PacketCable 音声設定

この章では、PacketCable 音声を配備してサービスを提供するために必要となる、すべての作業について説明します。この章は、PacketCable の次の使用形態に関する情報を含んでいます。

- PacketCable EMTA のセキュア プロビジョニング（P.5-2）
- PacketCable EMTA の BASIC プロビジョニング（P.5-5）
- Euro-PacketCable（P.5-6）

また、PacketCable 音声技術の配備を妨げるおそれのある問題を解決するための情報も示します。

- eMTA プロビジョニングのトラブルシューティング（P.5-8）
- トラブルシューティングのツール（P.5-12）
- トラブルシューティングのシナリオ（P.5-13）
- 証明書信頼階層（P.5-17）

この章は、PacketCable MTA Device Provisioning Specification（PKT-SPPROV1.5-I01-050128）の内容を熟知している読者を対象としています。詳細については、www.packetcable.com を参照してください。

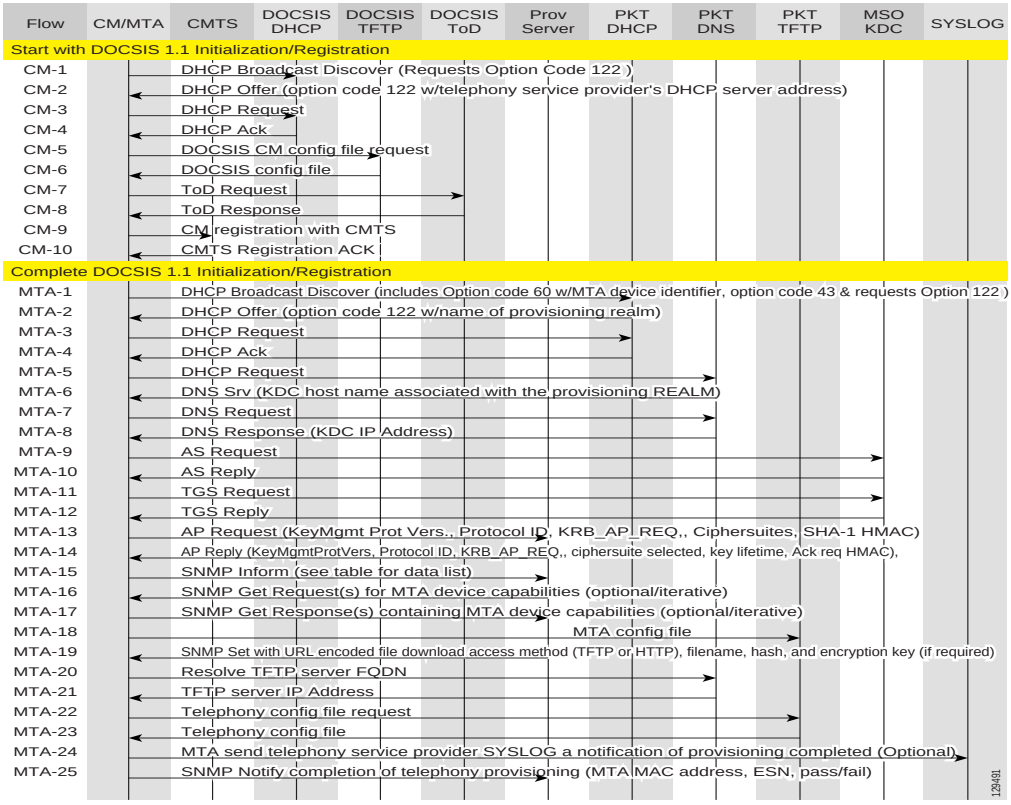
PacketCable EMTA のセキュア プロビジョニング

この項では、主にセキュアな PacketCable 音声プロビジョニングについて取り上げます。PacketCable Secure は、テレフォニー サービスの盗用や、悪意のあるサービス中断などが発生する可能性を最小限に抑えるように設計されています。PacketCable Secure では、Kerberos インフラストラクチャを利用して、MTA とプロビジョニング システムを相互に認証します。MTA とプロビジョニング システム間の対話をセキュリティで保護するために、SNMPv3 も使用されます。

BACC PacketCable のセキュアなプロビジョニングのフロー

PacketCable のプロビジョニングのすべてのフローは、一連のステップとして定義されます。EMTA プロビジョニングの問題点を診断するときは、ここで示すフロー説明を参考にすると、PacketCable プロビジョニング フローのどのステップが失敗しているかを特定できます。図 5-1 に、PacketCable 組み込み型 MTA のセキュアなプロビジョニングのフローを示します。

図 5-1　組み込み型 MTA のセキュアなプロビジョニングのフロー



（注）　データ パケットをキャプチャできるプロトコル アナライザ（プロトコル スニッファ）を使用して、どのステップが失敗しているかを正確に把握することを強くお勧めします。

また、KDC の障害の根本的な原因を把握するには、KDC ログ ファイルの内容が重要です。

1. CM-1 ～ 10 : これは通常の DOCSIS CM ブート フローで、PacketCable DHCP サーバのリストを MTA に提供するための DHCP オプション 122 が付加されます。MTA は、これらの DHCP サーバから DHCP OFFER を受け付けられるようになります。
2. MTA-1 ～ 4 : DHCP を使用して、MTA が自身を PacketCable MTA としてアナウンスし、どの機能およびプロビジョニング フロー（SECURE、BASIC など）をサポートしているかについて情報を提供します。MTA は、アドレス解決情報と DHCP オプション 122 も取得します。DHCP オプション 122 は、PacketCable ProvServ のアドレスとセキュリティ領域名を含んでいます。

   この情報は、MTA が KDC および ProvServer にアクセス可能になるために必要なものです。基本的なトラブルシューティングのヒントを次に示します。

   - CMTS 上で DHCP リレー エージェントが正しく設定されていることを確認する。CMTS が正しい DHCP サーバをポイントしていることを確認します。
   - MTA、CMTS、DHCP サーバ、DPE 間のルーティングが正しいことを確認する。
   - セカンダリ サブネットが CMTS 上で正しく設定されていることを確認する。
   - Network Registrar の DHCP 設定が正しいことを確認する。スコープが設定され、IP アドレスが利用可能であり、すべてのセカンダリ サブネットが設定されていることを確認します。
   - BACC の設定を確認する。cnr_ep.properties ファイルを確認して、必要な PacketCable CNR 拡張のプロパティが設定されていることを確認します。この properties ファイルの詳細については、付録 B「PacketCable DHCP オプションと BACC プロパティのマッピング」を参照してください。

     MTA がフロー ステップの MTA-1 ～ 2 を循環していることをパケット トレースで発見した場合は、DHCP オプション 122（領域名またはプロビジョニング サーバ FQDN のサブオプション）、DHCP オプション 12（ホスト名）、または DHCP オプション 15（ドメイン名）の設定に問題がある可能性があります。これらのオプションは、すべて MTA にとって必須となる DHCP コンテンツです。
3. MTA-5 ～ 8 : MTA が（DHCP オプション 122 で提供される）セキュリティ領域名を使用して、KDC サービスに対して DNS SRV ルックアップを実行し、KDC の IP アドレスを解決します。基本的なトラブルシューティングのヒントを次に示します。

   - パケット スニッファを使用して、Network Registrar DNS に送信される、送信先や形式が不正な DNS パケットを検出する。
   - Network Registrar DNS のログ レベルをパケット詳細トレースに設定して、Network Registrar DNS にどのようなパケットが到達するかを確認する。
   - DNS の設定を確認する。cnr_ep.properties に指定されている DNS サーバは、KDC の領域ゾーン、SRV レコード、および DNS「A」レコードを保持している必要があります。
4. MTA-9 : AS_REQ 要求メッセージが KDC によって使用され、MTA が認証されます。基本的なトラブルシューティングのヒントを次に示します。

   - KDC のログ ファイルを確認して、AS_REQ が到達しているかどうかを特定し、エラーや警告がないことを確認する。
   - KDC が、正しい MTA_Root 証明書を使用して設定されていることを確認する。MTA が AS_REQ メッセージに添付して送信する製造業者証明書およびデバイス証明書は、KDC にインストールされている MTA_Root 証明書とチェーンを構成する必要があります。

5. FQDN_REQ および FQDN_REP（フローには示していません）：KDC が MTA の MAC アドレスを MTA 証明書から抽出して、検証のために ProvServ に送信します。ProvServ がこの MAC アドレスの FQDN を保持している場合は、FQDN が KDC に返されます。KDC は、MTA から受信した FQDN を FQDN_REP 応答メッセージで受信した FQDN と比較します。

   基本的なトラブルシューティングのヒントを次に示します。

   - パケット スニッファを使用して、送信先や形式が不正な DNS パケットを検出する。MTA は、（MTA が DHCP オプション 122 で受信した）ProvServ の FQDN を AS_REP メッセージ内で KDC に渡します。KDC は、この FQDN を使用して ProvServ の IP アドレスを解決します。
   - KDC キー ファイルのファイル名と内容を確認する。DPE 内の KDC サービス キーは、KDC にあるサービス キーと一致している必要があります。KDC にあるサービス キー ファイルの名前は、非常に重要です。

6. MTA-10（AS_REP）：KDC がプロビジョニング サービス チケットを MTA に付与し、サービス プロバイダー証明書、ローカル システム プロバイダー証明書（オプション）、および KDC 証明書を MTA に送信します。MTA は、KDC によって送信された証明書が、MTA に格納されているサービス プロバイダー ルート証明書とチェーンを構成していることを確認します。これらの証明書がチェーンを構成していない場合、MTA はプロビジョニング フローのステップ MTA-1 に処理を戻します。KDC.cer ファイルの詳細については、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。基本的なトラブルシューティングのヒントを次に示します。

   - KDC のログ ファイルを表示して、AS_REP メッセージがデバイスに送信されたことを確認する。MTA がステップ MTA-1 ～ MTA-10 を循環していることをパケット トレースで発見した場合は、サービス プロバイダー証明書チェーンに問題があります。

7. MTA-13（AP_REQ）：MTA が、（MTA-10 で受信した）チケットを DHCP オプション 122 で指定されている ProvServ に提示します。

8. MTA-14（AP_REP）：ProvServ が KDC 共有秘密情報を使用して AP_REQ を復号化し、MTA の提示した ProvServ チケットを検証して、AP_REP を SNMPv3 キーを使用して送信します。以後の SNMPv3 は認証済みになり、必要な場合は暗号化されます。

9. MTA-15（SnmpV3 Inform）：MTA が、プロビジョニング情報を受信可能なことを ProvServ に通知します。

10. MTA-19（SNMPv3 SET）：ProvServ が、MTA 設定ファイルの URL、このファイルの暗号キー、およびこのファイルのハッシュ値を含んだ SNMPv3 SET を MTA に対して実行します。

11. MTA-22 ～ 23：MTA が、指定された TFTP サーバから VoIP 設定ファイルをダウンロードする処理を進めます。BACC によって、TFTP サーバが DPE コンポーネントに統合されていることに注意してください。

12. MTA-25（SnmpV3 Inform）：MTA が、新しい設定を受け付け可能かどうかを ProvServ に通知します。

PacketCable EMTA の BASIC プロビジョニング

BACC では、PacketCable BASIC もサポートしています。BASIC は、簡潔で DOCSIS に似た、ノンセキュアなプロビジョニング フローを提供します。

ここでは、BASIC.1 のフローについて説明します。

1. MTA-1：セキュアなフローと同様に実行されます。
2. MTA-2 : プロビジョニング システムが BASIC.1 モードで MTA をプロビジョニングするように設定されている場合、プロビジョニング システムは、オプション 122 のサブオプション 6 を含んだ DHCP OFFER を返します。このサブオプションには、特殊な予約済み領域名「BASIC.1」が含まれています。この予約済み領域名は、MTA に対して BASIC.1 プロビジョニング フローを使用するように指示するものです。また、この OFFER はプロビジョニング システムの IP アドレスをオプション 122.3 に保持しており、file フィールドと siaddr フィールドに MTA 設定ファイルの位置が入力されています。
3. MTA-3、4 : MTA DHCP 交換の残りの部分が実行されます（REQUEST および ACK が交換されます）。
4. MTA は、ステップ MTA-22 まで直接スキップします。file および siaddr の情報を使用して、MTA は設定ファイルをプロビジョニング システムから TFTP で取得します。

（注）　MTA および ProvServ の認証や、暗号化は一切発生しません。

BASIC.2 フローは BASIC.1 と同一ですが、次の点が異なります。

- MTA の DHCP オプション 122 のサブオプション 6 に、「BASIC.2」が入力される。
- フローの最後となる MTA-25 で、MTA がプロビジョニング ステータス SNMPv2c INFORM を発行する（INFORM ターゲットは、DHCP オプション 122 のサブオプション 3 で指定されたもの）。

BASIC PacketCable フローは DOCSIS フローと似ていますが、次の点が異なります。

- MTA と プロビジョニング システムの間で ToD 交換が発生しない。
- MTA 設定ファイルの中に、完全性ハッシュが含まれている必要がある。具体的には、設定ファイルの内容全体の SHA1 ハッシュが pktcMtadevConfigFileHash SNMP varbind に入力され、End of File TLV の直前の TLV 11 内に配置されている必要があります。
- BASIC.2 フローは、MTA が設定ファイルを受信して処理した後に、プロビジョニング ステータス SNMPv2c INFORM を発行する。この INFORM は、MTA のプロビジョニングが正常に完了したかどうか、つまりプロビジョニングに問題がなかったかどうかを BACC に通知するものです。問題がある場合は、エラーが生成されて、イベントが DPE から RDU に送信され、次に BACC クライアントに送信されることがあります。この INFORM は、設定ファイルの問題点をデバッグする場合に特に役立ちます。

DOCSIS フローの詳細については、第 4 章「DOCSIS 設定」を参照してください。

（注）　PacketCable BASIC プロビジョニング フローを使用する場合は、PacketCable BASIC 対応の eMTA を使用していることを事前に確認してください。eMTA は、BASIC に対応していることを DHCP DISCOVER のオプション 60、TLV 5.18（サポートされているフロー）で報告する必要があります。

PacketCable の TLV 38 と MIB のサポート

BACC は、一連の PacketCable 1.5 MIB を完全にサポートしています。

BACC は、PacketCable 設定テンプレートで TLV 38 をサポートしています。この TLV を使用して、複数の SNMP 通知ターゲットを設定できます。この TLV を設定すると、すべての通知が TLV 38 で設定したターゲットにも発行されます。

SNMP v2C 通知

BACC では、PacketCable MTA からの SNMP v2C TRAP 通知と SNMP v2C INFORM 通知の両方をサポートしています。

Euro-PacketCable

Euro-PacketCable サービスは、基本的には North American PacketCable サービスのヨーロッパ版にあたりますが、次の点が異なります。

- Euro-PacketCable では、使用する MIB が異なる。
- Euro-PacketCable では、使用するデバイス証明書（MTA_Root.cer）とサービス プロバイダー証明書（サービス プロバイダー ルート）のセットが異なる。

  Euro-PacketCable の証明書の場合は、kdc.ini に「euro-packetcable = true」プロパティが記述されている必要があります。詳細については、P.2-15 の「Euro-PacketCable のサポート」を参照してください。

  Euro-PacketCable を使用する場合は、PacketCable のプロパティ /pktcbl/prov/locale の値を必ず EURO に設定してください（デフォルトは NA（North America）です）。ロケールは、設定ファイル ユーティリティで指定することができます。詳細については、P.12-25 の「設定ファイル ユーティリティの使用方法」を参照してください。

Euro-PacketCable の MIB

Euro-PacketCable の MIB は、基本的にはドラフト IETF MIB のスナップショットです。MTA の設定ファイルは、MIB を参照する SNMPVarBind が基本的な構成要素です。PacketCable の MIB と Euro の MIB は大きく異なるため、PacketCable と Euro-PacketCable の設定ファイルには互換性がありません。インストール時に、PacketCable のサンプル ファイル（cw29_config.tmpl）と Euro-PacketCable のサンプル ファイル（ecw15_mta_config.tmpl）が <BACC_HOME>/rdu/samples ディレクトリにコピーされます。

BACC には、次の Euro-PacketCable MIB が付属しています。

- DOCS-IETF-BPI2-MIB
- INTEGRATED-SERVICES-MIB
- DIFFSERV-DSCP-TC
- DIFFSERV-MIB
- TCOMLABS-MIB
- PKTC-TCOMLABS-MTA-MIB
- PKTC-TCOMLABS-SIG-MIB

Euro-PacketCable の MIB の設定

Euro-PacketCable の MIB を使用するように BACC を設定するには、ロードされる MIB を指定している BACC RDU プロパティを変更する必要があります。デフォルトでは、このプロパティは PacketCable の MIB を含んでいます。

この操作は、次のいずれかの方法で実行できます。

- rdu.properties を修正して、RDU を再起動する。
- 管理者のユーザ インターフェイスを使用する。Configuration > Defaults > System Defaults に移動して、MIB リストを下に示したリストに置き換えます。RDU を再起動する必要はありません。
- Prov API の changeSystemDefaults() コールを使用する。RDU を再起動する必要はありません。

プロパティの名前は、/snmp/mibs/mibList（properties ファイル）、または SNMPPropertyKeys.MIB_LIST（Prov API の定数の名前）です。プロパティの値はカンマ区切り形式（CSV）で、下に示す必要な MIB 名で構成されています。

```
/snmp/mibs/mibList=SNMPv2-SMI,SNMPv2-TC,INET-ADDRESS-MIB,CISCO-SMI,CISCO-TC,SNMPv2-MIB
,RFC1213-MIB,IANAifType-MIB,IF-MIB,DOCS-IF-MIB,DOCS-IF-EXT-MIB,DOCS-BPI-MIB,CISCO-CABL
E-SPECTRUM-MIB,CISCO-DOCS-EXT-MIB,SNMP-FRAMEWORK-MIB,DOCS-CABLE-DEVICE-MIB,DOCS-CABLE-
DEVICE-MIB-OBSOLETE,DOCS-QOS-MIB,CISCO-CABLE-MODEM-MIB,DOCS-IETF-BPI2-MIB,INTEGRATED-S
ERVICES-MIB,DIFFSERV-DSCP-TC,DIFFSERV-MIB,TCOMLABS-MIB,PKTC-TCOMLABS-MTA-MIB,PKTC-TCOM
LABS-SIG-MIB
```

eMTA プロビジョニングのトラブルシューティング

PacketCable 組み込み型メディア ターミナル アダプタ（eMTA）のプロビジョニングは、比較的複雑なプロセスです。ただし、適切なツールと方法を使用することで、ごく簡単に eMTA を運用可能にすることができます。

この章では、Network Registrar と BACC の両方を使用していることを前提としています。ただし、情報の多くはこれ以外の配備状態にも適用されます。また、Network Registrar の基礎知識（スコープ、ポリシー、基本的な DNS ゾーン設定、およびレコード エントリ）と BACC の基礎知識（サービス クラス、DHCP 基準、外部ファイル、および BACC ディレクトリ構造）があることを前提としています。

PacketCable eMTA のプロビジョニング プロセスは、セキュアなフローの場合は 25 ステップで構成されます。BASIC フローでは、ステップの数はかなり少なくなります。eMTA をトラブルシューティングするには、PacketCable プロビジョニング仕様に基づいたこれらの 25 ステップに関する知識が不可欠です。

この項では、次のトピックについて取り上げます。

コンポーネント

eMTA をトラブルシューティングする前に、以降の項で説明する次のシステム コンポーネントについて理解する必要があります。

- 組み込み型メディア ターミナル アダプタ
- DHCP サーバ
- DNS サーバ
- 鍵発行局
- PacketCable プロビジョニング サーバ
- Call Management Server

組み込み型メディア ターミナル アダプタ

eMTA は、ケーブル モデム（CM）とメディア ターミナル アダプタ（MTA）を、よく利用されるソフトウェア イメージとともに 1 つのボックスに組み込んだものです。CM と MTA はいずれも固有の MAC アドレスを持っており、それぞれが DHCP を実行して固有の IP アドレスを取得します。eMTA は、少なくとも 3 つの証明書を保持しています。証明書の 1 つは、一意の MTA 証明書です。2 番目の証明書は、MTA の製造業者を識別するものです。デバイス証明書と製造業者証明書は、デバイスや製造業者を認証するために、いずれも MTA によって鍵発行局（KDC）に送信されます。3 番目の証明書は、KDC から MTA に送信される証明書を検証するためのテレフォニー ルート証明書です。KDC の証明書は、テレフォニー ルートを起点としてチェーンを構成するため、KDC 証明書の信頼性を検証するには、テレフォニー ルートが MTA 上に存在している必要があります。MTA 部分は、MTA を制御するコール エージェントを識別するための固有の設定ファイルを受信します。

DHCP サーバ

DOCSIS 仕様では、ケーブル モデムが自身の IP アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）を使用してネゴシエートするように規定されています。MTA は、DOCSIS ネットワーク上のほとんどの CPE と同様に、DHCP を使用して自身の IP アドレスおよびその他の必須情報（DNS サーバ、Kerberos 領域名のための PacketCable オプション 122、プロビジョニング サーバの FQDN）を取得する必要があります。

（注）　ケーブル モデム部分は、通常の必須 DHCP オプションに加えて、オプション 122 のサブオプション 1 も要求して取得する必要があります。このサブオプションは、オファーの送信元となる適切な DHCP サーバの IP アドレスとして、ケーブル モデム部分が MTA 部分に渡します。

PacketCable をサポートする BACC を使用すると、正しく設定した BACC は、オプション 122 フィールドに加えて、ToD サーバ、DNS サーバ、TFTP サーバのフィールドにも自動的に値を入力します。これらについて、Network Registrar ポリシーで明示的に設定する必要はありません。

DNS サーバ

ドメイン ネーム システム（DNS）サーバは、PacketCable のプロビジョニングに不可欠です。BACC アーキテクチャにおけるデバイス プロビジョニング エンジン（DPE）である PacketCable プロビジョニング サーバは、適切なゾーン内にアドレス（A）レコードを持っている必要があります。これは、このサーバの完全修飾ドメイン名（FQDN）が DHCP サーバによって MTA にオプション 122 で提供されるためです。KDC 領域は、Kerberos サーバの FQDN を記述したサーバ（SRV）レコードを含んでいる領域名と同じ名前でゾーンを持っている必要があります。

SRV レコードで指定される Kerberos サーバは、適切なゾーン内に自身の A レコードを持っている必要があります。MTA 設定ファイルで指定される Call Management Server（CMS）も、適切なゾーン内に A レコードを持っている必要があります。最後に、MTA 自体も適切なゾーン内に A レコードを持っている必要があります。これは、CMS は MTA の FQDN を解決することによって MTA に到達するためです。MTA の A レコードを作成する方法としては、ダイナミック DNS（DDNS）をお勧めします。DDNS の設定およびトラブルシューティングについては、Cisco Network Registrar のマニュアルを参照してください。

鍵発行局

KDC は、MTA の認証を担当します。このため、KDC は MTA の証明書を検証するとともに、MTA が KDC を認証できるように KDC 自身の証明書を提供する必要があります。また、KDC は DPE（プロビジョニング サーバ）と通信して、MTA がネットワーク上でプロビジョニングされていることを検証します。

PacketCable プロビジョニング サーバ

PacketCable プロビジョニング サーバは、SNMP を使用して MTA 設定ファイルの位置を MTA に伝達し、MTA のパラメータをプロビジョニングします。MTA とプロビジョニング サーバ間のすべての通信で、SNMPv3 が使用されます。SNMPv3 通信の開始に使用されるキーは、MTA によって、KDC との認証フェーズ中に取得されます。プロビジョニング サーバの機能は、BACC アーキテクチャにおける DPE によって提供されます。

Call Management Server

Call Management Server（CMS）は、基本的にはソフト スイッチ（コール エージェント）です。ケーブル ネットワーク上の QoS を制御するための追加の PacketCable 機能を備えています。PacketCable プロビジョニングが成功すると、MTA はネットワーク コール シグナリング（NCS）の Restart in Progress（RSIP）メッセージを CMS に送信します。

基本変数

この項では、eMTA の適切なプロビジョニングに必要となる基本変数について説明します。

- 証明書（P.5-10）
- スコープ選択タグ（P.5-11）
- MTA 設定ファイル（P.5-11）

証明書

MTA_Root.cer ファイルには、MTA ルート証明書（正式な PacketCable MTA ルートがルートになっている証明書）が含まれています。MTA_Root.cer は、通常は重大な問題を引き起こすことはありません。

プロビジョニングの対象となる MTA でどのテレフォニー ルート証明書が必要になるかについて、あらかじめ把握しておく必要があります。実稼働ネットワークへの配備では、実在の PacketCable ルートがルートになっているテレフォニー証明書を使用します。ルートには、ラボ環境およびテスト環境で使用される PacketCable テスト ルートもあります。KDC が自身を MTA に認証させるために使用する KDC 証明書は、MTA に格納されているものと同じテレフォニー ルート（PacketCable の実在ルートまたはテスト ルート）がルートになっている必要があります。MTA 製造業者のほとんどは、Telnet ログイン機能と HTTP ログイン機能の一方または両方を備えたテスト イメージをサポートしているため、どのテレフォニー ルートがイネーブルになっているかを特定して、使用されるルートを変更することができます（ほとんどの場合、選択できるのは PacketCable 実在ルートとテスト ルートのいずれかのみです）。

最も一般的なシナリオでは、次の証明書を（$BACC_HOME/kdc/solaris/packetcable/certificates ディレクトリから）ロードした KDC を使用します。

- CableLabs_Service_Provider_Root.cer
- Service_Provider.cer
- Local_System.cer
- KDC.cer
- MTA_Root.cer

最初の 4 つの証明書は、テレフォニー証明書チェーンを構成します。MTA_Root.cer ファイルは、MTA の送信する証明書を検証するために KDC が使用する MTA ルートを保持しています。

（注）　KDC 証明書のインストールおよび管理については、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。

PacketCable テスト ルートを現在使用しているかどうかを特定するには、CableLabs_Service_Provider_Root.cer ファイルを Windows で開いて、Subject OrgName エントリが **O = CableLabs** であることを確認するか、サブジェクト代替名が **CN=CABLELABS GENERATED TEST ROOT FOR EQUIPMENT TEST PURPOSES ONLY** と記述されていることを確認します。

KDC 証明書（KDC.cer）は、使用する領域名を保持しています。BACC（および対応する DNS ゾーン）で使用するように設定されている領域名は、この領域名と一致している必要があります。また、MTA 設定ファイルの領域オリジナル名が、テレフォニー ルート内にある組織名と一致している必要があります。

KDC 証明書は、対応する秘密鍵を持っています。この秘密鍵は、$BACC_HOME/kdc/solaris ディレクトリにインストールされている必要があります。秘密鍵の名前は、通常は KDC_private_key.pkcs8 または KDC_private_key_proprietary です。証明書を変更するときは、秘密鍵も変更する必要があります。

スコープ選択タグ

ほとんどのシナリオでは、BACC は、BACC 管理ユーザ インターフェイスの DHCP 基準ページで指定されている選択基準に一致しているスコープ選択タグを使用して、スコープからのすべての DHCP 要求の処理に関係します。クライアント クラスもスコープを BACC 処理に関連付けるために使用できます。この関連付けは、デバイスをプロビジョニングする前に実行する必要があります。

MTA 設定ファイル

MTA 設定ファイルは、CMS の位置を保持しています。また、領域名のエントリを保持している必要があります。この値は、使用中の証明書チェーンの値と一致している必要があります。

MTA 設定ファイル内の特定のテーブル エントリは、MTA にオプション 122 で配送された領域名に基づいてインデックス付けされます。MTA 設定ファイル内のこの領域名エントリは、オプション 122 で配送されたものと一致する必要があります。たとえば、オプション 122 で配送された領域名が **DEF.COM** であった場合、MTA 設定ファイルの pktcMtaDevRealm テーブルのエントリは、この領域名の ASCII 符号化文字値（Cisco Broadband Configurator を使用している場合はドット区切り 10 進形式）、68.69.70.46.67.79.77 で構成されるサフィックスを使用してインデックス付けされます。Web には、この変換を容易にする無料の ASCII 変換ページが多数存在しています。

トラブルシューティングのツール

PacketCable MTA Device Provisioning Specification に記述されている 25 の eMTA セキュア プロビジョニングのステップについては、図 5-1 に示しています。

この項では、次のトピックについて取り上げます。

ログ

次に示すログ ファイルを使用して、次の情報が管理されています。

- Network Registrar の 2 つのログ（name_dhcp_1_log と name_dns_1_log）。Network Registrar の直近のいくつかのログ エントリを保持しています。DHCP または DNS に関する問題については、これらのファイルを調べてください。
- $BACC_HOME/kdc/logs/kdc.log ファイル。KDC と MTA とのインタラクション、および KDC と DPE とのインタラクションのすべてを記録しています。
- $BACC_DATA/dpe/logs/dpe.log ファイル。MTA との SNMPv3 インタラクションに関連する主なステップを記録しています。ハードウェア DPE に対して作業している場合は、**show log** CLI コマンドも使用できます。

（注）　コマンドライン インターフェイスを使用して、SNMP、登録サーバ、および登録サーバの詳細メッセージのトレースを有効にしておくと、PacketCable に潜在的な問題があった場合のトラブルシューティングに役立ちます。適切なトラブルシューティング コマンドについては、『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』を参照してください。

Ethereal、SnifferPro、およびその他のパケット キャプチャ ツール

eMTA のトラブルシューティングには、パケット キャプチャ ツールが不可欠です。CableLabs がパッケージ化している Ethereal バージョンには、PacketCable 固有の数多くのパケット デコーダが含まれています。これらには、Kerberos の AS パケットおよび AP パケットが含まれます。

- 特定の障害が DHCP に関係していると考えられる場合は、CMTS ケーブル インターフェイスの IP アドレスと DHCP サーバの IP アドレスを送信元または宛先とするパケットをフィルタリングしながら、パケットをキャプチャします。
- 特定の障害が、DHCP の後に発生する 25 ステップのいずれかに関係していると考えられる場合は、eMTA の IP アドレスを送信元または宛先とするパケットをすべてフィルタリングします。この方法では、図 5-1 に示したプロビジョニング ステップ 5 ～ 25 を単純な手順で容易にトレースできます。

トラブルシューティングのシナリオ

組み込み型 MTA に関して発生するおそれのある障害のシナリオを、表 5-1 に示します。

表 5-1　トラブルシューティングのシナリオ

発生する問題	考えられる原因	対処の方法
KDC が起動しない。	KDC 証明書が秘密鍵と対応していません。	互いに対応する証明書と秘密鍵があることを確認します。
	KDC ライセンスが有効期限切れであるか、見つかりません。	KDC ライセンスを $BACC_HOME/kdc ディレクトリに復元します。
MTA デバイスが BACC の Devices ページに表示されない。	不正なケーブル ヘルパー アドレスが設定されている可能性があります。	ヘルパー アドレスを修正します。
	スコープ選択タグが、BACC ユーザ インターフェイスで選択されている DHCPCriteria と一致しません。	MTA スコープ選択タグが、関係する MTA について BACC で作成した PacketCable DHCP 基準のスコープ選択タグと一致していることを確認します。
	Network Registrar 拡張ポイントが正しくインストールされていません。	Network Registrar 拡張ポイントを再インストールします。正しい手順については、『*Cisco Broadband Access Center for Cable Installation Guide*』を参照してください。
	ケーブル モデム部分がオプション 122 を受信しませんでした。	ケーブル モデム部分のスコープのタグが、BACC に設定されている DOCSIS DHCP 基準と一致していることを確認します。
MTA が DHCP オファーを受け付けず、DHCP フローを循環し続ける。	無効な DHCP オプションが設定されています。	スコープ ポリシーに DNS サーバ オプションが含まれていること、または cnr_ep.properties ファイルにプライマリ DNS サーバとセカンダリ DNS サーバのエントリが含まれていることを確認します。
	DHCP オファーが、ケーブル モデム部分のオプション 122 のサブオプション 1 で指定されているものとは別の DHCP サーバから送信された可能性があります。	cnr_ep.properties ファイルを確認して、プライマリとセカンダリの DHCP サーバが正しく設定されていることを確認します。
KDC.log ファイルと ethereal　トレースの両方が、MTA が KDC にアクセスしないことを示している。	cnr_ep.properties ファイルと MTA スコープ ポリシーの一方または両方で、不正な DNS サーバが指定されています。	cnr_ep.properties の DNS サーバを確認し、修正します。
	Kerberos 領域のゾーンが見つからないか、正しく設定されていません。	領域と同じ名前のゾーンが作成されていること、およびゾーンが「SRV」レコードを「_kerberos._udp 0 0 88 <KDC FQDN>」形式で保持していることを確認します。
	KDC の「A」レコード エントリが見つからないか、正しくありません。	Kerberos ゾーンの「SRV」レコードに含まれている FQDN について、「A」レコードが存在していることを確認します。
	DPE の FQDN を解決できません。	dpe.properties の provFQDNs エントリに、DPE の正しい FQDN と IP が記述されていることを確認します。

表 5-1　トラブルシューティングのシナリオ（続き）

発生する問題	考えられる原因	対処の方法
Kerberos の AS-Request 中に、KDC が障害を報告する。	MTA 証明書が、KDC によって使用されている MTA ルートと一致しません。	MTA_Root.cer を現用システムで使用されているものと比較して、MTA_Root.cer が適切なことを確認します。 適切なものである場合は、MTA 自体で証明書に関する問題が発生している可能性があります。この状況は非常にまれであり、該当する場合は MTA 製造業者に連絡してください。
	プロビジョニング サーバに対する KDC からの FQDN ルックアップが失敗しました。デバイスが、まだ BACC でプロビジョニングされていない可能性があります。	デバイスが表示されることを確認します。サービス クラスと DHCP 基準が与えられている必要があります。
	クロック スキュー エラー。詳細については、P.3-8 の「PacketCable チェックリスト」を参照してください。	すべての BACC ネットワーク要素が NTP を介してクロック同期していることを確認します。詳細については、『*Broadband Access Center for Cable Command Line Interface Reference*』を参照してください。
	KDC と DPE の間にミスマッチが存在している可能性があります。 **（注）** 他のデバイスが正しくプロビジョニングされている場合、これは問題の原因ではありません。	次の 3 つのエントリが、$BACC_HOME/kdc/solaris/keys ディレクトリに存在していることを確認します。 • mtafqdnmap,dpe.abc.com@DEF.COM • mtaprovsrvr,dpe.abc.com@DEF.COM • krbtgt,DEF.COM@DEF.COM システムに、この例と異なる DPE FQDN と領域名が保持されています。これらのエントリの内容は、dpe.properties の「KDCServiceKey」エントリ、または keygen ユーティリティを使用して生成されるキーに含まれているエントリと一致している必要があります。
KDC は AS-Request と AS-Reply（図 5-1 のステップ 9 とステップ 10）が成功したことを報告するが、MTA はステップ 9 より後に進まず、このステップまでを再プロビジョニングし続ける。	MTA でロードされているかイネーブルになっているテレフォニー ルートと、KDC でロードされているテレフォニー ルートとの間で、証明書のミスマッチが存在しています。	MTA と KDC の証明書を確認します。
	非常にまれですが、テレフォニー証明書チェーンが破損している可能性があります。 **（注）** 他のデバイスが正しくプロビジョニングされている場合、これは問題の原因ではありません。	MTA で正しい証明書がロードされているか、イネーブルになっていることを確認します。正常にプロビジョニングできているデバイスがまったくない場合は、KDC 上で別の証明書を試してみます。

表 5-1　トラブルシューティングのシナリオ（続き）

発生する問題	考えられる原因	対処の方法
AP Request と AP Reply（図 5-1 のステップ 14）が失敗する。	クロック スキュー エラー。詳細については、P.3-8 の「PacketCable チェックリスト」を参照してください。	すべての BACC ネットワーク要素が NTP を介してクロック同期していることを確認します。詳細については、『*Broadband Access Center for Cable Command Line Interface Reference*』を参照してください。
	プロビジョニング サーバの FQDN を解決できません。	プロビジョニング サーバ（DPE）の DNS エントリが正しいことを確認します。dpe.properties の provFQDNs エントリに、プロビジョニング サーバ（DPE）の正しい FQDN と IP が保持されていることを確認します。
	MTA から DPE に到達するルートが存在していません。	ルーティングの問題を解決します。
MTA が設定ファイルの TFTP 要求を発行しない。	DPE 上で実行されている TFTP サーバに到達するためのルートが存在していません。	ルーティングの問題を解決します。
MTA が TFTP 設定ファイルを受信しない。	設定ファイルが DPE でキャッシュされていません。	次のプロビジョニング試行でファイルがキャッシュされるまで、待機します。この方法で失敗する場合には、MTA をリセットします。
	Network Registrar の MTA スコープ ポリシーに、矛盾する TFTP サーバ オプションが含まれています。	TFTP サーバの DPE アドレスは BACC が挿入するため、このオプションはポリシーから削除しても問題ありません。
MTA は設定ファイルを受信するが、dpe.log ファイルを参照すると、DPE が SNMP Inform（図 5-1 のステップ 25）の受信に失敗している。	次のいずれかが発生しています。 • 設定ファイル内部での矛盾 • テレフォニー証明書チェーンの領域オリジナル名との矛盾 • オプション 122 で提供されている領域名との矛盾	MTA 設定ファイルに一貫性があることを確認します。
RSIP が送信されていないにもかかわらず、MTA が成功を報告する（図 5-1 のステップ 25）。	MTA が、MTA 設定ファイルで指定されている CMS FQDN の IP アドレスを解決できません。	CMS の DNS エントリが存在していることを確認します。
	MTA が CMS の IP アドレスに到達できません。これは、ルートが設定されていないことを示しています。	ルーティングの問題をすべて解決します。
CMS サービスのために KDC に再度アクセスしようとしているにもかかわらず、MTA が成功を報告する（図 5-1 のステップ 25）。	MTA 設定ファイルが誤ったケーブル モデムをポイントしています。	設定ファイルを修正するか、設定ファイルにリストされている FQDN を使用するように Cisco BTS 10200 を再設定します。
	MTA 設定ファイルの pktcMtaDevCmsIPsecCtrl 値が見つからないか、1 に設定されています。これは、MTA がセキュア NCS コール シグナリングを実行すること、または CMS FQDN の ASCII サフィックスと一致しない ASCII サフィックスを使用することを意味します。	設定ファイルを修正します。セキュア シグナリングを実行する場合は、必要な手順に従って、セキュア シグナリングをサポートするように KDC と BTS を設定します。

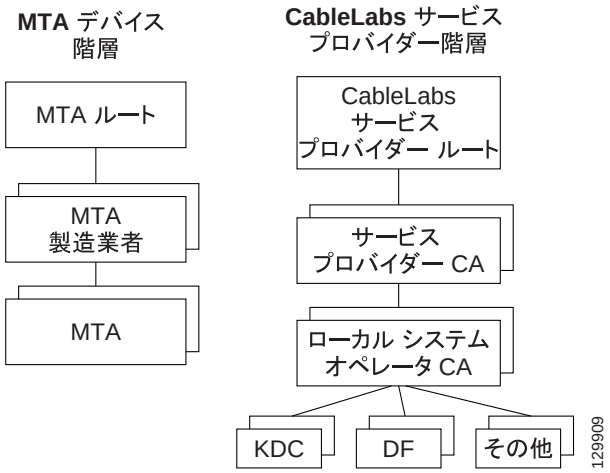
表 5-1　トラブルシューティングのシナリオ（続き）

発生する問題	考えられる原因	対処の方法
MTA が成功を報告して（図 5-1 のステップ 25）、RSIP を送信するが、ソフト スイッチからの応答がないか、応答としてエラーを受信する。	MTA が Cisco BTS 10200 上でプロビジョニングされていないか、不正にプロビジョニングされています。	MTA を Cisco BTS 10200 上でプロビジョニングします。
	eMTA の DNS エントリが存在していません。	適切な DNS ゾーンに eMTA のエントリを配置します。ダイナミック DNS を使用することをお勧めします。DDNS のイネーブル化については、Cisco Network Registrar のマニュアルを参照してください。

証明書信頼階層

BACC PacketCable には、図 5-2 に示すように、MTA デバイス証明書階層と CableLabs サービス プロバイダー証明書階層の 2 つの証明書階層があります。

図 5-2　PacketCable の証明書階層



BACC PacketCable の実装作業を行う前に、次の技術ドキュメントの内容を完全に理解しておく必要があります。

- *RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
- *DOCSIS Baseline Privacy Plus Interface Specification*（*SP-BPI+-I11-040407*、*2004 年 4 月 7 日*）

（注） Euro-PacketCable は PacketCable のセキュリティ仕様（PKT-SP-SEC-I08-030415）を使用していますが、Euro-PacketCable 環境で使用されるデジタル証明書に関しては、変更の必要な部分があります。Euro-PacketCable と PacketCable を可能な限り類似したものにするため、Euro-PacketCable では、セキュリティ仕様の新しいリビジョン（PKTSP-SEC-I08-030415）を含めて、PacketCable のすべてのセキュリティ技術を使用しています。

Euro-PacketCable 証明書の要素で PacketCable 証明書と異なっているものについては、以降の表で示します。

Euro-PacketCable では、Euro-PacketCable 証明書が有効となる唯一の証明書です。
PKT-SP-SEC-I08-030415 で述べられている、PacketCable 証明書について言及している PacketCable のすべての要件は、対応する Euro-PacketCable 証明書の要件に変更されます。

Euro-PacketCable 対応の組み込み型 MTA では、DOCSIS CVC CA の公開鍵の代わりに、Euro-DOCSIS ルート CVC CA の公開鍵が CM の不揮発性メモリに格納されている必要があります。
Euro-PacketCable 対応の独立型 MTA では、不揮発性メモリに tComLabs CVC ルート証明書と tComLabs CVC CA 証明書が格納されている必要があります。製造業者の CVC は、証明書チェーンを検証することで検証されます。

証明書の検証

PacketCable 証明書の検証では、通常は証明書のチェーン全体が検証されます。たとえば、プロビジョニング サーバが MTA デバイス証明書を検証するときは、次の証明書チェーンが検証されます。

MTA ルート証明書 + MTA 製造業者証明書 + MTA デバイス証明書

MTA 製造業者証明書の署名は MTA ルート証明書を使用して検証され、MTA デバイス証明書の署名は MTA 製造業者証明書を使用して検証されます。MTA ルート証明書は自己署名されていて、プロビジョニング サーバにとって既知のものです。MTA ルート証明書に存在する公開鍵は、この証明書自体の署名を検証するために使用されます。

チェーンの最初の証明書は、ケーブル経由で送信される証明書チェーンに通常は明示的に含まれていません。最初の証明書が明示的に含まれている場合、最初の証明書は、検証する側にとって既知のものである必要があり、変更が一切加えられていない必要があります。ただし例外として、証明書シリアル番号、有効期間、署名の値は変更されてもかまいません。ケーブル経由で渡された CableLabs サービス プロバイダー ルート証明書に、既知の CableLabs サービス プロバイダー ルート証明書と比較してこれら以外の変更点が存在している場合、比較を実行するデバイスは証明書の検証に失敗する必要があります。

証明書チェーンの検証のためのルール自体が、RFC 2459 に完全に準拠している必要があります。この RFC では、証明書パスの検証として言及されています。通常、X.509 証明書では、証明書の発行者名がもう一方の証明書のサブジェクト名と一致している場合、一連の緩やかな判定ルールがサポートされます。ルールが緩やかであるため、2 つの名前フィールドのバイナリ比較が一致していない場合でも、2 つの名前フィールドは一致していると宣言されることがあります。RFC 2459 では、実装が単純なバイナリ比較を使用して一致またはミスマッチを宣言できるように、認証局が名前フィールドの符号化を制限することを勧めています。

PacketCable のセキュリティは、この推奨事項に従っています。したがって、PacketCable 証明書の DER 符号化された tbsCertificate.issuer フィールドが、発行者の証明書の DER 符号化された tbsCertificate.subject フィールドと完全に一致している必要があります。実装は、DER 符号化された tbsCertificate.issuer フィールドと tbsCertificate.subject フィールドのバイナリ比較を実行することによって、発行者名をサブジェクト名と比較できます。

以降の項では、必要な証明書チェーンが指定されています。この証明書チェーンを使用して、図 5-2 に示している PacketCable 証明書信頼階層のリーフ ノード（最下層）に該当する各証明書を検証する必要があります。

入れ子化されている有効期間は検証されず、強制されません。このため、証明書の有効期間は、その証明書を発行した証明書の有効期間内に収まっている必要はありません。

MTA デバイス証明書階層

デバイス証明書階層は、DOCSIS1.1/BPI+ 階層のデバイス証明書階層をそのまま写したものです。一連の製造業者証明書の発行元証明書として使用される、CableLabs 発行の PacketCable MTA ルート証明書がルートになっています。製造業者証明書は、個々のデバイス証明書に署名するために使用されます。

以降の表に含まれている情報は、RFC 2459 に従った必須フィールドで使用する PacketCable 固有の値を示しています。これらの PacketCable 固有の値は、表 5-2 に従って指定する必要がありますが、Validity Period は各表で示されているとおりにする必要があります。必須フィールドの PacketCable での値が特に示されていない場合は、RFC 2459 のガイドラインに従う必要があります。

MTA ルート証明書

この証明書は、MTA ルート証明書、MTA 製造業者証明書、および MTA デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。

表 5-2　MTA ルート証明書

MTA ルート証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs OU=PacketCable CN=PacketCable Root Device Certificate Authority	**Euro-PacketCable** C=BE O=tComLabs OU=Euro-PacketCable CN=Euro-PacketCable Root Device Certificate Authority
Intended Usage	この証明書は、MTA 製造業者証明書に署名するために KDC によって使用されます。この証明書は MTA によって使用されることがないため、MTA MIB には表示されません。	
Signed By	自己署名	
Validity Period	20 年以上。この証明書を再発行する必要のない、十分な長さの有効期間であると想定されます。	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign) subjectKeyIdentifier[n,m] basicConstraints[c,m](cA=true, pathLenConstraint=1)	

MTA 製造業者証明書

この証明書は、MTA ルート証明書、MTA 製造業者証明書、および MTA デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。state/province、city、および製造業者のファシリティは、オプションのアトリビュートです。製造業者は、製造業者証明書を複数保有していることがあり、証明書が製造業者ごとに 1 つまたはそれ以上存在することがあります。同じ製造業者のすべての証明書が、製造時または現地でのアップデート中に各 MTA に提供される可能性があります。MTA は、MTA デバイス証明書の発行者名を MTA 製造業者証明書のサブジェクト名と比較して、使用する適切な証明書を選択する必要があります。デバイス証明書の authorityKeyIdentifier は、存在する場合、RFC 2459 に記述されているとおり、製造業者証明書の subjectKeyIdentifier と一致している必要があります。O と CN にある <CompanyName> フィールドは、2 つのインスタンス間で異なる場合があります。

表 5-3　MTA 製造業者証明書

MTA 製造業者証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs OU=PacketCable CN=PacketCable Root Device Certificate Authority	**Euro-PacketCable** C = <Country of Manufacturer> O = <Company Name> [stateOrProviceName = <state/province>] [localityName = <City>] OU = Euro-PacketCable [organizationalUnitName = <Manufacturing Location>] CN = <Company Name> Euro-PacketCable CA
Intended Usage	この証明書は各 MTA 製造業者に発行され、PacketCable Security Specification で規定されているとおり、（製造時または現地でのアップデート中に）セキュア コード ダウンロードの一環として各 MTA に提供されることがあります。この証明書は、読み取り専用パラメータとして MTA MIB に表示されます。この証明書は、KDC による認証中に、MTA デバイスのアイデンティティ（MAC アドレス）を認証するために MTA デバイス証明書とともに使用されます。	
Signed By	MTA ルート証明書の CA	
Validity Period	20 年	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign)、subjectKeyIdentifier[n,m]、authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)、basicConstraints[c,m](cA=true, pathLenConstraint=0)	

MTA デバイス証明書

この証明書は、MTA ルート証明書、MTA 製造業者証明書、および MTA デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。state/province、city、および製造業者のファシリティは、オプションのアトリビュートです。MAC アドレスは、6 組のコロン区切り 16 進数（「00:60:21:A5:0A:23」など）で記述されている必要があります。16 進数のアルファベット文字（A ～ F）は、大文字で記述されている必要があります。MTA デバイス証明書は、置換および更新しないでください。

表 5-4　MTA デバイス証明書

MTA デバイス証明書		
Subject Name Form	**PacketCable** C=<country> O = <Company Name> [ST=<state/province>] [L=<city>], OU=PacketCable [OU=<Product Name>] [OU=<Manufacturer's Facility>] CN=<MAC Address>	**Euro-PacketCable** C = <Country of Manufacturer> O = <Company Name> [ST=<state/province>] [L = <City>] OU = Euro-PacketCable [OU=<Product Name>] [OU = <Manufacturing Location>] CN=<MAC Address>
Intended Usage	この証明書は MTA 製造業者によって発行され、製造時にインストールされています。プロビジョニング サーバはこの証明書をアップデートできません。この証明書は、読み取り専用パラメータとして MTA MIB に表示されます。この証明書は、プロビジョニング中に MTA デバイスのアイデンティティ（MAC アドレス）を認証するために使用されます。	
Signed By	MTA 製造業者証明書の CA	
Validity Period	20 年以上	
Modulus Length	1024、1536、または 2048	
Extensions	keyUsage[c,o](digitalSignature, keyEncipherment) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)	

MTA 製造業者コード検証証明書

組み込み型 MTA のコード検証証明書（CVC）の仕様は、DOCSIS 仕様 SP-BPI+-I11-040407 で指定されている DOCSIS 1.1 CVC と同一である必要があります。

CableLabs サービス プロバイダー証明書階層

サービス プロバイダー証明書階層は、CableLabs 発行の CableLabs サービス プロバイダー ルート証明書がルートになっています。この証明書は、一連のサービス プロバイダー証明書の発行元証明書として使用されます。サービス プロバイダー証明書は、オプションのローカル システム証明書に署名するために使用されます。ローカル システム証明書が存在する場合は、ローカル システム証明書を使用して補助装置証明書が署名されます。存在しない場合には、補助証明書はサービス プロバイダーの CA によって署名されます。

表 5-5 に含まれている情報は、RFC 2459 に従った必須フィールドで使用する固有の値を示しています。これらの固有値に従って指定する必要があります。必須フィールドの値が特に示されていない場合は、RFC 2459 のガイドラインを遵守する必要があります。

CableLabs サービス プロバイダー ルート証明書

Kerberos キー管理を行うには、Kerberos プロトコルの PKINIT 拡張を使用して、事前に MTA と KDC の相互認証を実行しておく必要があります。MTA は、KDC 証明書チェーンを含んだ PKINIT Reply メッセージを受信した後に KDC を認証します。KDC の認証で、MTA は KDC 証明書チェーンを検証します。このチェーンは、CableLabs サービス プロバイダー ルート CA が署名した KDC のサービス プロバイダー証明書を含んでいます。

表 5-5　CableLabs サービス プロバイダー ルート証明書

CableLabs サービス プロバイダー ルート証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs CN=CableLabs Service Provider Root CA	**Euro-PacketCable** C=BE O=tComLabs CN=tComLabs Service Provider Root CA
Intended Usage	この証明書は、サービス プロバイダー CA 証明書に署名するために使用されます。この証明書は、各 MTA に製造時にインストールされるか、または PacketCable Security Specification で規定されているとおり、セキュア コード ダウンロードでインストールされます。プロビジョニング サーバでアップデートすることはできません。このルート証明書および対応する公開鍵は、MTA MIB に表示されません。	
Signed By	自己署名	
Validity Period	20 年以上。この証明書を再発行する必要のない、十分な長さの有効期間であると想定されます。	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign) subjectKeyIdentifier[n,m] basicConstraints[c,m](cA=true)	

サービス プロバイダー CA 証明書

これはサービス プロバイダーが保有する証明書で、CableLabs サービス プロバイダー ルート CA によって署名されます。CableLabs サービス プロバイダー ルート証明書、テレフォニー サービス プロバイダー証明書、オプションのローカル システム証明書、およびエンドエンティティ サーバ証明書で構成される証明書チェーンの一環として検証されます。認証する側のエンティティは、通常はすでに CableLabs サービス プロバイダー ルート証明書を所有しており、この証明書は、証明書チェーンの残りの部分とともに転送されることはありません。

サービス プロバイダー CA 証明書が常に明示的に証明書チェーンに含まれているため、サービス プロバイダーは、自身の証明書を柔軟に変更できます。変更時に、この証明書チェーンを検証する各エンティティ（たとえば、MTA は PKINIT Reply を検証します）を再設定する必要はありません。サービス プロバイダー CA 証明書を変更したら、そのたびに署名を CableLabs サービス プロバイダー ルート証明書を使用して検証する必要があります。ただし、同じサービス プロバイダーの新しい証明書では、SubjectName の OrganizationName アトリビュートが以前と同じ値に保たれている必要があります。O と CN にある <Company> フィールドは、2 つのインスタンス間で異なる場合があります。

表 5-6　CableLabs サービス プロバイダー CA 証明書

CableLabs サービス プロバイダー ルート証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company> CN=<Company> CableLabs Service Provider CA	**Euro-PacketCable** C=<Country> O=<Company> CN=<Company> tComLabs Service Provider CA
Intended Usage	この証明書は、サービス プロバイダー CA 証明書に署名するために使用されます。この証明書は、各 MTA に製造時にインストールされるか、または PacketCable Security Specification で規定されているとおり、セキュア コード ダウンロードでインストールされます。プロビジョニング サーバでアップデートすることはできません。このルート証明書および対応する公開鍵は、MTA MIB に表示されません。	
Signed By	自己署名	
Validity Period	20 年以上。この証明書を再発行する必要のない、十分な長さの有効期間であると想定されます。	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign cRLSign), subjectKeyIdentifier[n,m] basicConstraints[c,m](cA=true)	

ローカル システム CA 証明書

サービス プロバイダー CA は、ローカル システム CA（対応するローカル システム証明書を持つ）と呼ばれる地域別の認証局に証明書の発行を委任することがあります。ネットワーク サーバは、同じサービス プロバイダーの地域別の認証局の間を自由に移動できます。したがって、MTA MIB には、ローカル システム証明書に関する情報は含まれません（ローカル システム証明書では、MTA が特定地域内の KDC に制限される場合があるためです）。

表 5-7　ローカル システム CA 証明書

ローカル システム CA 証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company> OU=<Local System Name> CN=<Company> CableLabs Local System CA	**Euro-PacketCable** C=<Country> O=<Company> OU=<Local System Name> CN = <Company> tComLabs Local System CA
Intended Usage	サービス プロバイダー CA は、ローカル システム CA（対応するローカル システム証明書を持つ）と呼ばれる地域別の認証局に証明書の発行を委任することがあります。ネットワーク サーバは、同じサービス プロバイダーの地域別の認証局の間を自由に移動できます。したがって、MTA MIB には、ローカル システム証明書に関する情報は含まれません（ローカル システム証明書では、MTA が特定地域内の KDC に制限される場合があるためです）。	
Signed By	サービス プロバイダー CA 証明書	
Validity Period	20 年	
Modulus Length	1024, 1536, 2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign)、subjectKeyIdentifier[n,m]、authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)、basicConstraints[c,m](cA=true, pathLenConstraint=0)	

運用上の補助証明書

ここで説明する証明書は、すべてローカル システム CA またはサービス プロバイダー CA のいずれかによって署名されます。他の補助証明書がこの標準に将来追加されることがあります。

鍵発行局証明書

この証明書は、CableLabs サービス プロバイダー ルート証明書、サービス プロバイダー CA 証明書、および補助デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。PKINIT 仕様では、KDC 証明書に subjectAltName v.3 証明書拡張が含まれていることを要件としています。この拡張の値は、KDC の Kerberos プリンシパル名である必要があります。

表 5-8　鍵発行局証明書

鍵発行局証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company>, [OU=<Local System Name>] OU= CableLabs Key Distribution Center CN=<DNS Name>	**Euro-PacketCable** C=<Country> O=<Company> [OU = <Local System Name>] OU = tComLabs Key Distribution Center CN=<DNS Name>
Intended Usage	KDC サーバのアイデンティティを PKINIT 交換中に MTA に対して認証すること。この証明書は PKINIT 応答の中で MTA に渡されるため、MTA MIB には含まれておらず、プロビジョニング サーバがアップデートおよびクエリーすることはできません。	
Signed By	サービス プロバイダー CA 証明書またはローカル システム証明書	
Validity Period	20 年	
Modulus Length	1024、1536、または 2048	
Extensions	keyUsage[c,o](digitalSignature)authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)subjectAltName[n,m]	

配送機能（DF）

この証明書は、CableLabs サービス プロバイダー ルート証明書、サービス プロバイダー CA 証明書、および補助デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。この証明書は、（電子サーベイランスで使用される）DF 間でのフェーズ 1 IKE ドメイン間交換

に署名するために使用されます。Local System Name はオプションですが、ローカル システム CA がこの証明書に署名する場合は必須です。IP アドレスは、245.120.75.22 などの標準的なドット付き 4 数字列表記で指定する必要があります。

表 5-9　DF 証明書

DF 証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company> [OU = <Local System Name>] OU=PacketCable Electronic Surveillance CN=<IP address>	**Euro-PacketCable** C=<Country> O=<Company> [OU = <Local System Name>] OU = Euro-PacketCable Electronic Surveillance CNe = <IP address>
Intended Usage	IKE キー管理を認証するために、1 組の DF 間で IPsec セキュリティ アソシエーションを確立するのに使用されます。これらのセキュリティ アソシエーションは、合法的に傍聴されているサブジェクトが、新しい傍聴サーバ（DF）に転送される必要のあるコール情報を含んだコール メッセージとイベント メッセージを転送するときに使用されます。	
Signed By	サービス プロバイダー CA 証明書またはローカル システム CA 証明書	
Validity Period	20 年	
Modulus Length	2048	
Extensions	keyUsage[c,o](digitalSignature) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>) subjectAltName[n,m] (dNSName=<DNSName>)	

PacketCable サーバ証明書

これらの証明書は、CableLabs サービス プロバイダー ルート証明書、サービス プロバイダー証明書、ローカル システム オペレータ証明書（使用されている場合）、および補助デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。これらの証明書は、PacketCable システムの各種サーバを識別するために使用されます。たとえば、フェーズ 1 IKE 交換に署名するため、または PKINIT 交換を認証するために使用される場合があります。Local System Name はオプションですが、ローカル システム CA がこの証明書に署名する場合は必須です。IP アドレスの値は、245.120.75.22 などの標準的なドット区切り 10 進表記で指定する必要があります。DNS Name の値は、device.packetcable.com などの完全修飾ドメイン名（FQDN）で指定する必要があります。

表 5-10　PacketCable サーバ証明書

PacketCable サーバ証明書		
Subject Name Form	**PacketCable**	**Euro-PacketCable**
	C=<Country>	C=<Country>
	O=<Company>	O=<Company>
	OU=PacketCable	OU = Euro-PacketCable
	OU=[<Local System Name>]	[OU = <Local System Name>]
	OU=<Sub-System Name>	OU = <Sub-system Name>
	CN=<Server Identifier[:<Element ID>]>	CN=<Server Identifier[:<Element ID>]>
	<Server Identifier> の値は、サーバの FQDN または IP アドレスにする必要があります。オプションで、値の後にコロン（:）に続けて Element ID を記述できます（コロンの前後は空白なし）。 <Element ID> は、課金イベント メッセージに表示される ID です。イベント メッセージを生成できるすべてのサーバの証明書に含まれている必要があります。このようなサーバとしては、CMS、CMTS、および MGC があります。Element ID は 5 オクテットの右揃え ASCII 符号化数値文字列として定義し、余白には空白文字を埋め込みます。Element ID を証明書で使用するために変換するときは、空白文字を ASCII の 0（0x48）に変換する必要があります。 たとえば、CMTS の Element ID が「311」で IP アドレスが 123.210.234.12 である場合、CMTS の通常名は「123.210.234.12:00311」になります。 <Sub-System Name> の値は、次のいずれかにする必要があります。 • ボーダー プロキシの場合：bp • ケーブル モデム ターミネーション システムの場合：cmts • Call Management Server の場合：cms • メディア ゲートウェイの場合：mg • メディア ゲートウェイ コントローラの場合：mgc • メディア プレーヤーの場合：mp • メディア プレーヤー コントローラの場合：mpc • プロビジョニング サーバの場合：ps • レコード記録サーバの場合：rks • シグナリング ゲートウェイの場合：sg	commonName の仕様の詳細については、PKT-SP-SEC-IO8-030415 を参照してください。
Intended Usage	これらの証明書は、PacketCable システムの各種サーバを識別するために使用されます。たとえば、フェーズ 1 IKE 交換に署名するため、または PKINIT 交換でデバイスを認証するために使用される場合があります。	
Signed By	テレフォニー サービス プロバイダー証明書またはローカル システム証明書	
Validity Period	MSO ポリシーにより設定	

表 5-10　PacketCable サーバ証明書（続き）

PacketCable サーバ証明書	
Modulus Length	2048
Extensions	keyUsage[c,o](digitalSignaturekeyEncipherment) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA cert>) subjectAltName[n,m](dNSName=<DNSName> | iPAddress=<IP AddressName>) keyUsage タグはオプションです。使用する場合は、このタグをクリティカルとしてマークする必要があります。以降で特に説明のない限り、subjectAltName 拡張には、対応する名前値が、サブジェクトの CN フィールドで指定されているとおりに含まれている必要があります。

CMS 証明書の CN アトリビュート値は、Element ID にする必要があります。subjectAltName 拡張には、CMS の IP アドレスまたは FQDN のいずれかが含まれている必要があります。CMTS 証明書の CN アトリビュート値は、Element ID にする必要があります。subjectAltName 拡張には、CMTS の IP アドレスまたは FQDN のいずれかが含まれている必要があります。

MGC 証明書の CN アトリビュート値は、Element ID にする必要があります。subjectAltName 拡張には、MGC の IP アドレスまたは FQDN のいずれか含まれている必要があります。

証明書失効

現時点では、PacketCable の仕様範囲外です。

コード検証証明書階層

CableLabs コード検証証明書（CVC）PKI は汎用的な性質を持っており、CVC を必要とするすべての CableLabs プロジェクトに適用できます。つまり、基本インフラストラクチャをあらゆる CableLabs プロジェクトで再利用することができます。必要となるエンドエンティティ証明書は、プロジェクトごとに異なる場合がありますが、エンドエンティティ証明書が重複している場合は、1 つのエンドエンティティ証明書を使用してその重複に対応できる可能性があります。

CableLabs CVC 階層は、eMTA には適用されません。

CVC の全般的要件

すべてのコード検証証明書に対して、次の要件が適用されます。

- 証明書は、DER 符号化されている必要がある。
- 証明書は、バージョン 3 である必要がある。
- 証明書は、以降の各表で指定する拡張を含んでいる必要があり、その他の拡張を含んでいてはならない。
- 公開指数は、F4（10 進数の 65537）にする必要がある。

CableLabs コード検証ルート CA 証明書

この証明書は、CableLabs コード検証ルート CA 証明書、CableLabs コード検証 CA 証明書、およびコード検証証明書で構成される証明書チェーンの一環として検証する必要があります。証明書の検証方法の詳細については、P.5-18 の「証明書の検証」を参照してください。

表 5-11　CableLabs コード検証ルート CA 証明書

CableLabs コード検証ルート CA 証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs CN=CableLabs CVC Root CA	**Euro-PacketCable** C = BE O = tComLabs CN = tComLabs CVC Root CA
Intended Usage	この証明書は、コード検証 CA 証明書に署名するために使用されます。この証明書は、製造時に S-MTA 不揮発性メモリに含める必要があります。	
Signed By	自己署名	
Validity Period	20 年以上	
Modulus Length	2048	
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign) subjectkeyidentifier [n,m] basicConstraints[c,m](cA=true)	

CableLabs コード検証 CA 証明書

CableLabs コード検証 CA 証明書は、CableLabs コード検証ルート CA 証明書、CableLabs コード検証 CA 証明書、およびコード検証証明書で構成される証明書チェーンの一環として検証する必要があります。証明書の検証方法の詳細については、P.5-18 の「証明書の検証」を参照してください。CableLabs コード検証 CA は、複数存在する場合があります。S-MTA は、一度に 1 つずつ CableLabs CVC CA をサポートする必要があります。

表 5-12　CableLabs コード検証 CA 証明書

CableLabs コード検証 CA 証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs CN=CableLabs CVC CA	**Euro-PacketCable** C = BE O = tComLabs CN = tComLabs CVC CA
Intended Usage	この証明書は、CableLabs コード検証ルート CA によって CableLabs に発行されます。この証明書がコード検証証明書を発行します。この証明書は、製造時に S-MTA 不揮発性メモリに含める必要があります。	
Signed By	CableLabs コード検証ルート CA	
Validity Period	CableLabs ポリシーにより設定	
Modulus Length	2048	
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign) subjectKeyIdentifier[n,m] authorityKeyIdentifier [n,m] basicConstraints [c,m](cA=true, pathLenConstraint=0)	

製造業者コード検証証明書

CableLabs コード検証 CA は、認可された各製造業者に対して、この証明書を発行します。この証明書は、セキュアなソフトウェア ダウンロードのために CATV 事業者により設定されたポリシーで使用されます。

表 5-13　製造業者コード検証証明書

製造業者コード検証証明書		
Subject Name Form	**PacketCable** C=<country> O = <Company Name> [ST=<state/province>] [L=<city>] CN=<Company Name> Mfg CVC	**Euro-PacketCable** C=<Country> O = <Company Name> [ST=<state/province>] [L = <City>] CN=<Company Name> Mfg CVC
Intended Usage	CableLabs コード検証 CA は、認可された各製造業者に対して、この証明書を発行します。この証明書は、セキュアなソフトウェア ダウンロードのために CATV 事業者により設定されたポリシーで使用されます。	
Signed By	CableLabs コード検証 CA	tComLabs コード検証 CA 証明書
Validity Period	CableLabs ポリシーにより設定	
Modulus Length	1024, 1536, 2048	
Extensions	extendedKeyUsage [c,m] (id-kp-codeSigning) authorityKeyIdentifier [n,m]	

Organization の Company Name と Common Name の Company Name は、異なる場合があります。

サービス プロバイダー コード検証証明書

サービス プロバイダー コード検証証明書は、CableLabs コード検証ルート CA 証明書、CableLabs コード検証 CA 証明書、およびサービス プロバイダー コード検証証明書で構成される証明書チェーンの一環として検証する必要があります。証明書の検証方法の詳細については、P.5-18 の「証明書の検証」を参照してください。

表 5-14　サービス プロバイダー コード検証証明書

サービス プロバイダー コード検証証明書		
Subject Name Form	C=<country> O = <Company Name> [ST=<state/province>] [L=<city>] CN=<Company Name> Service Provider CVC	C=<Country> O = <Company Name> [ST=<state/province>] [L = <City>] CN=<Company Name> Service Provider CVC
Intended Usage	CableLabs コード検証 CA は、認可された各サービス プロバイダーに対して、この証明書を発行します。この証明書は、セキュアなソフトウェア ダウンロードのために CATV 事業者により設定されたポリシーで使用されます。	
Signed By	CableLabs コード検証 CA	tComLabs コード検証 CA 証明書
Validity Period	CableLabs ポリシーにより設定	
Modulus Length	1024, 1536, 2048	
Extensions	extendedKeyUsage [c,m] (id-kp-codeSigning) authorityKeyIdentifier [n,m]	

Organization の Company Name と Common Name の Company Name は、異なる場合があります。

CVC の証明書失効リスト

S-MTA は、CVC の証明書失効リスト（CRL）をサポートしている必要はありません。