



# プロビジョニング

---

- [プロビジョニングの概要 \(1 ページ\)](#)
- [プロビジョニング \(3 ページ\)](#)
- [TR69 プロビジョニング \(9 ページ\)](#)
- [通信の暗号化 \(11 ページ\)](#)
- [ネットワーク輻輳時の電話機の挙動 \(11 ページ\)](#)
- [社内での事前プロビジョニングとプロビジョニング サーバ \(11 ページ\)](#)
- [サーバの準備とソフトウェア ツール \(11 ページ\)](#)
- [社内デバイスの事前プロビジョニング \(14 ページ\)](#)
- [プロビジョニング サーバの設定 \(14 ページ\)](#)

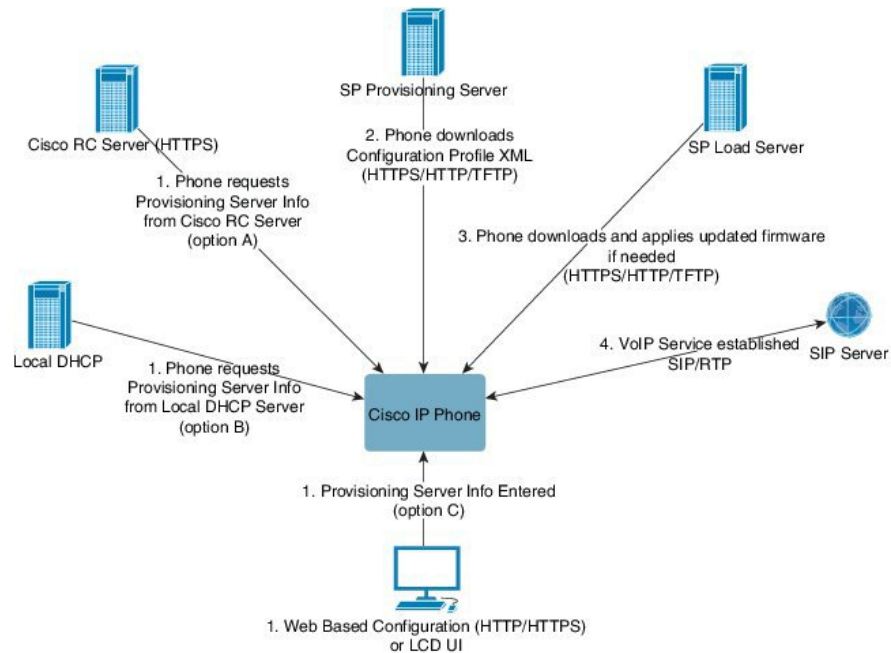
## プロビジョニングの概要

Cisco IP 電話は、自宅、ビジネスまたは企業環境の顧客を対象とした、Voice-over-IP (VoIP) サービスプロバイダーによる大規模な導入をねらいとしています。リモートでの管理と構成を使用した電話機のプロビジョニングにより、顧客側で電話機が適切に動作します。

電話機のカスタマイズされた現行の機能構成は、次を使用することでサポートされます。

- 電話機の信頼できるリモート制御。
- 電話機を制御する通信の暗号化。
- 合理化された電話機アカウントのバインディング。

電話機は、設定プロファイルまたは更新されたファームウェアをリモート サーバからダウンロードするようにプロビジョニングできます。ダウンロードは、電話機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、および設定された間隔で実行できます。プロビジョニングは通常、サービス プロバイダーによる共通の大規模 VoIP 導入の一部とされます。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。



電話機のプロビジョニングプロセスの概要は次のとおりです。

1. 電話機が設定されていない場合、次のいずれかのオプションを使用してプロビジョニングサーバ情報が電話機に適用されます。
  - **A** : HTTPS、DNS SRV、GDS (アクティベーションコードオンボーディング)、EDOS デバイスアクティベーションを使用して、Cisco 有効化データオーケストレーションシステム (EDOS) のリモートカスタマイズ (RC) サーバからダウンロードします。
  - **B** : ローカル DHCP サーバからクエリを実行します。
  - **C** : シスコフォンの Web ベースの設定ユーティリティ (Phone UI) を使用して手動で入力します。
2. 電話機は、HTTPS、HTTP、または TFTP プロトコルを使用してプロビジョニングサーバ情報をダウンロードし、構成の XML を適用します。
3. 電話機は更新されたファームウェアを、必要に応じて、HTTPS、HTTP、または TFTP を使用してダウンロードおよび適用します。
4. VoIP サービスは、指定された構成およびファームウェアを使用して確立されます。

VoIP サービスプロバイダーは、住宅やスモールビジネスの顧客に多くの電話機を導入することを目的としています。ビジネスまたはエンタープライズ環境で、電話機は端末ノードとして機能できます。プロバイダーはこれらのデバイスをインターネット上に広く分散します。デバイスは顧客宅内のルータやファイアウォールを介して接続されます。

電話機は、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。リモートでの管理と構成によって、顧客宅内で電話機が適切に動作します。

## プロビジョニング

リモートプロファイルに合わせて、電話機の内部の構成状態を定期的に、および電源投入時に、再同期するよう電話機を設定できます。電話機は通常のプロビジョニングサーバ（NPS）または Access Control Server（ACS）に接続します。

デフォルトでは、プロファイルの再同期は電話機がアイドル状態のときにのみ実行されます。この方法では、ソフトウェアのリブートがトリガーされたり、通話が中断されたりするアップグレードが回避されます。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に中間の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、または HTTPS サーバを使用できます。リモートファームウェアのアップグレードは、ファームウェアに機密情報が含まれていないため、TFTP または HTTP、あるいは HTTPS を使用して実現されます。

HTTPS が推奨されますが、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 の利用の詳細については、[通信の暗号化（11ページ）](#)を参照してください。安全な初回のプロビジョニングは、SSL機能を使用するメカニズムを通じて提供されます。プロビジョニングされていない電話機は、そのデバイスを対象にした256ビットの対称キーで暗号化されたプロファイルを受信できます。

## 電話のプロビジョニング方法

通常、Cisco IP 電話は最初にネットワークに接続したときにプロビジョニングされ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）する際に設定されたスケジュールされた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 や上級ユーザが、電話機のキーパッドを使用して電話機を手動でプロビジョニングすることを承認できます。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 の [ステータス (Status)] > [電話のステータス (Phone Status)] > [プロビジョニング (Provisioning)] を確認するか、Web ベース設定ユーティリティの [ステータス (Status)] タブにある [プロビジョニングステータス (Provisioning Status)] を確認してください。

## アクティベーションコードを使用した電話機のオンボード

この機能は、ファームウェアリリース 11-2-3MSR1、BroadWorks アプリケーション サーバリリース 22.0 (パッチ AP.as 22.0.1123、ap368163 およびその依存) で利用できます。ただし、この機能を使用するために、旧バージョンのファームウェアで電話機を変更することができます。

電話機に新しいファームウェアへのアップグレードと、アクティベーションコード画面をトリガーするための `gds://` プロファイルルールの使用を指示します。ユーザは、指定されたフィールドに 16 桁のコードを入力して、電話機を自動的にオンボードにします。

### 始める前に

アクティベーションコード経由でオンボードをサポートできるように `activation.webex.com` サービスがファイアウォールを通過できることを確認します。

### 手順

**ステップ 1** テキスト エディタまたは XML エディタで電話機の `config.xml` ファイルを編集します。

**ステップ 2** アクティベーションコードオンボードのプロファイルルールを設定するには、次の `config.xml` ファイルの例に従ってください。

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!-- Firmware Upgrade -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

**ステップ 3** 変更内容を `config.xml` ファイルに保存します。

## 短時間のアクティベーションコードを使用して自動プロビジョニングを有効にする

短時間アクティベーションコードを使用して自動プロビジョニングを有効にするには、以下の手順を実行します。

### 始める前に

お使いの電話機がファームウェアリリース 11.3 (1) 以降に更新されていることを確認してください。

リダイレクトプロファイル用の CDA サーバのセットアップ方法を確認します。

<https://community.cisco.com/t5/collaboration-voice-and-video/cisco-multi-platform-phones-cloud-provisioning-process/ta-p/3910244>



## HTTP プロビジョニング用DNS SRV

HTTP プロビジョニング用DNS SRV機能を使用すると、マルチプラットフォーム電話機の自動プロビジョニングが可能になります。ドメインネームシステムサービス (DNS SRV) レコードは、サービスとホスト名の間接続を確立します。電話機がプロビジョニングサービスの場所を検索する場合、まず指定された DNS SRV ドメイン名に対してクエリを実行し、次に SRV レコードを照会します。電話機は、サーバがアクセス可能であることを確認するためにレコードを検証します。次に、実際のプロビジョニングフローが続けられます。サービスプロバイダーは、この DNS SRV プロビジョニングフローを利用して自動プロビジョニングを提供することができます。

DNS SRV では、DHCP が提供するドメイン名の証明書で、ホスト名の検証を行います。すべての SRV レコードは、DHCP で指定されたドメイン名を含む有効な証明書を使用することが重要です。

DNS SRV クエリでは、次のように構造内の DHCP ドメイン名が含まれます。

`_<servicename>._<transport>.<domainName>`

例えば、`_ciscoprov-https._tls example.com`、電話機が `example.com` のルックアップを実行するように指示します。電話機は、DNS SRV クエリによって取得されたホスト名とポート番号を使用して、初期設定のダウンロードに使用される URL を作成します。

DNS SRV は、電話機が使用する多くの自動プロビジョニングメカニズムのうちの 1 つです。電話機は、次の順序でメカニズムの実行を試みます。

1. DHCP
2. DNS SRV
3. EDOS
4. GDS (アクティベーションコードオンボード)、または EDOS デバイスアクティベーション

次の表では、SRV レコードのフィールドについて説明します。

表 1: SRV レコード

フィールド	説明	例
<code>&lt;servicename&gt;</code>	サービス名は、下線で始まります。サーバサービスは、SRV レコードでシンボリック名を使用します。  サービスの後に、ピリオド(.)はサービスが確立され、次のセクションを開始されることを示します。	<code>_ciscoprov-https</code> 。または <code>_ciscoprov-http</code> 。  DNS SRV は、TFTP プロトコルをサポートしていません。TFTP を使用している場合、次のエラーメッセージが表示されます。エラー - TFTP スキームは、SRV ルックアップではサポートされていません。

フィールド	説明	例
<_proto.>	トランスポートプロトコルは、下線で始まります。 プロトコルに続くピリオドは、プロトコルセクションが終了したことを表します。	<b>_tls.</b> TLS で HTTPS を使用する必要があります。 または <b>_tcp.</b> TCP で HTTP を使用する必要があります。
domainName	サービスのドメイン名は、プロトコルの後に続きます。 ホスト名の検証：すべての SRV レコードは、元の DHCP 指定ドメイン名に基づいて検証されます。すべてのレコードが元のドメイン名を含む有効な証明書を使用していることが重要です。	<b>example.com</b>
TTL（存続可能時間）	レコードの有効期限の値 (秒単位)。	86400
クラス	インターネットタイプ—SRV レコードであることを示す標準 BIND 表記。	IN
<プライオリティ>	各回線には、優先順位番号が含まれています。番号が小さいほど、電話機は、この DNS SRV レコードに含まれるターゲットホスト名とポートを試行する順番が早くなります。	<b>10</b>
<ウェイト>	2つ以上のサービスが同じ優先順位を持っている場合、ウェイト番号によって先に処理される回線が決定されます。番号が小さいほど、電話機は、この DNS SRV レコードに含まれるターゲットホスト名とポートを試行する順番が早くなります。	<b>20</b>
<port>	オプションポート番号	<b>5060</b>
<ターゲット>	サービスを提供しているマシンの A レコード。 A レコードは、最も基本的なタイプの DNS レコードであり、ドメインまたはサブドメインを IP アドレスに置き換えるために使用されます。	<b>pr1.example.com</b>

### SRV 設定例

```
_service._proto.name. TTL クラス SRV プライオリティウェイトポートターゲット。
_ciscoprov-https._tls.example.com. 86400 IN SRV 10 10 5060 vcse.example.com.
_ciscoprov-https._tls.example.com. 86400 IN SRV 10 20 5060 pr2.example.com.
```

```
_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 50 5060 px1.example.com.  
_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 30 5060 px2.example.com.
```

## HTTP プロビジョニングに DNS SRV を使用する

新しい電話機は、自動プロビジョニングの1つの方法として DNS SRV を使用します。既存の電話機で、ネットワークが HTTP の DNS SRV を使用したプロビジョニング用に設定されている場合は、この機能を使用して電話機を再同期することができます。サンプルコンフィギュレーションファイル

```
<flat-profile>  
<!-- System Configuration -->  
<Primary_DNS ua="rw">10.89.68.150</Primary_DNS>  
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>  
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>  
<Profile_Authentication_Type ua="na">Basic Http Authentication  
</Profile_Authentication_Type>  
<Proxy_1_ ua="na">example.com</Proxy_1_>  
<Display_Name_1_ ua="na">4081001141</Display_Name_1_>  
<User_ID_1_ ua="na">4081001141</User_ID_1_>  
</flat-profile>
```

### 手順

---

次のいずれかの操作を実行します。次に [ウェブページ上の SRV オプションを使用してプロファイルルールを設定する \(8 ページ\)](#)、または [電話機上での SRV オプションを使用したプロファイルルールを設定 \(9 ページ\)](#)

- XML 設定ファイル (\$PSN.xml) をウェブサーバのルートディレクトリに配置します。
- XML 設定ファイル (\$MA.cfg) をウェブサーバのルートdirectory/Cisco/に配置します。

## ウェブページ上の SRV オプションを使用してプロファイルルールを設定する

SRV オプションを使用すると、設定ファイルを電話機にダウンロードすることができます。

### 始める前に

[電話機 ウェブインターフェイスへのアクセス](#)

### 手順

---

**ステップ 1** 音声 > プロビジョニング を選択します。

**ステップ 2** [プロファイルルール] フィールドに、SRV オプションを含むプロファイルルールを入力します。HTTP プロトコルと HTTP プロトコルのみがサポートされています。

例：



```
[--srv] https://example.com/$PSN.xml
```

## 電話機上での SRV オプションを使用したプロファイルルールの設定

電話機では、SRVオプションを使用して設定ファイルをダウンロードすることができます。

### 手順

**ステップ 1** [設定 (Settings)] を押します。

**ステップ 2** [デバイス管理 (Device administration)] > [プロファイルルール (Profile rule)] を選択します。

**ステップ 3** [--Srv] パラメータでプロファイルルールを入力します。HTTPプロトコルとHTTPSプロトコルのみがサポートされています。

例：

```
[--srv] https://example.com/$PSN.xml
```

**ステップ 4** [再同期 (Resync)] を押します。

## TR69 プロビジョニング

Cisco IP 電話では、管理者が Web UI を使用して TR69 パラメータを設定できます。パラメータについては (XML パラメータと TR69 パラメータの比較など)、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。

電話機は、DHCP オプション 43、60、および 125 の自動コンフィギュレーションサーバ (ACS) ディスカバリをサポートします。

- オプション 43 : ACS URL に関するベンダー固有の情報。
- オプション 60 : 電話機が dslforum.org で自身を ACS に対して識別するためのベンダークラス ID。
- オプション 125 : ゲートウェイ関連付けに関するベンダー固有の情報。

## TR69 RPC メソッド

### サポートされている RPC メソッド

電話機は、次のように、限定されたりリモート プロシージャ コール (RPC) メソッドのみをサポートします。

- GetRPCMethods

- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download : ダウンロード RPC メソッド。サポートされるファイル 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
  - カスタム認証局 (CA) ファイル
- Transfer Complete

## サポートされているイベント タイプ

電話機は、サポートされている機能とメソッド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 タイプのみサポートされます。

- Bootstrap
- Boot
- value change
- connection request
- Periodic
- Transfer Complete
- M Download
- M Reboot

## 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、または不正なアクセスからシステムを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、不正な顧客のアクティビティを防ぐことです。顧客の関心事は、アカウントの不正使用を防ぐことです。サービスプロバイダーは、管理 Web サーバへのアクセス制限に加え、プロビジョニングサーバとデバイス間の設定プロファイルの通信を暗号化できます。

## ネットワーク輻輳時の電話機の挙動

ネットワークパフォーマンスの低下の原因となるものは、電話の音声に影響を及ぼすため、場合によっては、通話が中断される可能性があります。ネットワークパフォーマンスの低下は、次のような原因が考えられます。

- 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
- サービス拒否攻撃など、ネットワーク上で発生した攻撃

## 社内での事前プロビジョニングとプロビジョニングサーバ

サービスプロバイダーは、プロファイルを使用して、RC ユニット以外で、電話機を事前プロビジョニングします。事前プロビジョニングプロファイルには、電話機を再同期するための制限されたパラメータを含めることができます。プロファイルには、リモートサーバで提供されるすべてのパラメータを含めることもできます。デフォルトでは、電話機は電源投入時に、プロファイルで設定された間隔で再同期します。ユーザが顧客宅内の電話機に接続すると、デバイスは更新されたプロファイルとすべてのファームウェア アップデートをダウンロードします。

この事前プロビジョニング、導入、およびリモートプロビジョニングのプロセスには、さまざまな方法があります。

## サーバの準備とソフトウェア ツール

この章の例では、1 台以上のサーバが使用可能であることが必要です。以下のサーバをローカル PC にインストールして実行できます。

- TFTP (UDP ポート 69)
- syslog (UDP ポート 514)
- HTTP (TCP ポート 80)

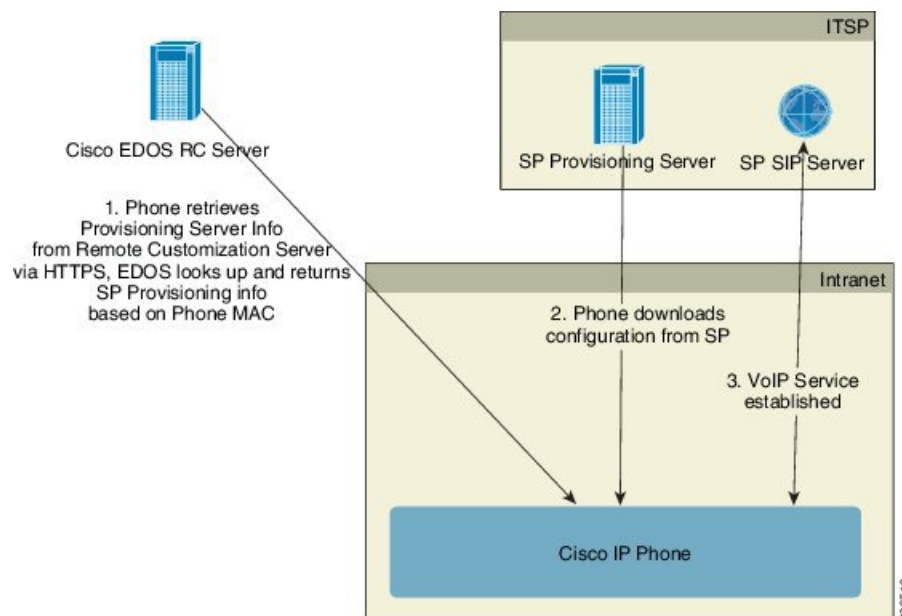
- HTTPS (TCP ポート 443)

サーバの構成をトラブルシューティングする場合は、サーバのタイプごとに、クライアントを別のサーバマシンにインストールすると便利です。この方法により、電話機との通信に関係なく、適切なサーバ動作になります。

また、次のソフトウェア ツールをインストールすることをお勧めします。

- 設定プロファイルを生成するために、オープンソースの `gzip` 圧縮ユーティリティをインストールします。
- プロファイルの暗号化および HTTPS 操作用に、オープンソースの `OpenSSL` ソフトウェアパッケージをインストールします。
- HTTPS を使用してダイナミック プロファイルの生成とワンステップのリモートプロビジョニングをテストするには、CGI スクリプトをサポートするスクリプト言語をお勧めします。オープンソースの `Perl` 言語ツールは、このようなスクリプト言語の一例です。
- プロビジョニングサーバと電話機間の安全な交換を確認するには、イーサネットパケットスニファ (無料でダウンロード可能な `Ethereal/Wireshark` など) をインストールします。電話機とプロビジョニングサーバ間の相互通信のイーサネットパケットトレースをキャプチャします。これを行うには、ポートミラーリング対応のスイッチに接続されている PC でパケットスニファを実行します。HTTPS トランザクションの場合は、`ssldump` ユティリティを使用できます。

## リモートカスタマイズ (RC) 配信



すべての電話機は、最初にプロビジョニングされるまで Cisco EDOS RC サーバに接続します。

RC 配信モデルでは、顧客はすでに Cisco EDOS RC サーバの特定のサービスプロバイダーに関連付けられている電話機を購入します。インターネット電話サービスプロバイダー (ITSP) は、プロビジョニングサーバを設定および保持し、それらのプロビジョニングサーバの情報を Cisco EDOS RC サーバに登録します。

インターネットに接続して電話機の電源を投入すると、プロビジョニングされていない電話機の [カスタマイズ状態 (Customization State)] は [オープン (Open)] になります。電話機は最初にローカル DHCP サーバにプロビジョニングサーバ情報を照会し、電話機のカスタマイズ状態を設定します。DHCP クエリが成功すると、[カスタマイズ状態 (Customization State)] は、[中止 (Aborted)] となり、DHCP が必要なプロビジョニングサーバ情報を提供するため RC は試行されません。

電話機を初めてネットワークに接続する場合、または初期設定へのリセット後にネットワークに接続する場合に、セットアップされている DHCP オプションがないと、電話機はゼロタッチプロビジョニングのためにデバイスアクティベーションサーバに接続します。新しい電話機は、プロビジョニングに「webapps.cisco.com」の代わりに「activate.cisco.com」を使用します。11.2(1) より前のファームウェアを搭載している電話機は、引き続き webapps.cisco.com を使用します。ファイアウォールで両方のドメイン名を許可することが推奨されます。

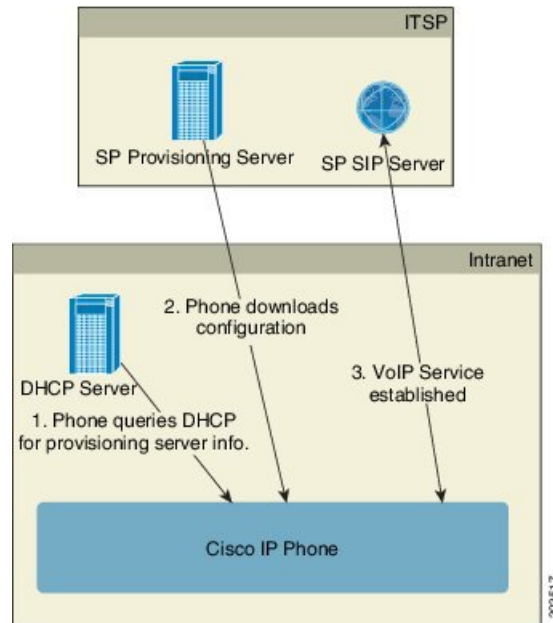
DHCP サーバがプロビジョニングサーバ情報を提供しない場合、電話機は Cisco EDOS RC サーバに照会して、その MAC アドレスとモデルを指定し、[カスタマイズ状態 (Customization State)] は [保留中 (Pending)] に設定されます。Cisco EDOS サーバは、プロビジョニングサーバの URL を含む、関連付けられたサービスプロバイダーのプロビジョニングサーバ情報で応答し、電話機の [カスタマイズ状態 (Customization State)] は、[カスタム保留中 (Custom Pending)] に設定されます。電話機は、resync URL コマンドを実行してサービスプロバイダーの設定を取得し、成功すると、[カスタマイズ状態 (Customization State)] は、[取得済み (Acquired)] になります。

Cisco EDOS RC サーバに、電話機に関連付けられているサービスプロバイダーがない場合、電話機の [カスタマイズ状態 (Customization State)] は [利用不可 (Unavailable)] になります。電話機を手動で設定するか、電話機のサービスプロバイダーの場合は Cisco EDOS サーバに関連付けを追加できます。

電話機が LCD または Web 設定ユーティリティでプロビジョニングされた場合、[カスタマイズ状態 (Customization State)] が [取得済み (Acquired)] になる前に、[カスタマイズ状態 (Customization State)] は [中止 (Aborted)] に設定され、電話機が初期設定にリセットされない限り、Cisco EDOS サーバは照会されません。

電話機がプロビジョニングされている場合、電話機が初期設定にリセットされない限り、Cisco EDOS RC サーバは使用できません。

## 社内デバイスの事前プロビジョニング



シスコの工場出荷時のデフォルト設定により、電話機は TFTP サーバのプロファイルと自動的に再同期を試みます。LAN 上で管理される DHCP サーバは、プロファイルに関する情報と、デバイスへの事前プロビジョニング用に設定された TFTP サーバに関する情報を提供します。サービス プロバイダーは、新しい電話機をそれぞれ LAN に接続します。電話機はローカルの TFTP サーバと自動的に再同期して、内部の状態を導入準備に初期化します。この事前プロビジョニングプロファイルには通常、リモートプロビジョニングサーバの URL が含まれます。プロビジョニングサーバは、デバイスが導入されて顧客ネットワークに接続された後、デバイスの更新を継続します。

電話機が顧客に出荷される前に、事前プロビジョニング済みデバイスのバーコードをスキャンしてその MAC アドレスまたはシリアル番号を記録できます。この情報は、電話機が再同期するプロファイルを作成するために使用できます。

顧客は電話機を受け取ると、ブロードバンドリンクにそれを接続します。電源を投入すると、電話機は事前プロビジョニングで設定された URL を使ってプロビジョニングサーバに接続します。これで電話機は、必要に応じてプロファイルやファームウェアを再同期して更新できます。

## プロビジョニングサーバの設定

このセクションでは、さまざまなサーバやシナリオを使用して電話機をプロビジョニングする際の設定要件を説明します。このドキュメントおよびテスト目的において、プロビジョニングサーバはローカル PC にインストールされ、実行されます。また、一般的に利用できるソフトウェア ツールは、電話機のプロビジョニングに役立ちます。

## TFTP のプロビジョニング

電話機は、プロビジョニングの再同期とファームウェアアップグレード両方の操作で TFTP をサポートします。デバイスをリモートで導入する場合、HTTPS が推奨されますが、HTTP や TFTP も使用できます。次に、ファイル暗号化をプロビジョニングしてセキュリティを強化します。NAT やルータ保護機能があれば、信頼性が高まります。TFTP は、プロビジョニングされていない多数のデバイスを社内で事前にプロビジョニングする場合に役立ちます。

電話機は、DHCP オプション 66 を使用して DHCP サーバから直接 TFTP サーバの IP アドレスを取得することができます。その TFTP サーバのファイルパスを使用して Profile\_Rule を設定している場合、デバイスは TFTP サーバからそのプロファイルをダウンロードします。ダウンロードは、デバイスが LAN に接続されているときに、電源投入時に実行されます。

工場出荷時のプロファイルを使用するデバイスの場合、電源投入時に、DHCP オプション 66 で指定したローカル TFTP サーバ上のこのファイルと再同期します。ファイルパスは、TFTP サーバの仮想ルート ディレクトリへの相対パスです。

## リモート エンドポイント制御と NAT

電話機はネットワーク アドレス変換 (NAT) と互換性があり、ルータ経由でインターネットにアクセスします。セキュリティを強化するため、ルータは、Symmetric NAT (インターネットから、保護されたネットワークに入ることを許可されるパケットを厳格に制限するパケットフィルタリング方針) の実装により、不正な着信パケットのブロックを試みる可能性があります。このため、TFTP を使用するリモート プロビジョニングはお勧めできません。

VoIP は、NAT トラバーサルの一部の形式が提供されている場合のみ NAT と共存できます。Simple Traversal of UDP through NAT (STUN) を設定します。このオプションでは、ユーザに以下が必要です。

- サービスのダイナミックな外部 (パブリック) IP アドレス
- STUN サーバ ソフトウェアを実行しているコンピュータ
- Asymmetric NAT 機能を備えたエッジデバイス

## HTTP のプロビジョニング

電話機は、リモート インターネット サイトの Web ページを要求するブラウザのように動作します。これにより、顧客のルータに Symmetric NAT や他の保護機能が実装されている場合でも、プロビジョニングサーバと通信するための信頼性の高い手段が提供されます。リモートの導入では、特に導入するユニットが社内のファイアウォールや NAT が有効なルータの背後で接続されている場合は、TFTP よりも HTTP や HTTPS の方が信頼性が高くなります。HTTP と HTTPS は次の要求タイプの説明では同じ意味で使用されます。

基本の HTTP ベースのプロビジョニングは、HTTP GET メソッドに依存して設定プロファイルを取得します。通常、導入されている電話機ごとに 1 つの設定ファイルが作成され、これらのファイルは HTTP サーバ ディレクトリ内に保存されます。サーバは GET リクエストを受け取ると、GET リクエスト ヘッダーで指定されるファイルを単純に返します。

カスタマーデータベースを照会してプロファイルをすぐに作成することで、静的プロファイルよりも、設定プロファイルを動的に生成できます。

電話機は、再同期を要求するときに、HTTP POST メソッドを使用して再同期設定データを要求できます。デバイスを設定して、特定のステータスと識別情報を HTTP POST リクエストの本文に含めてサーバに送信できます。サーバはこの情報を使用して必要な応答設定ファイルを生成したり、状態情報を保存して後から分析やトラッキングを実行したりできます。

GET および POST リクエストの両方の一部として、電話機はリクエストヘッダーの User-Agent フィールドに基本識別情報を自動的に含めます。この情報で、デバイスの製造者、製品名、現在のファームウェアバージョン、および製品シリアル番号を伝えます。

次の例は、CP-7832-3PCC の User-Agent リクエスト フィールドです。

```
User-Agent: Cisco-CP-7832-3PCC/11.0.1 (00562b043615)
```

ユーザエージェントは設定可能であり、設定されていない場合、電話機はこの値を使用します (デフォルト)。

電話機が HTTP を使用して設定プロファイルと再同期するように設定されている場合は、秘密情報を保護するために HTTPS を使用するか、プロファイルを暗号化することをお勧めします。HTTP を使用してダウンロードするプロファイルは、暗号化することで、設定ファイルに含まれている秘密情報が漏洩される危険性を防ぐことができます。この再同期モードでは、プロビジョニング サーバの処理負荷が HTTPS を使用する場合に比べて少なくなります。

電話機は、次のいずれかの暗号化方式で暗号化されたプロファイルを復号化できます：

- AES-256-CBC 暗号化
- RFC-8188 ベースの暗号化と AES-128-GCM 暗号化



(注) 電話機は、HTTP Version 1.0 と HTTP Version 1.1 をサポートし、HTTP Version 1.1 がネゴシエートトランスポートプロトコルの場合にはチャンク エンコードをサポートします。

## 再同期およびアップグレードでの HTTP ステータス コードの処理

電話機は、リモートプロビジョニング (再同期) に HTTP 応答をサポートします。現在の電話機の動作は、次の 3 つに分類されます。

- A : 成功。この場合、[定期再同期 (Resync Periodic) ] 値および [再同期ランダム遅延 (Resync Random Delay) ] 値により以降のリクエストが決定します。
- B : ファイルが見つからない、またはプロファイルの破損による失敗。[再同期エラー再試行遅延 (Resync Error Retry Delay) ] 値により以降のリクエストが決定します。
- C : 不正な URL または IP アドレスによる接続エラーが発生したことによるその他の失敗。[再同期エラー再試行遅延 (Resync Error Retry Delay) ] 値により以降のリクエストが決定します。



表 2: HTTP 応答での電話機の動作

HTTP ステータスコード	説明	電話機の動作
<b>301 Moved Permanently</b>	このリクエストと以降のリクエストは新しい場所送信する必要があります。	新しい場所でリクエストをすぐに再試行します。
<b>302 Found</b>	一時的な移動です。	新しい場所でリクエストをすぐに再試行します。
<b>3xx</b>	他の 3 xx 応答は処理されません。	C
<b>400 Bad Request</b>	シンタックスが無効なため、リクエストを処理できません。	C
<b>401 Unauthorized</b>	基本またはダイジェストのアクセス認証チャレンジ。	認証情報を使用してリクエストをすぐに再試行します。最大 2 回再試行できます。失敗した場合、電話機の動作は C です。
<b>403 Forbidden</b>	サーバが応答を拒否しています。	C
<b>404 Not Found</b>	リクエストされたリソースが見つかりません。以降のクライアントからのリクエストは許可されます。	B
<b>407 プロキシ認証が必要</b>	基本またはダイジェストのアクセス認証チャレンジ。	認証情報を使用してリクエストをすぐに再試行します。最大 2 回再試行できます。失敗した場合、電話機の動作は C です。
<b>4xx</b>	他のクライアントエラー ステータスコードは処理されません。	C
<b>500 内部サーバエラー</b>	一般的なエラー メッセージ。	電話機の動作は C です。
<b>501 実装されない</b>	サーバがリクエスト方法を認識しないか、リクエストを実行する機能がありません。	電話機の動作は C です。
<b>502 不正なゲートウェイ</b>	サーバはゲートウェイまたはプロキシとして動作し、アップストリームサーバから無効な応答を受信しています。	電話機の動作は C です。

HTTPステータスコード	説明	電話機の動作
<b>503 サービスは利用不可です</b>	サーバは現在使用できません（メンテナンスのため過負荷状態またはダウンしています）。これは一時的な状態です。	電話機の動作は C です。
<b>504 Gateway Timeout</b>	サーバはゲートウェイまたはプロキシとして動作し、アップストリームサーバから適切なタイミングで応答を受信しません。	C
<b>5xx</b>	その他のサーバエラー	C