Cisco Broadband Access Center for Cable アドミニストレータ ガイド

Release 3.0

Text Part Number: OL-8640-01-J

Cisco Broadband Access Center for Cable アドミニストレータ ガイド

CONTENTS

このマニュアルについて

『*Cisco Broadband Access Center for Cable アドミニストレータ ガイド*』をご利用いただきありがとうございます。このマニュアルでは、Cisco Broadband Access Center（以下 BAC と表記）に関する概念と構成について説明します。

ここでは、このマニュアルの後続の章について概要を示し、この BAC リリースをサポートする関連資料の詳細情報を提供します。また、このマニュアルで使用されているスタイルと表記法についても説明します。

（注） このマニュアルは、P.xvi の「製品マニュアル」に挙げられているマニュアルと併せてご利用ください。

ここでは、次の内容について説明します。

対象読者

『*Cisco Broadband Access Center for Cable アドミニストレータ ガイド*』は、ブロードバンド アクセスにおいて大規模なプロビジョニングを自動化するシステム管理者を対象としています。ネットワーク管理者は、次の項目について熟知している必要があります。

- 基本的なネットワークの概念および専門用語
- ネットワーク管理

マニュアルの構成

このマニュアルでは、BAC の管理方法と保守方法について説明します。

章	タイトル	説明
第 1 章	Broadband Access Center の概要	BAC の機能と特長について説明します。
第 2 章	Broadband Access Center のアーキテクチャ	この BAC リリースに実装されているシステム アーキテクチャについて説明します。
第 3 章	設定のワークフローとチェックリスト	BAC を設定する際のチェックリストを提供します。
第 4 章	CPE 管理の概要	CPE 管理の概要を示し、BAC 内でサポートされている重要な概念について説明します。
第 5 章	設定テンプレートの管理	BAC がサポートしている設定テンプレートについて説明します。また、カスタム 設定テンプレートを作成する方法についても説明します。
第 6 章	ファームウェア管理	BAC がサポートしているファームウェア管理機能について説明します。
第 7 章	パラメータ辞書	パラメータ辞書の使用について説明します。
第 8 章	CPE の履歴とトラブルシューティング	BAC を介して入手できるデバイス情報を使用して CPE をトラブルシューティングする方法について説明します。
第 9 章	Broadband Access Center の管理	BAC の管理に役立つ各種オプションについて説明します。
第 10 章	データベースの管理	RDU データベースを管理および保守する方法について説明します。
第 11 章	Broadband Access Center の監視	BAC サーバを監視する方法について説明します。
第 12 章	CWMP サービスの設定	BAC とともに使用できるように CWMP を設定する方法について説明します。
第 13 章	CWMP サービス セキュリティの設定	BAC を使用してセキュリティ オプションを強化する方法について説明します。
第 14 章	CWMP デバイス操作	BAC を使用してデバイス上で実行できる操作について説明します。
第 15 章	管理者のユーザ インターフェイスについて	管理者のユーザ インターフェイスを使用して BAC にアクセスする方法について説明します。
第 16 章	管理者のユーザ インターフェイスの使用方法	デバイス情報の検索、表示などの管理アクティビティについて説明します。

章	タイトル	説明
第 17 章	Broadband Access Center の設定	BAC 管理アプリケーションを使用して実行される設定アクティビティについて説明します。
第 18 章	BAC がサポートするツールと高度な概念	BAC の設定、保守、インストールの効率化、配備、使用に役立つ BAC ツールについて説明します。
第 19 章	Broadband Access Center のトラブルシューティング	BAC サーバをトラブルシューティングする方法について説明します。
	Glossary	このマニュアルで使用されている用語と、説明されている技術に一般的に使用される用語を定義します。

表記法

このマニュアルは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード	太字
ユーザが値を指定する変数	イタリック体
セッション情報およびシステム情報の表示出力	`screen` フォント
ユーザが入力する情報	太字の **`screen`** フォント
ユーザが入力する変数	イタリック体の *`screen`* フォント
メニュー項目およびボタン名	太字
本文中のメニュー項目の選択	**Option > Network Preferences**
表中のメニュー項目の選択	Option > Network Preferences

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

製品マニュアル

（注） 初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、Cisco.com で確認してください。

表 1 に、ご利用可能な製品マニュアルを示します。

表 1　製品マニュアル

マニュアル タイトル	ご利用形式
Release Notes for Cisco Broadband Access Center, Release 3.0	• 製品に付属している印刷マニュアル • 製品 CD に収録されている PDF • Cisco.com（次の URL を参照） http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_release_notes_list.html
Installation Guide for Cisco Broadband Access Center,Release 3.0	• 製品に付属している印刷マニュアル • 製品 CD に収録されている PDF • Cisco.com（次の URL を参照） http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_installation_guides_list.html
Cisco Broadband Access Center Administrator's Guide, Release 3.0	• 製品 CD に収録されている PDF • Cisco.com（次の URL を参照） http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_maintenance_guides_list.html
Cisco Broadband Access Center DPE CLI Reference, Release 3.0	• 製品 CD に収録されている PDF • Cisco.com（次の URL を参照） http://cisco.com/en/US/products/sw/netmgtsw/ps529/prod_command_reference_list.html

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。ここでは、シスコが提供する製品マニュアル リソースについて説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納したライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関するマニュアルにアクセスすることができます。また、この DVD を使用すると、次の URL のシスコの Web サイトに掲載されている HTML マニュアルおよび PDF ファイルにアクセスすることができます。

http://www.cisco.com/univercd/home/home.htm

Product Documentation DVD は、毎月作成され、月の半ばにリリースされます。DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store から Product Documentation DVD（Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

マニュアルの発注方法（英語版）

Cisco Marketplace にアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザの場合、Product Documentation Store からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードに登録してください。PSIRT RSS フィードへの登録方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または GnuPG などの互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 9.*x* を使用して暗号化された情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に PSIRT に問い合せ、他のデータ暗号化方法を確認してください。

Product Alerts および Field Notices

シスコ製品に対する変更やアップデートは、Cisco Product Alerts および Cisco Field Notices で発表されます。Cisco.com のプロダクト アラート ツールを使用すると、Cisco Product Alerts および Cisco Field Notices を受け取ることができます。このツールを使用すれば、プロファイルを作成して、情報を受け取る製品を選択できます。

プロダクト アラート ツールにアクセスするには、Cisco.com の登録ユーザとなる必要があります（Cisco.com にユーザ登録するには、http://tools.cisco.com/RPF/register/register.do にアクセスします）。登録ユーザは、http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en でこのツールを使用できます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注）オンラインまたは電話でサービス リクエストを発行する前に、**Cisco Product Identification Tool** を使用して製品のシリアル番号を確認してください。Cisco Technical Support & Documentation Web サイトでこのツールを使用するには、**Tools & Resources** リンクをクリックし、**All Tools (A-Z)** タブをクリックした後、アルファベット順のリストから **Cisco Product Identification Tool** を選択します。このツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

ヒント Cisco.com での表示および検索

ブラウザが Web ページをリフレッシュしていないと思われる場合は、Ctrl キーを押したまま F5 を押すことで強制的にブラウザに Web ページを更新させます。

技術情報を検索する場合は、Cisco.com の Web サイト全体ではなく、技術マニュアルに検索対象を絞り込みます。Cisco.com のホームページで、Search ボックスの下にある **Advanced Search** リンクをクリックし、**Technical Support & Documentation** オプション ボタンをクリックしてください。

Cisco.com の Web サイトまたは特定の技術マニュアルに関するフィードバックを送るには、Cisco.com のすべての Web ページの下部にある **Contacts & Feedback** をクリックします。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：既存のネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- 『*Cisco Product Quick Reference Guide*』は手軽でコンパクトな参照ツールです。チャネル パートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコ製品の最新情報が収録されます。『*Cisco Product Quick Reference Guide*』の注文方法および詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコのネットワーキング担当者向けの雑誌です。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンライン サービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

Broadband Access Center の概要

Cisco Broadband Access Center（BAC）は、ブロードバンド サービス プロバイダーのネットワークに存在する Customer Premises Equipment（CPE; 顧客宅内装置）をプロビジョニングおよび管理する作業を自動化します。

BAC は高性能の機能を備えているため、何百万もの CPE が存在するネットワークなど、実質的にどのような規模のネットワークにも適合するように BAC を拡大、縮小できます。また、BAC は分散アーキテクチャと集中管理を備えているため、ハイ アベイラビリティを実現できます。

このリリースでは、CPE のプロビジョニングおよび管理をサポートする際に、DSL Forum の CPE WAN Management Protocol（CWMP）を使用します。CWMP は、TR-069 仕様で定義された標準です。BAC には TR-069 で定義された機能が統合されているため、オペレータの効率が向上し、ネットワーク管理の問題が軽減されます。

BAC は、TR-069、TR-098、TR-104、および TR-106 標準に基づいて、デバイスをサポートします。サポートされるデバイスには、イーサネットおよび ADSL ゲートウェイ デバイス、無線ゲートウェイ、VoIP ATA などの CWMP 準拠のデバイスがあります。また、このリリースには、近く公開されるデータ モデル標準やベンダー固有のデータ モデルすべてを CWMP に基づいてサポートする、実行時に拡張可能なデータ モデルが搭載されています。

BAC には、冗長性やフェールオーバーなどの重要な機能があります。BAC の動作方法を制御できるプロビジョニング アプリケーション プログラミング インターフェイス（API）を利用することにより、新しい環境または既存の環境に BAC を統合することができます。プロビジョニング API を使用すると、BAC でデバイスを登録すること、デバイス構成ポリシーを割り当てること、CPE に対して任意の CWMP 操作を実行すること、および BAC プロビジョニング システム全体を構成することができます。

機能と利点

BAC を使用すると、急増しているホーム ネットワーキング デバイスを、サービス プロバイダーがより簡単にプロビジョニングおよび管理できるようになります。

この項では、BAC アーキテクチャがもたらす基本的な機能と利点について説明します。

- 構成管理：BAC では設定テンプレートを使用することで、作業が大幅に簡素化されます。この設定テンプレートには、CPE への構成の割り当てを簡単かつ柔軟に実行できるメカニズムがあります。このテンプレート処理メカニズムを使用すると、少数のテンプレートで、何百万というデバイスの構成をカスタマイズできます。

  このような XML ベースのテンプレートを使用すると、デバイスに対して、構成パラメータおよび値のほか、通知およびアクセス コントロールを設定できます。設定テンプレートでは、次の機能を使用できます。

  - 条件。BAC プロパティ値に基づいて、テンプレートのセクションを含めるか、または除外することができます。
  - インクルード。他のファイルからテンプレートの内容を含めることができます。
  - パラメータ代入。BAC プロパティ値をテンプレートのパラメータに代入できます。
  - 前提条件。テンプレートが所定の時間にデバイスに適用可能かどうかを評価できます。

- ファームウェア管理：一連のファームウェア イメージ ファイルの保守、および BAC システムから対応する CPE への配送を行います。ファームウェア ルール テンプレートにより、ファームウェア イメージ ファイルは、デバイス グループに関連付けられます。BAC は、関連付けられたファームウェア ルール テンプレート内のルールを使用して、デバイスにダウンロードするファームウェアを評価します。

  ファームウェア管理機能を使用すると、デバイスのファームウェア情報を表示すること、ファームウェア イメージをデータベースに追加すること、およびイメージ ファイルを特定の CPE に適用することができます。

- 広範なスケーラビリティ：スケーラビリティを拡張する手段として、CPE をパーティション化してプロビジョニング グループにします。各プロビジョニング グループは、CPE のサブセットだけに関連付けられます。プロビジョニング グループは、通常 1 つ以上の Device Provisioning Engine（DPE）で構成されるサーバを、論理的に（通常は地理的に）グループ化したものになるように設計されています。1 つのプロビジョニング グループで、最大 50 万個のデバイスのプロビジョニング ニーズに対処できます。デバイスの数が 50 万個を上回る場合は、追加のプロビジョニング グループを配置に加えることができます。

- 標準ベースのセキュリティ：TR-069 標準で定義された CWMP を使用して、高度のセキュリティを実現するように設計されています。また、CWMP セキュリティ モデルは、スケーラブルになるようにも設計されています。そのため、堅牢な CPE 実装が要求されない場合は基本的なセキュリティを実現し、より高度のセキュリティ メカニズムをサポートする場合はより高度のセキュリティを実現することができます。

  BAC では、Secure Sockets Layer（SSL）バージョン 3.0 プロトコルと Transport Layer Security（TLS）バージョン 1.0 プロトコルを TCP ベースのメッセージ システムに統合することで、オプションのセキュア通信を実現しています。HTTP over SSL/TLS（HTTPS とも呼ばれる）を使用すると、機密保持とデータ整合性が確保されるため、さまざまなコンポーネント間で証明書ベースの認証を行うことができます。

- バックエンド システムとの容易な統合。この統合には、次のような BAC メカニズムが使用されます。

  - BAC Java API。すべてのプロビジョニング操作および管理操作を実行するときに使用できます。
  - BAC パブリッシング拡張。RDU データを別のデータベースに書き込むときに便利です。
  - BAC Data Export ツール。BAC システムからファイルにデバイス情報を書き込むことができます。
  - SNMP エージェント。BAC のモニタリングに関する統合を簡素化します。

  - DPE コマンドライン インターフェイス。コマンドをコピー アンド ペーストするときに使用するローカル構成を簡素化します。
- 広範なサーバ管理：BAC では広範なサーバ パフォーマンス統計情報を表示できるため、モニタリングやトラブルシューティングが可能になります。
- デバイス診断およびトラブルシューティング：この機能を使用すると、1 つのデバイスに焦点を当てて診断情報を収集し、詳細に分析することができます。BAC には、診断を支援する次の機能があります。
  - デバイス履歴：デバイス プロビジョニングのライフサイクルで発生する重要なイベントの詳細な履歴を表示できます。
  - デバイス障害：障害が繰り返し発生するデバイスを検出します。このような障害は、ボトルネックとなってネットワーク パフォーマンスに影響を及ぼす場合があります。
  - デバイスのトラブルシューティング：トラブルシューティング対象に指定された一連のデバイスに関する、デバイスと BAC サーバとのインタラクションの詳細なレコードを表示できます。
  - 直接的なデバイス操作：IP Ping や Get Live Data などの操作をデバイスに実行して、より詳細に調べることができます。

サポート対象の技術

この BAC リリースでサポートされる CPE のプロビジョニングおよび管理では、TR-069 標準で定義された CWMP だけが使用されます。ただし、TR-069、TR-098、TR-104、および TR-106 拡張に基づくデータ モデルは、実質的にすべてサポートされます。

CWMP 技術

TR-069 は、CPE のリモート管理に関する標準です。この標準では CWMP が定義されています。CWMP を使用すると、CPE と Autoconfiguration Server（ACS; 自動構成サーバ）間の通信が可能になります。

CWMP には、その主要機能を使用してオペレータの効率を向上させ、ネットワーク管理の問題を軽減するメカニズムが詳細に規定されています。この主要機能には次のものがあります。

- 自動構成
- ファームウェア管理
- ステータスおよびパフォーマンスのモニタリング
- デバイス診断およびトラブルシューティング

CWMP に加え、TR-069 仕様では、Internet Gateway Device（IGD; インターネット ゲートウェイ デバイス）のバージョン 1.0 のデータ モデルも定義されています。IGD は TR-098 から拡張されたものです。TR-069 で定義された CWMP は、CWMP から拡張されたデータ モデルすべてと連動します。このようなデータ モデルには、TR-098、TR-104、および TR-106 で定義されたモデル、近く公開される新しいモデル、またはベンダー固有のモデルなどがあります。

Broadband Access Center のアーキテクチャ

この章では、この Broadband Access Center（BAC）リリースに実装されているシステム アーキテクチャについて説明します。

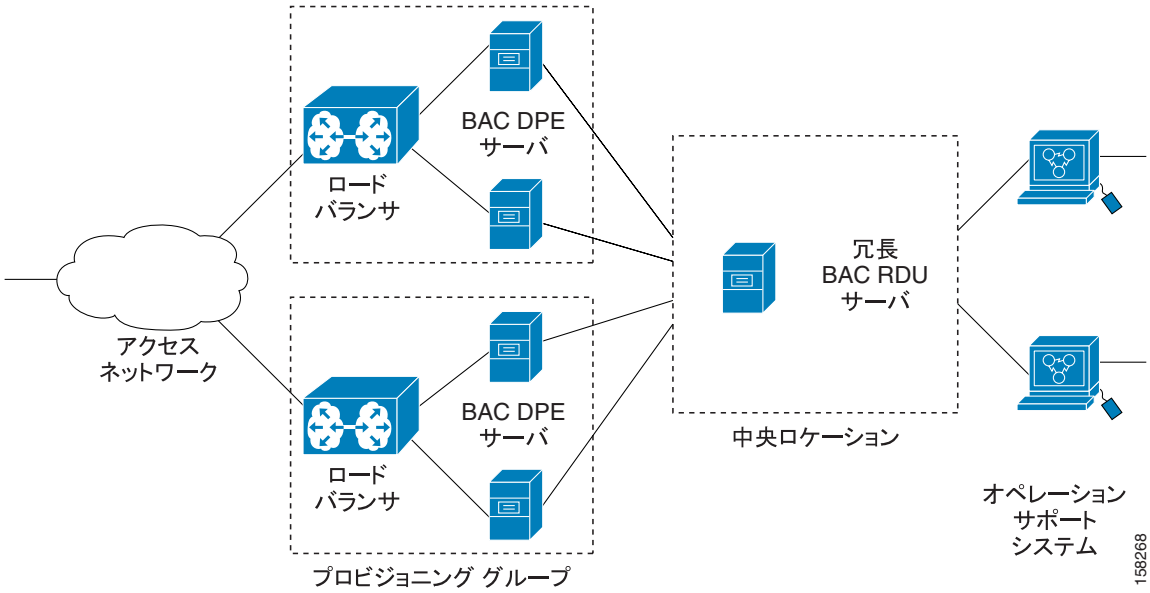
この章は、次の項で構成されています。

BAC の配備

BAC は、TR-069、TR-098、TR-104、および TR-106 標準に基づいて、デバイスをプロビジョニングします。サポートされるデバイスには、イーサネットおよび ADSL ゲートウェイ デバイス、無線ゲートウェイ、VoIP ATA などの CPE WAN Management Protocol（CWMP）準拠のデバイスがあります。

図 2-1 は、BAC ネットワークにおける一般的な完全冗長の CWMP 配備を示しています。

図 2-1　BAC における CWMP 配備



アーキテクチャ

ここでは、次に示すコンポーネントから成る BAC の基本アーキテクチャについて説明します。

- Regional Distribution Unit（RDU）。次の機能を提供します。
  - BAC システムの権限あるデータ格納
  - アプリケーション　プログラミング　インターフェイス（API）の要求を処理するためのサポート
  - システム全体のステータスおよび状態のモニタリング

  詳細については、P.2-4 の「Regional Distribution Unit」を参照してください。
- Device Provisioning Engine（DPE）。次の機能を提供します。
  - 顧客宅内装置（CPE）とのインターフェイス
  - 構成およびファームウェア ポリシーの命令キャッシュ
  - RDU および他の DPE から独立した操作
  - CPE WAN Management Protocol（CWMP）サービス
  - 構成用の IOS ライクなコマンドライン インターフェイス（CLI）
  - Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）ファイル サービス

  詳細については、P.2-4 の「Device Provisioning Engine」を参照してください。
- クライアントからシステムの機能をすべて制御できるようにするクライアント API。
- プロビジョニング グループ。次の機能を提供します。
  - 冗長クラスタ内の DPE サーバの論理的なグループ化
  - 冗長性とスケーラビリティ

  詳細については、P.2-6 の「プロビジョニング グループ」を参照してください。
- BAC プロセス ウォッチドッグ。次の機能を提供します。
  - すべての重要な BAC プロセスに対する管理モニタリング
  - プロセス自動再開機能
  - BAC コンポーネント プロセスを開始および中止する機能

  詳細については、P.2-8 の「BAC プロセス ウォッチドッグ」を参照してください。
- 管理者のユーザ インターフェイス。次の機能を提供します。
  - CWMP デバイスの追加、削除、および変更のほか、デバイスの検索、デバイスの詳細の取得、およびデバイス操作の実行に対するサポート
  - グローバル デフォルトの構成およびカスタム プロパティの定義に対するサポート
  - 追加のパフォーマンス統計情報を表示する機能
  - ファームウェア ルールおよび設定テンプレートの管理

  詳細については、P.9-3 の「管理者のユーザ インターフェイス」を参照してください。
- SNMP エージェント。次の事項をサポートします。
  - サードパーティの管理システム
  - SNMP バージョン v2
  - SNMP 通知

  詳細については、P.2-8 の「SNMP エージェント」を参照してください。

Regional Distribution Unit

Regional Distribution Unit（RDU）は、BAC プロビジョニング システムのプライマリ サーバです。RDU は Solaris 9 オペレーティング システムを実行しているサーバにインストールされます。

RDU には次の機能があります。

- デバイスからの事前プロビジョニングされたデータおよび検出されたデータの管理
- DPE 用の命令の生成、およびキャッシングのための DPE サーバへの配送
- DPE を最新の状態に保つための連携
- すべての BAC 機能に対する API 要求の処理
- BAC システムの管理

RDU は、拡張性のあるアーキテクチャにより新しい技術とサービスの追加をサポートします。

現行の BAC では、1 回のインストールで 1 つの RDU がサポートされます。RDU フェールオーバーをサポートする場合は、Veritas または Sun のクラスタリング ソフトウェアを使用することをお勧めします。フェールオーバーのセットアップでは、RAID（冗長ディスク アレイ）の共有ストレージを使用することをお勧めします。

Device Provisioning Engine

Device Provisioning Engine（DPE）は、RDU に代わって CPE と通信し、プロビジョニング機能や管理機能をすべて実行します。

RDU は、デバイスに対して実行する必要のあるアクションを指示する、DPE 用の命令を生成します。この命令は、関係する DPE サーバに配送され、そこでキャッシュされます。次に、この命令は CPE とのインタラクションで使用され、デバイスの構成、ファームウェアのアップグレード、およびデータの取得などのタスクを実行します。

各 DPE は最大 50 万個のデバイスの情報をキャッシュします。冗長性とスケーラビリティを確保するために複数の DPE を利用することができます。

DPE は次に示すアクティビティを管理します。

- 最新の命令セットを取得してキャッシュするための、RDU との同期
- ファイル ダウンロード サービスのための、CWMP および HTTP を使用した CPE との通信
- CPE との通信における認証と暗号化

DPE は、Solaris 9 オペレーティング システムを実行しているサーバにインストールされます。DPE の設定と管理には CLI が使用されます。CLI には、ローカルで、または Telnet を介してリモートでアクセスできます。DPE がサポートする CLI コマンドの詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

それ以外の重要な情報については、次の項を参照してください。

- DPE のライセンシング（P.2-5）
- DPE と RDU 間の同期（P.2-5）

また、命令の生成に関する概念を十分に理解しておいてください（P.4-6 の「命令の生成と処理」を参照）。

DPE のライセンシング

ライセンシングにより、ご使用になれる DPE（ノード）の数が管理されます。お持ちのライセンスより多くの DPE をインストールしようとすると、新しい DPE は RDU に登録されず、拒否されます。ライセンスされている既存の DPE は、オンラインのままになります。

（注） ライセンシングの目的上、登録済みの DPE は 1 つのノードと見なされます。

ライセンスの追加、評価ライセンスの拡張、または評価ライセンスの満了によってライセンスを変更するときは必ず、その変更がすぐに有効になります。

RDU データベースから登録済みの DPE を削除すると、ライセンスは解放されます。DPE は RDU に自動的に登録されるため、ライセンスを開放する場合は DPE をオフラインにする必要があります。次に、RDU の管理者のユーザ インターフェイスを使用して、DPE を RDU データベースから削除します。

（注） 特定のライセンスを介してイネーブルにした機能は、対応するライセンスがシステムから削除されても、引き続き動作します。

登録時に、ライセンシングの制約を超えるために拒否された DPE は、管理者のユーザ インターフェイスには表示されません。ライセンスの状態を判断するには、RDU と DPE のログファイルを調べる必要があります。

DPE と RDU 間の同期

BAC は複数の DPE をサポートします。各 DPE は、デバイスおよび RDU と通信します。インストール中に、各 DPE に対して次の項目を設定する必要があります。

- この DPE が属するプロビジョニング グループの名前。この名前により、各 DPE によるデバイス サービスの論理グループが判別されます。
- RDU の IP アドレスとポート番号。

DPE と RDU 間の同期とは、RDU との整合を取るために、DPE キャッシュを自動的に更新するプロセスです。DPE キャッシュは、デバイス用の命令を含む命令キャッシュと、デバイスに必要なファイルを含むファイル キャッシュから構成されます。

通常、RDU は、命令の更新に関するイベントを生成し、関係するすべての DPE に送信して DPE を最新の状態に保ちます。同期が必要になるのは、接続の切断によって DPE 側でいくつかのイベントが欠落した場合です。切断の原因としては、ネットワークの問題、管理目的での DPE サーバのダウン、または障害などが考えられます。また、同期は、RDU データベースをバックアップから復元するという特殊なケースでも使用されます。このケースでは、RDU との整合を取るために、DPE キャッシュのデータベースを古い状態に戻す必要があります。

（注） RDU と DPE 間の同期プロセスは自動的に実行されるため、管理操作は必要ありません。同期プロセスの実行中でも、DPE は CPE に対してプロビジョニング操作や管理操作をすべて実行できます。

DPE は RDU との接続を確立するたびに同期プロセスをトリガーします。

DPE は最初に起動したときに、RDU への接続を確立し、RDU に登録して命令変更の更新を受信します。次に、DPE と RDU が、ハートビート メッセージの交換を使用して、接続を監視します。DPE は、RDU への接続が切断されたと判断すると、接続の再確立を自動的に試みます。この試行は、成功するまでバックオフのリトライ間隔で続行されます。RDU も、接続の切断を検出すると、この DPE へのイベントの送信を停止します。接続の切断によって RDU からの更新イベントが DPE 側で欠落する場合があるため、DPE は、RDU との接続を確立するたびに同期を実行します。

RDU との接続を確立して登録するプロセスの間、DPE は *Registering* 状態になっています。

DPE は、必要な命令すべてのリストを RDU に要求します。このリストには、命令およびリビジョン番号の識別子が含まれています。ただし、命令の実際の内容は含まれていません。DPE はこのリストを使用して、ストレージ内の命令のうち、整合の取れていない（バージョン番号が間違っている）もの、欠落しているもの、および削除するものを判別します。同期リストを取得してストレージと比較するプロセスの間、DPE は *Synchronizing* 状態になっています。

RDU から取得する命令の判別が終了するとすぐに、DPE は RDU からの命令の取得を開始します。DPE が取得するのは、欠落している命令、または古くなった命令だけです。このプロセスの間、DPE は *Populating* 状態になっています。

DPE では、RDU が要求によって過負荷にならないようにするため、データを一定のレートで読み込みます。プロビジョニング グループ内の複数の DPE がデータを読み込む場合は、要求された命令がプロビジョニング グループ内のすべての DPE に送信されるため、読み込み時間が短縮されることがあります。データの読み込みを終了すると、DPE は *Ready* 状態になり、RDU と完全に同期の取れた状態になります。

DPE の状態を表示するには、管理者のユーザ インターフェイス（P.16-24 の「Device Provisioning Engine の表示」を参照）または DPE CLI（**show dpe** コマンド）を使用します。

プロビジョニング グループ

プロビジョニング グループは、通常 1 つ以上の DPE で構成されるサーバを、論理的に（通常は地理的に）グループ化したものになるように設計されています。特定のプロビジョニング グループ内の各 DPE では、RDU からの同一の命令セットがキャッシュされます。その結果、冗長性とロードバランシングが可能になります。1 つのプロビジョニング グループで、最大 50 万個のデバイスのプロビジョニング ニーズに対処できます。デバイスの数が 50 万個を上回る場合は、追加のプロビジョニング グループを配備に加えることができます。

（注） プロビジョニング　グループのサーバは各地域に設置する必要はありません。中央のネットワーク オペレーション センターに簡単に配備することができます。

詳細については、次の項を参照してください。

- ACS URL のディスカバリ（P.2-7）
- プロビジョニング グループのスケーラビリティ（P.2-7）

ACS URL のディスカバリ

BAC の分散アーキテクチャにおいて、RDU は中央集中型の集約ポイントであり、CPE と直接対話することがありません。CPE との必要なインタラクションはすべて、プロビジョニング グループに委任されます。各デバイスは、接続先となるプロビジョニング グループを、1 つの自動構成サーバ（ACS）の URL で識別します（ACS は DPE とも呼ばれます）。URL が更新されない限り、デバイスは同一の URL にある DPE と交信します。

特定のプロビジョニング グループ内の冗長 DPE はすべて、1 つの ACS URL を共有する必要があります。RDU は、各プロビジョニング グループに関連付けられている URL を認識するだけでなく、そのプロビジョニング グループ内のすべての DPE を認識する必要があります。必要に応じてデバイスを新しいプロビジョニング グループにリダイレクトする場合、RDU は、プロビジョニング グループの ACS URL に関する知識を使用します。

プロビジョニング グループの ACS URL は、RDU が DPE の登録から自動的に学習する場合と、API または管理者のユーザ インターフェイスからプロビジョニング グループ オブジェクトに設定される場合があります。ACS URL の設定については、P.3-8 の「プロビジョニング グループの設定ワークフロー」を参照してください。

CPE では、次のどちらかの方法で ACS（DPE）URL を特定できます。

- デバイスに URL を事前設定しておく。この ACS URL は、各プロビジョニング グループに関連付けられている BAC サーバの設定済み URL です。設定済み URL は、出荷前にデバイスに事前設定されるもので、割り当て済み URL とも呼ばれます。
- DHCP を介して URL を検出する。この ACS URL は、DHCP Discover、DHCP Request、または DHCP Inform への応答として返されます。このメカニズムは、主要なインターネット ゲートウェイ デバイスの配備に限定されます。これは、DHCP 要求を WAN 側に送信する機能が必要なためです。

（注） URL を事前設定によって割り当てる方法は、DHCP を介して検出する方法よりも安全なメカニズムです。

プロビジョニング グループのスケーラビリティ

プロビジョニング グループでは、BAC ネットワークのスケーラビリティを拡張する手段として、各プロビジョニング グループをデバイスのサブセットだけに関連付けます。このようなデバイスのパーティション化では、デバイスを地域的にグループ化することや、サービス プロバイダーによって定義されたポリシー別にグループ化することができます。プロビジョニング グループのサイズを制限すると、各 DPE がより効率的に必要な情報をキャッシュできるようになります。

サービス プロバイダーで配備を拡大するには、次の作業を行います。

- 既存の DPE サーバのハードウェアをアップグレードする。
- プロビジョニング グループに DPE サーバを追加する。
- プロビジョニング グループを追加する。

BAC プロセス ウォッチドッグ

BAC プロセス ウォッチドッグは、すべての BAC プロセスのランタイム状況を監視する管理エージェントです。このウォッチドッグ プロセスにより、プロセスが予想外に停止した場合に自動的に再開されるようになります。

BAC プロセス ウォッチドッグは、監視対象プロセスの状態を開始、停止、再開、決定するコマンド ライン ツールとして利用できます。

監視対象のアプリケーションが機能しなくなると、自動的に再開されます。何らかの理由で再開プロセスも機能しない場合は、BAC ウォッチドッグ プロセス サーバは所定の時間待機してから再び再開を試みます。

監視対象プロセスの管理方法の詳細については、P.9-1 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェント

BAC では、RDU サーバおよび DPE サーバについて基本的な SNMP v2 ベースのモニタリングがサポートされます。BAC SNMP エージェントでは SNMP 通知と SNMP トラップがサポートされます。snmp-server CLI コマンドを使用して DPE に SNMP エージェントを設定し、SNMP 設定コマンドライン ツールを使用して RDU に SNMP エージェントを設定できます。

SNMP 設定コマンドライン ツールの詳細については P.11-5 の「SNMP の使用によるサーバの監視」を、DPE CLI の詳細については『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

ロギング

イベントのロギングは DPE と RDU で実行されます。まれに、視認性向上のために、DPE イベントが RDU に記録されることもあります。ログ ファイルはそれぞれのログ ディレクトリに配置され、任意のテキスト エディタを使用して調べることができます。ログ ファイルを圧縮すると、トラブルシューティングや障害の解決のために Cisco Technical Assistance Center またはシステム インテグレータに電子メールで送信しやすくなります。また、RDU と DPE のログには、管理者のユーザ インターフェイスからアクセスすることもできます。

ログのレベルと構造、およびログ ファイルの番号付けと循環の詳細については、P.19-3 の「ロギング」を参照してください。

設定のワークフローとチェックリスト

この章は大きな 2 つの項で構成されており、さまざまなテクノロジーをサポートするように BAC コンポーネントを設定する際のプロセスを定義します。次の項で構成されています。

- コンポーネントのワークフロー（P.3-1）
- 技術のワークフロー（P.3-3）

コンポーネントのワークフロー

この項では、BAC でサポートされるテクノロジーに合せて各 BAC コンポーネントを設定する際に必要なワークフローについて説明します。これらの設定作業を行ってから、特定のテクノロジーをサポートするように BAC を設定します。

この項で説明するコンポーネントのワークフローはチェックリストの形式で用意されており、次のものがあります。

- RDU チェックリスト
- DPE チェックリスト

RDU チェックリスト

表 3-1 は、RDU 設定時のワークフローを示しています。

表 3-1　RDU ワークフロー チェックリスト

手順	参照先
1. BAC に利用されるシステム syslog サービスを設定する。	『*Installation Guide for Cisco Broadband Access Center, 3.0*』
2. BAC 管理者のユーザ インターフェイスにアクセスする。	管理者のユーザ インターフェイスの設定（P.15-2）
3. 管理者のパスワードを変更する。	管理者のユーザ インターフェイスの設定（P.15-2）
4. 適切なライセンス キーを追加する。	ライセンス キーの管理（P.17-18）
5. RDU データベース バックアップ手順を設定する。	バックアップと回復（P.10-6）
6. RDU SNMP エージェントを設定する。	snmpAgentCfgUtil.sh ツールの使用方法（P.11-6）

DPE チェックリスト

表 3-2 に示されている作業は、表 3-1 に示されている作業の後で実行する必要があります。

（注）アスタリスク（*）が付いている項目は、必須の作業または手順です。

表 3-2　DPE 設定チェックリスト

手順	参照先
1. BAC に利用されるシステム syslog サービスを設定する。	『*Installation Guide for Cisco Broadband Access Center, 3.0*』
2. パスワードを変更する。*	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **password** コマンド
3. プロビジョニング インターフェイスを設定する。	『*Cisco Broadband Access Center CPE CLI Reference, 3.0*』に示されている **interface ethernet** [**intf0** | **intf1**] コマンド
4. BAC の共有秘密情報を設定する。*	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **dpe shared-secret** コマンド
5. 目的の RDU に接続するために DPE を設定する。*	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **dpe rdu-server** コマンド
6. ネットワーク タイム プロトコル（NTP）を設定する。	Solaris のマニュアルに示されている設定情報
7. プロビジョニング グループの名前を設定する。*	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **dpe provisioning-group primary** コマンド
8. RDU およびネットワーク内のデバイスへの必要なルートを設定する。	Solaris のマニュアルに示されている設定情報
9. DPE SNMP エージェントを設定する。	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている SNMP エージェント コマンド
（注）SNMP エージェントを設定するには、DPE のコマンドライン インターフェイスまたは snmpAgentCfgUtil.sh ツールを使用します。詳細については、P.11-6 の「snmpAgentCfgUtil.sh ツールの使用方法」を参照してください。	
10. DPE が RDU に正常に接続され、登録されたことを確認する。	サーバの表示（P.16-24）

技術のワークフロー

この項では、特定の技術（この場合は CWMP）をサポートするように BAC を設定する際に必要な作業について説明します。これらの設定作業は、BAC コンポーネントの設定後に実行します。

この項で説明する CWMP 技術のワークフローはチェックリストの形式で用意されており、次のものがあります。

- RDU の設定ワークフロー（P.3-3）
- DPE の設定ワークフロー（P.3-5）
- プロビジョニング グループの設定ワークフロー（P.3-8）

RDU の設定ワークフロー

表 3-3 は、CWMP 技術について RDU を設定するのに必要な設定作業を示しています。

表 3-3　RDU の設定ワークフロー

手順	参照先
1. BAC のサービス クラスを使用してサービス プロファイルを作成する。 管理者のユーザ インターフェイスから、テンプレートで参照されるカスタム プロパティを定義します。カスタム プロパティは、設定およびファームウェア ルール テンプレートで参照できます。 サービスごとに、次の作業を行う必要があります。	カスタム プロパティの設定（P.17-7）
a. 設定テンプレートを作成する。 管理者のユーザ インターフェイスから、設定テンプレートを RDU に追加します。	ファイルの追加（P.17-15）
b. ファームウェア ルール テンプレートを作成する。 — 管理者のユーザ インターフェイスから、ファームウェア イメージを RDU に追加する。 — 管理者のユーザ インターフェイスから、ファームウェア ルール テンプレートを RDU に追加する。	 ファイルの追加（P.17-15） ファイルの追加（P.17-15）
c. 管理者のユーザ インターフェイスから、サービス クラスを作成する。 次の作業を確実に行います。 — 設定テンプレート ファイルを指定する。 — ファームウェア ルール ファイルを指定する。 — （オプション）プロパティを指定する。	サービス クラスの設定（P.17-2）
2. 管理者のユーザ インターフェイスから、CWMP 技術に関するデフォルト設定値を設定する。 — デフォルトのサービス クラスを設定する（たとえば、不明なデバイス用）。 — 次のいずれかのページで、接続要求サービスのデフォルトを設定する（**Configuration > Class of Service**、**Configuration > Defaults**、および **Devices**）。	デフォルトの設定（P.17-8）
3. CWMP デバイスを登録する。	BAC でのデバイス データの事前登録（P.3-4）

BAC でのデバイス データの事前登録

事前登録とは、デバイスが DPE と最初に交信する前に、デバイス レコードを RDU に追加する作業を指します。DPE は自動構成サーバ（ACS）とも呼ばれます。この作業は、通常、プロビジョニング API から実行されます。ただし、管理者のユーザ インターフェイスからデバイス データを事前登録することも可能です。

BAC でデバイス データを事前登録するには、次の手順に従います。

ステップ 1　API または管理者のユーザ インターフェイスを使用して、デバイス レコードを RDU データベースに追加します。

管理者のユーザ インターフェイスからデバイス レコードを追加するには、次の手順に従います。

a. **Devices** > **Manage Devices** の順に選択します。

b. Manage Devices ページで、**Add** をクリックします。

c. Add Device ページが表示されます。適切なフィールドに値を入力します。事前登録するデバイスの必須および推奨プロビジョニング属性は、次のとおりです。

必須
• デバイス識別子
• 登録されているサービス クラス
• ホーム プロビジョニング グループ
一般的な追加属性
（注） 追加属性は、顧客宅内装置（CPE）の認証方式に応じて、必須となる場合や、サポートされる場合があります。
• オーナー識別情報
• CPE パスワード（一意のクライアント証明書を使用するクライアント認証がイネーブルになっていない場合）
• 接続要求ユーザ名（このステップはオプション）
• 接続要求パスワード（このステップはオプション）
オプション
サービス クラスの接続要求方式（このステップはオプション） 接続要求方式を設定すると、自動構成サーバのデバイス認証がイネーブルになります。次のいずれかを選択します。 • Discovered • Use FQDN • Use IP

ステップ 2　デバイス レコードが事前登録されたかどうかを確認します。次の手順に従います。

- Device Details ページを調べる。次の手順に従います。

  Devices > **Manage Devices** ページで、デバイスに対応する **View Details** アイコン（）をクリックします。Device Details ページで、次の作業を行います。

  — デバイス設定が正しいかどうかを確認する。

  — 検出されたパラメータを検索する。デバイスが DPE との最初の交信をまだ開始していない場合、このパラメータは表示されません。

— デバイス履歴のログを確認する。

- RDU と DPE のログ ファイルを調べる（P.19-3 の「ロギング」を参照）。

ステップ 3　DPE に定期的な通知を送信するようにデバイスを設定します。これを行うには、設定テンプレートに *PeriodicInformEnable* 変数と *PeriodicInformInterval* 変数を設定します。

ステップ 4　BAC との最初のデバイス交信を開始します。次の手順に従います。

- API から接続要求を開始する。
- デバイスから次の定期交信があるまで待機する。
- リブートする。

ステップ 5　BAC との最初のデバイス交信を確認します。**Device** > **Manage Devices** > **Device Details** の順に選択し、検出されたプロパティが表示されるかどうかを確認します。また、履歴ログで詳細を確認します。

DPE の設定ワークフロー

この項では、DPE で CWMP をサポートできるようにする方法について説明します。これを行うには、次の設定を行います。

- CWMP 管理のための CWMP サービスを DPE に設定する。
  P.3-5 の「DPE に対する CWMP サービスの設定」を参照してください。
- ファームウェア管理のための HTTP ファイル サービスを DPE に設定する。
  P.3-7 の「DPE に対する HTTP ファイル サービスの設定」を参照してください。

DPE に対する CWMP サービスの設定

表 3-4 は、CWMP サービスを DPE に設定するのに必要な設定作業を示しています。

表 3-4　DPE の設定ワークフロー：CWMP 管理

手順	参照先
DPE 上で動作する CWMP サービスを設定します。 CWMP 技術を DPE に設定するには、CWMP サービスを少なくとも 1 つイネーブルにする必要があります。CWMP サービスをイネーブルにするには、次のコマンドを入力します。 **`service cwmp`** *`num`* **`enable true`** *num* は CWMP サービスを示します。1 または 2 を指定します。 デフォルトでは、CWMP サービスは次の状態になります。 — サービス 1 の場合はイネーブル — サービス 2 の場合はディセーブル	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている CWMP 技術のコマンド

表 3-4　DPE の設定ワークフロー：CWMP 管理（続き）

手順	参照先
1. CWMP サービスが CPE と通信するときのポートを設定する。 デフォルトでは、CWMP サービスは次のポートでリッスンするように設定されています。 — サーバ 1 の場合はポート 7547 — サーバ 2 の場合はポート 7548	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **service cwmp** *num* **port** *port* コマンド
2. CWMP サービスに対して、HTTP を使用したクライアント認証を設定する。 **（注）** クライアント認証時のセキュリティ　リスクを制限するため、Digest モード（デフォルト設定）を使用することをお勧めします。クライアント認証を Basic モードで使用することや、Basic 認証と Digest 認証を両方ともディセーブルにすることはお勧めできません。	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **service cwmp** *num* **client-auth** *mode* コマンド
3. CWMP サービスに対して、SSL 経由の証明書を使用したクライアント認証を設定する。	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **service cwmp** *num* **ssl client-auth** *mode* コマンド
4. DPE でデバイスを認識できない場合に構成を RDU に要求するように DPE を設定する。 **（注）** この機能をイネーブルにすると、RDU が DoS 攻撃（サービス拒絶攻撃）を受ける可能性があります。	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **service cwmp** num **allow-unknown-cpe** コマンド

DPE に対する HTTP ファイル サービスの設定

表 3-5 は、DPE 上で動作する HTTP ファイル サービスを設定するのに必要な設定作業を示しています。

表 3-5　DPE の設定ワークフロー：ファームウェア管理

手順	参照先
DPE 上で動作する HTTP ファイル サービスを設定します。 ファームウェア管理を DPE に設定するには、HTTP ファイル サービスを少なくとも 1 つイネーブルにする必要があります。HTTP ファイル サービスをイネーブルにするには、次のコマンドを入力します。 `service http` *num* `enable true` *num* は HTTP ファイル サービスを示します。1 または 2 を指定します。 デフォルトでは、HTTP サービスは次の状態になります。 — サービス 1 の場合はイネーブル — サービス 2 の場合はディセーブル	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている CWMP 技術のコマンド
1. HTTP ファイル サービスが CPE と通信するときのポートを設定する。 デフォルトでは、HTTP ファイル サービスは次のポートでリッスンするように設定されています。 — サーバ 1 の場合はポート 7549 — サーバ 2 の場合はポート 7550	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **service http** *num* **port** *port* コマンド
2. HTTP ファイル サービスに対して、クライアント認証を設定する。 **(注)** クライアント認証時のセキュリティ　リスクを制限するため、Digest モード（デフォルト設定）を使用することをお勧めします。クライアント認証を Basic モードで使用することや、Basic 認証と Digest 認証を両方ともディセーブルにすることは避ける必要があります。	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **service http** *num* **client-auth** *mode* コマンド
3. HTTP ファイル サービスに対して、SSL 経由の証明書を使用したクライアント認証を設定する。	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』に示されている **service http** *num* **ssl client-auth** *mode* コマンド

プロビジョニング グループの設定ワークフロー

まず、DPE が特定のプロビジョニング グループに追加されるように設定します（P.12-12 の「プロビジョニング グループへの DPE の追加」を参照）。その後、DPE が RDU への登録を行うと、プロビジョニング グループが自動的に作成されます。プロビジョニング グループが作成されたら、管理者のユーザ インターフェイスから BAC サーバの URL を割り当てて設定します。

プロビジョニング グループの URL を設定する前に、ローカルおよび地域の冗長性に関する BAC の概念を十分に理解しておいてください（P.12-11 の「プロビジョニング グループのスケーラビリティとフェールオーバー」を参照）。

（注） プロビジョニング グループを作成したら、ただちにプロビジョニング グループに URL を割り当てることをお勧めします。URL を割り当てると、プロビジョニング グループ間の CPE リダイレクションがイネーブルになります。ロード バランサを使用する場合は、ロード バランサのアドレスが ACS URL として使用されていることを確認します。

管理者のユーザ インターフェイスからプロビジョニング グループの ACS URL を設定するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーで、**Servers > Provisioning Groups** の順にクリックします。

ステップ 2　Manage Provisioning Groups ページが表示されます。適切なプロビジョニング グループの Identifier リンクをクリックします。

ステップ 3　View Provisioning Group Details ページが表示されます。Provisioning Group Properties 領域で、ACS URL フィールドに URL を入力します。

（注） 設定する URL によって、検出された ACS URL が上書きされることに留意してください。

ステップ 4　**Submit** をクリックします。

これで、プロビジョニング グループが、設定した URL にある BAC と交信するようになりました。

CPE 管理の概要

この章では、Broadband Access Center（BAC）で CPE WAN Management Protocol を使用して顧客宅内装置（CPE）を管理する方法について説明します。この章は、次の項で構成されています。

概要

BAC は CPE と通信する場合、CPE Wan Management Protocol（CWMP）を使用し、TR-069 やその他の関連するデータ モデル仕様で規定されているパラメータに従います。CWMP には、CPE を安全に管理するための、次のような機能があります。

- 自動構成および動的サービス プロビジョニング
- ファームウェア管理
- デバイス診断
- パフォーマンスおよびステータスのモニタリング

BAC は、TR-069、TR-098、TR-104、および TR-106 標準に基づいて、デバイスをサポートします。サポートされるデバイスには、イーサネットおよび ADSL ゲートウェイ デバイス、無線ゲートウェイ、VoIP ATA などの CWMP 準拠のデバイスがあります。また、このリリースには、近く公開されるデータ モデル標準やベンダー固有のデータ モデルすべてをサポートする、実行時に拡張可能なデータ モデルが搭載されています。

BAC デバイス オブジェクト モデル

BAC デバイス オブジェクト モデルは、DPE 用のデバイス管理命令として生成される、構成およびファームウェア ルールを制御する上で重要です。このプロセスは RDU で発生し、名前付き属性および関連付けを通じて制御されます。

デバイス オブジェクト モデルには、次の主要オブジェクトがあります。

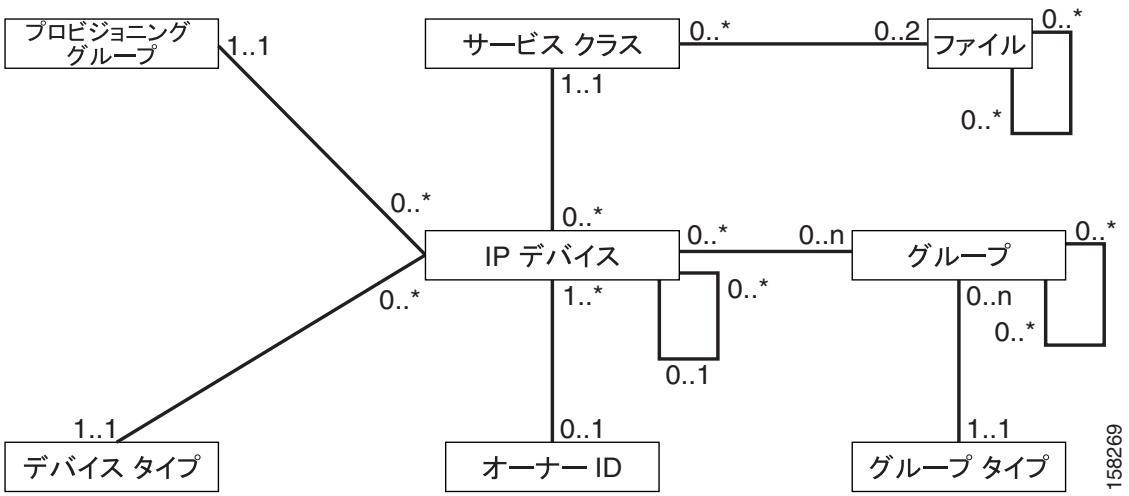
- IP デバイス：プロビジョニングを必要とするネットワーク エンティティを表します。
- オーナー ID：加入者の外部識別子を表します。
- デバイス タイプ：デバイスのタイプを表します。
- プロビジョニング グループ：特定の複数の DPE からサービスを受けるデバイスの論理グループを表します。
- サービス クラス：デバイスに割り当てる構成プロファイルを表します。
- ファイル：プロビジョニングで使用される、テンプレートやファームウェア　イメージを含むファイルのコンテナとして機能します。
- グループ：デバイスをグループ化するための顧客固有のメカニズム。

BAC デバイス データ モデルの各種オブジェクトには、次の共通要素があります。

- 名前。たとえば、Gold サービス クラス。
- 属性。たとえば、Device ID や Fully Qualified Domain Name（FQDN）。
- 関連付け。たとえば、デバイスとサービス クラスの関連付け。
- プロパティ。たとえば、デバイスを特定のプロビジョニング グループに追加することを指定するプロパティ。

デバイス データ モデルの各種オブジェクト間のインタラクションについては、図 4-1 を参照してください。

図 4-1　デバイス オブジェクト モデル



BAC デバイス オブジェクト モデルでは、IP デバイスは、サービス クラス、プロビジョニング グループ、およびデバイス タイプに関連付けられます。次に、サービス クラスは、設定テンプレートおよびファームウェア ルール テンプレートに関連付けられます。ファイルは他のファイルと相互に関連付けることができます。たとえば、ファームウェア ルール テンプレートをファームウェア イメージに関連付けることができます。

表 4-1 は、データ モデルの各オブジェクトに固有の属性および関連付けを示しています。

表 4-1　デバイス オブジェクトの関連付け

オブジェクト	関連付けられるオブジェクト
IP デバイス • 事前登録または登録解除が可能です（P.4-9 の「BAC におけるデバイス配備」を参照）。 • 属性には、Device ID (OUI-Serial) や FQDN があります。	• オーナー ID • プロビジョニング グループ • サービス クラス • デバイス タイプ
オーナー ID • デバイスに関連付けられます。そのため、デバイスに関連付けられた場合に限り存在します。 • グループ化をイネーブルにします。たとえば、*Joe* に属しているデバイスすべてをグループ化できます。	IP デバイス
デバイス タイプ • 技術（特に CWMP）を持つデバイスすべてに共通したデフォルトが格納されます。 • グループ化をイネーブルにします。たとえば、すべての CWMP デバイスをグループ化できます。	IP デバイス
ファイル • プロビジョニングで使用されるファイルが格納されます（たとえば、設定テンプレートやファームウェア ルール テンプレート）。	サービス クラス
サービス クラス • 属性には、Type、Name、および Properties があります（詳細については、P.4-3 の「サービス クラス」を参照してください）。	• IP デバイス • ファイル • 設定テンプレート（オプション） • ファームウェア ルール テンプレート（オプション）

サービス クラス

サービス クラスは RDU 抽象の 1 つで、テンプレートの形式でデバイスに渡される構成を表します。サービス クラスを使用すると、デバイスをグループ化して構成セットにすることができます。構成セットは、各種のサービス レベルまたはパッケージで CPE に提供されます。

サービス クラスには次の種類があります。

- 登録されているもの：デバイスの登録時にユーザによって指定されます。このサービス クラスは、明示的に、アプリケーション プログラミング インターフェイス（API）を介してデバイス レコードに追加されます。
- 選択されているもの：RDU 拡張によって選択され、返されます。

- 関連付けられているもの：登録、選択、またはその両方の操作によってデバイスに関連付けられます。このサービス クラスは、RDU 拡張によって選択されます。

デバイス用の選択されているサービス クラスが変更された場合は、デバイス構成用の命令が再生成されます。デバイス用の登録されているサービス クラスが変更された場合、それが選択されているサービス クラスでなくても、生成されたデバイス構成用の命令が再生成されます。その理由は、サービス クラスが適用するポリシーによって、選択されているサービス クラスが変更される可能性があるためです。

デバイス データ モデルに関連する概念には、次のものもあります。

- プロパティ階層（P.4-4）
- カスタム プロパティ（P.4-4）

プロパティ階層

BAC のプロパティを使用すると、BAC で API を介してデータにアクセスすることや、データを格納することができます。事前プロビジョニングされたデータ、検出されたデータ、およびステータス データは、API を介して、対応するオブジェクトのプロパティから取得できます。また、プロパティを使用すると、BAC を適切な粒度で（システム レベルからデバイス グループおよび個々のデバイスのレベルまで）設定できます。

デバイス関連のプロパティは、BAC プロパティ階層内の任意の許容ポイントで定義できます。プロパティを任意のレベルで割り当てられるかどうかの詳細については、API Javadoc を参照してください。

BAC プロパティ階層には柔軟性があり、システム全体またはサービス クラスのデフォルトを定義してから、個々のデバイスの設定で上書きすることができます。このプロパティ階層で使用できるプロパティは次のとおりです。

- デバイス
- プロビジョニング グループ
- サービス クラス
- デバイス タイプ
- システム デフォルト

カスタム プロパティ

カスタム プロパティを使用すると、新しいプロパティを定義できます。定義されたプロパティは、API を介して任意のオブジェクト上に格納することができます。

カスタム プロパティは、RDU で定義された変数名であるため、スペースを含めることはできません。テンプレート パーサーは、階層の下から上にプロパティを検索し、テンプレート オプション構文に変換します。詳細については、P.5-15 の「カスタム プロパティ」を参照してください。

CPE パラメータの検出

BAC では、CWMP で定義されたとおり、Remote Procedure Call（RPC; リモート プロシージャ コール）を使用して CPE パラメータを読み込むことができます。この操作では、必ず、Data Synchronization Instruction が使用されます。この命令は、CPE デバイス データが変更された場合に、CPE デバイスからのデータを検出し、そのデータを RDU に報告して、RDU を最新の状態に保ちます。この命令を使用すると、ソフトウェア バージョンやモデル名などの重要なパラメータについて、RDU を最新の状態に保つことができます。また、これらのパラメータを使用して、特定のデバイス タイプに固有の構成命令など、別の命令を生成することもできます。

表 4-2 は、BAC によって検出されるデフォルト パラメータを示しています。

表 4-2　検出されるデフォルト パラメータ

パラメータ	説明
Inform.DeviceId.Manufacturer	CPE の製造元を示します。
Inform.DeviceId.ManufacturerOUI	CPE 製造元の一意の識別子を示します。
Inform.DeviceId.ProductClass	製造元の *SerialNumber* パラメータが一意となる対象の製品または製品クラスを示します。
InternetGatewayDevice.DeviceInfo.HardwareVersion	CPE のハードウェア バージョンを示します。
InternetGatewayDevice.DeviceInfo.SoftwareVersion	CPE に現在インストールされているソフトウェア バージョンを示します。
InternetGatewayDevice.DeviceInfo.ModelName	CPE のモデル名を示します。
InternetGatewayDevice.ManagementServer.ParameterKey	サーバから前回実行された SetParameterValues、AddObject、または DeleteObject コールの *ParameterKey* の値を示します。

これらのプロパティを更新するには、API（/server/acs/discover/parameters プロパティを使用）または管理者のユーザ インターフェイスを使用します（P.12-8 の「デバイスからのデータの検出」を参照）。

（注） デバイスのルート オブジェクトが InternetGatewayDevice 以外（Device など）になっていても、パラメータは検出されます。

命令の生成と処理

命令の生成とは、CWMP デバイスに固有の命令セットを生成するプロセスです。デバイス テクノロジーを BAC に組み込むための技術拡張を使用することで、デバイスの詳細とプロビジョニング ルールが結合され、CPE に固有の命令セットが作成されます。作成された命令セットは、デバイスのプロビジョニング グループ内の DPE に転送され、そこでキャッシュされます。

BAC 配備内でデバイスを有効にすると、そのデバイスは BAC サーバとの交信を開始します。交信が確立すると、デバイスの事前設定されたポリシーが、DPE による管理操作を、デバイスに関連付けられている設定テンプレートまたはファームウェア ルール テンプレートに基づいて特定します。この事前設定されたポリシーは、デバイスのサービス レベル（サービス クラスとも呼ばれる）を特定します。デバイス構成には、認証情報、定期的な通知のレート、およびサービス クラスなど、顧客に必要なプロビジョニング情報を含めることができます。この信頼できるデバイスのプロビジョニング情報は、デバイス構成命令として、RDU から DPE に転送されます。

命令は、DPE 自動構成サーバ（ACS）が特定のデバイスに対して実行する論理的な操作となっています。命令では、GetParameterValues などの CWMP リモート プロシージャ コール（RPC）に直接マッピングすることや、ファームウェア ルールなどの追加ロジックを複数の CWMP RPC と組み合せることができます。

RDU は、「InstructionRecords」を DPE に渡して命令の処理を要求します。次に、DPE サーバが、この「InstructionRecords」を「Instructions」に変換し、その結果を「InstructionResponseRecords」として RDU に返します。

BAC は命令を生成するときに、次の機能を使用します。

- Instruction Generation Extension：1 つのデバイス用に「InstructionRecords」を生成します。
- Instruction Generation Service：複数のデバイス用に「InstructionRecords」を生成します。

  Instruction Generation Service の統計情報にアクセスするには、管理者のユーザ インターフェイスで **Servers > RDU > View Regional Distribution Unit Details** の順に選択します。

RDU が生成する各種の命令には、次のものがあります。

- Data Synchronization Instruction（DataSyncRecord）：ソフトウェア バージョンやモデル名などのさまざまな CPE パラメータについて、RDU を最新の状態に保ちます。また、これらのパラメータを使用して、特定のデバイス タイプに固有の構成命令など、別の命令を生成することもできます。パラメータの中には、接続時に毎回確認されるものもあれば、ファームウェア バージョンが変更されたときだけ確認されるものもあります。詳細については、P.12-8 の「デバイスからのデータの検出」を参照してください。
- Routable IP Address Instruction（RoutableIPAddressRecord）：特定のデバイスが到達可能かどうかを検出します。その際、接続要求を送信するために、DPE がデバイスとの TCP 接続を作成できるようにします。この命令は、デバイスの WAN IP アドレス（PPP または DHCP）を取得し、発信元 IP アドレスと比較します。IP アドレスが異なる場合、命令は RDU を更新します。
- Redirect Instruction：新しい BAC サーバを指定します。そのために、既存のサーバの URL を変更し、デバイスのプロビジョニング グループを変更します。リダイレクション命令は、この変更を効率的な方法で実行し、リダイレクションが実行されたことを RDU に示します。詳細については、P.14-6 の「デバイスのプロビジョニング グループのリダイレクト」を参照してください。
- Firmware Rules Instruction（FirmwareRulesRecord）：デバイスにダウンロードするファームウェア イメージを特定します。ファームウェア イメージ ファイルは、ファームウェア ルール テンプレートによってデバイス グループに関連付けられます。BAC は、関連付けられたテンプレート内のルールを使用して、CPE にダウンロードするファームウェアを評価します。この命令が有効になるのは、デバイスがファームウェア ルール テンプレートに関連付けられている場合のみです。

- Configuration Synchronization Instruction（ConfigSyncRecord）：DPE キャッシュに格納されている CPE 構成の同期をトリガーします。この命令が有効になるのは、デバイスが設定テンプレートに関連付けられている場合のみです。構成同期のプロセスについては、次の項で説明します。

デバイス構成同期

CPE 構成同期のプロセスでは、デバイスの構成が、デバイスのサービス クラス オブジェクトに関連付けられている設定テンプレートに基づいて、自動的に同期されます。このデバイス用の DPE に格納されている ConfigSync 命令に従って CPE 構成を同期するプロセスは、Configuration Synchronization と呼ばれます。

このプロセス中に、DPE は、サービス クラスを介してデバイスに関連付けられている設定テンプレート内で検出されたパラメータ値および属性をすべて設定します。その結果、次の処理が行われます。

- 通知に、設定テンプレート内の設定値が反映されます。通知の詳細については、P.5-7 の「通知」を参照してください。
- すべてのパラメータのアクセス コントロールに、設定テンプレート内の設定値が反映されます。アクセス コントロールの詳細については、P.5-8 の「アクセス コントロール」を参照してください。

CPE 構成は、TR-069 仕様で定義されたとおり、一意の構成キーに関連付けられます。この構成キーは DPE データベースに保存され、RPC の *ParameterKey* パラメータとして CPE に転送されます。

CPE が DPE との接続を確立するたびに、デバイスは Inform メッセージを DPE に転送して、*ParameterKey* の値を（構成のリビジョン番号の形式で）報告します。DPE では、この値を、特定のデバイスに対応するキャッシュ内の値と比較します。値が一致しない場合は、DPE とデバイスとの同期プロセスがトリガーされます。

構成同期プロセスは次の手順で行われます。

1. DPE がデバイスから *ParameterKey* を受信します。この *ParameterKey* の値が、DPE に格納されている値と一致した場合、同期は開始されません。*ParameterKey* の値が異なる場合は、同期プロセスが続行されます。
2. 構成の中でアクセス コントロールが設定されている場合、DPE は *AccessList* パラメータを ACS-only に設定します。アクセス コントロール機能は、デフォルトでイネーブルになっています。アクセス コントロールの詳細については、P.5-8 の「アクセス コントロール」を参照してください。
3. 通知機能がイネーブルの場合、DPE は通知属性を、デバイス構成で指定されたとおりに設定します。通知は、デフォルトでイネーブルになっています。通知の詳細については、P.5-7 の「通知」を参照してください。
4. DPE は、テンプレートに従ってデバイスのパラメータ値を設定すると、*ParameterKey* 引数に新しい構成のリビジョン番号を設定します。このリビジョン番号は、デバイスおよび DPE が接続を次に確立したときに、デバイス構成を同期するかどうかを判別するために使用されます。

（注） 同期プロセス中にデバイスと DPE との接続がタイムアウトした場合、CPE は DPE への再接続を試みます。この場合、Inform メッセージ内の *ParameterKey* の値は変更されません。これは、*ParameterKey* の値が変更されるのは、同期プロセスが成功した場合に限られるためです。CPE が DPE に再接続した場合、DPE は *ParameterKey* の最初の値を使用して、同期を最初から開始します。

5. DPE が *ParameterKey* 属性の新しい値を最後の更新として CPE に転送すると、同期プロセスが終了します。

（注）場合によっては、DPE とデバイスの *ParameterKey* が一致しても、デバイスの更新が必要になることがあります。

強制的に構成を同期するには、次の手順に従います。

1. **Devices** ページで、構成を同期するデバイスを検索します。
2. デバイスに対応する **Operations** アイコン（）をクリックします。
3. Device Operations ページが表示されます。Perform Device Operation の下のドロップダウン リストから、Force Configuration Synchronization を選択します。
4. **Submit** をクリックします。

   デバイス構成が DPE と同期されます。

BAC におけるデバイス配備

BAC 配備はプロビジョニング グループに分割され、各プロビジョニング グループはデバイスのサブセットだけに関連付けられます。耐障害性を確保するため、プロビジョニング グループによって提供されるサービスはすべて実装されます（P.12-11 の「プロビジョニング グループのスケーラビリティとフェールオーバー」を参照）。

（注）　デバイス管理では、主原則として、RDU がデバイスと直接通信することはありません。デバイス インタラクションはすべて、デバイスが属するプロビジョニング グループ内の DPE に委任されます。

BAC では、次の 2 つのデバイス配備オプションを使用できます。各オプションは、組み合せて使用することもできます。

- Preregistered：デバイスが DPE（ACS とも呼ばれる）と最初に交信する前に、デバイス レコードが RDU に追加されます。
- Unregistered：デバイスが DPE と最初に交信した後で、デバイス レコードが RDU に追加されます。

事前登録されたデバイス

このシナリオでは、デバイス データが BAC に事前プロビジョニングされ、デバイスが特定のサービス クラスに関連付けられます。そのサービス クラスは、加入者の登録先のサービスまたはデフォルト構成に対応させることができます。

事前登録されたデバイスには、サービス プロバイダーに固有の特定のパラメータが事前設定されています。これらのパラメータは、通常、工場出荷時のデフォルトとして「焼き付けられ」ます。

（注）　デバイスを工場出荷時のデフォルトにリセットすると、デバイス上の設定が、事前に焼き付けられた設定に戻るため、デバイスが再構成プロセスを実行する場合があります。

デバイス データは BAC で事前登録されます。この操作は、通常、API から行われます。ただし、管理者のユーザ インターフェイスから行うことも可能です。

事前設定を行うには、次の 3 つの条件があります。

- デバイスがネットワーク接続を確立できる。DSL デバイスの場合は、通常、ATM PVC の自動検出を使用し、認証用に PPP を使用する必要があります。IP アドレスは PPP または DHCP を介して取得されます。その他のデバイスでは、通常、既存のインターネット接続を使用し、アドレス割り当て用にローカル DHCP を使用します。
- CPE が適切なサービス プロバイダーの構成サーバと交信できる（つまり、CPE が ACS URL を認識している）。ACS URL は、デバイスに事前に焼き付ける（割り当てる）ことや、WAN 側から DHCP を使用して検出することができます。
- サービス プロバイダーが CPE を特定の加入者に関連付けることができる。このプロセスは、通常、加入者登録用の Operations Support Systems（OSS; オペレーション サポート システム）アプリケーションによって実行されます。BAC は、デバイス構成をプロビジョニングするための適切なデータで更新されます。

登録解除されたデバイス

このシナリオでは、デバイス データは BAC に事前に読み込まれていません。デバイス データが BAC に追加されるのは、デバイスが BAC サーバと最初に交信したときだけです。

BAC では、登録解除された（事前設定されたパラメータがない）デバイスをネットワーク上に表示し、デフォルトのアクセス権を付与することができます。ただし、デバイス データを BAC に事前登録することがサポートされていないため、登録解除されたデバイスの認証オプションは、共有秘密情報ではなく、証明書に基づくメカニズムの使用に限られます。また、事前登録されたデータがないため、BAC では、デバイスを動的に分類し、デバイスのデフォルト構成を特定する必要があります。

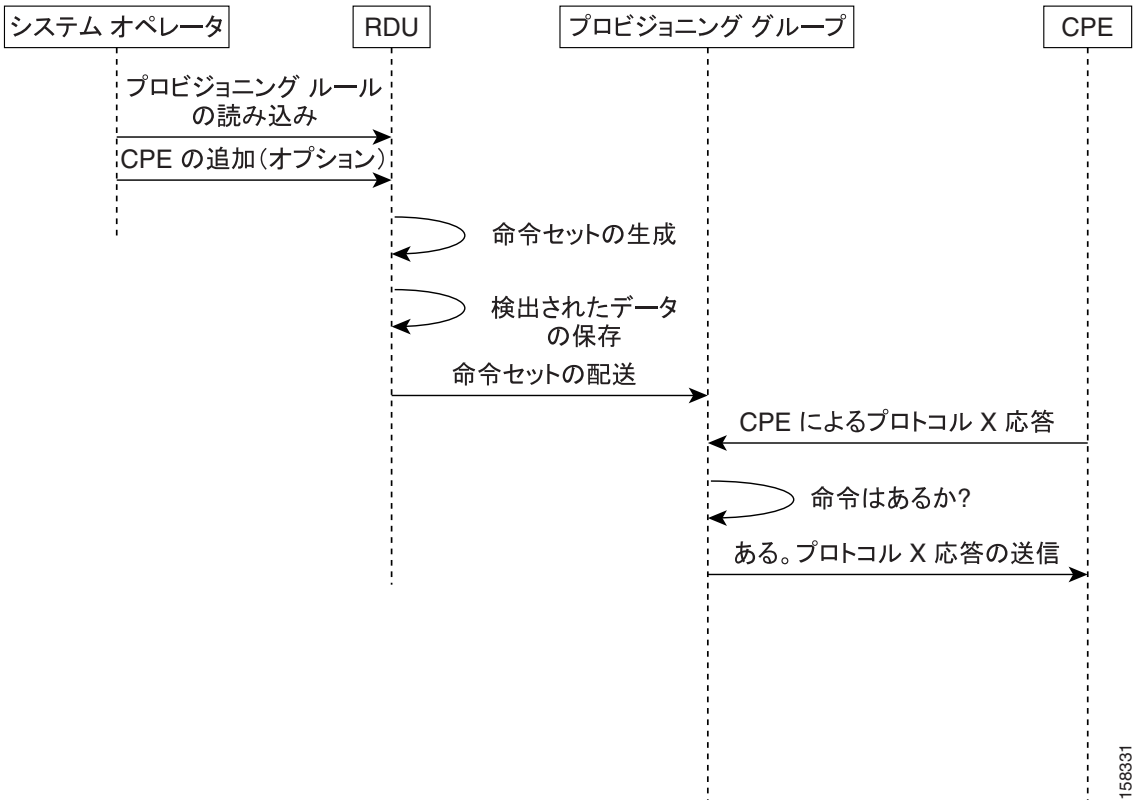
（注） 事前登録されたデバイス データを使用できない場合、不明なデバイスは認証されないため、DoS 攻撃を受ける確率が高くなります。

初期のプロビジョニング フロー

この項では、デバイスの設定ワークフローについて説明します。このワークフローは、事前登録されたデバイスであるか、登録解除されたデバイスであるかによって異なります。

図 4-2 は、共通的な初期の設定フローを示しています。

図 4-2　CPE の初期設定ワークフロー



事前登録されたデバイスの場合

a. BAC API から RDU に、さまざまなデバイス タイプ用に特別に定義された構成およびルールが読み込まれます。デバイスが事前設定され、サービス クラスに関連付けられます。

b. 事前設定されたデバイスが、事前設定された URL にある BAC サーバと交信して自分のプロビジョニング グループを特定し、プロビジョニング グループ サーバ（DPE）に対して自動プロビジョニングを開始します。

c. RDU が、デバイスに固有の命令を生成します。生成されるデバイス命令では、TR-069 Inform や HTTP ファイル要求など、さまざまな CPE プロトコル イベントに対する DPE 応答が指定されます。

d. デバイス命令セットが DPE に転送され、そこでキャッシュされます。この段階で、DPE は、このデバイスに対する以後の CPE プロトコル インタラクションを、RDU から独立して処理するようにプログラムされています。デバイスがネットワークに追加され、そのデバイスの構成が生成された場合、デバイスがブートすると、DPE は、事前登録されたデバイスとのインタラクションを開始できます。

e. デバイスとのインタラクションにおいて、追加情報を検出して RDU に転送することができます。この場合、RDU では、新しい命令を生成してすべての DPE に転送することがあります。

登録解除されたデバイスの場合

a. BAC API から RDU に、さまざまなデバイス タイプ用に特別に定義された構成およびルールが読み込まれます。

b. ブートアップ中、DPE はデバイス要求を受信すると、特定の CPE 用にキャッシュされている命令のローカル検索を実行します。CPE が以前にその DPE と交信したことがなく、デバイスデータが BAC に事前登録されていないため、命令は検出されません。次に、DPE は、関係する CPE 情報すべてを「命令セット」生成要求に組み込み、その要求を RDU に転送します。同時に、デバイス要求が拒否され、後でデバイスがリトライするようになります。

c. RDU が CPE に固有の命令を生成し、デバイスのプロビジョニング グループ内にあるすべての DPE に配送します。生成される CPE 命令では、TR-069 Inform や HTTP ファイル要求など、さまざまな CPE プロトコル イベントに対する DPE 応答が指定されます。

d. デバイス命令セットが DPE に配送され、そこでキャッシュされます。この段階で、DPE は、このデバイスに対する以後の CPE プロトコル インタラクションすべてを、RDU から独立して処理するようにプログラムされています。

不明なデバイスに関する次のパラメータが BAC によって検出されます。

- デバイス IP アドレスが、ルーティング可能か、または NAT されているか
- Inform.DeviceId.Manufacturer
- Inform.DeviceId.ManufacturerOUI
- Inform.DeviceId.ProductClass
- InternetGatewayDevice.DeviceInfo.HardwareVersion
- InternetGatewayDevice.DeviceInfo.SoftwareVersion
- InternetGatewayDevice.DeviceInfo.ModelName
- InternetGatewayDevice.ManagementServer.ParameterKey

（注） 検出されるパラメータのデフォルト　リストは変更できます。P.12-8 の「デバイスからのデータの検出」を参照してください。

e. デバイスが再接続し、デバイス用に生成された構成命令を RDU から受信し、DPE でキャッシュします。

プロビジョニング グループへのデバイスの割り当て

デバイスをプロビジョニング グループに割り当てる方法には、明示的、自動的、またはその両方を複合的に使用する方法の 3 つがあります。

明示的な割り当て

デバイスを明示的にプロビジョニング グループに割り当てることができます。デバイスがデフォルトのプロビジョニング グループに表示された場合、プロビジョニング システムでは、そのデバイスを API 経由で新しいプロビジョニング グループに割り当てることができます。BAC はそのデバイスと次に交信したときに、デバイスをリダイレクトします。

割り当てられたプロビジョニング グループと交信するようにデバイスを設定するには、BAC サーバの URL をプロビジョニング グループの URL に変更します。BAC サーバの URL が格納されます。それ以後、デバイスは新しいアドレスにある BAC と交信するようになります。

デバイスをプロビジョニング グループ間で移動するには、API または管理者のユーザ インターフェイスから、デバイスのホーム プロビジョニング グループを変更します。各プロビジョニング グループには URL が関連付けられています。次の交信時に、デバイスの ACS URL が新しいプロビジョニング グループの URL に変更されるため、簡単に移動できます。

ヒント　すべてのデバイスが最初にデフォルトのプロビジョニング グループと交信するように事前設定します。次に、リダイレクション機能を使用して、デバイスを適切なプロビジョニング グループに割り当てます。デバイスを別のプロビジョニング グループにリダイレクトするには、P.14-6 の「デバイスのプロビジョニング グループのリダイレクト」を参照してください。

自動メンバシップ

デバイスを明示的にプロビジョニング グループに割り当てない限り、そのデバイスは、最初に割り当てられたプロビジョニング グループからは移動されません。そのため、プロビジョニング グループへの CPE の割り当てを、ネットワークから指定できるようになります。デバイスを移動する場合は、自動メンバシップ機能を使用できます。この機能を使用すると、デバイスが移動しても、ローカル プロビジョニング グループからそのデバイスにサービスを提供できます。

デバイスが新しいプロビジョニング グループに表示された場合、デバイスはその新しいプロビジョニング グループに自動的に割り当てられ、デバイス データが古いプロビジョニング グループから削除されます。このプロセスでは、RDU との通信が行われます。その後、RDU は古いプロビジョニング グループと新しいプロビジョニング グループの両方で DPE を更新します。このプロセスは高負荷のため、多数のデバイスを移行しないように注意してください。

(注)　プロビジョニング　グループに対するデバイスの自動割り当てが動作するのは、どのプロビジョニング グループにも表示されない不明な（登録解除された）デバイスの自動割り当てを許可するように、DPE が設定されている場合だけです。デバイスが別のプロビジョニング グループに表示された場合、そのプロビジョニング グループが不明なデバイスによるアクセスを許可するように設定されているときは、BAC がデバイスをそのプロビジョニング グループに自動的に割り当てます。不明なデバイスのアクセス権を設定する方法の詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

複合的なアプローチ

デバイスの明示的な割り当てと、プロビジョニング グループへのデバイスの自動メンバシップを併用することができます。たとえば、登録解除された一般的なデバイスがネットワーク上でプロビジョニング グループ内に表示された場合、そのデバイスは自動的に割り当てられます。その後、OSS が API を使用して、そのデバイスを別のプロビジョニング グループに明示的に割り当てます。

デバイス診断

CWMP がサポートするデバイスのトラブルシューティングおよび診断機能を使用すると、1 つのデバイスに焦点を当てて診断情報を収集し、詳細に分析することができます。この機能では、デバイスに対して、次のデータを含む任意のデータをクエリーできます。

- 構成
- 稼働中の統計情報
- 障害表示
- ログ ファイル
- 診断結果

デバイス診断では、必ず、BAC がデバイスに対して一連の操作を実行します。これらの操作には次のものがあります。

- Reboot：デバイスをリブートします。このリブートは、主として診断用に使用されます。
- Request Connection：BAC に対する接続要求を開始します。
- Factory Reset：事前登録されたデバイス設定を、最初の工場出荷時の設定（加入者固有の設定が焼き付けられる前の設定）にリセットします。
- Display Live Data：デバイス パラメータをデバイスから直接表示します。表示するパラメータは指定可能です。
- Ping Diagnostic：CPE の IP アドレスに対して IP PING 診断テストを実行します。
- Force Firmware Upgrade：強制的に CPE のファームウェアを更新します。
- Force Configuration Synchronization：強制的に個々の CPE の構成を同期することができます。

これらのデバイス操作の実行に関する詳細については、P.16-16 の「デバイス操作の実行」を参照してください。

また、BAC には、トラブルシューティングを支援する次の機能もあります。

- デバイス履歴：デバイス プロビジョニングのライフサイクルで発生する重要なイベントの詳細な履歴を表示できます。P.8-1 の「デバイス履歴」を参照してください。
- デバイス障害：障害が繰り返し発生するデバイスを検出します。このような障害は、ボトルネックとなってネットワーク パフォーマンスに影響を及ぼす場合があります。P.8-7 の「デバイス障害」を参照してください。
- デバイスのトラブルシューティング：トラブルシューティング対象に指定された一連のデバイスに関する、デバイスと BAC サーバとのインタラクションの詳細なレコードを表示できます。P.8-10 の「デバイスのトラブルシューティング」を参照してください。
- パフォーマンス統計情報：主要なコンポーネント全体のシステム パフォーマンスに関連する詳細なパフォーマンス統計情報を表示できます。また、統計情報データを分析して、トラブルシューティングに役立てることもできます。P.11-14 の「パフォーマンス統計情報の監視」を参照してください。

設定テンプレートの管理

この章では、Broadband Access Center（BAC）でサポートされる、デバイス構成およびデバイス管理用のテンプレートについて説明します。この章は、次の項で構成されています。

概要

BAC 3.0 には、CPE WAN Management Protocol（CWMP）準拠のデバイスに構成を割り当てるための、拡張性のあるテンプレートベースのメカニズムがあります。このテンプレート処理メカニズムを使用すると、構成管理が簡素化されます。このメカニズムでは、少数のテンプレートを使用して、何百万という顧客宅内装置（CPE）の構成をカスタマイズすることができます。テンプレートの処理結果として、命令が生成されます。この命令は、デバイスのプロビジョニング グループ内の DPE に転送されます。この命令には、DPE がデバイスを構成するのに必要な情報がすべて含まれています。

独自のテンプレートを作成する前に、次の項目について十分に理解しておいてください。

- パラメータ辞書（P.7-1 の「パラメータ辞書」を参照）
- ファームウェア テンプレート（P.6-1 の「ファームウェア管理」を参照）

BAC テンプレートを使用して、読みやすい形式のテンプレート ファイルを作成し、迅速かつ簡単に編集することができます。サービス クラスでテンプレート ファイルを参照する前に、管理者のユーザ インターフェイスまたは API を使用して、そのファイルを RDU に追加しておく必要があります。

BAC テンプレートは、公開されているスキーマに従って記述された XML ドキュメントです。DPE に配送する特定のデバイス用の命令が RDU で生成される場合、共通のテンプレート プロセッサが、デバイスのサービス クラス オブジェクトを使用してテンプレートを取得します。このプロセッサは、次に、インクルードや条件などのテンプレート値を評価し、その値をテンプレート変数に代入します。その結果、処理されたテンプレートに相当する XML オブジェクトが出力されます。

処理された設定テンプレートを BAC システムに追加すると、その構文および内容が検証され、この XML テンプレートが整形式であることが確認されます。この検証では、パラメータの名前および値がパラメータ辞書内の定義と整合していることも確認されます。パラメータ辞書とは、サポートされるオブジェクトおよびパラメータを定義する XML ファイルです（P.7-1 の「パラメータ辞書」を参照してください）。

（注）この種の検証が行われるのは、テンプレートをシステムに追加した場合か、または既存のテンプレートの内容を置換した場合だけです。

BAC は、さまざまなファイルで定義されている XML スキーマを使用して、デバイス構成用の命令を生成します。表 5-1 は、これらのファイルとその場所を示しています。

表 5-1　設定テンプレートの処理に使用されるファイル

ファイル	目的	BAC で使用可能なオプション
設定テンプレートのサンプル	デバイス構成を定義する	サンプル テンプレート
	サンプル テンプレートは次の場所にあります。 *BPR_HOME/rdu/samples/cwmp*	
設定テンプレートスキーマ	設定テンプレートの構文を検証する	デフォルト テンプレート スキーマ
	デフォルト テンプレート スキーマは次の場所にあります。 • CWMP 構成スキーマ *BPR_HOME/rdu/templates/cwmp/schema/CwmpTemplateConstructs.xsd* • 共通テンプレート スキーマ *BPR_HOME/rdu/templates/cwmp/schema/CommonTemplateConstructs.xsd*	
パラメータ辞書	設定テンプレートの内容を検証する	デフォルト辞書 カスタム辞書
	デフォルト辞書は次の場所にあります。 • *BPR_HOME/rdu/templates/cwmp/dictionary/tr069-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/tr098-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/tr104-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/tr106-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/basic-cwmp-dictionary.xml*	
パラメータ辞書スキーマ	パラメータ辞書の構文を検証する	デフォルト辞書
	パラメータ辞書スキーマは次の場所にあります。 TR-069、TR-098、TR-104、および TR-106 辞書のスキーマ *BPR_HOME/rdu/templates/cwmp/schema/TemplateDictionarySchema.xsd*	

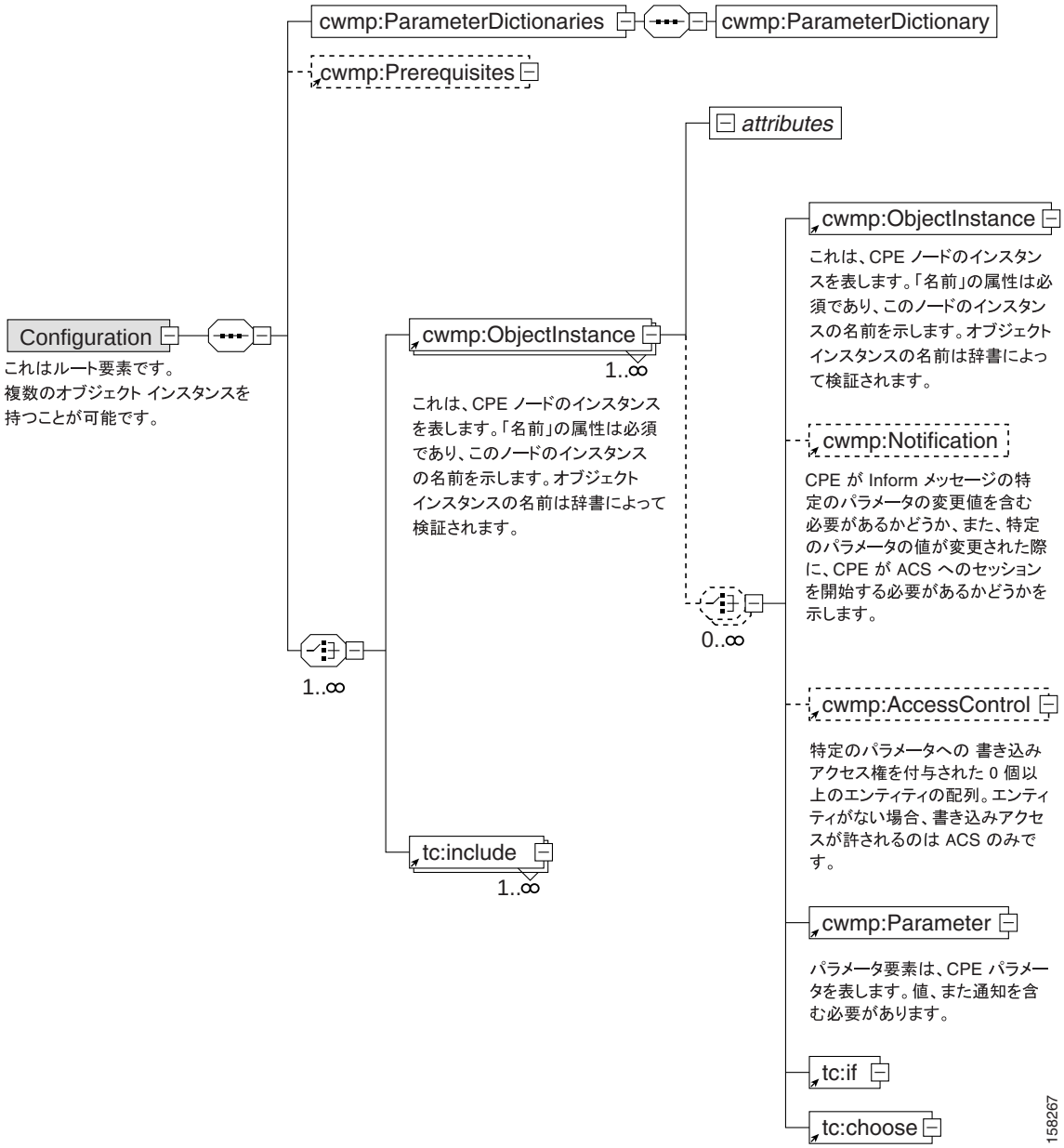
テンプレート ファイル（設定およびファームウェア ルール）を管理するには、管理者のユーザ インターフェイスを使用します。詳細については、P.17-13 の「ファイルの管理」を参照してください。

BAC テンプレートの機能

設定テンプレートとは、オブジェクトおよびパラメータの集合です。TR-069 デバイスでは、*InternetGatewayDevice* がルート オブジェクトですが、TR-106 では、*Device* がルート オブジェクトです。

図 5-1 は、TR-069 デバイス構成のスキーマを示しています。スキーマに登場する各要素については、次の各項で説明しています。

図 5-1　構成スキーマ



設定テンプレートは、次のコンポーネントで構成されます。

- **ObjectInstance**：TR-069 CPE ノードのインスタンスを表します。オブジェクトの「名前」を指定する必要があります。

  オブジェクトには、別のオブジェクトおよびパラメータを含めることができます。さらに、そのオブジェクトおよびパラメータにも、TR-069 仕様に従って別の要素を含めることができます。

  CPE オブジェクトには、次の要素を含めることができます。

  - Object：CPE ノードのインスタンスを表します。
  - Parameters：CPE パラメータを表します。値のほかに、Notification、Access Control、またはその両方を含める必要があります（P.5-5 の「パラメータ」を参照してください）。
  - Notification：このパラメータのすべてのレベルにあるすべての子パラメータについて、値の変更の通知をイネーブルにします（P.5-7 の「通知」を参照してください）。
  - Access Control：自動構成サーバ以外のエンティティ（ユーザ、SNMP、UPnP など）が、このオブジェクトの下にある任意の構成パラメータの値を変更できるかどうかを制御します（P.5-8 の「アクセス コントロール」を参照してください）。
- **Parameter Dictionary**：設定テンプレート内のオブジェクトおよびパラメータを検証するのに使用される定義が含まれています。BAC でサポートされる辞書は、テンプレートごとに 1 つだけです（P.7-1 の「パラメータ辞書」を参照してください）。
- **Prerequisites**：（オプション）デバイスを構成する前に満たされている必要がある条件を示します。この条件には、次の要素を含めることができます。
  - MaintenanceWindow：構成をデバイスに適用する時間を指定できます。
  - Expressions：構成を適用するための前提条件としてデバイス上のパラメータと一致している必要がある任意のパラメータを指定できます（たとえば、デバイスの特定のソフトウェアまたはハードウェア バージョン）。

  前提条件スキーマの図については、図 5-3 を参照してください。前提条件オプションの使用方法の詳細については、P.5-9 の「前提条件」を参照してください。

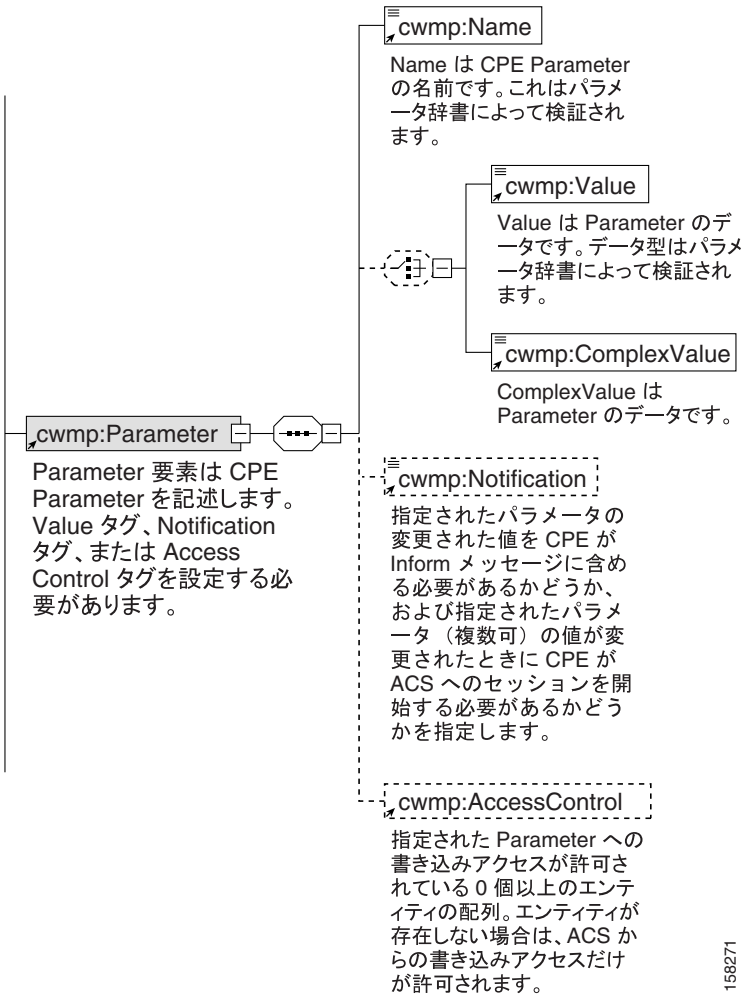
（注） 設定テンプレートにエラーが存在すると、そのテンプレートを BAC に追加する操作は失敗します。構成エラーを回避するため、次の事項をすべて確認してください。

- オブジェクト名とパラメータ名がパラメータ辞書に存在している。
- パラメータ値が、パラメータ辞書で指定されたタイプになっている。
- 書き込み可能でないパラメータに、値が設定されていない。ただし、Notification　属性または Access Control 属性（あるいは両方）を設定することはできます。
- システムで BAC カスタム プロパティまたはデバイス プロパティを通じて、代入可能な変数が定義されている。

パラメータ

この項では、設定テンプレート内のパラメータ オブジェクトに関連付けられたスキーマについて説明します（図 5-2 を参照）。

図 5-2　パラメータ スキーマ



CPE パラメータには、名前と値のペアが含まれます。

名前は、パラメータを識別します。また、ディレクトリ内のファイルと同様の階層構造を持ち、各レベルがドット（.）で区切られています。各レベルは、オブジェクト インスタンスに対応します。オブジェクトには、単一インスタンス（シングルトン）を持つものもあれば、複数インスタンスを持つものもあります。両方のオブジェクト インスタンスのパラメータ リストについては、次の各項で説明しています。

パラメータの値には、TR-069 仕様で定義されたデータ タイプのいずれかを指定できます。このデータ タイプには、**string**、**int**、**unsignedInt**、**boolean**、**dateTime**、および **base64** があり、いずれもパラメータ辞書によって検証されます（データ タイプの定義については、表 7-1 を参照してください）。

例 5-1 は、パラメータ値の設定方法を示しています。

例 5-1　パラメータ値の設定

```
<tc:Template
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:tc="urn:com:cisco:bac:common-template"
xmlns="urn:com:cisco:bac:cwmp-template"
xsi:schemaLocation="urn:com:cisco:bac:common-template CommonTemplateConstructs.xsd">

 <Configuration>
  <ParameterDictionaries>
    <ParameterDictionary>tr069-cwmp-dictionary.xml</ParameterDictionary>
  </ParameterDictionaries>
  <ObjectInstance name="InternetGatewayDevice">
    <ObjectInstance name="ManagementServer">
      <Parameter>
        <Name>PeriodicInformEnable</Name>
        <Value>true</Value>
      </Parameter>
      <Parameter>
        <Name>PeriodicInformInterval</Name>
        <Value>86400</Value>
      </Parameter>
    </ObjectInstance>
  </ObjectInstance>
 </Configuration>
</tc:Template>
```

単一インスタンス オブジェクトのパラメータ リスト

次の例は、単一インスタンス（シングルトン）を示しています。

```
InternetGatewayDevice.UserInterface.
```

シングルトンのパラメータは、次のように表すことができます。

```
InternetGatewayDevice.UserInterface.PasswordRequired = true
InternetGatewayDevice.UserInterface.ISPName = SBC
```

複数インスタンス オブジェクトのパラメータ リスト

TR-069 仕様では、複数インスタンスを持ち、各インスタンスに番号を割り当てることのできるオブジェクトが定義されています。複数インスタンスを持つことのできるオブジェクトを定義するには、パラメータ辞書を使用します。

たとえば、`InternetGatewayDevice.Layer3Forwarding.Forwarding` は複数インスタンス オブジェクトです。

このオブジェクトの 2 つのインスタンスは、次のように表すことができます。

```
InternetGatewayDevice.Layer3Forwarding.Forwarding.1.Enable = true
InternetGatewayDevice.Layer3Forwarding.Forwarding.2.Enable = false
```

（注） インスタンス番号はデバイスによって生成されます。パラメータ辞書は、複数インスタンスを持つことのできるオブジェクトを表すときに {i} を使用します。設定テンプレートでは、実際のインスタンス番号を使用して、編集するオブジェクトを示す必要があります（たとえば、`InternetGatewayDevice.WANDevice.1.WANConnectionNumberOfEntries`）。

通知

BAC の Notification 属性を使用すると、デバイスがパラメータ値の変更を DPE に通知できるようになります。通知は、デフォルトでオフになっています。

通知をイネーブルにすると、デバイスは、特定のパラメータの変更値を DPE へのデバイス Inform メッセージに含めるように指定され、さらに特定のパラメータの値が変更されたときは必ず DPE へのセッションを開始するように指定されます。

BAC では、TR-069 仕様で定義されたとおり、次に示す Notification 属性の値がサポートされています。

- `Off`：通知はオフに設定されます。

  デバイスは、指定されたパラメータの変更を BAC に通知する必要がなくなります。
- `Passive`：通知は Passive に設定されます。

  指定されたパラメータの値が変更されるたびに、デバイスは、Inform　メッセージ内の ParameterList に新しい値を含める必要があります。このメッセージは、BAC が次にセッションを確立したときに送信されます。
- `Active`：通知は Active に設定されます。

  指定されたパラメータの値が変更されるたびに、デバイスは、BAC とのセッションを開始し、関連付けられた Inform メッセージ内の ParameterList に新しい値を含める必要があります。パラメータの変更が 0 以外の通知設定によって Inform メッセージで送信されるたびに、Event コードの `4 VALUE CHANGE` を Events リストに含める必要があります。

（注） 特定のパラメータに通知を設定しようとしたときに、その設定が不適切と見なされた場合（たとえば、設定対象が、連続的に変化する統計の場合）、デバイスは `notification request rejected` エラーを返します。

通知の設定

次の例は、Notification 属性の設定方法を示しています。

この例では、UserInterface オブジェクトの設定ファイルを定義および生成し、すべてのパラメータに対して通知を Active に設定します。ISPName パラメータは、この通知設定を無効にして Passive に設定します。

```
<!--Set Notification of object InternetGatewayDevice.UserInterface.-->

<ObjectInstance name="InternetGatewayDevice">
    <ObjectInstance name="UserInterface">
            <Notification>Active</Notification> <!-- applies to all parameters under
this
                                                        object -->
            <Parameter>
                <Name>PasswordRequired</Name>
                <Value>true</Value>
            </Parameter>
            <Parameter>
                <Name>WarrantyDate</Name>
                <Value>2001-02-23T09:45:30+04:30</Value>
            </Parameter>
            <Parameter>
                <Name>ISPName</Name>
                <Value>SBC</Value>
                <Notification>Passive</Notification> <!--applies to only this
parameter-->
            </Parameter>
            <Parameter>
                <Name>ISPHomePage</Name>
                <Value>www.sbc.com</Value>
            </Parameter>
    </ObjectInstance>
</ObjectInstance>
```

アクセス コントロール

BAC のアクセス コントロールは、CPE の *AccessControl* 属性を通じてイネーブルになります。この属性は、設定テンプレートを使用して制御できます。CPE パラメータの変更は、変更アクセスを許可するようにアクセス コントロールが設定されていれば、LAN 自動構成プロトコルを介して行うことができます。たとえば、*AccessControl* 属性が Subscriber に設定されていれば、LAN 上の加入者はパラメータ値を変更できます。

AccessControl 属性の値は、特定のパラメータへの write アクセス権が付与されたエンティティを 0 個以上配列したものになります。エンティティが示されていない場合、BAC から実行できるのはパラメータ値の更新だけです。BAC では、TR-069 仕様に従って、このリストで Subscriber エンティティだけを定義します。その結果、LAN 上の加入者は、LAN 側の DSL CPE Configuration プロトコルや UPnP プロトコルなどを介して、write アクセスを実行できるようになります。

アクセス コントロールの設定

次の例は、BAC で設定テンプレートを使用してアクセス コントロールを設定する方法を示しています。

```
    <ObjectInstance name="InternetGatewayDevice">
            <ObjectInstance name="ManagementServer">
                <AccessControl>  <!--Allow LAN-side updates of this object and
parameters under it -->
                        <Entity>Subscriber</Entity>
                </AccessControl>
                <Parameter>
                    <Name>PeriodicInformEnable</Name>
                    <Value>true</Value>
                </Parameter>

                <Parameter>
                    <Name>PeriodicInformEnable</Name>
                    <AccessControl/>   <!-- Allow updates only from ACS (BAC) -->
                </Parameter>
            </ObjectInstance>
        </ObjectInstance>
```

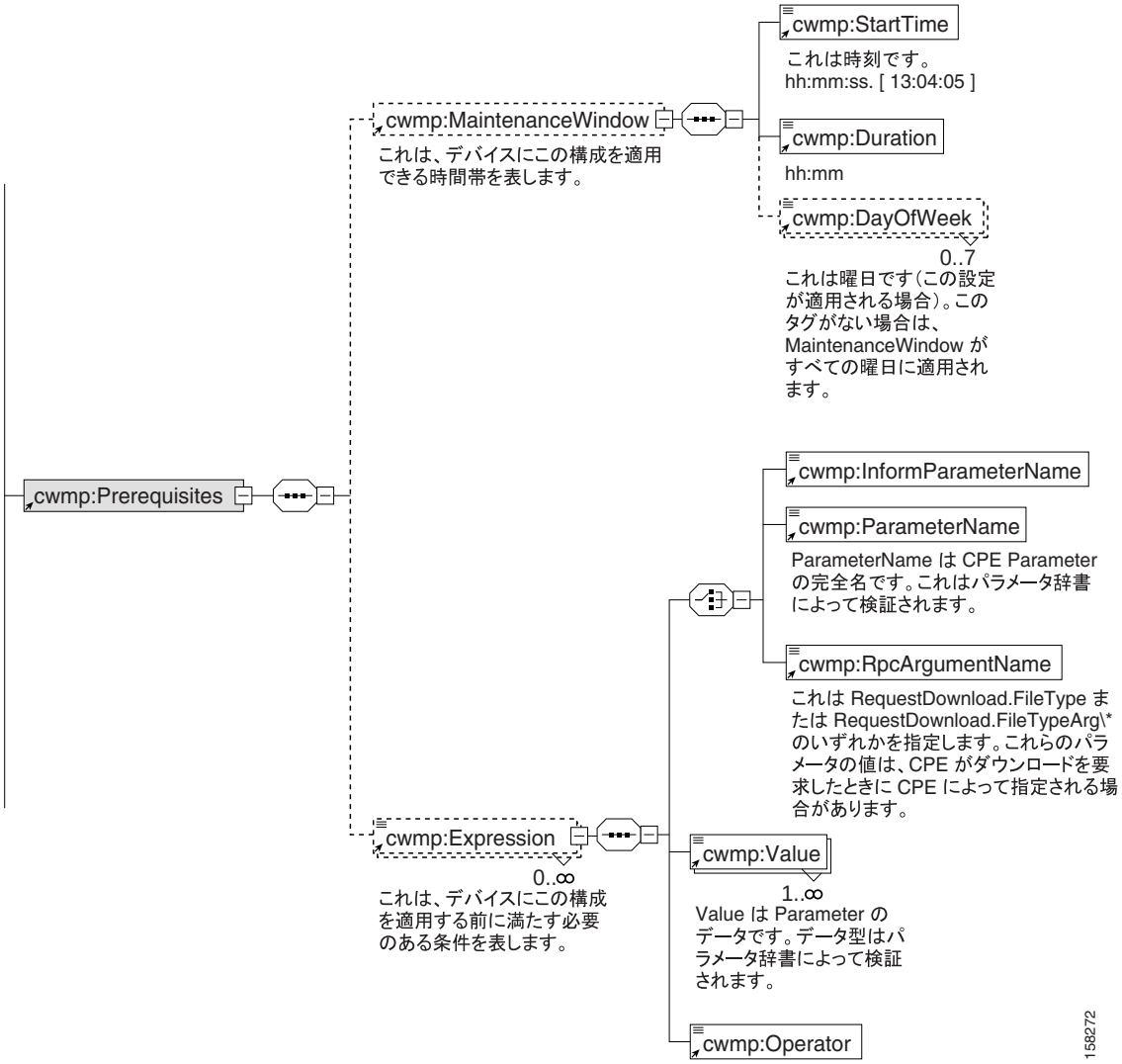
前提条件

BAC テンプレートには、前提条件オプションが含まれます。このオプションは、デバイスを構成するに前に満たされている必要がある条件を示します。たとえば、前提条件として、構成を適用するデバイスが特定のハードウェアまたはソフトウェア バージョンの要件を満たす必要があることを指定できます。

前提条件ルールは、命令に組み込まれ、DPE に送信されます。次に、DPE が、必要に応じてデバイスに問い合せ、前提条件が一致するかどうかを判別します。

図 5-3 は、前提条件オプションのスキーマを示しています。

図 5-3　前提条件スキーマ



前提条件を使用すると、次の要素によって構成の生成を操作することができます。

- Expressions
- MaintenanceWindow

式

式は、デバイス プロパティの情報を使用する条件となります。式には、Parameters、InformParameters、または rpcArguments を使用できます。式は、前提条件とファームウェア ルールの内部で使用され、デバイスが BAC と交信して構成を取得するときに処理されます。指定した式が *true* と評価された場合、条件は満たされ、対応する構成またはファームウェア ルールがデバイスに適用されます。詳細については、P.5-19 の「条件の使用方法」を参照してください。

Prerequisites タグには、式を 0 個以上含めることができます。

MaintenanceWindow

MaintenanceWindow 設定を使用すると、特定の構成を特定の CPE に適用する期間を指定できます。この評価は、デバイス交信時に DPE で実行され、その結果に応じて DPE ローカル時間が使用されます。

(注) DPE が動作するサーバに、タイム サーバ（NTP など）との自動同期を設定しておく必要があります。

MaintenanceWindow は次の要素で構成されます。

- *StartTime*：保守期間の開始を示す時間値を指定します。この値は、*hh:mm:ss* として定義されます。
- *Duration*：構成を適用できる *StartTime* からの期間を示す時間値を指定します。この値は、*hh:mm* として定義されます。
- *DayOfWeek*：構成を適用できる曜日を指定します。このタグがない場合は、すべての曜日でルールが有効になります。このタグはオプションです。

これらの要素を使用すると、このルールを実行できる期間を指定できるため、構成のアップグレード作業を、加入者が就寝している可能性が最も高い深夜に実行するように制限できます。

Prerequisites タグには、0 個または 1 個の MaintenanceWindow を含めることができます。

例 5-2　MaintenanceWindow の設定

次の例では、*StartTime*、*Duration*、および *DayOfWeek* タグの値によって、このルールが有効になる期間を定義しています。このテンプレートは、毎週月曜、火曜、および金曜の午前 1 時から 5 時間にわたって有効になります。

```
<Prerequisites>
    <MaintenanceWindow>
        <StartTime>01:00:00</StartTime>
        <Duration>05:00</Duration>
        <DayOfWeek>Monday</DayOfWeek>
        <DayOfWeek>Tuesday</DayOfWeek>
        <DayOfWeek>Friday</DayOfWeek>
    </MaintenanceWindow>
<Prerequisites>
```

MaintenanceWindow 期間のデバイス交信

MaintenanceWindow には、その期間にデバイスが BAC と交信することを保証するという重要な概念があります。

特定の日時に DPE と交信するようにデバイスを構成するには、設定テンプレートで *PeriodicInformTime* 変数の値を設定します。さらに、*RandomDateTimeInRange* タグで、デバイスが BAC と交信できる期間を指定します。

MaintenanceWindow 期間に BAC と交信するようにデバイスを設定する方法については、例 5-3 を参照してください。

例 5-3　MaintenanceWindow 期間に BAC と交信するためのデバイスの設定

次の例では、2007 年 1 月 1 日の午前 3 ～ 4 時にデバイスが初めて BAC と交信します。最初の交信後、デバイスは引き続き 30 分ごとに BAC と交信します。

- デバイスが Inform メソッド コールを使用してデバイス情報を BAC に定期的に送信することを示すため、`PeriodicInformEnable` を *true* に設定します。
- 30 分ごとに BAC との交信を試みるようデバイスに要求するため、`PeriodicInformInterval` を 30 分（1,800 秒）に設定します。この期間は、`PeriodicInformEnable` が *true* の場合に、デバイスが BAC との交信を試みる時間間隔となります。
- `PeriodicInformTime` には、デバイスが BAC との交信を開始する日付および時刻を設定します。

```
<ObjectInstance name="InternetGatewayDevice">
    <ObjectInstance name="ManagementServer">
            <Parameter>
                <Name>PeriodicInformEnable</Name>
                <Value>true</Value>
            </Parameter>
            <Parameter>
                <Name>PeriodicInformInterval</Name>
                <Value>1800</Value>
            </Parameter>
            <Parameter>
                <Name>PeriodicInformTime</Name>
                <ComplexValue>
                    <RandomDateTimeInRange>
                    <StartDateTime>
                        2006-01-27T01:00:00Z+03:00
                    </StartDateTime>
                    RandomizationIntervalMinutes>
                        60
                    </RandomizationIntervalMinutes>
                </RandomDateTimeInRange>
            </ComplexValue>
        </Parameter>
    </ObjectInstance>
</ObjectInstance>
```

PeriodicInformInterval の詳細については、DSL Forum の TR-069 に関する Technical Report を参照してください。

(注) ファームウェアのアップグレードも同様の方法で開始できます。ファームウェアのアップグレードが実行されるのは、通常、特定の期間だけです。MaintenanceWindow オプションを設定してファームウェア ルール テンプレートを定義したら、管理者のユーザ インターフェイスを使用してファームウェア ルール テンプレートをサービス クラス オブジェクトに関連付けます。この作業が完了すると、ファームウェア ルールが DPE にプッシュされます。DPE は、ファームウェア ルールを評価し、ファームウェア アップグレードが特定の期間に確実に実行されるようにします。

前提条件の設定

この項では、前提条件オプションの設定方法について説明します。

例 5-4　前提条件の設定

この例で、前提条件は、午前 1 時から 5 時間にわたってこのテンプレートが有効になることを示しています。このテンプレートは、この期間に BAC と交信するデバイスのうち、`EventCode` が *1 BOOT* に、製造元が *Acme, Inc* に設定されているデバイスすべてに適用できます。

```
<Prerequisites>
    <MaintenanceWindow>
        <StartTime>01:00:00</StartTime>
        <Duration>5:00</Duration>
    </MaintenanceWindow>
    <Expression>
        <InformParameterName>InternetGatewayDevice.DeviceInfo.EventCode</
        InformParameterName>
        <Value>1 BOOT</Value>
        <Operator>match</Operator>
    </Expression>
    <Expression>
        <ParameterName>InternetGatewayDevice.DeviceInfo.Manufacturer</ParameterName>
        <Value>Acme, Inc</Value>
        <Operator>matchIgnoreCase</Operator>
    </Expression>
 </Prerequisites>
```

設定テンプレートのオーサリング

BAC では、テンプレート構成体を使用して、1 つのテンプレートから多数のデバイス用にカスタマイズされた構成を作成するための命令を生成することができます。テンプレートからカスタム構成を作成するには、パラメータ代入や、テンプレートの内容に関する条件付きのインクルードまたは除外を使用します。これらの機能は、BAC プロパティ階層の値によって制御されます。テンプレートには他のテンプレートを含めることができます。このメカニズムにより、共通の構成を再利用できます。

サービス クラスでテンプレート ファイルを参照する前に、管理者のユーザ インターフェイスまたは API を使用して、そのファイルを RDU に追加しておく必要があります。

(注) テンプレート内の XML 要素は、次の 2 つのグループに分類されます。

- 先頭に **tc** が付いていない要素は、設定テンプレートに固有のものです。
- 先頭に **tc** が付いている要素は、設定テンプレートとファームウェア ルール テンプレートに共通した汎用構成体です。

ルート要素として `Configuration` を含む設定テンプレートは、例 5-5 のような構造に従う必要があります。

例 5-5　サンプルの設定テンプレート

```
<tc:Template
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:tc="urn:com:cisco:bac:common-template"
xmlns="urn:com:cisco:bac:cwmp-template"
xsi:schemaLocation="urn:com:cisco:bac:common-template CommonTemplateConstructs.xsd">


<Prerequisites>
    <MaintenanceWindow>
        <StartTime>01:00:00</StartTime>
        <Duration>2:30</Duration>
    </MaintenanceWindow>
    <Expression>
        <ParameterName>InternetGatewayDevice.DeviceInfo.Manufacturer</ParameterName>
        <Value>Acme, Inc</Value>
        <Operator>matchIgnoreCase</Operator>
    </Expression>
 </Prerequisites>
 <Configuration>
  <ParameterDictionaries>
    <ParameterDictionary>tr069-cwmp-dictionary.xml</ParameterDictionary>
  </ParameterDictionaries>
  <ObjectInstance name="InternetGatewayDevice">
    <ObjectInstance name="ManagementServer">
      <Parameter>
        <Name>PeriodicInformEnable</Name>
        <Value>true</Value>
      </Parameter>
      <Parameter>
        <Name>PeriodicInformInterval</Name>
        <Value>86400</Value>
      </Parameter>
    </ObjectInstance>
  </ObjectInstance>
 </Configuration>
</tc:Template>
```

設定テンプレートでは次の機能がサポートされています。

- パラメータ代入：VAR() 構成体を使用して、BAC プロパティ階層から XML 要素内容および要素属性に値を代入します（詳細については、P.5-16 の「パラメータ代入の使用方法」を参照してください）。
- インクルード：再利用可能なテンプレートの抜粋集を作成します。インクルードを使用すると、多くのサービス クラスで共通のオプションを定義する場合に、複数のテンプレートでオプションを重複させる必要がなくなり、便利です（詳細については、P.5-17 の「インクルードの使用方法」を参照してください）。
- 条件：テンプレートの内部でテキスト ブロックを含めるか、または除外します。条件文で囲むことのできるテキスト ブロックは、パラメータおよびオブジェクト インスタンス要素に制限されています（詳細については、P.5-19 の「条件の使用方法」を参照してください）。

カスタム プロパティ

BAC のプロパティを使用すると、API を介して、BAC に格納されているデータにアクセスできます。対応するオブジェクトのプロパティを使用し、API を介して、事前プロビジョニングされたデータ、検出されたデータ、およびステータス データを取得することができます。また、プロパティを使用すると、BAC を適切な粒度で（システム レベルからデバイス グループおよび個々のデバイスのレベルまで）設定できます。詳細については、P.4-4 の「プロパティ階層」を参照してください。

カスタム プロパティを使用すると、RDU データベースに保存される追加のカスタマイズ可能なデバイス情報を定義できます。カスタム プロパティは、通常、設定テンプレートおよびファームウェア ルール テンプレートにパラメータ値を代入するときに使用します。テンプレート パーサーは、階層の下から上にプロパティを検索し（最初はデバイス、次にプロビジョニング グループ、サービス クラス、デバイス タイプ、およびシステム デフォルトの順）、テンプレート オプション構文に変換します。VAR() 構成体を使用したテンプレート パラメータの代入の詳細については、次の項を参照してください。

例 5-6　デバイスからのユーザ名またはパスワードの取得

次の例は、テンプレートを使用して、さまざまなレベルからプロパティを取得する方法を示しています。たとえば、デバイスから資格情報のユーザ名とパスワードを取得します。

```
<tc:Template>
    <Configuration>
        <ParameterDictionaries>
            <ParameterDictionary>tr069-cwmp-dictionary.xml</ParameterDictionary>
        </ParameterDictionaries>
        <ObjectInstance name="InternetGatewayDevice">
            <ObjectInstance name="ManagementServer">
                <Parameter>
                    <Name>PeriodicInformEnable</Name>
                    <Value>true</Value>
                </Parameter>
                <Parameter>
                    <Name>PeriodicInformInterval</Name>
                    <Value>20</Value>
                    <Notification>Active</Notification>
                </Parameter>
                <Parameter>
                    <Name>ConnectionRequestUsername</Name>
                    <Value>VAR(name=/dt/username, defaultValue="User")</Value>
                </Parameter>
                <Parameter>
                    <Name>ConnectionRequestURL</Name>
                    <Value>VAR(name=/dt/pk, defaultValue="http://testURL")</Value>
                </Parameter>
            </ObjectInstance>
        </ObjectInstance>
    </Configuration>
</tc:Template>
```

管理者のユーザ インターフェイスからカスタム プロパティを設定するには、**Configuration > Custom Property** タブの順に選択します。Add Custom Property ページを使用して、カスタム プロパティを追加または削除します。詳細については、P.17-7 の「カスタム プロパティの設定」を参照してください。

注意　テンプレートが参照するカスタム プロパティを削除すると、RDU がデバイス用の命令の生成に失敗します。

パラメータ代入の使用方法

設定テンプレートからカスタム構成を作成するには、VAR() 構成体を使用して、BAC プロパティ階層からテンプレートに値を代入します。VAR() 構成体は、XML 要素値または要素属性の中に表示できます。また、この構成体を使用して、すべてまたは一部の値を代入することもできます。

次のリストは、BAC でサポートされている、パラメータ代入用の構成体を示しています。

- XML 要素内容に代入する BAC プロパティ値
- XML 要素属性に代入する BAC プロパティ値
- デフォルト値
- 部分的な XML 要素内容
- 特殊文字を含む値

構文の説明

```
VAR(token=someChar, name=someProperty, defaultValue=someValue)
```

- *token*：後続のフィールドを区切る文字を指定します。この要素はオプションで、デフォルトではカンマ（,）に設定されています。

（注）　デフォルト値にカンマ（,）が含まれている場合は、VAR() 構成体を開始するときに、トークン文字を指定してください。このトークンは、デフォルト値の中に表示されないものにする必要があります。また、トークン文字の後ろに VAR 終了ブラケットがあることを確認してください。

- *name*：代入するカスタム プロパティの名前、または参照する Standard Device プロパティの名前を指定します。
- *defaultValue*：参照するプロパティを使用できない場合に使用する値を指定します。

例 5-7　BAC カスタム プロパティへの値の設定

```
<Value>VAR(name=/cpe/version, defaultValue=4)</Value>
```

例 5-8　Standard Device プロパティの参照

```
<Value>VAR(name=/IPDevice/connectionRequestPath, defaultValue="http://test")</Value>
```

（注）　/IPDevice/connectionRequestPath の API 定数は、IPDeviceKeys.CONNECTION_REQUEST_PATH です。

例 5-9　*defaultValue* とカンマの併用

```
<Value>VAR(token=;;name=/cpe/usrStr; defaultValue=4,5;)</Value>
```

例 5-10　BAC プロパティに基づいた文字列値の作成

```
<Value>CWMP_VAR(name=/cpe/version, defaultValue=4).bin</Value>
```

`cpe/version` が `1-08` の場合、値は `CWMP_1-08.bin` になります。

インクルードの使用方法

インクルード ファイルを使用すると、再利用可能なテンプレートの抜粋集を作成できます。このファイルを使用すると、多くのサービス クラスで共通のオプションを定義する場合に、複数のテンプレートでオプションを重複させる必要がなくなり、便利です。

特定のファイルの内容をテンプレートに含めるには、**tc:include** 構成体を使用します。インクルードするファイルの内容をホスト テンプレートに挿入すると、ホスト テンプレートで指定されたパラメータ辞書によって、挿入後のテンプレートの内容が検証されます。

（注） インクルードするテンプレートで使用されているオブジェクトおよびパラメータが、ホスト　テンプレートと同じ辞書で定義されていない場合は、命令の生成中にパラメータの検証が失敗します。

tc:Include 要素は *href* 属性を指定します。*href* は、ホスト テンプレートにインクルードする BAC テンプレート ファイルの名前を示します。テンプレートでインクルード ディレクティブを使用する場合は、二重引用符（"）を使用します。

（注） インクルード　ファイルとテンプレートのファイル　タイプが一致していることを確認してください。たとえば、設定テンプレートを追加する場合は、インクルードするファイルすべてが Configuration Template ファイル タイプになっている必要があります。

例 5-11　インクルード ファイル

次の例は、ホスト テンプレートと、インクルードするテンプレートの内容を示しています。

インクルードするテンプレート：*informInterval.xml*

```
<!-- enable and set Periodic Inform value -->
<tc:Template :xsi="http://www.w3.org/2001/XMLSchema-instance"
:tc="urn:com:cisco:bac:common-template" ="urn:com:cisco:bac:cwmp-template"
:schemaLocation="urn:com:cisco:bac:common-template CommonTemplateConstructs.xsd">
    <Configuration>
        <ParameterDictionaries>
            <ParameterDictionary>tr069-cwmp-dictionary.xml</ParameterDictionary>
        </ParameterDictionaries>
        <ObjectInstance name="InternetGatewayDevice">
            <ObjectInstance name="ManagementServer">
                <Parameter>
                    <Name>PeriodicInformEnable</Name>
                    <Value>true</Value>
                </Parameter>
                <Parameter>
                    <Name>PeriodicInformInterval</Name>
                    <Value>30</Value>
                </Parameter>
            </ObjectInstance>
        </ObjectInstance>
    </Configuration>
</tc:Template>
```

ホスト テンプレート：*cwmp-config.xml*

```
<!-- set Periodic Inform value based on content of informInterval-cwmp.xml -->
<!-- set ManagmentServer.URL -->
<tc:Template :xsi="http://www.w3.org/2001/XMLSchema-instance"
:tc="urn:com:cisco:bac:common-template" ="urn:com:cisco:bac:cwmp-template"
:schemaLocation="urn:com:cisco:bac:common-template CommonTemplateConstructs.xsd">
<Configuration>
        <ParameterDictionaries>
            <ParameterDictionary>tr069-cwmp-dictionary.xml</ParameterDictionary>
        </ParameterDictionaries>
        <tc:include href="informInterval.xml"/>
        <ObjectInstance name="InternetGatewayDevice">
            <ObjectInstance name="ManagementServer">
                <Parameter>
                    <Name>URL</Name>
                    <Value>http://10.44.64.200:9595/acs</Value>
                </Parameter>
            </ObjectInstance>
        </ObjectInstance>

    </Configuration>
</tc:Template>
```

インクルードするファイルを挿入した後のテンプレート：*informInterval.xml*

```
<!-- set ManagmentServer.URL -->
<tc:Template :xsi="http://www.w3.org/2001/XMLSchema-instance"
:tc="urn:com:cisco:bac:common-template" ="urn:com:cisco:bac:cwmp-template"
:schemaLocation="urn:com:cisco:bac:common-template CommonTemplateConstructs.xsd">
    <Configuration>
        <ParameterDictionaries>
            <ParameterDictionary>tr069-cwmp-dictionary.xml</ParameterDictionary>
        </ParameterDictionaries>
        <ObjectInstance name="InternetGatewayDevice">
            <ObjectInstance name="ManagementServer">
                <Parameter>
                    <Name>PeriodicInformEnable</Name>
                    <Value>true</Value>
                </Parameter>
                <Parameter>
                    <Name>PeriodicInformInterval</Name>
                    <Value>30</Value>
                </Parameter>
            </ObjectInstance>
        </ObjectInstance>
        <ObjectInstance name="InternetGatewayDevice">
            <ObjectInstance name="ManagementServer">
                <Parameter>
                    <Name>URL</Name>
                    <Value>http:// 10.44.64.200:9595/acs</Value>
                </Parameter>
            </ObjectInstance>
        </ObjectInstance>
    </Configuration>
</tc:Template>
```

条件の使用方法

BAC では、テンプレート構成体の強力な条件式を使用して、構成の最終的なカスタマイズを行うことができます。

条件式の構成体を使用すると、テンプレートの内部でテキスト ブロックを含めるか、または除外することができます。この構成体の要素は、**tc:if**、**tc:choose**、および **tc:when** です。**tc:if** 構成体は、単純な単一条件の場合に使用します。論理的な **if...else if...else** 構成体の場合は、**tc:choose**、**tc:when**、および **tc:otherwise** の組み合せを使用します。**tc:if** および **tc:when** 構成体には、*test* 属性が必要です。*test* 属性とは、評価可能な式のことで、結果のオブジェクトは、ブール演算子（*true* または *false*）に変換できます。

tc:choose 要素は、想定された選択肢の中から 1 つを選択します。この要素には、一連の **tc:when** 要素と、それに続くオプションの **tc:otherwise** 要素が含まれます。各 **tc:when** 要素は、単一属性の *test* を持ちます。この属性は、式を指定します。

tc:when 要素と **tc:otherwise** 要素の内容は、有効なテンプレート セグメントです。**tc:choose** 要素が処理されると、次に、各 **tc:when** 要素がテストされます。このテストでは、式が評価され、結果のオブジェクトがブール演算子に変換されます。テストで true となった最初の **tc:when** 要素の内容だけがインスタンス化されます。**tc:when** が true にならなかった場合は、**tc:otherwise** 要素の内容がインスタンス化されます。**tc:when** 要素が true にならなかった場合、**tc:otherwise** 要素が示されていないときは、何も作成されません。

（注）式の内部でリテラル文字列を区切るには、一重引用符（'）または二重引用符（"）を使用します。ただし、テンプレート プロセッサは、引用符（' または "）を属性の終端として解釈します。この問題を避けるため、引用符は文字参照（" または '）として入力します（表 5-2 を参照してください）。一方、属性を二重引用符（"）で区切る場合は、式の内部で一重引用符（'）を使用できます（その逆も可能です）。

表 5-2 は、この BAC リリースでサポートされる条件テンプレート構成体を示しています。

表 5-2　BAC でサポートされる条件テンプレート構成体

条件文	If
条件文	If...else if...else
条件文	or
条件式	and
条件式	lessThan
条件式	lessThanEqual
条件式	greaterThan
条件式	greaterThanEqual
条件式	contains、notContains
条件式	containsIgnoreCase、notContainsIgnoreCase
条件式	equals、notEquals
条件式	equalsIgnoreCase、notEqualsIgnoreCase

XML では、左山カッコ（<）とアンパサンド（&）はサポートされていません。代わりに、定義済みのエンティティ（表 5-3 を参照）を使用してください。

表 5-3　BAC における XML 定義

サポートされていない文字	代用エンティティ
<（小なり）	<
<=（小なりまたは等しい）	<=
>（大なり）	>
>=（大なりまたは等しい）	>=
&（アンパサンド）	&
'（アポストロフィ）	'
"（二重引用符）	"

次の例は、さまざまな条件式を示しています。

例 5-12　数値のテスト条件

数値として 100 を使用：

```
<tc:if test="VAR(name=/cpe/version, defaultValue=20) > 100">
    <Parameter>
        <Name>Enable </Name>
        <Value>false</Value>
    </Parameter>
</tc:if>
```

例 5-13　文字列のテスト条件

文字列として 100 を使用：

```
<tc:if test="VAR(name=/cpe/version, defaultValue=20) > '100'">
    <Parameter>
        <Name>Enable </Name>
        <Value>false</Value>
    </Parameter>
</tc:if>
```

（注） 両者を数値として比較した場合、20 は 100 よりも「小なり」です。しかし、演算子（>）と文字列を組み合せて、文字列として比較した場合、20 は 100 よりも「大なり」(>)となります。

例 5-14　BAC プロパティ内のテキスト検索

テキストとして cwmp を使用：

```
<tc:if test="contains(VAR(name=/cpe/UsrStr, defaultValue=linksys), 'cwmp')">
    <Parameter>
        <Name>Enable </Name>
        <Value>false</Value>
    </Parameter>
</tc:if>
```

例 5-15　一重引用符を含むテキストの検索

cwmp’s test を使用：

```
<tc:if test="contains(VAR(name=/cpe/UsrStr, defaultValue=linksys), &quot;cwmp's
test&quot;)">
    <Parameter>
        <Name>Enable</Name>
        <Value>false</Value>
    </Parameter>
</tc:if>
```

例 5-16　二重引用符を含むテキストの検索

cwmp *test* を使用：

```
<tc:if test="contains(VAR(name=/cpe/UsrStr, defaultValue=linksys), 'cwmp
&quot;test&quot;')">
    <Parameter>
        <Name>Enable </Name>
        <Value>false</Value>
    </Parameter>
</tc:if>
```

条件文で囲むことのできるテキスト ブロックは、Parameter 要素と Object 要素に制限されています

例 5-17　選択肢からの選択

次の例は、**tc:choose** と **tc:when** を使用する場合の構文を示しています。

```
<tc:choose>
        <tc:when test="VAR(name=/cpe/version,defaultValue=11) > 12">
            <Parameter>
                <Name>UpgradeAvailable</Name>
                <Value>true</Value>
            </Parameter>
        </tc:when>
        <tc:when test="VAR(name=/db/version,defaultValue=15) > 14">
            <Parameter>
                <Name>UpgradeAvailable</Name>
                <Value>true</Value>
            </Parameter>
        </tc:when>
        <tc:otherwise>
            <Parameter>
                <Name>UpgradeAvailable</Name>
                <Value>false</Value>
            </Parameter>
        </tc:otherwise>
</tc:choose>
```

設定ユーティリティの使用方法

設定ユーティリティを使用すると、TR-069 テンプレート ファイル（設定およびファームウェア ルール）のテスト、検証、および表示を行うことができます。これらの作業は、独自の設定ファイルに関する命令を正常に展開するために重要です（テンプレートの詳細については、P.5-14 の「設定テンプレートのオーサリング」を参照してください）。

設定ユーティリティは、RDU をインストールし、ユーティリティを *BPR_HOME/rdu/bin* ディレクトリにインストールしたときにのみ利用可能です。

この項のすべての例では、RDU が運用中で、次の条件が適用されていることを前提にしています。

- BAC アプリケーションは、ホームディレクトリ（*/opt/CSCObac*）にインストールされています。
- RDU ログイン名は **admin** です。
- RDU ログイン パスワードは **changeme** です。

（注）この項の例では、一部が出力例にとって重要でない場合に、その部分を省略して切り詰めていることがあります。その場合は、例中のサマリーの直前に省略記号（...）を示しています。

この項では、次のトピックについて取り上げます。

設定ユーティリティの実行

以降の手順と例で、「設定ユーティリティを実行する」というフレーズは、指定されたディレクトリから **runCfgUtil.sh** コマンドを入力することを意味します。設定ユーティリティを実行するには、*BPR_HOME/rdu/bin* ディレクトリから次のコマンドを実行します。

```
runCfgUtil.sh options
```

利用可能な *options* は、次のとおりです。

- **-cwmp**：入力ファイルを CWMP 技術の設定テンプレート ファイルとして処理することを指定します。-cwmp は -a オプションと一緒に使用します。
- **-a** {**sc** | **gc**}：必要なアクションを指定します。次のどちらかを指定できます。
  - **sc**：構文チェックで XML テンプレートおよび辞書が整形式であるかどうかをテストするように指定します。**sc** は **–l** オプションと一緒に使用します。
  - **gc**：Instruction Generation Service（IGS）と同じ方法で設定テンプレートを処理します。**gc** は、（**–l** および **–data**）オプションまたは（**-l** および **-i**）オプションと一緒に使用します。
- **-l** *filename*：入力ファイルがローカル ファイル システムにあることを示します。たとえば、入力ファイルの名前が *any_file* の場合は、**-l any_file** と入力します。

（注）　**-l** を **-r** オプションと同時に使用することはできません。

- **-o** *filename*：テンプレート処理の出力を XML 形式で指定のファイルに保存します。たとえば、出力を *op_file* という名前のファイルに保存するには、**-o op_file** と入力します。この要素はオプションです。
- **-i** *device id*：テンプレートの処理中に変数代入用に使用するデバイスを指定します。変数値は、デバイスのプロパティを使用して取得されます。このオプションは **-r** オプションと一緒に使用します。
- **-r** *filename*：RDU に格納されているテンプレートの名前を指定します。このオプションは、**-l** オプションの代わりに使用します。
- **-u** *username*：RDU に接続するときに使用するユーザ名を指定します。
- **-p** *password*：RDU に接続するときに使用するパスワードを指定します。
- **-firmware**：入力ファイルがファームウェア ルール テンプレートであることを指定します。このオプションがない場合は、設定テンプレートと見なされます。

BAC へのテンプレートの追加

設定ユーティリティを使用して、BAC テンプレートをテストするには、次の手順に従います。

ステップ 1　P.5-14 の「設定テンプレートのオーサリング」の説明に従い、テンプレートを作成します。テンプレートに他のテンプレートを含める場合は、参照されるテンプレートすべてが同一のディレクトリにあることを確認します。

ステップ 2　ローカル ファイル システムで設定ユーティリティを実行します。テンプレートの構文をチェックするか、または IGS と同じ方法で設定ユーティリティにテンプレートを処理させた後、XML 出力を返すことができます。

処理するテンプレートが VAR() 構成体を使用してデバイス プロパティを参照する場合、結果の出力には、その VAR() 構成体の defaultValue が含まれます。

ステップ 3　テンプレート（および、そのテンプレートにインクルードするテンプレート）を RDU に追加します。

テンプレートが VAR() 構成体を使用してデバイス プロパティを参照する場合は、デバイス オプションを使用してサンプル テンプレートを生成します。

ステップ 4　テストが成功したら、そのテンプレートを使用するサービス クラスを設定します。

ローカル テンプレート ファイルの XML 構文の検証

runCfgUtil.sh コマンドを使用して、ローカル ファイル システムに格納されているテンプレート ファイルを検証します。

構文の説明

```
runCfgUtil.sh -cwmp -a sc -l file
```

- **-cwmp**：入力ファイルを CWMP テンプレート ファイルとして処理することを示します。
- **-a sc**：構文チェックを指定します。
- **-l**：入力ファイルがローカル ファイル システムにあることを指定します。
- *file*：検証する入力テンプレート ファイルを示します。

ローカル ファイル システムにあるテンプレート ファイルを使用するには、次の手順に従います。

ステップ 1　*/opt/CSCObac/rdu/samples/cwmp* にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。

（注）　この例では、*sample-cwmp-config.xml* という既存のテンプレート ファイルを使用します。これは CWMP テンプレートであるため、**-cwmp** オプションを使用します。

ステップ 3　次のコマンドを使用して、設定ユーティリティを実行します。

```
/opt/CSCObac/rdu/bin/runCfgUtil.sh -cwmp -a sc -l sample-cwmp-config.xml
```

- **-cwmp**：入力ファイルを CWMP テンプレート ファイルとして処理することを示します。
- **-l**：入力ファイルがローカル ファイル システムにあることを指定します。
- **sample-cwmp-config.xml**：検証する入力テンプレート ファイルを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Broadband Access Center Configuration Utility
Version: 3.0, Revision: 1.26
validating configuration template sample-cwmp-config.xml...
>sample-cwmp-config.xml is valid.
```

BAC に格納されているテンプレートの XML 構文の検証

runCfgUtil.sh コマンドを使用して、RDU データベースに格納されているテンプレート ファイルを検証します。

構文の説明

runCfgUtil.sh -cwmp -a sc -r *file* **-u** *username* **-p** *password*

- **-cwmp**：入力ファイルを CWMP テンプレート ファイルとして処理することを示します。
- **-a sc**：構文チェックを指定します。
- **-r** *file*：入力ファイルが RDU に追加したファイルであることを示します。
- **-u** *username*：RDU に接続するときに使用するユーザ名を指定します。
- **-p** *password*：RDU に接続するときに使用するパスワードを指定します。

RDU に追加したテンプレート ファイルを検証するには、次の手順に従います。

ステップ 1　*/opt/CSCObac/rdu/samples/cwmp* にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。

（注）　この例では、*sample-cwmp-config.xml*　という既存のテンプレート　ファイルを使用します。CWMP テンプレートを使用するため、**-cwmp** オプションを使用します。

ステップ 3　次のコマンドを使用して、設定ユーティリティを実行します。

```
./runCfgUtil.sh -cwmp -a sc -r sample-cwmp-config.xml -u admin -p changeme
```

- **sample-cwmp-config.xml**：入力ファイルを示します。
- **admin**：ユーザ名を示します。
- **changeme**：パスワードを示します。
- **-cwmp**：ファイルを CWMP テンプレートとして処理することを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Broadband Access Center Configuration Utility
Version: 3.0, Revision: 1.26
validating configuration template sample-cwmp-config.xml...
>sample-cwmp-config.xml is valid.
```

ローカル テンプレート ファイルのテンプレート処理のテスト

runCfgUtil.sh コマンドを使用して、ローカル テンプレート ファイルのテンプレート処理をテストします。

構文の説明

runCfgUtil.sh -cwmp -a gc -l *file* **-o** *file*

- **-cwmp**：入力ファイルを CWMP テンプレート ファイルとして処理することを示します。
- **-a gc**：構成の生成に関する命令を指定します。
- **-l** *file*：入力ファイルがローカル ファイル システムにあることを指定します。
- **-o** *file*：処理されたテンプレートを XML 形式で指定のファイルに保存することを指定します。

ローカル テンプレート ファイルのテンプレート処理をテストするには、次の手順に従います。

ステップ 1　*/opt/CSCObac/rdu/samples/cwmp* にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。この例では、*sample-cwmp-config.xml* という既存のテンプレート ファイルを使用します。

ステップ 3　次のコマンドを使用して、設定ユーティリティを実行します。

```
./opt/CSCObac/rdu/bin/runCfgUtil.sh -cwmp -a gc -l sample-cwmp-config.xml -o
output.xml
```

- **sample-cwmp-config.xml**：入力ファイルを示します。
- **output.xml**：処理されたテンプレートを XML 形式で保存するファイルを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Broadband Access Center Configuration Utility
Version: 3.0, Revision: 1.26
generating configuration from sample-cwmp-config.xml...
output.xml generated successfully.
```

output.xml ファイルを開いて、構成を表示することができます。

BAC に格納されているテンプレートのテンプレート処理のテスト

runCfgUtil.sh コマンドを使用して、RDU データベース内のテンプレートのテンプレート処理をテストします。

構文の説明

runCfgUtil.sh -cwmp -a gc -r *file* **-o** *file* **-u** *username* **-p** *password*

- **-cwmp**：入力ファイルを CWMP テンプレート ファイルとして処理することを示します。
- **-a gc**：構成の生成に関する命令を指定します。
- **-r** *file*：入力ファイルが RDU に追加したファイルであることを示します。
- **-o** *file*：処理されたテンプレートを XML 形式で指定のファイルに保存することを指定します。
- **-u** *username*：RDU に接続するときに使用するユーザ名を指定します。
- **-p** *password*：RDU に接続するときに使用するパスワードを指定します。

BAC に格納されているテンプレートのテンプレート処理をテストするには、次の手順に従います。

ステップ 1　*/opt/CSCObac/rdu/samples/cwmp* にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。この例では、*sample-cwmp-config.xml* という既存のテンプレート ファイルを使用します。

ステップ 3　次のコマンドを使用して、設定ユーティリティを実行します。

```
./runCfgUtil.sh -cwmp -a sc -r sample-cwmp-config.xml -o output.xml -u admin -p
changeme
```

- **sample-cwmp-config.xml**：入力ファイルを示します。
- **output.xml**：生成された構成を XML 形式で保存するファイルを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Broadband Access Center Configuration Utility
Version: 3.0, Revision: 1.26
generating configuration from sample-cwmp-config.xml...
output.xml generated successfully.
```

output.xml ファイルを開いて、構成を表示することができます。

BAC テンプレート ファイルとデバイスのテンプレート処理のテスト

runCfgUtil.sh コマンドを使用して、RDU データベースに格納されている、デバイスに関連付けられたファイルのテンプレート処理をテストします。

構文の説明

runCfgUtil.sh -cwmp -a gc -r *file* **-o** *file* **-i** *deviceID* **-u** *username* **-p** *password*

- **-cwmp**：入力ファイルを CWMP テンプレート ファイルとして処理することを示します。
- **-a gc**：構成の生成に関する命令を指定します。
- **-r** *file*：入力ファイルが RDU に追加したファイルであることを示します。
- **-o** *file*：処理されたテンプレートを XML 形式で指定のファイルに保存することを指定します。
- **-i** *deviceID*：使用するデバイスを指定します。変数値は、デバイスのプロパティを使用して取得されます。
- **-u** *username*：RDU に接続するときに使用するユーザ名を指定します。
- **-p** *password*：RDU に接続するときに使用するパスワードを指定します。

RDU に格納されている、デバイスに関連付けられたファイルのテンプレート処理をテストするには、次の手順に従います。

ステップ 1　管理者のユーザ インターフェイスを使用して、*/opt/CSCObac/rdu/samples/cwmp/sample-cwmp-var-config.xml* というテンプレート ファイルを BAC に追加します。

（注）　*sample-cwmp-var-config.xml* テンプレートには、/IPDevice/connectionRequestUsername デバイス プロパティへの参照が含まれています。プロパティの API 定数は、`IPDeviceKeys.CONNECTION_REQUEST_USERNAME` です。

ステップ 2　使用するテンプレート ファイルを選択します。この例では、*sample-cwmp-var-config.xml* という既存のテンプレート ファイルを使用します。

ステップ 3　BAC にすでに存在するデバイスを特定し、そのデバイスの ID を使用します。この例では、/IPDevice/connectionRequestUsername プロパティが *testUser* に設定されたデバイスを使用します。

ステップ 4　使用するデバイスを調べます。この例では、デバイスが RDU に存在し、変数がプロパティとして設定されているものとします。

ステップ 5　次のコマンドを使用して、設定ユーティリティを実行します。

```
./runCfgUtil.sh -cwmp -a gc -r sample-cwmp-var-config.xml -i OUI-1234 -o output.xml -u
admin -p changeme
```

- **sample-cwmp-var-config.xml**：入力ファイルを示します。
- **OUI-1234**：デバイスの ID を示します。このデバイス ID は、例として示す目的でのみ使用しています。
- **output.xml**：処理されたテンプレートを XML 形式で保存するファイルを示します。
- **admin**：この例で使用するデフォルトのユーザ名を示します。
- **changeme**：この例で使用するデフォルトのパスワードを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Broadband Access Center Configuration Utility
Version: 3.0, Revision: 1.26
generating configuration from sample-cwmp-var-config.xml...
output.xml generated successfully.
```

（注） *output.xml* ファイルを開いて、構成を表示することができます。
`VAR(name=/IPDevice/connectionRequestUsername, defaultValue=test)` 文は、*testUser* で置き換えられます。

ファームウェア管理

この章では、Broadband Access Center（BAC）における TR-069 準拠のデバイスのファームウェア管理について説明します。この章は、次の項で構成されています。

概要

ファームウェア管理では、一連のファームウェア イメージ ファイルの保守、および BAC システムから対応する顧客宅内装置（CPE）への配送を行います。ファームウェア ルール テンプレートにより、ファームウェア イメージ ファイルは、デバイス グループに関連付けられます。BAC は、関連付けられたファームウェア ルール テンプレート内のルールを使用して、デバイスにダウンロードするファームウェアを評価します。

ファームウェア管理機能を使用すると、デバイスのファームウェア情報を表示すること、ファームウェア イメージをデータベースに追加すること、およびイメージ ファイルを特定のデバイスに適用することができます。

BAC では、CPE ファームウェア管理用に、次の 2 つのメカニズムがサポートされています。

- ファームウェア ルール テンプレートを介したポリシーベースのファームウェア管理
- デバイス操作 API を介した直接的なファームウェア管理

  詳細については、P.6-3 の「ファームウェア ルール テンプレート」および P.6-5 の「直接的なファームウェア管理」を参照してください。

ファームウェア管理のプロセスでは、使用する管理方式に関係なく、デバイスは、ファイル サーバから新しいファームウェア イメージを取得するように指示されます。BAC は DPE にファイル サービスを提供します。ただし、CPE を他のファイル サーバに誘導することもできます。

ファームウェア ルールでは、事前プロビジョニングされた、または検出されたデバイス パラメータの一致に基づいて、ファームウェアをデバイスに適用できます。デバイス パラメータには、デバイス グループ メンバシップ、モデル、タイプ、現在の状態、および接続タイプなどがあります。DPE はファームウェアのダウンロードをトリガーするときに、ファイル サーバ上のファイルの場所と、認証の資格情報（ある場合）を使用して、Download RPC を実行します。BAC では、DPE サーバでのファイル ダウンロード用に、HTTP と HTTP over SSL（この章では SSL/TLS と呼ぶ）がサポートされています。

このダウンロードは、次のさまざまな方法で開始できます。

- ファームウェア ルール ベース。この方法では、デバイスが要求したファイルのダウンロードが、ファームウェア ルールによって許可または拒否されます。場合によっては、別のファイルがダウンロードされることもあります。ファームウェア ルールは、デバイスが DPE に接続するたびに実行されます。
- デバイスが、リブート後または特定のアクション後に定期的に DPE と交信する。特定のアクションには、デバイスのローカル ユーザ インターフェイスでユーザがボタンをクリックして開始するアップグレードなどがあります。デバイスが DPE と交信する方法に関係なく、ファームウェア ルールが実行され、特定のインタラクションの実行時にアップグレードが必要かどうか、および許可されるかどうかが判別されます。
- プロキシ。この方法では、外部アプリケーションが、特定のデバイス用に API ダウンロード操作を呼び出し、ファームウェア イメージ ファイルの場所を指定します。次に、DPE がデバイスに対して Download RPC を実行すると、デバイスが指定された場所からファイルをダウンロードします。

  ダウンロードは、次のどちらかの方法で行われます。

  — 即時。この方法では、DPE がデバイスに接続し、デバイスに対してファームウェアのダウンロードを指示します。

  — 接続時。この方法では、DPE がデバイスと次に交信したときに、デバイスに対してファームウェアのダウンロードを指示します。

ファームウェア管理メカニズム

この項では、BAC の CPE ファームウェア管理メカニズムについて説明します。このメカニズムは、次の要素で構成されています。

- ファームウェア ルール テンプレートを介したポリシーベースのファームウェア管理詳細については、P.6-3 の「ファームウェア ルール テンプレート」を参照してください。
- プロキシ操作を介した外部ファームウェア管理詳細については、P.6-5 の「直接的なファームウェア管理」を参照してください。

ファームウェア ルール テンプレート

ポリシーベースのファームウェア管理を設定するには、ルール テンプレートを使用します。ファームウェア ルール テンプレートは、公開されているスキーマ ドキュメントに従って記述された XML ドキュメントです。各テンプレートは、ファイルに格納して BAC にアップロードする必要があります。

各ファームウェア ルール テンプレートには、特定の条件に基づいてファームウェア更新をトリガーするルールが 1 つ以上含まれます。このテンプレートは、いくつでも、管理者のユーザ インターフェイスまたは API を介して BAC に追加できます。テンプレートは、`COS_CWMP_FIRMWARE_RULES_FILE` プロパティを介して、サービス クラス オブジェクトに関連付けられます。次に、各デバイスがサービス クラスに割り当てられます（BAC オブジェクトの関連付けについては、P.4-2 の「BAC デバイス オブジェクト モデル」を参照してください）。

このモデルでは、便利な方法でルールの定義を更新できます。ルールの定義は、多数のデバイスに適用されます。ルール テンプレートを更新すると、サービス クラスを介して間接的にテンプレートに関連付けられている CPE が、新しいポリシーに従って管理されます。

デバイスが BAC との接続を確立すると、デバイスのファームウェアと構成が、DPE にキャッシュされている構成およびファームウェア ルールに基づいて、自動的に同期されます。最初に、ファームウェア ルールが実行され、必要に応じてデバイスのファームウェアが更新されます。次に、デバイスの構成が同期されます。

BAC のファームウェア ルール処理は 2 段階に分かれています。最初に、RDU でテンプレートが処理され、条件や代入可能パラメータなどのテンプレート構成体が解釈されます（P.6-14 の「ファームウェア ルール テンプレートに対するテンプレート構成体の使用方法」を参照）。この処理では、RDU で使用できるデータ（デバイス プロパティやグループ）に基づいて、デバイスのルールをカスタマイズできます。このデータを事前プロビジョニングする場合は、API を使用します。RDU で以前にデバイスから検出され、格納されたデータも、テンプレートの構成に使用できます。テンプレートが処理されると、結果のルールが、デバイスのプロビジョニング グループ内の DPE に送信されます。このルールに動的な一致基準を設定すると、ファームウェア ルール ポリシーをより細分化できます。

ファームウェアの更新が必要かどうかを判別するため、DPE のルール エンジンがファームウェア ルールを評価します。ファームウェア ルールでは、次の基準が一致したときにファームウェアの更新をトリガーできます。

- Inform のイベント タイプ
- デバイスの RequestDownloadRPC 引数
- Inform のパラメータ値
- それ以外のデバイス パラメータの値
- MaintenanceWindow 期間

（注）デバイスへのファームウェアのダウンロードをスケジュール設定するには、MaintenanceWindow オプションを使用します。詳細については、P.5-11 の「MaintenanceWindow 期間のデバイス交信」を参照してください。

また、このルールには、ファームウェア管理用のポリシーを作成する強力なメカニズムがあります。たとえば、管理者は、現行のファームウェア バージョンを持つ特定モデルのデバイスすべてを、特定のサービス期間に別のファームウェアにアップグレードさせるルールを記述できます。

DPE は、ルールを使用したファームウェア選択のすべてのケースについて、エントリをログに記録します。また、ルールが一致しない場合も、エントリをログに記録します。このロギング メカニズムは、ファームウェア イメージ ファイルが関連付けられていないデバイスをトラッキングする場合や、単純にデバイス ファームウェアを最新状態にする場合に役立つことがあります。

BAC は、さまざまなファイルで定義されている XML スキーマを使用して、デバイス構成用の命令を生成します。表 6-1 は、これらのファイルとその場所を示しています。

表 6-1　ファームウェア ルールのテンプレート処理で使用されるファイル

ファイル	目的	BAC で使用可能なオプション
ファームウェア ルール テンプレートのサンプル	デバイス構成を定義する	サンプル テンプレート
	サンプル テンプレートは次の場所にあります。 *BPR_HOME/rdu/samples/cwmp*	
ファームウェア ルール テンプレート スキーマ	ファームウェア ルール テンプレートの構文を検証する	デフォルト テンプレート スキーマ
	デフォルト テンプレート スキーマは次の場所にあります。 • ファームウェア ルール テンプレート スキーマ *BPR_HOME/rdu/templates/cwmp/schema/FirmwareTemplateSchema.xsd* • 共通テンプレート スキーマ *BPR_HOME/rdu/templates/cwmp/schema/CommonTemplateConstructs.xsd*	
パラメータ辞書	ファームウェア ルール テンプレートの内容を検証する	デフォルト辞書
	デフォルト辞書は次の場所にあります。 • *BPR_HOME/rdu/templates/cwmp/dictionary/tr069-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/tr098-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/tr104-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/tr106-cwmp-dictionary.xml* • *BPR_HOME/rdu/templates/cwmp/dictionary/basic-cwmp-dictionary.xml*	
パラメータ辞書スキーマ	パラメータ辞書の構文を検証する	デフォルト辞書
	パラメータ辞書スキーマは次の場所にあります。 TR-069、TR-098、TR-104、および TR-106 辞書のスキーマ *BPR_HOME/rdu/templates/cwmp/schema/TemplateDictionarySchema.xsd*	

直接的なファームウェア管理

BAC のデバイス操作 API を使用すると、OSS が個々のデバイスに対して操作を実行できるようになります。BAC では、特に、標準の CWMP RPC 操作を実行できます。

デバイス操作 API を介してファームウェアを管理する場合、OSS では、CPE に対して実行する操作を精密に制御できます。OSS は、CPE のファームウェア更新に必要なリモート プロシージャ コール（RPC）に対応する特定の API コールを実行します。

たとえば、デバイスに対して Download RPC を呼び出すときは、対応する API コールが使用されます。このコマンドには、デバイスでダウンロードするファームウェア イメージ ファイルの URL のほか、必要に応じて認証の資格情報が含まれます。

デバイス操作の詳細については、P.14-1 の「CWMP デバイス操作」を参照してください。

ファイル サービス

ファームウェア管理のプロセスでは、使用する管理方式に関係なく、デバイスは、ファイル サーバから新しいファームウェア ファイルを取得するように指示されます。BAC は DPE サーバにファイル サービスを提供します。ただし、必要に応じて、CPE を他のファイル サーバに誘導することもできます。BAC でサポートされる各種の設定オプションについては、P.12-2 の「CWMP サービスの設定値」を参照してください。

ファームウェア ファイルの管理

ファームウェア ファイルの管理では、ファームウェア イメージ ファイルとファームウェア ルール テンプレート ファイルを管理します。この機能を使用すると、管理者やアプリケーションが API を使用して、ファームウェア イメージ ファイルとファームウェア ルール テンプレート ファイルの追加、削除、または置換を行うことや、ファームウェア イメージ ファイルとファイル情報を表示および検索することができます。ファームウェアの管理は、管理者のユーザ インターフェイスまたは API から行います。管理者のユーザ インターフェイスでファームウェア イメージ ファイルとファームウェア ルール テンプレートを管理するには、**Configuration** > **Files** の順に選択します。

ファームウェア ルール テンプレート ファイルは、デバイスのファームウェア イメージを特定します。このファイルは、`Firmware Rules Template` というファイル タイプで RDU データベースに格納されます。

ファームウェア イメージ ファイルは、`Firmware File` というファイル タイプで RDU データベースに格納されます。各ファームウェア イメージ ファイルには、`Firmware Version` 属性によって指定されたファームウェア バージョンが含まれます。DPE は、このファームウェア バージョン情報を使用して、ファームウェア ルールを評価します。

（注） ファームウェア イメージを中央サーバ（RDU）から管理すると、そのイメージは適切な DPE から自動的に配送または削除されます。

ファームウェア ファイルの管理では、ファイル タイプごとに次の操作を実行できます。

表 6-2　ファームウェア ファイルの管理操作

ファームウェア イメージ ファイル	ファームウェア ルール テンプレート
追加	追加 **（注）** ファームウェア ルール テンプレート ファイルをシステムに追加できるのは、このテンプレートが妥当な場合だけです。妥当でない場合、BAC は、テンプレートのエラー タイプを説明するエラー メッセージを表示します。
削除 **（注）** 既存のファームウェア イメージ ファイルがファームウェア ルール テンプレートで参照されている場合、そのファイルは削除できません。ファームウェア イメージ ファイルを正常に削除するには、ファームウェア ルール テンプレートから、そのファームウェア ファイルへの参照を削除してください。	削除 **（注）** ファームウェア ルール テンプレートがサービス クラスによって参照されている場合、そのテンプレートは削除できません。ファームウェア ルール テンプレートを正常に削除するには、そのサービス クラスへの参照を削除してください。
内容の取得	内容の取得
ファイル属性（サイズ、名前、プロパティなど）の取得	-

表 6-2　ファームウェア ファイルの管理操作（続き）

ファームウェア イメージ ファイル	ファームウェア ルール テンプレート
内容の置換またはファイル属性 / プロパティの変更（あるいは両方） （注）既存のファームウェア イメージ ファイルの置換は、そのファイルが API を介してファームウェア ファイル テンプレートに関連付けられていても実行できます。ただし、管理者のユーザ インターフェイスでは、ファームウェア イメージ ファイルを置換する前に、関連付けが存在することが通知されます。 ファームウェア イメージ ファイルの内容を置換すると、IGS によって、影響を受けるデバイスごとにファームウェア ルールが再生成され、そのルールがデバイスのプロビジョニング グループ内の DPE に配送されます。その後、デバイスが DPE と交信すると、新しいルールが実行されます。	ファイルの内容の置換またはファイルの属性およびプロパティの変更（あるいは両方）
名前、サフィックス、またはファイル タイプによる検索	-
-	管理者のユーザ インターフェイスからの、表形式のテンプレートの表示 （注）テンプレートが表形式で表示されるのは、テンプレートに条件が含まれていない場合だけです。

ファームウェア ルール テンプレートのオーサリング

BAC のファームウェア ルール テンプレートは、XML スキーマ ファイルに基づいています。このスキーマ ファイルは、*BPR_HOME/rdu/templates/cwmp/schema/FirmwareTemplateSchema.xsd* にあります。

ファームウェア ルールが実行されるのは、デバイスからの Inform が処理された後です。また、ルールの実行は、デバイスが RequestDownload RPC を実行した後にもトリガーされます。

ファームウェア ルール テンプレートは、次の要素で構成されます。

FirmwareTemplate：ルート要素。この要素には、1 つの Prerequisites タグと、1 つ以上の名前付き FirmwareRule 要素を含めることができます。

（注） ファームウェア ルールは順番に処理されます。ファームウェア ルールが一致した場合、それ以降のルールは処理されません。

- **Prerequisites**：ファームウェア ルール テンプレート内のルールを処理する前に満たされている必要がある条件が含まれます。前提条件には、0 個または 1 個の MaintenanceWindow、および 0 個以上の Expression を含めることができます。

  （注） ファームウェア テンプレートに対して Expression と MaintenanceWindow をイネーブルにする方法は、設定テンプレートの場合と同じです。

  - MaintenanceWindow：ファームウェア ルール テンプレートの処理が有効となる期間を表します。詳細については、P.5-9 の「前提条件」を参照してください。
  - Expression：このルールを評価するための 0 個以上の式。構文と定義は、*FirmwareRule* 要素で指定されている Expression と同じです。詳細については、P.6-9 の「Expression」を参照してください。
- **FirmwareRule**：各 FirmwareRule 要素には次の要素が含まれます。
  - Expression：このルールを評価するための 0 個以上の式。特定のルールに含まれているすべての式が一致した場合、ルールがファームウェア更新をトリガーします。詳細については、P.6-9 の「Expression」を参照してください。
  - InternalFirmwareFile または ExternalFirmwareFile：このどちらかを指定する必要があります。
  - InternalFirmwareFile を使用するのは、BAC ファイル サービスを使用し、API または管理者のユーザ インターフェイスを介してファームウェア イメージ ファイルをシステムに追加した場合です。
  - ExternalFirmwareFile は、外部ファイル サーバ上にあるファームウェア イメージ ファイルの情報を表します。

  詳細については、P.6-11 の「内部ファームウェア ファイルと外部ファームウェア ファイルの比較」を参照してください。

Expression

Expression は、テスト条件を表します。各 Expression には、*ParameterName*、*InformParameterName* または *RpcArgumentName* タグ、1 つ以上の *Value* タグ、および *Operator* タグを含める必要があります。BAC はこれらの要素を順番に処理し、ファームウェア イメージ ファイルの照合と割り当てを行います。

ParameterName

TR-069 パラメータの名前を指定します。*ParameterName* は、TR-069 パラメータ辞書を使用して検証されます。

DPE では、このパラメータの値を、Inform から取得するか、または同じセッション内の先行する GetParameterValues RPC コールから取得するように設定できます。ルールを処理するときにセッションでパラメータ値を使用できない場合、DPE はデバイスに対して、欠落しているパラメータ値をクエリーし、値を取得してからルールの評価を続行します。

詳細については、P.5-5 の「パラメータ」を参照してください。

InformParameterName

パラメータ辞書に示されていない Inform パラメータの名前を指定します。このエントリは検証されません。

たとえば、次の例の Expression は、デバイスの `Inform.EventCode` に次の指定値のどちらかが含まれている場合に *true* と評価されます。

```
<Expression>
    <InformParameter>Inform.EventCode</InformParameter>
    <Value>1 BOOT</Value>
    <Value>3 SCHEDULED</Value>
    <Operator>match</Operator>
</Expression>
```

BAC でサポートされている InformParameter タグのパラメータ名は次のとおりです。

- Inform.DeviceId.Manufacturer
- Inform.DeviceId.ManufacturerOUI
- Inform.DeviceId.ProductClass
- Inform.DeviceId.SerialNumber
- Inform.EventCode

Inform.EventCode の値については、DSL Forum の TR-069 に関する Technical Report を参照してください。

Value

パラメータのデータを指定します。特定のパラメータについて考えられる値を 1 つ以上示すことができます。値のデータ タイプは、辞書を使用して検証されます（使用可能な場合）。

RpcArgumentName

デバイスが報告するパラメータの名前を指定します。値は、RequestDownload.FileType と RequestDownload.FileTypeArg* のどちらかです。

- RequestDownload.FileType は、デバイスがダウンロードを要求するファイルのタイプを示します。
- RequestDownload.FileTypeArg* は、デバイスがダウンロード要求メッセージに含める可能性のある任意の引数を示します。アスタリスク（*）は、実際の引数名を表します。

例 6-3 を参照してください。

Operator

Parameter と Value を評価します。Expression を評価する場合、*Operator* には、次のいずれかを指定します。

- match：大文字と小文字を区別する比較で、デバイス パラメータの値が少なくとも 1 つの値と一致する必要があることを指定します。
- matchIgnoreCase：大文字と小文字を区別しない比較で、デバイス パラメータの値が少なくとも 1 つの値と一致する必要があることを指定します。
- matchAll：大文字と小文字を区別する比較で、デバイス パラメータの値がすべての値と一致する必要があることを指定します。
- matchAllIgnoreCase：大文字と小文字を区別しない比較で、デバイス　パラメータの値がすべての値と一致する必要があることを指定します。
- noMatch：大文字と小文字を区別する比較で、デバイス パラメータの値がどの値とも一致してはならないことを指定します。
- noMatchIgnoreCase：大文字と小文字を区別しない比較で、デバイス パラメータの値がどの値とも一致してはならないことを指定します。

例 6-1　Expression：match InformParameterName

次のサンプルの Expression において、一致条件は、*InformParameter* の `Inform.EventCode` が *1 BOOT* という値と完全に一致した場合に後続のルールが有効になることを示しています。デバイスは、自動構成サーバ（ACS）と交信するときに、この値を Inform メッセージで報告します。

```
<Expression>
<InformParameterName>Inform.EventCode</InformParameterName>
          <Value>1 BOOT</Value>
          <Operator>match</Operator>
</Expression>
```

例 6-2　Expression：match RpcArgumentName（RequestDownload.FileType）

次のサンプルの Expression では、一致条件は、RPCArgumentName の `RequestDownload.FileType` が *1 Firmware Upgrade Image* という値と完全に一致した場合に後続のルールが有効になることを示しています。

```
<Expression>
    <RpcArgumentName>RequestDownload.FileType</RpcArgumentName>
    <Value>1 Firmware Upgrade Image</Value>
    <Operator>match</Operator>
</Expression>
```

例 6-3　Expression：match RpcArgumentName（RequestDownload.FileTypeArg）

次のサンプルの Expression では、一致条件は、RPCArgumentName の `RequestDownload.FileTypeArg.Version` が *1.1* という値と一致した場合に後続のルールが有効になることを示しています。

（注） CWMP 仕様では、`Version` は、File Type が Web Content の場合に使用できる FileTypeArg となることが定義されています。

```
<Expression>
    <RpcArgumentName>RequestDownload.FileType</RpcArgumentName>
    <Value>2 Web Content</Value>
    <Operator>match</Operator>
</Expression>
<Expression>
    <RpcArgumentName>RequestDownload.FileTypeArg.Version</RpcArgumentName>
    <Value> 1.1 </Value>
    <Operator>match</Operator>
</Expression>
```

例 6-4　Expression：noMatch ParameterName

次のサンプルの Expression では、一致条件は、*Parameter* の `InternetGatewayDevice.DeviceInfo.SoftwareVersion` が *1.02* というソフトウェア バージョンと一致しない場合に後続のルールが有効になることを示しています。

```
<Expression>
   <ParameterName>InternetGatewayDevice.DeviceInfo.SoftwareVersion</ParameterName>
   <Value>1.02</Value>
   <Operator>noMatch</Operator>
</Expression>
```

内部ファームウェア ファイルと外部ファームウェア ファイルの比較

内部ファームウェア イメージ ファイル要素と外部ファームウェア イメージ ファイル要素は、ファームウェア イメージ ファイルが BAC ファイル サーバ内にあるか、リモート ファイル サーバにあるかを定義します。

InternalFirmwareFile

InternalFirmwareFile 要素は、RDU に追加されて DPE に自動的に配送されたファームウェア イメージのファイル名と、ファームウェア イメージをデバイスにダウンロードするときに使用される配送の転送方式を表します。次の要素で構成されます。

- `FileName`：RDU データベース内のファイルの名前を指定します。
- `DeliveryTransport`：HTTP または SSL/TLS 転送を指定します。

（注） 対応するファイル サービス（HTTP または SSL/TLS）を DPE に設定してください。設定の詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

同じ転送を使用する複数のサービス（たとえば、2 つの HTTP）を DPE に定義した場合、DPE は最初のサービスを選択してデバイスに提供します。

例

```
<InternalFirmwareFile>
        <FileName>sample-firmware-image.bin</FileName>
        <DeliveryTransport>HTTP</DeliveryTransport>
</InternalFirmwareFile>
```

ExternalFirmwareFile

ExternalFirmwareFile 要素は、リモート サーバにあるファームウェア イメージ ファイルの名前を表します。次の要素で構成されます。

- *FileURL*：リモート ロケーションにあるファームウェア イメージ ファイルの URL を指定します。
- *FileSize*：ダウンロードするファームウェア イメージ ファイルのサイズを指定します。
- *AuthenticationCredentials*：ファイル サーバによって HTTP 認証が実行される場合に使用するユーザ名とパスワードを指定します。ユーザ名とパスワードは、Download RPC を介してデバイスに転送されます。

（注） パスワードがクリア テキストで転送されないようにするため、CWMP に SSL/TLS を使用していることを確認してください。

代入可能なパラメータを使用することで、RDU でファームウェア ルールを処理するときに、テンプレート処理エンジンがデバイス レコードからデバイス固有のユーザ名とパスワードを取得するように設定できます。

例

```
<ExternalFirmwareFile>

        <FileURL>http://imageserver.isp.com/sample-firmware-image.bin</FileURL>
        <FileSize>3449</FileSize>
        <AuthenticationCredentials>
            <HttpUserName>test</HttpUserName>
            <HttpPassword>changeme</HttpPassword>
        </AuthenticationCredentials>
</ExternalFirmwareFile>
```

サンプルのファームウェア ルール テンプレート

次の例は、ルールを含むファームウェア テンプレートを示しています。

```
<FirmwareTemplate>
    <Prerequisites>
    <MaintenanceWindow>
        <StartTime>01:00:00</StartTime>
        <Duration>5:00</Duration>
    </MaintenanceWindow>
     <Expression>

<InformParameterName>InternetGatewayDevice.DeviceInfo.EventCode</InformParameterName>
        <Value>1 BOOT</Value>
        <Operator>match</Operator>
    </Expression>
         <Expression>
        <ParameterName>InternetGatewayDevice.DeviceInfo.Manufacturer</ParameterName>
        <Value>Acme</Value>
        <Operator>matchIgnoreCase</Operator>
    </Expression>
     </Prerequisites>
     <FirmwareRule name="AcmeInternalFileRule">
                <Expression>
            <InformParameterName>InternetGatewayDevice.DeviceInfo.SoftwareVersion
</InformPaameterNam>
             <Value>2</Value>
             <Operator>match</Operator>
         </Expression>
        <InternalFirmwareFile>
            <FileName>sample-firmware-image.bin</FileName>
            <DeliveryTransport>HTTP</DeliveryTransport>
        </InternalFirmwareFile>
</FirmwareRule>
     <FirmwareRule name="AcmeExternalFirmwareRule">
             <Expression>
            <InformParameterName>InternetGatewayDevice.DeviceInfo.SoftwareVersion
</InformParameterName>
            <Value>2.5</Value>
            <Operator>match</Operator>
        </Expression>
         <ExternalFirmwareFile>
            <FileURL>http://10.10.10.10:889/sample-firmware-image.bin</FileURL>
            <FileSize>3449</FileSize>
            <AuthenticationCredentials>
                <HttpUserName>test</HttpUserName>
                <HttpPassword>changeme</HttpPassword>
            </AuthenticationCredentials>
        </ExternalFirmwareFile>
    </FirmwareRule>
</FirmwareTemplate>
```

ファームウェア ルール テンプレートに対するテンプレート構成体の使用方法

BAC のテンプレート処理メカニズムを使用すると、少数のテンプレートで、多数の CPE 用にカスタマイズされた構成を生成できます。このメカニズムでは、必ず、テンプレート構成体が使用されます。

テンプレート構成体は、**tc:include**、**tc:if**、および **tc:choose** 条件文のいずれかです。条件文は BAC プロパティと一緒に使用されます。テンプレート プロセッサは、デバイス用の命令を生成するときに構成体を処理します。次に、命令が DPE に転送され、そこでキャッシュされます。

一方、FirmwareRule は、ファームウェア ルール テンプレート内のタグで、デバイスに送信するファームウェア イメージを表します。ファームウェア ルールには、デバイスが構成を取得するために BAC と交信したときに評価される Expression を含めることができます。Expression が *true* と評価された場合、デバイスは特定のファームウェア イメージ ファイルをダウンロードするように指示されます。

ファームウェア ルールでは、事前プロビジョニングされた、または検出されたデバイス パラメータの一致に基づいて、ファームウェアをデバイスに適用できます。デバイス パラメータには、デバイス グループ メンバシップ、モデル、タイプ、現在の状態、および接続タイプなどがあります。この処理は RDU で実行されます。実行時は、中央サーバで使用できる事前プロビジョニングされたデータまたは検出されたデータが使用されます。

このリリースでは、次の汎用クラスのテンプレート構成体がサポートされています。

- パラメータ代入：BAC データ モデル内のデバイス レコードまたはその他のオブジェクトに格納されているパラメータ値に基づいて、ルールの内容を挿入できます。

  詳細については、P.6-15 の「パラメータ代入の使用方法」を参照してください。
- インクルード：テンプレートに別のテンプレートを含めることができます。

  詳細については、P.6-15 の「インクルードの使用方法」を参照してください。
- 条件式：条件文の評価に基づいて、ルールの内容を挿入できます。

  詳細については、P.6-16 の「条件の使用方法」を参照してください。

これらのテンプレート構成体を指定するには、XML タグを **tc** プレフィックスと一緒に使用します。

（注） 先頭に **tc** が付いている要素は、ファームウェア ルール テンプレートと設定テンプレートに共通した汎用構成体です。

BAC ファームウェア ルール構成体は、次の場所にあるファイルで定義された XML スキーマに基づいています。

- *BPR_HOME/rdu/templates/cwmp/schema/FirmwareTemplateSchema.xsd*
- *BPR_HOME/rdu/templates/cwmp/schema/CommonTemplateConstructs.xsd*

（注） BAC Common Template 構成体の XML ネームスペースは、`xmlns:tc='urn:com:cisco:bac:common-template'` として定義されます。

パラメータ代入の使用方法

特定のデバイスに固有のファームウェア ルールを作成するには、VAR() 構成体を使用して、BAC プロパティ階層からテンプレートに値を代入します。VAR() 構成体は、XML 要素値または要素属性の中に表示できます。また、この構成体を使用して、すべてまたは一部の値を代入することもできます。

次のリストは、BAC でサポートされている、パラメータ代入用の構成体を示しています。

- XML 要素内容に代入する BAC プロパティ値
- XML 要素属性に代入する BAC プロパティ値
- デフォルト値
- 部分的な XML 要素内容
- 特殊文字を含む値

構文と具体例については、P.5-16 の「パラメータ代入の使用方法」を参照してください。

インクルードの使用方法

インクルード ファイルを使用すると、再利用可能なテンプレートの抜粋集を作成できます。このファイルを使用すると、多くのサービス クラスで共通のオプションを定義する場合に、複数のテンプレートでオプションを重複させる必要がなくなり、便利です。

特定のファイルの内容をテンプレートに含めるには、**tc:include** 構成体を使用します。インクルードするファイルの内容をホスト テンプレートに挿入すると、ホスト テンプレートで指定されたパラメータ辞書によって、挿入後のテンプレートの内容が検証されます。

(注) インクルードするテンプレートで使用されているオブジェクトおよびパラメータが、ホスト テンプレートと同じ辞書で定義されていない場合は、命令の生成中にパラメータの検証が失敗します。

tc:Include 要素は *href* 属性を指定します。*href* は、ホスト テンプレートにインクルードする BAC テンプレート ファイルの名前を示します。テンプレートでインクルード ディレクティブを使用する場合は、二重引用符（"）を使用します。

(注) テンプレートを別のテンプレートにインクルードする場合、インクルードするテンプレートのパラメータ辞書および前提条件タグは無視されます。ファームウェア テンプレートのスキーマでは、ファームウェア テンプレート内のインクルード タグの場所が規定されています。

構文と具体例については、P.5-17 の「インクルードの使用方法」を参照してください。

条件の使用方法

BAC では、テンプレート構成体の強力な条件式を使用して、構成の最終的なカスタマイズを行うことができます。

この条件式の構成体を使用すると、テンプレートの内部でテキスト ブロックを含めるか、または除外することができます。この構成体の要素は、**tc:if**、**tc:choose**、および **tc:when** です。条件の詳細と具体例については、P.5-19 の「条件の使用方法」を参照してください。

条件を使用して、デバイスのファームウェア アップグレードをバイパスさせることもできます。デバイスが、ファームウェア ルール テンプレートで指定された必須条件と一致しない場合、デバイスはアップグレードをバイパスします。例 6-5 を参照してください。

例 6-5　ファームウェア アップグレードのバイパス

次の例は、**if** 構成体を使用したファームウェア アップグレードのバイパスを表すファームウェア ルール テンプレートを示しています。

`checkVersion` が *true* に設定されている場合は、ルールによりデバイスのソフトウェア バージョンがチェックされ、バージョンが一致しない場合は、ファームウェア アップグレードがバイパスされます。`checkVersion` が *false* に設定されている場合、ソフトウェア バージョンはチェックされず、デバイスがファームウェアのダウンロードに関する命令を取得します。

```
<tc:Template xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:tc="urn:com:cisco:bac:common-template"
xmlns="urn:com:cisco:bac:firmware-template"
xsi:schemaLocation="urn:com:cisco:bac:common-template CommonTemplateConstructs.xsd">
<FirmwareTemplate>
    <ParameterDictionaries>
        <ParameterDictionary>tr069-cwmp-dictionary.xml</ParameterDictionary>
    </ParameterDictionaries>
    <!--  Upgrade rule: if software version is 0.00.22, direct the device to download
sample-firmware-image.bin -->
    <!--  devices that do not have software version 0.00.22 , will bypass firmware
upgrade. -->
- <FirmwareRule name="LinksysWAG54G2Rule">
<tc:if test="equals(VAR(name=/cpe/checkVersion,defaultValue=false), true)">
    <Expression>
</tc:if>
        <ParameterName>InternetGatewayDevice.DeviceInfo.SoftwareVersion</ParameterName>
        <Value>0.00.22</Value>
        <Operator>matchIgnoreCase</Operator>
    </Expression>
    <InternalFirmwareFile>
        <FileName>sample-firmware-image.bin</FileName>
        <DeliveryTransport>HTTP</DeliveryTransport>
    </InternalFirmwareFile>
  </FirmwareRule>
</FirmwareTemplate>
</tc:Template>
```

パラメータ辞書

この章では、CWMP に関する顧客宅内装置（CPE）の構成および管理のプロセスで使用されるパラメータ辞書について説明します。

この章は、次の項で構成されています。

概要

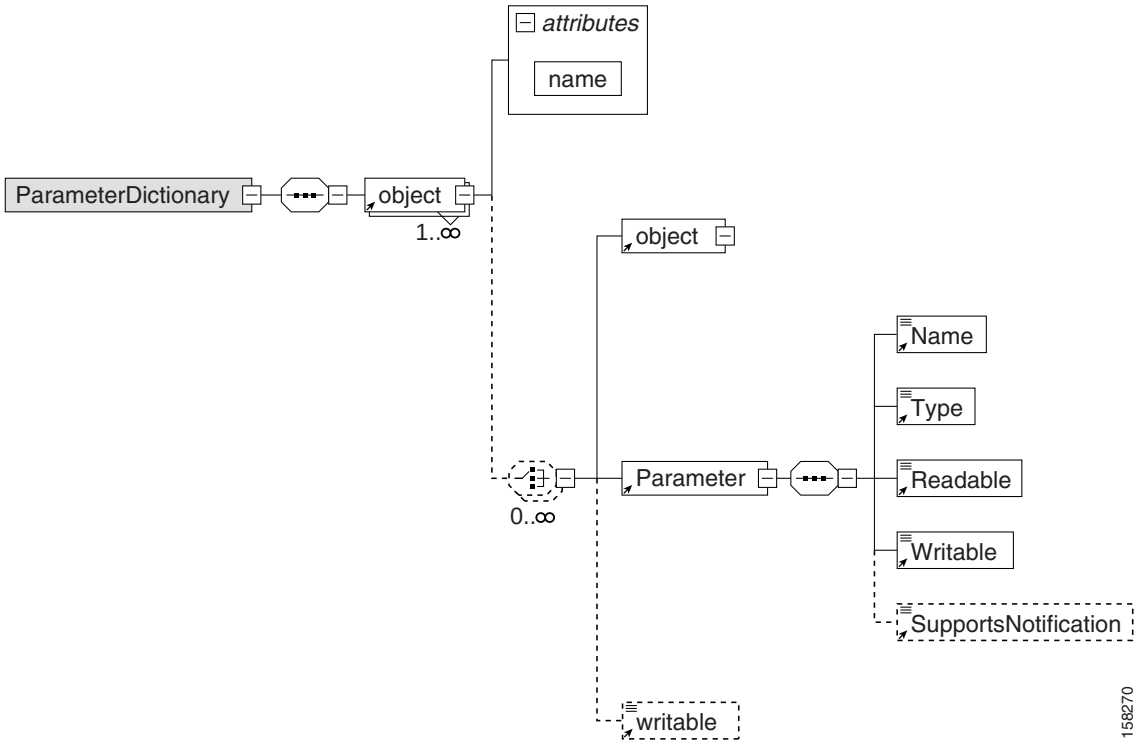
パラメータ辞書は、CWMP デバイスを構成するときに BAC が使用する有効なオブジェクトおよびパラメータが示された XML ファイルです。この辞書により、設定およびファームウェア ルール テンプレートで使用されるオブジェクトおよびパラメータが検証されます。

パラメータ辞書には、サポートされているオブジェクトおよびパラメータ（名前、タイプ、書き込み許可、および読み取り許可など）に関するメタデータが含まれています。各辞書は、ファイルに格納され、管理 API または管理者のユーザ インターフェイスを介して RDU に追加されます。

設定およびファームウェア ルール テンプレートには *ParameterDictionary* タグが含まれます。このタグは、特定のテンプレート内でパラメータを定義する辞書を示します。BAC は、テンプレートが参照する辞書を使用して、設定およびファームウェア ルール テンプレートを検証します。設定およびファームウェア ルール テンプレート内のパラメータ名と値はすべて、パラメータ辞書で参照されるパラメータとの互換性を持っている必要があります。

図 7-1 は、パラメータ辞書のスキーマを示しています。

図 7-1　パラメータ辞書スキーマ



（注） 設定またはファームウェア ルール テンプレートにエラーが存在すると、命令の生成中にそのテンプレート処理が失敗します。構成命令の生成エラーを回避するため、次の事項をすべて確認してください。

- オブジェクト名とパラメータ名が辞書に存在している。
- テンプレートで直接指定された、または代入可能なパラメータを介して指定されたパラメータ値が、辞書で指定されたタイプになっている。
- 書き込み可能でないパラメータに、値が設定されていない。ただし、設定テンプレートに通知属性またはアクセス コントロール属性（あるいは両方）を設定することはできます。

デフォルト辞書の使用方法

この BAC リリースのデフォルト辞書は、TR-069、TR-098、および TR-104 仕様で定義されたパラメータに従っています。各仕様は、次のデータ モデルに対応しています。

- TR-069：インターネット ゲートウェイ デバイス データ モデル 1.0
- TR-098：インターネット ゲートウェイ デバイス データ モデル 1.1（豊富な QoS 機能を含む）
- TR-104：ゲートウェイまたはスタンドアロン ATA 用の VoIP データ モデル

管理しやすくなるよう、*basic.cwmp.dict* 辞書には、すべての標準パラメータ（TR-098 および TR-104）の組み合せが含まれています。

これらのデフォルト辞書は次の場所にあります。

- *BPR_HOME/rdu/templates/cwmp/tr069-cwmp-dictionary.xml*
- *BPR_HOME/rdu/templates/cwmp/tr104-cwmp-dictionary.xml*
- *BPR_HOME/rdu/templates/cwmp/tr098-cwmp-dictionary.xml*
- *BPR_HOME/rdu/templates/cwmp/basic-cwmp-dictionary.xml*

（注） BAC ではデフォルト辞書を変更または削除することはできません。

テンプレートが参照する新しいユーザ定義の辞書を追加できます。この機能を使用すると、ベンダー固有のパラメータを含む CPE パラメータ モデルを BAC でサポートできるようになります。詳細については、次の「カスタム辞書」の項を参照してください。BAC では、ベンダー固有の辞書のサポートにより、WT-135（IPTV STB）や WT-140（NAS）などの先端のデータ モデルをすべて使用できます。

カスタム辞書

CWMP には、標準のパラメータに加えてベンダー固有のパラメータを使用できる、拡張性のあるメカニズムが含まれています。そのため、BAC システムにカスタム辞書を追加して、任意の CPE をサポートすることができます。この機能を使用すると、実質的にどのようなデータ モデルを持つデバイスでもサポートできます。このようなデータ モデルには、WT-135（IPTV STB）や WT-140（NAS）などの先端の標準データ モデルがあります。

BAC に対するカスタム辞書の追加、表示、置換、または削除は、管理者のユーザ インターフェイスまたは管理 API から行うことができます。

（注） カスタム辞書は、設定テンプレートには使用できません。BAC 設定テンプレートで使用できるのは、BAC データベースに含まれているパラメータ辞書だけです。

カスタム辞書を追加する場合は、以前の項で説明したように、この辞書がパラメータ辞書スキーマに基づいていることを確認してください。

パラメータ辞書の構文

BAC は、パラメータ辞書スキーマに従って、パラメータ辞書の構文を検証します。このスキーマは、*BPR_HOME/rdu/templates/cwmp/TemplateDictionarySchema.xsd* にあります。

標準オブジェクトにベンダー固有のパラメータを追加する場合は、必ず、それより高いレベルの標準オブジェクトとそのパラメータすべてをカスタム辞書で定義してください。

BAC では、TR-069 仕様で定義されたデータ タイプがすべてサポートされます。パラメータ辞書は、この BAC リリースでサポートされるデータ タイプを指定します。表 7-1 を参照してください。

表 7-1　BAC でサポートされるデータ タイプ

タイプ	説明
String	許容最大長を示すには、`string` *(N)* 構文を使用します。*(N)* は、文字列の最大長です。
int	-2,147,483,648 ～ +2,147,483,647 の範囲の整数（上限と下限も含む）。 値の範囲を指定するには、`int[Min:Max]` 構文を使用します。Min と Max の値も範囲に含まれます。Min または Max が省略されている場合は、制限がないことを示します。
unsignedInt	0 ～ 4,294,967,295 の範囲の符号なし整数（上限と下限も含む）。 値の範囲を指定するには、`unsignedInt[Min:Max]` 構文を使用します。Min と Max の値も範囲に含まれます。Min または Max が省略されている場合は、制限がないことを示します。
boolean	1 つの値。1 は true を、0 は false を表します。
dateTime	UTC（Universal Coordinated Time; 万国標準時）で表される時刻（別に指定した場合を除く）。たとえば、**2004-01-03T03:04:05-(or +)05:00** と表されます。
base64	許容最大長を指定するには、`base 64` *(N)* 構文を使用します。*(N)* は、Base64 符号化の後の最大文字数です。

サンプルのパラメータ辞書

次のサンプルは、TR-069 パラメータ リストとそれに対応する辞書スキーマを示しています。

名前	タイプ	書き込み	読み取り
InternetGatewayDevice	Object	-	R
InternetGatewayDevice.DeviceInfo	Object	-	R
X_HGI_ALG	Object	-	R
X_08017_ChipModel	string	-	R
ALGNumberOfEntries	unsignedInt	-	R
Manufacturer	string(64)	-	R

```
<ParameterDictionary xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="TemplateDictionarySchema.xsd">
<Object name="InternetGatewayDevice">
    <Object name="DeviceInfo">
     <Writable>false</Writable>
     <Parameter>
        <Name>Manufacturer</Name>
        <Type>string(64)</Type>
        <Readable>true</Readable>
        <Writable>false</Writable>
    </Parameter>
    <Parameter>
        <Name>X_08017_ChipModel</Name>
        <Type>string</Type>
        <Readable>true</Readable>
        <Writable>false</Writable>
    </Parameter>
  </Object>
- <!--  custom property: InternetGatewayDevice.X_HGI_ALG -->
- <!--  as defined for HGI's Application Layer Gateway Management -->
- <Object name="X_HGI_ALG">
    <Parameter>
        <Name>ALGNumberOfEntries</Name>
         <Type>unsignedint</Type>
         <Readable>true</Readable>
         <Writable>false</Writable>
    </Parameter>
  </Object>
</Object>
</ParameterDictionary>
```

ユーザ インターフェイスからのパラメータ辞書の管理

管理者のユーザ インターフェイスを使用すると、パラメータ辞書ファイルの管理や、パラメータ辞書の表示、追加、削除、または置換を行うことができます。ファイルをエクスポートするには、P.17-17 の「ファイルのエクスポート」を参照してください。

（注） デフォルト辞書を変更または削除することはできません。

パラメータ辞書の追加

BAC RDU データベースに新しいパラメータ辞書を追加するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Files** を選択します。View Files ページが表示されます。

ステップ 3　**Add** をクリックします。

ステップ 4　Add Files ページが表示されます。File Type ドロップダウン リストから Parameter Dictionary を選択します。

ステップ 5　Source File Name と File Name に適切な情報を入力します。

（注） ソースファイルの正確な名前が分からない場合は、**Browse** 機能を使用して目的のディレクトリまで移動し、そのファイルを選択します。

ステップ 6　**Submit** をクリックします。

新しいファイルが追加された状態で View Files ページが表示されます。

パラメータ辞書の表示

BAC RDU データベースに含まれているファイルの内容を表示するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Files** を選択します。

ステップ 3　View Files ページが表示されます。File Type ドロップダウン リストから Parameter Dictionary を選択します。

ステップ 4　検索対象に指定したファイルに対応する **View Details** アイコン（ ）をクリックします。

パラメータ辞書の内容が表示されます。

パラメータ辞書の削除

RDU データベースから既存のパラメータ辞書を削除するには、次の手順に従います。

（注） 組み込みのデフォルト辞書は削除できません。

ステップ 1　**Configuration** > **Files** の順に選択します。

ステップ 2　File Type ドロップダウン リストから Parameter Dictionary を選択します。

ステップ 3　削除するファイルをクリックします。

ステップ 4　**Delete** をクリックします。

削除したファイルが含まれていない状態で View Files ページが表示されます。

パラメータ辞書の置換

BAC RDU データベースに含まれている既存のパラメータ辞書の内容を置換するには、次の手順に従います。

（注） 組み込みのデフォルト辞書は変更できません。

ステップ 1　**Configuration** > **Files** の順に選択します。

ステップ 2　File Type ドロップダウン リストから Parameter Dictionary を選択します。

ステップ 3　検索結果で、置換するファイルに対応するリンクをクリックします。

ステップ 4　Replace File ページが表示されます。選択したファイル名がすでにこのページに表示されています。表示されているファイルと置換するソース ファイルのパスを入力します。ソースファイルの正確な名前や場所が分からない場合は、**Browse** 機能を使用して適切なディレクトリまで移動し、そのファイルを選択します。

ステップ 5　**Submit** をクリックします。置換ファイルを決定した後に確認ページが表示されて、置換後、影響を受けるデバイス用の命令が BAC によって再生成されることが示されます。

ステップ 6　**OK** をクリックします。

View Files ページが表示されます。

CPE の履歴とトラブルシューティング

この章では、トラブルシューティングを行う場合にデバイス情報を使用する方法について説明します。この場合に使用できる機能には次のものがあります。

- デバイス履歴（P.8-1）
- デバイス障害（P.8-7）
- デバイスのトラブルシューティング（P.8-10）

デバイス履歴

この項では、デバイス履歴機能について説明します。この機能を使用すると、デバイス プロビジョニングのライフサイクルで発生する重要なイベントの詳細な履歴を表示できます。この機能は、トラブルシューティングを行う場合に便利です。

デバイス履歴の表示は、API または管理者のユーザ インターフェイスから行うことができます。

- 特定のデバイスの履歴を取得するには、次の API を呼び出します。

  ```
  com.cisco.provisioning.cpe.api.ipdevice.history getHistory (DeviceID deviceID)
  ```

- 管理者のユーザ インターフェイスを使用して特定のデバイスの履歴を取得するには、P.16-13 の「デバイスの履歴の表示」を参照してください。

表 8-1 は、BAC のデバイス履歴機能でサポートされる特定のレコード タイプを示しています。

表 8-1　サポートされるデバイス履歴レコード

レコード タイプ	説明	メッセージ形式
AddedAutomatically	以前に登録解除されたデバイスが、DPE との交信後に BAC に自動的に追加されたときに記録されます。	*time*: Device record was automatically created.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device record was automatically created.`	

AddedViaAPI	デバイスがクライアント API を使用して BAC に追加されたときに記録されます。	*time*: Device record was added via API by user *username*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device record was added via API by user "admin".`	

UpdatedViaAPI	RDU に格納されているデバイス レコードが、クライアント API を使用して変更されたときに記録されます。	*time*: Device record was updated *reason* by user *username*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device record was updated via API command "IPDevice.changeClassOfService" by user "admin".`	

FirstContact	デバイスが BAC と最初に交信したときに記録されます。	*time*: Device made first contact with BAC.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device made first contact with BAC.`	

CPEDiscoveredData Updated	デバイスがデバイス パラメータの新しい値を報告したときに記録されます。この値は、検出されたデータとして RDU でトラッキングされます。 検出されたパラメータの詳細については、P.4-5 の「CPE パラメータの検出」を参照してください。	*time*: Recorded updates of *number* parameter values discovered from device.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Recorded updates of 2 parameter values discovered from device.`	

表 8-1　サポートされるデバイス履歴レコード（続き）

レコード タイプ	説明	メッセージ形式
ConfigGenRequested	デバイスに対する命令の再生成が開始されたときに記録されます。再生成された命令は、デバイスのプロビジョニング グループ内の DPE すべてに送信されます。	*time*: Device policy instructions regeneration initiated as a result of *reason* by user *username*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device policy instructions regeneration initiated as a result of execution of API Command "IPDevice.performOperation" by user "admin".`	

ConfigUpdated	BAC がデバイスの新しい構成を有効にしたときに記録されます。	*time*: Device was configured according to configuration version: *configuration revision*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device was configured according to configuration version: 215438bb.`	

UpdatedConfigAvailable	デバイス用の新しい構成命令が RDU から DPE に送信されたときに記録されます。	*time*: Configuration policy for device was updated; new version: *configuration revision*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Configuration policy for device was updated; new version: 215438bb.`	

ReportedNewConfig	デバイスが新しい構成を使用して、Inform メッセージに含まれている *ParameterKey* を介して報告したときに記録されます。	*time*: Device reported new configuration version: *configuration revision*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device reported new configuration version: 215438bb.`	

NewOperationQueued	新しいデバイス操作が、クライアント API または管理者のユーザ インターフェイスから開始され、BAC によってデバイス用の実行キューに入れられたときに記録されます。	*time*: On-connect operation *operation name* with ID *operation ID* was queued by user *username*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`On-connect operation "SetParamValues" with ID "15e2ccd:10c5f4b2ad0:80000024" was queued by user "admin".`	

表 8-1　サポートされるデバイス履歴レコード（続き）

レコード タイプ	説明	メッセージ形式
OperationExecuted	クライアント API または管理者のユーザ インターフェイスから開始した操作が、デバイスに対して正常に実行されたときに記録されます。	*time*: *Operation mode operation name* with ID *operation id* was executed on the device.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`On-connect operation "SetParamValues" with ID "15e2ccd:10c5f4b2ad0:80000024" was executed on the device.`	

OperationRemoved	BAC 内のキューに入っているデバイス操作が削除されたときに記録されます。	*time*: On-connect operation *operation name* with ID *operation id* was removed.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`On-connect operation "GetParamValues" with ID "15e2ccd:10c5f4b2ad0:80000025" was removed.`	

ReportedNewFirmware	デバイスが新しいファームウェアを使用して、Inform メッセージを介して報告したときに記録されます。	*time*: Device reported new firmware/software version: *firmware/software version*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Device reported new firmware/software version: 6d9bfec2.`	

UpdatedFirmwareRules Available	デバイス用の新しいファームウェア ルールが RDU から DPE に送信されたときに記録されます。	*time*: Firmware rules for device were updated; new version: *firmware rules revision*.

	例：
	`Tue Jul 11 18:41:42 EDT 2006:`
	`Firmware rules for device were updated; new version: 6d9bfec2.`	

デバイス履歴の設定

デバイス履歴機能を使用すると、デバイス プロビジョニングのライフサイクルで発生する重要なイベントを記録できます。この項では、この機能をイネーブルまたはディセーブルにする方法について説明します。

デバイス履歴のイネーブル化

デバイス履歴は、デフォルトでイネーブルになっています。この機能を API からイネーブルまたはディセーブルにするには、`SERVER_DEVICE_HISTORY_ENABLE_KEY` プロパティを使用します。

（注） デバイス履歴をイネーブルまたはディセーブルにするたびに、メッセージが *audit.log* に記録されます。また、デバイス履歴はトラブルシューティングのログにも格納されます。

デバイス履歴を管理者のユーザ インターフェイスからイネーブルまたはディセーブルにするには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーまたは Main Menu ページで、**Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Defaults** を選択します。

ステップ 3　Configure Defaults ページが表示されます。**System Defaults** をクリックします。

ステップ 4　デフォルト ページで、Device History に対応する **Enabled** オプション ボタンをクリックします。

（注）　デバイス履歴機能をディセーブルにするには、**Disabled** オプション ボタンをクリックします。デバイス履歴をディセーブルにすると、既存のデバイスの新しい更新や新しいデバイスの詳細がデバイス履歴に記録されなくなります。ただし、既存のイベントは保持されます。

ステップ 5　**Submit** をクリックするか、または **Reset** をクリックしてデフォルト値に戻します。

デバイス履歴の表示

管理者のユーザ インターフェイスからデバイス履歴を表示するには、次の手順に従います。

ステップ 1　**Devices** ページで、履歴を表示するデバイスを検索します。そのためには、いずれかの検索タイプを使用します。

ステップ 2　該当のデバイスに対応する **View Details** アイコン（）をクリックします。

ステップ 3　Device Details ページが表示されます。View Device History Details に対応する **View Details** アイコンをクリックします。

Device History Details ページが表示されます。

デバイス履歴を取得するには、API コマンドの `IPDevice.getDeviceHistory()` を使用します。

デバイス履歴のサイズの設定

管理者のユーザ インターフェイスからデバイス履歴エントリの最大数を設定するには、**Configuration** > **Defaults** > **System Defaults** の順に選択します。Maximum Device History Entries に対応するフィールドに値を入力します。デフォルトのエントリ数は 40 です。

この数を API から設定するには、`SERVER_MAX_DEVICE_HISTORY_SIZE` プロパティを設定します。

Maximum Device History Entries の値を小さくした場合、制限を超える既存のレコードが削除されるのは、新しいデバイス履歴が記録されたときです。このとき、デバイスの履歴は、管理者が設定したデバイス履歴エントリの最大数に従って更新されます。最大数を増やした場合、その時点より古いエントリは保持されます。最大数を減らした場合は、最も古いエントリから削除されます。

デバイス履歴レコード

デバイス履歴レコードは、循環リストに記録されます。リストが、管理者によって指定された制限に到達すると、最も古いエントリが削除されます。ただし、次に示すレコードは削除されません。

- AddedViaAPI（事前登録されたデバイスの場合）
- AddedAutomatically（登録解除されたデバイスの場合）
- FirstContact

デバイス アクティビティを幅広く記録する場合に影響を受ける可能性がある BAC のパフォーマンスを最適化するには、API から次のシステム プロパティを使用して、特定のイベント タイプをイネーブルまたはディセーブルにします。

（注） これらのプロパティは、デフォルトでディセーブルになっています。これらのオプションがデバイス履歴に影響を与えるのは、デバイス履歴機能をイネーブルにした場合だけです。

- `SERVER_DEVICE_HISTORY_IMMEDIATE_OP_ENABLE_KEY`
  即時操作に関する OperationExecuted 履歴を記録する。
- `SERVER_DEVICE_HISTORY_PROXY_OP_ENABLE_KEY`
  接続時のデバイス操作に関する NewOperationQueued、OperationRemoved、および OperationExecuted 履歴を記録する。

（注） `SERVER_DEVICE_HISTORY_IMMEDIATE_OP_ENABLE_KEY` プロパティをディセーブルにし、`SERVER_DEVICE_HISTORY_PROXY_OP_ENABLE_KEY` プロパティをイネーブルにした場合、即時操作はディセーブルになり、接続時操作はイネーブルになります。

- `SERVER_DEVICE_HISTORY_GEN_CONFIG_ENABLE_KEY`
  ConfigGenRequested 履歴を記録する。

これらのプロパティを管理者のユーザ インターフェイスからイネーブルまたはディセーブルにするには、次の手順に従います。

ステップ 1　**Configuration** > **Defaults** ページの順に選択します。

ステップ 2　画面の左隅にある **System Defaults** リンクをクリックします。

ステップ 3　イネーブルまたはディセーブルにする操作に対応するオプション ボタンをクリックします。

- 即時操作の履歴の記録をイネーブルにするには、Immediate Operation History に対応する **Enabled** オプション ボタンをクリックします。
- 接続時操作の履歴の記録をイネーブルにするには、On-Connect Operation History に対応する **Enabled** オプション ボタンをクリックします。
- 構成生成の履歴の記録をイネーブルにするには、Instruction Generation History に対応する **Enabled** オプション ボタンをクリックします。

これらの操作をディセーブルにするには、対応する **Disabled** オプション ボタンをクリックします。

ステップ 4　**Submit** をクリックします。

デバイス障害

大規模のインストールでは、デバイスで障害が繰り返し発生すると、ボトルネックとなってパフォーマンスに影響を及ぼす場合があります。障害が繰り返し発生する原因としては、デバイスの誤動作や BAC の設定ミスが考えられます。BAC を使用すると、Recurring Device Faults 機能を通じて、RDU および DPE サーバで繰り返し発生する障害を検出できます。

繰り返し発生する障害とは、短期間に何度も発生する障害や、高い確率で繰り返し発生する障害を指します。たとえば、BAC 構成ポリシーに基づいてデバイスを構成しようとしたときに、デバイスでパラメータが欠落していることが原因で障害が発生する場合があります。このような障害は、1 回しか発生していなくても、繰り返し発生する障害と見なされます。これは、この操作がデバイス交信ごとに実行されるためです。ただし、単発のデバイス操作を API から開始したときに障害が発生した場合、この障害は操作への応答として API クライアントに返されるため、繰り返し発生する障害とは見なされません。

また、次のシナリオを考慮してください。

- RDU にある設定テンプレートが、システムから削除されたプロパティを参照する場合がある。RDU がこのテンプレートを使用してデバイス用の命令を生成しようとすると、毎回エラーが発生します。このエラーにより、このデバイスは障害が繰り返し発生するデバイスと見なされます。そのため、このエラーはユーザに報告されます。
- デバイスのファームウェアのバグが原因で、デバイスが無効または不完全な Inform メッセージを送信する。この状態の Inform メッセージは、デバイス交信ごとに生成されます。この問題の場合も、繰り返し発生する障害と見なされます。

この機能を使用すると、特定のデバイスに関する最新の障害の詳細と、システム全体、RDU サーバ、および各 DPE サーバについて集約した障害の統計情報を表示できます。

次の操作の実行中は、RDU および DPE においてデバイス障害がモニタリングされます。

RDU において：
命令の生成中の障害
拡張の実行時の障害
DPE において：
CPE WAN Management Protocol の違反
DataSync 命令の処理中の障害。この命令は、デバイスからのデータを検出し、RDU を更新するように指示します。
Failures during FirmwareRules 命令の処理中の障害。この命令は、RDU ファームウェア ルール テンプレートで設定されたファームウェア ルールを実行するように指示します。
ConfigSync 命令の処理中の障害。この命令は、RDU 設定テンプレートに従ってデバイス構成を更新するように指示します。
UnknownDevice 命令の処理中の障害。この命令は、不明なデバイスまたは登録解除されたデバイスを処理するように指示します。

RDU および DPE では、繰り返し発生する障害のリストが保守されます。障害ごとに、発生日時、デバイスの ID、および障害の説明が加えられます。

障害のライフタイムが満了するとすぐに、その障害は期限切れとなって自動的にシステムから削除されます。障害がシステムから削除されると、それに応じて統計情報が調整されます。

（注）BAC では、管理者のユーザ インターフェイス上のデバイス障害リストに返されるデバイスの数が 1,000 に制限されています。障害デバイスの数が 1,000 を超えた場合は、メッセージが表示され、画面に表示されない障害デバイスも存在することが示されます。

パフォーマンスへの影響を避けるため、BAC では障害情報がディスク上に格納されません。サーバを再起動すると、そのサーバのメモリに保持されていた障害データは失われます。ただし、障害が再度繰り返し発生した場合、障害は報告されます。

デバイス障害の取得

デバイス障害の情報は、API および管理者のユーザ インターフェイスから取得できます。

API からは、次のプロパティを呼び出すことができます。

- `Configuration.getRDUDetails`：RDU にある障害デバイスのリストを返します。
- `Configuration.getDPEDetails`：DPE にある障害デバイスのリストを返します。
- `IPDevice.getDetails`：デバイスに関連する障害の情報を返します。

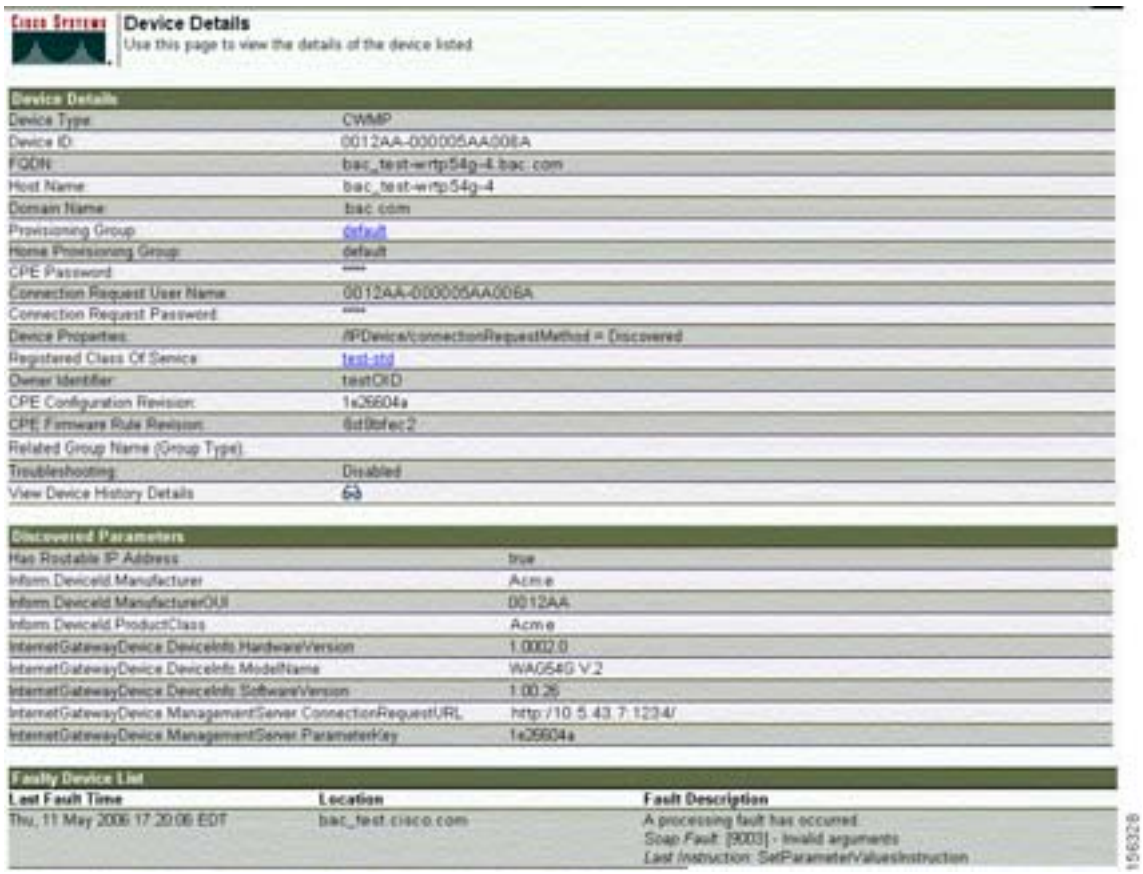
管理者のユーザ インターフェイスでは、次のように選択します。

- **Servers > RDU**：RDU レベルのデバイス障害の統計情報と、すべての DPE について集約した障害の統計情報が表示されます。デフォルトでは、1、3、12、および 72 時間間隔の統計情報が表示されます。
- **Servers > Provisioning Groups > Manage Provisioning Groups > View Provisioning Group Details**：プロビジョニング グループ内の各 DPE に関するデバイス障害の統計情報が表示されます。
- **Servers > DPEs > Manage Device Provisioning Engines > View Device Provisioning Engines Details**：障害デバイスの数が表示されます（ある場合）。Device with Faults に対応する **View Details** アイコンをクリックします。Device Details ページが表示され、DPE レベルのデバイス障害の統計情報が詳細に示されます。

  （注）**View Device Provisioning Engines Details** ページで **View Details** アイコンの横に Device with Faults オプションが表示されるのは、障害デバイスがある場合だけです。

- **Devices > Manage Devices > Device Details**：選択されたデバイスに関する最新の障害が表示されます（ある場合）。図 8-1 を参照してください。

図 8-1　Device Details ページに表示される障害の説明



BAC は、最新の障害デバイスの詳細を、各サーバで保守します。DPE の冗長性により、特定のデバイスが、時間とともに複数の DPE と交信するようになり、そのいずれかまたはすべての DPE 上の障害リストに加えられる場合があります。また、この同じデバイスが、RDU で障害を繰り返し発生する場合もあります。BAC では、すべてのサーバにあるデバイス障害を集約して表示することができます。ただし、各サーバでトラッキングされる障害は、常に、デバイスごとに最大 1 つであり、障害データは有効期限が切れるとメモリから削除されます。

デバイスのトラブルシューティング

この機能を使用すると、1 つ以上の特定のデバイスに関する、きわめて詳細なトラブルシューティング情報を収集できます。トラブルシューティング情報には、特定のデバイスまたはデバイス グループに関連するサーバ インタラクションがすべて含まれます。この情報には、管理者のユーザ インターフェイスの操作、RDU API 操作、DPE と CPE とのインタラクション、およびサーバ間の DPE と RDU とのインタラクションも含まれます。

1 つ以上の特定のデバイスに対して、トラブルシューティングをイネーブルまたはディセーブルにできます。この場合、ロギングをオンにしたり、特定のデバイス情報についてのログ ファイルを検索したりする必要はありません。

BAC は、詳細なトラブルシューティング情報を収集するデバイスのリストを、デバイス ID に基づいて保守します。トラブルシューティング情報は、RDU で一元的に保管され、デバイス単位で保守されます。DPE は、このデータを保管しません。反対に、DPE は、この情報を RDU に転送します。RDU は、この情報を受信すると、*BPR_DATA/rdu/logs* ディレクトリ内の *troubleshooting.log* デバイス ログ ファイルに書き込みます。

DPE から RDU への接続が失われた場合、DPE で発生している新しいトラブルシューティング イベントはすべて廃棄されます。トラブルシューティング情報のロギングが再開されるのは、RDU と DPE 間の接続が復元された場合だけです。

troubleshooting.log ファイルは、その他の *rdu.log*、*dpe.log*、および *audit.log* などのログ ファイルとは異なります。*troubleshooting.log* ファイルに記録されるのは、トラブルシューティング モードになっている特定のデバイス セットに関連する詳細なトラブルシューティング情報だけです。

（注） トラッキング機能は、トラブルシューティング グループに 1 つ以上のデバイスを追加しない限り、オフになっています。

特定のデバイスのトラブルシューティングをイネーブルまたはディセーブルにすると、その変更は即時にすべてのサーバ（RDU および DPE）で有効になるため、RDU または DPE をリブートする必要はありません。各サーバのログ ファイルには、トラブルシューティング モードになっているデバイスの現在のリストが示されます。

注意 デバイスのトラブルシューティング機能を使用する場合は、追加のメモリおよびディスク領域が必要になります。トラッキング対象のデバイス数が増えると、作成されたログの数をサポートするのに必要なメモリおよびディスク領域の容量も増えます。

デバイスのトラブルシューティングの設定

デバイスのトラブルシューティング機能は、1 つ以上のデバイスをトラブルシューティング モードに移行するまで、ディセーブルになっています。この項では、管理者のユーザ インターフェイスからデバイスのトラブルシューティングをイネーブルまたはディセーブルにする方法について説明します。また、トラブルシューティング モードのデバイスのリストを表示する方法や、特定のデバイスのトラブルシューティング ログを表示する方法についても説明します。

トラブルシューティング モードになるデバイスの最大数を設定すると、気付かないうちに膨大な数のデバイスをこのモードに移行して、サーバのパフォーマンスを低下させてしまうことを回避できます。デフォルトでは、この数は 100 に設定されています。管理者のユーザ インターフェイスから

トラブルシューティング モードに移行できるデバイスの最大数を設定するには、Systems Defaults ページで **Configuration** > **Defaults** タブの順にクリックします。Maximum Troubleshooting Device Count フィールドに値を入力します。

デバイスのトラブルシューティングのイネーブル化

デバイスのトラブルシューティングをイネーブルにするには、そのデバイスを BAC RDU で事前登録しておく必要があります。デバイスが事前登録されていない場合は、Manage Devices ページで **Add** ボタンをクリックして、デバイスを追加します。デバイスの追加については、P.16-12 の「デバイス レコードの追加」を参照してください。

RDU データベース内にすでに存在するデバイスのトラブルシューティングをイネーブルにするには、次の手順に従います。

ステップ 1　Manage Devices ページで、Search Type ドロップダウン リストをクリックし、Device Identifier Option Search オプションを選択します。この検索にはワイルドカード機能を使用できます（表 16-1 を参照してください）。**Search** をクリックします。

ステップ 2　デバイスのリストが表示されます。トラッキングするデバイスに対応する Identifier リンクをクリックします。

ステップ 3　Modify Device ページが表示され、各種のデバイス パラメータが示されます。Troubleshooting パラメータに対応する **Enabled** オプション ボタンをクリックします。

ステップ 4　**Submit** をクリックします。これで、デバイスのトラブルシューティングがイネーブルになりました。

特定のデバイスのトラブルシューティングがイネーブルになっているかどうかを確認するには、Device Details ページにアクセスし、Troubleshooting に対応するステータスを確認します。

デバイスのトラブルシューティングのディセーブル化

デバイスのトラブルシューティングをディセーブルにするには、次の手順に従います。

ステップ 1　**Devices** タブで、削除するデバイスを検索します。そのためには、いずれかの検索タイプを使用します。

ステップ 2　トラブルシューティング リストから削除するデバイスに対応する Identifier リンクをクリックします。

ステップ 3　Modify Device ページが表示されます。Troubleshooting パラメータに対応する **Disabled** オプション ボタンをクリックします。

ステップ 4　**Submit** をクリックします。

トラブルシューティング モードになっているデバイスのリストの表示

デバイスのトラブルシューティングをイネーブルにすると、そのデバイスは、トラブルシューティング モードのデバイスのリストを含む、特別なデバイス グループに自動的に追加されます。グループ タイプは **system** で、グループ名は **troubleshooting** です。このグループ内のデバイスのリストには、API または管理者のユーザ インターフェイスからアクセスできます。

トラブルシューティングが現在イネーブルになっているデバイスのリストを表示するには、次の手順に従います。

ステップ 1　**Manage Devices** ページで、Search Type ドロップダウン リストをクリックし、Group Search を選択します。

ステップ 2　Group (Group Type) ドロップダウン リストから、トラブルシューティング モードのデバイスすべてを表示するための、troubleshooting (system) オプションを選択します。

ステップ 3　**Search** をクリックします。

（注）　上記のほか、トラブルシューティング モードのデバイスのリストを表示するには、RDU ログ（*rdu.log*）および DPE ログ（*dpe.log*）を調べるという方法もあります。デバイスのリストの記録は、サーバが起動するたび、およびトラブルシューティングがイネーブルになっているデバイスのリストが変更されるたびに行われます。

トラブルシューティングがイネーブルになっているデバイスは、ログ レベルが 5（通知）に設定された状態でログ ファイルに表示されます。ログ ファイルの詳細については、P.19-3 の「ロギング」を参照してください。

デバイスのトラブルシューティング ログの表示

特定のデバイスのトラブルシューティング ログ ファイルは、次のどちらかの方法で表示できます。

- P.8-12 の「トラブルシューティング モードになっているデバイスのリストの表示」で説明されている手順に従う。その後、次の手順に従います。

ステップ 1　トラブルシューティング モードのデバイスのリストが表示された状態で、特定のデバイスに対応する **View Details** アイコンをクリックします。

ステップ 2　Device Details ページが表示されます。View Troubleshooting Log に対応する **View Details** アイコンをクリックします。

View Log File Contents ページが表示されます。

- 次の手順に従う。

ステップ 1　Manage Details ページの **Devices** タブで、Search Type ドロップダウン リストをクリックし、Device Identifier Option Search オプションを選択します。この検索にはワイルドカード文字（*）を使用できます。

ステップ 2　**Search** をクリックします。

ステップ 3　デバイスのリストが表示されます。ログ ファイルを確認するデバイスに対応する **View Details** アイコンをクリックします。

ステップ 4　Device Details ページが表示されます。View Troubleshooting Log に対応する **View Details** アイコンをクリックします。

View Log File Contents ページが表示されます。

デバイスのトラブルシューティング ログ エントリのカラー コーディングは、次のとおりです。

- BAC-TROUBLESHOOTINGINFO：情報メッセージは白色でマークされます。
- BAC-TROUBLESHOOTINGINPUT：BAC サーバで受信されたメッセージの詳細は灰色でマークされます。
- BAC-TROUBLESHOOTINGOUTPUT：BAC　サーバから送信されたメッセージの詳細は緑色でマークされます。
- BAC-TROUBLESHOOTINGERROR：エラー メッセージは赤色でマークされます。

Broadband Access Center の管理

この章では、Broadband Access Center（BAC）システムの管理に役立つ各種サブコンポーネントについて説明します。次のトピックについて説明します。

BAC プロセス ウォッチドッグ

BAC プロセス ウォッチドッグは、すべての BAC プロセスのランタイム状況を監視する管理プロセスです。このウォッチドッグ プロセスにより、プロセスが予想外に停止した場合に自動的に再開されるようになります。BAC コンポーネントを実行する各システム上で、BAC プロセス ウォッチドッグのインスタンスが 1 つ実行されます。

BAC ウォッチドッグは、監視対象プロセスの状態を開始、停止、再開、決定するコマンド ライン ツールとして利用できます。

監視対象のアプリケーションが機能しなくなると、自動的に再開します。何らかの理由で再開プロセスも機能しない場合は、BAC ウォッチドッグ プロセス サーバは所定の時間待機してから再び再開を試みます。

再開を試みる間隔は 1 秒から始まり、後続の試行で 5 分に達するまで指数関数的に長くなります。その後、プロセスの再開が成功するまで 5 分間隔で試みられます。再開の成功の 5 分後に、期間は再び自動的に 1 秒にリセットされます。

次に例を示します。

- プロセス A が失敗します。
- BAC プロセス ウォッチドッグ サーバはプロセスの再開を試み、1 回目の再開が失敗します。
- BAC プロセス ウォッチドッグ サーバは 2 秒間待機してからプロセスの再開を試み、2 回目の再開が失敗します。
- BAC プロセス ウォッチドッグ サーバは 4 秒間待機してからプロセスの再開を試み、3 回目の再開が失敗します。
- BAC プロセス ウォッチドッグ サーバは 16 秒間待機してからプロセスの再開を試みます。

コマンドラインからの BAC プロセス ウォッチドッグの使用

BAC ウォッチドッグ エージェントは、システムのブートアップのたびに自動的に起動します。そのため、このウォッチドッグは、同じシステムにインストールされている BAC システム コンポーネントも起動します。**/etc/init.d/bprAgent** コマンドを実行すると、単純なコマンドライン ユーティリティを使用して BAC ウォッチドッグを制御することもできます。

表 9-1 は、BAC ウォッチドッグ プロセスに対して使用できるコマンドライン インターフェイス コマンドを示しています。

表 9-1　BAC ウォッチドッグ エージェント CLI コマンド

コマンド	説明
bprAgent start	すべての監視対象プロセスを含む BAC ウォッチドッグ エージェントを開始します。
bprAgent stop	すべての監視対象プロセスを含む BAC ウォッチドッグ エージェントを中止します。
bprAgent restart	すべての監視対象プロセスを含む BAC ウォッチドッグ エージェントを再起動します。
bprAgent status	すべての監視対象プロセスを含む BAC ウォッチドッグ エージェントの状態を入手します。
bprAgent start *process-name*	特定の 1 つの監視対象プロセスを開始します。*process-name* 値がそのプロセスを識別します。
bprAgent stop *process-name*	特定の 1 つの監視対象プロセスを中止します。*process-name* 値がそのプロセスを識別します。
bprAgent restart *process-name*	特定の 1 つの監視対象プロセスを再開します。*process-name* 値がそのプロセスを識別します。
bprAgent status *process-name*	特定の 1 つの監視対象プロセスの状態を入手します。*process-name* 値がそのプロセスを識別します。

表 9-1 に示す *process-name* は、次のいずれかになります。

- rdu：RDU サーバを指定します。
- dpe：DPE サーバを指定します。
- snmpAgent：SNMP エージェントを指定します。
- tomcat：管理者のユーザ インターフェイスを指定します。
- cli：DPE コマンドライン インターフェイスを指定します。

(注) Solaris オペレーティング システムがリブートされると、BAC プロセス ウォッチドッグが最初に停止します。その結果、BAC サーバは正常にシャットダウンできます。オペレーティング システムをシャットダウンまたはリブートするには、Solaris **shutdown** コマンドを使用してください。Solaris **reboot** コマンドでは、アプリケーション シャットダウン フックは実行されません。BAC プロセスはシャットダウンされるのではなく、強制終了されるので注意してください。この処理は BAC に悪影響を与えるものではありませんが、場合によっては、サーバの起動が遅くなったり、特定の統計情報やパフォーマンス カウンタに歪みが生じることがあります。

BAC ウォッチドッグ デーモンでアクションをトリガーするイベント（プロセス障害および再起動を含む）は、ログ ファイル *BPR_HOME/agent/logs/agent.log* に記録されます。ウォッチドッグ デーモンでは、重要なイベントも標準の `local6` ファシリティの下の syslog に記録されます。

管理者のユーザ インターフェイス

BAC 管理者のユーザ インターフェイスは、BAC システムを集中管理するための Web ベースのアプリケーションです。このインターフェイスを使用して、次の作業を行うことができます。

- グローバル デフォルトの設定
- カスタム プロパティの定義
- サービス クラスの設定
- ファームウェア ルールおよび設定テンプレートの管理
- デバイス情報の追加および編集
- デバイスのグループ化
- デバイス操作の実行
- サーバの状態と統計情報の表示
- デバイス履歴の表示
- サーバ ログの表示
- ユーザの管理

このインターフェイスの使用方法については、それぞれ次の章を参照してください。

- 管理者のユーザ インターフェイスについて（P.15-1）：BAC 管理者のユーザ インターフェイスにアクセスする方法や設定方法について説明します。
- 管理者のユーザ インターフェイスの使用方法（P.16-1）：各種 BAC コンポーネントのモニタリングなど、管理作業を行う方法について説明します。
- Broadband Access Center の設定（P.17-1）：BAC を設定するために実行する作業について説明します。

コマンドライン インターフェイス

BAC CLI は、Telnet または SSH を使用して DPE を設定したり、DPE の状態を表示したりするために使用する、IOS に似たコマンドライン インターフェイスです。CLI では、組み込み型のコマンドヘルプとコマンドのオートコンプリート機能がサポートされています。

CLI の認証は、ローカルで設定したログイン パスワードとイネーブル パスワード、または TACACS+ サービスのリモート ユーザ名とパスワードを使用してイネーブルにできます。

DPE CLI にアクセスするには、ローカル ホストまたはリモート ホストからポート 2323 への Telnet セッションを開きます。

ローカル ホストから DPE CLI へのアクセス

ローカル ホストから CLI にアクセスするには、次のコマンドを使用できます。

```
# telnet localhost 2323
```

または

```
# telnet 0 2323
```

リモート ホストから DPE CLI へのアクセス

リモート ホストから CLI にアクセスするには、次のコマンドを入力します。

```
# telnet remote-hostname 2323
```

（注） CLI への Telnet 接続を確立できない場合は、CLI サーバが稼働していない可能性があります。その場合は、次のように入力してサーバを起動します。

```
# /etc/init.d/bprAgent start cli
```

CLI にアクセスした後、続行するには DPE パスワードを入力する必要があります。デフォルトのログイン パスワードとイネーブル パスワードは **changeme** です。

DPE がサポートする CLI コマンドの詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

SNMP エージェント

BAC では、DPE サーバおよび RDU サーバについて基本的な SNMP v2 ベースのモニタリングがサポートされます。BAC SNMP エージェントでは SNMP 通知と SNMP トラップがサポートされます。snmp-server CLI コマンドを使用して DPE に SNMP エージェントを設定し、SNMP 設定 CLI コマンドを使用して RDU に SNMP エージェントを設定できます。

SNMP エージェントでは、サーバの状態、サーバ固有の統計情報、サーバ間の通信、ライセンス情報など、BAC の重要な詳細情報のモニタリングもサポートされます。

SNMP 設定コマンドライン ツールの詳細については、P.11-1 の「Broadband Access Center の監視」を参照してください。DPE CLI の詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

BAC ツール

BAC には、特定の機能をより効率的に実行するための自動ツールが用意されています。表 9-2 は、この BAC リリースでサポートされている各種ツールを示しています。

表 9-2　BAC ツールのリスト

ツール	説明	参照先
設定ツール	BAC のテンプレートと設定ファイルをテスト、検証、および表示するために使用されます。	設定ユーティリティの使用方法（P.5-23）
BAC プロセス ウォッチドッグ	BAC ウォッチドッグ デーモンと連動して BAC システム コンポーネントの状態を監視し、サーバを停止または起動します。	コマンドラインからの BAC プロセス ウォッチドッグの使用（P.9-2）
SNMP エージェント設定ツール	SNMP エージェントを管理します。	snmpAgentCfgUtil.sh ツールの使用方法（P.11-6）
RDU ログ レベル ツール	RDU のログ レベルを設定し、デバッグログ出力をイネーブルまたはディセーブルにします。	RDU ログ レベル ツール（P.19-6）
デバイス エクスポート ツール	BAC バックアップ データベースからデバイス情報を取得し、その情報をフラット ファイルにエクスポートします。	deviceExport.sh ツールの使用方法（P.18-2）
ディスク容量モニタリング ツール	1 つまたは複数のファイル システムのしきい値を設定します。これらのしきい値を超えると、追加のディスク領域が利用可能になるまでアラートが生成されます。	disk_monitor.sh ツールの使用方法（P.18-5）
Keytool ユーティリティ	DPE 上の HTTP over SSL サービスをサポートする、証明書ストア内の証明書を管理します。	keytool を使用した DPE 鍵ストアの設定（P.13-4）

データベースの管理

この章では、RDU データベースの管理および保守について説明します。RDU データベースは、Broadband Access Center（BAC）の中央データベースです。BAC RDU には、十分なディスク容量を確保すること以外、保守は事実上必要ありません。管理者は、データベースのバックアップ手順と回復手順について理解し、熟知している必要があります。

この章は、次の項で構成されています。

障害復元力について

RDU データベースでは、アプリケーション障害、システム障害、停電のような予測できない問題などが原因で発生するデータベースの破損を防止するために、*先行書き込みロギング*と呼ばれる手法を使用しています。

先行書き込みロギングでは、データベース ファイルに変更を書き込む前に、すべてのデータベース変更の記述をデータベース ログ ファイルに書き込みます。このメカニズムによって、システム障害の原因になった可能性がある不適切なデータベース書き込みを修復できます。

RDU サーバでは、起動されるたびに自動回復が実行されます。この回復処理時に、データとデータベース ファイルとの同期をとるために、データベース ログ ファイルが使用されます。データベース ログには書き込まれたものの、データベースには書き込まれていなかったデータベース変更は、この自動回復の処理中にデータベースに書き込まれます。

このようにして、先行書き込みロギングによって、RDU サーバの再起動時にデータベースが自動的に修復されるので、RDU サーバの障害時にデータベースが破損しないことが実質的に保証されます。

先行書き込みロギングが正しく機能するには、次の条件が必要です。

- ファイル　システムおよび物理ストレージが、要求時にデータを確実に物理ストレージ内にフラッシュするように設定されている必要があります。たとえば、書き込みキャッシュが SDRAM だけで構成されたストレージ システムは、システム障害中にデータが失われるので、適切ではありません。ただし、ディスクアレイの書き込みキャッシュがバッテリー バックアップされていて、システム障害時にもデータが失われないことが保証されている場合は正しく機能します。システムがバッテリーによりバックアップされた書き込みキャッシュを備えていない場合、要求時には、メモリ内のデータ キャッシュが実行される代わりにデータ ディスクがフラッシュされます。
- ファイル システムは、RDU データベースのブロック サイズに合せて、ブロック サイズが 8192 バイトに設定されている必要があります。Solaris では、通常、明示的に調整しない限り、この設定がデフォルトです。

データベース ファイル

RDU データベースでは、ファイルが格納されたパーティションをマウントしたファイル システムを使用して、データがバイナリ ファイルに保存されます。システム障害発生後の回復時間が長くならないようにファイル システムを選択し、設定することがきわめて重要です。

データベース ファイルは RDU の動作にとってきわめて重要です。したがって、誤って削除するなどの手作業による操作が行われないように、データベース ファイルを保護するための特別な予防措置を講じる必要があります。これらの重要ファイルを保護するための標準的なシステム管理方法に従ってください。たとえば、これらのファイルには、root ユーザだけがアクセス可能なアクセス権を与える必要があります。また、運用中のシステムには root ユーザではなく、root ユーザよりも権限の低いユーザとしてログインし、sudo コマンドを使用して root 特権が必要なタスクを実行することも、有効な方法です。

データベース ストレージ ファイル

RDU サーバは、データベース ディレクトリにある *bpr.db* というファイルに自身のデータベースを格納します。このディレクトリは *BPR_DATA/rdu/db* ディレクトリにあり、コンポーネントのインストール時に BPR_DATA パラメータを指定することで設定します。データベースの移動の詳細については、P.10-9 の「データベースの場所の変更」を参照してください。

(注) 通常、データベース　ファイルはランダムにアクセスされます。したがって、最高のデータベース パフォーマンスを得るためには、シーク時間が最も速く、回転アクセス レイテンシが最も小さいディスクを選択する必要があります。

データベースのトランザクション ログ ファイル

RDU サーバでは、データベースのトランザクション ログは 10 MB のファイルに保存され、そのファイルはデータベースのログ ディレクトリに保存されます。このディレクトリは、BPR_DBLOG パラメータを指定することでインストール時に設定します。ログ ディレクトリは、*BPR_DBLOG/rdu/dblog* ディレクトリにあります。トランザクション ログの新しいディレクトリへの移動の詳細については、P.10-9 の「データベースの場所の変更」を参照してください。

データベースのログ ファイルの名前には、最初に log.00000001、次に log.00000002 というように連番が付けられます。

(注) トランザクション　ログが保存されるディスクは、通常、シーケンシャルにアクセスされるので、データはログ ファイルの最後に追加されます。最高のデータベース パフォーマンスを達成するには、このアクセス パターンを効率的に処理できるディスクを選択する必要があります。システム上で最も高速なディスクにデータベースのトランザクション ログ ディレクトリを置くことをお勧めします。また、1 GB のディスク容量を使用可能にしてください。

自動ログ管理

データベースのトランザクション ログ ファイルは、トランザクション データのデータベースへの書き込みが完了するまで、そのデータを保存しておくために使用されます。その後、トランザクション ログ データは冗長になり、ファイルがシステムから自動的に削除されます。通常の状況では、データベースのトランザクション ログ ディレクトリ内にあるログ ファイルの数は数個以内にする必要があります。時間の経過とともに古いトランザクション ログはなくなり、新しいトランザクション ログが作成されます。

注意　データベースのトランザクション ログは、データベースにとって不可欠です。トランザクション ログ ファイルを手動で削除すると、データベースが破損します。

各種データベース ファイル

データベース ディレクトリには、他にもデータベースの動作に不可欠なファイルが保存されています。これらのファイルは、*rdu.db* ファイルとともに *BPR_DATA/rdu/db* ディレクトリにあり、データベース バックアップの一環としてコピーされます。

- DB_VERSION：データベースの物理的および論理的なバージョンを識別するためのもので、RDU によって内部で使用されます。
- *history.log*：ログ ファイルの自動的な削除、バックアップ、回復、復元処理などの不可欠なデータベース管理タスクに関するロギング動作のために使用されます。このログ ファイルは、管理者に有用な履歴情報を提供するだけでなく、RDU のデータベース処理にとっても非常に重要です。

ディスク容量の要件

完全に実装されたデータベースのサイズは、次の多くの要素で決まります。

- RDU が管理するデバイス オブジェクト
- 各オブジェクト上に保存されているカスタム プロパティ
- 各デバイスについてトラッキングされたデバイス履歴レコード

各パーティション上で必要なディスク容量の概算値は、次のとおりです。

- BPR_DATA（デバイス オブジェクトごとに約 3 ～ 5 KB）
- BPR_DBLOG（500 MB 以上）

注意　これらの数値は、単なる指針として示したものなので、通常のシステム監視の必要がなくなるわけではありません。

disk_monitor.sh ツールを使用すると、使用可能なディスク容量を監視したり、管理者に警告したりできます。詳細については、P.18-5 の「disk_monitor.sh ツールの使用方法」を参照してください。

ディスク容量不足の対処方法

RDU サーバでディスク容量が不足すると、syslog ファシリティを通じて syslog アラートが生成され、RDU ログが記録されます。その後、RDU サーバは自動的に再起動を試みます。RDU サーバが再起動を試みたときに `out of disk space` エラーが再び発生し、もう一度再起動が試みられる場合があります。

RDU サーバは、空きディスク容量が使用可能になるまで、繰り返し再起動しようとします。空き容量がほぼなくなっているディスク上である程度のディスク領域を解放すると、次の再起動で RDU が正常に起動します。

データベースのサイズが増大して現在のディスク パーティションの容量を超えた場合、そのデータベースを新しいディスクまたはパーティションに移動する必要があります。この操作を行う方法については、P.10-9 の「データベースの場所の変更」を参照してください。

(注)　ディスク容量の使用率を監視して障害を防止するのが望ましい方法です。詳細については、P.18-5 の「disk_monitor.sh ツールの使用方法」を参照してください。

バックアップと回復

RDU サーバは、サーバを停止したり、サーバの活動を一時停止したりしなくても実行できる、効率性の高いバックアップ処理をサポートしています。データベースのバックアップおよび回復は、次の手順から構成されます。

- バックアップ：稼働中のサーバから RDU データベースのスナップショットをとります。
- 回復：データベース スナップショットを再利用するための準備をします。
- 復元：回復したデータベース スナップショットを RDU サーバにコピーします。

これらの手順のそれぞれに自動ツールが用意されています。これらのツールは対話モードまたはサイレント モードで使用できますが、これらのツールを使用するには root 特権が必要です。

データベースのバックアップ

バックアップとは、データベース ファイルをバックアップ ディレクトリにコピーする処理です。そのときに、これらのファイルを圧縮し、テープやその他のアーカイブに保存することができます。

RDU データベースのバックアップは、サーバのアクティビティを中断しないでファイルをコピーするだけなので、非常に効率的です。ただし、RDU データベース ディスクにアクセスするため、バックアップを行うと RDU のパフォーマンスが低下する場合があります。その逆の場合もあります。バックアップ中に発生した RDU のアクティビティにより、バックアップのパフォーマンスが低下します。そのため、バックアップは、RDU の使用率の低い時間帯に行う必要があります。

バックアップのパフォーマンスは、同時に実行されているシステム アクティビティ以外に、基礎となっているディスクおよびファイル システムのパフォーマンスからも影響を受けます。基本的にバックアップ速度は、データベース ファイルをコピー元からコピー先へコピーする速度と同じです。

BPR_HOME/rdu/bin ディレクトリにある **backupDb.sh** ツールを使用して、データベースのバックアップを行います。

- このツールを使用するには、バックアップ ファイルを保存するバックアップ先ディレクトリを指定する必要があります。このディレクトリは、現在のデータベース ファイル サイズの 120% に相当する使用可能ディスク容量があるディスクまたはパーティション上に存在する必要があります。
- 次の例で説明するように、このツールは、ユーザが指定したディレクトリの下に、タイムスタンプ付きのサブディレクトリを自動的に作成し、そこにバックアップを保存します。

例

backupDb.sh ツールの使用例を次に示します。

```
# backupDb.sh /var/backup
```

/var/backup には、データベースのバックアップ ディレクトリを指定します。

この例では、バックアップするすべてのデータベース ファイルは */var/backup/rdu-backup-20020925-130345* というディレクトリに格納されます。最下位のサブディレクトリ（*rdu-backup-20020925-130345*）は自動的に作成され、現在のタイムスタンプが付けられます。

（注） タイムスタンプ付きのサブディレクトリの形式は、*rdu-backup-yyyyMMdd-HHmmss* です。この例では、サブディレクトリは *rdu-backup-20060427-175430* になります。これは、そのディレクトリに 2006 年 4 月 27 日午後 5 時 54 分 30 秒に開始したバックアップが保存されていることを意味しています。

また、**backupDb.sh** ツールは、自動的に経過を画面にレポートし、その動作を *history.log* に記録します。

(注) **backupDb.sh** ツールを使用するときに、**–help** オプションを使用すると、使用状況情報を取得できます。また、必要であれば、**–nosubdir** というオプションのフラグを使用して、サブディレクトリの自動作成をディセーブルにできます。

データベースの回復

データベースの回復とは、データベースを一貫性のある状態に戻す処理です。バックアップは稼働中の RDU 上で行われるので、データベースはコピー中に変更される場合があります。ただし、データベースのログ ファイルによって、データベースを一貫性のある状態に戻せることが保証されています。

回復は、データベースのスナップショットに対して行われます。つまり、このタスクは、稼働中の RDU サーバ上のデータベースには作用しません。回復タスクは、バックアップの直後か、または、データベースを RDU サーバに復元する前に実行できます。

(注) シスコでは、バックアップを行うたびに、その直後に回復を行うことを推奨しています。この方法をとると、緊急時にバックアップしたデータベースをより速やかに復元できます。

データベースの回復に要する時間は、バックアップの一環としてコピーするデータベースのログ ファイルの数によって決まり、したがって、バックアップの実行時の RDU のアクティビティ レベルによって決まります。バックアップの実行時に RDU が同時に実行している活動の数が多いほど、バックアップの一環としてコピーする必要があるトランザクション ログ ファイルの数が多くなり、回復に要する時間が長くなります。一般に、データベースの回復の所要時間は、トランザクション ログ ファイルあたり 10 ～ 60 秒です。

BPR_HOME/rdu/bin ディレクトリにある **recoverDb.sh** ツールを使用して、データベースのスナップショットの回復を行います。このツールを使用するときは、バックアップの場所を指定する必要があります。このディレクトリでは、回復も行われます。

例

recoverDb.sh ツールの使用例を次に示します。

```
# recoverDb.sh /var/backup/rdu-backup-20060427-130345
```

この例では、*/var/backup/rdu-backup-20060427-130345* ディレクトリにあるスナップショットを一貫性のある状態に回復します。回復処理の経過は画面に表示され、そのアクティビティはスナップショット ディレクトリにある *history.log* ファイルに記録されます。

(注) **recoverDb.sh** ツールを使用するときに、**–help** オプションを使用して、ツールの使用状況情報を取得できます。

データベースの復元

データベースの復元とは、あらかじめ回復したデータベースのスナップショットを、RDU サーバによって使用されるデータベース上の場所にコピーする処理です。復元できるのは、あらかじめ回復しておいたデータベースだけです。

データベースの復元とは現行の RDU データベースの交換を意味するので、最初に古いデータベースを適切に削除し、アーカイブすることが非常に重要になります。

（注） 置換中にデータベースの削除を絶対に行わないでください。古いデータベースのコピーを残しておくと、将来のシステム診断が簡単になる場合があります。

BPR_HOME/rdu/bin ディレクトリにある **restoreDb.sh** ツールを使用して、現行の RDU データベースを別のデータベースと置換します。このツールを使用するときは、入力ディレクトリを指定する必要があります。このディレクトリには、RDU サーバに復元するデータベースの、回復したバックアップ スナップショットが含まれている必要があります。

（注） **restoreDb.sh** ツールを実行する前に、RDU サーバを停止する必要があります。また、データベースをバックアップしてから、データベース ファイルを *rdu/db* ディレクトリおよび *rdu/dblog* ディレクトリから削除する必要もあります。

例

restoreDb.sh ツールの実行例を次に示します。

```
# restoreDb.sh /var/backup/rdu-backup-20060427-130345
```

この例では、*/var/backup/rdu-backup-200604275-130345* ディレクトリにあるデータベースが RDU サーバに復元されます。

（注） **restoreDb.sh** ツールを使用するときに、**–help** オプションを使用すると、このツールについての使用状況情報を取得できます。

復元処理の完了後は、RDU を再起動する必要があります。RDU ログ ファイルには、起動が成功したことを示すメッセージが書き込まれます。

このツールを実行すると、経過がモニタに表示され、その動作が *history.log* ファイルに記録されます。

データベースの場所の変更

あるパーティションまたはディスクから、同じシステム上の別のパーティションまたはディスクにデータベースを移動することができます。管理上の理由で、この処理が必要になる場合があります。この処理を行うには、RDU サーバおよび BAC プロセス ウォッチドッグを停止する必要があります。

データベースの場所を変更する処理では、システム パラメータを変更し、該当のファイルを新しい場所にコピーします。次のパラメータの一方または両方を調整できます。

- *BPR_DATA*：このパラメータは、インストール時に最初に設定され、データベース、およびログや設定ファイルなどその他多くの重要なファイルが保存されるディレクトリを示しています。

  また、このディレクトリには、特に BAC プロセス ウォッチドッグ、DPE（同じシステムにインストールされている場合）、RDU、および SNMP エージェントのログ データが格納されます。
- *BPR_DBLOG*：このパラメータは、インストール時に最初に設定され、データベースのトランザクション ログ ファイルが保存されるディレクトリを示しています。

上記のパラメータの値は、*BPR_DATA/bpr_definitions.sh* というファイルに記録されます。このファイルを変更した場合、システム上で実行されているすべての BAC コンポーネントを再起動する必要があります。

データベースおよびトランザクション ファイルの場所を変更するには、次の手順に従います。

ステップ 1　**/etc/init.d/bprAgent stop** コマンドを実行して BAC プロセス ウォッチドッグおよびすべての BAC コンポーネントを停止します。

ステップ 2　*BPR_HOME/bpr_definitions.sh* ファイルのバックアップ コピーを作成します。

ステップ 3　このファイルを編集して、*BPR_DATA* パラメータおよび *BPR_DBLOG* パラメータの一方または両方を新しいディレクトリに変更します。

ステップ 4　このファイルを保存します。

ステップ 5　*BPR_DATA* ディレクトリと *BPR_DBLOG* ディレクトリの一方または両方の元のディレクトリ構造および内容を、新しい場所にコピーまたは移動します。コピーを行う場合は、すべてのファイルおよびディレクトリのアクセス権が維持されるようにしてください。

ステップ 6　**/etc/init.d/bprAgent start** コマンドを実行して、BAC プロセス ウォッチドッグおよびすべての BAC コンポーネントを起動します。

ステップ 7　該当のログ ファイルを監視して、すべてのコンポーネントが正常に起動したことを確認します。

Broadband Access Center の監視

この章では、Broadband Access Center（BAC）配備内の中央 RDU サーバおよび DPE サーバを監視する方法について説明します。次のトピックについて説明します。

syslog アラート メッセージ

BAC のアラートは、Solaris の syslog サービスを通して生成されます。syslog は、Solaris 上で情報のロギングを管理するためのクライアント / サーバ プロトコルです。BAC の syslog アラートは、ロギング サービスではありません。問題が発生した場合には通知されますが、問題の原因がいつも特定されるとは限りません。この情報は、該当する BAC ログ ファイルに書き込まれる場合もあります。

メッセージ形式

BAC がアラート メッセージを生成するときの形式は次のとおりです。

XXX-#-####: Message

- *XXX*：ファシリティ コードを表します。これには、次のものが含まれます。
  - RDU（Regional Distribution Unit）
  - DPE（Device Provisioning Engine）
  - AGENT（rduSnmpAgent または dpeSnmpAgent）
- #：使用されている重大度のレベルを表します。アラートのレベルは次の 3 つです。
  - 1：アラートを表します。
  - 3：エラーを表します。
  - 6：情報メッセージを表します。
- ###：数字のエラー コードを表します。詳細については、次の項を参照してください。
- *Message*：アラートのテキスト（メッセージ）を表します。

RDU のアラート

表 11-1 は、RDU のアラートを示しています。

表 11-1　RDU のアラート

アラート	説明
RDU-1-101: RDU ran out of disk space	RDU サーバが使用するストレージ パーティションの容量が不足していることを示します。このエラーが発生すると、RDU は自動的に再起動を試みますが、通常は、利用可能なストレージ容量が増加するまで同じエラーが再び発生します。 ディスクのアップグレードの詳細については、P.18-1 の「BAC がサポートするツールと高度な概念」を参照してください。
RDU-1-103: RDU ran out of memory	RDU のメモリが不足していることを示します。このエラーが発生すると、RDU サーバは自動的に再起動します。
RDU-1-111: Evaluation key for technology *[technology_name]* expired	指定したテクノロジーの評価キーの期限が満了した場合に生成されます。シスコの営業担当または TAC にお問い合せのうえ、新しいライセンス キーを入手してください。
RDU-1-115: You have used *[percent]*% of available *[technology_name]* licenses.	ライセンスの総許容数のうち使用されているライセンスの数をパーセントで示します。このアラートは、ライセンスの総許容量の 80% に達すると生成されます。
BPR-RDU-4-1140: DNS took *X* seconds for lookup of address [10.0.0.1/test.com]; Check DNS configuration and health of servers	DNS からの応答に遅延が発生しているため、BAC のパフォーマンスが低下している可能性があることを示します。このアラートは、IP アドレスのルックアップが 60 秒を上回るたびに生成されます。

（注） RDU の syslog アラートが送信されるたびに、追加の詳細が *BPR_DATA/rdu/logs/rdu.log* というログ ファイルに書き込まれます（追加の詳細がある場合）。

DPE のアラート

DPE の syslog アラートが送信されるたびに、追加の詳細が DPE ログに書き込まれます。

DPE ログにアクセスするには、**show log** コマンドを使用します。詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

DPE エラーの中には、RDU サーバのログ ファイルに伝播されるものもあります。これらのエラーは、*BPR_DATA/rdu/logs/rdu.log* ファイルで確認できます。

表 11-2 は、DPE のアラートを示しています。

表 11-2　DPE のアラート

アラート	説明
DPE-1-102: DPE ran out of disk space	DPE サーバが使用するストレージ パーティションの容量が不足しています。次の 3 つの解決策があります。 **a.** ディスクに常駐する過剰のサポート バンドルをクリアします。そうするには、不要なサポート バンドルを別のコンピュータへ移動した後、DPE の CLI から **clear bundles** コマンドを実行します。 **b.** DPE の CLI から **clear logs** コマンドを実行して、ディスク領域をクリアします。 **c.** 最後の手段として、DPE の CLI から **clear cache** コマンドを実行して、すべてのキャッシュ ファイルを削除し、DPE を強制的に RDU サーバと再同期します。
DPE-1-104: DPE ran out of memory	DPE プロセスのメモリが不足しています。このエラー状態になると、DPE は自動的に再起動します。 DPE に存在するデバイス構成の数を確認します。デバイス構成の数が多いほど、使用されるメモリは多くなります。デバイス構成の数を減らすには、DPE がサービスするプロビジョニング グループ内のデバイスの数を制限します。
DPE-1-109: Failed to connect to RDU	RDU に接続できません。次の作業を行う必要があります。 **a.** DPE ネットワークが正しく構成および接続されていることを確認します。 **b.** **dpe rdu-server** コマンドを使用して、DPE が正しい RDU に接続するよう構成されていること、および接続ポートが正しく構成されていることを確認します。 **c.** RDU プロセスが正しいサーバで実行され、正しいポートで受信されていることを確認します。RDU への接続が確立されるまで、数秒ごとに DPE から RDU プロセスへの再接続が試行されます。

ウォッチドッグ エージェントのアラート

ウォッチドッグ プロセスによって syslog アラートが送信されるたびに、エラーの詳細が *BPR_DATA/agent/logs/agent_console.log* ファイルに書き込まれます（エラーの詳細がある場合）。また、アラートで言及されている特定のコンポーネントに対応したログ ファイルにも出力されます。たとえば、*The rdu unexpectedly terminated* のようなアラートを予期せず受信した場合は、RDU サーバのログ ファイル（*BPR_DATA/rdu/logs/rdu.log*）で追加の情報を確認します。表 11-3 はウォッチドッグ エージェントのアラートを示します。

表 11-3　ウォッチドッグ エージェントのアラート

アラート	説明
AGENT-3-9001: Failed to start the *component*	ウォッチドッグが特定のコンポーネントの開始に失敗したことを示します。
AGENT-3-9002: The *component* unexpectedly terminated	エージェント プロセスで監視されていた特定のコンポーネントが、不意に失敗したことを示します。
AGENT-3-9003: Failed to stop the*component*	ウォッチドッグ エージェントが終了しようとしたコンポーネントが停止しなかったことを示します。
AGENT-6-9004: The *component* has started	ウォッチドッグ エージェントがコンポーネントを正常に起動するたびに生成されます。このメッセージは情報の提供のみを目的としています。
AGENT-6-9005: The *component* has stopped	ウォッチドッグ エージェントがコンポーネントを正常に停止するたびに生成されます。このメッセージは情報の提供のみを目的としています。

表 11-3 でウォッチドッグ エージェントのアラート リストに示されている *component* 変数は、次のコンポーネント値のいずれかを表します。

- rdu
- dpe
- tomcat
- cli
- snmpAgent

SNMP の使用によるサーバの監視

BAC では、SNMP を使用したサーバの監視がサポートされています。具体的には、SNMP ベースの管理システムを使用して、BAC サーバの状態、ライセンスの使用状況情報、サーバ接続、およびサーバ固有の統計情報を監視できます。

SNMP エージェント

BAC SNMP エージェントでは SNMP 通知と SNMP トラップがサポートされます。これ以降、それらをまとめて「通知」と呼びます。snmp-server CLI コマンドを使用して DPE に SNMP エージェントを設定し、**snmpAgentCfgutil.sh** ツールを使用して RDU に SNMP エージェントを設定できます。

SNMP 設定コマンドライン ツールの詳細については P.11-6 の「snmpAgentCfgUtil.sh ツールの使用方法」、DPE CLI の詳細については『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

MIB のサポート

BAC では、数種類の MIB がサポートされます。次の MIB があります。

- CISCO-BACC-DPE-MIB
- CISCO-BACC-RDU-MIB
- CISCO-BACC-SERVER-MIB

表 11-4 は、BAC でサポートされる MIB をまとめたものです。

表 11-4　BAC でサポートされる MIB

インストール コンポーネント	サポート対象の MIB
DPE	CISCO-BACC-SERVER-MIB
	CISCO-BACC-DPE-MIB
RDU	CISCO-BACC-SERVER-MIB
	CISCO-BACC-RDU-MIB

RDU SNMP エージェントでは、RDU の管理対象オブジェクトを定義する CISCO-BACC-RDU-MIB がサポートされます。この MIB は、RDU の状態に関する統計情報および RDU と DPE の間の通信インターフェイスに関する統計情報を定義します。

DPE SNMP エージェントでは、DPE の管理対象オブジェクトを定義する CISCO-BACC-DPE-MIB がサポートされます。この MIB は、基本的な DPE 設定情報および統計情報を提供します。

SNMP エージェントは CISCO-BACC-SERVER-MIB をサポートします。この MIB は、BAC 上のすべてのサーバに共通の管理対象オブジェクトを定義します。この MIB は、同一のデバイスにインストールされている複数の BAC サーバのモニタリングをサポートします。サーバの状態が変化するたびに `ciscoBaccServerStateChanged` 通知が生成されます。

(注) すべてのオブジェクトの説明については、*BPR_HOME/rdu/mibs* ディレクトリにある対応する MIB ファイルを参照してください。

snmpAgentCfgUtil.sh ツールの使用方法

snmpAgentCfgUtil.sh ツールを使用すると、Solaris システム上の SNMP エージェントを管理できます。

このツールは *BPR_HOME/snmp/bin* ディレクトリにあり、これを使用して、SNMP 通知を受信する他のホストのリストにホストを追加（またはリストから削除）したり、SNMP エージェント プロセスを起動および中止できます。

（注） Solaris コンピュータ上で動作する SNMP エージェントのデフォルト ポート番号は 8001 です。

snmpAgentCfgUtil.sh ツールは、次の操作に使用できます。

- ホストの追加（P.11-6）
- ホストの削除（P.11-7）
- SNMP エージェント コミュニティの追加（P.11-7）
- SNMP エージェント コミュニティの削除（P.11-8）
- SNMP エージェントの開始（P.11-8）
- SNMP エージェントの停止（P.11-9）
- SNMP エージェントの場所の変更（P.11-9）
- SNMP の連絡先の設定（P.11-10）
- SNMP エージェントの設定の表示（P.11-10）

ホストの追加

SNMP エージェントから SNMP 通知を受信するホストのリストにホスト アドレスを追加するには、次のコマンドを使用します。

構文の説明

snmpAgentCfgUtil.sh add host *host-addr* **community** *community* [**udp-port** *port*]

- *host-addr*：ホストのリストに追加するホストの IP アドレスを指定します。
- *community*：SNMP 通知を送信するときに使用するコミュニティ（リードまたはライト）を指定します。
- *port*：SNMP 通知の送信に使用する UDP ポートを示します。

例

```
# ./snmpAgentCfgUtil.sh add host test.cisco.com community trapCommunity udp-port 162
OK
Please restart [stop and start] SNMP agent.
```

（注） このコマンドを使用して加えた変更は、**/etc/init.d/bprAgent restart snmpAgent** コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-1 の「BAC プロセス ウォッチドッグ」を参照してください。

ホストの削除

SNMP エージェントから SNMP 通知を受信するホストのリストからホストを削除するには、次のコマンドを使用します。

構文の説明

snmpAgentCfgUtil.sh delete host *host-addr*

host-addr：ホストのリストから削除するホストの IP アドレスを指定します。

例

```
# ./snmpAgentCfgUtil.sh delete host test.cisco.com
OK
Please restart [stop and start] SNMP agent.
```

（注） このコマンドを使用して加えた変更は、**/etc/init.d/bprAgent restart snmpAgent** コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-1 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェント コミュニティの追加

SNMP コミュニティ ストリングを追加して、SNMP エージェントへのアクセスを制限するには、次のコマンドを使用します。SNMP コミュニティ名は、BAC SNMP エージェントにアクセスする SNMP マネージャとの間で共有秘密情報として使用されます。

構文の説明

snmpAgentCfgUtil.sh add community *string* [***ro*** | ***rw***]

- *string*：SNMP コミュニティを示します。
- **ro**：読み取り専用（**ro**）のコミュニティ ストリングを割り当てます。実行できるのは *get* 要求（クエリー）だけです。`ro` コミュニティ ストリングは、**get** 要求を許可しますが、**set** 操作は許可しません。ネットワーク管理システムと管理対象デバイスは、同じコミュニティ ストリングを参照する必要があります。
- **rw**：読み取りと書き込み（**rw**）コミュニティ ストリングを割り当てます。SNMP アプリケーションでは、**set** 操作に rw アクセスが必要です。`rw` コミュニティ ストリングを使用すると、Object Identifier（OID; オブジェクト識別子）値への書き込みアクセスが可能になります。

（注） デフォルトの **ro** および **rw** コミュニティ ストリングは、それぞれ `bacread` と `bacwrite` です。BAC を配備する前に、これらの値を変更することをお勧めします。これらの値を変更するには、新しいコミュニティ名を追加し、古いコミュニティ名を削除します。

例

```
# ./snmpAgentCfgUtil.sh add community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```

（注） このコマンドを使用して加えた変更は、**/etc/init.d/bprAgent restart snmpAgent** コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-1 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェント コミュニティの削除

SNMP コミュニティ ストリングを削除して、SNMP エージェントへのアクセスを禁止するには、次のコマンドを使用します。

構文の説明

snmpAgentCfgUtil.sh delete community *string* [***ro*** | ***rw***]

- *string*：SNMP コミュニティを示します。
- **ro**：読み取り専用（**ro**）のコミュニティ ストリングを割り当てます。
- **rw**：読み取りと書き込み（**rw**）コミュニティ ストリングを割り当てます。

（注） **ro** および **rw** コミュニティ ストリングの詳細については、P.11-7 の「SNMP エージェント コミュニティの追加」を参照してください。

例

```
# ./snmpAgentCfgUtil.sh delete community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```

（注） このコマンドを使用して加えた変更は、**/etc/init.d/bprAgent restart snmpAgent** コマンドを使用して SNMP エージェントを再起動するまで有効になりません。詳細については、P.9-1 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェントの開始

BAC がすでにインストールされている Solaris コンピュータで SNMP エージェント プロセスを開始するには、次のコマンドを使用します。

（注） SNMP エージェントは、**/etc/init.d/bprAgent start snmpAgent** コマンドを使用して BAC ウォッチドッグ プロセス エージェントを起動することでも開始できます。詳細については、P.9-2 の「コマンドラインからの BAC プロセス ウォッチドッグの使用」を参照してください。

例

```
# ./snmpAgentCfgUtil.sh start
Process snmpAgent has been started
```

SNMP エージェントの停止

BAC がすでにインストールされている Solaris コンピュータで SNMP エージェント プロセスを停止するには、次のコマンドを使用します。

（注）SNMP エージェントは、**/etc/init.d/bprAgent stop snmpAgent** コマンドを使用して BAC ウォッチドッグ プロセス エージェントを起動することでも停止できます。詳細については、P.9-2 の「コマンドラインからの BAC プロセス ウォッチドッグの使用」を参照してください。

例

```
# ./snmpAgentCfgUtil.sh stop
Process snmpAgent has stopped
```

SNMP エージェント リスニング ポートの設定

SNMP エージェントがリッスンするポート番号を指定するには、次のコマンドを使用します。RDU SNMP エージェントが使用するデフォルト ポート番号は 8001 です。

構文の説明

snmpAgentCfgUtil.sh udp-port *port*

port：SNMP エージェントがリッスンするポート番号を示します。

例

```
# ./snmpAgentCfgUtil.sh udp-port 8001
OK
Please restart [stop and start] SNMP agent.
```

SNMP エージェントの場所の変更

SNMP エージェントを実行するデバイスの場所を示す際に使用するテキスト文字列を入力するには、次のコマンドを使用します。たとえば、この文字列を使用してデバイスの物理的な場所を示すことができます。最大 255 文字の任意の文字列を入力できます。

構文の説明

snmpAgentCfgUtil.sh location *location*

location：エージェントの場所を示す文字列を指定します。

例

次の例では、SNMP エージェントの物理的な場所は、*equipment rack 5D* と示された装置ラックです。

```
# snmpAgentCfgUtil.sh location "equipment rack 5D"
```

SNMP の連絡先の設定

SNMP エージェントの連絡担当者と、この担当者への連絡方法を示す際に使用できるテキスト文字列を入力するには、次のコマンドを使用します。たとえば、この文字列を使用して、特定の担当者（電話番号を含む）を示すことができます。最大 255 文字の任意の文字列を入力できます。

構文の説明

snmpAgentCfgUtil.sh contact *contact-info*

contact-info：SNMP エージェントに関する連絡担当者を示す文字列を指定します。

例

次の例では、連絡担当者の名前は *Ace Duffy* で、内線番号は *1234* です。

```
# ./snmpAgentCfgUtil.sh contact "Ace Duffy - ext 1234"
```

SNMP エージェントの設定の表示

現在の SNMP 設定をすべて表示するには、次のコマンドを使用します。

構文の説明

snmpAgentCfgUtil.sh show

例

```
# ./snmpAgentCfgUtil.sh show
Location                      : Washington_1
Contact                       : John
Port Number                   : 8001
Notification Type             : trap
Notification Recipient Table  :
        [ Host IP address, Community, UDP Port ]
        [ 10.10.10.1, public, 162 ]
Access Control Table          :
        Read Only Communities
                bacread
        Read Write Communities
                bacwrite
```

SNMP 通知タイプの指定

SNMP エージェントから送信される通知のタイプ（トラップまたは通知）を指定するには、次のコマンドを使用します。デフォルトではエージェントからトラップが送信されますが、SNMP 通知を送信するように設定することもできます。

構文の説明

snmpAgentCfgUtil.sh inform [**retries** *retry_count* **timeout** *timeout*] | **trap**

パラメータは、リトライ間のバックオフ タイムアウトです。

例

```
snmpAgentCfgUtil.sh inform retries 3 timeout 1000
OK
Please restart [stop and start] SNMP agent.
```

（注） 設定内容を確認するには、**snmpAgentCfgUtil.sh show** コマンドを使用します。

```
#  ./snmpAgentCfgUtil.sh show
Location                      : <unknown>
Contact                       : <unknown>
Port Number                   : 8001
Notification Type             : inform
Notification Retries          : 3
Notification Timeout          : 1000
Notification Recipient Table  :
        [ Host IP address, Community, UDP Port ]
Access Control Table          :
        Read Only Communities
                bacread
        Read Write Communities
                bacwrite
```

サーバ状態の監視

この項では、BAC 配備内の RDU サーバおよび DPE サーバのパフォーマンスを監視する方法について説明します。監視対象のサーバは、中央 RDU サーバと DPE サーバです。

サーバ統計情報は、次の手段で確認できます。

- 管理者のユーザ インターフェイス
- DPE CLI
- RDU ログ ファイルおよび DPE ログ ファイル（管理者のユーザ インターフェイスまたは DPE CLI を使用）

管理者のユーザ インターフェイスの使用方法

管理者のユーザ インターフェイスで利用可能なサーバ統計情報を表示するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Server** タブをクリックします。

ステップ 2　セカンダリ ナビゲーション バーに、DPEs、Provisioning Group、RDU といったオプションが表示されます。

次のいずれかをクリックします。

- **DPEs** タブ：BAC データベースに現在登録されているすべての DPE を監視する場合
- **RDU** タブ：RDU の状態および統計情報を表示する場合

ステップ 3　クリックしたタブに応じて、次のように表示されます。

- **DPEs**：Manage Device Provisioning Engine ページが表示されます。このページに表示される各 DPE 名は、その DPE の詳細を表示する別ページへのリンクになっています。詳細ページを表示するには、このリンクをクリックします。
- **RDU**：View Regional Distribution Unit Details ページが表示されます。

DPE CLI の使用方法

DPE サーバの状態を監視するには、**show dpe** コマンドを実行して、DPE が動作しているかどうかを確認し、プロセスの状態と、DPE が動作している場合は、動作状態に関する統計情報を表示します。

（注）　このコマンドでは、DPE が正常に動作しているかどうかは示されません。プロセス自体が現在実行されていることだけが示されます。ただし、DPE が動作していれば、このコマンドで出力される統計情報を使用して、DPE が正常に要求を処理しているかどうかを判別できます。

例 11-1　show dpe の出力

```
dpe# show dpe
BAC Agent is running
Process dpe is not running

This result occurs when the DPE is not running.
dpe# show dpe
BAC Agent is running
Process dpe is running
Version BAC 3.0 (SOL_CBAC3_0_L_000000000000).
Caching 1 device configs and 1 external files.
0 sessions succeed and 0 sessions failed.
0 file requests succeed and 0 file requests failed.
0 immediate proxy operations received: 0 succeed, and 0 failed.
Connection status is Ready.
Running for 4 hours 30 mins 16 secs.
```

この結果は、DPE が動作している場合に発生します。

（注） 詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

パフォーマンス統計情報の監視

BAC では、システム パフォーマンスのトラブルシューティングに役立つさまざまな統計情報が提供されます。統計情報は、RDU、Provisioning API Command Engine、およびデバイス操作を含む、さまざまな主要コンポーネントで使用可能です。

パフォーマンス統計情報の収集は、管理者のユーザ インターフェイスまたは DPE CLI からイネーブルにできます。

- RDU　に関するパフォーマンス統計情報をイネーブルまたはディセーブルにするには、ユーザ インターフェイスから **Configuration > Defaults > System Defaults** を選択します。
  - この機能をイネーブルにするには、Performance Statistics Collection の **Enabled** オプション ボタンをクリックします。
  - この機能をディセーブルにするには、Performance Statistics Collection の **Disabled** オプション ボタンをクリックします。
- DPE　に関するパフォーマンス統計情報をイネーブルまたはディセーブルにするには、enabled モードの DPE CLI から **debug dpe statistics** を入力します。CLI からパフォーマンス統計情報をディセーブルにするには、**no debug dpe statistics** コマンドを使用します。

（注） デバッグ コマンドを使用する前に、**debug on** コマンドを実行して、DPE デバッグがイネーブルであることを確認してください。詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

パフォーマンス統計情報機能をイネーブルにした後は、*perfstat.log* ファイルのパフォーマンス統計情報を表示したり、**runStatAnalyzer.sh** ツールを使用してデータを分析したりできます。

管理者のユーザ インターフェイスを使用して、CWMP 統計情報を具体的に表示することもできます。**Servers > DPEs > Manage Device Provisioning Page > View Device Provisioning Engines Details** を選択します（図 16-5 を参照してください）。

パフォーマンス統計情報の収集の詳細については、次の各項を参照してください。

- perfstat.log について（P.11-14）
- runStatAnalyzer.sh について（P.11-15）

perfstat.log について

perfstat.log ファイルに記録されたデータを使用することで、パフォーマンス統計情報を監視できます。このファイルには、特定の間隔（5 分）で統計情報データが記録されます。*perfstat.log* ファイルは、RDU 用（*BPR_DATA/rdu/logs/statistics*）と DPE 用（*BPR_DATA/dpe/logs/statistics*）でそれぞれ別のディレクトリにあります。

各 *perfstat.log* ファイルには、最小で 1 日分、最大で 30 日分のデータが格納されます。パフォーマンス統計情報機能のオン / オフを切り替えることができるので、ログのデータは、必ずしも連続する日のデータではない場合があります。

perfstat.log ファイルの名前は、*perfstat.N*.log という形式で毎日変更されます。*N* は 1 ～ 29 のいずれかの値となります。たとえば、*perfstat.29.log* は最も古いログで、*perfstat.1.log* は最も新しく名前変更された *perfstat.log* ファイルです。

（注）　データは、カンマ区切りのベクトル形式で格納されます。各統計情報の形式は *yyyymmdd:hh:mm, component, interval-in-milliseconds, stat1-tag, stat1-value, stat2-tag, stat2-value, …* です。*stat1-tag* と *stat1-value* は、それぞれ各統計情報のタグ ID と値を示します。

runStatAnalyzer.sh について

BAC では、**runStatAnalyzer.sh** ツールを使用することで、パフォーマンス統計情報を分析したり、要約を出力したりできます。収集されたパフォーマンス統計情報を分析するには、次のディレクトリから **runStatAnalyzer.sh** ツールを実行します。

- *BPR_HOME/rdu/bin* ディレクトリ（RDU の場合）
- *BPR_HOME/dpe/bin* ディレクトリ（DPE の場合）

構文の説明

```
# runStatAnalyzer.sh [-d perfdata-dir] [-s start-time] [-e end-time] [-c component]
[-f output-format] [-help] [-help components] [-help statistics [component]]
```

- **perfdata-dir**：パフォーマンス統計情報を分析する対象のディレクトリを指定します。これは、次のデフォルト ディレクトリにある *perfstatN.dat* ファイルです。
  - *BPR_HOME/rdu/logs/statistics*（RDU の場合）
  - *BPR_HOME/dpe/logs/statistics*（DPE の場合）
- *start-time*：収集されたデータの分析を開始する時刻を指定します。デフォルトでは、収集された統計情報はすべて報告されます。*start-time* を指定するには、*yyyy-mm-dd:hh:mm* という時刻形式を使用します。
- *end-time*：収集されたデータの分析を終了する時刻を指定します。デフォルトでは、収集された統計情報はすべて報告されます。*end-time* を指定するには、*yyyy-mm-dd:hh:mm* という時刻形式を使用します。
- *component*：統計情報を分析する対象の BAC コンポーネントを指定します。すべてのコンポーネントを指定するか（ **all** オプションを使用）、サポートされているコンポーネントのリストから指定するかを選択できます。コンポーネントのリストを次に示します。

コンポーネント オプション	説明	該当サーバ	
		RDU	DPE
pace	Provisioning API Command Engine	✓	
rdu	Regional Distribution Unit	✓	
ext	拡張	✓	
cwmp	CWMP サービス		✓
httpfile	HTTP ファイル サービス		✓
proxyreq	Proxy Request Operations	✓	✓

（注）　デフォルトでは、すべてのコンポーネントの統計情報が分析されます。

- *output-format*：出力の形式を指定します。次の形式があります。
  - **summary**：トランザクション レートの要約を出力します。これがデフォルトのオプションです。

（注）　トランザクション レートの要約は、*perfstat.log* に記録された 5 分間隔のデータに基づいて計算されます。

－　**log**：ログ メッセージのような形式で出力します。

- **-help**：**runStatAnalyzer.sh** ツールの使用方法についての情報を提供します。
- **-help components**：統計情報の分析が可能な BAC コンポーネントについての情報を提供します。
- **-help statistics** *component*：各 BAC コンポーネントが返す統計情報についての情報を提供します。**pace**、**rdu**、**ext**、**cwmp**、**httpfile**、**proxyreq** のすべてのコンポーネントのヘルプを表示するか（**all** オプションを使用）、個々のコンポーネントのヘルプを表示するかを選択できます。

例 11-2　runStatAnalyzer.sh を使用したログ出力

```
# runStatAnalyzer.sh -s 2006-04-11:12:59 -e 2006-04-11:13:09 -c pace -f log

2006-04-11:12:59 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full
Queue 0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0;
Processed 0; Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec;
Processing maxTime 0 msec; CRS Completed 0
2006-04-11:13:04 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full
Queue 0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0;
Processed 0; Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec;
Processing maxTime 0 msec; CRS Completed 0
2006-04-11:13:09 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full
Queue 0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0;
Processed 0; Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec;
Processing maxTime 0 msec; CRS Completed 0
```

（注）　使用可能な統計情報の数は、指定したコンポーネントによって異なります。

例 11-3　runStatAnalyzer.sh を使用した要約出力

```
# runStatAnalyzer.sh -s 2006-04-11:12:59 -e 2006-04-11:13:29 -c pace -f summary

2006-04-11:13:04 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full
Queue 0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0;
Processed 0; Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec;
Processing maxTime 0 msec; CRS Completed 0
2006-04-11:13:29 PACE statistics last 30 minutes- In Queue 0; Dropped 0; Dropped-Full
Queue 0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0;
Processed 0; Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec;
Processing maxTime 0 msec; CRS Completed 0
```

（注）　要約データが表示されるのは、指定された間隔についてデータの完全なセットが利用可能な場合に限られます。たとえば、要約間隔が 30 分の場合、要約出力が表示されるのは 30 分ぶんのデータがある場合のみです。使用可能なデータに応じて、要約間隔は 5 分、30 分、60 分、3 時間、6 時間、12 時間、24 時間、7 日、14 日、21 日、30 日です。

CWMP サービスの設定

この章では、Broadband Access Center（BAC）で CWMP サービスを設定する方法について説明します。この章では、次のトピックについて説明します。

（注） プロビジョニング API を使用すると、管理者のユーザ インターフェイスから可能な多くの操作を実行できます。

CWMP サービスの設定値

CWMP は、GetParameterValues、SetParameterValues などの、リモート プロシージャ コール（RPC）のセットの仕様です。これらの RPC は、BAC が顧客宅内装置（CPE）を管理するためにパラメータの読み取りまたは書き込みを行う汎用メカニズムを定義します。次のパラメータがあります。

- デバイス構成情報
- ステータス情報
- パフォーマンス統計情報

DPE CLI を使用すると、DPE 上で CWMP 機能をイネーブルまたはディセーブルにできます。

DPE 上で設定できる機能には、次のものがあります。

- HTTP ベースの Basic または Digest 認証
- 証明書ベースの認証
- HTTP over SSL/TLS サービス設定
- 不明なデバイスの処理
- デバッグ設定
- セッション管理設定
- CWMP サービス設定
- HTTP ファイル サービス設定

これらのプロパティを設定する方法については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

DPE でのサービス ポートの設定

CWMP サービスがデバイスと通信するときに使用するポートを設定できます。要件に応じて、CWMP サービスの各インスタンス（CWMP RPC サービスおよび HTTP ファイル サービス）を個別に設定できます。表 12-1 は、サービスごとに、ポートを設定する方法を示しています。

表 12-1　サービスポートの設定

コマンド	構文の説明	デフォルト
CWMP RPC サービスの設定		
service cwmp *num* **port** *port*	• *num*：CWMP サービスを示します。1 または 2 になります。 • *port*：サービスで使用するポート番号を示します。	デフォルトでは、CWMP サービスは次のポートでリッスンするように設定されています。 • サービス 1 の場合：ポート 7547 • サービス 2 の場合：ポート 7548

	例：
	`dpe# service http 1 port 7547`
	`% OK (Requires DPE restart "# dpe reload")`	

表 12-1　サービスポートの設定（続き）

コマンド	構文の説明	デフォルト
HTTP ファイル サービスの設定		
service http *num* **port** *port*	• *num*：HTTP ファイル サービスを示します。1 または 2 になります。 • *port*：サービスで使用するポート番号を示します。	デフォルトでは、HTTP ファイル サービスは次のポートでリッスンするように設定されています。 • サービス 1 の場合：ポート 7549 • サービス 2 の場合：ポート 7550

	例：
	`dpe# service http 1 port 7549`
	`% OK (Requires DPE restart "# dpe reload")`	

（注） 設定手順の詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

接続要求サービス

接続要求は、DPE との CWMP セッションを確立するようにデバイスに指示します。BAC 接続要求サービスを使用すると、デバイス上で設定を有効にしたり、デバイスのファームウェア変更を実行したり、デバイスで即時操作を実行したりできます。

DPE によって開始された場合、接続要求は、DPE がデバイスとのセッションを確立するときに使用可能な唯一の方法です。セッションが確立されると、デバイスまたは DPE は、デバイス操作および設定変更を含む、任意の RPC を実行できます。

図 12-1　BAC における接続要求

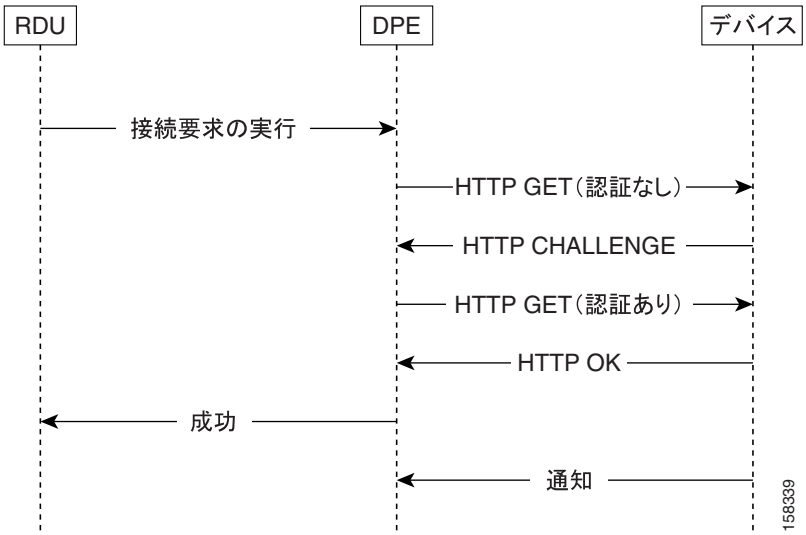


図 12-1 では、BAC における接続要求のフローについて説明します。RDU は、接続要求を、デバイスのプロビジョニング グループ内で使用可能な最適な DPE に委任します。接続要求が終了すると、DPE は結果を RDU に通知します。

接続要求オプションの設定

BAC を使用すると、次のプリファレンスを設定することにより接続要求の動作を制御できます。

- 認証の設定
- 接続要求方式の設定
- 到達可能性の設定

(注) プリファレンスは、デバイス オブジェクト上またはそのプロパティ階層内で設定できます。

認証の設定

RDU のデバイス オブジェクトで設定した 2 つのプロパティは、認証に影響を及ぼします。これらのプロパティは次のとおりです。

- API の場合：
  - `IPDeviceKeys.CONNECTION_REQUEST_USERNAME`
  - `IPDeviceKeys.CONNECTION_REQUEST_PASSWORD`
- 管理者のユーザ インターフェイスの場合：
  - **Devices** > **Modify Device** > Connection Request User Name field
  - **Devices** > **Modify Device** > Connection Request Password field

    Add Device ページでデバイスを追加するときに接続要求ユーザ名およびパスワードを設定したり、Modify Device ページでユーザ名およびパスワードを変更したりすることもできます。

どちらのプロパティも、DPE-CPE 認証に使用される接続要求ユーザ名およびパスワードを制御します。このユーザ名とパスワードは、DPE とデバイスの間で CWMP セッションを認証するために使用されるユーザ名およびパスワードとは異なります。これらのプロパティは単一のデバイス用なので、デバイス オブジェクトでしか設定できません。

接続要求パスワードを指定していない場合は、DPE に対してデバイスを認証する CWMP セッション パスワードが使用されます。接続要求ユーザ名も指定されていない場合、デバイス ID が使用されます。

(注) 接続要求の認証中に認証チャレンジを発行するかどうかは、図 12-1 が示すとおり、デバイスによって異なります。DPE は、HTTP Digest 認証によりチャレンジされることを予期しています。接続要求の処理のための DPE 設定はありません。

(注) API プロパティでは、デバイス パラメータは自動的には更新されません。対応する値をデバイス上で事前に設定するか、これらのプロパティを参照可能な設定テンプレートを使用して値を設定する必要があります。

接続要求方式の設定

プロビジョニング API または管理者のユーザ インターフェイスを使用して、BAC が接続要求の実行を試みる方式を指定できます。選択した方式により、デバイスにアクセスするときに使用される接続要求 URL を BAC が判別する方法が決定されます。

API プロパティ `IPDeviceKeys.CONNECTION_REQUEST_METHOD` では、接続要求の方式を指定します（各方式については次に説明します）。

（注） このプロパティは、デバイス階層の任意の場所で指定できます。

管理者のユーザ インターフェイスを使用してデフォルトの接続要求方式を設定するには、**Configuration > Default > CWMP Defaults** を選択し、ドロップダウン リストのオプションを選択します。

BAC は、接続要求を設定する次の 3 つの方式をサポートします。

- Discovered
- Using FQDN
- Using IP

方式によってパフォーマンス レベルと管理性が異なるので、接続要求の方式を選択するときは、パフォーマンスと管理性を考慮する必要があります。接続要求の方式を選択する前に、各方式の推奨事項を参照してください。

Discovered 方式の接続要求

Discovered 方式では、CPE が DPE と対話する間、DPE がデバイスと対話するたびに、InternetGatewayDevice.ManagementServer.ConnectionRequestURL パラメータに対応するデバイスの接続要求 URL を検出するようにデータ同期命令を修正します。RDU は、このパラメータに対するすべての更新を記録し、接続要求を行うときにその情報を使用します。

（注） 接続要求が試行される前に、この値が検出されている必要があります。

推奨事項：このパラメータ値はデバイスの WAN IP アドレスが変更されるたびに変化し、すべての更新が RDU に格納される必要があるので、これは接続要求で最適な方法ではありません。

Use FQDN 方式の接続要求

Use FQDN 方式は、RDU でそのデバイスに指定されている完全修飾ドメイン名（FQDN）を使用して、デバイスの接続要求 URL を構築します。この方式は、FQDN を、API で次のプロパティに指定されている値とともに使用します。

- `IPDeviceKeys.CONNECTION_REQUEST_PORT`
- `IPDeviceKeys.CONNECTION_REQUEST_PATH`

これらのプロパティは、管理者のユーザ インターフェイス上でも指定できます。手順は次のとおりです。

ステップ 1　**Devices > Manage Devices** を選択します。

ステップ 2　次の方法のいずれかを使用します。

- デバイス レコードを追加します。追加するには、**Add** ボタンをクリックします。Add Device ページが表示されます。
- デバイス レコードを検索します。検索するには、Search Type を指定し、選択する検索タイプに固有の画面コンポーネントの値を入力します。デバイスのリストが表示されます。目的のデバイスに対応する Identifier リンクをクリックします。Modify Device ページが表示されます。

ステップ 3　Property Name ドロップダウン リストから /IPDevice/connectionRequestPort および /IPDevice/connectionRequestPath のプロパティを選択し、Property Value フィールドに適切な値を入力します。

（注）　/IPDevice/connectionRequestPort および /IPDevice/connectionRequestPath の API 定数は、それぞれ `IPDeviceKeys.CONNECTION_REQUEST_PORT` および `IPDeviceKeys.CONNECTION_REQUEST_PATH` です。

ステップ 4　**Add** をクリックします。

（注）　ポートとパスのプロパティは、プロパティ階層の任意の場所で指定できます。

推奨事項：Use FQDN 方式は、デバイスの正しい IP アドレスを使用して更新している DNS に依存するので、デバイスの IP アドレスが変更されるたびに BAC を更新する必要はありません。それ以降、このオプションは、接続要求で最もスケーラブルなオプションです。

Use IP 方式の接続要求

Use IP 方式は、Discovered 方式と同じメカニズムを使用してデバイスの WAN IP アドレスを検出します。その後、次の API プロパティの値を使用してデバイスの接続要求 URL を構築します。

- `IPDeviceKeys.CONNECTION_REQUEST_PORT`
- `IPDeviceKeys.CONNECTION_REQUEST_PATH`

これらのプロパティは、管理者のユーザ インターフェイス上でも指定できます。手順は次のとおりです。

ステップ 1　**Devices > Manage Devices** を選択します。

ステップ 2　次の方法のいずれかを使用します。

- デバイス レコードを追加します。追加するには、**Add** ボタンをクリックします。Add Device ページが表示されます。
- デバイス レコードを検索します。検索するには、Search Type を指定し、選択する検索タイプに固有の画面コンポーネントの値を入力します。デバイスのリストが表示されます。目的のデバイスに対応する Identifier リンクをクリックします。Modify Device ページが表示されます。

ステップ 3　Property Name ドロップダウン リストから /IPDevice/connectionRequestPort および /IPDevice/connectionRequestPath のプロパティを選択し、Property Value フィールドに適切な値を入力します。

（注）　/IPDevice/connectionRequestPort および /IPDevice/connectionRequestPath の API 定数は、それぞれ `IPDeviceKeys.CONNECTION_REQUEST_PORT` および `IPDeviceKeys.CONNECTION_REQUEST_PATH` です。

ステップ 4　**Add** をクリックします。

推奨事項：Use IP 方式は、デバイスの WAN IP アドレスを持つ RDU に依存しているので、接続要求を試行する前に WAN IP アドレスが検出される必要があります。また、デバイスの WAN IP アドレスは変更されるので、新しい IP アドレスを使用して RDU を更新する必要があります。したがって、このオプションは、接続要求に最適な方式ではありません。

接続要求のディセーブル化

接続要求サービスをディセーブルにするように選択できます。このオプションは、デバイスが NAT を使用しており、接続要求が可能ではない場合に便利です。

（注）　接続要求がディセーブルになっている場合でも、API デバイス操作を介して ConnectionRequest を使用できます。

到達可能性の設定

到達可能性は、接続要求の設定で重要な役割を果たします。デバイスの報告された IP アドレスとその発信元 IP アドレスが一致しない場合、それはデバイスが NAT 標準を使用していることを示すので、BAC は接続要求を拒否します。そのため、通常、設定要求は正常に実行されません。この動作は、管理者のユーザ インターフェイスまたは API から変更できます。

API を使用して、`IPDeviceKeys.FORCE_ROUTABLE_IP_ADDRESS` プロパティを *true* に設定し、デバイスの発信元 IP アドレスに不一致があるかどうかに関係なく接続要求を許可します。

管理者のユーザ インターフェイスから次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** を選択します。

ステップ 2　次の方法のいずれかを使用します。

- デバイス レコードを追加します。追加するには、**Add** ボタンをクリックします。Add Device ページが表示されます。
- デバイス レコードを検索します。検索するには、Search Type を指定し、選択する検索タイプに固有の画面コンポーネントの値を入力します。デバイスのリストが表示されます。目的のデバイスに対応する Identifier リンクをクリックします。Modify Device ページが表示されます。

ステップ 3　Property Value ドロップダウン リストから、/IPDevice/forceRouteIPAddress を選択し、プロパティ値を設定します。

（注）　/IPDevice/forceRouteIPAddress の API 定数は、`IPDeviceKeys.FORCE_ROUTABLE_IP_ADDRESS` です。

ステップ 4　**Add** をクリックします。

（注）　このプロパティは、デバイスの階層の任意の場所で指定できます。

デバイスからのデータの検出

この項では、Discovery of Data 機能について説明します。この機能は、デバイスからパラメータの事前定義セットを取得し、それらのパラメータを後で使用できるように RDU に格納します。検出されたこのデータを使用すると、デバイスの一部のキー属性とその現在の構成を提供することにより、デバイス ファームウェアおよびデバイス構成を管理できます。検出されたパラメータは、これらの値がデバイス上で変更されるたびに RDU で更新されます。

データ検出は、RDU で設定できます。RDU は、以前の検出プロセス中に各デバイスについて検出された、検出ポリシー命令およびパラメータの値を適切な DPE に転送します。デバイスとの対話中に、DPE は、デバイスに固有の検出ポリシー命令を参照し、どのパラメータを検出する必要があるかを判別します。

パラメータ値が検出されると、既存のデバイス パラメータが、デバイスにすでに格納されているパラメータと比較されます。値が変更されている場合、または初めて取得される場合、このデータは RDU で更新されます。更新を受信するときに RDU が使用可能でない場合、新しく検出されたデータは破棄され、次回デバイスが DPE に接続するときにデータ検出の全プロセスが開始されます。

検出されたパラメータはデバイス レコードに格納され、管理者のユーザ インターフェイスを使用して表示するか、API `IPDevice.getDetails()` コールを介して取得することができます。検出されたパラメータをユーザ インターフェイス経由で表示するには、プライマリ ナビゲーション バーの **Devices** タブの下にある Manage Devices ページにアクセスします。検索オプションを使用してデバイスを見つけ、デバイスに対応する **View Details** アイコン（）をクリックします。デバイスについて検出されたパラメータの詳細を示す Device Details ページが表示されます。

以降の項では、次のトピックについて説明します。

- データ検出の設定（P.12-9）
- データ検出のトラブルシューティング（P.12-10）

データ検出の設定

データ検出ポリシーは、RDU から設定します。このポリシーには、いくつかのパラメータが含まれており、そのパラメータがチェックされるタイミングは次のとおりです。

- デバイスにアクセスするたび
- ファームウェアのアップグレード時のみ

データ検出プロセスは、デバイスが DPE にアクセスするたびに実行されるので、デバイスが新しいバージョンのファームウェアを報告した場合に限り、特定のパラメータの検証が実行されるように設定できます。このチェックにより、ファームウェアのアップグレード時にしか値が変更されないパラメータを検証する必要はなくなります。たとえば、ファームウェアのアップグレードがない場合、デバイス モデル名は変更されません。そのため、ファームウェアのアップグレードが実行されない限り、デバイスでこのパラメータをチェックする必要はありません。

BAC は、データ検出のデフォルト設定で出荷されます。このデフォルト設定は、次の 2 つの方法で拡張できます。

- パラメータをカスタム リストに追加する。
- デフォルトのリストを変更する。ただし、このオプションは推奨されていません。

アクセスごとにチェックされるパラメータの設定

`ServerDefaultsKeys.CWMP_DISCOVER_PARAMETERS` プロパティを使用すると、デバイスが DPE に接続するたびにパラメータが検出されるように、パラメータのデフォルトのリストを設定できます。`IPDeviceKeys.CWMP_CUSTOM_DISCOVER_PARAMETERS` プロパティの値としてパラメータのカンマ区切りリストを提供することにより、デフォルトのリストにパラメータを追加できます。デフォルトのリストには、次のパラメータが含まれます。

- Inform.DeviceId.Manufacturer
- Inform.DeviceId.ManufacturerOUI
- Inform.DeviceId.ProductClass
- InternetGatewayDevice.DeviceInfo.HardwareVersion
- InternetGatewayDevice.DeviceInfo.SoftwareVersion
- InternetGatewayDevice.ManagementServer.ParameterKey

次に例を示します。

```
IPDeviceKeys.CWMP_CUSTOM_DISCOVER_PARAMETERS=
InternetGatewayDevice.ManagementServer.URL,
InternetGatewayDevice.ManagementServer.PeriodicInformEnable
```

ファームウェアのアップグレード時にチェックされるパラメータの設定

`ServerDefaultsKeys.CWMP_FIRMWARE_CHANGED_CPE_PARAMETERS` プロパティを使用すると、ファームウェアのアップグレードのたびにパラメータが検出されるように、パラメータのデフォルトのリストを設定できます。このデフォルト リストには、InternetGatewayDevice.DeviceInfo.ModelName パラメータが含まれます。

このリストをカスタマイズしてさらに多くのパラメータを含めるには、`IPDeviceKeys.CWMP_CUSTOM_FIRMWARE_CHANGED_PARAMETERS` プロパティを使用します。

データ検出のトラブルシューティング

表 12-2 に示されているタスクのいずれかを使用して、DPE CLI からデータ検出のトラブルシューティングを実行することもできます。

表 12-2　DPE からのデータ検出のトラブルシューティング

タスク	使用するコマンド	説明
情報レベル ロギングをイネーブルにする	dpe# **log level 6-info**	情報メッセージを表示します。
デバイス ログを表示する	dpe# **show log** dpe# **show log last 100** dpe# **show log run** **(注)** リストされている 3 つのコマンドのどれでも使用できます。	直近のいくつかの DPE ログ エントリを表示します。 DPE ログの最後の 100 行を表示します。 実行中の DPE ログを表示します。

	例
	
	この例は説明を目的としているため、**show log run** コマンドの出力は短縮されています。
	
	`dpe# show log run`
	
	`% Press <enter> to stop.`
	
	`2006 08 04 00:47:01 EDT: %BAC-DPE-6-0104: Obtained configuration for device [0014BF-CJJ005B00009] from RDU.`
	
	`2006 08 04 00:47:21 EDT: %BAC-CWMP-6-5129: Device [0014BF-CJJ005B00009]. Source IP [10.86.147.149]. Retrieving [1] discovered CPE parameters.`
	
	`2006 08 04 00:47:21 EDT: %BAC-CWMP-6-5107: Device [0014BF-CJJ005B00009]. Source IP [10.86.147.149]. Sent [GetParameterValues] message.`
	
	`2006 08 04 00:47:21 EDT: %BAC-CWMP-6-5106: Device [0014BF-CJJ005B00009]. Source IP [10.86.147.149]. Received [GetParameterValuesResponse] message.`
	
	`2006 08 04 00:47:21 EDT: %BAC-CWMP-6-5120: Device [0014BF-CJJ005B00009]. Source IP [10.86.147.149]. New data discovered from CPE. Queued update of [7] parameters to RDU.`
	
	(注) **show log** コマンドの出力が、ここに示されているサンプル出力と同様であれば、データ検出は正常に完了しました。	

デバッグをイネーブルにする	dpe# **debug on** dpe# **debug service cwmp** *num* **data-sync** *num*：CWMP サービスのインスタンスを指定します。1 または 2 になります。	CWMP サービスのデータ同期プロセスのデバッグ ロギングをイネーブルにします。
特定のデバイスのデータ検出設定を表示する	dpe# **show device-config** *device-id* *device-id*：デバイスの ID を指定します。	DPE でキャッシュされるデバイス設定を表示します。

(注) これらのコマンドの使用方法の詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

プロビジョニング グループのスケーラビリティとフェールオーバー

この項では、この BAC リリースで提供されるスケーラビリティとフェールオーバーの機能について説明します。

BAC のスケーラビリティとフェールオーバーは、数百万のデバイスが配備されているネットワークを含む、実質的にどのような規模のネットワークにも適合する高度のアベイラビリティを実現します。BAC は、DPE 冗長性やフェールオーバーの保護などの重要な機能も提供します。

BAC 配備のスケーラビリティは、プロビジョニング グループを通じて実現されます。各プロビジョニング グループは、一群の CPE と通信する複数の冗長 DPE サーバから成るクラスタです。プロビジョニング グループを使用すると、各プロビジョニング グループがデバイスのサブセットにのみ責任を負うようになるので、BAC ネットワークのスケーラビリティが高まります。このデバイスのパーティション化は、地域別のグループ化や、サービス プロバイダーによって定義されている他のポリシーと並行して実現できます。

配備を拡張するには、管理者は次の操作を行うことができます。

- 既存の DPE サーバ ハードウェアをアップグレードする
- DPE サーバをプロビジョニング グループに追加する
- プロビジョニング グループを追加して、デバイスをそれらのグループに再分散する

BAC は、プロビジョニング グループへのデバイスの明示的な割り当てと自動メンバシップをサポートします。詳細については、P.4-1 の「CPE 管理の概要」を参照してください。

BAC における冗長性

冗長性により、次の事項が保証されます。

- ネットワーク アプリケーションに高いアベイラビリティが提供される。
- ユーザは、単一のポイント障害による長いネットワーク遅延やブラック ホールを経験することがない。

BAC は、ローカル サーバおよび地域別サーバの冗長性をサポートします。

ローカルでの冗長性

BAC プロビジョニング グループは、一群の CPE と通信する複数の冗長 DPE サーバから成るクラスタです。単一の URL が、各プロビジョニング グループを識別します。プロビジョニング グループへのすべての CPE 要求は、使用可能な DPE 間でロードバランスされます。各 DPE は、プロビジョニング グループ内の任意のデバイスを処理できます。

地域別の冗長性

地域別の冗長性を使用すると、地域的な障害が発生した場合に、異なる場所にある DPE が一時的に CPE 要求を処理できるようになります。この配備を推進する最も簡単な方法は、プロビジョニング グループ内の各 DPE を地理的に異なるさまざまな位置に設定することです。そのような設定では、CPE 要求はさまざまな地域にある DPE によって処理され、プロビジョニング グループの範囲内で地域的なフェールオーバーが提供されます。

ただし、配備によっては、CPE 要求を 1 つの場所にあるサーバで処理し、障害が発生した場合にのみ別の場所にある DPE にフェールオーバーする必要が生じる場合があります。そのような場合、別々の地域に存在する DPE を 1 つのプロビジョニング グループ内で見つけ、通常の状態では CPE 要求が特定地域の DPE のサブセットにのみ方向付けられるようにネットワークを設定することができます。

通常は、DNS 技術を使用して地域別の冗長性を設定できます。地域別の冗長性のためにネットワークを設定するには、所定のプロビジョニング名の BAC ホスト名が DPE の 1 つのセットを表す IP アドレスに正常に解決されることを確認します。しかし、そのセット内の DPE サーバのいずれもキープアライブに応答しない場合（ICMP、HTTP GET、または TCP ハンドシェークなど）、DNS サーバは、2 番目のセットに含まれる DPE の IP アドレスに BAC ホスト名を解決する必要があります。次に、CPE 要求は DPE の別のセットに方向付けられます。両方のセットの DPE は同じプロビジョニング グループに属しているので、新しい DPE は要求にすぐに応答できます。それ以降の DNS ルックアップ要求は、使用可能になるとただちに DPE のプライマリ セットにフォールバックされます。

地域別の冗長性は、Cisco 11500 Content Services Switch などのロード バランシング機能を備えるソフトウェアまたはハードウェアを使用して設定できます。

DPE ロード バランシング

BAC は、DPE 冗長性およびロード バランシングの次のメカニズムをサポートします。

- DNS ラウンド ロビンの使用方法（P.12-12）
- ハードウェア ロード バランサの使用方法（P.12-12）

DNS ラウンド ロビンの使用方法

DNS ラウンド ロビン メカニズムを使用すると、DNS サーバは、そのデバイスの自動構成サーバ（ACS）ホスト名を解決するときに DPE IP のリストをシャッフルします。次に、デバイスは、リスト内の最初の IP アドレスを ACS ホスト名として使用します。

サービス プロバイダーが DNS キャッシング サーバを制御しない場合、このオプションは推奨されません。また、停電が発生した場合、多数のデバイスが、DNS サーバによってキャッシュされた同じオーダー IP アドレスを受け取ることによりパフォーマンスが影響を受け、DNS ラウンド ロビンが適切に動作しなくなる場合があります。この問題に対処するため、DNS サーバの TTL を非常に短い値（1 秒）に設定することをお勧めします。

ハードウェア ロード バランサの使用方法

ハードウェア ロード バランサの使用時、ACS URL は、IP アドレスを含むか、または、DNS サーバによって単一の IP アドレスに解決されます。プロビジョニング グループのすべての DPE は、Cisco 11500 Content Services Switch（CSS）などの、ハードウェア ロード バランサの単一仮想 IP アドレスの背後に隠されています。ハードウェア ロード バランサは、その仮想 IP アドレスを、任意の数のロード バランシング アルゴリズムに基づいて固有の DPE IP アドレスに変換するように設定します。ロード バランサの冗長ペアを使用すると、冗長性が向上し、複数のプロビジョニング グループを処理できるようになる場合があります。

プロビジョニング グループへの DPE の追加

この項では、DPE を新しいプロビジョニング グループに追加する方法について説明します。DPE をプロビジョニング グループに追加する場合、次の 3 つのオプションがあります。

- DPE をプロビジョニング グループに追加する。
- デバイスと DPE の間に Cisco 11500 CSS などのハードウェア ロード バランサを使用する配備で、プロビジョニング グループに DPE を追加する。この場合、ロード バランサを更新する必要があります。
- DNS サーバがラウンド ロビンを使用してプロビジョニング グループの複数の DPE に解決する配備で、プロビジョニング グループに DPE を追加する。

DPE をプロビジョニング グループに追加するには、次の手順に従います。

ステップ 1　DPE CLI から DPE を設定します。実行する必要がある設定には、次のものがあります。

- DPE が属する必要があるプロビジョニング グループの指定。次のように入力します。

  ```
  dpe# dpe provisioning-group primary name
  ```

  — *name*：割り当てられているプライマリ プロビジョニング グループを示します。
- DPE が接続する RDU の指定。次のように入力します。

  ```
  dpe# dpe rdu-server {host | ip} port
  ```

  — *host*：RDU が実行しているホストの FQDN を示します。
  — *ip*：RDU の IP アドレスを示します。
  — *port*：DPE 接続で RDU がリッスンするポート番号を示します。デフォルトでは、このポート番号は 49187 です。
- 特定のインターフェイスの FQDN の指定。プロビジョニング FQDN は、特定の DPE インターフェイスにアクセスするデバイスに与えられる FQDN です。次のように入力します。

  ```
  dpe# interface ethernet {intf0 | intf1} provisioning fqdn fqdn
  ```

  — *intf0* | *intf1*：イーサネット インターフェイスを示します。
  — *fqdn*：指定されたインターフェイスで設定される FQDN を示します。
  特定のプロビジョニング グループ内では、すべての DPE に対して同じ FQDN を使用する必要があります。DPE がロード バランサの背後に位置する場合は、ロード バランサの FQDN をインターフェイス FQDN として使用し、同一のロード バランシング グループに属するすべての DPE で FQDN が同じであることを確認します。

(注)　CWMP サービスおよび HTTP ファイル サービスを 1 つの DPE で設定して、他の DPE の設定と一致させる必要もあります。設定オプションの詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。P.3-1 の「設定のワークフローとチェックリスト」も参照してください。

ステップ 2　**dpe start** コマンドを使用して DPE を起動し、DPE が同期をとり、RDU からのデバイス設定命令を読み込めるようにします。

ステップ 3　ロード バランサを使用している場合、オプションで、DPE アドレスをロード バランサに追加します。

ステップ 4　DNS ラウンド ロビン技術を使用している場合、オプションで、DPE アドレスを DNS サーバに追加します。

Cisco CSS を使用する DPE ロード バランシング

この項では、BAC トラフィックのロード バランシングのために Cisco 11501 CSS を設定する方法について説明します。Cisco CSS フロントエンド サーバは、BAC がサポートする CWMP デバイスからの着信 TCP トラフィックを処理し、Cisco CSS バックエンド サーバ（この場合は DPE）全体で TCP セッションをロードバランシングします。

（注） Cisco CSS が設定されている場合、Cisco CSS はフロントエンド サーバとバックエンド サーバで HTTP over SSL（この項では SSL と呼びます）をサポートします。

初期 CSS 設定

Cisco CSS に初めて電源を入れると起動時設定メニューが表示されます。これは、イーサネット管理ポートの IP アドレス、サブネット マスク、デフォルトのゲートウェイといった最小設定を行うためのメニューです。この情報は設定しないでください。

次に、デフォルトのユーザ名（**admin**）とパスワード（**system**）を変更するよう求めるメッセージが表示されます。オプションで、これらの資格情報を変更できます。ユーザ名の長さは 1 文字から 16 文字、パスワードの長さは 6 文字から 16 文字にする必要があります。

次に、追加の設定情報を求めるメッセージが表示されます。実行時設定および起動時設定を後でクリアする場合は、追加の設定情報を入力する必要があります。

例 12-1 は、Cisco CSS の初期設定を示しています。

例 12-1　Cisco CSS の初期設定

```
Checking for Existing Config...

No startup-config was found, continue with the setup script [y/n]? y

Note: Pressing 'q' after any prompt quits setup.
      Pressing <CR> after any [y/n] defaults to 'y'.


Warning: All circuit VLAN IP addresses must be on a different
         subnet than the Ethernet Mgt port IP address.
         The existing Ethernet Mgt port IP address is: 0.0.0.0

Add an IP address to VLAN1:     [default = 192.168.10.1]? 10.86.147.51
Add an IP subnet mask to VLAN1: [default = 255.255.255.0]? 255.255.255.224

Would you like to specify a default gateway?  [y/n]? y

Warning: The default gateway IP address must be on the same subnet
         as VLAN1. VLAN1 IP address is: 10.86.147.51

Add IP address for default gateway: [default = 10.86.147.2]? 10.86.147.33
Pinging the default gateway: 0% Success.

Which feature do you want to configure?
[1] Layer3 load balancing
[2] Layer5 load balancing
[3] Proxy cache
[4] Transparent cache
[5] Exit script
Enter the number of the feature you want to configure: 5

Showing the Running Config

CSS11501#  show running-config
!Generated on 07/17/2006 13:00:30
!Active version: sg0750103

configure


!************************** GLOBAL **************************
  ip route 0.0.0.0 0.0.0.0 10.86.147.33 1

!************************* CIRCUIT *************************
circuit VLAN1

  ip address 10.86.147.51 255.255.255.224

CSS11501#
```

VLAN 1 はデフォルトの VLAN であるため、Cisco CSS の 8 個のポートはすべて Cisco CSS のフロントエンド ポートとして使用できます。しかし、この例の目的に合せて、イーサネット ポート 0 はフロントエンド サーバ ポートとして使用されます。フロントエンド ルータまたはスイッチは、顧客のネットワークから Cisco CSS または DPE にアクセスするのを許可するために使用します。Cisco CSS に接続されたこのスイッチまたはルータ上のインターフェイスの IP アドレスは、デフォルトのゲートウェイの Cisco CSS で設定されたアドレスです（10.86.147.33）。FTP サーバ（IP アドレス 10.86.147.53）は、Cisco CSS のイーサネット ポート 8 に接続されます。この FTP サーバは、後の設定で使用します。

Cisco CSS での DPE ロード バランシングの設定

この項で説明する設定を使用すると、バックエンド DPE サーバ間の顧客ネットワーク内で、デバイスからのトラフィックの簡易ロード バランシングを実行できます。使用されるロード バランシングのアルゴリズムは、単純ラウンドロビンです。CWMP デバイスは HTTP を使用して Cisco CSS に接続し、接続は HTTP 形式で DPE サーバに渡されます。

（注） CSS の設定の詳細については、『*Cisco Content Services Switch SSL Configuration Guide（Software Version 7.40）*』を参照してください。

例 12-2　Cisco CSS での DPE ロード バランシングの設定

次の例は、同じサブネット上の 2 台の DPE サーバを使用する設定を示しています。この例の DPE サーバの IP アドレスは 11.32.0.26/12 および 11.32.0.27/12 です。イーサネット ポートに割り当てられたバックエンド サーバ Cisco CSS VLAN の IP アドレスは 11.32.0.1/12 です。コンテンツ ルールで設定されている VIP アドレスおよび TCP ポートは、10.86.147.52 および 7547 です。CWMP デバイスが Cisco CSS に接続し、DPE 間のロード バランシングを実行するときに使用する URL は、*http://10.86.147.52:7547/acs* です。

ステップ 1　設定モードで Cisco CSS にログインします。

```
CSS11501#config t<cr>
```

ステップ 2　DPE が使用する 2 つのインターフェイスを設定し、次のコマンドを使用してそれらを VLAN2 に割り当てます。

```
CSS11501(config)#interface e1<cr>
CSS11501(config-if[e1])#bridge vlan 2<cr>
CSS11501(config-if[e1])#interface e2<cr>
CSS11501(config-if[e2])#bridge vlan 2<cr>
CSS11501(config-if[e2]}#exit<cr>
```

ステップ 3　2 つの DPE が使用する VLAN 2 を設定します。

```
CSS11501(config)#circuit VLAN2<cr>
CSS11501(config-circuit[VLAN2])#ip address 11.32.0.1/12<cr>
Create ip interface <11.32.0.1>, [y/n]:y<cr>
CSS11501(config-circuit-ip[VLAN2-11.32.0.1])#exit<cr>
CSS11501(config-circuit[VLAN2])#exit<cr>
```

ステップ 4　それぞれの DPE に割り当てられるサービスを設定し、サービスを有効にします。

（注） 2 つのサービスは後にコンテンツ ルールに追加され、コンテンツ ルールは 2 つの DPE にわたって HTTP トラフィックをロード バランシングするように設定されます。

```
CSS11501(config)# service DPE-1<cr>
Create service <DPE-1>, [y/n]:y
CSS11501(config-service[DPE-1])#keepalive type tcp<cr>
CSS11501(config-service[DPE-1])#keepalive port tcp 7547<cr>
CSS11501(config-service[DPE-1])#ip address 11.32.0.26<cr>
CSS11501(config-service[DPE-1])#active<cr>
CSS11501(config-service[DPE-1])# service DPE-2<cr>

Create service <DPE-2>, [y/n]:y
CSS11501(config-service[DPE-2])# keepalive type tcp<cr>
CSS11501(config-service[DPE-2])# keepalive port 7547<cr>
CSS11501(config-service[DPE-2])# ip address 11.32.0.27<cr>
CSS11501(config-service[DPE-2])# active<cr>
CSS11501(config-service[DPE-2])#exit<cr>
```

ステップ 5　着信 HTTP トラフィックをロード バランシングするために使用されるコンテンツ ルールを含むオーナーを設定します。オーナー名として任意の名前を選択できます。

```
CSS11501(config)# owner User1<cr>
Create owner <User1>, [y/n]:y
CSS11501(config-owner[User1])#
```

ステップ 6　次のコマンドを使用してコンテンツ ルールを設定し、それを有効にします。

（注）　コンテンツ ルールの VIP アドレスは、CWMP デバイスが Cisco CSS に接続するときに使用する IP アドレスです。

```
CSS11501(config-owner[User1])# content Clear-text<cr>
Create content <Clear-text>, [y/n]:y
CSS11501(config-owner-content[User1-Clear-text])# protocol tcp<cr>
CSS11501(config-owner-content[User1-Clear-text])# port 7547<cr>
CSS11501(config-owner-content[User1-Clear-text])# add service DPE-1<cr>
CSS11501(config-owner-content[User1-Clear-text])# add service DPE-2<cr>
CSS11501(config-owner-content[User1-Clear-text])# vip address 10.86.147.52<cr>
CSS11501(config-owner-content[User1-Clear-text])#active<cr>
CSS11501(config-owner-content[User1-Clear-text])#exit<cr>
CSS11501(config-owner[User1])#exit<cr>
CSS11501(config)#exit<cr>
CSS11501#
```

ステップ 7　これで、設定は完了しました。実行時設定を起動時設定にコピーし、Cisco CSS のリブートのたびにロードされる永続的な設定レコードを作成します。

```
CSS11501# copy running-config startup-config<cr>
Working..(\) 100%
CSS11501#
```

Cisco CSS でのクライアント証明書認証の設定

次の例では、デバイスは SSL を使用して Cisco CSS に接続します。接続は、HTTP 形式で DPE サーバまで渡されます。Cisco CSS は、デバイスから送信された証明書を認証します。オプションで、証明書が HTTP ヘッダー経由で DPE に転送されるようにすることができます。

例 12-3　Cisco CSS でのクライアント証明書認証の設定

次の例は、同じサブネット上の 2 台の DPE サーバを使用する設定を示しています。この例の DPE サーバの IP アドレスは、11.32.0.26/12 および 11.32.0.27/12 です。DPE が接続するイーサネット ポートに割り当てられたバックエンド サーバ Cisco CSS VLAN の IP アドレスは 11.32.0.1/12 です。コンテンツ ルールで設定されている VIP アドレスおよび TCP ポートは、10.86.147.52 および 7548 です。デバイスが Cisco CSS に接続するときに使用する URL は、*http://10.86.147.52:7548/acs* です。

ステップ 1　設定モードで Cisco CSS にログインします。

```
CSS11501#config t<cr>
```

ステップ 2　DPE が使用する 2 つのインターフェイスを設定し、次のコマンドを使用してそれらを VLAN2 に割り当てます。

```
CSS11501(config)#interface e1<cr>
CSS11501(config-if[e1])#bridge vlan 2<cr>
CSS11501(config-if[e1])#interface e2<cr>
CSS11501(config-if[e2])#bridge vlan 2<cr>
CSS11501(config-if[e2]}#exit<cr>
```

ステップ 3　2 つの DPE が使用する VLAN 2 を設定します。

```
CSS11501(config)#circuit VLAN2<cr>
CSS11501(config-circuit[VLAN2])#ip address 11.32.0.1/12<cr>
Create ip interface <11.32.0.1>, [y/n]:y<cr>
CSS11501(config-circuit-ip[VLAN2-11.32.0.1])#exit<cr>
CSS11501(config-circuit[VLAN2])#exit<cr>
```

ステップ 4　それぞれの DPE に割り当てられるサービスを設定し、サービスを有効にします。

（注）　2 つのサービスは後にコンテンツ ルールに追加され、コンテンツ ルールは 2 つの DPE にわたって HTTP トラフィックをロード バランシングするように設定されます。

```
CSS11501(config)# service DPE-1<cr>
Create service <DPE-1>, [y/n]:y
CSS11501(config-service[DPE-1])#keepalive type tcp<cr>
CSS11501(config-service[DPE-1])#keepalive port tcp 7547<cr>
CSS11501(config-service[DPE-1])#ip address 11.32.0.26<cr>
CSS11501(config-service[DPE-1])#active<cr>
CSS11501(config-service[DPE-1])# service DPE-2<cr>

Create service <DPE-2>, [y/n]:y
CSS11501(config-service[DPE-2])# keepalive type tcp<cr>
CSS11501(config-service[DPE-2])# keepalive port 7547<cr>
CSS11501(config-service[DPE-2])# ip address 11.32.0.27<cr>
CSS11501(config-service[DPE-2])# active<cr>
CSS11501(config-service[DPE-2])#exit<cr>
```

ステップ 5　着信 HTTP トラフィックをロード バランシングするために使用されるコンテンツ ルールを含むオーナーを設定します。オーナー名として任意の名前を選択できます。

```
CSS11501(config)# owner User1<cr>
Create owner <User1>, [y/n]:y
CSS11501(config-owner[User1])#
```

ステップ 6　FTP サーバの ftp レコードを設定します。ftp レコードは、デバイスのルート証明書をダウンロードするために使用されます。Cisco CSS はこの設定を使用して、デバイスからのクライアント証明書と、Cisco CSS サーバを認証するためにデバイスに送信される Cisco CSS サーバ証明書および秘密鍵を認証します。

（注）　この例で使用する `ssl-machine` という名前の ftp レコードは、ユーザ定義の名前であり、証明書が Cisco CSS にロードされたときに FTP サーバの参照としてのみ使用されます。

この例の目的に合せて、FTP 接続を作成するために使用されるユーザ名とパスワードは、それぞれ `root` および `cisco` です。証明書と鍵が格納される FTP サーバ上のディレクトリは、*/var/tmp/ftp* です。

```
CSS11501(config)#ftp-record ssl-machine 10.86.147.53 root "cisco" /var/tmp/ftp<cr>
CSS11501(config)#exit<cr>
CSS11501#
```

ステップ 7　FTP サーバから証明書と鍵をロードします。

この例で使用する CWMP ルート証明書は `cwmp_root.cer`、Cisco CSS サーバ証明書は `css.cer`、Cisco CSS 秘密鍵は `css.key` です。

```
CSS11501#copy ssl ftp ssl-machine import cwmp_root.cer PEM "password"<cr>
CSS11501#copy ssl ftp ssl-machine import css.cer PEM "password"<cr>
CSS11501#copy ssl ftp ssl-mcahine import css.key PKCS12 "password"<cr>
```

（注）　この例で使用される証明書は PEM 形式、Cisco CSS 秘密鍵は PKCS12 形式です。これらのファイルのサポートされる形式は、DER、PEM、および PKCS12 です。ユーザ定義可能なパスワード（**password**）は、データ暗号規格ファイル内のファイルを符号化します。

ステップ 8　ロードした証明書と鍵を、後で SSL プロキシ リストを設定するときに参照可能な名前に関連付けます。次のコマンドを使用します。

```
CSS11501#config t<cr?
CSS11501(config)#ssl associate cert ca-root-cert cwmp_root.cer <cr>
CSS11501(config)#ssl associate cert css-server-cert css.cer <cr>
CSS11501(config)#ssl associate rsakey css-server-key css.key <cr>
CSS11501(config)#
```

ステップ 9　SSL プロキシ リストを設定します。このリストでは、次の事項を設定します。

- 使用される証明書と鍵
- バックエンド DPE サーバ向けのコンテンツ ルールの VIP アドレスを使用した優先暗号方式
- デバイスが Cisco CSS に接続するときに使用する VIP アドレスおよび TCP ポート

(注) プロキシ リストには、任意の名前を定義できます。

```
CSS11501(config)#ssl-proxy-list SSL<cr>
Create Ssl-list <SSL>, [y/n]:y
CSS11501(config-ssl-proxy-list[SSL]}#ssl-server 1<cr>
CSS11501(config-ssl-proxy-list[SSL])#ssl-server 1 port 7548<cr>
CSS11501(config-ssl-proxy-list[SSL])#ssl-server 1 rsakey css-server-key<cr>
CSS11501(config-ssl-proxy-list[SSL])#ssl-server 1 rsacert css-server-cert<cr>
CSS11501(config-ssl-proxy-list[SSL])#ssl-server 1 cacert ca-root-cert<cr>
CSS11501(config-ssl-proxy-list[SSL]}#ssl-server 1 cipher rsa-with-rc4-128-md5
10.86.147.60 7547
CSS11501(config-ssl-proxy-list[SSL])#ssl-server 1 authentication enable<cr>
CSS11501(config-ssl-proxy-list[SSL])#ssl-server 1 vip address 10.86.147.52<cr>
```

ステップ 10 HTTP ヘッダーのクライアント証明書を DPE に渡す場合は、次のコマンドを追加します。

```
CSS11501(config-ssl-proxy-list[SSL])#ssl-server 1 http-header client-cert<cr>
```

ステップ 11 **ssl-proxy-list** を有効にします。

```
CSS11501(config-ssl-proxy-list[SSL])#active<cr>
CSS11501(config-ssl-proxy-list[SSL])#exit<cr>
CSS11501(config)#
```

ステップ 12 **ssl-proxy-list** を参照する SSL サービスを設定します。サービス名は、ユーザが定義できます。

```
CSS11501(config)# service SSL<cr>
Create service <SSL>, [y/n]:y
CSS11501(config-service[SSL])#type ssl-accel<cr>
CSS11501(config-service[SSL])#add ssl-proxy-list SSL <cr>
CSS11501(config-service[SSL])#keepalive type none<cr>
CSS11501(config-service[SSL])#slot 2<cr>
CSS11501(config-service[SSL])#active<cr>
CSS11501(config-service[SSL])#exit<cr>
CSS11501(config)#
```

ステップ 13 **ssl-proxy-list** から出力された VIP アドレスおよびポート番号と一致するコンテンツ ルールを定義します。

```
CSS11501(config)#owner User1<cr>
CSS11501(config-owner[User1])#content Clear-text<cr>
CSS11501(config-owner[User1])#protocol tcp<cr>
CSS11501(config-owner[User1])#port 7547<cr>
CSS11501(config-owner[User1])# vip address 10.86.147.60<cr>
CSS11501(config-owner[User1])#add service DPE-1<cr>
CSS11501(config-owner[User1])#add service DPE-2<cr>
CSS11501(config-owner[User1])#active<cr>
CSS11501(config-owner[User1])#exit<cr>
```

ステップ 14 デバイスから送信された URL 内のアドレスおよびポート番号と一致するコンテンツ ルールを定義します。

```
CSS11501(config)#owner User1<cr>
CSS11501(config-owner[User1])#content SSL
Create content <SSL>, [y/n]:y
CSS11501(config-owner-content[User1-SSL])#protocol tcp<cr>
CSS11501(config-owner-content[User1-SSL])#port 7548<cr>
CSS11501(config-owner-content[User1-SSL])#add service SSL<cr>
CSS11501(config-owner-content[User1-SSL])#vip address 10.86.147.52<cr>
CSS11501(config-owner-content[User1-SSL])#active<cr>
CSS11501(config-owner-content[User1-SSL])#exit<cr>
CSS11501(config-owner[User1])#exit<cr>
CSS11501(config)#exit<cr>
CSS11501#
```

ステップ 15 最後に、実行時設定を起動時設定に保存します。

```
CSS11501#copy running-config startup-config<cr>
Working..(\) 100%
CSS11501#
```

CWMP サービス セキュリティの設定

この章では、認証および暗号化を含む、Broadband Access Center（BAC）の CWMP サービスのセキュリティ オプションについて説明します。この章では、DPE で CWMP サービスおよび HTTP ファイル サービスの HTTP over SSL 転送（この章では SSL と呼びます）をイネーブルにする方法と、証明書管理ツールを使用して DPE に証明書ストアを作成する方法について説明します。

この章では、次のトピックについて説明します。

概要

BAC は、RFC 2246 で定義されているとおり、SSL（特に SSL 3.0 および TLS 1.0）を使用することにより、CWMP デバイスのセキュア プロビジョニングをサポートします。RFC 2617 で定義されているとおり、Basic および Digest 認証を使用することにより、DPE との共有秘密情報に基づいてデバイス認証をサポートします。

BAC は、DPE で複数のサービスを提供します。それには、CWMP サービスの 2 つのインスタンスと、HTTP ファイル サービスの 2 つのインスタンスが含まれます。各サービスは、個別にイネーブルにして設定します。その際、同じ DPE で、各種デバイスを異なる方法で柔軟に処理するための、さまざまなセキュリティ オプションを指定できます。

BAC はさらに、一意または汎用のクライアント証明書を使用することにより、セキュアなデバイス認証も提供します。

- 汎用：顧客宅内装置（CPE）すべてまたは CPE の大部分に共通の汎用証明書を使用することにより、SSL 経由のデバイス証明書認証をイネーブルにします。たとえば、特定の配備内のすべての VoIP デバイスが、サービス プロバイダーが発行する同一の汎用証明書を持つことができます。クライアント証明書は、署名機関鍵に対して検証されますが、所定のデバイスのアイデンティティは確立しません。デバイス識別子は、HTTP Basic または Digest 認証を介して提供されるデータを使用するか、CWMP Inform メッセージのデータを使用して形成されます。
- 一意：各デバイスが提供する一意の証明書を使用することにより、SSL 経由のクライアント証明書認証をイネーブルにします。署名認証局の公開鍵を使用してクライアント証明書が検証された後、クライアント証明書の CN フィールドを使用してデバイスの一意の識別子が形成されます。

BAC は、Cisco 11500 Content Services Switch（CSS）などのハードウェア ロード バランサおよび SSL アクセラレータで、クライアント証明書認証を実行する固有のオプションをサポートします。このシナリオでは、ダウンストリーム Cisco CSS は証明書の検証を実行し、SSL セッション（特にクライアント証明書フィールド）に関する情報をデバイス証明書から抽出し、そのデータを特殊 HTTP ヘッダーに挿入します。次に BAC は、Cisco CSS ヘッダー ClientCert-Subject-CN から CN フィールドを取得し、一意のデバイス識別子を形成します。

BAC では、認証オプションを組み合せて使用できます。たとえば、SSL を使用してデバイスが汎用証明書を持っていることを検証し、SSL 接続が確立された後に、追加の HTTP Basic または Digest 認証を実行することができます。

BAC は、no-device 認証のオプションも提供しています。このオプションは、デバイスが DPE のダウンストリームで認証され、デバイスが提示するアイデンティティが信頼できる場合に便利です。BAC DPE が認証なしで実行するよう設定されている場合、BAC DPE は Inform メッセージからデバイスのアイデンティティを抽出して、それを信頼します。

SSL を使用すると、デバイスと DPE の間のトラフィックを暗号化できます。BAC は、デバイスに対して使用する暗号化アルゴリズムや暗号鍵長さを判別する、さまざまな暗号スイートをサポートします。CLI を使用すると、DPE 上で受け入れ可能な暗号スイートを設定できます。別のオプションは、ハードウェア ロード バランサおよびアクセラレータで SSL を終端させることにより、スケーラビリティを高めることです。

（注） DPE CLI を使用して、CWMP サービスおよび HTTP ファイル サービスのセキュリティ オプションを設定します。設定手順については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

BAC における鍵と証明書の管理

DPE は、SSL プロトコルが認証に必要とする証明書を鍵ストアに格納します。この鍵ストアはファイル形式のデータベースで、秘密鍵とそれに関連付けられている公開鍵の X.509 証明書が含まれます。

DPE サーバには 2 つの鍵ストアがあります。これらの鍵ストアは、cacerts 鍵ストアとサーバ証明書鍵ストアです。cacerts 鍵ストアには、デバイスのクライアント証明書を認証するときに DPE が信頼できる公開鍵証明書が含まれます。サーバ証明書鍵ストアには、デバイスに対して DPE を認証するために使用される、サーバ側の証明書の秘密鍵および関連付けられている証明書チェーンが含まれます。

すべての DPE SSL サービスは、単一の cacerts 鍵ストアを共有します。この鍵ストアには、任意の数の署名機関証明書を含めることができます。cacerts 鍵ストアの名前は固定されており、常に *BPR_HOME/jre/lib/security* ディレクトリに存在している必要があります。BAC には、デフォルトの cacerts 鍵ストアが付属しています。これは署名機関証明書を追加および削除することにより操作できます。

cacerts 鍵ストアとは対照的に、サーバ証明書鍵ストアは複数存在することができ、異なるサーバ証明書鍵ストアを使用するように DPE 内の各 SSL サービスを設定できます。各サーバ証明書鍵ストアには、1 つの証明書チェーンのみ含めることができます。サーバ証明書鍵ストアは、*BPR_HOME/dpe/conf* ディレクトリに存在している必要があります。

SSL が DPE で終端され、プロビジョニング グループに複数の DPE が含まれる場合、同一の鍵ストアですべての DPE を設定する必要があります。プロビジョニング グループのすべての DPE を解決するために自動構成サーバ（ACS）の同じ完全修飾ドメイン名（FQDN）URL が使用されるので、同一の鍵ストアが必要です。TR-069 仕様で定義されているとおり、ACS URL は、鍵ストアにインポートされるサーバ証明書の通常名（CN）の値と同一である必要があります。

（注） DPE には、servercerts という名前のデフォルトのサンプル サーバ証明書鍵ストアが付属しています。この鍵ストアには、自己署名サーバ証明書が含まれています。しかし、通常、CWMP デバイスは、自己署名証明書を信頼しないので、デバイス プロビジョニングの SSL をイネーブルにするためにサンプルの鍵ストアを使用することはできません。その代わり、秘密鍵を使用して署名付き ACS 証明書を取得し、これを使用して新しいサーバ証明書鍵ストアを作成する必要があります（P.13-4 の「keytool を使用した DPE 鍵ストアの設定」を参照してください）。ACS 証明書を取得して設定する前に、デフォルトの鍵ストアを使用して SSL サービス リンクをテストできます。

SSL サービスの設定

BAC で SSL をイネーブルにするには、次の手順に従います。

ステップ 1　秘密鍵および関連付けられている ACS 公開鍵証明書を含む、サーバ証明書鍵ストアを作成します。このプロセスでは、サーバ証明書の署名機関の公開証明書をロードするために cacerts 鍵ストアを更新することも必要です。

ステップ 2　オプションで、クライアント証明書を使用するように CPE 認証を設定する場合は、CPE 証明書を検証できる CPE 認証局のルート証明書の公開鍵を使用して、cacerts 鍵ストアを更新します。詳細については、P.13-4 の「keytool を使用した DPE 鍵ストアの設定」を参照してください。

ステップ 3　DPE CLI から、新しいサーバ証明書鍵ストアを使用するように DPE を設定します。詳細については、P.13-13 の「DPE サービスのセキュリティの設定」を参照してください。

ステップ 4　DPE CLI を使用して、CWMP サービスまたは HTTP ファイル サービスの SSL 転送をイネーブルにします。詳細については、P.13-13 の「DPE サービスのセキュリティの設定」を参照してください。

（注）　鍵ストアに対する変更が有効であることを確認するには、CLI から **dpe reload** コマンドを使用するか、ウォッチドッグ エージェントのコマンドラインから **/etc/init.d/bprAgent restart dpe** コマンドを使用して、DPE を再起動する必要があります（P.9-2 の「コマンドラインからの BAC プロセス ウォッチドッグの使用」を参照してください）。

keytool を使用した DPE 鍵ストアの設定

BAC では、keytool ユーティリティを使用してサーバ証明書鍵ストアおよび cacerts 鍵ストアを設定します。keytool は、DPE サーバ上の証明書を管理するために使用する、鍵と証明書管理のユーティリティです。

keytool ユーティリティは、BAC のデフォルトのインストール ディレクトリ */opt/CSCObac/jre/bin/keytool* にあります。DPE サーバへのセキュア接続を使用して、keytool ユーティリティを実行します。

（注）　鍵ストアのファイル形式は keytool のリリースによって異なるので、この BAC のバージョンに付属している keytool ツールを実行する必要があります。

サーバ証明書を設定するには、次の手順に従います。

ステップ 1　keytool を使用して、新しい秘密鍵で新しいサービス鍵ストアを作成します。詳細については、P.13-7 の「新しい証明書のサーバ証明書鍵ストアおよび秘密鍵の生成」を参照してください。

ステップ 2　証明書署名要求（CSR）を生成します。詳細については、P.13-9 の「証明書署名要求の生成」を参照してください。

ステップ 3　CSR を使用して、署名機関に公開証明書を要求します。詳細については、P.13-9 の「証明書署名要求の生成」を参照してください。

ステップ 4　署名機関の公開鍵を cacerts 鍵ストアにロードします。詳細については、P.13-10 の「cacerts 鍵ストアへの署名機関証明書のインポート」を参照してください。

ステップ 5　署名付きサーバ証明書をサーバ鍵ストアにロードします。詳細については、P.13-10 の「サーバ証明書鍵ストアへの署名付き証明書のインポート」を参照してください。

ステップ 6　新しい鍵ストア ファイルを DPE の *BPR_HOME/dpe/conf* ディレクトリに入れます。

ステップ 7　CLI で、新しい鍵ストアを使用するように DPE サービスの 1 つを設定します。詳細については、P.13-4 の「SSL サービスの設定」を参照してください。

ステップ 8　CLI から **dpe reload** コマンドを使用するか、ウォッチドッグ エージェントのコマンドラインから **/etc/init.d/bprAgent restart dpe** コマンドを使用して DPE を再起動します（P.9-2 の「コマンドラインからの BAC プロセス ウォッチドッグの使用」を参照してください）。

（注）　デバイス認証でクライアント証明書の使用をイネーブルにするには、デバイス証明書の署名機関の公開証明書が cacerts 鍵ストアにロードされていることを確認してください。詳細については、P.13-10 の「cacerts 鍵ストアへの署名機関証明書のインポート」に示す手順に従います。

既存の署名付きサーバ証明書のインポート

署名付きサーバ証明書があり、それを鍵ストアにロードする場合は、証明書に関連付けられている秘密鍵を知っている必要があります。この場合、上記の手順ではなく、この項の手順に従ってください。秘密鍵と署名付き証明書の両方を組み合せた、PCKS#12 ファイル形式を使用します。このファイルを **keystore import-pkcs12** コマンドを使用して鍵ストアにロードできます。

既存の署名付きサーバ証明書でサーバ証明書を設定するには、次の手順に従います。

ステップ 1　**keystore import-pkcs12** コマンドを使用して、SSL クライアントに対する DPE の認証で使用された DPE 互換ファイルに既存の秘密鍵と証明書をロードします。

このコマンドを使用する場合、構文は次のようになります。

```
keystore import-pkcs12 keystore-filename pkcs12-filename keystore-password
key-password
export-password export-key-password
```

- *keystore-filename*：作成する鍵ストア ファイルを示します。ファイルがすでに存在する場合は、上書きされます。

  （注）　必ず鍵ストア ファイルのフル パスを指定してください。

- *pkcs12-filename*：鍵と証明書をインポートする PKCS#12 ファイルを示します。

- *keystore-password*：鍵ストア ファイルを作成したときに使用した秘密鍵パスワードと鍵ストア パスワードを示します。このパスワードの長さは、6 文字から 30 文字にする必要があります。
- *key-password*：DPE 鍵ストア内の鍵にアクセスするために使用されるパスワードを示します。このパスワードの長さは、6 文字から 30 文字にする必要があります。
- *export-password*：PKCS#12 ファイルの鍵を復号化するために使用されるパスワードを示します。このエクスポート パスワードの長さは、6 文字から 30 文字にする必要があります。
- *export-key-password*：PKCS#12 鍵ストア内の鍵にアクセスするために使用されるパスワードを示します。このパスワードの長さは、6 文字から 30 文字にする必要があります。

次に例を示します。

```
dpe# keystore import-pkcs12 example.keystore example.pkcs12 changeme changeme changeme
changeme
% Reading alias [1]

% Reading alias [1]: key with format [PKCS8] algorithm [RSA]

% Reading alias [1]: cert type [X.509]

% Created JKS keystore: example.keystore

% OK
```

ステップ 2　新しい鍵ストア ファイルを *BPR_HOME/dpe/conf* ディレクトリにコピーします。

ステップ 3　CLI で、新しい鍵ストアを使用するように DPE サービスの 1 つを設定します。詳細については、P.13-4 の「SSL サービスの設定」を参照してください。

ステップ 4　CLI から **dpe reload** コマンドを使用するか、ウォッチドッグ エージェントのコマンドラインから **/etc/init.d/bprAgent restart dpe** コマンドを使用して DPE を再起動します（P.9-2 の「コマンドラインからの BAC プロセス ウォッチドッグの使用」を参照してください）。

Keytool コマンドの使用

keytool ユーティリティでは、コマンド パラメータを使用して DPE 鍵ストアを設定します。表 13-1 は、keytool のコマンドと説明を示しています。

表 13-1　Keytool のコマンド

-alias *alias*	証明書チェーンと秘密鍵を格納する鍵ストア エントリに割り当てられたアイデンティティを示します。これ以降の keytool コマンドでは、エンティティを参照するときに同じエイリアスを使用する必要があります。
-dname *dname*	サブジェクトおよび発行元により指定された名前など、エンティティを識別するときに使用する X.500 認定者名を示します。
-file *csr_file*	エクスポートする CSR ファイルを示します。
-file *cert_file*	証明書が読み取られるファイルを示します。
-keyalg *keyalg*	鍵ペアの作成に使用されるアルゴリズムを示します。値は DSA（デフォルト）および RSA です。

表 13-1　Keytool のコマンド（続き）

-keysize *keysize*	鍵サイズを指定します。値は 64 ビットの倍数にする必要があります。
-keypass *keypass*	鍵ペアに割り当てられているパスワードを示します。
-keystore *keystore*	鍵ストアの名前と場所をカスタマイズします。
-noprompt	インポート操作中にプロンプトが発行されないように指定します。
-provider *provider_class_name*	サービス プロバイダーがセキュリティ プロパティ ファイルにリストされていない場合、暗号化サービス プロバイダーのマスター クラス ファイルの名前を示します。
-rfc	証明書の MD5 フィンガープリントの出力が、印刷可能な符号化形式で表示されるように指定します。
-storepass *storepass*	鍵ストアに割り当てられているパスワードを示します。
-sigalg *sigalg*	証明書に署名するために使用されるアルゴリズムを示します。
-storetype *storetype*	鍵ストアに割り当てられているタイプまたは鍵ストアへのエントリを示します。
-trustcacerts	信頼のチェーンで、追加の証明書が考慮されるよう指定します。
-v	証明書の MD5 フィンガープリントの出力が、人間が判読可能な形式で印刷されるように指定します。
-validity *valDays*	有効期間を示します。デフォルトは 90 日です。

（注） keytool および一般的な証明書管理の概念の詳細については、Sun Microsystems のマニュアルを参照してください。

新しい証明書のサーバ証明書鍵ストアおよび秘密鍵の生成

keytool -genkey コマンドは、鍵ペア（公開鍵および関連付けられている秘密鍵）を生成し、公開鍵を X.509 の自己署名証明書にラップします。これが単一要素証明書チェーンとして格納されます。この証明書チェーンと秘密鍵は、エイリアスによって識別される新しい鍵ストアのエントリに格納されます。

（注） エイリアスに使用する名前は、重要ではありません。その目的は、複数の鍵ペアを持つ場合に鍵ストア内の鍵ペアを識別することです。BAC では、サーバ証明書鍵ストアには 1 つの鍵ペアを定義しますが、鍵ストアは複数持つことができます。

例 13-1　Keytool -genkey

次の例では、鍵ストア ファイルの名前として *train-1.keystore* を使用します。任意のファイル名を使用できますが、*servercerts* は、BAC が提供するサンプルの鍵ストアと競合するので推奨されていません。

```
dpe# ./keytool -keystore train-1.keystore -alias train-1 -genkey -keyalg RSA
Enter keystore password:  changeme
What is your first and last name?
  [Unknown]:  train-1.bac.test
What is the name of your organizational unit?
  [Unknown]:  BAC Training
What is the name of your organization?
  [Unknown]:  Acme Device, Inc.
What is the name of your City or Locality?
  [Unknown]:  Boxborough
What is the name of your State or Province?
  [Unknown]:  MA
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=train-1.bac.test, OU=BAC Training, O="Acme Device, Inc.", L=Boxborough, ST=MA,
C=US correct?
  [no]:  yes

Enter key password for <train-1>
        (RETURN if same as keystore password):
```

この例では、証明書の CN フィールドに *train-1.bac.test* が挿入され、ACS URL に含まれている FQDN を表します。TR-069 仕様に従って、デバイスは証明書の署名を検証し、証明書内の CN フィールドがアクセス先の URL のフィールドと一致することを確認します。

自己署名証明書の表示

keytool -list 引数は、エイリアスによって識別される鍵ストア エントリの内容を表示します。エイリアスを指定しない場合、鍵ストアの内容全体が表示されます。

-list を **-v** と組み合せると、エイリアスに関連付けられている証明書チェーンが表示されます。次の **keytool -list** のサンプル出力は、単一の自己署名証明書が含まれる鍵ストアを示しています。

例 13-2　Keytool -list

```
# ./keytool -keystore train-1.keystore -list -v
Enter keystore password:  changeme

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: train-1
Creation date: Nov 8, 2005
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=train-1.bac.test, OU=BAC Training, O="Acme Device, Inc.", L=Boxborough,
ST=MA, C=US
Issuer: CN=train-1.bac.test, OU=BAC Training, O="Acme Device, Inc.", L=Boxborough,
ST=MA, C=US
Serial number: 43714f22
Valid from: Tue Nov 08 20:21:38 EST 2005 until: Mon Feb 06 20:21:38 EST 2006
Certificate fingerprints:
         MD5:  CF:D4:CB:D1:20:6F:8C:12:ED:EA:2F:21:53:57:E5:1D
         SHA1: DD:AE:96:02:71:55:F8:1F:14:4F:D7:64:9C:FE:91:DE:65:C9:BB:49
```

証明書署名要求の生成

一連の手順におけるこの時点では、鍵ストアに秘密鍵と X.509 自己署名証明書が含まれています。DPE ACS がこの証明書でデバイスの初期ハンドシェークに応答を試みる場合、デバイスは、CPE が信頼した認証局が証明書に署名しなかったことを示す TLS アラート `bad CA` により証明書を拒否します。したがって、CPE が信頼する署名機関が証明書に署名する必要があります。

(注) SSL をサポートするには、デバイスに、信頼する署名機関の事前に設定された公開証明書のリストを含める必要があります。デバイスが信頼する機関の 1 つが、ACS 証明書に署名する必要があります。

keytool -certreq コマンド パラメータは、証明書署名要求（CSR）を生成します。このコマンドは、業界標準の PKCS#10 形式で CRS を生成します。

例 13-3　Keytool -certreq

次の例では、**alias** *train-1* に事前に存在する自己署名証明書を鍵ストアとともに使用して、証明書署名要求を生成し、要求を `train-1.csr` ファイルに出力します。

```
dpe# ./keytool -keystore train-1.keystore -alias train-1 -certreq -file train-1.csr
Enter keystore password:  changeme
```

次のステップでは、CSR ファイルを署名機関に送信します。署名機関、またはその署名機関向けの秘密鍵を所有する管理者は、この要求に基づいて署名付き証明書を生成します。管理者からは、署名機関の公開証明書を取得する必要もあります。

署名付き証明書の検証

署名された証明書を受け取った後、**keytool -printcert** コマンドを使用して、自己署名証明書のファイル形式が正しいかどうか、また正しいオーナーおよび発行元フィールドを使用しているかどうかを確認します。コマンドは、**-file** *cert_file* パラメータから証明書を読み取り、その内容を人間が判読可能な形式で出力します。

例 13-4　Keytool -printcert

この例の *train-1.crt* ファイルは、管理者が提供する署名付き証明書を示します。

```
dpe# ./keytool -printcert -file train-1.crt
Owner: CN=train-1.bac.test, OU=BAC Training, O="Acme Device, Inc.", ST=MA, C=US
Issuer: EMAILADDRESS=linksys-certadmin@cisco.com, CN=Acme Device Provisioning Root
Authority 1, OU=Acme Device Certificate Authority, O="Acme Device, Inc.", L=Irvine,
ST=California, C=US
Serial number: 1
Valid from: Tue Nov 08 12:40:28 EST 2005 until: Thu Nov 08 12:40:28 EST 2007
Certificate fingerprints:
         MD5:  25:8E:98:C5:5C:23:5C:A0:4D:51:CF:2A:AA:2A:FC:42
         SHA1: 05:C1:2D:C6:94:78:D1:40:88:6A:55:67:43:27:68:D3:AC:43:C6:A5
```

(注) keytool は、X.509 v1、v2、および v3 の証明書と、そのタイプの証明書から成る PKCS#7 形式の証明書チェーンを出力できます。出力されるデータは、バイナリ符号化形式で提供されるか、RFC 1421 で定義されているように、印刷可能符号化形式（Base64 符号化とも呼ばれる）で提供される必要があります。

cacerts 鍵ストアへの署名機関証明書のインポート

証明書をサーバ証明書鍵ストアにインポートする前に、署名機関の公開証明書を cacerts 鍵ストアにインポートする必要があります。証明書を鍵ストアにインポートするときに、keytool は、証明書とその署名機関との間で信頼チェーンを確立できるかどうかを確認するからです。信頼のチェーンを確立できない場合は、エラー メッセージが表示されます。

（注） BAC に組み込まれている cacerts ファイルには、一般的な第三者署名機関のいくつかのルート証明書が付属しています。cacerts 鍵ストアは、keytool ユーティリティを使用して管理できます。デフォルトの cacerts 鍵ストアのパスワードは **changeit** です。cacerts データベース ファイルは、*BPR_HOME/jre/lib/security* ディレクトリにあります。
cacerts 鍵ストアをいずれかの場所にコピーする必要はありません。DPE は、再起動の直後に新しい鍵ストアを使用します。

例 13-5　Keytool -import（署名機関証明書）

```
# ./keytool -import -alias DeviceProvRoot -file rootCA4.crt -keystore
/opt/CSCObac/jre/lib/security/cacerts
Enter keystore password:  changeit
Owner: EMAILADDRESS=linksys-certadmin@cisco.com, CN=Acme Device Provisioning Root
Authority 1, OU=Acme Device Certificate Authority, O="Acme Device, Inc.", L=Irvine,
ST=California, C=US
Issuer: EMAILADDRESS=linksys-certadmin@cisco.com, CN=Acme Device Provisioning Root
Authority 1, OU=Acme Device Certificate Authority, O="Acme Device, Inc.", L=Irvine,
ST=California, C=US
Serial number: 8bcbc07a0768c1eb78e6c5c93c0c2ff0
Valid from: Fri Jul 01 21:22:12 EDT 2005 until: Mon Jun 29 21:22:12 EDT 2015
Certificate fingerprints:
         MD5:  C4:D4:09:6A:60:34:A0:00:96:4F:4D:47:23:86:8C:FA
         SHA1: B0:CC:6D:CD:BB:62:1B:A1:15:D3:2D:68:7E:D0:4A:0C:91:C2:A5:FD
Trust this certificate? [no]:  yes
Certificate was added to keystore.
```

（注） keytool は、X.509 v1、v2、および v3 の証明書と、そのタイプの証明書から成る PKCS#7 形式の証明書チェーンをインポートできます。インポートされるデータは、バイナリ符号化形式で提供されるか、RFC 1421 で定義されているように、印刷可能符号化形式（Base64 符号化とも呼ばれる）で提供される必要があります。

サーバ証明書鍵ストアへの署名付き証明書のインポート

署名機関の公開証明書を cacerts 鍵ストアにインポートした後は、署名付きサーバ証明書を DPE サーバ証明書鍵ストアにインポートする必要があります。鍵ストアには、秘密鍵および対応する自己署名証明書（公開鍵）がすでに格納されています。署名応答（署名付き証明書）をインポートすることにより、鍵ストアは、署名付き証明書をサーバ証明書鍵ストア内の既存の秘密鍵に関連付けるように変更されます。

証明書応答を鍵ストアにインポートする場合、*cacerts* ファイル内の証明書に対する **-import** コマンドで **-trustcacerts** フラグを使用し、サブジェクトの鍵ストア内の証明書応答との信頼チェーンを確立する必要があります。

例 13-6　Keytool -import（署名付きサーバ証明書）

```
dpe# ./keytool -import -trustcacerts -file train-1.crt -keystore train-1.keystore
-alias train-1
Enter key password: changeme2
Enter keystore password:  changeme
Certificate reply was installed in keystore.
Certificate was added to keystore.
```

署名付きサーバ証明書を DPE サーバ証明書鍵ストアにインポートした後、**keytool -printcert** コマンドを使用して鍵ストアの内容を確認します。詳細は、P.13-9 の「署名付き証明書の検証」に記載されています。これで、**-printcert** の出力が、発行元が署名認証局であり、ルート信頼証明書を持つ署名機関を介して信頼チェーンが確立されたことを示すようになりました。

クライアント認証の証明書のインポート

このステップを実行する必要があるのは、DPE でクライアント証明書を使用してクライアント認証を設定した場合だけです。クライアント証明書を使用してクライアント認証をイネーブルにした場合、cacerts 鍵ストアには、CPE クライアント証明書に署名した署名機関の公開証明書が含まれている必要があります。DPE で、提供された証明書の検証をイネーブルにするには、この証明書が必要です。

例 13-7　Keytool -import（署名機関証明書）

```
# ./keytool -import -alias DeviceClientRoot -file rootCA3.crt -keystore
/opt/CSCObac/jre/lib/security/cacerts
Enter keystore password:  changeit
Owner: EMAILADDRESS=linksys-certadmin@cisco.com, CN=Acme Device Client Root Authority
1, OU=Acme Device Certificate Authority, O=Acme Device LLC., L=Irvine, ST=California,
C=US
Issuer: EMAILADDRESS=linksys-certadmin@cisco.com, CN=Acme Device Client Root Authority
1, OU=Acme Device Certificate Authority, O=Acme Device LLC., L=Irvine, ST=California,
C=US
Serial number: d07d8a7badba7cb6446998b1ea89879f
Valid from: Fri Jul 01 21:19:50 EDT 2005 until: Mon Jun 29 21:19:50 EDT 2015
Certificate fingerprints:
         MD5:  40:B0:40:49:37:3A:51:1F:0D:78:B6:B3:E2:2C:1A:E8
         SHA1: 96:F5:84:71:84:CC:0A:A2:1E:7B:44:A2:B6:F5:B7:3D:C4:9F:81:3B
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

（注） この手順は、P.13-10 の「cacerts 鍵ストアへの署名機関証明書のインポート」で説明されている手順とまったく同じです。いずれの場合も、署名機関の公開証明書をロードします。サーバ証明書の署名機関が、デバイス証明書の署名機関と同じ場合は、署名は 1 度だけ追加します。

DPE へのサービス プロバイダー鍵ストアの提供

署名付き公開鍵証明書が含まれる新しいサービス証明書鍵ストアを取得したら、鍵ストア ファイルを DPE にコピーする必要があります。ファイルは、*BPR_HOME/dpe/conf* ディレクトリにコピーする必要があります。

例 13-8　DPE 設定ディレクトリへの鍵ストアのコピー

```
dpe# cp train-1.keystore /opt/CSCObac/dpe/conf
```

このステップが完了したら、DPE CLI を使用して、新しい鍵ストアを使用するように DPE サービスを設定できます。

(注) cacerts 鍵ストアをコピーする必要はありません。DPE は、再起動されるとただちに新しい鍵ストアを使用します。

詳細については、P.13-13 の「DPE サービスのセキュリティの設定」を参照してください。DPE 設定コマンドの詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

DPE サービスのセキュリティの設定

この項では、認証オプションを設定する方法、および DPE サービスに SSL を設定する方法について説明します。

DPE セキュリティ オプションは、DPE CLI から設定できます。詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

DPE は、実行中の 2 つの CWMP サービスと 2 つの HTTP ファイル サービスを並行してサポートします。各サービスには異なる設定のセキュリティ オプションを定義でき、異なるポートで実行できます。デフォルトでは、1 つの CWMP サービスと 1 つの HTTP サービスのみがイネーブルにされ、SSL なしで設定されています。2 つの追加のサーバは SSL 用に設定されていますが、デフォルトではディセーブルになっています。

表 13-2 では、CWMP サービスおよび HTTP ファイル サービスの各インスタンスのデフォルト設定を指定します。

表 13-2　CWMP 技術のデフォルト設定

	CWMP サービス		HTTP ファイル サービス	
	サービス 1	**サービス 2**	**ファイル サービス 1**	**ファイル サービス 2**
デフォルト モード	イネーブル	ディセーブル	イネーブル	ディセーブル
認証	Digest	Digest	Digest	Digest
ポート番号	7547	7548	7549	7550
SSL プロトコル	ディセーブル	イネーブル	ディセーブル	イネーブル

DPE での SSL の設定

所定のサービスで SSL をイネーブルにするには、次の手順に従います。

ステップ 1　HTTP クライアント認証を設定します。Basic または Digest モードで認証をイネーブルにするか、HTTP 認証をディセーブルにできます。

ステップ 2　サービスの SSL プロトコルをイネーブルにします。

ステップ 3　デバイスが DPE 上のサービスにアクセスするときに使用するポートを設定します。

ステップ 4　鍵ストアのファイル名、鍵ストアのパスワード、および鍵のパスワードを設定します。

ステップ 5　SSL を使用してクライアント証明書認証を設定します。クライアント認証は、汎用または一意のクライアント証明書を使用するように設定できます。

ステップ 6　オプションで、CWMP サービスまたは HTTP ファイル サービスの他のインスタンスをディセーブルにします。

ステップ 7　1 つのサービスのインスタンスを 1 つイネーブルにします。サービスは、CWMP サービスまたは HTTP ファイル サービスのいずれかです。

ステップ 8　**dpe reload** コマンドを使用して DPE を再起動し、変更が有効になっていることを確認します。

CWMP サービスの SSL のイネーブル化

次の例は、CWMP サービスの 1 つのインスタンスで SSL をイネーブルにするためのコマンドを示しています。この例では、クライアント証明書および Basic モードの HTTP 認証を使用することにより、SSL クライアントの二重の認証をイネーブルにします。

```
dpe# service cwmp 2 client-auth basic
% OK (Basic authentication was enabled. Digest authentication was disabled. Requires
DPE restart "> dpe reload")

dpe# service cwmp 2 port 7548
% OK (Requires DPE restart "> dpe reload")

dpe# service cwmp 2 ssl enable true
% OK (Requires DPE restart "> dpe reload")

dpe# service cwmp 2 ssl keystore train-1.keystore changeme changeme2
% OK (Requires DPE restart "> dpe reload")

dpe# service cwmp 2 ssl client-auth client-cert-unique
% OK (Requires DPE restart "> dpe reload")

dpe# service cwmp 1 enabled false
% OK (Requires DPE restart "> dpe reload")

dpe# service cwmp 2 enable true
% OK (Requires DPE restart "> dpe reload")

dpe# dpe reload
Process dpe has been restarted.

% OK
```

（注） この例では、CWMP インスタンス 2 の SSL 転送を設定します。例では、`train-1.keystore` が、署名付きのサーバ用の公開鍵証明書とともにプリロードされていること、また鍵ストア ファイルが DPE の *BPR_HOME/dpe/conf* ディレクトリに移動されたことを想定しています。

HTTP ファイル サービスの SSL のイネーブル化

次の例は、HTTP ファイル サービスの 1 つのインスタンスで SSL プロトコルをイネーブルにするためのコマンドを示しています。この例では、クライアント認証はディセーブルにされるので、認証チャレンジなしでアクセスできます。

```
dpe# service http 2 client-auth none
% OK (Requires DPE restart "> dpe reload")

dpe# service http 2 port 7550
% OK (Requires DPE restart "> dpe reload")

dpe# service http 2 ssl enable true
% OK (Requires DPE restart "> dpe reload")

dpe# service http 2 ssl keystore train-1.keystore changeme changeme2
% OK (Requires DPE restart "> dpe reload")

dpe# service http 2 ssl client-auth none
% OK (Requires DPE restart "> dpe reload")

dpe# service http 1 enable false
% OK (Requires DPE restart "> dpe reload")

dpe# service http 2 enable true
% OK (Requires DPE restart "> dpe reload")

dpe# dpe reload
Process dpe has been restarted.

% OK
```

（注） 詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

CPE 認証の設定

CPE 認証は、次の事項を通じてサポートされます。

- HTTP Basic または Digest 認証を使用する共有秘密情報。
- SSL を使用するクライアント証明書。共有秘密情報 HTTP ベースの認証の代わりとして、または追加機能として、証明書ベースのクライアント認証を使用できます。
- 外部クライアント証明書認証。このシナリオでは、SSL　接続は、クライアントの認証も行うハードウェア ロード バランサで終端します。

認証の目的は、信頼されるデバイス ID を確立することです。この ID は、DPE キャッシュでデバイス命令を検索するために使用されます。このデバイス ID は、BAC RDU データベースのデバイス レコードに事前プロビジョニングされたデバイス識別子と相関関係にあります。共有秘密情報 HTTP ベースの認証の場合、ユーザ名はデバイスのアイデンティティを確立するために使用され、デバイス ID として処理されます。一意のクライアント証明書を使用する認証の場合、デバイス ID はデバイス証明書の CN フィールドから取得されます。外部エンティティ（Cisco CSS 15000 シリーズ ロード バランサなど）によるクライアント証明書の場合、CN フィールドを含む証明書データは、HTTP ヘッダーで DPE に渡されます。

(注) クライアントを信頼できる場合、クライアント認証を行わないように選択することもできます。たとえば、加入者の物理ラインに基づいて、クライアントによるネットワーク アクセスがすでに認証されている場合もあります。この場合は、BAC を認証なしで設定することができます。Inform メッセージから、信頼されるデバイス ID が取得されます。

DPE 認証オプションは、DPE CLI から設定できます。

共有秘密情報の認証

BAC は、CPE と DPE との間の共有パスワードに基づく HTTP 認証をサポートします。この認証は、Basic および Digest の 2 つのモードで使用可能です。

(注) クライアント認証中のセキュリティ リスクを限定するため、Digest モード（デフォルトの設定）の使用が推奨されています。Basic モードではクライアント認証を使用しないようにしてください。

DPE CLI から Basic または Digest モードで認証を設定するには、次のコマンドを使用します。

```
# service {cwmp | http} num client-auth mode
```

- *num*：サービスのインスタンスを指定します。1 または 2 になります。
- *mode*：サービスのクライアント認証モードを示します。クライアント認証モードには、次のものがあります。
  - basic：Basic HTTP 認証をイネーブルにします。
  - digest：Digest HTTP 認証をイネーブルにします。これがデフォルト設定です。
  - none：Basic および Digest 認証をディセーブルにします。

詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

デバイス パスワードの変更

BAC では、デバイスの共有秘密情報を設定できます。共有秘密情報は、`IPDeviceKeys.CPE_PASSWORD` プロパティを使用してデバイス レコードに格納されます。CPE は、HTTP ベースの認証中に、このパスワードを知っていることを証明する必要があります。Basic モードでは、パスワードは符号化クリア テキストとして送信されますが、Digest モードでは、デバイスはパスワードを送信することなくパスワードに関する知識を持っていることを証明できます。

パスワードは、次の方法で設定できます。

- API 上では、`IPDeviceKeys.CPE_PASSWORD` プロパティを使用します。
- 管理者のユーザ インターフェイス上では、**Devices** > **Add Device** ページまたは **Modify Device** ページにある CPE Password フィールドを使用します。

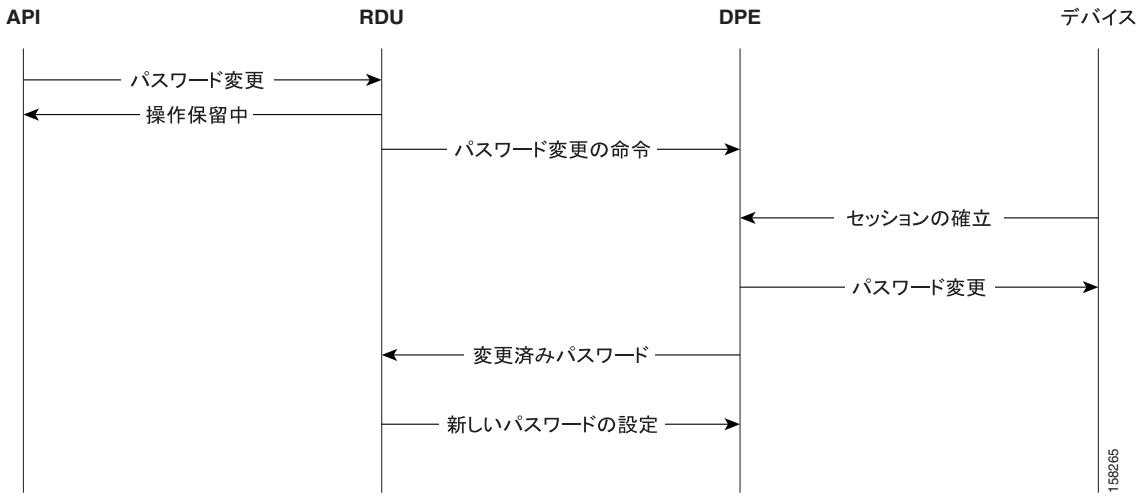
(注) RDU への DPE 接続が使用可能でない場合、CPE パスワードは変更できません。

SSL を使用してクライアント証明書によりクライアント認証をイネーブルにした場合、CPE パスワードはオプションです。

BAC によって使用されるパスワードの変更と、デバイスによって使用されるパスワードの変更を、区別する必要があります。BAC のデバイス レコードでパスワードを設定する場合、以前のパスワードの値に応じて結果は異なります。パスワードがデバイス レコードですでに設定されている場合、BAC はこれを変更して、実際のデバイスでパスワードを変更するプロセスを開始します。ただし、デバイス レコードに以前のパスワード値が存在しない（または空の文字列であった）場合、BAC はデバイス レコードに新しいパスワードを設定しますが、実際のデバイスのパスワードの変更は開始しません。したがって、BAC 内でのみパスワードを既存の値から別の値に変更する場合は、最初に BAC で値をリセット（空の文字列に設定）してから、それを新しい値に設定する必要があります。

図 13-1 は、実際のデバイスでパスワードを変更するために BAC が使用するプロセスを示しています。BAC が、デバイスを認証するために最初に古いパスワードを使用してから、新しいパスワードを設定する必要があるため、このプロセスは複雑になっています。パスワードの変更が確認されてからのみ、BAC は以前のパスワードを無効にしてデータベースから削除します。

図 13-1　パスワード変更のフロー



RDU のデバイス オブジェクトでパスワードが変更された後、パスワード変更命令はデバイス設定に含められます。この時点では、デバイスを認証するために引き続き古いパスワードが使用されます。次に、新しい設定命令がデバイスのプロビジョニング グループ内のすべての DPE に転送されます。

デバイスが BAC と次のセッションを作成するとき、デバイスは古いパスワードで認証されます。その後、新しいパスワードは SetParameterValues RPC を介して設定されます。DPE が変更を RDU に通知すると、RDU はデバイス パスワードを変更し、新しいパスワードが含まれる新しい設定命令を生成します。その後、古いパスワードは BAC に格納されなくなります。

新しいパスワードは、デバイスで設定されるまで変更可能です。たとえば、デバイスの元のパスワード（*password*）が *newpassword* に変更されたとします。しかし、新しいパスワードを設定するためにデバイスが BAC に接続する前であれば、パスワードは引き続き変更できます。この例を示すため、ここでパスワードを *n3wpa550d* に変更したと仮定します。デバイスが BAC に接続するまで、デバイスは引き続き古いパスワード（*password*）で認証されます。新しいパスワード（*n3wpa550d*）は、デバイスの BAC との次のセッション中に設定されます。

デバイス パスワードの修正

スペルが間違っているパスワードを、RDU で変更することもできます。たとえば、*password* の代わりに *passwrod* と入力した場合、最初にパスワードを削除して送信します。この時点で、デバイス オブジェクトには、関連付けられているパスワードはありません。次に、デバイスにパスワードを追加します。

(注) この方法は、デバイス内のパスワードではなく、BAC 内のパスワードを変更する場合に使用します。

管理者のユーザ インターフェイスからデバイス パスワードを修正するには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** から、適切なデバイスに対応する Identifier リンクをクリックします。

ステップ 2　Modify Device ページが表示されます。CPE Password フィールドのデバイス パスワードを削除します。

ステップ 3　**Submit** をクリックします。

ステップ 4　**Modify Device** ページに戻ります。正しいパスワードを入力します。

ステップ 5　**Submit** をクリックします。

これで、RDU のデバイス レコードでパスワードが変更されました。この手順の後、実際のデバイス上でパスワードの変更は開始されません。

クライアント証明書認証

認証のために、デバイスにより提供された検証済みの証明書を要求するように、DPE を設定できます。次の証明書が含まれます。

- 汎用：すべての CPE または CPE の大部分に共通の汎用証明書を使用して、SSL 経由のデバイス証明書認証をイネーブルにします。
- 一意：各 CPE が提供する一意の証明書を使用することにより SSL 経由のクライアント証明書認証をイネーブルにします。

デバイス証明書が一意である場合、HTTP 認証を使用する必要はありません。しかし、すべてのデバイスで同じ証明書が使用される場合（つまり、サービス プロバイダーが使用する単一デバイス証明書）、追加の HTTP 認証を設定する必要があります。

DPE CLI からクライアント証明書認証を設定するには、次のコマンドを使用します。

```
# service {cwmp | http} num ssl client-auth mode
```

- *num*：サービスのインスタンスを示します。1 または 2 になります。デフォルトで、SSL によるクライアント証明書認証は次のようになります。
  - サービス 1 の場合：ディセーブル
  - サービス 2 の場合：ディセーブル

- *mode*：クライアント証明書認証のモードを示します。BAC は次のモードをサポートします。
  - client-cert-generic：デバイスのセットに共通の証明書を使用します。
  - client-cert-unique：デバイスに一意の証明書を使用します。
  - none：クライアント証明書認証をディセーブルにします。

外部クライアント証明書認証

SSL 接続は、ロード バランサなど、DPE の外側で終端させることができます。この場合、DPE は SSL サービスなしで設定できます。

SSL 接続の終端として CSS 11500 などのロード バランサを使用する場合、DPE は一意の証明書を受け取らないので、HTTP 認証（Basic または Digest）を持たないデバイスを識別することは不可能になります。この問題を解決するため、ロード バランサは、証明書情報が含まれる追加の HTTP ヘッダーを挿入します。

単一のセッションに複数の TCP 接続が含まれる場合、それぞれの接続が認証されます（イネーブル時）。セッションの cookie により、デバイスと既存のセッション状態がバインドされます。

CSS でクライアント証明書認証を設定する方法の詳細については、P.12-18 の「Cisco CSS でのクライアント証明書認証の設定」を参照してください。

BAC における認証オプション

この項では、BAC で CWMP サービスおよび HTTP ファイル サービスに対して使用可能なクライアント認証オプションの組み合せの概要を説明します。これらのサービスの各インスタンスは、要件に合せて DPE CLI から個別に設定できます。

BAC は、CPE と DPE との間の共有パスワードに基づく Basic および Digest モードの HTTP 認証をサポートします。HTTP ベースの認証を使用する場合は、Digest モードを使用することをお勧めします。

各 CPE に一意の証明書を使用して CPE 認証を設定することもできます。この場合、HTTP 認証は必要ありません。ただし、すべての CPE または CPE の大部分に共通の汎用証明書を使用して CPE 認証を設定する場合、追加の HTTP 認証を要求するように DPE を設定することをお勧めします。

表 13-3 は、BAC がサポートするさまざまなオプションと、認証を設定するために DPE CLI から使用するコマンドを示しています。各コマンドの詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

表 13-3　BAC における認証オプション

オプション	使用するコマンド
HTTP を使用	
Basic または Digest モードで HTTP を使用してデバイス認証をイネーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth** {**basic** | **digest**}
HTTP を使用するデバイス認証をディセーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth none**
(注) HTTP を使用するデバイス認証がディセーブルになっている場合、信頼されるデバイスのアイデンティティは、デバイスからの Inform メッセージの値を使用して形成されます。	
SSL を使用	
SSL 接続で、HTTP Basic または Digest モードのデバイス認証をイネーブルにする。クライアント証明書認証は使用しない。	**service** {**cwmp** | **http**} *num* **client-auth** {**basic** | **digest**} **service** {**cwmp** | **http**} *num* **ssl client-auth none**
一意のクライアント証明書に基づく SSL 接続で、HTTP Basic または Digest モードでデバイス認証をイネーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth** {**basic** | **digest**} **service** {**cwmp** | **http**} *num* **ssl client-auth client-cert-unique**
(注) HTTP ベース（Basic または Digest）の認証、および一意の証明書を使用する認証を要求するように DPE を設定した場合、デバイスは両方のメカニズムを使用して認証されます。この二重認証シナリオでは、デバイスの一意の識別子は、クライアント証明書の CN フィールドを使用して形成されます。その結果、信頼されるデバイス ID が確立されます。	
汎用のクライアント証明書に基づく SSL 接続で、HTTP Basic または Digest モードでデバイス認証をイネーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth** {**basic** | **digest**} **service** {**cwmp** | **http**} *num* **ssl client-auth client-cert-generic**
HTTP Basic または Digest 認証、および Cisco CSS 11500 によるクライアント証明書認証を使用してデバイス認証をイネーブルにする。	**service** {**cwmp**| **http**} *num* **client-auth** {**basic** | **digest**} **service** {**cwmp** | **http**} *num* **ssl client-auth client-cert-css-ext**
(注) この二重の認証のシナリオでは、信頼されるデバイス ID は、Cisco CSS による認証に基づいて確立され、HTTP ヘッダーを使用する DPE に伝達されます。	
Cisco CSS 11500 によって検証されたクライアント証明書に基づくデバイス認証をイネーブルにする。	**service** {**cwmp** | **http**} *num* **ssl client-auth client-cert-css-ext**
デバイス認証およびクライアント証明書認証をディセーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth none** **service** {**cwmp** | **http**} *num* **ssl client-auth none**
(注) デバイス認証およびクライアント証明書認証がディセーブルになっている場合、デバイスは信頼済み、または事前認証済みと見なされ、DPE は CWMP Inform メッセージからのデータを使用して、信頼されるデバイスのアイデンティティを確立します。	

表 13-3　BAC における認証オプション（続き）

オプション	使用するコマンド
HTTP ベースのデバイス認証をディセーブルにし、各 CPE が提供する一意の証明書を使用して SSL 経由のクライアント認証をイネーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth none** **service** {**cwmp** | **http**} *num* **ssl client-auth client-cert-unique**
HTTP ベースのデバイス認証をディセーブルにし、汎用の証明書を使用して SSL 経由のクライアント認証をイネーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth none** **service** {**cwmp** | **http**} *num* **ssl client-auth client-cert-generic**
HTTP ベースのデバイス認証をディセーブルにし、Cisco CSS 11500 によって検証されたクライアント証明書に基づく認証をイネーブルにする。	**service** {**cwmp** | **http**} *num* **client-auth none** **service** {**cwmp** | **http**} *num* **ssl client-auth client-cert-css-ext**

（注） HTTP ベースのデバイス認証がディセーブルで、汎用の証明書を使用するようにクライアント証明書認証がイネーブルになっている場合、デバイスは信頼済み、または事前認証済みであると見なされ、DPE は CWMP Inform メッセージからのデータを使用して、信頼されるデバイスのアイデンティティを確立します。

CWMP デバイス操作

この章では、Broadband Access Center（BAC）のデバイス操作のメカニズムについて説明します。このメカニズムを使用すると、デバイスに対する CPE WAN Management Protocol（CWMP）リモート プロシージャ コールを実行し、デバイスのプロビジョニング グループの変更などの保守作業を行うことができます。

この章では、次のトピックについて説明します。

概要

デバイスに対して個別の CWMP Remote Procedure Call（RPC; リモート プロシージャ コール）を即時に実行するか、デバイスが次回 BAC に接続するときに実行するには、デバイス操作を使用します。プロビジョニング API からこの機能を使用することにより、デバイスと BAC の間の対話のトラブルシューティング、データの収集、またはカスタマイズを行うことができます。

デバイス操作をバッチで送信するには、`IPDevice.performOperation()` API コールを使用します。（詳細については、API Javadoc を参照してください）。一部の操作は、管理者のユーザ インターフェイスから実行できます。この項では、デバイス操作が API または管理者のユーザ インターフェイスのどちらを使用して開始されるかに関係なく、デバイス操作の基になっている概念に重点を置いて説明します。

（注） BAC のインストール中に、いくつかのサンプル ファイルが *BPR_HOME/rdu/samples* ディレクトリにコピーされます。このディレクトリの内容は次のとおりです。

- *cwmp* ディレクトリ。このディレクトリには **parameter-list.xml* ファイルがあります。これらのファイルには、管理者のユーザ インターフェイスを使用してデバイスのライブ データを取得するときに使用するパラメータ リストが記述されています。
- *provapi* ディレクトリ。このディレクトリには、API を使用してデバイス操作を実行できる方法が記述されている *CwmpDiagnosticImmediate.java* と *CwmpDiagnosticOnConnect.java* ファイルがあります。

表 14-1 は、この BAC リリースでサポートされているデバイス操作を示しています。

表 14-1　BAC でサポートされているデバイス操作

操作名	説明
CreateObjectInstance	デバイスのデータ モデル内にオブジェクト インスタンスを作成します。
DeleteObjectInstance	デバイスのデータ モデルからオブジェクトを削除します。
Download	ファイルのダウンロードを実行するようにデバイスに指示します。
FactoryReset	デバイスの設定を工場出荷時のデフォルト状態にリセットします。
Reboot	デバイスにリブートを指示します。
GetParamAttributes	デバイスのパラメータの属性を取得します。
GetParamNames	デバイスによって公開されたパラメータの名前を取得します。
GetParamValues	デバイスのパラメータ空間からパラメータの値を取得します。
GetRPCMethods	デバイスでサポートされている RPC メソッドのリストを取得します。
SetParamAttributes	Notification や Access List など、デバイス パラメータ属性の値を設定します。
SetParamValues	デバイス パラメータの値を設定します。
ChangeProvGroup	デバイスを新しいプロビジョニング グループにリダイレクトします。
GenerateConfig	デバイスの命令セットを再生成します。
PassThrough	デバイスに汎用 SOAP メッセージを送信します。
RemoveOperation	保留中の接続時デバイス操作を削除します。
RequestConnection	デバイスへの接続要求を開始します。

すべてのデバイス操作は、データの同期化、設定の同期化、ファームウェア ルールのダウンロードなどの他の設定サービスの前に実行されます。

注意　デバイス操作では、デバイス設定の更新は実行しないでください。デバイス操作を使用して行った設定はすべて、設定プロセスによって上書きされる可能性があります。

デバイス操作の接続モード

BAC では、次の 2 つのモードでデバイス操作を実行できます。

- 即時
- 接続時

即時モード

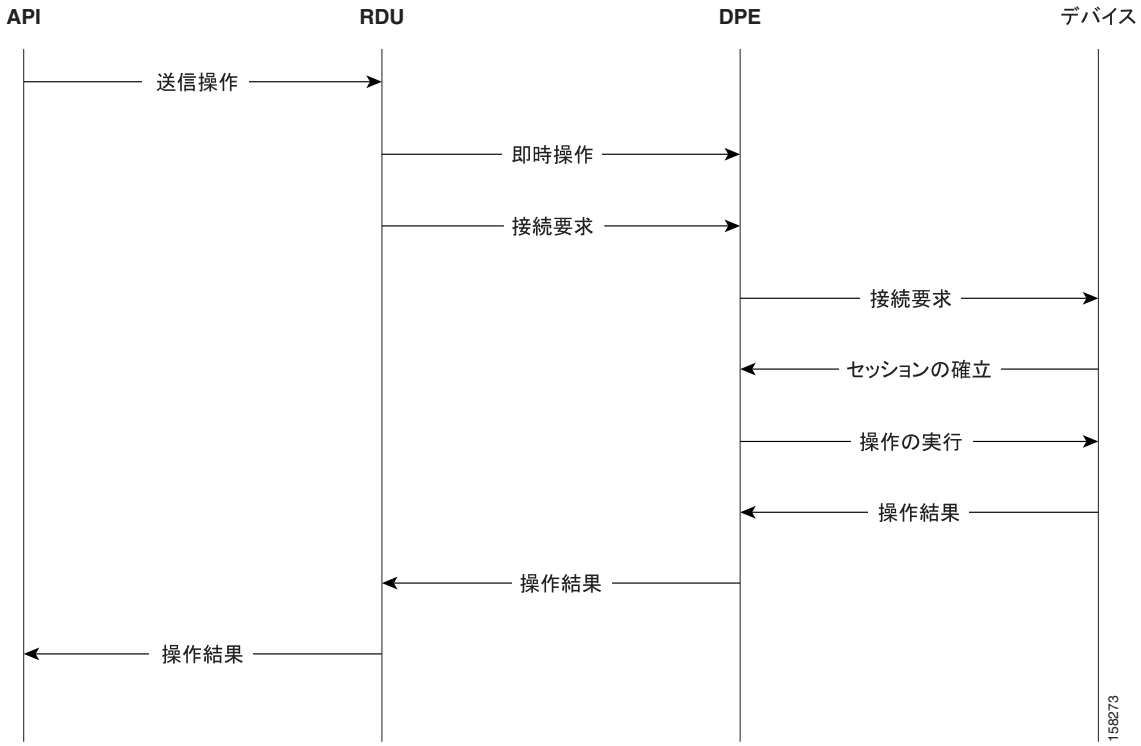
即時実行は、デバイスが到達可能であることを前提としており、デバイスへの接続要求を最初に発行する DPE によって行われます。デバイスが到達可能でない場合、操作は自動的に失敗します。1 つの接続要求を作成し、CWMP デバイスとの管理セッションを 1 つにすることで、複数の操作を同じバッチで実行できるようになり、パフォーマンスを向上させることができます。

クライアントは、タイムアウト期間を使用して、API バッチを即時モードで送信します。タイムアウトが設定されていない場合、即時操作がタイムアウトになるまでの時間は、デフォルトで 60 秒です。デバイス操作がタイムアウトになった場合、またはそのバッチがタイムアウトになった場合、エラーが返されます。

（注） デバイスに対して即時操作の実行を試みる前に、デバイスが到達可能であり、BAC がデバイスへの接続要求を実行するように設定されていることを確認してください。P.12-3 の「接続要求サービス」を参照してください。

図 14-1 は、即時操作の上位フローを示しています。

図 14-1　即時操作モードのワークフロー



即時実行を指定して performOperation() API メソッドを呼び出すと、RDU は、対応する操作命令を構築して、デバイスのプロビジョニング グループ内のすべての DPE に送信します。次に、RDU は接続要求命令をプロビジョニング グループ内の特定の DPE に送信します。DPE はそれを受けて、接続要求通知をデバイスに送信します。

デバイスが DPE との接続を確立すると、DPE は新しいセッションを作成し、デバイスに対して操作を実行します。セッションが閉じられると、DPE は操作の結果を RDU に返します。RDU はその結果をバッチのコマンド ステータスで API クライアントに転送します。

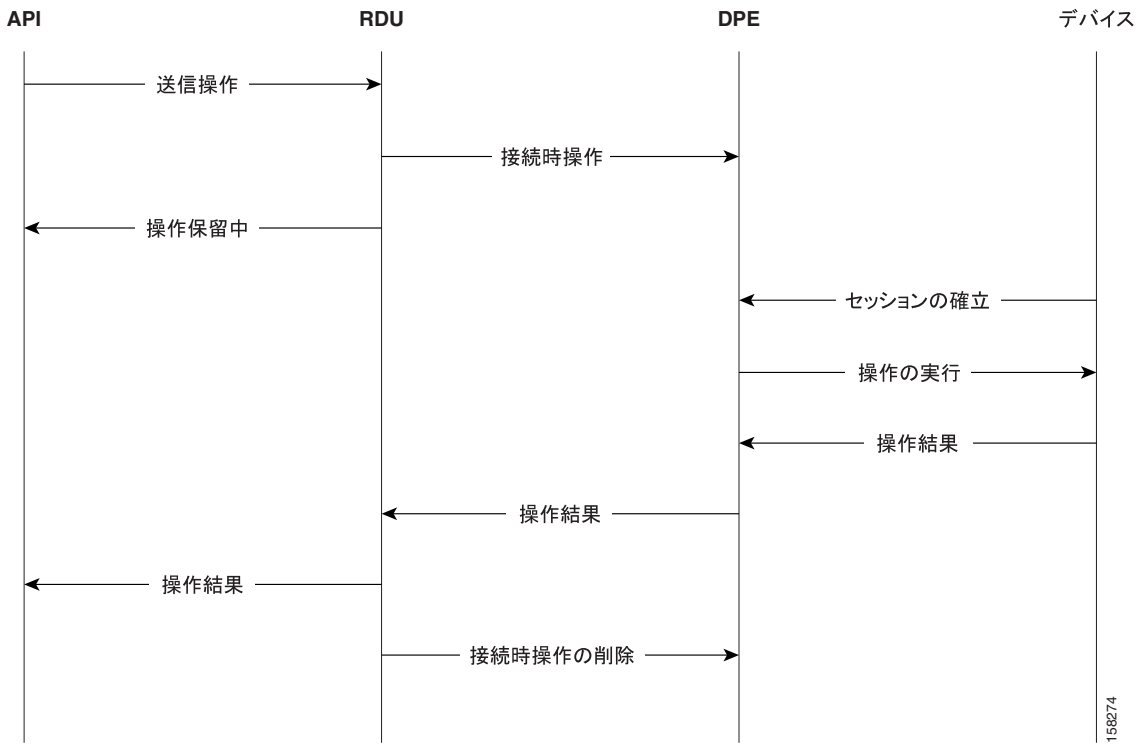
接続時モード

接続時実行を使用すると、到達可能でないデバイスをサポートできます。CWMP デバイスからの定期的な Inform RPC と併用するのが最善です。

接続時操作は、デバイスのプロビジョニング グループ内の各 DPE で保持されます。接続時操作は、RDU が（AsyncOperationEvent を介してクライアントに実行結果を通知した後）DPE に削除を指示するまで DPE から削除されません。

図 14-2 は、接続時操作の上位フローを示しています。

図 14-2　接続時操作モードのワークフロー



API クライアントは、接続時実行を指定して IPDeviceOperation を構築します。API クライアントは適切な AsyncOperationEvent リスナーを登録し、performOperation() API メソッドを呼び出します。次に、RDU は対応する操作命令を構築し、デバイスのプロビジョニング グループ内のすべての DPE に送信します。DPE は内部データベースに操作を保存します。RDU バッチが完了し、BatchStatus が API クライアントに返されます。

即時操作の実行時と異なり、DPE はデバイスへの接続要求通知を開始しません。

デバイスが次回 DPE に接続するときに、DPE はデバイスとの新しいセッションを作成し、デバイスに対して操作を実行します。セッションが終了すると、操作の結果が RDU に送信され、RDU は登録済みのすべての API クライアント リスナーに AsyncOperationEvent を送信します。

（注） 即時操作は、必ず接続時操作より先に実行されます。BAC を使用して、各操作モードを組み込み型の命令と組み合せることができますが、各命令が相互に無効にすることがないよう確認する必要があります。たとえば、デバイスの設定テンプレートで InternetGatewayDevice.ManagementServer.PeriodicInformEnable が *false* に指定されている場合、デバイス操作で指定を *true* に変更しても、設定テンプレートは必ずデバイス操作の後に実行されるため、設定テンプレートによって指定は *false* に上書きされます。

条件付き実行

上記に加えて、即時操作および接続時操作は、デバイスからの Inform メッセージ内の TR-069 Event Code に基づいて条件付きで実行されます。デバイスの Inform で報告されている Event Code と、操作で指定された Event Code のリストの間に共通部分がない場合、操作は実行されません。

たとえば、1 つの操作では、Inform Event Code リストに `6 CONNECTION REQUEST` が含まれていることが条件だとします。この場合、操作が実行されるのは、Autoconfiguration Server（ACS; 自動構成サーバ）接続要求により接続しているとデバイスが報告した場合に限られます。定期的な Inform などの他の理由により、デバイスが接続しているとの報告があった場合、操作は実行されません。

デバイスのプロビジョニング グループの管理

CWMP デバイスのプロビジョニング グループは、RDU のデバイス オブジェクトに対して指定します。次の手段があります。

- プロビジョニング API：`IPDeviceKeys.HOME_PROV_GROUP` プロパティを使用します。
- 管理者のユーザ インターフェイス：Devices の各ページにある Home Provisioning Group ドロップダウン リストを使用します。

デバイスのプロビジョニング グループの管理では、場合によっては、デバイスのプロビジョニング グループをリダイレクトまたは修正する必要があります。

- デバイスのプロビジョニング グループのリダイレクト

  特定のプロビジョニング グループ（たとえば、PG1）と通信しているデバイスを、別のプロビジョニング グループ（PG2）と通信するようにリダイレクトします。
- デバイスのプロビジョニング グループの修正

  デバイスのプロビジョニング グループが BAC で誤っている場合、BAC だけで変更する必要があります。たとえば、PG1 への接続を試行するデバイスが、BAC で PG2 にプロビジョニングされている場合などです。

次の各項では、それぞれの使用例について詳細に説明します。

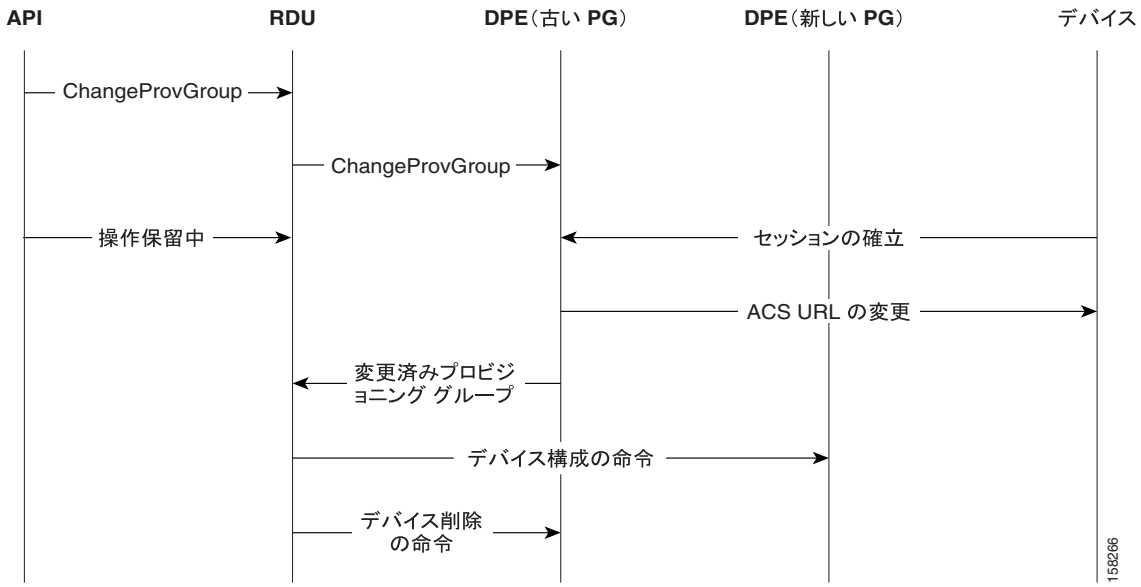
（注） DPE が RDU に接続できない場合、デバイスのプロビジョニング グループを変更することはできません。

デバイスのプロビジョニング グループのリダイレクト

このプロセスでは、新しいプロビジョニング グループ内の DPE にデバイス命令を配信し、その DPE がデバイス要求を処理できるようにします。また、デバイスに、新しいプロビジョニング グループの場所（ACS URL）を指示します。BAC を使用してこの変更を最も効率的に行うには、リダイレクト命令を使用します。

図 14-3 は、`IPDevice.performOperation()` API コールで ChangeProvGroup 操作を使用する場合の上位フローを示しています。

図 14-3　プロビジョニング グループのリダイレクトのワークフロー



ChangeProvGroup 操作が RDU で実行されると、リダイレクト命令（またはプロビジョニング グループ変更命令）はデバイス設定に含められます。この時点では、デバイスはまだ既存のプロビジョニング グループに割り当てられています。次に、新しい設定命令がデバイスのプロビジョニング グループ内のすべての DPE に転送されます。

デバイスが次回 BAC とセッションを（接続要求などから）確立すると、デバイスは認証され、DPE は新しい DPE が設定された URL を SetParameterValues RPC を介して設定します（プロビジョニング グループの ACS URL は、管理者のユーザ インターフェイスで設定できます。P.3-8 の「プロビジョニング グループの設定ワークフロー」を参照してください。ACS URL が設定されていない場合、検出された URL が使用されます。検出された URL とは、DPE インターフェイスの設定に基づいて自動的に構築された URL のことです）。

（注） プロビジョニング グループの設定済み URL は、検出された URL より常に優先されます。

RDU に変更が通知されると、RDU はデバイスのプロビジョニング グループを変更し、そのデバイスに関する新しい設定命令セットを生成します。デバイスの設定は、その後、デバイスの新しいプロビジョニング グループ内のすべての DPE に送信されます。こうして、デバイスは新しいプロビジョニング グループに接続し、その DPE サーバ グループから管理されるようになります。

デバイスのプロビジョニング グループの修正

デバイスに対する誤ったプロビジョニング グループ指定を、単にリセットすることもできます。このシナリオでは、実際のデバイスを変更する必要はありません。必要な操作は BAC の更新だけです。

誤っているプロビジョニング グループを API で変更するには、`IPDevice.changeProperties()` API を呼び出し、`IPDeviceKeys.HOME_PROV_GROUP` プロパティでプロビジョニング グループを修正します。詳細については、API Javadoc を参照してください。

誤ったプロビジョニング グループ指定を管理者のユーザ インターフェイスで変更するには、次の手順に従います。

(注) ホーム プロビジョニング グループを管理者のユーザ インターフェイスから変更する場合、修正されるのは BAC 内のプロビジョニング グループだけです。デバイスはこの変更の影響を受けません。

ステップ 1　プライマリ ナビゲーション バーの **Devices** タブをクリックします。

ステップ 2　Manage Devices ページが表示されます。適切なデバイスに対応する Identifier リンクをクリックします。

ステップ 3　Modify Device ページが表示されます。Home Provisioning Group ドロップダウン リストから目的のオプションを選択します。

ステップ 4　**Submit** をクリックして、デバイスへの変更を保存します。

これで、デバイスは特定のプロビジョニング グループに割り当てられます。

管理者のユーザ インターフェイスについて

この章では、Broadband Access Center（BAC）管理者のユーザ インターフェイスにアクセスする方法と、そのインターフェイス自体について説明します。この章では次のトピックについて説明します。

P.16-1 の「管理者のユーザ インターフェイスの使用方法」では、このユーザ インターフェイスを使用して管理作業を実行する方法を説明します。Device Provisioning Engine（DPE）へのアクセス、監視、および制御で使用する CLI コマンドについては、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』に説明があります。

管理者のユーザ インターフェイスの設定

管理者のユーザ インターフェイスを使用する前に、*adminui.properties* ファイルの内容を確認してください。このファイルには、インターフェイスの動作を指定する各種のコントロールが含まれています。

テキスト エディタを使用してこのファイルを開き、必要な機能を実行するようにその内容を変更できます。変更を完了して保存し、このユーザ インターフェイスを再起動すると、すべての変更が有効になります。

管理者のユーザ インターフェイスを起動するには、次のように入力します。

```
# etc/init.d/bprAgent tomcat start
```

管理者のユーザ インターフェイスを停止するには、次のように入力します。

```
# etc/init.d/bprAgent tomcat stop
```

このユーザ インターフェイスは、*adminui.properties* ファイルにあるオプションを使用して設定できます。これらのオプションは、BAC の設定によって制御するか、*BPR_HOME/rdu/conf* ディレクトリにある *adminui.properties* ファイルで定義します。

構成パラメータは次のとおりです。

- /adminui/port：RDU のリスニング ポートを指定します。デフォルトでは、このポート番号は 49187 です。
- /adminui/fqdn：RDU を実行するホストの完全修飾ドメイン名を指定します。デフォルトでは、この値はホストの FQDN です。たとえば、bac_test.ACME.COM です。
- /adminui/maxReturned：検索結果の最大件数を指定します。デフォルトでは、この数は 1000 です。
- /adminui/pageSize：1 ページに表示される検索結果の件数を指定します。この数は 25、50、または 75 に設定できます。デフォルト値は 25 です。
- /adminui/refresh：リフレッシュ機能をイネーブルにするか、ディセーブルにするかを指定します。デフォルトでは、このオプションはディセーブルになっています。
- /adminui/extensions：BAC での拡張の使用をイネーブルにするか、ディセーブルにするかを指定します。拡張を使用すると、BAC の動作を強化したり、新しいデバイス テクノロジーのサポートを追加したりできます。デフォルトでは、拡張の使用はイネーブルになっています。
- /adminui/maxFileSize：BAC にアップロードされるファイルの最大サイズを指定します。デフォルトでは、このファイル サイズは 10 MB です。
- /adminui/refreshRate：画面がリフレッシュされるまでの時間の長さ（秒数）を指定します。デフォルトでは、この値は 90 秒です。このオプションの値を設定する前に、/adminu/refresh オプションがイネーブルであることを確認してください。
- /adminui/timeout：アイドル セッションがタイムアウトになるまでの時間の長さ（秒数）を指定します。デフォルトでは、この時間は 300 秒に設定されています。
- /adminui/noOfLines：このユーザ インターフェイスに表示される *rdu.log* または *dpe.log* の、最後の行番号を指定します。デフォルトでは、表示される行数は 250 です。
- /adminui/noOfFiles：表示されるトラブルシューティング ログ ファイルの数を指定します。デフォルトでは、表示できるファイルの数は 1 です。一度に表示できるファイルの最大数は 5 です。

例 15-1　adminui.properties ファイルのサンプル

```
/adminui/port=49187
/adminui/fqdn=doc.cisco.com
/adminui/maxReturned=1000
/adminui/pageSize=25
/adminui/refresh=disabled
/adminui/extensions=enabled
/adminui/maxFileSize=10000000
/adminui/refreshRate=90
/adminui/timeout=300
/adminui/noOfLines=250
/adminui/noOfFiles=1
```

管理者のユーザ インターフェイスへのアクセス

管理者のユーザ インターフェイスには、BAC アプリケーションの URL にアクセスできる任意のコンピュータからアクセスできます。

ログイン

このユーザ インターフェイスには、管理ユーザ、読み取り / 書き込みユーザ、または読み取り専用ユーザとしてログインできます。P.16-2 の「ユーザ管理」で説明するとおり、実行可能な機能は各ユーザ タイプで異なりますが、ユーザ インターフェイスには同じ方法でアクセスします。

管理者のユーザ インターフェイスにアクセスするには、次の手順に従います。

ステップ 1　Web ブラウザを起動します。

表 15-1 は、この BAC リリースでサポートされるブラウザのリストを示しています。

表 15-1　ブラウザのプラットフォーム サポート

プラットフォーム	サポートするブラウザ
Windows 2000（Service Pack 2）	Internet Explorer 6.0 以降
Windows 2000、Windows XP、Solaris、Linux	Mozilla 1.7.3

ステップ 2　次の構文を使用して、管理者の場所を入力します。

```
http://machine_name/
```

- *machine_name*：Regional Distribution Unit（RDU）を実行しているコンピュータを示します。

（注）　HTTP over SSL（HTTPS とも呼ばれる）を使用して管理者のユーザ インターフェイスにアクセスするには、`https://machine_name/` と入力します。

サーバ側の管理アプリケーションは、コンピュータ ポート上で実行されます。デフォルトでは、このポート番号は次のとおりです。

- HTTP over TCP の場合：80
- HTTP over SSL の場合：443

メイン ログイン ページ（図 15-1）が表示されます。

図 15-1　ログイン ページ

ステップ 3　デフォルトのユーザ名（**admin**）とパスワード（**changeme**）を入力します。

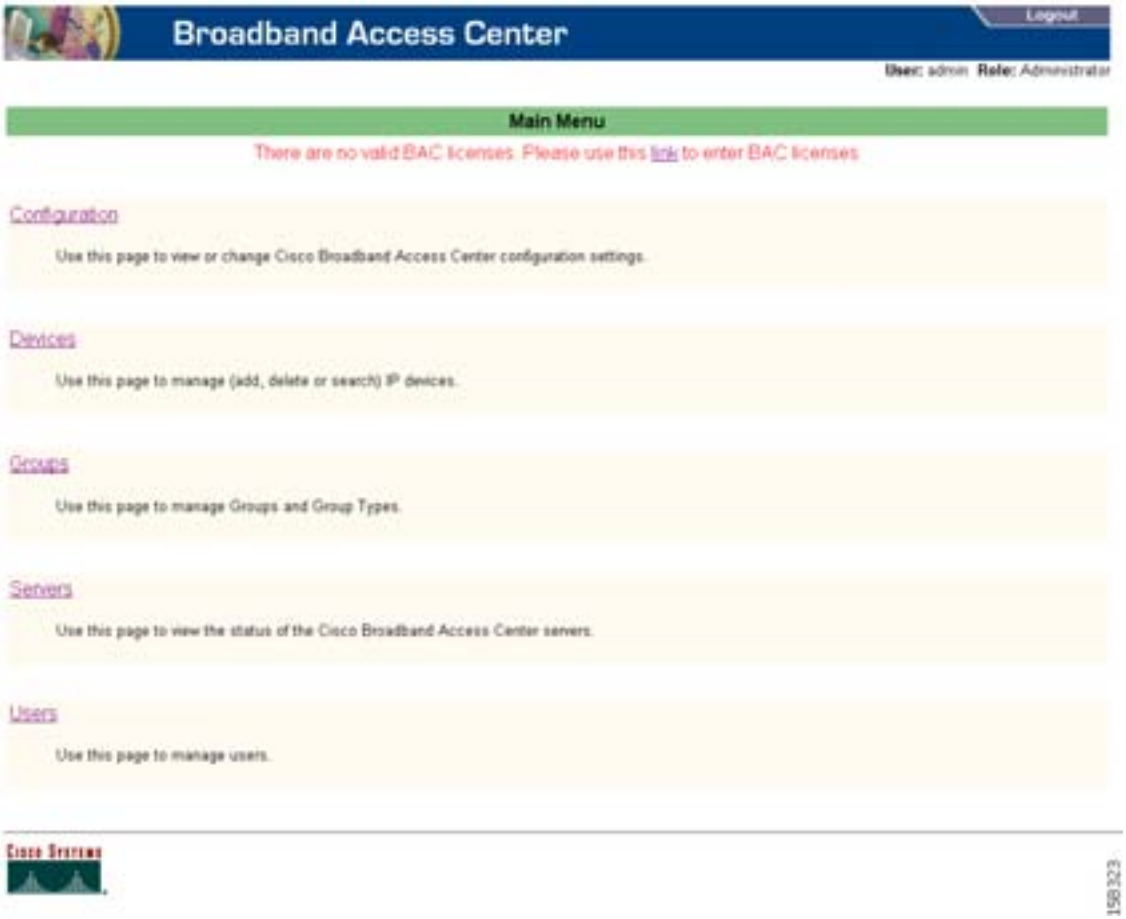
a.　初めてログインする場合は、Change Password 画面が表示されます。新しいパスワードを入力して、確認します。

（注）　ログインした RDU サーバの FQDN が User Login 領域に表示されます。

ステップ 4　**Login** をクリックすると、Main Menu ページ（図 15-2）が表示されます。

（注）　ページの上部にあるリンクを使用して、新しい BAC ライセンスを追加してください。このページでは、使用許諾を得たテクノロジー ライセンスを入力できます。詳細については、P.17-1 の「Broadband Access Center の設定」を参照してください。

図 15-2　Main Menu ページ



ログアウト

BAC からログアウトするには、次の手順に従います。

ステップ 1　ページの右上にある **Logout** をクリックします。

ステップ 2　確認ダイアログが表示されます。**OK** をクリックします。

User Login ページ（図 15-1）に戻ります。

管理者のユーザ インターフェイスのアイコンについて

BAC 管理者のユーザ インターフェイスには、特定の機能を実行するときに使用できるアイコンがあります。表 15-2 は、これらのアイコンを示しています。

表 15-2　管理者のユーザ インターフェイスのアイコン

アイコン	説明
	このアイコンには次の役割があります。 • View Details アイコン：特定のデバイスまたはファイルの詳細を表示できます。 • Operations アイコン：特定のデバイスでの操作を実行できます。
	Delete アイコン：特定のオブジェクトを削除します。
	Export アイコン：特定のファイルの内容をクライアントのコンピュータにエクスポートします。

これらのアイコンは、管理者のユーザ インターフェイスで実行する手順に関する項で使用されています。次の項があります。

- 管理者のユーザ インターフェイスの使用方法（P.16-1）
- Broadband Access Center の設定（P.17-1）

管理者のユーザ インターフェイスの使用方法

この章では、Broadband Access Center（BAC）管理者のユーザ インターフェイスから実行する管理作業について説明します。管理作業には主に、次のような BAC コンポーネントのアクションの監視があります。

（注）この章で説明する手順は、チュートリアルの形式で示されています。可能な限り、各手順の結果を表す例を示すようにしてあります。
サーバの設定の詳細については、P.17-1 の「Broadband Access Center の設定」を参照してください。

ユーザ管理

ユーザの管理には、BAC を管理するユーザの追加、修正、削除があります。ユーザ タイプによっては、このメニューを使用して、ユーザを追加、修正、および削除できます。このメニューには、BAC を使用するように設定されているユーザがすべて表示され、それらのユーザのユーザ タイプも示されます。

BAC ユーザには、管理者、読み取り / 書き込みユーザ、読み取り専用ユーザという 3 つのタイプがあります。各ユーザ タイプはアクセス レベルが異なり、一意のアクセス権を付与されているため、アクセスを確実に制御してプロビジョニング データの一貫性を保つことができます。

割り当てられているユーザ タイプは、管理者のユーザ インターフェイスの各画面の右上近くに表示されます。

管理者

BAC が認識する管理者は 1 名のみです。このユーザは、デバイス データを表示、追加、修正、削除したり、他のユーザを作成したりできます。管理者は、他のユーザのアクセス権を読み取り / 書き込みから読み取り専用に変更することや、読み取り専用から読み取り / 書き込みに変更することもできます。また、他の任意のユーザ タイプのパスワードを変更することもできます。

「管理者」ユーザを削除することはできません。

読み取り / 書き込みユーザ

読み取り / 書き込みユーザは管理者と同じ機能を実行できますが、他のユーザを作成することや、他のユーザのユーザ タイプおよびパスワードを変更することはできません。読み取り / 書き込みユーザは、自分のパスワードを変更できます。

読み取り専用ユーザ

読み取り専用ユーザは、自分のパスワードの変更や、デバイス データの表示などの基本的なアクセスを実行できますが、デバイス データを変更することはできません。デバイスの動作を中断させるような操作は、一切実行できません。たとえば、命令のリセットや再生成は実行できません。

この項では、BAC ユーザ管理の次の手順について説明します。

- 新規ユーザの追加
- ユーザの修正
- ユーザの削除

(注) ユーザを追加または削除できるのは、管理者としてログインしている場合のみです。

新規ユーザの追加

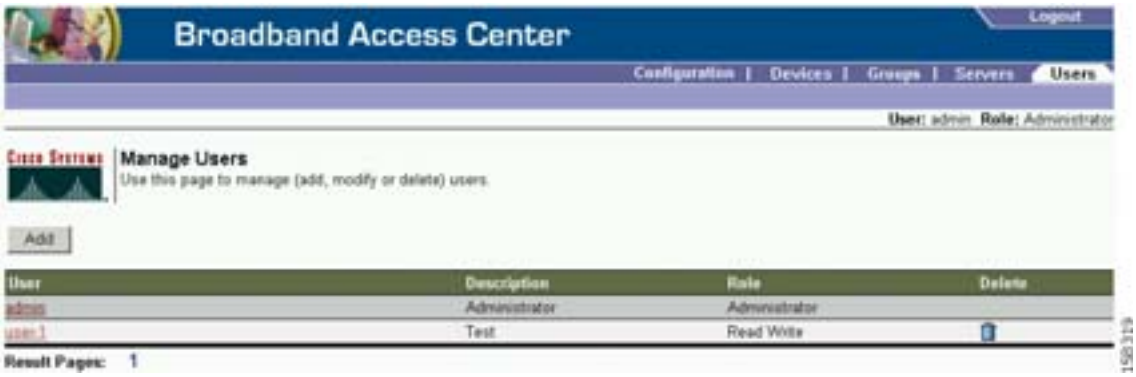
新規ユーザの追加は、ユーザ名を入力し、パスワードを作成する単純な手順です。ただし、新規ユーザを作成するときは、ユーザを読み取り / 書き込みユーザと読み取り専用ユーザのどちらのタイプにするかを決定する必要があります。BAC には、1 つの管理者ユーザがあらかじめ作成されています。管理者を新規ユーザとして作成することはできません。

新規ユーザを追加するには、次の手順に従います。

ステップ 1　Main Menu またはプライマリ ナビゲーション バーから **Users** をクリックします。

ステップ 2　Manage Users ページが表示されます（図 16-1 を参照してください）。**Add** をクリックして Add User ページを表示します。

図 16-1　Manage Users ページ



ステップ 3　新規ユーザのユーザ名とパスワードを入力します。

ステップ 4　新規ユーザのパスワードを確認のためにもう一度入力し、新規ユーザのロールを読み取り専用または読み取り / 書き込みのどちらにするかを選択します。各ユーザ タイプの詳細については、P.16-2 の「ユーザ管理」を参照してください。

ステップ 5　新規ユーザの簡単な説明を入力します。

ヒント　説明フィールドを使用して、ユーザの仕事または役職がわかるようにしたり、新規ユーザを区別したりします。

ステップ 6　**Submit** をクリックします。

新規ユーザが追加された状態で Manage Users ページが表示されます。

（注）　新規ユーザのパスワードは、記録して安全な場所に保管する必要があります。これは、パスワードの紛失または盗用、および不正な侵入を防ぐために役立ちます。

ユーザの修正

どのユーザ タイプでも自分のパスワードとユーザ説明は修正できますが、他のユーザの情報を修正できるのは管理者のみです。

ユーザ プロパティを修正するには、次の手順に従います。

ステップ 1　Main Menu またはプライマリ ナビゲーション バーから **Users** をクリックします。

ステップ 2　Manage User ページが表示されます。適切なユーザ名をクリックして対象ユーザの Modify User ページを表示します。

ステップ 3　パスワード、ユーザ タイプ（管理者としてログインしている場合）、およびユーザ説明に対して必要な変更を行います。

ステップ 4　**Submit** をクリックします。

ユーザ情報が修正された状態で Manage Users ページが表示されます。

ユーザの削除

Manage Users ページに表示される管理者以外のユーザは、管理者のみが削除できます。**admin** という名前のデフォルト ユーザを削除することはできません。

ユーザを削除するには、次の手順に従います。

ステップ 1　Main Menu またはプライマリ ナビゲーション バーから **Users** をクリックします。

ステップ 2　Manage User ページが表示されます。削除するユーザに対応する **Delete** アイコン（🗑）をクリックします。

ステップ 3　Delete User ダイアログボックスが表示されます。**OK** をクリックします。

削除したユーザが含まれていない状態で Manage Users ページが表示されます。

デバイス管理

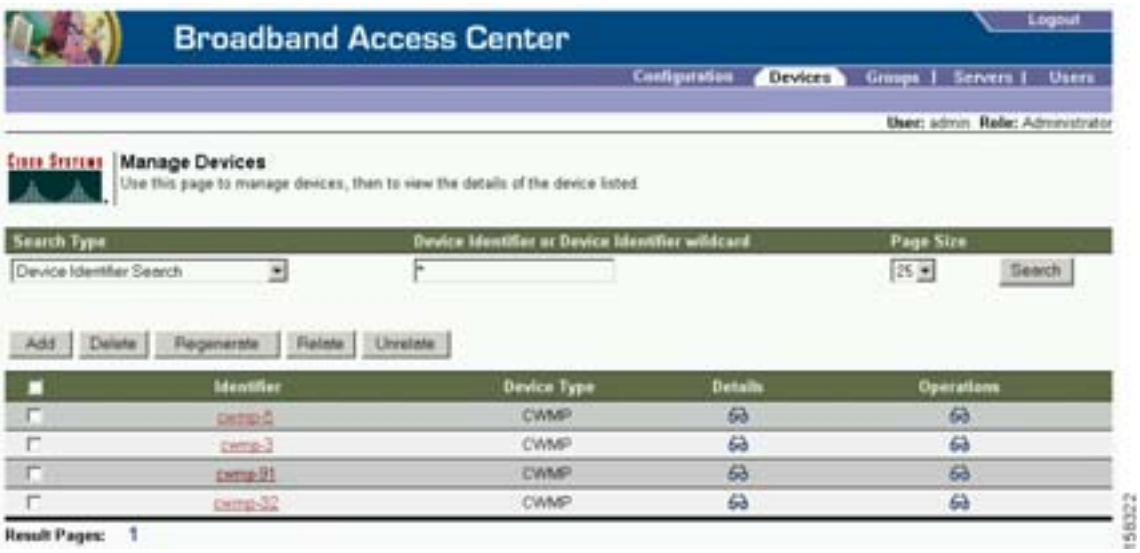
TR-069 対応のデバイスをプロビジョニングおよび管理するには、Devices メニューを使用します。次の操作を実行できます。

- 特定のデバイス、または指定した基準を共有しているデバイスのグループを検索する。P.16-6 の「デバイスの検索」を参照してください。
- RDU データベースを対象として、デバイスを追加、修正、または削除する。次の各項を参照してください。
  - デバイス レコードの追加（P.16-12）
  - デバイス レコードの削除（P.16-13）
- 設定、プロパティ、検出されたデータ、障害などのデバイス データを表示する。P.16-9 の「デバイスの詳細の表示」を参照してください。
- デバイス命令を再生成する。P.16-13 の「デバイス命令の再生成」を参照してください。
- 任意のデバイスを、特定のグループを対象として関連付けまたは関連付け解除する。P.16-14 の「デバイスの関連付けと関連付け解除」を参照してください。
- デバイスのトラブルシューティングをイネーブルにする。P.8-10 の「デバイスのトラブルシューティングの設定」を参照してください。
- デバイスに対して、IP PING やライブ データ取得などの各種操作を実行して、より多くの情報を収集する。P.16-16 の「デバイス操作の実行」を参照してください。

Manage Devices ページ

Manage Devices ページは、Main Menu またはプライマリ ナビゲーション バーの **Devices** をクリックすると表示されます。このページ（図 16-2）には、すべてのデバイス管理機能の実行に必要なフィールドとコントロールが含まれています。

図 16-2　Manage Devices ページ



デバイスの検索

BAC を使用して、さまざまな方法でデバイス情報を検索できます。

検索タイプを選択するには、Manage Devices ページで Search Type ドロップダウン リストをクリックします。後続の検索ページには、選択した検索タイプに固有の画面コンポーネントが含まれます。

Manage Devices ページでは、互いに関連する 2 つの独立領域を利用して、検索結果を生成します。この結果を使用して、多くのデバイス管理機能を実行できます。この領域とは、実行する検索を定義する Search Type ドロップダウン リストと、その検索タイプの内容を指定する検索値フィールドです。次の検索を実行できます。

- Device Identifier Search：デバイス ID を使用して検索します。この検索機能では、検索文字列の末尾のワイルドカードがサポートされています。特定のデバイスのデバイス ID 全体を指定して、1 つのデバイスだけをルックアップすることもできます。
- FQDN Search：デバイスに関連付けられている Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用して検索します。
- Group Search：特定のグループに属しているデバイスを検索します。
- Owner ID search：デバイスに関連付けられているオーナー ID を使用して検索します。オーナー ID は、サービス加入者のアカウント番号などを示す場合があります。この検索機能では、ワイルドカード検索はサポートされていません。
- Registered Class of Service Search：デバイスにプロビジョニングされているサービス クラスを使用して検索します。
- Related Class of Service Search：登録されているサービス クラスと選択されているサービス クラスの両方を使用して検索します。
- Selected Class of Service Search：RDU によって選択されたサービス クラスを使用して、登録されているサービス クラスを何らかの理由で保持できないデバイスを検索します。

実行可能な検索の中には、ワイルドカード文字（*）を使用して検索機能を拡張できるものがあります。BAC には、各検索で使用できる特定のワイルドカードがあります。表 16-1 は、それらのワイルドカードを示しています。

表 16-1　デバイス管理でサポートされる検索

検索メニュー	検索タイプのオプション
Device Identifier Search	デバイス ID 全体、または末尾にワイルドカード アスタリスク（*）文字を使用したデバイス ID の一部。 たとえば、ID が 0010BF-ZAA001A00001 のデバイスを検索するには、0010BF-* を指定できますが、*-ZAA001A00001 を使用した場合は結果を得られません。
FQDN Search	FQDN 全体、または先頭にワイルドカード アスタリスク（*）文字を使用した FQDN の一部。 たとえば、FQDN が IGW-1234.ACME.COM のデバイスを検索するには、次のように指定できます。 • *.acme.com • *.com • *

表 16-1　デバイス管理でサポートされる検索（続き）

検索メニュー	検索タイプのオプション
Group Search	Group Name (Group Type) • ドロップダウン リスト デバイス ID 全体、または末尾にワイルドカード アスタリスク（*）文字を使用したデバイス ID の一部。
Owner ID Search	Owner ID ワイルドカード検索はサポートされていません。完全なオーナー ID を入力する必要があります。
Registered Class of Service Search	Class of Service (Type) • ドロップダウン ボックス
Related Class of Service Search	Class of Service (Type) • ドロップダウン ボックス
Selected Class of Service Search	Class of Service (Type) • ドロップダウン ボックス

また、Page Size ドロップダウン リストを使用すると、1 ページあたりの検索結果表示件数を制限できます。結果表示件数は、25、50、または 75 から選択できます。検索結果の数が選択したページサイズよりも大きい場合は、ページ コントロールがページの左下に表示されます。これらのコントロールを使用して、1 ページずつ前後にスクロールしたり、特定のページを選択できます。

（注）任意のクエリーから返される結果の最大数は 1,000 で、1 ページに表示される結果の最大数は 75 です。デフォルトの最大数を変更するには、*BPR_HOME/rdu/conf/adminui.properties* ファイルの /adminui/maxReturned プロパティを修正し、**bprAgent restart tomcat** コマンド（*/etc/init.d/* ディレクトリにあります）を実行して、BAC Tomcat コンポーネントを再起動します。

デバイス管理コントロール

ここで説明するボタンは、検索機能フィールドのすぐ下に配置されており、通常は検索機能と連携して使用します。たとえば、特定のデバイス グループに属するデバイスを検索して、何らかの管理機能を実行することができます。次のボタンを使用できますが、使用する検索タイプによっては、それぞれの管理機能を利用できない場合があります。

Add

Add ボタンを使用すると、新しいデバイスを RDU データベースに追加できます。適切な手順については、P.16-12 の「デバイス レコードの追加」を参照してください。

Delete

Delete ボタンを使用すると、選択したデバイス（複数可）を RDU データベースから削除できます。適切な手順については、P.16-13 の「デバイス レコードの削除」を参照してください。

Regenerate

Regenerate ボタンを使用すると、選択したデバイス（複数可）に対する命令の再生成を即時に実行できます。

Relate

Relate ボタンを使用すると、デバイスを特定のグループ（API ではノードと呼ばれる）に関連付けることができます。関連付けにはデバイス ID を使用します。

Unrelate

Unrelate ボタンは、選択したデバイスと、そのデバイスが現在関連付けられているグループとの関連付けを解除します。

デバイスを検索すると、次に示すヘッダーまたはリンクがページに表示され、その下に結果が返されます。

Identifier

検索基準と一致するすべてのデバイスを示します。表示される各 ID には、そのデバイスを修正できる別ページへのリンクが設定されます。

Device Type

利用可能なデバイス タイプが表示されます。この場合は、CWMP です。

Details

選択したデバイスに関する利用可能なすべての詳細情報が表示されます。詳細については、P.16-9 の「デバイスの詳細の表示」を参照してください。

Operations

利用可能なデバイス操作のドロップダウン リストが表示されます。詳細については、P.16-16 の「デバイス操作の実行」を参照してください。

デバイスの詳細の表示

検索結果で示された任意のデバイスの詳細を表示できます。

任意のデバイスの詳細を表示するには、表示するデバイスの **View Details** アイコン（）をクリックして Device Details ページを表示します。図 16-3 に、Device Details ページの例を示します。

図 16-3　Device Details ページ

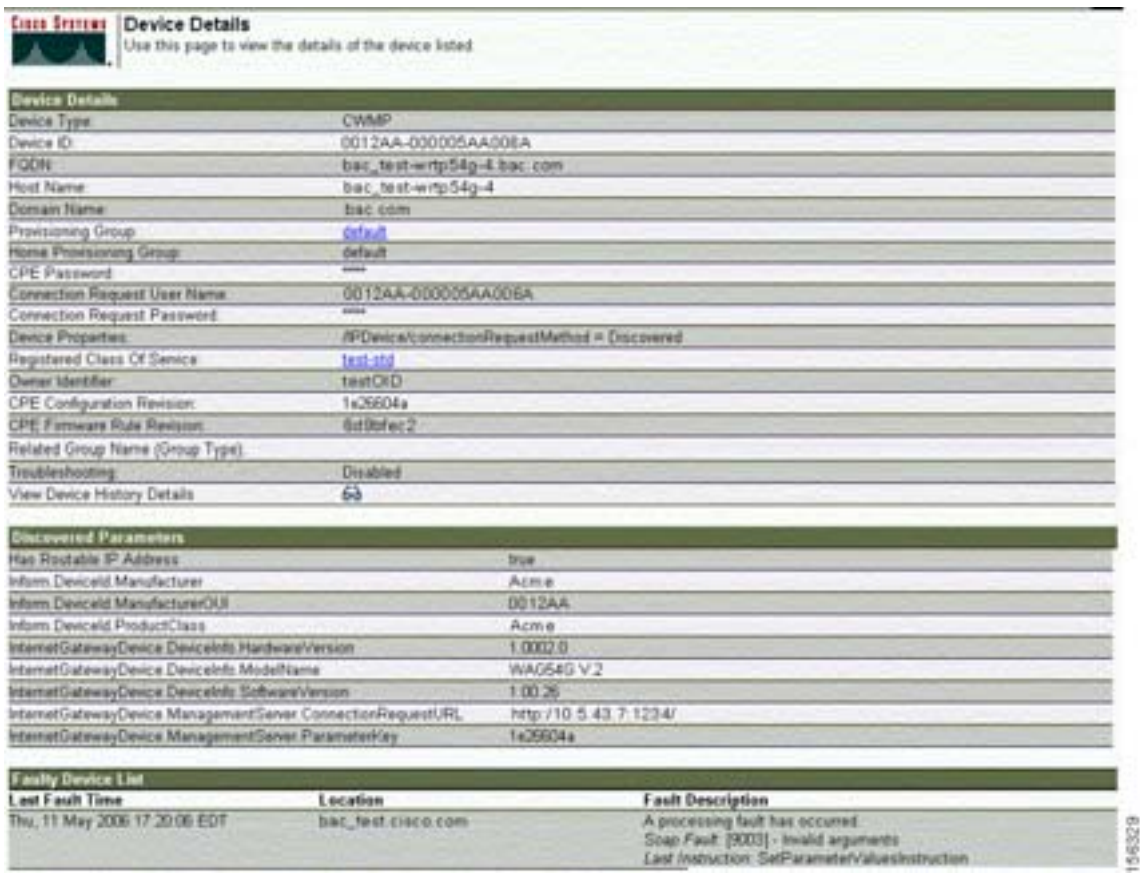


図 16-3 のフィールドを表 16-2 に示します。

表 16-2　Device Details ページ

フィールドまたはボタン	説明
Device Details	
Device Type	デバイス タイプを示します。
DeviceID	デバイス ID を示します。
FQDN	選択したデバイスの完全修飾ドメイン名を示します。たとえば、IGW-1234.ACME.COM は完全修飾ドメイン名です。
Host Name	ホストを示します。たとえば、上記の FQDN の場合、IGW-1234 がホスト名です。
Domain Name	ホストが存在するドメインを示します。たとえば、上記の FQDN の場合は ACME.COM がドメイン名です。

表 16-2　Device Details ページ （続き）

フィールドまたはボタン	説明
Provisioning Group	デバイスが事前に、または自動的に割り当てられているプロビジョニング グループを示します。
Home Provisioning Group	デバイスが属するプロビジョニング グループを示します。
CPE Password	BAC への接続を確立するときにデバイスの認証に使用されるパスワードを示します。このパスワードは、Customer Premises Equipment（CPE; 顧客宅内装置）の HTTP ベースの認証でのみ使用されます。セキュリティの目的により、パスワードが設定されている場合は、実際の値に関係なくアスタリスク（*）文字列が返されます。パスワードが設定されていない場合は、空の値が表示されます。
Connection Request User Name	BAC から CPE への接続要求の認証に使用されるユーザ名を示します。
Connection Request Password	BAC から CPE への接続要求の認証に使用されるパスワードを示します。セキュリティの目的により、このパラメータでは、実際の値に関係なく空の文字列が返されます。
Device Properties	このデバイスに設定できる、このページに表示されていないプロパティを示します。このフィールドには、カスタム プロパティの表示が含まれます。
Registered Class of Service	このデバイスに割り当てられたサービス クラスを示します。拡張により、デバイスで別のサービス クラスが選択されている場合は、Selected Class of Service という追加フィールドが表示されます。
Owner Identifier	デバイスを示します。ユーザ ID およびアカウント番号になるか、空白のままになります。
CPE Configuration Revision	設定ルールのリビジョン番号を示します。この番号は、設定の同期化が成功した後に、デバイスの *ParameterKey* で設定します。
CPE Firmware Rule Revision	この CPE のファームウェア ルールのリビジョンを示します。
Related Group Name (Group Type)	このデバイスが関連付けられているグループの名前とタイプを示します。詳細については、P.16-20 の「グループ管理」を参照してください。
Troubleshooting	CPE のトラブルシューティングがイネーブルであるか、ディセーブルであるかを示します。 **（注）** トラブルシューティングがイネーブルの場合、このページに View Troubleshooting Log リンクが表示されます。
View Device History Details	CPE の設定変更履歴へのリンクを提供します。

Discovered Parameters

（注） このセクションには、デバイスから検出されたすべてのパラメータ（存在する場合）が含まれます。検出されたパラメータがデバイスで使用可能でない場合、このセクションは表示されません。検出されたパラメータの設定方法の詳細については、P.4-5 の「CPE パラメータの検出」を参照してください。

表 16-2　Device Details ページ （続き）

フィールドまたはボタン	説明
Has Routable IP Address	デバイスが一般に到達可能であるかどうかを示します。つまり、最後の要求の発信元 IP アドレスが、Inform メッセージで CPE によって報告された WAN IP アドレスと同じかどうかを示します。
Inform.DeviceId.Manufacturer	最後の Inform メッセージで報告された CPE の製造業者を示します。
Inform.DeviceId.ManufacturerOUI	最後の Inform メッセージで報告された CPE の製造業者の固有識別子を示します。
Inform.DeviceId.ProductClass	*SerialNumber* パラメータが一意性を保持している、製造業者の製品または製品クラスを示します。デバイスは、このパラメータについて Inform メッセージで報告します。
InternetGatewayDevice.DeviceInfo.HardwareVersion	CPE のハードウェア バージョンを示します。
InternetGatewayDevice.DeviceInfo.ModelName	CPE のモデル名を示します。
InternetGatewayDevice.DeviceInfo.SoftwareVersion	CPE に現在インストールされているソフトウェア バージョンを示します。ソフトウェア バージョンは、ファームウェア バージョンとも呼ばれます。
InternetGatewayDevice.ManagementServer.ParameterKey	最後の Inform メッセージでデバイスによって報告された *ParameterKey* の値、または DPE によって最後に設定された *ParameterKey* の値のうち、新しい方の値を示します。
Faulty Device List	
（注） この情報は、デバイスで障害が発生した場合にのみ表示されます。詳細については、P.8-7 の「デバイス障害」を参照してください。	
Last Fault Time	このデバイスで、繰り返し発生する障害が発生した日時を示します。
Location	この障害が発生したサーバを示します。
Fault Description	繰り返し発生する障害の説明を示します。

デバイスの管理

Devices メニューを使用すると、RDU データベースにデバイスを追加し、プロビジョニングされたデータを更新することができます。デバイス管理には、次の作業があります。

- RDU デバイス レコードの追加、削除、および修正。
- 命令の再生成。
- 管理オブジェクト（プロビジョニング グループ、サービス クラス、グループなど）への、選択したデバイスの関連付け。
- デバイスに対する操作の実行。これらの操作は、実際にはデバイス上で実行されます。次の操作があります。
  - Reboot
  - Request Connection
  - Factory Reset
  - Display Live Data

— Ping Diagnostic
— Force Firmware Upgrade
— Force Configuration Synchronization

これらの操作の詳細については、P.16-16 の「デバイス操作の実行」を参照してください。

この項では、新しいデバイスまたは既存のデバイスに対して、各種のデバイス管理機能を実行する方法について説明します。

デバイス レコードの追加

デバイス レコードを追加するには、次の手順に従います。

ステップ 1　Manage Devices ページから **Add** をクリックします。

ステップ 2　Add Device ページが表示されます。デバイス タイプとサービス クラスを選択し、このページのその他のフィールドに入力します。

ステップ 3　この項のここまでで説明したフィールドに加えて、オプションで、既存のプロパティ名と値のペアに新しい値を追加できます。

- Property Name：カスタムまたは組み込みデバイス プロパティの名前を示します。
- Property Value：プロパティの値を示します。

プロパティを追加するには、**Add** をクリックします。

ステップ 4　**Submit** をクリックしてデバイスを追加するか、**Reset** をクリックしてすべてのフィールドをクリアします。

デバイス レコードの修正

デバイス レコードを修正するには、次の手順に従います。

ステップ 1　Manage Devices ページから、適切なデバイスに対応する Identifier リンクをクリックします。

ステップ 2　Modify Device ページが表示されます。適切なフィールドにデータを入力します。**Add** をクリックして既存の任意のプロパティ名と値のペアを修正するか、**Delete** ボタンをクリックして任意のペアを削除します。

ステップ 3　**Submit** をクリックしてこのデバイスに対する変更を保存するか、**Reset** をクリックしてすべてのフィールドをクリアします。

デバイス レコードの削除

デバイス レコードの削除は単純な手順ですが、慎重に使用する必要があります。削除を取り消すには、以前バックアップしたデータベースを復元するか、そのデバイスを再度追加する必要があります。

(注) バックアップしたデータベースの復元が必要になった場合は、P.10-8 の「データベースの復元」を参照してください。

デバイス レコードを削除するには、次の手順に従います。

ステップ 1　Manage Devices ページで、削除するデバイスを検索します。そのためには、いずれかの検索タイプを使用します。

ステップ 2　適切なデバイスの左にあるチェックボックスをオンにします。

ステップ 3　**Delete** をクリックします。

RDU データベースにストアされているデバイス レコードが削除されます。

デバイスの履歴の表示

デバイス構成の履歴を表示するには、次の手順に従います。

ステップ 1　Manage Devices ページで、履歴を表示するデバイスを検索します。そのためには、いずれかの検索タイプを使用します。

ステップ 2　そのデバイスに対応する **View Details** アイコンをクリックします。

ステップ 3　Device Details ページが表示されます。View Device History Details の **View Details** アイコンをクリックします。

Device History Details ページが表示されます。

デバイス命令の再生成

Regenerate ボタンまたは API 操作を使用すると、デバイスに対する命令の再生成を即時に実行できます。命令は、デバイスのプロビジョニング グループ内の DPE に送信されます。通常、命令を再生成するプロセスは、デバイスやサービス クラスに対する変更、または影響を及ぼすその他の変更の後に自動的にトリガーされます。ただし、サービス クラスに対する変更が行われた後は、システムがすべてのデバイスに対する命令を再生成するまで時間がかかります。このボタンを使用すると、特定のデバイスに対する命令の再生成を迅速化できます。通常、これは、予防的なトラブルシューティングで役立ちます。

デバイス命令は、次の場合に自動的に再生成されます。

- サービス クラスに関連付けられたファイル（つまりテンプレート）が更新されたとき。
- デバイス タイプのデフォルトのサービス クラスが変更されたとき。
- プロビジョニング グループ オブジェクトが管理者のユーザ インターフェイスまたは API を介して変更されたとき。
- サービス クラス オブジェクトのプロパティが変更されたとき。
- DPE が構成再生成要求を RDU に送信したとき。
- デバイスのプロパティまたは関連付けが更新されたとき。

加えられた変更がデバイス命令に影響するかどうかを BAC システムは判別できないので、一部の命令は自動的には再生成できません。そのような場合は、`generationConfiguration()` メソッドまたは管理者のユーザ インターフェイスを使用して、命令を手動で再生成する必要があります。手動で命令を再生成する必要があるのは、次の場合です。

- テクノロジー デフォルトが変更されたとき。
- システム デフォルトが変更されたとき。

（注） 命令が再生成される方法に関係なく、デバイス構成が有効になるまで命令はデバイスに伝播されません。デバイス構成が有効になるのは、デバイスがスケジュールに従って DPE に接続するか、DPE から開始された接続要求の結果として DPE に接続したときです。

デバイスの関連付けと関連付け解除

任意の数の任意のグループを定義できます。関連付け機能を使用すると、デバイスを特定のグループに関連付けることができ、さらにはグループを特定のグループ タイプに関連付けることができます。

グループへのデバイスの関連付け

（注） 管理者のユーザ インターフェイスを使用する場合、デバイスは、1 つずつしかグループに関連付けられません。

デバイスをグループに関連付けるには、次の手順に従います。

ステップ 1　Manage Devices ページで、グループに関連付けるデバイスを検索します。そのためには、いずれかの検索タイプを使用します。

ステップ 2　デバイス ID に対応するチェックボックスをオンにし、**Relate** ボタンをクリックします。

ステップ 3　Relate Device to Group(s) ページが表示されます。ドロップダウン リストから Group Type を選択し、定義済みグループのリストからグループを選択します。

（注） Group リストから複数のグループを選択するには、**Control** キーまたは **Shift** キーを押します。

ステップ 4　**Submit** をクリックします。

Manage Devices ページが表示されます。

（注）　デバイスがグループに追加されたことを確認するには、そのデバイスに対応する **View Details** アイコンをクリックします。表示された Device Details ページで、Related Group Name (Group Type) の状態を確認します。

グループからのデバイスの関連付け解除

（注）　管理者のユーザ インターフェイスを使用する場合、デバイスは、1 つずつしかグループに関連付けられません。

デバイスをグループから関連付け解除するには、次の手順に従います。

ステップ 1　Manage Devices ページで、グループから関連付け解除するデバイスを検索します。

ステップ 2　デバイス ID に対応するチェックボックスをオンにし、**Unrelate** ボタンをクリックします。

ステップ 3　Unrelate Device from Group ページが表示されます。定義済みグループのリストから、デバイスを関連付け解除するグループを選択します。

（注）　Group リストから複数のグループを選択するには、**Control** キーまたは **Shift** キーを押します。

ステップ 4　**Submit** をクリックします。

Manage Devices ページが表示されます。

グループ内のデバイスの検索

特定のグループに属するデバイスを検索するには、次の手順に従います。

ステップ 1　Manage Devices ページで、Search Type の下のドロップダウン リストから Group Search オプションを選択します。

ステップ 2　Group Name (Group Type) オプションと Device Identifier オプションが表示されます。Group Name (Group Type) ドロップダウン リストから、検索するデバイスのグループ名を選択します。

ステップ 3　Device Identifier フィールドにデバイス ID を入力するか、ワイルドカード（*）を使用します。

ステップ 4　**Search** をクリックします。

グループに関連付けられているデバイスが表示されます。

デバイス操作の実行

Device Operations ページでは、次の機能を実行できます。

- Reboot：デバイスをリブートします。この操作は、主に診断の目的で使用されます。
- Request Connection：BAC との CWMP セッションを確立するようにデバイスに指示します。
- Factory Reset：デバイスの登録済みの設定を工場出荷時の設定にリセットします。
- Display Live Data：デバイス パラメータの現在の値を表示します。

  このデバイス操作で表示するパラメータを選択するには、Parameter List File ドロップダウン ボックスからオプションを選択します。各パラメータ リストは XML ファイルで、各ファイルが返すパラメータの詳細が示されています。パラメータを表示するには、**View Details** アイコンをクリックします。

  取得するパラメータを、パラメータ リストで定義することもできます。BAC には、ライブ データ テンプレートのサンプル リストが用意されています。これらのテンプレートでは、ライブ データを表示するためのクエリーで読み取る各種パラメータを指定します。
- Ping Diagnostic：デバイスから任意のホストへの IP PING 診断を実行できます。

（注）　上記のすべての操作では、デバイスが到達可能でない場合、エラー メッセージが表示されます。

- Force Firmware Upgrade：ファームウェア ルールで設定されている MaintenanceWindow の制限にかかわらず、次回接続時にデバイスがファームウェアのアップデートを実行するよう強制します。
- Force Configuration Synchronization：デバイス上の現在の構成バージョンに関係なく、個々のデバイスが設定を同期するよう強制します。

（注）　ファームウェアのアップグレードまたは設定の同期を強制する操作は、デバイスが Autoconfiguration Server（ACS; 自動構成サーバ）に次回接続したときに有効になります。

リブートの実行

デバイスをリブートするには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、適切なデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコン（）をクリックします。

ステップ 3　Device Operations ページが表示されます。Device Operation の下のドロップダウン リストから Reboot を選択します。

ステップ 4　**Submit** をクリックします。

接続要求の実行

接続要求を開始するようデバイスに強制するには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、適切なデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコンをクリックします。

ステップ 3　Device Operations ページが表示されます。Device Operation の下のドロップダウン リストから Request Connection を選択します。

ステップ 4　**Submit** をクリックします。

工場出荷時設定へのリセットの実行

デバイスの設定を工場出荷時の設定にリセットするには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、適切なデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコンをクリックします。

ステップ 3　Device Operations ページが表示されます。Device Operation の下のドロップダウン リストから Factory Reset を選択します。

ステップ 4　**Submit** をクリックします。

ライブ データの表示

デバイスのパラメータを表示するには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、適切なデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコンをクリックします。

ステップ 3　Device Operations ページが表示されます。Device Operation の下のドロップダウン リストから Display Live Data を選択します。

ステップ 4　Device Operations ページが表示されます。この操作がタイムアウトになるまでの時間の長さを秒単位で入力します。デフォルトのタイムアウトは 90 秒です。

ステップ 5　Parameter List File ドロップダウン リストからファイルを選択します。それぞれのファイルは、返されるパラメータの詳細が記述された XML ファイルです。**View Details** アイコンをクリックして、パラメータを表示します。

（注）　これらのサンプル テンプレートは、**Configuration** > **Files** タブでも表示できます。View Files ページで、File Type ドロップダウン リストの下の Parameter List オプションを選択します。**Search** をクリックします。サンプル パラメータ リスト ファイルのリストが表示されます。

ステップ 6　**Submit** をクリックします。

（注）　デバイスが到達可能でない場合は、エラー メッセージが表示されます。

PING 診断の実行

デバイスの IP アドレスを使用してデバイスに対する PING 操作を実行するには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、適切なデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコンをクリックします。

ステップ 3　Device Operations ページが表示されます。Device Operation の下のドロップダウン リストから Ping Diagnostic を選択します。

ステップ 4　Device Operations ページが表示されます。次のフィールドに値を入力します。

- Device operation timeout (in seconds)：PING 操作がタイムアウトになるまでの時間の長さを指定します。
- Name of the hostname to be pinged：PING を実行する CPE のホスト名を指定します。
- Interface：CPE 上で PING を実行するときに使用する WAN インターフェイスを指定します。
- Number of repetitions：PING 操作を実行する回数を指定します。
- Time out：PING パケットのタイムアウトを指定します。
- Data block size：各 PING パケットのサイズを指定します。
- DSCP：各 PING パケットの DSCP 値を指定します。

ステップ 5　**Submit** をクリックします。

ファームウェア アップグレードの強制実行

次回接続時にデバイスがファームウェアのアップロードを実行するように強制し、ファームウェアルールに設定された MaintenanceWindow の制限を回避するには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、設定を同期するデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコンをクリックします。

ステップ 3　Device Operations ページが表示されます。Perform Device Operation の下のドロップダウン リストから Force Firmware Upgrade を選択します。

ステップ 4　**Submit** をクリックします。

設定同期化の強制実行

デバイス上の現在の構成バージョンに関係なく、デバイスが DPE と次回接続するときにデバイス設定の同期を実行するように強制するには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、設定を同期するデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコンをクリックします。

ステップ 3　Device Operations ページが表示されます。Perform Device Operation の下のドロップダウン リストから Force Configuration Synchronization を選択します。

ステップ 4　**Submit** をクリックします。

デバイスの設定が DPE と同期されます。

デバイス操作のタイムアウトの設定

デバイス操作が実行されるまでの制限時間の長さを設定できます。その時間が経過すると、操作はタイムアウトになります。

（注）　この項で説明されている手順に加えて、デフォルトのタイムアウトまでの時間は、**Configuration** > **Defaults** > **CWMP Defaults** を選択して Device Operation Timeout フィールドを表示させて設定することもできます。

デバイス操作のタイムアウト値を設定するには、次の手順に従います。

ステップ 1　**Devices** > **Manage Devices** ページで、適切なデバイスを検索します。

ステップ 2　そのデバイスに対応する **Operations** アイコンをクリックします。

ステップ 3　Device Operations ページが表示されます。Device Operation の下のドロップダウン リストから、実行する操作を選択します。

ステップ 4　Device Operation Timeout フィールドに値を秒単位で入力します。デバイス操作のタイムアウトのデフォルト値は 90 秒です。

ステップ 5　**Submit** をクリックします。

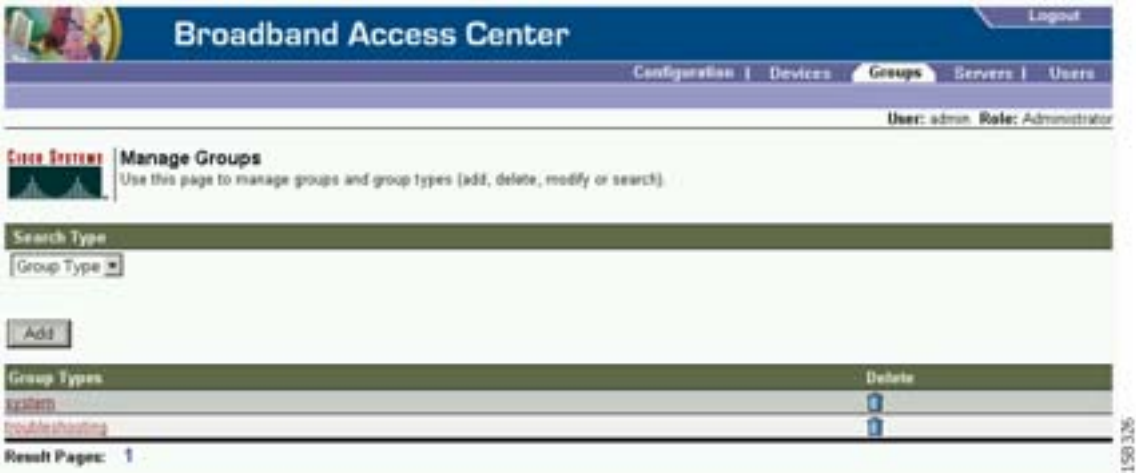
グループ管理

グループの管理では、グループとグループ タイプの作成、修正、削除を実行できます。

グループ タイプの管理

Main Menu またはプライマリ メニュー バーから Groups を選択して、Manage Groups ページ（図 16-4）にアクセスします。このページを表示すると、デフォルト設定では Group Type が選択されています。

図 16-4　Manage Groups ページ



グループ タイプの追加

新しいグループ タイプを追加するには、次の手順に従います。

ステップ 1　**Groups** タブをクリックします。

ステップ 2　Manage Groups ページが表示されます。**Add** をクリックします。

ステップ 3　Add Group Type ページが表示されます。新しいグループ タイプの名前を入力します。

ステップ 4　カスタム プロパティが定義されている場合は、Property Name and Property Name セクションが表示されます。オプションで、ドロップダウン リストから Property Name を選択し、必要な Property Value を入力します。プロパティはいくつでも必要なだけ追加することができます。

ステップ 5　**Add** をクリックします。

ステップ 6　選択後、**Submit** をクリックします。

新しいグループ タイプが RDU に記録され、Manage Group Types ページに新しいグループ タイプが表示されます。

グループ タイプの修正

グループ タイプのプロパティを修正するには、次の手順に従います。

ステップ 1　**Groups** タブをクリックします。

ステップ 2　Manage Groups ページが表示されます。適切なグループ タイプを見つけてクリックします。

ステップ 3　Modify Group Type ページが表示されます。Property Name と Property Value のペアに対して必要な修正を行います。特定のペアを削除する必要がある場合は、適切なペアの隣にある **Delete** をクリックします。

ステップ 4　**Submit** をクリックします。

情報が適切に修正された状態で Manage Groups ページが表示されます。

グループ タイプの削除

グループ タイプを削除するには、次の手順に従います。

ステップ 1　**Groups** タブをクリックします。

ステップ 2　Manage Groups ページが表示されます。適切なグループ タイプを見つけて、そのグループ タイプに対応する **Delete** アイコン（🗑）をクリックします。

ステップ 3　Delete Group Type ダイアログボックスで、**OK** をクリックして選択したグループ タイプを削除します。または、**Cancel** をクリックして前のページに戻ります。

削除したグループ タイプが消えた状態で Manage Groups ページが表示されます。

グループの管理

グループを作成および修正し、不要なグループを削除できます。

新規グループの追加

新規グループを追加するには、次の手順に従います。

ステップ 1　Manage Groups ページのドロップダウン リストから Group を選択します。**Add** をクリックします。

ステップ 2　Add Group ページが表示されます。新規グループの名前を入力して、このノードに使用する適切な Group Type を選択します。

ステップ 3　**Submit** をクリックします。

ステップ 4　新規グループが追加された状態で Manage Groups ページが表示されます。

カスタム プロパティを定義してある場合は、Property Name and Property Value セクションが表示されます。オプションで、ドロップダウン リストから適切な Property Name を選択し、必要な Property Value を入力します。

ステップ 5　**Add** をクリックして、該当する Property Name と Property Value のペアの数を増やします。

ステップ 6　**Submit** をクリックします。

新規グループが RDU に記録され、Manage Groups ページに新規グループが表示されます。

グループの修正

グループ プロパティを修正するには、次の手順に従います。

ステップ 1　適切なグループを見つけてクリックします。

ステップ 2　Modify Group ページが表示されます。Property Name と Property Value のペアに対して必要な修正を行います。特定のペアを削除する必要がある場合は、適切なペアの隣にある **Delete** をクリックします。

ステップ 3　**Submit** をクリックします。

情報が適切に修正された状態で Manage Group ページが表示されます。

グループの削除

Manage Groups ページに表示されるグループを削除するには、そのグループに対応するチェックボックスをオンにして、**Delete** ボタンをクリックします。

グループ対グループの関連付けと関連付け解除

関連付け機能と関連付け解除機能は、グループ オブジェクト間の関連性を確立するために使用します。この関連性を確立または解除するには、次の手順に従います。

ステップ 1　選択したグループについて、目的に応じて **Relate** または **Unrelate** をクリックします。Relate Group ページまたは Unrelate Group ページが表示されます。

ステップ 2　適切な Group Type をドロップダウン リストから選択し、ノードの関連付けまたは関連付け解除の対象となるグループを選択します。

ステップ 3　**Submit** をクリックします。

Manage Groups ページが表示されます。

グループの詳細の表示

グループの詳細を表示するには、次の手順に従います。

ステップ 1　Manage Groups ページで、Search Type ドロップダウン リストから Group オプションを選択します。

ステップ 2　適切なグループ タイプを選択し、適切なフィールドにグループまたはグループ ワイルドカードを入力します。

ステップ 3　**Search** をクリックします。

ステップ 4　詳細を表示するグループに対応するリンクをクリックします。

Modify Group ページが表示され、グループ名とグループ タイプの詳細が示されます。

サーバの表示

この項では、BAC サーバ ページについて説明します。

- Device Provisioning Engine の表示（P.16-24）
- プロビジョニング グループの表示（P.16-26）
- Regional Distribution Unit の詳細の表示（P.16-28）

Device Provisioning Engine の表示

Manage Device Provisioning Engines ページで、現在 BAC データベースに登録されているすべての DPE のリストを監視できます。このページに表示される各 DPE 名は、その DPE の詳細を表示する別ページへのリンクになっています。詳細ページ（例：図 16-5）を表示するには、このリンクをクリックします。

（注）　RDU は、DPE が RDU に接続するときに使用する DPE インターフェイスで DNS 逆ルックアップを実行することで、DPE の名前を判別します。

図 16-5　View Device Provisioning Engines Details ページ

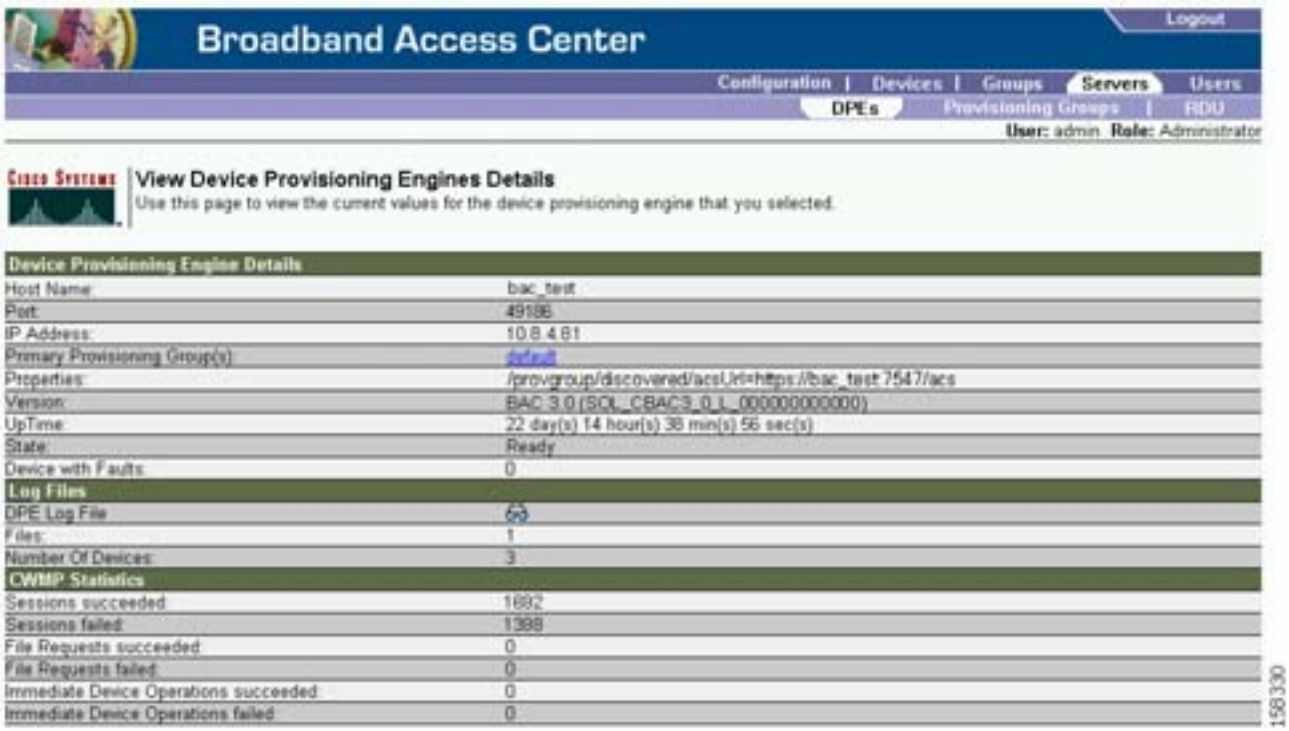


図 16-5 のフィールドとボタンを表 16-3 に示します。

表 16-3　View Device Provisioning Engines Details ページ

フィールドまたはボタン	説明
Device Provisioning Engine Details	
Host Name	DPE ホスト名を示します。
Port	DPE が RDU への接続を確立するときに使用した DPE ポート番号を示します。
IP Address	DPE の IP アドレスを示します。
Primary Provisioning Group(s)	選択した DPE が属するプライマリ プロビジョニング グループを示します。これはアクティブ リンクで、クリックすると、そのプロビジョニング グループの Provisioning Group Details ページが表示されます。
Properties	この DPE に設定されているプロパティを示します。
Version	現在使用中の DPE ソフトウェアのバージョンを示します。
UpTime	DPE が最後に起動してから、動作が継続している合計時間を示します。
State	DPE が動作可能かどうかを示します。示される状態には、次のものがあります。 • Registering • Initializing • Synchronizing • Populating • Ready • Offline 各状態の詳細については、P.2-5 の「DPE と RDU 間の同期」を参照してください。 **(注)** このフィールドに Offline と示されている場合、Uptime フィールド以降のオプションは表示されません。Offline 以外の状態にある DPE は、クライアント要求を処理する準備が整っています。
Device with Faults	この DPE で障害のあるデバイスの数が表示されます。この数がゼロより大きい場合、View Details アイコンが表示されます。このアイコンをクリックすると、障害のあるデバイスの詳細が表示されます。
Log Files	
DPE Log File	View Details アイコンが表示されます。このアイコンをクリックすると、View Log File Contents ページが表示され、*dpe.log* の詳細を確認できます。
Files	DPE でキャッシュされているファイル（ファームウェア イメージなど）の数を示します。
Number of Devices	DPE が命令を保持している対象の CWMP デバイスの数を示します。完全に同期されている DPE の場合、この数は DPE のプロビジョニング グループ内の CWMP デバイスの数に等しくなります。

表 16-3　View Device Provisioning Engines Details ページ（続き）

フィールドまたはボタン	説明
CWMP Statistics	
（注）　このセクションには、DPE が最後に起動されてからの統計情報が表示されます。	
Sessions succeeded	成功した CWMP セッションの数を示します。
Sessions failed	失敗した CWMP セッションの数を示します。
File Requests Succeeded	成功したファームウェア ファイル ダウンロード要求の数を示します。
File Requests Failed	失敗したファームウェア ファイル ダウンロード要求の数を示します。
Immediate Device Operations Succeeded	成功した即時デバイス操作の数を示します。
Immediate Device Operations failed	失敗した即時デバイス操作の数を示します。

プロビジョニング グループの表示

Manage Provisioning Groups ページを使用して、現在のプロビジョニング グループをすべて監視できます。このリストに表示される各プロビジョニング グループは、そのグループの詳細ページへのリンクになっています。詳細ページ（例：図 16-6）を表示するには、このリンクをクリックします。

図 16-6　View Provisioning Group Details ページ

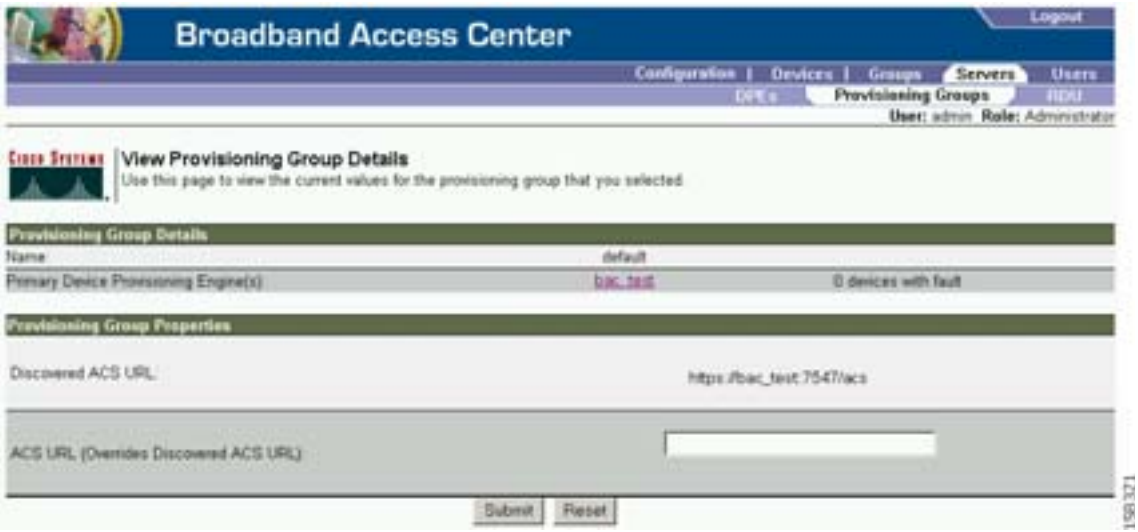


図 16-6 のフィールドとボタンを表 16-4 に示します。表 16-4 で説明するフィールドには、アクティブ リンクが含まれていることがあります。クリックすると、対応する詳細ページが表示されます。

表 16-4　View Provisioning Group Details ページ

フィールドまたはボタン	説明
Provisioning Group Details	
Name	List Provisioning Groups ページで選択したプロビジョニング グループ名を示します。
Primary Device Provisioning Engine(s)	このプロビジョニング グループのプライマリ DPE のホスト名を示します。
Provisioning Group Properties	
Discovered ACS URL	プロビジョニング グループが DPE に接続するときに使用する DPE URL を示します。検出された URL は、DPE CLI を使用したプロビジョニング操作用に設定された DPE インターフェイスに基づいています。パラメータは、最後に RDU に登録された DPE からの登録情報に基づいています。この URL は、別のプロビジョニング グループへの CPE のリダイレクトなどの操作で使用されます。
ACS URL (Overrides Discovered ACS URL)	各プロビジョニング グループに関連付けられている BAC サーバの設定済み URL を示します。この URL は、特定のプロビジョニング グループ内の DPE にデバイスが接続するために使用されます。また、別のプロビジョニング グループへの CPE のリダイレクトなどの操作でも使用されます。
Submit	行った変更を有効化または実装します。
Reset	すべての設定を元の設定に戻します。

Regional Distribution Unit の詳細の表示

Servers メニューの RDU オプションを使用すると、RDU の詳細が表示されます。RDU 詳細ページの例を図 16-7 に示します。

図 16-7　View Regional Distribution Unit Details ページ

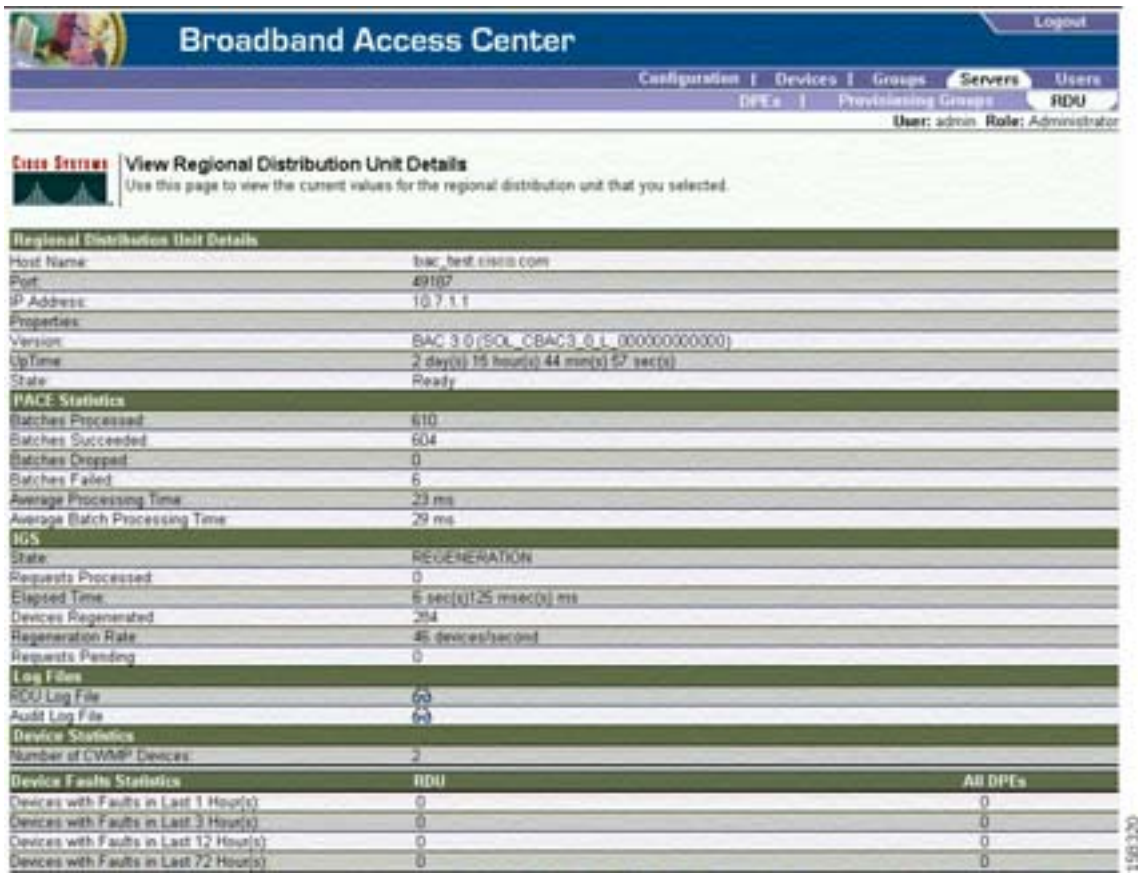


図 16-7 のフィールドとボタンを表 16-5 に示します。

表 16-5　View Regional Distribution Unit Details ページ

フィールドまたはボタン	説明
Regional Distribution Unit Details	
Host Name	Regional Distribution Unit を実行しているシステムのホスト名を示します。
Port	DPE からの接続に使用する RDU リスニング ポート番号を示します。デフォルトのポート番号は 49187 ですが、RDU のインストール時に別のポートを選択できます。
IP Address	RDU に割り当てられている IP アドレスを示します。
Properties	RDU で設定されているプロパティを示します。
Version	現在使用中の RDU ソフトウェアのバージョンを示します。
UpTime	RDU が最後にダウンしてから、動作可能状態が継続している合計時間を示します。

表 16-5　View Regional Distribution Unit Details ページ（続き）

フィールドまたはボタン	説明
State	RDU が要求に応答するかどうかを示します。管理者のユーザ インターフェイスで表示される唯一の状態は Ready です。
PACE Statistics	
Batches Processed	RDU が最後に起動してから処理された、個々のバッチの数を示します。
Batches Succeeded	RDU が最後に起動してから正常に処理された、個々のバッチの数を示します。
Batches Dropped	RDU が最後に起動してから破棄されたバッチの数を示します。
Batches Failed	RDU が最後に起動してから処理が失敗したバッチの数を示します。
Average Processing Time	RDU がビジーでキューに留まっていた時間を除いて、バッチの処理にかかった平均時間をミリ秒単位で示します。
Average Batch Processing Time	RDU がビジーでキューに留まっていた時間を含めて、バッチの処理にかかった平均時間をミリ秒単位で示します。
IGS 命令生成サービスについての情報を示します。	
State	命令生成サービスの動作状態を示します。次の状態があります。 • Idle：IGS が要求の再生成を処理しないことを示します。 • Regeneration：IGS が要求の再生成を処理することを示します。 • Waiting Regeneration：IGS がデバイスに対する命令を再生成できないことを示します。IGS がこの状態から先に進まない場合は、*rdu.log* で詳細を確認してください。
Requests Processed	RDU が最後に起動してから処理された命令生成要求の数を示します。
Elapsed Time	再生成の開始から経過した時間を秒単位で示します。
Devices Regenerated	再生成プロセスが開始されてから再生成されたデバイス命令の数を示します。
Regeneration rate	再生成プロセスが開始されてから再生成されたデバイス命令の累積比率を示します。
Requests pending	キューに入っている再生成要求の数を示します。
Log Files	
RDU Log File	View Details アイコンが表示されます。このアイコンをクリックすると、View Log File Contents ページが表示され、*rdu.log* ファイルの詳細を確認できます。
Audit Log File	View Details アイコンが表示されます。このアイコンをクリックすると、View Log File Contents ページが表示され、*audit.log* ファイルの詳細を確認できます。
Device Statistics	
Number of CWMP Devices	RDU データベース内のデバイスの数を示します。

表 16-5　View Regional Distribution Unit Details ページ（続き）

フィールドまたはボタン	説明
Device Faults Statistics	
Devices with Faults in Last 1 Hour(s)	過去 1 時間以内に RDU と DPE の両方で障害のあったデバイスの数を示します。
Devices with Faults in Last 3 Hour(s)	過去 3 時間以内に RDU と DPE の両方で障害のあったデバイスの数を示します。
Devices with Faults in Last 12 Hour(s)	過去 12 時間以内に RDU と DPE の両方で障害のあったデバイスの数を示します。
Devices with Faults in Last 72 Hour(s)	過去 72 時間以内に RDU と DPE の両方で障害のあったデバイスの数を示します。

Broadband Access Center の設定

この章では、Configuration メニューでオプションを選択して行う、Broadband Access Center（BAC）の設定作業について説明します。この作業は次のとおりです。

サービス クラスの設定

BAC 管理者のユーザ インターフェイスを使用すると、お客様に提供するサービス クラスを設定できます。管理者のユーザ インターフェイスを使用して、選択したサービス クラスを追加、修正、表示、または削除できます。図 17-1 に示されるような Manage Class of Service ページで作業を開始します。

図 17-1　Manage Class of Service ページ

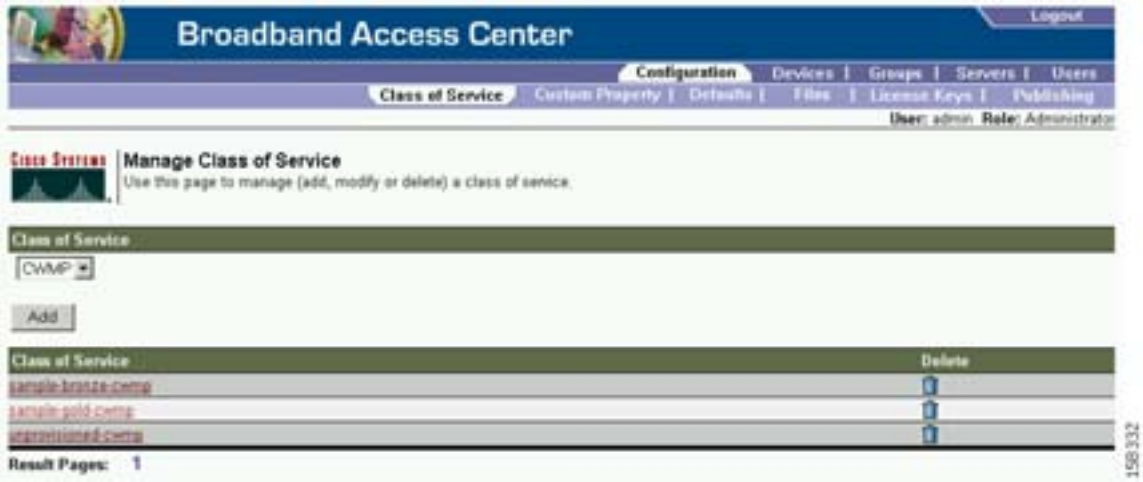


図 17-1 のフィールドとボタンを表 17-1 に示します。

表 17-1　Manage Class of Service ページ

フィールドまたはボタン	説明
Class of Service	
Class of Service	検索できるテクノロジー サービス クラスを示すドロップダウン リストです。画面に表示される選択肢には次のものがあります。 • CWMP **(注)** これらのテクノロジー分野の詳細については、P.17-8 の「デフォルトの設定」を参照してください。
Add	新しいサービス クラスを追加します。
Class of Service	
Class of Service リスト	サービス クラス オブジェクトの名前が表示されます。
Delete	選択されたサービス クラスを削除します。

表 17-2 に、Add Class of Service ページに表示されるフィールドとボタンを示します。

表 17-2　Add Class of Service ページ

フィールドまたはボタン	説明
Class of Service Name and Type	
Class of Service Name	新しいサービス クラスの名前を入力します。
Class of Service Type	選択できるサービス クラスのタイプが表示されるドロップダウン リストです。
Configuration Template File	サービス クラスと関連付ける設定テンプレート ファイルを選択するドロップダウン リストです。
Firmware Rule File	サービス クラスと関連付けるファームウェア ルール ファイルを選択するドロップダウン リストです。
Property Name/Value	
Property Name	適切なプロパティを指定します。ドロップダウン リストから適切なプロパティを選択できます。
Property Value	プロパティ名に対する値を指定します。ドロップダウン リストから適切な値を選択できます。
Add	Property Name と Property Value の新しいペアを追加して、新しいサービス クラスを作成します。
Submit	行った変更を有効化または実装します。
Reset	すべての設定を元の設定に戻します。

サービス クラスの追加

特定のサービス クラスを追加するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Class of Service** を選択します。

ステップ 3　**Add** をクリックします。

ステップ 4　Add Class of Service ページが表示されます。このページでは、選択したサービス クラスの各種の設定を指定します。新しいサービス クラスの名前を入力します。

たとえば、Gold-Classic という名前の CWMP 用の新しいサービス クラスを作成するとします。その場合、Class of Service Name に **provisioned-cwmp** を入力し、サービス タイプ ドロップダウン リストから CWMP を選択します。

ステップ 5　設定テンプレート ファイルを選択します。たとえば、*sample-cwmp-config.xml* を設定テンプレート ファイルのドロップダウン リストから選択します。

ステップ 6　ファームウェア ルール ファイルも選択します。たとえば、*sample-cwmp-firmware-rules.xml* をファームウェア ルール ファイルのドロップダウン リストから選択します。

ステップ 7　Property Name フィールドと Property Value フィールドに、それぞれプロパティ名とプロパティ値を入力します。この操作により、このサービス クラス オブジェクトの標準またはカスタムのプロパティを設定できます。

たとえば、プロパティ名として /IPDevice/connectionRequestMethod を選択します。Property Value ドロップダウン リストから Discovered を選択してから、この手順の残りを続行します。

（注） /IPDevice/connectionRequestMethod の API 定数は、`IPDeviceKeys.CONNECTION_REQUEST_METHOD` です。

このページには、プロパティ名とプロパティ値のペアが複数表示される場合があります。サービス クラスから不要なペアを削除するには、**Delete** ボタンを使用します。

ステップ 8　**Add** をクリックして、定義するサービス クラスにそのプロパティを追加します。

ステップ 9　**Submit** をクリックして、この手順を完了させるか、または、**Reset** をクリックして、すべてのフィールドを元の設定に戻します。

サービス クラスを確定すると、Manage Class of Service ページが表示され、新規に追加されたサービス クラスが示されます。

サービス クラスの修正

サービス クラスを修正するには、種々のプロパティを選択し、適切なプロパティ値を割り当てます。サービス クラスを初めて作成する場合は、適切なプロパティをすべて選択し、値を割り当てます。入力内容に誤りがあった場合や、特定のサービス クラスを修正することが必要になった場合は、以前の修正を確定する前にプロパティ値を修正するか、または Property Name と Property Value のペアをまとめて削除します。

（注） サービス クラス オブジェクトに変更を加えると、影響を受けるすべてのデバイスに対する命令が Instruction Generation Service（IGS）によって再生成され、DPE に送信されます。IGS では、このタスクはバックグラウンド ジョブとして実行されます。IGS の状態は、View RDU Details ページから確認できます。

サービス クラスのプロパティを追加、削除、または修正するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Class of Service** を選択します。

ステップ 3　修正するサービス クラスを選択します。

ステップ 4　適切なサービス クラスに対応するリンクをクリックします。Modify Class of Service ページが表示されます。ページの説明の下に、選択したサービス クラスの名前およびタイプが表示されます。

- 選択したサービス クラスに新しいプロパティを追加するには、次の手順に従います。
  - Property Name ドロップダウンから、選択したサービス クラスに割り当てる最初のプロパティを選択し、そのプロパティの適切な値を選択してから、**Add** をクリックします。

- 選択したサービス クラスに割り当てる他のすべてのプロパティについて、この手順を繰り返します。

- 選択したサービス クラスのプロパティを削除するには、次の手順に従います。
  - Property Name ドロップダウンのすぐ上にあるリストで、不要なプロパティを見つけます。
  - **Delete** ボタンをクリックします。
- プロパティに現在割り当てられている値を修正するには、次の手順に従います。
  - 上記と同じ方法で、該当するプロパティを削除します。
  - 同じプロパティをサービス クラスに再度追加し、Property Value に新しい値を入力します。

（注） 業務に必須のプロパティを削除した場合は、変更を確定する前に、そのプロパティを再度追加し、適切な値を選択する必要があります。

ステップ 5　**Submit** をクリックして、サービス クラスに対する修正を実行します。**Submit** をクリックすると、サービス クラスに追加された各プロパティが表示されます。次に、選択したサービス クラスでデバイスに対する命令を再生成するための確認ページが表示されます。

ステップ 6　**OK** をクリックします。

Manage Class of Service ページで、修正したサービス クラスが使用可能になります。

サービス クラスの削除

既存のサービス クラスはすべて削除できます。ただし、削除する前に、そのサービス クラスに関連付けられたデバイスが存在しないことを確認する必要があります。

ヒント 削除するサービス クラスに関連付けられたデバイスが多数存在する場合は、BAC アプリケーション プログラミング インターフェイス（API）を使用して、これらすべてのデバイスに別のサービス クラスを再割り当てするプログラムを記述します。

サービス クラスを削除するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Class of Service** を選択します。

ステップ 3　適切なサービス クラスの **Delete** アイコン（🗑）をクリックすると、確認ダイアログボックスが表示されます。

（注） サービス クラスにデバイスが関連付けられている場合、または、デフォルトのサービス クラスとして指定されている場合、そのサービス クラスは削除できません。したがって、**unprovisioned-cwmp** サービス クラス オブジェクトは削除できません。

ステップ 4　**OK** をクリックしてファイルを削除するか、または、**Cancel** をクリックして Manage Class of Service ページに戻ります（図 17-1 を参照してください）。

デバイスが関連付けられているサービス クラスを削除しようとすると、次のエラー メッセージが表示されます。

```
The following error(s) occurred while processing your request.
Error: Class Of Service [sample-COS] has devices associated with it, unable to delete

Please correct the error(s) and resubmit your request.
```

エラー メッセージでは、特定のサービス クラスが指定されます。この例では、*sample-COS* と指定されています。

カスタム プロパティの設定

カスタム プロパティを使用すると、RDU データベースに保存される追加のカスタマイズ可能なデバイス情報を指定できます。Custom Property 設定ページが Configuration メニューの下にあります。このページを使用して、カスタム プロパティを追加または削除します。

注意　カスタム プロパティは使用中でも削除できますが、削除すると、そのプロパティを使用している他の領域に深刻な障害が起こる原因になります。

カスタム プロパティを定義すると、プロパティ階層で使用できるようになります。プロパティ階層の使用方法については、P.5-14 の「設定テンプレートのオーサリング」を参照してください。プロパティ階層で使用するためのプロパティは、次のオブジェクトで設定できます。

- Device
- Provisioning Group
- Class of Service
- Device Type
- システム デフォルト

また、プロパティは Group オブジェクトおよび Group Type オブジェクトでも設定できますが、それらのプロパティはプロパティ階層に含まれません。

カスタム プロパティを設定するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Custom Property** を選択します。Manage BAC Custom Properties ページが表示されます。

- カスタム プロパティを追加するには、次の手順に従います。
  - Manage BAC Custom Properties ページで **Add** をクリックします。Add Custom Property ページが表示されます。
  - 新しいカスタム プロパティの名前を入力します。
  - ドロップダウン リストからカスタム プロパティ値のタイプを選択します。
  - 選択後、**Submit** をクリックします。プロパティが管理データベースに追加されると、Manage BAC Custom Properties ページが表示されます。
- カスタム プロパティを削除するには、次の手順に従います。
  - Manage BAC Custom Properties ページから削除するカスタム プロパティを指定します。
  - 適切なカスタム プロパティに対応する **Delete** アイコンをクリックします。カスタム プロパティ削除ダイアログボックスが表示されます。
  - **OK** をクリックして、そのカスタム プロパティを削除します。

デフォルトの設定

Configuration オプションから選択した Defaults ページを使用すると、Regional Distribution Unit（RDU）および CWMP テクノロジーを含む、システム全体のデフォルト設定にアクセスできます。

設定オプションの選択

特定のデフォルト タイプを設定する手順は、すべて共通です。この手順に従って目的のデフォルト ページを表示してから、この章の該当する項で、ページの各部分の説明を参照してください。

ステップ 1　プライマリ ナビゲーション バーまたは Main Menu ページで、**Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Defaults** を選択します。

ステップ 3　Configure Defaults ページが表示されます。画面の左側にあるリストから、適切なデフォルト タイプを選択します。

対応するデフォルト ページが表示されます。

CWMP のデフォルト

CWMP Defaults ページ（図 17-2）には、CWMP テクノロジーの設定内容のリストが表示されます。

図 17-2　CWMP Defaults の Configure Defaults ページ

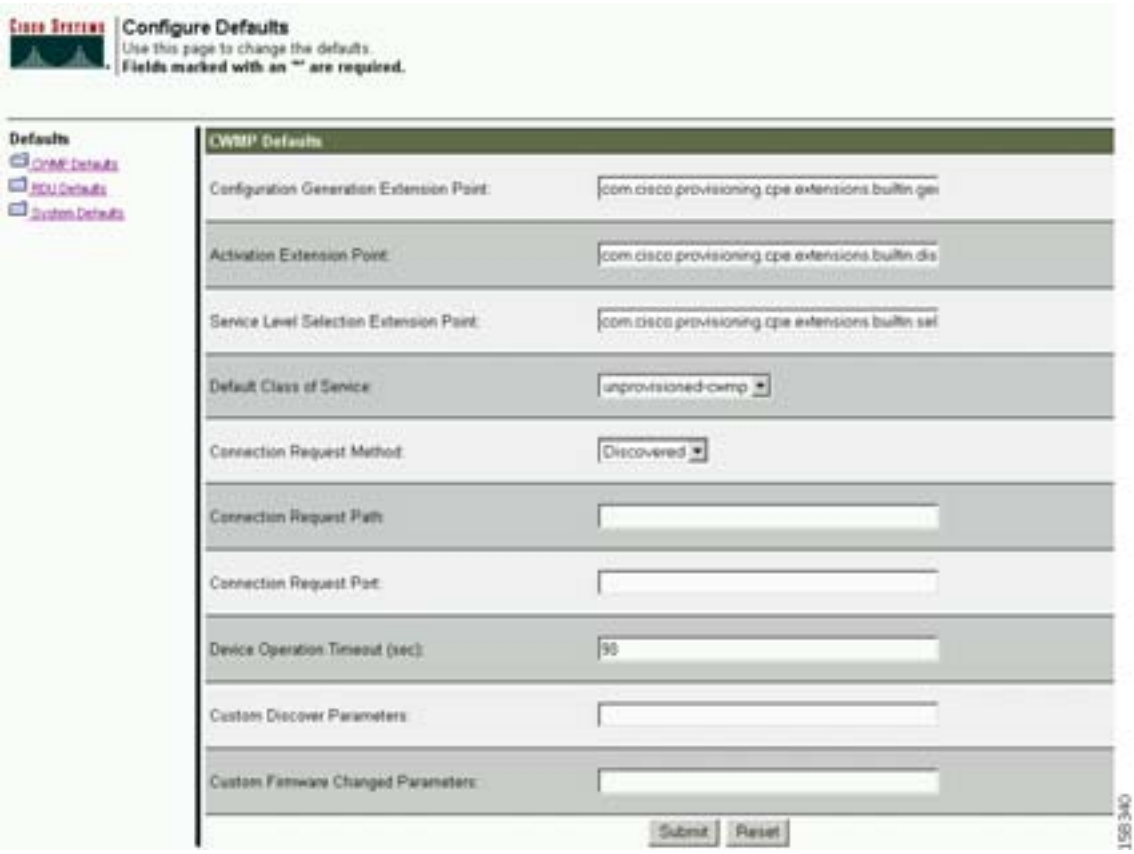


図 17-2 にあるすべてのフィールドとボタンを表 17-3 に示します。

表 17-3　CWMP Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Configuration Generation Extension Point	他のテクノロジー拡張ポイントが実行される前に実行する共通拡張ポイントを指定します。
Activation Extension Point	デバイスを有効にする拡張ポイントを指定します。
Service Level Extension Point	設定の生成に使用するサービス クラスを特定し、その情報を RDU に返す拡張ポイントを示します。
Default Class of Service	デフォルトのサービス クラスに変更を加えると、デフォルトのサービス クラスに関連付けられたすべてのデバイスに関する命令が再生成されます。Instruction Generation Service（IGS）は、命令の自動再生成を実行し、それらの命令を適切な DPE に配信します。このページにそれ以外の変更を行っても、現行のデバイスに影響を与えません。
Connection Request Method	BAC が接続要求を実行するために試みる方法を指定します。Disabled オプションを選択してこの機能をディセーブルにするか、次の中から選択することができます。 • Discovered • Use FQDN • Use IP 選択した方法によって、BAC が、デバイスへの接続に使用する接続要求 URL を判別する方法が決まります。
Connection Request Path	デバイスの IP アドレスに基づいて URL パスを指定します。DPE はこのパスを使用して、接続要求 URL を構築します。
Connection Request Port	デバイスのポート番号を指定します。DPE はこのポート番号を使用して、接続要求 URL を構築します。
Device Operation Timeout	デバイス操作がタイムアウトになるまでの時間を秒単位で指定します。
Custom Discover Parameters	デバイスから検出される必要があるカスタム パラメータを、カンマ区切り形式で指定します。
Custom Firmware Changed Parameters	デバイスで新しいファームウェア バージョンが報告された場合にチェックする必要がある、カスタム パラメータを指定します。
Submit	行った変更を有効化または実装します。
Reset	すべての設定を元の設定に戻します。

RDU のデフォルト

RDU Defaults リンクをクリックすると、RDU Defaults ページ（図 17-3 を参照）が表示されます。このページを使用して、RDU の動作に影響を与える設定を行います。

図 17-3　RDU Defaults の Configure Defaults ページ

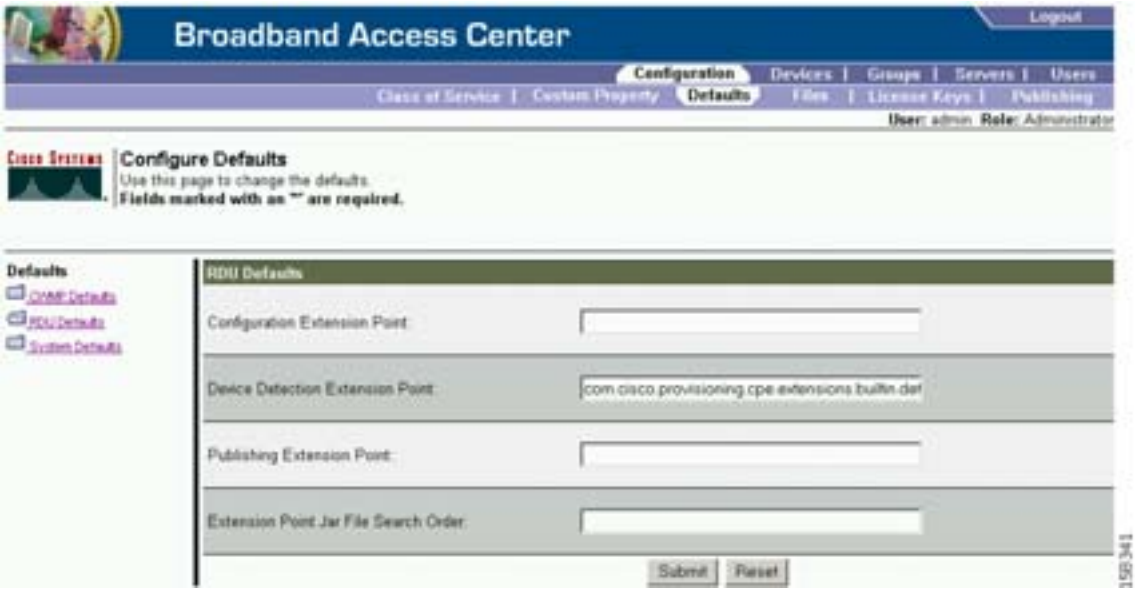


図 17-3 にあるすべてのフィールドとボタンを表 17-4 に示します。

表 17-4　RDU Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Configuration Extension Point	他のテクノロジー拡張が実行される前に実行する設定拡張を指定します。
Device Detection Extension Point	デバイスのタイプを判別するために使用する拡張を示します。
Publishing Extension Point	RDU パブリッシング プラグインに使用される拡張を指定します。これは、RDU データを別のデータベースにパブリッシングするときに役立ちます。
Extension Point Jar File Search Order	上記の 4 つのフィールドにリストされている Jar ファイルでクラスを検索するときの順序を指定します。
Submit	行った変更を有効化または実装します。
Reset	すべての設定を元の設定に戻します。

（注）　RDU 拡張ポイントの詳細については、P.17-20 の「RDU 拡張の管理」を参照してください。

システムのデフォルト

Systems Defaults リンクをクリックすると、System Defaults ページ（図 17-4 を参照）が表示されます。

図 17-4　System Defaults の Configure Defaults ページ

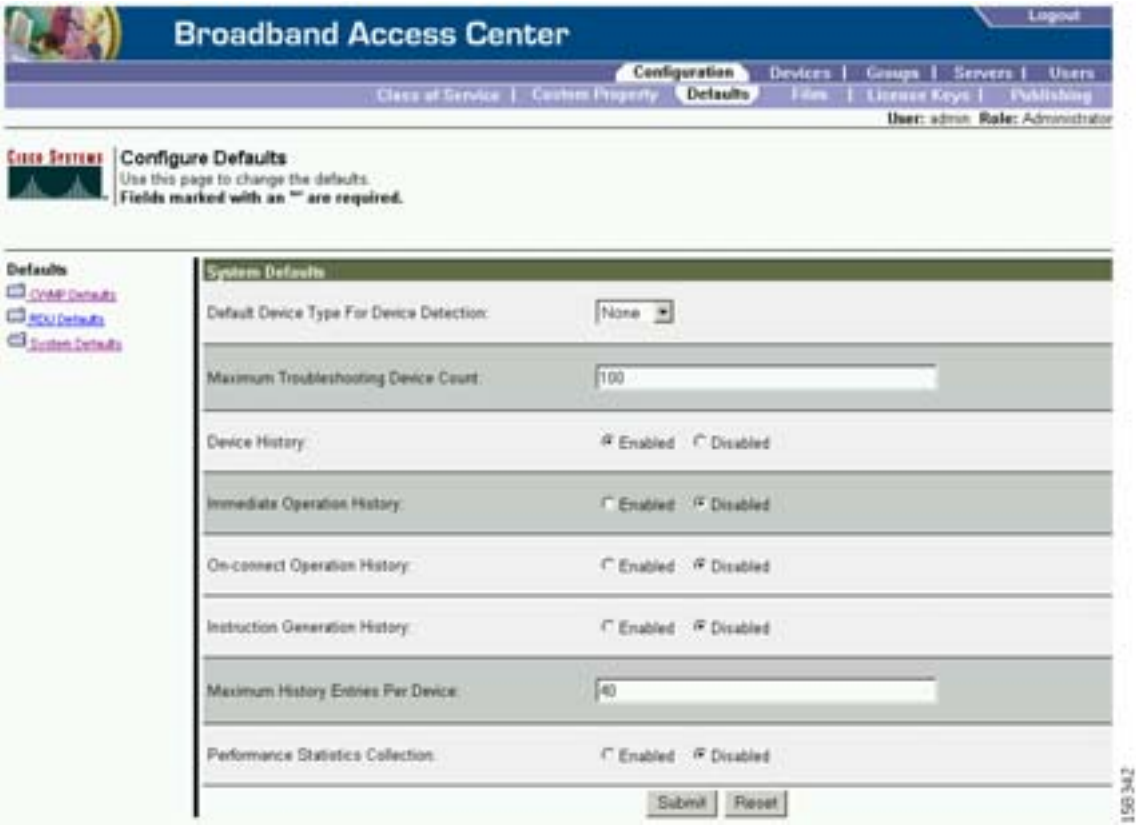


図 17-4 にあるすべてのフィールドとボタンを表 17-5 に示します。

表 17-5　System Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Default Device Type for Device Detection	これまで RDU に登録されていないデバイスのデフォルトのデバイス タイプを指定します。次のオプションがあります。 • CWMP • None デバイス検出拡張がデバイス タイプを特定できない場合、デバイス タイプは「デフォルト タイプ」（CWMP または None）に指定されます。デフォルトのデバイス タイプを None に設定した場合、デバイス レコードは RDU に追加されません。 **（注）** 登録されていないデバイスが RDU に構成を要求できるのは、DPE コマンドライン インターフェイスで **service cwmp** *num* **allow-unknown-cpe** オプションをイネーブルにした場合のみです。それ以外の場合、不明なデバイスからの要求は RDU に転送されません。

表 17-5　System Defaults の Configure Defaults ページ （続き）

フィールドまたはボタン	説明
Maximum Troubleshooting Device Count	一度にトラブルシューティングを行うことができるデバイスの最大数を指定します。デフォルトの数は 100 です。
Device History	デバイス レコードおよびデバイス構成のロギングをイネーブルにするか、ディセーブルにするかを示します。
Immediate Operation History	API から即時モードで開始されたデバイス操作の履歴のロギングをイネーブルにするか、ディセーブルにするかを示します。
On-Connect Operation History	API から接続時モードで開始されたデバイス操作の履歴のロギングをイネーブルにするか、ディセーブルにするかを示します。
Instruction Generation History	デバイスに対する命令の生成履歴のロギングをイネーブルにするか、ディセーブルにするかを示します。
Maximum History Entries Per Device	デバイスごとに格納されるデバイス履歴のエントリの最大数を指定します。デフォルトのエントリ数は 40 です。
Performance Statistics Collection	統計情報の収集をイネーブルにするかどうかを指定します。パフォーマンス統計情報については、P.11-14 の「パフォーマンス統計情報の監視」を参照してください。
Submit	行った変更を有効化または実装します。
Reset	すべての設定を元の設定に戻します。

ファイルの管理

BAC 管理者のユーザ インターフェイスを使用すると、CWMP ファイルまたはデバイスのソフトウェア イメージを動的に生成するためのテンプレート ファイルおよびパラメータ辞書を管理できます（図 17-5 を参照してください）。次に示すいずれかのファイル タイプを追加、削除、置換、またはエクスポートできます。

- Configuration Template：CWMP 設定ポリシーが記述された XML ファイルです。パラメータ値の設定、Notification 属性、および Access Control 属性などが含まれます。詳細については、P.5-14 の「設定テンプレートのオーサリング」を参照してください。
- Firmware File：デバイス ファームウェアのイメージです。機能をアップグレードするために、デバイスにダウンロードできます。BAC は、このファイル タイプをその他のバイナリ ファイルと同様に扱います。詳細については、P.6-1 の「ファームウェア管理」を参照してください。
- Firmware Rules Template：公開されたスキーマ文書に従って記述された XML ファイルです。各ファームウェア ルール テンプレートには、特定の条件に基づいてファームウェア アップデートをトリガーするルールが 1 つ以上含まれています。詳細については、P.6-1 の「ファームウェア管理」を参照してください。
- JAR File：BAC の拡張をロードするために使用されます。
- Parameter Dictionary：デバイスを設定するときに BAC で使用される、有効なオブジェクトとパラメータのリストが記述された XML ファイルです。辞書により、設定テンプレートおよびファームウェア ルール テンプレートで使用されているオブジェクトとパラメータが検証されます。詳細については、P.7-1 の「パラメータ辞書」を参照してください。
- Parameter List：デバイスが BAC に接続するたびに取得される、デバイスで事前定義されているパラメータのリストが記述された XML ファイルです。

（注）図 17-5 は、Manage Files ページで Search ボタンをクリックした後に表示されるページです。

図 17-5　Manage Files ページ

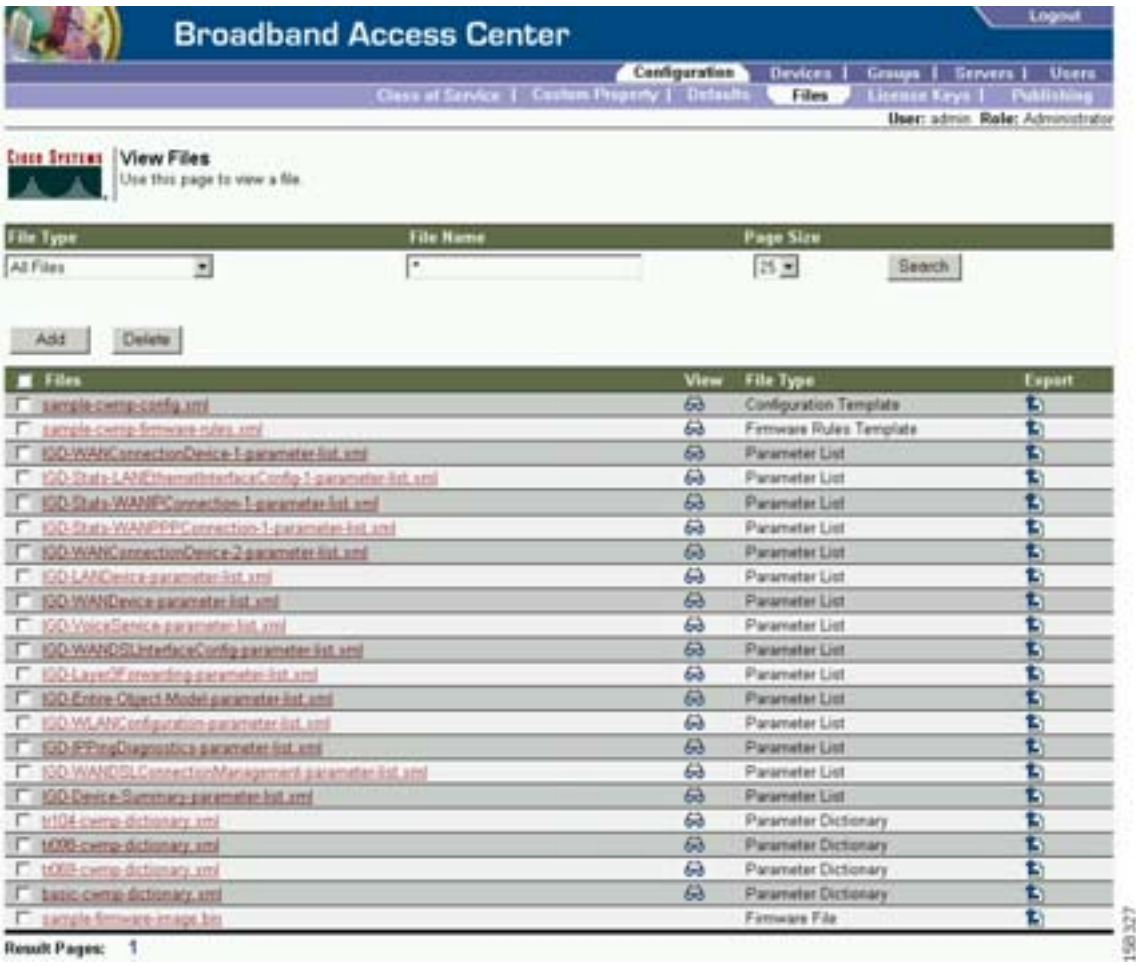


図 17-5 のフィールドとボタンを表 17-6 に示します。

表 17-6　Manage Files ページ

フィールドまたはボタン	説明
File Type	
File Type	ファイル タイプを指定します。
File Name	ファイル名を指定します。この値には、完全なファイル名を指定するか、文字列の先頭にワイルドカード文字を含めて、所定のサフィックスに一致するすべてのファイルを対象にすることができます。
Page Size	表示するページの長さを指定します。
Search	選択された File Type および File Name 検索パラメータに一致する名前を使用して、ファイルの検索を開始します。
Add	新しいファイルを追加します。
Delete	選択したファイルをデータベースから削除します。

表 17-6　Manage Files ページ （続き）

フィールドまたはボタン	説明
Files	
Files list	検索基準と一致したファイルのリストが表示されます。 （注）　このリストで選択した項目を削除するには、その項目のすぐ左にあるチェックボックスをオンにする必要があります。
View	選択したファイルの詳細情報が表示されます。
File Type	ファイルのタイプが示されます。たとえば、Configuration Template、Firmware Rules Template、Parameter List などです。
Export	選択したファイルをクライアントのコンピュータにエクスポートします。

ファイルの追加

既存のファイルを RDU データベースに追加するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Files** を選択します。

ステップ 3　View Files ページが表示されます。**Add** をクリックします。

ステップ 4　Add Files ページが表示されます。File Type を選択します。

（注）　Firmware ファイル タイプの場合、情報の提供のみを目的とした 2 つの追加フィールド、Firmware Version と Description が表示されます。これらのフィールドには任意の文字列を入力できます。

ステップ 5　Source File Name および File Name に値を入力します。ソースファイルの正確な名前が分からない場合は、**Browse** 機能を使用して目的のディレクトリを見つけて、そのファイルを選択します。デフォルトでは、最大 10 MB のファイル サイズがサポートされています。

ステップ 6　**Submit** をクリックします。

View Files ページが表示され、追加されたファイルが示されます。

ファイルの表示

ファイルの内容を表示するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Files** を選択します。

ステップ 3　View Files ページが表示されます。File Type を使用して、必要なファイルを検索します。

ステップ 4　検索で指定したファイル タイプに対応する **View Details** アイコン（）をクリックします。

View File ページが表示されます。

ファイルの置換

既存のファイルを置換するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Files** を選択します。

ステップ 3　検索出力リストから、置換するファイルに対応するリンクを選択します。

ステップ 4　Replace File ページが表示されます。選択したファイル名がすでにこのページに表示されています。ファイル名が表示されているファイルと置換する、ソース ファイルのパスおよびファイル名を入力します。

（注）　ソース ファイルの正確な名前や場所が分からない場合は、**Browse** 機能を使用して目的のディレクトリを見つけて、そのファイルを選択します。

ステップ 5　**Submit** をクリックします。

（注）　サービス　クラスに関連付けられている設定テンプレートまたはファームウェア　テンプレートをアップデートする場合、置換ファイルを送信すると、影響を受けるデバイスに対する命令が BAC によって再生成されることを示す確認ページが表示されます。Instruction Generation Service は、このテンプレートに関連付けられているすべてのデバイスに対する命令を、サービス クラスの関連付けを介して自動的に再生成し、新しい命令を適切な DPE に送信します。

ステップ 6　**OK** をクリックします。View Files ページが表示されます。

ファイルのエクスポート

エクスポート機能を使用して、ファイルを自分のローカル ハード ドライブにコピーできます。

（注） 次に示す手順は、Internet Explorer を使用している場合のものです。Netscape Navigator を使用している場合は、手順が異なります。

ファイルをエクスポートするには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Files** を選択します。

ステップ 3　エクスポートするファイルを指定します。

ステップ 4　バイナリ ファイルをエクスポートするには、**Export** アイコン（）をクリックします。ファイルを開くか、または保存するよう求めるメッセージが表示されます。テンプレートなどの XML ファイルをエクスポートする場合、Export アイコンをクリックすると、ファイルの内容が表示されます。したがって、Export アイコンを右クリックし、**Save Target As** を選択する必要があります。

ステップ 5　BAC 管理者のユーザ インターフェイスに戻ります。

ファイルの削除

既存のファイルを削除するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Files** を選択します。

ステップ 3　Files 領域に、修正するファイルのファイル名を入力します。

ステップ 4　**Search** をクリックします。

ステップ 5　該当のファイルが Files リストに表示されます。該当の 1 つまたは複数のファイルを選択します。

ステップ 6　**Delete** をクリックします。

注意　サービス　クラスに直接リンクされていないが、サービス　クラスにリンクされている他のテンプレート ファイルによって参照されるテンプレート ファイルを削除すると、命令の再生成サービスが失敗する原因になります。

（注） サービス　クラスに関連付けられているファイルは削除できません。操作を続ける前に、サービス クラスの関連付けを解除する必要があります。詳細については、P.17-2 の「サービス クラスの設定」を参照してください。

ライセンス キーの管理

ソフトウェア ライセンスは、特定の機能を有効にするか、または自分の環境の機能を高めるために使用します。それぞれのライセンスは、永久ライセンスまたは評価ライセンスとして入手できます。

- Permanent：永久ライセンスは、自分のネットワーク環境で使用するために購入するライセンスで、それに対応する特定の機能が有効になります。
- Evaluation：評価ライセンスは、インストール後の所定の期間、機能が有効になります。新しい永久ライセンス番号を入力することによって、評価ライセンスを永久ライセンスにアップグレードできます。

注意　評価ライセンス キーがインストールされた状態で、完全運用のネットワークへの展開を行わないようにしてください。評価ライセンスを使用して行ったプロビジョニングは、その評価ライセンスの期限が満了した時点で無効になります。

評価ライセンスから永久ライセンスにアップグレードするときに、ソフトウェアを再インストールしたり、BAC を再設定する必要はありません。BAC 管理者のユーザ インターフェイスを使用して、永久ライセンスを提供するだけです。

Manage License Keys ページ（図 17-6）に、自分の実装用に入力したライセンスのリストが表示されます。この BAC リリースでは、CWMP 準拠デバイスおよび DPE の、評価ライセンスと永久ライセンスの両方がサポートされます。また、使用可能な各ライセンスのステータスが有効または期限満了のいずれかで表示されるか、あるいは期限満了日が表示されます。

（注）　ライセンスを追加することで、永久ライセンスをアップグレードして、ライセンスされるデバイスの数を増やすことができます。ライセンスされたデバイスの数が上限に達すると、新しいデバイスをプロビジョニングできませんが、すでにプロビジョニングされた既存のデバイスは引き続きサービスを受けられます。

図 17-6　Manage License Keys ページ

ライセンスの追加と修正

ライセンスを追加、修正、またはアップグレードするには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **License Keys** を選択します。

ステップ 3　シスコシステムズの代理店または Cisco Technical Assistance Center（TAC）の Web サイトから新しいライセンス キーを取得します。TAC の連絡先については、このガイドの「このマニュアルについて」を参照してください。

ステップ 4　License Key フィールドに新しいライセンス キーを入力します。

ステップ 5　**Add/Upgrade** をクリックして新しいライセンス キーをインストールします。永久ライセンス キーを入力すると、対応する評価ライセンス キー（そのキーがインストールされていた場合）が無効になります。新しいテクノロジーに対するライセンス キー（永久または評価）を入力すると、テクノロジー リストにそのテクノロジーが表示されます。

RDU 拡張の管理

カスタム拡張の作成は、基本的には、プログラミング作業です。BAC 管理者のユーザ インターフェイスと併用することで、この作業では、BAC の動作を強化したり、新しいデバイス テクノロジーのサポートを追加したりできます。

拡張の管理には、次の作業があります。

- 新しいクラスの作成（P.17-20）
- RDU カスタム拡張のインストール（P.17-20）
- RDU 拡張の表示（P.17-21）

（注） 拡張ポイントが連続的に実行されるようにすることによって、複数の拡張ポイントを指定できます。これを行うには、カンマ区切りリスト形式で拡張ポイントを指定します。

新しいクラスの作成

次の手順は、カスタム拡張の作成プロセス全体をより明確に説明するためのものです。さまざまなタイプの拡張を作成できます。次の手順では、パブリッシング拡張を使用します。

新しいクラスを作成するには、次の手順に従います。

ステップ 1　カスタム パブリッシング拡張に関する Java ソース ファイルを作成し、コンパイルします。

ステップ 2　拡張クラスを記述する Jar ファイルのマニフェスト ファイルを作成します。

ステップ 3　カスタム拡張ポイントに関する Jar ファイルを作成します。Jar ファイルには任意の名前を割り当てることができますが、特性を説明するような名前にする必要があります。また、他の既存の Jar ファイルと同じ名前にすることはできません。

RDU カスタム拡張のインストール

Jar ファイルを作成したら、管理者のユーザ インターフェイスを使用してファイルをインストールします。

ステップ 1　P.17-15 の「ファイルの追加」を参照して、新しい Jar ファイルを追加します。

（注） JAR ファイル タイプを選択します。Browse 機能を使用して、P.17-20 の「新しいクラスの作成」の手順で作成した Jar ファイルを見つけ、このファイルをソース ファイルとして選択します。File Name を空白のままにすると、ソース ファイルと外部ファイルの両方に同じファイル名が割り当てられます。このファイル名が、管理者のユーザ インターフェイスに表示されます。

ステップ 2　**Submit** をクリックします。

ステップ 3　RDU Defaults の Configure Defaults ページに戻り、新しく追加された Jar ファイルが Extension Point Jar File Search Order フィールドに表示されることを確認します。

ステップ 4　Publishing Extension Point フィールドに拡張クラス名を入力します。

（注）　クラス名が Jar ファイル内に存在しない場合や、BAC が他のエラーを検出した場合は、RDU からエラーが返されます。このエラーは、主に Jar ファイルを置換するときに発生します。たとえば、設定したクラスが置換 Jar ファイル内で見つからない場合などです。

ステップ 5　**Submit** をクリックして、変更を RDU データベースにコミットします。

ステップ 6　RDU 拡張を表示し、正しい拡張がロードされることを確認します。

RDU 拡張の表示

すべての RDU 拡張の属性は、View Regional Distribution Unit Details ページに直接表示できます。このページには、インストールされている拡張 Jar ファイルとロードされた拡張クラス ファイルに関する詳細が表示されます。

プロビジョニング データのパブリッシング

BAC には、追跡したプロビジョニング データを外部データストアにリアルタイムにパブリッシングする機能があります。そのためには、目的のデータストアにデータを書き込むパブリッシング プラグインを開発する必要があります。Manage Publishing ページには、プラグインの名前、その現在のステータス（イネーブルかどうか）、およびイネーブルまたはディセーブルにするためのスイッチが表示されます。

実装に必要なプラグインはすべてイネーブルにすることができますが、パブリッシング プラグインを使用するとシステム パフォーマンスが低下することがあるため、注意が必要です。

（注） BAC にはパブリッシング プラグインが付属していません。管理者は自分でプラグインを作成し、それらを JAR ファイルと同じ方法で BAC にロードする必要があります（P.17-15 の「ファイルの追加」を参照してください）。その後、Manage Publishing ページからプラグインを管理します。

データストアの変更のパブリッシング

パブリッシング プラグインをイネーブルまたはディセーブルにするには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Publishing** を選択します。

ステップ 3　Manage Publishing ページが表示されます。このページには、使用可能なデータベースのすべてのプラグインのリストが表示され、それぞれのプラグインの現在のステータスが示されます。目的のプラグインをイネーブルまたはディセーブルにするには、対応するステータス インジケータをクリックします。ステータスをクリックすることで、イネーブルとディセーブルが切り替わります。

パブリッシング プラグイン設定の修正

これらの設定は、プラグインの作成者が各自のデータストアの RDU にプラグイン設定を保存するための便利な手段です。パブリッシング プラグイン設定を修正するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Publishing** を選択します。Manage Publishing ページが表示されます。

ステップ 3　修正するプラグインに対応するリンクをクリックします。Modify Publishing Plug-Ins ページが表示されます。

Modify Publishing Plug-Ins ページに表示されるフィールドを表 17-7 に示します。

表 17-7　Modify Publishing Plug-ins ページ

フィールドまたはボタン	説明
Plug-In	パブリッシング プラグインの名前が表示されます。
Server	データストアがあるサーバの名前を指定します。
Port	データストアがあるポートの番号を指定します。
IP Address	データストアがあるサーバの IP アドレスを指定します。通常、この IP アドレスは、サーバ名を使用しない場合に指定します。
User	データストアにアクセスするためのユーザ名を指定します。
Password	データストアにアクセスするためのユーザのパスワードを指定します。
Confirm Password	確認のため、上のフィールドに入力したパスワードをこのフィールドにも入力します。

ステップ 4　Server、Port、IP Address、User、Password、および Confirm Password の各フィールドに必要な値を入力します。これらはすべて必須フィールドなので、これらの情報を入力しなければ、次の操作へ進むことができません。

ステップ 5　**Submit** をクリックして、選択したプラグインへの変更を実行するか、または、**Reset** をクリックして、このページのすべてのフィールドをクリアします。

BAC がサポートするツールと高度な概念

この章では、Broadband Access Center（BAC）の保守、および製品のインストール、配備、使用の高速化と改善に役立つツールとその使用方法について説明します。

この章では、次のトピックについて取り上げます。

- deviceExport.sh ツールの使用方法（P.18-2）
- disk_monitor.sh ツールの使用方法（P.18-5）

このリリースでサポートされているその他のツールのリストについては、P.9-5 の「BAC ツール」を参照してください。

（注） この項では、ツールの使用方法の例を示します。多くの場合、ツールのファイル名には *BPR_HOME* と指定されたパスが含まれます。これは、デフォルトのインストール ディレクトリ位置を示しています。

deviceExport.sh ツールの使用方法

デバイス エクスポート ツールを使用すると、デバイスに関する情報を取得できます。このツールは、BAC システムからデバイス情報を取得し、フラット ファイルにエクスポートします。このファイルは、データを外部アプリケーションにインポートするときに使用できます。

deviceExport.sh ツール（*BPR_HOME/rdu/bin* ディレクトリ内）は、デバイス情報を、RDU データベースのバックアップ スナップショットから Comma Separated Value（CSV; カンマ区切り形式）ファイルにエクスポートします。

（注） デバイス エクスポート ツールは、バックアップ データベースに対してのみ使用できます。RDU ライブ データベースからデバイス情報をエクスポートすることはできません。

エクスポートするデバイス プロパティのリストを制御ファイルに指定する必要があります。制御ファイルとは、エクスポートに必要なフィールドを定義する XML ファイルのことです。ツールには、サンプルの制御ファイルを生成するオプションがあります。そのファイルを編集して、エクスポートするプロパティを設定できます。**deviceExport.sh -samplectrl** コマンドを実行すると、BAC で事前に定義されており、エクスポートに使用可能なプロパティのリストを生成できます（制御出力のサンプルについては、例 18-2 を参照してください）。

アプリケーション間のデータ交換では、CSV 形式が広く使用されています。CSV 形式のファイルについては、次のルールに注意してください。

- 各デバイスは 1 行に出力されます。
- 各行の末尾には UNIX 形式の行区切り記号（\n）が含まれます。
- 各フィールドはカンマ（,）で区切られています。
- フィールドに空白、カンマ、または行区切り記号が含まれる場合、そのフィールドは二重引用符（"）で囲まれます。フィールドに二重引用符が含まれる場合は、二重引用符を 2 回繰り返してエスケープします。たとえば、"file name" は ""file name"" と記述します。
- ブール型のフィールドでは、*true* または *false* が出力されます。
- バイト配列は、UTF-8 で符号化された文字列に出力されます。
- フィールドがリストの場合、各項目がカンマで区切られた書式に設定された文字列に変換されます。たとえば、ノード リストは、「node1, node2, node3」として出力されます。
- フィールドがマップである場合、そのフィールドは長い文字列に変換されます。キーとデータは、カンマで区切られます。たとえば、マップの出力は「(key1, data1)(key2, data2)(key3, data3)」のようになります。
- フィールドの値がヌルであるか存在しない場合、空の文字列が出力され、その後ろにカンマが続きます。
- 最初の行はフィールド名で、カンマで区切られています。
- 各レコードの終わりにカンマはありません。

例 18-1　CSV 形式のサンプル

```
74:7b:7b:f0:e7:80,admin,true,2,"node1,node2,node3","(prop1,value1)(prop2,value2)",,,
```

構文の説明

deviceExport.sh コマンドを使用するには、次の構文を使用します。

```
# ./deviceExport.sh [-help] [-samplectrl] controlfile backupdir outputdir
```

- *controlfile*：制御ファイルへのパスを指定します。制御ファイルには、エクスポートに必要なフィールドを定義します。
- *backupdir*：ディレクトリへのパスを指定します。このディレクトリには、データ ソースとして使用するバックアップ データベース ファイルが含まれます（データベースをバックアップするには、**backupDb.sh** ツールを使用します。P.10-6 の「バックアップと回復」を参照してください）。
- *outputdir*：出力ファイルの出力先を指定します。ディレクトリが存在しない場合、新しいディレクトリが作成されます。
- **help**：ツールの使用方法に関する情報を生成します。
- **samplectrl**：サンプルの制御ファイル（サポートされるプロパティとデバイス タイプが記述されたもの）を現在のディレクトリに生成します。制御ファイルとは、サポートされるプロパティとデバイス タイプが示された XML ファイルのことです。この XML ファイルを編集することにより、不要なプロパティを削除したり、特定のタイプのデバイスだけをエクスポートするように選択したりできます。制御ファイルの出力サンプルについては、例 18-2 を参照してください。

例 18-2　制御ファイルのサンプル

```
# ./deviceExport.sh -samplectrl
<?xml version='1.0' encoding='utf-8'?>
<!DOCTYPE CONTROLFILE SYSTEM "device-export-control.dtd">

<!--SAMPLE CONTROL FILE-->
<CONTROLFILE>

    <!--Start of field list(REQUIRED)
        The field list specifies the device properties that will be exported.
        All supported standard fields are listed below. Remove unwanted
        fields by deleting the line that contains the field name. Customer
        defined properties are not listed but can be added to the list.
    -->
    <FIELDLIST>
        <FIELD>GenericObjectKeys.OID_REVISION_NUMBER</FIELD>
        <FIELD>DeviceDetailsKeys.DEVICE_TYPE</FIELD>
        <FIELD>DeviceDetailsKeys.OWNER_ID</FIELD>
        <FIELD>DeviceDetailsKeys.NODE_DETAILS</FIELD>
        <FIELD>DeviceDetailsKeys.DEVICE_ID</FIELD>
        <FIELD>DeviceDetailsKeys.FQDN</FIELD>
        <FIELD>DeviceDetailsKeys.HOST</FIELD>
        <FIELD>DeviceDetailsKeys.DOMAIN</FIELD>
        <FIELD>DeviceDetailsKeys.IS_IN_REQUIRED_PROV_GROUP</FIELD>
        <FIELD>DeviceDetailsKeys.IS_REGISTERED</FIELD>
        <FIELD>DeviceDetailsKeys.IS_PROVISIONED</FIELD>
        <FIELD>DeviceDetailsKeys.PROV_GROUP</FIELD>
        <FIELD>DeviceDetailsKeys.CLASS_OF_SERVICE</FIELD>
        <FIELD>DeviceDetailsKeys.CLASS_OF_SERVICE_SELECTED</FIELD>
        <FIELD>DeviceDetailsKeys.PROPERTIES</FIELD>
        <FIELD>DeviceDetailsKeys.PROPERTIES_DETECTED</FIELD>
        <FIELD>DeviceDetailsKeys.PROPERTIES_SELECTED</FIELD>
        <FIELD>DeviceDetailsKeys.REASON</FIELD>
        <FIELD>DeviceDetailsKeys.EXPLANATION</FIELD>
        <FIELD>DeviceDetailsKeys.CONFIGURATION_REVISION</FIELD>
        <FIELD>DeviceDetailsKeys.FIRMWARE_CONFIGURATION_REVISION</FIELD>
        <FIELD>DeviceDetailsKeys.REPORTED_IP_ADDRESS</FIELD>
        <FIELD>DeviceDetailsKeys.SOURCE_IP_ADDRESS</FIELD>
        <FIELD>DeviceDetailsKeys.ROUTABLE_IP_ADDRESS</FIELD>
        <FIELD>DeviceDetailsKeys.DEVICE_FAULTS</FIELD>
        <FIELD>DeviceDetailsKeys.PENDING_ON_CONNECT_OPERATION_IDS</FIELD>
        <FIELD>DeviceDetailsKeys.PASSWORD_IS_PROTECTED</FIELD>
        <FIELD>IPDeviceKeys.HOME_PROV_GROUP</FIELD>
        <FIELD>IPDeviceKeys.CPE_PASSWORD</FIELD>
        <FIELD>IPDeviceKeys.CONNECTION_REQUEST_USERNAME</FIELD>
        <FIELD>IPDeviceKeys.CONNECTION_REQUEST_PASSWORD</FIELD>
    </FIELDLIST>
    <!--End of field list-->

</CONTROLFILE>
```

（注）　DOCTYPE CONTROLFILE SYSTEM は、XML の検証に使用する *device-export-control.dtd* という .dtd ファイルを参照します。このファイルは、*BPR_HOME/rdu/bin* ディレクトリにインストールされています。

例 18-3　バックアップ スナップショットからのデータのエクスポート

バックアップ スナップショットからデータをエクスポートする例を、次に示します。

```
# ./deviceExport.sh control.xml rdu-backup-20061227-145538 /data/rduexport
Starting exporting devices...

Using backup database in /tmp/rdu-backup-20061227-145538
Device export finished in 28m11s.
```

（注）　エクスポートされたファイルは、指定したディレクトリ内に生成されます。上記の例では、*/data/rduexport* ディレクトリです。ディレクトリのフル パスを指定する必要はありません。

BAC バックアップ データベースからのエクスポートが正常に完了すると、デバイス エクスポート ツールはデバイス ファイルを作成します。このファイルには、BAC バックアップ データベースから正常にエクスポートされたデバイス　　レコードのリストが含まれます。ファイル名は、bac-device-details-*yyyyMMdd-HHmmss*.csv です。

ここで、*yyyyMMdd-HHmmss* は、ファイルが生成された時刻を示します。

disk_monitor.sh ツールの使用方法

利用可能なディスク領域を監視することは、重要なシステム管理作業です。多数のカスタム スクリプトまたは市販のツールを使用して、この作業を実行できます。disk_monitor.sh ツールは、この作業を行うためのサンプル ツールです。

disk_monitor.sh ツールは *BBPR_HOME/rdu/sample/tools* ディレクトリにあり、1 つ以上のファイル システムのしきい値を設定します。これらのしきい値を超えると、追加のディスク領域が利用可能になるまで、60 秒ごとに Solaris の syslog 機能によってアラートが生成されます。

（注） 少なくとも、disk_monitor.sh スクリプトを使用して *BPR_DATA* および *BPR_DBLOG* ディレクトリを監視することをお勧めします。

構文の説明

```
# ./disk_monitor.sh file system-directory x
```

- *file system-directory*：監視するファイル システムのディレクトリを示します。
- *x*：指定したファイル システムに適用するしきい値をパーセントで示します。

例 18-4　ディスク領域の監視

データベース ログが保存されるファイル システム（ここでは */var/CSCObpr*）の利用率が 80% に達したときに、通知するものとします。次のコマンドを入力します。

```
# ./disk_monitor.sh /var/CSCObac 80&
```

データベース ログのディスク領域の利用率が 80% に達すると、次のようなアラートが syslog ファイルに送信されます。

```
Dec 7 8:16:03 perf-u80-1 BPR: [ID 702911 local6.warning] File system /var/bpr usage is
81% (threshold is 80%)
```

（注） 起動時にこの監視を実行するように Solaris を設定してください。その設定により、システムのリブート後に監視が自動的に開始されます。

Broadband Access Center のトラブルシューティング

この章では、Broadband Access Center（BAC）のトラブルシューティングを行う方法の詳細について説明します。この章では、次のトピックについて説明します。

トラブルシューティングのチェックリスト

BAC のトラブルシューティングでは、表 19-1 に示すチェックリストを使用します。

表 19-1　トラブルシューティングのチェックリスト

手順	参照先
1. BAC コンポーネントがインストールされているすべてのシステムで、BAC のプロセスが稼働しているかどうかを確認します。	コマンドラインからの BAC プロセス ウォッチドッグの使用（P.9-2）
2. BAC のコンポーネント ログで、重大度の高いエラーが示されていないかどうかを確認します。これには、次のものに関して記録された情報が含まれます。 — RDU — DPE	 RDU のログ（P.19-5） DPE のログ（P.19-9）
3. 管理者のユーザ インターフェイスからサーバのアップ タイムを表示し、サーバがバウンスしていないことを確認します。	サーバの表示（P.16-24）
4. 管理者のユーザ インターフェイスから、RDU および DPE のサービス パフォーマンス統計情報を表示します。トランザクション時間が長くなっているなど、異常な数値がないか確認します。	サーバの表示（P.16-24）
5. syslog アラート ログを確認します。	syslog アラート メッセージ（P.11-1）
6. 次のようなオペレーティング システムおよびハードウェアのリソースを確認します。 — ディスク領域 — CPU 時間 — メモリ	 特定のコマンドについては、Solaris のマニュアルを参照してください。
7. 特定のデバイスのトラブルシューティングを行う場合は、管理者のユーザ インターフェイスからデバイス構成の履歴を表示します。	デバイスの履歴の表示（P.16-13）
8. 特定のデバイスのトラブルシューティングを行う場合は、DPE でキャッシュされているデバイス命令を表示します。	『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』の **show device-config** コマンドの説明
9. 管理者のユーザ インターフェイスから、個々のデバイスのトラブルシューティングを設定します。しばらく経過してから、トラブルシューティング ログを調べます。	デバイスのトラブルシューティングの設定（P.8-10）
10. システム、RDU、DPE、または特定のデバイスのデバイス障害データを表示します。	デバイス障害（P.8-7）
11. RDU または適切な DPE でより高いロギング レベルを設定し、詳細なログ情報を取得します。	RDU ログ レベル ツール（P.19-6） 『*Cisco Broadband Access Center DPE CLI Reference, 3.0*』の **log level** コマンドの説明

ロギング

イベントのロギングは DPE と RDU の両方で実行されます。まれに、視認性向上のために、DPE イベントが RDU に記録されることもあります。ログ ファイルはそれぞれのログ ディレクトリに配置され、任意のテキスト ファイル ビューアを使用して調べることができます。ログ ファイルを圧縮すると、トラブルシューティングや障害の解決のために TAC またはシステム インテグレータに電子メールで送信しやすくなります。

この項では、次のトピックについて取り上げます。

ログのレベルおよび構造

ログ ファイルの構造は、ここで説明するとともに、例 19-1 で例示しています。ログ ファイルの構造に含まれる情報は次のとおりです。

- Domain Name：ログ ファイルが生成されたコンピュータの名前。
- Date and Time：メッセージがログに記録された日時。ここには、該当するシステムの時間帯も示されます。
- Facility：システムを識別します（この場合は BAC）。
- Sub-facility：BAC のサブシステムまたはコンポーネントを識別します。
- Security Level：ログの問題を処理するときの緊急性を識別するために使用される重大度。ログ システムでは、7 段階のログ レベル（表 19-2 を参照）が定義されます。次のログ レベルの設定方法については、P.19-4 の「ログ レベルの設定」を参照してください。

表 19-2　ログ レベル

ログ レベル	説明
0：緊急	システムが不安定です。すべての緊急メッセージを保存するように、ロギング機能を設定します。
1：アラート	すぐに対応が必要です。すぐに対応が必要なすべてのアクティビティ、およびさらに深刻な活動を保存するように、ロギング機能を設定します。
2：クリティカル	クリティカルな状態が存在します。すべてのエラー メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
3：エラー	エラー状態が存在します。すべてのエラー メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
4：警告	警告状態が存在します。すべての警告メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
5：通知	通常ですが、重大な状態が存在します。すべての通知メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。

表 19-2　ログ レベル （続き）

ログ レベル	説明
6：情報	情報メッセージ。利用可能なすべてのロギング メッセージを保存するように、ロギング機能を設定します。

（注）　7（デバッグ）として知られるもう 1 つのレベルは、シスコでデバッグの目的にのみ使用されます。Cisco TAC で指示された場合を除き、このレベルは使用しないようにしてください。

- Msg ID：メッセージ テキストの固有な識別子。
- Message：実際のログ メッセージ。

例 19-1　ログ ファイルのサンプル

Domain Name	Data and Time	Facility	Sub-facility	Security Level	Msg ID	Message
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0236:	BAC Regional Distribution Unit starting up
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0566:	Initialized API defaults
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0568:	Initialized server defaults
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0569:	Created default admin user
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0574:	Loaded 6 license keys
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0575:	Database initialization completed in 471 msec
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0015:	Unable to locate manifest file
BAC1:	2006 04 21 07:28:00 EDT:	BAC-	RDU-	6	0280:	Command error

ログ レベルの設定

RDU と DPE のログ レベルは、いずれも特定の要件に合せて設定できます。たとえば、RDU のログ レベルを「警告」、DPE のログ レベルを「アラート」に設定できます。

ログ メッセージは、特定のイベントの発生に基づいて記述されます。イベントが発生するたびに、該当するログ メッセージとログ レベルが割り当てられます。ログ レベルが設定したレベル以下であれば、メッセージがログに書き込まれます。レベルが設定した値より高い場合、メッセージはログに書き込まれません。

たとえば、ログ レベルが 4（警告）に設定されているとします。ログ ファイルには、ログ レベルが 4 以下に設定されているイベントの生成するメッセージがすべて書き込まれます。ログ レベルが 6（情報）に設定されている場合、ログ ファイルにはすべてのメッセージが書き込まれます。したがって、ログ レベルを高く設定するほど、ログ ファイルのサイズは大きくなります。

DPE に対するログ レベルを設定するには、DPE コマンドラインから **log level** コマンドを使用します。詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

RDU でのログ レベルを設定するには、P.19-6 の「RDU ログ レベル ツール」を参照してください。

ログ ファイルの循環

perfstat.log 以外のすべてのログ ファイルには、設定済みの最大ファイル サイズに基づいて番号が付けられ、ロール オーバーされます。デフォルトの最大ファイル サイズは 10 MB です（API から最大ファイル サイズを設定するには、`ServerDefaultsKeys.SERVER_LOG_MAXSIZE` プロパティを使用します）。ログ ファイルが設定済みの制限に達すると、データは別のファイルにロール オーバーされます。このファイルの名前は、*XXX.N*.log という形式で変更されます。内容は次のとおりです。

- *XXX*：ログ ファイルの名前を指定します。
- *N*：1 ～ 29 のいずれかの値を示します。

たとえば、*rdu.log* が 10 MB の制限に達すると、このファイルの名前は *rdu.1.log* に変更されます。ファイルのサイズが 10 MB 増えるたびに、最新のファイルの名前は *rdu.2.log*、*rdu.3.log* のように変更されます。したがって、*rdu.7.log* ファイルには、*rdu.4.log* より新しいデータが含まれます。ただし、最新のログ情報が保存されているのは、常に *rdu.log* です。

perfstat.log ファイルの場合、名前は毎日変更されます。このファイルは、perfstat.*N*.log という形式でロール オーバーされます。*N* は 1 ～ 29 のいずれかの値となります。たとえば、*perfstat.29.log* は最も古いログで、*perfstat.1.log* は最も新しく名前変更された *perfstat.log* ファイルです。

BAC は、一時に最大 10 個のログ ファイルを保存します。RDU サーバおよび DPE サーバのログ ファイルのリストについては、それぞれ、P.19-5 の「RDU のログ」、P.19-9 の「DPE のログ」を参照してください。

RDU のログ

RDU には次の 4 つのログがあり、*BPR_DATA/rdu/logs* ディレクトリで保持されます。

- *rdu.log*：設定されたロギング重要度レベルに従って、すべての RDU イベントを記録します（デフォルトのログ レベルの設定方法については、P.19-7 の「RDU ログ レベルの設定」を参照してください）。*rdu.log* を表示するには、P.19-6 の「rdu.log ファイルの表示」を参照してください。
- *audit.log*：BAC　の設定または機能に対して行われた高いレベルの変更がすべて記録されます。このような変更を行ったユーザも記録されます。*audit.log* を表示するには、P.19-6 の「audit.log ファイルの表示」を参照してください。
- *troubleshooting.log*：特定のデバイスまたはデバイス グループのトラブルシューティングに役立つ詳細なデバイス情報が記録されます。この場合、ロギングをオンにしたり、デバイス固有またはグループ固有の情報についてのログ ファイルを検索したりする必要はありません。管理者のユーザ インターフェイスから *troubleshooting.log* を表示するには、P.8-12 の「デバイスのトラブルシューティング ログの表示」を参照してください。
- *perfstats.log*：デバイスのパフォーマンス統計情報が記録されます。この情報は、システム　パフォーマンスに関連した問題のトラブルシューティングに役立ちます。詳細については、P.11-1 の「Broadband Access Center の監視」を参照してください。

rdu.log ファイルの表示

rdu.log ファイルを表示するには、任意のテキスト エディタを使用できます。また、このログ ファイルは、管理者のユーザ インターフェイスからも表示できます。次の手順に従います。

ステップ 1　**Servers** の下の **RDU** タブを選択します。

ステップ 2　View Regional Distribution Unit Details ページが表示されます。RDU Log File に対応する **View Details** アイコン（）をクリックします。

View Log File Contents ページが表示され、*rdu.log* からのデータが示されます。

audit.log ファイルの表示

audit.log ファイルを表示するには、任意のテキスト エディタを使用できます。また、このログ ファイルは、管理者のユーザ インターフェイスからも表示できます。次の手順に従います。

ステップ 1　**Servers** の下の **RDU** タブを選択します。

ステップ 2　View Regional Distribution Unit Details ページが表示されます。Audit Log File に対応する **View Details** アイコンをクリックします。

View Log File Contents ページが表示され、*audit.log* からのデータが示されます。

RDU ログ レベル ツール

RDU ログ レベル ツールを使用して、コマンドラインから RDU の現在のログ レベルを変更します。**setLogLevel.sh** コマンドを使用します。このツールは *BPR_HOME/rdu/bin* ディレクトリにあります。表 19-2 は、利用可能なログ レベルと、イネーブルにした場合にログ ファイルに書き込まれるメッセージの種類を示しています。

安定した動作状態を維持するためには、RDU ロギング レベルを警告レベルのままにすることをお勧めします。デバッグ動作中に安定した状態パフォーマンスを維持する必要がある場合は、情報レベルを注意して使用することをお勧めします。情報レベルに設定して実行すると大量のログ エントリが作成され、このことがパフォーマンスに悪影響を与える可能性があるため、注意が必要です。

（注）　ログ レベル ツールを実行するには、RDU プロセスが稼働している必要があります。また、**setLogLevel.sh** コマンドを使用してこのツールを実行する特権も必要です。

RDU ログ レベル ツールの使用方法

すべての例では、RDU のユーザ名は **admin**、RDU のパスワードは **changeme** とし、RDU サーバが稼働中であることを前提にしています。

次のコマンドを入力して、RDU ログ レベル ツールを実行します。

```
setLogLevel.sh [0..6] [-help] [-show] [-default] [-debug]
```

内容は次のとおりです。

- *-[0..6]*：使用するログ レベルを示します。利用可能なレベルのリストについては、表 19-2 を参照してください。
- **-help**：ツールのヘルプを表示します。
- **-show**：RDU サーバの現在のログ レベル設定を表示します。
- **-default**：RDU をインストール デフォルト レベルの 5（通知）に設定します。
- **-debug**：RDU サーバのカテゴリのトレースをイネーブルまたはディセーブルにするように、対話モードを設定します。

（注） シスコのサポート スタッフの指示があった場合にのみ、デバッグ設定をイネーブルにしてください。

このツールを使用して、次の機能も実行できます。

- RDU ログ レベルの設定（P.19-7）
- RDU の現在のログ レベルの表示（P.19-8）

RDU ログ レベルの設定

このツールを使用して、ロギング レベルをある値から別の値に変更できます。

次の例では、RDU ロギング レベルを警告レベル（**setLogLevel.sh** コマンドでは数値 4 で示されるレベル）に設定する方法を示します。実際のログ レベル設定は手順にとって重要ではないので、必要に応じて読み替えてください。

RDU ロギング レベルを設定するには、次の手順に従います。

ステップ 1　*BPR_HOME/rdu/bin* にディレクトリを変更します。

ステップ 2　次のコマンドを使用して、RDU ログ レベル ツールを実行します。

```
setLogLevel.sh 4
```

次のプロンプトが表示されます。

```
Please type RDU username:
```

ステップ 3　プロンプトに対して、RDU ユーザ名を入力します。この例では、デフォルト ユーザ名（admin）を使用します。

```
Please type RDU username: admin
```

次のプロンプトが表示されます。

```
Please type RDU password:
```

ステップ 4　プロンプトに対して、RDU　のパスワードを入力します。この例では、デフォルト　パスワード（**changeme**）を使用します。

```
Please type RDU password: changeme
```

次のメッセージが表示され、ログ レベルが変更されたことが通知されます。この例では、レベル 5（通知）から 4（警告）に変更されました。

```
RDU Log level was changed from 5 (notification) to 4 (warning).
```

RDU の現在のログ レベルの表示

このツールを使用して、ロギング レベルの値を変更する前に、RDU ログを表示し、設定されている値を判別できます。

RDU の現在のロギング レベルを表示するには、次の手順に従います。

ステップ 1　*BPR_HOME/rdu/bin* にディレクトリを変更します。

ステップ 2　次のコマンドを実行します。

```
setLogLevel.sh -show
```

次のプロンプトが表示されます。

```
Please type RDU username:
```

ステップ 3　RDU ユーザ名（**admin**）を入力し、**Enter** キーを押します。

```
Please type RDU username: admin
```

次のプロンプトが表示されます。

```
Please type RDU password:
```

ステップ 4　RDU パスワード（**changeme**）を入力し、**Enter** キーを押します。

```
Please type RDU password: changeme
```

次のメッセージが表示されます。

```
The logging is currently set at level: 4 (warning)

All tracing is currently disabled.
```

DPE のログ

DPE は、*BPR_DATA/dpe/logs* ディレクトリにログを保持しています。

- *dpe.log*：デフォルト レベルが設定されているすべてのイベントを記録します。システム障害が連続して起こるなど、DPE で破局的な障害が発生した場合、破局的なエラーは rdu.log ファイルにも記録されます。
- *perfstats.log*：デバイスのパフォーマンス統計情報が記録されます。この情報は、システム　パフォーマンスに関連した問題のトラブルシューティングに役立ちます。詳細については、P.11-1 の「Broadband Access Center の監視」を参照してください。

dpe.log ファイルの表示

dpe.log ファイルを表示するには、任意のテキスト ビューアを使用できます。また、DPE の CLI から **show log** コマンドを使用して、ログ ファイルの内容を表示することもできます。詳細については、『*Cisco Broadband Access Center DPE CLI Reference, Release 3.0*』を参照してください。

さらに、BAC 管理者のユーザ インターフェイスを使用して DPE ログ ファイルを表示することもできます。次の手順に従います。

ステップ 1　**Servers** > **DPEs** を選択します。

ステップ 2　ログ ファイルを表示する DPE に対応するリンクをクリックします。

ステップ 3　View Device Provisioning Engines Details ページが表示されます。*dpe.log* ファイルの内容を表示するには、Log Files 領域で DPE Log File の **View Details** アイコンをクリックします。

A

API

アプリケーション プログラミング インターフェイス（Application programming interface）。サービスへのインターフェイスを定義する関数呼び出し規定の仕様です。

B

Broadband Access Center（BAC）

ブロードバンド ホーム ネットワークの管理とプロビジョニングを行うための統合ソリューション。BAC は、大量のデバイスをサポートできるスケーラブルな製品です。

C

CPE WAN Management Protocol（CWMP）

DSL Forum の TR-069 仕様で定義されている規格。CWMP は、TR-069 で定義されている機能を統合することで、オペレータの効率を高め、ネットワーク管理の問題を軽減します。

D

Device Provisioning Engine（DPE）

DPE サーバは、デバイス命令をキャッシュし、CWMP サービスを実行します。これらの分散型サーバは、RDU と自動的に同期して最新の命令を取得し、BAC のスケーラビリティを実現します。

H

HTTPS

「Secure Sockets Layer」および「Transport Layer Security」を参照。

I

IP アドレス

IP アドレスは、インターネットにパケットで送信される情報の送信者または受信者を識別する 32 ビットの数値です。

R

Regional Distribution Unit（RDU）

RDU は BAC プロビジョニング システムの主要サーバです。デバイス命令の生成を管理し、すべての API 要求を処理し、BAC システムを管理します。

S

Secure Sockets Layer（SSL）

インターネットで秘密文書を送信するためのプロトコル。SSL は、2 つの鍵を使用してデータを暗号化する暗号システムです。1 つは全員に知らされる公開鍵で、もう 1 つはメッセージの受信者のみが知っている秘密鍵です。規定により、SSL 接続を必要とする URL は、http: の代わりに https: で始まります。BAC 3.0 は SSLv3 をサポートしています。

「Transport Layer Security」を参照してください。

T

Transport Layer Security（TLS）

インターネットで通信するクライアント/サーバ アプリケーション間のプライバシーとデータ整合性を保証するプロトコル。BAC 3.0 は TLSv1 をサポートしています。

「Secure Sockets Layer」を参照してください。

TR-069

CPE WAN Management Protocol（CWMP）を定義する規格。CPE と自動構成サーバの間の通信を可能にします。

V

Voice over IP（VoIP）

IP ベースのデータ ネットワークによる通話呼および FAX 送信を行うためのメカニズム。最適な QoS と優れた費用対効果を発揮します。

あ

アラート

問題をオペレータまたは管理者に通知する syslog または SNMP メッセージ。

暗号スイート

SSL モジュールで鍵交換、認証、およびメッセージ認証コードを実行するのに必要な暗号アルゴリズム。

う

ウォッチドッグ エージェント

ウォッチドッグ エージェントは、RDU、JRun、SNMP の各エージェントなどの BAC コンポーネント プロセスを監視、中止、開始、再開するデーモン プロセスです。

か

監査ログ

RDU データベースの大きな変更の概要が含まれているログ ファイル。システム デフォルト、テクノロジー デフォルト、サービス クラスの変更が含まれます。

完全修飾ドメイン名（FQDN）

FQDN は、ホスト名以外も含む、システムの完全名です。たとえば、cisco がホスト名で、www.cisco.com が FQDN です。

き

キャッシング　前のトランザクションで学習した情報を後のトランザクションで処理するために使用する複製の形式。

共有秘密情報　2 台のサーバまたはデバイス間で安全な通信を行うために使用する文字列。

こ

顧客宅内装置（CPE）　電話、コンピュータ、モデムなど、顧客側で用意され、インストールされる着信側機器。

し

自動構成サーバ（ACS）　単一のデバイスまたはデバイスの集合のプロビジョニングを行うサーバ。BAC では、ACS は BAC サーバを指します。場合によっては DPE を指すこともあります。

冗長性　インターネットワーキングでの、デバイス、サービス、接続などの複製。障害が発生した場合は、障害が発生したデバイス、サービス、接続の代わりに、冗長なデバイス、サービス、接続が機能を実行します。

て

テンプレート ファイル　デバイスの構成またはファームウェア ルールが記述された XML ファイル。

ね

ネットワーク アドレス変換（NAT）　グローバルに一意な IP アドレスを使用する必要性を減らすメカニズムです。NAT を使用すると、グローバルに一意でないアドレスをグローバルにルーティング可能なアドレス空間に変換することによって、このようなアドレスを持つ組織をインターネットに接続できます。

ネットワーク オペレータ　日常的にネットワークを監視および制御し、アラームの確認と対応、スループットの監視、新しい回線の構成、問題の解決などの作業を実行する人。「ネットワーク管理者」も参照。

ネットワーク管理者　ネットワークの運用、保守、および管理を担当する人。「ネットワーク オペレータ」も参照。

ネットワーク タイム プロトコル（NTP）　NTP は、ネットワークを通じてサーバ クロックを同期させるためのプロトコルです。

は

パブリッシング　プロビジョニング情報を外部データストアにリアルタイムで提供すること。データをデータストアに書き込むために、パブリッシング プラグインを開発する必要があります。

ふ

ブロードバンド　複数の独立した信号を 1 本のケーブルに多重化する転送システム。テレコミュニケーションの用語では、音声レベルのチャネル（4 kHz）を超える帯域幅のチャネルのことです。LAN の用語では、アナログ シグナリングを使用する同軸ケーブルのことです。

プロビジョニング API オペレーティング システムにさまざまな機能を実行させるために、プログラムで使用できる一連の BAC 関数。

プロビジョニング グループ 関連付けられた DPE サーバのセットが定義されているデバイスのグループ化。グループ化は、ネットワーク トポロジまたは地理的条件に基づいています。

め

命令の生成 デバイスに対するポリシー命令を RDU で生成し、それらの命令を DPE に配信するプロセス。命令は DPE によってキャッシュされ、CPE で実行する必要があるアクションについての情報が提供されます。アクションには、設定、ファームウェアのアップグレード、またはその他の操作が含まれる場合があります。

A

B

C

D

F

G

I

N

R

S

T

V

あ

う

え

か

き

く

こ

さ

し

す

せ

ち

つ

て

と

に

ね

は

ふ

ま

め

ゆ

ら

ろ