サードパーティ コール制御向け Cisco IP Phone 7800 シリーズ、8800 シリーズ プロビジョニング ガイド

2016 年 1 月 29 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号は以下のシスコ Web サイトを
ご覧ください。
www.cisco.com/go/offices

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 準拠装置に関する記述: この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述: この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの制限は、住宅地で使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。干渉しているかどうかは、装置の電源のオン/オフによって判断できます。

- 受信アンテナの向きを変えるか、場所を移動します。
- 装置と受信機との距離を離します。
- 受信機と別の回路にあるコンセントに装置を接続します。
- 販売業者またはラジオやテレビに詳しい技術者に連絡します。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

CONTENTS

CHAPTER 1

導入とプロビジョニング

プロビジョニング サーバ

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。

バルク配布

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—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。(「「要素タグのプロパティ」セクション (2-2 ページ)」で説明されています)。
- 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。(「「LCD GUI のアクセス制御」セクション (2-4 ページ)」で説明されています)。
- 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。

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）

CHAPTER 2

プロビジョニング スクリプト

Cisco IP Phone は、オープンな公開された構文に基づくプロファイル形式を受け入れます。オープン形式では、XML に類似したシンプルな構文が使用されます。

このドキュメントの例では、オープン形式（XML スタイル）の構文による設定プロファイルが使用されます。付録 A「サンプル設定ファイル」でサンプル プロファイルを参照できます。

お客様の Cisco IP Phone の詳細については、お客様のデバイスのアドミニストレーション ガイドを参照してください。各ガイドでは、管理 Web サーバで設定できるパラメータについて説明しています。

設定プロファイルの形式

設定プロファイルは、Cisco IP Phone のパラメータ値を定義します。

設定プロファイルのオープン形式では、標準的な XML 作成ツールを使用して、パラメータと値をコンパイルします。

（注） UTF-8 文字セットのみがサポートされます。エディタでプロファイルを変更する場合、エンコーディング形式を変更しないでください。変更すると、Cisco IP Phone がファイルを認識できません。

Cisco IP Phone の各モデルの機能セットは異なっているため、パラメータ セットも異なります。

オープン形式（XML スタイル）プロファイル

オープン形式プロファイルは、要素を階層構造で記述する XML のような構文によるテキストファイルで、要素の属性と値を含んでいます。この形式により、標準的なツールを使用して設定ファイルを作成できるようになります。この形式の設定ファイルは、再同期操作の間に、プロビジョニング サーバから Cisco IP Phone に送信できます。このファイルは、バイナリ オブジェクトとしてコンパイルなしで送信できます。

Cisco IP Phone は、標準的なツールで生成される設定形式を受け入れることができます。この機能によって、既存のデータベースから設定プロファイルを生成するバックエンドのプロビジョニング サーバ ソフトウェアの開発が容易になります。

設定プロファイルの機密情報を保護するため、プロビジョニング サーバは、HTTPS が保護するセキュアなチャネルを使って、この種のファイルを電話に提供します。必要に応じて、gzip 圧縮アルゴリズム（RFC1951）を使用してファイルを圧縮できます。このファイルは、256 ビット AES 対称キー暗号化で暗号化できます。

例:オープン プロファイル形式

```
<device> <flat-profile>
<Resync_On_Reset> Yes
 </Resync_On_Reset>
<Resync_Periodic> 7200
 </Resync_Periodic>
<Profile_Rule>
  tftp://prov.telco.com:6900/cisco/config/CP_x8xx_3PCC.cfg
 </Profile_Rule>
</flat-profile> </device>
```

<flat-profile> 要素タグは、Cisco IP Phone の認識するすべてのパラメータの要素を囲みます。

（注） 2.0.6 以前のファームウェアバージョン を含む Cisco IP Phone は、オープン形式プロファイルをサポートしていません。

関連項目

- オープン プロファイル（XML スタイル）の圧縮と暗号化（2-6 ページ）

設定ファイルのコンポーネント

設定ファイルには、次のコンポーネントを含めることができます。

- 要素タグ
- 属性（Attributes）
- パラメータ
- 書式設定機能

要素タグのプロパティ

- Cisco IP Phone は、特別な <flat-profile> 要素でカプセル化された適切なパラメータ名で要素を認識しています。
- <flat-profile> 要素は、他の任意の要素内にカプセル化することができます。
- 要素名は、山カッコで囲まれています。
- ほとんどの要素名は、デバイスの管理 Web ページのフィールド名と同様ですが、以下の変更を伴います。
  - 要素名には、スペースや特殊文字が含まれないことがあります。管理 Web フィールド名から要素名を生成するには、すべてのスペースや特殊文字 [、]、(、)、/ をアンダースコアに置き換えます。

    例:<Resync_On_Reset> 要素は、[リセット時の再同期（Resync On Resetreset）] フィールドを表します。
  - 各要素名は固有である必要があります。管理 Web ページでは、同じフィールドは、[回線（Line）]、[ユーザ（User）]、および [拡張（Extension）] ページなど、複数の Web ページに表示される場合があります。ページ タブに表示される番号を示すには、要素名に [n] を追加します。

    例:<Dial_Plan[1]> 要素は、[回線 1（Line 1）] の [ダイヤル プラン（Dial Plan）] を表します。

- 始めの要素タグすべては、一致する終わりの要素タグを伴う必要があります。次に例を示します。

```
<device> <flat-profile>
<Resync_On_Reset> Yes
   </Resync_On_Reset>
<Resync_Periodic> 7200
   </Resync_Periodic>
<Profile_Rule>tftp://prov.telco.com: 6900/cisco/config/CP_x8xx_3PCC.cfg
   </Profile_Rule>
</flat-profile> </device>
```

- 要素タグは、大文字と小文字を区別します。
- 空の要素タグは許容されます。始めの要素タグを対応する要素タグなしで入力し、最後の山カッコ(>)の前にスペースとスラッシュを挿入します。この例では、プロファイル ルール B は空です。

```
<Profile_Rule_B />
```

- 認識されない要素名は無視されます。
- 再同期処理の際に、どのユーザ指定の値も上書きされないようにするため、空の要素タグを使用します。次の例では、ユーザの短縮ダイヤルの設定は変更されません。

```
<Speed_Dial_2_2_  ua="rw"/>
  <Speed_Dial_3_2_  ua="rw"/>
  <Speed_Dial_4_2_  ua="rw"/>
  <Speed_Dial_5_2_  ua="rw"/>
  <Speed_Dial_6_2_  ua="rw"/>
  <Speed_Dial_7_2_  ua="rw"/>
  <Speed_Dial_8_2_  ua="rw"/>
  <Speed_Dial_9_2_  ua="rw"/>
<device> </flat-profile> </device>
```

- 空の文字列に対応するパラメータを設定するため、空の値を使用します。始めと終わりの要素を、間に値を何も含めずに入力します。次の例では、GPP_A パラメータは空の文字列に設定されます。

```
<device> <flat-profile>
<GPP_A>
  </GPP_A>
</flat-profile> </device>
```

ユーザ アクセスの属性

ユーザ アクセスの **(ua)** 属性は、特定のパラメータに対するユーザ アカウントへのアクセスを制御します。**ua** 属性タグが要素タグで指定されなかった場合、工場出荷時のデフォルトのユーザ アクセスが、適用済みの対応するパラメータに対して適用されます。この属性は、管理者アカウントによるアクセスに影響しません。

ua 属性が存在する場合には、次のいずれかの値にする必要があります。

- na—アクセスなし
- ro—読み取りのみ
- rw—読み取りと書き込み

次の例は、**ua** 属性を示しています。

```
<device> <flat-profile>
  <SIP_TOS_DiffServ_Value_1_   ua=”na”/>
  <Dial_Plan_1_   ua=”ro”/>
  <Dial_Plan_2_   ua=”rw”/>
</flat-profile> </device>
```

二重引用符で **ua** オプションの値を囲む必要があります。

LCD GUI のアクセス制御

<Phone-UI-User-Mode> パラメータを有効にすると、電話の GUI は、GUI がメニュー項目を表示するときに、関連するパラメータのユーザ アクセスの属性を受け入れます。

単一の設定パラメータに関連付けられたメニュー エントリの場合:

- “ua=na”(“ua” は「ユーザ アクセス(user access)」を意味する)属性を含むパラメータのプロビジョニングにより、エントリは非表示になります。
- “ua=ro” 属性を含むパラメータのプロビジョニングにより、エントリは読み取り専用で編集不可能になります。

複数の設定パラメータに関連付けられたメニュー エントリの場合:

- “ua=na” 属性を含むすべての関連するパラメータのプロビジョニングにより、エントリは非表示になります。

(注) 通常のユーザまたは管理者として LCD GUI からログインすると、すべての設定ページのデフォルトの表示は [ユーザ モード(User Mode)] になります。管理者ログインの後、このモードは [管理者モード(Admin Mode)] に切り替わり、属性は “ua=xx” となって、すべてのパラメータは無視されます。

パラメータのプロパティ

次のプロパティがパラメータに適用されます。

- プロファイルに指定されていないどのパラメータも、Cisco IP Phone で変更されることはありません。
- 認識されないパラメータは無視されます。
- Cisco IP Phone は、限られた数のパラメータ名に対する任意の設定可能なエイリアスを認識します。
- オープン形式プロファイルに同じパラメータ タグが複数回含まれている場合、最後のタグが先行するタグに上書きされます。パラメータの設定値の不注意な上書きを防ぐため、各プロファイルが指定するパラメータのインスタンスを最大でも 1 つにすることをお勧めします。

書式設定

次のプロパティが文字列の書式設定に適用されます。

- コメントは、標準的な XML 構文で作成できます。

```
<!-- My comment is typed here -->
```

- 先頭および後続のスペースは、読みやすさのために許容されますが、パラメータ値からは除外されます。
- 値の中での改行は、スペースに変換されます。
- <?　?> 形式の XML ヘッダーは許容されますが、Cisco IP Phone はこれを無視します。
- 特殊文字を入力するには、次の表に示すように、基本的な XML の文字エスケープを使用します。

特殊文字	XML のエスケープ シーケンス
&（アンパサンド）	&amp;
<（より小さい）	&lt;
>（より大きい）	&gt;
’ (アポストロフィ)	&apos;
”（二重引用符）	&quot;

次の例では、文字エスケープは、ダイヤル プラン ルールに必要な記号よりも大きいことと小さいことを示すために入力されます。この例では、Dial_Plan[1] パラメータを（S0 <:18005551212>）に等しく設定する情報ホットラインのダイヤル プランを定義します。

```
<device> <flat-profile>
  <Dial_Plan_1_>
    (S0 &lt;:18005551212&gt;)
 </Dial_Plan_1_>
</flat-profile> </device>
```

- 10 進数および 16 進数の値（s.a.(と .）を使用する数字のエスケープが変換されます。
- ファームウェアは、完全な Unicode 文字セットをサポートしておらず、ASCII のサブセットのみをサポートしています。

オープン プロファイル（XML スタイル）の圧縮と暗号化

オープン設定プロファイルを圧縮して、プロビジョニング サーバのネットワーク負荷を軽減することができます。このプロファイルは、機密情報を保護するために暗号化することもできます。圧縮は必要ではありませんが、暗号化の前に行う必要があります。

オープン プロファイルの圧縮

サポートされている圧縮方法は、gzip 圧縮アルゴリズム（RFC1951）です。gzip ユーティリティと、同じアルゴリズム（zlib）を実装する圧縮ライブラリは、インターネット サイトから入手できます。

圧縮を識別するため、Cisco IP Phone は、gzip 互換のヘッダーを含めるための圧縮ファイルを要求します。元のオープン プロファイルで gzip ユーティリティを呼び出すと、ヘッダーが生成されます。Cisco IP Phone は、ダウンロードされたファイル ヘッダーを検査し、ファイル形式を確認します。

たとえば、`profile.xml` が有効なプロファイルの場合、`profile.xml.gz` も受け入れられます。次のコマンドのいずれも、このプロファイル タイプを生成できます。

- `>gzip profile.xml`

  元のファイルを圧縮ファイルと置き換えます。

- `>cat profile.xml | gzip > profile.xml.gz`

  元のファイルを残したまま、新しい圧縮ファイルを作成します。

圧縮のチュートリアルについては、「「プロファイルの gzip 圧縮を開く」セクション（4-14 ページ）」を参照してください。

AES の使用によるオープン プロファイルの暗号化

対称キー暗号化は、ファイルが圧縮されているかどうかにかかわりなく、オープン設定プロファイルの暗号化に使用できます。サポートされる暗号化アルゴリズムは、暗号ブロック連鎖モードで適用される、256 ビット キーを使用する American Encryption Standard（AES）です。

（注）　圧縮および暗号化されたオープン形式プロファイルを Cisco IP Phone が認識できるようにするため、圧縮を暗号化に先行させる必要があります。「「OpenSSL を使用したプロファイル暗号化」セクション（4-15 ページ）」は、暗号化に関するチュートリアルを提供しています。

OpenSSL 暗号化ツールは、さまざまなインターネット サイトからダウンロード可能で、暗号化を実行できます。256 ビット AES 暗号化のサポートには、AES コードを有効にするため、ツールの再コンパイルが必要になる場合があります。ファームウェアは、バージョン openssl-0.9.7c でテスト済みです。

暗号化ファイルについては、プロファイルは、次のコマンドによって生成されたものと同じ形式をもつファイルを要求します。

```
# example encryption key = SecretPhrase1234

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml -out profile.cfg

# analogous invocation for a compressed xml file

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml.gz -out profile.cfg
```

小文字の -k は、秘密鍵に先行します。秘密鍵は、いずれかのプレーン テキストの文字列で、ランダムな 64 ビット salt の生成に使用されます。-k 引数で指定された秘密を使用して、暗号化ツールは、ランダムな 128 ビット初期ベクトルと実際の 256 ビット暗号キーを生成します。

この形式の暗号化を設定プロファイルで使用する場合、ファイルを復号できるように、秘密鍵の値を電話に知らせる必要があります。この値は、プロファイル URL で修飾子として指定されます。構文は次のとおりで、明示的な URL を使用します。

```
[--key “SecretPhrase1234”] http://prov.telco.com/path/profile.cfg
```

この値は、Profile_Rule パラメータのいずれかを使用してプログラムされます。このキーは、先立ってユニットに事前プロビジョニングしておく必要があります。秘密鍵のブートストラップは、HTTPS を使用することで安全に実現できます。

対称キー暗号化によるオフラインでの設定プロファイルの事前暗号化により、再同期プロファイルに HTTP を使用することが可能になります。プロビジョニング サーバは、Cisco IP Phone 導入後の最初のプロビジョニングを処理するために HTTPS を使用します。この機能は、大規模導入時の HTTPS サーバの負荷を軽減します。

最終的なファイル名は特定の形式を必要としませんが、通常、.cfg 拡張子で終わるファイル名は設定プロファイルを示します。

コメント

開発とスクリプト作成の際、パラメータ値の先頭に # の文字を入力して、プロビジョニング パラメータを一時的に無効にすると便利です。これにより、パラメータの残りのテキストが効果的にコメント アウトされます。

例

値 “`# http://192.168.1.200/sample.cfg`” を含む Profile_Rule は、空の Profile_Rule に相当します。# 文字によるコメント機能は、Profile_Rule*、Upgrade_Rule、および Resync_Trigger_* パラメータに適用されます。

マクロ展開

複数のプロビジョニング パラメータは、評価される前に内部でのマクロ展開により処理されます。この評価前の手順によって、Cisco IP Phone の再同期およびアップグレード アクティビティの制御がより柔軟になります。

次のパラメータ グループは、評価の前にマクロ展開により処理されます。

- Resync_Trigger_*
- Profile_Rule*
- Log_xxx_Msg
- Upgrade_Rule

特定の条件下では、一部の汎用パラメータ（GPP_*）も、[オプション再同期引数（Optional Resync Arguments）] セクションで明示的に示されているように、マクロ展開により処理されます。

マクロ展開の際、名前付き変数の内容は、$NAME および $(NAME) 形式の式を置き換えます。そのような変数には、汎用パラメータ、複数の製品識別子、特定のイベント タイマー、プロビジョニングの状態の値が含まれます。完全なリストについては、「「マクロ展開変数」セクション（5-5 ページ）」を参照してください。

次の例では、式 $(MAU) を使用して MAC アドレス 000E08012345 を挿入します。

管理者は次の式を入力します。$(MAU)config.cfg
MAC アドレス 000E08012345 のデバイスのマクロ展開の結果は次のとおりです。
000E08012345config.cfg

マクロ名が認識されない場合には、展開されません。たとえば、STRANGE は有効なマクロ名として認識されませんが、MAU は有効なマクロ名として認識されます。

管理者は次の式を入力します。$STRANGE$MAU.cfg
MAC アドレス 000E08012345 のデバイスのマクロ展開の結果は次のとおりです。
$STRANGE000E08012345.cfg

マクロ展開は、再帰的に適用されません。たとえば、$$MAU” は $MAU” に展開し（$$ が展開される）、MAC アドレスになることはありません。

特殊な用途のパラメータである GPP_SA から GPP_SD の内容は、マクロ式 $SA から $SD にマッピングされます。これらのパラメータは、再同期 URL の **--key** オプションの引数としてのみマクロ展開します。

マクロ式は、MAC アドレスの一部分と同様、マクロ変数の部分文字列のみを使用するように、式を修飾できます。

部分文字列マクロ展開の構文は、$(NAME:p) と $(NAME:p:q) で、p と q は負ではない整数です。この展開により、文字のオフセット p で開始される長さ q（q が指定されない場合には文字列の終端まで）のマクロ変数部分文字列が生成されます。次の例を参照してください。

管理者は次の式を入力します。$(MAU:4)
MAC アドレス 000E08012345 のデバイスのマクロ展開の結果は次のとおりです。08012345

管理者は次の式を入力します。$(MAU:8:2)
MAC アドレス 000E08012345 のデバイスのマクロ展開の結果は次のとおりです。23

条件式

条件式で、再同期イベントをトリガーし、再同期およびアップグレードの操作に対する代替 URL を選択できます。

条件式は、比較のリストで構成されており、**and** 演算子によって分割されます。すべての比較は、条件が true になる要件を満たしている必要があります。

各比較は、3 つのタイプのリテラルのうち 1 つを関連付けることができます。

- 整数値
- ソフトウェアまたはハードウェアのバージョン番号
- 二重引用符の文字列

バージョン番号

3PCC 電話の公式リリース ソフトウェア バージョンは、7800 シリーズの電話の 形式 sip78xx.v1-v2-v3-v4-3PCC と、8800 シリーズの電話の sip88xx.v1-v2-v3-v4-3PCC 形式を使用しています。比較文字列には、同じ形式を使用する必要があります。そうしない場合、結果として形式解析エラーが発生します。

このソフトウェア バージョンでは、v1-v2-v3-v4 には異なる桁と文字を指定できますが、数字で始まっている必要があります。ソフトウェア バージョンを比較する際、v1-v2-v3-v4 は順に比較され、左端の桁が後続の桁よりも優先されます。

v[x] に数字のみが含まれている場合、その数字が比較されます。v[x] に数字とアルファベット文字が含まれている場合、まず数字が比較され、次に文字がアルファベット順に比較されます。

有効なバージョン番号の例

sip78yy.10-3-1-7-3PCC

一方、10.3.1 は、無効な形式です。

比較

sip88xx.10-3-1-7-3PCC > sip88xx.9-3-1-7-3PCC

sip78xx.10-3-1-7-3PCC < sip78xx.10-3-1MN-1-3PCC

囲まれた文字列は、等しいか等しくないかについて比較できます。整数とバージョン番号も、算術的に比較できます。比較演算子は、記号または略語で表すことができます。略語は、オープン形式プロファイルで条件を表すのに便利です。

演算子	代替構文	説明	整数とバージョンのオペランドに適用可能	囲まれた文字列のオペランドに適用可能
=	eq	次の値と等しい	○	○
!=	ne	等しくない	○	○
<	lt	より少ない	○	X
<=	le	右辺と比較して小さいか等しい	○	X
>	gt	より大きい	○	X
>=	ge	右辺と比較して大きいか等しい	○	X

2.0.6 よりも前のファームウェアバージョンへのレガシー サポートの場合、not-equal-to 演算子を、(2 文字の != 文字列の代わりに) 単一の！の文字で表すことができます。

条件式には、通常、マクロ展開された変数が含まれます。次に例を示します。

```
$REGTMR1 gt 300 and $PRVTMR gt 1200 and “$EXTIP” ne “”

$SWVER ge 2.0.6 and “$CCERT” eq “Installed”
```

文字列リテラルが要求されるときに、マクロ変数を二重引用符で囲むことは重要です。バージョン番号の番号が要求されるときには、そうしないでください。

2.0.6 より前のファームウェア バージョンのレガシー サポートの場合、左辺オペランドのない関係式は、暗黙的な左辺として $SWVER を使用します。たとえば、! 1.0.33 は、$SWVER = 1.0.33 に相当します。

Profile_Rule* Upgrade_Rule パラメータのコンテキストで使用すると、次のアップグレード ルールの例に示すように、条件式を構文 “(expr)?” で囲む必要があります。

```
($SWVER ne sip78xx.10-3-1-10-3PCC)? http://ps.tell.com/sw/sip78xx.10-3-1-10-3PCC.loads
```

Resync_Trigger_* パラメータを設定する場合には、カッコを含む上記の構文を使用しないでください。

割り当て式

任意のパラメータが、Profile_Rule* と Upgrade_Rule パラメータのコンテキストで事前に割り当てられた値である場合もあります。この手順によって、プロファイルを取得する前に、割り当ての実行が発生します。

このような割り当ての構文は、個々のパラメータ割り当てのリストで、(assignments)! のようにカッコで囲まれており、各割り当ては次の形式で表されます。

ParameterXMLName = “Value”

認識されたパラメータ名は、XML ベースのプロファイル名に対応します。

いずれのパラメータにも、この方法で新しい値を割り当てる事が可能で、マクロ展開が適用されます。たとえば、次の例は有効な割り当て式です。

```
(User_ID_1_ = “uid$B”; GPP_C = “”; GPP_D = “$MA”;)!
```

単一の小文字 a から p は、汎用パラメータ GPP_A から GPP_P を参照することもできます。上の例は、次の例と同等です。

```
(User_ID_1_ = “uid$B”; c = “”; d = “$MA”;)!
```

読みやすいようにスペースを使用します。

URL 構文

標準的な URL 構文を使用して、設定ファイルとファームウェア ロードを、各々 Profile_Rule* および Upgrade_Rule パラメータに取得する方法を指定します。構文は次のようになります。

```
[ scheme:// ] [ server [:port]] filepath
```

scheme は次のいずれかの値です。

- tftp
- http
- https

scheme を省略すると、tftp が使用されます。server には、DNS に認識されるホスト名または数値による IP アドレスを使用できます。port は、接続先 UDP または TCP ポート番号です。filepath は、ルート ディレクトリ (/) から始める必要があります。これは絶対パスである必要があるためです。

server が見つからない場合、DHCP（オプション 66）で指定される tftp サーバが使用されます。

port が見つからない場合、指定されたスキームの標準ポートが使用されます。（tftp は UDP ポート 69、http は TCP ポート 80、https は TCP ポート 443を使用します）。

filepath が存在する必要があります。静的ファイルを参照する必要はありませんが、CGI で取得されたダイナミック コンテンツを指定することもできます。

マクロ展開は、URL 内で適用されます。有効な URL の例を次に示します。

```
/$MA.cfg
/cisco/sip78xx.10-3-1-3PCC.loads
192.168.1.130/profiles/init.cfg
tftp://prov.call.com/cpe/cisco$MA.cfg
http://neptune.speak.net:8080/prov/$D/$E.cfg
https://secure.me.com/profile?Linksys
```

オプション再同期引数

オプションの引数である **key** が、角カッコで集合的に囲まれて、Profile_Rule* パラメータに入力した URL の前に付く場合があります。

key

Key オプションは、暗号キーの指定に使用されます。明示的なキーによる、暗号化されたプロファイルの復号化が必要です。キー自体は、**--key** の語に続く（おそらく引用された）文字列として指定されます。

使用例

```
[--key VerySecretValue]
[--key “my secret phrase”]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

カッコで囲まれたオプションの引数は、マクロ展開されます。特殊な用途のパラメータ（GPP_SA から GPP_SD）は、Key オプションの引数として使用される場合に限り、マクロ変数にマクロ展開されます。次の例を参照してください。

```
[--key $SC]
[--key “$SD”]
```

オープン形式プロファイルの場合、**--key** に対する引数は、**openssl** に与えられた **-k** オプションと一致している必要があります。

IP テレフォニー デバイスへのプロファイルの適用

XML 設定スクリプトを作成した後、Cisco IP Phone に渡して適用する必要があります。設定を適用するには、次の方法のいずれかを選択してください。

TFTP と再同期 URL

設定ファイルを PC の TFTP サーバ アプリケーションにポストするには、次の手順を実行します。

ステップ 1　PC を電話の LAN に接続します。

ステップ 2　PC の TFTP サーバ アプリケーションを開始し、設定ファイルが TFTP サーバのルート ディレクトリで使用できることを確認します。

ステップ 3　Web ブラウザで、Cisco IP Phone の LAN IP アドレス、コンピュータの IP アドレス、ファイル名、およびログイン クレデンシャルを入力します。次の形式を使用します。

http://<*WAN_IP_Address*>/admin/resync?tftp://<*PC_IP_Address*>/<*file_name*>&xuser=admin&xpassword=<*password*>

例：

```
http://192.168.15.1/admin/resync?tftp://192.168.15.100/my_config.xml&xuser=admin&xpassword=admin
```

cURL を使用したダイレクト HTTP ポスト

cURL を使用して設定を Cisco IP Phone にポストするには、次の手順を実行します。このコマンド ライン ツールは、URL の構文でデータを転送するために使用されます。cURL をダウンロードする方法については、次を参照してください:

http://curl.haxx.se/download.html

ステップ 1　Cisco IP Phone の LAN ポートに PC を接続します。

ステップ 2　次の cURL コマンドを入力して、設定ファイルを Cisco IP Phone にポストしてください。

```
curl -d @my_config.xml
“http://192.168.15.1/admin/config.xml&xuser=admin&xpassword=admin”
```

プロビジョニング パラメータ

このセクションでは、機能に応じて大まかにまとめられたプロビジョニング パラメータについて説明します。

次のプロビジョニング パラメータのタイプが存在します。

- 汎用
- イネーブル
- トリガー
- 設定可能なスケジュール
- プロファイル ルール
- アップグレード ルール（Upgrade Rule）

汎用パラメータ

汎用パラメータ GPP_* は、特定のプロビジョニング サーバ ソリューションと連携するように Cisco IP Phone を設定するときに、自由文字列のレジスタとして使用されます。GPP_* パラメータは、デフォルトでは空です。これらは、次を含むさまざまな値に設定できます。

- 暗号化キー（Encryption keys）
- URL
- マルチステージ プロビジョニング ステータス情報
- Post 要求テンプレート
- パラメータ名エイリアス マップ
- 最終的に完全なパラメータ値に組み込まれる部分文字列値。

GPP_* パラメータは、他のプロビジョニング パラメータ内でのマクロ展開に利用できます。この目的のため、GPP_A から GPP_P の内容を識別するには、単一の小文字マクロ名（A から P）があれば十分です。また、2 文字の大文字のマクロ名 SA から SD は、**key** URL オプションの引数として使用される特殊なケースとして、GPP_SA から GPP_SD を識別します。

これらのパラメータは、プロビジョニングとアップグレードのルールで変数として使用できます。$GPP_A など、変数名の前に ‘$’ の文字を付けることにより参照されます。

たとえば、GPP_A に 文字列 ABC が含まれ、GPP_B に 123 が含まれる場合、式 AB マクロ は ABC123 に展開します。

ステップ 1　電話の Web ユーザ インターフェイス で、[管理者ログイン（Admin Login）] > [詳細（advanced）] > [音声（Voice）] > [プロビジョニング（Provisioning）] と移動します。

ステップ 2　[汎用パラメータ（General Purpose Parameters）] セクションまでスクロールします。

ステップ 3　フィールドに有効な値、GPP A から GPP P を入力します。

ステップ 4　[すべての変更を送信（Submit All Changes）] をクリックします。

イネーブル

Provision_Enable および Upgrade_Enable パラメータは、プロファイルの再同期とファームウェア アップグレードの操作すべてを制御します。これらのパラメータは、再同期とアップグレードをそれぞれ個別に制御します。これらのパラメータは、管理 Web サーバによって発行される URL コマンドの再同期とアップグレードも制御します。両方のパラメータは、デフォルトでは [はい（yes）] に設定されています。

Resync_From_SIP パラメータは、再同期操作を要求します。SIP NOTIFY イベントは、サービス プロバイダーのプロキシ サーバから Cisco IP Phone へ送信されます。有効にすると、プロキシが再同期を要求できるようになります。これを実行するため、プロキシは、Event: resync ヘッダーを含む SIP NOTIFY メッセージをデバイスに送信します。

デバイスは、401 応答（使用したクレデンシャルを理由に認証を拒否）でその要求にチャレンジします。デバイスは、プロキシからの再同期要求を引き受ける前に、認証済みの後続要求を求めます。Event: reboot_now および Event: restart_now ヘッダーは、それぞれコールド再起動とウォーム再起動を実行し、これらもチャレンジを受けます。

残り 2 つのイネーブルは、Resync_On_Reset と Resync_After_Upgrade_Attempt です。これらのパラメータは、電源投入ソフトウェアの再起動と各アップグレード試行の後に、デバイスが再同期操作を実行したかどうかを判定します。

Resync_On_Reset を有効にすると、デバイスは、リセットが実行される前のブートアップ シーケンスに先立って、ランダム遅延を発生させます。この遅延は、Resync_Random_Delay（秒単位）が指定する値を上限とするランダムな時間です。同時に起動する電話のプールの場合、この遅延が、各ユニットからの再同期要求の開始時刻を分散させます。この機能は、地域の停電時に、大規模な宅内導入で役立つ場合があります。

トリガー

Cisco IP Phone は、特定の間隔で、または特定の時間に再同期することを可能にします。

特定の間隔での再同期

Cisco IP Phone は、プロビジョニング サーバと定期的に再同期されるよう設計されています。再同期の間隔は、Resync_Periodic（秒単位）で設定されます。この値が空の場合、デバイスは定期的に再同期されません。

再同期は、通常、音声回線がアイドル状態になっているときに発生します。音声回線がアクティブで、再同期が予定されている場合、Cisco IP Phone は、回線が再度アイドル状態になるまで再同期手順を延期します。ただし、電話が Forced_Resync_Delay（秒単位）を超えて待機することはありません。再同期によって、設定パラメータ値が変更される場合があります。この変更により、ファームウェアのリブートが発生し、再同期時にアクティブだった音声接続が切断されます。

Cisco IP Phone がサーバからプロファイルを取得できなかった場合、ダウンロードしたファイルが破損していた場合、または内部エラーが発生した場合には、再同期操作が失敗する可能性があります。デバイスは、Resync_Error_Retry_Delay（秒単位）で指定された時間が経過した後、再び再同期を試行します。Resync_Error_Retry_Delay が 0 に設定されている場合、再同期の試行が失敗した後に、デバイスが再同期を試みることはありません。

アップグレードが失敗すると、Upgrade_Error_Retry_Delay（秒単位）の後に再試行が実行されます。

2 つの設定可能なパラメータ、Resync_Trigger_1 と Resync_Trigger_2 を使用して、再同期を条件付きでトリガーできます。各パラメータは、マクロ展開される条件式でプログラムできます。これらのパラメータのいずれかの条件が true と評価される場合、再同期操作は、定期的な再同期タイマーの期限が切れた場合のようにトリガーされます。

次の例の条件は、再同期をトリガーします。この例では、電話の最後のアップグレード試行から 5 分（300秒）以上が経過し、最後の再同期試行から少なくとも 10 分（600秒）が経過しています。

```
$UPGTMR gt 300 and $PRVTMR ge 600
```

特定の時間での再同期

Resync_At パラメータは、特定の時間に電話が再同期されることを可能にします。このパラメータは、24 時間形式（hhmm）を使用して時間を指定します。

Resync_At_Random_Delay パラメータは、指定されていない遅延時間で電話が再同期されることを可能にします。このパラメータは、正の整数の形式を使用して時間を指定します。

同時に再同期するよう設定された多数の電話から、サーバに再同期要求が押し寄せることは避ける必要があります。そのため、電話は、指定された時間の最大で 10 分後に再同期をトリガーします。

たとえば、再同期時間を 1000（午前 10 時）に設定すると、電話は、午前 10 時と午前 10 時 10 分の間のいずれかの時間に再同期をトリガーします。

デフォルトでは、この機能は無効になっています。Resync_At パラメータがプロビジョニングされると、Resync_Periodic パラメータは無視されます。

設定可能なスケジュール

次のプロビジョニング パラメータを使用して、定期的な再同期のスケジュールを設定することが可能で、再同期およびアップグレードが失敗した場合の再試行間隔も指定できます。

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

各パラメータは、単一の遅延値（秒単位）を受け入れます。新しく展開された構文は、連続的な遅延要素のカンマ区切りリストを許容します。シーケンスの最後の要素は、暗黙的に際限なく繰り返されます。次に例を示します。

```
Resync_Periodic=7200
Resync_Error_Retry_Delay=1800,3600,7200,14400
```

前の例では、Cisco IP Phone が 2 時間ごとに定期的に再同期されます。再同期障害が発生すると、デバイスは、30 分、1 時間、2 時間、4 時間の間隔で再試行します。正常に再同期されるまで、デバイスは、4 時間間隔で試行し続けます。

次の例のとおり、必要に応じて、プラス記号を使用して、ランダムな追加の遅延を付加する別の数値を指定することもできます。

```
Resync_Periodic=3600+600
Resync_Error_Retry_Delay=1800+300,3600+600,7200+900
```

前の例で、デバイスは、1 時間（プラス最大 10 分の追加のランダム遅延）ごとに定期的に再同期されます。再同期障害が発生すると、デバイスは、次の間隔で再試行します。30 分（プラス 最大 5 分）。1 時間（プラス 最大 10 分）、2 時間（プラス最大 15 分）。正常に再同期されるまで、デバイスは、2 時間間隔（プラス最大 15 分）で試行し続けます。

別の例を示します。

```
Upgrade_Error_Retry_Delay  =  1800,3600,7200,14400+3600
```

この例では、リモート アップグレードに失敗した場合、デバイスは、30 分後にアップグレードを再試行し、次に 1 時間後、次は 2 時間後に再試行します。それでもアップグレードに失敗する場合、デバイスは、アップグレードが成功するまで、4 時間から 5 時間ごとに再試行します。

プロファイル ルール

Cisco IP Phone は、複数のリモート設定プロファイル パラメータ（Profile_Rule*）を提供します。そのため、各再同期操作は、異なるサーバが管理する複数のファイルを取得できます。

最も簡単なシナリオでは、デバイスは、関係するすべての内部パラメータを更新する、中央サーバの単一のプロファイルに対して定期的に再同期されます。そうでない場合、プロファイルを異なるファイルの間で分割することができます。1 つのファイルは、導入時の Cisco IP Phone すべてに対して共通のファイルになります。他とは異なる固有のファイルが各アカウントに提供されます。暗号キーと証明書情報は、別のサーバに保存されている、さらに別のプロファイルから取得することも可能です。

再同期操作の時間になると、Cisco IP Phone は、4 つの Profile_Rule* パラメータを順に評価します。

1. Profile_Rule
2. Profile_Rule_B
3. Profile_Rule_C
4. Profile_Rule_D

各評価の結果、リモート プロビジョニング サーバからプロファイルが取得され、いくつかの内部パラメータのアップデートが発生する可能性があります。評価が失敗すると、再同期シーケンスは中断され、Resync_Error_Retry_Delay パラメータ（秒単位）によって指定された開始時間から再試行されます。すべての評価が成功すると、デバイスは、Resync_Periodic パラメータで指定された秒数の間待機した後、次の再同期を実行します。

各 Profile_Rule* パラメータの内容は、一連の選択肢で構成されます。それらの選択肢は、|(パイプ)文字で区切られます。各選択肢は、条件式、割り当て式、プロファイルの URL、および関連 URL のオプションで構成されています。これらすべてのコンポーネントは、各選択肢内のオプションです。次に示すのは、オプションの有効な組み合わせと、それらが存在する場合に従わなければならない表示順序です。

```
[ conditional-expr ] [ assignment-expr ] [[ options ] URL ]
```

各 Profile_Rule* パラメータ内で、最後の 1 つを除くすべての選択肢は、条件式を示す必要があります。この式は、次のように評価され処理されます。

1. 条件は、true と評価されるものが見つかるまで(または条件式を含まない 1 つの選択肢が見つかるまで)、左から右に評価されます。
2. いずれかの割り当て式を伴う場合には、それも評価されます。
3. 選択肢の一部として URL が指定される場合、指定された URL にあるプロファイルのダウンロードが試行されます。システムは、内部パラメータの更新を状況に応じて試行します。

すべての選択肢が条件式を含むものの、いずれも true と評価されない場合(またはプロファイル ルール全体が空の場合)、Profile_Rule* パラメータの全体がスキップされます。シーケンス内の次のプロファイル ルール パラメータが評価されます。

単一の Profile_Rule* パラメータに対して有効なプログラミングの例

この例は、指定された URL のプロファイルに対して無条件で再同期し、リモート プロビジョニング サーバに対して HTTP GET 要求を実行します。

```
http://remote.server.com/cisco/$MA.cfg
```

この例では、デバイスは、[回線 1(Line 1)] の登録ステータスに応じて、2 つの異なる URL に対して再同期します。登録が失われた場合、デバイスは、CGI スクリプトに対して HTTP POST を実行します。デバイスは、デバイスの状態に関する追加情報を提供する可能性のある、マクロ展開された GPP_A の内容を送信します。

```
($PRVTMR ge 600)? http://p.tel.com/has-reg.cfg
| [--post a] http://p.tel.com/lost-reg?
```

この例では、デバイスは、同じサーバに対して再同期されます。デバイスは、ユニットに証明書がインストールされていない場合、追加情報を提供します(2.0 よりも前のレガシー ユニットの場合)。

```
("$CCERT" eq "Installed")? https://p.tel.com/config?
| https://p.tel.com/config?cisco$MAU
```

この例では、[回線 1(Line 1)]は、GPP_A が最初の URL で Provisioned に等しくなるよう設定されるまでは無効です。その後、第 2 の URL に対して再同期されます。

```
("$A" ne "Provisioned")? (Line_Enable_1_ = "No";)! https://p.tel.com/init-prov
| https://p.tel.com/configs
```

この例では、サーバが返すプロファイルは、XML 要素タグを含むと想定します。これらのタグは、GPP_B に保存されるエイリアス マップにより、適切なパラメータ名に再配置される必要があります。

```
[--alias b] https://p.tel.com/account/$PN$MA.xml
```

再同期は、通常、要求されたプロファイルがサーバから受信されなかった場合に失敗と見なされます。Resync_Fails_On_FNF パラメータは、このデフォルトの動作をオーバーライドできます。Resync_Fails_On_FNF が [いいえ(No)] に設定されると、デバイスは、サーバからの file-not-found 応答を正常な再同期として受け入れます。Resync_Fails_On_FNF のデフォルト値は [いいえ(Yes)] です。

アップグレード ルール

Cisco IP Phone は、1 つの設定可能なリモート アップグレード パラメータ、Upgrade_Rule を提供します。このパラメータは、プロファイル ルール パラメータと類似した構文を受け入れます。URL オプションは、アップグレードではサポートされませんが、条件式と割り当て式は使用できます。条件式を使用すると、| 文字で区切られた複数の選択肢をパラメータに含めることができます。各選択肢の構文は次のとおりです。

```
[ conditional-expr ] [ assignment-expr ] URL
```

Profile_Rule* パラメータの場合、Upgrade_Rule パラメータは、条件式の要件が満たされるか、選択肢が条件式を含まなくなるまで、各選択肢を評価します。付属の割り当て式が指定されている場合、それも評価されます。次に、指定された URL に対するアップグレードが試行されます。

Upgrade_Rule が条件式を含まない URL を含む場合、デバイスは、URL の指定するファームウェア イメージに対してアップグレードを実行します。マクロ展開とルールの評価の後、デバイスは、ルールが変更されるか、scheme + server + port + filepath の有効な組み合わせが変更されるまで、アップグレードを再試行しません。

ファームウェア アップグレードを試行する際、デバイスは、手順の最初に音声を無効にし、手順の最後にリブートします。デバイスは、音声回線が現在非アクティブになっている場合にのみ、Upgrade_Rule の内容に基づくアップグレードを自動的に開始します。

Cisco IP Phone 7800 シリーズ の場合を次の例に示します。

```
http://p.tel.com/firmware/sip78xx.10-3-1-3PCC.loads
```

Cisco IP Phone 8800 シリーズ の場合は次のとおりです。

```
http://p.tel.com/firmware/sip88xx.10-3-1-3PCC.loads
```

この例では、Upgrade_Rule は、指定された URL に保存されたイメージに対してファームウェアをアップグレードします。

Cisco IP Phone 7800シリーズの別の例を次に示します。

```
("$F" ne "beta-customer")? http://p.tel.com/firmware/sip78xx.10-3-1-3PCC.loads
| http://p.tel.com/firmware/sip78xx.10-3-1-3PCC.loads
```

Cisco IP Phone 8880 シリーズ の場合は次のとおりです。

```
("$F" ne "beta-customer")? http://p.tel.com/firmware/sip88xx.10-3-1-3PCC.loads
| http://p.tel.com/firmware/sip88xx.10-3-1-3PCC.loads
```

この例では、汎用パラメータ GPP_F の内容に基づいて、2 つのイメージのいずれかをロードするようユニットに指示します。

デバイスは、便利なカスタマイズ オプションとなり得る、ファームウェア リビジョン番号に関するダウングレード制限を設定できます。有効なファームウェア リビジョン番号が Downgrade_Rev_Limit パラメータで設定されると、デバイスは、指定された制限よりも前のファームウェア バージョンに対するアップグレードの試行を拒否します。

データ型

設定プロファイル パラメータで使用されるのは、次のデータ型です。

- Uns<n>—符号なし n ビット値（n = 8、16、または32）。値が n ビットにフィットする限り、10 進数または 16 進数の形式（たとえば 12 または 0x18）で指定できます。
- Sig<n>—符号付 n ビット値。10 進数または 16 進数の形式で指定できます。“-” 記号を負の値の前に付ける必要があります。正の値の前 + 記号はオプションです。
- Str<n>—最大 n 個の非予約文字を含む一般的な文字列。
- Float<n>—小数点以下第 n 位までを含む浮動小数点値。
- Time<n>—小数点以下第 n 位までを含む秒単位の継続時間。追加で指定された小数点以下の桁は無視されます。
- PwrLevel—小数点以下第 1 位を含む、dBm で表される電力レベル。–13.5 や 1.5（dBm）など。
- Bool—“yes” または “no” のいずれかのブール値。
- {a,b,c,…}—a、b、c、…からの選択肢。
- IP—x.x.x.x の形式の IP アドレス。x は 0 と 255 の間。例：10.1.2.100
- Port—TCP/UDP ポート番号（0-65535）。10 進数または 16 進数の形式で指定できます。
- UserID—URL に表示されるユーザ ID。最大 63 文字。
- FQDN—完全修飾ドメイン名。“sip.Cisco.com:5060” または “109.12.14.12:12345” など。最大 63 文字を指定できます。
- Phone—電話番号の文字列。14081234567、*69、*72、345678 など。または、1234@10.10.10.100:5068 や jsmith@Cisco.com などの一般的な URL。この文字列には最大 39 文字を含めることができます。
- ActCode—補足サービスのアクティベーション コード。*69 など。このコードには最大 7 文字を含めることができます。
- PhTmplt—電話番号のテンプレート。各テンプレートには、カンマ（,）で区切られる 1 つ以上のパターンを含めることができます。各パターンの冒頭のスペースは無視されます。“?” と “*” はワイルドカード文字を示します。正確に表わすには、%xx を使用します。たとえば、%2a は * を表します。このテンプレートには最大 39 文字を含めることができます。例：“1408*, 1510*”、“1408123????, 555?1.”
- RscTmplt—SIP 応答ステータス コードのテンプレート。“404, 5*”、“61?”、“407, 408, 487, 481” など。最大 39 文字を指定できます。
- CadScript—信号のパターン パラメータを指定する小スクリプト。最大 127 文字。

  構文は $S_1[;S_2]$ で、次の意味があります。

  $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$ で、*セクション（section）*として知られています。$on_{i,j}$ と $off_{i,j}$ は、*セグメント（segment）*の秒単位の on/off 継続時間です。i = 1 または 2、および j = 1 から 6 です。D_i は、セクションの継続時間の合計（秒単位）です。すべての継続時間には、1 ms 単位の精度を実現するため、小数点以下第 3 位まで含めることができます。ワイルドカード文字 “*” は無限の期間を意味します。セクション内のセグメントは、順に実行され、全継続期間が実行されるまで繰り返されます。

  例 1：

```
60(2/4)

Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60 s
Number of Segments = 1
Segment 1: On=2s, Off=4s
```

```
Total Ring Length = 60s
```

例 2—特殊呼び出し音（短、短、短、長）

```
60(.2/.2,.2/.2,.2/.2,1/4)

Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60s
Number of Segments = 4
Segment 1: On=0.2s, Off=0.2s
Segment 2: On=0.2s, Off=0.2s
Segment 3: On=0.2s, Off=0.2s
Segment 4: On=1.0s, Off=4.0s

Total Ring Length = 60s
```

- FreqScript—呼び出し音の周波数およびレベルのパラメータを指定する小スクリプト。127 文字まで含めることができます。構文は $F_1@L_1[,F_2@_{L2}[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$ で、F_1–F_6 は Hz 単位の周波数を表します（符号なし整数のみ）。L_1–L_6 は、対応する dBm 単位のレベルを表します（小数点以下第 1 位までを含む）。カンマ前後のスペースは許容されますが、推奨されません。

  例 1—コール ウェイティング トーン

```
440@-10

Number of Frequencies = 1
Frequency 2 = 440 Hz at -10 dBm
```

  例 2—ダイヤル トーン

```
350@-19,440@-19

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
```

- ToneScript—コール プログレス トーンの周波数、レベル、パターンのパラメータを指定する小スクリプト。スクリプトには最大 127 文字を指定できます。構文は FreqScript;Z_1[;Z_2] です。セクション Z_1 は、CadScript の S_1 に類似していますが、各 on/off セグメントの後に、周波数コンポーネント パラメータ $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$ が続きます。$fi,j = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$ です。$1 < n_k < 6$ は、このセグメントで使用される、FreqScript の周波数コンポーネントを指定します。複数の周波数コンポーネントが 1 つのセグメントで使用される場合、それらのコンポーネントは 1 つにまとめられます。

  例 1—ダイヤル トーン

```
350@-19,440@-19;10(*/0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 10 s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 10s
```

  例 2—断続トーン

```
350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)
```

```
Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 2
Cadence Section 1: Section Length = 2s
Number of Segments = 1
Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
Cadence Section 2: Section Length = 10s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 12s
```

例 3—SIT トーン

```
985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0)
Number of Frequencies = 3
Frequency 1 = 985 Hz at -16 dBm
Frequency 2 = 1428 Hz at -16 dBm
Frequency 3 = 1777 Hz at -16 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 20s
Number of Segments = 4
Segment 1: On=0.38s, Off=0s, with Frequency 1
Segment 2: On=0.38s, Off=0s, with Frequency 2
Segment 3: On=0.38s, Off=0s, with Frequency 3
Segment 4: On=0s, Off=4s, with no frequency components
Total Tone Length = 20s
```

- ProvisioningRuleSyntax—設定再同期およびファームウェア アップグレード ルールの定義に使用されます。
- DialPlanScript—[回線 1(Line 1)] および [回線 2（Line 2）] のダイヤル プランの指定に使用される構文のスクリプトを作成します。

メモ

- <Par Name> は、設定パラメータの名前を表します。プロファイルでは、**Par_Name** のように、スペースをアンダースコア “_” に置き換えて対応するタグが作成されます。
- 空のデフォルト値フィールドは、空の文字列 < **“”** > を意味します。
- Cisco IP Phone は、特定のプロファイルに存在しないタグの最後の設定値を使用し続けます。
- テンプレートは、指定された順序で比較されます。最初に、*not the closest* で、一致が選択されます。パラメータ名は完全に一致する必要があります。
- プロファイル内のあるパラメータに複数の定義が指定されている場合、Cisco IP Phone ではファイル内の最後の定義が有効になります。
- 空のパラメータ値でパラメータを指定すると、指定されたパラメータは強制的にデフォルト値に戻されます。代わりに空の文字列を指定するには、パラメータ値として空の文字列 **""** を使用します。

プロファイル更新とファームウェア アップグレード

Cisco IP Phone は、セキュアなリモート プロビジョニング（設定）とファームウェア アップグレードをサポートします。プロビジョニングされていない電話は、そのデバイスを対象とする暗号化プロファイルを受信できます。SSL 機能を使用するセキュアな最初のプロビジョニング機能があるため、電話は明示的なキーを必要としません。

プロファイル更新やファームウェア アップグレードを開始または完了するのに、ユーザによる介入は必要ありません。以前のリリースから将来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、Cisco IP Phone のアップグレード 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。プロファイルの再同期は、再同期がソフトウェアのリブートをトリガーして通話が切断される可能性があるため、Cisco IP Phone がアイドル状態のときにのみ試行されます。

汎用パラメータは、プロビジョニング プロセスを管理します。各 Cisco IP Phone は、通常のプロビジョニング サーバ（NPS）と定期的にコンタクトをとるよう設定することができます。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するため、セキュア プロトコルを使用する必要はありません。NPS には、クライアント証明書を備えた標準的な TFTP、HTTP または HTTPS サーバのいずれかを使用できます。

管理者は、電話の Web ユーザ インターフェイス を使用して、Cisco IP Phone をアップグレード、リブート、再起動、または再起動することができます。また管理者は、これらのタスクを、SIP Notify メッセージを使用して実行することもできます。

設定プロファイルは、サービス プロバイダーのプロビジョニング システムと統合される、一般的なオープン ソース ツールを使用して生成されます。（プロビジョニングの詳細については、『*Cisco IP Phone 7800 Series and 8800 Series for Third-Party Call Control Provisioning Guide*』を参照してください）。

関連項目

- プロファイル更新の許可と設定（2-21 ページ）
- ファームウェア アップグレードの許可と設定（2-22 ページ）

プロファイル更新の許可と設定

プロファイル更新は、指定された間隔で許可できます。更新されたプロファイルは、TFTP、HTTP、または HTTPS を使用してサーバから電話に送信されます。

ステップ 1　[管理者ログイン（Admin Login）] > [詳細（advanced）] > [音声（Voice）] > [プロビジョニング（Provisioning）] とクリックします。

ステップ 2　[設定プロファイル（Configuration Profile）] セクションで、[プロビジョン有効（Provision Enable）] ドロップダウン リスト ボックスから **[はい（Yes）]** を選択します。

ステップ 3　パラメータを入力します。

ステップ 4　[すべての変更を送信（Submit All Changes）] をクリックします。

ファームウェア アップグレードの許可と設定

ファームウェアのアップデートは、指定された間隔で許可できます。更新されたファームウェアは、TFTP または HTTP を使用してサーバから電話に送信されます。ファームウェアには個人情報が含まれていないため、ファームウェア アップグレードでセキュリティは問題になりません。

ステップ 1　[管理者ログイン（Admin Login）] > [詳細（advanced）] > [音声（Voice）] > [プロビジョニング（Provisioning）] とクリックします。

ステップ 2　[ファームウェア アップグレード（Firmware Upgrade）] セクションで、[アップグレード有効化（Upgrade Enable）] ドロップダウン リスト ボックスから **[はい（Yes）]** を選択します。

ステップ 3　パラメータを入力します。

ステップ 4　[すべての変更を送信（Submit All Changes）] をクリックします。

tftp/http/https によるファームウェア アップグレード

3PCC は、tftp/http/https による単一のイメージ アップグレードをサポートします。

（注）　デバイス（新しいベースおよび DCU を含む）は、9.3(3)など、以前のファームウェア リリースにはダウングレードしない可能性があります。詳細については、最新のリリース ノート ドキュメント『*Cisco IP Phone 7800 Series for Third-Party Call Control Release Notes*』または『*Cisco IP Phone 8800 Series for Third-Party Call Control Release Notes*』のいずれかで、ハードウェア情報とファームウェアとハードウェアの互換性に関する情報を参照してください。

はじめる前に

ファームウェア ロード ファイルは、アクセス可能なサーバにダウンロードする必要があります。

ステップ 1　3PCC イメージの名前を次のように変更します。

cp-x8xx-sip.10-3-1-3PCC.cop
変更後
cp-x8xx-sip.10-3-1-3PCC.tar.gz

ステップ 2　“tar –xzvf” コマンドを使用して tar ボールを解凍します。

ステップ 3　フォルダを tftp/http/https のダウンロード ディレクトリにコピーします。

ステップ 4　電話の Web ユーザ インターフェイス で、[管理者ログイン（Admin Login）] > [詳細（advanced）] > [音声（Voice）] > [プロビジョニング（Provisioning）] と移動します。

ステップ 5　ロード ファイル名を検索し、有効な URL に追加します。

ステップ 6　[すべての変更を送信（Submit All Changes）] をクリックします。

ブラウザ コマンドによるファームウェア アップグレード

ブラウザのアドレス バーに入力されたアップグレード コマンドを使用して、電話のファームウェアをアップグレードすることができます。電話は、アイドル状態の場合にのみ更新されます。更新は、コールが完了すると自動的に試行されます。

ステップ：1　Web ブラウザの URL で Cisco IP Phone CP-78xx-3PCC をアップグレードするには、次のコマンドを入力します。

```
http://<phone_ip>/admin/upgrade?<schema>://<serv_ip[:port]>/filepath
```

企業に対するサードパーティ コール制御からのファームウェア アップグレード

ステップ 1　ダウンロード サーバにエンタープライズ ロードを配置します。

ステップ 2　電話の Web ユーザ インターフェイス で、[管理者ログイン（Admin Login）] > [詳細（advanced）] > [音声（Voice）] > [プロビジョニング（Provisioning）] と移動します。

ステップ 3　[ファームウェア アップグレード（Firmware Upgrade）] セクションで、[エンタープライズ イメージ アップグレードの有効化（Enable Enterprise Image Upgrade）] ドロップダウン リスト ボックスから [はい（Yes）] を選択します。

ステップ 4　[ファームウェア アップグレード（Firmware Upgrade）] セクションで、有効な URL 形式に [アップグレード ルール（Upgrade Rule）] フィールドを設定します。

```
<schema>:// <server[:port]> /filepath
```

ステップ 5　[すべての変更を送信（Submit All Changes）] をクリックします。

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

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。

コメント　サードパーティ コール制御向け Cisco IP Phone 7800/8800 シリーズは、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（HTTP Status Code）	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
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

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（HTTP Status Code）	説明	電話機の動作
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。Cisco 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。サードパーティ コール制御向け Cisco IP Phone 7800/8800 シリーズは、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、サードパーティ コール制御向け Cisco IP Phone 8841 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前記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。

プロビジョニングの例

この章では、Cisco IP Phone とプロビジョニング サーバ間で設定プロファイルを転送する手順を、例を挙げて説明します。

- 基本的な再同期（4-1 ページ）
- 安全な HTTPS 再同期（4-7 ページ）
- プロファイル管理（4-14 ページ）

設定プロファイルの作成については、第 2 章「プロビジョニング スクリプト」を参照してください。

基本的な再同期

ここでは、Cisco IP Phone の基本的な再同期機能について説明します。

TFTP の再同期

Cisco IP Phone は、設定プロファイルの取得に複数のネットワーク プロトコルをサポートしています。最も基本的なプロファイルの転送プロトコルは TFTP（RFC1350）です。TFTP は、プライベート LAN ネットワーク内のネットワーク デバイスのプロビジョニングに広く使用されています。インターネット経由のリモート エンドポイントの導入に使用するのはお勧めしませんが、TFTP は、小規模な組織内での導入、社内でのプロビジョニング、および開発とテストで使用するには便利です。社内でのプロビジョニングについては、「社内デバイスのプロビジョニング」セクション（3-2 ページ）を参照してください。この演習では、TFTP サーバからファイルをダウンロードした後に、プロファイルを変更します。

演習

ステップ 1 LAN 環境で、ハブ、スイッチ、または小規模なルータに PC および Cisco IP Phone を接続します。

ステップ 2 PC で、TFTP サーバをインストールして有効化します。

ステップ 3 テキスト エディタを使用して、例に示すように、GPP_A の値に 12345678 を設定した設定プロファイルを作成します。

```
<device> <flat-profile>
  <GPP_A> 12345678
  </GPP_A>
</flat-profile> </device>
```

ステップ 4　プロファイルに basic.txt という名前を付けて、TFTP サーバのルート ディレクトリに保存します。

次の方法で、TFTP サーバが正しく設定されていることを確認できます：Cisco IP Phone 以外の TFTP クライアントを使用して basic.txt ファイルをリクエストします。できれば、プロビジョニング サーバとは別のホストで実行されている TFTP クライアントを使用します。

ステップ 5　PC の Web ブラウザで admin/advanced のページを開きます。たとえば、電話機の IP アドレスが 192.168.1.100 の場合は次の URL を使用します。

```
http://192.168.1.100/admin/advanced
```

ステップ 6　[プロビジョニング（Provisioning）] タブを選択し、汎用パラメータの GPP_A から GPP_P の値を確認します。これらは空である必要があります。

ステップ 7　Web ブラウザ ウィンドウで再同期 URL を開き、テスト用 Cisco IP Phone を設定プロファイル basic.txt に再同期します。

TFTP サーバの IP アドレスが 192.168.1.200 の場合、コマンドはこの例のようになります。

```
http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt
```

このコマンドを Cisco IP Phone が受信すると、アドレス 192.168.1.100 のデバイスは、IP アドレスが 192.168.1.200 の TFTP サーバにファイル basic.txt をリクエストします。電話機はダウンロードしたファイルを解析し、GPP_A パラメータを値 12345678 に更新します。

ステップ 8　パラメータが正しく更新されていることを次の手順で確認します。PC の Web ブラウザの admin/advanced のページを更新し、そのページの [プロビジョニング（Provisioning）] タブを選択します。

GPP_A パラメータが値 12345678 になっている必要があります。

syslog を使用したロギング

デバイスがプロビジョニング サーバとの再同期を開始する際、および再同期が完了または失敗した後、Cisco IP Phone は syslog メッセージを専用の syslog サーバに送信します。このサーバは、Web サーバ管理（admin/advanced、[システム（System）] タブ、Syslog_Server パラメータ）で確認できます。syslog サーバの IP アドレスをデバイスに設定し、これ以降の演習中に生成されるメッセージを監視します。

演習

ステップ 1　ローカル PC に syslog サーバをインストールして有効化します。

ステップ 2　次のように、PC の IP アドレスをプロファイルの Syslog_Server パラメータに設定して、変更を送信します。

```
<Syslog_Server ua="na">192.168.1.210</Syslog_Server>
```

ステップ 3　[システム（System）] タブをクリックし、Syslog_Server パラメータにローカル syslog サーバの値を入力します。

ステップ 4　「TFTP の再同期」の演習で説明されているようにして、再同期操作を繰り返します。

デバイスは再同期中に 2 件の syslog メッセージを生成します。最初のメッセージは、リクエストが進行中であることを示します。2 番目のメッセージは、再同期が成功または失敗したことを示します。

ステップ 5　syslog サーバが以下のようなメッセージを受信したことを確認します。

```
CP-78xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txt
CP-88xx-3PCC 00:0e:08:ab:cd:ef -- Successful resync tftp://192.168.1.200/basic.txt
```

詳細なメッセージを利用できるようにするには、次のように、(Syslog_Server パラメータの代わりに)Debug_Server パラメータに syslog サーバの IP アドレスを設定し、Debug_Level パラメータに 0 ～ 3 の範囲(3 が最も詳細)の値を設定します。

```
<Debug_Server ua="na">192.168.1.210</Debug_Server>
<Debug_Level ua="na">3</Debug_Level>
```

これらのメッセージの内容は、次のパラメータを使用して設定できます。

- Log_Request_Msg
- Log_Success_Msg
- Log_Failure_Msg

これらのパラメータのいずれかが削除されると、対応する syslog メッセージは生成されなくなります。

デバイスの自動再同期

(エンドポイントに明示的な再同期リクエストを送信するのではなく)デバイスを定期的にプロビジョニング サーバに再同期させて、サーバに対して行われたプロファイルの変更を確実にエンドポイント デバイスに伝達することができます。

Cisco IP Phone にサーバへの定期的な再同期を行わせるには、Profile_Rule パラメータを使用して設定プロファイルの URL を定義し、さらに Resync_Periodic パラメータを使用して再同期間隔を定義します。

演習

ステップ 1　Web ブラウザを使用して、admin/advanced のページの [プロビジョニング(Provisioning)] タブを開きます。

ステップ 2　Profile_Rule パラメータを定義します。次の例では、TFTP サーバの IP アドレスを 192.168.1.200 と仮定しています。

```
<Profile_Rule ua="na">tftp://192.168.1.200/basic.txt</Profile_Rule>
```

ステップ 3　Resync_Periodic パラメータに、テスト用として **30** 秒などの小さい値を入力します。

```
<Resync_Periodic ua="na">30</Resync_Periodic>
```

ステップ 4　[すべての変更を送信(Submit all Changes)] をクリックします。

新しいパラメータ設定により、Cisco IP Phone は URL で指定された設定ファイルに対して 1 分間に 2 回再同期を行います。

ステップ 5　syslog トレースの結果メッセージを(「syslog を使用したロギング」セクションで説明されているようにして)確認します。

ステップ 6　Resync_On_Reset パラメータが次のように [はい(yes)] に設定されていることを確認します。

```
<Resync_On_Reset ua="na">Yes</Resync_On_Reset>
```

ステップ 7　電源を再投入して、Cisco IP Phone を強制的にプロビジョニング サーバと再同期させます。

サーバが無応答など、何らかの理由で再同期操作が失敗すると、ユニットは（Resync_Error_Retry_Delay に設定した秒数だけ）待機した後、もう一度再同期を試みます。Resync_Error_Retry_Delay が 0 の場合、Cisco IP Phone は再同期が失敗しても、再同期を試行しません。

ステップ 8　（任意）Resync_Error_Retry_Delay の値に **30** などの小さい数値を設定します。

```
<Resync_Error_Retry_Delay ua="na">30</Resync_Error_Retry_Delay>
```

ステップ 9　TFTP サーバを無効化して、syslog 出力の結果を確認します。

固有のプロファイル、マクロ展開、および HTTP

各 Cisco IP Phone の User_ID、Display_Name といったパラメータに個別の値を設定する必要があるような導入では、サービス プロバイダーが、導入されるデバイスそれぞれに固有のプロファイルを作成して、プロビジョニング サーバでそれらのプロファイルをホストすることができます。事前に定義されたプロファイルの命名規則に従って、それぞれの Cisco IP Phone が自身のプロファイルに次々と再同期するよう設定される必要があります。

プロファイル URL の構文には、組み込み変数のマクロ展開を使用して、各 Cisco IP Phone に固有の識別情報（MAC アドレス、シリアル番号など）を含めることができます。マクロ展開を使用すれば、各プロファイルの複数箇所で前記の値を指定する必要がなくなります。

プロファイルのルールは、Cisco IP Phone に適用される前にマクロ展開の適用を受けます。マクロ展開は値の数値を制御します。たとえば、

- $MA は、ユニットの 12 桁の MAC アドレスに展開されます（小文字の 16 進数を使用）。たとえば、000e08abcdef などのようになります。
- $SN は、ユニットのシリアル番号に展開されます。たとえば、88012BA01234 などのようになります。

GPP_A から GPP_P までのすべての汎用パラメータなど、他の値も同様にマクロ展開されます。この手順の例が「TFTP の再同期」セクションで説明されています。マクロ展開は URL のファイル名だけでなく、プロファイル ルール パラメータの任意の部分に適用できます。これらのパラメータは $A ～ $P として参照されます。マクロ展開で使用できるすべての変数の一覧については、「マクロ展開変数」セクション（5-5 ページ）を参照してください。

この演習では、Cisco IP Phone に固有のプロファイルを TFTP サーバ上でプロビジョニングします。演習では例として Cisco Phone 7841 を使用しますが、この内容はすべての Cisco IP Phone 7800/8800 シリーズ モデルに共通です。

演習

ステップ 1　製品ラベルで電話機の MAC アドレスを確認します（MAC アドレスは、000e08aabbcc などの、数字と小文字の 16 進数を使用する番号です）。

ステップ 2　設定ファイル `basic.txt`（「TFTP の再同期」の演習で説明されています）を、**CP-***x8xx*-3PCC_*macaddress*.cfg という名前の新しいファイルにコピーします（*x8xx* をモデル番号に、*macaddress* を電話機の MAC アドレスにそれぞれ置き換えます）。次に例を示します。

```
CP-7841-3PCC_000e08abcdef.cfg
```

ステップ 3　TFTP サーバの仮想ルート ディレクトリに新しいファイルを移動します。

ステップ 4　admin/advanced のページの [プロビジョニング（Provisioning）] タブを開きます。

ステップ 5　Profile_Rule パラメータに `tftp://192.168.1.200/CP-7841-3PCC$MA.cfg` と入力します。

```
<Profile_Rule ua="na">
  tftp://192.168.1.200/CP-7841-3PCC$MA.cfg
</Profile_Rule>
```

ステップ 6　[すべての変更を送信（Submit All Changes）] をクリックします。これにより、リブートと再同期がただちに行われます。

次の再同期時に、$MA マクロの式が MAC アドレスに展開されて、Cisco IP Phone は新しいファイルを取得します。

HTTP GET 再同期

HTTP は TCP 接続を確立し、TFTP は信頼性に劣る UDP を使用するため、HTTP は TFTP より信頼性の高い再同期方式を提供します。また、HTTP サーバは、TFTP サーバと比べてより強化されたフィルタリング機能とロギング機能を備えています。

クライアント側の Cisco IP Phone が HTTP を使用した再同期を使用できるようにするために、サーバで特別な構成設定を行う必要はありません。GET メソッドで HTTP を使用するための Profile_Rule パラメータの構文は、TFTP の場合の構文と同様です。標準的な Web ブラウザで HTTP サーバからプロファイルを取得できるならば、Cisco IP Phone も同様にできます。

演習

ステップ 1　ローカル PC またはその他のアクセス可能なホストに HTTP サーバをインストールします（オープン ソースの Apache サーバがインターネットからダウンロードできます）。

ステップ 2　設定プロファイル `basic.txt`（「TFTP の再同期」の演習で説明されています）をそのインストールしたサーバの仮想ルート ディレクトリにコピーします。

ステップ 3　サーバが適切にインストールされ、basic.txt にアクセスできることを確認するために、Web ブラウザを使用してプロファイルにアクセスします。

ステップ 4　プロファイルが定期的にダウンロードできるようにするために、テスト用 Cisco IP Phone の Profile_Rule を変更し、TFTP サーバの代わりに HTTP サーバを指すようにします。

たとえば、HTTP サーバが 192.168.1.300 と仮定した場合、次の値を入力します。

```
<Profile_Rule ua="na">
http://192.168.1.200/basic.txt
</Profile_Rule>
```

ステップ 5　[すべての変更を送信（Submit All Changes）] をクリックします。これにより、リブートと再同期がただちに行われます。

ステップ 6　Cisco IP Phone が送信した syslog メッセージを確認します。定期的な再同期で、HTTP サーバからプロファイルが取得されている必要があります。

ステップ 7　HTTP サーバのログで、テスト用 Cisco IP Phone を特定する情報がユーザ エージェントのログにどのように表示されるかを確認します。

この情報には、製造者、製品名、現在のファームウェア バージョン、およびシリアル番号が含まれている必要があります。

Cisco XML を介したプロビジョニング

ここでは x8xx として表される Cisco IP Phone 7800/8800 シリーズはそれぞれ、Cisco XLM の機能を介して以下のようにしてプロビジョニングされます。

CP-x8xx-3PCC では Cisco XML の機能が拡張され、XML オブジェクトを介したプロビジョニングがサポートされています。

```
<CP-x8xx-3PCCExecute>
        <ExecuteItem URL=Resync:[profile-rule]/>
</CP-x8xx-3PCCExecute>
```

XML オブジェクトを受信した後、CP-x8xx-3PCC はプロビジョニング ファイルを [profile-rule] からダウンロードします。このルールでは、XML サービス アプリケーションの開発を容易にするマクロが使用されています。

マクロ展開を使用した URL の解決

複数のプロファイルがあるサーバ上のサブディレクトリでは、多数の導入済みデバイスを管理するための便利な方法が提供されます。プロファイル URL には以下を含めることができます。

- プロビジョニング サーバ名または明示的な IP アドレス。プロファイルで、プロビジョニング サーバが名前で指定されている場合、Cisco IP Phone は DNS ルックアップを実行して名前を解決します。
- サーバ名の後に続く標準の構文 *:port* を使用して、URL で指定される非標準サーバ ポート。
- 標準 URL 表記を使用して指定され、マクロ展開により管理されるプロファイルが保存されている、サーバ仮想ルート ディレクトリのサブディレクトリ。

たとえば、次の Profile_Rule は、ポート 6900 の接続をリスニングするホスト prov.telco.com で実行されている TFTP サーバから、サーバの /cisco/config サブディレクトリにあるプロファイル CP-7841-3PCC.cfg をリクエストします。

```
<Profile_Rule ua="na">
tftp://prov.telco.com:6900/cisco/config/$PN.cfg
</Profile_Rule>
```

各 Cisco IP Phone のプロファイルは汎用パラメータにより特定できます。これらはマクロ展開を使用して共通プロファイル ルール内で値が参照されます。

たとえば、GPP_B に `Dj6Lmp23Q` が定義されていると仮定します。

Profile_Rule は次の値になります。

```
tftp://prov.telco.com/cisco/$B/$MA.cfg
```

デバイスの再同期およびマクロの展開時に、MAC アドレスが 000e08012345 の Cisco IP Phone は、デバイスの MAC アドレスを含む名前が記載されたプロファイルを、次の URL でリクエストします。

```
tftp://prov.telco.com/cisco/Dj6Lmp23Q/000e08012345.cfg
```

安全な HTTPS 再同期

安全な通信プロセスを使用して再同期を行うために、Cisco IP Phone では以下の方式が使用できます。

- 基本的な HTTPS 再同期
- クライアント証明書認証を使用した HTTPS
- HTTPS クライアントのフィルタリングとダイナミック コンテンツ

関連項目

- 基本的な HTTPS 再同期（4-7 ページ）
- クライアント証明書認証を使用した HTTPS（4-9 ページ）
- HTTPS クライアントのフィルタリングとダイナミック コンテンツ（4-9 ページ）

基本的な HTTPS 再同期

HTTPS では、リモート プロビジョニングの HTTP に SSL が追加されるため、以下が可能になります。

- Cisco IP Phone はプロビジョニング サーバを認証することができます。
- プロビジョニング サーバは Cisco IP Phone を認証することができます。
- Cisco IP Phone とプロビジョニング サーバ間で交換される情報の機密性が保証されます。

SSL は、Cisco IP Phone とプロビジョニング サーバに事前にインストールされている公開キー/秘密キーのペアを使用して、Cisco IP Phone とサーバ間の各接続に対して、秘密の（対称）キーを生成して交換します。

クライアント側の Cisco IP Phone が HTTPS を使用した再同期を使用できるようにするために、サーバで特別な構成設定を行う必要はありません。GET メソッドで HTTPS を使用するための Profile_Rule パラメータの構文は、HTTP または TFTP の場合の構文と同様です。標準的な Web ブラウザで HTTPS サーバからプロファイルを取得できるならば、Cisco IP Phone も同様にできます。

HTTPS サーバのインストールに加えて、Cisco が署名した SSL サーバ証明書がプロビジョニング サーバにインストールされている必要があります。Cisco が署名したサーバ証明書をサーバが提供しない場合、デバイスは HTTPS を使用するサーバに再同期できません。音声製品向けの署名付き SSL 証明書を作成する手順については、https://supportforums.cisco.com/docs/DOC-9852 を参照してください。

演習

ステップ 1　通常のホスト名変換により、ネットワーク DNS サーバによって IP アドレスが特定されるホストに、HTTPS サーバをインストールします。

オープン ソース Apache サーバが、オープン ソース mod_ssl パッケージと共にインストールされている場合には、HTTPS サーバとして動作するように設定できます。

ステップ 2　そのサーバのサーバ証明書署名要求を生成します。この手順では、オープン ソースの OpenSSL パッケージまたは同等のソフトウェアのインストールが必要な場合があります。OpenSSL を使用する場合、基本 CSR ファイルを生成するコマンドは次のとおりです。

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

このコマンドにより公開キー/秘密キーのペアが生成され、privkey.pem ファイルに保存されます。

ステップ 3　署名のために Cisco に CSR ファイル（provserver.csr）を提出します（詳細については、https://supportforums.cisco.com/docs/DOC-9852 を参照してください）。署名付きサーバ証明書が、Sipura CA クライアント ルート証明書 spacroot.cert と共に返送されます。

ステップ 4　署名付きサーバ証明書、秘密キーのペアのファイル、およびクライアント ルート証明書をサーバの適切な場所に保存します。

Linux に Apache をインストールしている場合、これらは通常以下の場所にあります。

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```

ステップ 5　サーバを再起動します。

ステップ 6　設定ファイル `basic.txt`（「TFTP の再同期」の演習で説明されています）を HTTPS サーバの仮想ルート ディレクトリにコピーします。

ステップ 7　ローカル PC で標準的なブラウザを使用して、HTTPS サーバから basic.txt をダウンロードし、サーバの動作が適切であることを確認します。

ステップ 8　サーバが提供したサーバ証明書を確認します。

Cisco をルート CA として受け入れるようにブラウザが事前に設定されていない場合、ブラウザは証明書が有効であることほとんど認識しません。ただし、Cisco IP Phone では証明書がこの方法で署名されることを期待しています。

テスト用デバイスの Profile_Rule を変更して、HTTPS サーバへの参照が含まれるようにします。たとえば次のように設定します。

```
<Profile_Rule ua="na">
https://my.server.com/basic.txt
</Profile_Rule>
```

この例では、HTTPS サーバの名前が `my.server.com` であると仮定しています。

ステップ 9　[すべての変更を送信（Submit All Changes）] をクリックします。

ステップ 10　Cisco IP Phone が送信した syslog トレースを確認します。

再同期で HTTPS サーバからプロファイルが取得されたことが、syslog メッセージに示されている必要があります。

ステップ 11　（任意）Cisco IP Phone サブネットでイーサネット プロトコル アナライザを使用して、パケットが暗号化されていることを確認します。

この演習では、クライアント証明書の検証は有効になっていません。Cisco IP Phone とサーバ間の接続は暗号化されます。ただし、ファイル名とディレクトリの場所が分かれば、あらゆるクライアントがサーバに接続し、ファイルをリクエストできるため、転送は安全ではありません。安全に再同期するためには、サーバは、「クライアント証明書認証を使用した HTTPS」セクションで説明されている演習の手順に従ってクライアントを認証する必要もあります。

クライアント証明書認証を使用した HTTPS

工場出荷時のデフォルト設定では、サーバはクライアントから SSL クライアント証明書をリクエストしません。あらゆるクライアントがサーバに接続し、プロファイルをリクエストできるため、プロファイルの転送は安全ではありません。設定を編集して、クライアント認証を有効にすることができます。サーバは、接続リクエストを受け入れる前に Cisco IP Phone を認証するために、クライアント証明書が必要です。

この要件があるため、適切な認証情報がないブラウザを使用して、再同期操作を個別にテストすることはできません。テスト用 Cisco IP Phone とサーバ間の HTTPS 接続での SSL キー交換は、ssldump ユーティリティで確認できます。このユーティリティのトレースにより、クライアントとサーバ間の相互通信が表示されます。

演習

ステップ 1　HTTPS サーバでクライアント証明書認証を有効化します。

ステップ 2　Apache（v.2）では、サーバ設定ファイルを次のように設定します。

```
SSLVerifyClient  require
```

また、spacroot.cert が、「基本的な HTTPS 再同期」の演習で説明されている手順で保存されていることを確認します。

ステップ 3　HTTPS サーバを再起動した後、Cisco IP Phone からの syslog トレースを確認します。

これで、サーバに再同期するたびに対称認証が実行されるようになりました。これにより、プロファイルが転送される前にサーバ証明書とクライアント証明書の両方が検証されます。

ステップ 4　ssldump を使用して、Cisco IP Phone と HTTPS サーバ間の再同期接続を採取します。

クライアント証明書の検証がサーバで適切に有効化されている場合には、ssldump トレースには、プロファイルを含む暗号化されたパケットの前に、証明書が相互に交換されたことが示されます（最初にサーバからクライアントへ、次にクライアントからサーバへ）。

クライアントの認証が有効化されていると、有効なクライアント証明書と一致する MAC アドレスの Cisco IP Phone のみが、プロビジョニング サーバのプロファイルをリクエストできます。サーバは、通常のブラウザやその他の不正なデバイスからのリクエストを拒否します。

HTTPS クライアントのフィルタリングとダイナミック コンテンツ

クライアント証明書が必要となるように HTTPS サーバが設定されている場合、再同期している Cisco IP Phone が証明書の情報により識別され、正しい設定情報が渡されます。

HTTPS サーバにより、証明書の情報が、再同期リクエストの一環として起動される CGI スクリプト（またはコンパイルされた CGI プログラム）で使用可能になります。説明の都合から、この演習ではオープン ソースの Perl スクリプト言語を使用し、HTTPS サーバとして Apache（v.2）が使用されていると仮定します。

演習

ステップ 1　HTTPS サーバを実行しているホストに Perl をインストールします。

ステップ 2　以下の Perl リフレクタ スクリプトを生成します。

```
#!/usr/bin/perl -wT
use strict;
print “Content-Type: text/plain\n\n”;
print “<flat-profile><GPP_D>”;

print “OU=$ENV{‘SSL_CLIENT_I_DN_OU’},\n”;
print “L=$ENV{‘SSL_CLIENT_I_DN_L’},\n”;
print “S=$ENV{‘SSL_CLIENT_I_DN_S’}\n”;
print “</GPP_D></flat-profile>”;
```

ステップ 3　このファイルに reflect.pl という名前を付けて、HTTPS サーバの CGI スクリプトのディレクトリに、実行権限（Linux では chmod 755）で保存します。

ステップ 4　サーバの CGI スクリプトにアクセスできるかどうかを確認します（/cgi-bin/...で）。

ステップ 5　テスト用デバイスで Profile_Rule を変更し、次の例のようにしてリフレクタ スクリプトに再同期します。

```
https://prov.server.com/cgi-bin/reflect.pl?
```

ステップ 6　[すべての変更を送信（Submit All Changes）] をクリックします。

ステップ 7　syslog トレースを参照し、再同期が成功したことを確認します。

ステップ 8　admin/advanced のページの [プロビジョニング（Provisioning）] タブを開きます。

ステップ 9　GPP_D パラメータにスクリプトが採取した情報が含まれていることを確認します。

テスト用デバイスが製造者からの固有の証明書を保持している場合、この情報には、製品名、MAC アドレス、およびシリアル番号が含まれています。ユニットがファームウェア リリース 2.0 より前に製造されている場合、この情報には一般的な文字列が含まれています。

同様なスクリプトにより、再同期デバイスに関する情報を識別し、適切な設定パラメータ値をデバイスに提供できます。

HTTPS 証明書

Cisco IP Phone は、デバイスからプロビジョニング サーバへの HTTPS リクエストに基づく信頼性の高い安全なプロビジョニング手段を提供します。サーバ証明書とクライアント証明書の両方が、Cisco IP Phone からサーバ、およびサーバから Cisco IP Phone の認証で使用されます。

電話機で HTTPS を使用するには、証明書署名要求（CSR）を生成し、Cisco に提出する必要があります。Cisco IP Phone は、プロビジョニング サーバへのインストール用の証明書を生成します。Cisco IP Phone は、プロビジョニング サーバとの HTTPS 接続を確立しようとする際に証明書を受け入れます。

HTTPS 方式

HTTPS によりクライアントとサーバ間の通信が暗号化されるため、他のネットワーク デバイスからメッセージの内容が保護されます。クライアントとサーバ間の通信本文の暗号化方式は、対称キー暗号化に基づいています。対称キー暗号化では、公開キー/秘密キーの暗号化によって保護された安全なチャネル上で、1 つの秘密キーをクライアントとサーバで共有します。

秘密キーで暗号化されたメッセージは、同じキーを使用しなければ復号化できません。HTTPS は、対称暗号化アルゴリズムを広くサポートしています。Cisco IP Phone では、128 ビット RC4 に加えて、米国の暗号化標準（AES）を使用した 256 ビットまでの対称暗号化を実装しています。

HTTPS はまた、安全なトランザクションで実行されるサーバとクライアントの認証も提供します。これにより、プロビジョニング サーバと個々のクライアントは、ネットワーク上の他のデバイスによってスプーフィングできなくなります。この機能は、リモート エンドポイント プロビジョニングでは必須です。

サーバとクライアント間の認証は、公開キーが含まれている証明書を使用し、公開キー/秘密キー暗号化によって実行されます。公開キーで暗号化されたテキストは、対応する秘密キーでのみ復号化できます（逆も同様です）。Cisco IP Phone は、Rivest-Shamir-Adleman（RSA）アルゴリズムを公開キー/秘密キーの暗号化でサポートしています。

SSL サーバ証明書

安全なプロビジョニング サーバには個別に、Cisco が直接署名したセキュア ソケット レイヤ（SSL）サーバ証明書が発行されています。Cisco IP Phone で動作するファームウェアは、Cisco の証明書のみを有効として認識します。クライアントは、HTTPS を使用してサーバに接続する際、Cisco によって署名されていないサーバ証明書を拒否します。

この方式により、Cisco IP Phone への不正アクセスや、プロビジョニング サーバをスプーフィングする試みからサービス プロバイダーを保護します。このような保護がない場合、攻撃者は、Cisco IP Phone を再プロビジョニングして、設定情報を取得したり、別の VoIP サービスを使用したりする可能性があります。有効なサーバ証明書に対応する秘密キーを使用しないと、攻撃者は Cisco IP Phone との通信を確立できません。

サーバ証明書を取得する

ステップ 1　証明書のプロセスについては、ユーザを担当する Cisco のサポート担当者に確認してください。特定のサポート担当者がいない場合は、電子メールで ciscosb-certadmin@cisco.com にリクエストを送信してください。

ステップ 2　CSR（証明書署名要求）で使用される秘密キーを生成します。このキーは秘密であり、Cisco のサポートに提供する必要はありません。オープン ソースの「openssl」を使用してキーを生成します。次に例を示します。

```
openssl genrsa -out <file.key> 1024
```

ステップ 3　ユーザの組織と場所を識別するフィールドを含む CSR を生成します。次に例を示します。

```
openssl req -new -key <file.key> -out <file.csr>
```

以下の情報が必要です。

- 件名フィールド：共通名（CN）を入力します。これは FQDN（完全修飾ドメイン名）構文である必要があります。SSL 認証のハンドシェイク中に、Cisco IP Phone は、受信した証明書がそれを提出した装置からのものであるかどうかを確認します。
- サーバ ホスト名：たとえば、provserv.domain.com など。
- 電子メールアドレス：必要な場合にカスタマー サポートがユーザに連絡を取れるようにするために、電子メールアドレスを入力します。この電子メールアドレスは、CSR に表示されます。

ステップ 4　Cisco のサポート担当者または次のアドレスに、CSR（zip ファイル形式）を電子メールで送信します ciscosb-certadmin@cisco.com 証明書が Cisco によって署名されます。Cisco は、システムにインストールする証明書をユーザに送信します。

クライアント証明書

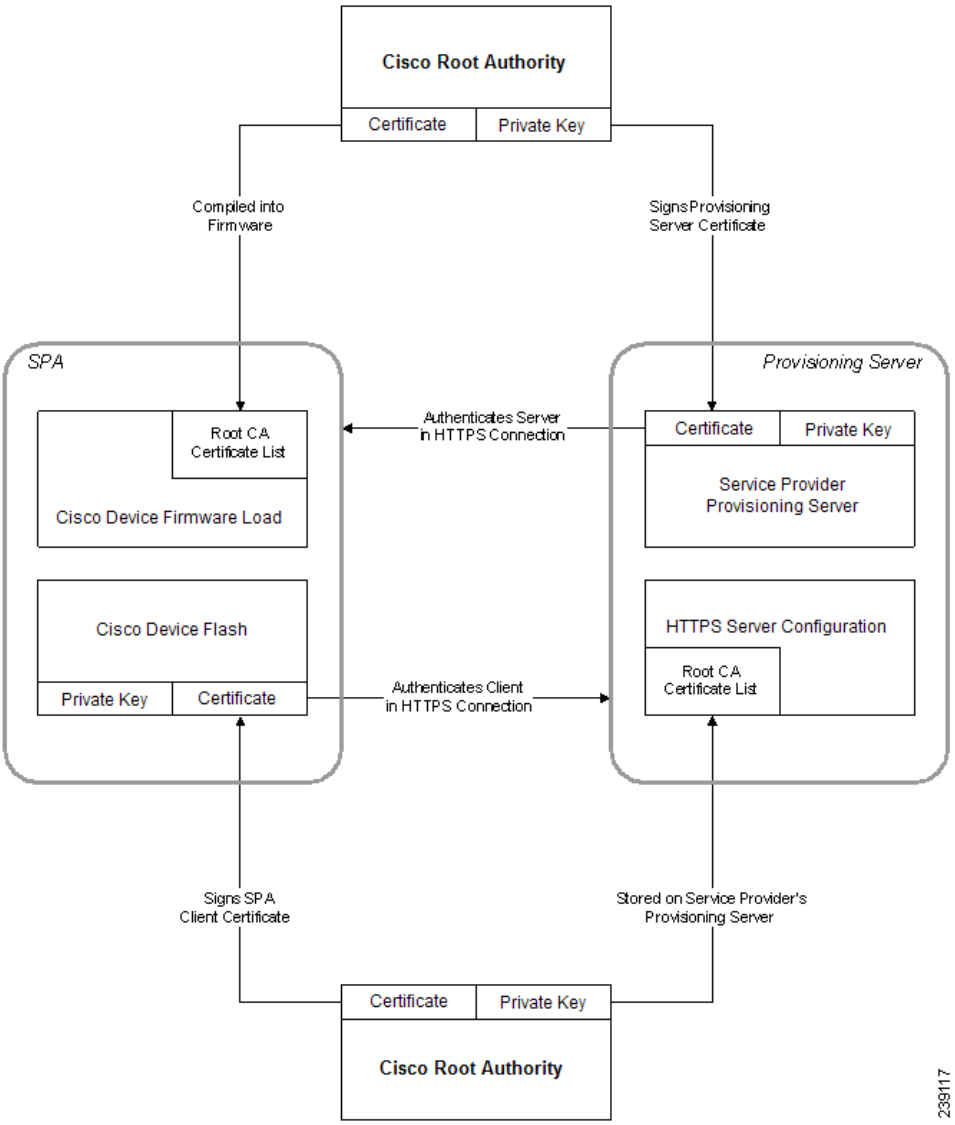
Cisco IP Phone への直接攻撃以外にも、攻撃者は、標準的な Web ブラウザや他の HTTPS クライアントを介してプロビジョニング サーバに接続し、プロビジョニング サーバから設定プロファイルを取得しようとする可能性があります。この種の攻撃を防ぐため、各 Cisco IP Phone は、Cisco によって署名され、個々のエンドポイントに関する識別情報を含む固有のクライアント証明書も保持しています。デバイスのクライアント証明書を認証できる認証局ルート証明書が、各サービス プロバイダーに提供されます。この認証パスにより、プロビジョニング サーバは不正な設定プロファイルのリクエストを拒否することができます。

証明書の構造

サーバ証明書とクライアント証明書の組み合わせにより、リモート Cisco IP Phone とそのプロビジョニング サーバ間のセキュア通信が保証されます。図 4-1 には、Cisco クライアント、プロビジョニング サーバ、および認証局間での、証明書、公開キー/秘密キーのペア、および署名するルート認証局の関係が図示されています。

図の上半分には、個別のプロビジョニング サーバ証明書への署名に使用されるプロビジョニング サーバ ルート認証局が示されています。対応するルート証明書がファームウェアに組み込まれ、これを使用して、Cisco IP Phone は正規のプロビジョニング サーバを認証することができます。

図 4-1　　認証局のフロー



カスタム認証局を設定する

ネットワーク上のネットワーク デバイスおよびユーザの認証にデジタル証明書が使用できます。これは、ネットワーク ノード間の IPSec セッションのネゴシエートに使用できます。

サード パーティは認証局証明書を使用して、通信を試みている複数のノードを検証し、認証します。各ノードには公開キーと秘密キーがあります。公開キーでデータを暗号化します。秘密キーでデータを復号化します。ノードは同じソースから証明書を取得しているため、それぞれの同一性が保証されます。

デバイスは、サードパーティの認証局（CA）により提供されるデジタル証明書を使用して、IPSec 接続を認証することができます。

電話機は、ファームウェアに組み込まれて事前にロードされる、以下の一連のルート認証局をサポートしています。

- Cisco Small Business CA 証明書
- CyberTrust CA 証明書
- Verisign CA 証明書
- Sipura ルート CA 証明書
- Linksys ルート CA 証明書

ステップ 1　[管理者ログイン（Admin Login）] > [詳細（advanced）] > [情報（Info）] > [ステータスをダウンロード（Download Status）] の順にクリックします。

ステップ 2　[カスタム CA ステータス（Custom CA Status）] までスクロールし、以下のフィールドを確認します。

- [カスタム CA プロビジョニング ステータス（Custom CA Provisioning Status）] : プロビジョニングのステータスを示します。
  - 最後のプロビジョニングが mm/dd/yyyy HH:MM:SS に成功した
  - 最後のプロビジョニングが mm/dd/yyyy HH:MM:SS に失敗した
- [カスタム CA 情報（Custom CA Info）] : カスタム CA に関する情報を表示します。
  - [インストール済み（Installed）] :「CN 値」が表示されます。ここで、「CN 値」は最初の証明書の件名フィールドの CN パラメータの値です。
  - [未インストール（Not Installed）] : カスタム CA 証明書がインストールされていない場合に表示されます。

プロファイル管理

ここでは、ダウンロードの準備として設定プロファイルの構成を説明します。機能の説明のために、ローカル PC からの TFTP を再同期手段として使用しますが、HTTP または HTTPS も同様に使用できます。

プロファイルの gzip 圧縮を開く

プロファイルですべてのパラメータを個々に指定すると、XML 形式の設定プロファイルはかなり大きくなる可能性があります。プロビジョニング サーバの負荷を軽減するため、Cisco IP Phone では、gzip ユーティリティ（RFC 1951）がサポートするデフレート圧縮形式を使用した XML ファイルの圧縮がサポートされています。

（注）　圧縮され暗号化された XML プロファイルを Cisco IP Phone が認識できるようにするために、暗号化より先に圧縮が行われる必要があります。

カスタマイズされたバックエンド プロビジョニング サーバ ソリューションに統合する場合は、スタンドアロン gzip ユーティリティの代わりにオープン ソースの zlib 圧縮ライブラリを使用して、プロファイルの圧縮が実行できます。ただし、Cisco IP Phone はファイルに有効な gzip ヘッダーが含まれていることを期待しています。

演習

ステップ 1　ローカル PC に gzip をインストールします。

ステップ 2　コマンド ラインから gzip を起動して、設定プロファイル `basic.txt`（「TFTP の再同期」の演習で説明されています）を圧縮します。

```
gzip basic.txt
```

これにより、縮小ファイル `basic.txt.gz` が生成されます。

ステップ 3　TFTP サーバの仮想ルート ディレクトリにファイル `basic.txt.gz` を保存します。

ステップ 4　次の例に示すようにして、テスト用デバイスで Profile_Rule を変更し、元の XML ファイルの代わりに縮小ファイルに再同期するようにします。

```
tftp://192.168.1.200/basic.txt.gz
```

ステップ 5　[すべての変更を送信（Submit All Changes）] をクリックします。

ステップ 6　Cisco IP Phone からの syslog トレースを確認します。

再同期時、Cisco IP Phone は新しいファイルをダウンロードし、これを使用して自身のパラメータを更新します。

関連項目

- オープン プロファイルの圧縮（2-6 ページ）

OpenSSL を使用したプロファイル暗号化

圧縮または未圧縮のプロファイルが暗号化できます（ただし、ファイルは暗号化される前に圧縮されている必要があります）。暗号化は、Cisco IP Phone とプロビジョニング サーバ間の通信に TFTP または HTTP が使用される場合など、プロファイル情報の機密性が特に問題となる場面で有用です。

Cisco IP Phone は、256 ビット AES アルゴリズムを使用する対称キー暗号化をサポートしています。この暗号化は、オープン ソースの OpenSSL パッケージを使用して実行できます。

演習

ステップ 1　ローカル PC に OpenSSL をインストールします。この際、AES を有効にするために OpenSSL アプリケーションの再コンパイルが必要な場合があります。

ステップ 2　設定ファイル `basic.txt`（「TFTP の再同期」の演習で説明されています）を使用し、次のコマンドを実行して暗号化されたファイルを生成します。

```
>openssl enc -aes-256-cbc -k MyOwnSecret -in basic.txt -out basic.cfg
```

XML プロファイルは圧縮と暗号化の両方が行えるため、プロファイルの gzip 圧縮を開くで作成された圧縮ファイル basic.txt.gz も使用できます。

ステップ 3　TFTP サーバの仮想ルート ディレクトリに、暗号化された basic.cfg ファイルを保存します。

ステップ 4　テスト用デバイスで Profile_Rule を変更し、元の XML ファイルの代わりに暗号化されたファイルに再同期するようにします。暗号キーは、次の URL オプションで Cisco IP Phone に通知されます。

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

ステップ 5　[すべての変更を送信（Submit All Changes）] をクリックします。

ステップ 6　Cisco IP Phone からの syslog トレースを確認します。

再同期時、Cisco IP Phone は新しいファイルをダウンロードし、これを使用して自身のパラメータを更新します。

関連項目

- AES の使用によるオープン プロファイルの暗号化（2-6 ページ）

分けられたプロファイル

Cisco IP Phone は再同期のたびに複数の個別のプロファイルをダウンロードします。この作業により、別々のサーバのさまざまなプロファイル情報を管理し、アカウント固有の値とは別の共通の設定パラメータ値をメンテナンスすることが可能になります。

演習

ステップ 1　これ以前の演習とは異なるパラメータに値を指定する、新しい XML プロファイル basic2.txt を作成します。たとえば、プロファイル basic.txt に次を追加します。

```
<GPP_B>ABCD</GPP_B>
```

ステップ 2　TFTP サーバの仮想ルート ディレクトリにプロファイル basic2.txt を保存します。

ステップ 3　フォルダにある、以前の演習で使用した 1 番目のプロファイル ルールはそのままにして、2 番目のプロファイル ルール（Profile_Rule_B）を設定し、新しいファイルを指すようにします。

```
<Profile_Rule_B ua="na">tftp://192.168.1.200/basic2.txt
</Profile_Rule_B>
```

ステップ 4　[すべての変更を送信（Submit All Changes）] をクリックします。

これで、Cisco IP Phone は、再同期操作の時刻になるたびに、1 番目と 2 番目の両方のプロファイルに再同期するようになりました。

ステップ 5　syslog トレースを参照し、期待した動作が行われていることを確認します。

CHAPTER 5

プロビジョニング パラメータ

この章では、設定プロファイルのスクリプトで使用できるプロビジョニング パラメータを説明します。

設定プロファイル パラメータ

次の表で、[プロビジョニング（Provisioning）] タブ下の [設定プロファイル パラメータ（Configuration Profile Parameters）] セクションの各パラメータの機能と使用方法を定義します。

パラメータ名	説明とデフォルト値
プロビジョン有効（Provision Enable）	ファームウェアのアップグレード操作に関係なく、すべての再同期操作を制御します。[はい（Yes）] に設定すると、リモート プロビジョニングが有効になります。 デフォルト値は [はい（Yes）] です。
リセット時の再同期（Resync On Reset）	パラメータの更新とファームウェアのアップグレードにより生じるリブートを除き、再同期がリブートの度に開始されます。 デフォルト値は [はい（Yes）] です。
再同期ランダム遅延（Resync Random Delay）	秒単位で指定される、リセットを実行する前のブートアップ シーケンスに続くランダム遅延。同時に電源がオンになるようにスケジュールされた IP テレフォニー デバイスのプールでは、これにより、各ユニットがプロビジョニング サーバに再同期要求を送信する時間が延びます。この機能は、地域の停電時に、大規模な宅内導入に役立つ可能性があります。
再同期の時間（Resync At）	デバイスがプロビジョニング サーバによって再同期する時間と分（HHmm）。 デフォルト値は空です。この値が無効な場合、パラメータは無視されます。このパラメータが有効な値に設定されると、[定期再同期（Resync Periodic）] パラメータが無視されます。

パラメータ名	説明とデフォルト値
再同期時刻ランダム遅延（Resync At Random Delay）	多数のデバイスの電源が同時にオンになったときに、プロビジョニング サーバの過負荷状態を回避できます。 複数の電話からサーバへの再同期要求のフラッディングを回避するため、電話は、時間と分の範囲と、時間と分およびランダム遅延（hhmm、hhmm+random_delay）を再同期します。たとえば、ランダム遅延 = （Resync At Random Delay + 30)/60 分とします。 秒単位の入力値は、最終的な random_delay の間隔を計算するため、繰り上げて分単位に丸められます。 この機能は、パラメータをゼロに設定すると無効になります。デフォルト値は 600 秒（10 分）です。パラメータ値が 600 未満に設定された場合は、デフォルト値が使用されます。
定期再同期（Resync Periodic）	プロビジョニング サーバによる定期的な再同期の時間間隔。関連する再同期タイマーは、サーバとの最初の同期が成功した後に初めてアクティブになります。 定期的な再同期を無効にするには、このパラメータをゼロに設定します。 デフォルト値は 3600 秒です。
再同期エラー再試行遅延（Resync Error Retry Delay）	IP テレフォニー デバイスがサーバからプロファイルを取得できなかったために再同期操作が失敗した場合、ダウンロードしたファイルが破損していた場合、または内部エラーが発生した場合は、指定された時間（秒単位）後に、デバイスが再度、再同期を試みます。 遅延が 0 に設定されている場合、再同期の試行が失敗した後、デバイスは再同期を試みません。
強制再同期遅延（Forced Resync Delay）	Cisco IP Phone が再同期を実行するまでの待機時間の最大遅延（秒単位）。 電話回線の 1 つがアクティブになっている間、デバイスは再同期しません。再同期は数秒かかる場合があるため、デバイスが長時間アイドルになるまで待機してから再同期することを推奨します。そうすることにより、ユーザは中断されずに通話を続けることができます。 デバイスは、すべての回線がアイドルになったときにカウントダウンを開始するタイマーを備えています。このパラメータは、カウンタの初期値です。再同期イベントは、このカウンタがゼロになるまで遅延します。 デフォルト値は 14,400 秒です。
SIP からの再同期（Resync From SIP）	再同期が有効にされ、SIP NOTIFY メッセージによってトリガーされます。 デフォルト値は [はい（Yes）] です。
再同期トリガー 1、再同期トリガー 2（Resync Trigger 1, Resync Trigger 2）	設定可能な再同期トリガー条件。再同期は、これらのパラメータ内の論理式が TRUE に評価されたときにトリガーされます。 デフォルト値は（空）です。

パラメータ名	説明とデフォルト値
FNF 時の再同期失敗（Resync Fails On FNF）	再同期は、要求されたプロファイルがサーバから受信されなかった場合に失敗と見なされます。この動作は、このパラメータによってオーバーライドできます。これが [いいえ（No）] に設定されると、デバイスは、サーバからの *file-not-found* 応答を正常な再同期として受け入れます。
プロファイル ルール（Profile Rule） プロファイル ルール B（Profile Rule B） プロファイル ルール C（Profile Rule C） プロファイル ルール D（Profile Rule D）	順に評価されるリモート設定プロファイル ルール。各再同期操作は、複数のサーバによって管理されている可能性のある複数のファイルを取得できます。
使用する再同期オプション（Resync Option To Use）	ファームウェアとプロファイルを取得するために使用されるカンマで区切られた再同期オプション。
ログ要求メッセージ（Log Request Msg）	このパラメータには、再同期の試みの開始時点で syslog サーバに送信されるメッセージが含まれます。 デフォルト値は $PN $MACです。再同期 の要求: $SCHEME://$SERVIP:$PORT$PATH。
ログ成功メッセージ（Log Success Msg）	再同期の試みの正常終了時点で発行される syslog メッセージ。 デフォルト値は $PN $MAC。再同期の成功: $SCHEME://$SERVIP:$PORT$PATH -- $ERR。
ログ失敗メッセージ（Log Failure Msg）	再同期の試行が失敗した後に発行される syslog メッセージ。 デフォルト値は $PN $MAC です。再同期の失敗:$ERR。
ユーザ設定可能再同期（User Configurable Resync）	ユーザが IP 電話画面から電話を再同期できるようにします。

ファームウェア アップグレード パラメータ

次の表で、[プロビジョニング（Provisioning）] タブの [ファーウェア アップグレード（Firmware Upgrade）] セクションの各パラメータの機能と使用方法を定義します。

パラメータ名	説明とデフォルト値
アップグレード有効（Upgrade Enable）	再同期アクションとは無関係に、ファームウェア アップグレードを有効にします。 デフォルト値は [はい（Yes）] です。
アップグレード エラー再試行遅延（Upgrade Error Retry Delay）	アップグレードの失敗時に適用されるアップグレード再試行の間隔（秒単位）。デバイスは、ファームウェア アップグレードの試行に失敗すると有効になるファームウェア アップグレード エラー タイマーを備えています。同タイマーは、このパラメータの値で初期化されます。このタイマーが 0 までカウントダウンすると、次のファームウェア アップグレードが試行されます。 デフォルト値は 3600 秒です。
アップグレード ルール（Upgrade Rule）	このパラメータは、プロファイル ルールと同じ構文をもつ、ファームウェア アップグレードのスクリプトです。アップグレードの条件と、関連するファームウェアの URL を定義します。 デフォルト値は（空）です。
エンタープライズ イメージ アップグレードの有効化（Enable Enterprise Image Upgrade）	3PCC ロードからエンタープライズ ロードまでのファームウェアのアップデートを可能にします。 デフォルト値は [いいえ（No）] です。

汎用パラメータ

次の表で、[プロビジョニング（Provisioning）] タブの [汎用パラメータ（General Purpose Parameters）] セクションの各パラメータの機能と使用方法を定義します。

パラメータ名	説明とデフォルト値
GPP_SA、GPP_SB、GPP_SC、GPP_SD	暗号キーとパスワードを保持するように設計された特殊な用途のプロビジョニング パラメータ。暗号化機能の整合性を確認するには、これらのパラメータを秘密にしておく必要があります。そのため、これらのパラメータは、デバイス設定の Web ページに表示されず、SIP NOTIFY コマンドに応じて送信される設定レポートに含まれていません。 デフォルト値は（空）です。
GPP_A から GPP_P	汎用プロビジョニング パラメータ。これらのパラメータは、プロビジョニングとアップグレードのルールで変数として使用できます。$GPP_A など、‘$’ の文字を含む変数名を付加することにより参照されます。 デフォルト値は（空）です。

マクロ展開変数

特定のマクロ変数は、次のプロビジョニング パラメータ内で認識されます。

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Upgrade_Rule
- Log_*
- GPP_*（特定の条件下で）

これらのパラメータの中で、$NAME または $(NAME) などの構文のタイプは、認識および展開されます。

マクロ変数の部分文字列は、表記 $(NAME:p) と $(NAME:p:q) で指定することができます（p と q は負ではない整数。バージョン 2.0.11 以降で使用可能）。結果として表示されるマクロ展開は、文字のオフセット p で開始される長さ q の部分文字列になります（q が指定されない場合には文字列の終端まで）。たとえば、GPP_A に ABCDEF が含まれている場合、$(A:2) は CDEF へと展開し、$(A:2:3) は CDE へと展開します。

認識されない名前は変換されず、$NAME または $(NAME) 形式は、展開後のパラメータ値において変更されません。

パラメータ名	説明とデフォルト値
$	$$ 形式は、単一の $ 文字に展開されます。
A から P	汎用パラメータ GPP_A から GPP_P の内容で置き換えられます。
MA	小文字の 16 進数、たとえば 000e08aabbcc を使用する MAC アドレス。
MAU	大文字の 16 進数、たとえば 000E08AABBCC を使用する MAC アドレス。
MAC	小文字の 16 進数と、00:0e:08:aa:bb:cc のように 16 進数の桁のペアを分割するコロンを使用する MAC アドレス。
PN	製品名。CP-7841-3PCC、など。
PSN	製品シリアル番号。V03 など。
SN	シリアル番号の文字列、88012BA01234 など。
CCERT	SSL クライアント証明書のステータス。インストール済みまたは未インストール。
IP	ローカル サブネット内での Cisco IP Phone の IP アドレス、192.168.1.100 など。
EXTIP	インターネットで表示される Cisco IP Phone の外部 IP、66.43.16.52 など。
SWVER	ソフトウェア バージョンの文字列。sip78xx.10-3-1-1-3PCC など。
HWVER	ハードウェア バージョンの文字列、2.0.1 など。
SCHEME	再同期またはアップグレード URL の解析後に取得される、TFTP、HTTP、HTTPS のうちいずれかのファイル アクセス スキーム。

パラメータ名	説明とデフォルト値
SERV	再同期またはアップグレード URL の解析後に取得される、要求ターゲット サーバのホスト名。
SERVIP	おそらく DNS ルックアップに続いて、再同期またはアップグレード URL の解析後に取得される、要求ターゲット サーバの IP アドレス。
PORT	再同期またはアップグレード URL の解析後に取得される、要求ターゲットの UDP/TCP ポート。
PATH	再同期またはアップグレード URL の解析後に取得される、要求ターゲットのファイル パス。
ERR	再同期またはアップグレード試行の結果メッセージ。結果 syslog メッセージの生成にのみ有効です。アップグレード試行の場合、値は UPGERR 変数で保持されます。
ISCUST	ユニットがカスタマイズされていれば、値 = 1 です。そうでない場合には 0 です。[WebUI 情報（WebUI Info）] ページでカスタマイズのステータスを確認できます。
SA から SD	セキュアなキー文字列にするため、パラメータ GPP_SA から GPP_SD の内容で置き換えられます。

内部エラー コード

Cisco IP Phone は、特定のエラー状態におけるユニットの動作をきめ細かく制御する際の設定を容易にするため、多数の内部エラー コード（X00-X99）を定義します。

パラメータ名	説明とデフォルト値
X00	SIP 要求を送信するときのトランスポート層（または ICMP）のエラー。
X20	応答待機中の SIP 要求のタイムアウト。
X40	一般的な SIP 制御エラー（たとえば、200 および ACK メッセージにおける SDP の受け入れられないコーデック、または ACK 待機中のタイムアウト）。
X60	指定されたダイヤル プランによれば無効なダイヤル済み番号。

サンプル設定ファイル

XML オープン形式のサンプル

```
<?xml version="1.0" encoding="UTF-8"?>
<device xsi:type="axl:XIPPhone" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <flat-profile>



  <!-- System Configuration -->

  <Restricted_Access_Domains ua="na"/>
  <Enable_Web_Server ua="na">Yes</Enable_Web_Server>
  <Web_Server_Port ua="na">80</Web_Server_Port>
  <Enable_Web_Admin_Access ua="na">Yes</Enable_Web_Admin_Access>
  <Admin_Password ua="na"/>
  <User_Password ua="rw"/>
  <Phone-UI-user-mode ua="na">No</Phone-UI-user-mode>


  <!-- Internet Connection Type  -->

  <Connection_Type ua="rw">DHCP</Connection_Type>


  <!--  Static IP Settings -->

  <Static_IP ua="rw"/>
  <NetMask ua="rw"/>
  <Gateway ua="rw"/>


  <!-- Optional Network Configuration -->

  <HostName ua="rw"/>
  <Domain ua="rw"/>
  <Primary_DNS ua="rw"/>
  <Secondary_DNS ua="rw"/>
  <Syslog_Server ua="na"/>
  <Debug_Level ua="na"/>0</Debug_Level>
  <Layer_2_Logging ua="na">No</Layer_2_Logging>
  <Primary_NTP_Server ua="na">us.pool.ntp.org</Primary_NTP_Server>
  <Secondary_NTP_Server ua="na"/>
  <SSH_Access ua="na">No</SSH_Access>
  <DNS_Cache_TTL_Ignore ua="na">Yes</DNS_Cache_TTL_Ignore>
  <SSH_User_ID ua="na"/>
```

```
<SSH_Password ua="na"/>


<!-- VLAN Settings -->

<Enable_CDP ua="na">Yes</Enable_CDP>
<Enable_LLDP-MED ua="na">Yes</Enable_LLDP-MED>
<Network_Startup_Delay ua="na">3</Network_Startup_Delay>
<VLAN_ID ua="rw">4095</VLAN_ID>


<!-- Inventory Settings -->

<Asset_ID ua="na"/>


<!--  SIP Parameters   -->

<Max_Forward ua="na">70</Max_Forward>
<Max_Redirection ua="na">5</Max_Redirection>
<SIP_User_Agent_Name ua="na">$VERSION</SIP_User_Agent_Name>
<SIP_Server_Name ua="na">$VERSION</SIP_Server_Name>
<SIP_Reg_User_Agent_Name ua="na" />
<SIP_Accept_Language ua="na" />
<RFC_2543_Call_Hold ua="na">No</RFC_2543_Call_Hold>
<SIP_TCP_Port_Min ua="na">5060</SIP_TCP_Port_Min>
<SIP_TCP_Port_Max ua="na">5080</SIP_TCP_Port_Max>
<Caller_ID_Header ua="na">PAID-RPID-FROM</Caller_ID_Header>
<Max_INVITE_Retry_Attempts ua="na">3</Max_INVITE_Retry_Attempts>
<Max_NON-INVITE_Retry_Attempts ua="na">3</Max_NON-INVITE_Retry_Attempts>

<!--  SIP Timer Values   -->

<SIP_T1 ua="na">0.5</SIP_T1>
<SIP_T2 ua="na">4</SIP_T2>
<INVITE_Expires ua="na">240</INVITE_Expires>
<ReINVITE_Expires ua="na">30</ReINVITE_Expires>
<Reg_Retry_Intvl ua="na">30</Reg_Retry_Intvl>
<Reg_Retry_Long_Intvl ua="na">1200</Reg_Retry_Long_Intvl>
<Reg_Retry_Random_Delay ua="na">0</Reg_Retry_Random_Delay>
<Reg_Retry_Long_Random_Delay ua="na">0</Reg_Retry_Long_Random_Delay>
<Reg_Retry_Intvl_Cap ua="na">0</Reg_Retry_Intvl_Cap>


<!--  Response Status Code Handling  -->

<Try_Backup_RSC ua="na">5??, 6??</Try_Backup_RSC>
<Retry_Reg_RSC ua="na">5??, 6??</Retry_Reg_RSC>


<!--  RTP Parameters   -->

<RTP_Port_Min ua="na">16384</RTP_Port_Min>
<RTP_Port_Max ua="na">16538</RTP_Port_Max>
<RTP_Packet_Size ua="na">0.02</RTP_Packet_Size>
<RTCP_Tx_Enable ua="na">No</RTCP_Tx_Enable>


<!--  SDP Payload Types   -->

<AVT_Dynamic_Payload ua="na">101</AVT_Dynamic_Payload>


<!--  NAT Support Parameters  -->
```

```
  <NAT_Keep_Alive_Intvl ua="na">15</NAT_Keep_Alive_Intvl>


<!--  Configuration Profile  -->

  <Provision_Enable ua="na">Yes</Provision_Enable>
  <Resync_On_Reset ua="na">Yes</Resync_On_Reset>
  <Resync_Random_Delay ua="na">2</Resync_Random_Delay>
  <Resync_At__HHmm_ ua="na">0100</Resync_At__HHmm_>
  <Resync_At_Random_Delay ua="na">600</Resync_At_Random_Delay>
  <Resync_Periodic ua="na">3600</Resync_Periodic>
  <Resync_Error_Retry_Delay ua="na">3600</Resync_Error_Retry_Delay>
  <Forced_Resync_Delay ua="na">14400</Forced_Resync_Delay>
  <Resync_Fails_On_FNF ua="na">Yes</Resync_Fails_On_FNF>
  <Profile_Rule ua="na">http://10.74.10.225/yxue2/ut/7841System_wSBC.xml</Profile_Rule>
  <Profile_Rule_B ua="na" />
  <Profile_Rule_C ua="na">/ut/Register2.xml</Profile_Rule_C>
  <Profile_Rule_D ua="na" />
  <Resync_DHCP_Option_To_Use ua="na">160,159,66,150</Resync_DHCP_Option_To_Use>
  <Log_Request_Msg ua="na">$PN $MAC -- Requesting %s
$SCHEME://$SERVIP:$PORT$PATH</Log_Request_Msg>
  <Log_Success_Msg ua="na">$PN $MAC -- Successful %s $SCHEME://$SERVIP:$PORT$PATH --
$ERR</Log_Success_Msg>
  <Log_Failure_Msg ua="na">$PN $MAC -- %s failed: $ERR</Log_Failure_Msg>
  <User_Configurable_Resync ua="na">Yes</User_Configurable_Resync>
  <!--  Firmware Upgrade   -->

  <Upgrade_Enable ua="na">Yes</Upgrade_Enable>
  <Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
  <Upgrade_Rule ua="na" />
  <Enable_Enterprise_Image_Upgrade ua="na">No</Enable_Enterprise_Image_Upgrade>


  <!--  CA Settings   -->

  <Custom_CA_Rule ua="na" />


  <!--  General Purpose Parameters  -->
  <GPP_A ua="na" />
  <GPP_B ua="na" />
  <GPP_C ua="na" />
  <GPP_D ua="na" />
  <GPP_E ua="na" />
  <GPP_F ua="na" />
  <GPP_G ua="na" />
  <GPP_H ua="na" />
  <GPP_I ua="na" />
  <GPP_J ua="na" />
  <GPP_K ua="na" />
  <GPP_L ua="na" />
  <GPP_M ua="na" />
  <GPP_N ua="na" />
  <GPP_O ua="na" />
  <GPP_P ua="na" />


  <!--  Control Timer Values (sec)  -->

  <Interdigit_Long_Timer ua="na">10</Interdigit_Long_Timer>
  <Interdigit_Short_Timer ua="na">3</Interdigit_Short_Timer>
```

```
  <!--  Time  -->

  <Time_Zone ua="na">GMT-8:00</Time_Zone>
  <Time_Offset__HH_mm_ ua="na">00/00</Time_Offset__HH_mm_>
  <Ignore_DHCP_Time_Offset ua="na">No</Ignore_DHCP_Time_Offset>
  <Daylight_Saving_Time_Rule
ua="na">start=3/-1/7/2;end=10/-1/7/2;save=1</Daylight_Saving_Time_Rule>
  <Daylight_Saving_Time_Enable ua="na">Yes</Daylight_Saving_Time_Enable>


  <!--  Localization  -->

  <Dictionary_Server_Script ua="na" />
  <Language_Selection ua="na" />
  <Locale ua="na">en-US</Locale>

- <!--  QoS Settings  -->

  <SIP_TOS_Value ua="na">0x60</SIP_TOS_Value>
  <RTP_TOS_Value ua="na">0xb8</RTP_TOS_Value>


  <!--  General  -->

  <Station_Display_Name ua="na" />
  <Text_Logo ua="na" />
  <PNG_Picture_Download_URL ua="na" />
  <Select_Logo ua="na">Default</Select_Logo>
  <Select_Background_Picture ua="na">None</Select_Background_Picture>
  <Screen_Saver_Enable ua="rw">No</Screen_Saver_Enable>
  <Screen_Saver_Wait ua="rw">300</Screen_Saver_Wait>
  <Screen_Saver_Icon ua="rw">Background Picture</Screen_Saver_Icon>
  <Co-branding_Banner_Picture_Download_URL ua="na" />


  <!--  Miscellaneous Line Key Settings  -->

  <Call_Appearances_Per_Line ua="na">2</Call_Appearances_Per_Line>


  <!--  Supplementary Services  -->

  <Conference_Serv ua="na">Yes</Conference_Serv>
  <Attn_Transfer_Serv ua="na">Yes</Attn_Transfer_Serv>
  <Blind_Transfer_Serv ua="na">Yes</Blind_Transfer_Serv>
  <Cfwd_All_Serv ua="na">Yes</Cfwd_All_Serv>
  <Cfwd_Busy_Serv ua="na">Yes</Cfwd_Busy_Serv>
  <Cfwd_No_Ans_Serv ua="na">Yes</Cfwd_No_Ans_Serv>


  <!--  BroadSoft Settings  -->

  <Directory_Enable ua="na">Yes</Directory_Enable>
  <XSI_Host_Server ua="na">xsi.iop1.broadworks.net</XSI_Host_Server>
  <Directory_Name ua="na">IOP1</Directory_Name>
  <Directory_Type ua="na">Enterprise</Directory_Type>
  <Directory_User_ID ua="na">broadsoft_user</Directory_User_ID>
  <Directory_Password ua="na" />


<!--  LDAP Corporate Directory Search  -->

  <LDAP_Dir_Enable ua="na">No</LDAP_Dir_Enable>
  <LDAP_Corp_Dir_Name ua="na" />
```

```
<LDAP_Server ua="na" />
<LDAP_Auth_Method ua="na">None</LDAP_Auth_Method>
<LDAP_Client_DN ua="na" />
<LDAP_Username ua="na" />
<LDAP_Password ua="na" />
<LDAP_Search_Base ua="na" />
<LDAP_Last_Name_Filter ua="na" />
<LDAP_First_Name_Filter ua="na" />
<LDAP_Search_Item_3 ua="na" />
<LDAP_Item_3_Filter ua="na" />
<LDAP_Search_Item_4 ua="na" />
<LDAP_Item_4_Filter ua="na" />
<LDAP_Display_Attrs ua="na" />
<LDAP_Number_Mapping ua="na" />


<!--  XML Service  -->

<XML_Directory_Service_Name ua="na" />
<XML_Directory_Service_URL ua="na" />
<XML_Application_Service_Name ua="na" />
<XML_Application_Service_URL ua="na" />
<XML_User_Name ua="na" />
<XML_Password ua="na" />


<!--  Call Forward  -->

<Cfwd_All_Dest ua="rw" />
<Cfwd_Busy_Dest ua="rw" />
<Cfwd_No_Ans_Dest ua="rw" />
<Cfwd_No_Ans_Delay ua="rw">20</Cfwd_No_Ans_Delay>


<!--  Speed Dial  -->

<Speed_Dial_2 ua="na" />
<Speed_Dial_3 ua="na" />
<Speed_Dial_4 ua="na" />
<Speed_Dial_5 ua="na" />
<Speed_Dial_6 ua="na" />
<Speed_Dial_7 ua="na" />
<Speed_Dial_8 ua="na" />
<Speed_Dial_9 ua="na" />


<!--  Supplementary Services  -->

<Time_Format ua="rw">12hr</Time_Format>
<Date_Format ua="rw">month/day</Date_Format>


<!--  Audio  -->

<Ringer_Volume ua="rw">8</Ringer_Volume>
<Speaker_Volume ua="rw">8</Speaker_Volume>


<!--  LCD  -->

<LCD_Contrast ua="rw">16</LCD_Contrast>
<Back_Light_Timer ua="na">10s</Back_Light_Timer>
<!--  General  -->
```

```
<Line_Enable_1_ ua="na">Yes</Line_Enable_1_>


<!--  NAT Settings  -->

<NAT_Keep_Alive_Enable_1_ ua="na">No</NAT_Keep_Alive_Enable_1_>
<NAT_Keep_Alive_Msg_1_ ua="na">$NOTIFY</NAT_Keep_Alive_Msg_1_>


<!--  SIP Settings  -->

<SIP_Transport_1_ ua="na">UDP</SIP_Transport_1_>
<SIP_Port_1_ ua="na">5060</SIP_Port_1_>
<SIP_100REL_Enable_1_ ua="na">Yes</SIP_100REL_Enable_1_>
<Auth_Resync-Reboot_1_ ua="na">Yes</Auth_Resync-Reboot_1_>
<SIP_Remote-Party-ID_1_ ua="na">Yes</SIP_Remote-Party-ID_1_>
<Refer-To_Target_Contact_1_ ua="na">No</Refer-To_Target_Contact_1_>
<SIP_Debug_Option_1_ ua="na">None</SIP_Debug_Option_1_>
<Sticky_183_1_ ua="na">No</Sticky_183_1_>
<Auth_INVITE_1_ ua="na">No</Auth_INVITE_1_>
<User_Equal_Phone_1_ ua="na">No</User_Equal_Phone_1_>


<!--  Call Feature Settings  -->

<Default_Ring_1_ ua="rw">1</Default_Ring_1_>
<Conference_Bridge_URL_1_ ua="na" />


<!--  Proxy and Registration  -->
<Proxy_1_ ua="na" />
<Outbound_Proxy_1_ ua="na">199.19.193.9</Outbound_Proxy_1_>
<Alternate_Proxy_1_ ua="na" />
<Alternate_Outbound_Proxy_1_ ua="na" />
<Register_1_ ua="na">Yes</Register_1_>
<Make_Call_Without_Reg_1_ ua="na">No</Make_Call_Without_Reg_1_>
<Register_Expires_1_ ua="na">3600</Register_Expires_1_>
<Use_DNS_SRV_1_ ua="na">Yes</Use_DNS_SRV_1_>
<Proxy_Fallback_Intvl_1_ ua="na">3600</Proxy_Fallback_Intvl_1_>
<Dual_Registration_1_ ua="na">No</Dual_Registration_1_>


<!--  Subscriber Information  -->

<Display_Name_1_ ua="na" />
<User_ID_1_ ua="na" />
<Password_1_ ua="na" />
<Auth_ID_1_ ua="na" />
<Reversed_Auth_Realm_1_ ua="na" />


<!--  Audio Configuration  -->

<Preferred_Codec_1_ ua="na">G722</Preferred_Codec_1_>
<Use_Pref_Codec_Only_1_ ua="na">No</Use_Pref_Codec_Only_1_>
<Second_Preferred_Codec_1_ ua="na">Unspecified</Second_Preferred_Codec_1_>
<Third_Preferred_Codec_1_ ua="na">Unspecified</Third_Preferred_Codec_1_>
<G711u_Enable_1_ ua="na">Yes</G711u_Enable_1_>
<G711a_Enable_1_ ua="na">Yes</G711a_Enable_1_>
<G729a_Enable_1_ ua="na">Yes</G729a_Enable_1_>
<G729ab_Enable_1_ ua="na">Yes</G729ab_Enable_1_>
<G722_Enable_1_ ua="na">Yes</G722_Enable_1_>
<iLBC_Enable_1_ ua="na">Yes</iLBC_Enable_1_>
<Silence_Supp_Enable_1_ ua="na">No</Silence_Supp_Enable_1_>
```

```
  <DTMF_Tx_Method_1_ ua="na">Auto</DTMF_Tx_Method_1_>


  <!--  Dial Plan  -->
  <Dial_Plan_1_ ua="na">( <8:>x.| [*#]xx[*x] | [*#]xx.| [2-9]11S0 | 00 | 011x.|
[0-1][2-9]xxxxxxxxx | 0 | [2-9]xxxxxxxxx | xxxx )</Dial_Plan_1_>

  </flat-profile>
  </device>
```

略語

A/D	アナログ/デジタル コンバータ
ANC	非通知着信
B2BUA	連続ユーザ エージェント
Bool	ブール値。プロファイルで、[はい（yes）] と [いいえ（no）]、または [1] と [0] として指定されます。
CA	Certificate Authority
CAS	CPE アラート シグナル
CDR	詳しい通話記録（Call Detail Record）
CID	発信者 ID
CIDCW	コール ウェイティング発信者 ID
CNG	Comfort Noise Generation（コンフォート ノイズ生成）
CPC	発信側の制御
CPE	顧客宅内機器
CWCID	コール ウェイティング発信者 ID
CWT	コール ウェイティング トーン
D/A	アナログ/デジタル コンバータ
dB	デシベル
dBm	1 ミリワット当たり dB
DHCP	ダイナミック ホスト コンフィギュレーション プロトコル
DNS	ドメイン ネーム システム
DRAM	ダイナミック ランダム アクセス メモリ
DSL	デジタル サブスクライバ ループ
DSP	デジタル シグナル プロセッサ
DTAS	データ端末アラート シグナル（CAS と同じ）
DTMF	デュアル トーン多重周波数
FQDN	Fully Qualified Domain Name（完全修飾ドメイン名）
FSK	周波数偏移変調

FXS	Foreign eXchange Station
GW	ゲートウェイ
ITU	国際電気通信連合
HTML	ハイパーテキスト マークアップ言語
HTTP	ハイパーテキスト転送プロトコル
HTTPS	HTTP over SSL
ICMP	Internet Control Message Protocol; インターネット制御メッセージ プロトコル
IGMP	Internet Group Management Protocol; インターネット グループ管理プロトコル
ILEC	Incumbent Local Exchange Carrier
IP	インターネット プロトコル
ISP	インターネット サービス プロバイダー
ITSP	インターネット テレフォニー サービス プロバイダー
IVR	自動音声応答装置
LAN	ローカル エリア ネットワーク
LBR	低ビットレート
LBRC	低ビットレート コーデック
MC	Mini 証明書
MGCP	Media Gateway Control Protocol
MOH	Music On Hold（保留音）
MOS	平均オピニオン評点（1-5、数字が大きいほど評価が高くなる）
ms	Millisecond; ミリ秒
MSA	音源アダプタ
MWI	メッセージ待機インジケータ
OSI	オープン スイッチング間隔
PCB	プリント回路基板
PR	極性反転
PS	Provisioning Server
PSQM	知覚通話品質測定（1-5、数字が小さいほど評価が高くなる）
PSTN	Public Switched Telephone Network
NAT	ネットワーク アドレス変換
OOB	アウトオブバンド
REQT	（SIP）要求メッセージ
RESP	（SIP）応答メッセージ
RSC	（SIP）応答ステータス コード、404、302、600 など
RTP	Real Time Protocol
RTT	ラウンドトリップ時間
SAS	ストリーミング オーディオ サーバ

SDP	Session Description Protocol
SDRAM	同期 DRAM
sec	秒
SIP	Session Initiation Protocol
SLA	共有ライン アピアランス
SLIC	加入者線インターフェイス回線
SP	サービス プロバイダー
SSL	Secure Socket Layer
TFTP	トリビアル ファイル転送プロトコル
TCP	伝送制御プロトコル
UA	ユーザ エージェント（User Agent）
uC	マイクロ コントローラ
UDP	ユーザ データグラム プロトコル
URL	Uniform Resource Locator
VM	[ボイスメール（Voicemail）]
VMWI	ビジュアル メッセージ待機表示/インジケータ
VQ	音声品質
WAN	ワイド エリア ネットワーク
XML	拡張マークアップ言語

関連資料

Cisco では、ユーザおよびユーザのお客様が Cisco IP Phone のメリットを十分に得られるように広範囲のリソースを提供しています。

次の項を使用して、関連情報を取得してください。

Cisco IP Phone 7800 シリーズのマニュアル

お使いの言語、電話機モデル、および Cisco Unified Communications Manager リリースに特化した文書を参照してください。次のドキュメント URL から参照してください。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/tsd-products-support-series-home.html

Cisco IP Phone 8800 シリーズのマニュアル

お使いの言語、電話機モデル、および Cisco Unified Communications Manager リリースに特化した文書を参照してください。次のドキュメント URL から参照してください。

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-series-home.html

Cisco IP Phone ファームウェアのサポート ポリシー

Cisco IP Phone のサポート ポリシーの詳細については、次の URL を参照してください。
http://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-ip-phone-7900-series/116684-technote-ipphone-00.html

マニュアル、テクニカル サポート、その他の有用な情報

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。