# Cisco Broadband Access Center DPE CLI リファレンス

Release 3.0

Text Part Number: OL-8639-01-J

# CONTENTS

# このマニュアルについて

『*Cisco Broadband Access Center DPE CLI リファレンス*』では、Cisco Broadband Access Center（以下、BAC）をサポートするコマンドライン インターフェイス（CLI）コマンドについて説明しています。

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、このマニュアルで使用されているスタイルと表記法を説明します。

この章には、次の項があります。



## 対象読者

このマニュアルは、BAC の Device Provisioning Engine（DPE）の CLI を使用する方を対象としています。

# マニュアルの構成

このマニュアルは、主に次の章から構成されています。

| | | |
|---|---|---|
| 第 1 章 | Broadband Access Center CLI の概要 | DPE CLI の詳細、および DPE へのアクセス方法について説明しています。 |
| 第 2 章 | システム コマンド | DPE システムのさまざまな側面を管理するために使用するコマンドについて説明します。 |
| 第 3 章 | DPE 構成のコマンド | DPE の設定に使用するコマンドについて説明しています。 |
| 第 4 章 | CWMP 技術のコマンド | CWMP 技術に関するコマンドについて説明しています。 |
| 第 5 章 | SNMP エージェントのコマンド | DPE における SNMP エージェントのプロセスに関するコマンドについて説明しています。 |
| 第 6 章 | DPE 用のログおよびデバッグ コマンド | DPE のログ管理に関するコマンドについて説明しています。 |
| 第 7 章 | CWMP 技術のデバッグ コマンド | CWMP 技術のデバッグに関するコマンドについて説明しています。 |
| 第 8 章 | サポートとトラブルシューティングのコマンド | DPE のサポートとトラブルシューティングに使用するコマンドについて説明しています。 |
| | 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<br>• 製品 CD に収録されている PDF<br>• Cisco.com 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<br>• 製品 CD に収録されている PDF<br>• Cisco.com 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<br>• Cisco.com 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<br>• Cisco.com 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

シスコの Web サイトの各国語版には、次の URL からアクセスしてください。

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 で通知されます。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）：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、シスコのチャネル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ク専門家向けの雑誌です。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 CLI の概要

この章では、コマンドライン インターフェイス（CLI）を開始して Broadband Access Center（BAC）の Device Provisioning Engine（DPE）にアクセスする方法について説明します。

## ローカル ホストからの DPE CLI へのアクセス

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

ローカル ホストから CLI にアクセスするには、次のいずれかのコマンドを使用します。

```
# telnet localhost 2323
```

または

```
# telnet 0 2323
```

# リモート ホストからの 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 サーバが実行していないことが考えられます。その場合は、サーバを起動する必要があります。サーバを起動するには、次のコマンドを入力します。

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

CLI にアクセスしたら、操作を続行する前に 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および イネーブル パスワードは、**changeme** です。

ログイン パスワードの変更方法については P.2-7 の「password」、イネーブル パスワードの変更方法については P.2-4 の「enable password」で、それぞれのコマンドを参照してください。

**例**

```
bac_host# telnet 0 2323

Trying 0.0.0.0...
Connected to 0.
Escape character is '^]'.

bac_host BAC Device Provisioning Engine


User Access Verification

Password:

bac_host> enable
Password:
bac_host#
```

CHAPTER 2

# システム コマンド

この章では、Broadband Access Center（BAC）の Device Provisioning Engine（DPE）を管理および監視するために使用するコマンドライン インターフェイス（CLI）コマンドについて説明します。

DPE 全体に作用するシステム コマンドには、次のようなものがあります。

# aaa authentication

このコマンドは、ローカル ユーザ（ログイン）認証またはリモート TACACS+ ユーザ認証を実行するように CLI を設定するときに使用します。この設定は、すべての Telnet インターフェイスおよびコンソール CLI インターフェイスに適用されます。

TACACS+ は、多数のネットワーク デバイスの中央集中型アクセス コントロール、および DPE CLI でのユーザ認証をサポートする、TCP ベースのプロトコルです。TACACS+ の使用により、DPE は TACACS+ サーバで設定された各ユーザ名、およびログイン パスワードとイネーブル パスワードを使って、複数のユーザをサポートします。

## シンタックスの説明

**aaa authentication** *mode*

*mode* には、次のいずれかを指定します。

- **local**：このモードでは、ユーザ認証はローカル ログイン経由でイネーブルになります。
- **tacacs**：このモードでは、TACACS+ サーバ リスト内の各サーバとの TACACS+ 交換が CLI によって順次に試行されます。この試行は、指定した回数だけ継続されます。プロトコル交換が成功する前にサーバ リストの最後に到達した場合は、自動的にローカル認証モードになります。したがって、TACACS+ サービスがまったく使用不可である場合でも CLI にアクセスできます。

**（注）** TACACS+ 認証では、TACACS+ で設定されたユーザ名とパスワードを入力するように求められますが、ローカル認証では、ローカルで設定されたパスワードの入力だけが求められます。

## デフォルト

デフォルトでは、CLI ユーザのログイン認証はローカル モードでイネーブルになります。

## 例

```
dpe# aaa authentication tacacs
% OK
```

# disable

このコマンドは、DPE でイネーブル モードから抜けるときに使用します。ディセーブル モードをアクティブにすると、CLI では、システム構成を表示できるコマンドだけが利用可能になります。

(注)　このコマンドは、DPE CLI がイネーブル モードになっている場合にのみ使用します。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# disable
dpe>
```

# enable

このコマンドは、イネーブル モードで DPE を入力するときに使用します。システム構成を表示するときにイネーブル モードである必要はありませんが、システムの構成、状態、およびデータを変更するときはイネーブル モードにする必要があります。

コマンドを入力すると、ローカルで設定されたイネーブル パスワードを入力するように求められます。イネーブル モードのパスワードの設定については、P.2-4 の「enable password」を参照してください。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe> enable
Password:
dpe#
```

# enable password

このコマンドは、イネーブル モードで DPE にアクセスするためのローカル パスワードを変更するときに使用します。イネーブル パスワードは、イネーブル モードでのみ変更できます。

パスワードを変更すると、その時点からどのユーザもイネーブル モードに入るために新しいパスワードの使用が要求されます。

**（注）** このコマンドを使用しても、ログイン パスワードは変更されません。ローカルのイネーブル パスワードが変わるだけです。

## シンタックスの説明

**enable password** コマンドを入力するときは、コマンドラインまたは表示されたプロンプトに対して、パスワードを指定できます。

**enable password** *password*

*password*：ローカルで設定された現在有効なパスワードを指定します。または、オプションで新しいパスワードを指定します。このパラメータを省略した場合は、パスワードを入力するように求められます。

## 例

**（注）** 例によっては、パスワードのメッセージが異なることに注意してください。

### 例 1

```
dpe# enable password
New enable password:
Retype new enable password:
Password changed successfully.
```

これは、パスワードを入力するように求められ、そのパスワードが正常に変更されたときの結果です。

### 例 2

```
dpe# enable password
New enable password:
Retype new enable password:
Sorry, passwords do not match.
```

これは、パスワードが正しく入力されなかったときの結果です。

### 例 3

```
dpe# enable password cisco
Password changed successfully
```

これは、入力を求められていないのにパスワードを入力し、そのパスワードが正常に変更されたときの結果です。

# exit

このコマンドは、DPE への Telnet 接続を閉じてログイン プロンプトに戻るときに使用します。このコマンドを実行すると、Telnet 接続が閉じられたことを示すメッセージが表示されます。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# exit
% Connection closed.
```

# help

このコマンドは、DPE CLI の使用方法に関するヘルプ画面を表示するときに使用します。特定のコマンドについてのヘルプが必要な場合は *command* **?** と入力します。利用可能なコマンドをすべて表示するには **?** と入力します。

コマンドを入力すると、画面プロンプトが表示され、ヘルプ機能の使用方法が示されます。

**コマンド タイプ**　2 種類のヘルプが用意されています。

1. コマンドの引数を入力しようとしているときは、完全なヘルプが利用できます。**show ?** のように入力すると、指定可能な引数の説明が表示されます。
2. たとえば **show c?** のように、引数の一部だけを入力し、それに相当する引数を調べたいときは、部分的なヘルプが用意されています。

**シンタックスの説明**　キーワードや引数はありません。

**例**

**（注）**　例によっては、ヘルプのメッセージが異なることに注意してください。

**例 1**

```
dpe# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. "show
?") and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to
know what arguments match the input (e.g. "show c?").
```

これは、**help** コマンドを使用したときの結果です。

### 例 2

```
dpe# show ?
  bundles          Shows the archived bundles.
  clock            Shows the current system time.
  commands         Shows the full command hierarchy.
  cpu              Shows the current CPU usage.
  device-config    Show device configuration.
  disk             Shows the current disk usage.
  dpe              Shows the status of the DPE process if started.
  files            Shows files in DPE cache.
  hostname         Shows the system hostname.
  ip               Shows IP configuration details.
  log              Shows recent log entries.
  memory           Shows the current memory usage.
  running-config   Shows the appliance configuration.
  version          Shows DPE version.
```

これは、コマンド（この例では **show ?** コマンド）に対して完全なヘルプ機能を実行したときの結果です。

### 例 3

```
dpe# show c?
clock     commands  cpu
dpe# show clock
Sat Jul 15 01:43:19 EDT 2006
```

これは、コマンド（この例では **show clock** コマンド）の引数に対して部分的なヘルプ機能を実行したときの結果です。

# password

このコマンドは、DPE へのアクセスに使用するローカル システム パスワード（DPE でイネーブル モードにアクセスするために使用するパスワードとは異なる）を変更するときに使用します。以降のログインでは、システム パスワードは、管理者アカウントを使用することによって自動的に変更されます。

**（注）** このコマンドによって変更された内容は新しいユーザには有効ですが、現在ログインしているユーザの接続は解除されません。
TACACS+ ユーザ認証を使用している場合、ローカル システム パスワードは、DPE が TACACS+ サーバと通信できないときにだけ使用されます。

## シンタックスの説明

**password** *password*

*password*：新しい DPE パスワードを表します。

## 例

### 例 1

```
dpe# password
New password:
Retype new password:
Password changed successfully.
```

これは、パスワードを入力するように求められ、そのパスワードが正常に変更されたときの結果です。

### 例 2

```
dpe# password
New password:
Retype new password:
Sorry, passwords do not match.
```

これは、パスワードが正しく入力されなかったときの結果です。

### 例 3

```
dpe# password cisco
Password changed successfully.
```

これは、パスワードが正常に変更されたときの結果です（記述の容易な方法を使用）。

# show

特定の DPE 機能に関する情報を表示するには、**show** コマンドを使用します。表 2-1 は、**show** コマンドとともに使用できる各種キーワードを一覧表示しています。

**表 2-1　show コマンドのリスト**

| コマンドの使用方法 | シンタックスの説明 | 戻り値および例 |
|---|---|---|
| **show clock** | | |
| 現在のシステムの時刻と日付を表示します。 | キーワードや引数はありません。 | `dpe# show clock`<br>`Mon Jun 16 04:21:25 EDT 2006` |
| **show commands** | | |
| 利用可能な DPE コマンドの一覧を表示します。表示されるコマンドは、使用中の接続モード（イネーブルまたはディセーブル）によって異なります。 | キーワードや引数はありません。 | **例 1**<br>`dpe> show commands`<br>`> enable`<br>`> exit`<br>`> help`<br>`> show bundles`<br>`> show clock`<br>`> show commands`<br>`> show cpu`<br>`> show disk`<br>`> show dpe`<br>`> show dpe config`<br>`> show files`<br>`> show hostname`<br>`> show ip`<br>`> show ip route`<br>`> show log`<br>`> show log last <1..9999>`<br>`> show memory`<br>`> show running-config`<br>`> show version`<br>`> uptime`<br>これは、ディセーブル モードでの結果です。<br>**（注）** ここでは、出力例の一部のみ紹介しています。<br>**例 2**<br>`dpe# show commands`<br>`> aaa authentication local`<br>`> aaa authentication tacacs`<br>`> clear bundles`<br>`> clear cache`<br>`> debug dpe cache`<br>`> debug dpe connection`<br>`> debug dpe dpe-server`<br>`> debug dpe statistics`<br>`> debug on`<br>`> debug service cwmp 1 client-auth-all`<br>`> debug service cwmp 1 client-auth-failures`<br>`> debug service cwmp 1 extension`<br>`> debug service cwmp 1 firmware`<br>`[more]`<br>これは、イネーブル モードでの結果です。 |

**表 2-1　show コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 戻り値および例 |
|---|---|---|
| **show cpu** | | |
| DPE が実行されているデバイスの CPU 使用状況を表します。コマンドを入力すると、CPU のアクティビティと統計が表示されます。 | キーワードや引数はありません。 | **show cpu** を入力すると、DPE から、プロセッサごとの統計が次のヘッダーで定義された表形式で返されます。<br>**（注）** 特に記載のない限り、すべての値の単位は秒あたりのイベント数です。<br>• CPU：プロセッサ ID。<br>• minf：軽度の障害。<br>• mjf：重度の障害。<br>• xcal：プロセッサ間の相互呼び出し。<br>• intr：割り込み。<br>• ithr：スレッド割り込み（クロック割り込みはカウントしません）。<br>• csw：コンテキスト スイッチ。<br>• icsw：非自発的なコンテキスト スイッチ。<br>• migr：スレッド移行（別のプロセッサへ）。<br>• smtx：ミューテックスのスピン。<br>• srw：リーダーまたはライターのスピン ロック。<br>• syscl：システム コール。<br>• usr：ユーザ時間（%）。<br>• sys：システム時間（%）。<br>• wt：待ち時間（%）。<br>• idl：アイドル時間（%）。 |
| **show disk** | | |
| DPE が現在使用しているディスクを表します。コマンドを入力すると、ディスク ドライブ統計が表示されます。 | キーワードや引数はありません。 | **show disk** を入力すると、DPE は次のヘッダーの値を返します。<br>• Filesystem：ファイル システムのパスを示します。<br>• Size：ファイル システムのサイズ（KB）を示します。<br>• Used：使用済みのディスク領域（KB）を示します。<br>• Avail：使用可能なディスク領域（KB）を示します。<br>• Capacity：ディスクの容量（%）を示します。<br>• Mounted on：ファイル システムが搭載されているリソースを示します。通常、リソースはディレクトリです。 |

表 2-1　show コマンドのリスト（続き）

| コマンドの使用方法 | シンタックスの説明 | 戻り値および例 |
|---|---|---|
| **show files** | | |
| DPE にキャッシュされている外部ファイルを表します。 | キーワードや引数はありません。 | dpe# **show files**<br><br>The list of files currently in DPE cache<br><br>filename　　size<br><br>sample-firmware-image.bin　　4239368<br><br>DPE caching 1 external files.<br>Listing the first 1 files, 0 files omitted |
| **show hostname** | | |
| DPE ホスト名を表示します。 | キーワードや引数はありません。 | dpe# **show hostname**<br>hostname = BAC_host |
| **show ip** | | |
| DPE の現在の一般的な IP 設定を表示します。これらは DPE のリブート時に使用される設定です。 | キーワードや引数はありません。 | dpe# **show ip**<br>hostname = BAC_host<br>domainname = abc.com<br>gateway = 10.10.20.10 |

**表 2-1　show コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 戻り値および例 |
|---|---|---|
| **show ip route** | | |
| DPE の IP ルーティング テーブル（すべてのカスタム ルートを含む）を表示します。デフォルト ゲートウェイには、フラグ列で G フラグが付けられています。 | キーワードや引数はありません。 | **show ip route** を入力すると、DPE から次のヘッダーの値を持つルーティング テーブルが返されます。<br>• Destination：宛先ネットワークまたは宛先ホストを示します。<br>• Mask：ルートに関連付けられたサブネット マスクを示します。<br>• Gateway：発信インターフェイスのアドレスを示します。<br>• Device：ルートに使用されるネットワーク インターフェイスを示します。<br>• Mxfrg：パスの最大転送単位を示します。<br>• Rtt：ルートが有効期限切れになる前に残されている時間（分単位）を示します。<br>• Ref：現在アクティブなルートの使用数を示します。<br>• Flg：ルートの状態を示します。次のとおりです。<br>— U：上へ。<br>— H：ネットワークではなく、ホストへ。<br>— G：ゲートウェイへ。<br>• Out：このインターフェイスまたはルートから送出されるパケットの数を表します。<br>• In/Fwd：このインターフェイスまたはルートで受信されるパケットの数を表します。 |

表 2-1　show コマンドのリスト（続き）

| コマンドの使用方法 | シンタックスの説明 | 戻り値および例 |
|---|---|---|
| **show memory** | | |
| DPE が実行されているデバイスで現在使用可能なメモリおよびスワップ領域を表します。 | キーワードや引数はありません。 | **show memory** を入力すると、次のヘッダーに対する値が DPE から返されます。<br>• kthr：次の 3 つの状態のそれぞれにおけるカーネル スレッドの数を示します。<br>— r：キューの実行。<br>— b：入出力の待機中にブロックされたプロセス。<br>— w：スワップされたアイドル プロセス。<br>• memory：仮想メモリおよび実メモリの使用状況を示します。これには、次のようなものがあります。<br>— swap：確保されていない空きスワップ領域（KB）。<br>— free：空きメモリ（KB）。<br>• page：ページ障害およびページング　アクティビティを示します（秒単位）。<br>— re：空きリストから再要求されるページを表示します。<br>— mf：軽度の障害を表示します。<br>— pi：メモリ内のページを表示します（KB/秒）。<br>— po：メモリ外のページを表示します（KB/ 秒）。<br>— fr：開放されたページ　スキャナのアクティビティを表示します（KB/ 秒）。<br>— de：書き込み後に開放されたページを表示します（KB/ 秒）。<br>— sr：スキャンされたページの数を表示します（ページ単位）。<br>• disk：1 秒当たりのディスク処理数を示します。S 列は、システム上の異なるディスクを表します。<br>• faults：トラップ レートまたは割り込みレートを示します（秒単位）。<br>— /in：割り込み。<br>— sy：システム コール。<br>— cs：コンテキスト スイッチ。<br>• cpu：CPU 時間の使用状況を示します。<br>— us：ユーザ時間（%）。<br>— sy：システム時間（%）。<br>— id：アイドル時間（%）。 |

**表 2-1　show コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 戻り値および例 |
|---|---|---|
| **show running-config** | | |
| DPE の現在の設定を表示します。オプションを設定する実際のコマンドを使用すると、すべての設定オプションが表示されます。 | キーワードや引数はありません。 | dpe# **show running-config**<br>dpe port 49186<br>dpe rdu-server server_x.cisco.com 49187<br>service cwmp 1 client-auth digest<br>service cwmp 1 enabled true<br>service cwmp 1 port 7547<br>service cwmp 1 ssl cipher<br>all-cipher-suites<br><br>**（注）** ここでは、出力例の一部のみ紹介しています。 |
| **show version** | | |
| DPE ソフトウェアの現在のバージョンを表します。 | キーワードや引数はありません。 | dpe# **show version**<br>Version: BAC 3.0 (bac_30_S_000000000000) |

# tacacs-server host

このコマンドは、TACACS+ クライアントの TACACS+ サーバ リストの末尾に TACACS+ サーバを追加するときに使用します。TACACS+ 認証がイネーブルの場合、クライアントは、リストされている順序で各サーバへのユーザ ログイン認証を試行します。この試行は、認証交換が成功するまで、またはリストの最後に到達するまで継続されます。リストの最後に到達した場合、クライアントは自動的にローカル認証モードに戻ります（ローカル システム パスワードを使用）。

オプションで、各 TACACS+ サーバごとに暗号キーを指定できます。この暗号キーを使用する場合、暗号キーは、指定した TACACS+ サーバで設定されているキーと一致する必要があります。暗号キーを省略すると、TACACS+ 暗号化はディセーブルになります。

CLI の TACACS+ サーバ リストから TACACS+ サーバを削除するには、このコマンドの **no** 形式を使用します。詳細については、P.2-15 の「no tacacs-server host」を参照してください。

## シンタックスの説明

**tacacs-server host** *host* [**key** *encryption-key*]

- *host*：TACACS+ サーバの IP アドレスまたはホスト名のいずれかを指定します。
- *encryption-key*：実際の暗号キーを表します。

## 例

### 例 1

次の例では、IP アドレス（10.0.1.1）を使用し、暗号化なしで TACACS+ サーバを追加しています。

```
dpe# tacacs-server host 10.0.1.1
% OK
```

### 例 2

次の例では、IP アドレス（10.0.1.1）を使用し、暗号キー（hg667YHHj）を指定して TACACS+ サーバを追加しています。

```
dpe# tacacs-server host 10.0.1.1 key hg667YHHj
% OK
```

### 例 3

次の例では、ホスト名（tacacs1.cisco.com）を使用し、暗号化なしで TACACS+ サーバを追加しています。

```
dpe# tacacs-server host tacacs1.cisco.com
% OK
```

### 例 4

次の例では、ホスト名（tacacs1.cisco.com）を使用し、暗号キー（hg667YHHj）を指定して TACACS+ サーバを追加しています。

```
dpe# tacacs-server host tacacs1.cisco.com key hg667YHHj
% OK
```

# no tacacs-server host

このコマンドは、CLI の TACACS+ サーバ リストから TACACS+ サーバを削除するときに使用します。

**シンタックスの説明**　**no tacacs-server host** *host*

*host*：TACACS+ サーバの IP アドレスまたはホスト名を指定します。

**例**

**例 1**

次の例では、IP アドレスを使用して TACACS+ サーバを削除しています。

```
dpe# no tacacs-server host 10.0.1.1
% OK
```

**例 2**

次の例では、ホスト名を使用して TACACS+ サーバを削除しています。

```
dpe# no tacacs-server host tacacs1.abc.com
% OK
```

# tacacs-server retries

このコマンドは、特定の TACACS+ サーバを到達不能であると TACACS+ クライアントが見なすまで実行される TACACS+ プロトコル交換のリトライ回数を設定するときに使用します。この制限に達すると、TACACS+ クライアントは TACACS+ サーバ リストの次のサーバに進みます。または、TACACS+ リストの最後に到達した場合は、ローカル認証に戻ります。

**シンタックスの説明**　**tacacs-server retries** *value*

*value*：1 ～ 100 の無次元数を指定します。

**（注）**　この値はすべての TACACS+ サーバに適用されます。

**デフォルト**

特定の TACACS+ サーバが到達不能であると TACACS+ クライアントが見なすまで、TACACS+ プロトコル交換がリトライされる回数は、デフォルトでは 2 に設定されています。

**例**

```
dpe# tacacs-server retries 10
% OK
```

# tacacs-server timeout

このコマンドは、プロトコル交換が失敗したと見なすまで TACACS+ クライアントが TACACS+ サーバの応答を待機する最大時間を設定するときに使用します。

**シンタックスの説明**　**tacacs-server timeout** *value*

*value*：CLI が待機する期間を指定します。この値の有効範囲は 1 ～ 300 秒です。

**（注）**　この値はすべての TACACS+ サーバに適用されます。

**デフォルト**　タイムアウトになるまで CLI が TACACS+ サーバの応答を待機する最大時間です。デフォルトでは 5 秒です。

**例**

```
dpe# tacacs-server timeout 10
% OK
```

# uptime

このコマンドは、システムの稼動時間の長さを表示するときに使用します。この情報は、デバイスがリブートする頻度を測定するときに役立ちます。また、安定した状態での DPE の信頼性をチェックするときにも有用です。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# uptime
11:42pm  up 72 day(s),  8:02,  1 user,  load average: 0.00, 0.02, 0.02
```

CHAPTER 3

# DPE 構成のコマンド

この章では、Broadband Access Center（BAC）の Device Provisioning Engine（DPE）を管理および監視するために使用するコマンドライン インターフェイス（CLI）コマンドについて説明します。

この章で説明するコマンドは、次のとおりです。

# clear cache

このコマンドは、DPE キャッシュ全体を消去して、サーバをクリーンな状態にリセットするときに使用します。DPE を再起動すると、RDU に接続されて、RDU データベースに格納されている情報を基にキャッシュが再作成されます。

**（注）** DPE キャッシュを消去する前に、**dpe stop** コマンドを実行して必ず DPE を停止してください。詳細については、P.3-7 の「dpe start | stop」を参照してください。

DPE で大きな問題が発生したときは、キャッシュをクリアするだけです。このコマンドを実行すると、自動的に DPE のデバイス キャッシュが再作成されるか、キャッシュへの読み込みが再開されます。このプロセスは、完了までに長時間かかる場合があります。

コマンドを入力すると、DPE キャッシュがクリアされ、その結果クリアになったディスク領域の大きさを示すプロンプトが表示されます。キャッシュがクリアできなかった場合は、失敗の理由が表示されます。

## シンタックスの説明

キーワードや引数はありません。

## 例

### 例 1

```
dpe# clear cache
Clearing DPE cache...
+ 417792 bytes cleared.
```

これは、キャッシュが正常にクリアされたときの結果です。

### 例 2

```
dpe# clear cache
DPE must be stopped before clearing cache.
```

これは、DPE が停止されていなかったときの結果です。

### 例 3

```
dpe# clear cache
Clearing DPE cache...
+ Cache already cleared.
```

これは、キャッシュがすでにクリアされていたときの結果です。

# dpe port

このコマンドは、CLI サーバが DPE と通信するためのポートを指定するときに使用します。

**(注)** ポート番号を変更する前に、DPE を停止する必要があります。稼動中の DPE でこのコマンドを実行しようとすると、次のエラー メッセージが表示されます。

```
ERROR: DPE must be stopped before changing the port number.
```

このコマンドによって変更された内容を有効にするには、DPE を再起動する必要があります。DPE の起動と停止については、P.3-7 の「dpe start | stop」を参照してください。

## シンタックスの説明

**dpe port** *port*

*port*：DPE への接続用に割り当てられたポート番号を表します。

## デフォルト

DPE が使用するポートは、デフォルトでは 49186 です。

## 例

```
dpe# dpe port 49186
% OK
```

# dpe provisioning-group primary

このコマンドは、特定のプライマリ プロビジョニング グループのメンバとして DPE を指定するときに使用します。ほとんどの DPE は単一のプライマリ プロビジョニング グループを使用して構成されますが、複数のプロビジョニング グループを選択すると、複数の DHCP サーバでこの DPE を使用できるようになります。

デバイス数の多い新しいプロビジョニング グループを割り当てたときに、ネットワーク内のデバイス数およびデバイス構成のサイズによっては、DPE を再起動するのに長時間かかる場合があります。これは、各プロビジョニング グループではキャッシュの同期化、新しいプロビジョニング グループではキャッシュの完全な再作成が必要なためです。

**（注）** 通常の状況では、プロビジョニング グループは、DPE が最初にネットワーク上に配置されたときにのみ変更する必要があります。

このコマンドを使用したときは、このコマンドの後に **dpe reload** コマンドを実行して、変更内容を有効にしてください。詳細については、P.3-6 の「dpe reload」を参照してください。

構成されたプライマリ プロビジョニング グループを削除するには、このコマンドの **no** 形式を使用します。詳細については、P.3-5 の「no dpe provisioning-group primary」を参照してください。

## シンタックスの説明

**dpe provisioning-group primary** *name* [*name**]

- *name*：割り当てられたプライマリ プロビジョニング グループを表します。
- *name**：複数のプロビジョニング グループのエントリを許可します。複数のプロビジョニング グループを指定するときは、名前の間にスペースを挿入する必要があります。

**（注）** 配置済みのテクノロジーによっては、DPE が所属できるプロビジョニング グループを 1 つ以上指定できる場合があります。この BAC のリリースでは、DPE を 1 つのプロビジョニング グループに指定することを要求する CWMP 技術のみがサポートされます。

## 例

### 例 1

```
dpe# dpe provisioning-group primary PrimaryProvGroup
% OK (Requires DPE restart "# dpe reload")
```

### 例 2

```
dpe# dpe provisioning-group primary provisioning-grp-1 provisioning-grp-2
% OK (Requires DPE restart "# dpe reload")
```

# no dpe provisioning-group primary

このコマンドは、構成されたプライマリ プロビジョニング グループをクリアするときに使用します。プライマリ プロビジョニング グループが利用できない場合、他のプロビジョニング グループのバックアップまたは TFTP ファイル キャッシュとして、DPE を使用することができます。

このコマンドを使用したときは、このコマンドの後に **dpe reload** コマンドを実行して、変更内容を有効にしてください。詳細については、P.3-6 の「dpe reload」を参照してください。

DPE サーバで使用されるプライマリ プロビジョニング グループを設定するには、P.3-4 の「dpe provisioning-group primary」を使用します。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# no dpe provisioning-group primary
% OK (Requires DPE restart "# dpe reload")
```

# dpe rdu-server

このコマンドは、この DPE が接続される RDU を表示するときに使用します。通常、RDU はデフォルトのポートに設定しますが、セキュリティ上の理由から、RDU を非デフォルトのポートで実行するように設定することもできます。

このコマンドを使用したときは、このコマンドの後に **dpe reload** コマンドを実行して、変更内容を有効にしてください。詳細については、P.3-6 の「dpe reload」を参照してください。

**シンタックスの説明**　**dpe rdu-server** *{host | ip} port*

- *host*：RDU が実行されているホストの完全修飾ドメイン名を表します。
- *ip*：RDU の IP アドレスを表します。
- *port*：DPE との接続に使用される RDU のリスニング ポート番号（デフォルトでは 49187）を表します。

**例**

**例 1**

```
dpe# dpe rdu-server rdu.cisco.com 49187
% OK (Requires DPE restart "# dpe reload")
```

これは、RDU ホストの完全修飾ドメイン名を指定したときの結果です。

**例 2**

```
dpe# dpe rdu-server 10.10.20.1 49187
% OK (Requires DPE restart "# dpe reload")
```

これは、RDU ホストの IP アドレスを指定したときの結果です。

# dpe reload

このコマンドは、DPE を再起動するときに使用します。DPE は、リロード オペレーションを行う前に実行されている必要があります。DPE が 60 秒以内に停止されていない場合、BAC プロセス ウォッチドッグ（bprAgent）によって DPE が自動的に停止され、その旨を伝えるアラート メッセージが表示されます。メッセージが表示された後、DPE が再起動します。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# dpe reload
Process dpe has been restarted
```

# dpe shared-secret

このコマンドは、RDU との通信に必要な共有秘密情報を設定するときに使用します。2 台のサーバで設定された共有秘密情報が一致しない場合、通信は失敗します。

このコマンドを使用したときは、このコマンドの後に **dpe reload** コマンドを実行して、変更内容を有効にしてください。詳細については、P.3-6 の「dpe reload」を参照してください。

**シンタックスの説明**　**dpe shared-secret** *secret*

*secret*：RDU の共有秘密を表します。

**デフォルト**　RDU との通信に必要なデフォルトの共有秘密情報は、**secret** です。

**例**

```
dpe# dpe shared-secret private
% OK (Requires DPE restart "# dpe reload")
```

# dpe start | stop

このコマンドは、DPE を起動または停止するときに使用します。

**シンタックスの説明**

```
dpe start | stop
```

- **start**：DPE を起動します。このコマンドは、DPE が実行されていないときにのみ使用できます。DPE を正常に起動しても、DPE が正常に実行されるという保証はありません。DPE ログをチェックして、DPE が正しく起動されたことを確認します。さらに、ログを定期的にチェックして、別のエラーが発生していないかどうかを確認します。
- **stop**：DPE を停止します。このコマンドは、DPE が実行されているときにのみ使用できます。DPE が 60 秒以内に停止されていない場合、DPE エージェントによって DPE が自動的に停止され、その旨を伝えるアラート メッセージが表示されます。

**例**

**例 1**

```
dpe# dpe start
Process dpe has been started
```

**例 1**

```
dpe# dpe stop
dpe is stopped
```

# interface ethernet provisioning enabled

このコマンドは、イーサネットのインターフェイスをプロビジョニング要求の処理に使用するかどうかを制御するときに使用します。このコマンドにより、DPE による RDU とのインタラクションが、CPE とのインタラクションから分離されます。具体的には、イネーブル化されたインターフェイスの完全修飾ドメイン名が、CPE デバイスが実行するファイルのダウンロード用 URL として設定されます（FQDN の設定については、P.3-8 の「interface ethernet provisioning fqdn」を参照してください）。

このコマンドを使用したときは、このコマンドの後に **reload** コマンドを実行して、変更内容を有効にしてください。詳細については、P.3-6 の「dpe reload」を参照してください。

**シンタックスの説明**

```
interface ethernet {intf0 | intf1} provisioning enabled {true | false}
```

- *intf0* | *intf1*：イーサネットのインターフェイスを表します。
- **true**：イネーブルになっているプロビジョニングを示します。
- **false**：ディセーブルになっているプロビジョニングを示します。

**デフォルト**

イーサネット インターフェイスのプロビジョニング操作は、デフォルトではディセーブルになっています。

**例**

```
dpe# interface ethernet hme0 provisioning enabled true
% OK (Requires DPE restart "# dpe reload")
```

# interface ethernet provisioning fqdn

このコマンドは、特定のインターフェイスに完全修飾ドメイン名（FQDN）を設定するときに使用します。プロビジョニング FQDN は、特定の DPE インターフェイスを接続するために CPE デバイスに設定する FQDN です。CWMP では、RDU のプロビジョニング グループ オブジェクトで異なる値が設定されている場合を除き、この FQDN は CPE のリダイレクト（または同等の）機能を実行するときに、自動構成サーバの URL を作成するために使用されます。

**（注）** 特定のプロビジョニング グループ内では、すべての DPE に必ず同一の FQDN を使用してください。DPE がロード バランサの背後にある場合は、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、同じロード バランサ グループの一部であるすべての DPE で、この FQDN が同一であることを確認してください。

インターフェイスに FQDN を設定する前に、このインターフェイスでプロビジョニングがイネーブルになっていることを確認してください。インターフェイス上でプロビジョニングをイネーブルにするには、P.3-7 の「interface ethernet provisioning enabled」を参照してください。

このコマンドを使用したときは、このコマンドの後に **reload** コマンドを実行して、変更内容を有効にする必要があります。詳細については、P.3-6 の「dpe reload」を参照してください。

**シンタックスの説明**

**interface ethernet** {*intf0* | *intf1*} **provisioning fqdn** *fqdn*

- *intf0* | *intf1*：イーサネットのインターフェイスを表します。
- *fqdn*：特定のインターフェイスに設定される完全修飾ドメイン名を表します。

**例**

```
dpe# interface ethernet hme0 provisioning fqdn cisco.com
% OK (Requires DPE restart "> dpe reload")
```

# show device-config

このコマンドは、DPE にキャッシュされたデバイス構成を表示するときに使用します。

このコマンドをライセンスのない DPE で実行した場合は、次のようなメッセージが表示されます。

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for a DPE license.
```

## シンタックスの説明

**show device-config** *device-ID*

*device-ID*：デバイスを表します。

## 例

この使用例の目的上、デバイスの ID を *0014XX-XXX000000001* と仮定します。

```
dpe# dpe show device-config 0014XX-XXX000000001
HTTP configuration for device 0014XX-XXX000000001 in default provisioning-group:

   HTTP Configuration
       Instruction records:

          HttpAuthRecord :
             IS_PERSISTENT : true
             IS_AUTO_RUN : true
             USERNAME : 0014XX-XXX000000001
             PASSWORD : <value is set>

          RoutableIPAddressRecord :
             OPERATION_ID : 3c342b:10a8f88a32c:80000042
             UPDATE_IP : false
             HAS_ROUTABLE_IP : null

          Data Synchronization Instruction :
             IS_PERSISTENT : true
             IS_AUTO_RUN : true
             DATA_SYNC_PARAMS :
                InternetGatewayDevice.DeviceInfo.SoftwareVersion : null
                Inform.DeviceId.ProductClass : null
                Inform.DeviceId.ManufacturerOUI : null
                InternetGatewayDevice.DeviceInfo.HardwareVersion : null
                InternetGatewayDevice.ManagementServer.ParameterKey : null
                Inform.DeviceId.Manufacturer : null
                InternetGatewayDevice.DeviceInfo.ModelName : null
             FIRMWARE_CHANGED_PARAMS :
                InternetGatewayDevice.DeviceInfo.ModelName

          Firmware Rules Instruction :
             IS_PERSISTENT : true
             FIRMWARE_RULES :
             version : 1.0
             CwmpFirmwareRules :
                CwmpFirmwareRule: AcmeWAG54G2Rule
                   Expressions :
                         CwmpExpression:
                            Parameter : null
                            InformParameter : Inform.EventCode
                            RpcArgument : null
                            Value : [1 BOOT, 2 PERIODIC]
                            Operator : match
```

```
                              CwmpExpression:
                                 Parameter : InternetGatewayDevice.DeviceInfo.SoftwareVersion
                                  InformParameter : null
                                  RpcArgument : null
                                  Value : [66]
                                  Operator : matchAllIgnoreCase
                        InternalFile :
                           FirmwareFile : sample-firmware-image.bin
                           FileDeliveryTransport : HTTP
                  FORCE_FIRMWARE_UPGRADE : false

            Configuration Synchronization Instruction :
               OPERATION_ID : 3c342b:10a8f88a32c:80000043
               IS_PERSISTENT : true
               CONFIG :
                  version : 1.0
                  CwmpParameter :
                     fullName :
InternetGatewayDevice.ManagementServer.PeriodicInformEnable
                     value : true
                     type : boolean
                     notification : 0
                  CwmpParameter :
                     fullName :
InternetGatewayDevice.ManagementServer.PeriodicInformInterval
                     value : 86400
                     type : unsignedInt
                     notification : 0
               CONFIG_REV_NUMBER : 559207259
               FORCE_CONFIG_UPGRADE : false

      Real Time Proxy Operations:
          Instruction records:

            No instruction found.
```

# show dpe

このコマンドは、DPE が実行されているかどうかをチェックするときに使用します。結果として、プロセスの状態および稼動の統計（実行されている場合）が表示されます。このコマンドによって、DPE が正常に実行されているかどうかは確認できません。プロセスが実行されているかどうかのみ示されます。ただし、DPE が実行されているときには、このコマンドが出力する統計を使用して、DPE によって要求が正常にサービスされているかどうかを確認できます。

このコマンドをライセンスのない DPE で実行した場合は、次のようなメッセージが表示されます。

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for a DPE license.
```

**シンタックスの説明**　キーワードや引数はありません。

**例**

**例 1**

```
dpe# show dpe
BAC Agent is running
Process dpe is not running
```

これは、DPE が実行されていないときの結果です。

**例 2**

```
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.
```

これは、DPE が実行されているときの結果です。

# show dpe config

このコマンドは、現在の DPE 設定を表示するときに使用します。コマンドを入力すると、DPE の構成が表示されます。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# show dpe config
dpe port          = 49186
rdu host          = host.abc.com
rdu port          = 49187
primary groups    = default
secondary groups = [no value]
```

CHAPTER 4

# CWMP 技術のコマンド

この章では、Broadband Access Center（BAC）の Device Provisioning Engine（DPE）上の CPE WAN 管理プロトコル（CWMP）技術を管理および監視するために使用する、コマンドライン インターフェイス（CLI）コマンドについて説明します。

この章で説明するコマンドを使用すると、DPE で CWMP サービスおよび HTTP ファイル サービスの設定を構成できます。どちらのサービスにもサービス 1 および サービス 2 という独自のインスタンスがあります。これらのインスタンスは、個別に設定する必要があります。

サービスごとに異なるオプションを設定できるよう、BAC は異なるインスタンスをサポートします。たとえば CWMP サービス 1 は、デフォルトでは HTTP ダイジェスト認証を要求するように設定されていますが、HTTP over SSL/TLS はサポートしていません。このサービスは、ポート 7547 で実行されるように設定されており、デフォルトではイネーブルになっています。CWMP サービス 2 は、HTTP over SSL/TLS を使用するポート 7547 で実行されるよう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。実際の要件に合わせて、各サービスのこれらのデフォルトを再設定できます。各サービスのデフォルト設定については、表 4-1 を参照してください。

**表 4-1　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** | **サービス 1** | **サービス 2** |
| 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 | ダイジェスト | ダイジェスト | ダイジェスト | ダイジェスト |
| ポート番号 | 7547 | 7548 | 7549 | 7550 |
| SSL/TLS 上での HTTP | ディセーブル | イネーブル | ディセーブル | イネーブル |

**（注）** CWMP 関連サービスを、グローバルにイネーブルまたはディセーブルにすることはできません。CWMP 機能は、個別でのみイネーブルまたはディセーブルにできます。

この章で説明するコマンドは、次のとおりです。

# service cwmp

これは、DPE で実行されている CWMP サービスに対してさまざまな設定を構成するときに使用するコマンドのグローバル構文です。これらのコマンドを使用すると、次のことが可能です。

- CWMP サービスをイネーブルにする
- サービスのインスタンスを指定する
- クライアント認証およびクライアント証明書認証を設定する
- サービスのポート番号を設定する
- SSL/TLS 上で HTTP を使用するようにサービスを設定する

**service cwmp** は、表 4-2 に記載されているコマンドと併せて使用してください。

**（注）** これらのコマンドを使用するときは、特に記載のない限り、DPE を再起動して変更内容を有効にする必要があります。DPE を再起動するには、**dpe reload** コマンドを実行します（P.3-6 の「dpe reload」を参照してください）。

**表 4-2　service cwmp コマンドのリスト**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service cwmp** *num* **allow-unknown-cpe**<br><br>**no service cwmp** *num* **allow-unknown-cpe** | | |
| DPE で不明なデバイスに対して DPE が RDU に構成要求することをイネーブルまたはディセーブルにします。<br><br>**（注）** この機能をイネーブル化すると、RDU に対する DoS 攻撃が可能になる場合があります。このコマンドを有効にするために、DPE を再起動する必要はありません。 | *num*：CWMP サービス（1 または 2）を表します。 | `dpe# service cwmp 1 allow-unknown-cpe`<br>`% OK` |

**表 4-2　service cwmp コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service cwmp** *num* **client-auth** *mode* | | |
| DPE 上の CWMP サービスに対して HTTP を使用することにより、クライアント認証をイネーブルまたはディセーブルにします。<br><br>BAC の認証オプションのリストについては、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | • *num*：CWMP サービス（1 または 2）を表します。<br>• *mode*：CWMP サービスのクライアント認証モードを表します。クライアント認証モードには、次のようなものがあります。<br>— **basic**：基本 HTTP 認証をイネーブルにします。<br>— **digest**：ダイジェスト HTTP 認証をイネーブルにします。これがデフォルトの設定です。<br>— **none**：基本およびダイジェスト認証をディセーブルにします。このモードでは、CWMP サービスは Inform メッセージ内の Device ID を使用して CPE を認証します。<br><br>**（注）** クライアント認証中のセキュリティ リスクを制限するため、ダイジェストモード（デフォルト設定）を使用することをお勧めします。基本モードでクライアント認証を許可したり、基本およびダイジェスト認証を完全にディセーブルにしたりすることは推奨されていません。 | `dpe# service cwmp 1 client-auth digest`<br>`% OK (Digest authentication was enabled. Basic authentication was disabled. Requires DPE restart "# dpe reload")` |
| **service cwmp** *num* **enable {true \| false}** | | |
| DPE 上で実行されている CWMP サービスをイネーブルまたはディセーブルにします。 | • *num*：CWMP サービス（1 または 2）を表します。<br>デフォルトでは、CWMP サービスは次のようになっています。<br>— サービス 1 ではイネーブル。<br>— サービス 2 ではディセーブル。<br>• **true**：CWMP サービスをイネーブルにします。<br>• **false**：CWMP サービスをディセーブルにします。 | `dpe# service cwmp 2 enable true`<br>`% OK (Requires DPE restart "# dpe reload")` |
| **service cwmp** *num* **port** *port* | | |
| CWMP サービスが CPE と通信するポートを表します。異なるポート番号を指定することにより、DPE が、他のアプリケーションによって使用されるポート間の共有違反を回避できるようになります。 | • *num*：CWMP サービス（1 または 2）を表します。<br>• *port*：サービスが使用するポート番号を表します。<br>デフォルトでは、CWMP サービスは次のポートで受信するように設定されています。<br>— サービス 1 の場合はポート 7547。<br>— サービス 2 の場合はポート 7548。 | `dpe# service cwmp 1 port 7547`<br>`% OK (Requires DPE restart "# dpe reload")` |

**表 4-2　service cwmp コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service cwmp session timeout** *value* | | |
| CWMP セッションのタイムアウト期間を設定します。<br><br>**（注）** このコマンドを有効にするために、DPE を再起動する必要はありません。 | *value*：CWMP セッションのタイムアウト期間をミリ秒（ms）で表します。タイムアウト期間は、1000 ms（1 秒）から 3000000 ms（50 分）までの任意の値です。<br><br>デフォルトでは、タイムアウト期間は 60000 ms（60 秒）に設定されています。 | dpe# **service cwmp session timeout 60000**<br>% OK |
| **service cwmp** *num* **ssl client-auth** *mode* | | |
| DPE 上で実行されている CWMP サービスに対して HTTP over SSL/TLS を使用することにより、クライアント証明書認証をイネーブルまたはディセーブルにします。<br><br>BAC の認証オプションのリストについては、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | • *num*：CWMP サービス（1 または 2）を表します。<br>デフォルトでは、SSL/TLS でのクライアント証明書認証は次のようになっています。<br>— サービス 1 ではディセーブル。<br>— サービス 2 ではディセーブル。<br>• *mode*：CWMP サービスのクライアント証明書認証モードを表します。BAC のサポート対象は、次のとおりです。<br>— **client-cert-generic**：すべての CPE または CPE の大きなサブセットに共通の汎用証明書を使用して、SSL/TLS でクライアント証明書認証をイネーブルにします。クライアント証明書は、署名認証局の公開鍵を使用して認証されます。この鍵は、DPE キーストアで事前設定されます。この証明書認証プロセスにより、証明書が有効であることが確認されますが、特定デバイスの ID は確立されません。したがって、デバイスの識別情報は、クライアント証明書の CN フィールド内のデータを使用することによっては生成されません。その代わり、デバイスの識別情報は基本またはダイジェスト認証経由で提供されたデータ、または CWMP Inform メッセージ内のデータを使用することによって生成されます。<br>— **client-cert-unique**：各 CPE が提供する一意の証明書を使用して、SSL/TLS で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認証されると、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固有識別情報が生成されます。<br>— **none**：CWMP サービスに対して HTTP over SSL/TLS を使用して、クライアント証明書認証をディセーブルにします。 | **例 1**<br>dpe# **service cwmp 1 ssl client-auth client-cert-generic**<br>% OK (Requires DPE restart "# dpe reload")<br><br>**例 2**<br>dpe# **service cwmp 1 ssl client-auth client-cert-unique**<br>% OK (Requires DPE restart "# dpe reload") |

**表 4-2　service cwmp コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service cwmp** *num* **ssl client-auth client-cert-css-ext** | | |
| HTTP over SSL/TLS を使用する接続が Cisco CSS 11500 シリーズ Content Services Switch（CSS 11500）で終端している CPE の、認証をイネーブルにします。下流 CSS は、CPE デバイスから SSL セッションに関する情報（特にクライアント証明書フィールド）を取り出し、そのデータをさまざまな HTTP ヘッダーに挿入します。その後 BAC は、CSS ヘッダーの ClientCert-Subject-CN から CN フィールドを取得して、固有のデバイス識別情報を作成します。<br><br>**（注）** このコマンドをイネーブルにする前に、必ず CSS を設定して、クライアント証明書フィールドを HTTP ヘッダーに挿入してください。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。<br><br>BAC の認証オプションのリストについては、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | *num*：CWMP サービス（1 または 2）を表します。<br><br>デフォルトでは、CWMP サービスに対して HTTP over SSL/TLS を使用するクライアント証明書認証は、次のようになっています。<br>• サービス 1 ではディセーブル。<br>• サービス 2 ではディセーブル。 | dpe# **service cwmp ssl 1 client-auth client-cert-css-ext**<br>% OK (Requires DPE restart "# dpe reload") |

**表 4-2　service cwmp コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service cwmp** *num* **ssl cipher {all-cipher-suites \| *value*}**<br><br>**no service cwmp** *num* **ssl cipher {all-cipher-suites \| *value*}** | | |
| 暗号アルゴリズムまたは暗号を使用して、DPE サーバと CPE の間の認証をイネーブルまたはディセーブルにします。これらの暗号アルゴリズムまたは暗号は、証明書管理およびセッション管理用に、HTTP over SSL/TLS によってサポートされています。SSL ハンドシェイク中、DPE サーバと CPE デバイスは、これら両方でイネーブルになっている最も強い暗号スイートを特定し、SSL セッションでそのスイートを使用します。<br><br>**（注）** BAC は、DPE のコマンドラインインターフェイスから設定可能な暗号スイートのリストをサポートします。BAC でサポートされる暗号スイートのリストについては、表 4-5 を参照してください。 | • *num*：CWMP サービス（1 または 2）を表します。<br>• **all-cipher-suites**：CWMP　サービスに対して HTTP over SSL/TLS を使用して、すべての暗号スイートがセッションを認証するのをイネーブルにします。これがデフォルトの設定です。<br><br>**（注）** **service cwmp ssl cipher all-cipher-suites** コマンドは、個々の暗号を設定していない場合にのみ動作します。個々の暗号スイートをディセーブルにするには、**no service cwmp ssl cipher** *value* コマンドを使用します。すべての暗号をディセーブルにするには、**no service cwmp ssl cipher all-cipher-suites** コマンドを使用します。<br><br>• *value*：CWMP サービスに対して HTTP over SSL/TLS を使用して、セッションを認証するためにイネーブルにする、個々の暗号を表します。任意の暗号スイートをイネーブルまたはディセーブルにできます。<br><br>各暗号スイートは、特定の暗号法の機能に関連付けられている一連のアルゴリズムを指定します。BAC でサポートされる暗号法アルゴリズムのリストについては、表 4-4 を参照してください。 | **例 1**<br>`dpe# service cwmp 1 ssl cipher all-cipher-suites`<br>`% OK (Requires DPE restart "# dpe reload")`<br><br>**例 2**<br>`dpe# service cwmp 1 ssl cipher ssl_dh_anon_with_des_cbc_sha`<br>`% OK (Requires DPE restart "# dpe reload")` |
| **service cwmp** *num* **ssl enable {true \| false}** | | |
| DPE 上の CWMP サービスに対して、SSL/TLS 上での HTTP の使用をイネーブルまたはディセーブルにします。<br><br>**（注）** DPE を再起動する前にキーストア ファイルおよびキーストア パスワードを設定しないと、CWMP サービスが起動しなくなります。キーストア ファイルおよびキーストア パスワードの設定方法については、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | • *num*：CWMP サービス（1 または 2）を表します。<br>• **true**：SSL/TLS トランスポートをイネーブルにします。サービス 2 でのデフォルト設定です。<br>• **false**：SSL/TLS トランスポートをディセーブルにします。サービス 1 でのデフォルト設定です。 | `dpe# service cwmp 1 ssl enable true`<br>`% OK (Requires DPE restart "# dpe reload")` |

**表 4-2　service cwmp コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service cwmp** *num* **ssl keystore** *keystore-filename keystore-password key-password* | | |
| プロビジョニング サーバ証明書が含まれるキーストア ファイルを設定します。この証明書は、HTTP over SSL/TLS を使用して、デバイスに対してプロビジョニング サーバを認証するのに使用されます。<br><br>**（注）** この設定は、サービスのインスタンスがイネーブルになっており（**service cwmp 2** の場合と同様、デフォルトではディセーブルになっている）、このサービスに対して SSL/TLS プロトコルがイネーブルになっている場合にのみ関連します。SSL/TLS トランスポートをイネーブルにするには、**service cwmp** *num* **ssl enable true** コマンドを使用します。 | • *num*：CWMP サービス（1 または 2）を表します。<br>• *keystore-filename*：以前に作成したキーストア ファイルを表します。<br>• *keystore-password*：キーストア ファイルの作成時に使用したキーストア パスワードを表します。キーストア パスワードの文字数は、6 ～ 30 文字にする必要があります。<br>• *key-password*：キーストア ファイルの作成時に使用した秘密鍵パスワードを表します。秘密鍵パスワードの文字数は、6 ～ 30 文字にする必要があります。 | dpe# **service cwmp 1 ssl keystore example.keystore changeme changeme**<br>% OK (Requires DPE restart "# dpe reload") |
| DPE は、自己署名証明書が含まれるデフォルトのサンプル キーストアとともに出荷されます。ただし、CWMP デバイスは自己署名証明書を信頼しないので、このキーストアを使用して HTTP over SSL/TLS にデバイスをプロビジョニングさせることはできません。代わりに、署名済みのサービス プロバイダー証明書およびキーストアを取得する必要があります。詳細については、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | | |

# keystore import-pkcs12

このコマンドは、既存の秘密鍵と証明書を、SSL クライアントへの DPE の認証で使用する DPE 互換ファイルにインポートするときに使用します。**keystore import-pkcs12** コマンドにより PKCS#12 ファイルが開かれ、内容が読み取られ、JKS と呼ばれる Sun 独自の Java キーストア形式で新規のキーストアが書き込まれます。

PKCS#12 ファイル形式は、証明書と秘密鍵を格納するために使用する規格です。たとえば、Microsoft Windows 2000 IIS 5.0 サーバからインポートされた証明書がこれに該当します。

**（注）** 秘密鍵と証明書が別々のファイルに格納されている場合は、**keystore import-pkcs12** コマンドを実行する前に、これらのファイルを単一の PKCS#12 ファイルに結合してください。
次の例に記載されている構文を使用できます。この例では、**openssl** コマンドによって、`example.key` 内の鍵と `example.crt file` 内の証明書が `example.pkcs12` ファイルに結合されています。
`# openssl pkcs12 -inkey example.key -in example.crt -export -out example.pkcs12`

## シンタックスの説明

**keystore import-pkcs12** *keystore-filename pkcs12-filename keystore-password* key-password *export-password export-key-password*

- *keystore-filename*：作成される JKS キーストア ファイルを表します。ファイルがすでに存在している場合、ファイルは上書きされます。

  **（注）** 必ずキーストア ファイルのフル パスを指定してください。

- *pkcs12-filename*：鍵と証明書のインポート元である PKCS#12 ファイルを表します。
- *keystore-password*：キーストア ファイルの作成時に使用した秘密鍵パスワードおよびキーストア パスワードを表します。このパスワードの文字数は、6 ～ 30 文字にする必要があります。
- *key-password*：DPE キーストア内の鍵へのアクセスに使用されるパスワードを表します。このパスワードの文字数は、6 ～ 30 文字にする必要があります。
- *export-password*：PKCS#12 ファイル内の鍵の複合化に使用されるパスワードを表します。エクスポート パスワードの文字数は、6 ～ 30 文字にする必要があります。
- *export-key-password*：PKCS#12 キーストア内の鍵へのアクセスに使用されるパスワードを表します。このパスワードの文字数は、6 ～ 30 文字にする必要があります。

## 例

```
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
```

# service http

これは、DPE で実行されている HTTP サービスに対してさまざまな設定を構成するときに使用するコマンドのグローバル構文です。これらのコマンドを使用すると、次のことが可能です。

- サービスをイネーブルにする
- サービスのインスタンスを指定する
- クライアント認証およびクライアント証明書認証を設定する
- サービスのポート番号を設定する
- SSL/TLS 上で HTTP を使用するようにサービスを設定する

**service http** は、表 4-3 に記載されているコマンドのリストと併せて使用してください。

**（注）** これらのコマンドを使用するときは、特に記載のない限り、DPE を再起動して変更内容を有効にする必要があります。DPE を再起動するには、**dpe reload** コマンド（P.3-6 の「dpe reload」を参照）を実行します。

**表 4-3　service http コマンドのリスト**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service http** *num* **client-auth** *mode* | | |
| DPE 上の HTTP ファイル サービスに対するクライアント認証をイネーブルまたはディセーブルにします。<br><br>BAC の認証オプションのリストについては、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | • *num*：HTTP サービス（1 または 2）を表します。<br>• *mode*：HTTP ファイル サービスのクライアント認証モードを表します。クライアント認証モードには、次のようなものがあります。<br>— **basic**：基本 HTTP ファイル サービス認証をイネーブルにします。<br>— **digest**：ダイジェスト HTTP ファイル サービス認証をイネーブルにします。これがデフォルトの設定です。<br>— **none**：基本およびダイジェスト認証をディセーブルにします。このモードでは、HTTP ファイル サービスは Inform メッセージ内の Device ID を使用して CPE を認証します。<br><br>**（注）** クライアント認証中のセキュリティ リスクを制限するため、ダイジェスト モード（デフォルト設定）を使用することをお勧めします。基本モードでクライアント認証を許可したり、基本およびダイジェスト認証をディセーブルにしたりすることは推奨されていません。 | `dpe# service http 1 client-auth digest`<br>`% OK (Digest authentication was enabled. Basic authentication was disabled. Requires DPE restart "# dpe reload")` |

**表 4-3　service http コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service http** *num* **enable {true \| false}** | | |
| DPE 上で実行されている HTTP ファイル サービスをイネーブルまたはディセーブルにします。 | • *num*：HTTP ファイル サービス（1 または 2）を表します。<br>デフォルトでは、HTTP ファイル サービスは次のようになっています。<br>— サービス 1 ではイネーブル。<br>— サービス 2 ではディセーブル。<br>• **true**：HTTP ファイル サービスをイネーブルにします。<br>• **false**：HTTP ファイル サービスをディセーブルにします。 | dpe# **service http 2 enable true**<br>% OK (Requires DPE restart "# dpe reload") |
| **service http** *num* **port** *port* | | |
| HTTP ファイル サービスが CPE デバイスと通信するポートを表します。異なるポート番号を指定することにより、DPE が、他のアプリケーションによって使用されるポート間の共有違反を回避できるようになります。 | • *num*：HTTP ファイル サービス（1 または 2）を表します。<br>デフォルトでは、HTTP ファイル サービスは次のポートをリスニングするように設定されています。<br>— サービス 1 の場合はポート 7549。<br>— サービス 2 の場合はポート 7550。<br>• *port*：サービスが使用するポート番号を表します。<br>**（注）** **service http port** コマンドは、指定されたポート番号が別のアプリケーションまたはシステム ユーティリティによって使用されているかどうかはチェックしません。 | dpe# **service http 1 port 7549**<br>% OK (Requires DPE restart "# dpe reload") |

**表 4-3　service http コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service http** *num* **ssl client-auth** *mode* | | |
| DPE 上で実行されている HTTP ファイル サービスに対して HTTP over SSL/TLS を使用することにより、クライアント証明書認証をイネーブルまたはディセーブルにします。<br><br>BAC の認証オプションのリストについては、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | • *num*：HTTP ファイル サービス（1 または 2）を表します。<br><br>デフォルトでは、HTTP ファイル サービスに対して HTTP over SSL/TLS を使用するクライアント証明書認証は、次のようになっています。<br>— サービス 1 ではディセーブル。<br>— サービス 2 ではディセーブル。<br>• *mode*：HTTP ファイル サービスのクライアント証明書認証モードを表します。BAC のサポート対象は、次のとおりです。<br>— **client-cert-generic**：すべての CPE または CPE の大きなサブセットに共通の汎用証明書を使用して、SSL/TLS で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は、クライアント証明書を認証するために使用されます。この鍵は、DPE キーストアで事前設定されます。この証明書認証プロセスにより、証明書が有効であることが確認されますが、特定デバイスの ID は確立されません。したがって、デバイスの識別情報は、クライアント証明書の CN フィールド内のデータを使用することによっては生成されません。その代わり、デバイスの識別情報は基本またはダイジェスト認証経由で提供されたデータ、または CWMP Inform メッセージ内のデータを使用することによって生成されます。<br>— **client-cert-unique**：各 CPE が提供する一意の証明書を使用して、SSL/TLS で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認証されると、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固有識別情報が生成されます。<br>— **none**：HTTP over SSL/TLS を使用して、クライアント証明書認証をディセーブルにします。 | **例 1**<br>`dpe# service http 1 ssl client-auth client-cert-generic`<br>`% OK (Requires DPE restart "# dpe reload")`<br><br>**例 2**<br>`dpe# service http 1 ssl client-auth client-cert-unique`<br>`% OK (Requires DPE restart "# dpe reload")` |

**表 4-3　service http コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service http** *num* **ssl client-auth client-cert-css-ext** | | |
| HTTP over SSL/TLS を使用する接続が Cisco CSS 11500 シリーズ Content Services Switch（CSS 11500）で終端している CPE の、認証をイネーブルにします。下流 CSS は、CPE デバイスから SSL セッションに関する情報（特にクライアント証明書フィールド）を取り出し、そのデータをさまざまな HTTP ヘッダーに挿入します。その後 BAC は、CSS ヘッダーの ClientCert-Subject-CN から CN フィールドを取得して、固有のデバイス識別情報を作成します。<br><br>**（注）** このコマンドをイネーブルにする前に、必ず CSS を設定して、クライアント証明書フィールドを HTTP ヘッダーに挿入してください。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。<br><br>BAC の認証オプションのリストについては、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | *num*：HTTP ファイル サービス（1 または 2）を表します。<br><br>デフォルトでは、HTTP ファイル サービスに対して HTTP over SSL/TLS を使用するクライアント証明書認証は、次のようになっています。<br>• サービス 1 ではディセーブル。<br>• サービス 2 ではディセーブル。 | dpe# **service http ssl 1 client-auth client-cert-css-ext**<br>% OK (Requires DPE restart "# dpe reload") |

**表 4-3　service http コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service http** *num* **ssl cipher {all-cipher-suites \|** *value***}**<br><br>**no service http** *num* **ssl cipher {all-cipher-suites \|** *value***}** | | |
| 暗号アルゴリズムまたは暗号を使用して、DPE サーバと CPE の間の認証をイネーブルまたはディセーブルにします。これらの暗号アルゴリズムまたは暗号は、証明書管理およびセッション管理用に HTTP over SSL/TLS によってサポートされています。SSL ハンドシェイク中、DPE サーバと CPE デバイスは、これら両方でイネーブルになっている最も強い暗号スイートを特定し、SSL セッションでそのスイートを使用します。<br><br>**（注）** BAC は、DPE のコマンドライン インターフェイスから設定可能な暗号スイートのリストをサポートします。BAC がサポートする暗号スイートのリストについては、表 4-5 を参照してください。 | • *num*：HTTP ファイル サービス（1 または 2）を表します。<br>• **all-cipher-suites**：HTTP ファイル サービスに対して HTTP over SSL/TLS を使用して、すべての暗号スイートがセッションを認証するのをイネーブルにします。これがデフォルトの設定です。<br><br>**（注）** **service http ssl cipher all-cipher-suites** コマンドは、個々の暗号を設定していない場合にのみ動作します。個々の暗号スイートをディセーブルにするには、**no service http ssl cipher** *value* コマンドを使用します。すべての暗号をディセーブルにするには、**no service http ssl cipher all-cipher-suites** コマンドを使用します。<br><br>• *value*：HTTP ファイル サービスに対して HTTP over SSL/TLS を使用してセッションを認証する際に、イネーブルにする個々の暗号を表します。任意の暗号スイートをイネーブルまたはディセーブルにできます。<br>各暗号スイートは、特定の暗号法の機能に関連付けられている一連のアルゴリズムを指定します。BAC がサポートする暗号法アルゴリズムのリストについては、表 4-4 を参照してください。 | **例 1**<br>`dpe# service http 1 ssl cipher all-cipher-suites`<br>`% OK (Requires DPE restart "# dpe reload")`<br><br>**例 2**<br>`dpe# service http 1 ssl cipher ssl_dh_anon_with_des_cbc_sha`<br>`% OK (Requires DPE restart "# dpe reload")` |
| **service http** *num* **ssl enable {true \| false}** | | |
| DPE 上の HTTP ファイル サービスに対して、SSL/TLS 上での HTTP の使用をイネーブルまたはディセーブルにします。<br><br>**（注）** DPE を再起動する前にキーストア ファイルおよびキーストア パスワードを設定しないと、HTTP ファイル サービスが起動しなくなります。キーストア ファイルおよびキーストア パスワードの設定方法については、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | • *num*：HTTP ファイル サービス（1 または 2）を表します。<br>• **true**：SSL/TLS トランスポートをイネーブルにします。サービス 2 でのデフォルト設定です。<br>• **false**：SSL/TLS トランスポートをディセーブルにします。サービス 1 でのデフォルト設定です。 | `dpe# service http 1 ssl enable true`<br>`% OK (Requires DPE restart "# dpe reload")` |

**表 4-3　service http コマンドのリスト（続き）**

| コマンドの使用方法 | シンタックスの説明 | 例 |
|---|---|---|
| **service http** *num* **ssl keystore** *keystore-filename keystore-password key-pasword* | | |
| プロビジョニング サーバ証明書が含まれるキーストア ファイルを設定します。この証明書は、HTTP over SSL/TLS を使用して、デバイスに対してプロビジョニング サーバを認証するのに使用されます。<br><br>**（注）** この設定は、サービスのインスタンスがイネーブルになっており（service http 2 の場合と同様、デフォルトではディセーブルになっている）、このサービスに対して HTTP over SSL/TLS がイネーブルになっている場合にのみ関連します。SSL/TLS トランスポートをイネーブルにするには、**service http** *num* **ssl enable true** コマンドを使用します。 | • *num*：HTTP ファイル サービス（1 または 2）を表します。<br>• *keystore-filename*：以前に作成したキーストア ファイルを表します。<br>• *keystore-password*：キーストア ファイルの作成時に使用したキーストア パスワードを表します。キーストア パスワードの文字数は、6 ～ 30 文字にする必要があります。<br>• *key-password*：キーストア ファイルの作成時に使用した秘密鍵パスワードを表します。秘密鍵パスワードの文字数は、6 ～ 30 文字にする必要があります。 | `dpe# service http 1 ssl keystore example.keystore changeme changeme`<br>`% OK (Requires DPE restart "# dpe reload")` |
| DPE は、自己署名証明書が含まれるデフォルトのサンプル キーストアとともに出荷されます。ただし、CWMP デバイスは自己署名証明書を信頼しないので、このキーストアを使用して HTTP over SSL/TLS にデバイスをプロビジョニングさせることはできません。代わりに、署名済みのサービス プロバイダー証明書およびキーストアを取得する必要があります。署名済みのサービス プロバイダー証明書、およびキーストアの取得方法に関する詳細については、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。 | | |

### 暗号スイートの選択

一般的な SSL セッションでは、安全な接続を確立および保持するため、暗号化サイファが必要になります。暗号スイートは、SSL/TLS プロトコルがクライアント / サーバ交換を認証し、安全な接続を確立および保持するのに必要な暗号アルゴリズムを提供します。

表 4-4 は、この BAC のリリースでサポートされる暗号法アルゴリズムを定義しています。

**表 4-4　BAC でサポートされる暗号法アルゴリズム**

| 暗号法の機能 | BAC でサポートされるアルゴリズム |
|---|---|
| SSL のバージョン | SSL バージョン 3.0、および Transport Layer Security（TLS）バージョン 1.0 |
| 公開鍵の交換および鍵共有アルゴリズム | • RSA（鍵交換およびキー合意アルゴリズム）<br>暗号化およびデジタル署名に使用される Rivest、Shamir、Adelman アルゴリズム。<br>- 512 ビット、768 ビット、1024 ビット、および 2048 ビット<br>• DSA（証明書署名アルゴリズム）<br>Digital Signature Standard（DSS; デジタル シグニチャ規格）の一部として使用されるデジタル署名アルゴリズム。<br>- 512 ビット、768 ビット、および 1024 ビット<br>• Diffie-Hellman（鍵交換アルゴリズム）<br>- 512 ビット、768 ビット、1024 ビット、および 2048 ビット |
| 暗号化タイプ | • DES<br>データ暗号規格（Data Encryption Standard）は、56 ビットのキーを 64 ビットの各データ ブロックに適用します。このキーは、暗号化と復号化に使用されます。<br>• 3DES またはトリプル DES<br>DES が 3 つのキーで使用されている場合のための、トリプル データ暗号規格（Triple-Strength Data Encryption Standard）。<br>• RC4<br>Rivest Cipher 4。ファイル暗号化に使用される、可変キー サイズのストリーム暗号。 |
| メッセージ認証アルゴリズム | • Message Digest 5（MD5; メッセージ ダイジェスト 5）<br>128 ビットのメッセージ ダイジェストを作成するデジタル署名アプリケーションで使用されるアルゴリズム。このメッセージ ダイジェストは、メッセージに対して一意であり、データ整合性を確認するために使用されます。<br>• Secure Hash Algorithm（SHA）<br>160 ビットのハッシュ値を作成するデジタル シグニチャ規格で使用されるアルゴリズム。 |

**（注）** 暗号スイートの詳細については、『*Cisco Content Services Switch SSL Configuration Guide (Software Version 7.40)*』を参照してください。

**注意**　dh-anon シリーズの暗号スイートは、いずれのパーティも認証されない、完全に匿名の Diffie-Hellman 通信を対象としています。この暗号スイートは攻撃を受けやすいので注意してください。

タイトルに「export」が含まれる暗号スイートは、アメリカ合衆国外で使用されることを意図したもので、キー サイズが制限された暗号アルゴリズムを使用しています（たとえば、128 ビットの暗号化を行う 3DES または RC4）。

**表 4-5　BAC でサポートされる暗号スイート**

| 暗号スイート | エクスポートの可否 | 使用される鍵交換アルゴリズム |
|---|---|---|
| all-cipher-suites | 不可 | EDH * |
| ssl_dh_anon_export_with_des40_cbc_sha | 可 | DH ** |
| ssl_dh_anon_with_des_cbc_sha | 不可 | DH ** |
| ssl_dh_anon_export_with_rc4_40_md5 | 可 | DH ** |
| ssl_dh_anon_with_3des_ede_cbc_sha | 不可 | DH ** |
| ssl_dhe_dss_with_des_cbc_sha | 不可 | DH ** |
| ssl_dh_anon_with_rc4_128_md5 | 不可 | DH ** |
| ssl_dhe_dss_export_with_des40_cbc_sha | 可 | EDH * |
| ssl_dhe_dss_with_3des_ede_cbc_sha | 不可 | EDH * |
| ssl_dhe_rsa_export_with_des40_cbc_sha | 可 | EDH * |
| ssl_dhe_rsa_with_3des_ede_cbc_sha | 不可 | EDH * |
| ssl_dhe_rsa_with_des_cbc_sha | 不可 | EDH * |
| ssl_rsa_export_with_des40_cbc_sha | 可 | RSA |
| ssl_rsa_export_with_rc4_40_md5 | 可 | RSA |
| ssl_rsa_with_3des_ede_cbc_sha | 不可 | RSA |
| ssl_rsa_with_des_cbc_sha | 不可 | RSA |
| ssl_rsa_with_null_md5 | 不可 | RSA |
| ssl_rsa_with_null_sha | 不可 | RSA |
| ssl_rsa_with_rc4_128_md5 | 不可 | RSA |
| ssl_rsa_with_rc4_128_sha | 不可 | RSA |
| tls_dh_anon_with_aes_128_cbc_sha | 不可 | DH ** |
| tls_dhe_dss_with_aes_128_cbc_sha | 不可 | EDH * |
| tls_dhe_rsa_with_aes_128_cbc_sha | 不可 | EDH * |
| tls_rsa_with_aes_128_cbc_sha | 不可 | RSA |

* Ephemeral Diffie-Hellman アルゴリズムを意味する
** Diffie-Hellman アルゴリズムを意味する

CHAPTER 5

# SNMP エージェントのコマンド

この章では、Broadband Access Center（BAC）の Device Provisioning Engine（DPE）上の SNMP エージェントを管理および監視するために使用するコマンドライン インターフェイス（CLI）コマンドについて説明します。

この章で説明するコマンドは、次のとおりです。

# snmp-server community

このコマンドは、外部の SNMP マネージャが DPE の SNMP エージェントにアクセスするための、コミュニティのアクセス ストリングを設定するときに使用します。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

特定のコミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します（P.5-2 の「no snmp-server community」を参照してください）。

**シンタックスの説明**　**snmp-server community** *string* [**ro** | **rw**]

- *string*：SNMP コミュニティを表します。
- **ro**：読み取り専用（ro）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。NMS 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 オペレーションに 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、OID 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 を配置する前に、これらの値を変更することをお勧めします。

**例**

```
dpe# snmp-server community test_community ro
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

# no snmp-server community

このコマンドは、特定のコミュニティ ストリングを削除するときに使用します。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

外部の SNMP マネージャが DPE の SNMP エージェントにアクセスするための、コミュニティのアクセス ストリングを設定するには、**snmp-server community** コマンドを使用します。詳細については、P.5-2 の「snmp-server community」を参照してください。

**シンタックスの説明**　**no snmp-server community** *string*

*string*：SNMP コミュニティを表します。

**例**

```
dpe# no snmp-server community test_community
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

# snmp-server contact

このコマンドは、MIB II で定義されているシステム接点（sysContact）を示す文字列を入力するときに使用します。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

DPE 担当者のシステム接点を削除するには、このコマンドの **no** 形式を使用します。詳細については、P.5-3 の「no snmp-server」を参照してください。

**シンタックスの説明**　**snmp-server contact** *text*

*text*：DPE 担当者の接点名を表します。

**例**

```
dpe# snmp-server contact joe
% OK (Requires SNMP server restart "# snmp-server reload")
```

# no snmp-server

このコマンドは、DPE 担当者のシステム接点を削除するときに使用します。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

システム接点を示す文字列を入力するには、**snmp-server contact** コマンドを使用します。詳細については、P.5-3 の「snmp-server contact」を参照してください。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# no snmp-server contact
% OK (Requires SNMP server restart "# snmp-server reload")
```

# snmp-server host

このコマンドは、すべての SNMP 通知の受信者を指定するときに使用します。このコマンドを複数のインスタンスで使用して、複数の通知受信者を指定することができます。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

指定された通知受信者を削除するには、このコマンドの **no** 形式を使用します。詳細については、P.5-4 の「no snmp-server host」を参照してください。

**シンタックスの説明**

**snmp-server host** *host-addr* **notification community** *community* **udp-port** *port*

- *host-addr*：通知の送信先となるホストの IP アドレスを指定します。
- *community*：SNMP 通知の送信中に使用するコミュニティ ストリングを指定します。
- *port*：SNMP 通知の送信に使用する UDP ポートを表します。デフォルトの UDP ポート番号は 162 です。

**例**

```
dpe# snmp-server host 10.10.10.5 notification community public udp-port 162
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

# no snmp-server host

このコマンドは、指定された通知受信者を削除するときに使用します。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

すべての SNMP 通知の受信者を指定するには、**snmp-server host** コマンドを使用します。詳細については、P.5-4 の「snmp-server host」を参照してください。

**シンタックスの説明**

**no snmp-server host** *host-addr* **notification**

*host-addr*：ホストの IP アドレスを表します。

**例**

```
dpe# no snmp-server host 10.10.10.5 notification
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

# snmp-server inform

このコマンドは、SNMP エージェントから SNMP マネージャに送信される SNMP 通知のタイプを指定するときに使用します。デフォルトではトラップが送信されますが、このコマンドを使用すると、トラップではなく SNMP 情報が送信されます。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

SNMP 通知を切り替えて、デフォルト設定であるトラップに戻すには、このコマンドの **no** 形式を使用します。詳細については、P.5-5 の「no snmp-server inform」を参照してください。

**シンタックスの説明**

**snmp-server inform** [**retries** *count* **timeout** *time*]

- *count*：SNMP エージェントからマネージャに情報を送信できる回数を表します。設定したリトライ回数に達する前にタイムアウト期間が終了した場合、SNMP サーバは情報の送信を停止します。
- *time*：SNMP サーバが情報の送信を継続する時間の長さ（ミリ秒）を表します。タイムアウト期間が終了する前に最大リトライ回数に達した場合、SNMP サーバは情報の送信を停止します。

**（注）** SNMP 情報を設定するときのリトライ回数およびタイムアウトを指定することはオプションです。指定しない場合は、デフォルト値のリトライ回数 1 回および 5000 ミリ秒が使用されます。

**例**

```
dpe# snmp-server inform retries 5 timeout 500
% OK ()
Requires SNMP server restart "# snmp-server reload"
```

この例では、SNMP 情報は、リトライが停止されるまでに最大 5 回送信されます。リトライが 5 回行われる前に 500 ミリ秒のタイムアウト期間が終了した場合、情報の送信は停止されます。

# no snmp-server inform

このコマンドは、SNMP マネージャに送信される SNMP 通知を切り替えて、デフォルト設定であるトラップに戻すときに使用します。

送信される SNMP 通知のタイプを指定するには、**snmp-server inform** コマンドを使用します。詳細については、P.5-5 の「snmp-server inform」を参照してください。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# no snmp-server inform
% OK
```

# snmp-server location

このコマンドは、MIB II で定義されているシステム ロケーション（sysLocation）を示す文字列を入力するときに使用します。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

システム ロケーションを削除するには、このコマンドの **no** 形式を使用します。詳細については、P.5-6 の「no snmp-server location」を参照してください。

**シンタックスの説明**　**snmp-server location** *text*

*text*：DPE の物理ロケーションを表します。

**例**

```
dpe# snmp-server location st_louis
% OK (Requires SNMP server restart "# snmp-server reload")
```

# no snmp-server location

このコマンドは、システム ロケーションを削除するときに使用します。

このコマンドを使用したときは、このコマンドの後に **snmp-server reload** コマンドを実行して SNMP エージェントを再起動する必要があります。詳細については、P.5-7 の「snmp-server reload」を参照してください。

システム ロケーションを示す文字列を入力するには、**snmp-server location** コマンドを使用します。詳細については、P.5-6 の「snmp-server location」を参照してください。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# no snmp-server location
% OK (Requires SNMP server restart "# snmp-server reload")
```

# snmp-server reload

このコマンドは、DPE の SNMP エージェントのプロセスをリロードするときに使用します。このコマンドを入力すると、リロードされた SNMP エージェント プロセスが表示されます。

**(注)** RDU および DPE で SNMP プロセスが起動すると、システムの動作時間を含むトラップが送信されます。ただし、BAC トラップ通知はデフォルトではディセーブルになっています。対応する MIB オブジェクトを SNMP 経由で設定することによってのみ、トラップ通知をイネーブルにできます。CLI または管理者ユーザ インターフェイス経由で、トラップ通知をイネーブルにすることはできません。

この BAC のリリースでは、CISCO-BACC-SERVER-MIB ファイルで定義されているトラップ通知だけがサポートされます。詳細については、*BPR_HOME/rdu/mibs* ディレクトリの MIB ファイルを参照してください。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# snmp-server reload
Process snmpAgent has been restarted
dpe#
```

# snmp-server start | stop

このコマンドは、DPE の SNMP エージェントのプロセスを起動または停止するときに使用します。

**シンタックスの説明**　**snmp-server start** | **stop**

- **start**：DPE の SNMP エージェントのプロセスを開始します。

  **(注)** このコマンドは、SNMP エージェントが動作していないときにのみ使用してください。SNMP エージェントがすでに動作しているときにこのコマンドを実行すると、次のメッセージが表示されます。

  ```
  Process snmpAgent is already running
  ```

- **stop**：DPE の SNMP エージェントのプロセスを停止します。

**例**

**例 1**

```
dpe# snmp-server start
Process snmpAgent has been started
% OK
```

**例 2**

```
dpe# snmp-server stop
Process snmpAgent has been stopped
dpe#
```

# snmp-server udp-port

このコマンドは、SNMP エージェントがリッスンする UDP ポート番号を特定するときに使用します。

DPE では、他のアプリケーションが使用するポート間の共有違反を回避するためにこのコマンドが必要です。ポート番号を変更することにより、ポートの競合が発生しなくなります。

SNMP エージェントのデフォルトのポート番号 8001 は、Solaris コンピュータ上の他の SNMP エージェントとのポートの競合を回避する標準的な SNMP エージェント ポートとは異なります。

**（注）** SNMP エージェントが使用する UDP ポートを標準的なポート（番号 161）に変更することをお勧めします。

SNMP エージェントがリッスンするポートを変更してデフォルトの UDP ポート番号に戻すには、このコマンドの **no** 形式を使用します。詳細については、P.5-8 の「no snmp-server udp-port」を参照してください。

**シンタックスの説明**　**snmp-server udp-port** *port*

*port*：SNMP エージェントがリッスンする UDP ポートを表します。

**例**

```
dpe# snmp-server udp-port 161
% OK
```

# no snmp-server udp-port

このコマンドは、SNMP エージェントがリッスンするポートを変更して、デフォルトの UDP ポート番号（8001）に戻すときに使用します。

**（注）** SNMP エージェントの標準的なポート番号である 161 以外のポート番号を使用すると、同じ Solaris コンピュータで実行されている他の SNMP エージェントとポートの競合が発生する可能性が高まります。

SNMP エージェントがリッスンする UDP ポート番号を特定するには、**snmp-server udp-port** コマンドを使用します。詳細については、P.5-8 の「snmp-server udp-port」を参照してください。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# no snmp-server udp-port
% OK
```

CHAPTER 6

# DPE 用のログおよびデバッグ コマンド

この章では、Broadband Access Center（BAC）の Device Provisioning Engine（DPE）をデバッグし、BAC ログ システムを管理および監視するために使用するコマンドライン インターフェイス（CLI）コマンドについて説明します。

(注) 任意のデバッグ コマンドを使用する前に、DPE のデバッグがイネーブルになっていることを確認してください。この機能をイネーブルにするには、**debug on** コマンドを実行します。詳細については、P.6-5 の「debug on」を参照してください。

この項で説明するコマンドは、次のとおりです。

# clear logs

このコマンドは、システムに存在する古いログ ファイルを削除するときに使用します。次のファイルが対象となります。

- DPE ログ
- Syslog

時の経過とともに、古いログ ファイルは DPE 内に蓄積します。このようなログをバンドルするには、**support bundle state** コマンドを使用します。必要なファイルが消失されるのを防ぐため、ログをクリアする前に、バンドルを作成することをお勧めします。

このコマンドを使用すると、ログをグリアしていることを示すプロンプトが表示されます。クリアされたログ ファイルの数も示されます。

**例**

```
dpe# clear logs
Clearing historic log files...
+ Removing 1 DPE log files...
+ No more historic logs.
```

# debug dpe

**debug dpe** は、DPE のさまざまなサービスのデバッグに使用するコマンドのグローバル構文です。

(注) 次の表に示すコマンドをライセンスのない DPE で実行した場合は、次のようなメッセージが表示されます。

```
This DPE is not licensed.Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

表 6-1 は、DPE のデバッグで使用できるさまざまなコマンドを示します。

**表 6-1　debug dpe コマンドのリスト**

| コマンドの使用方法 | 例 |
|---|---|
| **debug dpe cache**<br><br>**no debug dpe cache** | |
| DPE キャッシュのデバッグ ロギングをイネーブルにします。次のような DPE キャッシュに関するメッセージが記録されます。<br>• キャッシュ エントリのロギングの要求。<br>• キャッシュのアップデート。<br>• DPE サブシステムによるその他のインタラクション。<br>DPE キャッシュのデバッグ ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug dpe cache**<br>% OK |
| **debug dpe connection**<br><br>**no debug dpe connection** | |
| DPE 接続のデバッグをイネーブルにします。通信サブシステムのステータスやエラー メッセージが記録されます。このコマンドは、DPE と RDU との間の通信に関する問題を検出するときに使用します。DPE 接続のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug dpe connection**<br>% OK |
| **debug dpe dpe-server**<br><br>**no debug dpe dpe-server** | |
| DPE サーバのデバッグをイネーブルにします。DPE サーバの総合的なステータスや問題に関するログ メッセージが記録されます。DPE サーバのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug dpe dpe-server**<br>% OK |

表 6-1　debug dpe コマンドのリスト（続き）

| コマンドの使用方法 | 例 |
|---|---|
| **debug dpe event-manager**<br><br>**no debug dpe event-manager** | |
| DPE イベント マネージャのデバッグをイネーブルにします。イベント マネージャのステータスに関するログ メッセージや状態が記録されます。DPE イベント マネージャのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。<br><br>DPE イベント マネージャのデバッグは、デフォルトではイネーブルになっています。 | dpe# **debug dpe event-manager**<br>% OK |
| **debug dpe exceptions**<br><br>**no debug dpe exceptions** | |
| DPE 例外のデバッグをイネーブルにします。システムのオペレーション中に発生した例外の完全なスタック トレースが記録されます。システムの破損や異常動作のように異例の事態が発生した場合、Cisco TAC サポートにお問い合せいただく前にこのコマンドを実行すると、貴重な情報を提示することができます。DPE 例外のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。<br><br>DPE 例外のデバッグは、デフォルトではイネーブルになっています。 | dpe# **debug dpe exceptions**<br>% OK |
| **debug dpe framework**<br><br>**no debug dpe framework** | |
| DPE フレームワークのデバッグをイネーブルにします。DPE サーバの基礎をなすフレームワークに関するログ情報が記録されます。この基礎をなすインフラストラクチャによって、BAC の各種サーバは支えられています。DPE フレームワークのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。<br><br>DPE フレームワークのデバッグは、デフォルトではイネーブルになっています。 | dpe# **debug dpe framework**<br>% OK |
| **debug dpe messaging**<br><br>**no debug dpe messaging** | |
| DPE メッセージングのデバッグをイネーブルにします。DPE のメッセージング サブシステムに関する詳細情報が記録されます。このサブシステムは、主に DPE と RDU との間の通信に使用されます。DPE メッセージングのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug dpe messaging**<br>% OK |
| **debug dpe statistics**<br><br>**no debug dpe statistics** | |
| パフォーマンス統計の集合をイネーブルにします。DPE パフォーマンス統計の集合のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug dpe statistics**<br>% OK |

# debug on

このコマンドは、デバッグ ロギングをイネーブルにするときに使用します。予想されるシステムの問題をトラブルシューティングするときに役立ちます。このコマンド以外に、**debug dpe cache** などのコマンドを使用して、特定のデバッグ カテゴリを個々にイネーブルにする必要があります。

デバッグ ロギングをディセーブルにするには、**no debug** コマンドを実行します。詳細については、P.6-5 の「no debug」を参照してください。

**注意**　デバッグ ロギングをイネーブルにすると、DPE のパフォーマンスに重大な影響が及ぶ可能性があります。デバッグをイネーブルにした状態で、DPE を長時間にわたって実行しないようにします。

このコマンドをライセンスのない DPE で実行した場合は、次のようなメッセージが表示されます。

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

**デフォルト**　デバッグ ロギングは、デフォルトではイネーブルになっています。

**例**

```
dpe# debug on
% OK
```

# no debug

このコマンドは、すべてのデバッグ ロギングをディセーブルにするときに使用します。

このコマンドをライセンスのない DPE で実行した場合は、次のようなメッセージが表示されます。

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

デバッグをイネーブルにするには、**debug on** コマンドを使用します。詳細については、P.6-5 の「debug on」を参照してください。

**例**

```
dpe# no debug
% OK
```

# log level

このコマンドは、保存される DPE ログ メッセージの最小レベルを設定するときに使用します。ログ レベルの詳細については、『*Cisco Broadband Access Center Administrator's Guide, Release 3.0*』を参照してください。

このコマンドをライセンスのない DPE で実行した場合は、次のようなメッセージが表示されます。

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

## シンタックスの説明

**log level** *number*

*number*：保存されるログ レベルを数字で表します。BAC がサポートするログ レベルは、表 6-2 のとおりです。

**表 6-2　DPE ログ レベル**

| ログ レベル番号 | 説明 |
|---|---|
| 0（緊急） | 緊急なメッセージをすべて保存します。 |
| 1（アラート） | 即時のアクションが必要なアクティビティ、およびそれ以上のレベルのアクティビティをすべて保存します。 |
| 2（クリティカル） | 異常な状態、およびそれ以上のレベルの状態をすべて保存します。 |
| 3（エラー） | エラー メッセージ、およびそれ以上のレベルのメッセージをすべて保存します。 |
| 4（警告） | 警告メッセージ、およびそれ以上のレベルのメッセージをすべて保存します。 |
| 5（通知） | 通知メッセージ、およびそれ以上のレベルのメッセージをすべて保存します。 |
| 6（情報） | 出力されたログ メッセージをすべて保存します。 |

**（注）** 特定のログ レベルを設定すると、設定されたレベルおよびそれ以下のメッセージが保存されます。たとえば、ログ レベルを 5（通知）に設定すると、レベル 4 以下のログ レベルのメッセージを生成するイベントがすべてログ ファイルに書き込まれます。
ロギング システムのログ レベルは、ログの問題に対処する際の緊急性を表すために使用されます。ログ レベルの中では、0（緊急）が最も重要度が高いレベルで、主に情報ログ メッセージを保存する 6（情報）が最も重要度が低いレベルです。

## デフォルト

保存される DPE ログ メッセージの最小レベルは、デフォルトでは 5（通知）に設定されています。

## 例

```
dpe# log level 6
% OK
```

# show log

このコマンドは、DPE の最新のログ エントリをすべて表示するときに使用します。ログには、システム エラーや重大な問題のロギングを含め、一般的な DPE プロセスの情報が記録されます。システムが困難な状態に陥っているときは、このログをチェックします。ログに含まれる情報が不十分な場合は、デバッグ ロギング機能をイネーブルにして、問題に関連したカテゴリをさまざまに変更してみます。

## シンタックスの説明

**show log** [**last** *1..999* | **run**]

- **last** *1..999*：DPE の最新のログ エントリから、指定された数のエントリを表示します。*1..999* は、表示するログ エントリの数を指定しますこれは省略可能な要素です。
- **run**：実行中の DPE ログを表示します。このコマンドを実行すると、DPE ログに記録されたすべてのメッセージの表示が開始されます。コマンドの実行は、Enter キーを押すまで継続されます。これは省略可能な要素です。

## 例

### 例 1

```
dpe# show log
2006 02 14 07:50:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:
BACThread[Connector,5,BAC,alive]
```

**（注）** ここでは、説明のためにコマンドの出力例の一部のみ紹介しています。

### 例 2

```
dpe# show log last 3
2006 02 14 07:51:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:     Cwmp1Thread-1
2006 02 14 07:51:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:     Http1Thread-0
2006 02 14 07:51:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:     Http1Thread-1
```

### 例 3

```
dpe# show log run
% Press <enter> to stop.
2006 02 14 07:53:22 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: OSStatusService: current CPU load
percentage 1%
2006 02 14 07:53:25 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: MemoryMonitor: Memory:
2006 02 14 07:53:25 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: MemoryMonitor: Total memory
29777920
2006 02 14 07:53:25 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: MemoryMonitor: Free memory
4058120
2006 02 14 07:53:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor: Threads:

Stopped.
```

CHAPTER 7

# CWMP 技術のデバッグ コマンド

この章では、Broadband Access Center（BAC）の Device Provisioning Engine（DPE）の CWMP 技術をデバッグするために使用するコマンドライン インターフェイス（CLI）コマンドについて説明します。

(注) 任意のデバッグ コマンドを使用する前に、**debug on** コマンドを実行して、DPE のデバッグをイネーブルにする必要があります。詳細については、P.6-5 の「debug on」を参照してください。

この章で説明するコマンドは、次のとおりです。

### debug service *type*

これは、DPE で実行されている CWMP サービスおよび HTTP ファイル サービスのデバッグに使用するコマンドのグローバル構文です。

## シンタックスの説明

**debug service** *type num*

- *type*：サービス（CWMP または HTTP）を指定します。
  - — CWMP：DPE 上での CWMP サービスのデバッグをイネーブルにします。
  - — HTTP：DPE 上での HTTP ファイル サービスのデバッグをイネーブルにします。
- *num*：サービス（1 または 2）のインスタンスを指定します。

CWMP サービスのデバッグに使用されるコマンドのリストについては、P.7-3 の「debug service cwmp」を参照してください。

HTTP ファイル サービスのデバッグに使用されるコマンドのリストについては、P.7-8 の「debug service http」を参照してください。

# debug service cwmp

この項では、DPE で実行されている CWMP サービスのデバッグに使用するコマンドについて説明します。

**（注）** 次の任意のデバッグ コマンドを使用する前に、DPE のデバッグがイネーブルになっていることを確認してください。この機能をイネーブルにするには、**debug on** コマンドを実行します。詳細については、P.6-5 の「debug on」を参照してください。

## シンタックスの説明

**debug service cwmp** *num*

*num*：サービス（1 または 2）のインスタンスを指定します。

表 7-1 に、CWMP サービスのデバッグに使用できるコマンドを示します。

**表 7-1　debug service cwmp コマンドのリスト**

| コマンドの使用方法 | 例 |
|---|---|
| **debug service cwmp** *num* **client-auth-all**<br><br>**no debug service cwmp** *num* **client-auth-all** | |
| CWMP サービスの成功および失敗したクライアント認証の詳細なデバッグをイネーブルにします。CWMP サービスの成功および失敗した認証の詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 client-auth-all**<br>% OK |
| **debug service cwmp** *num* **client-auth-failures**<br><br>**no debug service cwmp** *num* **client-auth-failures** | |
| CWMP サービスの失敗したクライアント認証の詳細なデバッグをイネーブルにします。CWMP サービスの失敗したクライアント認証の詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 client-auth-failures**<br>% OK |
| **debug service cwmp connection-request-service**<br><br>**no debug service cwmp connection-request-service** | |
| DPE から CPE デバイスへの要求を伴う、CWMP 接続要求サービスのデバッグをイネーブルにします。CWMP 接続要求サービスのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。<br><br>**（注）** このコマンドの CWMP インスタンスを指定する必要はありません。 | dpe# **no debug service cwmp connection-request-service**<br>% OK |

表 7-1　debug service cwmp コマンドのリスト（続き）

| コマンドの使用方法 | 例 |
|---|---|
| **debug service cwmp** *num* **cpe-config-sync**<br><br>**no debug service cwmp** *num* **cpe-config-sync** | |
| CPE デバイスとの DPE のインタラクションを伴う、CWMP サービスのデバイス構成の同期の詳細なデバッグをイネーブルにします。CWMP デバイス構成の同期サービスの詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 cpe-config-sync**<br>% OK |
| **debug service cwmp** *num* **data-sync**<br><br>**no debug service cwmp** *num* **data-sync** | |
| RDU と CPE デバイスとの間のインタラクションにおいて、CWMP サービスのデータ同期の詳細なデバッグをイネーブルにします。このデータは、RDU に転送されるデバイス ディスカバリおよびデバイス アップデートに関連しています。データ同期サービスの詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 data-sync**<br>% OK |
| **debug service cwmp** *num* **device-operations**<br><br>**no debug service cwmp** *num* **device-operations** | |
| DPE でのデバイス操作の実行のデバッグをイネーブルにします。DPE でのデバイス操作の実行のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 device-operations**<br>% OK |
| **debug service cwmp device-operations-cache**<br><br>**no debug service cwmp device-operations-cache** | |
| すべての CWMP サービスが使用する、即時モードでのデバイス操作キャッシュのデバッグをイネーブルにします。すべての CWMP サービスが使用する即時モードでのデバイス操作キャッシュのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。<br><br>**（注）** このコマンドの CWMP インスタンスを指定する必要はありません。 | dpe# **debug service cwmp device-operations-cache**<br>% OK |
| **debug service cwmp** *num* **errors**<br><br>**no debug service cwmp** *num* **errors** | |
| DPE 上で実行されている CWMP サービスが関係したインタラクションで発生した、低レベル エラーのデバッグをイネーブルにします。通常は、これらのエラーはログされません。CWMP サービスが関係したインタラクションで発生した、低レベル エラーのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 errors**<br>% OK |

表 7-1　debug service cwmp コマンドのリスト（続き）

| コマンドの使用方法 | 例 |
|---|---|
| **debug service cwmp** *num* **extension**<br><br>**no debug service cwmp** *num* **extension** | |
| DPE 上で実行されている CWMP サービスのサービス拡張のデバッグをイネーブルにします。CWMP サービスのサービス拡張のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 extension**<br>% OK |
| **debug service cwmp** *num* **firmware**<br><br>**no debug service cwmp** *num* **firmware** | |
| CWMP サービスのファームウェア規則の実行のデバッグをイネーブルにします。これらの規則には、デバイス ファームウェアの状態を詳細に記述するメッセージおよび条件が含まれます。CWMP サービスのファームウェア規則の実行のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 firmware**<br>% OK |
| **debug service cwmp** *num* **http-details**<br><br>**no debug service cwmp** *num* **http-details** | |
| DPE 上で実行されている CWMP サービスの低レベル詳細情報のデバッグをイネーブルにします。CWMP サービスの低レベル詳細情報のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 http-details**<br>% OK |
| **debug service cwmp** *num* **http-details**<br><br>**no debug service cwmp** *num* **http-faults** | |
| DPE 上で実行されている CWMP サービスが関係したインタラクションで発生した、エラー応答のデバッグをイネーブルにします。CWMP サービスが関係したインタラクションで発生した、エラー応答のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 http-faults**<br>% OK |
| **debug service cwmp** *num* **http-headers**<br><br>**no debug service cwmp** *num* **http-headers** | |
| CWMP サービスの要求および応答ヘッダーの詳細なデバッグをイネーブルにします。CWMP サービスの要求および応答ヘッダーの詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 http-headers**<br>% OK |
| **debug service cwmp** *num* **http-requests**<br><br>**no debug service cwmp** *num* **http-requests** | |
| CWMP サービスのメッセージのペイロードでの要求に関する、詳細なデバッグをイネーブルにします。CWMP サービスのメッセージのペイロードでの要求に関する詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 http-requests**<br>% OK |

表 7-1　debug service cwmp コマンドのリスト（続き）

| コマンドの使用方法 | 例 |
|---|---|
| **debug service cwmp** *num* **http-responses**<br><br>**no debug service cwmp** *num* **http-responses** | |
| CWMP サービスのメッセージのペイロードでの応答に関する、詳細なデバッグをイネーブルにします。CWMP サービスのメッセージのペイロードでの応答に関する詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 http-responses**<br>% OK |
| **debug service cwmp** *num* **instr-gen-requests**<br><br>**no debug service cwmp** *num* **instr-gen-requests** | |
| CPE デバイスとのインタラクションを伴う、CWMP サービスの命令生成要求のデバッグをイネーブルにします。命令生成要求のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 instr-gen-requests**<br>% OK |
| **debug service cwmp** *num* **instruction-details**<br><br>**no debug service cwmp** *num* **instruction-details** | |
| CPE デバイスとのインタラクションを伴う、CWMP サービスの命令処理の詳細なデバッグをイネーブルにします。CWMP サービスの命令処理の詳細なデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 instruction-details**<br>% OK |
| **debug service cwmp** *num* **instruction-lookup**<br><br>**no debug service cwmp** *num* **instruction-lookup** | |
| CPE デバイスとのインタラクションを伴う、CWMP サービスの DPE 命令ルックアップ詳細情報のデバッグをイネーブルにします。CWMP サービスの DPE 命令ルックアップ詳細情報のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 instruction-lookup**<br>% OK |
| **debug service cwmp** *num* **instruction-rpc**<br><br>**no debug service cwmp** *num* **instruction-rpc** | |
| CPE デバイスとのインタラクションを伴う、CWMP サービスの RPC 命令処理のデバッグをイネーブルにします。CWMP サービスの RPC 命令処理のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 instruction-rpc**<br>% OK |
| **debug service cwmp** *num* **instruction-states**<br><br>**no debug service cwmp** *num* **instruction-states** | |
| CWMP サービスの命令処理中の、命令状態遷移のデバッグをイネーブルにします。CWMP サービスの命令処理の際の命令状態遷移のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 instruction-states**<br>% OK |

表 7-1　debug service cwmp コマンドのリスト（続き）

| コマンドの使用方法 | 例 |
|---|---|
| **debug service cwmp** *num* **ipe**<br><br>**no debug service cwmp** *num* **ipe** | |
| CWMP サービスの DPE 命令処理エンジンの実行のデバッグをイネーブルにします。CWMP サービスの DPE 命令処理エンジンの実行のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 ipe**<br>% OK |
| **debug service cwmp** *num* **session**<br><br>**no debug service cwmp** *num* **session** | |
| DPE と CPE デバイスとの間の、CWMP セッションのライフサイクルのデバッグをイネーブルにします。CWMP セッションのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 session**<br>% OK |
| **debug service cwmp session-manager**<br><br>**no debug service cwmp session-manager** | |
| セッションの管理に責任を負う CWMP サービスの、セッション　マネージャのデバッグをイネーブルにします。CWMP サービスのセッション マネージャのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。<br><br>**（注）** このコマンドの CWMP インスタンスを指定する必要はありません。 | dpe# **debug service cwmp session-manager**<br>% OK |
| **debug service cwmp** *num* **soap-faults**<br><br>**no debug service cwmp** *num* **soap-faults** | |
| CPE デバイスとのインタラクションを伴う、CWMP サービスの受信および送信されたすべての SOAP 障害のデバッグをイネーブルにします。CWMP サービスのすべての SOAP 障害のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 soap-faults**<br>% OK |
| **debug service cwmp** *num* **soap-informs**<br><br>**no debug service cwmp** *num* **soap-informs** | |
| DPU と CPE デバイスの間のインタラクションにおける CWMP サービスの、受信されたすべての Inform メッセージのデバッグをイネーブルにします。CWMP サービスのすべての受信済み Inform メッセージのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 soap-informs**<br>% OK |
| **debug service cwmp** *num* **unknown-devices**<br><br>**no debug service cwmp** *num* **unknown-devices** | |
| DPE キャッシュに格納されていないデバイス構成の処理のデバッグをイネーブルにします。DPE キャッシュに格納されていないデバイス構成の処理のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service cwmp 1 unknown-devices**<br>% OK |

# debug service http

この項では、DPE で実行されている HTTP ファイル サービスのデバッグに使用するコマンドについて説明します。

**（注）** 任意のデバッグ コマンドを使用する前に、DPE のデバッグがイネーブルになっていることを確認してください。この機能をイネーブルにするには、**debug on** コマンドを実行します。詳細については、P.6-5 の「debug on」を参照してください。

## シンタックスの説明

**debug service http** *num*

*num*：サービス（1 または 2）のインスタンスを指定します。

表 7-2 に、HTTP ファイル サービスのデバッグに使用できるコマンドを示します。

**表 7-2　debug service http コマンドのリスト**

| コマンドの使用方法 | 例 |
|---|---|
| **debug service http** *num* **client-auth-all**<br><br>**no debug service http** *num* **client-auth-all** | |
| HTTP サービスの成功および失敗したクライアント認証のデバッグをイネーブルにします。HTTP サービスの成功および失敗したクライアント認証のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service http 1 client-auth-all**<br>% OK |
| **debug service http** *num* **client-auth-failures**<br><br>**no debug service http** *num* **client-auth-failures** | |
| HTTP サービスの失敗したクライアント認証のデバッグをイネーブルにします。HTTP サービスの失敗したクライアント認証のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service http 1 client-auth-failures**<br>% OK |
| **debug service http** *num* **details**<br><br>**no debug service http** *num* **details** | |
| DPE 上で実行されている HTTP サービスの、低レベル詳細情報のデバッグをイネーブルにします。HTTP サービスの低レベル詳細情報のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service http 1 details**<br>% OK |
| **debug service http** *num* **errors**<br><br>**no debug service http** *num* **errors** | |
| DPE 上で実行されている HTTP サービスの、要求エラーのデバッグをイネーブルにします。HTTP サービスへの要求エラーのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service http 1 errors**<br>% OK |

表 7-2　debug service http コマンドのリスト（続き）

| コマンドの使用方法 | 例 |
|---|---|
| **debug service http** *num* **faults**<br><br>**no debug service http** *num* **faults** | |
| DPE 上で実行されている HTTP サービスのエラー応答のデバッグをイネーブルにします。HTTP サービスのエラー応答のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service http 1 faults**<br>% OK |
| **debug service http** *num* **headers**<br><br>**no debug service http** *num* **headers** | |
| DPE 上で実行されている HTTP サービスの要求および応答ヘッダーのデバッグをイネーブルにします。HTTP サービスの要求および応答ヘッダーのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service http 1 headers**<br>% OK |
| **debug service http** *num* **request-processing**<br><br>**no debug service http** *num* **request-processing** | |
| DPE 上で実行されている HTTP サービスの、成功および失敗した要求処理のデバッグをイネーブルにします。HTTP サービスの成功および失敗した要求処理のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。 | dpe# **debug service http 1 request-processing**<br>% OK |
| **debug service http framework**<br><br>**no debug service http framework** | |
| 特定のサービスに関連付けられていない HTTP フレームワークのアクティビティのデバッグをイネーブルにします。HTTP フレームワークのアクティビティのデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。<br><br>**(注)** このコマンドの HTTP インスタンスを指定する必要はありません。 | dpe# **debug service http framework**<br>% OK |

# debug service ssl

このコマンドは、DPE と CPE デバイスとの間の CWMP 交換において、SSL/TLS 接続を受け入れる処理のデバッグをイネーブルにするときに使用します。SSL/TLS 接続を許可する処理のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

このコマンドを使用したときは、DPE を再起動して変更内容を有効にする必要があります。DPE を再起動するには、**dpe reload** コマンドを実行します。詳細については、P.3-6 の「dpe reload」を参照してください。

**例**

```
dpe# debug service ssl
% OK (Requires DPE restart "# dpe reload")
```

CHAPTER 8

# サポートとトラブルシューティングのコマンド

この章では、Broadband Access Center（BAC）の Device Provisioning Engine（DPE）のトラブルシューティング サポートを提供するために使用するコマンドライン インターフェイス（CLI）コマンドについて説明します。

この章で説明するコマンドは、次のとおりです。

# clear bundles

このコマンドは、DPE に存在するアーカイブ済みのバンドルをクリアするときに使用します。このようなバンドルは、**support bundles** コマンドを使用して作成されるもので、通常は、Cisco TAC で使用されるアーカイブ済みのログとステート情報が含まれます。アーカイブ済みのステートは消失するため、このコマンドを実行する前に、すべてのバンドルが取得されたことを確認してください。

コマンドを入力すると、バンドルをクリアしていることを示すプロンプトが表示されます。それが完了すると、クリアされたディスク領域の量がバイト単位で表示されます。

**シンタックスの説明**　キーワードや引数はありません。

**例**

**例 1**

```
dpe# clear bundles
Clearing Cisco support bundles...
+ 10101760 bytes cleared.
```

これは、存在するアーカイブ済みのバンドルがクリアされたときの結果です。

**例 2**

```
dpe# clear bundles
Clearing Cisco support bundles...
+ No bundles to clear.
```

これは、クリアするアーカイブ済みバンドルが存在していないときの結果です。

# show bundles

このコマンドは、発信ディレクトリで現在利用できるすべてのバンドルを表示するときに使用します。このようなバンドルは、**support bundle** コマンドで作成します。

コマンドを入力すると、アーカイブされているバンドルが表示されます。ただし、バンドルが存在しない場合は、利用可能なバンドルがないことを示すプロンプトが表示されます。

**シンタックスの説明**　キーワードや引数はありません。

**例**

**例 1**

```
dpe# show bundles
outgoing/cache-20060214-002023.bac
outgoing/state-20060214-002230.bac
```

これは、現在アーカイブされているバンドルが存在するときの結果です。

**例 2**

```
dpe# show bundles
No bundles currently available.
```

これは、現在アーカイブされているバンドルが存在しないときの結果です。

# support bundle cache

このコマンドは、現在の DPE キャッシュをバンドルするときに使用します。このコマンドは、Cisco TAC に送信するためのキャッシュをアーカイブするときに役立ちます。作成したバンドルは、FTP サーバの発信ディレクトリから利用できます。

コマンドを入力すると、TAC によって使用されるキャッシュ バンドルが作成されます。このコマンドにより、バンドル ファイルの圧縮サイズなどを含むバンドルの詳細が表示されます。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# support bundle cache
Creating cache bundle for Cisco support...
+ outgoing/cache-20060721-000218.bac
+ Adding & compressing DPE cache...
+ Size: 11780584 bytes
```

# support bundle state

このコマンドは、現在の DPE ステートをバンドルするときに使用します。このコマンドは、Cisco TAC に送信するための DPE の設定とログ ファイルをアーカイブするときに役立ちます。作成したバンドルは、FTP サーバの発信ディレクトリから利用できます。

**（注）**　Cisco TAC に情報を送信するときは、このコマンドで取得した DPE バンドル、および RDU で取得したステート　　バンドルを送信する必要があります。このバンドルを生成するには、*BPR_HOME*/rdu/bin ディレクトリから **bundleState.sh** コマンドを実行します。

*BPR_HOME*/rdu/bin/bundlestate のスクリプトは、RDU で利用できます。このスクリプトは、Cisco TAC に情報を送信するときに、RDU システム ステート（ログなど）をバンドルするために使用します。

コマンドを入力すると、DPE の現在のステートがまとめてバンドルされます。そのバンドル ファイルは圧縮され、TAC で使用されるものとして識別されます。

**シンタックスの説明**　キーワードや引数はありません。

**例**

```
dpe# support bundle state
Creating state bundle for Cisco support...
+ /outgoing/state-20060721-000340.bac
+ Adding a process listing to the support bundle...
+ Adding a network connection listing to the support bundle...
+ Adding and compressing files for support bundle...
+ Size: 1205782 bytes
```


## 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）**

DSL フォーラムの CPE WAN 管理プロトコル（TR-069 仕様で定義されている規格）を使用して、Subscriber Edge サービスのプロビジョニングと管理を行うブロードバンド サービス プロバイダーの統合ソリューションです。BAC は、大量のデバイスをサポートすることができるスケーラブルな製品です。

## C

**CPE WAN 管理プロトコル（CWMP）**

DSL フォーラムの 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して、オペレータ効率を高め、ネットワーク管理の問題を減らします。

## D

**Device Provisioning Engine（DPE）**

Device Provisioning Engine 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提供します。

## 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）**

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。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）** インターネット経由で私的な文書を伝送するためのプロトコル。SSL で使用される暗号システムでは、データを暗号化するために 2 種類の鍵が使用されます。公開鍵は一般に公開される鍵で、秘密鍵はメッセージの受信者以外には公開されない鍵です。慣習的に、SSL 接続を要求する URL は *http:* ではなく、*https:* で始まります。BAC 3.0 は、SSLv3 をサポートしています。
「TLS」を参照。

## T

**Transport Layer Security（TLS）** インターネット上で通信を行うクライアント / サーバ アプリケーションの間で、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。
「SSL」を参照。

**TR-069** CPE と自動構成サーバの間の通信をイネーブルにする CPE WAN 管理プロトコル（CWMP）を定義する規格。

## 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 送信を可能にし、最適な QoS と優れた費用対効果を発揮するメカニズム。

## 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 モジュールが鍵交換、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を提供します。

## 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 および 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）** Fully qualified domain name。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です。

## し

**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

**デバッグ** 管理者がプログラムを段階的に実行し、データを検査し、変数の値などの条件を監視するのを可能にする、プログラムのデバッグを支援するために設計されたオペレーション。

**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規則が含まれる XML ファイル。

## ね

**ネットワーク管理者** ネットワークの運用、メンテナンス、および管理を担当する人。

**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。

## 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** ネットワーク トポロジまたは地理的条件に基づいて、関連付けられた DPE サーバの定義済みセットを持つデバイスのグループ。

## め

**命令生成** RDU でデバイスに対するポリシー命令を生成し、それらの命令を DPE に配信する処理。これらの命令は DPE でキャッシュされ、CPE で実行する必要があるアクションに関して通知を受けます。このアクションには、設定、ファームウェアのアップグレード、およびその他のオペレーションなどがあります。


## C



## D

## F



## S



## T



## あ



## か



## こ

## さ



## し

## ち



## て

## と



## ね



## ふ



## ほ



## ま



## よ



## ら



## ろ