Cisco Desktop Collaboration Experience

- Cisco Desktop Collaboration Experience DX600 シリーズ，1 ページ
- ネットワーク プロトコル，4 ページ
- サポートされる機能，10 ページ
- セキュリティ機能，12 ページ
- Cisco Desktop Collaboration Experience の導入，22 ページ

Cisco Desktop Collaboration Experience DX600 シリーズ

Cisco Desktop Collaboration Experience DX650は、インターネットプロトコル（IP）ネットワークでの音声通信を提供します。 Cisco Desktop Collaboration Experience DX650 は、デジタル ビジネス電話機と同じように機能し、電話コールの発受信に加えて、ミュート、保留、転送、スピードダイヤル、コール転送などの機能を使用できます。 また、データ ネットワークに接続するため、IP テレフォニー機能が拡張され、ネットワーク情報やサービス、およびカスタマイズ可能な機能やサービスにアクセスできるようになります。

Cisco Desktop Collaboration Experience DX600 シリーズ デバイスの機能は次のとおりです。

- 24 ビットの電話カラー スクリーン（タッチスクリーン サポート付き）
- フル ビデオ機能
- ギガビット イーサネット接続機能
- 外部のマイクロフォンおよびスピーカのサポート
- ワイヤレス ヘッドセット用 Bluetooth のサポート
- Wi-Fi によるネットワーク接続機能
- USB ポート

Cisco Desktop Collaboration Experience DX650 は、他のネットワーク デバイスと同様に設定と管理を行う必要があります。 これらの電話機は、G.711a-law、G.711 mu-law、G.722、G.729a、G.729ab、

iLBC、およびiSACコーデックのエンコード、およびG.711a-law、G.711 mu-law、G.722、G.729、G.729a、G.729b、G.729ab、iLBC、および iSAC コーデックのデコードをサポートしています。

注意 セル方式の電話、携帯電話、GSM 電話、または双方向ラジオをCisco Desktop Collaboration Experience DX650 のすぐ近くで使用すると、相互干渉が発生することがあります。 詳細については、干渉が発生するデバイスの製造元のマニュアルを参照してください。

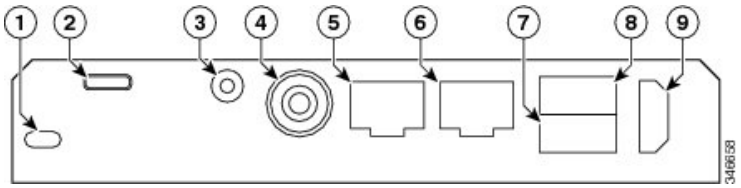
ここでは、Cisco Desktop Collaboration Experience DX650 のコンポーネントについて説明します。詳細については、『*Cisco Desktop Collaboration Experience DX600 Series User Guide*』を参照してください。

Cisco Desktop Collaboration Experience DX650

ここでは、Cisco Desktop Collaboration Experience DX650 の属性に関して説明します。

電話機ケーブルの取り付け

次の図および表を参照して、電話機を接続してください。



1	Kensington 製セキュリティ スロット	6	コンピュータ ポート
2	microUSB ポート	7	補助ポート
3	回線入力/出力ポート	8	USB ポート
4	電源ポート	9	HDMI® ポート
5	ネットワーク ポート		

Cisco Desktop Collaboration Experience DX650 のボタンとハードウェア

次の図で、電話機の重要な部分を説明します。

表 *1*：電話機のボタンとハードウェア

	項目	説明
1	プライバシー シャッター スライド スイッチ	スイッチをスライドさせて、カメラのシャッターを開いたり閉じたりします。
2	カメラ	ビデオ通話のための前面カメラ。
3	電話スクリーン	電話機の機能を表示します。
4	キーパッド	電話番号をダイヤルできます。
5	microSD カード スロット	microSD カードを接続できます。
6	ロック ボタン	電話スクリーンのロック、電話機の再起動、電話機のオンとオフの切り替えに使用します。
7	転送ボタン	コールを転送します。
8	通話を終了ボタン	通話を終了します。
9	保留ボタン	コールを保留にする、または保留中のコールを解除します。
10	会議ボタン	会議コールを開始します。

	項目	説明
11	音量ボタン	ハンドセット、ヘッドセット、スピーカーフォンの音量（オフフック）、および呼出音の音量（オンフック）を制御します。
12	スピーカー ボタン	スピーカーフォン モードのオン/オフを切り替えます。 スピーカーフォンがオンになっているとき、ボタンは点灯しています。
13	ビデオの停止ボタン	ビデオのオン/オフを切り替えます。 ビデオが停止中の場合、ボタンが点灯します。
14	ヘッドセット ボタン	ヘッドセット モードのオン/オフを切り替えます。 ヘッドセットがオンになっているとき、ボタンは点灯しています。
15	ミュート ボタン	マイクロフォン モードのオン/オフを切り替えます。 マイクロフォンがミュートになっているとき、ボタンは点灯しています。
16	ライト ストリップを備えたハンドセット	着信コールまたは新しいボイス メッセージがあることを示します。

電話機およびケーブル ロック

ラップトップ ケーブル ロックを使用して、Cisco Desktop Collaboration Experience DX650 をデスクトップに固定できます。 ロックを電話機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、電話機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。

ネットワーク プロトコル

Cisco Desktop Collaboration Experience DX600 シリーズの電話機は、音声通信に必要ないくつかの業界標準ネットワーク プロトコルとシスコ ネットワーク プロトコルをサポートしています。 次の表に、Cisco Desktop Collaboration Experience DX600 シリーズの電話機でサポートされるネットワーク プロトコルの概要を示します。

表 *2* : サポートされるネットワーク プロトコル *Cisco Desktop Collaboration Experience DX650*

ネットワーク プロトコル	目的	使用方法
Bluetooth	Bluetooth は、短距離におけるデバイスの通信方法を指定する Wireless Personal Area Network（WPAN）プロトコルです。	Cisco Desktop Collaboration Experience DX600 シリーズでは、Bluetooth 3.0 をサポートします。 Cisco Desktop Collaboration Experience DX600 シリーズはハンズフリー プロファイル（HFP）、Advanced Audio Distribution Profile（A2DP）、Human Interface Device Profile（HID）、Object Push Profile（OPP）および Phone Book Access Profile（PBAP）をサポートします。
ブートストラッププロトコル（BootP）	BootP は、特定の起動情報（IP アドレスなど）を Cisco Desktop Collaboration Experience DX650 などのネットワーク デバイスが検出できるようにするものです。	—
Cisco Discovery Protocol（CDP）	CDP は、シスコの製造するすべての装置で動作するデバイス検出プロトコルです。 デバイスは、CDP を使用して自身の存在をネットワーク内の他のデバイスにアドバタイズし、他のデバイスの情報を受信することができます。	Cisco Desktop Collaboration Experience DX650 では、補助 VLAN ID、ポートごとの電源管理の詳細情報、Quality of Service（QoS）設定情報などの情報を、CDP を使用して Cisco Catalyst スイッチとやり取りしています。
Cisco Peer-to-Peer Distribution Protocol（CPPDP）	CPPDP は、デバイスのピアツーピア階層を形成するために使用されるシスコ独自のプロトコルです。この階層はピア デバイスからネイバー デバイスにファームウェア ファイルを配布するために使用されます。	CPPDP は、ピア ファームウェア共有機能で使用されます。

ネットワーク プロトコル	目的	使用方法
ダイナミック ホスト コンフィギュレーションプロトコル（DHCP）	DHCP は、IP アドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。 DHCP を使用すると、Cisco Desktop Collaboration Experience DX600 シリーズデバイスをネットワークに接続すれば、その電話機が機能するようになります。IP アドレスを手動で割り当てたり、ネットワーク パラメータを別途設定したりする必要はありません。	DHCP は、デフォルトで有効になっています。 無効にした場合は、個々の電話機がある場所で、IP アドレス、サブネット マスク、ゲートウェイ、および TFTP サーバを手動で設定する必要があります。 シスコでは、DHCP のカスタム オプション 150 を使用することを推奨します。 この方法では、TFTP サーバの IP アドレスをオプション値として設定します。サポートされているその他の DHCP 設定については、『*Cisco Unified Communications Manager System Guide*』の「Dynamic Host Configuration Protocol」および「Cisco TFTP」の章を参照してください。 （注） オプション 150 を使用できない場合、DHCP オプション 66 の使用を試みることができます。
ハイパーテキスト転送プロトコル（HTTP）	HTTP は、インターネットや Web 経由で情報を転送し、ドキュメントを移送するための標準的な手段です。	Cisco Desktop Collaboration Experience DX600 シリーズの電話機は、XML サービスおよびトラブルシューティングのために HTTP を使用します。
Hypertext Transfer Protocol Secure（HTTPS）	Hypertext Transfer Protocol Secure（HTTPS）は、サーバの暗号化とセキュアな ID を確保できるように、ハイパーテキスト転送プロトコルと SSL/TLS プロトコルを組み合わせたものです。	HTTP と HTTPS の両方をサポートする Web アプリケーションには 2 つの URL が設定されています。 Cisco Desktop Collaboration Experience HTTPS をサポートする DX600 シリーズの電話機は HTTPS URL を選択します。

ネットワーク プロトコル	目的	使用方法
IEEE 802.1X	IEEE 802.1X 標準は、クライアント/サーバベースのアクセスコントロールと認証プロトコルを定義します。これにより、未承認のクライアントが一般にアクセス可能なポートから LAN に接続するのを制限します。 クライアントが認証されるまでは、802.1X アクセスコントロールによって、クライアントが接続されているポートを経由する Extensible Authentication Protocol over LAN（EAPOL）トラフィックのみが許可されます。認証が完了すると、標準トラフィックがポートを通過できます。	Cisco Desktop Collaboration Experience DX600 シリーズの電話機では、EAP-FAST および EAP-TLS の認証方式をサポートすることによって、IEEE 802.1X 標準が実装されます。 電話機で 802.1X 認証が有効になっている場合、PC ポートとボイス VLAN を無効にする必要があります。 詳細については、802.1X 認証のサポート，（20 ページ）を参照してください。
IEEE 802.11a/b/g/n	IEEE 802.11 標準は、ワイヤレス ローカル エリア ネットワーク（WLAN）におけるデバイスの通信方法を指定します。 802.11a は 5 GHz 帯域で動作し、802.11b および 802.11g は 2.4 GHz 帯域で動作します。 802.11.n は、2.4 GHz 帯域または 5GHz 帯域のいずれかで動作します。	802.11 インターフェイスは、イーサネットのケーブル接続が利用できないか望ましくない場合の展開オプションです。
インターネット プロトコル（IP）	IP は、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。	IP を使用して通信するには、ネットワーク デバイスに対して、IP アドレス、ドメイン名、ゲートウェイ、およびネットマスクが割り当てられている必要があります。 IP アドレス、サブネット、およびゲートウェイの識別情報は、Dynamic Host Configuration Protocol（DHCP）を通じて Cisco DX650 を使用する場合は、自動的に割り当てられます。 DHCP を使用しない場合は、個々の電話機がある場所で、これらのプロパティを手動で割り当てる必要があります。
Link Layer Discovery Protocol（LLDP）	LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコデバイスとサードパーティ製デバイスでサポートされています。	Cisco DX650 は、PC ポートで LLDP をサポートします。

ネットワーク プロトコル	目的	使用方法
Link Layer Discovery Protocol - Media Endpoint Devices（LLDP-MED）	LLDP-MED は、音声製品用 LLDP 標準の拡張です。	Cisco DX650 は、PC ポートで LLDP をサポートします。
リアルタイム トランスポート プロトコル（RTP）	RTP は、インタラクティブな音声やビデオなどのリアルタイム データをデータ ネットワーク経由で転送するための標準プロトコルです。	Cisco DX650 は、次のような情報を通信するために、SW ポート上で LLDP-MED をサポートします。 • ボイス VLAN の設定 • デバイスの検出 • 電源管理 • インベントリ管理 LLDP-MED サポートの詳細については、LLDP-MED および『Cisco Discovery Protocol』ホワイト ペーパーを参照してください。 http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml
リアルタイム制御プロトコル（RTCP）	RTCP は RTP と連動して、RTP ストリーム上で QoS データ（ジッター、遅延、ラウンドトリップ遅延など）を伝送します。 また、RTCP は、ビデオ エクスペリエンスが向上するように、オーディオ ストリームとビデオ ストリームを同期する際にも使用されます。	音声コールの RTCP は、デフォルトでは無効になっています。（ビデオ コールの音声ストリームとビデオ ストリームの両方を含む）ビデオ コールの RTCP は、デフォルトでは無効になっています。 Cisco Unified Communications Manager Administration からの個々の電話機の RTCP を有効または無効にすることができます。

ネットワーク プロトコル	目的	使用方法
セッション記述プロトコル（SDP）	SDP は SIP プロトコルの一部であり、2 つのエンドポイント間で接続が確立されている間に、どのパラメータを使用できるかを決定します。 会議は、会議に参加するすべてのエンドポイントがサポートする SDP 機能だけを使用して確立されます。	コーデック タイプ、DTMF 検出、コンフォート ノイズなどの SDP 機能は、通常は運用中の Cisco Unified Communications Manager またはメディア ゲートウェイでグローバルに設定されています。 SIP エンドポイントの中には、これらのパラメータをエンドポイント上で設定できるものがあります。
Session Initiation Protocol（SIP）	SIP は、IP を介したマルチメディア会議のためのインターネット技術特別調査委員会（IETF）標準です。 SIP は、アプリケーション層の ASCII ベースの制御プロトコルであり（RFC 3261 で規定）、2 つ以上のエンドポイント間でコールを確立、維持、および終了するために使用できます。	他の VoIP プロトコルと同様に、SIP はシグナリングとセッション管理の機能をパケット テレフォニー ネットワークの内部で処理します。 シグナリングによって、ネットワーク境界を越えてコール情報を伝送することが可能になります。セッション管理とは、エンドツーエンド コールの属性を制御する機能を提供することです。
伝送制御プロトコル（TCP）	TCP は、コネクション型の転送プロトコルです。	Cisco DX600 シリーズの電話機では、Cisco Unified Communications Manager への接続、および XML サービスへのアクセスに TCP を使用します。
トランスポート レイヤ セキュリティ（TLS）	TLS は、通信のセキュリティ保護と認証に使用される標準プロトコルです。	セキュリティが実装されると、Cisco DX600 シリーズの電話機では、Cisco Unified Communications Manager に安全に登録するときに TLS プロトコルが使用されます。

ネットワーク プロトコル	目的	使用方法
トリビアルファイル転送プロトコル（TFTP）	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 Cisco DX650 で TFTP を使用すると、電話タイプ固有の設定ファイルを取得できます。	TFTP は DHCP サーバが自動的に識別する TFTP サーバがネットワーク内に必要です。 DHCP サーバが指定する以外の TFTP サーバを電話機で使用する場合は、電話機の [ネットワークの設定（Network Configuration）] メニューを使用して、TFTP サーバの IP アドレスを手動で割り当てる必要があります。 詳細については、『*Cisco Unified Communications Manager System Guide*』の「Cisco TFTP」の章を参照してください。
ユーザ データグラム プロトコル（UDP）	UDP は、データ パケットを配信するためのコネクションレス型メッセージング プロトコルです。	UDP は RTP ストリームにのみ使用されます。 電話機の SIP シグナリングでは UDP をサポートしていません。

関連トピック

Cisco Unified IP Communications 製品の連携
[イーサネット設定（Ethernet settings）] メニュー
電話機の起動プロセス

サポートされる機能

Cisco Desktop Collaboration Experience DX600 シリーズ電話機は、デジタル ビジネス フォンとほぼ同様に機能し、コールを発信および受信できます。 Cisco Desktop Collaboration Experience DX650 は従来のテレフォニー機能に加えて、電話機をネットワーク デバイスとして管理およびモニタする機能も備えています。

次の各項では、電話機の機能について説明します。

機能の概要

Cisco Desktop Collaboration Experience DX600 では、Cisco WebEx、Cisco Unified Presence、インスタントメッセージング、電子メール、ビジュアルボイスメール、Cisco Unified Communications Manager の音声とビデオテレフォニー機能など、コラボレーションアプリケーションの統合スイートが提供されます。また Cisco DX600 シリーズの電話機は、Virtual Desktop Infrastructure（VDI）および

クラウド コンピューティングを提供します。 Cisco DX600 シリーズの電話機は、Google Play™ のアプリケーションもサポートします。 Cisco DX600 シリーズ電話機がサポートする機能の概要について、およびそれらの設定方法に関するヒントについては、機能、テンプレート、サービス、およびユーザ セットアップを参照してください。

Cisco DX600 シリーズの電話機は、他のネットワーク デバイスと同様に、Cisco Unified Communications Manager および IP ネットワークの他の部分にアクセスできるように設定する必要があります。 DHCP を使用すると、デバイスに設定する設定値が少なくなります。 ただし、ネットワークで必要な場合は、IP アドレス、TFTP サーバ、サブネット情報などの情報を手動で設定できます。

Cisco DX600 シリーズの電話機は、IP ネットワーク上の他のサービスやデバイスと連携することで、高度な機能を提供できます。 たとえば、Cisco Unified Communications Manager を社内の Lightweight Directory Access Protocol 3（LDAP3）標準ディレクトリと統合すると、ユーザが同僚の連絡先情報を IP Phone で直接検索できるようになります。

さらに、Cisco DX600 シリーズの電話機はネットワーク デバイスであるため、詳細なステータス情報を IP Phone から直接取得することができます。 この情報は、ユーザが Cisco DX600 シリーズの電話機を使用しているときに生じた問題をトラブルシューティングするのに役立ちます。

テレフォニー機能の管理

Cisco DX600 の追加の設定値は、Cisco Unified Communications Manager Administration から変更できます。 この Web ベースのアプリケーションを使用して、電話機登録基準とコーリング サーチスペースのセットアップ、社内ディレクトリとサービスの設定、その他のタスクを行うことができます。 詳細については、関連項目および Cisco Unified Communications Manager のマニュアルを参照してください。

Cisco Unified Communications Manager の管理ページの詳細については、Cisco Unified Communications Manager のマニュアル（『*Cisco Unified Communications Manager Administration Guide*』など）を参照してください。 また、このアプリケーションで参照できる状況依存ヘルプも参考情報として利用できます。

Cisco Unified Communications Manager のマニュアルには、次の Web サイトでアクセスできます。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Business Edition 5000 のマニュアルには、次の場所からアクセスできます。

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

ネットワーク パラメータ

DHCP、TFTP、IP の設定値などのパラメータは、電話機で設定できます。 また、現在のコールに関する統計情報や、ファームウェアのバージョンも電話機で取得できます。

エンド ユーザ向けの情報

システム管理者は、多くの場合、ネットワーク内や社内の Cisco DX600 シリーズの電話機ユーザの主な情報源になります。 機能や手順について確実に最新の情報を伝えるために、Cisco Desktop Collaboration Experience DX600 シリーズのマニュアルをよく読んでおいてください。 Cisco Desktop Collaboration Experience DX600 シリーズの Web サイトに必ずアクセスしてください。

http://www.cisco.com/en/US/products/ps12956/tsd_products_support_series_home.html

このサイトから、このサブページにあるさまざまなユーザ ガイドを見ることができます。

http://www.cisco.com/en/US/products/ps12956/products_user_guide_list.html

マニュアルを提供することの他に重要な点は、使用可能な Cisco Desktop Collaboration Experience DX600 シリーズの機能を伝えること（企業やネットワーク独自の機能を含む）、およびそれらの機能にアクセスし、必要に応じてカスタマイズする方法を教えることです。

セキュリティ機能

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

これらの脅威を軽減するため、Cisco Unified IP テレフォニー ネットワークは、電話機とサーバの間にセキュアな（暗号化された）通信ストリームを確立し、維持します。ファイルはデジタル署名してから電話機に転送し、Cisco Desktop Collaboration Experience DX600 シリーズの電話機間では、メディア ストリームとコール シグナリングを暗号化します。

Cisco DX650 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電話セキュリティ プロファイルを使用します。デバイスにセキュリティ プロファイルを適用する方法については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Unified Communications Manager の管理ページでセキュリティ関連の設定を行うと、電話機の設定ファイルに重要な情報が保存されます。 設定ファイルのプライバシーを確保するには、そのファイルを暗号化用に設定する必要があります。 詳細については、 の「Configuring Encrypted Phone Configuration Files」の章を参照してください。

次の表に、このマニュアルおよび他のマニュアルで、セキュリティに関する詳細情報が記載されている場所を示します。

表 *3*： *Cisco DX600* シリーズおよび *Cisco Unified Communications Manager* セキュリティに関するトピック

トピック	参照
Cisco Unified Communications Manager および Cisco DX600 シリーズの電話機に関するセットアップ情報、設定情報、およびトラブルシューティング情報を含む、セキュリティの詳細な説明	『*Cisco Unified Communications Manager Security Guide*』を参照してください。

トピック	参照
Cisco DX600 シリーズ電話機でサポートされるセキュリティ機能	サポート対象のセキュリティ機能, （14 ページ）を参照してください。 『*Cisco DX600 Series Wireless LAN Deployment Guide*』を参照してください。
セキュリティ機能に関する制約	セキュリティ上の制約事項, （20 ページ）を参照してください。
セキュリティ プロファイル名の表示	サポート対象のセキュリティ機能, （14 ページ） では、Cisco DX600 シリーズの電話機がサポートするセキュリティ機能の概要を示します。これらの機能と、Cisco Unified Communications Manager および Cisco DX600 シリーズの電話機のセキュリティの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
セキュリティが実装されているコールの識別	セキュアな電話コール, （17 ページ）を参照してください。
エクステンションモビリティ HTTPS のサポート	ネットワーク プロトコル, （4 ページ）を参照してください。
TLS 接続	ネットワーク プロトコル, （4 ページ）およびCisco Unified Communications Manager での電話機の追加方法を参照してください。
セキュリティと電話機の起動プロセス	電話機の起動プロセスを参照してください。
セキュリティと電話機の設定ファイル	Cisco Unified Communications Manager での電話機の追加方法を参照してください。
セキュリティが実装されているときの電話機での [TFTP サーバ 1（TFTP Server 1）] または [TFTP サーバ 2（TFTP Server 2）] オプションの変更	[TFTP サーバの設定（TFTP Server Settings）] メニューを参照してください。
電話機からアクセスする [セキュリティのセットアップ（Security Setup）] メニューの項目	[個人セットアップ（Personal setup）] メニューを参照してください。
電話機の Web ページへのアクセスの無効化	Web ページへのアクセスの有効化および無効化を参照してください。
トラブルシューティング	『*Cisco Unified Communications Manager Security Guide*』を参照してください。
電話機からの CTL ファイルの削除	Cisco Desktop Collaboration Experience のリセットを参照してください。
電話機のリセットまたは復元	Cisco Desktop Collaboration Experience のリセットを参照してください。
Cisco DX600 シリーズの電話機の 802.1X 認証	802.1X 認証のサポート, （20 ページ） を参照してください。

サポート対象のセキュリティ機能

次の表に、Cisco DX650 でサポートされるセキュリティ機能の概要を示します。 これらの機能と、Cisco Unified Communications Manager および Cisco Unified IP Phone のセキュリティの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco DX650 の現在のセキュリティ設定については、[アプリケーション（Applications）] [設定（Settings）] [Security（セキュリティ）] をタップします。 詳細については、[個人セットアップ（Personal setup）] メニューを参照してください。

表 *4*：セキュリティ機能の概要

機能	説明
イメージ認証	署名付きのバイナリ ファイル（拡張子 .sgn）によって、ファームウェア イメージが電話機へのロード前に改ざんされることを防止します。 イメージが改ざんされると、電話機は認証プロセスに失敗し、新しいイメージを拒否します。
カスタマーサイト証明書のインストール	各 Cisco DX650 には、デバイス認証用に一意の証明書が必要です。 Cisco DX650 には製造元でインストールされる証明書（MIC）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 Administration で、Certificate Authority Proxy Function（CAPF）を使用して証明書をインストールするように指定できます。 あるいは、デバイス上の [エンタープライズ セキュリティ（Enterprise security）] メニューからローカルで有効な証明書（LSC）をインストールします。 詳細については、Cisco Desktop Collaboration Experience 電話機のセキュリティを参照してください。
イメージの暗号化	暗号化バイナリ ファイル（拡張子 .sebn）によって、ファームウェア イメージが電話機へのロード前に改ざんされることを防止します。 イメージが改ざんされると、電話機は認証プロセスに失敗し、新しいイメージを拒否します。
デバイス認証	Cisco Unified Communications Manager サーバと電話機間で、一方のエンティティが他方のエンティティの証明書を受け入れるときに行われます。 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判別し、必要に応じて TLS プロトコルを使用してエンティティ間にセキュアなシグナリング パスを作成します。 Cisco Unified Communications Manager では、認証できない電話機は登録されません。

機能	説明
ファイル認証	電話機がダウンロードするデジタル署名ファイルを検証します。 ファイルの作成後、ファイルの改ざんが発生しないように、電話機でシグニチャを検証します。 認証に失敗したファイルは、電話機のフラッシュ メモリに書き込まれません。 電話機はこのようなファイルを拒否し、処理を続行しません。
ファイルの暗号化	暗号化により、ファイルの機密性の高い情報が電話機に転送される間に漏えいしないように保護されます。 さらに、電話機でも、ファイルが作成後に改ざんされていないことを、署名を確認することで確認します。 認証に失敗したファイルは、電話機のフラッシュ メモリに書き込まれません。 電話機はこのようなファイルを拒否し、処理を続行しません。
シグナリング認証	TLS プロトコルを使用して、シグナリング パケットが転送中に改ざんされていないことを検証します。
製造元でインストールされる証明書	各 Cisco DX600 シリーズの電話機は、デバイス認証に使用する固有の、製造元でインストールされる証明書（MIC）が含まれています。 MIC は、個々の電話機を識別するために長期的に割り当てられた証明を提供し、Cisco Unified Communications Manager はこれを使用して電話機を認証します。
メディアの暗号化	SRTP を使用して、サポートされるデバイス間のメディア ストリームがセキュアであること、および意図したデバイスのみがデータを受信し、読み取ることを保証します。 デバイスのメディア マスターのキー ペアの作成、デバイスへのキーの配布、キーが転送される間のキーの配布のセキュリティの確保などが含まれます。
CAPF（Certificate Authority Proxy Function）	電話機に非常に高い処理負荷がかかる、証明書生成手順の一部を実装します。また、キーの生成および証明書のインストールのために電話機と対話します。 電話機の代わりに、お客様指定の認証局に証明書を要求するよう CAPF を設定できます。または、ローカルで証明書を生成するように CAPF を設定することもできます。
セキュリティ プロファイル	電話機がセキュリティ保護、認証、または暗号化の対象になるかどうかを定義します。 この表の他の項目は、セキュリティ機能について説明しています。 これらの機能と、Cisco Unified Communications Manager および Cisco DX600 シリーズの電話セキュリティに関する詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
暗号化された設定ファイル	電話機の設定ファイルのプライバシーを確保できるようにします。
電話機の Web サーバの無効化（オプション）	セキュリティ上の目的で、電話機の Web ページ（ここには電話機のさまざまな処理の統計情報が表示される）とユーザ オプション Web ページへのアクセスを防止できます。 詳細については、ユーザ オプション Web ページの管理を参照してください。

機能	説明
電話機のセキュリティ強化	Cisco Unified Communications Manager の管理ページから制御する追加セキュリティ オプション。 • PC ポートの無効化 • Gratuitous ARP（GARP）の無効化 • PC ボイス VLAN の無効化 • Web アプリケーションへの限定的なアクセスの提供 • Bluetooth アクセサリ ポートの無効化 • 電話機の Web ページへのアクセスを無効にする • 画面ロックが必要 • Google Play へのアクセス制御 • 未知の提供元からのアプリケーションのインストールに対するアクセス制御
802.1X 認証	Cisco DX600 シリーズの電話機は 802.1X 認証を使用して、ネットワークへのアクセスの要求およびネットワーク アクセスができます。詳細については、802.1X 認証のサポート，（20 ページ）を参照してください。
SRST 向けのセキュアな SIP フェールオーバー	セキュリティ目的で Survivable Remote Site Telephony（SRST）リファレンスを設定してから、Cisco Unified Communications Manager の管理ページで従属デバイスをリセットすると、TFTP サーバは電話機の cnf.xml ファイルに SRST 証明書を追加し、そのファイルを電話機に送信します。その後、セキュアな電話機は TLS 接続を使用して、SRST 対応ルータと相互に対話します。
シグナリング暗号化	デバイスと Cisco Unified Communications Manager サーバとの間で送信されるすべての SCCP および SIP シグナリング メッセージが確実に暗号化されます。

セキュリティ プロファイル（Security Profiles）

Cisco Unified Communications Manager をサポートしている Cisco Desktop Collaboration Experience DX600デバイスは、すべてセキュリティプロファイルを使用します。このプロファイルは、電話機がセキュリティ保護、認証、または暗号化の対象になるかどうかを定義するものです。セキュリティ プロファイルを設定し、電話機に適用する方法については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

電話機に設定されているセキュリティ モードを確認するには、[セキュリティ設定（Security Configuration）] メニューの [セキュリティ モード（Security Mode）] の設定を表示します。

セキュアな電話コール

Cisco DX650 に対するセキュリティは、Cisco Unified Communications Manager Administration の [電話（Phone）] ウィンドウから [保護されたデバイス（Protected Device）] パラメータを有効にすることで実装されます。 セキュリティが実装されている場合、セキュアな電話コールは、Cisco DX650 画面上の [セキュア コール（Secure Call）] アイコンによって識別できます。

セキュアなコールでは、すべてのコール シグナリングとメディア ストリームが暗号化されます。セキュアなコールは高度なレベルのセキュリティを提供し、コールに整合性とプライバシーを提供します。 進行中のコールが暗号化されている場合、Cisco DX650 の [エンタープライズ セキュリティの設定（Enterprise security settings）] メニューの [セキュリティ モード（Security Mode）] ステータスで [暗号化済み（Encrypted）] が示されます。

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

セキュアなコールでは、コールが暗号化され、発側と着側の両方のデバイスが保護されたデバイスとして設定されている場合、セキュア トーン機能が Cisco Unified Communications Manager 上で有効になっていれば、ユーザへの通知に 2 秒間のトーンが再生されます。 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、Cisco Desktop Collaboration Experience は、ノンセキュア通知トーン（6 回のビープ音）を再生して、コールが保護されていないことをユーザに警告します。 セキュア通知トーン機能および設定要件の詳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） ビデオは非セキュアで送信されます。 したがって、発側と着側の Cisco DX650 デバイスが両方ともセキュアであっても、[暗号化済み（Encrypted）] 鍵アイコンがビデオ コールに対して表示されることはありません。

ここでは、コール セキュリティについて説明します。

セキュアな会議コールの特定

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

1. ユーザがセキュアな Cisco DX650 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そのコールに割り当てます。

3 参加者が追加されると、Cisco Unified Communications Manager は、各デバイスのセキュリティ モードを検証し、セキュアな会議のレベルを維持します。

4 Cisco DX650 は、電話会議のセキュリティ レベルを表示します。

（注） 参加者デバイスのセキュリティ モードおよびセキュアな会議ブリッジの可用性に応じて、さまざまな連携動作、制約事項、および制限事項が電話会議のセキュリティ レベルに影響します。 Cisco DX650 では、セキュアなオーディオ電話会議のみがサポートされます。ビデオはセキュアになりません。 このような連携動作については、コール セキュリティの連携動作と制限事項, （18 ページ） を参照してください。

セキュアな電話コールの識別

セキュアなコールは、ご使用の Cisco DX650 と相手側の電話機がセキュアなコール用に設定されている場合に確立されます。 それらは、同一のシスコ IP ネットワーク内に存在することも、シスコ IP ネットワークの外部にあるネットワーク上に存在することもできます。 セキュアな電話会議は、次のプロセスに従って確立されます。

1 ユーザがセキュアな Cisco DX650（暗号化セキュリティ モード）からコールを開始します。

2 Cisco DX650 は、[エンタープライズ セキュリティ（Enterprise security）] メニューに [暗号化済み（Encrypted）] ステータスを表示します。 このステータスは、Cisco DX650 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、接続相手の電話機が同様にセキュアであるとは限りません。

3 セキュアな相手側デバイスにコールが接続されると、セキュリティ トーンが再生されます。これは、会話の両側が暗号化され、セキュアであることを示しています。 それ以外の場合は、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 上で有効になっている場合にのみ再生されます。 Cisco Unified Communications Manager 上でセキュア 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、非セキュア トーンが再生されます。 詳細については、の「Configuring Secure and Nonsecure Indication Tones」の章を参照してください。『Cisco Unified Communications Manager Security Guide』

コール セキュリティの連携動作と制限事項

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

表 *5*：割り込み使用時のコール セキュリティの連携動作

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

次の表は、発信側の電話機のセキュリティ レベル、参加者のセキュリティ レベル、およびセキュアな会議ブリッジの可用性に応じた、会議のセキュリティ レベルの変更に関する情報を示しています。

表 *6*：会議コールのセキュリティの制限事項

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

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

電話機が Cisco TelePresence をコールする場合、最大帯域幅は 320 kbps です。

デバイス セキュリティ情報のリモートでの確認

手順

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

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

セキュリティ上の制約事項

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

割り込みの開始側の電話機に暗号化が設定されている場合、割り込みの開始側は暗号化された電話機からセキュアでないコールに割り込むことができます。 割り込みが発生すると、Cisco Unified Communications Manager はそのコールをセキュアでないコールに分類します。

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

802.1X 認証のサポート

Cisco Desktop Collaboration Experience デバイスは 802.1X 認証をサポートします。

概要

Cisco Desktop Collaboration Experience デバイスと Cisco Catalyst スイッチは、従来から Cisco Discovery Protocol（CDP）を使用して相互を識別し、VLAN 割り当てやインライン パワー要件などのパラメータを特定していました。 CDP では、ローカルに接続されたワークステーションは識別されません。 Cisco Desktop Collaboration Experience 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、Cisco Desktop Collaboration Experience 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、Cisco Desktop Collaboration Experience 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 Desktop Collaboration Experience デバイスまた、プロキシ EAPOL ログオフ メカニズムも提供します。 ローカルに接続された PC が IP フォンから切断された場合でも、LAN スイッチと IP フォン間のリンクは維持されるので、LAN スイッチは物理リンクの障害を認識しません。 ネットワークの完全性が脅かされるのを避けるため、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 Desktop Collaboration Experience にはまた、802.1x サプリカントも含まれています。 このサプリカントを使用して、ネットワーク管理者は IP 電話と LAN スイッチ ポートの接続を制御できます。 電話機に含まれる 802.1X サプリカントの現在のリリースでは、ネットワーク認証に EAP-FAST オプションと EAP-TLS オプションが使用されています。

必要なネットワーク コンポーネント

Cisco Desktop Collaboration Experience デバイスでの 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。

- Cisco Desktop Collaboration Experience デバイス：電話機は、ネットワークにアクセスするための要求を開始する 802.1x サプリカントとして機能します。
- Cisco Secure Access Control Server（ACS）（またはその他のサードパーティ製認証サーバ）：認証サーバと電話機の両方に、電話機を認証するための共有秘密が設定されている必要があります。
- Cisco Catalyst スイッチ（またはその他のサードパーティ製スイッチ）：スイッチは、オーセンティケータとして機能し、電話機と認証サーバの間でメッセージを渡すことができるように、802.1X をサポートしている必要があります。 この交換が完了した後、スイッチはネットワークへの電話機のアクセスを許可または拒否します。

ベスト プラクティス

次に、802.1X 設定の要件および推奨事項について説明します。

- 802.1X 認証の有効化: 802.1X 標準を使用して Cisco Desktop Collaboration Experience DX600 を認証するには、電話機で 802.1X を有効にする前に、その他のコンポーネントを正しく設定しておく必要があります。
- PC ポートの設定：802.1X 標準では VLAN の使用が考慮されないため、特定のスイッチ ポートに対してデバイスを 1 つだけ認証することを推奨します。 ただし、一部のスイッチ（Cisco Catalyst スイッチなど）はマルチドメイン認証をサポートしています。 スイッチの設定により、PC を電話機の PC ポートに接続できるかどうかが決定されます。
  - 有効：複数ドメインの認証をサポートするスイッチを使用している場合、PC ポートを有効化し、そのポートに PC を接続できます。 この場合、スイッチと接続先 PC 間の認証情報の交換をモニタするために、Cisco Desktop Collaboration Experience DX600 はプロキシ EAPOL ログオフをサポートします。 Cisco Catalyst スイッチでの IEEE 802.1X サポートの詳細については、次の URL にある Cisco Catalyst スイッチのコンフィギュレーション ガイドを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

- 無効：スイッチで同じポート上の複数の 802.1X 準拠デバイスがサポートされていない場合は、802.1X 認証を有効にするときに PC ポートを無効にするようにしてください。このポートを無効にしないで PC を接続しようとすると、スイッチは電話機と PC の両方に対してネットワーク アクセスを拒否します。

- ボイス VLAN の設定：802.1X 標準では VLAN が考慮されないため、この設定をスイッチのサポートに基づいて行うようにしてください。
  - 有効：複数ドメインの認証をサポートするスイッチを使用している場合は、ボイス VLAN を引き続き使用できます。
  - 無効：スイッチで複数ドメインの認証がサポートされていない場合は、ボイス VLAN を無効にし、ポートをネイティブ VLAN に割り当てることを検討してください。

関連トピック

[イーサネット設定（Ethernet settings）] メニュー

Cisco Desktop Collaboration Experience の導入

新しいIPテレフォニーシステムを導入するときは、システム管理者とネットワーク管理者がいくつかの初期設定作業を実施して、ネットワークをIPテレフォニーサービス用に準備する必要があります。 Cisco IP テレフォニー ネットワークのセットアップと設定に関する情報およびチェックリストについては、『*Cisco Unified Communications Manager System Guide*』の「System Configuration Overview」の章を参照してください。

Cisco Unified Communications Manager で IP テレフォニー システムをセットアップし、システム全体にわたる機能を設定したら、Cisco Desktop Collaboration Experience デバイスをシステムに追加できます。

Cisco Unified Communications Manager での Cisco Desktop Collaboration Experience のセットアップ

Cisco Desktop Collaboration Experience デバイスを Cisco Unified Communications Manager データベースに追加するには、次の方法を利用できます。

- 自動登録
- Cisco Unified CM の管理
- Cisco Unified Communications Manager 一括管理ツール
- 一括管理ツール（BAT）と Tool for Autoregistered Phones Support（TAPS）

Cisco Unified Communications Manager で電話機を設定する方法の詳細については、次の資料を参照してください。

- 『*Cisco Unified Communications Manager System Guide*』の「Cisco Unified IP Phones」の章
- 『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone setup」の章
- 『*Cisco Unified Communications Manager Administration Guide*』の「Autoregistration setup」の章
- 『*Cisco Unified Communications Manager Bulk Administration Guide*』

関連トピック

Cisco Unified Communications Manager での電話機の追加方法

Cisco Desktop Collaboration Experienceデバイスのセット アップ Cisco Unified Communications Manager

次の手順では、Cisco Unified Communications Manager の管理ページでの Cisco Desktop Collaboration Experience DX600 シリーズ デバイスの設定タスクの概要を示します。 この手順では、推奨する順序に従って設定するプロセスを解説しています。 一部のタスクは、システムおよびユーザのニーズによっては省略できます。 手順および内容の詳細については、手順に示した資料を参照してください。

手順

ステップ 1 電話機について、次の情報を収集します。

- 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 MAC アドレス）

  （注） Cisco Desktop Collaboration Experience DX600 シリーズ デバイスは、イーサネット MAC アドレスおよび無線 LAN MAC アドレスの 2 種類を使用します。 Cisco Desktop Collaboration Experience DX600 は、Cisco Unified Communications Manager に追加されるとき、イーサネット MAC アドレスを使用してプロビジョニングされる必要があります。

- Cisco Desktop Collaboration Experience DX650 の物理的な場所 Cisco Desktop Collaboration Experience DX650
- Cisco Desktop Collaboration Experience DX650 ユーザの名前またはユーザ ID
- デバイス プール（Device Pool）
- パーティション、コーリング サーチ スペース、およびロケーションの情報
- 回線の数と、それに関連して Cisco Desktop Collaboration に割り当てる電話番号（DN） Cisco Desktop Collaboration Experience DX650
- Cisco Desktop Collaboration Experience DX650 に関連付ける Cisco Unified Communications Manager ユーザ Cisco Desktop Collaboration Experience DX650

- Cisco Desktop Collaboration Experience DX650 テレフォニー機能またはアプリケーションに影響する、Cisco Desktop Collaboration Experience DX650 の使用状況情報

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

ステップ 2 電話機に対応する十分なユニット ライセンスがあることを確認します。 詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』の「Licensing」の章を参照してください。

ステップ 3 （必要に応じて）回線ボタン、スピード ダイヤル ボタン、サービス URL ボタンを変更して、電話ボタン テンプレートカスタマイズします。 プライバシー、すべてのコール、モビリティ ボタンを追加して、ユーザのニーズに対応します。
詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Phone button template setup」の章を参照してください。

ステップ 4 [電話の設定（Phone Configuration）] ウィンドウの必須フィールドに値を入力して、電話機を追加および設定します。 フィールド名の横にあるアスタリスク（*）は、MAC アドレスやデバイス プールなどの必須フィールドを示します。
この手順は、デバイスをデフォルトの設定で Cisco Unified Communications Manager データベースに追加します。

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

[プロダクト固有の設定（Product Specific Configuration）] フィールドについては「?」を参照してください。 ボタン ヘルプ（[電話の設定（Phone Configuration）] ウィンドウ内）

（注） Cisco Unified Communications Manager データベースに電話機とユーザの両方を同時に追加する場合は、『*Cisco Unified Communications Manager Administration Guide*』の「Quick user and phone addition」の章を参照してください。

ステップ 5 [電話番号の設定（Directory Number Configuration）] ウィンドウの必須フィールドに値を入力して、電話機に電話番号（回線）を追加し、設定します。 フィールド名の横にあるアスタリスク（*）は、電話番号やプレゼンス グループなどの必須フィールドを示します。
この手順では、プライマリとセカンダリの電話番号、および電話番号に関連付ける機能を電話機に追加します。

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

ステップ 6 短縮ダイヤル ボタンを設定し、短縮ダイヤル番号を割り当てます。
ユーザは、Cisco Unified Communications Manager ユーザ オプションを使用することで、スピードダイヤルの設定値を電話機上で変更できます。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone setup」の章の「Speed-dial and abbreviated-dial setup」の項を参照してください。

ステップ 7 Cisco Unified IP Phone サービスを設定し、IP Phone サービス（任意）を提供するためにサービスを割り当てます。

ユーザは、Cisco Unified Communications Manager ユーザ オプション Web ページで、使用している電話機のサービスを追加または変更できます。

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

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

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

ステップ 8 IP Phone のサービスや URL へのアクセスを提供するために、プログラム可能なボタン（オプション）にサービスを割り当てます。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Cisco Unified IP Phone setup」の章の「Service URL button setup」の項を参照してください。

ステップ 9 必須フィールドを設定して、ユーザ情報を追加します。 フィールド名の横にあるアスタリスク（*）は、ユーザ ID や姓などの必須フィールドを示します。 この手順では、Cisco Unified Communications Manager のグローバル ディレクトリにユーザ情報を追加します。

（注） パスワード（ユーザ オプション Web ページ用）と PIN（Cisco エクステンション モビリティまたはパーソナル ディレクトリ用）を割り当てます。

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

（注） ユーザに関する情報を保存するために会社が Lightweight Directory Access Protocol（LDAP）ディレクトリを使用している場合、既存の LDAP ディレクトリを使用するために Cisco Unified Communications をインストールして設定できます。

（注） Cisco Unified Communications Manager データベースに電話機とユーザの両方を同時に追加する場合は、『*Cisco Unified Communications Manager Administration Guide*』の「Quick user and phone addition」の章を参照してください。

ステップ 10 ユーザをユーザ グループに関連付けます。 この手順では、ユーザ グループ内のすべてのユーザに適用される、共通のロールと権限のリストをユーザに割り当てます。 管理者は、ユーザ グループ、ロール、および権限を管理することによって、システムユーザのアクセス レベル（つまり、セキュリティのレベル）を制御できます。 たとえば、ユーザをシスコの標準 CCM エンド ユーザ グループに追加する必要があります。こうすると、ユーザが Cisco Unified Communications Manager ユーザ オプションにアクセスできるようになります。

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

- 『End user setup』の章の「End user settings」の項
- 『Access control group setup』の章の「Add users to access control groups」の項

ステップ 11 （任意）ユーザを電話機に関連付けます。この手順では、コールの転送、スピードダイヤル番号やサービスの追加などについて、ユーザが電話機を制御できるようにします。
電話機の中には、会議室にある電話機など、ユーザが関連付けられないものもあります。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「End user setup」の章の「Associate devices to end user」の項を参照してください。

Cisco Desktop Collaboration Experience の設置

電話機を Cisco Unified Communications Manager データベースに追加したら、次は電話機を設置します。 電話機は、管理者（または電話機のユーザ）がユーザの作業場所に設置します。

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

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

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

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

Cisco Desktop Collaboration Experience DX600 シリーズの電話機のセット アップ

次の手順では、Cisco Desktop Collaboration Experience DX600 シリーズ電話機の設置タスクの概要およびチェックリストを示します。 この手順では、推奨する順序に従って電話機を設置するプロセスを解説しています。 一部のタスクは、システムおよびユーザのニーズによっては省略できます。 手順および内容の詳細については、手順に示した資料を参照してください。

手順

ステップ 1 電話機の電源を次の中から選択します。

- Power over Ethernet（PoE）
- 外部電源

（注） Cisco Desktop Collaboration Experience DX600 シリーズの電話機を WLAN 環境で使用する場合、外部電源が必要です。

詳細については、Cisco Desktop Collaboration Experience の電源 を参照してください。

ステップ 2 電話機を組み立て、電話機の位置を調節し、ネットワーク ケーブルを接続します。 Cisco Desktop Collaboration Experience DX600 シリーズの電話機を WLAN 環境で使用している場合は、ステップ 5 を参照してください。
この手順では、電話機の位置を決めて設置し、ネットワークに接続します。 詳細については、Cisco Desktop Collaboration Experience の設置 を参照してください。

ステップ 3 電話機の起動プロセスをモニタします。 この手順では、プライマリとセカンダリの電話番号、および電話番号に関連付ける機能を電話機に追加し、電話機が正しく設定されていることを確認します。
詳細については、電話機の起動確認 を参照してください。

ステップ 4 ワイヤレス ネットワークで Cisco Desktop Collaboration Experience DX600 シリーズのネットワークのシリーズの電話機を展開するように選択した場合は、ステップ 5 に進みます。
IP ネットワーク用の電話上でイーサネットのネットワーク設定値を設定する場合、DHCP を使用するか、手動で IP アドレスを入力して、電話機の IP アドレスを設定します。 詳細については、ネットワーク設定（Network Settings）および [イーサネット設定（Ethernet settings）] メニューを参照してください。

ステップ 5 ワイヤレス ネットワーク上に Cisco Desktop Collaboration Experience DX600 シリーズ デバイスを展開するように選択する場合、次を実行する必要があります。

- ワイヤレス ネットワークを設定します。
- Cisco Unified Communications Manager Administration で、電話機のワイヤレス LAN を有効にします。
- 電話機にワイヤレス ネットワーク プロファイルを設定します。

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

詳細については、VoIP ワイヤレス ネットワーク を参照してください。

ステップ 6 電話機および機能が正常に動作することを確認するために、Cisco Desktop Collaboration Experience DX600 シリーズの電話機にコールを発信します。
『*Cisco Desktop Collaboration Experience DX600 Series User Guide*』を参照してください。

ステップ 7 エンド ユーザに対して、電話機の使用方法および電話機のオプションの設定方法を通知します。
詳細については、次を参照してください。 社内サポート Web サイト