CHAPTER 2

Broadband Access Center for Cable システム アーキテクチャ

この章では、この Broadband Access Center for Cable（BACC）リリースで実装されるシステム アーキテクチャについて説明します。この章に示すアーキテクチャは、あくまでも説明のためであり、BACC 製品を使用する場合のバックグラウンドとして示すものです。

アーキテクチャ

ここでは、以下のコンポーネントから成る BACC 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。
  - BACC システムの権限あるデータ格納
  - API の要求を処理するためのサポート
  - デバイス検出エンジン、デバイス構成エンジン、デバイス中断エンジン。デバイスの種類の決定、構成の生成、特定のデバイス中断のサポートのために、インストールされているさまざまな拡張機能を呼び出します。

  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。
  - TFTP プロトコル サーバ
  - 構成のキャッシュ
  - 冗長性
  - 時刻サーバ
  - PacketCable プロビジョニング サービス

  詳細については、P.2-6 の「Device Provisioning Engine」を参照してください。
- プロビジョニング グループ

  詳細については、P.2-11 の「プロビジョニング グループ」を参照してください。
- Cisco Network Registrar サーバ。次の機能を提供します。
  - ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）
  - ドメイン ネーム システム（DNS）

  詳細については、P.2-12 の「Cisco Network Registrar」を参照してください。
- Kerberos サーバ。PacketCable MTA を認証します。詳細については、P.2-14 の「鍵発行局」を参照してください。
- SNMP エージェント。次の機能を提供します。
  - SNMP バージョン v2c のサポート
  - SNMP 通知のサポート

  詳細については、P.2-19 の「SNMP エージェント」を参照してください。
- BACC エージェント。次の機能を提供します。
  - すべての重要な BACC 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
  - BACC 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.2-20 の「BACC エージェント」を参照してください。

登録モード

登録モードによって、サービス プロバイダーは加入者との対話数を制御することができます。登録されたすべてのデバイスを対象に、サービス プロバイダーはデバイスに対する変更があれば処理するように準備する必要があります。そのため、背後に登録解除されたコンピュータのあるケーブル モデムを 100 台登録する作業と、背後に登録済みのコンピュータが大量に存在する可能性のあるケーブル モデムを 100 台登録する作業には、大きな違いがあります。この理由により、サービス プロバイダーは登録モードを標準モード、無差別モード、およびローミング モードから慎重に選択する必要があります。

標準モード

標準モード（固定モードとも呼ぶ）で動作しているときに、コンピュータを別のケーブル モデムの背後に移すと、そのコンピュータにはプロビジョニング解除されたアクセス権が与えられます。

無差別モード

デバイスだけが登録されます。DHCP サーバは別のデバイスの背後で動作するデバイスのリース情報を維持します。登録されたデバイスの背後にあるすべてのデバイスは、ネットワーク アクセスを受け付けます。

ローミング モード

ローミング モードでは、登録されたデバイスが他のすべての登録済みデバイスの背後にあるサービス クラスを受け付けることができます。これによって、たとえば、場所を移動しながらラップトップを使用し、複数のケーブル モデムからサービスを入手することができます。

混在モード

無差別モードとローミング モードを混在させて、2 つの別個のモードとして使用し、同時に共存させることもできます。

Regional Distribution Unit

RDU は BACC プロビジョニング システムの主要サーバです。RDU は以下の機能も提供します。

- デバイス構成生成の管理
- BACC システムの権限あるデータ格納
- デバイス中断
- すべてのアプリケーション プログラミング インターフェイス（API）の要求が通過する情報センター機能
- BACC 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。また、RDU は以下のこともサポートします。

- API によるデータ アクセスと操作
- スケーラビリティのための DPE への構成の分配
- 外部クライアント、オペレーション サポート システム（OSS）、API によるその他のプロビジョニング関連の機能性

RDU の概念については、次のセクションで説明します。

- デバイス構成の生成（P.2-4）
- サービス レベル選択（P.2-5）
- Regional Distribution Unit のフェールオーバー（P.2-5）

（注）　RDU は、DPE および Network Registrar 拡張の名前を、それらが RDU に接続するインターフェイスによって判別します。つまり、DPE または Network Registrar 拡張の名前は、RDU マシンが判断した名前になります。このため、RDU でその名前を解決（両方向）できる必要があります。

デバイス構成の生成

デバイスはブート時に BACC に構成を要求します。この構成がデバイスのサービス レベルを決定します。デバイス構成には、DHCP IP アドレスの選択、帯域幅、データ レート、フロー制御、通信速度、サービス レベルなど、顧客が必要とするプロビジョニング情報を含めることができます。構成には、任意のデバイスの DHCP 構成と TFTP ファイルを含めることができます。プロビジョニングされていないデバイスがインストールされ、ブート操作が実行されると、適切な技術のデフォルト設定が BACC から入手され、DHCP または TFTP によってデバイスに送信されます。サポートされる技術ごとに、デフォルトの設定を変更することができます。

サービス レベル選択

サービス レベル選択拡張ポイントは、RDU が使用する基準を決定し、デバイス構成の生成時に使用される基準を RDU に通知します。RDU は各デバイスについてこの情報を RDU データベースに保存します。デバイスは 1 つの基準セットを受け付けるように登録されていても、実際には 2 つ目のセットを選択する場合があります。構成生成の拡張は、選択された基準を検索して使用します。したがって、RDU 自動再生成は 2 つ目の基準セットが使用されることを認識するので、その基準に何らかの変更が発生した場合にはデバイス構成が再生成されます。

サービス レベル選択拡張ポイントは、さまざまなテクノロジー デフォルト ページで入力されます（詳細については、P.10-8 の「デフォルトの設定」を参照）。これらは拡張のカンマ区切りリストとして入力され、その特定の拡張ポイント向けの拡張として使用できるオブジェクトの作成をインスタンス化します。これらのプロパティにはデフォルトで、ゼロまたは組み込み拡張の 1 つが入力されます。独自のカスタム拡張をインストールしている場合を除き、これらの拡張は修正しないでください。

Regional Distribution Unit のフェールオーバー

最新バージョンの Broadband Access Center for Cable では、1 回のインストールにつき 1 つの RDU をサポートします。フェールオーバーに対応するには、お持ちのハードウェアの冗長システムをご利用になるか、ホットスワップ機能を持つ同様のシステムをご用意ください。

Device Provisioning Engine

Cisco Device Provisioning Engine（DPE）は RDU と通信して、デバイスに構成を割り当てます。各 DPE は最大 100 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、デバイスの設定ファイルの提供を含むすべての構成要求を処理します。DPE は Cisco Network Registrar DHCP サーバと統合され、各デバイスの IP アドレスの割り当てを制御します。複数の DPE が単一の DHCP サーバと通信することができます。

DPE は以下のアクティビティを管理します。

- 最終段階のデバイス構成の生成（DOCSIS タイムスタンプなど）
- 組み込み TFTP サーバを介した設定ファイルのやり取り
- Cisco Network Registrar との統合
- 時刻プロトコル サーバ
- 音声技術プロビジョニング サービス

Device Provisioning Engine の種類

最新バージョンの BACC では、従来のハードウェア デバイス（DPE-590 または DPE-2115 のいずれか）と、ソフトウェア限定の Solaris DPE の 2 種類の DPE がサポートされます。詳細については、P.2-6 の「ハードウェア Device Provisioning Engine」および P.2-7 の「Solaris Device Provisioning Engine」を参照してください。

ここでは、さまざまな種類の DPE の他、以下の主要な DPE コンポーネントについて説明します。

- DPE ライセンス キー（P.2-7）
- TACACS+ および DPE 認証（P.2-7）
- DPE サーバの割り当て（P.2-8）
- TFTP サーバ（P.2-9）
- プロビジョニング グループ（P.2-11）

ハードウェア Device Provisioning Engine

最新バージョンの BACC では、DPE-590 および DPE-2115 ハードウェア Device Provisioning Engine をサポートします。デバイス自体、ポート、コネクタ、および背面パネルのコンポーネントの詳細については、次のマニュアルを参照してください。

- DPE-590 の場合は、『*Cisco Content Engine 500 Series Hardware Installation Guide*』を参照してください。次の URL からアクセスできます。

  www.cisco.com/en/US/products/hw/contnetw/ps761/products_installation_guide_book09186a00800801e0.html

- DPE-2115 の場合は、『*Installation and Setup Guide for the Cisco 1102 VLAN Policy Server*』を参照してください。次の URL からアクセスできます。

  www.cisco.com/en/US/products/sw/secursw/ps2136/products_installation_and_configuration_guide_book09186a00801f0d02.html

（注）　DPE-2115 と Catalyst スイッチとの間のインターフェイス リンクが中断されるときは、データ トラフィックが流れる前にデフォルトの 30 秒遅延が発生しています。

Solaris Device Provisioning Engine

Solaris DPE は、Solaris 8 または Solaris 9 オペレーティング システムで動作するコンピュータに BACC 製品の当該部分がインストールされているという点を除き、ハードウェア DPE と同じように機能します。ごく少数の例外を除き、ハードウェアでも Solaris DPE でも、同じコマンドライン インターフェイス CLI が使用されます。各 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 for Cable Command Line Interface Reference*』を参照してください。

DPE ライセンス キー

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、そのような新しい DPE は登録されず、拒否されます。一方、既存の有効な DPE はオンラインのままとなり、任意で RDU に再登録されます。

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

RDU に登録する DPE のライセンス数には、バージョン番号または種類に関係なく、ハードウェアと Solaris DPE が含まれます。BACC ラボ インストールの一部として利用されるものも含まれます。詳細については、『*Broadband Access Center for Cable Installation Guide*』を参照してください。

ライセンスの追加、評価ライセンスの拡張、評価ライセンスの満了のいずれか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 DPE を削除すると、ライセンスは解放されます。

削除された DPE は、対応するすべてのプロビジョニング グループから除外され、DPE が利用不可能となったことが Network Registrar のすべての拡張部分に通知されます。そのため、過去に削除された DPE が再登録されると、再びライセンスが与えられたとみなされ、RDU から再び削除されるまで、あるいはライセンスが満了するときまでその状態が続きます。

RDU を介してライセンスが与えられていない 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、DPE と RDU のログファイル（dpe.log と rdu.log）を調べる必要があります。

BPR 2.0.x または BACC 2.5 のいずれかを実行する削除済みもしくはライセンスなしのハードウェア DPE は、常に RDU への登録を試みます。これは、上記のバージョンのソフトウェアを実行するデバイスにとって正常な動作であり、拒否された登録はすべて RDU ログ、およびこの状況を識別する SYSLOG アラートの生成に記録されます。

TACACS+ および DPE 認証

Terminal Access Controller Access Control System plus（TACACS+）は TCP ベースのプロトコルで、多数のネットワーク デバイスを対象とする中央集中型のアクセス コントロールと、DPE CLI のユーザ認証をサポートします。TACACS+ を使用して DPE は複数のユーザをサポートすることができます。各ユーザ名とログインおよびイネーブル パスワードは TACACS+ サーバで設定されます。TACACS+ は TACACS+ クライアント / サーバ プロトコルを実装するために使用されます（ASCII ログインのみ）。

TACACS+ 特権レベル

TACACS+ サーバは TACACS+ プロトコルを使用して DPE にログインするユーザを認証します。TACACS+ クライアントはそのユーザに設定される特定のサービス レベルを指定します。表 2-1 は、DPE ユーザのアクセスを許可するために使用される 2 つのサービス レベルを示します。

表 2-1　TACACS+ サービス レベル

モード	説明
ログイン	router> プロンプトでのユーザレベル コマンド
イネーブル	router# プロンプトでのイネーブルレベル コマンド

TACACS+ クライアント設定

TACACS+ は Command Line Interface（CLI; コマンドライン インターフェイス）を使用して設定される多数のプロパティを使用します。これらの TACACS+ 関連の CLI コマンドについては、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

TACACS+ をイネーブルにする場合、管理者はすべての TACACS+ サーバの IP アドレスまたは FQDN を、デフォルト値以外を使用して指定する必要があります。

管理者は次の設定についても、該当する場合はデフォルト値を使用して指定することができます。

- 各 TACACS+ サーバの共有秘密キー。このキーは DPE と TACACS+ サーバとの間のデータ暗号化に使用されます。特定の TACACS+ サーバの共有秘密情報を省略するように選択した場合、TACACS+ メッセージ暗号化は使用されません。
- TACACS+ サーバのタイムアウト値。これは、TACACS+ サーバがプロトコル要求に応答するのを TACACS+ クライアントが待機する最長時間です。
- TACACS+ サーバのリトライ回数。これは、TACACS+ クライアントが TACACS+ サーバとの有効なプロトコル交換を試みる回数を示します。

（注）　これらのコマンドは、ハードウェア DPE と Solaris DPE の両方で使用できます。ハードウェア DPE ではコンソール モードだけが使用できます。

DPE サーバの割り当て

BACC は複数の DPE をサポートします。それらの DPE はデバイス、DHCP フェールオーバー構成、および RDU と通信します。インストール中に、以下のように DPE の割り当てを行う必要があります。

- 1 つ以上のデバイス論理グループまたはプロビジョニング グループに責任を負うように DPE を割り当てる。
- RDU の IP アドレスとポート番号

DPE の主な目的は、顧客のデバイスの電源投入またはリブートのたびに、そのデバイスに構成を送信することです。これを迅速に実行するために、DPE は各デバイスの構成のコピーをローカル キャッシュ データベースに保存します。

（注）　DPE は単一のプロビジョニング グループに割り当てる必要があります。

TFTP サーバ

統合された TFTP サーバは、デバイスおよびデバイス以外の要求元から DOCSIS 設定ファイルを含むファイル要求を受信します。その後、このサーバは要求元にファイルを送信します。

TFTP サーバは、ローカル ファイル システム アクセスに利用されるホーム ディレクトリに配置されます。ローカル ファイルは BACC_DATA/dpe/tftp ディレクトリに格納されます。

デフォルトでは、TFTP サーバは TFTP 読み取り用のキャッシュだけに表示されます。ただし、tftp allow-read-access コマンドが実行された場合は、TFTP サーバはキャッシュを確認する前にまずローカル ファイル システムを確認します。ファイルがローカル ファイル システムにある場合は、そこから読み取られます。そうでない場合は、TFTP サーバはキャッシュを確認します。そこにファイルがあれば、サーバはそれを利用します。そこにファイルがない場合は、サーバはファイル要求を RDU に送信します。ローカル ファイル システムからの読み取りアクセスをイネーブルにできる場合、ディレクトリ構造読み取り要求はローカル ファイル システムからだけ許可されます。

BACC はローカル ファイル システムへの書き込みだけを許可します。DPE キャッシュへの書き込みは一切許可しません。tftp allow-write-access DPE CLI コマンドを実行すると、BACC は TFTP ホーム ディレクトリへの書き込みを許可します。デフォルトでは、ディレクトリまたは上書きファイルの作成は許可されません。これを変更するには、tftp allow-create-dirs コマンドまたは tftp allow-override コマンドを実行します。

DOCSIS 共有秘密情報

動的 DOCSIS 設定ファイルについてのみ、BACC を使用して、複数の異なる DOCSIS Shared Secret（DSS; DOCSIS 共有秘密情報）を異なる CMTS に属するデバイス上で定義することができます。このように、信頼のおけない共有秘密情報により、信頼のおけない CMTS の数は限られたものとなり、配置全体のすべての CMTS が対象となることはありません。

DSS は DPE ごとに設定できますが、プロビジョニング グループ単位で設定する必要があり、そのプロビジョニング グループで CMTS に設定されている内容と一致する必要があります。

注意　単一のプロビジョニング グループ内で複数の DSS を設定すると、場合によっては CMTS のパフォーマンスが低下する可能性があります。これは、実質的に BACC には何の影響もありません。

共有秘密情報は、クリア テキストまたは IOS 暗号化形式で入力できます。

クリア テキストで入力する場合、DSS は IOS バージョン 12.2BC に適合するように暗号化されます。また、管理者のユーザ インターフェイスまたは API を使用して RDU から DSS を設定することもできます。この場合、DSS はクリア テキストで入力され、RDU に格納され、すべての DPE に渡されます。そのため、このように入力された DSS は DPE に保存される前に暗号化されます。

対応する CLI コマンドを使用して直接 DSS を DPE で設定する場合、この設定は RDU から設定する内容よりも優先されます。

DOCSIS 共有秘密情報のリセット

DSS のセキュリティが侵害された場合、または管理目的で共有秘密情報を変更する場合には、CLI コマンドの show running config を実行し、表示された設定から DOCSIS 共有秘密情報の行を DPE 設定にコピー アンド ペーストして戻すことができます。このようにして、Cisco CMTS での入力内容を DPE CLI にコピーすることができます。詳細については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

（注）　上で説明したように共有秘密情報を変更するには、CMTS が V 12.2BC より新しいソフトウェア バージョンで実行されている必要があります。

DSS を変更する必要があるときは、次の作業を行う必要があります。

ステップ 1　リセットする DOCSIS 共有秘密情報を持つプロビジョニング グループを確認します。

ステップ 2　そのプロビジョニング グループに関連付けられた DPE および CMTS のリストを調べます。

ステップ 3　CMTS 上でプライマリ DSS を変更します。

ステップ 4　CMTS 上で信頼のおけない DSS をセカンダリ DSS に変更します。これにより、すべての DOCSIS 設定ファイルが新しい DSS を使用するように正しく変更されるまで、ケーブル モデムで登録を続行できるようにする必要があります。

ステップ 5　影響を受けた DPE を判別し、それぞれ DSS を変更します。

ステップ 6　DOCSIS 設定ファイルが新しい DSS を使用していることを確認してから、CMTS の信頼のおけないセカンダリ共有秘密情報を CMTS 設定から削除します。

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、2 つ以上の DPE と DHCP サーバのフェールオーバー ペアから成る地域別のサーバのグループ化を目的として設計されています。この設計により、最高 100 万個のデバイスのプロビジョニングの必要性に対処することができます。デバイスの数が 100 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。

（注）　プロビジョニング グループのサーバは各地域に設置される必要はありません。中央の NOC に簡単に配置することができます。

冗長性とロード シェアリングをサポートするために、各プロビジョニング グループは任意の数の DPE に対応できます。DHCP サーバから要求が入ってくると、その要求はプロビジョニング グループの DPE 間に分配され、デバイスと特定の DPE の間にアフィニティが確立されます。プロビジョニング グループ内の DPE が安定した状態にある間、このアフィニティは保たれます。特定のデバイスは通常同一の DPE に割り当てられるため、負荷がかかる Kerberos チケット再発行処理を行わずに済みます。

Cisco Network Registrar

Network Registrar には、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）およびドメイン ネーム システム（DNS）の機能があります。完全な管理ユーザ インターフェイスがあり、カスタマイズされた BACC 設定画面と組み合せれば、大規模な企業管理システム内で利用できます。

（注）　Network Registrar の詳細については、『*Network Registrar User's Guide*』、『*Network Registrar CLI Reference*』、および『*Network Registrar Installation Guide*』を参照してください。

ダイナミック ホスト コンフィギュレーション プロトコル

DHCP サーバは、TCP/IP ネットワーク上で IP アドレスを設定するプロセスを自動化します。このプロトコルは、デバイスをネットワークに接続するときにシステム管理者が遂行する機能の多くを実行します。DHCP はネットワーク ポリシーの決定を自動的に管理するため、手動の設定が不要になります。これにより、ネットワーク デバイスの設定の柔軟性と可動性が高まり、管理しやすくなります。

DHCP フェールオーバーを使用すると、DHCP サーバ ペアの一方が機能を停止した場合に他方が処理を引き継げるようにサーバが機能します。サーバのペアをプライマリ サーバとバックアップ サーバと呼びます。通常の状況では、プライマリ サーバがすべての DHCP 機能を実行します。プライマリ サーバが使用できなくなった場合、バックアップ サーバが処理を引き継ぎます。このようにして DHCP フェールオーバーは、プライマリ サーバの障害時に DHCP サービスの利用停止を防ぎます。

ドメイン ネーム システム

ドメイン ネーム システム（DNS）サーバは、IP アドレス、ホスト名、ルーティング情報など、ネットワーク全体のホストに関する情報を格納します。DNS は主に IP アドレスとドメイン名との変換のためにその情報を利用します。このように www.cisco.com などの名前を IP アドレスに変換することで、インターネットベースのアプリケーションへのアクセスが簡素化されます。

DNS ディレクトリ サービスには次のものが含まれます。

- DNS データ
- DNS サーバ
- サーバからデータを呼び出すためのインターネット プロトコル
- 音声プロビジョニングのためのダイナミック DNS

リース予約

BACC リース予約は、Network Registrar の Central Configuration Management（CCM）と連動して、プロビジョニング時にデバイスに固定 IP アドレスを割り当てます。

新しいデバイスのプロビジョニング時に、BACC は IP アドレスが指定されているかどうかを判別し、アドレスが有効な IP アドレスであることを確認する Network Registrar サーバを判別します。確認後に、リース予約機能により、Network Registrar CCM を使用してデバイスの予約が作成されます。

リース予約は BACC でサポートされるすべてのテクノロジーで動作します。次の機能があります。

- BACC グラフィカル ユーザ インターフェイスを使用した IP アドレス予約の追加および削除が可能になります。詳細については、P.9-14 の「デバイスの管理」を参照してください。
- すでに使用されている IP アドレスを予約しようとして発生したすべてのエラー、または予約が CCM サーバから削除されているかどうかについて報告します。

（注）　リース予約が適切に動作するためには、ライセンスを取得した CCM サーバが存在する CNS Network Registrar バージョン 6.1.2.3 をネットワークにインストールしておく必要があります。

BACC にリース予約を実装する前に、CCM アドレス、ポート、ユーザ名、およびパスワードを設定する必要があります。これらのパラメータは RDU Defaults ページから設定します。変更は動的に行われ、入力後すぐ有効になります（これらの構成パラメータについては、P.10-20 の「RDU Defaults」を参照）。

（注）　リース予約機能はデフォルトでは無効に設定され、所定の時間 CCM にアクセスできないときはタイムアウトになります。

鍵発行局

Key Distribution Center（KDC; 鍵発行局）は、MTA を認証してセキュリティ チケットを与えるのに利用される認証サーバです。

（注）　KDC はマルチプロセッサ コンピュータでサポートされます。

デフォルトの KDC のプロパティ

KDC には、BACC のインストール中に <BACC_HOME>/kdc/solaris/kdc.ini プロパティ ファイルに読み込まれるデフォルトのプロパティがいくつかあります。このファイルを編集し、操作要求に応じて値を変更することができます。変更を行った後、プロパティ ファイル、キー、または証明書の変更を有効にするには KDC を再起動する必要があります。デフォルトでは、プロパティは以下のように設定されています。

- interface address: Kerberos 着信メッセージのために KDC に監視させる必要があるローカル イーサネット インターフェイスの IP アドレスです。次に例を示します。

  ```
  interface address = 10.10.10.1
  ```

- FQDN：KDC がインストールされている Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を識別します。次に例を示します。

  ```
  FQDN = kdc.cisco.com
  ```

（注）　インストール中に、KDC Realm Name 画面から interface address と FQDN を入力します。詳細については、『*Broadband Access Center for Cable Installation Guide*』を参照してください。

- maximum log file size : KDC が一連のログファイルを生成します。このプロパティはログファイルの最大サイズ（キロバイト）を指定します。そのため、最新ファイルがこの最大サイズに達したときに限り、KDC は新しいログファイルを作成します。次に例を示します。

  ```
  maximum log file size = 1000
  ```

- *n* saved log files：KDC が保存する古いログファイルの数を定義します。デフォルト値は 7 ですが、必要に応じた数を指定することができます。次に例を示します。

  ```
  n saved log files = 10
  ```

- log debug level：ログファイルのロギング レベルを指定します。

  ```
  log debug level = 5
  ```

- minimum (maximum) ps backoff：BACC が FQDN-REQUEST に応答するまでの KDC の最短（または最長）待ち時間を 0.1 秒単位で指定します。次に例を示します。

  ```
  minimum ps backoff = 150
  ```

上記の例の値を使用すると、例に挙げた INI ファイルに含まれるデータは例 2-1 と同じになります。

例 2-1　サンプル KDC INI 設定ファイル

```
interface address =  10.10.10.1
FQDN = kdc.cisco.com
maximum log file size = 1000
n saved log files = 10
log debug level = 5
minimum ps backoff = 150
maximum ps backoff = 300
```

最短および最長のチケット継続時間を設定すると、配置中に発生する可能性がある過剰な数のチケット要求を効果的に取り除くことができます。大半の配置が従来の勤務時間中に行われ、過度の負荷がパフォーマンスに悪影響を及ぼす場合があることを考えると、これは有益なことです。

（注）　チケット継続時間を短くすると、MTA は頻繁に KDC を認証しなければならなくなります。この方法により電話エンドポイントの認証に対する管理が強まる一方、KDC に対するメッセージの負荷がはるかに重くなり、ネットワークのトラフィックも増加します。たいていの場合、デフォルトの設定は適切であり、変更は必要ありません。

- maximum ticket duration : KDC が生成するチケットの最長継続期間を定義します。デフォルトの単位は「時間」ですが、**m** または **d** を追加すると、それぞれ単位が「分」、「日」に変更されます。

  デフォルトの値は 168（7 日間）です。これは PacketCable のセキュリティの仕様を満たすのに必要な継続時間であるため、この値を変更しないことをお勧めします。次に例を示します。

  ```
  maximum ticket duration = 168
  ```

- minimum ticket duration : KDC が生成するチケットの最短継続期間を定義します。デフォルトの単位は「時間」ですが、**m** または **d** を追加すると、それぞれ単位が「分」、「日」に変更されます。

  デフォルトの値は 144（6 日間）です。この値を変更しないことをお勧めします。次に例を示します。

  ```
  minimum ticket duration = 144
  ```

Euro-PacketCable のサポート

Key Distribution Center（KDC; 鍵発行局）コンポーネントは、Euro-PacketCable（tComLabs）証明書チェーンをサポートします。例 2-2 に Euro-PacketCable 対応の KDC 設定ファイルの例を示します。

例 2-2　Euro-PacketCable 対応の KDC 設定ファイルの例

```
[general]
interface address = 10.10.10.1
FQDN = servername.cisco.com
maximum log file size = 10000
n saved log files = 100
log debug level = 5 minimum
ps backoff = 150 maximum
ps backoff = 300
euro-packetcable = true
```

KDC 証明書

KDC の認証に使用される証明書は BACC に同梱されていません。Cable Television Laboratories Inc.（CableLabs）から必要な証明書を入手する必要があります。その証明書の内容は MTA にインストールされているものと一致しなければなりません。詳細については、P.12-42 の「KDC 証明書を管理するための PKCert.sh ツールの使用方法」を参照してください。

注意　証明書がインストールされないと、KDC は機能しません。

KDC ライセンス

シスコの代理店から KDC ライセンスをご入手のうえ、適切なディレクトリにインストールしてください。

KDC ライセンス ファイルをインストールするには、以下の手順を実行します。

ステップ 1　ライセンス ファイルを入手します。

ステップ 2　ライセンス ファイルを <BACC_HOME>/kdc ディレクトリにコピーします。

注意　ASCII ファイルとしてコピーしないように注意してください。このファイルには、ASCII 転送中に不要な変更が行われやすいバイナリ データが含まれています。

ステップ 3　KDC ライセンス ファイルの名前が **backkdc.license** ではない場合、ファイル名を **bacckdc.license** に変更します。

ステップ 4　/etc/init.d ディレクトリから **bprAgent restart kdc** コマンドを実行して、KDC サーバを再起動し、変更を有効にします。

（注）　KDC ライセンス ファイルは転送プロセスにより損傷を受ける可能性があるため、異なるオペレーティング システム間でコピーすることはできません。

複数領域のサポート

BACC KDC は複数領域の管理をサポートします。

追加領域を設定するには、次の手順に従います。

ステップ 1　KDC 証明書が格納されているディレクトリを見つけます。

ステップ 2　そのディレクトリに、目的の領域名と一致する名前のサブディレクトリを作成します。このサブディレクトリは大文字だけを使用して作成する必要があります。

ステップ 3　このディレクトリに、領域の KDC 証明書および秘密鍵を配置します。

ステップ 4　新しい領域が KDC 証明書と同じサービス プロバイダーにチェーン化されていない場合は、証明書ディレクトリ内の証明書とは異なる、より高いレベルの追加証明書をすべて含めます。ただし、すべての領域は同じ証明書チェーンをルートとする必要があるため、KDC のインストールごとに 1 つのロケール（PacketCable、Euro-PacketCable）だけがサポートされます。

（注）　指定された任意の DPE は単一の領域にサービスを提供するように制限されます。

BACC MIB

Broadband Access Center for Cable はさまざまな MIB をサポートします。次の MIB があります。

- CISCO-BACC-DPE-MIB：P.2-19 の「MIB のサポート」を参照してください。
- CISCO-APPLIANCE-MIB：P.2-19 の「MIB のサポート」を参照してください。
- CISCO-BACC-RDU-MIB：P.2-19 の「SNMP エージェント」を参照してください。
- CISCO-BACC-SERVER-MIB：すべての BACC サーバに共通する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 BACC 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。

表 2-2 に、インストールのタイプに応じた BACC MIB のサポートをまとめます。各インストール タイプの説明については、『*Cisco Broadband Access Center for Cable Installation Guide*』を参照してください。

表 2-2　BACC でサポートされる MIB

インストールのタイプ	サポート対象の MIB
Solaris DPE	CISCO-BACC-SERVER-MIB
	CISCO-BACC-DPE-MIB
ハードウェア DPE	RFC1213 - MIB II
	CISCO-APPLIANCE-MIB
	CISCO-BACC-SERVER-MIB
	CISCO-BACC-DPE-MIB
RDU	CISCO-BACC-SERVER-MIB
	CISCO-BACC-RDU-MIB

BACC エージェント

この項では、BACC エージェントの機能とエージェントが重要な理由について説明します。続いて、エージェントの使用および理解に必要なすべての詳細情報について説明します。対象のエージェントは次のとおりです。

SNMP エージェント

BACC 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。BACC SNMP エージェントでは SNMP 通知と SNMP トラップの両方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 設定コマンドライン ツールの詳細については P.12-49 の「snmpAgentCfgUtil.sh コマンドの使用方法」、DPE CLI の詳細については『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

MIB のサポート

RFC 1213（MIB-II）の他、SNMP エージェントは CISCO-CW-APPLIANCE-MIB もサポートします。この MIB はハードウェア DPE にインストールされたソフトウェア コンポーネントの管理対象オブジェクトを定義します。MIB は CPU、メモリ、およびディスクの使用率を監視し、使用率が特定のしきい値を上回ると通知を生成します。通知は、イネーブルとディセーブルを選択して設定できます。リソースの使用率は定期的にポーリングされ、連続する 2 つのデータ ポイントの平均がしきい値を上回ると、通知が生成されます。

SNMP エージェントは CISCO-BACC-DPE-MIB もサポートします。この MIB は Solaris DPE にインストールされたソフトウェア コンポーネントの管理対象オブジェクトを定義します。DPE は、すべてのサポート対象デバイスで使用されるデバイス構成および設定ファイルのローカル キャッシュを管理します。この MIB によって、TFTP サーバおよび ToD サーバのエントリなど、いくつかの基本 DPE 設定および統計情報が提供されます。

SNMP エージェントでは、Cisco NMS アプリケーションの状態の通知と関連オブジェクトを定義する CISCO-NMS-APPL-HEALTH-MIB がサポートされます。そのような通知は、NMS アプリケーションの状態を知らせるために OSS/NMS に送信されます。たとえば、開始、中止、機能不全、使用中、またはアプリケーションの何らかの異常終了などの状態を通知します。デフォルトの MIB として MIB-II が使用されます。

SNMP エージェントでは、RDU サーバの起動、シャットダウン、障害、または終了状態の変化を知らせるために cnaHealthNotif トラップが生成されます。

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 には、RDU と DPE 間、および RDU と Network Registrar 間の統計情報を定義する管理対象オブジェクトも含まれます。

（注）　これらの MIB は <BACC_HOME>/rdu/mibs ディレクトリにあります。

BACC エージェント

BACC エージェントは、すべての BACC 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。

BACC エージェントは、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。

監視対象プロセス

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、BACC エージェント サーバは所定の時間待機してから再び再開を試みます。

（注）　Network Registrar の拡張を監視するには、BACC エージェントおよび SNMP エージェントを利用する必要はありません。

再開を試みる間隔は 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。
- BACC エージェント 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。
- BACC エージェント 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。
- BACC エージェント 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。
- BACC エージェント サーバは 16 秒間待機してからプロセスの再開を試み、4 回目の再開が失敗します。

BACC エージェント コマンドライン

BACC 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、このエージェントは、制御対象として設定されている BACC システム コンポーネントも起動します。BACC エージェントは単純なコマンド ライン インターフェイスからも制御できます。このためには、/etc/init.d ディレクトリから bprAgent コマンドを実行します。

表 2-3 は、BACC エージェントに利用できる CLI コマンドを示します。CLI は etc/init.d ディレクトリから実行できます。

表 2-3　BACC コマンドライン インターフェイス

コマンド	説明
bprAgent start	すべての監視対象プロセスを含む BACC 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 BACC エージェントを中止します。

表 2-3　BACC コマンドライン インターフェイス （続き）

コマンド	説明
bprAgent restart	すべての監視対象プロセスを含む BACC 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 BACC 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。

（注） 表 2-3 の中の <*process-name*> は、rdu プロセス、kdc プロセス、dpe プロセス、SnmpAgent プロセス、jrun プロセス（管理者およびサンプル ユーザ インターフェイスを実行する）のいずれかになります。CLI プロセスは Lab および DPE のインストール時にも監視されます。

（注） RDU は Solaris 環境で動作します。Solaris **reboot** コマンドが利用されるたびに正常にシャットダウンしないことがあります。システムを終了するための優先コマンドは、**shutdown** です。

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 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 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。

Regional Distribution Unit のログ

RDU には次の 2 つのログがあり、BACC_DATA/rdu/logs ディレクトリで保持されます。

- rdu.log：設定されたデフォルト レベルを持つ RDU イベントがすべて記録されます。デフォルトのログ レベルの設定方法については、P.12-40 の「RDU ログ レベルの設定」を参照してください。
- audit.log：BACC 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。

Device Provisioning Engine のログ

DPE では dpe.log ファイルが BACC_DATA/dpe/logs ディレクトリで保持されます。このファイルには、設定されたデフォルト レベルを持つすべてのイベントも記録されます。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。

DPE サーバで PacketCable がイネーブルになっている場合、DPE では詳細なデバッグ情報を提供するために SNMPService.logyyy.log ログ ファイルが使用されます。ファイルの内容を表示するには、DPE の CLI コマンドである **show packetcable snmp log** を使用します。このファイルも BACC_DATA/dpe/logs ディレクトリにあります。PacketCable コマンドの使用方法については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

（注）　PacketCable ログ メッセージは dpe.log ファイルに送信され、詳細な SNMP デバッグは SNMPService.logyyy.log ファイルに送信されます。

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 2-3 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 BACC）。
- SubFacility：BACC のサブシステムまたはコンポーネント。
- Severity Number：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.2-23 の「ログ レベルの設定」を参照してください。
  - 0：緊急。システムが不安定な状態です。
  - 1：アラート。すぐに対応が必要です。
  - 2：クリティカル。クリティカルな状態が存在します。

- 3：エラー。エラー状態が存在します。
- 4：警告。警告状態が存在します。
- 5：通知。通常ですが、重大な状態が存在します。
- 6：情報。情報メッセージのみです。

（注）　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。

- Message 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。

（注）　ロギングの詳細については、P.12-39 の「RDU ログ レベル ツール」を参照してください。

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。

例 2-3　ログ ファイルのサンプル

Domain Name	Data and Time	Facility	Sub-facility	Security Level	Msg ID	Message
BACC1:	2005 3 16 03:06:11 EST:	BPR-	RDU-		0236:	BPR Regional Distribution Unit starting up
BACC1:	2005 3 16 03:06:15 EST:	BPR-	RDU-	5	0566:	Initialized API defaults
BACC1:	2005 3 16 03:06:15 EST:	BPR-	RDU-	5	0567:	Initialized CNR defaults
BACC1:	2005 3 16 03:06:15 EST:	BPR-	RDU-	5	0568:	Initialized server defaults
BACC1:	2005 3 16 03:06:18 EST:	BPR-	RDU-	5	0570:	Initialized DOCSIS defaults
BACC1:	2005 3 16 03:06:18 EST:	BPR-	RDU-	5	0571:	Initialized computer defaults
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0573:	Initialized CableHome defaults
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0572:	Initialized PacketCable defaults
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0569:	Created default admin user
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0574:	Loaded 6 license keys
BACC1:	2005 3 16 03:06:20 EST:	BPR-	RDU-	5	0575:	Database initialization completed in 471 msec
BACC1:	2005 3 16 03:06:25 EST:	BPR-	RDU-	3	0015:	Unable to locate manifest file
BACC1:	2005 3 16 03:06:28 EST:	BPR-	RDU-	3	0280:	Command error

（注）　このログ ファイルでは KDC は考慮されていません。

dpe.log ファイルの表示

ログ ファイルの内容を表示するには、DPE の CLI から **show log** コマンドを使用します。詳細については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

BACC では、DHCP サーバの拡張から拡張のトレース レベル設定に基づいてログ メッセージが生成されます。拡張のトレース レベルは、管理者のユーザ インターフェイスを使用して変更することができます。

変更するには、次の手順に従います。

ステップ 1　DHCP Server を選択して、拡張設定を展開します。

ステップ 2　変更を有効にするため、DHCP サーバをリロードします。

管理者のユーザ インターフェイス

BACC 管理者のユーザ インターフェイスは、HTML ベースのアプリケーションで、システムに登録されたユーザとデバイスを設定および管理することができます。このユーザ 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。

- 第 8 章「管理者のユーザ インターフェイスについて」では、BACC 管理ユーザ インターフェイスへのアクセス方法と、各種のインターフェイス コンポーネントについて説明します。
- 第 9 章「Broadband Access Center for Cable 管理者のユーザ インターフェイスの使用方法」では、各種 BACC 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。
- 第 10 章「Broadband Access Center for Cable の設定」では、BACC を設定するために実行する作業について説明します。

サンプル ユーザ インターフェイス

BACC 製品には Sample User Interface（SUI; サンプル ユーザ インターフェイス）アプリケーションも付属しています。SUI の説明は、第 11 章「サンプル ユーザ インターフェイスの設定および使用方法」にあります。これは、ラボ テストのシナリオで BACC を使用して、セルフプロビジョニングと事前プロビジョニング、およびその他の BACC 基本機能を実行する場合のデモを行うために使用します。BACC のフル配備では、課金、OSS、およびワークフローの各アプリケーションのいずれかまたはすべてが SUI 機能を備えることになります。

注意　SUI を実稼動環境で使用することは想定されていません。デモでの使用のみを目的としています。