導入とプロビジョニング

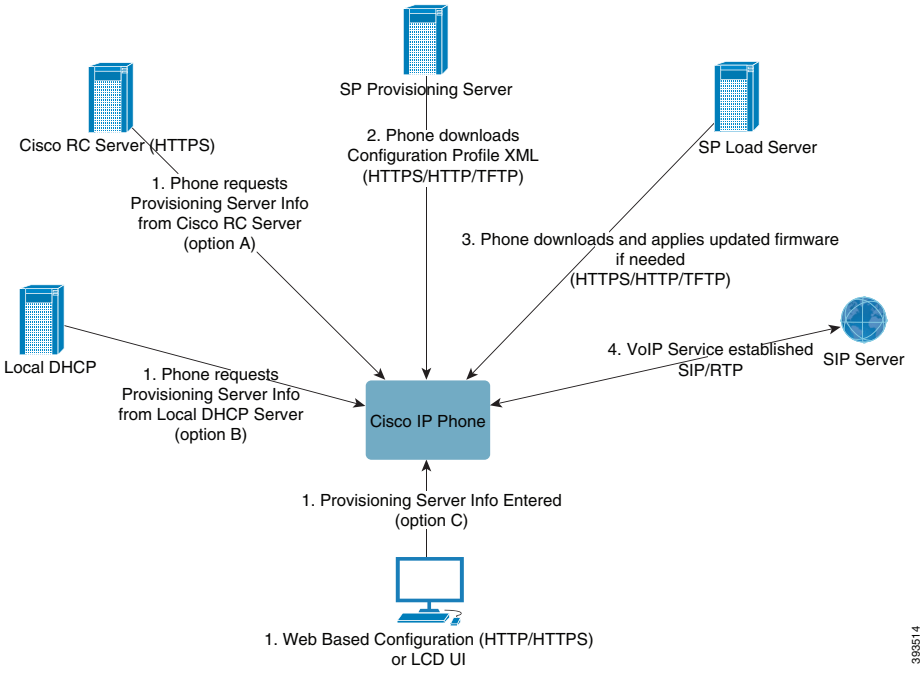
プロビジョニングの概要

Cisco IP Phone は、VoIP サービス プロバイダーによる自宅環境、ビジネス環境、または企業環境の顧客への大規模導入を対象としており、リモート管理および構成を通じて Cisco IP Phone をプロビジョニングすることで顧客サイトでの Cisco IP Phone の適切な動作を保証します。

次の機能は、カスタマイズされた稼働中の構成をサポートします。

- Cisco IP Phone の信頼性の高いリモート制御
- Cisco IP Phone を制御する通信の暗号化
- 効率化されたエンドポイント アカウントのバインディング

電話は、リモート サーバから設定プロファイルまたは更新されたファームウェアをダウンロードするようにプロビジョニングすることができます。ダウンロードは、電話がネットワークに接続されたとき、電源が投入されたとき、および設定された時間間隔で実行される場合があります。プロビジョニングは、通常、サービス プロバイダーに共通する大規模 Voice-over-IP（VoIP）導入の一環として行われます。設定プロファイルまたは更新されたファームウェア、あるいはその両方は、TFTP、HTTP、または HTTPS を使用してデバイスに転送されます。



Cisco IP Phone は、サービス プロバイダーのバックエンド設備のリモート内線として使用できます。リモート管理および構成は、顧客宅内での Cisco IP Phone の適切な稼働を実現します。

次の機能は、カスタマイズされた稼働中の構成をサポートします。

- Cisco IP Phone の信頼性の高いリモート制御
- Cisco IP Phone を制御する通信の暗号化

効率化されたエンドポイント アカウントのバインディング。電話は、リモート サーバから設定プロファイルまたは更新されたファームウェアをダウンロードするようにプロビジョニングすることができます。ダウンロードは、電話がネットワークに接続されたとき、電源が投入されたとき、および設定された時間間隔で実行される場合があります。プロビジョニングは、通常、大規模 Voice-over-IP（VoIP）導入の一環としてサービス プロバイダーによって行われます。設定プロファイルまたは更新されたファームウェアは、TFTP、HTTP、または HTTPS を使用してデバイスに転送されます。

Cisco IP Phone は、家庭やスモール ビジネスを営む顧客への VoIP サービス プロバイダーによる大規模導入を対象としています。ビジネスまたは企業環境において、Cisco IP Phone は端末ノードとして機能します。これらのデバイスは、顧客宅内のルータとファイアウォールを経由して接続され、インターネットを介して広く利用されています。

TR69 プロビジョニング

Cisco IP Phone では、Web UI を使用して管理者が TR69 パラメータを設定できます。パラメータ関連の情報については、対応する電話機シリーズのアドミニストレーション ガイドを参照してください。

MPP 電話機は、DHCP オプション 43、60、および 125 で ACS 検出をサポートします。

オプション 43：ベンダー固有の情報（ACS URL の場合）

オプション 60：ベンダー クラスの ID（MPP 電話機では、ACS に対し「dslforum.org」でそれ自体を識別）

オプション125：ベンダー固有の情報（ゲートウェイ関連付けの場合）

RPC の方式

サポートされている RPC の方式

MPP 電話機は、次に示すように、限定された RPC 方式のみをサポートしています。

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download：ダウンロード RPC 方式。サポートされているファイル タイプは次のとおりです。
  - ファームウェア アップグレード イメージ
  - ベンダー設定ファイル
  - カスタム CA ファイル
- Transfer Complete

サポートされているイベント タイプ

MPP 電話機は、サポートされている機能および方式に基づいてイベント タイプをサポートします。次のイベント タイプのみがサポートされています。

- Bootstrap
- Boot
- value change
- connection request

- Periodic
- Transfer Complete
- M Download
- M Reboot

ネットワークの輻輳時の電話の動作

ネットワークのパフォーマンスを低下させる要因はすべて、音声とビデオの品質にも影響します。場合によっては、コールがドロップすることもあります。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

電話への悪影響を軽減するかまたは防止するには、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します。

展開

Cisco IP Phone は、次の導入モデルに基づいて、プロビジョニングに役立つ機能を提供します。

- バルク配布—サービス プロバイダーは、バルク量 でCisco IP Phone を入手し、社内で事前プロビジョニングします。その後、デバイスは VoIP サービス契約の一環として顧客に提供されます。
- 小売配布—顧客は、小売店からCisco IP Phone を購入し、サービス プロバイダーに VoIP サービスを依頼します。その後、サービス プロバイダーは、デバイスのセキュアなリモート設定をサポートする必要があります。

バルク分散

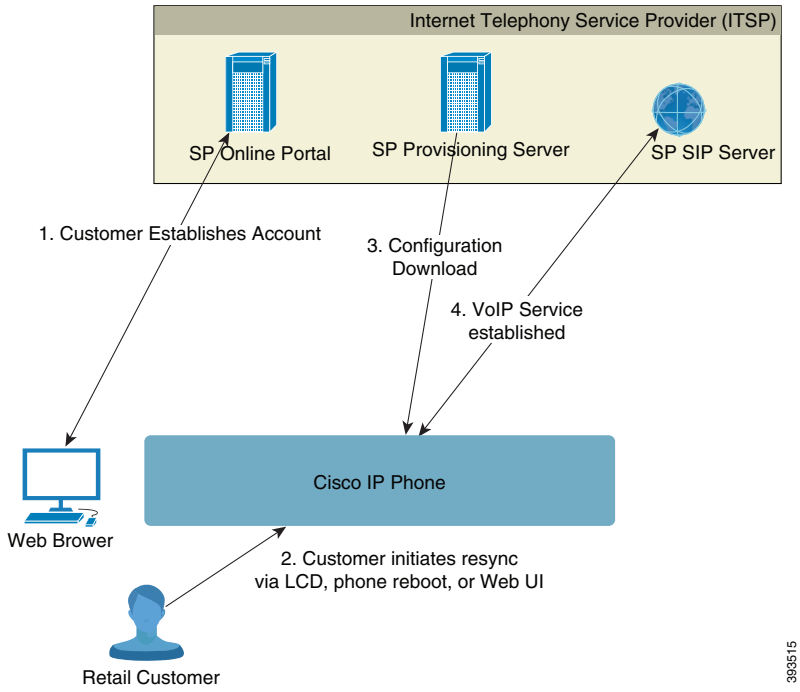
このモデルでは、サービス プロバイダーが VoIP サービス契約の一環として顧客に Cisco IP Phone を提供します。デバイスは、RC ユニットか、そうでない場合には社内で事前プロビジョニングされます。

Cisco は、デバイス プロファイルとファームウェアの更新をダウンロードする Cisco 製サーバと再同期するよう RC ユニットを事前プロビジョニングします。

サービス プロバイダーは、再同期を制御するパラメータなど、必要なパラメータで Cisco IP Phone を事前プロビジョニングできます。事前プロビジョニングにはさまざまな方法があります。

- 社内で DHCP と TFTP を使用する方法
- リモートで TFTP、HTTP、HTTPS を使用する方法
- 社内でのプロビジョニングとリモート プロビジョニングの組み合わせ

小売配布



Cisco IP Phone には、内部構成を表示し、新しい設定パラメータの値を受け入れる Web ベースの設定ユーティリティが含まれます。またサーバは、リモート プロファイルの再同期とファームウェアのアップグレード操作を実行するための特殊な URL コマンド構文も受け入れます。

小売配布モデルでは、顧客は Cisco IP Phone を購入し、特定のサービスに加入します。Internet Telephony Service Provider（ITSP）は、プロビジョニング サーバを設定および保守し、サービス プロバイダーのサーバと再同期するよう電話をプロビジョニングします。

顧客は、サービスにログインし、オンライン ポータルを通じて VoIP のアカウントを設定し、割り当てられたサービス アカウントにデバイスをバインドします。プロビジョニングされていない Cisco IP Phone は、再同期 URL コマンドを用いて、特定のプロビジョニング サーバと再同期するよう指示されます。この URL コマンドには、通常、新しいアカウントにデバイスを関連付けるためのアカウントのカスタマー ID 番号または英数字コードが含まれています。

次の例では、SuperVoIP サービスに対してプロビジョニングするように、IP アドレス 192.168.1.102 を割り当てられた DHCP のデバイスが表示されます。

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

この例では、1234abcd が新しいアカウントのカスタマー ID 番号です。リモート プロビジョニング サーバは、URL と指定されたカスタマー ID に基づいて、再同期要求を実行している電話機と新しいアカウントを関連付けます。この最初の再同期操作を通じて、電話はシングル ステップで設定されます。電話は、まず再同期に、その後サーバ上の恒常的な URL へと自動的に送信されます。次に例を示します。

```
https://prov.supervoip.com/cisco-init
```

最初のアクセスと恒常的なアクセスのいずれの場合にも、プロビジョニング サーバは、HTTPS/SSL 接続のセキュリティを確保するために Cisco IP Phone のクライアント証明書を使用します。プロビジョニング サーバは、関連付けられたサービス アカウントに基づいて、正しい設定パラメータ値を指定します。

デバイスに電源が投入されるか、または指定した時間が経過すると、Cisco IP Phone は再同期し、最新の設定パラメータをダウンロードします。これらのパラメータにより、短縮ダイヤル番号の設定、BLF、ユーザが変更できる機能の制限などの目標に対応することができます。

関連項目

- 社内デバイスのプロビジョニング（3-3 ページ）

再同期プロセス

各 Cisco IP Phone のファームウェアには、新しい設定パラメータ値を受け入れる管理 Web サーバが含まれています。Cisco IP Phone は、デバイス プロファイルでの resync URL コマンドにより指定されたプロビジョニング サーバを使用してリブート後またはスケジュールされた間隔で再同期するように設定できる場合があります。

デフォルトでは、Web サーバは有効になっています。Web サーバを無効または有効にするには、resync URL コマンドを使用します。

必要に応じて、「resync」アクション URL を通じて、即時再同期を要求することができます。この resync URL コマンドには、ユーザのアカウントにデバイスを一意に関連付けるためのアカウントのカスタマー ID 番号または英数字コードが含まれている場合があります。

例

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/1234abcd
```

この例では、IP アドレス 192.168.1.102 が割り当てられた DHCP デバイスが、prov.supervoip.com の SuperVoIP サービスに対してプロビジョニングするように指定されています。新しいアカウントのカスタマー ID 番号は 1234abcd です。リモート プロビジョニング サーバは、URL とカスタマー ID に基づいて、再同期要求を実行している Cisco IP Phone とアカウントを関連付けます。

この最初の再同期操作を通じて、Cisco IP Phone はシングル ステップで設定されます。電話は、まず再同期に、その後サーバ上の恒常的な URL へと自動的に送信されます。

最初のアクセスと恒常的なアクセスのいずれの場合にも、プロビジョニング サーバは、認証にクライアント証明書を使用します。サーバは、関連付けられたサービス アカウントに基づいて、設定パラメータ値を指定します。

プロビジョニング

Cisco IP Phone は、リモート プロファイルのマッチングのため、定期的に、および電源を投入したときに、内部構成の状態を再同期するように設定できます。電話は、通常のプロビジョニング サーバ（NPS）またはアクセス コントロール サーバ（ACS）とコンタクトをとります。

デフォルトでは、Cisco IP Phone がアイドル状態になった場合にのみ、プロファイルの再同期が実行されます。この手順により、アップグレードがソフトウェアのリブートを発生させたり、通話が中断したりする事態を回避できます。以前のリリースから現在のアップグレード状態に到達するため、中間アップグレードが必要になった場合、アップグレード ロジックは、マルチステージ アップグレードを自動化できます。

通常のプロビジョニング サーバ

通常のプロビジョニング サーバ（NPS）には、TFTP、HTTP、HTTPS サーバを使用できます。リモート ファームウェア アップグレードは、TFTP か HTTP、または HTTPS を使用して実行されます。これは、ファームウェアに保護が必要な情報が含まれていないためです。

HTTPS は推奨しませんが、NPS との通信では、共有秘密キーを使用して更新されたプロファイルを暗号化できるため、セキュア プロトコルを使用する必要はありません。HTTPS の利用方法の詳細については、通信の暗号化（7 ページ）を参照してください。セキュアな最初のプロビジョニングは、SSL 機能を使用するメカニズムによって実現されます。プロビジョニングされていない Cisco IP Phone は、同デバイスを対象とする 256 ビット対称キー暗号化プロファイルを受信できます。

設定アクセス制御

Cisco IP Phone ファームウェアは、一部のパラメータへのエンドユーザのアクセスを制限する機能を提供します。ファームウェアは、**Admin** アカウントまたは **User** アカウントにサインインするのに必要な権限を提供します。各々を個別にパスワードで保護することができます。

- Admin アカウント—サービス プロバイダーがすべての管理 Web サーバ パラメータにフル アクセスできるようにします。
- ユーザ アカウント—ユーザが管理 Web サーバ パラメータのサブセットを設定できるようにします。

サービス プロバイダーは、プロビジョニング プロファイルのユーザ アカウントを次のように制限できます。

- 設定を作成する際に、ユーザ アカウントがどの設定パラメータを使用できるようにするかを示します。
- 管理 Web サーバへのユーザ アクセスを無効にします。
- LCD GUI のユーザ アクセスを無効にします。
- 再同期、アップグレード、または回線 1 に対する SIP 登録を目的として、デバイスからアクセスできるインターネット ドメインを制限します。

関連項目

- 要素タグのプロパティ（2-2 ページ）
- アクセス コントロール（2-4 ページ）

通信の暗号化

デバイスに送信される設定パラメータには、認証コードや、システムを不正アクセスから保護するその他の情報を含めることができます。サービス プロバイダーの関心事は、認証を受けていない顧客のアクティビティを阻止することです。顧客の関心事は、アカウントの不正な使用を阻止することです。サービス プロバイダーは、管理 Web サーバへのアクセスの制限に加えて、プロビジョニング サーバとデバイスの間における設定プロファイルの通信を暗号化できます。

電話のプロビジョニングの手順

通常、Cisco IP Phone は、ネットワークに初めて接続するときに、プロビジョニングを実行するよう設定されています。電話機は、サービス プロバイダーまたは VAR が電話機を事前プロビジョニング（設定）するときに設定されたスケジュール間隔でプロビジョニングされます。サービス プロバイダーは、VAR または上級ユーザが、電話のキーパッドを使用して電話を手動でプロビジョニングすることを許可できます。また、電話機の Web UI を使用してプロビジョニングを設定することもできます。

電話機の LCD UI から、[ステータス（Status）] > [電話ステータス（Phone Status）] > [プロビジョニング（Provisioning）] を確認するか、Web ベースの [設定ユーティリティ（Configuration Utility）] の [ステータス（Status）] タブで [プロビジョニング ステータス（Provisioning Status）] を確認します。

関連項目

- キーパッドからの手動による電話のプロビジョニング（1-8 ページ）

キーパッドからの手動による電話のプロビジョニング

手順 1　[アプリケーション（Applications）] を押します。

手順 2　[プロファイル ルール（Profile Rule）] を選択します。

手順 3　次の形式でプロファイル ルールを入力します。

protocol://server[:port]/profile_pathname

次に例を示します。

```
tftp://192.168.1.5/CP_x8xx_3PCC.cfg
```

プロトコルが指定されていない場合、TFTP が選択されます。サーバ名が指定されなかった場合は、URL を要求するホストがサーバ名として使用されます。ポートが指定されなかった場合は、デフォルト ポートが使用されます（TFTP 用の 69、HTTP 用の 80、または HTTPS 用の 443）。

手順 4　[再同期（Resync）] ソフトキー https://bst.cloudapps.cisco.com/bugsearch/ を押します。

関連項目

- 電話のプロビジョニングの手順（1-8 ページ）