



Cisco IP 電話のセキュリティ

- [電話ネットワークのセキュリティ強化機能 \(1 ページ\)](#)
- [サポート対象のセキュリティ機能 \(2 ページ\)](#)

電話ネットワークのセキュリティ強化機能

Cisco Unified Communications Manager 11.5(1) および 12.0(1) では、強化されたセキュリティ環境での動作が可能です。これらの強化機能により、電話ネットワークが、一連の厳密なセキュリティ管理とリスク管理の制御下で動作するようになり、自分自身とユーザが保護されます。

Cisco Unified Communications Manager 12.5 (1)は拡張セキュリティ環境に対応していません。Cisco Unified Communications Manager 12.5 (1)にアップグレードする前にFIPSを無効にすると、TFTP やその他のサービスが正しく機能しなくなります。

強化されたセキュリティ環境には、次の機能が含まれています。

- 連絡先検索認証。
- リモート監査ロギングのデフォルト プロトコルとしての TCP。
- FIPS モード。
- クレデンシャル ポリシーの改善。
- デジタル署名のための SHA-2 ファミリ ハッシュのサポート。
- 512 および 4096 ビットの RSA キー サイズのサポート。

Cisco Unified Communications Manager リリース 14.0 および Cisco IP 電話ファームウェア リリース 14.0 以降では、電話機は SIP OAuth 認証をサポートします。

OAuth は、Cisco Unified Communications Manager リリース 14.0(1) SU1 以降のプロキシ トリビアルファイル転送プロトコル (TFTP) および Cisco IP 電話ファームウェア リリース 14.1(1) でサポートされます。プロキシ TFTP およびプロキシ TFTP 用の OAuth は、Mobile and Remote Access (MRA) ではサポートされません。

セキュリティ設定に関するその他の情報については、以下を参考にしてください。

- *Cisco Unified Communications Manager* システム設定ガイド、リリース 14.0(1) 以降 (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>)。
- *Cisco IP* 電話 7800および8800シリーズのセキュリティの概要 (<https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html>)
- *Cisco Unified Communications Manager* セキュリティガイド (<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>)



(注) Cisco IP 電話には、限られた数の Identity Trust List (ITL) ファイルのみ保存できます。Cisco Unified Communications Manager が電話機に送信できるファイルの数を制限する必要があるため、電話機の ITL ファイルは最大 64K に制限されています。

サポート対象のセキュリティ機能

セキュリティ機能は、電話機の 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、電話機と 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、電話機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) 以降の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、Cisco IP 電話に次のセキュリティ機能が提供されます。

- 電話機の設定ファイルの署名
- 電話機の設定ファイルの暗号化
- HTTPS with Tomcat および他の Web サービスの利用



(注) シグナリングおよびメディア機能を保護するには、引き続き、CTL クライアントを実行し、ハードウェア eToken を使用する必要があります。

Cisco Unified Communications Manager システムに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 IP 電話間では、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。

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）が電話機にインストールされます。LSC は Cisco Unified Communications Manager の管理ページで設定できます。詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。あるいは、電話機の [セキュリティのセットアップ（Security Setup）] メニューから LSC のインストールを開始することもできます。このメニューでは、LSC の更新および削除も実行できます。

WLAN 認証を使用する EAP-TLS のユーザ証明書として LSC を使用することはできません。

電話機では電話セキュリティ プロファイルを使用します。この中では、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します。電話へセキュリティ プロファイルを適用する方法の詳細は、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco Unified Communications Manager の管理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、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

Cisco IP 電話 8800 シリーズは、連邦情報処理標準（FIPS）に準拠します。正常に機能するには、FIPS モードで 2048 ビット以上のキー サイズが必要です。証明書が 2048 ビット未満の場合、電話機は Cisco Unified Communications Manager に登録されず、「電話機を登録できませんでした。[証明書のキー サイズは FIPS に準拠していません（Cert key size is not FIPS compliant）]」が表示されます。

電話機に LSC がある場合、FIPS を有効にする前に、LSC キー サイズを 2048 ビット以上に更新しておく必要があります。

次の表に、電話機でサポート対象セキュリティ機能の概要を示します。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。


セキュリティ モード、信頼リスト、802.1X 認証など電話機の現在のセキュリティ設定を表示するには、[アプリケーション（Applications）]  を押し、[管理者設定（Admin Settings）]> [セキュリティのセットアップ（Security setup）] の順に選択します。

表 1: セキュリティ機能の概要

機能	説明
イメージ認証（Image authentication）	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。
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。

機能	説明
カスタマーサイト証明書のインストール	各 Cisco IP 電話は、デバイス認証に一意の証明書を必要とします。電話機には 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 の管理ページで、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、電話機の [セキュリティ設定 (Security Configuration)] 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 (Device authentication)]	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。電話機と 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。
ファイル認証 (File authentication)	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。認証できないファイルは、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。認証できないファイルは、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。
Manufacturing Installed Certificate (製造元でインストールされる証明書)	各 Cisco IP 電話には、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。
メディア暗号化	SRTPを使用して、サポート対象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)	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。

機能	説明
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。
暗号化された設定ファイル (Encrypted configuration files)	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）とセルフ ケア ポータルへのアクセスを防止できます。
電話のセキュリティ強化 (Phone hardening)	<p>Cisco Unified Communications Manager の管理ページから制御する追加セキュリティ オプションです。</p> <ul style="list-style-type: none"> • 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 • [設定 (Setting)] メニューへのアクセスの無効化。または、[設定 (Preferences)] メニューにアクセスすること、音量の変更を保存することのみ可能な、限定的なアクセスの提供 • 電話機の Web ページへのアクセスの無効化 • Bluetooth アクセサリ ポートの無効化 • TLS 暗号の制限
802.1X 認証	Cisco IP 電話は 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 (31 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。
信頼リストの更新アラーム	電話機で信頼リストが更新されると、Cisco Unified Communications Manager は更新の成功または失敗を示すアラームを受信します。詳細については、以下の表を参照してください。

機能	説明
AES 256 暗号化 (AES 256 Encryption)	<p>Cisco Unified Communications Manager リリース 10.5(2)以降の以降に接続している電話機は、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。これにより電話機は、SHA-2 (Secure Hash Algorithm) 標準および Federal Information Processing Standard (FIPS) に準拠する AES-256 ベースの暗号を使用して TLS 1.2 接続を開始し、サポートすることができます。暗号は次のとおりです。</p> <ul style="list-style-type: none"> • TLS 接続用 : <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • sRTP 用 : <ul style="list-style-type: none"> • AEAD_AES_256_GCM • AEAD_AES_128_GCM <p>詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。</p>
楕円曲線デジタル署名アルゴリズム (ECDSA) 証明書	<p>コモンクライテリア (共通基準、CC) 認証の一部として、バージョン 11.0 の ECDSA 証明書が Cisco Unified Communications Manager によって追加されました。これはバージョン CUCM 11.5 およびそれ以降からのすべての Voice Operating System (VOS) 製品に影響を与えます。</p>

次の表に、信頼リストの更新アラームのメッセージとその意味を示します。詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

表 2: 信頼リストの更新アラームのメッセージ

コードおよびメッセージ	説明
1 - TL_SUCCESS	新しい CTL や ITL を受信
2 - CTL_INITIAL_SUCCESS	新しい CTL を受信、既存の TL なし
3 - ITL_INITIAL_SUCCESS	新しい ITL を受信、既存の TL なし
4 - TL_INITIAL_SUCCESS	新しい CTL および ITL を受信、既存の TL なし
5 - TL_FAILED_OLD_CTL	新しい CTL への更新に失敗したが、以前の TL あり
6 - TL_FAILED_NO_TL	新しい TL への更新に失敗、古い TL なし
7 - TL_FAILED	一般的な障害
8 - TL_FAILED_OLD_ITL	新しい ITL への更新に失敗したが、以前の TL あり
9 - TL_FAILED_OLD_TL	新しい TL への更新に失敗したが、以前の TL あり

[セキュリティのセットアップ (Security Setup)] メニューには、さまざまなセキュリティ設定に関する情報が表示されます。メニューでは、[信頼リスト (Trust List)] メニューにもアクセスでき、CTL ファイルまたは ITL ファイルが電話機にインストールされているかどうかを示します。

次の表に、[セキュリティのセットアップ (Security Setup)] メニューのオプションを示します。

表 3: [セキュリティのセットアップ (Security Setup)] メニュー

オプション	説明	変更の手順
セキュリティ モード	電話機に設定されているセキュリティ モードを表示します。	From Cisco Unified Communications Manager の管理で、[デバイス (Device)] > [電話 (Phone)] を選択します。この設定は [電話の設定 (Phone Configuration)] ウィンドウの [プロトコル固有情報 (Protocol Specific Information)] の部分に表示されます。
LSC	セキュリティ機能で使用する、ローカルで有効な証明書が電話機にインストールされている ([はい (Yes)]) かインストールされていない ([いいえ (No)]) かを示します。	電話機における LSC の詳しい管理方法については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

オプション	説明	変更の手順
信頼リスト	<p>[信頼リスト (Trust List)] は、CTL ファイル、ITL ファイル、および署名済み設定ファイル用のサブメニューを備えています。</p> <p>[CTL ファイル (CTL File)] サブメニューは、CTL ファイルの内容を表示します。[ITL ファイル (ITL File)] サブメニューは、ITL ファイルの内容を表示します。</p> <p>[信頼リスト (Trust List)] メニューには、次の情報が表示されます。</p> <ul style="list-style-type: none"> • [CTL 署名 (CTL Signature)] : CTL ファイルの SHA1 ハッシュ • [Unified CM/TFTP サーバ (Unified CM/TFTP Server)] : 電話機で使用する Cisco Unified Communications Manager と TFTP サーバの名前。このサーバに証明書がインストールされている場合は、証明書アイコンが表示されます。 • [CAPF サーバ (CAPF Server)] : 電話機が使用する CAPF サーバの名前。このサーバに証明書がインストールされている場合は、証明書アイコンが表示されます。 • [SRST ルータ (SRST Router)] : 電話機で使用可能な、信頼できる SRST ルータの IP アドレス。このサーバに証明書がインストールされている場合は、証明書アイコンが表示されます。 	<p>詳細については、重要な証明書のローカルでのセットアップ (8 ページ) を参照してください。</p>
802.1X 認証	この電話機に 802.1X 認証を有効にできます。	802.1X 認証 (31 ページ) を参照してください。

関連トピック

[Cisco Unified Communications Managerのマニュアル](#)

重要な証明書のローカルでのセットアップ

この作業は、認証文字列方式を使用した LSC の設定に適用されます。

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) のセキュリティ設定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 が実行および設定されていること。

これらの設定の詳細については、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。

手順

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

ステップ 2 電話機から、[アプリケーション (Applications)]  を押します。

ステップ 3 [管理設定 (Admin Settings)] > [セキュリティ設定 (Security Setup)] を選択します。

(注) Cisco Unified Communications Manager の管理ページの [電話の設定 (Phone Configuration)] ウィンドウにある設定アクセス フィールドを使用すると、[設定 (Settings)] メニューへのアクセスを制御できます。

ステップ 4 [LSC] を選択し、[選択 (Select)] または [更新 (Update)] を押します。

認証文字列を要求するプロンプトが電話機に表示されます。

ステップ 5 認証コードを入力し、[送信 (Submit)] を押します。

CAPF の設定に応じて、電話機で 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、[セキュリティ設定 (Security Configuration)] メニューの [LSC] オプション フィールドに一連のメッセージが表示されるので、進捗状況をモニタできます。手順が完了すると、電話機に [インストール済み (Installed)] または [未インストール (Not Installed)] と表示されます。

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。

電話機のインストール手順が正常に実行されると、「インストール済み (Installed)」メッセージが表示されます。電話機に「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、電話機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 を削除し、電話機に「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 サーバはこのエラーメッセージをログに記録します。ログを見つけ、エラーメッセージの意味を理解するには、CAPF サーバ ドキュメントを参照してください。


FIPS モードの有効化

手順

-
- ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択し、電話機を見つけます。
 - ステップ 2 [Product Specific Configuration] 領域まで移動します。
 - ステップ 3 [FIPS モード (FIPS Mode)] フィールドを [有効 (Enabled)] に設定します。
 - ステップ 4 [設定の適用 (Apply Config)] を選択します。
 - ステップ 5 保存を選択します。
 - ステップ 6 電話機を再起動します。
-

電話コールのセキュリティ

電話機にセキュリティを実装している場合は、電話スクリーンに表示されるアイコンによって、セキュアな電話コールや暗号化された電話コールを識別できます。また、コールの開始時にセキュリティ トーンが再生される場合は、接続された電話機がセキュアであり保護されているかどうか判断できます。

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。処理中のコールが暗号化されているときは、電話スクリーンのコール時間タイマーの右側にあるコール進捗アイコンが、次のアイコン  に変化します。



-
- (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の開始時にセキュリティ トーンが再生され、接続先の電話機もセキュアな音声を送受信していることを示します。セキュアでない電話機にコールが接続されると、セキュリティ トーンは再生されません。



-
- (注) セキュアなコールは、2 台の電話機間でのみサポートされます。電話会議や共有回線などの一部の機能は、セキュアなコールが設定されているときは使用できません。
-


Cisco Unified Communications Manager で電話機をセキュア（暗号化および信頼された）として設定した場合、その電話機には「保護」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、保護された電話機は、コールの初めに通知トーンを再生するように設定できます。

- [保護されたデバイス (Protected Device)] : セキュアな電話機のステータスを保護に変更するには、Cisco Unified Communications Manager の管理ページの [電話の設定 (Phone Configuration)] ウィンドウにある [保護されたデバイス (Protected Device)] チェックボックスをオンにします ([デバイス (Device)] > [電話 (Phone)])。
- [セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] : 保護された電話機で、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)] 設定を [はい (True)] に設定します。デフォルトでは、[セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] は [いいえ (False)] に設定されます。このオプションは、Cisco Unified Communications Manager の管理 ([システム (System)] > [サービス パラメータ (Service Parameters)]) で設定します。サーバを選択してから、Unified Communications Manager サービスを選択します。[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウで、[機能 - セキュア トーン (Feature - Secure Tone)] 領域内にあるオプションを選択します。デフォルトは False です。

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電話機で会議を開始します。
2. Cisco Unified Communications Manager が、コールにセキュアな会議ブリッジを割り当てます。
3. 参加者が追加されると、Cisco Unified Communications Manager は、各電話機のセキュリティ 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. 電話機に会議コールのセキュリティ レベルが表示されます。セキュアな会議では、電話機の画面の [会議 (Conference)] の右側にセキュア アイコン  が表示されます。



- (注) セキュアなコールは、2台の電話機の間でサポートされます。保護された電話機では、セキュアなコールが設定されている場合、会議コール、シェアドライン、エクステンション モビリティなどの一部の機能を使用できません。

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 4: 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	ミーティング	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さず、コールを拒否します (Does not meet security level, call rejected)」というメッセージが表示されます。
セキュア	ミーティング	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。

セキュアな電話コールの識別

ユーザの電話機および相手側の電話機でセキュアなコールが設定されている場合にセキュアなコールが確立されます。相手側の電話機は、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。セキュアなコールは2台の電話機間でのみ形成できます。セキュアな会議ブリッジのセットアップ後、電話会議ではセキュアなコールがサポートされます。

セキュアなコールは、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電話機（セキュリティモードで保護された電話機）でコールを開始します。
2. 電話スクリーンにセキュアアイコン  が表示されます。このアイコンは、この電話機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. そのコールが別のセキュアな電話機に接続された場合は、ユーザにセキュリティトーンが聞こえ、通話の両端が暗号化および保護されていることを示します。コールが非セキュアな電話機に接続された場合は、ユーザにはセキュリティトーンが聞こえません。



- (注) セキュアなコールは、2台の電話機の間でサポートされます。保護された電話機では、セキュアなコールが設定されている場合、会議コール、シェアドライン、エクステンションモビリティなどの一部の機能を使用できません。

保護された電話機だけで、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。保護されていない電話機ではトーンは聞こえません。コール中にコール全体のステータスが変化すると、それに従って通知トーンも変化し、保護された電話機は対応するトーンを再生します。

このような状況にない場合、保護された電話機はトーンを再生しません。

- [セキュア インディケーション トーンの再生 (Play Secure Indication Tone)] オプションが有効になっている場合
 - 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、電話機はセキュア 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場合、電話機は、非セキュアのインディケーション トーンを再生します (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。

割り込みの暗号化

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。

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。

WLAN セキュリティ

通信圏内にあるすべての WLAN デバイスは他の WLAN トラフィックをすべて受信できるため、WLAN 内の音声通信の保護は重要です。侵入者による音声トラフィックの操作や傍受を防止するため、Cisco SAFE セキュリティ アーキテクチャは、Cisco IP 電話 と Cisco Aironet AP を

サポートします。ネットワーク内のセキュリティの詳細については、
http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html を参照してください。

Cisco Wireless IP テレフォニー ソリューションは、ワイヤレス Cisco IP 電話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。

- オープン認証：オープン システムでは、任意のワイヤレス デバイスが認証を要求できます。要求を受けた AP は、任意のリクエストまたはユーザのリスト上にあるリクエストだけに認証を与える場合があります。ワイヤレス デバイスと AP との間の通信は暗号化されない可能性もあります。暗号化される場合、デバイスは有線と同等のプライバシー（WEP）キーを使用してセキュリティを提供できます。WEP を使用しているデバイスは、WEP を使用している AP での認証だけを試みます。
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）
 認証：このクライアント サーバのセキュリティ アーキテクチャは、AP と、Cisco Access Control Server（ACS）などの RADIUS サーバとの間の Transport Level Security（TLS）トンネル内の EAP トランザクションを暗号化します。

TLS トンネルでは、クライアント（電話機）と RADIUS サーバの間の認証に Protected Access Credential（PAC）が使用されます。サーバは Authority ID（AID）をクライアント（電話機）に送信します。それを受けてクライアントは適切な PAC を選択します。クライアント（電話機）は PAC-Opaque を RADIUS サーバに返します。サーバは、プライマリキーで PAC を復号します。これで両方のエンドポイントに同じ PAC キーが含まれ、TLS トンネルが構築されます。EAP-FAST では、自動 PAC プロビジョニングがサポートされていますが、RADIUS サーバ上で有効にする必要があります。



- (注) Cisco ACS での PAC の有効期限は、デフォルトで 1 週間です。電話機に期限切れの PAC が存在する場合、電話機が新しい PAC を取得するまでの間は、RADIUS サーバでの認証に比較的長い時間がかかります。PAC プロビジョニングの遅延を回避するには、ACS サーバまたは RADIUS サーバで PAC の有効期間を 90 日以上に設定します。

- 拡張認証プロトコル-トランスポート層セキュリティ（EAP-TLS）認証：EAP-TLS では、認証とネットワークアクセスにクライアント証明書が必要です。有線 EAP-TLS の場合、クライアント証明書は電話機の MIC または LSC のいずれかです。LSC は、有線 EAP-TLS に推奨されるクライアント認証証明書です。
- Protected Extensible Authentication Protocol（PEAP）：クライアント（電話機）と RADIUS サーバ間の、シスコ独自のパスワードベースの相互認証方式です。Cisco IP 電話は、ワイヤレス ネットワークでの認証に PEAP を使用できます。PEAP-MSCHAPV2 と PEAP-GTC の両方の認証メカニズムがサポートされます。

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 および電話機に格納されている WPA 事前共有キーよりも高いセキュリティを提供します。
- **高速安全ローミング:** RADIUS サーバとワイヤレス ドメインサーバ (WDS) 上の情報を使用してキーを管理および認証します。WDS は、高速でセキュアな再認証用に、CKKM 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。Cisco IP 電話 8800 シリーズは 802.11r (FT) をサポートしています。高速セキュアローミングを可能にするために、11r (FT) と CKKM の両方がサポートされています。しかしスコは 802.11r (FT) 無線方式を利用することを強く推奨します。

WPA/WPA2 および CKKM では、暗号化キーは電話機に入力されず、AP と電話機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、各電話機に入力する必要があります。

音声トラフィックの安全性を確保するため、Cisco IP 電話 では、暗号化方式として WEP、TKIP、および Advanced Encryption Standards (AES) をサポートします。暗号化にこれらのメカニズムを使用すると、AP と Cisco IP 電話 との間で、シグナリング SIP パケットと音声リアルタイム トランスポート プロトコル (RTP) パケットの両方が暗号化されます。

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、電話機で設定された WEP キーと AP で設定された WEP キーが一致する必要があります。Cisco IP 電話 は、40 ビット暗号化または 128 ビット暗号化を使用し、電話機および AP で静的なままの WEP キーをサポートしています。

EAP と CKKM の認証では、暗号化に WEP キーを使用できます。RADIUS サーバは WEP キーを管理し、すべての音声パケットの暗号化を認証した後で一意のキーを AP に渡します。そのため、次の WEP キーを各認証で変更できます。

TKIP

WPA と CKKM 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。AES は、128 ビットサイズの暗号ブロック連鎖 (CBC) 暗号化を使用し、最小のキー サイズとして 128、192、および 256 ビットのキーをサポートします。Cisco IP 電話 は 256 ビットのキー サイズをサポートします。



(注) Cisco IP 電話 は、CMIC による Cisco Key Integrity Protocol (CKIP) をサポートしません。

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

一部の認証方式では、特定のタイプの暗号化が必要です。オープン認証では、セキュリティを高めるために、暗号化で静的 WEP を使用できます。ただし、共有キー認証を使用している場合は、暗号化に静的 WEP を設定し、電話機で WEP キーを設定する必要があります。



(注)

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

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

表 5: 認証方式と暗号化方式

Cisco IP 電話の設定	AP の設定			
Security Mode	セキュリティ	Key Management	暗号化	高速ローミング
なし	なし	なし	なし	該当なし
WEP	Static WEP	スタティック	WEP	該当なし
PSK	PSK	WPA	TKIP	なし
		WPA2	AES	FT
EAP-FAST	EAP-FAST	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM
EAP-TLS	EAP-TLS	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM

Cisco IP 電話の設定	AP の設定			
PEAP-MSCHAPV2	PEAP-MSCHAPV2	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM
PEAP-GTC	PEAP-GTC	802.1x	WEP	CCKM
		WPA	TKIP	CCKM
		WPA2	AES	FT、CCKM

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

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

認証モードのセットアップ

このプロファイルの認証モードを選択するには、次の手順を実行します。

手順

ステップ 1 設定するネットワーク プロファイルを選択します。

ステップ 2 認証モードを選択します。

(注) 選択したモードによっては、[ワイヤレスセキュリティ (Wireless Security)] または [ワイヤレス暗号化 (Wireless Encryption)] で追加オプションを設定する必要があります。詳細については、[WLAN セキュリティ \(13 ページ\)](#) を参照してください。

ステップ 3 [保存 (Save)] をクリックして変更を加えます。

ワイヤレス セキュリティ クレデンシャル

ネットワークで EAP-FAST および PEAP がユーザ認証に使用されている場合、リモート認証ダイヤルインユーザサービス (RADIUS) と電話機が必要な場合にユーザ名およびパスワードの両方を設定する必要があります。



(注) ネットワーク内のドメインを使用している場合、`domain\username` の形式でユーザ名とドメイン名を入力する必要があります。

次の操作によって、既存の Wi-Fi パスワードがクリアされる可能性があります。

- 無効なユーザ ID またはパスワードを入力する
- EAP タイプが PEAP-MSCHAPV2 または PEAP-GTC に設定されているときに、無効または期限切れのルート CA 証明書をインストールする
- 新しい EAP タイプに電話機を変更する前に、電話機によって使用される RADIUS サーバの EAP タイプを無効にする

EAP タイプを変更するには、示されている順序で以下を実行します。

- RADIUS の新しい EAP タイプを有効にします。
- 電話機の EAP タイプを新しい EAP タイプに変更します。

新しい EAP タイプが RADIUS サーバで有効にされるまで、電話機に設定された現在の EAP タイプを保持します。新しい EAP タイプが RADIUS サーバで有効にされたら、電話機の EAP タイプを変更できます。すべての電話機が新しい EAP タイプに変更されたら、必要に応じて前の EAP タイプを無効にすることができます。

ユーザ名とパスワードのセットアップ

ネットワーク プロファイルのユーザ名またはパスワードを入力または変更するには、RADIUS サーバに設定されているものと同じユーザ名およびパスワード文字列を使用する必要があります。ユーザ名またはパスワードエントリの最大長は、64 文字です。

[ワイヤレス セキュリティ クレデンシャル (Wireless Security Credentials)] でユーザ名とパスワードをセットアップするには、次の手順を実行します。

手順

-
- ステップ 1** ネットワーク プロファイルを選択します。
 - ステップ 2** [ユーザ名 (UserName)] フィールドに、このプロファイルのネットワーク ユーザ名を入力します。
 - ステップ 3** [パスワード (Password)] フィールドに、このプロファイルのネットワーク パスワード文字列を入力します。
 - ステップ 4** [保存 (Save)] をクリックして変更を加えます。
-

事前共有キーの設定

次のセクションを使用して、事前共有キーを設定するときにガイドしてください。

事前共有キーの形式

Cisco IP 電話は、ASCII 形式と 16 進数形式をサポートしています。WPA 事前共有キーを設定している場合は、次の形式のいずれかを使用する必要があります。

16 進数

16 進数のキーの場合は、64 の 16 進数（0 ～ 9、A ～ F）を入力します。たとえば、AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C のように入力します。

ASCII

ASCII キーの場合は、0 ～ 9、A ～ Z（大文字と小文字）、すべての記号を使用した文字列を、長さ 8 ～ 63 文字で入力します。たとえば、GREG12356789ZXYW のように入力します。

PSK のセットアップ

[ワイヤレス クレデンシャル（Wireless Credentials）] 領域で PSK をセットアップするには、次の手順を実行します。

手順

-
- ステップ 1** [自動（AKM）（Auto（AKM））] を使用するネットワーク プロファイルを選択し、WPA 事前共有キーまたは WPA2 事前共有キーをイネーブルにします。
 - ステップ 2** [キーの種類] 領域に適切なキーを入力します。
 - ステップ 3** [パスフレーズ/事前共有キー（Passphrase/Pre-shared key）] フィールドに ASCII 文字列または 16 進数を入力します。
 - ステップ 4** [保存（Save）] をクリックして変更を加えます。
-

ワイヤレス暗号化

ワイヤレス ネットワークが WEP 暗号化を使用しており、認証モードを [オープン+WEP（Open+WEP）] または [共有キー+WEP（Shared Key+WEP）] に設定している場合は、ASCII WEP キーまたは 16 進数 WEP キーを入力する必要があります。

電話機の WEP キーとアクセス ポイントに割り当てられた WEP キーは一致する必要があります。Cisco IP 電話 および Cisco Aironet アクセス ポイントは、40 ビットおよび 128 ビットの両方の暗号キーをサポートしています。

WEP キーの形式

WEP キーの設定時には、次の形式のいずれかを使用する必要があります。

16 進数

16 進数キーの場合は、次のいずれかのキー サイズを使用します。

40 ビット

16 進数（0 ～ 9、A ～ F）を使用する 10 桁の暗号化キー文字列を入力します。たとえば、ABCD123456 のように入力します。

128 ビット

16 進数（0～9、A～F）を使用する 26 桁の暗号化キー文字列を入力します。たとえば、AB123456789CD01234567890EF のように入力します。

ASCII

ASCII キーの場合は、0～9、A～Z（大文字と小文字）およびすべての記号を使用する、次のいずれかのキー サイズの文字列を入力します。

40 ビット

5 文字の文字列を入力します。たとえば、GREG5 のように入力します。

128 ビット

13 文字の文字列を入力します。たとえば、GREGSSECRET13 のように入力します。

WEP キーのセットアップ

WEP キーを設定するには、次の手順を実行します。

手順

ステップ 1 [オープン+WEP（Open+WEP）] または [共有+WEP（Shared+WEP）] を使用するネットワーク プロファイルを選択します。

ステップ 2 [キーの種類] 領域に適切なキーを入力します。

ステップ 3 [キー サイズ（Key Size）] 領域で、次の文字形式のいずれかを選択します。

- 40
- 128

ステップ 4 選択したキー タイプとキー サイズに基づいて、[暗号キー（Encryption Key）] フィールドに適切なキー文字列を入力します。 [WEP キーの形式（19 ページ）](#) を参照してください。

ステップ 5 [保存（Save）] をクリックして変更を加えます。

Microsoft 証明書サービスを使用した CA 証明書のエクスポート

ACS から認証サーバルート証明書をエクスポートします。追加情報については、CA または RADIUS のドキュメントを参照してください。

製造元でインストールされる証明書

シスコでは、工場出荷時に製造元でインストールされる証明書（MIC）を電話機に組み込んでいます。

EAP-TLS 認証時には、ACS サーバは電話機の信頼度を確認し、電話機は ACS サーバの信頼度を確認する必要があります。

MICを確認するには、製造元ルート証明書と製造元認証局（CA）証明書を Cisco IP 電話 からエクスポートし、Cisco ACS サーバにインストールする必要があります。これらの2つの証明書は、Cisco ACS サーバによる MIC の確認に使用される、信頼証明書チェーンの一部です。

Cisco ACS 証明書を確認するには、Cisco ACS サーバの信頼される下位証明書（ある場合）とルート証明書（CA が作成）をエクスポートし、電話機にインストールする必要があります。これらの証明書は、ACS サーバからの証明書の信頼度を確認するために使用される信頼証明書チェーンの一部です。

ユーザがインストールした証明書

ユーザがインストールした証明書を使用するには、証明書署名要求（CSR）が生成されて、承認のために CA へ送信されている必要があります。ユーザ証明書は、CSR なしで CA によって生成することもできます。

EAP-TLS 認証時には、ACS サーバは電話機の信頼度を確認し、電話機は ACS サーバの信頼度を確認します。

ユーザがインストールした証明書の信頼性を確認するには、ユーザ証明書を承認した CA からの信頼される下位証明書（ある場合）とルート証明書を Cisco ACS サーバにインストールする必要があります。これらの証明書は、ユーザがインストールした証明書の信頼度を確認するために使用される信頼証明書チェーンの一部です。

Cisco ACS 証明書を確認するには、Cisco ACS サーバの信頼される下位証明書（ある場合）とルート証明書（CA が作成）をエクスポートし、エクスポートした証明書を電話機にインストールします。これらの証明書は、ACS サーバからの証明書の信頼度を確認するために使用される信頼証明書チェーンの一部です。

EAP-TLS 認証証明書のインストール

EAP-TLS の認証証明書をインストールするには、次の手順を実行します。

手順

ステップ 1 電話機の Web ページで、電話機に Cisco Unified Communications Manager の日付と時刻を設定します。

ステップ 2 製造元でインストールされる証明書（MIC）を使用する場合：

- a) 電話機の Web ページで、CA ルート証明書と製造元 CA 証明書をエクスポートします。
- b) Internet Explorer で、Cisco ACS サーバに証明書をインストールし、信頼リストを編集します。
- c) ルート CA を電話機にインポートします。

詳細については、以下を参照してください。

- [ACS での証明書のエクスポートおよびインストール](#)（22 ページ）
- [Microsoft 証明書サービスを使用した CA 証明書のエクスポート](#)（23 ページ）

ステップ 3 ACS 設定ツールを使用して、ユーザ アカウントを設定します。

詳細については、以下を参照してください。

- [ACS ユーザ アカウントのセットアップと証明書のインストール](#) (25 ページ)
- 『*User Guide for Cisco Secure ACS for Windows*』 (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>)

Set Date and Time

EAP-TLS で使用される証明書ベースの認証では、Cisco IP 電話の内部クロックが正しく設定されている必要があります。電話機の日付と時刻は、Cisco Unified Communications Manager に登録されたときに変わる場合があります。



(注) 新しいサーバ認証証明書が要求され、ローカル時間がグリニッジ標準時 (GMT) よりも遅れている場合は、認証証明書の検証に失敗します。GMT よりも先にローカルの日付と時刻を設定することをお勧めします。

電話機を正しいローカルの日付と時刻に設定するには、次の手順を実行します。

手順

ステップ 1 左側のナビゲーション ペインで [日付および時刻 (Date & Time)] を選択します。

ステップ 2 [現在の電話機の日時 (Current Phone Date & Time)] フィールドの設定値が [ローカルの日時 (Local Date & Time)] フィールドと異なる場合は、[電話機のローカルの日時を設定 (Set Phone to Local Date & Time)] をクリックします。

ステップ 3 [電話機の再起動 (Phone Restart)] をクリックし、次に [OK] をクリックします。

ACS での証明書のエクスポートおよびインストール

MIC を使用するには、製造元ルート証明書と製造元 CA 証明書をエクスポートし、Cisco ACS サーバにインストールします。

製造元ルート証明書と製造元 CA 証明書を ACS サーバにエクスポートするには、次の手順を実行します。

手順

ステップ 1 電話機の Web ページで、[証明書 (Certificates)] を選択します。

ステップ 2 製造元ルート証明書の横にある [エクスポート (Export)] をクリックします。

ステップ 3 証明書を保存し、それを ACS サーバにコピーします。

ステップ 4 製造元 CA 証明書に関して、ステップ 1 と 2 を繰り返します。

ステップ 5 [ACS サーバシステム設定 (ACS Server System Configuration)] ページで、各証明書へのファイルパスを指定し、証明書をインストールします。

(注) ACS 設定ツールの使用方法の詳細については、ACS のオンライン ヘルプまたは『*User Guide for Cisco Secure ACS for Windows*』 (<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html>) を参照してください。

ステップ 6 [証明書信頼リスト (CTL) の編集 (Edit the Certificate Trust List (CTL))] ページで、ACS によって信頼されている証明書を追加します。

ACS 証明書のエクスポート方法

ACS からエクスポートする証明書のタイプによって、次の方式のいずれかを使用します。

- ユーザがインストールした証明書または ACS 証明書が署名された ACS サーバから CA 証明書をエクスポートするには、[Microsoft 証明書サービスを使用した CA 証明書のエクスポート \(23 ページ\)](#) を参照してください。
- 自己署名証明書を使用する ACS サーバから CA 証明書をエクスポートするには、[Internet Explorer を使用して ACS から CA 証明書をエクスポートする \(24 ページ\)](#) を参照してください。

Microsoft 証明書サービスを使用した CA 証明書のエクスポート

ユーザがインストールした証明書または ACS 証明書が署名された ACS サーバから CA 証明書をエクスポートする場合は、この方式を使用します。

[Microsoft 証明書サービス (Microsoft Certificate Services)] Web ページを使用して CA 証明書をエクスポートするには、次の手順を実行します。

手順

ステップ 1 [Microsoft 証明書サービス (Microsoft Certificate Services)] Web ページで、[CA 証明書、証明書チェーン、または CRL のダウンロード (Download a CA certificate, certificate chain or CRL)] をクリックします。

ステップ 2 次のページで、テキストボックス内の現在 CA 証明書を強調表示し、[エンコード方式 (Encoding Method)] として [DER] を選択し、[CA 証明書のダウンロード (Download CA certificate)] をクリックします。

ステップ 3 CA 証明書を保存します。

Internet Explorer を使用して ACS から CA 証明書をエクスポートする

自己署名証明書を使用する ACS サーバから CA 証明書をエクスポートする場合は、この方式を使用します。

Internet Explorer を使用して ACS サーバから証明書をエクスポートするには、次の手順を実行します。

手順

-
- ステップ 1** Internet Explorer で [ツール (Tools)] > [インターネット オプション (Internet Options)] > を選択し、[コンテンツ (Content)] タブをクリックします。
 - ステップ 2** [証明書 (Certificates)] 下で、[証明書 (Certificates)] をクリックし、[信頼されたルート証明機関 (Trusted Root Certification Authorities)] タブをクリックします。
 - ステップ 3** ルート証明書を強調表示し、[エクスポート (Export)] をクリックします。[証明書のエクスポート ウィザード (Certificate Import Wizard)] が表示されます。
 - ステップ 4** [次へ (Next)] をクリックします。
 - ステップ 5** 次のウィンドウで [DER encoded binary X.509 (.CER)] を選択し、[次へ (Next)] をクリックします。
 - ステップ 6** 証明書の名前を指定し、[次へ (Next)] をクリックします。
 - ステップ 7** 電話機にインストールする CA 証明書を保存します。
-

ユーザがインストールした証明書の要求およびインポート

証明書を要求して電話機にインストールするには、次の手順を実行します。

手順

-
- ステップ 1** 電話機の Web ページで、EAP-TLS を使用しているネットワーク プロファイルを選択し、[EAP-TLS 証明書 (EAP-TLS Certificate)] フィールドで [ユーザによってインストールされる証明書 (User Installed)] を選択します。
 - ステップ 2** [Certificates] をクリックします。
 [ユーザ証明書のインストール (User Certificate Installation)] ページの [一般名 (Common Name)] フィールドは、ACS サーバのユーザ名と一致する必要があります。
 (注) [一般名 (Common Name)] フィールドは、必要に応じて編集できます。編集した場合も、ACS サーバのユーザ名と一致していることを確認してください。[ACS ユーザ アカウントのセットアップと証明書のインストール \(25 ページ\)](#) を参照してください。

- ステップ3** 証明書に表示する情報を入力し、[送信 (Submit)] をクリックして証明書署名要求 (CSR) を生成します。

認証サーバルート証明書のインストール

電話機に認証サーバルート証明書をインストールするには、次の手順を実行します。

手順

- ステップ1** ACS から認証サーバルート証明書をエクスポートします。 [ACS 証明書のエクスポート方法 \(23 ページ\)](#) を参照してください。
- ステップ2** 電話機の Web ページに移動し、[証明書 (Certificates)] を選択します。
- ステップ3** 認証サーバルート証明書の横にある [インポート (Import)] をクリックします。
- ステップ4** 電話機を再起動します。

ACS ユーザ アカウントのセットアップと証明書のインストール

ユーザアカウント名を設定し、電話機の MIC ルート証明書を ACS にインストールするには、次の手順を実行します。



- (注) ACS 設定ツールの使用方法の詳細については、ACS のオンライン ヘルプまたは『*User Guide for Cisco Secure ACS for Windows*』を参照してください。

手順

- ステップ1** ACS 設定ツールの [ユーザ セットアップ (User Setup)] ページで、電話機のユーザ アカウント名を作成します (未設定の場合)。
- 通常、ユーザ名には末尾に電話機の MAC アドレスを含めます。EAP-TLS の場合は、パスワードは不要です。
- (注) ユーザ名が、[ユーザ証明書のインストール (User Certificate Installation)] ページの [一般名 (Common Name)] フィールドと一致していることを確認してください。
[ユーザがインストールした証明書の要求およびインポート \(24 ページ\)](#) を参照してください。
- ステップ2** [システム設定 (System Configuration)] ページの [EAP-TLS] セクションで次のフィールドをイネーブルにします。
- **Allow EAP-TLS**
 - **証明書 CN の比較 (Certificate CN comparison)**

- ステップ 3** [ACS 認証局のセットアップ (ACS Certification Authority Setup)] ページで、製造元ルート証明書と製造元 CA 証明書を ACS サーバに追加します。
- ステップ 4** [ACS 証明書信頼リスト (ACS Certificate Trust List)] で製造元ルート証明書と製造元 CA 証明書の両方をイネーブルにします。

PEAP の設定

Protected Extensible Authentication Protocol (PEAP) は、サーバ側の公開キー証明書を使用してクライアントを認証するために、クライアントと認証サーバの間に暗号化された SSL/TLS トンネルを構築します。

Cisco IP 電話 8865 は、SCEP 経由または手動インストール方法のいずれかでインストールできるサーバ証明書を 1 つだけサポートしていますが、両方はサポートしていません。電話機は TFTP による証明書のインストール方法をサポートしていません。



- (注) 認証サーバの検証は、認証サーバ証明書をインポートすることによってイネーブルにできません。

事前準備

電話機の PEAP 認証を設定する前に、次の Cisco Secure ACS 要件を満たしていることを確認します。

- ACS ルート証明書がインストールされていること。
- 証明書をインストールして、PEAP のサーバ検証を有効にすることもできます。サーバ証明書をインストールすると、サーバ検証が自動的に有効になります。
- [EAP-MSCHAPv2 を許可 (Allow EAP-MSCHAPv2)] 設定がイネーブルになっていること。
- ユーザアカウントとパスワードが設定されていること。
- パスワード認証の場合は、ローカル ACS データベースまたは外部データベース (Windows または LDAP) を使用できること。

PEAP 認証の有効化

手順

- ステップ 1** [電話の設定(Phone Configuration)] Web ページで、認証モードとして [PEAP] を選択します
- ステップ 2** ユーザ名とパスワードを入力します。

ワイヤレス LAN セキュリティ

Wi-Fi をサポートするシスコの電話機には追加のセキュリティ要件があり、追加の設定が必要になります。これらの追加手順には、証明書のインストール、および電話機と Cisco Unified Communications Manager でのセキュリティの設定が含まれます。

追加情報については、『*Security Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco IP 電話の管理ページ

Wi-Fi をサポートするシスコの電話機には、他の電話機のページとは異なる特別な Web ページがあります。Simple Certificate Enrollment Protocol (SCEP) を使用できない場合に、電話機のセキュリティを設定するため、これらの特別な Web ページを使用します。これらのページを使用して、セキュリティ証明書を手動で電話機にインストールしたり、セキュリティ証明書をダウンロードしたり、電話機の日時を手動で設定したりします。

これらの Web ページには、デバイス情報、ネットワーク設定、ログ、統計情報など、他の電話機の Web ページに表示されるものと同じ情報が表示されます。

関連トピック

[Cisco IP 電話の Web ページ](#)

電話機の管理ページの設定

管理 Web ページは、電話機が工場から出荷された時点で有効になっていて、パスワードは「Cisco」に設定されています。ただし、電話機を Cisco Unified Communications Manager に登録する場合は、管理 Web ページを必ず有効にし、新しいパスワードを設定する必要があります。

電話機を登録した後、Web ページを初めて使用する前に、この Web ページを有効にして、サインイン クレデンシャルを設定します。

有効にすると、管理 Web ページには、HTTPS ポート 8443 (<https://x.x.x.x:8443> (x.x.x.x は電話機の IP アドレスです)) でアクセスできます。

始める前に

管理 Web ページを有効にする前に、パスワードを決定します。パスワードには文字と数字を任意に組み合わせて指定できますが、長さは 8 ～ 127 文字の間にする必要があります。

ユーザ名は admin に固定されています。

手順

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

ステップ 2 電話機を特定します。

電話管理の Web ページにアクセスします。


- ステップ 3 [プロダクト固有の設定] の項で、[Web 管理 (Web Admin)] を [有効 (Enabled)] に設定します。
- ステップ 4 [管理パスワード (Admin Password)] フィールドにパスワードを入力します。
- ステップ 5 [保存 (Save)] を選択し、[OK] をクリックします。
- ステップ 6 [設定の適用 (Apply Config)] を選択し、[OK] をクリックします。
- ステップ 7 電話機を再起動します。

電話管理の Web ページにアクセスします。

管理 Web ページにアクセスするとき、管理ポートを指定する必要があります。

手順

ステップ 1 次のように電話機の IP アドレスを取得します。

- Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択し、電話機を見つけます。Cisco Unified Communications Manager に登録されている電話機の IP アドレスが、[Find and List Phones] ウィンドウと [Phone Configuration] ウィンドウの上部に表示されます。
- 電話機で [アプリケーション (Applications)]  を押して、[電話の情報] を選択し、[IPv4 アドレス (IPv4 address)] フィールドまでスクロールします。

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 Cisco IP 電話の IP アドレスです。

https://<IP_address>:8443

ステップ 3 [Password] フィールドにパスワードを入力します。

ステップ 4 [送信 (Submit)] をクリックします。

電話機の管理 Web ページからユーザ証明書をインストールする

Simple Certificate Enrollment Protocol (SCEP) を使用できない場合、電話機にユーザ証明書を手動でインストールすることができます。

製造元でインストールされる証明書 (MIC) を EAP-TLS 用のユーザ証明書として使用できます。

ユーザ証明書をインストールした後、RADIUS サーバの信頼リストに追加する必要があります。

始める前に

電話機のユーザ証明書をインストールするには、その前に以下を用意する必要があります。

- PC に保存されたユーザ証明書。証明書は PKCS #12 形式である必要があります。

- 証明書の抽出パスワード。

手順

-
- ステップ 1** 電話機の管理 Web ページで、[証明書 (Certificates)] を選択します。
 - ステップ 2** [ユーザインストール (User install)] フィールドを見つけて [インストール (Install)] をクリックします。
 - ステップ 3** PC の証明書を参照します。
 - ステップ 4** [抽出パスワード (Extract password)] フィールドに、証明書の抽出パスワードを入力します。
 - ステップ 5** [アップロード (Upload)] をクリックします。
 - ステップ 6** アップロードが完了したら、電話機を再起動します。
-

電話機の管理 Web ページから認証サーバ証明書をインストールする

Simple Certificate Enrollment Protocol (SCEP) を使用できない場合、電話機に認証サーバ証明書を手動でインストールすることができます。

RADIUS サーバ証明書を発行したルート CA 証明書は、EAP-TLS 用にインストールする必要があります。

始める前に

電話機に証明書をインストールするには、その前に認証サーバ証明書を PC に保存する必要があります。証明書は PEM (Base 64) または DER 形式でエンコードする必要があります。

手順

-
- ステップ 1** 電話機の管理 Web ページで、[証明書 (Certificates)] を選択します。
 - ステップ 2** [認証サーバ CA (管理 Web ページ) (Authentication server CA (Admin webpage))] フィールドを見つけて [インストール (Install)] をクリックします。
 - ステップ 3** PC の証明書を参照します。
 - ステップ 4** [アップロード (Upload)] をクリックします。
 - ステップ 5** アップロードが完了したら、電話機を再起動します。

複数の証明書をインストールする場合は、電話機を再起動する前に、すべての証明書をインストールします。

電話機の管理 Web ページからセキュリティ証明書を手動で削除する

Simple Certificate Enrollment Protocol (SCEP) を使用できない場合、電話機からセキュリティ証明書を手動で削除することができます。

手順

ステップ 1 電話機の管理 Web ページで、[証明書 (Certificates)] を選択します。

ステップ 2 [Certificates] ページで証明書を見つけます。

ステップ 3 [削除 (Delete)] をクリックします。

ステップ 4 削除プロセスが完了したら、電話機を再起動します。

手動での電話機の日時の設定

証明書ベースの認証では、電話機に正しい日時を表示する必要があります。認証サーバは、電話機の日時を証明書の失効日と照合します。電話機とサーバの日時が一致しないと、電話機は動作を停止します。

電話機がネットワークから正しい情報を受信していない場合、次の手順を使用して電話機の日時を手動で設定します。

手順

ステップ 1 電話機の管理 Web ページで、[Date & Time] までスクロールします。

ステップ 2 次のいずれかの選択肢を実行します。

- ローカルサーバに電話機を同期する場合は、[電話機のローカルの日時を設定 (Set Phone to Local Date & Time)] をクリックします。
- [日付および時刻の指定 (Specify Date & Time)] フィールドで、メニューを使用して、月、日、年、時、分、秒を選択し、[電話機を特定の日に設定 (Set Phone to Specific Date & Time)] をクリックします。

SCEP セットアップ

Simple Certificate Enrollment Protocol (SCEP) は、証明書の自動プロビジョニングおよび更新の標準です。これにより、電話機に証明書を手動でインストールせずに済みます。

SCEP プロダクト固有の設定パラメータの設定

電話機の Web ページで次の SCEP パラメータを設定する必要があります。

- RA IP アドレス
- SCEP サーバのルート CA 証明書の SHA-1 または SHA-256 フィンガープリント

Cisco IOS の登録局 (RA) は、SCEP サーバへのプロキシとして機能します。電話機の SCEP クライアントは、Cisco Unified Communications Manager からダウンロードされたパラメータを

使用します。パラメータを設定すると、電話機から RA に SCEP getcs 要求が送信され、定義されたフィンガープリントを使用してルート CA 証明書が検証されます。

手順

-
- ステップ 1 Cisco Unified Communications Manager Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
 - ステップ 2 電話機を特定します。
 - ステップ 3 [Product Specific Configuration Layout] 領域までスクロールします。
 - ステップ 4 [WLAN SCEP Server] チェックボックスをオンにして、SCEP パラメータをアクティブ化します。
 - ステップ 5 [WLAN Root CA Fingerprint (SHA256 or SHA1)] チェックボックスをオンにして、SCEP QED パラメータをアクティブ化します。
-

Simple Certificate Enrollment Protocol サーバのサポート

Simple Certificate Enrollment Protocol (SCEP) サーバを使用する場合、サーバはユーザとサーバ証明書を自動的に維持できます。SCEP サーバで、次のように SCEP 登録エージェント (RA) を設定します。

- PKI トラスト ポイントとして機能する
- PKI RA として機能する
- RADIUS サーバを使用してデバイス認証を実行する

詳細については、SCEP サーバのマニュアルを参照してください。

802.1X 認証

Cisco IP 電話 は 802.1X 認証をサポートします。

Cisco IP 電話 と Cisco Catalyst スイッチは、従来 Cisco Discovery Protocol (CDP) を使用して互いを識別し、VLAN 割り当てやインライン所要電力などのパラメータを決定します。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 IP 電話は、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 IP 電話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、IP フォン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 IP 電話はまた、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 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、IP フォン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。

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 IP 電話:** 電話機は、ネットワークへのアクセス要求を開始します。Cisco IP 電話には、802.1x サプリカントが含まれています。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。
- **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。


802.1X を設定するには、次の手順を実行する必要があります。

- **電話機で 802.1X 認証をイネーブルにする前に、他のコンポーネントを設定します。**
- **PC ポートの設定：**802.1X 標準では VLAN 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まります。
 - **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 IP 電話はプロキシ 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、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。

802.1X 認証へのアクセス

次の手順に従って、802.1X 認証の設定にアクセスできます。

手順

- ステップ 1 [アプリケーション（Applications）] ボタン  を押します。
- ステップ 2 [管理者設定（Admin settings）] > [セキュリティのセットアップ（Security Setup）] > [802.1X 認証（802.1X Authentication）] を選択します。
- ステップ 3 [\[802.1X 認証（802.1X Authentication）\] オプション（33 ページ）](#) の説明に従ってオプションを設定します。
- ステップ 4 メニューを終了するには、[終了（Exit）] を押します。

[802.1X 認証（802.1X Authentication）] オプション

次の表では、802.1X 認証オプションについて説明します。

表 6: 802.1X 認証の設定

オプション	説明	変更の手順
デバイス認証	802.1X 認証が有効かどうかを示します。 <ul style="list-style-type: none">• [有効（Enabled）]：電話機は 802.1X 認証を使用してネットワーク アクセスを要求します。• [無効（Disabled）]：デフォルト設定です。電話機は、CDP を使用して VLAN およびネットワーク アクセスを取得します。	[デバイス認証（Device Authentication）フィールドの設定（34 ページ）] してください。
Transaction Status （トランザクションステータス）	[状態（State）]：802.1x 認証の状態を表示します。 <ul style="list-style-type: none">• [切断済み（Disconnected）]：802.1x 認証が電話機に設定されていないことを示します。• [認証済み（Authenticated）]：電話が認証されたことを示します。• [保留（Held）]：認証プロセスが進行中であることを示します。 [プロトコル（Protocol）]：802.1x 認証に使用される EAP 方式を表示します（EAP-FAST または EAP-TLS である場合があります）。	表示のみ。変更不可。

[デバイス認証 (Device Authentication)] フィールドの設定

手順

ステップ 1 [アプリケーション (Applications)] ボタン  を押します。

ステップ 2 [管理者設定 (Admin settings)] > [セキュリティのセットアップ (Security Setup)] > [802.1X 認証 (802.1X Authentication)] を選択します。

ステップ 3 [デバイス認証 (Device Authentication)] オプションを設定します。

- はい
- なし

ステップ 4 [適用 (Apply)] を押します。

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。