技術的な詳細

物理環境および動作環境に関する仕様

次の表に、会議電話の物理仕様と動作環境仕様を示します。

表 *1*：物理仕様および動作環境仕様

仕様	値または範囲
動作温度	0 ～ 40 °C（32 ～ 104 °F）
動作相対湿度	10 ～ 90%（結露しないこと）
保管温度	–10 ～ 60 °C（14 ～ 140 °F）
高さ	278 mm（10.9 インチ）
幅	278 mm（10.9 インチ）
奥行	61.3 mm（2.4 インチ）
重量	1852 g（4.07 ポンド）

仕様	値または範囲
電源	PoE インジェクタを介した IEEE PoE クラス 3。この電話機は、IEEE 802.3af および 802.3at スイッチ ブレードの両方に対応しており、Cisco Discovery Protocol と Link Layer Discovery Protocol - Power over Ethernet（LLDP-PoE）の両方をサポートします。 接続された LAN スイッチが PoE をサポートしていない場合、他のオプションには非PoEイーサネットインジェクタが含まれます。WiFi を導入するには、Cisco IP Conference Phone 8832 電源アダプタが必要です。
セキュリティ機能	セキュア ブート
ケーブル	USB-C
距離要件	イーサネット仕様では、各電話機とスイッチ間のケーブル長を 100 メートル以内と想定しています。

詳細については、次の『*Cisco IP Conference Phone 8832* データ シート』を参照してください：https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/datasheet-listing.html

電話機の所要電力

では、以下の電源を使用できます。

- を使用した PoE（Power over Ethernet）の導入
- を使用した非 PoE イーサネットの導入
- Cisco IP Conference Phone 8832 電源アダプタを使用した Wi-Fi の導入

表 *2 : Cisco IP Conference Phone* 電源のガイドライン

電源の種類	ガイドライン
PoE 電源：USB-C ケーブルを介して電話機に接続されている または を通じて電力を供給。	または を使用している場合は、スイッチのバックアップ電源を確保して、停電時でも電話機の動作が中断しないようにします。 スイッチ上で実行されている CatOS または IOS のバージョンが、予定している電話機配置をサポートしていることを確認します。オペレーティング システムのバージョンに関する情報については、スイッチのマニュアルを参照してください。 PoEを使用して給電される電話機を設置する場合は、インジェクタを LAN に接続した後、USB-C ケーブルを電話機に接続してください。PoE を使用した電話機を撤去する場合は、電話機からUSB-C ケーブルを取り外した後、アダプタの電源を切断してください。
外部電源 • を使用した非 PoE イーサネットの導入 • Cisco IP Conference Phone 8832 電源アダプタを使用した Wi-Fi の導入 • およびCisco IP Conference Phone 8832 電源アダプタを使用した、非 PoE イーサネットの導入	外部電源を使用して給電される電話機を設置する場合は、インジェクタを電源とイーサネットに接続した後、USB-C ケーブルを電話機に接続してください。外部電源を使用した電話機を撤去する場合は、電話機からUSB-C ケーブルを取り外した後、アダプタの電源を切断してください。

サポートされるネットワーク プロトコル

では、音声通信に必要な複数の業界標準およびシスコのネットワーク プロトコルがサポートされています。次の表に、電話機でサポートされるネットワーク プロトコルの概要を示します。

表 *3 : Cisco IP Conference Phone* でサポートされるネットワーク プロトコル

ネットワーク プロトコル	目的	使用方法に関する特記事項
ブートストラップ プロトコル（BootP）	BOOTP は、電話機などのネットワーク デバイスを有効化し、IPアドレスなどの確かなスタートアップ情報を見つけます。	—

ネットワーク プロトコル	目的	使用方法に関する特記事項
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、ネットワーク内の他のデバイスの情報を受信できます。	電話機はCDPを使用して、ポートの電源管理ごとのAuxiliary VLAN IDなどの情報とCisco Catalystスイッチの Quality of Service（QoS）設定情報を通信します。
Dynamic Host Configuration Protocol（DHCP）	DHCPは、IPアドレスを動的に確保して、ネットワークデバイスに割り当てるものです。 DHCPを使用すると、IP Phoneをネットワークに接続すれば、その電話機が機能するようになります。IPアドレスを手動で割り当てたり、ネットワークパラメータを別途設定したりする必要はありません。	DHCPは、デフォルトで有効になっています。無効にした場合は、個々の電話機がある場所で、IPアドレス、サブネットマスク、ゲートウェイ、およびTFTPサーバを手動で設定する必要があります。 DHCPのカスタム オプション150を使用することを推奨します。この方式では、TFTPサーバのIPアドレスをオプション値として設定しています。サポートされているDHCP設定を追加するには、お使いのCisco Unified Communications Managerのリリースにあるドキュメンテーションを確認してください。 （注） オプション150を使用できない場合は、DHCPオプション66を使用します。
Hypertext Transfer Protocol（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プロトコルです。	電話機は、XMLサービス、プロビジョニング、アップグレード、トラブルシューティングの目的で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の両方をサポートしているWebアプリケーションでは、2つのURLが設定されています。HTTPSをサポートする電話機では、HTTPS URLを選択します。 サービスへの接続がHTTPS経由である場合、鍵のアイコンがユーザに表示されます。

ネットワーク プロトコル	目的	使用方法に関する特記事項
IEEE 802.1X	IEEE 802.1X 標準規格では、クライアントサーバベースのアクセス制御と、認証されていないクライアントがパブリックにアクセスできるポートからLANに接続するのを規制する認証プロトコルを定義します。 802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由ではExtensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。	電話機は、認証方式EAP-FASTおよびEAP-TLS をサポートする IEEE 802.1X 標準規格を実装します。 電話機で 802.1X 認証が有効である場合は、ボイスVLANを無効にします。
インターネット プロトコル（IP）	IPは、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。	IP を使用して通信するには、ネットワーク デバイスに対して、IP アドレス、サブネット、およびゲートウェイが割り当てられている必要があります。 Dynamic Host Configuration Protocol（DHCP）を使用できる電話機を使用している場合、IPアドレス、サブネット、ゲートウェイ ID 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。 電話機は、IPv6アドレスをサポートしています。詳細については、Cisco Unified Communications Managerのご使用のリリースのマニュアルを参照してください。
Link Layer Discovery Protocol（LLDP）	LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコデバイスとサードパーティ製デバイスでサポートされています。	電話機は PC ポートの LLDP をサポートしています。

ネットワーク プロトコル	目的	使用方法に関する特記事項
Link Layer Discovery Protocol-Media Endpoint Devices（LLDP-MED）	LLDP-MEDは、音声製品用に開発された、LLDP 標準の拡張です。	電話機は、SW ポートでLLDP-MED をサポートし、次のような情報を通信します。 • 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、ホワイト ペーパー『*LLDP-MED and Cisco Discovery Protocol*』（URL：[illegible]）を参照してください。
Real-Time Transport Protocol（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。	電話機はRTPプロトコルを使用して、他の電話機およびゲートウェイとの間でリアルタイム音声トラフィックを送受信します。
リアルタイム制御プロトコル（RTCP）	RTCP は RTP と連動して、RTP ストリーム上で QoS データ（ジッタ、遅延、ラウンドトリップ遅延など）を伝送します。	RTCP は、デフォルトで有効になっています。
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 Voice over IP（VoIP）プロトコルと同様に、SIP はパケット テレフォニー ネットワークにおけるシグナリングとセッション管理の機能に対応するよう設計されています。シグナリングは、ネットワーク境界を越えてコール情報を伝送する機能です。セッション管理は、エンドツーエンド コールの属性を制御する機能です。
セキュア リアルタイム転送プロトコル（SRTP）	SRTP は、Real-Time Protocol（RTP）Audio/Video Profile の拡張で、RTP パケットと Real-Time Control Protocol（RTCP）パケットの整合性を保証して、2 つのエンドポイント間のメディア パケットの認証、整合性、および暗号化を実現します。	電話機は、メディア暗号化のために SRTP を使用します。

ネットワーク プロトコル	目的	使用方法に関する特記事項
Transmission Control Protocol（TCP）	TCPは、コネクション型の転送プロトコルです。	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。
Transport Layer Security（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ている場合、Cisco Unified Communications Manager でセキュアな登録をするときに、電話機はTLSプロトコルを使用します。詳細については、お使いの Cisco Unified Communications Manager リリースのマニュアルを参照してください。
Trivial File Transfer Protocol（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。 電話機で TFTP を使用すると、電話機のタイプ固有の設定ファイルを入手できます。	TFTP では、ネットワーク内に TFTP サーバが必要です。このサーバは、DHCP サーバで自動的に識別できます。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 [ネットワークのセットアップ（Network Setup）] 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、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。

外部デバイス

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

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

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

- RF または AF の信号源から外部デバイスを離す。
- RF または AF の信号源から外部デバイスのケーブルの経路を離す。

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

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

⚠

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

ネットワーク輻輳時の電話の動作

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

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

電話機への悪影響を減らしたり、なくしたりするには、電話機が使用されていない時間に管理上のネットワーク タスクをスケジュールするか、テストから電話機を除外してください。