# 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


- 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 （1 ページ）
- サーバの準備とソフトウェア ツール （1 ページ）
- 社内デバイスの事前プロビジョニング （4 ページ）
- プロビジョニング サーバの設定 （5 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

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）

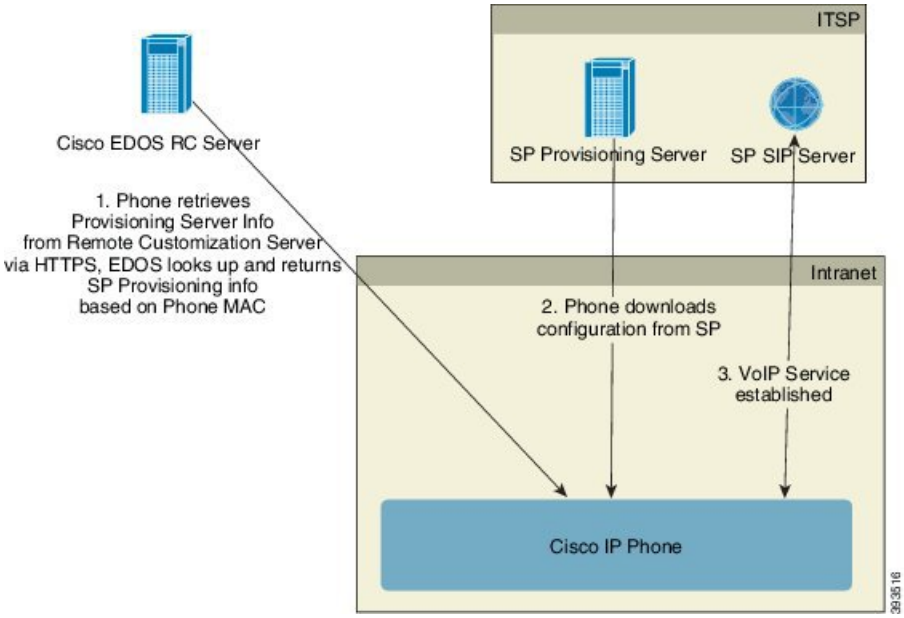
- HTTPS（TCP ポート 443）

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 サーバと電話機の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 ユー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。

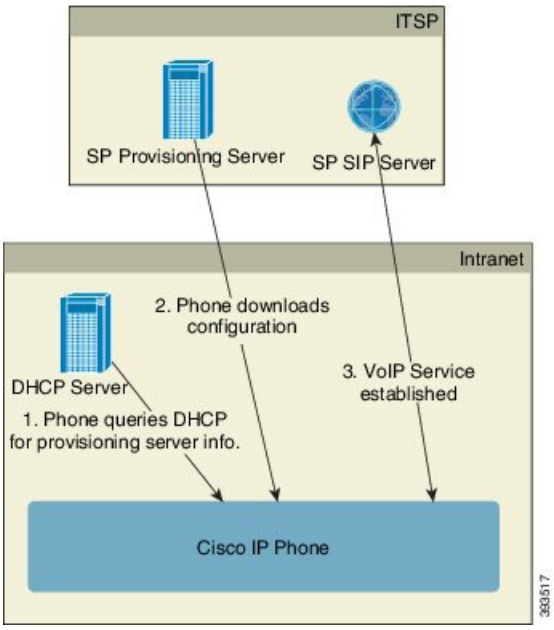
DHCP サーバがプロビジョニング サーバ情報を提供しない場合、電話機は Cisco EDOS RC サーバに照会して、その MAC アドレスとモデルを指定し、[カスタマイズ状態（Customization State）] は [保留中（Pending）] に設定されます。Cisco EDOS サーバは、プロビジョニング サーバの URL を含む、関連付けられたサービス プロバイダーのプロビジョニング サーバ情報で応答し、電話機の [カスタマイズ状態（Customization State）] は、[カスタム保留中（Custom Pending）] に設定されます。電話機は、resync URL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

### 関連トピック

小売配布
TFTP のプロビジョニング （5 ページ）

# 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。

工場出荷時のデフォルト設定で提供される Profile_Rule は *&PN*.cfg です。この *&PN* は、電話機モデル名を表します。

たとえば、CP-7841-3PCC の場合、ファイル名は CP-7841-3PCC.cfg です。CP-7832-3PCC の場合、ファイル名は CP-7832-3PCC.cfg です。

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。

**関連トピック**

社内デバイスの事前プロビジョニング （4 ページ）

## 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に使用されます。

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)
```

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 *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** | このリクエストと以降のリクエストは新しい場所に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。 |
| **302 Found** | 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。 |
| **3xx** | 他の 3 xx 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、リクエストを処理できません。 | 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 回再試行できます。失敗した場合、電話機の動作は C です。 |
| **403 Forbidden** | サーバが応答を拒否しています。 | C |
| **404 Not Found** | 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 |
| **407 プロキシ認証が必要** | 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。 |

| HTTP ステータス コード | 説明 | 電話機の動作 |
|---|---|---|
| **4xx** | 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 内部サーバ エラー** | 一般的なエラー メッセージ。 | 電話機の動作は C です。 |
| **501 実装されない** | 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。 |
| **502 不正なゲートウェイ** | 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。 |
| **503 サービスは利用不可です** | 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。 |
| **504 Gateway Timeout** | 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 |
| **5xx** | その他のサーバ エラー | C |

# HTTPS プロビジョニング

電話機は、リモートに導入されたユニットを管理する際のセキュリティを強化するために、プロビジョニング用に HTTPS をサポートします。各電話機は、Sipura CA サーバ ルート証明書に加えて、固有の SLL クライアント証明書（および関連付けられた秘密キー）を保持します。ルート証明書を使って、電話機は認証されたプロビジョニング サーバを認識し、認証されていないサーバを拒否できます。一方、クライアント証明書を使うと、プロビジョニング サーバはリクエストを発行した個々のデバイスを識別できます。

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 を使用した電話機の再同期先とな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。サーバ証明書はシスコ サーバの CA ルート キーで署名される必要があります。導入済みのすべてのユニットはすべての証明書を保持します。署名されたサーバ証明書を取得するには、サービス プロバイダーが証明書署名要求をシスコに送信します。シスコはプロビジョニング サーバへ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）フィールドと、対象内でサーバを実行しているホストの FQDN を含める必要があります。オプションで、ホストの FQDN に続く情報

をスラッシュ（/）文字で区切って含めることができます。次の例は、電話機で有効として受け入れられる CN エントリです。

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

電話機では、サーバ証明書の検証に加えて、サーバ証明書で指定されたサーバ名の DNS ルックアップに対してサーバ IP アドレスをテストします。

## 署名付きサーバ証明書の取得

OpenSSL ユーティリティで、証明書署名要求を生成できます。次の例は、1024 ビットの RSA 公開キーと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
```

このコマンドでは、**privkey.pem** と対応する証明書署名要求 **provserver.csr** にサーバの秘密キーが生成されます。サービスプロバイダーは、**privkey.pem** 秘密キーを維持し、署名のために **provserver.csr** をシスコに提出します。**provserver.csr** ファイルを受信すると、シスコは署名付きサーバ証明書 **provserver.crt** を生成します。

**手順**

**ステップ 1** https://software.cisco.com/software/edos/home に移動し、CCO クレデンシャルでログインします。

（注） 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をお勧めします。

**ステップ 2** [証明書の管理（Certificate Management）] を選択します。

[CSRの署名（Sign CSR）] タブで、前の手順の CSR を署名用にアップロードします。

**ステップ 3** [製品の選択（Select Product）] ドロップダウン リスト ボックスから [SPA1xxファームウェア1.3.3以降（SPA1xx firmware 1.3.3 and newer）]、[SPA232Dファームウェア1.3.3以降（SPA232D firmware 1.3.3 and newer）]、[SPA5xxファームウェア7.5.6以降（SPA5xx firmware 7.5.6 and newer）]、[CP-78xx-3PCC]、および [CP-88xx-3PCC] を選択します。

**ステップ 4** [CSRファイル（CSR File）] フィールドで、[参照（Browse）] をクリックし、署名用に CSR を選択します。

**ステップ 5** 暗号方式を選択します。

- MD5
- SHA1
- SHA256

SHA256 暗号化を選択することが推奨されます。

**ステップ 6** [サインイン期間（Sign in Duration）] ドロップダウン リスト ボックスで、適切な期間（1 年など）を選択します。

**ステップ 7** [証明書の署名要求（Sign Certificate Request）] をクリックします。

**ステップ 8** 署名付き証明書を受信するには、次のいずれかのオプションを選択します。

- [受信者の電子メールアドレスを入力する（Enter Recipient's Email Address）]：電子メールで証明書を受け取る場合は、このフィールドに電子メール アドレスを入力します。
- [ダウンロード（Download）]：署名付き証明書をダウンロードする場合は、このオプションを選択します。

**ステップ 9** [送信] をクリックします。

署名付きサーバ証明書は、前に指定した電子メールアドレスに送信されるか、ダウンロードされます。

## マルチプラットフォーム フォンの CA クライアント ルート証明書

シスコは、サービス プロバイダーにマルチプラットフォーム フォンのクライアント ルート証明書も提供しています。このルート証明書により、各電話機で保持されるクライアント証明書が本物であることが証明されます。マルチプラットフォーム フォンは、Verisign、Cybertrust などで提供される証明書のように、サードパーティの署名付き証明書もサポートします。

各デバイスが HTTPS セッション中に提供する固有のクライアント証明書では、その件名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、安全な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。

次は、Cisco IP Phone 7841 マルチプラットフォーム フォンのクライアント証明書にある件名フィールドの例で、以下の要素を示しています。

```
OU=CP-7841-3PCC, L=88012BA01234, S=000e08abcdef
```

次は、Cisco IP Conference Phone 7832 マルチプラットフォーム フォンのクライアント証明書にある件名フィールドの例で、以下の要素を示しています。

```
OU=CP-7832-3PCC, L=88012BA01234, S=000e08abcdef
```

電話機が個別の証明書を保持するかどうかを判断するには、$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、Installed または

Not Installed のいずれかに展開されます。一般的な証明書の場合は、User-Agent フィールドの HTTP リクエスト ヘッダーからユニットのシリアル番号を取得できます。

HTTPS サーバを設定して、接続しているクライアントに SSL 証明書を要求することができます。これを有効にすると、サーバは、シスコが提供するマルチプラットフォーム フォンのクライアント ルート証明書を使用してクライアント証明書を検証できます。その後、サーバは、以降の処理のために証明書情報を CGI に提供できます。

証明書の保存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 サーバの署名付き証明書、関連付けられた秘密キー、マルチプラットフォーム フォン CA クライアントのルート証明書を保存するファイル パスは次のようになります。

```
# 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
```

個別の情報は、HTTPS サーバの資料を参照してください。

シスコのクライアント証明書ルート認証局が、独自の証明書にそれぞれ署名します。関連するルート証明書が作成され、クライアント認証の目的でサービス プロバイダーがそれを利用できるようになります。

## 冗長プロビジョニング サーバ

プロビジョニング サーバは、IP アドレスまたは完全修飾ドメイン名（FQDN）で指定できます。FQDN を使用すると、冗長なプロビジョニング 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 によって識別される場合、電話機は DNS を介して FQDN を IP アドレスに解決しようとします。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には使用できません。電話機は、サーバが応答するまで A レコードの処理を続行します。A レコードの応答にサーバが関連付けられていない場合、電話機は 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 syslog サーバを電話機に設定している場合、再同期およびアップグレード操作のメッセージが syslog サーバに送信されます。メッセージはリモート ファイル リクエストの開始時（設定プロファイルまたはファームウェアのロード）、および操作の完了時（成功または失敗を示す）に生成できます。

ログに記録されたメッセージは次のパラメータで設定され、実際の syslog メッセージにマクロ展開されます。

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg