



Cisco IP Phone の概要

Cisco IP Phone はフル機能を装備した電話機であり、Internet Protocol (IP) による音声通信を実現します。従来のアナログ電話機と同じように機能し、コールの発信や着信のほか、消音、保留、転送、短縮ダイヤルなどの機能も利用できます。さらに、ご使用のデータ ネットワークに接続できるため、拡張 IP テレフォニー機能により、ネットワークの情報やサービス、およびカスタマイズ可能な機能やサービスなども利用できます。また、ファイルの認証、デバイスの認証、シグナリングの暗号化、メディアの暗号化などを含むセキュリティ機能もサポートしています。

このマニュアルでの説明は、Cisco IP Phone 7960G および Cisco IP Phone 7940G を対象としています。これらの電話機は、G.711、G.729、G.729a、G.729b、G.729ab、およびワイドバンド (16 ビット、16kHz) の各音声圧縮方式をサポートしています。

Cisco IP Phone 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。

この章は、次の項で構成されています。

- [Cisco IP Phone 7960G/7940G モデルの概要 \(P.1-2\)](#)
- [使用するネットワーク プロトコル \(P.1-6\)](#)
- [Cisco IP Phone 7960G/7940G モデルでサポートされる機能 \(P.1-9\)](#)
- [Cisco IP Phone のセキュリティ機能の概要 \(P.1-12\)](#)
- [Cisco IP Phone 7960G/7940G モデルの設置と設定に関する要件の概要 \(P.1-19\)](#)
- [設定オプションのロックとロック解除 \(P.1-23\)](#)

- [Cisco IP Phone の MAC アドレスの確認 \(P.1-24\)](#)

**注意**

Cisco IP Phone の非常に近くで携帯電話、GSM 電話、または双方向ラジオを使用すると、干渉が起こる場合があります。詳細については、干渉デバイスの製造元の資料を参照してください。

Cisco IP Phone 7960G/7940G モデルの概要

Cisco IP Phone 7960G/7940G モデルはフル機能を装備した複数回線の電話機です。これらはマネージャ向け電話機として IP テレフォニー ネットワークで機能し、従来のアナログ電話機に取って代わるものです。

Cisco IP Phone 7960G モデルと 7940G モデルは、使用可能な回線ボタン（短縮ダイヤル ボタン）の数が違うだけです。Cisco IP Phone 7940G には 2 回線、7960G には 6 回線あります。

これらのモデルの主要コンポーネントを [図 1-1](#) と [図 1-2](#) に示します。また、それらの図の次にある表は、各主要コンポーネントについて説明しています。

図 1-1 Cisco IP Phone 7960G



図 1-2 Cisco IP Phone 7940G



1	受話器（メッセージ受信インジケータのランプ付き）	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。
2	LCD スクリーン	時刻、日付、電話番号、発信者 ID、回線またはコール ステータス、およびソフトキー タブなどを表示します。
3	モデル タイプ	Cisco IP Phone のモデルを示します。
4	プログラマブル ボタン 	設定に応じて、電話回線（回線ボタン）、短縮ダイヤル番号（短縮ダイヤル ボタン）、Web ベースの電話サービス（たとえば、個人アドレス帳など）、または電話機能（たとえば、プライバシー ボタンなど）にアクセスできます。 Cisco IP Phone 7960G には 6 個のプログラマブル ボタンがあり、7940G には 2 個のプログラマブル ボタンがあります。
5	フットスタンド ボタン	電話機本体の角度を調節します。
6	ディレクトリ ボタン 	[ディレクトリ] メニューを開閉します。コール ログおよび社内ディレクトリにアクセスするために使用します。
7	? ボタン 	電話機のボタンまたは機能のヘルプを LCD スクリーンに表示します。また、現在のコールに関するステータス情報も提供します。
8	設定ボタン 	[セッテイ] メニューを開閉します。コントラスト、呼び出し音、ネットワーク構成、ステータス情報など、電話機の設定にアクセスするために使用します。
9	スピーカ ボタン 	スピーカのオンとオフを切り替えます。
10	ミュート ボタン 	消音のオンとオフを切り替えます。

11	ヘッドセット ボタン 	ヘッドセットのオンとオフを切り替えます。
12	音量ボタン 	現在使用中の受話器、ヘッドセット、またはスピーカフォンの音量を調節します。また、呼び出し音の音量（受話器を置いている場合）や LCD スクリーンのコントラストも調節します。
13	サービス ボタン 	[サービス] メニューを開閉します。電話サービスにアクセスするために使用します（利用可能な場合）。
14	メッセージ ボタン 	通常はボイス メッセージ システムに自動ダイヤルします（利用可能な場合）。
15	ナビゲーション ボタン 	メニューのスクロールや項目の選択に使用します。
16	キーパッド	電話番号のダイヤル、文字の入力、およびメニュー項目の選択に使用します。
17	ソフトキー	LCD スクリーンの下部に表示されている機能をそれぞれアクティブにします。ソフトキーの機能は、電話機の状況に応じて変わります。

使用するネットワーク プロトコル

Cisco IP Phone は、音声通信に必要な、複数の業界標準ネットワーク プロトコルおよびシスコ ネットワーク プロトコルをサポートしています。表 1-1 は、Cisco IP Phone 7960G/7940G モデルがサポートしているネットワーク プロトコルの概要を説明しています。

表 1-1 Cisco IP Phone がサポートしているネットワーク プロトコル

ネットワーク プロトコル	目的	使用上の注意
ブートストラップ プ ロトコル (BootP)	BootP を使用すると、ネットワーク デバイス (Cisco IP Phone など) は特定の起動情報 (そのデバイスの IP アドレスなど) を検出できます。	BootP を使用して IP アドレスを Cisco IP Phone に割り当てている場合、電話機のネットワーク構成の設定値として [BOOTP サーバ] オプションが「Yes」と表示されます。
シスコ検出プロトコ ル (CDP)	すべてのシスコ製の機器上で実行されるデバイス検出プロトコルです。 CDP を使用すると、デバイスはその存在を他のデバイスに通知し、ネットワーク内の他のデバイスに関する情報を受け取ることができます。	Cisco IP Phone は、CDP を使用して、補助 VLAN ID、ポート単位の電源管理の詳細、サービス品質 (QoS) 設定情報などを Cisco Catalyst スイッチとの間で通信します。
ダイナミック ホスト コンフィギュレー ション プロトコル (DHCP)	IP アドレスをネットワーク デバイスに動的に配分し、割り当てます。 DHCP を使用すると、手動による IP アドレスの割り当てや、必要なその他のネットワーク パラメータ設定を行わずに、IP Phone をネットワークに接続して操作可能にすることができます。	DHCP はデフォルトで有効になっています。無効になっている場合は、各電話機にローカルで 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 カスタム オプション 150 の使用をお勧めします。この方式を使用すると、TFTP サーバの IP アドレスをオプション値として設定できます。その他の DHCP 設定については、『Cisco CallManager システム ガイド』を参照してください。

表 1-1 Cisco IP Phone がサポートしているネットワーク プロトコル (続き)

ネットワーク プロトコル	目的	使用上の注意
インターネット プロ トコル (IP)	ネットワーク上でパケットをアドレ ス指定し、送信するメッセージプロト コルです。	IP を使用した通信では、ネットワーク デバイスに IP アドレス、サブネット、 およびゲートウェイを割り当てる必 要があります。 ダイナミック ホスト コンフィギュ レーションプロトコル (DHCP) を指 定して Cisco IP Phone を使用する場合 は、IP アドレス、サブネット、および ゲートウェイの識別情報が自動的に 割り当てられます。DHCP を使用しな い場合は、各電話機にローカルでこれ らのプロパティを手動で割り当てる 必要があります。
リアルタイム転送プ ロトコル (RTP)	対話型の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 を介して転送するための標準プロト コルです。	Cisco IP Phone は、RTP プロトコルを 使用して、他の電話機やゲートウェイ との間でリアルタイムの音声トラ フィックを送受信します。
伝送制御プロトコル (TCP)	コネクション型の転送プロトコルで す。	Cisco IP Phone は、TCP を使用して Cisco CallManager に接続し、XML サービスにアクセスします。
トランスポート層セ キュリティ (TLS)	通信の保護と認証を行うための標準 プロトコルです。	セキュリティが実装されている場合、 Cisco IP Phone は、Cisco CallManager へ の安全な登録や Certificate Authority Proxy Function (CAPF) との通信を行 う際に、TLS プロトコルを使用しま す。

表 1-1 Cisco IP Phone がサポートしているネットワーク プロトコル (続き)

ネットワーク プロトコル	目的	使用上の注意
トリビアルファイル 転送プロトコル (TFTP)	ネットワークでのファイル転送を可能にするプロトコルです。 Cisco IP Phone では、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 を使用するには、ネットワーク内に TFTP サーバが必要です。このサーバは、DHCP サーバから自動的に識別できます。DHCP サーバによって指定される TFTP サーバ以外の TFTP サーバを電話機で使用する場合は、電話機の [ネットワークノセッテイ] メニューを使用して、その 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。
ユーザ データグラム プロトコル (UDP)	データ パケットを配送するためのコネクションレス型メッセージ プロトコルです。	Cisco IP Phone は RTP ストリームを送受信します。RTP ストリームでは、UDP が使用されます。

関連項目

- [他の Cisco IP テレフォニー製品との相互対話の概要 \(P.2-2\)](#)
- [電話機の始動プロセスの概要 \(P.2-4\)](#)
- [ネットワークノセッテイ メニューのオプション \(P.4-7\)](#)

Cisco IP Phone 7960G/7940G モデルでサポートされる機能

Cisco IP Phone 7960G/7940G モデルは、従来のアナログ電話機と同じように機能し、発信や着信を行うことができます。このような従来のテレフォニー機能に加えて、Cisco IP Phone には、電話機をネットワーク デバイスとして管理し、モニタできる機能が含まれています。

この項では、次のトピックについて取り上げます。

- [機能の概要 \(P.1-9\)](#)
- [テレフォニー機能の設定 \(P.1-10\)](#)
- [Cisco IP Phone を使用したネットワーク機能の設定 \(P.1-11\)](#)
- [ユーザへの機能情報の提供 \(P.1-11\)](#)

機能の概要

Cisco IP Phone は、自動転送、コール転送、リダイヤル、短縮ダイヤル、電話会議、ボイス メッセージ システムへのアクセスなど、従来のテレフォニー機能を提供します。その他にも、多様な機能を備えています。Cisco IP Phone がサポートするテレフォニー機能の概要、およびそれらの機能を設定する際のヒントについては、[P.5-2 の「Cisco CallManager を使用したテレフォニー機能の設定」](#)を参照してください。

他のネットワーク デバイスと同様に、Cisco IP Phone についても、Cisco CallManager や IP ネットワーク全体にアクセスできるように設定しておく必要があります。DHCP を使用すると、電話機に設定する設定値の数が少なくなりますが、IP アドレス、TFTP サーバ、およびサブネット マスクは、ネットワークで必要な場合には手動で設定できます。Cisco IP Phone にネットワーク設定値を設定する手順については、[第 4 章「Cisco IP Phone のネットワーク設定値の設定」](#)を参照してください。

Cisco IP Phone には、IP ネットワーク上の他のサービスやデバイスとの相互対話による拡張機能が用意されています。たとえば、Cisco IP Phone を社内の Lightweight Directory Access Protocol 3 (LDAP3) 標準ディレクトリに統合すると、ユーザはほかの社員の連絡先情報を自分の IP Phone から直接検索できるようになります。また、XML を使用すると、天気予報、株価情報、商品相場などの Web ベースの情報にアクセスすることもできます。このようなサービスの設定につい

では、P.5-9 の「社内ディレクトリの設定」および P.5-14 の「サービスの設定」を参照してください。

Cisco IP Phone 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 Cisco IP Phone から直接取得できます。このステータス情報は、IP Phone の使用時に発生した問題のトラブルシューティングに役立ちます。詳細については、第 6 章「Cisco IP Phone でのモデル情報、ステータス、統計、およびセキュリティ情報の表示」を参照してください。

関連項目

- Cisco IP Phone のネットワーク設定値の設定 (P.4-1)
- 機能、テンプレート、サービス、およびユーザの設定 (P.5-1)
- Cisco IP Phone のトラブルシューティング (P.8-1)

テレフォニー機能の設定

Cisco IP Phone に関するその他の設定は、Cisco CallManager Administration アプリケーションから変更できます。この Web ベースのアプリケーションは、主に、電話機の登録基準やコール検索スペースの設定、社内のディレクトリやサービスの設定、および電話ボタン テンプレートの変更に使用します。P.5-2 の「Cisco CallManager を使用したテレフォニー機能の設定」を参照してください。

このマニュアルには、Cisco CallManager Administration に関連する手順については一部だけを説明している箇所もあります。これらの説明は、Cisco CallManager アプリケーション内の適切なページを示し、初歩的なガイダンスを提供することを目的としています。

Cisco CallManager Administration アプリケーションの詳細については、『Cisco CallManager Administration Guide (Cisco CallManager アドミニストレーションガイド)』など、Cisco CallManager のマニュアルを参照してください。また、アプリケーションに用意されているコンテキスト ヘルプをガイダンスとして使用することもできます。

Cisco CallManager のマニュアル一覧は、次の URL で参照できます。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm

関連項目

- [Cisco CallManager を使用したテレフォニー機能の設定 \(P.5-2\)](#)

Cisco IP Phone を使用したネットワーク機能の設定

DHCP、TFTP、IP の設定値などの機能は、電話機自体で設定できます。電話機の現在のコールやファームウェア バージョンに関する統計情報も取得できません。

電話機での機能の設定と統計情報の表示の詳細については、第 4 章「Cisco IP Phone のネットワーク設定値の設定」および第 6 章「Cisco IP Phone でのモデル情報、ステータス、統計、およびセキュリティ情報の表示」を参照してください。

関連項目

- [Cisco IP Phone のネットワーク設定値の設定 \(P.4-1\)](#)
- [Cisco IP Phone のトラブルシューティング \(P.8-1\)](#)

ユーザへの機能情報の提供

システム管理者は、多くの場合、自分が管理するネットワークや社内の Cisco IP Phone ユーザから質問を受ける立場にあります。最新の機能や手順に関する情報を提供できるように、Cisco IP Phone のマニュアルを十分に理解しておく必要があります。次の Cisco IP Phone の Web サイトにアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

このサイトから、各種ユーザ ガイドを表示できます。発注方法の詳細については、P.xxi の「技術情報の入手方法」を参照してください。

マニュアルの提供に加えて、利用可能な Cisco IP Phone 機能（自社固有の機能やご使用のネットワーク固有の機能も含む）、および、それらの機能の利用方法とカスタマイズ方法（可能な場合）をユーザに知らせることも重要です。

システム管理者が電話機のユーザに提供する必要がある主要な情報については、付録 A「Web サイトを使用したユーザへの情報提供」を参照してください。

Cisco IP Phone のセキュリティ機能の概要

Cisco CallManager システムにセキュリティを実装すると、データ改ざんやなりすましから電話機を保護できます。これらの攻撃を軽減するために、Cisco IP テレフォニー ネットワークは、電話機とサーバ間に認証および暗号化された通信ストリームを確立し、それを維持するとともに、ファイルが電話機に転送される前にそのファイルにデジタル署名します。

表 1-2 は、本書および他のマニュアルに記載されているセキュリティに関する追加情報の参照先を示しています。

表 1-2 Cisco IP Phone および Cisco CallManager のセキュリティに関するトピック

トピック	参照先
セキュリティの詳細説明（Cisco CallManager および Cisco IP Phone のセットアップ、設定、トラブルシューティングに関する情報を含む）	『Cisco CallManager セキュリティ ガイド』を参照してください。
Cisco IP Phone でサポートされているセキュリティ機能	P.1-13 の「サポートされているセキュリティ機能の概要」 を参照してください。
セキュリティ機能に関する制約事項	P.1-17 の「セキュリティの制約事項」 を参照してください。
電話機がリセットしたときに CAPF がその電話機と相互対話する方法	P.1-18 の「電話機リセット時の CAPF の相互対話」 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	P.1-16 の「認証および暗号化されたコールの識別」 を参照してください。
TLS 接続	P.1-6 の「使用するネットワーク プロトコル」 を参照してください。
セキュリティと電話機の始動プロセス	P.2-4 の「電話機の始動プロセスの概要」 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	P.2-7 の「電話機の設定ファイルの概要」 を参照してください。
電話機へのローカルで有効な証明書 (LSC) の設定	P.3-17 の「Cisco IP Phone へのセキュリティの設定」 を参照してください。

表 1-2 Cisco IP Phone および Cisco CallManager のセキュリティに関するトピック（続き）

トピック	参照先
電話機の「ネットワークノセッテイ」メニューにある CallManager 1 ～ CallManager 5 の各オプションのセキュリティアイコンの確認	P.4-18 の「Cisco CallManager オプション」 を参照してください。
電話機の「セキュリティセッテイ」メニューのセキュリティ項目	P.6-16 の「セキュリティセッテイ メニュー」 を参照してください。
セキュリティが実装されている場合の、電話機の「TFTP サーバ 1」オプションの変更	P.6-17 の「CTL ファイル メニュー」 を参照してください。
電話機からの証明書信頼リスト（CTL）ファイルの削除	P.6-17 の「CTL ファイル メニュー」 を参照してください。
電話機の「シンライリスト」メニューのセキュリティ項目	P.6-19 の「シンライリスト 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	P.7-5 の「Web ページへのアクセスの無効化」 を参照してください。
トラブルシューティング	• P.8-13 の「Cisco IP Phone のセキュリティのトラブルシューティング」 を参照してください。 • 『Cisco CallManager セキュリティ ガイド』を参照してください。
電話機のリセットと復元	P.8-20 の「Cisco IP Phone のリセットまたは復元」 を参照してください。

サポートされているセキュリティ機能の概要

この項では、電話機でサポートされているセキュリティ機能の概要を説明しています。これらの機能の詳細、および Cisco CallManager と Cisco IP Phone のセキュリティの詳細については、『Cisco CallManager セキュリティ ガイド』を参照してください。

また、セキュリティの相互対話、制約事項、および制限のリストを入手する際にも、『Cisco CallManager セキュリティ ガイド』を参照してください。

電話機の現在のセキュリティの設定値を確認するには、[セッテイ] > [セキュリティセッテイ] の順に選択します。詳細については、P.6-16 の「[セキュリティセッテイ メニュー](#)」を参照してください。



(注)

ほとんどのセキュリティ機能は、Certificate Trust List (CTL; 証明書信頼リスト) が電話機にインストールされている場合にだけ利用可能になります。CTL の詳細については、『Cisco CallManager セキュリティ ガイド』を参照してください。

- ・ イメージ認証：ファームウェア イメージが電話機にロードされる前に、署名付きバイナリ ファイル (.sbn または .sb2 という拡張子を持つ) を使用して、ファームウェア イメージに対する改ざんを防止します。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、その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 IP Phone は、デバイス認証に使用する固有の証明書を要求します。この証明書は、電話機から直接インストールできます。または、CAPF サーバから自動的にインストールすることもできます。
- ・ デバイス認証：各エンティティが他のエンティティの証明書を受信したときに、Cisco CallManager サーバと電話機の間で実行されます。デバイス認証は、電話機と Cisco CallManager の間で安全な接続が行われるかどうかを判別します。また、必要な場合には、TLS プロトコルを使用してエンティティ間に安全なシグナリング パスを作成します。セキュリティが設定されている場合、Cisco CallManager は、認証できない電話機は登録しません。
- ・ ファイル認証：電話機がダウンロードするデジタル署名付きファイルを検証します。電話機は、署名を検証して、ファイル作成後にファイルが改ざんされていないことを確認します。認証に失敗したファイルは、電話機のフラッシュ メモリに書き込まれません。
- ・ シグナリング認証：TLS プロトコルを使用して、伝送中のシグナリング パケットに対して改ざんが行われていないことを検証します。
- ・ セキュアな SRST リファレンス：ユーザがセキュリティの SRST リファレンスを設定し Cisco CallManager Administration の従属デバイスをリセットした後に、TFTP サーバは SRST 証明書を電話機の cnf.xml ファイルに追加し、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 対応のルータと相互対話します。

- メディアの暗号化：SRTP を使用して、サポートされているデバイス間の音声メディア ストリームをセキュリティで保護するとともに、目的のデバイスだけがデータを受信して読み取ることができるようにします。具体的には、デバイスのメディア マスター キー ペアの作成、デバイスへのキーの送信、および転送中のキーの送信に対するセキュリティ保護を行います。
- シグナリングの暗号化：デバイスと Cisco CallManager サーバ間で送信されるすべての SCCP シグナリング メッセージを暗号化します。
- CAPF (Certificate Authority Proxy Function)：電話機に代わって、Certificate Authority (CA; 認証権限) サーバと通信します。CAPF サーバは、非常に煩雑な証明書生成手順の一部を電話機のために実行します。また、電話機と相互対話しながら、キーの生成と証明書のインストールを行います。電話機に代わって、カスタマー固有の認証局から証明書を要求するように CAPF サーバを設定できます。または、ローカルで証明書を生成するように設定できます。さらに、さまざまな処理を実行する指示を電話機に与えるように CAPF サーバを設定することもできます。具体的には、公開 / 秘密キー ペアの生成、一部のメッセージの暗号化、署名、復号化、証明書とキー ペアの保存、取得、削除などの処理です。

電話機に CAPF セッションのステータスが表示されます。電話機は、CAPF サーバとの接続中に通信エラーまたは停電が発生した場合、自動的に再接続を試行します。

- 電話機のセキュリティの強化：次に示すセキュリティの追加オプションです。これらのオプションは、Cisco CallManager Administration から制御します。
 - PC ポートの無効化
 - Gratuitous ARP の無効化
 - PC ボイス VLAN アクセスの無効化
 - [セッテイ] メニューへのアクセスの無効化、またはアクセス制限 ([コントラスト] や [ヨビダシオンタイプ] の設定値へのアクセスおよび音量の設定変更の保存だけを許可する)
 - 電話機の Web ページへのアクセスの無効化



(注) [PC ポートラムコウニスル]、[GARP Enabled (GARP を使う)]、および [Voice VLAN Enabled (ボイス VLAN を使う)] の現在の設定値を表示するには、電話機の [ネットワークノセッテイ] メニューを調べます。詳細については、[P.4-7](#) の「[ネットワークノセッテイ メニューのオプション](#)」を参照してください。

関連項目

- [Cisco IP Phone のセキュリティ機能の概要 \(P.1-12\)](#)
- [認証および暗号化されたコールの識別 \(P.1-16\)](#)
- [セキュリティの制約事項 \(P.1-17\)](#)
- [電話機リセット時の CAPF の相互対話 \(P.1-18\)](#)

認証および暗号化されたコールの識別

電話機にセキュリティが実装されている場合、認証および暗号化されたコールは、電話機の LCD スクリーンに表示されるアイコンで識別できます。

コールが認証された場合、そのコールの確立に関与したすべてのデバイスは Cisco CallManager によって認証されます。進行中のコールがエンドツーエンドで認証されると、電話機の LCD スクリーンの通話時間を表示するタイマーの右側にあるコールの状態を示すアイコンが次のアイコンに変わります。



Cisco IP デバイス間のメディア ストリームが認証および暗号化されると、電話機の LCD スクリーンの通話時間を表示するタイマーの右側にあるコールの状態を示すアイコンが次のアイコンに変わります。電話会議、コールの転送、保留などのタスクを実行したときに、このアイコンが表示されないことがあります。これらのタスクに関連付けられているメディア ストリームが暗号化されない場合は、コールのセキュリティ ステータスは暗号化済みからノンセキュアに変わります。



(注)

IP 以外のコール レッグ (たとえば H.323 や PSTN) を介してルーティングされるコールは、IP ネットワーク内では暗号化されているとしても、またロック アイコンがそのコールに関連付けられているとしても、ノンセキュアになります。

関連項目

- [Cisco IP Phone のセキュリティ機能の概要 \(P.1-12\)](#)
- [セキュリティの制約事項 \(P.1-17\)](#)
- [電話機リセット時の CAPF の相互対話 \(P.1-18\)](#)

セキュリティの制約事項

暗号化されたコールには、次の制約事項が適用されます。

- 暗号化が設定されていて、ワイドバンド コーデック リージョンに関連付けられている電話機に対して、暗号化されたコールを確立する際に、Cisco CallManager はワイドバンド コーデックを無視し、電話機が提供するコーデック リストの中から別のサポートされているコーデックを選択します。コール内の他のデバイスに暗号化が設定されていない場合、Cisco CallManager はワイドバンド コーデックを使用して、認証されたコールまたはノンセキュア コールを確立することがあります。
- 割り込みに使用される電話機に暗号化が設定されていない場合、ユーザは暗号化されたコールに対して割り込みを実行できません。この場合、割り込みが失敗したときに、ユーザが割り込みを実行した電話機でリオーダー音（速いビジー音）が再生されます。

発信側の電話機に暗号化が設定されている場合、割り込みの発信側は、暗号化された電話機から認証されたコールまたはノンセキュア コールに対して割り込みを実行できます。Cisco CallManager は、割り込みが実行されたコールをノンセキュアとして分類します。

発信側の電話機に暗号化が設定されている場合、割り込みの発信側は、暗号化されたコールに対して割り込みを実行でき、その電話機は対象のコールが暗号化されていることを示します。

割り込みに使用される電話機がノンセキュアの場合でも、ユーザは認証されたコールに対して割り込みを実行できます。発信側の電話機がセキュリティをサポートしていない場合でも、認証アイコンはコール内の認証されたデバイスに引き続き表示されます。

電話機リセット時の CAPF の相互対話

次の例は、Cisco IP Phone が Cisco CallManager によってリセットされたときに、CAPF がその Cisco IP Phone と相互対話する方法を示しています。これらの例では、LSC が電話機にまだ存在しない場合、および CAPF の Authentication Mode に対して By Existing Certificate が選択された場合に、CAPF 証明書の処理が失敗します。

例 1

この例では、Device Security Mode を Non-secure に設定し、CAPF の Authentication Mode を By Null String または By Existing Certificate (... に優先) に設定した後に、電話機がリセットされます。リセットされた直後に、電話機はプライマリ Cisco CallManager に登録され、設定ファイルを受信します。次に、電話機は自動的に CAPF とのセッションを開始して LSC をダウンロードします。電話機に LSC がダウンロードされたら、Device Security Mode を Authenticated または Encrypted に設定する必要があります。

例 2

この例では、Device Security Mode を Authenticated または Encrypted に設定し、CAPF の Authentication Mode を By Null String または By Existing Certificate (... に優先) に設定した後に、電話機がリセットされます。CAPF セッションが終了し、電話機に LSC がインストールされるまで、電話機はプライマリ Cisco CallManager に登録されません。セッションが終了したら、電話機は登録され、認証済みまたは暗号化済みのモードでただちに実行されます。

正しい LSC が設定されていない電話機は自動的に CAPF サーバと通信せずに登録が失敗するので、この例では By Authentication String を設定することはできません。

Cisco IP Phone 7960G/7940G モデルの設置と設定に関する要件の概要

Cisco IP Phone 7960G/7940G モデルの設置および設定を行うには、ネットワーク設定値の一部を設定し、Cisco CallManager をセットアップして、電話機にローカルで変更を加える必要があります。

必要な手順の概要については、[表 1-3](#) を参照してください。これらの手順の詳細については、参照先欄の資料を参照してください。

表 1-3 Cisco IP Phone の設定手順の概要

必要な作業	目的	参照先
1. Cisco CallManager Administration で使用される次の情報を収集します。 - デバイス プールやコール検索スペースなど、[デバイスジョウホウ] フィールドに要求される情報（該当する場合） - 電話機に関連付ける Cisco CallManager ユーザ - 電話機に割り当てる回線数とそれに対応する電話番号 - 電話機に追加して設定する機能	Cisco CallManager Administration の Phone Configuration Web ページで電話機を設定する際に、これらの情報を参照します。 使用可能な関連情報がある場合、このページの [デバイスジョウホウ] フィールドにはデータが自動的に読み込まれます。各デバイスに対するシステムの設定値を上書きする必要がある場合は、フィールドの内容を修正します。	P.2-12 の「Cisco CallManager データベースへの電話機の追加」 を参照してください。 P.5-2 の「Cisco CallManager を使用したテレフォニー機能の設定」 を参照してください。 『Cisco CallManager システムガイド』を参照してください。 『Cisco CallManager アドミニストレーションガイド』を参照してください。
2. Cisco CallManager システム にセキュリティを実装します（オプション）。	セキュリティを確立します。セキュリティには、データ改ざんやなりすましからの保護が含まれます。	『Cisco CallManager セキュリティガイド』を参照してください。

表 1-3 Cisco IP Phone の設定手順の概要 (続き)

必要な作業	目的	参照先
3. 音声通信を処理するためのルータ、ゲートウェイ、およびスイッチを設定します。	IP テレフォニー ネットワーク用のインフラストラクチャを確立します。	P.2-3 の「Cisco IP Phone と Cisco Catalyst ファミリー スイッチ間の相互対話方法の概要」、および、それらのデバイスに付属のマニュアルを参照してください。
4. Cisco CallManager データベースに電話機を追加する方法を決定します。次の方法があります。 - 自動登録を使用する。 - Cisco CallManager Administration だけを使用する。 - Bulk Administration Tool (BAT) だけを使用する。 - BAT と Tool for Auto-Registered Phones Support (TAPS) を使用する。	Cisco CallManager に電話機を追加する方法によって、電話番号を割り当てる方法が決まります。また、事前に MAC アドレスを取得する必要があるかどうかも判断できます。  (注) セキュリティが実装されている場合、自動登録はサポートされません。	- P.2-12 の「Cisco CallManager データベースへの電話機の追加」を参照してください。 『Cisco CallManager アドミニストレーションガイド』を参照してください。 『Cisco CallManager Bulk Administration Tool ユーザガイド』を参照してください。
5. IP Phone から MAC アドレスを取得します。	自動登録だけを使用するか、または自動登録と Tool for Auto-Registered Phones Support (TAPS) と連携して、Cisco CallManager データベースに電話機を追加する場合、この作業は不要です。	P.1-24 の「Cisco IP Phone の MAC アドレスの確認」を参照してください。
6. 電源の供給元を Cisco AC アダプタにするか、Cisco Catalyst スイッチにするかを選択します。	電話機の電源供給元を、電源コードを介した外部電源にするか、イーサネット ケーブルを介したインライン電源にするかを決定します。	- P.2-9 の「Cisco IP Phone への電力の供給」を参照してください。 - Cisco Catalyst スイッチに付属のマニュアルを参照してください。

表 1-3 Cisco IP Phone の設定手順の概要（続き）

必要な作業	目的	参照先
7. 電話機をネットワークに設置します。	電話機をネットワークに追加します。	第 3 章「Cisco IP Phone のセットアップ」を参照してください。
8. Cisco IP Phone 7914 拡張モジュールを Cisco IP Phone 7960G に追加します。	14 個の回線または短縮ダイヤル番号を追加することにより、Cisco IP Phone 7960G の機能を拡張します。	P.2-16 の「Cisco IP Phone 7914 拡張モジュールをサポートするための Cisco IP Phone 7960G の設定」を参照してください。
9. ネットワーク設定値を Cisco IP Phone に設定します。	IP 設定値を設定し（ネットワークで DHCP を使用しない場合）、TFTP サーバを割り当てます。	P.4-7 の「ネットワークノセッティメニューのオプション」を参照してください。
10. Cisco CallManager システムでセキュリティが有効になっている場合、Cisco IP Phone にセキュリティを設定します。	ローカルで有効な証明書（LSC）を電話機にインストールします。これは、セキュリティに必要な作業です。	P.3-17 の「Cisco IP Phone へのセキュリティの設定」を参照してください。
11. 電話機の機能（コール待機、コール転送、コールパーク、コールピックアップなど）を設定します。	拡張テレフォニー機能を提供します。	• P.5-2 の「Cisco CallManager を使用したテレフォニー機能の設定」を参照してください。 • 『Cisco CallManager アドミニストレーションガイド』を参照してください。 • 『Cisco CallManager 機能およびサービスガイド』を参照してください。
12. ボタン テンプレートを変更します。	カスタマイズされた電話ボタンを提供します。	P.5-11 の「電話ボタン テンプレートの変更」を参照してください。

表 1-3 Cisco IP Phone の設定手順の概要（続き）

必要な作業	目的	参照先
13. Cisco IP Phone サービスを設定します。	ユーザが株式相場や天気予報などの情報にアクセスできるようにします。これらの情報は、対話型のコンテンツとしてテキストとグラフィックスで電話機に表示されます。	• P.5-14 の「サービスの設定」を参照してください。 • 『Cisco CallManager アドミニストレーションガイド』を参照してください。
14. ディレクトリを設定します。	ユーザが社内ディレクトリの検索や個人番号の保存を行うことができますようにします。	• P.5-9 の「社内ディレクトリと個人ディレクトリの設定」を参照してください。 • 『Cisco CallManager アドミニストレーションガイド』を参照してください。
15. Cisco CallManager にユーザを追加します。	ユーザを電話機に関連付けて、そのユーザが、Cisco CallManager のユーザ オプション Web ページにアクセスして、コール転送や短縮ダイヤルなどの機能を設定し、サービスに加入できるようにします。	• P.5-15 の「Cisco CallManager へのユーザの追加」を参照してください。 • 『Cisco CallManager アドミニストレーションガイド』を参照してください。
16. 電話機の使用方法と電話機のオプションの設定方法をエンド ユーザに知らせます。	Cisco IP Phone を正しく使用するために必要な情報をユーザが持っていることを確認します。	付録 A 「Web サイトを使用したユーザへの情報提供」 を参照してください。

設定オプションのロックとロック解除

電話機の動作に影響を与えるような変更をユーザが行えないようにするために、[ネットワークノセッテイ] メニューおよび[セキュリティセッテイ] メニューの設定オプションは、デフォルトでロックされています。これらのオプションを変更し、このマニュアルに記載されている手順の多くを実行するには、事前にこれらのオプションをロック解除しておく必要があります。

オプションが変更できなくなっている場合は、ロックされた鍵のアイコンが[ネットワークノセッテイ] メニューに表示されます。オプションのロックが解除され、変更できるようになっている場合、このメニューには次のようなロックを解除された鍵のアイコンが表示されます。



[ネットワークノセッテイ] メニューまたは[セキュリティセッテイ] メニューのオプションをロックまたはロック解除するには、メニューを表示する前、またはメニューが表示されている間に ****#** を押します。この操作を行うことにより、オプションがロックされるか、ロックが解除されます（直前の状態によりどちらかになります）。

設定オプションを変更した後は、必ずオプションをロックしてください。



注意

****#** を押してオプションをロック解除した直後に、再び ****#** を押してオプションをロックしないでください。電話機はこのような連続操作を ****##** と解釈するため、電話機がリセットされます。オプションをロック解除した後に再びロックする場合は、少なくとも 10 秒間待ってから、****#** を押すようにしてください。

関連項目

- [ネットワークノセッテイ メニューの表示 \(P.4-2\)](#)
- [ネットワークノセッテイ メニューの設定を編集する場合のガイドライン \(P.4-4\)](#)
- [ネットワークの設定オプションの概要 \(P.4-5\)](#)
- [ネットワークノセッテイ メニューのオプション \(P.4-7\)](#)

Cisco IP Phone の MAC アドレスの確認

このマニュアルに記載されているいくつかの手順では、Cisco IP Phone の MAC アドレスを確認する必要があります。電話機の MAC アドレスを確認するには、次の方法があります。

- 電話機から、[セッテイ] > [モデルジョウホウ] の順に選択し、[MAC アドレス] フィールドを調べる。
- 電話機の背面にある MAC ラベルを調べる。
- 電話機の Web ページを表示し、[デバイスジョウホウ] ハイパーリンクをクリックする。

Web ページへのアクセス方法については、[P.7-3 の「IP Phone の Web ページへのアクセス」](#)を参照してください。