CHAPTER 3

社内でのプロビジョニングおよびプロビジョニング サーバ

社内でのプロビジョニングおよびプロビジョニング 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 ユニット以外に Cisco IP Phone のプロビジョニングを行います。プロビジョニング プロファイルには、Cisco IP Phone を再同期するためのパラメータをある程度含めることができます。プロファイルには、リモート サーバから提供されるすべてのパラメータが記載できます。デフォルトでは、電源投入時と、プロファイルで設定された間隔で、Cisco IP Phone が再同期を行います。ユーザが顧客の環境で Cisco IP Phone 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のアップデートをダウンロードします。

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、多くの方法があります。

サーバの準備とソフトウェア ツール

本章の例では、1 台以上のサーバが必要です。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）

サーバの構成でのトラブルシューティングを容易にするために、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してください。このプラクティスでは、Cisco IP Phone との相互通信とは無関係に、サーバの動作を適切に設定します。

Cisco は、以下のソフトウェア ツールもインストールすることを推奨します。

- 設定プロファイルを生成する場合には、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 動作を使用する場合には、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 プロファイル生成とワンステップ リモート プロビジョニングをテストする場合には、CGI スクリプトをサポートするスクリプト言語のインストールを推奨します。そのようなスクリプト言語には、オープン ソースの Perl 言語ツールなどがあります。
- プロビジョニング サーバと Cisco IP Phone 間の安全なデータ交換を確認する場合には、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。Cisco IP Phone とプロビジョニング サーバ間の相互通信におけるイーサネット パケット トレースを採取します。このためには、ポートのミラーリングが有効になっているスイッチに接続している 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には、ssldump ユーティリティが使用できます。

社内デバイスのプロビジョニング

Cisco の工場出荷時のデフォルト設定により、Cisco IP Phone は自動的に、TFTP サーバのプロファイルとの再同期を試みます。LAN 上で管理されている 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 Cisco IP Phone をそれぞれ LAN に接続します。Cisco IP Phone は自動的にローカル TFTP サーバと再同期して、自身を導入準備状態に初期化します。このプロビジョニング 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 が含まれています。プロビジョニング サーバは、デバイスが導入されて顧客のネットワークに接続された後に、デバイスの更新を継続して行います。

Cisco IP Phone が顧客に出荷される前に、プロビジョニング済みデバイスのバーコードがスキャンされ、その MAC アドレスとシリアル番号が記録されます。この情報は、Cisco IP Phone が再同期するプロファイルを作成するのに使用できます。

顧客は Cisco IP Phone を受け取ると、それをブロードバンド リンクに接続します。電源投入後、Cisco IP Phone はプロビジョニング中に設定された URL を使用して、プロビジョニング サーバに接続します。このようにして、Cisco IP Phone は必要に応じてプロファイルと再同期し、ファームウェアを更新します。

プロビジョニング サーバの設定

ここでは、さまざまなサーバやシナリオを使用する場合の、Cisco IP Phone のプロビジョニングの設定要件について説明します。このドキュメントの目的およびテスト上の都合から、プロビジョニング サーバはローカル PC にインストールして実行します。また、Cisco IP Phone のプロビジョニングには、一般的に利用可能なソフトウェア ツールも有用です。

TFTP のプロビジョニング

Cisco IP Phone は、プロビジョニングの再同期およびファームウェア アップグレード動作の両方で TFTP をサポートします。デバイスをリモートで導入する際には、信頼性に優れ、NAT およびルータ保護機能を有する HTTP をプロビジョニングに使用することを推奨します。TFTP は、社内にあるプロビジョニングされていない大量のデバイスをプロビジョニングするのに有用です。

Cisco IP Phone 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 アドレスを取得できます。Profile_Rule にその TFTP サーバのファイルパスが設定されている場合、デバイスは TFTP サーバから自身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 に接続されている場合に電源投入時に行われます。

工場出荷時のデフォルト設定で提供される Profile_Rule は *$PN*.cfg です。*$PN* には、CP-7841-3PCC などの電話機のモデル名が入ります。たとえば、CP-8841-3PCC の場合、ファイル名は CP-8841-3PCC.cfg になります。プロファイルが工場出荷時設定のままのデバイスは、電源投入後、DHCP オプション 66 で指定されたローカル TFTP サーバにあるこのファイルと再同期します（ファイルパスは、TFTP サーバ仮想ルート ディレクトリへの相対パスです）。

関連項目

- 社内デバイスのプロビジョニング（3-2 ページ）

リモート エンドポイント制御と NAT

Cisco IP Phone は、ネットワーク アドレス変換（NAT）を利用して、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、不正な受信パケットのブロックを試みる可能性があります。したがって、TFTP を使用したリモート プロビジョニングは推奨しません。

Voice over IP は、NAT トラバーサルのフォームの一部が提供されている場合にのみ、NAT で使用できます。Simple Traversal of UDP through NAT（STUN）を設定します。このオプションでは以下が必要です。

- サービスのダイナミック外部（パブリック）IP アドレス
- STUN サーバ ソフトウェアが動作するコンピュータ
- Symmetric NAT 機能を備えたエッジ デバイス

HTTP のプロビジョニング

Cisco IP Phone 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、導入されるユニットが社内のファイアウォールまたは NAT 機能が有効なルータの背後に接続される場合に、TFTP よりも HTTP および HTTPS を使用した方が信頼性が高くなります。

基本的な HTTP ベースのプロビジョニングでは、HTTP GET メソッドを使用して設定プロファイルを取得します。通常、導入される Cisco IP Phone ごとに設定ファイルが 1 つ作成され、それらは HTTP サーバのディレクトリに保存されます。サーバが GET リクエストを受信すると、GET リクエスト ヘッダーで指定されたファイルを単純に返します。

または、リクエストされた URL により、GET メソッドを使用して CGI スクリプトが起動される場合もあります。カスタマー データベースのクエリやオンザフライでのプロファイルの作成により、設定プロファイルが動的に生成されます。

CGI により再同期リクエストが処理される際、Cisco IP Phone は HTTP POST メソッドを使用して再同期設定データをリクエストできます。デバイスを設定して、特定ステータスと識別情報を HTTP POST リクエストの本文内にまとめてサーバに送信することができます。サーバはこの情報を使用して、必要な応答設定プロファイルを生成したり、後で分析やトラッキングに使用するためにステータス情報を保存したりします。

GET および POST のリクエストの一部として、Cisco IP Phone 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入力します。この情報には、デバイスの製造者、製品名、現行のファームウェア バージョン、および製品シリアル番号が含まれています。

次は、CP-8841-3PCC の場合の User-Agent リクエスト フィールドの例です。

```
User-Agent: cisco/CP-8841-3PCC (88012BA01234)
```

Cisco IP Phone が HTTP を使用して設定プロファイルと再同期するよう設定されている場合、機密情報を保護するためにプロファイルを暗号化することを推奨します。Cisco IP Phone では、プロファイルの暗号化に CBC モードの 256 ビット AES をサポートしています。HTTP を使用して Cisco IP Phone によりダウンロードされるプロファイルを暗号化すれば、設定プロファイル内の機密情報が漏えいする危険性が回避されます。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 を使用するよりも少なくなります。

(注)　Cisco IP Phone 7800 シリーズ、および 8800 シリーズ Multiplatform Phone は、HTTP Version 1.0、HTTP Version1.1 をサポートします。また、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

この電話機では、リモート プロビジョニング（再同期）時に強化された HTTP 応答が使用できます。現在の電話機は、次の 3 つの方法に分類されます。

- A：成功。この場合、[定期再同期（Resync Periodic）] の値および [再同期ランダム遅延（Resync Random Delay）] の値により以降のリクエストが変わります。
- 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）] の値により以降のリクエストが変わります。
- C：不正な URL または IP アドレスにより接続エラーが発生した場合のその他の失敗。[再同期エラー再試行遅延（Resync Error Retry Delay）] の値により以降のリクエストが変わります。

表 3-1　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
301 Moved Permanently	このリクエストおよび以降のリクエストは、新しい場所に向けて送信する必要があります。	新しい場所を使用してリクエストをすぐに再試行します。
302 Found	一時的に移動されています。	新しい場所を使用してリクエストをすぐに再試行します。
3xx	その他の 3xx 応答は処理されません。	C
400 Bad Request	シンタックスが無効なため、要求を処理できません。	C
401 Unauthorized	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 回試行します。これが失敗すると、電話機の動作は C です。
403 Forbidden	サーバが応答を拒否しました。	C

表 3-1　HTTP 応答での電話機の動作（続き）

HTTP ステータス コード	説明	電話機の動作
404 Not Found	リクエストされたリソースが見つかりません。これに続くクライアントからのリクエストは問題なく処理されます。	B
407 Proxy Authentication Required	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 回試行します。これが失敗すると、電話機の動作は C です。
4xx	その他のクライアント エラー ステータス コードは処理されません。	C
500 Internal Server Error	一般的なエラー メッセージ。	Cisco IP Phone の動作は C です。
501 Not Implemented	サーバがリクエスト方法を認識しない、またはリクエストを実行する機能がありません。	Cisco IP Phone の動作は C です。
502 Bad Gateway	サーバがゲートウェイまたはプロキシとして動作している場合に、アップストリーム サーバから無効な応答を受信しました。	Cisco IP Phone の動作は C です。
503 Service Unavailable	サーバは現在使用できません（過負荷状態またはメンテナンスのためダウンしています）。これは一時的なステートです。	Cisco IP Phone の動作は C です。
504 Gateway Timeout	サーバがゲートウェイまたはプロキシとして動作している場合に、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でした。	C
5xx	その他のサーバ エラー	C

HTTPS プロビジョニング

導入済みのユニットのリモート管理におけるセキュリティを強化するため、Cisco IP Phone ではプロビジョニング時に HTTPS をサポートしています。各 Cisco IP Phone は、Sipura CA サーバ ルート証明書のほかに固有の SLL クライアント証明書（および関連付けられている秘密キー）を保持します。サーバ ルート証明書を使用して、Cisco IP Phone は、承認されたプロビジョニング サーバを認識し、非承認サーバを拒否することができます。一方、クライアント証明書により、プロビジョニング サーバはリクエストを発行する個々のデバイスを特定できます。

HTTPS を使用して導入を管理するサービス プロバイダーでは、HTTPS を使用して Cisco IP Phone が再同期するプロビジョニング サーバごとに、サーバ証明書を生成する必要があります。サーバ証明書は、Cisco サーバ CA ルート キーにより署名され、導入済みのすべてのユニットがその証明書を保持する必要があります。署名済みサーバ証明書を取得するために、サービス プロバイダーは証明書署名要求を Cisco に送信する必要があります。Cisco は、プロビジョニング サーバでのインストール用にサーバ証明書に署名して返送します。

プロビジョニング サーバ証明書には、共通名（CN）フィールド、および対象内でサーバを実行しているホストの FQDN が含まれている必要があります。またオプションで、スラッシュ（/）文字で区切られた情報がホストの FQDN の後に含まれている場合があります。次は、Cisco IP Phone により有効として受け入れられる CN エントリの例です。

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

サーバ証明書の確認に加えて、Cisco IP Phone は、サーバ証明書で指定されたサーバ名の DNS ルックアップにより、サーバ IP アドレスをテストします。

OpenSSL ユーティリティは証明書署名要求を生成できます。次の例は、1024 ビット RSA の公開キー/秘密キーのペアおよび証明書署名要求を生成する **openssl** コマンドを示しています。

```
openssl req -new -out provserver.csr
```

このコマンドにより、サーバの秘密キーが **privkey.pem** に、対応する証明書署名要求が **provserver.csr** にそれぞれ生成されます。サービス プロバイダーは、**privkey.pem** を秘密にして、**provserver.csr** を署名のために Cisco に提出します。シスコは **provserver.csr** ファイルを受信すると、署名されたサーバ証明書として **provserver.crt** を生成します。

Cisco はまた、サービス プロバイダーに Sipura CA クライアント ルート証明書も提供します。このルート証明書により、それぞれの Cisco IP Phone が保持するクライアント証明書が本物であることが保証されます。Cisco IP Phone 7800 シリーズ、および 8800 シリーズ Multiplatform Phone は、Verisign、Cybertrust などが提供するサードパーティの署名済み証明書もサポートします。

HTTPS セッション中に各デバイスが提供する固有のクライアント証明書には、該当するフィールドに識別情報が埋め込まれています。この情報は、HTTPS サーバを介して、安全性の高いリクエストを処理するために起動される CGI スクリプトで使用できます。特に、証明書の件名は、ユニットの製品名（OU 要素）、MAC アドレス（S 要素）、シリアル番号（L 要素）を示します。次の例は、Cisco IP Phone 8841 Multiplatform Phone の場合に、クライアント証明書の件名フィールドに表示される次の各要素を示しています。

```
OU=CP-8841-3PCC, L=88012BA01234, S=000e08abcdef
```

ファームウェア 2.0.x より前に製造されたユニットには、個別の SSL クライアント証明書が含まれていません。これらのユニットが 2.0.x ツリーのファームウェア リリースにアップグレードされると、HTTPS を使用しているセキュア サーバに接続できるようになりますが、サーバがユニットにクライアント証明書を要求した場合には、ユニットは一般的なクライアント証明書だけを提供できます。この一般的な証明書には、識別子フィールドに次の情報が含まれます。

```
OU=cisco.com, L=ciscogeneric, S=ciscogeneric
```

Cisco IP Phone が個別の証明書を保持するかどうかを決定するには、$CCERT プロビジョニング マクロ変数を使用します。変数の値は、固有のクライアント証明書の有無に従って、インストールまたはインストールなしのいずれかに展開されます。一般的な証明書の場合、HTTP リクエスト ヘッダーの User-Agent フィールドからユニットのシリアル番号が取得できます。

HTTPS サーバを設定して、接続しているクライアントから SSL 証明書をリクエストすることができます。これを有効にすると、サーバは Cisco が提供する Sipura CA クライアント ルート証明書を使用して、クライアント証明書を確認できます。その後、サーバは、以降のプロビジョニングで CGI に証明書情報を提供できます。

証明書を保存する場所はさまざまです。たとえば、Apache をインストールした場合には、プロビジョニング サーバにより署名された証明書や、関連付けられた秘密キー、Sipura CA クライアント ルート証明書の保存場所のファイル パスは以下のようになります。

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

個別の情報については、HTTPS サーバのドキュメントを参照してください。

ファームウェア リリース 2.0.6 以降では、HTTPS を使用したサーバへの SSL 接続用に、次の暗号スイートがサポートされます。

表 3-2　HTTPS サーバへの接続用にサポートされる暗号スイート

数値コード	暗号スイート
0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
0x002f	TLS_RSA_WITH_AES_128_CBC_SHA
0x0005	TLS_RSA_WITH_RC4_128_SHA
0x0004	TLS_RSA_WITH_RC4_128_MD5
0x0062	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
0x0060	TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5

冗長プロビジョニング サーバ

IP アドレスまたは完全修飾ドメイン名（FQDN）にプロビジョニング サーバを指定することができます。FQDN を使用すると、冗長プロビジョニング サーバの導入が容易になります。プロビジョニング サーバが FQDN により識別される場合、Cisco IP Phone は DNS を介して FQDN から IP アドレスを解決します。プロビジョニングでは DNS A レコードのみサポートされます。DNS SRV のアドレス解決はプロビジョニングでは使用できません。Cisco IP Phone はサーバが応答するまで A レコードの処理を続けます。A レコードに関連付けられているサーバが応答しない場合、Cisco IP Phone は syslog サーバにエラーを記録します。

syslog サーバ

<Syslog_Server> パラメータを使用して Cisco IP Phone に syslog サーバが設定されている場合、再同期およびアップグレード操作のメッセージが syslog サーバに記録されます。メッセージは、リモート ファイル リクエスト（設定プロファイルまたはファームウェアのロード）の開始時および操作の終了時に生成できます（成功または失敗を示します）。

記録されるメッセージは以下のパラメータで設定され、実際の syslog メッセージへとマクロ展開されます。

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

Cisco クライアント証明書ルート認証局が、固有の各証明書に署名します。対応するルート証明書が、クライアント認証の目的でサービス プロバイダーにより使用できるようになります。