is an extension of the LLDP standard for voice products.	The device sup port to commu • Voice VL • Device di • Power ma • Inventory For more infor support, see th Discovery Prot http://www.cisc technologies_w paper0900aecd

Network Protocol	Purpose	Usage Notes
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	The device uses th receive real-time v phones and gatewa
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round-trip delay) on RTP streams. RTCP is also used to synchronize the audio and video stream in order to provide a better video experience.	RTCP for audio ca RTCP for video ca streams and video enabled by default RTCP on individu Unified Communi Administration.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, s detection, and com configured on a gl Communications M in operation. Some configuration of th endpoint itself.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP pr functions of signali within a packet tel allows transportati network boundarie provides the ability an end-to-end call.
Telepresence Interoperability Protocol (TIP)/Multiplex (MUX)	TIP/MUX is an IP protocol that is used to negotiate audio and video media options between endpoints prior to reception or transmission of media.	TIP/MUX is invok conferences and en
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	The device uses TC Unified Communi access XML servic
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	Upon security impl the TLS protocol v with Cisco Unified
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the device, TFTP enables you to obtain a configuration file specific to the device type.	TFTP requires a T that the DHCP ser identify. If you wa server other than th specifies, you mus address of the TFT Settings applicatio For more informat chapter in the *Cisc Manager System C*

Network Protocol	Purpose	Usage Notes
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used or signaling on the

電力要件

Cisco DX シリーズ デバイスは外部電源で動作します。外部電源は個別の電源装置によって提供されます。

Cisco DX650 Power over Ethernet（PoE）で電力を供給することもできます。スイッチはイーサネット ケーブル経由で PoE を提供できます。

（注） 外部電源を使用する場合、イーサネット ケーブルを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。

電力に関する注意事項

Cisco DX70 および Cisco DX80 に電源を供給するには、付属の Lite-On PA-1600-2A-LF 電源または FSP075-DMAA1 を使用します。Cisco DX650 に電力を供給するには、次の表を参照してください。

表 *7 : Cisco DX650* 電力のガイドライン

電源の種類	ガイドライン
外部電源：CP-PWR-CUBE-4 外部電源を通じて電力を供給	デバイスでは、CP-PWR-CUBE-4 電源を使用します。 （注） ワイヤレス ネットワークにデバイスを展開する場合は、CP-PW 使用する必要があります。
[外部電源（External power）]：Cisco Unified IP 電話 パワー インジェクタ経由で供給	Cisco Unified IP 電話 パワー インジェクタは Cisco DX650 で使用できま 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 パワーを供給します。Cisco Unified IP 電話 パワーインジェクタは、ス と電話間に接続されます。また、通電していないスイッチと電話間で ケーブル長をサポートします。

電源の種類	ガイドライン
[PoE 電源（PoE power）]：イーサネット ケーブルを介して電話機に接続されているスイッチを通じて電力を供給。	Cisco DX650 は、IEEE 802.3af クラス 3 電源オン信号ペアおよびスペア ペトします。 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 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 ります。 スイッチ上で実行している CatOS または IOS のバージョンが、予定して 配置をサポートしていることを確認します。オペレーティング システム ンに関する情報については、スイッチのマニュアルを参照してください。 NG-PoE+ のサポート：NG-PoE+ スイッチがサポートされている限り、デ IEEE 802.3at よりも多くの電力を消費できます。

電力削減

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

Power Saveモード

Power Saveモードでは、デバイスが使用されていないときにはスクリーンのバックライトが消灯します。デバイスは、ユーザーがハンドセットを持ち上げるか、任意のボタンを押さない限り、スケジュールされた期間中、Power Save モードのままになります。Cisco Unified Communications Manager の **[電話の構成（Phone Configuration）]** ウィンドウの [製品固有の構成（Product Specific Configuration）] 領域で、次のパラメータを構成します。

Days Display Not Active

バックライトが非アクティブのままである日数を指定します。

Display on Time

バックライトが自動的にアクティブになる時刻をスケジュールします。

Display on Duration

プログラムされたスケジュールによってバックライトが有効になった後、バックライトがアクティブである時間の長さを示します。

EnergyWise モード

省電力モードに加えて、デバイスは Cisco EnergyWise（Power Save Plus）モードをサポートしています。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、他のパラメータに加え、スリープおよびウェイクの時刻も設定します。これらのパラメータは、構成 XML ファイルの一部としてデバイスへ送信されます。 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指定します。

[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）]

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。

オーディオ アラートの有効化

これを有効にすると、**[電話機をオフにする時刻（Phone Off Time）]** で指定した時刻の 10 分前に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）]

デバイスが存在する 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されるセキュリティ シークレット パスワードを指定します。

[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場合、給電機器（PSE）はデバイスに最小限の電力を供給して **[電源/ロック（Power/Lock）]** ボタンを点灯させ、**[電源/ロック（Power/Lock）]** ボタン を使用してスリープ状態の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、デバイスで消費でき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）（Threshold Limit Value (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、デバイスがアクセサリの電源を投入できなくなります。

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

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 と電力ネゴシエーションを無効にすると、デバイスは最大 15.4 W までアクセサリに電力を供給できます。

Additional Information About Power

The documents in the following table provide more information on the following topics:

- Cisco switches that work with Cisco Unified IP Phones
- Cisco IOS releases that support bidirectional power negotiation
- Other requirements and restrictions about power

Document Topic	URL
Cisco Unified IP Phones Power Injector	http://www.cisco.com/c/en/us/products/collaboration-endpoin unified-ip-phone-power-injector/index.html
PoE Solutions	http://www.cisco.com/c/en/us/solutions/enterprise-networks/ power-over-ethernet-solutions/index.html
Cisco Catalyst Switches	http://www.cisco.com/cisco/web/psa/default.html?mode=proc http://www.cisco.com/c/en/us/products/switches/index.html
Integrated Service Routers	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS Software	http://www.cisco.com/c/en/us/products/ios-nx-os-software/ind

外部デバイス

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

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

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

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

注意 欧州連合諸国では、EMC Directive（89/336/EC）に完全に準拠した外部スピーカ、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 ポートおよび USB シリアル コンソール データ情報

Cisco DX シリーズ デバイスには USB ポートと、場合によってはマイクロ USB ポートが含まれます。デバイスは、USB ポートへの最大 10 個のアクセサリの接続をサポートします。デバイスに接続されている各アクセサリは、最大数に含まれます。サポートされているアクセサリには、USB シリアル ケーブル、USB マウス、USB キーボード、USB 電源ハブ、および USB メモリ スティックが含まれます。

（注） すべての USB ハブに電源を供給する必要があるため、1 つ以上のハブを含むキーボードは、電源が供給されていないハブを含むため、これらのデバイスでは許可されません。

Android Debug Bridge（ADB）アクセスに USB 接続を使用することもできます。ADB アクセスには、Cisco DX650、Cisco DX70 のマイクロ USB ポート、および Cisco DX80 の USB タイプ B ポートを使用します。ADB の使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 コンソールを使用すると、USB ポートをコンソールとして使用できるため、シリアル ポートが不要になります。次の表には、USB コンソールの設定を示します。

表 *8 : USB* コンソール設定

パラメータ	設定
ボーレート	115200
データ	8 ビット
パリティ	none
停止	1 ビット
フロー制御	none

（注） デバイスにはドライバが事前ロードされているため、Cisco は限られた数のケーブル タイプのみをサポートしています。Cisco では、IOGEAR USB シリアル アダプタの使用を推奨しています。

USB コンソールの使用

USB コンソール ケーブルの一方の端には USB インターフェイスがあり、もう一方の端にはシリアル インターフェイスがあります。USB インターフェイスは、デバイスの任意の USB ポートに接続できます。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 の場合は、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 には、マイクロ 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、ヌル モデム ケーブルを介して 2 本の USB コンソール ケーブルを背中合わせに接続できます。

手順

ステップ 1 Cisco Unified Communications Manager で、デバイス ページのクレデンシャルを設定します。

ステップ 2 ウィンドウの [製品仕様構成レイアウト（Product Specific Configuration Layout）] 部分で USB デバッグを有効にします。

ステップ 3 USB シリアル ケーブルをデバイスに接続します。デバイスの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、**[戻る（ Return ）]** をタップしてサインインします。

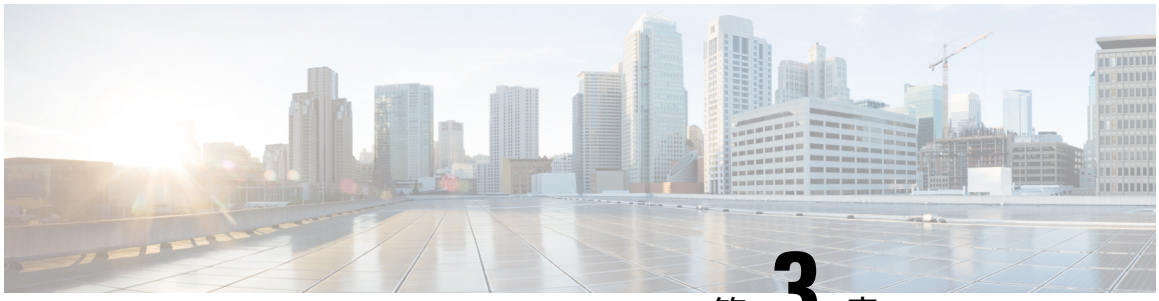
ステップ 5 $prompt screen の後、debugsh などのツールを使用して問題を診断できます。

ネットワーク輻輳時の行動

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

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

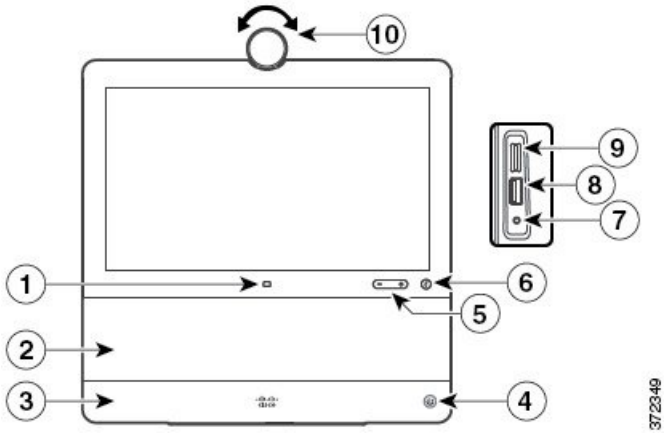
悪影響を減少または排除するには、管理ネットワーク タスクをデバイスが使用されない時間にスケジュールするか、テストからデバイスを除外します。



第 3 章

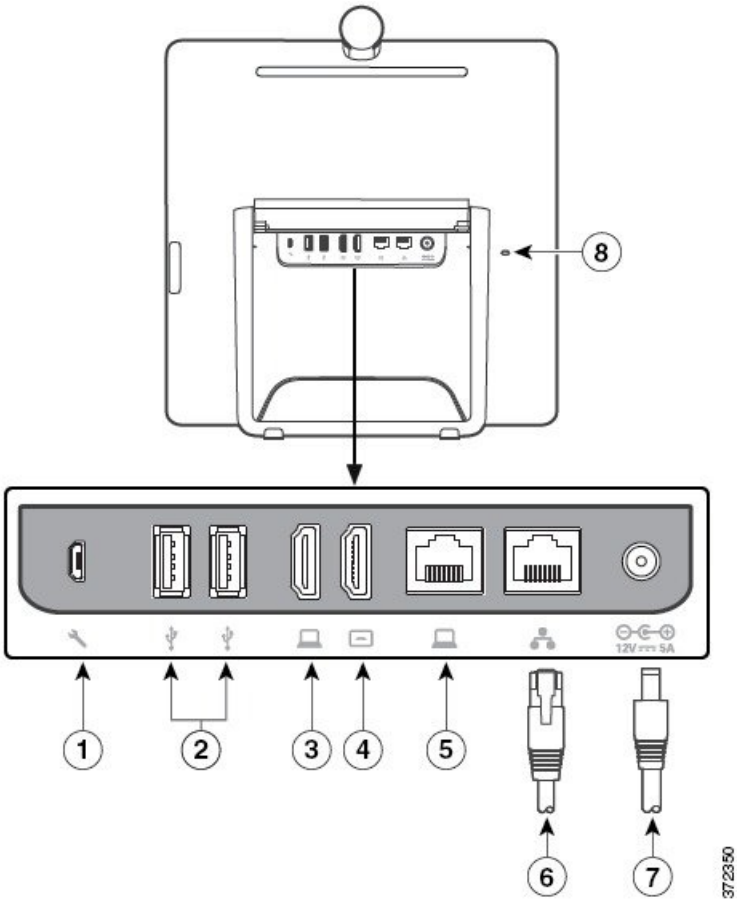
デバイスの説明

Cisco DX70 ハードウェア



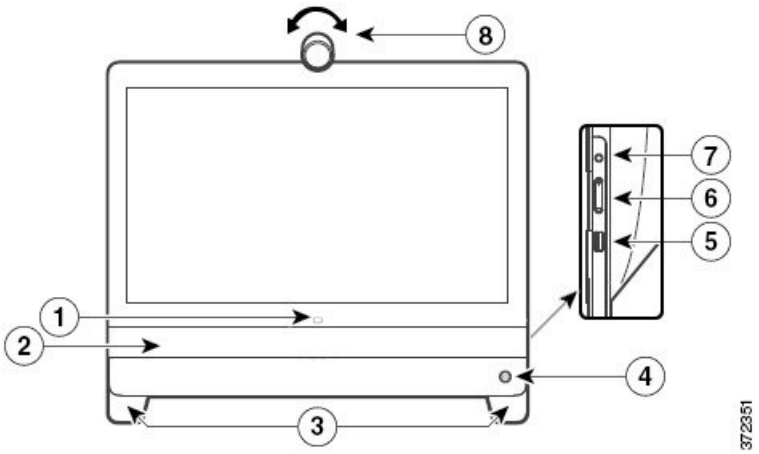
1	[ソース（Source）] ボタン	6	ミュート ボタン
2	[スピーカー（Speaker）]	7	ミニ ジャック 3.5 mm 出力
3	マイクロフォン	8	USB 充電ポート
4	電源ボタン	9	microSD カード スロット
5	[音量ボタン（Volume button）]	10	ライバシーシャッター付きカメラ

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

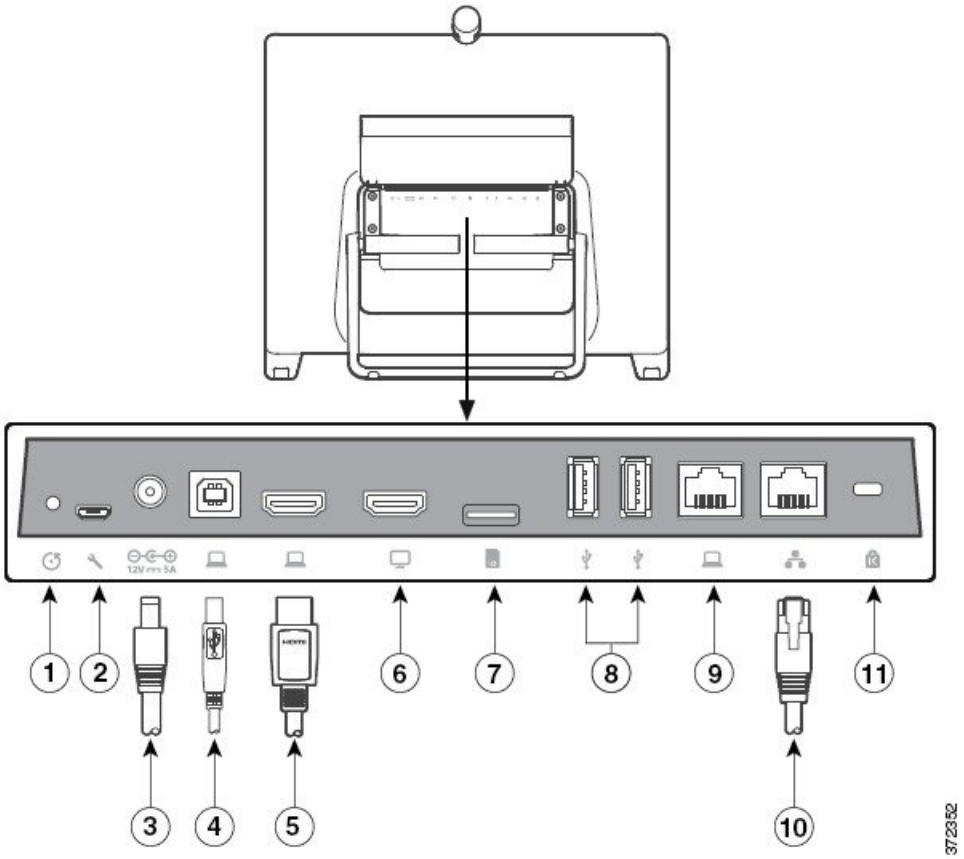


1	[ソース（Source）] ボタン	5	USB ポート
2	[スピーカー（Speaker）]	6	[音量ボタン（Volume button）]
3	各脚内のマイク	7	ミュート ボタン
4	電源ボタン	8	ライバシーシャッター付きカメラ

Cisco DX80 には、音響エコーキャンセラ（AEC）とラップトップ シャドウイングが含まれています。コールの遠端にいるユーザーは、マイクの 1 つの前にラップトップなどの障害物を置いても、クリアな音質を体験できます。現在のマイクが物体によってブロックされている場合、デバイスは自動的に反対側の足の他のマイク アレイに切り替わります。

Cisco DX80 には、2 つのマイク アレイ ビーム フォーミングも含まれます。ユーザーがビームの外（つまり、カメラ ビューの外）に移動すると、遠端に送信される音声が弱くなります。ピックアップ ビーム内（ユニットの前）に位置し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

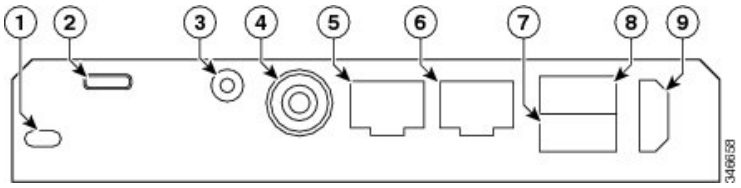


1	初期設定リセット ピンホール	7	microSD カード スロット
2	micro-B USB ポート	8	USB ポート
3	電源ポート	9	コンピュータ ポート
4	USB タイプ B ポート	10	ネットワークポート
5	HDMI 入力	11	Kensington セキュリティ スロット（K-Slot）
6	HDMI 出力		

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	Micro Secure Digital Standard Capacity（HDSC）スロット	14	[ビデオの停止（Stop Video）] ボタン
6	[ロック（Lock）] 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（End call）] 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		

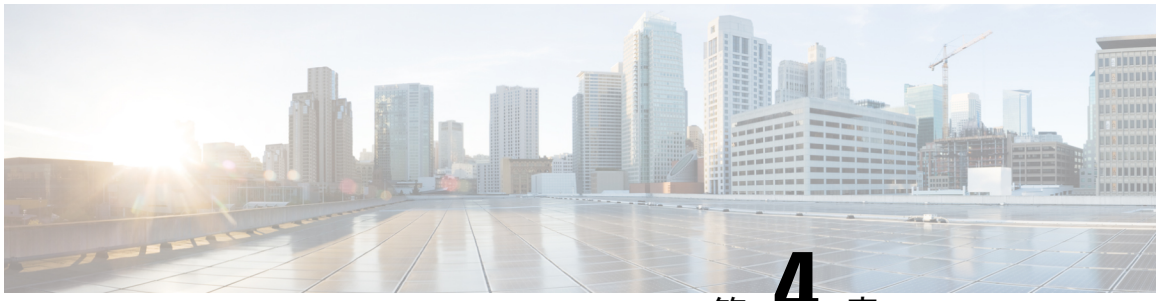
Cisco DX650 のケーブルの取り付け



1	Kensington 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		

No Radio ハードウェア

Cisco DX70 および Cisco DX80 の No Radio（NR）ハードウェア バージョンは、Wi-Fi または Bluetooth 機能をサポートしていません。



第 4 章

Wi-Fi ネットワークのセットアップ

ネットワーク要件

デバイスをネットワーク内のエンドポイントとして正常に機能させるには、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） デバイスには、Cisco Unified Communications Manager から取得した日時が表示されます。ユーザーが設定アプリケーションで **[日付と時刻の自動設定（Automatic date and time）]** をオフにした場合は、時刻がサーバー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 上で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およびビデオをサポートするように構成されています。
- 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。

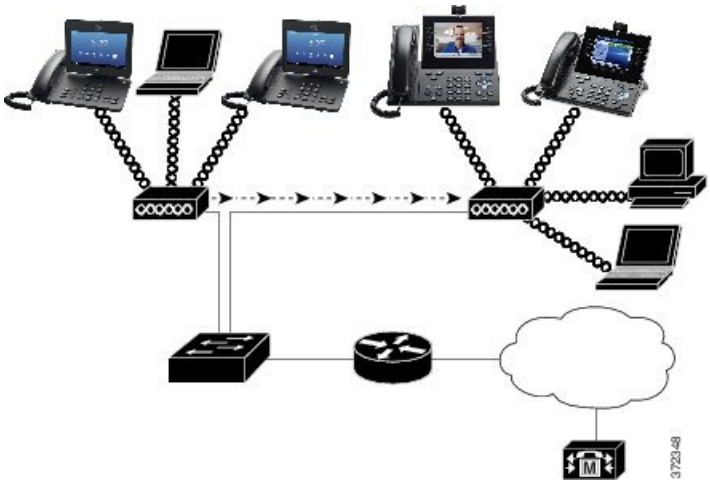
Wireless LAN

Note For instructions on deploying and configuring a wireless Cisco DX シリーズ device, see the 『*Cisco DX Series Wireless LAN Deployment Guide*』.

Devices with wireless capability can provide voice communication within the corporate WLAN. The device depends on and interacts with wireless access points (AP) and key Cisco IP Telephony components, including Cisco Unified Communications Manager Administration, to provide wireless voice communication.

Cisco DX シリーズ devices exhibit Wi-Fi capabilities that can use 802.11a, 802.11b, 802.11g, and 802.11n Wi-Fi.

The following figure shows a typical WLAN topology that enables the wireless transmission of voice for wireless IP telephony.



When a Cisco DX シリーズ device powers on, it searches for and associates with an AP if the device wireless access is set to On. If remembered networks are not within range, you can select a broadcasted network or manually add a network.

The AP uses the connection to the wired network to transmit data and voice packets to and from the switches and routers. Voice signaling is transmitted to the Cisco Unified Communications Manager server for call processing and routing.

APs are critical components in a WLAN because they provide the wireless links or hot spots to the network. In some WLANs, each AP has a wired connection to an Ethernet switch, such as a Cisco Catalyst 3750,

that is configured on a LAN. The switch provides access to gateways and the Cisco Unified Communications Manager server to support wireless IP telephony.

Some networks contain wired components that support wireless components. The wired components can comprise switches, routers, and bridges with special modules to enable wireless capability.

For more information about Cisco Unified Wireless Networks, see http://www.cisco.com/c/en/us/products/wireless/index.html.

Wi-Fi ネットワーク コンポーネント

デバイスは、コールを正常に発着信するために、WLAN 内の複数のネットワーク コンポーネントと連携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 チャネルとドメイン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（モバイルではない）エンドポイントであるため、ローカル環境の変更により、デバイスがアクセスポイント間をローミングし、音声とビデオのパフォーマンスに影響を与え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

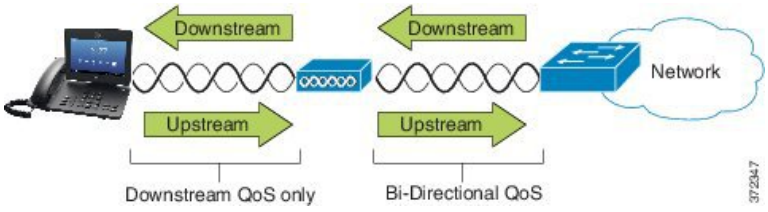
デバイスは起動時に、認識できる SSID と暗号タイプを持つ AP をスキャンします。デバイスにより、一連の利用可能な AP リストが構築、維持され、現在の構成に基づく最適な AP が選択されます。

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 TCP を使用するため、AP がフル稼働状態の場合に Cisco Unified Communications Manager 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との間で送受信されるフレームはドロップされ、Cisco Unified Communications Manager の登録解除の原因となることがあります。したがって、Cisco では SIP CAC を無効にすることを推奨します。

（注） DSCP、COS、および WMM UP マーキングは、ビデオ フレームの最適な伝送のために正しく表示されます。デバイスは音声およびビデオ CAC をサポートしていません。 SOP CAC を実装することを推奨します。

デバイスは、異なるタイプのデバイスでビデオが発生した場合に、フレキシブル DSCP およびビデオ プロモーション機能を使用して、一貫性のない QoS および一貫性のない帯域幅アカウンティングを解決します。

フレキシブル DSCP の設定

手順

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

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 では、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、リソース）を管理して、電話会議やルート プランニングなどの機能を動作させます。

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に登録および構成されるまで、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 を構成する方法の詳細については、『*Cisco Unified Communications Manager Administration Guide*』、『*Cisco Unified Communications Manager* システム ガイド』、および『*Cisco DX Series Wireless LAN Deployment Guide*』を参照してください。

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 デバイスは以下の基準をサポートします。

- 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。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、送信電力、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、使用すべき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構成は、関連付けられた AP 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、AP 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を使用します。

直接拡散方式（DSSS）

周波数範囲または帯域幅全体に信号を拡散することで、干渉を防止します。DSSS テクノロジーは、複数のデバイスが干渉なしで通信できるように、複数の周波数でデータのチャンクを多重化します。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別なコードがあります。他のすべてのデータ パケットは無視されます。Cisco ワイヤレス 802.11b/g 製品は、DSSS テクノロジーを使用して WLAN 上の複数のデバイスをサポートします。

直交周波数分割多重方式（OFDM）

RF を使用して信号を送信します。OFDM は、1 つの高速データ キャリアを複数の低速キャリアに分割して、RF スペクトル全体で並行して送信する物理層エンコーディング技術です。802.11g および 802.11a で使用する場合、OFDM は 54 Mbps のデータレートをサポートできます。

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標準別に比較します。

表 *11 : IEEE* 標準規格によるデータ 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 ル • 40 ル Mb
非オーバーラップ 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。

Security for Communications in WLANs

Because all WLAN devices that are within range can receive all other WLAN traffic, security of voice communications is critical in WLANs. To ensure that intruders do not manipulate or intercept voice traffic, the Cisco SAFE Security Architecture supports Cisco DX シリーズ devices and Cisco Aironet APs. For more information about security in networks, see http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html.

認証方式

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

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
- CCKM（Cisco Centralized Key Management）
- オープン

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。

認証方式の詳細については、『『*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に、Cisco DX シリーズ デバイスは、暗号化として WEP、TKIP、および Advanced Encryption Standards（AES）をサポートしています。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 で構成された 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。

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

AP Authentication and Encryption Options

Authentication and encryption schemes are set up within the wireless LAN. VLANs are configured in the network and on the APs and specify different combinations of authentication and encryption. An SSID associates with a VLAN and the particular authentication and encryption scheme. In order for wireless client devices to authenticate successfully, you must configure the same SSIDs with their authentication and encryption schemes on the APs and on the device.

Note

- When you use WPA pre-shared key or WPA2 pre-shared key, the pre-shared key must be statically set on the device. These keys must match the keys that are on the AP.
- Cisco DX シリーズ devices do not support auto EAP negotiation; to use EAP-FAST mode, you must specify it.

The following table provides a list of authentication and encryption schemes that are configured on the Cisco Aironet APs that the devices support. The table shows the network configuration option for the device that corresponds to the AP configuration.

Table 12: Authentication and Encryption Schemes

Cisco WLAN Configuration			**Cisco DX シリーズ Configuration**
Authentication	Key management	Common encryption	Authentication
Open	None	None	None
Static WEP	None	WEP	WEP

Cisco WLAN Configuration			Cisco DX シリーズ Configuration
EAP-FAST	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > MSCHAPV2
PEAP-GTC	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA or WPA2 with optional CCKM	TKIP or AES	802.1x EAP > TLS
WPA/WPA2-PSK	WPA-PSK or WPA2-PSK	TKIP or AES	WPA/WPA2 PSK

For additional information about Cisco WLAN Security, see http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html.

For more information about configuring authentication and encryption schemes on APs, see the *Cisco Aironet Configuration Guide* for your model and release under the following URL:

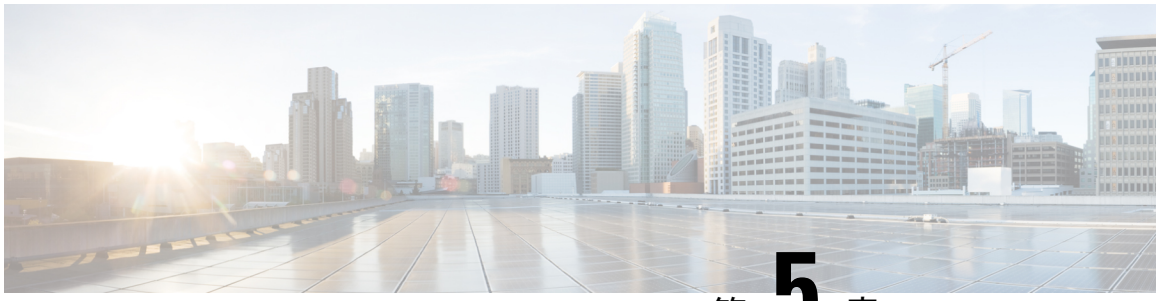
http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=278875243

WLANs and Roaming

Cisco DX シリーズ devices support Cisco Centralized Key Management (CCKM), a centralized key management protocol that provides a cache of session credentials on the wireless domain server (WDS).

For details about CCKM, see the *Cisco Fast Secure Roaming Application Note* at:

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



第 5 章

展開

設定ファイル

TFTP サーバは Cisco Unified Communications Manager に接続するためのパラメータを定義するデバイス構成ファイルを保存します。Cisco Unified Communications Manager でデバイス接続先回線のリセットが必要となる変更を行うと、通常は、変更内容がデバイスの構成ファイルに自動的に反映されます。

構成ファイルには、デバイスがどのイメージロードを実行するかも記述されています。ロードイメージが、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、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のロードのサイズにより、デバイスと TFTP サーバの間で TCP ポート 6970 を開く必要があります。

次の条件を満たしている場合、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の構成ファイルにアクセスします。

- Cisco Unified Communications Manager の自動登録が有効になります。
- デバイスが Cisco Unified Communications Manager データベースに追加されていません。
- デバイスが初めて登録されます。

（注） コンフィギュレーションファイルのデバイスセキュリティモードが [認証済み（Authenticated）] または [暗号化済み（Encrypted）] に設定されているが、デバイスが CTL ファイルまたは ITL ファイルを受信していない場合、デバイスは安全に登録できるようにファイルの取得を 4 回試行します。

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

Cisco DX シリーズ デバイスはコンフィギュレーション ファイル SEPmac_address.cnf.xml にアクセスします。mac_address はデバイスのイーサネット MAC アドレスです。CTL または ITL ファイルがインストールされている場合、デバイスは 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。 Cisco Unified Communications Manager Administration の **[電話の構成（Phone Configuration）]** ウィンドウの [説明（**Description** ）] フィールドは、デバイスを最初に構成したときに事前に入力されます。MAC アドレスはデバイスを固有に識別します。

MAC アドレスの確認

次の方法で、デバイスの MAC アドレスを判別できます。

手順

- デバイスから、**[アプリケーション（Applications）]** > **[設定（Settings）]** > **[デバイスの > ステータスについて（About deviceStatus）]** をタップし、**[イーサネット MAC アドレス（Ethernet MACAddress）]** フィールドを確認します。
- デバイスの背面にある MAC ラベルを確認する。
- 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 デバイス追加方法

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

表 *13 : Cisco Unified Communications Manager* へのデバイスの追加方法

方法	MAC アドレスの必要性	注記
自動登録	×	電話番号の自動割り当てが可能です。
自動登録電話サポート（TAPS）向けのツールを備えた自動登録	いいえ	自動登録と一括管理ツールが必要です。デバイスと Cisco Unified Communications Manager Administration の情報を更新します。
Cisco Unified Communications Managerの管理	はい	デバイスを個々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（Self-Provisioning）]	いいえ	ユーザーが自分のデバイスをプロビジョニングできるようにします。

自動登録

デバイスを設置する前に自動登録を有効にしておくと、次のことが可能になります。

- 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します。
- デバイスを IP テレフォニー ネットワークに物理的に接続したときに、そのデバイスを Cisco Unified Communications Manager データベースに自動的に追加できます。自動登録中に、Cisco Unified Communications Manager は連続するディレクトリ番号の中から次に使用可能なものをデバイスに割り当てます。
- Cisco Unified Communications Manager データベースにデバイスをすばやく入力し、Cisco Unified Communications Manager からディレクトリ番号などの設定を変更します。
- 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ます。

（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。場合によっては、自動登録の使用が望まれないこともあります（たとえば電話に特定のディレクトリ番号を割り当てる場合、または『*Cisco Unified Communications Manager Security Guide*』で説明された Cisco Unified Communications Manager とのセキュアな接続を使用する場合など）。自動登録の有効化の

詳細については、『『*Cisco Unified Communications Manager Security Guide*』』の「自動登録の 「設定」」セクションを参照してください。

自動登録および TAPS

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

TAPS は一括管理ツール（BAT）と連携して、ダミー MAC アドレスを使用して Cisco Unified Communications Manager データベースに追加されたデバイスのバッチをアップデートします。TAPS を使用して、MAC アドレスを更新し、事前定義された構成をダウンロードします。

（注） 自動登録および 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、一括管理ツールを使用します。

TAPS を実装するには、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、音声プロンプトに従います。プロセスが完了すると、デバイスにはディレクトリ番号やその他の設定が含まれ、デバイスが正しい MAC アドレスで Cisco Unified Communications Manager 管理でアップデートされます。

TAPS が機能するためには、自動登録は Cisco Unified Communications Manager 管理で有効にする必要があります（**System** > **Cisco Unified CM**）。

（注） Cisco CTL クライアントを通じてクラスタを混合モードに構成すると、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、自動登録は自動で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 のデバイス追加

Cisco Unified Communications Manager データベースにデバイスを個別に追加できます。それには、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ら、 Cisco Unified Communications Manager 管理で、**[デバイスの** > **電話（DevicePhone）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[電話タイプ（Phone Type）]** ドロップダウン リストからデバイス タイプを選択します。

（注） Cisco Unified Communications Manager 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 デバイス固有のパラメータ（デバイス プール、デバイス セキュリティ プロファイルなど）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。

詳細については、『*Cisco Unified Communications Manager* システム ガイド』の「システム構成概要」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）を使用すると、複数のデバイスの登録などの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 バイス固有のパラメータ（デバイス プール、デバイス セキュリティ プロファイルなど）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 Communications Manager の [管理（Administration）] から、**[デバイス（Device）]** > **[電話（Phone）]** > **[新規追加（Add New）]** を選択し、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により、ユーザーは管理者の労力を軽減してデバイスをセットアップできます。セルフプロビジョニングが有効になっている場合、ユーザーはデバイスのセット

アップ時にログイン情報を入力します。デバイスの MAC アドレスおよびその他の構成情報は、 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「「セルフプロビジョニング」」の章を参照してください。

セルフプロビジョニングを有効化

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**[ユーザー管理（ User Management）]**、 > **[ユーザー設定（User Setting）]**、 > **[ユーザー プロファイル（User Profile）]** の順に選択します。

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

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

ステップ 4 [セルフサービス ユーザー ID（Self-Service User ID）] を設定します。

ステップ 5 **[ユーザー管理（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。

14Cisco Unified Communications Manager のユーザー追加

このセクションでは、 Cisco Unified Communications Manager にユーザーを追加する手順について説明します。オペレーティング システムとユーザーを追加する方法に応じて、このセクションのいずれかの手順に従います。

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、 Cisco Unified Communications Manager にユーザーを直接追加できます。

（注） LDAP が同期されている場合、 Cisco Unified Communications Manager にユーザーを追加することはできません。

手順

ステップ 1 **[ユーザー管理（User Management）]** > **[エンドユーザー（End User）]** の順に選択し、**[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 [ユーザー情報（User Information）] ペインで、次の情報を入力します。

- [ユーザー ID（User ID）]：エンド ユーザーの識別名を入力します。Cisco Unified Communications Manager では、作成後のユーザー ID の変更を許可しません。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 ユーザー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 ユーザーの姓を入力します。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 ユーザーのプライマリ電話番号を入力します。エンド ユーザーは、デバイスに複数の回線を接続できます。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 デバイス モデルの特定 （46 ページ） に進みます。

外部 LDAP ディレクトリからのユーザーの追加

LDAP ディレクトリ（Cisco Unified Communication サーバ ディレクトリ以外）にユーザーを追加した場合、そのディレクトリを、同じユーザーとデバイスを追加する Cisco Unified Communications Manager に、以下の手順ですぐに同期させることが可能です。

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 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 ディレクトリと Cisco Unified Communications Manager との同期を即座には行わない場合は、[LDAPディレクトリ（LDAP Directory）] ウィンドウの [LDAPディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] で、次回の自動同期スケジュールが決定されます。ただし、新規ユーザーをデバイスに関連付けるには、その前に同期を完了しておく必要があります。

ステップ 6 デバイス モデルの特定 （46 ページ） に進みます。

デバイス モデルの特定

手順

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

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[電話タイプ（Phone Type）]** ドロップダウン リストからデバイス モデルを選択し、**[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 回線設定の構成 （46 ページ） に進みます。

回線設定の構成

[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 **[ディレクトリ番号（Directory Number）]** フィールドで、**[電話番号（Telephone Number）]** フィールドで（**[ユーザー構成（User Configuration）]** ウィンドウ内）に表示されている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 **[コーリング検索スペース（ Calling Search Space ）]** ドロップダウン リスト（**[ディレクトリ番号の構成（Directory Number Configuration ）]** ウィンドウの [ディレクトリ番号の設定（Directory Number Settings）] ペイン）から、適切なコーリング検索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 **[ディレクトリ番号構成（Directory Number Configuration）]** ウィンドウの **[コール転送設定（Call Forward Settings）]** ページで、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送信先を選択します。

例：

ビジー信号を受信した内線および外線の着信コールをこの回線のボイス メールに転送する場合は、[コール転送設定（Call Forward Settings）] ペインの **[ボイス メール（Voice Mail）]** チェックボックスをオンにします。

ステップ 6 **[ディレクトリ番号の構成（ 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、次のように構成します。

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ー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 情報の送出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」を入力できます。X は電話番号を表し、パターンの末尾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) [保存（Save）] をクリックします。

（注） この設定は、右側にある **[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、現在のデバイスにのみ適用されます。（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 構成されている回線にユーザーを関連付けるには、ウィンドウの下にある **[エンド ユーザーの関連付け（Associate End Users）]** をクリックします。

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

b) ユーザー名の横にあるチェック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。
ユーザー名とユーザー ID は **[電話番号の構成**（Directory Number Configuration）] ウィンドウの [回線に関連付けられているユーザー（Users Associated With Line）] ペインに表示されます。

c) [保存（Save）] をクリックします。

これでユーザーが、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 ユーザーとデバイスの関連付け （48 ページ） に進みます。

ユーザーとデバイスの関連付け

手順

ステップ 1 Cisco Unified Communications Manager の管理から、**[ユーザーの管理（User Management）]** > **[エンド ユーザー（End User）]** を選択します。
[ユーザーの検索と一覧表示（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、ユーザーのリンクを選択します。

ステップ 4 **[デバイスの関連付け （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。

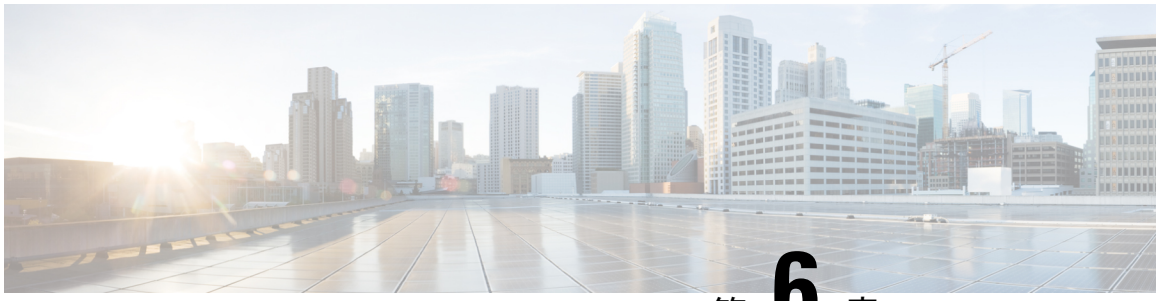
ステップ 8 **[関連リンク（Related Links）]** ドロップダウン リストで **[ユーザーの設定に戻る（Back to User）]** を選択し、**[検索（Go）]** をクリックします。
[エンドユーザーの構成（End User Configuration）] ウィンドウが表示され、選択した関連付けられたデバイスが [制御するデバイス（Controlled Devices）] ペインに表示されます。

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

Survivable Remote Site Telephony

Survivable Remote Site Telephony（SRST）は、制御する Cisco Unified Communications Manager との通信が切断された場合でも、基本的なコール機能にアクセスできるようにします。このシナリオでは、デバイスは進行中のコールをアクティブ状態に維持でき、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、ユーザーのデバイスにアラート メッセージが表示されます。SRST には、Cisco IOS バージョン 12.4(20) 以降が必要です。

（注） SRST は IPv6 をサポートしていません。



第 6 章

インストール

Cisco DX シリーズ デバイスの設置

Cisco Unified Communications Manager データベースにデバイスを追加したら、デバイスのインストールを完了できます。管理者（またはユーザー）は、ユーザーの場所にデバイスを設置できます。

（注） デバイスを設置する前に、新しいデバイスであっても、デバイスを最新のファームウェア イメージにアップグレードします。アップグレードの詳細については、次の場所にあるデバイスの 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

デバイスを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され、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、デバイス上でネットワーク設定値を構成します。

自動登録を使用した場合は、デバイスをユーザーに関連付ける、ディレクトリ番号を変更するなど、デバイスの特定の構成情報をアップデートする必要があります。

次の手順では、Cisco DX シリーズデバイスの設置タスクの概要とチェックリストを示します。この手順では、デバイスの設置を推奨する順序を示します。一部のタスクは、システムおよびユーザーのニーズによっては省略できます。

手順

ステップ 1 電源を次の中から選択します。

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

（注） PoE+ 802.3at では、マウスやキーボードなどのデバイスに接続されているアクセサリが電力をネゴシエートします。アクセサリに十分な電力が供給されていない場合は、エラー メッセージが画面に表示されます。デバイスを WLAN 環境で使用する場合は、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。
この手順では、ネットワーク内のデバイスを見つけてインストールします。

ステップ 3 デバイスの起動プロセスをモニタします。この手順では、プライマリとセカンダリのディレクトリ番号、およびディレクトリ番号に関連付ける機能をデバイスに追加し、デバイスが正しく構成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 ネットワークに対してデバイスでイーサネット ネットワーク設定を構成する場合、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にデバイスを展開する場合は、次の手順を実行する必要があります。

- ワイヤレス ネットワークを構成します。
- Cisco Unified Communications Manager 管理でデバイスのワイヤレス LAN を有効にします。
- デバイスでワイヤレス ネットワーク プロファイルを構成します。

（注） イーサネット ケーブルがデバイスに接続されている場合、デバイスのワイヤレス LAN は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と機能が正常に動作することを確認します。

ステップ 7 エンド ユーザーに対して、デバイスの使用方法および構成方法を通知します。

ワイヤレス LAN の設定

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および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 ネットワークの完全な設定情報については、「『*Cisco DX Series Wireless LAN Deployment Guide*』」を参照してください。

Cisco Unified Communications Manager 管理のワイヤレス LAN 設定

Cisco Unified Communications Manager で、デバイスの 「Wi-Fi」 と呼ばれるパラメータを有効にする必要があります。 Cisco Unified Communications Manager 管理の次のいずれかの場所で、このパラメータを有効にできます。

- 特定のデバイスでワイヤレス LAN を有効にするには、特定のデバイスの [製品固有の設定レイアウト（Product Specific Configuration Layout）] セクション（**[デバイス（Device）]** > **[電話（Phone）]**）で Wi-Fi パラメータの **[有効（ Enable）]** を選択し、**[共通設定のオーバーライド（ Override Common Settings）]** をオンにします。
- デバイスのグループに対してワイヤレス LAN を有効にするには、**[共通の電話プロファイルの構成（Common Phone Profile Configuration ）]** 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 Wi-Fi パラメータの **[有効化（Enable）]** を選択し、**[共通設定のオーバーライド（Override Common Settings）]** をオンにしてから、デバイス（**[デバイス（Device）]** > **[電話（Phone）]** をその共通の電話プロファイルに関連付けます。
- ネットワーク内のすべての WLAN 対応デバイスでワイヤレス LAN を有効にするには、**[エンタープライズ電話 の構成（Enterprise Phone Configuration）]** ウィンドウ（**[システム（System）]** > **[エンタープライズ電話の構成]（Enterprise Phone Configuration）]**）で、Wi-Fi パラメータの **[有効化（Enable）]** を選択し、**[共通設定のオーバーライド（Override Common Settings）]** をオンにします。

（注） Cisco Unified Communications Manager 管理（**[デバイス（Device）]** > **[電話（Phone）]**）の **[電話構成（Phone Configuration）]** ウィンドウで、MAC アドレスを構成するときにイーサネット MAC アドレスを使用します。Cisco Unified Communications Manager の登録では、無線 MAC アドレスを使用しません。

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 Communications Manager 管理で、**[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 プロファイルを構成し、**[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 Communications Manager 管理で、**[デバイス > 電話 > ワイヤレス LAN プロファイル グループ（DevicePhoneWireless 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 グループを構成し、**[保存（Save）]** をクリックします。

ステップ 3 **[システム > デバイス プール（System 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 > 電話（Device 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。

ネットワーク設定構成

ネットワークで DHCP を使用していない場合、ネットワークでデバイスをインストールした後、デバイスでこれらのネットワーク設定を構成する必要があります。

- IP アドレス
- IP サブネット情報
- IPv6 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（Settings）] アプリケーションで、**[イーサネット（Ethernet）] > [IPv4 構成（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します。

- [IP アドレス（IP Address）]
- ゲートウェイ
- ネットマスク
- ドメイン名

（注） オプション 15 を使用して、複数のドメイン名をデバイスに送信できます。各ドメイン名はスペースで区切る必要があります。カンマなどの他のデリミタはサポートされていません。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。繰り返しますが、スペースは唯一の有効なデリミタです。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（Settings）] アプリケーションで、[**イーサネット** > **IPv6 構成（ EthernetIPv6 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します。

- 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） オプション 15 を使用して、複数のドメイン名をデバイスに送信できます。各ドメイン名はスペースで区切る必要があります。カンマなどの他のデリミタはサポートされていません。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。繰り返しますが、スペースは唯一の有効なデリミタです。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 プロキシの構成

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）]** をタップします。

ステップ 2 プロキシ設定タイプを選択します。

a) 手動プロキシを設定するには、プロキシのホスト名、プロキシ ポート、およびプロキシ バイパスを入力します。該当する場合は、**[プロキシは認証が必要（Proxy require 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を入力します。該当する場合は、**[プロキシは認証が必要（Proxy require authentication）]** を オンにします。

管理 VLAN の設定

手順

ステップ 1 [設定（Settings）] 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 の値を入力し、**[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（Settings）] アプリケーションで、**[イーサネット** > **SW ポート速度（EthernetSW 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構成するか、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 ポートの構成（PC Port config）] オプションを同じ設定値に変更する必要があります。

PC ポートの速度の設定

手順

ステップ 1 [設定（Settings）] アプリケーションで、**[イーサネット（Ethernet）]** > **[PC ポート速度（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構成するか、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 ポートの構成（SW Port config）] オプション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（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 認証情報を入力し、**[接続（Connect）]** をタップします。

非表示の Wi-Fi ネットワークに接続

手順

ステップ 1 設定アプリケーションで、[Wi-Fi（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、セキュリティ タイプとログイン情報（該当する場合）を選択します。

ステップ 5 [保存（Save）] をタップします。

Wi-Fi Web プロキシの構成

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からワイヤレス ネットワークを長押しします。

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 **[詳細オプションの表示（Show advanced options）]**をチェックします。

ステップ 5 プロキシ設定タイプを選択します。

a) 手動プロキシを設定するには、プロキシのホスト名、プロキシ ポート、およびプロキシ バイパスを入力します。該当する場合は、**[プロキシは認証が必要（Proxy require 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を入力します。該当する場合は、**[プロキシは認証が必要（Proxy require 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 設定の構成

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からワイヤレス ネットワークを長押しします。

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 **[詳細オプションの表示（Show advanced options）]**をチェックします。

ステップ 5 IP 設定タイプを選択し、以下を構成します。

- [IP アドレス（IP Address）]
- 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 周波数バンドの設定

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 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

Mobile and Remote Access through Expressway requires Cisco Expressway 8.6 or later and Cisco Unified Communications Manager 10.5.2 SU2 or Cisco Unified Communications Manager 11.0 or later.

Cisco Expressway provides a way for remote workers to easily and securely connect their Cisco DX Series devices into the corporate network without using a virtual private network (VPN) client tunnel. Expressway uses Transport Layer Security (TLS) to secure network traffic. For a DX Series device to authenticate an Expressway certificate and establish a TLS session, the Expressway certificate must be signed by a public Certificate Authority that is trusted by the DX Series firmware. It is not possible to install or trust other CA certificates on DX Series devices for authenticating an Expressway certificate. See www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-technical-reference-list.html for the list of supported CA certificates.

To ensure that the users are able to use the Problem Report Tool, you must add the Problem Report Tool server address to the Expressway HTTP server allow list

When logging in to Expressway, the user is prompted for a Service Name, User ID, and Password. On first boot, off-premise users are prompted to log in to Expressway by the Setup Assistant. For devices that have previously been deployed, either on-premise or off-premise, you must convert the device to use Expressway.

With the **User Credentials Persistent for Expressway Sign In** parameter set in the Product Specific Options on Cisco Unified Communications Manager, the device stores a user's login credentials so that users do not need re-enter this information. User credentials stored on the device are encrypted.

For more information, see *Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide*.

Mobile and Remote Access Limitations and Restrictions

- DX Series devices connected through Expressway cannot access web browsing, or email services hosted inside the enterprise network.

- The Off Hook/KPML Dialing, Mobility, DND, Call Back, and drop conference participants features are only supported with Expressway 8.6 and later.
- Busy Line Field features require Cisco Unified Communications Manager 11.0 or later.
- A device connected through Expressway cannot download APKs from an APK server inside the enterprise network. The device can download APKs from an APK server on a public network as long as the host is accessible.
- You do not have SSH access to the device from the corporate network.
- You do not have access to the device web page from the corporate network.
- Self-provisioning is not supported through Expressway.

Expressway 用ユーザー ログイン情報の有効化

手順

ステップ 1 個別デバイスの構成ウィンドウまたは **[共通の電話プロファイル（Common Phone Profile）]** ウィンドウの [製品固有構成レイアウト（Product Specific Configuration Layout）] 領域に移動します。

ステップ 2 **[Expressway ログイン用ユーザ クレデンシャル パーシステント（User Credentials Persistent for Expressway Sign In）]** をオンにします。

Expressway を介してデバイスをモバイル & リモート アクセスに変換

始める前に

デバイスのファームウェアは 10.2(4) 以降である必要があります。

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 [ネットワーク設定のリセット（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を有効にする（Enable automatic local telephony discovery ）]** をオフにし、**[リセット（Reset）]** をタップします。
ネットワーク接続をリセットします。デバイスが有線ネットワークに接続されている場合は、自動的に再接続されます。デバイスがワイヤレスで導入されている場合は、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）]**、**[ユーザー名（ Username）]**、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 [ログイン（Sign in）] をタップします。

Expressway デバイスを VPN に変換

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 [ネットワーク設定のリセット（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 サーバー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て接続します。

オフプレミス デバイスからオンプレミスに変換

手順

デバイスをエンタープライズ ネットワークに接続します。
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 許可リストに問題報告ツール サーバーの追加

手順

ステップ 1 Expressway で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** に移動します。
ステップ 2 **[HTTP サーバー許可リスト（HTTP server allow list）]** をクリックします。
ステップ 3 Problem Report Tool HTTP サーバーのホスト名または IP アドレスを構成します。

許可済み認証リクエスト レートの設定

デバイスのモバイルおよびリモートアクセス認証のレートは、デフォルトで制御されます。デフォルト設定は、300 秒で 3 認証です。Expressway サーバーが HTTP 429 「Too many Requests」エラーを発行している場合は、このレートを増やすことができます。

手順

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

ステップ 2 **[認証レート制御（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サーバの設定（TFTP Server Settings）] をタップします。

ステップ 3 **[代替 TFTP サーバの使用（Use Alternate TFTP Server）]** をタップします。

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）]** をタップします。

ステップ 4 **[TFTP サーバー 1（TFTP Server1）]** 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 サーバー 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）]** をタップします。

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 is a VPN client that provides remote users with secure VPN connections to the Cisco 5500 Series ASA running ASA Version 8.0, and later (with AnyConnect Mobile License) or Adaptive Security Device Manager (ASDM) 6.0 and later.

For more information about ASA, see https://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（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 サーバ アドレスの説明を入力します。
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（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 ログイン情報も入力します。
- [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認証情報を入力します。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 コール体験の最適化

ビデオ帯域幅の設定を調整して、VPN を介したビデオ コール エクスペリエンスを最適化します。720p のビデオ解像度には、1.5 Mbps の帯域幅が必要です。帯域幅の設定を低くすると、ビデオ解像度が低くなります。

（注） スループットは、ネットワーク上で共有されている他のトラフィックや時刻などの要因により、時間の経過とともに変化します。これらのバリエーションは、ビデオエクスペリエンスに影響を与える可能性があります。

手順

ステップ 1 VPN から接続解除します。

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メモします。

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 から入手できます。

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 [動画帯域幅（Video bandwidth）] をタップします。

ステップ 7 速度テストの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 VPN の構成

[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することができます。デバイスが信頼できるネットワークの外部にある場合、またはデバイスと Cisco Unified Communications Manager 間のネットワーク トラフィックが信頼できないネットワークを通過する必要がある場合は、VPN 接続を使用します。

これらのステップに従い、VPN プロファイルを構成します。詳細については、『『*Cisco Unified Communications Manager Security Guide*』』および『*Cisco Unified Communications* オペレーティング システム管理ガイド』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 ゲートウェイを構成します。

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

b) ゲートウェイ名、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。各ゲートウェイに少なくとも 1 つの証明書を割り当てます。利用可能な VPN 証明書リストに、VPN ロールに関連付けられた証明書のみが表示されます。

VPN ゲートウェイ URL は、ゲートウェイのメイン コンセントレータ用です。

ステップ 4 VPN グループを構成します。**[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 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 プロファイルを構成します。**[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を有効にする（ Enable Auto-Detect Network Connection ）]** が有効になっている場合、VPN クライアントは、企業ネットワークの外にあることを検出した場合にのみ実行されます。

[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共通名は、VPN クライアントが接続されている URL と一致する必要があります。

[パスワードの永続化を有効にする（Enable Password Persistence）] が有効になっている場合、ユーザー パスワードはキャッシュされます。[VPNパスワードをデバイスに保存（Store VPN Password on Device）] も有効になっている場合、サインインが失敗するまで、ユーザーパスワードがデバイスに保存されます。

ステップ 6 VPN 機能を構成します。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN 機能構成（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（Common Phone Profile）] を割り当てます。**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[共通の電話プロファイル（Common Phone Profile）]** の順に選択します。

VPN 構成設定

次の表に、Cisco Unified Communications Manager でデバイスの VPN 構成オプションを説明します。

表 *14 : VPN* 構成オプション

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	VPNグループ構成でVPNが有効になっています。	[表示のみ（Display Only）]：変

オプション	説明	変更の手順
ユーザー定義 VPN プロファイル	オプションが有効か無効かを示します。	個々のデバイス構成ウィンドウま **電話プロファイル（Common Pho** ウィンドウ（[製品固有の構成レ （Product Specific Configuration lay で、[ユーザー定義プロファイルの User Defined Profiles）] を [オン（ [オフ（Off）] に設定します。 （注） マルチレベル構成で使用で 理者は、デバイス、共通、 タープライズ レベルで変更 Cisco Unified Communicatio でこの機能が無効になって ユーザー定義の VPN プロ デバイスのリストから削除 **い VPN 接続の追加（ Add** **Connection ）]** は無効にな
常に VPN が必要	オプションが有効か無効かを示します。	**[デバイス（Device）]>[デバイス設** **Settings）] > [共通の電話プロファ** **（Common Phone Profile）]** の順に す。 目的のプロファイルを選択します [常にVPNが必要（Always Require [オン（On）] または [オフ（Off） す。 （注） [常に VPN が必要（Always VPN）] 設定により、enabl autoNetworkDetect 値が True れます。

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）]	オプションが有効か無効かを示します。	**[デバイス（Device）]>[デバイ Settings）] > [共通の電話プロ（Common Phone Profile）]** ま **（Device）] > [電話（Phone）] （Phone Configuration）[** また [デバイス上に VPN パスワード VPN Password on Device）] を [または [オフ（Off）] に設定しま （注） [VPN パスワードをデバ （Store VPN Password on 構成された VPN プロフ ワードの永続化が有効に クライアント認証方式が とパスワード（User and または 「[パスワードの only）]」 の場合にのみ

（注） ネットワーク構成の変更は、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、プロキシは構成されず、VPN に使用されません。

VPN 認証

Cisco DX シリーズ デバイスは、次の VPN 認証方法をサポートします。

- ユーザ名とパスワード
- 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 がユーザー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）がユーザー名を設定します。

Cisco Unified Communications Manager で指定されている認証は、ASA で設定されている認証と一致する必要があります。認証が ASA の認証と一致しない場合、ユーザー VPN は引き続き許可されますが、パスワードの永続性と自動接続機能は適用されません。

起動プロセス

ネットワークに接続すると、Cisco DX シリーズデバイスは標準の起動プロセスを実行します。実際のネットワークの設定によっては、次の手順のうち、デバイスで実行されるのは一部だけになる場合があります。

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。**[起動中...（ 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たが、IP アドレスが割り当てられていない場合、ユーザーは管理者に問い合わせるように求められます。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 ネットワーク接続の確立を試みます。

2. （ワイヤレス LAN のみ）アクセス ポイントのスキャン。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、一致する Service Set Identifier (SSID) と認証タイプを含むアクセス ポイントをスキャンします。デバイスは、ネットワーク プロファイル構成に一致するアクセス ポイントに関連付けられます。

3. （ワイヤレス LAN のみ）アクセス ポイントの認証。デバイスは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。デバイスには不揮発性フラッシュ メモリがあり、ファームウェア イメージやユーザー定義の設定値が保存されます。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ファームウェア イメージをロードします。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e を Cisco Catalyst スイッチに接続している場合、スイッチは、スイッチ上に定義されているボイス VLAN をデバイスに通知します。デバイスは、Dynamic Host Configuration Protocol（DHCP）要求を使用して IP アドレスの取得を開始するには、VLAN メンバーシップ情報をあらかじめ把握している必要があります。

6. IP アドレスの取得. デバイスで DHCP を使用して IP アドレスを取得する場合、デバイスは DHCP サーバーにクエリを発行してアドレスを取得します。ネットワーク内で DHCP を使用しない場合は、各デバイスにスタティック 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以外に、デバイスを TFTP サーバに転送します。デバイスの IP アドレスを静的に定義した場合は、デバイスがある場所で TFTP サーバーを構成する必要があります。構成すると、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、ユーザーは Expressway にサインインするように求められます。

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

8. （Expressway に接続されているデバイスはこの手順をスキップします）

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 と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 に接続されているデバイスはこの手順をスキップします）

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。証明書がサーバーとのセキュア接続の認証、またはサーバー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 以降では、ITL ファイルがサポートされています。

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

11. Cisco Unified Communications Manager にお問い合わせください。構成ファイルは、デバイスと Cisco Unified Communications Manager との間の通信方法、およびロード ID をデバイスに提供する方法を定義します。TFTP サーバーからファイルを取得した後、リストで優先順位が最も高い Cisco Unified Communications Manager に接続を試みます。

デバイスのセキュリティ プロファイルがセキュアな信号（暗号化または認証）に構成され、Cisco Unified Communications Manager がセキュア モードに設定されている場合、デバイスは TLS 接続を行います。それ以外の場合は、デバイスは非セキュア 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、 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 データベースへの自動登録を試行します。

（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、デバイスを Cisco Unified Communications Manager データベースに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場合は、**[ようこそ（Welcome）]** 画面を表示し、セットアップ アシスタントを実行します。

起動中の TFTP サーバーを手動で設定

手順

ステップ 1 画面に [起動中...（Starting up...）] と表示されている間に、画面の左上隅を 3 回タップします。

ステップ 2 [起動中...（ Starting up... ）] の末尾に追加のピリオドが追加され、キー シーケンスが検出されたことを示します。

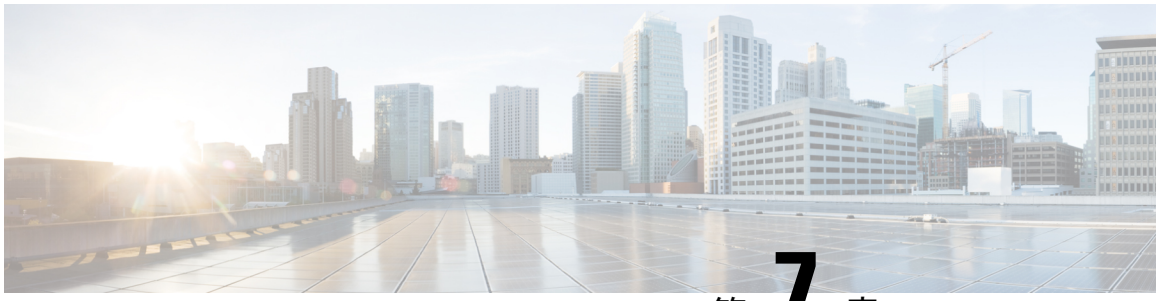
ステップ 3 TFTP 構成画面が表示されます。TFTP サーバー アドレスを入力し、**[確認（Confirm）]** をタップします。

起動確認22-02-2018 09:42

デバイスが電源に接続されると起動診断プロセスを開始し、次の一連の手順を実行します。

1. 起動のさまざまな段階で、デバイスがハードウェアをチェックしている間（Cisco DX650 のみ：ハンドセットのライトとミュート ボタンが赤く点滅し、ヘッドセット ボタンとスピーカー ボタンが緑に点滅します）、[ロック/電源（Lock/Power）] ボタンが点灯します（白）。
2. [電話（Phone）] アイコンがステータス バーに表示されます。

デバイスがこれらのステージを適切に完了すると、正常に起動し、[ロック/電源（Lock/Power）] ボタンが点灯したままになります。



第 7 章

連絡先

操作モード別の連絡先およびディレクトリ

連絡先ソース	パブリック モード	簡易モード	拡張モード
デバイスで作成	はい	はい	はい
Bluetooth からインポート	はい	はい	はい
Cisco ユーザー データ サービス（UDS）	はい	はい	はい
Jabber	いいえ	いいえ	○
Exchange グローバル アドレス リスト	いいえ	いいえ	○
Google	いいえ	いいえ	○
サードパーティ製アプリケーション	いいえ	いいえ	○

ローカルの連絡先

ローカル連絡先は、ユーザーが DX デバイスで作成する連絡先です。ローカル連絡先には、Bluetooth 経由で携帯電話からインポートされた連絡先を含めることもできます。

ユーザーは、一度に 200 件を超えるコンタクトをインポートしないことをお勧めします。

拡張モードでは、ローカルの連絡先には、Jabber、Exchangeアカウント、Googleアカウント、または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も含めることができます。

電話番号を持つローカル連絡先は、コール アプリケーションの [連絡先（Contacts）] タブで使用できます。すべてのローカル連絡先は、People アプリケーションで使用できます。

社内ディレクトリ

社内ディレクトリを使用すると、ユーザーは同僚の連絡先情報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構成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のユーザーに関する情報を保存し、Active Directory（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。

代替電話帳サーバーの設定

始める前に

代替電話帳サーバーでは、UDS および HTTPS プロトコルのみがサポートされます。

Expressway を介した Mobile and Remote Access を使用している場合は、代替電話帳サーバを Expressway サーバーの HTTP 許可リストに追加し、UDS サーバーの CA 証明書を Expressway サーバーの信頼リストにインポートします。Expressway による代替電話帳のサポートでは、要求は 256 文字に制限されます。これには、代行電話帳サーバーのホスト名、API 文字列、およびユーザーが入力した検索クエリ名が含まれます。

手順

ステップ 1 デバイスの [デバイス構成（Device Configuration）] ウィンドウの [製品固有の構成レイアウト（Product Specific Configuration Layout）] 部分で、**[代替電話帳サーバ タイプ（ Alternate phone book server type ）]** を [UDS] に設定します。

ステップ 2 [代替電話帳サーバーのアドレス（**Alternate phone book server address** ）] フィールドに電話帳サーバーの URL を入力します。URL にポートを含めない場合、デバイスは自動的にデフォルトのポート（8443）を使用します。

企業写真ディレクトリの設定

ユーザーが UDS を使用して社内ディレクトリを検索したとき、およびユーザーがローカル連絡先として追加したディレクトリ検索結果に対して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。

（注） 会社の写真ディレクトリでは、クレデンシャル（ユーザー名やパスワードなど）による認証を要求してはなりません。認証が必要な写真ディレクトリを指定した場合、ディレクトリ写真は DX デバイスに表示されません。

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 **会社の写真ディレクトリ** を **`http://<servername>/<path>/%%uid%%`** **に設定します。** **`<image file extension>`**。

ステップ 3 **[共通設定のオーバーライド（Override Common Settings）]** をオンにします。

連絡先検索

Cisco DX シリーズ ユーザーは、ローカルに保存されている連絡先、[履歴（Recents）]、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ーは、Jabber の連絡先や Exchange などのオンライン ディレクトリを検索することもできます。

ユーザーは次の条件で検索できます。

- 名（First name）
- 姓（Last name）
- 電話番号
- ユーザー名

ユーザーが [コール（Calls）] タブに番号を入力すると、デバイスは [通話履歴（Recents）] のみを検索します。ユーザーが [コール（Calls）] タブにテキストを入力すると、デバイスは使用可能なすべてのソースを姓名で検索します。重複する連絡先は検索結果から削除されます。

ユーザーは、[ディレクトリ（Directory）] タブで社内ディレクトリを検索できます。社内ディレクトリ検索では、最大 25 件の結果が表示されます。

検索結果には、写真（使用可能な場合）、名と姓、および 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る場合は、URI が表示されます。

アプリケーション ダイヤル ルール（Application Dial Rules）

アプリケーション ダイヤル ルールは、共有の携帯電話の連絡先をネットワークでダイヤル可能な番号に変換するために使用します。アプリケーション ダイヤル ルールは、ユーザが番号を手動でダイヤルした場合、またはユーザがコールを発信する前に番号が編集された場合は適用されません。

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

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

アプリケーション ダイヤル ルールの設定

手順

ステップ 1 [Cisco Unified 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。

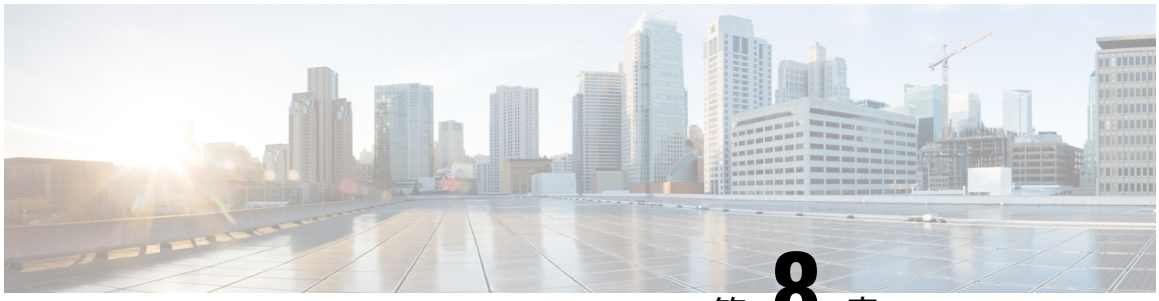
ステップ 2 [新規追加（Add New）] を選択して新規のアプリケーション ダイヤル ルールを作成するか、既存のアプリケーション ダイヤル ルールを選択してそれを編集します。

ステップ 3 次のフィールドを入力します。

- [名前（Name）]：このフィールドには、ダイヤル ルールの一意の名前を入力します。名前は最大 20 文字の英数字で、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア文字（_）の任意の組み合わせを含めることができます。

- [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 ルールを適用する電話番号の最初の桁を入力します。
- [削除する合計桁数（Total Digits to be Removed）]：この必須フィールドには、アプリケーション ダイヤル ルールに該当する電話番号から Cisco Unified Communications Manager によって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 ルールに該当する電話番号の先頭に追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）] に情報を入力する際に表示されます。このフィールドでは、アプリケーション ダイヤル ルールの優先順位を設定できます。

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



第 8 章

セルフ ケア ポータルの管理

セルフ ケア ポータルの概要

Cisco Unified Communications セルフ ケア ポータルでは、ユーザが電話機の機能および設定をカスタマイズしたり制御したりすることができます。

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

ユーザーによって 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、ユーザーを 標準 Cisco Unified Communications Manager エンドユーザーグループに追加します。

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

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

  https://<server_name:portnumber>/ucmuser/。server_name は、Web サーバーがインストールされているホストで、portnumber その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。

これらの設定は、ユーザーを Cisco Unified Communications Manager に追加した時に入力した値と同じです。

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

セルフ ケア ポータルへのユーザ アクセスのセットアップ

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

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザー管理（User Management）] > [エンドユーザー（End User）]** の順に選択します。

ステップ 2 ユーザを検索します。

ステップ 3 ユーザの [ID] リンクをクリックします。

ステップ 4 ユーザのパスワードと PIN が設定されていることを確認します。

ステップ 5 [アクセス許可情報（Permission Information）] セクションで、[グループ（Groups）] リストに [標準CCMエンドユーザ（Standard CCM End Users）] が含まれていることを確認します。

ステップ 6 [保存（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、次のオプションは、[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で [エンタープライズパラメータ設定（Enterprise Parameters Configuration）] の設定値を使用して設定する必要があります。

- 呼出音設定の表示（Show Ring Settings）
- 回線のテキストラベル設定の表示（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。

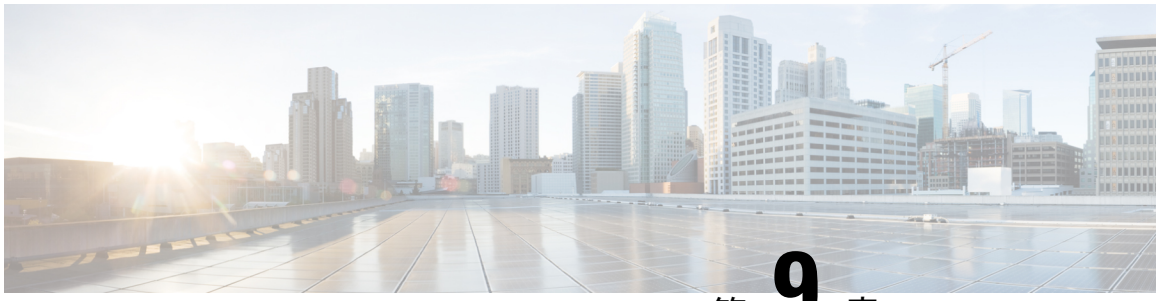
手順

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 9 章

付属品

Bluetooth アクセサリ

ユーザーは、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 デバイスにペアリングできます。

ユーザーは一度に複数の Bluetooth デバイスをペアリングできますが、一度にペアリングできる Bluetooth オーディオ デバイスは 1 つだけです。

Bluetooth を有効にすると、ワイヤレス ネットワーク接続が低下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 帯域を使用する必要があります。

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、ペアリングされたデバイスで使用可能な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、そのプロファイルはオフになり、ユーザーはそのプロファイルを有効にできません。

ハンズフリー プロファイル

Cisco DX シリーズデバイスはさまざまなハンズフリープロファイル機能をサポートしており、アクセサリ（Bluetooth ワイヤレス ヘッドセットおよび Bluetooth 対応携帯電話など）を使用することで、デバイスを操作することなく特定のタスクを実行することができます。例えば、

ユーザーはデバイス上でリダイヤルをタップするのではなく、ヘッドセットのメーカーの指示に従って、Bluetooth ワイヤレス ヘッドセットから番号をリダイヤルすることができます。

Bluetooth アクセサリには、次のハンズフリー機能が適用されます。

- Bluetooth HFP の接続/切断ステータスを処理します。
- Audio Gateway（AG）で電話番号をダイヤルしてコールを発信します。
- コールがいつ接続または切断されたかを示します。
- コールが着信したときにアプリケーションに通知します（インバンド着信音）。
- インバンド着信を有効または無効にします。
- 電話機のステータス（発信者 ID、信号強度、バッテリ レベルなど、AG から）を報告します。
- 通話を応答または拒否します。
- 発信者 ID を含むコール待機通知を受信します。
- コールを保留にして、待機中のコールに切り替えます。
- AG およびコール アプリケーションで、保留中のコールとアクティブなコールを切り替えます。
- 音声を携帯電話に切り替え、音声をハンズフリーユニットに戻します。
- 携帯電話のコール リストを取得します。

ハンズフリー デバイスは、機能のアクティベート方法が異なる場合があります。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、メーカーのマニュアルを参照してください。

電話帳へのアクセス プロファイル

Bluetooth 電話帳アクセス プロファイル（PBAP）を使用すると、ユーザーはペアリングされた携帯電話から Cisco DX シリーズ デバイスに連絡先と通話履歴を共有できます。ユーザーは、携帯電話をペアリングするときに、連絡先と通話履歴を手動でダウンロードするか、自動的にダウンロードするかを選択できます。また、連絡先をデバイスに保存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 Communications Manager の管理で、**[デバイスの > 電話（Device Phone）]** を選択し、変更するデバイスを見つけて、そのデバイスの **[電話の構成（Phone Configuration）]** ウィンドウに移動します。

ステップ 2 **[電話の構成（Phone Configuration ）]** ウィンドウで、[Bluetooth（Bluetooth）] 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リングするデバイスをタップします。

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

Bluetoothを無効にする

手順

ステップ 1 [Cisco Unified Communications Manager Administration] で、**[Device]** > **[Phone]** を選択します。

ステップ 2 **[電話の検索と一覧表示（Find and List Phones）]** ウィンドウで、変更するデバイスの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 **[電話の構成（ Phone Configuration ）]** ウィンドウの [製品固有の構成のレイアウト（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、デバイスをデスクトップに固定できます。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、アドオン Logitech C920-C Webcam または Logitech C930e を外部カメラとしてサポートします。

外部カメラをデバイスに接続すると、ユーザはポイントツーポイントのビデオコールを発信できます。外部カメラを機能させるには、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） Cisco DX650 が Power over Ethernet によって電源供給されている場合、外部カメラには 802.3at が必要です。電話機が Power over Ethernet によって電源供給されていない場合、外部カメラには外部電源が必要です。

外部カメラ設定

外部カメラをデバイスに接続すると、ユーザーは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。

外部カメラ設置後のチェックの実施

手順

ステップ 1 [外部カメラが接続されました（External Camera Connected）] という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 デバイスと外部カメラを、視野内に明るい光が入らない位置に移動します。

ステップ 5 ユーザーが正面から照らされるように、デバイスと外部カメラを移動します。

外部スピーカーおよびマイクロフォン

外部スピーカー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。ライン入出力ジャックを使用して、外部 PC タイプ マイクや電源スピーカー（アンプ付き）をデバイスに接続することができます。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ーが無効になります。

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

ヘッドセット

Cisco ではサードパーティ ヘッドセットの内部テストを実行しますが、Cisco はヘッドセットまたはヘッドセット ベンダーの製品を認定またはサポートしていません。

デバイスは、ヘッドセットのマイクが検出するバックグラウンドノイズを一部低減しますが、バックグラウンドノイズをさらに低減して全体的な音声品質を向上させる場合は、ノイズキャンセリング ヘッドセットを使用します。

Cisco では、不要な無線周波数（RF）信号および可聴周波数（AF）信号を遮蔽するヘッドセットなど、高品質な外部デバイスの使用を推奨します。ヘッドセットの品質や、携帯電話や双方向ラジオなどの他のデバイスとの距離によっては、雑音やエコーが入ることもあります。可聴ハム雑音などのノイズは、相手方だけに聞こえる場合もあれば、ユーザーおよび相手方の両方に聞こえる場合もあります。ハム音またはバズ音は、さまざまな外的な要因、たとえば、電灯、電気モーター、大型の PC モニタなどによって引き起こされる場合があります。

（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。

デバイスが展開される場所によってこれらの環境およびハードウェアが異なるため、すべての環境において最適な唯一のヘッドセットは存在しません。

Cisco では、ヘッドセットを購入し、大規模に展開する前に、想定される環境でヘッドセットをテストし、パフォーマンスを確認することを推奨しています。

（注） 同時に動作するのは1つのヘッドセット タイプのみです。デバイスに接続されている Bluetooth ヘッドセットおよびアナログ ヘッドセットの両方を使用する場合、Bluetooth ヘッドセットを有効にすると、アナログ ヘッドセットは無効になります。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。USB ヘッドセットを Bluetooth ヘッドセットが有効になっているデバイスにプラグ接続するとき、Bluetooth およびアナログ ヘッドセットの両方を無効にします。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 つのヘッドセットに接続できます。最後に接続されたヘッドセットがデフォルトとして使用されます。通常、ペアリングはヘッドセットごとに1回実行されます。

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

Bluetooth ヘッドセットのワイドバンドはサポートされていません。Bluetooth ヘッドセットを使用すると、音声品質が低下する場合があります。

最適なパフォーマンスは、1～2 メートル（3～6 フィート）の範囲で得られます。ヘッドセットは5個以上接続できますが、最後に接続され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 30 フィート（10 m）を超えて離れていると、Bluetooth の接続は 15 ～ 20 秒間のタイムアウト後にドロップされます。ペア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。電力節約モードで動作する特定のデバイスの場合、ユーザーは操作ボタンをタップして再接続を開始し、ヘッドセットを「ウェイク アップ」させることができます。

干渉が発生する可能性が考えられます。Cisco 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のユーザー 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 モードにします。

（注） ヘッドセットを検出/ペアリング モードにする手順は、ヘッドセットに固有です。ペアリング手順については、ヘッドセットの製造元の指示を参照してください。

正常にペアリングしてデバイスに接続するには、ヘッドセットが検出/ペアリングモードになっている必要があります。

ステップ 2 まだ行っていない場合は、デバイスの Bluetooth をオンにします。

Bluetooth がオンになっているかどうかを確認するには、ステータスバーの Bluetooth アイコンを探します。

ステップ 3 **[デバイスのスキャン（Scan for devices）]** を選択します。

Bluetooth デバイスが見つかると、その名前がウィンドウに表示されます。

デバイスは自動的に PIN 0000 を使用してヘッドセットとペアリングします。ヘッドセットが別の PIN を使用している場合は、ヘッドセットに付属のユーザー ガイドに記載されている正しい PIN を入力します。

（注） ペアリングに失敗した場合、デバイスは正しい PIN を入力するように求めます。

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行します。デバイスが接続できない場合は、エラー アラートが表示され、ユーザーに失敗の理由が通知されます。デバイスがアクセサリを接続しようとすると、10秒のタイムアウトが発生します。接続に成功せずにタイマーが期限切れになると、エラー アラートが表示されます。

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

ヘッドセットがデバイスの範囲外にある場合、Bluetooth は 15 ～ 20 秒のタイムアウト後に接続を切断します。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。ヘッドセットを起動して再接続プロセスを開始するには、ヘッドセットの操作ボタンをタップする必要があります。

ユーザーがアクティブ コールで Bluetooth ヘッドセットを使用していて、ヘッドセットがオフに設定されているか、範囲外にあるか、何らかの理由で切断されている場合、アラートがユーザーにスピーカー/ヘッドセットでコールを続行するか、またはコールします。ユーザーが 30 秒以内にアクションを実行しない場合、コールは終了します。

Bluetooth ヘッドセットの削除

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 ヘッドセットのベース ステーション）は、任意の USB ポートに接続できます。

USB ヘッドセットの有効化

USB ヘッドセットを使用するには、USB ポートを有効にする必要があります。デフォルトでは、USB ポートが無効になっています。USB ポートが無効になっている場合は、Cisco Unified Communications Manager 管理の **[電話の構成（Phone Configuration ）]** ウィンドウ（**[デバイスの > 電話（DevicePhone）]**）、**[エンタープライズの電話の構成（Enterprise Phone Configuration）]** ウィンドウ（**[システム > エンタープライズの電話の構成（SystemEnterprise 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 USB ポートを有効にできます。）。

手順

ステップ 1 ウィンドウの [製品固有の構成（Product Specific Configuration）] レイアウト部分で、該当する 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）] パラメータで **[音声クラス（Audio Class）]** を選択し、 **[共通設定のオーバーライド（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 Communications Manager Administration で有効にした USB ポートを無効にします（または 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 シングルプラグヘッドセットをサポートします。ユーザーは、ヘッドセットを使用してコールを発信および応答できます。

有線ヘッドセットの接続

手順

ヘッドセットをヘッドセット ポートに差し込みます。

有線ヘッドセットの無効化

ヘッドセットを無効にするには、 Cisco Unified Communications Manager 管理を使用します。これを行うと、スピーカーフォンも無効になります。

手順

ステップ 1 Cisco Unified Communications Manager 管理から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 **[電話構成（Phone Configuration）]** ウィンドウ（[製品固有の構成レイアウト（Product Specific Configuration layout）] 領域）で、**[スピーカーフォンおよび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 は、HDMI ポートを介して外部ディスプレイデバイスをサポートします。HDMI ケーブルの一方の端をHDMIポートに、もう一方の端をモニターのHDMIポートに挿入して、モニタをデバイスに接続します。

Cisco DX650 壁取り付けキット

Cisco DX650 を壁面に取り付けるには、 Cisco DX650 壁面取り付けキットに含まれ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、デバイスとは別に注文する必要があります。

はじめる前に

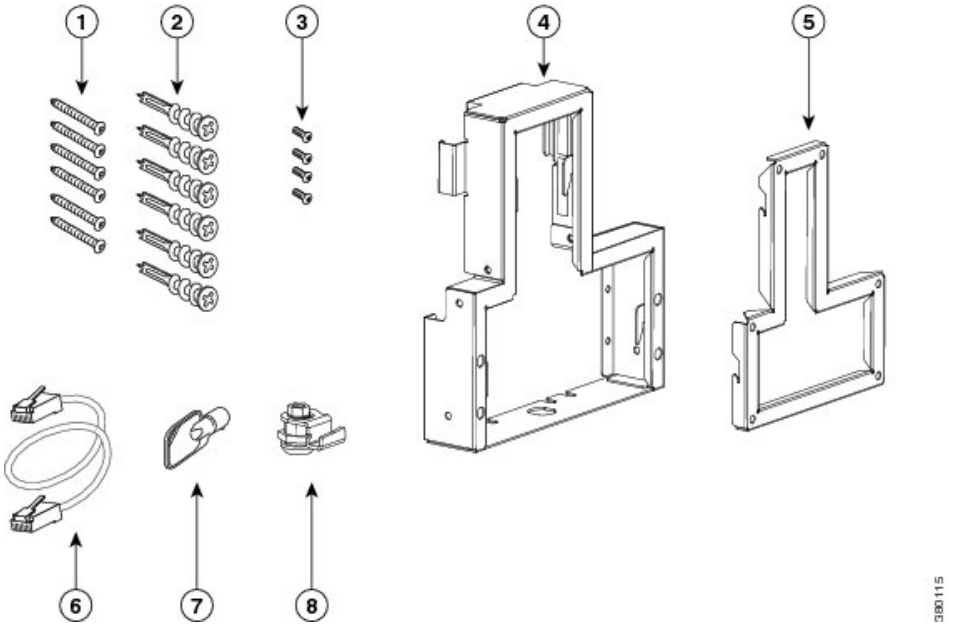
ブラケットの取り付けには、次の工具が必要です。

- No.1 および No.2 プラス ドライバ
- レベル

壁取り付けコンポーネント

（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。レンガやコンクリートなどの他の表面に取り付ける場合は、独自のハードウェアを用意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 x 6 個	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	1 つのロックダウン キー
4	電話機用ブラケット x 1 個	8	1 つのロック

壁取り付けの設置

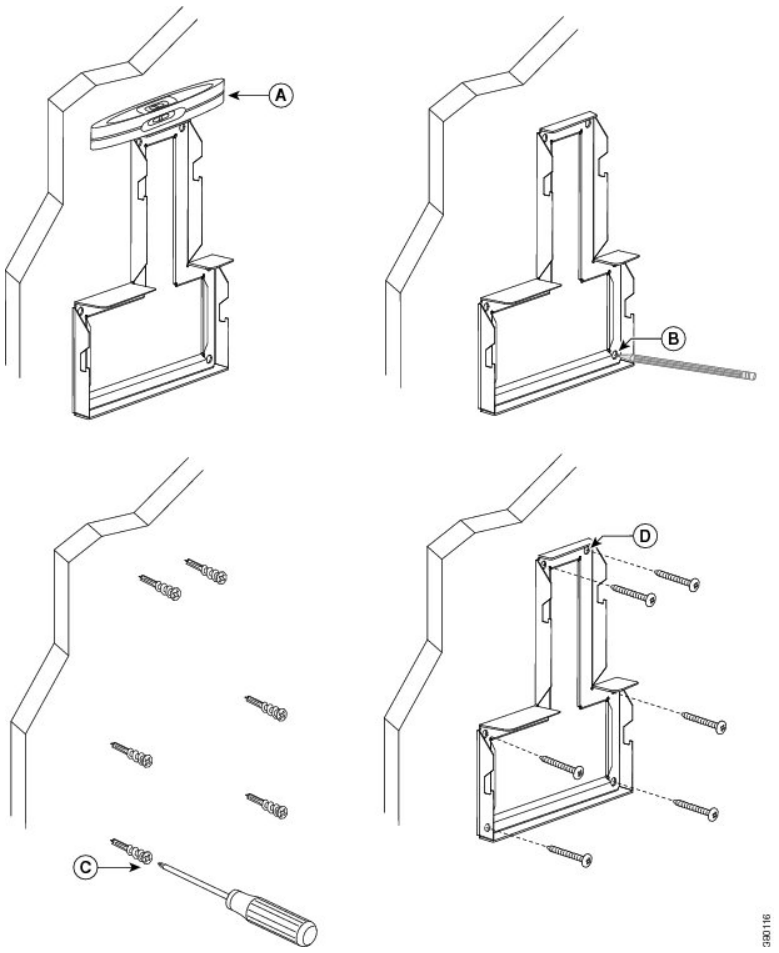
手順

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) アンカーを鉛筆マークの上に慎重に置いて、#2 のプラス ドライバーでアンカーを壁に押し込みます。
c) アンカーを時計回りの方向に回し、壁面と平らになるまで押し込みます。
d) 付属のネジと #2 のプラス ドライバーを使用して、ブラケットを壁面に設置します。

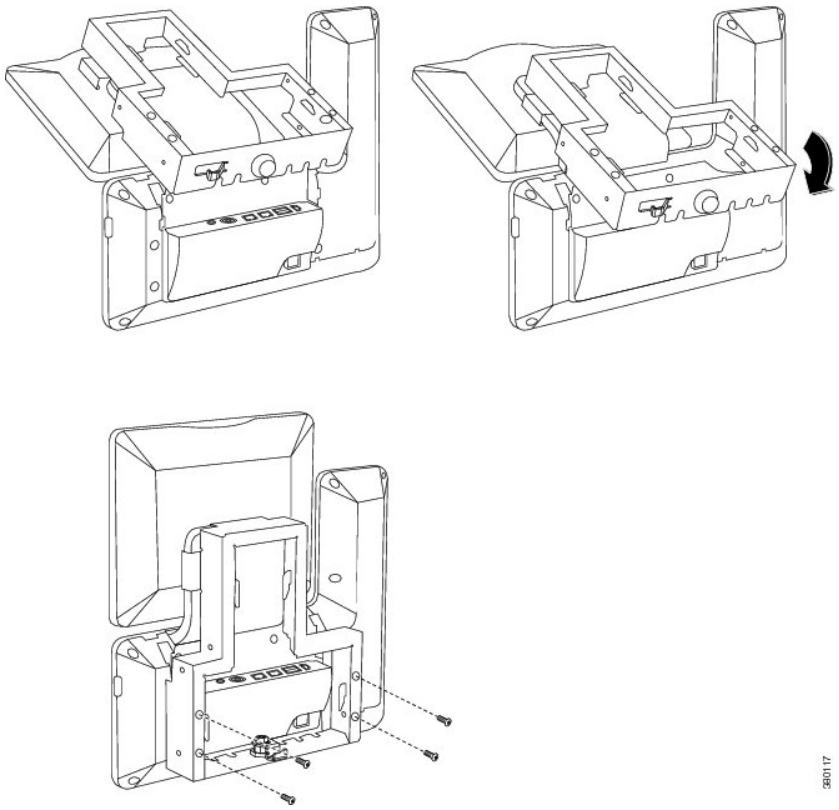
図 *2:* 壁面用ブラケットの設置



ステップ 2 電話機用ブラケットをデバイスに装着します。

a) デバイスのベースから接続されているコードを取り外します。
b) 電話機用ブラケットを電話機にスライドします。ブラケットの穴から、デバイス 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、電話用ブラケットをデバイスに固定します。
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

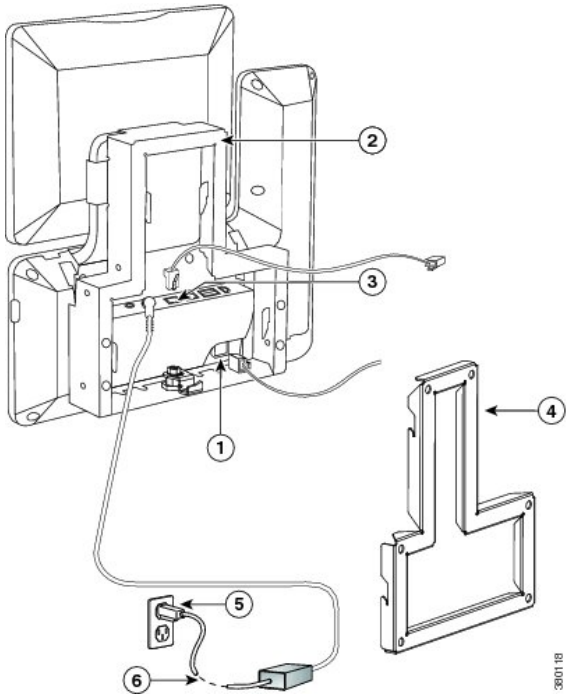


ステップ 3 イーサネット ケーブルを 10/100/1000 SW ネットワーク ポートと壁面のジャックに接続します。

ネットワーク デバイス（コンピュータなど）をデバイスに接続している場合、ケーブルを 10/100/1000 コンピュータ（PC アクセス）ポートに接続します。

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。

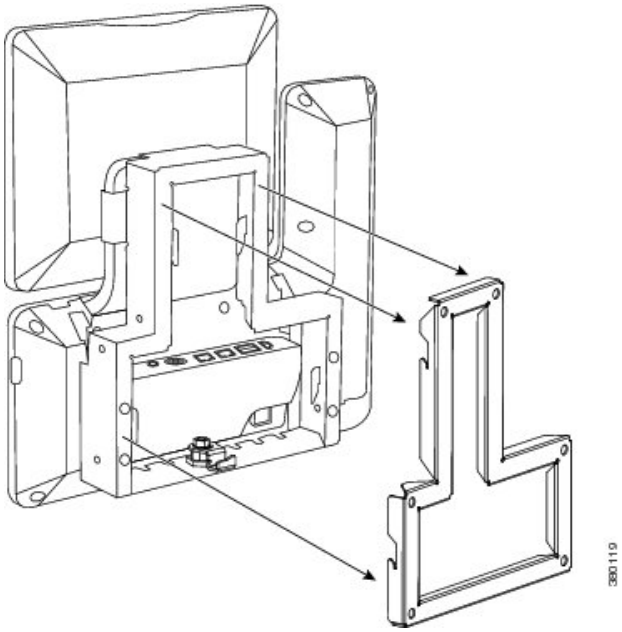
図 *4 :* ケーブルの接続



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 デバイスを壁面ブラケットに取り付けるには、電話機用ブラケット上部のタブを壁面ブラケットのスロットに差し込みます。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。

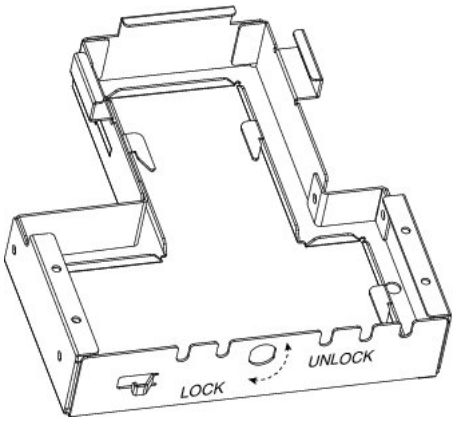
図 *5:* 壁面用ブラケットへのデバイスの設置

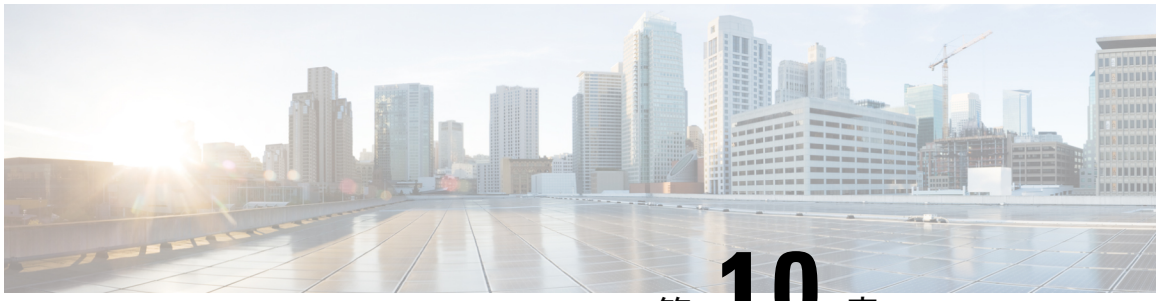


ステップ 5 ロックダウン キーを使用して、デバイスを壁面用ブラケットにロックします。

電話機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 フック付き電話機ブラケット





第 10 章

セキュリティ機能

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 リリース 8.5(1) 以降にはデフォルトでセキュリティ機能が搭載されており、CTLクライアントを実行しなくても、デバイスに次のセキュリティ機能が提供されます。

- 構成ファイルの署名
- 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 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。『*Cisco Unified Communications Manager Security Guide*』で説明されているように、Cisco Unified Communications Manager 管理を使用して LSC を構成できます。

あるいは、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 の更新および削除も実行できます。

セキュリティ機能の概要

Cisco Unified Communications Manager システムでセキュリティを実装すると、デバイスや Cisco Unified Communications Manager サーバの ID 盗用、データの改ざん、およびコール シグナリングとメディア ストリームの改ざんを防止できます。

これらの脅威を軽減するため、Cisco 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・維持します。ファイルはデジタル署名してからデバイスに転送されます。デバイス間ではメディア ストリームとコール シグナリングが暗号化されます。

Cisco DX シリーズ デバイスは、デバイスがセキュリティ保護の対象になるかどうかを定義するデバイス セキュリティ プロファイルを使用します。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は、「『*Cisco Unified Communications Manager Security Guide*』」を参照してください。

Cisco Unified Communications Manager 管理のセキュリティ関連設定を構成する場合、構成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「「暗号化電話構成ファイルの設定」」の章を参照してください。

次の表に、電話でサポートす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

特長	説明
イメージ認証	署名済みバイナリ ファイル（拡張子 .sbn）および暗号化バイナリ ファイル（拡張子 .sebn）によって、ファームウェア イメージがデバイスへのロード前に改ざんされることを防止します。 イメージが改ざんされると、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	各デバイスは、デバイス認証に一意の証明書を必要とします。デバイスには Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）が含まれますが、追加のセキュリティについては、Cisco Unified Communications Manager 管理ページで、Certificate Authority Proxy Function（CAPF; 認証局プロキシ関数）を使用して証明書のインストールを指定できます。あるいは、デバイスの [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決定します。必要に応じて、TLS プロトコルを介してエンティティ間にセキュアなシグナリング パスを作成します。 Cisco Unified Communications Manager は、デバイスを認証できる場合を除き、デバイスを登録しません。

特長	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ファイルを検証します。ファイル作成後のファイルの改ざんを防ぐため、デバイスでシグニチャを検証します。認証できないファイルは、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	暗号化は、ファイルがデバイスに転送されている間、機密情報の漏洩を防ぎます。さらにデバイス側でも、ファイルが作成後に改ざんされていないことを署名確認により認証します。認証できないファイルは、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、固有の製造元でインストールされる証明書（MIC）が内蔵されており、デバイス認証に使用されます。MIC は、個々のデバイスを識別するために永続的に割り当てられた証明であり、Cisco Unified Communications Manager はこれを使用してデバイスを認証します。
メディア暗号化	SRTP を使用して、サポートされるデバイス間のメディア ストリームがセキュアであること、および意図したデバイスのみがデータを受信し、読み取ることを保証します。デバイスのメディア プライマリ キーペアの作成、デバイスへのキーの配布、キーが転送される間のキーの配布のセキュリティの確保などが含まれます。
CAPF（Certificate Authority Proxy Function）	デバイスに非常に高い処理負荷がかかる、証明書生成手順の一部を実装します。また、キーの生成および証明書のインストールのためにデバイスと対話します。デバイスの代わりに、お客様指定の認証局に証明書を要求するよう CAPF を構成できます。または、ローカルで証明書を生成するように CAPF を構成することもできます。
セキュリティ プロファイル（Security profile）	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。これらの機能に関する詳細は、『*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	デバイスの構成ファイルのプライバシーを確保できるようにします。
電話機の Web サーバの無効化（オプション）	セキュリティ上の目的で、デバイスの 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。

特長	説明
電話のセキュリティ強化	Cisco Unified Communications Manager 管理ページから制御する追加セキュリティ オプション。 • PC ポートの無効化 • Gratuitous ARP（GARP）の無効化 • PC ボイス VLAN アクセスの無効化 • Web アプリケーションへのアクセスの制限 • Bluetooth アクセサリ ポートの無効化 • デバイスの Web ページへのアクセスの無効化 • スクリーン ロック必須 • Google Play へのアクセスの制御™ • 不明なソースからのアプリケーションのインストールへのアクセスを制御する
802.1X 認証	デバイスは 802.1X 認証を使用して、ネットワークへのアクセスの要求およびネットワーク アクセスができます。
SRST 向けのセキュアな SIP フェールオーバー	セキュリティ目的で Survivable Remote Site Telephony（SRST）リファレンスを構成してから、Cisco Unified Communications Manager 管理ページで従属デバイスをリセットすると、TFTP サーバはデバイスの 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 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・提供できます。

セキュリティ プロファイル（Security Profiles）

Cisco DX シリーズ デバイスは、デバイスが非セキュア、認証、または暗号化のいずれであるかを定義するセキュリティ プロファイルを使用します。セキュリティ プロファイルの構成とデバイスへのプロファイルの適用については、「『*Cisco Unified Communications Manager Security Guide*』」を参照してください。

デバイスに設定されているセキュリティ モードを表示するには、[設定（Settings）] アプリケーションの [セキュリティ（Security）] メニューを表示します。

SE Android

Android™（SE Android）のセキュリティ拡張機能は、デバイスのセキュリティを強化します。SE Androidは、デバイス上で不正または危険なコードの実行を防止することで、悪意のあるアプリケーションから保護します。SE Android は次の処理を実行します。

- プロセスによる権限昇格を防止できます
- root などの特権プロセスが侵害された場合に、誤用を防止し、損害を制限できます
- 一元化された分析可能なポリシーを提供
- 未検出の脆弱性から保護

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

- 許可
- 適用

ポリシーに違反するものはすべてログに記録されます。モードが enforcing の場合、アクションは拒否されます。ポリシーまたはモードに対するユーザー制御も管理者制御も存在しません。

アップグレードおよび SE Android

リリース 10.2(2) にアップグレードすると、 Cisco DX650 は既存のフィールドユニットで動作する必要があり、強制モードを有効にする前に初期設定の状態にリセットする必要があるため、permissiveモードのままになります。permissiveモードでは、SE Androidはエンドポイントの動作に影響を与えません。

Cisco DX650が初期設定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。このアクションにより、SE Android保護がアクティブになり、ポリシーに違反するアクションの拒否が開始されます。

Enforcing モードは、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、有効なままです。リリース 10.2(2) 以降にアップグレードすると、初期設定へのリセットが実行されるまで、デバイスは permissive モードに戻ります。

Cisco DX70 および Cisco DX80 デバイスは、初期設定から常に enforcing モードになっています。Cisco DX70 および Cisco DX80 デバイスを permissive モードにすることはできません。

SE Android トラブルシューティング

ポリシーは、アプリケーションが実行できることを想定して調整されます。ただし、許可する必要がある操作がポリシーによって禁止されている場合があります。ポリシーエラーの症状には、次のようなものがあります。

- サードパーティまたはその他のアプリが起動時または実行中にエラーを表示します。
- アプリケーションまたは機能は、 Cisco DX650 などの permissive モードのエンドポイントでは動作しますが、同様に構成された強制モードのデバイスでは動作しません。
- SE Androidは常時稼働の機能であり、管理者の制御下にはありません。現場での問題を診断し、欠陥として報告する必要があります。

SE Androidポリシーの問題の診断

手順

ステップ 1 SE Android モードを決定します。

a) 設定アプリケーションで、**[端末について（About device）]** > **[SELinux 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 に関連していません。

ステップ 2 モードが enforcing の場合は、permissive モードのデバイスで再テストします。
問題が permissive モードで再現できない場合、問題は SE Android に関連している可能性が高いです。

ステップ 3 問題が SE Android に関連しているか、特定できない場合は、ログを収集して報告します。

ADB Shell 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場合があります。

完全な結果を得るには、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。

Enforcing モードでは、多くのディレクトリが立ち入り禁止であるため、ファイル システムを自由に参照することもできません。

SE Android ログ収集

問題を報告するには、次の情報を収集します。

- 問題の簡単な説明（発生時刻を含む）
- 問題のスクリーンショット（可能な場合）
- debugsh **show selinux all** コマンドの出力
- Problem Reporting Tool（PRT）の出力

ローカルでの重要な証明書のセットアップ

始める前に

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

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

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 の構成後に設定された CAPF 認証コードを入手します。

ステップ 2 [設定（Settings）] アプリケーションで、**[セキュリティ（Security）]** > **エンタープライズ セキュリティ設定**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 の構成に応じて、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。この作業の間、一連のメッセージが表示されるので、進捗状況をモニタリングできます。

（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。**[キャンセル（Cancel）]** をタップすると、いつでもプロセスを停止できます。

インストール手順が正常に完了すると、デバイスに [インストール済み（ Installed）] と表示されます。デバイスに [未インストール（Not Installed）] と表示された場合は、認証文字列に誤りがあるか、デバイスのアップグレードが有効になっていない可能性があります。CAPF 操作で LSC が削除され、デバイスに [未インストール（Not Installed）] と表示された場合、それは操作が成功したことを示しています。CAPF サーバで生成されたエラーメッセージを確認し、適切なアクションを実行します。

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

SHA-256 製造元でインストールされる証明書

Cisco DX70 および Cisco DX80 は、RSA 2048 キーを使用した SHA-256 のシグネチャ アルゴリズムを使用する製造元でインストールされる証明書（MIC）を使用します。シグネチャアルゴリズムには、 Cisco Unified Communications Manager、Cisco Secure Access Control Server（ACS）、および Secure SRST のサポートが必要です。

SHA-256 MIC 機能には、次のサポート要件があります。

- Cisco Unified Communications Manager リリース 9.1(2) 以降：
- ACS リリース 5.2 以降。

（注） ACS 5.2 以降では、EAP-TLS 内部方式を使用した EAP-FAST はサポートされません。EAP-TLS を使用するか、EAP-TLS 内部方式を使用した EAP-FAST の場合は ISE に移行します。

- IOS 12.4(15)T1 以降
- Cisco Identity Services Engine リリースは 1.1 以降です。EAP-TLS 内部方式を使用した EAP-FAST は、ISE リリース 1.2 以降でサポートされています。

このシリーズの電話機の MIC を発行する Cisco 認証局は、別のアプリケーションが使用され、これらのアプリケーションが電話機から MIC を認証する必要がある場合、次のリンクから取得できます。

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

アプリケーションが Cisco DX シリーズ デバイスの MIC を認証するには、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 Communications Manager Administration の **[電話の構成（Phone Configuration）]** ウィンドウで [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ている場合、コールアプリケーションに [セキュア コール（Secure Call）] アイコンが表示されている場合は、セキュアな通話を示します。

セキュアなコールでは、すべてのコール シグナリングとメディア ストリームが暗号化されます。セキュアなコールは高度なレベルのセキュリティを提供し、コールに整合性とプライバシーを提供します。進行中のコールが暗号化されている場合、[設定（Settings）] 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 ）]** の [セキュリティ モード（Security Mode）] ステータスが [暗号化（Encrypted）] と表示されます。

（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 コールでは、コールが暗号化され、両方のデバイスが保護されたデバイスとして設定されている場合、および Cisco Unified Communications Managerでセキュア トーン機能が有効になっている場合、2 秒間のトーンがユーザーに通知されます。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、デバイスは非セキュア表示トーン（6 ビープ）を再生し、コールが保護されていないことをユーザーに警告する。セキュ

ア通知トーン機能および構成要件の詳細な説明については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

（注） 音声とビデオはセキュアとして送信できますが、プレゼンテーションは非セキュアとして送信されます。**[暗号化されたロック（Encrypted lock）]** アイコンは、デフォルトでプレゼンテーションを使用したコールに表示されます。**[システム（System）]**>**[サービス パラメータ（Service Parameter）]** の Cisco Unified Communications Manager の別のオプションに、**[セキュア コール アイコン表示ポリシーが必要（Secure Call Icon Display Policy Required）]** を構成できます。デフォルトでは、**[BFCP および iX トランスポート以外の全メディアを暗号化すべき（All media except BFCP and iX transports must be encrypted）]** に設定されています。

セキュアな電話コールの識別

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に構成されている場合、セキュアなコールが確立されます。両方のデバイスは、同じ Cisco IP ネットワーク内にあっても、Cisco IP ネットワーク以外のネットワークにあってもかまいません。セキュアな電話会議は、次のプロセスに従って確立されます。

1. ユーザーがセキュアなデバイス（暗号化セキュリティ モード）でコールを開始します。
2. デバイスは、[設定（Settings）] 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 [暗号化（Encrypted）] ステータスを示します。このステータスは、このデバイスがセキュアなコール用に設定されていることを示しますが、接続する他の電話機もセキュアであるという意味ではありません。
3. コールが別のセキュアなデバイスに接続される場合、セキュリティ トーンが再生されます。これは、会話の両端が暗号化されセキュアであることを示します。それ以外の場合は、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「「セキュアおよび非セキュア表示トーンの設定」」の章を参照してください。

セキュアな会議コールの識別

セキュアな会議コールを開始し、参加者のセキュリティ レベルをモニタすることができます。セキュアな電話会議は、次のプロセスに従って確立されます。

1. ユーザーがセキュアなデバイスで会議を開始します。
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、各電話のセキュリティ 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. デバイスでは会議コールのセキュリティ レベルが表示されます。

さまざまなインタラクション、制限、および制限が、参加者のデバイスのセキュリティモードとセキュアな会議ブリッジの可用性によって決定される会議コールのセキュリティ レベルに影響します。 Cisco DX シリーズ デバイスは、セキュアな音声およびビデオ会議コールをサポートします。

音声とビデオはセキュアとして送信できますが、プレゼンテーションは非セキュアとして送信されます。**[暗号化（Encrypted）]** ロック アイコンは、デフォルトでプレゼンテーション付きの会議コールに表示されます。**[システム（System）] > [サービス パラメータ（Service Parameter）]** の Cisco Unified Communications Manager の別のオプションに、**[セキュア コール アイコン表示ポリシーが必要（Secure Call Icon Display Policy Required）]** を構成できます。デフォルトでは、**[BFCP および iX トランスポート以外の全メディアを暗号化すべき（All media except BFCP and iX transports must be encrypted）]** に設定されています。

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。次の表に、割り込み機能によるコールセキュリティ レベルの変更に関する情報を示します。

表 *16 :* コール セキュリティと割り込み機能の連携動作

発信側電話機のセキュリティ レベル	使用する機能	コールセキュリティ レベル	動作結果
非セキュア	割込み	暗号化されたコール（Encrypted call）	コールが割り込まれ、非セキュア コールと別される
セキュア	割込み	暗号化されたコール（Encrypted call）	コールが割り込まれ、セキュア コールとしされる

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された、会議のセキュリティ レベルの変更に関する情報を示しています。

表 *17 :* 会議コールのセキュリティの制限事項

発信側電話機のセキュリティ レベル	使用する機能	参加者のセキュリティ レベル	動作結果
非セキュア	会議（Conference）	強化されたセキュリティ	非セキュアな会議ブリッジ 非セキュアな会議

発信側電話機のセキュリティ レベル	使用する機能	参加者のセキュリティ レベル	動作結果
強化されたセキュリティ	会議（Conference）	少なくとも1台のメンバーが非セキュア。	セキュアな会議ブリッジ 非セキュアな会議
強化されたセキュリティ	会議（Conference）	強化されたセキュリティ	セキュアな会議ブリッジ セキュアな暗号化レベルの会議
非セキュア	Meet-Me	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 レベルを満ん。コールは拒否されました（Doe Security Level, call rejected）」という受け取ります。
強化されたセキュリティ	Meet-Me	最小限のセキュリティ レベルが非セキュア。	セキュアな会議ブリッジ 会議はすべてのコールを受け入れま

セキュアなビデオが VPN および Cisco Virtualization Experience Client（VXC）VPN を介して使用されている場合、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。

リモートでのデバイス セキュリティ情報のチェック

手順

ステップ 1 デバイスの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か以前に登録されており、デバイス構成ページで Web アクセスが有効になっている必要があります。

ステップ 2 Web ブラウザで、 **http://** に移動します。<device ip>デバイスのセキュリティ情報を表示する/SecurityInformation 、または **http://** /SecurityInformationX：デバイスのセキュリティ情報を XML 形式で表示します。

割り込みのための暗号化

デバイスに暗号化が構成されていない場合、ユーザーは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構成されている場合、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コールに分類します。

割り込みの開始側のデバイスに暗号化が構成されている場合、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す。CDP では、ローカルに接続されたワークステーションは識別されません。Cisco 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際 LAN スイッチとして動作しません。

Cisco DX シリーズデバイスはまた、プロキシ EAPOL ログオフ メカニズムも提供します。ローカルに接続された PC が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保持するため、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。これは、LAN スイッチにダウンストリーム PC の認証エントリをクリアさせます。

Cisco DX シリーズ デバイスには 802.1X サプリカントも含まれています。このサプリカントを使用して、ネットワーク管理者はデバイスと LAN スイッチ ポート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 デバイスの 802.1X 認証のサポートには、次のようなコンポーネントが必要です。これには、以下が含まれます。

- デバイス自体が 802.1X サプリカントとして機能し、ネットワークへのアクセス要求を開始します。
- Cisco Secure Access Control Server（ACS）（またはその他のサードパーティ認証サーバ）。認証サーバは、デバイスを認証する共有秘密を使用して設定する必要があります。
- Cisco Catalyst スイッチ（またはその他のサードパーティ製スイッチ）。スイッチは、オーセンティケータとして機能し、デバイスと認証サーバの間でメッセージを渡すことができるように、802.1X をサポートしている必要があります。この交換が完了した後、スイッチはネットワークへのデバイスのアクセスを許可または拒否します。

Best Practices

The following list describes requirements and recommendations for 802.1X configuration.

- Enable 802.1X Authentication: If you want to use the 802.1X standard to authenticate Cisco DX シリーズ devices, be sure that you properly configure the other components before you enable authentication on the device.
- Configure PC Port: The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the device.
  - Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, the devices support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:

    http://www.cisco.com/c/en/us/support/switches/catalyst-6500-series-switches/tsd-products-support-series-home.html
  - Disabled: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the device and the PC.
- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
  - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assignment of the port to the native VLAN.

画面ロックおよび自動ロックセットアップ

[画面ロックタイムアウト（Screen Lock Timeout）] の値は、画面がオフになり、画面ロックがアクティブになったときの通常のデバイスアイドルタイムアウトを制御します。変数は、1 ～ 60 分の範囲で構成できます。

[自動ロック（Automatic Lock）] は、ディスプレイが暗くなったり消灯したりする前に、ディスプレイが点灯し続ける時間を制御します。デバイスが Always On モードの場合、デバイスは暗くなります。デバイスが省電力モードになっている場合は、完全にオフになります。省電力モードの詳細については、「電力削減 （12 ページ）」を参照してください。

[自動ロック（Automatic Lock）] の値は、最大 10 分に構成できます。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）]** の順に選択します。

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も小さくなっています	[画面ロックタイムアウト（Screen Lock Timeout）] の値に達すると、画面は最大の明るさのままになります。ロックされた画面が表示されます。
自動ロックの値が画面ロックのタイムアウト値よりも小さくなっています	[自動ロック（Automatic Lock）] の値に達すると、次の 2 つの結果が考えられます。 • デバイスが [常にオン（Always On）] モードの場合、自動ロック値に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（Screen Lock Timeout）] の値に達すると、デバイスがロックされ、淡色表示されたままになります。 • デバイスが省電力モードの場合、[自動ロック（Automatic Lock）] の値に達するとデバイスがロックされ、電源がオフになります。[画面ロックタイムアウト（Screen Lock Timeout）] の値に達すると、それ以上の変更は行われません。
[画面ロック タイムアウト（Screen Lock Timeout）] の値は、[自動ロック（Automatic Lock）] の値と同じです。	この値に達すると、画面は最大の明るさのままになります。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設定

この機能を使用すると、画面のロックを解除するために使用される PIN/パスワードをリセットできます。ユーザーは、 Cisco Unified Communications Manager または構成済みの Google™ アカウントのログイン情報を使用して 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 Communications Manager の管理から、**[ユーザーの管理（User Management）]** > **[エンド ユーザー（End User）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 必要なユーザー情報を入力します。

ステップ 4 **[デバイス情報（ Device Information ）]** ウィンドウで、ユーザー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、ユーザー Cisco Unified Communications Manager 管理者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 エンドユーザー（Standard CCM End Users）]**を選択します。

ステップ 8 **[保存（Save）]**、**[構成の適用（Apply Config）]** の順にクリックします。デバイスが再登録されると、ユーザーはデバイスに構成されます。

設定での管理者パスワードの設定

[共通電話プロファイル（ Common Phone Profile ）] ウィンドウの **[ローカル電話ロック解除パスワード（Local Phone Unlock Password ）]** フィールドにパスワードを設定することで、設定アプリケーションへのアクセスを制限できます。

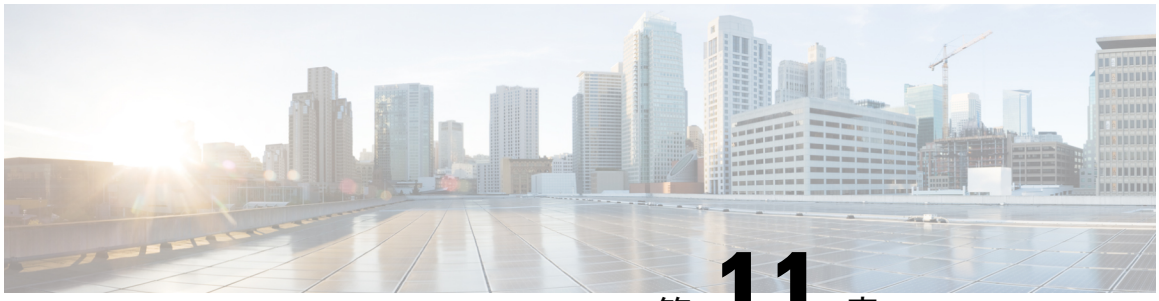
共通の電話プロファイルがデバイスに適用されると、ユーザーは[設定（Settings）]アプリケーションを開くときにパスワードの入力を求められます。サインイン画面には、問題レポートツールを使用して問題を報告するためのリンクがあります。すべての設定ショートカットがデスクトップから削除されます。[設定（Settings）] ショートカットはシステム トレイから削除されますが、ユーザーはコール中にコール統計にアクセスできます。ユーザーはデスクトップの壁紙を変更できません。

手順

ステップ 1 DX デバイスの **[共通の電話プロファイル（Common Phone Profile）]** ウィンドウに移動します。

ステップ 2 **[ローカル電話ロック解除パスワード（Local Phone Unlock Password）]** フィールドで英数字のパスワードを入力します。

ステップ 3 変更を保存して、**[構成の適用（Apply Config）]** をクリックします。



第 11 章

機能とサービス

利用可能なテレフォニー機能

Cisco DX シリーズ デバイスは、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 音声およびビデオ テレフォニー機能など、統合されたコラボレーション アプリケーション スイートを提供します。これらのデバイスは、Google Play のアプリケーションもサポートしています。

Cisco DX シリーズ デバイスをネットワークにインストールし、それらのネットワーク設定を構成し、 Cisco Unified Communications Managerに追加した後、 Cisco Unified Communications Manager 管理を使用してテレフォニー機能を構成し、サービスをセットアップする必要があります。

（注） Cisco Unified Communications Manager には、各種のテレフォニー機能を設定するためのサービス パラメータもいくつかあります。サービス パラメータのアクセスおよび構成に関する詳細は、『*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 パラメータ構成（Service Parameter Configuration）]** ウィンドウで、パラメータ名または疑問符（?）のヘルプボタンをクリックします。

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始める前に、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* システム ガイド』の「「Cisco Unified IP 電話」」の章
- 『*Features and Services Guide for Cisco Unified Communications Manager*』、「「割り込みとプライバシー」」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）]** > **[電話機（Phone）]** の順に選択します。

ステップ 2 構成するデバイスを見つけます。

ステップ 3 [デバイス情報（Device Information）] レイアウト 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) **[System（システム）]** > **[Service Parameters（サービス パラメータ）]** を選択します。
b) 適切なサーバおよびサービスを選択します。
c) [クラスタワイド パラメータ（デバイス - 電話）（Clusterwide Parameters (Device - Phone)）] ペインまでスクロールして、[ビルト イン ブリッジの有効（Builtin Bridge Enable）] を [オン（On）] に設定します。
d) [保存（Save）] を選択します。

すべてのコール

ユーザーはアクティブ コールと保留中のコールのリストを表示できます。このリストは、時系列順にソートされます（古い順）。ユーザーは、着信コールと完了コールのリストを表示することもできます。このリストは、新しいものから古いものの順にソートされます。

プライマリ回線における全コール

プライマリ回線がすべてのコール機能を引き継ぐことを許可します。すべての着信コールはプライマリ回線のコール リストに表示され、プライマリ回線で応答できます。

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。デバイスでヘッドセットの自動応答が有効になっていても、ヘッドセットがデバイスに接続されていない場合、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「「電話番号の設定」」の章を参照してください。

自動ダイヤル

ユーザーは、発信、着信、不在着信を含む [最近の通話履歴（Recent Call History）] で一致する番号を選択できます。コールを発信するには、これらのコール リストのいずれかから番号を選択するか、手動で番号を入力します。

割込み

ユーザー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ます。割り込みによって、コールは会議に切り替えられます。ユーザーと他の参加者は、会議機能にアクセスできます。

（注） [ビルトイン ブリッジ有効化（Built In Bridge Enable）] サービス パラメータが [オフ（Off）] に設定されている場合でも、ユーザーは割り込みを使用できます。ユーザーがデバイスで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で割り込み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*』、「「Cisco Unified IP 電話セットアップ」」の章
- *Cisco Unified Communications Manager* 『システム ガイド』の「「Cisco Unified IP 電話」」章
- 『*Features and Services Guide for Cisco Unified Communications Manager*』、「「割り込みとプライバシー」」章
- 『*Cisco Unified Communications Manager Administration Guide*』、「「機能管理ポリシー」」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、通話記録、ディレクトリ リスト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 および在籍サービス」」の章を参照してください。

Call Forward

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。

追加のコマンド オプションは次のとおりです。

- 対象の番号から発信されたコールを転送ではなく着信させます。
- コール転送ループがコール転送チェーンの最大リンク数を超えないようにします。

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*』、「[電話番号の設定（Directory Number Setup）]」の章を参照してください。
- 『*Cisco Unified Communications Manager* システム ガイド』「「Cisco Unified IP 電話」」の章。

発信回線 ID

発信者回線の識別に使用する完全な外線番号を有効にすることができます。

詳細については、『*Cisco Unified Communications Manager* システム ガイド』の「「Cisco Unified IP 電話」」の章を参照してください。

発信回線 ID の表記

ユーザーは、ケースバイケースで発信者番号を有効または制限できます。

詳細については、『*Cisco Unified Communications Manager* システム ガイド』の「「Cisco Unified IP 電話」」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

ユーザーは、共有デバイス上の Cisco エクステンション モビリティ サービスにログインすることで、共有デバイスから自分のデバイス構成（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。

（注） この機能は、Expressway を介したモバイルおよびリモート アクセスで展開されている DX シリーズ デバイスではサポートされていません。

デバイスにログインするために、ユーザーは管理者が提供するエクステンションモビリティのログイン情報を入力します。これらのログイン情報は、ユーザーの画面ロック PIN とは異なります。

詳細については、『*Features and Services Guide for Cisco Unified Communications Manager*』の「エクステンション モビリティ」の章を参照してください。

拡張モビリティ/マルチユーザー

拡張モビリティ マルチユーザー機能は、拡張モビリティのログイン/ログアウト プロセスを使用します。ユーザーがログインすると、 Cisco Unified Communications Manager サーバがユーザー ログイン情報を認証します。サーバは拡張モビリティ機能と同じメッセージング スキームを使用します。

ユーザー A がデバイスに初めてログインすると、デバイスはリブート サイクルを実行し、デバイス上にユーザー A のユーザー パーティションを作成します。デバイスは、ユーザー A にセットアップウィザードを表示します。ユーザーAは個人用アプリケーションとデータ専用のスペースを取得し、コール アプリケーションはCisco DX シリーズ デバイスと同様に動作します。最初のログイン後、ユーザー A はアプリケーション関連の設定を行います。ユーザー A がこのデバイスからログアウトすると、ユーザー A が次にデバイスにログインするときに、ユーザー設定が保存されます。

ユーザー A がデバイスからログアウトすると、ユーザー B はユーザー B のログイン情報を使用してデバイスにログインできます。ユーザー B は、ユーザー B のパーティションを取得すると、同じエクスペリエンスを実現します。最初のログインでは、セットアップ ウィザードはユーザー B に個人用アプリケーションとデータをセットアップするように求めます。また、ユーザー B には、 Cisco DX シリーズ デバイスで通常どおりに動作するコール アプリケーションもあります。

パーティションは完全に分離されているため、どのユーザーも他のユーザーのデータを見ることはできません。

拡張モビリティ マルチユーザーは、エンタープライズ マルチユーザー アプローチを提供します。システム管理者は、拡張モビリティ マルチユーザー用に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ーにログイン情報を提供します。適切なログイン情報を使用すると、ユーザーは特定のデバイスにのみログインし、自分のアカウントを構成できます。これには、自分のアカウントの削除も含まれます。ユーザーは、同じデバイス上の他のユーザーのアカウントを変更できません。

アルゴリズムによって、特定のデバイスにログインできるユーザーの数が制限されます。デバイスの最大ユーザー数は、各ユーザーの使用状況によって異なります。デバイスのフラッシュ メモリが特定の商を下回ると、最も最近ログインしたユーザーのアカウントが削除され、新しいユーザーがログインするためのスペースが作成されます。したがって、新しいユーザーがスペース不足でログインに失敗することはありません。

Cisco Extension Mobility

DX シリーズ デバイスの Cisco Extension Mobility を構成するには、次の手順に示す順序で手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**[デバイス（Device）] > [デバイス設定（Device Settings）] > [デバイス プロファイル（Device Profile）]** を選択し、**[新規追加（Add New）]** をクリックします。

a) デバイス タイプを入力します。
b) [デバイス プロファイル名（Device Profile Name）] を入力し、**[保存（Save）]** をクリックします。
c) ディレクトリ番号と必要な情報を入力して、**[保存（Save）]** をクリックします。

ステップ 2 **[ユーザー管理（User Management）] > [エンドユーザー（End User）]** を選択し、ユーザーを作成します。

a) [Extension Mobility 利用可能プロファイル（Extension Mobility Available Profiles）] で、ユーザー デバイス プロファイルを選択し、下矢印をクリックします。これにより、選択したサービスが [制御されたプロファイル（Controlled Profiles）] ボックスに配置されます。
b) [保存（Save）] をクリックします。

ステップ 3 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

a) デバイス タイプを選択します。
b) ユーザー ID を選択します。
c) **[電話の設定（Phone Configuration）]** ウィンドウの [製品固有の構成レイアウト（Product Specific Configuration Layout）] 領域の [Extension 情報（Extension Information）] で、**[Extension Mobility の有効化（Enable Extension Mobility）]** をオンにします。
d) **[電話の設定（Phone Configuration）]** ウィンドウの [製品固有の構成レイアウト（Product Specific Configuration Layout）] 領域で、[マルチユーザー（Multi-User）] ドロップダウン リスト ボックスの **[有効（Enabled）]** の値を選択します。

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 フォン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 DX シリーズ デバイスの Cisco Mobility 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 モビリティ」」の章を参照してください。

会議

- ユーザーは複数の相手と同時に会話することができます。そのためには、各参加者に個別にコールを行います。
- 標準（アドホック）会議では、参加者が参加者を追加または削除できます。
- ユーザーが、同一電話回線上にある 2 つ以上のコールに参加し、1 つの会議コールとして接続したうえで、そのコールに留まることができます。

これらの機能を有効にするには、[拡張アドホック会議（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）を使用します。

会議の詳細については、『*Cisco Unified Communications Manager*システム ガイド』の「「会議ブリッジ」」の章を参照してください。

セキュアな会議

セキュアな会議では、セキュアなデバイスがセキュアな会議ブリッジを使用して電話会議を行うことができます。新しい参加者が追加されると、すべての参加者がセキュアなデバイスを使用している限り、[セキュア コール（Secure Call）] 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* システム ガイド』の「「会議ブリッジ」」の章
- 『*Cisco Unified Communications Manager Administration Guide*』、「「会議ブリッジの設定」」の章
- 『*Cisco Unified Communications Manager Security Guide*』

即転送

拡張即時転送を有効にすると、ユーザーはこの機能を使用して、着信コールをボイス メッセージング システムに直接転送できます。

コールをボイスメールに転送する方法の詳細については、「『*Features and Services Guide for Cisco Unified Communications Manager*』」の「「即時転送」」の章を参照して ください。

拡張即時転送の詳細については、『*Cisco Unified Communications Manager* システム ガイド』の「「Cisco Unified IP 電話」」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） DND は 911 コールに影響しません。

次の DND 関連のパラメータは、 Cisco Unified Communications Manager 管理で構成できます。

- [サイレント（Do Not Disturb）]：このチェックボックスを使用すると、デバイスごとにDNDを有効にすることができます。Cisco Unified Communications Manager管理で、**[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）]：DNDがアクティブのときに着信コールに対してデバイスでアラートを発生させる場合、その再生するアラート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「「」サイレント」の章を参照してください。

ゲートウェイ録音

この機能は、コールを録音サーバーに送信するようにMedia Gatewayに指示し、コールモニタリングを改善します。

詳細な情報と手順については、『『*Features and Services Guide for Cisco Unified Communications Manager*』』の「「モニタリングと録音」」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「「保留音」」の章を参照してください。

無視

ユーザーが通知ウィンドウから着信コールを無視できるようにします。

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、ユーザーに対する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*』、「「メッセージ待機設定」」の章
- *Cisco Unified Communications Manager*『システム ガイド』の「「Cisco Unified Communications Manager へのボイス メール接続」」の章

ミュート

デバイスのスピーカー、ハンドセット、ヘッドセットなど、すべての入力デバイスの音声入力をミュートします。

プラス ダイヤル

ユーザーが先頭にプラス **+** 記号を付けて E.164 番号をダイヤルできるようにします。

+ 記号をダイヤルするには、ユーザーは ***** キーを 1 秒以上押し続ける必要があります。これは、オンフックまたはオフフック通話の最初の桁をダイヤルする場合にのみ適用されます。

保護されたコール

2 つのデバイス間のセキュアな（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が示されます。会議コール、共有回線、回線を超えた参加などのいくつかの機能は、保護されたコールが構成されている場合利用できません。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。

着信音の設定

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

詳細については、「『*Cisco Unified Communications Manager Administration Guide*』」の「「電話番号の設定」」の章を参照して ください。

呼出音

ユーザーは、着信コールや新しいボイス メッセージをデバイスで示す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

デバイスが Cisco Unified Communications Manager でセキュア（暗号化され、信頼できる）なものとして構成されている場合、「保護」というステータスを割り当てることができます。その

後、必要に応じて保護されたデバイスは、コールの開始時に通知トーンを再生するように構成できます。

- [保護されたデバイス（）]：Cisco Unified Communications Manager 管理でセキュア デバイスのステータスを保護に変更するには、**[デバイス（Device）]** > **[電話（Phone）]** > **[電話構成（Phone Configuration）]** の **[保護されたデバイス（Protected Device）]** をオンにします。
- [セキュアインディケーショントーンの再生（Play Secure Indication Tone）]：保護されたデバイスで、セキュアまたは非セキュアな通知トーンの再生を有効にするには、[セキュアインディケーショントーンの再生（Play Secure Indication Tone）] を [はい（True）] に設定します。（デフォルトは [いいえ（False）] です。）**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** のCisco Unified Communications Manager 管理のこのオプションを設定します。サーバーおよび Cisco CallManager サービスを選択します。**[サービス パラメータ構成（Service Parameter Configuration）]** ウィンドウで、[機能 - セキュアトーン（Feature - Secure Tone）] 領域内にあるオプションを選択します。（デフォルトは [いいえ（False）] です。）

保護されたデバイスだけで、セキュアまたは非セキュアなインディケーション トーンが再生されます。（保護されていないデバイスにはトーンが聞こえません）。コール中にコール状態全体が変化すると、それに応じて表示音も変化します。その時点で、保護されたデバイスは適切なトーンを再生します。

保護されたデバイスは、このような状況でトーンを再生します。もしくは、再生しません。

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

サービスアビリティ

管理者は、デバイスからデバッグ情報を素早く簡単に収集できます。

この機能は、SSH を使用して各電話にリモートでアクセスします。この機能を使用するには、各電話機の SSH が有効になっている必要があります。

共有回線

複数のデバイスで同じディレクトリ番号を共有したり、ディレクトリ番号を同僚と共有したりできるようにします。

詳細については、『*Cisco Unified Communications Manager*システム ガイド』の「「ディレクトリ番号」」の章を参照してください。

スピードダイヤル

特定の接続先電話番号への短縮ダイヤルを構成できます。

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。

ユーザーは2つのコールを相互に接続できます。ユーザーは、通話を継続することも、通話を継続せずにコールを転送することもできます。

Uniform Resource Identifier ダイヤリング

Uniform Resource Identifier（URI）ダイヤル機能により、ユーザーは英数字の URI アドレスをディレクトリ番号として使用して電話をかけることができます（例：**bob@cisco.com**）。接続先を選択するには、ユーザーが URI アドレスを入力する必要があります。

スクリーンに、URI コールのコール情報が表示されます。コール ログは、電話機の通話履歴および [詳細（Details）] ページにURI コール情報が保存されます。

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。

ビデオのトグル

ユーザーは、ビデオ コール中にビデオのオンとオフを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* システム ガイド』の「「Cisco Unified Communications Manager へのボイス メール接続」」の章

ビジュアル ボイスメールのセットアップ

ビジュアル ボイスメールは、Cisco Unified Communications Manager 管理から、すべてのデバイスまたは個別ユーザーまたはユーザ グループに設定されます。すべてのデバイスにビジュアル ボイスメールを構成する場合は、次の手順を使用します。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**[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、**[標準共通電話プロファイル（Standard Common Phone Profile）]** を選択します。

ステップ 3 **[製品固有の構成レイアウト（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 スタンドアロン構成用に を構成する場合は、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 フェールオーバー構成用に を設定する場合は、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、**[構成の適用（Apply Config）]** をクリックします。

ビジュアル ボイスメールの構成と同期の詳細については、『『*Cisco Unified Communications Manager Administration Guide*』』の「「ボイスメール プロファイルの構成」」の章を参照してください。

特定のユーザーまたはグループ向けのビジュアル ボイスメールの設定

特定のユーザーまたはユーザーのグループにビジュアル ボイスメールを構成する場合は、次の手順を使用します。

手順

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

ステップ 2 検索するユーザーに関連付けるデバイスを選択します。

ステップ 3 **[製品固有の構成レイアウト（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 スタンドアロン構成用に を構成する場合は、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 フェールオーバー構成用に を設定する場合は、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、**[構成の適用（Apply Config）]** をクリックします。

ステップ 5 **[リセット（Reset）]** および **[再起動（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 デバイスでセキュア メッセージを許可するには、Cisco Unified Communications Manager 管理から、**[システム設定（System Settings）]** > **[詳細 API 構成（Advanced API Configuration）]** を選択し、**[CUMI によるセキュアメッセージ録音へのアクセスを許可（ Allow Access to Secure Message Recordings through CUMI）]** と **[CUMI によるメッセージ添付ファイルを許可（Allow Message Attachments through CUMI）]** の両方を有効にします。

ステップ 7 ディレクトリ写真がビジュアル ボイスメールで構成されるように Cisco Unified Communications Manager を構成するには、**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[共通電話プロファイル（Common Phone Profile）]** を選択し、[共通電話プロファイル（CommonPhone Profile）] を選択して、**[会社の写真ディレクトリ（ Company Photo Directory）]** フィールドに組織の写真ディレクトリの URL を入力します。

ビジュアル ボイスメールの構成と同期の詳細については、『『*Cisco Unified Communications Manager Administration Guide*』』の「「ボイスメール プロファイルの構成」」の章を参照してください。

機能ボタン

次の表に、コール制御バーで利用可能な機能や、プログラム可能な機能ボタンとして構成が必要な機能に関する情報を提供します。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、プログラム可能な機能ボタンだけは Cisco Unified Communications Manager の管理ページでの設定が必要です。

表 *19 :* 機能と対応するボタン

機能名	コール制御バー ボタン	プログラム可能な機能ボタン
折り返し		×
Call Forward	X	
すべてのコールの転送		○
コール パーク	×	
コールピックアップ		X
Cisco Mobility		X
会議（追加）	X	

機能名	コール制御バー ボタン	プログラム可能な機能ボタン
転送（Divert）		X
サイレント		×
終了	X	
グループピックアップ		×
保留	×	
ハントグループ		×
インターコム		○
迷惑呼 ID（MCID）		×
Meet Me		×
プライバシー		X
リダイヤル		X
共有（DX70 および DX80 のみ）	×	
スピード ダイヤル		X
動画の停止		X
転送	X	

機能制御ポリシーの設定

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するには、機能制御ポリシー構成でこれらの機能を有効または無効にします。機能制御ポリシー構成で機能を無効にすると、その機能へのユーザー アクセスが制限されます。

手順

ステップ 1 Cisco Unified Communications Manager 管理から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[機能管理ポリシー（Feature Control Policy）]** を選択します。
[機能制御ポリシーのの検索と一覧表示（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）]：機能制御ポリシーの名前を入力します。

- [説明（Description）]：説明を入力します。
- [機能制御（Feature Control）]セクション：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 次の設定に含めて、 Cisco DX シリーズ デバイスにポリシーを適用します。

- [エンタープライズ パラメータ構成（Enterprise Parameters Configuration）]：システム内のすべての Cisco DX シリーズ 個のデバイスに適用されます。
- [共通の電話プロファイル構成（Common Phone Profile Configuration）]：グループ内のすべての Cisco DX シリーズ 個のデバイスに適用されます。
- [電話の構成（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、構成できる機能のリストとデフォルト値を示します。

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（Default value）]
割込み	有効
コールバック	有効
コールピックアップ	[無効（Disabled）]
会議リスト	有効
転送（アラート）	[無効（Disabled）]
即転送(接続済み)	[無効（Disabled）]
不在転送（Forward All）	有効
グループコールピックアップ	[無効（Disabled）]
Meet Me	[無効（Disabled）]
モビリティ	[無効（Disabled）]
他のコールピックアップ	[無効（Disabled）]
パーク	[無効（Disabled）]
リダイヤル	有効
発信者のレポート	[無効（Disabled）]
品質のレポート	[無効（Disabled）]
スピードダイヤル	有効

詳細については、「『*Cisco Unified Communications Manager Administration Guide*』」の「「機能制御ポリシーの設定」」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 電話サービス設定」」の章を参照してください。回線ボタンの構成の詳細については、『『*Cisco Unified Communications Manager Administration Guide*』』の「「Cisco Unified IP Phone 設定」」の章および「「スピードダイアル ボタンの構成」」のセクションを参照してください。

手順

ステップ 1 Cisco Unified Communications Manager 管理から、**[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[電話ボタン テンプレート（Phone Button Template）]** を選択します。

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 テンプレートの構成（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 を使用して新しい電話ボタン テンプレートを作成します。

ステップ 7 **[デバイス（Device）]** > **[電話（Phone）]** を選択して、電話機の **[電話の構成（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、**[リセット（Reset）]** をクリックして変更を実装します。

これで、ユーザーがセルフ ケア ポータルにアクセスできるようになり、デバイスのボタンにサービスが関連付けられました。

製品固有オプションの構成

Cisco Unified Communications Manager Administration では、次のいずれかのウィンドウで、デバイスの製品固有の構成パラメータを設定できます。

- **[エンタープライズ電話の構成（Enterprise Phone Configuration）]** ウィンドウ（**[システム（System）]** > **[エンタープライズ電話の構成（Enterprise Phone Configuration）]**）
- ウィンドウの [製品固有の構成レイアウト（Product Specific Configuration Layout）] の **[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）]**）
- ウィンドウの [製品固有の構成レイアウト（Product Specific Configuration Layout）] の **[デバイス構成（Device 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]**）

パラメータを設定した後、更新する各設定の [共通設定のオーバーライド（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つの構成ウィンドウでパラメータを設定する場合、以下の順序で設定が優先されます。

1. **[デバイス構成（Device 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構成（Enterprise Phone Configuration）]** ウィンドウ

次の表に、[デバイス構成（Device Configuration）] ウィンドウで使用可能な製品固有の設定オプションを示します。[デバイス構成（Device Configuration）] ウィンドウでは使用できない [共通の電話プロファイル（Common Phone Profile）] ウィンドウと [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウで使用できる他の製品固有の構成オプションがありますが、これらの他のオプションはDXシリーズデバイスに影響しない場合があります。

表 *21 : Cisco DX* シリーズ 製品固有の構成オプション

特長	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を無効にします。スピーカーフォン機能を無効に 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 を使用できます。 デフォルト：False

特長	説明
スピーカーフォンおよびヘッドセットの無効化	すべてのスピーカー フォン機能とヘッドセットマイクを無効にします。 デフォルト：False
[USBを無効にする（Disable USB）]	デバイス上の USB ポートを無効にします。 デフォルト：False
[SDIO]	電話の SDIO デバイスが有効であるか、無効であるかを示します。 デフォルト：[無効（Disabled）]
[Bluetooth]	デバイスの Bluetooth サービスが有効であるか、無効であるかを示します。 デフォルト：有効
Bluetooth 連絡先のインポートを許可（Allow Bluetooth Contacts Import）	ユーザーは、Bluetooth デバイスから連絡先と通話履歴をインポートして同期で デフォルト：[有効（Enabled）]
[Bluetooth モバイル ハンズフリー モードを許可（Allow Bluetooth Mobile Handsfree Mode）]	ユーザーがデスク フォンで携帯電話回線を使用できるようにします。 デフォルト：有効
Days Display Not Active	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。 デフォルト：一般的に、米国企業では [土曜日（Saturday）] と [日曜日（Sunday されます。 （注） リストにはすべての曜日が含まれています。バックライトを土曜日と日 にするには、Ctrl キーを押しながら [土曜日（Saturday）] と [日曜日（Su 選択します。
Display On Time	オフ スケジュールにリストされている日にディスプレイが自動的にオンになる ます。 デフォルト：07:30 最大長：5 （注） 24 時間形式で値を入力します。00:00 が一日の始まりで、23:59 が一日の す。

特長	説明
Display On Duration	プログラミングされたスケジュールによって電源がオンになったときに、ラ アクティブになるまでの時間を指定します。 デフォルト：10:30 最大長：5 （注） 最大値は 24 時間です。この値は、時間と分の形式です。たとえば、 1 時間 30 分の表示をアクティブにします。
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設定を有効にすると、コー 時点でディスプレイがオンになります。 デフォルト：有効
[Power Save Plus の有効化（Enable Power Save Plus）]	Power Save Plus 機能を有効にするには、デバイスをスケジュールに従ってオ 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 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の が維持されます。デバイスの他のすべての機能はオフになります。Power Sa を使用すると、[電話をオンにする時刻（Phone On Time）] と [電話をオフにす Off Time）] フィールドで指定した期間にデバイスがオフになります。この期 に、組織の通常営業時間外に指定されます。点灯しているキーを押すと、ラ を完全に復元できます。点灯しているキーを押すと、電話機の電源が再投入 動作する前に Unified CM に再登録されます。このフィールドで日付を選択す の考慮事項を示す通知メッセージが続けて表示されます。Power Save Plus を とによって、この通知で指定された条件に同意したことになります。 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 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 同意したことになります。 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 お客様が負うものとします。 2. Cisco はお客様がモードを選択することに関して一切の責任を負わず、モ することに関するすべての責任はお客様の責任となります。 3. コール、発信、およびその他に対するモードの影響をユーザーに十分通 デフォルト：どの日も選択されていません。

特長	説明
[電話機をオンにする時刻（Phone On Time）]	[Power Save Plusを有効にする（Enable Power Save Plus）] リスト ボックスで選択 付で、デバイスの電源が自動的にオンになる時刻を指定します。24時間形式で します。00:00 は午前 0 時を表します。たとえば、午前 7:00（0700）に電話を自 ンにするには、07:00 と入力します。午後 2:00（1400）に電話をオンにするには 入力します。このフィールドが空白の場合、デバイスは00:00に自動的にオンに デフォルト：0:00 最大長：5
[電話をオフにする時刻（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 クスで選択された日付で、デバイスの電源が自動的にオフになる時刻を指定しま 分の形式で時刻を入力します。このフィールドが空白の場合、デバイスは午前0 に自動的にオフになります。 （注） [電話をオンにする時刻（Phone On Time）] が空白（または 00:00）で、[電 にする時刻（Phone Off Time）] が空白（または 24:00）の場合、デバイス ままになり、EnergyWise によるオーバーライドの送信を許可しない限り Save Plus 機能は事実上無効になります。 デフォルト：24:00 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、デバイスが給電側機器（PSE）に電源オフを要求するまでに スがアイドル状態になっている必要がある時間（分単位）を表します。このフ 値は以下の場合に有効になります。 • デバイスがスケジュール通りに節電プラス モードにあり、ユーザーがキー めに節電プラス モードから解除された場合 • 接続スイッチでデバイスが再びオンになった場合 • [電話をオフにする時刻（Phone Off Time）] になったが、通話中の場合単位 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になっている場合、[電話をオフにする時刻（Phone フィールドで指定された時刻の 10 分前にオーディオ アラートを再生するよう が設定されます。デフォルトでは無効になっています。このチェックボックス るのは、[Power Save Plusを有効にする（Enable Power Save Plus）] リスト ボック 以上が選択されている場合だけです。
[EnergyWise ドメイン（EnergyWise Domain）]	このフィールドは、電話が参加する EnergyWise ドメインを定義します。Energy インは、Power Save Plus 機能のために必要です。[Power Save Plusを有効にする Power Save Plus）] リスト ボックスで日付を選択した場合は、EnergyWise ドメ する必要があります。デフォルトは空白です。 最大長：127

特長	説明
[EnergyWise エンドポイントのセキュリティシークレット（EnergyWise Endpoint Security Secret）]	このフィールドは、EnergyWise ドメイン内で通信に使用されるパスワード定義します。EnergyWise ドメインおよび共有秘密は、Power Save Plus 機能のす。[Power Save Plusを有効にする（Enable Power Save Plus）] リスト ボック択した場合は、EnergyWise ドメインと秘密を指定する必要があります。デフです。 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。いくつかされます。1 つ目に、[Power Save Plusを有効にする（Enable Power Save Plus）で 1 日以上を選択する必要があります。[Power Save Plusを有効にする（Ena Plus）] リストボックスで日付が選択されていない場合、デバイスをオフにの指示は無視されます。2 つ目に、[Unified CMの管理（Unified CM Adminis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ます。たとえば、[ディスプレイをオフにする時刻（Display Off Time）] が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（D フィールドの値は 06:00（午前 6 時）となり、[Power Save Plusを有効にする 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 Time）] で構成された午前 6 時まで有効になります（ユーザーによる介入が仮定した場合）。午前 6 時になると、デバイスがオンになり、[Unified CM の 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があります。さらに、すべてのユーザー操作が有効になり、EnergyWise によの電源がオフにされた後に、ユーザーがキーを押すと、ユーザーの操作の結イスがオンになります。デフォルトでは、オフになっています。
[録音トーン（Recording Tone）]	デバイスで録音トーンを有効にするかどうかを構成するために使用できます デフォルト：無効
[録音トーンのローカル音量（Recording Tone Local Volume）]	ローカルパーティに聞こえる録音トーンの音量設定を構成するために使用で音量設定は、聞き取りに使用される実際のデバイス（ハンドセット、スピーヘッドセット）に関係なく適用されます。音量設定は 0 ～ 100 % の範囲内でがあります。0 % ではトーンなし、100 % では現在の設定と同じ音量になりルト値は 100 % です。
[録音トーンのリモート音量（Recording Tone Remote Volume）]	リモートパーティに聞こえる録音トーンの音量設定を構成するために使用で設定は 0 ～ 100 % の範囲内で指定する必要があります。0 % では -66 dBM または -4 dBM です。デフォルト値は -10 dBM または 50 % です。
録音トーンの長さ	オーディオストリームに録音トーンを挿入する時間をミリ秒単位で示します。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 ファイルの値に設このパラメータの有効な値の範囲は 1 ～ 3000 ミリ秒です。

特長	説明
[G.722およびiSACコーデックをアドバタイズ（Advertise G.722 and iSAC Codecs）]	通話アプリケーションがワイドバンド コーデックを Cisco Unified Communicatio にアドバタイズするかどうかを示します。 コーデックのネゴシエーションでは、次の 2 つの手順が実行されます。 **1.** 通話アプリケーションは、サポートされているコーデックを Cisco Unified Cor Managerにアドバタイズする必要があります。 **2.** Cisco Unified Communications Manager が、通話試行に関連するすべてのデバ 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 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。 [システムデフォルトの使用（Use System Default）] 有効な値は、次のとおりです。 • [システム デフォルト（System Default）]：コール アプリケーションは、エ イズ パラメータで指定された設定と異なります。G.722 および iSAC コー ドバタイズします。 • [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 C Communications Managerにアドバタイズしません。 • 有効：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 Unifie Communications Managerにアドバタイズします。
[ビデオコール（Video Calling）]	有効にすると、デバイスがビデオ コールに参加することを示します。 デフォルト：有効
デバイス UI プロファイル（Device UI Profile）	デバイスのユーザー インターフェイス特性を変更して、基本ビデオ発信者（[シ （Simple）] モード）、または一般コラボレーション ユーザー（[拡張（Enhanc ど、特定のユーザーの役割に合わせて最適化します。 デフォルト：シンプル（Simple）

特長	説明
Wifi	デバイス上の Wi-Fi が有効であるか、無効であるかを示します。 （注） [エンタープライズ（Enterprise）] および [共通（Common）] 設定では メータがデフォルト値（[有効（Enabled）]）に設定され、**[共通設定の イド（ Override Common Settings ）]** チェックボックスがオンになっ （注） [デバイス（Device）] 設定では、Wifi パラメータはデフォルト値（[有 （Enabled）]）のままですが、**[共通設定のオーバーライド（ Overrid Settings ）]** チェックボックスはオンになっていません。 ヒント 企業および共通レベルの展開環境のデフォルト設定が [無効（Disabled） すべてのデバイスに対して Wifi のデフォルトを [無効（Disabled）] に が企業ポリシーである場合を除き、Wifi パラメータを [有効（Enabled てデバイスの新しい共通電話プロファイルを作成することをお勧めし デフォルト：有効
[PC ポート（PC Port）]	PC ポートが有効か無効かを示します。 デフォルト：[有効（Enabled）]
[PC ポートへのスパン（Span to PC Port）]	デバイスで 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 （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や、 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 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** を選択します。この機能を使用するには、[PC の音声 VLAN へのアク VLAN Access）] を有効にする必要があります。 デフォルト：[無効（Disabled）]
[PC の音声 VLAN へのアクセス（PC Voice VLAN Access）]	PC ポートに接続されたデバイスに、ボイス VLAN へのアクセスを許可する します。 （注） ボイス VLAN アクセスを無効にすると、接続された PC はボイス VL タの送受信ができなくなります。また、デバイスによって送受信され PC で受信することもできなくなります。 デフォルト：[有効（Enabled）]
[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構成を許可します デフォルト：[無効（Disabled）]
[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構成を許可 は、デバイス上での手動設定よりも優先されます。 デフォルト：[無効（Disabled）]

特長	説明
[Unified CM 接続障害の検出（Detect Unified CM Connection Failure）]	このフィールドでは、バックアップ Unified CM/SRST へのデバイスのフェール発生する前の最初のステップである、Cisco Unified Communications Manager（U 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（標準のシステム レートで Unified CM 接続エラーの検出を実行）または [遅延（標準より約 4 倍遅いレートで Unified CM 接続エラーの検出を実行）です。Un 続エラーの高速認識のためには、[標準（Normal）] を選択します。接続を再確うにするためにフェールオーバーを少し遅らせる場合は、[Delayed] を選択しま（Normal）] と [遅延（Delayed）] の接続エラー検出の正確な時間の差は、常に 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のみ適用され デフォルト：[標準（Normal）]
[無償 ARP（Gratuitous ARP）]	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 （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 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 す。 デフォルト：無効
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。 **Warning** デバイスが Cisco 以外のスイッチに接続されている場合にのみ、ネットワ トで CDP を無効にします。詳細については、『*Cisco Unified Communicatio Administration Guide*』を参照してください。 デフォルト：有効
Cisco Discovery Protocol（CDP）：PC Port	PC ポートで CDP がサポートされているかどうかを示します。 デフォルト：有効
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 にできます。 デフォルト：有効
Link Layer Discovery Protocol（LLDP）：PC Port	管理者は、PC ポート上で Link Layer Discovery Protocol（LLDP）を有効または無 ます。 デフォルト：[有効（Enabled）]

特長	説明
[LLDP アセット ID（LLDP Asset ID）]	管理者は、Link Layer Discovery Protocol 用のアセット ID を設定できます。 最大長：32
[LLDP 電源優先度（LLDP Power Priority）]	管理者は、Link Layer Discovery Protocol 用の電源優先度を設定できます。 デフォルト：[不明（Unknown）]
[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。 （注） [電力ネゴシエーション（Power Negotiation）] 機能は、電力ネゴシエ 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。 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 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。 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 ポートを同じ速度とデュプレックスに同期する します。自動ネゴシエーション用に設定されているポートのみが速度を変更 デフォルト：無効
802.1x 認証	802.1x 認証機能のステータスを指定します。オプション • [有効（Enabled）]：デバイスは、802.1X認証を使用してネットワークア します。 • [無効（Disabled）]：デフォルト設定では、デバイスは CDP を使用して ネットワークアクセスを取得します。 デフォルト：ユーザー制御
FIPS Mode	このパラメータは、デバイスの連邦情報処理標準（FIPS）モードを設定しま ションが有効な場合、デバイスは FIPS 140-2 レベル 1 準拠のデバイスです。 デフォルトで、ディセーブルになっています。
[常に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 Com Manager の構成済みの VPN プロファイルで接続を確立するかどうかを示し デフォルト：[いいえ（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 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 場合、ユーザーのVPNパスワードはメモリに格納され、以降の接続で自動的 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 効の場合、ユーザーのVPNパスワードはデバイスに保存され、再起動時も保 デフォルト：[いいえ（False）]

特長	説明
[ユーザ定義VPNプロファイルの許可（Allow User-Defined VPN Profiles）]	ユーザーは AnyConnect VPN クライアントを使用して VPN プロファイルを作成うかを制御します。無効にすると、ユーザは VPN プロファイルを作成できませ デフォルト：[はい（True）]
[スクリーンロック必須（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 • ユーザー制御。 • [暗証番号（PIN）]：数字のパスワードで、少なくとも 4 桁の長さが必要で • [パスワード（Password）]：英数字のパスワードは、少なくとも 4 つの英数れ、そのうち 1 つは数字以外の文字、1つは大文字である必要があります デフォルト：[暗証番号（PIN）]
最大スクリーン ロック タイムアウト	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す。 デフォルト：600 最小値：15 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する（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 デフォルト：[はい（True）] （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、のタイムアウトに関連するすべてのサードパーティ製デバイス管理ポリきされます。
[オーディオコール中にデバイスのロック（Lock Device During Audio Call）]	デバイスが充電中状態で、アクティブなボイス メールが進行中の場合、管理者リーン ロック暗証番号の強制タイマーをオーバーライドして、オーディオコーをアクティブなままにすることができます。スクリーン ロック タイマーは、オコールが完了し、タイマーの時間を超過した後で有効になります。 デフォルト：[無効（Disabled）]
[Kerberos サーバ（Kerberos Server）]	Web プロキシ Kerberos の認証サーバ。 最大長：256

特長	説明
[Kerberosレルム（Kerberos Realm）]	Web プロキシ Kerberos の認証 realm。 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、ア ロードとアップグレードを取得することを示します。 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 最大長：256
ピア ファームウェア共有	サブネット内の単一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 に配布できるようにするために、ピアツーピア イメージ配布を有効または無 デフォルト：[有効（Enabled）]
[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 デフォルト：リモート システムの IP アドレス 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。 デフォルト：プリセット（Preset）
Web アクセス	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 うかを示します。 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。 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 デフォルト：無効
Android Debug Bridge（ADB）	デバイスの ADB を有効または無効にします [有効（Enabled）]、[無効（Disabled）]、または [ユーザー制御（User Contro できます。 デフォルト：無効
マルチユーザ（Multi-User）	マルチユーザーをデバイスで有効にするか、無効にするかを示します。 デフォルト：無効

特長	説明
[不明な提供元からのアプリケーションの許可（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 Se （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 から、ユーザーが Android アプリケーションをデバイス上にインストールでき を制御します。 [有効（Enabled）]、[無効（Disabled）]、または [ユーザー制御（User Controlled できます。 デフォルト：無効
Google Play からのアプリケーションを許可	Google からユーザーが Android アプリケーションをインストールできるかどう ます。 （注） Google Play にある一部のアプリケーションには、GPS や背面カメラなど DX シリーズ デバイスでは使用できないハードウェア要件がある場合があ 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 を保証できません。 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 ケーション クライアントが有効な場合、ユーザーは Cisco Unified Communicatio 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。 デフォルト：False
[企業写真ディレクトリ（Company Photo Directory）]	デバイスがユーザーをクエリし、そのユーザーに関連付けられている画像を取 ができる URL を指定します。 例：http://www.cisco.com/dir/photo/zoom/%%uid%%。uid は従業員のユーザー ID デフォルト：写真ディレクトリ URL 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。 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 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。 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 最大長：256
プレゼンスおよびチャットサーバ(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。 デフォルト：プライマリ プレゼンス サーバの IP アドレス 最大長：256

特長	説明
[プレゼンスおよびチャットサーバタイプ（Presence and Chat Server Type）]	デバイスが使用するセカンダリ プレゼンスおよび IM サーバのタイプを指定 Cisco Unified Presence または Cisco WebEx Connect に設定できます。 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 Webe で使用されるエンタープライズ ドメイン。 デフォルト：空のフィールド 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 最大長：256
Expressway ログイン用ユーザ クレデンシャル パーシステント	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と ます。 デフォルト：[無効（Disabled）]
[カスタマー サポートのアップロード URL（Customer support upload URL）]	これは、ユーザーがエンドポイントで「問題報告ツール」から問題報告フ きるサーバ アドレスを設定します。 最大長：256
クラッシュ レポートの自動アップロード	このエンドポイントからクラッシュ レポートを自動的にアップロードするに を有効にします デフォルト：無効
代替電話帳サーバのタイプ	デフォルトで、エンドポイントは登録先の UCM 上の UDS サーバーを使用し 電話帳サーバーの使用を希望する場合は、このパラメータを代替電話帳のア 合わせて、エンドポイントのデフォルト設定をオーバーライドします。UDS 帳タイプを UDS として設定します。 デフォルト：UDS
代替電話帳サーバのアドレス	デフォルトで、エンドポイントは登録先の UCM 上の UDS サーバを使用しま 話帳サーバの使用を希望する場合は、このパラメータを代替電話帳のタイプ て、エンドポイントのデフォルト設定をオーバーライドします。フィールドに バの完全な URL が必要です。UDS サーバ URL の例：https://uds-host-name:8443 最大長：256

（注） 追加の構成の詳細については、『*Cisco DX Series Wireless LAN Deployment Guide*』 を参照してください。

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、高解像度のマルチタッチ カラー LCD と内蔵カメラによるビデオ通話をサポートしています。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）] に設定されている場合、[ビデオの自動送信（Auto Transmit Video）] 設定はグレー表示されます。**[製品固有の構成レイアウト（Product Specific Configuration Layout）]** ウィンドウでビデオ コールが無効になっている場合、[コール設定（Call settings）] メニューのすべてのビデオ設定はグレー表示されます。

表 *22*: ビデオ送信の解像度と機能

ビデオタイプ	ビデオ解像度	FPS	ビデオ ビット レート範囲（帯域幅）	DX650 外部カメラのサポート
240p	432 x 240	15	64 ～ 149 kbps	はい。ただし、Logicool C930e は 424 X 240 のビデオ解像度を使用します。
240p	432 x 240	30	150 ～ 299 kbps	はい。ただし、Logicool C930e は 424 X 240 のビデオ解像度を使用します。
360p	640 x 360	30	300 ～ 599 kbps	はい
480p	848 X 480	30	600 ～ 799 kbps	はい。ただし、Logicool C920-C は 864 x 480 のビデオ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、これらの解像度の一部（600pなど）をサポートしておらず、外部カメラが動作できる最小ビットレートは 64 kbps です。

（注） Cisco DX650 が Logicool C920-C Web カメラを使用しているコール中にあり、リモート デバイスがパケット化モード 0 のみをサポートしている場合、最大送信解像度は 640x360 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 1920x1080 です。

（注） Cisco DX シリーズ デバイスの VGA を超える最適な解像度は w360p です。 400 kbps ～ 999 kbps 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設定

インスタントメッセージングとプレゼンスを使用すると、ユーザーはいつでも、どこでも、どのデバイスでも通信できます。Cisco DX シリーズ デバイスは、Cisco Unified Presence または Webex バックエンド サーバのいずれかで Jabber IM をサポートします。セキュリティ上の理由から、すべてのクラウドベースのインスタント メッセージングとプレゼンス 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 **[製品固有の構成（Product Specific Configuration）]** ウィンドウで、デバイス、グループ、またはエンタープライズ レベルで構成します。プレゼンスおよびIMサーバ（プライマリ）およびプレゼンスおよびIM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、プレゼンスおよびIMサーバのタイプを指定します。

アプリケーションの設定

ユーザー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および拡張できます。アプリケーションは Google Play からダウンロードできます。Cisco Unified Communications Manager 管理では、（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 [製品固有の構成レイアウト（Product Specific Configuration Layout）] 領域で）次のパラメータを構成することで、アプリケーションにアクセスできます。

- [不明なソースからのアプリケーションを許可（Allow Applications from Unknown Sources）]：ユーザーが Google Play 以外のソースから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。

- [Google Play からのアプリケーションを許可（Allow Applications from Google Play）]：ユーザーが Google Play から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。
- [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）]：管理者が Cisco Unified Communications Manager からアプリケーションをプッシュする機能を制御します。

  UCM アプリケーションは、 Cisco Unified Communications Manager で作成された Android アプリケーションを登録または登録解除するため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 Android アプリケーションをサブスクライブまたはサブスクライブ解除するのと同じ機能を提供しますが、デバイスからこれを行う利便性が追加されます。

[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）]

手順

ステップ 1 デバイスの **[デバイス構成（Device Configuration）]** ウィンドウの [製品固有の構成レイアウト（Product Specific Configuration Layout）] 部分で、**[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。

このアクションにより、デバイスに UCM アプリケーション クライアントがインストールされます。

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た後、デバイス ユーザーは、UCM アプリケーション クライアントにログインすることで、 Cisco Unified Communications Manager で作成されたアプリケーションを登録または登録解除できます。

エンドユーザーを作成して UCM アプリにログイン

管理者は、エンドユーザーを作成し、エンドユーザーをデバイスに関連付け、エンドユーザーをデバイス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 エンドユーザーを作成します。（Cisco Unified Communications Manager 管理で、**[ユーザー管理（User Management）]** > **[エンドユーザー（End User）]** を選択して新しいエンドユーザーを作成します）。

ステップ 2 デバイスをエンドユーザーに関連付けて、デバイスがエンドユーザーの [管理対象デバイス（Controlled Devices）] の下に表示されるようにします。

ステップ 3 標準 CCM エンドユーザー権限をエンドユーザーに割り当てます。

ステップ 4 デバイスの **[デバイス構成（Device Configuration）]** ウィンドウで、このエンドユーザを **[所有者ユーザー ID（Owner User ID）]** フィールドに割り当てます。

UCM アプリでユーザーの登録

デバイス ユーザーは、デバイス上の UCM アプリを使用して、 Cisco Unified Communications Manager で作成されたアプリケーションを登録または登録解除します。

手順

ステップ 1 エンドユーザーのログイン情報を使用して、デバイスの UCM アプリケーションにログインします。

ログインに成功すると、 Cisco Unified Communications Manager で作成されたすべての Android アプリケーションが UCM アプリケーションに表示されます。

ステップ 2 アプリケーションを登録するには、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。

このアクションにより、デバイスへのアプリケーションのダウンロードとインストールがトリガされます。

（注） 一部のアプリケーションは、詳細情報をユーザーに提示します。ボックスをオンにするか、アプリケーションを選択すると、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に登録するには、2番目の画面のチェックボックスをオンにして、**[戻る（Back）]** をタップします。このアクションにより、インストールがトリガされます。

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にあるチェックボックスをオフにします。

Cisco Unified Communications Manager を介して Android APK ファイルをプッシュする

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サービスとして構成し、次にデバイスをサービスに登録します。

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 Communications Manager 管理で Android サービスを追加します。

ステップ 3 デバイスを Android サービスに登録します。

Cisco Unified Communications Manager 管理で Android サービスを追加する

Cisco Unified Communications Manager 管理で Android サービスを追加するには、次の手順を実行します。

始める前に

この手順は、APK から AndroidManifest ファイルを抽出した後に使用します。

手順

ステップ 1 Cisco Unified Communications Manager 管理で、**[デバイス（Device）]** > **[デバイス設定（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 から抽出した 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 このウィンドウの他のフィールドはオプションです。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 電話サービスへのデバイスの登録

始める前に

デバイスをその電話サービスに登録する前に、 Cisco Unified Communications Manager の管理で Android 電話サービスを追加する必要があります。

手順

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

ステップ 2 表示される **[電話の検索と一覧表示（ Find and List Phone ）]** ウィンドウで、Android 電話サービスに登録するデバイスを検索します。

ステップ 3 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 デバイスの**[電話構成（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。

<device name> ウィンドウに登録された Cisco IP 電話サービスが開きます。

ステップ 5 デバイスの [登録済み Cisco IP 電話サービス（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 ボックスを使用して、作成したサービスを選択します。

このアクションにより、指定したサービスへのデバイスのサブスクリプションがトリガされます。

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 12 章

カスタマイズ（Customization）

ワイドバンド コーデック設定

デフォルトでは、G.722 コーデックが Cisco DX シリーズ デバイスに対して有効になっています。Cisco Unified Communications Manager が G.722 を使用するように構成されており、通話先が G.722 エンドポイントをサポートしている場合、G.711 の代わりに G.722 コーデックを使用してコールを接続します。

この状態は、ユーザがワイドバンド ヘッドセットまたはワイドバンド ハンドセットを有効にしているかどうかを問わず発生します。ヘッドセットまたはハンドセットが有効になっている場合、ユーザはコール中の音声の感度がより高く感じられます。感度が高いということは、音声の明瞭度がより向上することを意味しますが、遠くの相手には、書類がガサガサする音や近くの会話など、より多くの背景ノイズが聞こえることを意味します。 ワイドバンドヘッドセットまたはハンドセットがない場合でも、G.722の高い感度を煩わしく感じるユーザーもいます。他のユーザーは、G.722 の追加感度が煩わしく感じる可能性があります。

[G.722 コーデックのアドバタイズ（Advertise G.722 Codec）] サービス パラメータは、パラメータが構成されている Cisco Unified Communications Manager 管理によって、この Cisco Unified Communications Manager サーバまたは特定の電話機に登録されたすべてのデバイスに対してワイドバンドがサポートされているかどうかに影響します。

- [G.722 コーデックのアドバタイズ（Advertise G.722 Codec）] フィールド： Cisco Unified Communications Manager 管理から、**[システム（System）]**>**[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。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 G.722 を Cisco Unified Communications Manager] にアドバタイズすることを意味します。コールにおいて通話元および通話先の電話機が機能

セットで G.722 をサポートしている場合、Cisco Unified Communications Manager は可能な限りコールにこのコーデックを選択します。

- 特定のデバイスが G.722 コーデックをアドバタイズします。 Cisco Unified Communications Manager 管理から、**[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が指定する値を使用します。デバイスごとにこれを上書きする場合は、**[電話の構成（Phone Configuration）]** ウィンドウの [製品固有の構成（Product Specific Configuration）] 領域の [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。

操作モード

Cisco DX シリーズ デバイスはさまざまな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（Simple Mode）] です。

次の表に、各モードでユーザー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
コール アプリケーション	はい	はい	はい
ロック画面	いいえ	○	はい
ネットワークの設定	いいえ	○	はい
ホーム画面	いいえ	○	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
ビジュアル ボイスメール	いいえ	○	はい
Cisco User Data Service	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
最近使用したアプリケーションのリスト	いいえ	○	はい
外部ストレージ デバイス	いいえ	いいえ	○
Jabber IM	いいえ	いいえ	○

機能	パブリック モード	簡易モード	拡張モード
Android アプリケーション	いいえ	いいえ	○

オペレーティング モードの設定

始める前に

シンプル 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お勧めします。簡易モードまたはパブリック モードでは電子メールアプリケーションが無効になるため、ユーザーは問題レポート ツールを使用して管理者にログを電子メールで送信することはできません。ログは、有用性 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、『*Cisco DX* シリーズのリリース ノート』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構成（ 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 **[電話の構成（ Phone Configuration ）]** ウィンドウで、**[デバイス UI プロファイル（ Device UI Profile ）]** を目的のモードに設定します。

ステップ 3 **[共通設定のオーバーライド（Override Common Settings）]** をオンにします。
拡張モードから公共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。公共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、デバイスも再起動します。公共モードと簡易モードを切り替えても、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 Communications Manager 管理（Cisco Unified Communications Manager Administration）] ページから、自分またはユーザーがデバイスのデフォルトの壁紙を設定できるかどうかを制御できます。DX シリーズ デバイスのタイプごとに、5 つのホーム画面にまたがる異なるサイズの壁紙画像が必要です。

壁紙コントロールの割り当て

デフォルトでは、ユーザーは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）]**>**[デバイス設定（Device Settings）]**>**[共通電話のプロファイル（Common Phone Profile）]** に移動します。

ステップ 2 壁紙の制御を管理者に制限するには、**[エンドユーザーが電話の背景イメージ設定にアクセスできるようにする（Enable End User Access to Phone Background Image Settings）]** をオフにします。

デフォルトの壁紙指定（DX70 および DX80）

Cisco DX70 および DX80 の壁紙には、2985x1080 の画像解像度を推奨します。壁紙は 5 つの画面にまたがって表示され、各画面の幅は 1920px 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 Desktops/2985x1080x24 フォルダに壁紙画像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 Communications Manager 管理の [DX70 および DX80 共通電話プロファイル（DX70 and DX80Common Phone Profile）] に移動し、以下を変更します。

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 Image）]** に壁紙の画像ファイル名を入力します。
c) **[共通設定のオーバーライド（Override Common Settings）]** をオンにします。

ステップ 4 構成を保存し、共通の電話プロファイルに適用します。

ステップ 5 電話デバイスのページで、壁紙をロードするデバイスに設定を適用します。

エンドポイントの大規模なネットワークがある場合は、すべてのデバイスに構成を適用するか、Cisco Unified Communications Manager サーバを再起動して、すべてのエンドポイントがイメージを取得するようにします。

デフォルトの壁紙指定（DX650）

Cisco DX650 の壁紙には、1569x600 の画像解像度を推奨します。壁紙は 5 つの画面にまたがり、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 Desktops/1569x600x24 フォルダに壁紙画像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 Communications Manager Administration の [DX650 共通電話プロファイル（DX650 Common Phone Profile）] に移動し、以下を変更します。

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 Image）]** に壁紙の画像ファイル名を入力します。

c) **[共通設定のオーバーライド（Override Common Settings）]** をオンにします。

ステップ 4 共通の電話プロファイルに構成を保存して適用します。

ステップ 5 電話デバイスのページで、壁紙をロードするデバイスに設定を適用します。

エンドポイントの大規模なネットワークがある場合は、すべてのデバイスに構成を適用するか、すべてのエンドポイントがイメージを取得するように Cisco Unified Communications Manager サーバーを再起動します。

SSH アクセス

ポート 22 を介した SSH デーモンへのアクセスを有効または無効にできます。ポート 22 を開いたままにしておくと、デバイスはサービス拒否（DoS）攻撃を受けやすい状態になります。デフォルトでは、SSH デーモンは無効になっています。

SSH アクセスでは、2 セットのクレデンシャルを順番に入力する必要があります。

1. Cisco Unified Communications Manager 構成の [セキュア シェル情報（Secure Shell Information）] セクションで指定されたセキュア シェル ユーザーとセキュア シェル パスワード
2. デバッグ ユーザー 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構成（**[デバイス（Device）]**>**[デバイス設定（Device Settings）]**>**[共通電話プロファイル（Common Phone Profile）]**）
- 電話構成（**[デバイス（Device）]** > **[電話ウィンドウ（Phone windows）]**）

Unified Communications Manager エンドポイント ロケール インストーラ

デフォルトでは、デバイスは英語（米国）のロケール用に設定されます。それ以外のロケールで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 エンドポイント ロケール インストーラを、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ー インターフェイス用の最新版の翻訳テキストおよび国別の電話トーンをシステムにインストールし、デバイスで使用できるようにします。

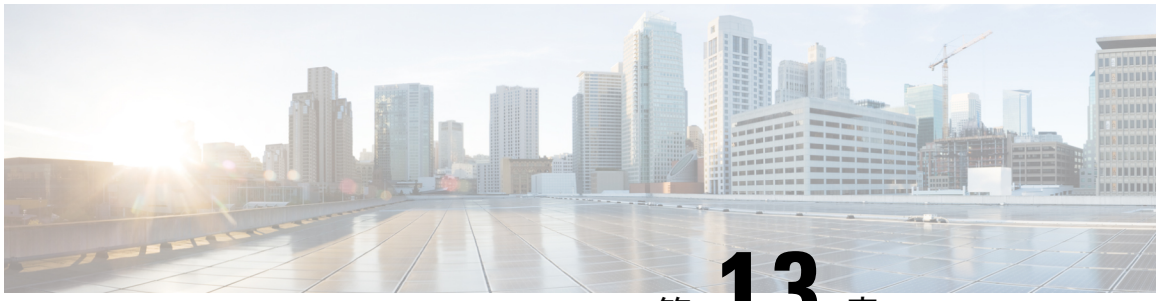
特定のリリースに必要なロケール インストーラにアクセスするには、http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245 にアクセスし、お使いのデバイス モデルに移動して、Unified Communications Manager エンドポイント ロケール インストーラのリンクを選択します。

詳細については、『*Cisco Unified Communications* オペレーティング システム管理ガイド』の「「ローカル インストーラ」」の章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 コードを表す「「+」」記号が表示されることがあります。電話システムの設定によっては、「「+」」記号ではなく正しい国際ダイヤル コードが表示される場合があります。国際ダイヤル コードが表示されない場合は、必要に応じて、「「+」」記号を通話場所の国際エスケープ コードに手動で置き換えて番号を編集した後にダイヤルします。また、コール ログやディレクトリ エントリには受信コールの完全な国際電話番号が表示され、電話機のディスプレイには国際コード（国番号）が省略された国内用の短い番号が表示される場合もあります。



第 13 章

メンテナンス

デバイスのリセット

デバイスのリセットは、さまざまな構成およびセキュリティ設定をリセットまたは復元する方法、またはデバイスでエラーが発生した場合にデバイスを回復する方法を提供します。

次の手順では、実行できるリセットのタイプについて説明します。

（注） 3つのリセット方法はすべて、すべてのユーザーデータが削除され、デバイスから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、デバイスで次のことが発生します。

- [ユーザー構成設定（User configuration settings）]：デフォルト値にリセットします。
- [ネットワーク構成設定（Network configuration settings）]：デフォルト値にリセットします。
- [コール履歴（Call histories）]：消去されます。
- [ロケール情報（Locale information）]：デフォルト値にリセットします。

- [セキュリティ設定（Security settings）]：デフォルト値にリセットします。これには、CTL ファイルの削除と、[802.1x デバイス認証（802.1x Device Authentication）] パラメータの [無効（Disabled）] への変更が含まれます。

（注） 初期状態にリセットする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

これらの操作のいずれかを使用して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 管理者 Web GUI
  1. デバイス構成ウィンドウの [製品固有の構成レイアウト（Product Specific Configuration Layout）] 領域で、**[デバイスのワイプ（Wipe Device）]** を有効にします。
  2. 管理 GUI から [構成の適用（Apply Config）]、[再起動（Restart）]、または [リセット（Reset）] コマンドを発行して、ワイプをデバイスにプッシュします。

- 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&リセット（Backup & reset）]** > **[初期状態にリセット（Factory data reset）]** を選択します。

     （注） デバイスで PIN またはパスワードが構成されている場合は、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：キーを押すシーケンス

  この方法は、デバイスが PIN またはパスワードロックで保護されていて、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。

  次の手順に従い、Cisco DX70 をリセットして起動します。

  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（Mute）]** ボタンが赤色に点灯するまで、**[音量アップ（Volume Up）]** ボタンを押し続けます。
  3. **[音量アップ（Volume Up）]** ボタンを放し、**[ミュート（Mute）]** ボタンを 3 秒間押し続けます。

  次の手順に従い、Cisco DX80 をリセットして起動します。

  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。

次の手順に従い、Cisco DX650 をリセットして起動します。

1. **[#]** キーを押したままにして、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）が赤色に 1 回点滅してから点灯したままになったら、**[#]** 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 Cisco Unified Communications Manager から構成変更を受信し、アップグレードをロードします。次のプロトコルは、デバイスが変更要求を処理する方法を記述します。

- [リセット（Reset）] は、アクティブ コールが終了するまで待機します。
- デバイスの画面がオンになっている場合は、変更と再起動の必要性について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 ボックスには、次のオプションがあります。
  - [再起動（Restart）] : ポップアップ ダイアログ ボックスを閉じ、デバイスを再起動します（デフォルト アクション）。
  - [スヌーズ（Snooze）] : ポップアップ ダイアログボックスを 1 時間閉じます。ユーザーは、最大 24 時間スヌーズするようにデバイスを設定できます。スヌーズ後はデバイスが再起動します。

（注） ポップアップ ダイアログボックスには、60 秒のカウントダウン タイマーがあります。ユーザーが操作しない場合、デフォルトのアクションが開始されます。

ユーザーがデバイスをスヌーズに設定すると、ユーザーは通知リストからいつでも手動でデバイスをリセットできます。

- デバイスの画面がオフの場合、アクティブな音声は要求を待機し続けます。

リモート ロック

この機能を使用すると、 Cisco Unified Communications Managerの [デバイス構成（Device Configuration）] ウィンドウからデバイスをロックできます。

デバイスがリモート ロック要求を受信すると、デバイスはアクティブ コールをただちに終了し、デバイスがロックされます。要求時にデバイスがシステムに登録されていない場合、デバイスは次回システムに登録されたときにロックされます。

（注） リモート ロック要求を発行した後は、要求をキャンセルできません。

リモート ロック デバイス

手順

ステップ 1 デバイスの **[電話の構成（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）]** をクリックして、ロックの確認メッセージを受け入れます。

ロック ステータスは、デバイスの **[電話の構成（ Phone Configuration ）]** ウィンドウの [デバイス ロック/ワイプ ステータス（Device Lock/Wipe Status）] セクションで確認できます。

リモートワイプ

この機能を使用すると、 Cisco Unified Communications Manager の [デバイス構成（Device Configuration）] ウィンドウからデバイスのデータを消去できます。

デバイスは、リモートワイプ要求を受信すると、アクティブなコールをただちに終了し、デバイスデータを消去します。要求時にデバイスがシステムに登録されていない場合、データは次にデバイスがシステムに登録されたときに消去されます。

（注） リモート ワイプ要求を発行した後は、要求をキャンセルできません。

リモート ワイプ デバイス

手順

ステップ 1 デバイスの **[電話の構成（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）]** をクリックして、ワイプの確認メッセージを受け入れます。

ワイプステータスは、デバイスの **[電話の設定（Phone Configuration）]** ウィンドウの [デバイス ロック/ワイプ ステータス（Device Lock/Wipe Status）] セクションで確認できます。

Cisco DX70 のブート代用イメージ

手順

ステップ 1 デバイスをオンにして、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（Mute）]** ボタンが赤色に点灯するまで、**[音量ダウン（Volume Down）]** ボタンを押し続けます。

ステップ 3 **[音量ダウン（Volume Down）]** ボタンを放し、**[ミュート（Mute）]** ボタンを 3 秒間押し続けます。

Cisco DX80 のブート代用イメージ

手順

ステップ 1 **[音量ダウン（Volume Down）]** 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（Volume Down）]** ボタンを放し、**[ミュート（Mute）]** ボタンを押します。

Cisco DX650 のブート代用イメージ

手順

ステップ 1 デバイスの電源をオフにするには、電源を切断します。

ステップ 2 ***** キーを押したままにして、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、***** キーを離します。
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後にデータの非互換性が存在する場合に、工場出荷時設定へのリセットが不要になります。

（注） ファームウェアの以前のリリースにダウングレードすると、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する場合は、データを失わず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し、デバイスがデータを移行できない場合は、アラームが表示されます。ユーザー データをバックアップするか、デバイスのリモート ワイプを実行するようにユーザーに指示します。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設定へのリセットを検出し、移行、ダウングレード、およびリブートを上書きします。デバイスが再起動すると、ダウングレードされたファームウェアがロードされます。

ログ プロファイルのデバッグ

デバイスまたはデバイス グループのデバッグ ログ プロファイルをリモートでオンにできます。

通話処理にデバッグ ログ プロファイルを設定

手順

ステップ 1 個別デバイスの構成ウィンドウまたは [共通の電話プロファイル（Common Phone Profile）] ウィンドウの [製品固有構成レイアウト（Product Specific Configuration Layout）] 領域に移動します。

ステップ 2 **[ログ 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 デバッグ ロギングが有効になっていることが通知領域に表示されます。ユーザーはメッセージを展開して詳細を確認できますが、通知を閉じることはできません。

デバッグ ログ プロファイルをデフォルトにリセット

手順

ステップ 1 個別デバイスの構成ウィンドウまたは [共通の電話プロファイル（Common Phone Profile）] ウィンドウの [製品固有構成レイアウト（Product Specific Configuration Layout）] 領域に移動します。

ステップ 2 **[ログ 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 変更を適用して保存します。

ステップ 4 現在のデバッグ レベルを維持するには、**[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。

ユーザー サポート

デバイスで機能の一部を適切に使用するには、ユーザーはあなた、または所属のネットワーク チームから情報を受け取るか、サポートのためにあなたに連絡できるようにする必要があります。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ーに提供しておく必要があります。

Cisco では、社内サポート サイトに Web ページを作成して、デバイスに関する重要な情報をユーザーに提供することをお勧めします。

問題レポート ツール

ユーザが問題レポートを送信する際は、問題レポート ツールを使用します。

（注） 問題のトラブルシューティングを行う場合、Cisco TAC は問題レポート ツールのログを必要とします。電話機を再起動すると、ログは消去されます。電話機を再起動する前に、ログを収集します。

ユーザが問題レポートを発行するには、問題レポート ツールにアクセスし、問題が発生した日時と、問題の詳細を記入します。

Cisco Unified Communications Manager の [カスタマーサポートアップロードURL（Customer Support Upload URL）] フィールドにサーバ アドレスを追加する必要があります。

カスタマー サポート アップロード URL の設定

サーバでアップロード スクリプトを使用して PRT ファイルを受信する必要があります。PRT は、HTTP POST メカニズムを使用し、次のパラメータをアップロード（マルチパート MIME エンコーディングを使用）に含めます。

- devicename（例：「SEP001122334455」）
- serialno（例：「FCH12345ABC」）
- username（Cisco Unified Communications Manager 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」）

次にサンプル スクリプトを示します。このスクリプトはあくまで参考例です。シスコでは、お客様のサーバにインストールされたアップロード スクリプトをサポートしていません。

```
<?php

// NOTE: you may need to edit your php.ini file to allow larger
// size file uploads to work.
// Modify the setting for upload_max_filesize
// I used:  upload_max_filesize = 20M

// Retrieve the name of the uploaded file
$filename = basename($_FILES['prt_file']['name']);

// Get rid of quotes around the device name, serial number and username if they exist
$devicename = $_POST['devicename'];
$devicename = trim($devicename, "'\"");

$serialno = $_POST['serialno'];
$serialno = trim($serialno, "'\"");

$username = $_POST['username'];
$username = trim($username, "'\"");

// where to put the file
$fullfilename = "/var/prtuploads/".$filename;

// If the file upload is unsuccessful, return a 500 error and
// inform the user to try again

if(!move_uploaded_file($_FILES['prt_file']['tmp_name'], $fullfilename)) {
        header("HTTP/1.0 500 Internal Server Error");
        die("Error: You must select a file to upload.");
}

?>
```

手順

ステップ 1 PRT アップロード スクリプトを実行できるサーバを設定します。

ステップ 2 ニーズに合わせて、上記のパラメータを処理できるスクリプトを作成したり、用意されているサンプル スクリプトを編集したりします。

ステップ 3 サーバにスクリプトをアップロードします。

ステップ 4 Cisco Unified Communications Manager で、個々のデバイス設定ウィンドウ、[共通の電話プロファイル（Common Phone Profile）] ウィンドウ、または[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] 領域に移動します。

ステップ 5 [カスタマー サポートのアップロードURL（Customer support upload URL）] をオンにし、アップロード サーバ URL を入力します。

例：

http://example.com/prtscript.php

ステップ 6 変更を保存します。

Web ブラウザからスクリーンショットを取得

手順

ブラウザを使用して、次の URL にアクセスします。**http://http://<Endpoint IP Address>/CGI/Screenshot**
認証を求めるプロンプトが表示されます。関連付けられたユーザー ID 名とパスワードを使用します。

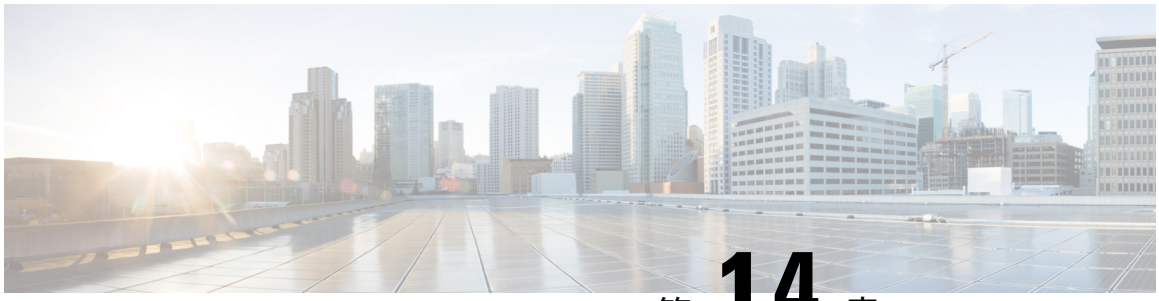
デバイスからスクリーンショットを撮影

手順

[音量ダウン（Vol Down）] ボタンと **[電源/ロック（Power/Lock）]** ボタンを 3 秒間押します。

アプリケーションサポート

問題がデバイスの問題なのか、アプリケーションの問題なのかを評価します。問題がアプリケーションに関連している場合は、アプリケーション サポート センターに直接お問い合わせください。



第 14 章

モデル情報ステータスおよび統計情報

モデル情報（Model Information）

モデル情報を表示するには、[設定（Settings）] アプリケーションで**[デバイスについて（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含まれています。

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	デバイスに関する追加情報を提供するサブメニュー。
Cisco ユーザー ガイド	ドキュメントへのリンクを提供します。
法的情報	オープンソース ライセンスを含みます。
モデル番号	モデル番号。
Android バージョン	Android のバージョンを示します。
カーネル バージョン	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 ステータス	enforcing または permissive を示します。
[Cisco ロード情報（Cisco Load Information）]	
アクティブロード	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。

項目	説明
（注） デバイスがアップグレード中の場合は、「Cisco ロード情報」グループの下に「アップグレードの進捗」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ているサーバーの DNS または IP アドレス。
スタンバイサーバー	スタンバイ サーバの DNS または IP アドレス。
シスコ コラボレーション問題報告ツール	
シスコ コラボレーション問題報告ツール	問題を報告するためのツール。タップして、日付、時刻、問題のアプリケーションの問題の説明、およびカスタマー サポートの電子メール アドレスを選択して入力します。**[電子メールレポートの作成（ Create email report）]** をタップしてログ情報を収集し、サポートに送信します。

ユーザーがセキュアなまたは認証済みサーバーに接続している場合、対応するアイコン（ロックまたは証明）はホーム画面のサーバー オプションの右に表示されます。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。

デバイスのステータス

デバイス ステータスを表示するには、設定アプリケーションで **[デバイスについて（About device）]** > **[ステータス（Status）]** を選択します。

表 *24 :* デバイスのステータス

項目	説明
ステータス メッセージ	[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	デバイスのモバイル電話番号を示します。
IP アドレス	デバイスの IP アドレスを示します。
Wi-Fi MAC アドレス	現在の Wi-Fi 接続の MAC アドレスを提供します。
イーサネット MAC アドレス	現在のイーサネット接続の MAC アドレスを提供します。
Bluetooth アドレス	Bluetooth チップセットの MAC アドレスを提供します。
DHCP 情報	[DHCP 情報（DHCP Information）] 画面を表示します。

項目	説明
Up time	デバイスの実行時間。
現在のアクセス ポイン	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。
イーサネット統計情報	[イーサネット統計（Ethernet Statistics）] 画面を表示します。ここには、イーサネット トラフィック統計が表示されます。
WLAN 統計情報	該当する場合は、WLAN 統計画面を表示します。
コールの統計情報（音声）	現在のコールの音声部分のカウンタと統計情報を提供します。
コールの統計情報	現在のコールのビデオ部分のカウンタと統計情報を提供します。
コール統計（プレゼンテーション）	現在のコールのプレゼンテーション部分のカウンタと統計情報を提供します。

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、デバイスが生成した直近 50 件のステータス メッセージが表示されます。次の表に、表示される可能性のあるステータス メッセージを示します。この表には、エラーに対処するために実行できるアクションも含まれています。

[ステータス メッセージ（Status messages）] 画面を表示するには、**[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、**[クリア（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）	ファイル システムに対して、構成ファイルのサイズが大きすぎます。	デバイスの電源を一度切ってから再投入しま
チェックサム エラー（Checksum Error）	ダウンロードしたソフトウェア ファイルが破損しています。	デバイスのファームウェアの新しいコピーを TFTPPath ディレクトリに置きます。ファイルクトリにコピーできるのは、TFTP サーバ ソシャットダウンされているときだけです。そコピーすると、ファイルが破損する可能性が

メッセージ	説明	考えられる状況と対処方法
DHCP タイムアウト（DHCP timeout）	DHCP サーバが応答しませんでした。	• ネットワーク ビジー：このエラーは、ネット が軽減されると、自動的に解決します。 • DHCP サーバと電話との間にネットワーク接 ネットワーク接続を確認してください。 • DHCP サーバがダウンしている：DHCP サー 確認してください。 • エラーが続く：スタティック IP アドレスを ことを検討してください。
DNS タイムアウト（DNS timeout）	DNS サーバが応答しませんでした。	• ネットワーク ビジー：このエラーは、ネット が軽減されると、自動的に解決します。 • DNS サーバと電話との間にネットワーク接 ネットワーク接続を確認してください。 • DNS サーバがダウンしている：DNS サーバ 認してください。
DNS 不明ホスト（DNS unknown host）	IPv4 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 Communicat のホスト名が DNSで適切に構成されているこ てください。 • ホスト名ではなく IP アドレスを使用するこ てください。
IP が重複しています（Duplicate IP）	デバイスに割り当てられた IP アドレスは、別のデバイスが使用中です。	• デバイスにスタティック IP アドレスが割り いる場合は、重複する IP アドレスを割り当 ことを確認してください。 • DHCP を使用している場合は、DHCP サーバ 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
		[TFTPファイルの管理（TFTP File Management）]
		レクトリに存在することを確認してください。
		• ネットワーク ロケールと同じ名前のサブディ
		存在するファイル：
		  • tones.xml
		• ユーザー ロケールと同じ名前のサブディレク
		するファイル：
		  • glyphs.xml
		  • dictionary.xml
		  • kate.xml

メッセージ	説明	考えられる状況と対処方法
ファイルが見つかりません <Cfg ファイル>（File not found <Cfg File>）	TFTP サーバで、名前ベースのデフォルトの設定ファイルが見つかりませんでした。	コンフィギュレーション ファイルは、デバイス Communications Manager データベースに追加されます。電話機が Cisco Unified Communicatio タベースに存在しない場合、TFTP サーバは が見つかりません（CFG File Not Found を生成します。 • デバイスが Cisco Unified Communications されていません。 デバイスの自動登録を許可しない場合は Communications Manager にデバイスを手 要があります。 • DHCP を使用している場合は、DHCP サ TFTP サーバを指定していることを確認 • スタティック IP アドレスを使用してい 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。	デバイスは、電源をオフ/オンにするか、また レスをリセットするまで、アイドル状態のま
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。	このデバイスでのハードウェア変更をサポー バージョンのソフトウェアをインストールし 生します。 デバイスに割り当てられたロード ID を確認 Unified Communications Managerから、**[デバイ [電話（Phone）]**を選択します）。デバイス 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 いる場合は、デフォルト ルータが構成さ 確認してください。 • DHCP を使用している場合は、DHCP サ トルータを提供していません。DHCP サ 認してください。
DNS サーバ IP がありません（No DNS server IP）	名前は指定されていましたが、DHCP またはスタティック IP 設定で DNS サーバのアドレスが指定されていませんでした。	• デバイスにスタティック IP アドレスが割 いる場合は、DNS サーバーが構成されて してください。 • DHCP を使用している場合は、DHCP サー バを提供していません。DHCP サーバの ください。

メッセージ	説明	考えられる状況と対処方法
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。	信頼ファイルが Cisco Unified Communications Ma されていません。これはデフォルトではセキュ ポートしません。 信頼リストの詳細については、『*Cisco Unified Co* *Manager Security Guide*』 を参照してください。
Cisco Unified Communications Manager によって再起動が要求されました	Cisco Unified Communications Managerからの要求に基づいてデバイスが再起動しています。	Cisco Unified Communications Manager内のデバイ 更が行われた可能性があり、[適用（**Apply**）] を を有効にしました。
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 TFTP サーバを指定していることを確認して • スタティック IP アドレスを使用している場 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サーバーから提供されたエラー コードを認識していません。	Cisco Technical Assistance Center (TAC) に連絡して
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 が軽減されると、自動的に解決します。 • TFTPサーバーと電話との間にネットワーク接 ネットワーク接続を確認してください。 • TFTPサーバがダウンしている：TFTPサー 確認してください。
タイムアウト	サプリカントが802.1X トランザクションを実行しようとしましたが、オーセンティケータが存在しないためにタイムアウトになりました。	通常は、802.1Xがスイッチに設定されていない場 タイムアウトします。
信頼リストの更新に失敗しました。検証に失敗しました	CTL ファイルおよび ITL ファイルの更新に失敗しました。	エラーが発生した場合に表示されるメッセージ。
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 てください。
デバイス名に対応するXmlDefault.cnf.xml, または .cnf.xml	コンフィギュレーション 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 ギュレーション ファイルの名前を示す情報メッセ します。

イーサネット統計情報

[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。以下の表には、この画面で表示される情報を説明しています。

イーサネット統計情報を表示するには、[設定（Settings）] アプリケーションで **[イーサネット統計 > 情報について > （ About deviceStatusEthernet 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、**[クリア（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 Framesrx フレーム	受信パケット数
Tx フレーム	送信パケット数
Rx Broadcasts	受信したブロードキャスト パケットの数
ポート 1	スイッチ ポートの速度とデュプレックス
ポート 2	PC ポートの速度とデュプレックス
CDP ステータス	現在の CDP ステータス

WLAN 統計

[WLAN統計情報（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。以下の表には、この画面で表示される情報を説明しています。

[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

項目	説明
Tx バイト数（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 パケット数
Rx パケット数（rx packets）	受信されたデータ パケット数

項目	説明
ドロップされたTxパケット数（tx packets dropped）	ドロップされた送信済みデータ パケット数
ドロップされたTxパケット数（rx packets dropped）	ドロップされた受信済みデータ パケット数
Tx パケット エラー（tx packet errors）	送信済みデータ パケット エラー数
Rx パケット エラー（rx packet errors）	受信済みデータ 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数
Tx リトライ（tx retry）	受信側デバイスによって確認応答された1回の再送信メッセージ数
Txマルチ リトライ（tx multi retry）	成功するまでの送信再試行回数
Tx 失敗（tx failure）	送信されなかったフレーム数
RTS 成功（rts success）	対応する CTS を受信しました
RTS 失敗（rts failure）	受信されなかったフレーム数。
ACK 失敗（ack failure）	アクセス ポイントが伝送を確認しませんでした
Rx 重複フレーム（rx duplicate frames）	送信された重複マルチキャスト パケット数
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
ローミング数	現在のアクセス ポイントからローミングされた回数

音声通話の統計情報

電話機の [コールの統計（Call Statistics）] 画面にアクセスすると、最新のコールのカウンタ、統計、および音声品質メトリックを表示できます。

（注） Web ブラウザを使用して、[ストリームの統計（Streaming Statistics）] Web ページにアクセスし、リモートにコール統計情報を表示できます。この Web ページには、デバイスでは表示できない追加の RTP 制御プロトコル（RTCP）統計が含まれています。

単一のコールが複数の音声ストリームを使用する場合がありますが、最後の音声ストリームに関するデータだけがキャプチャされます。音声ストリームは、2つのエンドポイント間のパケットストリームです。一方のエンドポイントが保留になると、コールが引き続き接続されている場合でも、音声ストリームは停止します。コールが再開されると、新しい音声パケット ストリームが開始され、以前のコール データは新しいコール データによって上書きされます。

最新の音声ストリームに関する情報のコール統計（音声）を表示するには、**[設定（Settings）]**> **[デバイスについて（About device）]** > **[ステータス（Status）]** > **[コール統計（音声）（Call statistics (audio)）]**を選択します。

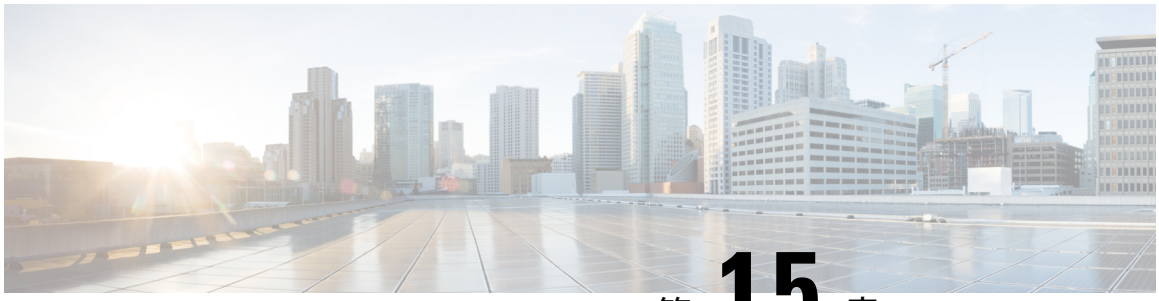
以下の表では、コール統計（音声）画面が提供する項目を一覧にして説明します。

表 *28 :* コール統計項目

項目	説明
受信コーデック	受信された音声ストリームのタイプ（RTP ストリーミング オーディオの送信元コーデック）。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）	送信された音声ストリームのタイプ（RTP ストリーミング オーディオの送信元コーデック）。AAC-LD,, G.722, iSAC, G.711 u-law, G.711 A-law, iLBC and G.729.
受信サイズ	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）	音声ストリームの開始以降に受信した RTP 音声パケットの数。 （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）	音声ストリームが開かれて以降に送信された RTP 音声パケットの数。 （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 ジッターの推定平均値（パケットがネットワークを経由する際の動的な遅延）（ミリ秒単位）。
最大ジッター（Max Jitter）	受信中の音声ストリームが開始されてから測定された最大ジッター（ミリ秒単位）。
受信削除	受信中の音声ストリームで廃棄された RTP パケットの数（不良パケット、過度の遅延などによる）。 （注） デバイスは、Cisco ゲートウェイが生成するペイロード 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）。 欠落している RTP パケットの割合がカッコ内に表示されます。
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）を使用している場合は、アクティブな音声を 3 秒集めるために、もっと長い間隔が必要になる可能性があります。
最大フレーム損失率（Max Conceal Ratio）	音声ストリームの開始以降、最も高い間隔の損失率。
フレーム損失発生秒数（Conceal 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	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。
送信者 DSCP	送信側 SIP シグナリング パケットの DSCP 値
受信の DSCP（Receiver DSCP）	受信者 SIP シグナリングパケットの DSCP 値

項目	説明
送信者 RTCP DSCP	送信者 RTP パケットの DSCP 値
受信者r RTCP DSCP	送信者 RTP パケットの DSCP 値



第 15 章

リモートモニタリング

Web ページアクセスの有効化と無効化

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。これにより、この章で説明されている Web ページおよびセルフ ケア ポータルにアクセスできなくなります。

手順

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

ステップ 2 デバイスの検索条件を指定して **[検索（Find）]** をクリックするか、または **[検索（Find）]** をクリックしてすべての電話の一覧を表示します。

ステップ 3 デバイス名をクリックして、デバイスの **[電話の構成（Phone Configuration）]** ウィンドウを開きます。

ステップ 4 [プロダクト固有の構成レイアウト（Product Specific Configuration Layout）] 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、**[有効（ Enabled ）]** を選択して Web ページアクセスを有効にするか、**[無効（Disabled ）]** を選択して Web ページ アクセスを無効にします。

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 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を使用して、デバイスの IP アドレスを取得します。

- Cisco Unified Communications Manager でデバイスを検索するには、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。Cisco Unified Communications Manager に登録されているデバイスでは、IP アドレスが、**[電話の検索と一覧表示（Find and List Phones）]** ウィンドウおよび **[電話の構成（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）]** > **[デバイスのステータス DHCP 情報（About device）]** > **[ステータス（Status）]** > **[DHCP 情報（DHCP Information）]** を選択し、Wi-Fi またはイーサネットの 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、次のトピックが含まれています。

- [デバイス情報（Device Information）]：デバイス設定と関連情報を含みます。
- [ネットワーク設定（Network Setup）]：ネットワークの設定情報を含みます。
- [セキュリティ情報（Security Information）]：セキュリティ情報を提供します。
- [イーサネット統計情報（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表示します。
  - [アクセス（Access）]：デバイスとの間のネットワーク 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）]：デバイスとの間のネットワーク 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 統計情報（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使用可能な情報を提供する以下のハイパーリンクを含みます。
  - [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。
  - [ステータス メッセージ（Status Messages）]：デバイスが最後に起動してから生成された最新のステータス メッセージ最大 10 件が含まれます。
  - [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 Technical Assistance Center (TAC) に有用なデバッグ メッセージを含みます。

- [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 ページの [デバイス情報（Device Information）] 領域には、デバイス設定と関連情報を含みます。

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	イーサネット ネットワーク状態
Wi-Fi ネットワーク状態	Wi-Fi ネットワーク状態
[MAC アドレス（MAC Address）]	イーサネットMACドレス
WLAN MAC アドレス	Wi-Fi 接続の IP アドレス
ホスト名	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

項目	説明
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	デバイスで実行しているファームウェアの ID
ハードウェアリビジョン	デバイスのハードウェアの変更値
シリアル番号（Serial Number）	デバイス固有のシリアル番号
モデル番号	デバイスのモデル番号
メッセージ受信	デバイスのプライマリ回線で待機しているボイス メッセージがあるかどうかを示します。
UDI	デバイスに関する次の Cisco Unique Device Identifier（UDI）情報を表示します。 • [デバイス タイプ（Device Type）]：ハードウェア タイプを示します。 • [デバイスの説明（Device Description）]：示されたモデル タイプに関連付けられているデバイスの名前を表示します。 • [シリアル番号（Serial Number）]：デバイスの一意のシリアル番号を指定します。
時間	デバイスが属する Cisco Unified Communications Manager の日付/時刻グループから取得した時刻
タイムゾーン	デバイスが属する Cisco Unified Communications Manager の日付/時刻グループから取得されたタイムゾーン
日付	デバイスが属する Cisco Unified Communications Manager の日付/時刻グループから取得した日付

ネットワーク 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、ネットワークの設定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、デバイスの [設定（Settings）] アプリケーションから表示および設定できます。

表 *30* : ネットワークの設定項目

項目	説明
Wi-Fi 情報	
Wifi DHCP サーバー	デバイスの Wifi IP アドレス取得元となる Dynamic Host Configuration Protocol（DHCP）サーバの IP アドレス。
WiFi MAC アドレス	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。
Wi-Fi ホスト名	DHCP サーバがデバイスに割り当てたホスト名。
Wi-Fi ドメイン名	デバイスが所属するドメイン ネーム システム（DNS）ドメインの名前。
Wi-Fi IPアドレス	デバイスの Internet Protocol（IP）アドレス。
Wifi サブネット マスク	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	デバイスが使用するデフォルト ルータ。
Wi-Fi DNS サーバー 1	デバイスで使用されるプライマリ Domain Name System（DNS）サーバー。
Wi-Fi DNS サーバー 2	デバイスで使用されるオプションのバックアップ DNS サーバー。
Wifi EAP 認証	EAP 認証設定を示します。
Wifi SSID	現在の Wi-Fi SSID を示します
Wi-Fiセキュリティ モード	現在の Wi-Fi セキュリティ モードを示します
Wifi 80211 モード	現在の Wi-Fi 80211 モードを示します
イーサネット情報	
イーサネット DHCP サーバー	デバイスの IP アドレス取得元となる Dynamic Host Configuration Protocol（DHCP）サーバの IP アドレス。
イーサネットMACドレス	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 ホスト名	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	デバイスが所属するドメイン ネーム システム（DNS）ドメインの名前。
Ethernet IP Address	デバイスの Internet Protocol（IP）アドレス。
イーサネット サブネット マスク	デバイスで使用されるサブネット マスク。

項目	説明
イーサネット DNS サーバ 1	デバイスで使用されるプライマリ Domain Name System（DNS）サーバー。
イーサネット DNS サーバー 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）	デバイスがメンバーになっている、Cisco Catalyst スイッチに構成された補助仮想ローカル エリア ネットワーク（VLAN）。
Admin. VLAN ID	デバイスがメンバーになっている補助 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	スイッチ ポートの速度とデュプレックス。次のいずれかになります。 • [A]：自動ネゴシエーション • [10H]：10BaseT/半二重 • [10F]：10BaseT/全二重 • [100H]：100BaseT/半二重 • [100F]：100BaseT/全二重 • [1000F]：1000BaseT/全二重 • [リンクがありません（No Link）]：スイッチ ポートへの接続がありません。
PC ポート速度	スイッチ ポートの速度とデュプレックス。次のいずれかになります。 • [A]：自動ネゴシエーション • [10H]：10-BaseT/半二重 • [10F]：10-BaseT/全二重 • [100H]：100-BaseT/半二重 • [100F]：100-BaseT/全二重 • [1000F]：1000-BaseT/全二重 • [リンクがありません（No Link）]：スイッチ ポートへの接続がありません。
IPv6 情報	
IP アドレッシング モード	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 優先順位モードを示します。
IPv6 自動構成	IPv6 自動構成が有効か無効かを示します。
重複アドレス検出	重複アドレス検出が有効か無効かを示します。

項目	説明
[リダイレクト メッセージを承認（Accept Redirect Messages）]	リダイレクト メッセージの受け入れが有効か無効かを示します。
[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 エコー要求への応答が有効か無効かを示します。
IPv6 アドレス	電話のインターネット プロトコル バージョン 6（IPv6）アドレス。
IPv6 プレフィックス長	IPv6 プレフィックス長を示します。
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）	電話機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 サーバー
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します。
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 Trivial File Transfer Protocol（TFTP）サーバー。
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 Trivial File Transfer Protocol（TFTP）サーバー。
CUCM の設定	

項目	説明
CUCM サーバー 1 ～ 5	デバイスを登録可能な Cisco Unified Communications Manager サーバーのホスト名または IP アドレス（優先度順）。限定された Cisco Unified Communications Manager 機能を提供できる SRST ルータが使用可能な場合、項目にそのルータの IP アドレスが表示されることもあります。 使用可能なサーバーについては、この項目に Cisco Unified Communications Manager サーバの IP アドレスと、次の状態のいずれかが表示されます。 • **[アクティブ（Active）]**：電話機が現在コール処理サービスを受けている Cisco Unified Communications Manager サーバー。 • **[スタンバイ（Standby）]**：現在のサーバーが使用不能になった場合に、電話機が切り替える先の Cisco Unified Communications Manager サーバー。 • **[ブランク（Blank）]**：この Cisco Unified Communications Manager サーバーへの現在の接続はありません 項目には、Survivable Remote Site Telephony（SRST）指定も含めることができます。これは、限定された Cisco Unified Communications Manager 機能を提供できる SRST ルータを特定します。このルータは、他のすべての Cisco Unified Communications Manager サーバーが到達不能になった場合に、コールの処理を引き継ぎます。SRST Cisco Unified Communications Manager は、アクティブであっても、常にサーバーのリストの最後尾に表示されます。 Cisco Unified Communications Manager 管理の [デバイス プール（Device Pool）] ウィンドウで SRST ルータ アドレスを構成します。
Information URL	この機能は、Cisco DX シリーズ デバイスの両方で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 デバイスの両方で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 デバイスの両方でサポートされていません。
サービス URL	この機能は、Cisco DX シリーズ デバイスの両方でサポートされていません。
転送の遅延（Forwarding Delay）	リスニングおよびラーニング ステートで費やされる時間。
アイドル URL	この機能は、Cisco DX シリーズ デバイスの両方でサポートされていません。

項目	説明
URL のアイドル時間（Idle URL Time）	この機能は、Cisco DX シリーズ デバイスの両方でサポートされていません。
プロキシサーバーの URL	この機能は、Cisco DX シリーズ デバイスの両方で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 デバイスの両方で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 Trivial File Transfer Protocol（TFTP）サーバー。
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 Trivial File Transfer Protocol（TFTP）サーバー。
代替 TFTP（Alternate TFTP）	デバイスが代替 TFTP サーバーを使用しているかどうかを示します。
ユーザ ロケール（User Locale）	デバイス ユーザーに関連付けられているユーザー 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、ユーザー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 ネットワークに関連付けられているユーザー 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。
ユーザー ロケール バージョン	デバイスにロードされたユーザー 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	デバイス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	デバイスの PC ポートが有効か無効かを示します。
GARP を使う	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	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。
ボイス VLAN アクセスを有効化	デバイスの PC ポートに接続されたデバイスから音声 VLAN へのアクセスを許可するかどうかを示します。
自動選択回線	デバイスの自動選択回線が有効になっているかどうかを示します。
通話制御の DSCP	コール制御シグナリングの DSCP IP 分類。
設定用 Dscp。	デバイスの構成転送の DSCP IP 分類。

項目	説明
サービス用 DSCP	デバイスベースのサービスの 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	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。
PC ポートのスパン	デバイスでネットワーク 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 ポート上の CDP	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）。 CDP が Cisco Unified Communications Manager で無効な場合、PC ポートの CDP を無効にすると CVTA が動作しなくなることが示す警告が表示されます。 PC ポートとスイッチ ポートの CDP に関する現在の値は、[設定（Settings）] アプリケーションに表示されます。
SW ポート上の CDP	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）。 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 を割り当てる場合は、スイッチ ポートで CDP を有効にします。 デバイスが Cisco スイッチに接続されるとき、スイッチ ポートで CDP を有効にします。 CDP が Cisco Unified Communications Manager で無効になっているときは、デバイスを Cisco スイッチ以外のスイッチに接続した場合に限り、スイッチ ポートで CDP を無効にすることを示す警告が表示されます。 PC ポートとスイッチ ポートの CDP に関する現在の値は、[設定（Settings）] アプリケーションに表示されます。
[LLDP]：MED SW ポート	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	PC ポートで Link Layer Discovery Protocol（LLDP）が有効になっているかどうかを示します。

項目	説明
LLDP Power Priority	デバイスの電力優先度をスイッチに通知し、これにより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。 • [不明（Unknown）] : デフォルト • 低 • 高 • クリティカル
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。
Switch Port Remote Configuration	管理者は、 Cisco Unified Communications Manager 管理を使用して、デバイス テーブル ポートの速度と機能をリモートで構成できます。
PC Port Remote Configuration	管理者は、 Cisco Unified Communications Manager 管理を使用して、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、および 802.1X 認証に関する情報が表示されます。

表 *31* : セキュリティ情報の項目

項目	説明
シグナリング セキュリティ モード	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（IPv4）	IPv4 の CAPF サーバー アドレスを示します。
CAPF サーバー（IPv6）	IPv6 の CAPF サーバー アドレスを示します。
CAPF ポート	CAPF ポートを示します。
CTL ファイル	
CTL 署名	CTL 署名を表示します。

項目	説明
CUCM サーバ/TFTP サーバー	CUCM/TFTP サーバーのアドレスを示します
アプリケーション サーバ	アプリケーション サーバーを示します
CAPF サーバー	CAPF サーバーを示します
ITL ファイル（ITL File）	
ITL 署名	ITL 署名を表示
CAPF サーバー	CAPF サーバーを示します
信頼検証サービス（TVS）	TVS アドレスを示します
CUCM サーバー/TFTP サーバー	CUCM/TFTP サーバーのアドレスを示します
設定ファイル	ITL 構成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	
デバイス認証	802.1X デバイス認証が有効になっているかどうかを示します。
Transaction Status（トランザクション ステータス）	802.1Xトランザクション ステータスが有効かどうかを示します。
プロトコル	802.1X プロトコルを示します。
デバイス ID	デバイス ID を表示します。

イーサネット統計情報

デバイスの Web ページにある次のイーサネット統計ハイパーリンクには、ネットワーク トラフィックに関する情報が表示されます。ネットワーク統計エリアを表示するには、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。最初の表では、この領域の項目について説明します。
- アクセス領域：デバイスとの間のネットワーク トラフィックに関する情報を提供します。2 番目の表では、この領域の項目について説明します。

- [ネットワーク（Network）] 領域：デバイスとの間のネットワーク トラフィックに関する情報を提供します。2 番目の表では、この領域の項目について説明します。

表 *32 : [*イーサネット情報（*Ethernet Information***）*]* の項目**

項目	説明
Tx Framestx フレーム	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	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	Direct Memory Access (DMA) 記述子がないために生じた廃棄されたパケットの総数

表 *33 :* アクセス項目とネットワーク項目

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総数。
Rx alignErr	フレーム チェック シーケンス（FCS）が無効であり長さが 64 ～ 1522 バイトの受信パケット総数
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。

項目	説明
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	受信した 64 バイト未満の FCS エラー パケットまたはアライン エラー パケットの総数
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総数。
Rx longGood	1522 バイトを超えるサイズの有効なパケットを受信した総数
Rx longErr	1522 バイトを超えるサイズの FCS エラー パケットまたはアライン エラー パケットを受信した総数
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総数
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総数
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総数
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総数
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総数
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総数
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総数
Tx excessDefer	使用中であることが原因で送信が遅延したパケットの総数
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	デバイスで受信した有効なパケット（マルチキャスト、ブロードキャスト、およびユニキャスト）の総数
Tx Collisions	パケットの送信中に生じた衝突の総数
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総数。

項目	説明
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パケット 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	キャッシュでタイムアウトになった LLDP フレームの総数。
LLDP FramesDiscardedTotal	必須 TLV のいずれかについて、欠落している、順序に誤りがある、または範囲を超える文字列長が含まれているために廃棄された LLDP フレームの総数。
LLDP FramesInErrorsTotal	受信したフレームのうち、検出可能な 1 つ以上のエラーが存在したフレームの総数
LLDP FramesInTotal	デバイスで受信した 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
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 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	速度とデュプレックス モード

WLAN の設定

デバイスの Web ページにある次の [WLAN 設定（WLAN Setup）] ハイパーリンクには、ワイヤレス ネットワークの設定情報とその他の設定に関する情報が表示されます。

- 現在の AP
- WLAN 統計

表 *34 :* 現在の *AP*

項目	説明
AP Name	現在のアクセス ポイント名を表示します。
[MAC アドレス（MAC Address）]	AP の MAC アドレスです。
現在のチャネル	この AP で測定された最新のチャネル。
前回の RSSI（Last RSSI）	この AP で測定された最新の RSSI。
ビーコン間隔	ビーコン間の時間単位の数。時間単位は 1.024 msec です。
最小レート	AP が必要とする最小データ レート。
最大レート	AP が必要とする最大データ レート。
WMM サポート済み	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と最大コール密度の達成にとって重要です。
Noise	現在のノイズ レベルを示します。
負荷	現在の負荷を示します。
品質	音声品質を示します。

表 *35 : WLAN* 統計

項目	説明
NetDevice統計情報	
Txバイト	デバイスが送信する合計バイト数。
Rx Bytes	デバイスが受信する合計バイト数。

項目	説明
Tx Packets	デバイスが送信するパケットの総数。
Rx Packets	デバイスが受信する合計パケット数。
ドロップされた Tx パケット数	デバイスがドロップした送信済みパケットの総数。
ドロップされた Tx パケット数	デバイスがドロップした受信パケットの総数。
Tx エラー パケット数	送信されたエラー パケットの総数。
Rx エラー パケット数	受信されたエラー パケットの合計数。
ファームウェア統計情報	
マルチキャスト Tx フレーム	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	パケットの送信に失敗しました。
Retry	合計再試行回数のカウンタ。
複数の再試行	パケットの送信には、成功するまでに 2 回以上の再試行が必要でした。
フレーム重複	デバイスが受信した重複パケットの数。
RTS 成功	対応する CTS を受信しました。
RTS 失敗	対応する CTS が受信されませんでした。
ACK 失敗	AP が送信を確認しませんでした。
Rx フラグメント	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	デバイスが受信したマルチキャスト パケットの数。
FCSエラー	受信した MPDU でフレーム チェックサム（FCS）エラーが検出されると増分します。
Tx フレーム	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	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、非アクティブなロードのアーカイブ ログ、最後のリブートのログ、現在のロードのアーカイブ ログ、および問題レポート ツールが生成する圧縮されたログのコレクションが含まれます。
- [コア ダンプ（Core Dumps）]：個々のダンプ ファイルへのハイパーリンクが含まれます。コア ダンプ（tombstone_xx）には、アプリケーション クラッシュのデータが含まれます。ANR ファイル（traces.txt）には、デバイスが応答していないと判断し、ユーザーがアプリケーションの終了を選択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）]：デバイスが最後に起動してから生成された最新のステータス メッセージ最大 50 件が含まれます。この情報は、デバイスの [ステータス メッセージ（Status Messages）] 画面でも確認できます。
- [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 メッセージを含みます。

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の送受信サービスの作動中に、情報をストリーミングします。

デバイスの Web ページにある [ストリームの統計（Streaming Statistics）] 領域には、ストリームに関する情報が表示されます。

[ストリーミング統計（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、**[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*：ストリームの統計領域の項目

項目	説明
リモートアドレス	ストリームの宛先の IP アドレスおよび UDP ポート。
Local Address	デバイスの IP アドレスと UDP ポート。
Start Time	Cisco Unified Communications Manager デバイスが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。

項目	説明
ストリーム ステータス	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	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）	この接続を開始してから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）	この接続を開始してからデバイスが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（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（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	この接続で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。 この接続でデータの受信を開始してから失われたRTPデータ パケットのパーセンテージがカッコ内に表示されます。
平均ジッター（Avg Jitter）	RTP データ パケットの内部到着時間の平均偏差の推定値（ミリ秒単位）。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。
送信した受信者レポート（注を参照）	RTCP 受信レポートが送信された回数。
送信した受信レポート時間（注を参照）	RTCP 受信レポートが送信された時間を示す内部タイム スタンプ。

項目	説明
受信パケット	この接続でデータの受信を開始して以来、デバイスが受信したRTPデータ パケットの総数。コールがマルチキャスト 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。
受信側オクテット	この接続で受信を開始して以降、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。コールがマルチキャスト 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）	隠蔽フレームの合計数を、音声ストリームの開始から受信した音声フレームの合計数で割ったもの。
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）を使用している場合は、アクティブな音声を 3 秒集めるために、もっと長い間隔が必要になる可能性があります。
最大フレーム損失率（Max Conceal Ratio）	音声ストリームの開始以降、最も高い間隔の損失率。
フレーム損失発生秒数（Conceal Secs）	音声ストリームの開始以降、隠蔽イベント（フレーム損失）があった秒数（[深刻なフレーム損失発生秒数（Severely Conceal Secs）] の値を含む）。
深刻なフレーム損失発生秒数（Severely Conceal Secs）	音声ストリームの開始以降、5%を超える隠蔽イベント（フレーム損失）があった秒数。
遅延（注を参照）	ネットワーク遅延の推定値（ミリ秒単位）。ラウンドトリップ遅延の実行中の平均値を表します。これは、RTCP 受信レポート ブロックの受信時に測定されます。
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）。
受信した送信者レポート（注を参照）	RTCP 送信レポートが受信された回数。
受信した送信者レポート時間（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）。

項目	説明
[受信破棄（Receiver Discarded）]	ネットワークから受信したがバッファから廃棄された RTP パケット。
受信した受信者レポート（注を参照）	RTCP 受信レポートが受信された回数。
受信した受信者レポート時間	RTCP 受信者レポートが最後に受信された時間。
受信者暗号化	受信者ストリームが暗号化されているかどうかを示します。
送信者暗号化	送信側ストリームが暗号化されているかどうかを示します。
送信者フレーム	ビデオ ストリームが開始されてからデバイスが送信したビデオフレームの数。
送信者部分フレーム	ビデオ ストリームが開かれてからデバイスが送信した P フレームの数。
送信者 IFrames	ビデオ ストリームが開かれてからデバイスが送信した I フレームの数。
送信者フレーム レート	ビデオ フレームが送信されるレート（1 秒あたりのフレーム数）。
送信者帯域幅	送信されたビデオストリームの帯域幅（kbps（キロビット/秒）単位）。
送信者解像度	デバイスが送信するビデオ ストリームの解像度。
受信者フレーム	ビデオストリームが開かれてからデバイスが受信したビデオフレームの数。
受信者部分フレーム	ビデオ ストリームが開かれてからデバイスが受信した P フレームの数。
受信者 IFrames	ビデオ ストリームが開かれてからデバイスが受信した I フレームの数。
受信者 IFrames Req	ビデオストリームが開かれてからデバイスがリモートエンドポイントに送信した IDR 要求の数。
受信者フレーム レート	ビデオ フレームが受信されるレート（1 秒あたりのフレーム数）。
受信者フレーム損失（Receiver Frames Lost）	ビデオストリームが開かれてからビデオデコーダが報告した損失フレーム数。

項目	説明
受信者フレーム エラー（Receiver Frames Errors）	ビデオストリームが開かれてからビデオデコーダが報告したエラーの数。
受信者帯域幅	受信したビデオストリームの帯域幅（kbps（キロビット/秒）単位）。
受信者解像度	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	ドメイン名を示します。
送信者参加	デバイスがストリームの送信を開始した回数
受信者参加	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 パケットがいつネットワークに送信されるかを示すタイム スタンプ。
受信者の開始時間	ネットワークから最初の RTP パケットを受信した時刻を示すタイム スタンプ。
送信者 DSCP	送信側 SIP シグナリング パケットの DSCP 値
受信の DSCP（Receiver DSCP）	受信者 SIP シグナリングパケットの DSCP 値
送信者 RTCP DSCP	送信者 RTP パケットの DSCP 値
受信者r RTCP DSCP	送信者 RTP パケットの DSCP 値
このビデオでは	ビデオ コールを示します。
プレゼンテーションでは	プレゼンテーション コールを示します。
送信者アクティブ	送信者がアクティブであることを示します。
受信者アクティブ	受信者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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。