CHAPTER 1

導入とプロビジョニング

プロビジョニングの概要

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、大量の Voice-over-IP（VoIP）導入の一部として行われ、サービス プロバイダーに限定されます。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。

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。

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

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

電話への悪影響を減らしたり、なくしたりするには、電話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するか、テストから電話を除外してください。

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 PIN 番号または英数字コードが含まれます。

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 PIN 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 PIN を使用して、再同期要求を実行している電話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、認証に Cisco IP Phone 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、指定した時間が経過すると、Cisco IP Phone は再同期し、最新の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、ハント グループの設定、スピード ダイヤル番号の設定、およびユーザが変更できる機能の制限といった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（3-2 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 プロファイルの再同期 URL コマンドで指定したプロビジョニング 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 PIN 番号または英数字コードが含まれます。

例

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

この例では、`prov.supervoip.com` で 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。新しいアカウントの PIN 番号は 1234abcd です。リモート プロビジョニング サーバは、URL と PIN を使用して、再同期要求を実行している Cisco IP Phone 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、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 または HTTP を使用して実行されますが、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、HTTPS を使用して実行されることはありません。

NPS と通信する場合、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。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。

プロビジョニングの状態

状態	説明
MFG-RESET 製造時の状態へのリセット	デバイスは、完全にプロビジョニング前の状態に戻ります。設定可能なすべてのパラメータは、デフォルト値に戻ります。 IVR をサポートしていない電話の場合、LCD の [セットアップ(Setup)] で、工場出荷時の状態へのリセットを実行します。 エンドユーザが製造時の状態へのリセットを実行できるようにすることで、いつでもデバイスをアクセス可能な状態に戻すことが可能になります。
SP-CUST サービス プロバイダーのカスタマイズ	Profile_Rule パラメータは、サービス プロバイダーに固有のプロビジョニング サーバを使用して、デバイス固有の設定プロファイルをポイントします。次の方法で再同期を開始します。 • ローカル DHCP サーバを使用した自動設定—DGCP が、TFTP サーバ名または IPv4 アドレスを指定します。TFTP サーバには、設定ファイル内の Profile_Rule パラメータが含まれています。 • 再同期 URL のエントリー この URL は、Web ブラウザを起動し、URL 構文を入力して、特定の TFTP サーバ に再同期するよう要求します。 http://*x.x.x.x*/admin/resync?*prvserv*/*device.cfg* 引数の説明 *x.x.x.x*—Cisco IP Phone の IP アドレス *prvserv*—対象とする TFTP サーバ *device.cfg*—サーバ上の設定ファイルの名前。 • Profile_Rule パラメータの編集— Web インターフェイスのプロビジョニング ペインを開き、Profile_Rule パラメータに TFTP の URL を入力します。たとえば、*prserv*/cp-x8xx-3pcc.cfg のように入力します。 • 設定ファイルの Profile_Rule の変更—特定の TFTP サーバ に接続し、MAC アドレスの指定する設定ファイルを要求します。 たとえば、このエントリによって、プロビジョニング サーバと接続し、$MA パラメータの指定する MAC アドレスを持つデバイスに固有のプロファイルを要求します。 `Profile_Rule tftp.callme.com/profile/$MA/cp-x8xx-3pcc.cfg;`

状態	説明

SEC-PRV-1
セキュアなプロビジョニング—初期設定
	最初に、デバイス固有の CFG ファイルが、より強固な暗号化を有効にするよう、デバイス プロファイルを再設定します。CFG ファイルは、256 ビット暗号キーをプログラムし、ランダムに生成された TFTP ディレクトリをポイントします。たとえば、CFG ファイルに次のキーが含められる場合があります。
	`Profile_Rule [--key $A] tftp.callme.com/profile/$B/cp-x8xx-3pcc.cfg;`
	`GPP_A 8e4ca259…;  # 256 bit key`
	`GPP_B Gp3sqLn…;  # random CFG file path directory`

SEC-PRV-2 セキュアなプロビジョニング—完全設定	最初の SEC-PRV-1 プロビジョニングの後、プロファイルの再同期操作は、256 ビット暗号化 CFG ファイルを取得します。CFG ファイルは、Cisco IP Phone を、プロビジョニング サーバに同期されている状態に保ちます。 プロファイル パラメータは、この暗号化プロファイルによって再設定され、保持されます。SEC-PRV-2 設定の暗号キーとランダムなディレクトリ内の場所を定期的に変更して、セキュリティを強化することも可能です。

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。
- IVR を使用して、工場出荷時の状態にリセットする機能を無効にします。
- 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)
- LCD GUI のアクセス制御 (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。電話は、サービス プロバイダーまたは VAR が電話を事前プロビジョニング（設定）するときに設定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 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。

電話のミュート ボタンは、プロビジョニング プロセスのステータスを示すために次のパターンで点滅します。

- 赤/オレンジでゆっくりと点滅（1.0 秒点灯、1.0 秒消灯）—サーバにコンタクト中ですが、サーバは解決不能、接続不能であるか、サーバがダウンしています。
- 赤/オレンジで速く点滅（0.2 秒点灯、0.2 秒消灯、0.2 秒点灯、1.4 秒消灯）—見つからないファイルや破損したファイルでサーバが応答しています。

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（1-6 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

ステップ 1　[セットアップ（Setup）] を押してから、[プロファイル ルール（Profile Rule）] にスクロールします。

ステップ 2　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）。

ステップ 3　[再同期（Resync）] ソフトキーを押します。

関連項目

- 電話のプロビジョニングの手順（1-6 ページ）