CHAPTER 16

Broadband Access Center のトラブルシューティング

この章では、Broadband Access Center（BAC）のトラブルシューティングを行う方法の詳細について説明します。この章は、次の項で構成されています。

BAC プロビジョニングに関連する FAQ のリストについては、付録 E「Broadband Access Center のプロビジョニングに関する FAQ」を参照してください。

トラブルシューティングのチェックリスト

BAC のトラブルシューティングでは、表 16-1 に示すチェックリストを使用します。

表 16-1　トラブルシューティングのチェックリスト

手順	参照先	確認
1. BAC コンポーネントがインストールされているすべてのシステムで、BAC のプロセスが稼働しているかどうかを確認します。	コマンドラインからの BAC プロセス ウォッチドッグの使用方法（P.9-2）	❑
2. BAC のコンポーネント ログで、重大度の高いエラーが示されていないかどうかを確認します。これには、次のものに関して記録された情報が含まれます。 － RDU － DPE	RDU のログ（P.10-4） DPE のログ（P.10-8）	❑
3. 管理者のユーザ インターフェイスからサーバのアップ タイムを表示し、サーバがバウンスしていないことを確認します。	サーバの表示（P.12-23）	❑
4. 管理者のユーザ インターフェイスから、RDU および DPE のサービス パフォーマンス統計情報を表示します。トランザクション時間が長くなっているなど、異常な数値がないか確認します。	サーバの表示（P.12-23）	❑
5. syslog アラート ログを確認します。	付録 A「アラートとエラー メッセージ」	❑
6. 次のようなオペレーティング システムおよびハードウェアのリソースを確認します。 － ディスク領域 － CPU 時間 － メモリ	特定のコマンドについては、Solaris のマニュアルを参照してください。	❑
7. 特定のデバイスのトラブルシューティングを行う場合は、DPE でキャッシュされているデバイス命令を表示します。	**show device-config** コマンド（『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照）	❑
8. 管理者のユーザ インターフェイスから、個々のデバイスのトラブルシューティングを設定します。しばらく経過してから、トラブルシューティング ログを調べます。	トラブルシューティングのためのデバイスの設定（P.16-3）	❑
9. RDU または適切な DPE でより高いロギング レベルを設定し、詳細なログ情報を取得します。	RDU ログ レベル ツールの使用方法（P.10-5） **log level** コマンド（『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照）	❑

デバイス ID に基づくデバイスのトラブルシューティング

この機能を使用すると、1 つ以上の特定のデバイスに関する詳細な診断情報を収集できます。トラブルシューティング情報には、特定のデバイスまたはデバイス グループに関連するサーバ インタラクションがすべて含まれます。この情報には、管理者のユーザ インターフェイスの操作、RDU Application Programming Interface（API; アプリケーション プログラミング インターフェイス）の操作、DPE とデバイスとのインタラクション、およびサーバ間の DPE と RDU のインタラクションも含まれます。

1 つ以上の特定のデバイスに対して、ノード管理によって診断をイネーブルまたはディセーブルにできます。この場合、ロギングをオンにしたり、特定のデバイス情報についてのログ ファイルを検索したりする必要はありません。

BAC はデバイス ID（MAC アドレスと DUID）に基づいてデバイスのリストを保持しており、それについての詳細な診断情報が収集されます。トラブルシューティング情報は RDU で一元的に保管され、デバイス単位で保持されます。DPE と Cisco Network Registrar 拡張は、どちらもこのデータを保存しません。この情報は RDU に転送されます。RDU は、その情報を受信すると、*BPR_DATA/rdu/logs* ディレクトリの *troubleshooting.log* ファイルに書き込みます。

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

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

DPE は、診断される特定のデバイスの MAC アドレスと DUID をそのデバイスの IP アドレスにマッピングします。DPE は、診断されるデバイスの Network Registrar 拡張から IP アップデートを受信します。

新しいデバイスやグループの追加など、デバイス トラッキング リストに対するすべての修正は、すべてのサーバでただちに実行されます。RDU または DPE をリブートする必要はありません。各サーバのログ ファイルには、診断モードになっているデバイスの現在のリストが示されます。

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

トラブルシューティングのためのデバイスの設定

デバイス診断は、1 つ以上のデバイスが診断モードに設定されるまでディセーブルになっています。

デバイスの診断をイネーブルにするには、そのデバイスを BAC RDU で事前登録しておく必要があります。デバイスが事前登録されていない場合は、Manage Devices ページで Add ボタンをクリックして、デバイスを追加します。デバイスの追加については、P.12-14 の「デバイス レコードの追加」を参照してください。

診断モードになるデバイスの最大数を設定すると、気付かないうちに膨大な数のデバイスをこのモードに移行して、サーバのパフォーマンスを低下させてしまうことを回避できます。デフォルトでは、この数が 25 に設定されています。管理者のユーザ インターフェイスからトラブルシューティング モードに移行できるデバイスの最大数を設定するには、Systems Defaults ページで **Configuration > Defaults** タブの順にクリックします。Maximum Diagnostics Device Count フィールドに値を入力します。

ノードへのデバイスの関連付け

デバイスは、特定のノードに関連させることによってトラブルシューティングを行うことができます。関連付け機能により、MAC アドレスまたは DUID を使用してデバイスを特定のノードに関連付けます。さらにその特定のノードは、特定のノード タイプに関連付けられます。（P.12-17 の「デバイスの関連付けと関連付け解除」を参照してください）。関連付けによってデバイスについての膨大な量の情報が記録されるので、それらの情報に基づいて潜在的な問題のトラブルシューティングを実行できます。

表 16-2 に、関連付け機能と関連付け解除機能を使用したワークフローの例を示します。

表 16-2　関連付け / 関連付け解除プロセスのサンプル

手順	作業
1.	問題が存在するかどうかを判断し、影響を受けるデバイスを識別します。
2.	デバイスをノードに関連付けます。
3.	デバイスのトラフィックが確実に通過するように数分待つか、またはデバイスのハードブートを実行します。
4.	ワード プロセッシング アプリケーションで *BPR_DATA/rdu/logs/troubleshooting.log* ファイルを開き、特定のデバイスの MAC アドレスまたは DUID のエントリを見つけます。
5.	問題を識別、訂正、テスト、および検証します。
6.	デバイスをノードから関連付け解除します。

診断モードになっているデバイスのリストの表示

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

診断が現在イネーブルになっているデバイスのリストを表示するには、次の手順に従います。

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

ステップ 2　Node Name (Node Type) ドロップダウン リストから、診断モードのデバイスすべてを表示するための、**system-diagnostics (system)** オプションを選択します。

ステップ 3　**Search** をクリックします。

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

診断がイネーブルになっているデバイスは、ログ レベルが 5（通知）に設定された状態でログ ファイルに表示されます。ログ ファイルの詳細については、P.10-2 の「イベントのロギング」を参照してください。

例

次の例では、MTA のトラブルシューティングを行う間のログ出力を示しています。

```
bac-test.example.com:2005 03 04 18:38:24 EST:%BAC-DIAGNOSTICS-3-4055:[##MTA-9a
Unconfirmed FQDN Request Received from [/10.10.10.5 ['kdcquery']. Client with IP
Address [10.10.20.2] and MAC Address [1,6,00:00 :ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:24 EST:%BAC-DIAGNOSTICS-3-4082:[Results of BACC
Lookup. FQDN: [1-6-00-00-ca-b7-7e-91.example.com MAC: 1,6,00:00:ca:b7:7e:91. Client
with IP Address [10.10.20.2] and MAC Address [1,6,00:00:ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:24 EST:%BAC-DIAGNOSTICS-3-4070:[##MTA-9b FQDN
Reply Sent to [/10.10.20.2(41142) for MTA 1,6,00:00:ca:b7:7e:91. Client with IP
Address [10.10.20.2] and MAC Address [1,6, 00:00:ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:26 EST:%BAC-DIAGNOSTICS-3-4132:[##MTA-13
Incoming APREQ received from [/10.10.20.2:1293. Client with IP Address [10.10.20.2]
and MAC  Address [1,6,00:00:ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:26 EST:%BAC-DIAGNOSTICS-3-4141:[##MTA-13 APREP
sent to [/10.10.20.2(1293) For MTA 1,6,00:00:ca:b7:7e:91. Client with IP Address
[10.10.20.2] and MAC Address [1,6,00:00: ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:26 EST:%BAC-DIAGNOSTICS-3-0764:[[##MTA-15 SNMPv3
INFORM Received From 10.10.20.2. Client with IP Address [10.10.20.2] and MAC Address
[1,6,00:00:ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:26 EST:%BAC-DIAGNOSTICS-3-0764:[[##MTA-19 SNMPv3
SET Sent to 10.10.20.2. Client with IP Address [10.10.20.2] and MAC Address
[1,6,00:00:ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:26 EST:%BAC-DIAGNOSTICS-3-1092:[Received a TFTP
[read] request from [10.10.20.2:1271] for [bpr01060000cab77e910002]; Client with MAC
Address [1,6,00:00:ca:b7:7e:91] and IP Address [10.10.20.2]]
bac-test.example.com:2005 03 04 18:38:26 EST:%BAC-DIAGNOSTICS-3-1155:[##MTA-23
Finished handling [read] request from [10.10.20.2:1271] for [bpr01060000cab77e910002];
Transferred [236] bytes to Client with MAC Address [1,6,00:00:ca:b7:7e:91] and IP
Address [10.10.20.2]]
bac-test.example.com:2005 03 04 18:38:27 EST:%BAC-DIAGNOSTICS-3-0764:[[##MTA-25 SNMP
Provisioning State INFORM Received from 10.10.20.2. Client with IP Address
[10.10.20.2] and MAC Address [1,6,00:00:ca:b7:7e:91]]]
bac-test.example.com:2005 03 04 18:38:27 EST:%BAC-DIAGNOSTICS-3-0764:[[MTA
Configuration Confirmed, Returned 'pass' as the final MTA provisioning state for
10.10.20.2. Client with IP Address [10.10.20.2] and MAC Address
[1,6,00:00:ca:b7:7e:91]]]
```

診断ツールによるトラブルシューティング

診断ツールを使用すると、BAC サーバのパフォーマンスの統計情報を特定のタイプの統計にまで掘り下げて収集することができます。このツールで実行されるタスクごとに個別のスクリプトを使用すると、次の作業を実行できます。

- 診断情報を同時に収集する（**startDiagnostics.sh**）
- 診断を途中で中止する（**stopDiagnostics.sh**）
- 診断情報の収集ステータスを判断する（**statusDiagnostics.sh**）

診断ツールは、問題が発生したためにトラブルシューティング用の追加データが必要になったときに同時に実行したり、cron ジョブによって指定されたスケジュールで定期的に実行されるように設定したりすることができます。

注意　診断ツールを使用する場合は、診断データを保存するための十分なスペースをシステムで確保してください。

診断ツールは次の場所にあります。

- RDU：*BPR_HOME/rdu/diagnostics/bin*
- DPE：*BPR_HOME/dpe/diagnostics/bin*
- Cisco Network Registrar：*BPR_HOME/cnr_ep/diagnostics/bin*

（注）　収集した診断情報は、**bundleState.sh**　スクリプトを使用してバンドルできます。詳細については、P.16-11 の「サポートを受けるためのサーバ状態のバンドル」を参照してください。

startDiagnostics.sh ツールの使用方法

startDiagnostics.sh ツールは次の 2 種類のモードで実行できます。

- 対話：このモードでは、必要な診断データをオプションのリストから選択できます。
- 非対話：このモードでは、引数が書き込まれた応答ファイルを最初に生成します。次に、**startDiagnostics.sh** スクリプトを実行します。このツールにより、応答ファイルで指定されている引数に基づいて診断データが収集されます。

シンタックスの説明　***startDiagnostics.sh*** [***-r*** *response_file*] | [***-g*** *response_file*] [***-help***]

- ***startDiagnostics.sh***：対話モードで診断を実行します。
- *response_file*：応答ファイルを指定します。
- ***-r*** *response_file*：非対話モードで診断ツールを実行するために生成された応答ファイルを使用します。
- ***-g*** response_file：診断を実行せずに応答ファイルを生成します。
- ***-help***：ツールのヘルプを表示します。***-help*** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。

対話モードでの startDiagnostics.sh の実行

引数を何も指定しないで **startDiagnostics.sh** を入力すると、診断ツールは対話モードで実行され、RDU、DPE、および Network Registrar の各サーバから収集する統計情報を選択するよう求めるメッセージが表示されます。

注意　システム パフォーマンスに深刻な影響を与える可能性があるので、統計情報は慎重に処理してください。

シンタックスの説明　***startDiagnostics.sh*** [***-help***]

- ***startDiagnostics.sh***：対話モードで診断を実行します。
- ***-help***：ツールのヘルプを表示します。***-help*** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。

例

```
# ./startDiagnostics.sh

Please enter directory where to put output files [] /var/CSCObac
   Please enter the duration of the diagnostic (sec) [600]

Please select statistics you would like to gather on RDU

   CPU statistics (y/n/q)? [y]
   Process statistics (y/n/q)? [n]
   IO statistics (y/n/q)? [y]
   Memory statistics (y/n/q)? [y]
   Network statistics (y/n/q)? [y]
   RDU API traffic (y/n/q)? [y]
   RDU CNR traffic (y/n/q)? [y]
   RDU DPE traffic (y/n/q)? [y]
   RDU CNR extension traffic (y/n/q)? [y]
   RDU SNMP traffic (y/n/q)? [y]
   System Configuration (y/n/q)? [y]

Enter addition argument for RDU API traffic
   Please enter RDU Server port [49187]

Enter addition arguments for RDU DPE traffic
   Enter DPE ip addr if you want to capture traffic by ip addr [] 10.10.29.1
   Enter DPE port number if you want to capture traffic by port number [] 49186

Enter addition arguments for RDU CNR_EX traffic
   Enter Ip addr if you want to capture traffic by Cnr Extension IP addr [] 10.10.85.2
   Enter port number if you want to capture traffic by Cnr Extension port []

You could run statusDiagnostics.sh to find out the status of the diagnostics.
You could run stopDiagnostics.sh to stop the diagnostics.
You could run bundleState.sh to bundle the output when diagnostics is complete.
```

（注）　次のオプションの統計をイネーブルにしていない場合、ツールは例にある追加引数の値を要求しません。

- RDU-API トラフィック
- RDU-DPE トラフィック
- RDU-Network Registrar 拡張トラフィック

startDiagnostics.sh ツールを実行すると、ツールを実行したディレクトリの下位に統計ごとの出力ファイルが作成されます。出力ファイルをバンドルし、Cisco Technical Assistance Center に転送してサポートを受けることもできます。サポートを受けるには、System Diagnostics Capture プロンプトで **y** と入力します。

次に例を示します。

```
System Configuration (y/n/q)? [y]
```

サーバ状態のバンドルの詳細については、P.16-11 の「サポートを受けるためのサーバ状態のバンドル」を参照してください。

非対話モードでの startDiagnostics.sh の実行

非対話モードで **startDiagnostics.sh** ツールを初めて実行する前に、応答ファイルを生成する必要があります。その後、1 つのコマンドだけを実行すると、応答ファイルにある引数に基づいて診断情報が収集されます。

シンタックスの説明

startDiagnostics.sh {***-g*** *response_file* | ***-r*** *response_file*} [***-help***]

- ***-g***：応答ファイルを生成します。このオプションは、応答ファイルを初めて生成する場合にのみ使用する必要があります
- ***-r***：応答ファイルを使用して診断ツールを実行します。
- *response_file*：応答ファイルの名前を指定します。
- ***-help***：ツールのヘルプを表示します。***-help*** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。

例

応答ファイルを生成するときの結果を次に示します。

```
# ./startDiagnostics.sh -g response.txt

Please enter directory where to put output files [] /var/CSCObac
   Please enter the duration of the diagnostic (sec) [600]

Please select statistics you would like to gather on RDU

   CPU statistics (y/n/q)? [y]
   Process statistics (y/n/q)? [n]
   IO statistics (y/n/q)? [y]
   Memory statistics (y/n/q)? [y]
   Network statistics (y/n/q)? [y]
   RDU API traffic (y/n/q)? [y] n
   RDU CNR traffic (y/n/q)? [y]
   RDU DPE traffic (y/n/q)? [y] n
   RDU CNR extension traffic (y/n/q)? [y] n
   RDU SNMP traffic (y/n/q)? [y]
   System Configuration (y/n/q)? [y]

Finished generate response file (response.txt).
```

response.txt は、**startDiagnostics.sh** スクリプトを実行するディレクトリの下位ディレクトリに生成されます。この場合は、*BPR_HOME/rdu/diagnostics/bin* です。RDU 診断用に生成される応答ファイルのサンプルを次に示します。

```
test.bundle.direcotry=/var/CSCObac
test.bundle.duration.sec=100
test.cpu.enable=true
test.process.enable=false
test.io.enable=true
test.memory.enable=true
test.network.enable=true
test.rdu_api_traffic.enable=true
test.rdu_cnr_traffic.enable=true
test.rdu_dpe_traffic.enable=true
test.rdu_cnr_ex_traffic.enable=true
test.rdu_snmp_traffic.enable=true
test.system_config.enable=true
test.rdu.port=49187
test.dpe.port=49186
test.dpe.ip=10.10.29.1
test.cnr_ex.ip=10.10.85.2
test.cnr_ex.port=
EOF
```

生成した応答ファイルを使用して診断ツールを実行したときの結果を次に示します。

```
# ./startDiagnostics.sh -r response.txt

You could run statusDiagnostics.sh to find out the status of the diagnostics.
You could run stopDiagnostics.sh to stop the diagnostics.
```

startDiagnostics.sh ツールを実行すると、ツールを実行したディレクトリの下位に統計ごとの出力ファイルが作成されます。

statusDiagnostics.sh ツールの使用方法

statusDiagnostics.sh ツールを使用して、必要な統計情報の診断収集のステータスを判断します。

シンタックスの説明　***statusDiagnostics.sh*** により、統計情報ごとに診断収集のステータスを表示します。

（注）　***statusDiagnostics.sh*** ツールでは ***-help*** オプションを使用できません。

例

```
# ./statusDiagnostics.sh
   CPU diagnostic is running.
   Process diagnostics stopped.
   IO diagnostic is running.
   Memory diagnostic is running.
   Network diagnostic is running.
   Rdu api traffic diagnostic is running.
   Rdu cnr traffic diagnostic is running.
   Rdu dpe traffic diagnostic is running.
   Rdu cnr_ex traffic diagnostic is running.
   Rdu snmp traffic diagnostic is running.
```

stopDiagnostics.sh ツールの使用方法

stopDiagnostics.sh ツールを使用して、統計情報の 1 つまたはすべてに対する診断の実行を中止します。このツールは、対話モードまたは非対話モードで実行できます。

対話モードでの stopDiagnostics.sh の実行

何も引数を指定せずに **stopDiagnostics.sh** を対話モードで実行すると、すべての統計情報または特定の統計情報の診断を中止するかどうかを尋ねるメッセージが表示されます。

シンタックスの説明　***stopDiagnostics.sh*** [***-help***]

- ***stopDiagnostics.sh***：対話モードでの診断収集を中止します。
- ***-help***：ツールのヘルプを表示します。***-help*** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。

例

```
# ./stopDiagnostics.sh

This script allowed to stop specific diagnostic or all diagnostics.
If you would like to stop specific diagnostics, say no to question below.

   Would you like to stop all diagnostics (y/n/q)? [y]
```

非対話モードでの stopDiagnostics.sh の実行

stopDiagnostics.sh を非対話モードで実行すると、すべての統計の診断が中止されます。

シンタックスの説明　***stopDiagnostics.sh -a*** [***-help***]

- ***-a***：メッセージが表示されることなく、すべての統計に対する診断が中止されます。
- ***-help***：ツールのヘルプを表示します。***-help*** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。

例

```
# ./stopDiagnostics.sh -a
#
```

サポートを受けるためのサーバ状態のバンドル

BPR_HOME/{rdu | dpe}/diagnostics/bin ディレクトリにある診断ツールを使用して、サーバ設定や他の診断情報を生成できます（これらのツールの実行方法については、P.16-6 の「診断ツールによるトラブルシューティング」を参照してください）。サポートを受けるためにこの診断情報を Cisco Technical Assistance Center に送信するには、診断ツールを使用して作成される出力ディレクトリをバンドルしてアーカイブを作成する必要があります。このタスクを実行するには、**bundleState.sh** ツールを使用します。

bundleState.sh ツールによって診断情報が収集されるわけではありません。**startDiagnostics.sh** などのツールによって収集されるデータの zip ファイルと tar ファイルを作成するだけです。

バンドルする診断情報には、少なくともシステム設定に関連した情報を含める必要があります。システム情報を生成するには、次のいずれかのツールを使用します。

- captureConfiguration.sh：マウントとディスクの設定、メモリ、およびオペレーティング システムとハードウェアのデータなどのシステム設定情報を収集します。このスクリプトを実行する場合は、出力ディレクトリを指定する必要があります。
- startDiagnostics.sh：BAC サーバのパフォーマンス統計情報を収集します。このスクリプトを実行してシステム設定を取り込む場合は、System Configuration プロンプトで **y** と入力する必要があります。次に例を示します。

  ```
  System Configuration (y/n/q)? [y]
  ```

  詳細については、P.16-6 の「startDiagnostics.sh ツールの使用方法」を参照してください。

問題によっては、追加の診断情報を収集してバンドルに追加するようシスコのサポート担当者から指示される場合があります。

シンタックスの説明

bundleState.sh *archive_directory output_directory* [***-help***]

- *archive_directory*：バンドルするディレクトリ。
- *output_directory*：バンドルの出力先ディレクトリ。
- ***-help***：ツールのヘルプを表示します。***-help*** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。

例

```
# ./bundleState.sh /var/CSCObac /var/CSCObac
/var/CSCObac/state-20071129-064042
Creating state bundle for Cisco support...
+ /var/CSCObac/state-20071129-064042.bpr
+ Compressing state bundle...
+ Size: 3736K compressed, 83776K uncompressed
```

DOCSIS ネットワークのトラブルシューティング

BAC および Cisco uBR7246 CMTS に関する DOCSIS テクノロジーのトラブルシューティングの詳細については、次のアドレスにある『*Troubleshooting uBR Cable Modems Not Coming Online*』を参照してください。
http://www.cisco.com/en/US/tech/tk86/tk89/technologies_tech_note09186a0080094eb1.shtml

PacketCable eMTA プロビジョニングのトラブルシューティング

この項では、PacketCable 音声テクノロジーの配備において考えられる問題の解決に役立つ情報を提供します。

- トラブルシューティングのツール（P.16-15）
- トラブルシューティングのシナリオ（P.16-16）
- 証明書信頼階層（P.16-20）

この項では、PacketCable Multimedia Terminal Adapter（MTA; マルチメディア ターミナル アダプタ）デバイスのプロビジョニング仕様（PKT-SPPROV1.5-I01-050128）の内容を理解していることを前提としています。詳細については、PacketCable の Web サイトを参照してください。

プロビジョニング PacketCable 組み込み型 MTA（eMTA）は、比較的複雑なプロセスですが、適切なツールを使用し、要領を理解すれば、簡単に eMTA を使用することができます。

この項では、Network Registrar と BAC の両方が使用中であることを前提としていますが、情報の多くは他の配備環境にも当てはまります。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）および BAC の基礎知識（サービス クラス、DHCP 基準、ファイル、および BAC ディレクトリ構造）があることを前提としています。

PacketCable eMTA プロビジョニング プロセスは、セキュアなフローを実現するために 25 のステップで構成されています。基本フローの手順数はそれよりも大幅に少ない数です。eMTA のトラブルシューティングを行うには、PacketCable プロビジョニング仕様にある 25 のステップについての知識が不可欠です。第 7 章「PacketCable 音声設定」を参照してください。

この項では、次のトピックについて説明します。

- コンポーネント（P.16-12）
- 主要な変数（P.16-14）

コンポーネント

eMTA のトラブルシューティングを行う前に、次のシステム コンポーネントを理解してください。

- eMTA
- DHCP サーバ
- DNS サーバ
- KDC
- PacketCable プロビジョニング サーバ
- コール管理サーバ

eMTA

eMTA はケーブル モデムと MTA で構成され、共通のソフトウェア イメージを備えており、1 つのボックスに組み込まれています。CM と MTA はそれぞれ独自の MAC アドレスを持ち、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 には、最低でも 3 つの証明書があります。1 つは固有の MTA 証明書です。2 つ目の証明書は MTA の製造業者を特定します。デバイスと製造業者の証明書は、両方とも認証で使用するために MTA によって KDC に送信されます。3 つ目の証明書は、KDC から MTA に送信される証明書を検証するために使用されるテレフォニー ルート証明書です。KDC 証明書はテレフォニー ルートをルートとする証明書チェーンに組み込まれるため、そのテレフォニー ルートは、KDC 証明書の正当性を検証するために MTA に存在する必要があります。MTA 部分では独自の設定ファイルを受信し、制御するコール エージェントを特定するために使用します。

DHCP サーバ

DOCSIS 仕様では、DHCP を使用してケーブル モデムがその IP アドレスをネゴシエートするように規定しています。MTA は、DOCSIS ネットワークのほとんどの CPE と同様に、DHCP を使用して IP アドレスや他の重要な情報（DNS サーバ、Kerberos レルム名の PacketCable Option 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 モデム部分では、通常必要とされる DHCP オプションの他に、Option 122 のサブオプション 1 を要求して受信する必要があります。ケーブル モデム部分は、オファーを受信するときの正しい送信元 DHCP サーバの IP アドレスとして、そのサブオプションを MTA 部分に渡します。

PacketCable サポート付きの BAC を使用する場合は、BAC の設定が正しければ、ToD サーバ、DNS サーバ、TFTP サーバ、および Option 122 のフィールドに値が自動的に取り込まれます。これらのフィールドを 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

Domain Name System（DNS; ドメイン ネーム システム）サーバは、PacketCable プロビジョニングの基本的な要素です。PacketCable プロビジョニング サーバは、BAC アーキテクチャでの Device Provisioning Engine（DPE）です。Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が DHCP サーバにより Option 122 で MTA に提供されるため、適切なゾーンのアドレス（A）レコードを持っている必要があります。KDC レルムには、Kerberos サーバの FQDN が記録されているサーバ（SRV）レコードを含むレルム名と同じ名前のゾーンが存在する必要があります。

SRV レコードで指定される Kerberos サーバ自体は、適切なゾーンの A レコードを持っている必要があります。また MTA 設定ファイルで指定されている Call Management Server（CMS; コール管理サーバ）も、適切なゾーンの A レコードを持っている必要があります。さらに、CMS は MTA の FQDN を解決することによってその MTA に到達するため、MTA 自体も適切なゾーンの A レコードを持っている必要があります。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）を使用することをお勧めします。DDNS の設定およびトラブルシューティングの詳細については、Cisco Network Registrar のマニュアルを参照してください。

KDC

KDC は、MTA の認証を行います。そのため、MTA の証明書を検査するとともに、KDC 自体の証明書を提示して MTA が KDC を認証できるようにする必要があります。また、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、MTA 設定ファイルの場所を MTA に伝達したり、SNMP 経由で MTA パラメータをプロビジョニングしたりします。MTA とプロビジョニング サーバの間のすべての通信で、SNMPv3 を使用します。SNMPv3 通信を開始するためのキーは、KDC との認証フェーズ中に MTA が取得します。プロビジョニング サーバの機能は、BAC アーキテクチャの DPE によって提供されます。

コール管理サーバ

コール管理サーバ（CMS）は、基本的にはソフト スイッチ、つまりコール エージェントです。追加の PacketCable 機能として、たとえばケーブル ネットワークの QoS を制御したりします。MTA は、PacketCable プロビジョニングに成功すると、Network Call Signaling（NCS; ネットワーク コール シグナリング）の Restart in Progress（RSIP; 再起動中）メッセージを CMS に送信します。

主要な変数

この項では、eMTA を適正にプロビジョニングするために必要とされる主な変数について説明します。

- 証明書（P.16-14）
- スコープ選択タグ（P.16-15）
- MTA 設定ファイル（P.16-15）

証明書

MTA_Root.cer ファイルには、MTA ルート証明書（正式な PacketCable MTA ルートをルートとする証明書）が含まれています。

プロビジョニングの対象となる MTA で必要とされるテレフォニー ルート証明書を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の際に、PacketCable の実稼働ルートをルートとするテレフォニー証明書を使用します。テスト環境で使用される PacketCable テスト ルートもあります。

KDC がそれ自体を MTA に対して認証するために使用する KDC 証明書のルートは、MTA に保存されているルート（PacketCable の実稼働ルートまたはテスト ルート）と同じテレフォニー ルートになっている必要があります。ほとんどの MTA ベンダーは Telnet または HTTP ログイン機能を備えたテスト イメージをサポートしているため、イネーブルになっているテレフォニー ルートを判別し、使用するルートを変更できます（ほとんどの場合、選択できるのは PacketCable の実在ルートとテスト ルートのどちらかのみです）。

最も一般的なシナリオでは、（*BPR_HOME/kdc/solaris/packetcable/certificates* ディレクトリから）次の証明書と一緒にロードした 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* ファイルには、MTA によって送信される証明書を検証するために、KDC が使用する MTA ルートが記述されています。

（注）　KDC 証明書のインストールと管理の詳細については、P.14-3 の「PKCert.sh ツールの使用方法」を参照してください。

PacketCable テスト ルートを使用しているかどうかを判断するには、Windows で *CableLabs_Service_Provider_Root.cer* ファイルを開き、Subject OrgName エントリが **O = CableLabs** になっていることを確認するか、または Subject Alternative 名が **CN=CABLELABS GENERATED TEST ROOT FOR EQUIPMENT TEST PURPOSES ONLY** になっていることを確認します。

KDC 証明書（*KDC.cer*）には、使用するレルム名が記述されています。BAC（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レルム名は、このレルム名と一致している必要があります。また、MTA 設定ファイルのレルム org 名は、テレフォニー ルートに含まれる組織名と一致している必要があります。

KDC 証明書には、対応する秘密鍵が記述されており、*BPR_HOME/kdc/solaris* ディレクトリにインストールする必要があります。通常、秘密鍵の名前は、KDC_private_key.pkcs8 または KDC_private_key_proprietary です。証明書を変更する場合は、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において、BAC は、スコープ選択タグの付いたスコープからのすべての DHCP 要求の処理に関係があります。スコープ選択タグは、BAC 管理者のユーザ インターフェイスの DHCP Criteria ページで指定される選択基準に一致します。スコープを BAC 処理に関連付けるためにクライアント クラスを使用することもできます。この関連付けは、必ずデバイスをプロビジョニングする前に行ってください。

MTA 設定ファイル

MTA 設定ファイルには、CMS の場所が記述されています。また、レルム名のエントリが必ず記述されています。この値は、使用中の証明書チェーンの値と一致する必要があります。

MTA 設定ファイル内の特定のテーブル エントリは、MTA に Option 122 で配信されたレルム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レルム名エントリは、Option 122 で配信されたレルム名と一致する必要があります。たとえば、Option 122 で配信されたレルム名が **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、68.69.70.46.67.79.77 などのようにこのレルム名の ASCII 符号化文字値（Cisco Broadband Configurator を使用する場合はドット区切りの 10 進形式）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 上には、この変換を容易に行うことができる無償の ASCII 変換ページが数多くあります。

トラブルシューティングのツール

PacketCable MTA デバイスのプロビジョニング仕様で規定されている 25 の eMTA セキュア プロビジョニングのステップを図 7-1 に示します。この項では、次のトピックについて取り上げます。

- ログ（P.16-15）
- Ethereal、SnifferPro、およびその他のパケット キャプチャ ツール（P.16-16）

ログ

情報を保持するために次のログ ファイルが使用されます。

- Network Registrar には、ログが 2 つ（*name_dhcp_1_log* および *name_dns_1_log*）あります。これらのログには、Network Registrar からの最新のロギング エントリが記録されます。DHCP または DNS に関連した問題の場合には、これらのファイルを調べてください。
- *BPR_HOME/kdc/logs/kdc.log* ファイルには、KDC と MTA のインタラクションすべてと、KDC と DPE のインタラクションが表示されます。

- *BPR_DATA/dpe/logs/dpe.log* ファイルには、SNMPv3 の MTA とのインタラクションに関連する主な手順が表示されます。

（注）　コマンドライン インターフェイス（CLI）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すると、潜在的な PacketCable 問題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用のコマンドの使用方法の詳細については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』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

パケット キャプチャ ツールは、eMTA のトラブルシューティングに不可欠のツールです。CableLabs がパッケージ化している Ethereal バージョンには、PacketCable に固有のパケット デコーダが数多く含まれています。たとえば、Kerberos の AS パケットや AP パケットなどがあります。

- 障害の原因が DHCP に関連していると疑われる場合は、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。
- 障害の原因が DHCP 以降の 25 のステップのいずれかに関連していると疑われる場合は、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。この方法により、図 7-1 に示されるプロビジョニングのステップ 5 ～ 25 を非常に簡単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

表 16-3 に示すシナリオは、eMTA が関係する可能性のある障害です。

表 16-3　トラブルシューティングのシナリオ

予想される問題	考えられる原因	対処方法
KDC が起動しない。	KDC 証明書が秘密鍵に対応していません。	証明書と秘密鍵を確実に一致させます。
	KDC ライセンスの期限が切れているか、または消失しています。	KDC ライセンスを *BPR_HOME/kdc* ディレクトリに復元します。
MTA デバイスが BAC 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 BAC ユーザ インターフェイスで選択された DHCP 基準と一致しません。	関係する MTA について、MTA スコープ選択タグが、作成された PacketCable DHCP 基準のスコープ選択タグと一致することを BAC で確認します。
	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。『*Installation and Setup Guide for Cisco Broadband Access Center 4.0*』を参照してください。
	ケーブル モデム部分が Option 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、BAC に対して設定されている DOCSIS DHCP 基準と一致することを確認します。

表 16-3　トラブルシューティングのシナリオ（続き）

予想される問題	考えられる原因	対処方法
MTA デバイスが DHCP オファーを受け入れず、DHCP フローのサイクルを続ける。	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を確認するか、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 Option 122 のサブオプション 1 で指定されている DHCP サーバとは異なるサーバから送信された可能性があります。	*cnr_ep.properties* ファイルを調べ、メインとバックアップの 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 トレースの両方で、MTA デバイスが KDC に問い合せていないことが示される。	*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 サーバを確認または訂正します。
	Kerberos レルムのゾーンが存在しないか、または正しく設定されていません。	レルムと同じ名前のゾーンが作成されており、「_kerberos._udp 0 0 88 *KDC FQDN*」形式の「SRV」レコードが含まれていることを確認します。
	KDC の「A」レコード エントリが存在しないか、または正しくありません。	Kerberos ゾーンの「SRV」レコードに含まれている FQDN の「A」レコードが存在することを確認します。
	DPE 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 があることを確認します。

表 16-3　トラブルシューティングのシナリオ（続き）

予想される問題	考えられる原因	対処方法
Kerberos の AS 要求中に、KDC が障害を報告する。	MTA 証明書が KDC で使用される MTA ルートと一致しません。	*MTA_Root.cer* を稼働システムで使用されている証明書と比較することにより、*MTA_Root.cer* が正しいことを確認します。 正しい場合、MTA 自体で証明書の問題が発生している可能性があります。このような状況は非常にまれですが、そうなった場合には、MTA の製造業者に連絡してください。
	KDC によるプロビジョニング サーバへの FQDN ルックアップに失敗しました。そのデバイスは、BAC でまだ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 基準の両方が指定されている必要があります。
	クロック スキュー エラーです。詳細については、P.3-7 の「PacketCable ワークフロー」を参照してください。	すべての BAC ネットワーク要素が、NTP を介してクロック同期されていることを確認します。『*Broadband Access Center DPE CLI Reference 4.0*』を参照してください。
	KDC と DPE の間に不一致が存在す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は、これが問題の原因とは考えられません。	*BPR_HOME/kdc/solaris/keys* ディレクトリに次の 3 つのエントリがあ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 ご使用のシステムの DPE FQDN とレルム名は、この例の場合とは異なります。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たキーのいずれかのエントリと一致している必要があります。
KDC により、AS 要求 / 応答（図 7-1 のステップ 9 と 10）で成功と報告されるが、TMA デバイスがステップ 9 より先に進まない。	MTA でロードまたはイネーブルにされているテレフォニー ルートと、KDC にロードされているテレフォニー ルートの間に証明書の不一致があります。	MTA と KDC の証明書を確認してください。
	非常にまれなことですが、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またはイネーブルされていることを確認します。正しくプロビジョニングできるデバイスがない場合は、KDC にある別の証明書を試してください。

表 16-3　トラブルシューティングのシナリオ（続き）

予想される問題	考えられる原因	対処方法
AP 要求 / 応答（図 7-1 のステップ 14）で障害が発生する。	クロック スキュー エラーです。詳細については、P.3-7 の「PacketCable ワークフロー」を参照してください。	すべての BAC ネットワーク要素が、NTP を介してクロック同期されていることを確認します。『*Broadband Access Center DPE CLI 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 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 があることを確認します。
	MTA から DPE へのルートがありません。	ルーティング問題を修正します。
MTA デバイスが設定ファイルの TFTP 要求を発行しない。	DPE で実行されている TFTP サーバへのルートがありません。	ルーティング問題を修正します。
MTA デバイスが TFTP 設定ファイルを受信しない。	DPE で設定ファイルがキャッシュされません。	次のプロビジョニングが試行されてファイルがキャッシュされるまで待ちます。これでキャッシュされない場合は、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。	BAC が TFTP サーバの DPE アドレスを挿入するため、ポリシーからこのオプションを安全に削除できます。
MTA デバイスは設定ファイルを受信するが、DPE は *dpe.log* ファイルにある SNMP Inform（図 7-1 のステップ 25）の受信に失敗する。	次のいずれかの状況が考えられます。 • 設定ファイルの内部での矛盾。 • テレフォニー証明書チェーンのレルム起点との矛盾。 • Option 122 でのレルム名との矛盾。	MTA 設定ファイルに整合性があることを確認します。
RSIP が送信されなくても、MTA デバイスが成功と報告する（図 7-1 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 エントリが存在す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ます。	すべてのルーティング問題を解決します。
MTA デバイスが、CMS サービスを受けるために KDC に再び問い合せるにもかかわらず、成功と報告する（図 7-1 のステップ 25）。	MTA 設定ファイルが誤ったケーブル モデムを示しています。	設定ファイルを訂正するか、設定ファイルのリストにある 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 値が存在しないか、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。	設定ファイルを訂正します。セキュア シグナリングを実行する場合は、サポートのために必要な手順を実行して KDC と BTS を設定します。

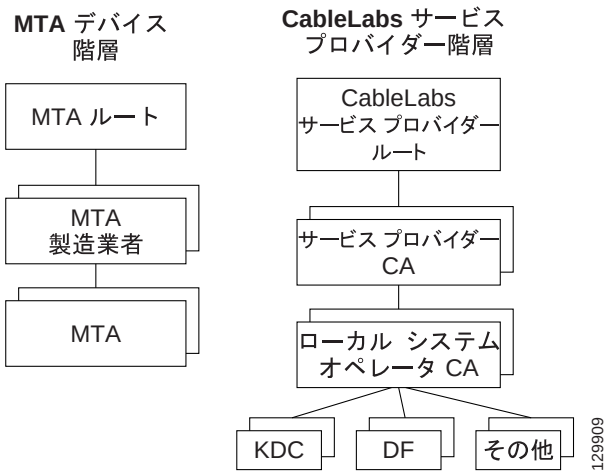
表 16-3　トラブルシューティングのシナリオ（続き）

予想される問題	考えられる原因	対処方法
MTA デバイスが成功と報告し（図 7-1 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、応答でエラーが返される。	MTA が Cisco BTS 10200 上でプロビジョニングされていないか、または正しくプロビジョニングされていません。	Cisco BTS 10200 で MTA をプロビジョニングします。
	eMTA DNS エントリが存在しません。	eMTA の正しい DNS ゾーンにエントリを配置します。ダイナミック DNS の使用をお勧めします。DDNS のイネーブル化の詳細については、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

BAC PacketCable に関係する証明書階層には、図 16-1 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 つがあります。

図 16-1　PacketCable 証明書階層



PacketCable を BAC に実装する前に、次の技術ドキュメントの内容に精通しておいてください。

- *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 では 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連して、いくつかの変更を行う必要があります。Euro PacketCable と PacketCable をできるだけ類似した状態に保つため、Euro PacketCable ではすべての PacketCable セキュリティ技術を使用しており、その中にはセキュリティ仕様 [PKTSP-SEC-I08-030415] の新しいリビジョンも含まれます。

PacketCable 証明書とは異なる Euro-PacketCable 証明書の要素を以下の表に示します。

Euro PacketCable では、Euro-PacketCable 証明書が唯一有効な証明書です。PacketCable 証明書を参照する PacketCable の [PKT-SP-SEC-I08-030415] に記載されているすべての要件は、Euro-PacketCable 証明書の対応する要件に変更されます。

Euro-PacketCable 準拠 eMTA では、ケーブル モデムの非揮発性メモリの中に、DOCSIS CVC CA の公開鍵の代わりに、Euro-DOCSIS ルート CVC CA の公開鍵が保存されている必要があります。Euro PacketCable 準拠の独立型 MTA では、tComLabs CVC ルート証明書と tComLabs CVC CA 証明書が非揮発性メモリに保存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査することで検証されます。

証明書の検証

PacketCable 証明書の検証には、一般に、証明書チェーン全体の検証が含まれます。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場合、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 ルート証明書によって検証され、MTA デバイス証明書の署名は MTA 製造業者証明書の署名によって検証されます。MTA ルート証明書は自己署名され、プロビジョニング サーバに前もって知らされます。MTA ルート証明書内の公開鍵は、この同じ証明書の署名を検証するために使用されます。

通常、チェーンの最初の証明書は、通信経路を通して送信される証明書チェーンに明示的に指定されていません。最初の証明書が明示的に含まれている場合は、検証する側にあらかじめ知らされている必要があり、証明書のシリアル番号、有効期間、および署名の値などの例外を除いて、証明書に変更が一切ないようにする必要があります。既知の CableLabs サービス プロバイダーのルート証明書と比較して、通信経路を通して渡された CableLabs サービス プロバイダーのルート証明書に変更があると、比較を行うデバイスは証明書の検証に必ず失敗します。

証明書チェーン検証の実際のルールは、RFC 2459 に完全に準拠している必要があります。RFC 2459 では、証明書チェーン検証を証明書パス検証と呼んでいます。一般に、X.509 証明書は、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かどうかを判定するための自由なルール セットをサポートしています。このルール セットでは、2 つの名前フィールドのバイナリ比較が一致していることを示さなくても、それらの名前フィールドが一致すると宣言される場合があります。RFC 2459 では、実装環境において、単純なバイナリ比較を使用して一致または不一致を宣言することができるように、認証局で名前フィールドの符号化を制限するよう推奨しています。

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、その発行者の証明書の 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。実装環境では、DER 符号化された tbsCertificate.issuer フィールドど 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、発行者名とサブジェクト名を比較することができます。

次の項では、必要な証明書チェーンを指定します。それらの証明書チェーンを使用して、図 16-1 に示す PacketCable 証明書信頼階層の（最下位の）リーフ ノードに存在する各証明書を検証する必要があります。

入れ子になっている有効期間は検査されず、故意に実行されてはいません。このため、証明書の有効期間は、それを発行した証明書の有効期間内に入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ミラーリングしています。ルートは CableLabs 発行の PacketCable MTA ルート証明書で、このルート証明書は、一連の製造業者証明書の発行元証明書として使用されます。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。

以降の表に示す情報には、RFC 2459 に従った必須フィールドの PacketCable 固有の値が含まれています。これらの PacketCable 固有の値は、表 16-4 の情報に従って指定する必要があります。ただし、有効期間の値は、それぞれの表で指定されている値にします。PacketCable での必須フィールドが明示的に示されていない場合は、RFC 2459 のガイドラインに従ってください。

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部として検証する必要があります。

表 16-4 に、MTA ルート証明書に関係する値のリストを示します。

表 16-4　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使用されるとともに、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が生じることがないように、十分な長さの有効期間が設定されています。	
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部として検証する必要があります。州、市、および製造業者の施設は、オプションの属性です。製造業者は、複数の製造業者証明書を備えることがあり、製造業者ごとに 1 つ以上の証明書が存在する場合もあります。同じ製造業者の証明書すべてを、製造時または現地でのアップデート中に各 MTA に提供することができます。MTA は、MTA デバイス証明書にある発行者名を MTA 製造業者証明書にあるサブジェクト名と照合して、使用する適切な証明書を選択する必要があります。存在する場合は、RFC 2459 で規定されているように、デバイス証明書の authorityKeyIdentifier が製造業者証明書の subjectKeyIdentifier と一致する必要があります。O および CN の *CompanyName* フィールドは、その 2 つのインスタンス間で異なる場合があります。

表 16-5 に、MTA 製造業者証明書に関係する値のリストを示します。

表 16-5　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* [stateOrProvinceName = *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 製造業者に対して発行され、PacketCable セキュリティ仕様の規定どおり（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 にインストールできます。この証明書は、MTA MIB 中に読み取り専用パラメータとして表示されます。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 デバイス証明書と一緒に使用されます。	
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部として検証する必要があります。州、市、および製造業者の施設は、オプションの属性です。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）として指定する必要があります。16 進数のアルファベット文字（A ～ F）は、大文字で表記する必要があります。MTA デバイス証明書は、置換または更新しないでください。

表 16-6 に、MTA デバイス証明書に関係する値のリストを示します。

表 16-6　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、MTA MIB 中に読み取り専用パラメータとして表示されます。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

eMTA のコード検証証明書（CVC）仕様は、DOCSIS 仕様 SP-BPI+-I11-040407 で指定されている DOCSIS 1.1 CVC と同一の仕様にする必要があります。

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のルートは、CableLabs 発行の CableLabs サービス プロバイダー ルート証明書です。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 プロバイダーの証明書は、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、補助装置証明書に署名するためにその証明書が使用されます。存在しない場合には、サービス プロバイダーの CA が補助証明書に署名します。

表 16-7 の情報には、RFC 2459 での必須フィールドに対する固有の値が含まれています。それらの固有値を使用する必要があります。必須フィールドがリストに含まれていない場合は、RFC 2459 のガイドラインに厳密に従う必要があります。

CableLabs サービス プロバイダー ルート証明書

Kerberos キー管理を実行できるようにするには、Kerberos プロトコルに対する PKINIT 拡張を使用して、事前に MTA と KDC で相互認証を実行する必要があります。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 の認証を行う場合、MTA 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む KDC 証明書チェーンを検証します。

表 16-7 に、CableLabs サービス プロバイダー ルート 証明書に関係する値のリストを示します。

表 16-7　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、製造時に各 MTA にインストールされるか、または PacketCable セキュリティ仕様の規定どおりセキュア コード ダウンロードによってインストールされ、プロビジョニング サーバが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、いずれも MTA MIB に表示されることはありません。	
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が生じることがないように、十分な長さの有効期間が設定されています。	
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 プロバイダーが保持する証明書で、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 サーバ証明書が含まれる証明書チェーンの一部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、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 証明書を変更するたびに、CableLabs サービス プロバイダー ルート証明書を使用してその署名を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 属性を以前と同じ値に保つ必要があります。O および CN にある *Company* フィールドは、その 2 つのインスタンス間で異なる場合があります。

表 16-8 に、CableLabs サービス プロバイダー CA 証明書に関係する値のリストを示します。

表 16-8　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、製造時に各 MTA にインストールされるか、または PacketCable セキュリティ仕様の規定どおりセキュア コード ダウンロードによってインストールされ、プロビジョニング サーバが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、いずれも MTA MIB に表示されることはありません。	
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が生じることがないように、十分な長さの有効期間が設定されています。	
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 と呼ばれる地域別の認証局（対応するローカル システム証明書を発行する）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ていません（ローカル システム証明書により、MTA が特定地域内の KDC に制限される可能性があります）。

表 16-9 に、ローカル システム CA 証明書に関係する値のリストを示します。

表 16-9　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 と呼ばれる地域別の認証局（対応するローカル システム証明書を発行する）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ていません（ローカル システム証明書により、MTA が特定地域内の KDC に制限される可能性があります）。	

表 16-9　ローカル システム CA 証明書 （続き）

ローカル システム CA 証明書	
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

この項に示すすべての証明書は、ローカル システム CA またはサービス プロバイダー CA によって署名されます。この標準には、将来的に他の補助証明書が追加されることがあります。

KDC 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部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 証明書拡張を含めるよう規定しています。この証明書拡張の値は、KDC の Kerberos プリンシパル名にする必要があります。

表 16-10 に、KDC 証明書に関係する値のリストを示します。

表 16-10　KDC 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照会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]	

配信機能（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部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 16-11 に、DF 証明書に関係する値のリストを示します。

表 16-11　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部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ことがあります。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 16-12 に、PacketCable Server 証明書に関係する値のリストを示します。

表 16-12　PacketCable サーバ証明書

PacketCable サーバ証明書		
Subject Name Form	**PacketCable** C=*Country* O=*Company* OU=PacketCable OU=[*Local System Name*] OU=*Sub-System Name* 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、オプションで、その値の後にコロン（:）（前後にスペースなし）と Element ID を続けることができます。 *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。このようなサーバには、CMS、CMTS、および MGC があります。[8] は、5 オクテット右揃えの、空白文字が入力された、ASCII 符号化数値文字列として Element ID を定義します。証明書で使用するために Element ID を変換するときには、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 の場合、CMTS の通常名は「123.210.234.12:00311」となります。 *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 • コール管理サーバの場合：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	**Euro PacketCable** C=*Country* O=*Company* OU=Euro-PacketCable [OU=*Local System Name*] OU=*Sub-system Name* CN=*Server Identifier*[:*Element ID*] commonName の追加仕様については、[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	

表 16-12　PacketCable サーバ証明書 （続き）

PacketCable サーバ証明書	
Validity Period	MSO ポリシーにより設定
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。特に説明のない限り、次の subjectAltName 拡張には、サブジェクトの CN フィールドで指定された対応する名前値が含まれている必要があります。

CMS 証明書の CN 属性値は、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 属性値は、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 属性値は、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 のいずれかが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 は汎用性を備えており、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によって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をサポートできます。

CableLabs CVC 階層は、eMTA には適用されません。

CVC の共通要件

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 にする必要がある。
- 証明書は、以降の各表で指定されてい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）である必要がある。

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部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.16-21 の「証明書の検証」を参照してください。

表 16-13 に、CableLabs コード検証ルート CA 証明書に関係する値のリストを示します。

表 16-13　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 の非揮発性メモリに保存される必要があります。	
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部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.16-21 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、同時に 1 つの CableLabs CVC CA をサポートする必要があります。

表 16-14 に、CableLabs コード検証 CA 証明書に関係する値のリストを示します。

表 16-14　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 の非揮発性メモリに保存される必要があります。	
Signed By	CableLabs コード検証ルート CA	
Validity Period	CableLabs ポリシーにより設定	

表 16-14　CableLabs コード検証 CA 証明書 （続き）

CableLabs コード検証 CA 証明書	
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 16-15 に、製造業者コード検証証明書に関係する値のリストを示します。

表 16-15　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 は、Common Name の Company Name と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部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.16-21 の「証明書の検証」を参照してください。

表 16-16 に、サービス プロバイダー コード検証証明書に関係する値のリストを示します。

表 16-16　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 は Common Name の Company Name と異なる場合があります。

CVC の証明書失効リスト

CVC の証明書失効リスト（CRL）をサポートする場合に、S-MTA は不要です。