CHAPTER 7

# Cisco Unified IP Phone の設定値の設定

Cisco Unified IP Phone には、設定可能な数多くのネットワーク設定値が用意されています。電話機をユーザが使用できる状態にするには、これらの設定値の修正が必要になる場合もあります。電話機のメニューを使用して、これらの設定値にアクセスし、その一部を変更することができます。電話機で表示専用になっている設定値は、Cisco Unified Communications Manager の管理ページで設定できます。

この章は、次の項で構成されています。



## Cisco Unified IP Phone のセットアップ メニュー

Cisco Unified IP Phone には、次の設定メニューが用意されています。

- [ネットワークのセットアップ（Network Setup）]：さまざまなネットワーク設定値を表示および設定するためのオプションを提供します。詳細については、「[イーサネットのセットアップ（Ethernet Setup）] メニュー」（P.7-4）を参照してください。
  - [イーサネットのセットアップ（Ethernet Setup）]：[ネットワークのセットアップ（Network Setup）] メニューのサブメニューです。[イーサネットのセットアップ（Ethernet Setup）] のメニュー項目はイーサネット ネットワーク上の Cisco Unified IP Phone を設定するための設定オプションを提供します。詳細については、「[イーサネットのセットアップ（Ethernet Setup）] メニュー」（P.7-4）を参照してください。
  - [WLAN のセットアップ（WLAN Setup）]：[ネットワークのセットアップ（Network Setup）] メニューのサブメニューです。[WLAN のセットアップ（WLAN Setup）] のメニュー項目は、Cisco Unified IP Phone を Wireless Local Area Network（WLAN; ワイヤレス ローカル エリア ネットワーク）に設定するための設定オプションを提供します。詳細については、「[WLAN のセットアップ（WLAN Setup）] メニュー」（P.7-7）を参照してください。
  - [IPv4 のセットアップ（IPv4 Setup）]：[イーサネットのセットアップ（Ethernet Setup）] メニューおよび [WLAN のセットアップ（WLAN Setup）] メニューのサブメニューです。IPv4 メニュー項目を使用して、追加のネットワーク オプションを表示および設定できます。詳細については、「[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション」（P.7-11）を参照してください。

- [セキュリティのセットアップ（Security Setup）]：さまざまなセキュリティ設定を表示および設定するためのオプションを提供します。詳細については、「[セキュリティのセットアップ（Security Setup）] メニュー」（P.7-15）を参照してください。

[ネットワークのセットアップ（Network Setup）] メニューにあるオプション設定値を変更するには、オプションのロックを編集のために解除しておく必要があります。手順については、「オプションのロック解除とロック」（P.7-3）を参照してください。

オプション設定値の編集や変更に使用できるキーについては、「設定値の編集」（P.7-3）を参照してください。

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（ウィンドウの [プロダクト固有の情報（Product Specific Information）] 部分にある）を使用すると、電話機のユーザが電話機の設定値にアクセスできるかどうかを制御できます。

### 関連項目

- 「セットアップ メニューの表示」（P.7-2）
- 「オプションのロック解除とロック」（P.7-3）
- 「設定値の編集」（P.7-3）
- 「[イーサネットのセットアップ（Ethernet Setup）] メニュー」（P.7-4）
- 「[WLAN のセットアップ（WLAN Setup）] メニュー」（P.7-7）
- 「[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション」（P.7-11）
- 「[セキュリティのセットアップ（Security Setup）] メニュー」（P.7-15）

## セットアップ メニューの表示

設定メニューを表示するには、次の手順を実行します。

### 手順

**ステップ 1**　アプリケーション ボタン を押します。

**ステップ 2**　[管理者設定（Administrator Settings）] を選択します。

**ステップ 3**　[ネットワークのセットアップ（Network Setup）] または [セキュリティのセットアップ（Security Setup）] を選択します。

**（注）**　[ステータス（Status）] メニューの詳細については、第 10 章「Cisco Unified IP Phone のモデル情報、ステータス、および統計の表示」を参照してください。[設定のリセット（Reset Settings）] メニューの詳細については、第 12 章「トラブルシューティングとメンテナンス」を参照してください。

**ステップ 4**　必要な場合はユーザ ID とパスワードを入力し、[ログイン（Sign-In）] をクリックします。

**ステップ 5**　次のいずれかの操作を実行して、目的のメニューを表示します。

- ナビゲーション パッドの矢印を使用して目的のメニューを選択し、選択ボタンを押します。
- 電話機のキーパッドを使用して、メニューに対応する番号を入力します。

**ステップ 6**　サブメニューを表示するには、ステップ 5 を繰り返します。

**ステップ 7**　メニューを終了するには、[ 終了（Exit）] ソフトキーまたは U ターン型の矢印のソフトキー を押します。

**関連項目**

- 「オプションのロック解除とロック」（P.7-3）
- 「設定値の編集」（P.7-3）
- 「[ イーサネットのセットアップ（Ethernet Setup）] メニュー」（P.7-4）
- 「[WLAN のセットアップ（WLAN Setup）] メニュー」（P.7-7）
- 「[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション」（P.7-11）
- 「[ セキュリティのセットアップ（Security Setup）] メニュー」（P.7-15）

# オプションのロック解除とロック

電話機にパスワードを設定すると、電話スクリーンの [ 管理者設定（Admin Settings）] でパスワードを入力しない限り、管理者オプションを変更できなくなります。

電話機にパスワードを適用するには、Cisco Unified Communications Manager の管理ページで、[ 共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウを表示します（[ デバイス（Device）] > [ デバイスの設定（Device Settings）] > [ 共通の電話プロファイル（Common Phone Profile）]）。[ 電話ロック解除パスワード（Local Phone Unlock Password）] オプションで、パスワードを入力します。電話機が使用する共通の電話プロファイルに、パスワードを適用します。

**関連項目**

- 「セットアップ メニューの表示」（P.7-2）
- 「設定値の編集」（P.7-3）
- 「[ イーサネットのセットアップ（Ethernet Setup）] メニュー」（P.7-4）
- 「[WLAN のセットアップ（WLAN Setup）] メニュー」（P.7-7）
- 「[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション」（P.7-11）

# 設定値の編集

オプション設定値を編集するときは、次のガイドラインに従ってください。

- 編集するフィールドを強調表示するには、ナビゲーション パッドの矢印を使用します。次にナビゲーション パッドの選択ボタンを押すと、強調表示したフィールドがアクティブになります（編集可能なフィールド上で 2 回たたいてもフィールドをアクティブにできます）。フィールドがアクティブになると、値を入力できます。
- 数値と文字を入力するには、キーパッド上のキーを使用します。
- キーパッドを使用して文字を入力するには、対応する数値キーを使用します。キーを 1 回または何回か押して、個々の文字を表示します。たとえば、2 キーを 1 回押すと「a」、すばやく 2 回押すと「b」、すばやく 3 回押すと「c」です。しばらく待機すると、カーソルが自動的に進んで、次の文字を入力できるようになります。
- 入力を誤ったときは、矢印ソフトキー を押します。このソフトキーを押すと、カーソルの左側にある文字が削除されます。

- 変更内容を保存しない場合は、[保存（Save）] ソフトキーを押す前に、[キャンセル（Cancel）] ソフトキーを押します。
- IP アドレスを入力するには、ユーザ用に分割されている 4 個のセグメントに値を入力します。左端からピリオドまでの数字を入力し終わったら、右向き矢印キーを使用して次のセグメントに移動します。左端の数字の後のピリオドは自動的に挿入されます。

（注）　Cisco Unified IP Phone では、必要に応じて、いくつかの方法でオプション設定値をリセットまたは復元することができます。詳細については、「Cisco Unified IP Phone のリセット」（P.12-15）を参照してください。

**関連項目**


- 「セットアップ メニューの表示」（P.7-2）
- 「オプションのロック解除とロック」（P.7-3）
- 「[イーサネットのセットアップ（Ethernet Setup）] メニュー」（P.7-4）
- 「[WLAN のセットアップ（WLAN Setup）] メニュー」（P.7-7）
- 「[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション」（P.7-11）


# [イーサネットのセットアップ（Ethernet Setup）] メニュー

[イーサネットのセットアップ（Ethernet Setup）] メニューは、さまざまなネットワーク設定値を表示および設定するためのオプションを提供します。表 7-1 に、これらのオプションの説明を示します。また、該当する場合には、それらの変更方法についても併せて説明します。

[イーサネットのセットアップ（Ethernet Setup）] メニューにアクセスする方法については、「セットアップ メニューの表示」（P.7-2）を参照してください。

オプションの編集に使用できるキーについては、「設定値の編集」（P.7-3）を参照してください。

（注）　イーサネット データ フィールドは、VPN 接続が確立されたときに上書きされます。

表 7-1　[イーサネットのセットアップ（Ethernet Setup）] メニューのオプション

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| IPv4 のセットアップ（IPv4 Setup） | [IPv4 のセットアップ（IPv4 Setup）] 設定サブメニューでは、次の作業を実行できます。<br>• DHCP サーバによって割り当てられた IP アドレスの、電話機による使用のオン/オフ。<br>• IP アドレス、サブネット マスク、デフォルト ルータ、DNS サーバ、および代替 TFTP サーバの手動設定。<br>IPv4 アドレス フィールドの詳細については、表 7-3 を参照してください。 | [IPv4 のセットアップ（IPv4 Setup）] までスクロールし、選択ボタンを押します。 |
| MAC Address | 電話機固有の Media Access Control（MAC; メディア アクセス コントロール）アドレス。 | 表示のみ（変更不可）。 |
| ドメイン名（Domain Name） | 電話機が常駐しているドメイン ネーム システム（DNS）ドメインの名前。 | 1. [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。<br>2. [ドメイン名（Domain Name）] オプションまでスクロールし、[選択（Select）] キーを押して、新しいドメイン名を入力します。<br>3. [適用（Apply）] ソフトキーを押します。 |
| 接続先 VLAN ID（Operational VLAN ID） | 電話機が所属する、Cisco Catalyst スイッチに設定された補助 Virtual Local Area Network（VLAN; 仮想 LAN）。<br>電話機が補助 VLAN をまだ受信していない場合、このオプションは管理 VLAN を示しています。<br>補助 VLAN と管理 VLAN のいずれも設定されていない場合、このオプションは空白になります。 | 表示のみ（変更不可）。<br>電話機は、Cisco Discovery Protocol（CDP）または Link Level Discovery Protocol Media Endpoint Discovery（LLDP-MED）を通じて接続先 VLAN ID を取得します。ID の情報は電話機が接続されているスイッチから提供されます。VLAN ID を手動で割り当てるには、[管理 VLAN ID（Admin VLAN ID）] オプションを使用します。 |
| 管理 VLAN ID（Admin. VLAN ID） | 電話機がメンバーになっている補助 VLAN。<br>電話機がスイッチから補助 VLAN を受信していない場合のみ使用され、その他の場合は無視されます。 | 1. [管理 VLAN ID（Admin VLAN ID）] オプションまでスクロールし、[選択（Select）] ソフトキーを押して、新しい管理 VLAN 設定値を入力します。<br>2. [適用（Apply）] ソフトキーを押します。 |

表 7-1　[イーサネットのセットアップ（Ethernet Setup）] メニューのオプション （続き）

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| PC VLAN | ボイス VLAN をサポートしないサードパーティ スイッチと電話機が連携できるようにします。このオプションを変更する前に、[管理 VLAN ID（Admin VLAN ID）] オプションを設定する必要があります。 | 1. [管理 VLAN ID（Admin VLAN ID）] オプションが設定されていることを確認してください。<br>2. [PC VLAN] オプションまでスクロールし、[選択（Select）] ソフトキーを押して、新しい PC VLAN 設定値を入力します。<br>3. [適用（Apply）] ソフトキーを押します。 |
| SW ポートのセットアップ（SW Port Setup） | ネットワーク ポートの速度とデュプレックス 有効な値は、次のとおりです。<br>• 自動ネゴシエーション（Auto Negotiate）<br>• [1000 フル（1000 Full）] : 1000-BaseT/ 全二重<br>• [100 ハーフ（100 Half）] : 100-BaseT/ 半二重<br>• [100 フル（100 Full）] : 100-BaseT/ 全二重<br>• [10 ハーフ（10 Half）] : 10-BaseT/ 半二重<br>• [10 フル（10 Full）] : 10-BaseT/ 全二重<br>電話機がスイッチに接続されている場合は、スイッチ上のポートを電話機と同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。<br>このオプションの設定値を変更する場合は、[PC ポート設定（PC Port Configuration）] オプションを同じ設定値に変更する必要があります。 | 1. [ネットワークの設定（Network Configuration）] のオプションのロックを解除します。<br>2. [SW ポート設定（SW Port Configuration）] オプションまでスクロールし、[選択（Select）] ソフトキーを押します。<br>3. 目的の設定値までスクロールし、[選択（Select）] キーを押します。 |
| PC ポートのセットアップ（PC Port Setup） | コンピュータ（アクセス）ポートの速度とデュプレックス。有効な値は、次のとおりです。<br>• 自動ネゴシエーション（Auto Negotiate）<br>• [1000 フル（1000 Full）] : 1000-BaseT/ 全二重<br>• [100 ハーフ（100 Half）] : 100-BaseT/ 半二重<br>• [100 フル（100 Full）] : 100-BaseT/ 全二重<br>• [10 ハーフ（10 Half）] : 10-BaseT/ 半二重<br>• [10 フル（10 Full）] : 10-BaseT/ 全二重<br>電話機がスイッチに接続されている場合は、スイッチ上のポートを電話機と同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。<br>このオプションの設定値を変更する場合は、[SW ポート設定（SW Port Configuration）] オプションを同じ設定値に変更する必要があります。 | 1. [ネットワークの設定（Network Configuration）] のオプションのロックを解除します。<br>2. [PC ポート設定（PC Port Configuration）] オプションまでスクロールし、[選択（Select）] ソフトキーを押します。<br>3. 目的の設定値までスクロールし、[選択（Select）] キーを押します。<br>複数の電話機の設定を同時に行うには、[エンタープライズ電話の設定（Enterprise Phone Configuration）]（[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configurations）]）で [リモート ポート設定（Remote Port Configuration）] を有効にします。<br>**（注）** Unified CM のリモート ポート設定用にポートが設定されている場合は、電話機のデータを変更することはできません。 |

**関連項目**

- 「セットアップ メニューの表示」（P.7-2）
- 「オプションのロック解除とロック」（P.7-3）
- 「[WLAN のセットアップ（WLAN Setup）] メニュー」（P.7-7）
- 「[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション」（P.7-11）

# [WLAN のセットアップ（WLAN Setup）] メニュー

[WLAN のセットアップ（WLAN Setup）] メニューは、さまざまなネットワーク設定値を表示および設定するためのオプションを提供します。表 7-2 に、これらのオプションの説明を示します。また、該当する場合には、それらの変更方法についても併せて説明します。

**（注）** WLAN の設定値は、Cisco Unified IP Phone キーパッドでのみ設定できます。Cisco Unified IP Phone を WLAN モードで使用している場合は、AC アダプタを使用する必要があります。イーサネットに接続すると、WLAN は無効になります。

[WLAN のセットアップ（WLAN Setup）] メニューにアクセスする方法については、「セットアップ メニューの表示」（P.7-2）を参照してください。

オプションの編集に使用できるキーについては、「設定値の編集」（P.7-3）を参照してください。

**表 7-2　[WLAN のセットアップ（WLAN Setup）] メニューのオプション**

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| ワイヤレス（Wireless） | Cisco Unified IP Phone でのワイヤレス ラジオを有効または無効にするときに使用します。有効な値は、次のとおりです。<br>• [オン（On）]：電話機のワイヤレス ラジオを有効にします。<br>• [オフ（Off）]：電話機のワイヤレス ラジオを無効にします。<br>デフォルト：[オン（On）] | 1. [ワイヤレス（Wireless）] オプションまでスクロールしてからトグル スイッチを使用すると、オンとオフの設定値を切り替えることができます。<br>2. [適用（Apply）] ソフトキーを押します。 |
| WLAN サイン イン アクセス（WLAN Sign in Access） | メインの [アプリケーション（Applications）] メニューで、[WLAN サイン イン アクセス（WLAN Sign in Access）] ウィンドウの表示を有効にします。<br>• [オン（On）]：[WLAN サイン イン アクセス（WLAN Sign in Access）] ウィンドウの表示を有効にします。この値をオンにすると、メインの [アプリケーション（Applications）] メニューで、WLAN ユーザ ID およびパスワードのサイン インまたは変更ができます。オンにせずにサイン イン情報を変更するには、[セキュリティ（Security）] メニュー レベルまでナビゲートしてから、サイン イン クレデンシャルが必要な LEAP または EAP-FAST のいずれかの方法を選択します。<br>• [オフ（Off）]：[WLAN サイン イン アクセス（WLAN Sign in Access）] ウィンドウは表示されません。<br>デフォルト：[オフ（Off）] | 1. [ワイヤレス サイン イン（Wireless Sign In）] オプションまでスクロールしてから、トグル スイッチを使用すると、オンとオフの設定値を切り替えることができます。<br>2. [適用（Apply）] ソフトキーを押します。 |
| IPv4 のセットアップ（IPv4 Setup） | [IPv4 のセットアップ（IPv4 Setup）] 設定サブメニューでは、次の作業を実行できます。<br>• DHCP サーバによって割り当てられた IP アドレスの、電話機による使用のオン / オフ。<br>• IP アドレス、サブネット マスク、デフォルト ルータ、DNS サーバ、および代替 TFTP サーバの手動設定。<br>IPv4 アドレス フィールドの詳細については、表 7-3 を参照してください。 | [IPv4 のセットアップ（IPv4 Setup）] までスクロールし、選択ボタンを押します。 |
| MAC Address | 電話機固有の Media Access Control（MAC; メディア アクセス コントロール）アドレス。 | 表示のみ（変更不可）。 |

表 7-2　[WLAN のセットアップ（WLAN Setup）] メニューのオプション （続き）

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| ドメイン名（Domain Name） | 電話機が常駐しているドメイン ネーム システム（DNS）ドメインの名前。 | 1. [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。<br>2. [ドメイン名（Domain Name）] オプションまでスクロールし、[選択（Select）] キーを押して、新しいドメイン名を入力します。<br>3. [適用（Apply）] ソフトキーを押します。 |
| SSID | ワイヤレス アクセス ポイントにアクセスする固有識別情報、Service Set Identifier（SSID; サービス セット ID）を指定します。 | 1. SSID のオプションまでスクロールしてから、[選択（Select）] ソフトキーを押し、SSID を入力します。<br>2. [適用（Apply）] ソフトキーを押します。 |

表 7-2　[WLAN のセットアップ（WLAN Setup）] メニューのオプション （続き）

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| セキュリティ モード（Security Mode） | 電話機が WLAN へのアクセスに使用する認証のタイプです。有効な値は、次のとおりです。<br>• [ 開く（Open）] : 暗号化せず、すべての Access Point（AP; アクセス ポイント）にアクセスします。<br>• [WEP で開く（Open with WEP）] : 802.11 認証を行ったうえでオープンにするが、データの暗号化に Wired Equivalent Privacy（WEP; 有線と同等のプライバシー）を使用します。すべての AP へのアクセスおよび、ローカル AP での WEP キーを通じた認証を指定します。<br>• [ 共有キー（Shared Key）] : WEP を使用した共有キーの認証です。<br>• [LEAP] : Lightweight Extensible Authentication Protocol（LEAP）の認証では、ユーザ名と暗号化されたセキュアなパスワードをネットワークの RADIUS サーバと交換します（EAP のシスコ独自のバージョン）。LEAP では WPA および WPA2 をサポートしています。<br>• [EAP-FAST] : Extensible Authentication Protocol Flexible Authentication via Secure Tunneling（EAP-FAST）では、ユーザ名と暗号化されたセキュアなパスワードをネットワークの RADIUS サーバと交換します。このネットワークでは、Protected Access Credential（PAC）を使用することで認証用のセキュアなトンネルが確立されています。EAP-FAST では WPA および WPA2 をサポートしています。<br>• [AKM] : アクセス ポイントから提示される設定情報から 802.11 認証メカニズムを自動的に選択します。このモードで設定している場合、WPA-PSK または WPA バージョン 1 または 2 を使用できます。<br>**（注）** AKM を選択するときは次の点を考慮します。1）AKM は WPA、WPA2 または CCKM を使用する場合は 802.1x 対応 LEAP を使用する。2）AKM は最強のキー管理タイプを優先としたうえで最強の暗号キーを使用する暗号化方式を選択する。3）CCKM は WPA2 ではサポートされない。 | 1. [ セキュリティ モード（Security Mode）] オプションまでスクロールし、目的の値を強調表示します。<br>2. [ 適用（Apply）] をクリックします。 |
| 802.11 モード（802.11 Mode） | WLAN で使用されるワイヤレス信号規格を指定します。有効な値は、次のとおりです。<br>• [ 自動（Auto）] : デフォルト値。可能な場合は 5.0 Ghz を優先とします。<br>• 802.11a<br>• 802.11b/g | 1. [802.11 モード（802.11 Mode）] オプションまでスクロールし、目的の値を強調表示します。<br>2. [ 適用（Apply）] をクリックします。 |

# [IPv4 のセットアップ（IPv4 Setup）] メニューのオプション

[IPv4 のセットアップ（IPv4 Setup）] メニューは、[ イーサネットのセットアップ（Ethernet Setup）] メニューおよび [WLAN のセットアップ（WLAN Setup）] メニューのサブメニューです。IPv4 のメニューに到達するには、[ イーサネットのセットアップ（Ethernet Setup）] メニューまたは [WLAN のセットアップ（WLAN Setup）] メニューから IPv4 のオプションを選択します。

表 7-3 に、[IPv4 のセットアップ（IPv4 Setup）] メニューのオプションの説明を示します。

オプションの編集に使用できるキーについては、「設定値の編集」（P.7-3）を参照してください。

**表 7-3　[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション**

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| DHCP を使う（DHCP Enabled） | 電話機の DHCP が有効か無効かを示します。<br>DHCP が有効な場合、DHCP サーバによって電話に IP アドレスが割り当てられます。DHCP が無効な場合、管理者が、電話機に手動で IP アドレスを割り当てる必要があります。 | [DHCP を使う（DHCP Enabled）] オプションまでスクロールし、[ いいえ（No）] ソフトキーを押して DHCP を無効にするか、[ はい（Yes）] ソフトキーを押して DHCP を有効にします。 |
| IP Address | 電話機のインターネット プロトコル（IP）アドレス。<br>IP アドレスをこのオプションで割り当てる場合は、サブネット マスクとデフォルト ルータも割り当てる必要があります。この表の [ サブネット マスク（Subnet Mask）] オプションと [ デフォルト ルータ（Default Router）] オプションを参照してください。 | 1. [DHCP を使う（DHCP Enabled）] オプションを [ いいえ（No）] に設定します。<br>2. [IP アドレス（IP Address）] オプションまでスクロールし、[ 選択（Select）] ソフトキーを押して、新しい IP アドレスを入力します。<br>3. [ 適用（Apply）] ソフトキーを押します。 |
| サブネット マスク（Subnet Mask） | 電話機で使用されるサブネット マスク。 | 1. [DHCP を使う（DHCP Enabled）] オプションを [ いいえ（No）] に設定します。<br>2. [ サブネット マスク（Subnet Mask）] オプションまでスクロールし、[ 選択（Select）] ソフトキーを押して、新しいサブネット マスクを入力します。<br>3. [ 適用（Apply）] ソフトキーを押します。 |

表 7-3　[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション （続き）

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| デフォルト ルータ（Default Router） | 電話機で使用される、デフォルト ルータ。 | 1. [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。<br>2. 目的の [デフォルト ルータ（Default Router）] オプションまでスクロールし、[選択（Select）] ソフトキーを押して、新しいルータの IP アドレスを入力します。<br>3. [適用（Apply）] ソフトキーを押します。 |
| DNS サーバ 1（DNS Server 1）<br>DNS サーバ 2（DNS Server 2）<br>DNS サーバ 3（DNS Server 3） | 電話機で使用されるプライマリ ドメイン ネーム システム（DNS）サーバ（[DNS サーバ 1（DNS Server 1）]）およびオプションのバックアップ DNS サーバ（[DNS サーバ 2（DNS Server 2）] ～ [DNS サーバ 3（DNS Server 3）]）。 | 1. [DHCP を使う（DHCP Enabled）] オプションを [いいえ（No）] に設定します。<br>2. 目的の [DNS サーバ（DNS Server）] オプションまでスクロールし、[選択（Select）] ソフトキーを押して、新しい DNS サーバの IP アドレスを入力します。<br>3. [適用（Apply）] ソフトキーを押します。<br>4. 必要に応じて手順 2 と 3 を繰り返してバックアップ DNS サーバを割り当てます。 |
| 代替 TFTP（Alternate TFTP） | 電話機が代替 TFTP サーバを使用しているかどうかを示します。 | 電話機で代替 TFTP サーバを使用する場合は、[代替 TFTP（Alternate TFTP）] オプションまでスクロールし、[はい（Yes）] ソフトキーを押します。使用しない場合は、[いいえ（No）] ソフトキーを押します。 |

表 7-3　[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション （続き）

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| TFTP サーバ 1（TFTP Server 1） | 電話機で使用される、プライマリの Trivial File Transfer Protocol（TFTP）サーバ。ネットワークで DHCP を使用していない場合、このサーバを変更するには [TFTP サーバ 1（TFTP Server 1）] オプションを使用する必要があります。<br><br>[ 代替 TFTP（Alternate TFTP）] オプションを [ はい（Yes）] に設定した場合は、[TFTP サーバ 1（TFTP Server 1）] オプションに 0 以外の値を入力する必要があります。<br><br>プライマリ TFTP サーバもバックアップ TFTP サーバも、電話機の CTL ファイルまたは ITL ファイルに記述されていない場合は、[TFTP サーバ 1（TFTP Server 1）] オプションの変更内容を保存する前に、これらのファイルをロック解除する必要があります。この場合、[TFTP サーバ 1（TFTP Server 1）] オプションへの変更を保存すると、ファイルは削除されます。新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 1 アドレスからダウンロードされます。<br><br>電話機が TFTP サーバを探すとき、プロトコルに関係なく、手動で割り当てられた TFTP サーバが優先されます。IPv6 と IPv4 の両方の TFTP サーバが設定に含まれる場合、電話機は、手動で割り当てられた IPv6 TFTP サーバおよび IPv4 TFTP サーバを優先することによって、TFTP サーバを探す順序の優先順位を決定します。電話機は、次の順序で TFTP サーバを探します。<br><br>**1.** 手動で割り当てられた IPv6 TFTP サーバ<br>**2.** 手動で割り当てられた IPv4 TFTP サーバ<br>**3.** DHCPv6 が割り当てられた TFTP サーバ<br>**4.** DHCP が割り当てられた TFTP サーバ<br><br>**（注）** CTL および ITL ファイルの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。 | **1.** 必要に応じて（電話機の管理ドメインを変更する場合など）、CTL ファイルまたは ITL ファイルをロック解除します。CTL ファイルと ITL ファイルの両方がある場合は、いずれかのファイルをロック解除します。<br><br>**2.** DHCP を有効にしている場合は、[ 代替 TFTP（Alternate TFTP）] オプションを [Yes] に設定します。<br><br>**3.** [TFTP サーバ 1（TFTP Server 1）] オプションまでスクロールし、[ 選択（Select）] ソフトキーを押して、新しい TFTP サーバの IP アドレスを入力します。<br><br>**4.** [ 適用（Apply）] ソフトキーを押し、[ 保存（Save）] を押します。 |

表 7-3　[IPv4 のセットアップ（IPv4 Setup）] メニューのオプション （続き）

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| TFTP サーバ 2（TFTP Server 2） | プライマリの TFTP サーバが使用不能の場合に、電話機で使用されるオプションのバックアップ TFTP サーバ。<br><br>プライマリ TFTP サーバもバックアップ TFTP サーバも、電話機の CTL ファイルまたは ITL ファイルに記述されていない場合は、[TFTP サーバ 2（TFTP Server 2）] オプションの変更内容を保存する前に、これらのファイルのいずれかをロック解除する必要があります。この場合、[TFTP サーバ 2（TFTP Server 2）] オプションへの変更を保存すると、ファイルのいずれかは削除されます。新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 2 アドレスからダウンロードされます。<br><br>電話機が TFTP サーバを探すとき、プロトコルに関係なく、手動で割り当てられた TFTP サーバが優先されます。IPv6 と IPv4 の両方の TFTP サーバが設定に含まれる場合、電話機は、手動で割り当てられた IPv6 TFTP サーバおよび IPv4 TFTP サーバを優先することによって、TFTP サーバを探す順序の優先順位を決定します。電話機は、次の順序で TFTP サーバを探します。<br><br>**1.** 手動で割り当てられた IPv6 TFTP サーバ<br>**2.** 手動で割り当てられた IPv4 TFTP サーバ<br>**3.** DHCPv6 が割り当てられた TFTP サーバ<br>**4.** DHCP が割り当てられた TFTP サーバ<br><br>**（注）** CTL または ITL ファイルの詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。 | **1.** 必要に応じて（電話機の管理ドメインを変更する場合など）、CTL ファイルまたは ITL ファイルをロック解除します。CTL ファイルと ITL ファイルの両方がある場合は、どちらかのファイルをロック解除します。<br>**2.** [ ネットワークの設定（Network Configuration）] のオプションのロックを解除します。<br>**3.** [TFTP サーバ 1（TFTP Server 1）] オプションに IP アドレスを入力します。<br>**4.** [TFTP サーバ 2（TFTP Server 2）] オプションまでスクロールし、[ 選択（Select）] ソフトキーを押して、新しいバックアップ TFTP サーバの IP アドレスを入力します。セカンダリの TFTP サーバがない場合は、[ 削除（Delete）] ソフトキーを使用して前の値のフィールドをクリアします。<br>**5.** [ 適用（Apply）] ソフトキーを押し、[ 保存（Save）] を押します。<br><br>CTL ファイルまたは ITL ファイルのロックを解除し忘れた場合、どちらかのファイルで TFTP サーバ 2 アドレスを変更した後、[ セキュリティ設定（Security Configuration）] メニューから [ 削除（Erase）] ソフトキーを押すことによって、それらのファイルを削除できます。新しい CTL ファイルまたは ITL ファイルが新しい TFTP サーバ 2 アドレスからダウンロードされます。 |
| BOOTP サーバ（BOOTP Server） | 電話機が IP アドレスを DHCP サーバではなく BOOTP サーバから受信するかどうかを示します。 | 表示のみのフィールドです。 |
| DHCP アドレス解放（DHCP Address Released） | DHCP によって割り当てられた IP アドレスを解放します。 | このフィールドは DHCP が有効な場合に編集できます。VLAN から電話機を削除して、再割り当てのために電話機の IP アドレスを解放する場合は、このオプションを [ はい（Yes）] に設定し、[ 適用（Apply）] ソフトキーを押します。 |

### 関連項目

- 「セットアップ メニューの表示」（P.7-2）
- 「オプションのロック解除とロック」（P.7-3）
- 「設定値の編集」（P.7-3）

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

[管理者設定（Admin Settings）] メニューから直接アクセスする [セキュリティのセットアップ（Security Setup）] メニューは、さまざまなセキュリティ設定に関する情報を提供します。また、[信頼リスト（Trust List）] メニューへのアクセスも提供し、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も示します。

[セキュリティのセットアップ（Security Setup）] メニューおよびサブメニューへのアクセス方法については、「セットアップ メニューの表示」（P.7-2）を参照してください。

表 7-4 で、[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について説明します。

**表 7-4　セキュリティ メニュー設定**

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| セキュリティ モード（Security Mode） | 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。 | Cisco Unified Communications Manager の管理ページで、[デバイス（Device）] > [電話（Phone）] > [電話の設定（Phone Configuration）] を選択します。この設定はウィンドウの [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される、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。 | 電話機の LSC を管理する方法については、『*Cisco Unified Communications Manager Security Guide*』の「Using the Certificate Authority Proxy Function」の章を参照してください。 |
| 信頼リスト（Trust List） | [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。<br>[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。 | 詳細については、「[信頼リスト（Trust List）] メニュー」（P.7-16）を参照してください。 |
| 802.1X 認証 | この電話機に 802.1X 認証を有効にできます。 | 「802.1X 認証およびトランザクションのステータス」（P.7-17）を参照してください。 |

# [信頼リスト（Trust List）] メニュー

[信頼リスト（Trust List）] メニューは、CTL、ITL、および署名済み設定ファイルの各サブメニューを含むトップレベルのメニューを示します。署名済み設定ファイルの内容は SRST です。

[信頼リスト（Trust List）] メニューには、証明書が関連付けられているコンポーネントだけが表示されます。表 7-5 で、[信頼リスト（Trust List）] メニューのオプションについて説明します。

**表 7-5　[信頼リスト（Trust List）] メニューの設定**

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| CTL 署名（CTL Signature） | CTL ファイルの MD5 ハッシュ。 | この設定の詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Configuring the Cisco CTL Client」の項を参照してください。 |
| Unified CM/TFTP サーバ（Unified CM/TFTP Server） | 電話で使用されている Cisco Unified Communications Manager および TFTP サーバの通常名。このサーバの証明書がインストールされている 場合は、証明書のアイコンも表示されます。 | この設定の詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Configuring the Cisco CTL Client」の項を参照してください。 |
| CAPF サーバ（CAPF Server） | 電話機で使用されている CAPF の通常名。このサーバの証明書がインストールされている場合は、証明書のアイコンも表示されます。 | この設定の詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Configuring the Cisco CTL Client」の項を参照してください。 |
| SRST ルータ（SRST Router） | 電話機で使用可能な信頼された SRST ルータの IP アドレス（そのようなデバイスが Cisco Unified Communications Manager の管理ページに設定されている場合）。このサーバの証明書がインストールされている場合は、証明書のアイコンも表示されます。 | この設定の詳細については、『*Cisco Unified Communications Manager Security Guide*』の「Configuring the Cisco CTL Client」の項を参照してください。 |

# 802.1X 認証およびトランザクションのステータス

[802.1X 認証の設定（802.1X Authentication Settings）] メニューでは、802.1X 認証を有効にし、トランザクションのステータスを表示できます。表 7-6 にこれらのオプションを示します。

アプリケーション ボタン を押し、[ 管理者設定（Administrator Settings）] > [ セキュリティのセットアップ（Security Setup）] > [802.1X 認証（802.1X Authentication）] を選択すると、[802.1 X 認証（802.1X Authentication）] の設定にアクセスできます。このメニューを終了するには、[ 終了（Exit）] ソフトキーを押します。

**表 7-6　802.1X 認証の設定**

| オプション（Option） | 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。<br>• [ 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。<br>• [ 無効（Disabled）] : デフォルト設定。電話機は CDP を使用して VLAN およびネットワークにアクセスします。 | 1. アプリケーション ボタン を押し、[ 管理者設定（Administrator Settings）] > [ セキュリティのセットアップ（Security Setup）] > [802.1X 認証（802.1 X Authentication）] > [ デバイス認証（Device Authentication）] を選択します。<br>2. [ デバイス認証（Device Authentication）] オプションを [ 有効（Enabled）] または [ 無効（Disabled）] に設定します。<br>3. [ 適用（Apply）] ソフトキーを押します。 |
| EAP-MD5 | 次のメニュー オプション（下記の説明を参照）を使用して、802.1X 認証用のパスワードを指定します。<br>• Device ID<br>• 共有秘密キー（Shared Secret）<br>• レルム（Realm） | アプリケーション ボタン を押し、[ 管理者設定（Administrator Settings）] > [ セキュリティの設定（Security Setup）] > [802.1X 認証（802.1X Authentication）] > [EAP-MD5] の順に選択します。 |
| | [ デバイス ID（Device ID）] : 電話機のモデル番号と固有の MAC アドレスから生成された ID が、CP-<model>-SEP-<MAC> という形式で表示されます。 | 表示のみ（変更不可）。 |
| | [ 共有秘密鍵（Shared Secret）] : 電話機および認証サーバで使用するパスワードを選択します。パスワードには 6 ～ 32 文字の数字と文字を組み合わます。<br>**（注）** 802.1X 認証を無効にしている場合や電話機を工場出荷時の状態にリセット（すべての設定をリセット）した場合は、共有秘密が削除されます。 | 1. [EAP-MD5] > [ 共有秘密鍵（Shared Secret）] を選択します。<br>2. 共有秘密鍵を入力します。<br>3. [ 適用（Apply）] ソフトキーを押します。<br>削除された共有秘密から復帰する方法については、「Cisco Unified IP Phone セキュリティのトラブルシューティング」（P.12-9）を参照してください。 |
| | [ レルム（Realm）] : ユーザ ネットワーク ドメインを示します。常に [ ネットワーク（Network）] に設定されます。 | 表示のみ（変更不可）。 |

表 7-6　802.1X 認証の設定 （続き）

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| トランザクション ステータス（Transaction Status） | • [状態（State）]：802.1x 認証の状態を表示します。<br>– [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。<br>– [認証済み（Authenticated）]：電話機が認証されていることを示します。<br>– [保留（Held）]：認証プロセスが進行中であることを示します。<br>• [プロトコル（Protocol）]：802.1x 認証で使用されている EAP 方式（EAP-MD5、EAP-FAST または EAP-TLS のいずれかが使用可能）が表示されます。 | 表示のみ（変更不可）。 |

# [VPN の設定（VPN Configuration）] メニュー

[VPN の設定（VPN Configuration）] メニューでは、Secure Sockets Layer（SSL）を使用した VPN クライアントの接続を有効にすることができます。VPN 接続は、電話機が信頼ネットワークの外部にある場合、または電話機と Unified CM の間で非信頼ネットワークを通過する必要がある場合に使用されます。

システム管理者は電話機に VPN 機能を設定する必要があるかどうかを判断し、VPN 機能を有効にします。

電話機が VPN 用に設定されている場合は、UCM サーバ上で設定される [ネットワーク接続の自動検出（Auto-Detect Network Connection）] のステータスが、VPN 接続が可能かどうかを決定します。

- [ネットワーク接続の自動検出（Auto-Detect Network Connection）] が無効の場合、VPN 接続は可能です。[ログイン（Sign In）] 画面が表示され、システム管理者が電話機に設定した認証方式に基づいて、クレデンシャルに関する指示が表示されます。電話機の [アプリケーション（Applications）] > [VPN] ウィンドウで、[VPN 有効（VPN Enabled）] フィールドを [オン（On）] または [オフ（Off）] にして、電話機の VPN 接続を試行する機能をオンまたはオフに切り替えることができます。
- [ネットワーク接続の自動検出（Auto-Detect Network Connection）] が有効な場合は、VPN を介して接続できないため、[ログイン（Sign In）] 画面は表示されず、クレデンシャルに関する指示は表示されません。

## VPN への接続

次の手順を使用して、VPN による接続を行います。

### 手順

**ステップ 1**　電話機の電源をオンにし、VPN クライアント用の [ログイン（Sign In）] 画面が表示された後（証明書認証モードの場合は除く）、設定された認証方式に基づいて次のクレデンシャルを入力します。

- ユーザ名とパスワード：システム管理者から提供されたユーザ名とパスワードを入力します。
- 証明書とパスワード：システム管理者から提供されたパスワードを入力します。ユーザ名は証明書から得られます。

- 証明書：認証に証明書だけを使用する電話機では、[ ログイン（Sign In）] 画面は表示されず、VPN 接続を試行している電話機のステータスが電話機に表示されます。

（特定の状況下で電源が失われたり、リセットされたりすると、保存されているクレデンシャルがクリアされます）。

電話機に [ ログイン（Sign In）] 画面が表示されている場合、画面は点灯したままとなり、電力節約モードに入りません。これは、ユーザに電話機が未登録であることを警告しています。電話機を長時間この状態のままにすると、ユーザが再びログインしたときに、ディスプレイに短時間だけ残像が生じる場合がありますが、その後、残像は消えます。

**ステップ 2**　[ ログイン（Sign In）] ソフトキーを選択して接続します。

（電話機が接続を試みているときに [ キャンセル（Cancel）] を押すと、接続の試みは停止され、再び [ ログイン（Sign In）] 画面が表示されます。その後、[ キャンセル（Cancel）] を押すと VPN メニューが表示され、[VPN] フィールドが [ オフ（Off）] として表示されます。電話機は、ユーザが [VPN 有効（VPN Enabled）] フィールドを [ オン（On）] に設定するまで、再度の接続を試みません。

## [VPN の設定（VPN Configuration）] の設定

表 7-7 は Cisco Unified IP Phone での VPN 接続オプションの説明です。

**表 7-7　[VPN の設定（VPN Configuration）] の設定**

| オプション（Option） | 説明 | 変更の手順 |
|---|---|---|
| VPN 有効（VPN Enabled） | [ ネットワーク接続の自動検出の有効化（Enable Auto-Detect Network Connection）] が無効になっている場合、[VPN 有効（VPN Enabled）] を [ オン（On）] または [ オフ（Off）] にして、電話機の VPN 接続試行機能のオン / オフを切り替えます。 | [ アプリケーション（Applications）] > [VPN] を選択します。<br>VPN オプションを [ オン（On）] または [ オフ（Off）] に設定します。<br>Cisco Unified Communications Manager でこの機能が無効になっている場合、このオプションは無効になります。 |
| クレデンシャルの変更（Change Credentials） | ユーザ ID とパスワードを変更します。<br>認証が証明書のみの場合、または [VPN 有効（VPN Enabled）] がオフの場合、このオプションはグレー表示されます。 | — |
| VPN のステータス（VPN Status） | オプションが有効になっているか無効になっているかを示します。 | 表示専用：Unified CM 上で設定されます。 |