プライム ケーブル プロビジョニングのトラブルシューティング

このセクションでは、プライム ケーブル プロビジョニングでトラブルシューティングする方法の詳細を提供します。

プライム ケーブル プロビジョニングに関連する Faq のリストについては、『Frequently Asked Questions』を参照してください。

顧客の特定の問題と解決策については、サポート サイトに投稿されているテクニカル ノートを参照することもできます。

この章では、次の内容について説明します。

トラブルシューティング のチェックリスト

プライム ケーブル プロビジョニングでトラブルシューティングして、次の表で説明されているチェックリストを使用します。

表 *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	チェックを入れる
1. プライム ケーブルプロビジョニングがインストールされているすべてのシステムで、プライム ケーブル プロビジョニングがアップされているか確認します。	Using Prime Cable Provisioning Process Watchdog from CLI	❑
2. 重大度の高いエラーの兆候について、プライム ケーブル プロビジョニング コンポーネント ログを確認します。これらには、次の記録情報を含みます。 • RDU • DPE	地域の配布ユニット ログ デバイス プロビジョニング エンジン ログ	❑
3. 管理者ユーザー インターフェイスからサーバ アップタイムを表示して、サーバがバウンスしないことを確認します。	Admin UI を使用したサーバのモニタリング	❑
4. 管理者ユーザー インターフェイスからRDUおよびDPEサービス パフォーマンス統計を表示します。拡張トランザクション時間など、通常とは異なる番号を確認します。	Admin UI を使用したサーバのモニタリング	❑
5. Syslog アラートのログを確認します。	アラートおよびエラー メッセージ	❑
6. 次のように、オペレーティング システムとハードウェア リソースを確認します。 • ディスク容量 • CPU time • Memory	特定コマンドのドキュメント。	❑

手順	参照先	チェックを入れる
7. 特定のデバイスをトラブルシューティングするには、DPE にキャッシュされているデバイスの手順を確認します。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **show device-config**。	❑
8. 管理者ユーザー 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、一定期間が過ぎたらトラブルシューティング ログを検査します。	トラブルシューティングのためのデバイス設定	❑
9. 詳細なロギング情報については、RDU または適切な DPE で高レベルのロギングを設定します。	RDU ログ レベル ツールの使用 Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **log level** コマンド	❑

デバイス ID 別のデバイスのトラブルシューティング

この機能を使用して、1 つ以上の特定のデバイスに関する詳細な診断を収集することができます。トラブルシューティング情報には、特定のデバイスやデバイスのグループに関連するすべてのサーバのインタラクションが含まれます。この情報には、管理者ユーザーインターフェイス操作、RDU アプリケーション プログラミング インターフェイス（API）操作、デバイスとの DPE インタラクション、サーバ間の DPE-to-RDU インタラクションが含まれます。

ログ記録をオンにしたり、特定のデバイス情報のログファイルを通して検索したりすることなく、1 個以上の特定のデバイスに対してグループ管理で診断情報を有効または無効にできます。

プライム ケーブル プロビジョニングは、詳細な診断を収集するデバイス 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ます。トラブルシューティング情報は RDU で一元的に保存され、デバイスベースごとに保持されます。DPE も Cisco Prime Network Registrar 拡張機能もこのデータを保存しません。それ以外に、RDU にこの情報を転送し、情報を受信して *BPR_DATA/rdu/*ログ 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、*rdu.log*、*dpe.log*、*audit.log* など他のログ ファイルと異なります。診断モードでデバイスの特定の設定に関連する詳細なトラブルシューティング情報のみログに記録します。

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 拡張で発生したすべての新しいトラブルシューティング イベントは廃棄されます。トラブルシューティング情報のロギングは、RDU への接続を復元後にのみを再開します。

DPE は、デバイスの IP アドレスに対して診断する MAC アドレスと特定のデバイスの DUID をマッピングします。DPE は診断するデバイスの Network Registrar 拡張機能から IP 更新を受信します。

新しいデバイスまたはグループの追加などデバイス トラッキング リストへの変更は、すべてのサーバですぐに反映されます。RDU または DPE を再起動する必要はありません。それぞれのサーバのログ ファイルは、現在の診断モードのデバイス リストを一覧にしています。

⚠

注意 追加メモリおよびディスク容量は、デバイスのトラブルシューティング機能が使用される場合に必要です。トラッキング対象のデバイスの数が増えると、作成したログ量をサポートするために必要なメモリとディスク容量になります。

トラブルシューティングのためのデバイス設定

デバイス診断は、1 個以上のデバイスが診断モードに設定されている場合無効です。

デバイスの診断を有効にするため、デバイスをプライム ケーブル プロビジョニング RDU で事前登録する必要があります。デバイスがまだ事前登録されていない場合、[Add（追加）] ボタンをクリックして、[Manage Devices（デバイスの管理）] ページからデバイスを追加します。デバイスを追加する方法については、『Adding Device Records』を参照してください。

診断モードでデバイスの最大数を設定し、過剰なデバイスが誤ってこのモードになることを防ぎ、サーバのパフォーマンス低下を回避できます。デフォルトでは、許可されるデバイスの最大数は 25 です。Admin UI からデバイスの最大数を設定するには、**[Configuration（設定）] > [Defaults（デフォルト）]** で [Systems Defaults（システム デフォルト）] ページをクリックします。[Maximum Diagnostics Device Count（診断デバイスの最大カウント）] フィールドに値を入力します。

Relating a Device to a Group

特定のグループに関連付けることで、デバイスをトラブルシューティングできます。関連付け機能を使用して、MAC アドレスまたは DUID を使用して、デバイスを特定のグループに関連付けます。これは、特定のグループ タイプに関連付けられます。（『Relating and Unrelating Devices』を参照してください。）デバイスに大量の情報を記録します。情報を使用して、潜在的な問題をトラブルシューティングできます。

次の表では、関連付けと関連付け解除機能を使用する可能なワークフローを特定します。

表 *2:* サンプルの関連付け/関連付け解除プロセス

手順	操作
1.	問題が存在しているかどうか確認し、どのデバイスが影響を受けるかを特定します。
2.	デバイスをグループに関連付けします。

手順	操作
3.	デバイス トラフィックが送信されるまで数分間待機するか、デバイスのハード ブートを実行します。
4.	文章処理アプリケーションで *BPR_DATA/rdu/logs/troubleshooting.log* ファイルを開き、MACアドレスまたは特定のデバイスの DUID のエントリを検索します。
5.	問題を特定、修正、テスト、確認します。
6.	グループからデバイスの関連付けを解除します。

Viewing List of Devices in Diagnostics Mode

デバイスのトラブルシューティングを有効にすると、デバイスはトラブルシューティング モードでデバイスのリストを含む特別なデバイス グループに自動的に追加されます。グループ タイプは **system** であり、グループ名は **system-diagnostics** です。API または管理者ユーザー インターフェイスからこのグループ内のデバイスのリストにアクセスできます。

現在診断に有効になっているデバイスのリストを表示するには。

ステップ 1 [Manage Devices（デバイスの管理）] ページで、[Search Type（検索タイプ）] ドロップダウンリストをクリックし、[Group Search（グループ検索）] を選択します。

ステップ 2 [Group Name (Group Type)（グループ名（グループ タイプ））] ドロップダウンリストから、**system-diagnostics (system)** オプションを選択して診断モードのすべてのデバイスを表示します。

ステップ 3 [検索（Search）] をクリックします。

（注） 診断モードでデバイスのリストを表示する別の方法は、RDU ログ（*rdu.log*）および DPE ログ（*dpe.log*）ファイルを参照してください。サーバが起動するとき、そして診断が有効になっているデバイスのリストに変更があるときに、デバイスのリストが記録されます。診断に有効になっているデバイスは、5-notification のログ レベルのログ ファイルに表示されます。ログ ファイルの詳細は、『Monitoring Component Logs』を参照してください。

例

この例では、MTA をトラブルシューティングするときのログ出力について説明しています。

```
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]]]
```

診断ツールを使用したトラブルシューティング

プライム ケーブル プロビジョニング サーバにパフォーマンス統計情報を収集する診断ツールを使用できます（統計情報の特定タイプまで）。このツールを実行する各タスクに個別のスクリプトを使用して、次のことが可能です。

- 診断を同時に収集します（**startDiagnostics.sh**）
- 診断を途中で停止します（**stopDiagnostics.sh**）
- 診断収集の状態を確認します（**statusDiagnostics.sh**）

問題が発生し、トラブルシューティングに追加データが必要な場合、同時に診断ツールを使用するか、cron ジョブを介して特定のスケジュールで定期的に実行するように設定できます。

注意 診断ツールを使用する場合、診断データを保存するために十分な領域が確保されていることを確認します。

診断ツールは次の場所に存在します。

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

（注） **bundleState.sh** スクリプトを使用して収集された診断をバンドルできます。詳細については、『サポートのためのサーバ状態のバンドリング』を参照してください。

StartDiagnostics.sh ツールの使用

2 つのモードで **startDiagnostics.sh** ツールを実行できます。

- インタラクティブ：このモードでは、オプションのリストから必要な診断データを選択できます。
- 非インタラクティブ：このモードでは、最初に引数を含む応答ファイルを生成します。次に、**startDiagnostics.sh** スクリプトを実行する場合、ツールは応答ファイルで指定された引数に基づき診断データを収集します。

構文の説明

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

- **startDiagnostics.sh**：インタラクティブ モードで診断を実行します。
- *response_file*：応答ファイルを特定します
- **-r** *response_file*：非インタラクティブ モードで、生成された応答ファイルを使用して診断ツールを実行します。
- **-g** response_file：診断の実行せず、応答ファイルが生成されます
- **-help**：ツールのヘルプを表示します。**-help** オプションのみを使用する必要があります。他のオプションで使用しないでください。

インタラクティブ モードで startDiagnostics.sh の実行

引数を指定せず **startDiagnostics.sh** を入力する場合、診断ツールはインタラクティブ モードで実行され、RDU、DPE、Network Registrar サーバから目的の統計情報を選択するように求められます。

注意 システム パフォーマンスに重大な影響を与える可能性があるため、十分に注意して統計情報を処理します。

構文の説明

startDiagnostics.sh [**-help**]

- **startDiagnostics.sh**：インタラクティブ 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** オプションのみを使用する必要があります。他のオプションで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情報を有効にしない場合、ツールは例で示すような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 ツールを実行後、各統計情報の出力ファイルがツールを実行するディレクトリの下で作成されます。出力ファイルをバンドルし、それらをサポートのためCisco Technical Assistance Center に転送できます。そのためには、システム診断キャプチャ 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についての詳細は、『サポートのためのサーバ状態のバンドリング』を参照してください。

静的モードで startDiagnostics.sh の実行

最初に非インタラクティブ モードで **startDiagnostics.sh** を実行する前に、応答ファイルを生成する必要があります。その後、応答ファイルに含まれる引数に基づき診断情報を収集する単一コマンドのみ実行する必要があります。

構文の説明

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

- **-g**：応答ファイルを生成します。最初に応答ファイルを生成するときにのみ、このオプションを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** オプションのみを使用する必要があります。他のオプションで使用しないでください。

例

この結果は、応答ファイルを生成するときに発生します。

```
# ./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で生成されます。この例では、*BPR_HOME/rdu/diagnostics/bin*。RDU 診断に生成されたサンプル応答ファイルは次のとおり機能します。

```
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を実行する場合に、この結果が発生します。

```
# ./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 ツールを実行後、各統計情報の出力ファイルがツールを実行するディレクトリの下で作成されます。

StatusDiagnostics.sh ツールの使用

statusDiagnostics.sh ツールを使用して、必要な統計情報の診断コレクションの状態を判別するツールです。

構文の説明

statusDiagnostics.sh各統計情報の診断コレクションのステータスが表示されます。

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

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

stopDiagnostics.sh ツールを使用して、1 個の統計情報またはすべての統計情報に実行している診断を停止します。インタラクティブ モードまたは非インタラクティブ モードで、このツールを実行することができます。

インタラクティブ モードで stopDiagnostics.sh の実行

引数がない状態でインタラクティブ モードで **stopDiagnostics.sh** を実行し、すべての統計または特定の統計の診断を停止する場合指定するように求められます。

構文の説明

stopDiagnostics.sh [**-help**]

- **stopDiagnostics.sh**：インタラクティブ モードで診断の収集を停止します。
- **-help**：ツールのヘルプを表示します。**-help** オプションのみを使用する必要があります。他のオプションで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]
```

静的なモードの stopDiagnostics.sh の実行

非インタラクティブ モードで **stopDiagnostics.sh** を実行すると、すべての統計情報で診断が停止します。

構文の説明

stopDiagnostics.sh -a [**-help**]

- **-a**：要求なくすべての統計情報の診断を停止します。
- **-help**：ツールのヘルプを表示します。**-help** オプションのみを使用する必要があります。他のオプションで使用しないでください。

例

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

サポートのためのサーバ状態のバンドリング

サーバ設定とその他の診断情報を、*BPR_HOME/{rdu | dpe}/diagnostics/bin* ディレクトリの診断ツールを使用して生成できます。（これらのツールを実行する方法については、『診断ツールを使用したトラブルシューティング』を参照してください。）Cisco Technical Assistance Center へのサポートに診断情報を使用できるようにするには、診断ツールを使用して作成された出力ディレクトリをアーカイブにバンドルする必要があります。このタスクを実行するのには、**bundleState.sh** ツールを使用します。

BundleState.sh ツールは診断を収集していないことに注意してください。**startDiagnostics.sh** が収集するツールのデータを圧縮および tar のみします。

バンドルする診断はシステム設定に関連する情報を最低限含む必要があります。システム情報を生成するには、いずれかを使用します。

- captureConfiguration.sh：設置、ディスク設定、メモリ、オペレーティング システム、ハードウェア データなど、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と、出力ディレクトリを指定する必要があります。
- startDiagnostics.sh：プライム ケーブル プロビジョニングのパフォーマンス統計情報を収集します。システム設定をキャプチャするためにこのスクリプトを実行する場合、システム設定プロンプトで **y** を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、『StartDiagnostics.sh ツールの使用』を参照してください。

特定の問題については、Cisco のサポート担当者が追加の診断情報を収集し、バンドルするように指示できます。

構文の説明

bundleState.sh*archive_directoryoutput_directory*[**-help**]

- *archive_directory*：バンドルするディレクトリ。
- *output_directory*：バンドルを出力するディレクトリ。
- **-help**：ツールのヘルプを表示します。**-help** オプションのみを使用する必要があります。他のオプションで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

プライム ケーブル プロビジョニングおよび 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については、『*Troubleshooting uBR Cable Modems Not Coming Online*』: http://www.cisco.com/en/US/tech/tk86/tk89/technologies_tech_note09186a0080094eb1.shtml を参照してください。

Troubleshooting PacketCable Provisioning

このセクションでは、PacketCable 音声テクノロジ導入の問題を解決するのに役立つ情報について説明しています。

- トラブルシューティング ツール
- トラブルシューティング シナリオ
- Certificate Trust Hierarchy, page 26-20

このセクションでは、PacketCable マルチ メディア終端アダプタ（MTA）デバイスのプロビジョニング仕様、PKT-SP-PROV1.5-I01-050128 および PacketCable 2.0 E UE プロビジョニング フレームワーク仕様、PKT-SP-EUE-PROV-I07-110825 に精通していることを前提としています。詳細については、PacketCable web サイトを参照してください。

MTA（eMTA）または E-DVA が組み込まれているプロビジョニング PacketCable は、比較的複雑なプロセスですが、適切なツールと「企業の手法」により、eMTAs または E-DVA の運用は容易になります。

このセクションでは、Prime Network Registrar とプライム ケーブル プロビジョニングの両方を使用していることを前提としていますが、多くの情報を他の導入にも適用しています。Network Registrar（範囲、ポリシー、基本 DNS ゾーン設定、記録エントリ）およびプライム ケーブル プロビジョニング（サービス クラス、DHCP 条件、ファイル、プライム ケーブル プロビジョニング ディレクトリ構造）の基本的な知識があることを前提としています。

PacketCable eMTA または E-DVA プロビジョニング プロセスは、25 段階の Secure フローで構成されています。基本フローはそれよりもはるかに少ない手順です。EMTAs または E DVA トラブルシューティングについては、PacketCable プロビジョニング仕様から 25 手順の知識は絶対に必要です。『Configuring PacketCable』を参照してください。

ここでは、次の内容について説明します。

- コンポーネント
- 主な変数

コンポーネント

eMTA をトラブルシューティングする前に、次のシステム コンポーネントを十分に理解する必要があります。

- 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 は一般的なソフトウェア イメージのケーブル モデムであり、1 つのボックス内に存在する MTA です。CM および MTA は、各自 MAC アドレスを有し、それぞれ独自の IP アドレスを取得する DHCP を実行します。eMTA には、次の 3 つの証明書が最低限含まれます。第一の証明書は、固有の MTA 証明書です。第二の証明書は、MTA 製造元を識別します。デバイスおよびベンダーの両方の証明書は、KDC 自体の認証のため MTA により送信されます。第三の証明書は、KDC により MTA に送信された証明書の検証に使用されるテレフォニー ルート証明書です。テレフォニー ルートから KDC 証明書をチェーンされるため、テレフォニー ルートは KDC 証明書の信頼性を確認するために MTA に存在している必要があります。MTA 部分は独自の設定ファイルを受信し、これは特にコール エージェントの制御を識別するために使用されます。

DHCP サーバ

DOCSIS 仕様は、ケーブル モデムが DHCP を使用して IP アドレスをネゴシエートすることを要求します。DOCSIS ネットワークのほとんどの CPE にように、MTA はその IP アドレスとその他の重要な情報を取得するために、DHCP を使用する必要があります（DNS サーバ、Kerberos レルム名の PacketCable オプション 122、プロビジョニング サーバ FQDN）。

（注） 通常必要とされる DHCP オプションに加えて、ケーブル モデム部分はオプション 122 サブオプション 1 を要求し受信する必要があります。これは、オファーを承認する適切な DHCP サーバの IP アドレスとして、MTA 部分に送信されます。

PacketCable サポートによりプライム ケーブル プロビジョニングを使用する場合、適切に設定されたプライム ケーブル プロビジョニングが ToD サーバ、DNS サーバ、TFTP サーバ、オプション 122 フィールドに自動的に入力することに注意してください。これらは、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。プライム ケーブル プロビジョニング アーキテクチャのデバイス 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、その完全修飾ドメイン名（FQDN）が DHCP サーバによってオプション 122 の MTA に提供されるため、適切なゾーンのアドレス（A）レコードが必要です。KDC レルムは Kerberos サーバの FQDN を含むサーバ（SRV）レコードを含んでいるレルム名と同じ名前のゾーンが必須です。

SRV レコードで識別されている Kerberos サーバは、適切なゾーンに A レコードが必要です。MTA 設定ファイルで識別されたコール管理サーバ（CMS）は、適切なゾーンの A レコードが必要です。最後に、FQDN を解決することで CMS が MTA に到達するため、MTA には適切なゾーンの A レコードが必須です。ダイナミック DNS（DDNS）は、MTA の A レコードを作成

する基本的な方法です。DDNS の設定とトラブルシューティングに関する詳細は、Cisco Prime Network Registrar のマニュアルを参照してください。

KDC

KDC は、MTA の認証に責任を負います。その結果、MTA 証明書を確認し、MTA が KDC を認証するために独自の証明書を提供する必要があります。DPE（プロビジョニング サーバ）と通信し、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、MTA に対して MTA 設定ファイルの場所の通信や、SNMP 経由の MTA パラメータのプロビジョニングを担当します。SNMPv3 は、MTA およびプロビジョニング サーバ間のすべての通信に使用されます。SNMPv3 通信を開始するために使用するキーは、KDC とその認証フェーズ中に、MTA で取得されます。プロビジョニング サーバ機能は、プライム ケーブルプロビジョニング アーキテクチャで、DPEにより提供されます。

コール管理サーバ

コール管理サーバ（CMS）は基本的にソフトスイッチまたはコールエージェントであり、ケーブル ネットワークで特に、サービスの品質を制御する PacketCable 機能を追加します。PacketCableMTA はプロビジョニングが成功したら、ネットワーク コール信号（NCS）の再起動が進行中（RSIP）であることを通知するメッセージを CMS に送信し ます。

主な変数

このセクションでは、eMTA を正しくプロビジョニングに必要な主な変数について説明します。

- 証明書
- 範囲選択タグ
- MTA 設定ファイル

証明書

MTA_Root.cer ファイルには、MTA ルート証明書が含まれます（公式の PacketCable MTA ルートにルートされている証明書）。

プロビジョニングする MTA に必要なテレフォニー ルート証明書を前もって知る必要があります。実稼働ネットワークでの展開は、PacketCable の実際のルートでルートされてい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。

MTA に対して認証するため KDC で使用される KDC 証明書は、MTA に保存されている同じテレフォニー ルートでルートされる必要があります（PacketCable 実際またはテスト ルート）。ほとんどの MTA ベンダーでは、Telnet/HTTP ログイン機能を持つテスト 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有効か判断し、使用されているルートを変更できます（ほとんどの場合、PacketCable の実際またはテスト ルート間でのみ選択可能です）。

最も一般的なシナリオでは、次のように証明書（*BPR_HOME/kdc/<Operating System>/packetcable/certificates* ディレクトリから）とともにロードされている KDC があります。

- *CableLabs_Service_Provider_Root.cer*
- *Service_Provider.cer*
- *Local_System.cer*
- *KDC*
- *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で構成されています。*MTA_Root.cer* ファイルには、KDC により使用されている MTA ルートが含まれ、MTA から送信された証明書を検証します。

（注） KDC 証明書のインストールおよび管理に関する詳細は、『Using PKCert.sh』を参照してください。

PacketCable テスト ルートを使用するか判断するには、Windows では *CableLabs_Service_Provider_Root.cer*ファイルを開き、Subject OrgName エントリが **O＝CableLabs** であることを確認し、Subject Alternative name が **CN=CABLELABS GENERATED TEST ROOT FOR EQUIPMENT TEST PURPOSES ONLY** を読み取ることをチェックします。

KDC 証明書（*KDC.cer*）には、使用するレルム名が含まれています。プライム ケーブル プロビジョニング（および対応する DNS 名）を使用するように設定されているレルム名は、このレルム名に一致する必要があります。さらに、MTA 設定ファイル レルム名はテレフォニー ルートに表示されている組織名と一致する必要があります。

KDC 証明書には、*BPR_HOME/kdc/linux* ディレクトリにインストールされている対応するプライベート キーあります。通常これは KDC_private_key.pkcs8 または KDC_private_key_proprietary と呼ばれます。証明書を変更する際、秘密キーを変更する必要があります。

範囲選択タグ

ほとんどのシナリオで、プライム ケーブル プロビジョニングは、プライム ケーブル プロビジョニング管理者ユーザー インターフェイスの DHCP 条件ページで指定されている選択条件に一致する範囲選択タグを使用した、範囲からすべての DHCP 要求の処理に関係します。クライアント クラスは、プライム ケーブル プロビジョニングへの範囲設定に使用できます。デバイスのプロビジョニングを試行する前に、この関連付けを確認してください。

MTA 設定ファイル

MTA 設定ファイルには CMS の場所が含まれています。さらに、レルム名のエントリを含める必要があります。この値は、使用中の証明書チェーンと一致する必要があります。

オプション 122 で MTA に配信されたレルム名別に、MTA 設定ファイル内で表のエントリに一定のインデックスが付けられます。MTA 設定ファイルのこのレルム名のエントリは、オプション 122 で配信されたものと一致する必要があります。たとえば、**DEF.COM** がオプション 122 で配信されたレルム名だった場合、pktcMtaDevRealm 表の MTA 設定ファイル エントリは、レルム名の ASCII-コード文字値（Cisco Broadband Configurator を使用する場合、10 進形式ドット区切り文字）で構成されたサフィックスでインデックス化されます。例：68.69.70.46.67.79.77。多くのフリー ASCII 変換ページが Web 上で使用でき、Web によるこの変換が簡単になります。

トラブルシューティング ツール

PacketCable MTA デバイスのプロビジョニング仕様に記載されている 25 eMTA セキュリティで保護プロビジョニング手順は、図 1 で説明されています。この章の内容は次のとおりです。

- ログ
- Ethereal、SnifferPro、またはその他のパケット キャプチャ ツール

ログ

これらのログ ファイルは、次の情報を保持するために使用されます。

- Network Registrar には、2 つのログ（*name_dhcp_1_log* と *name_dns_1_log*）があり、Network Registrar から最新のログ エントリが含まれています。DHCP または DNS 関連の問題について、これらのファイルを確認します。
- *BPR_HOME/kdc/logs/kdc.log* ファイルは、MTAとインタラクションがあるすべての KDC と、DPE とインタラクションがある KDC を示します。
- *BPR_DATA/dpe/logs/dpe.log*ファイルは、MTA とインタラクションがある SNMPv3 に関連する主要な手順を示します。

（注） snmp のトレーシング、登録サーバ、登録サーバの詳細メッセージをオンにして、コマンドライン インターフェイス（CLI）を使用し、潜在的な PacketCable 問題のトラブルシューティングをサポートします。適切なトラブルシューティング コマンドについては、Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド を参照してください。

Ethereal、SnifferPro、またはその他のパケット キャプチャ ツール

パケット キャプチャ ツールは、eMTAs のトラブルシューティングを行うときに不可欠です。CableLabs によってパッケージ化された Ethereal バージョンには、多数の PacketCable に固のパケット デコーダが含まれています。これらには、Kerberos AS および AP パケットが含まれます。

- 特定の障害が DHCP に関連している疑いがある場合は、送信元または宛先へのパケット、CMTS ケーブル インターフェイス IP アドレス、DHCP サーバ IP アドレスのフィルタリングを行いながらパケットをキャプチャします。
- 特定の障害が DHCP 後に発生している手順 25 のいずれかに関連している疑いがある場合、eMTA IP アドレスのすべてのパケットをフィルタ リングします。これにより、図 1 で示されるように、手順 5 ～ 25 をプロビジョニングする際に、非常に簡単かつフォローしやすいトレースが可能です。

トラブルシューティング シナリオ

次の表に記載されているシナリオは、eMTAs が関係する可能性のある障害です。

表 *3:* トラブルシューティング シナリオ

次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
KDC が開始されません。	KDC 証明書が、秘密キーに対応していません。	証明書および秘密キーが一致することを確認します。
	KDC ライセンスが期限切れか、またはありません。	*BPR_HOME/kdc*ディレクトリに KDC ライセンスを復元します。

次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
MTA デバイスは、Prime ケーブル プロビジョニング Devices] ページには表示されません。	不適切なケーブル 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。
	スコープ選択タグは、プライム ケーブル プロビジョニング Admin UI で選択されている DHCP 条件と一致しません。	関連する MTA のプライム ケーブル プロビジョニングで、MTA スコープ選択タグが作成された PacketCable DHCP 条件のものと一致す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。Cisco プライム ケーブル プロビジョニング 6.1.1 クイック スタート ガイドを参照してください。
	ケーブル モデムの部分は、オプション 122 を受信しませんでした。	ケーブル モデムの部分のスコープのタグが、プライム ケーブル プロビジョニング用に設定された DOCSIS DHCP 基準に一致することを確認します。
MTA デバイスでは、DHCP オファーを受け入れず、DHCP フローを通じて継続的に再投入します。	設定されている無効な DHCP オプションがあります。	スコープ ポリシーに DNS サーバ オプションが含まれることを確認するか、*cnr_ep.properties*ファイルにプライマリおよびセカンダリ DNS サーバのエントリが含まれていることを確認するか、その両方を確認してください。
	DHCP オファーには、ケーブル モデム ポーションのオプション 122 サブオプション 1 で示されたものとは異なる DHCP サーバから来るものもあります。	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するために、*cnr_ep.properties*ファイルを確認します。

次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
Kdc.log ファイルと ethereal トレースの両方は、MTA デバイスが KDC に接続していないことを示しています。	誤った DNS サーバは、*cnr_ep.properties* ファイルまたは MTA スコープ ポリシー、またはその両方で指定されます。	*cnr_ep.properties* DNS サーバを確認または修正します。
	ゾーンは存在しないか、Kerberos レルムに対して誤って設定されています。	レルムと同じ名前のゾーンが作成され、'_kerberos._udp 0 0 88 *KDC FQDN*' 形式の 「SRV」 レコードが含まれています。
	欠落しているか、誤っている KDC「A」レコード エントリがあります。	「A」 レコードが Kerberos ゾーンの「SRV」 レコードに含まれている FQDN に対して存在することを保証します。
	DPE FQDN を解決することはできません。	*dpe.properties* の provFQDNs エントリに、DPE の正しい FQDN および IP があることを確認します。

次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
KDC は、Kerberos AS-要求中に障害が報告されます。	MTA 証明書は、KDC で使用されている MTA ルートと一致しません。	動作中のシステムで使用される*MTA_Root.cer*に対して比較することで、*MTA_Root.cer*が正しいことを確認します。 正しい場合は、MTA 自体に証明書の問題がある可能性があります。この状況は非常に珍しく、この場合は、MTA 製造元に問い合わせてください。
	Prov サーバへの KDC による FQDN ルックアップは失敗しました。デバイスは、プライム ケーブル プロビジョニングでプロビジョニングされない場合があります。	デバイスが表示されることを確認します。これは、クラスのサービスと DHCP 条件の両方に指定する必要があります。
	クロック スキュー エラー。詳細については、PacketCable のワークフローを参照してください。	すべてのプライム ケーブルのプロビジョニング ネットワーク要素が、NTP 軽油でクロック同期されていることを保証します。Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイドを参照してください。
	KDC と DPE 間に不一致があります。 （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、これが問題の原因にはならない場合があります。	

次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
		これら 3 つのエントリが *BPR_HOME/kdc/<Operating System>/keys*ディレクトリに存在することを確認します。 • mtafqdnma,dpe.abc.com@DEF.COM • mtaprovsrvr,dpe.abc.com@DEF.COM • krbtgt,DEF.COM@DEF.COM お使いのシステムの DPE FQDN とレルム名は、次の例とは異なります。これらのエントリの内容は、dpe.properties 'KDCServiceKey' エントリまたは KeyGen ユーティリティを使用して生成したキーのいずれかのエントリと一致する必要があります。
KDC は、AS-要求/応答で成功を報告しますが (図 1 で示されているステップ 9 および 10)、MTA デバイスが過去のステップ 9 を超えて移動することはありません。	MTA でロードまたは有効になったテレフォニー ルートち KDC でロードされたルートの間の証明書の不一致があります。	MTA と KDC の証明書を確認します。
	あまり確率は高くありませんが、破損したテレフォニー証明書チェーンがある可能性があります。 （注） その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、問題の原因ではありません。	適切な証明書が MTA でロードされるか、有効になっていることを確認します。どのデバイスも正しくプロビジョニングされない場合は、KDC で異なる証明書を試してください。

次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
AP 要求/応答での障害 (図 1 のステップ 14)。	クロック スキュー エラー。追加情報については、PacketCable のワークフローを参照してください。	すべてのプライム ケーブル プロビジョニング ネットワーク要素が、NTP 軽油でクロック同期されていることを保証します。Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイドを参照してください。
	Prov サーバの FQDN を解決することはできません。	プロビジョニング サーバ (DPE) に、適切な DNS エントリがあることを確認します。Dpe.properties provFQDNs エントリに正しい FQDN およびプロビジョニング サーバ (DPE) の IP アドレスがあることを確認します。
	MTA から DPE へのルートはありません。	ルーティングの問題点を修正します。
MTA デバイスでは、設定ファイルの TFTP 要求が決して発行されません。	DPE で実行中の TFTP サーバへのルートはありません。	ルーティングの問題点を修正します。
MTA デバイスは、TFTP 設定ファイルを決して受信しません。	設定ファイルは DPE でキャッシュされません。	ファイルがキャッシュされる時点で、次のプロビジョニングが試行されるまで待ちます。これが失敗すると、MTA をリセットします。
	Network registrar MTA スコープ ポリシーに競合する TFTP サーバ オプションが含まれています。	プライム ケーブル プロビジョニングは、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。

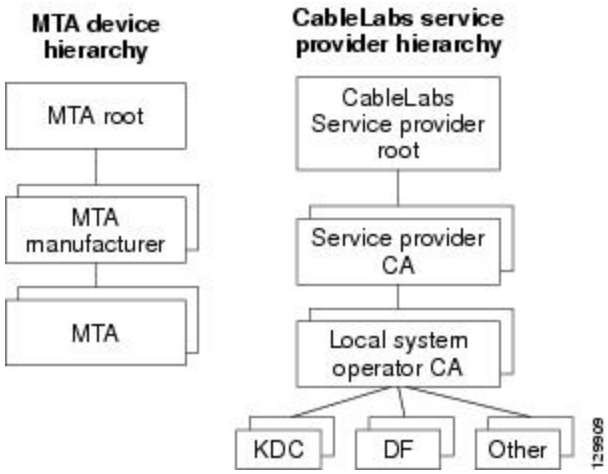
次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
MTA デバイスは、設定ファイルを受け取りますが、DPE は *dpe.log* ファイルでみられるように、SNMP Inform（図 1 のステップ 25）を受け取ることができません。	次のいずれかになります。 • 設定ファイルの内部の競合。 • テレフォニー証明書チェーンのレルムの送信元との競合。 • オプション 122 で指定されるレルム名の競合。	MTA 設定ファイルが一貫性のあることを確認します。
MTA デバイスは、RSIP が送信されなくても、成功をレポート (ステップ 25 図 1) します。	MTA は、MTA 設定ファイルで指定された 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 は、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の問題を解決します。
CMS サービスの KDC にもう一度問い合わせに進みますが、MTA デバイスの成功をレポート (ステップ 25 図 1) します。	MTA 設定ファイルが不適切なケーブル モデムを指しています。	設定ファイルを修正するか、Ciisco BTS 10200 を再構成して、構成ファイルにリストされた FQDN を使用します。
	MTA 設定ファイルで、pktcMtaDevCmsIPsecCtrl 値が不足しているか、それが 1 に設定されます。これは、セキュリティで保護された NCS コール シグナリングを実行するか、CMS FQDN のもの一致しない ASCII サフィックスを使用します。	設定ファイルを修正します。セキュリティで保護されたシグナリングを実行する場合は、KDC と BTS をサポートのために設定するために必要な手順を実行します。

次の問題が発生した場合...	次の潜在的な原因を示す...	これを修正するための是正措置は...
MTA デバイスの成功をレポート (図 1 のステップ 25) し、RSIP ですが、応答がないか、またはソフト スイッチから応答でエラーを取得します。	MTA がプロビジョニングを解除されるか、Cisco BTS 10200 で正しくないプロビジョニングをされています。	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 の適切な DNS ゾーンにエントリを配置します。ダイナミック DNS が、優先方式です。DDNS を有効にすることについては、Cisco Prime Network Registrar マニュアルを参照してください。

証明書信頼階層

次に示すように、プライム ケーブル プロビジョニング PacketCable、MTA デバイスの証明書階層および CableLabs サービス プロバイダーの証明書階層に関係している 2 つの証明書階層があります。

図 *1 : PacketCable* 証明書階層



プライム ケーブルのプロビジョニングで PacketCable を実装する前に、これらの技術資料を十分に理解する必要があります。

- *RFC 2459 Internet X.509* 公開キー インフラストラクチャ証明書と *CRL* プロファイル
- *DOCSIS* ベースライン プライバシ プラス インターフェイス仕様、*SP-BPI +-I11-040407*、*2004* 年 *4* 月 *7* 日

（注） ユーロ PacketCable は、PacketCable [PKT-SP-秒-I08-030415] からセキュリティ仕様を使用している一方で、ユーロ PacketCable 環境で使用されるデジタル証明書に関連するいくつかの変更が必要です。ユーロ PacketCable および PacketCable をできるだけ同じように保持するには、ユーロ PacketCable は、セキュリティ仕様 [PKTSP-秒-I08-030415] の新しいリビジョンを含め、すべての PacketCable セキュリティ テクノロジーを使用します。

PacketCable 証明書とは異なるユーロ PacketCable 証明書の要素は、以下の表に示されます。

ユーロ PacketCable の場合、ユーロ PacketCable 証明書のみが有効な証明書です。PacketCable 証明書を参照する PacketCable の [PKT-SP-SEC-I08-030415] で示されている要件は、ユーロ PacketCable 証明書の対応する要件に変更されています。

ユーロ PacketCable 対応 eMTA には、DOCSIS CVC CA の公開キーの代わりに、ケーブル モデムの不揮発性メモリに保存されているユーロ DOCSIS ルート CVC CA 公開キーをもっていなければなりません。ユーロ PacketCable に準拠するスタンドアロンの MTA は、不揮発性メモリに保存されている tComLabs CVC ルート証明書、および tComLabs CVC CA 証明書をもっていなければなりません。製造元の CVC は、証明書チェーンを確認することによって検証されます。

証明書の検証

通常 PacketCable 証明書の検証には、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と、証明書の次のチェーンが検証されます。

MTA ルート証明書 + MTA 製造元証明書 + MTA デバイス証明書

MTA の製造元証明書の署名が 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が MTA 製造元証明書を使用して検証されます。MTA ルート証明書は、自己署名でありプロビジョニング サーバの前に知られています。MTA ルート証明書に存在する公開キーは、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、最初の証明書チェーンでは、回線を介して送信される証明書チェーンに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、事前に確認側にすでに知られており、証明書のシリアル番号、有効期間、署名値の例外により、証明書への変更を含ま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 ルート証明書と比較して、回線を経由して送信された CableLabs サービス プロバイダ ルート証明書に存在するこれら以外を変更する場合、比較を行うデバイスは証明書の検証が失敗します。

証明書チェーン検証の正確なルールは、RFC 2459、ここと呼ばれるに証明書のパスの検証に完全に準拠する必要があります。一般に X.509 証明書は、証明書の発行元名が別の件名と一致するか判断する一連の文字ルールをサポートします。ルールはそのような 2 つの名前フィールドは、2 つの名前フィールドのバイナリ比較が一致しない場合でも一致できるように宣言します。実装がシンプルなバイナリ比較を使用して一致または不一致を宣言できるように、RFC 2459 では認証局が名前フィールドのエンコーディングを制限するように推奨します。

PacketCable セキュリティはこの推奨事項に従います。したがって、PacketCable 証明書の [DER-encoded tbsCertificate.issuer] フィールドには、発行者証明書の [DER-encoded

tbsCertificate.subject] フィールドに、完全一致する必要があります。実装は、[DER-encoded tbsCertificate.issuer and tbsCertificate.subject] フィールドのバイナリ比較を実行して、件名と発行元名を比較できます。

下のセクションは必要な証明書チェーンを指定し、図 1 : PacketCable 証明書階層 （25 ページ）で説明されている PacketCable 証明書信頼階層で、リーフ グループ（下）に表示される各証明書を検証するために使用する必要があります。

有効期間ネストがチェックされておらず、意図的に適用されません。したがって、証明書の有効期間は、発行した証明書の有効期間内ではない必要があります。

MTA デバイス証明書階層

デバイス証明書階層は、DOCSIS1.1/BPI+階層を正確にミラーリングします。これは、CableLabs 発行 PacketCable MTA ルート証明書にルートされ、一連の製造元の証明書発行として使用されます。製造元証明書は、個々 のデバイス証明書への署名に使用されます。

次の表に記載されている情報には、RFC 2459 に従って必須フィールドの PacketCable 固有の値が含まれています。これらの PacketCable 固有の値は、固有の表に記載がある有効期間を除き、表 4 : MTA ルート証明書 に従う必要があります。必須フィールドが特に PacketCable のリストにない場合は、RFC 2459 のガイドラインに従います。

MTA ルート証明書

MTA ルート証明書、MTA 製造元証明書、MTA デバイス証明書が含まれている証明書チェーンの一部として、この証明書を検証する必要があります。

次の表は、MTA ルート証明書に関連する値を示します。

表 *4 : MTA* ルート証明書

MTA ルート証明書		
件名	PacketCable c=US O = CableLabs OU = PacketCable CN = PacketCable ルート デバイス認証局	ヨーロッパ仕様 PacketCable C=BE O = tComLabs OU = ヨーロッパ仕様 PacketCable CN = ヨーロッパ仕様 PacketCable ルート デバイス認証局
使用目的	この証明書は、MTA 製造元証明書に署名するために使用され、KDC によって使用されます。この証明書は、MTA によって使用されていないため、MTA MIB に表示されません。	
署名者	Self-signed	

MTA ルート証明書	
有効期間	20 年間。有効期間はこの証明書が再発行されないように長くなることを意図しています。
係数長	2048
拡張機能	keyUsage [c、m](keyCertSign, cRLSign) subjectKeyIdentifier [n、m] basicConstraints[c,m](cA=true, pathLenConstraint=1)

MTA 製造元の証明書

MTA ルート証明書、MTA 製造元証明書、MTA デバイス証明書が含まれている証明書チェーンの一部として、この証明書を検証する必要があります。州/県、市町村、製造元私設はオプションの属性です。製造元は1個以上の製造元の証明書を有する可能性があり、製造元ごとに1 個以上の証明書が存在する可能性があります。同じ製造元のすべての証明書は、製造時またはフィールドの更新時に、各 MTA に提供可能可能性があります。MTA は、MTA 製造元の証明書の件名と MTA デバイス証明書の発行元名を一致させて、使用に適切な証明書を選択する必要があります。存在する場合、デバイス証明書の authorityKeyIdentifier は RFC 2459 の説明に従って、製造元の証明書の subjectKeyIdentifier と一致する必要があります。O および CN に存在する *[CompanyName]* フィールドは、2 つのインスタンスで異なる可能性があります。

次の表は、MTA 製造元の証明書に関連する値を示します。

表 *5: MTA* 製造元の証明書

MTA 製造元の証明書		
件名フォーム	PacketCable c=US O = CableLabs OU = PacketCable CN = PacketCable ルート デバイス認証局	ヨーロッパ仕様 PacketCable C=*Country of Manufacturer* O=*Company Name* [stateOrProvinceName = *State/Province*] [localityName=*City*] OU = ヨーロッパ仕様 PacketCable [organizationalUnitName= *Manufacturing Location*] CN=*Company Name* Euro-PacketCable CA

MTA 製造元の証明書	
使用目的	この証明書は MTA 製造者ごとに発行され、各 MTA に PacketCable セキュリティ仕様で指定されたように、セキュアコード ダウンロードの一部として提供可能です（製造時またはフィールド更新時）。この証明書は、MTA MIB の読み取り専用パラメータとして表示されます。MTA デバイス証明書を持つこの証明書は、KDC により認証中に、MTA デバイス ID を認証するために使用されます（MAC アドレス）。
署名者	MTA ルート証明書 CA
有効期間	20 年間
係数長	2048
拡張機能	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

MTA ルート証明書、MTA 製造元証明書、MTA デバイス証明書が含まれている証明書チェーンの一部として、この証明書を検証する必要があります。州/県、市町村、製造元私設はオプションの属性です。MAC アドレスはコロンで区切られ、16 進数の 6 個のペアとして表現する必要があります。例：“00:60:21:A5:0A:23”。アルファ 16 進文字（A ~ F）は、大文字で表現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。

次の表は、MTA デバイス証明書に関連する値を示します。

表 *6 : MTA* デバイス証明書

MTA デバイス証明書		
件フォーム	PacketCable C=*Country* O=*Company Name* [ST=*State/Province*] [L=*City*], OU=PacketCable [OU=*Product Name*] [OU=*Manufacturer's Facility*] CN=*MAC Address*	ヨーロッパ仕様 PacketCable C=*Country of Manufacturer* O=*Company Name* [ST=*State/Province*] [L=*City*] OU = ヨーロッパ仕様 PacketCable [OU=*Product Name*] [OU=*Manufacturing Location*] CN =*MAC* アドレス

MTA デバイス証明書	
使用目的	この証明書は MTA の製造元により発行され、工場出荷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、この証明書を更新できません。この証明書は MTA MIB 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、プロビジョニング時に MTA デバイス ID（MAC アドレス）の認証に使用されます。
署名者	MTA 製造元の証明書 CA
有効期間	20 年以上
係数の長さ	1024、1536 または 2048
拡張機能	keyUsage [c、o](digitalSignature, keyEncipherment) authorityKeyIdentifier[n,m](keyIdentifier=*subjectKeyIdentifier value from CA certificate*)

MTA メーカー コード検証証明書

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

CableLabs サービス プロバイダ証明書階層

サービス プロバイダ証明書階層は、CableLabs 発行 CableLabs サービス プロバイダのルート証明書でルートされます。その証明書は、一連のサービス プロバイダの発行証明書として使用されます。サービス プロバイダの証明書は、オプションのローカル システム証明書への署名に使用されます。ローカル システム証明書が存在する場合、補助機器証明書の署名に使用されます。そうでない場合、補助証明書はサービス プロバイダの CA により署名されます。

表 7 : CableLabs サービス プロバイダ ルート証明書に含まれる情報には、RFC 2459 に準拠した必須フィールドの特定の値が含まれています。これらの特定の値は、次のとおりにする必要があります。必須フィールドが特にリストにない場合は、RFC 2459 のガイドラインに正確に従う必要があります。

CableLabs サービス プロバイダ ルート証明書

Kerberos キー管理を実行する前に、MTA と KDC により Kerberos プロトコルへの PKINIT 拡張子を使用して相互認証を実行する必要があります。KDC 証明書チェーンを含む PKINIT 応答メッセージの受信後に、MTA は KDC を認証します。KDC を認証では、MTA は CableLabs サービス プロバイダ ルート CA によって署名された KDC のサービス プロバイダの証明書を含む、KDC 証明書チェーンを確認します。

次の表は、CableLabs プロバイダ ルート証明書に関連する値を示します。

表 *7 : CableLabs* サービス プロバイダ ルート証明書

CableLabs サービス プロバイダ ルート証明書		
件名フォーム	PacketCable c=US O = CableLabs CN=CableLabs Service Provider Root CA	ヨーロッパ仕様 PacketCable C=BE O = tComLabs CN=tComLabs Service Provider Root CA
使用目的	この証明書は、サービス プバイダ CA 証明書に署名するために使用されます。この証明書は、製造時または PacketCable セキュリティ仕様で指定されたセキュア コードのダウンロードの時に各 MTA にインストールされ、プロビジョニング サーバでは更新できません。MTA mib では、このルート証明書や対応する公開キーが表示されません。	
署名者	Self-signed	
有効期間	20 年間。有効期間はこの証明書が再発行されないように長くなることを意図しています。	
係数長	2048	
拡張機能	keyUsage [c、m](keyCertSign, cRLSign) subjectKeyIdentifier [n、m] basicConstraints[c,m](cA=true)	

Service Provider CA Certificate

これは、サービス プロバイダによって保持される証明書であり、CableLabs サービス プロバイダ ルート CA によって署名されています。これは、CableLabs サービス プロバイダ ルート証明書、テレフォニー サービス プロバイダ証明書、任意のローカル システム証明書、終了エンティティ 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。認証エンティティは、通常すでに CableLabs サービス プロバイダ ルート証明書を保有しており、証明書チェーンの残りの部分では送信されません。

サービス プロバイダ CA 証明書が証明書チェーンに常に明示的に含まれている事実により、サービス プロバイダはこの証明書チェーンを検証する各エンティティの再設定を行う必要なく、証明書を柔軟に変更できます。サービス プロバイダ CA 証明書が変更されるたびに、その署名を CableLabs サービス プロバイダ ルート証明書で検証する必要があります。ただし、同じサービス プロバイダの新しい証明書は、SubjectName の OrganizationName 属性と同じ値を保持する必要があります。O と CN に存在する *[Company]* フィールドは、2 つのインスタンスで異なる可能性があります。

次の表は、CableLabs サービス プロバイダ CA 証明書に関連する値を示します。

表 *8 : CableLabs* サービス プロバイダ *CA* 証明書

CableLabs サービス プロバイダ ルート証明書		
件名フォーム	PacketCable C=*Country* O=*Company* CN=*Company* CableLabs Service Provider CA	ヨーロッパ仕様 PacketCable C=*Country* O=*Company* CN=*Company* tComLabs Service Provider CA
使用目的	この証明書は、サービス プバイダ CA 証明書に署名するために使用されます。この証明書は、製造時または PacketCable セキュリティ仕様で指定されたセキュア コードのダウンロードの時に各 MTA にインストールされ、プロビジョニング サーバでは更新できません。MTA mib では、このルート証明書や対応する公開キーが表示されません。	
署名者	Self-signed	
有効期間	20 年間。有効期間はこの証明書が再発行されないように長くなることを意図しています。	
係数長	2048	
拡張機能	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 CA は、ローカル システム CA（対応するローカル システム証明書と）と呼ばれる地域の認証局に、証明書の発行を委任する可能性があります。ネットワーク サーバは、同じサービスプロバイダの地域の認証局の間で自由に移動が許可されます。したがって、MTA MIB は、ローカル システム証明書（特定の地域内で MTA から KDC に制限する可能性がある）に関する情報を含みません。

次の表は、ローカル システム CA 証明書に関連する値を示します。

表 *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		
件名フォーム	PacketCable C=*Country* O=*Company* OU=*Local System Name* CN=*Company* CableLabs Local System CA	ヨーロッパ仕様 PacketCable C=*Country* O=*Company* OU=*Local System Name* CN=*Company* tComLabs Local System CA

ローカル システム CA 証明書	
使用目的	サービス プロバイダ CA は、ローカル システム CA（対応するローカル システム証明書と）と呼ばれる地域の認証局に、証明書の発行を委任する可能性があります。ネットワーク サーバは、同じサービス プロバイダの地域の認証局の間で自由に移動が許可されます。したがって、MTA MIB は、ローカル システム証明書（特定の地域内で MTA から KDC に制限する可能性がある）に関する情報を含みません。
署名者	サービス プロバイダ CA 証明書
有効期間	20 年間
係数の長さ	1024、1536、2048
拡張機能	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier[n,m], authorityKeyIdentifier[n,m](keyIdentifier=*subjectKeyIdentifier value from CA certificate*), basicConstraints[c,m](cA=true, pathLenConstraint=0)

操作補助証明書

これらすべては、ローカル システム CA またはサービス プロバイダ CA によって署名されます。その他の補助証明書は、後でこの標準に追加される可能性があります。

KDC 証明書

CableLabs Service Provider Root Certificate、Service Provider CA Certificate、Ancillary Device Certificates を含む証明書チェーンの一部として、この証明書を検証する必要があります。PKINIT 仕様では KDC 証明書が必要であり、の値は、KDC の Kerberos プリンシパル名の値である、subjectAltName v.3 証明書の拡張を含める必要があります。

次の表は、KDC 証明書に関連する値を示します。

表 *10 : KDC* 証明書

キー発行局		
件名	PacketCable C=*Country* O=*Company* [OU=*Local System Name*] OU= ey Distribution Center（キー発行局） CN =*DNS* 名	ヨーロッパ仕様 PacketCable C=*Country* O=*Company* [OU=*Local System Name*] OU= tComLabs Key Distribution Center（キー発行局） CN =*DNS* 名

キー発行局	
使用目的	PKINIT 交換中に MTA へ KDC サーバの ID を確認します。この証明書は PKINIT 応答内部の MTA に送信されるため、MTA MIB には含まれておらず、サーバのプロビジョニングにより更新またはクエリできません。
署名者	サービス プロバイダ CA 証明書またはローカル システム証明書
有効期間	20 年間
係数の長さ	1024、1536 または 2048
拡張機能	keyUsage[c,o](digitalSignature)authorityKeyIdentifier[n,m](keyIdentifier=*subjectKeyIdentifier value from CA certificate*)subjectAltName[n,m]

配信機能（DF）

CableLabs Service Provider Root Certificate、Service Provider CA Certificate、Ancillary Device Certificates を含む証明書チェーンの一部として、この証明書を検証する必要があります。この証明書は、DF 間のフェーズ 1 内部ドメイン交換の署名に使用されます（これは、電子監視で使用されます)。ローカル システム名はオプションですが、ローカル システムの CA 証明書に署名するときに必須です。標準的な表記で IP アドレスを指定する必要があります。
例： 245.120.75.22。

次の表は、DF 証明書に関連する値を示します。

表 *11 : DF* 証明書

DF 証明書		
件フォーム	PacketCable C=*Country* O=*Company* [OU=*Local System Name*] OU=PacketCable Electronic Surveillance CN =*IP address*	ヨーロッパ仕様 PacketCable C=*Country* O=*Company* [OU=*Local System Name*] OU=Euro-PacketCable Electronic Surveillance CNe =*IP address*
使用目的	IKE キー管理を認証するため、DF ペア間の IPsec セキュリティ アソシエーションを確立するのに使用します。合法的に通信傍受されたサブジェクトを通話に転送したり、通話情報を含むイベント メッセージを新しい通信傍受サーバ（DF）に転送する必要がある場合、これらのセキュリティ アソシエーションが使用されます。	

DF 証明書	
署名者	サービス プロバイダ CA 証明書またはローカル システム CA 証明書
有効期間	20 年間
係数長	2048
拡張機能	keyUsage[c,o](digitalSignature)authorityKeyIdentifier[n,m](keyIdentifier=*subjectKeyIdentifier value from CA certificate*)subjectAltName[n,m](dNSName=*DNSName*)

PacketCable Server Certificates

これらの証明書はCableLabsサービス プロバイダ ルート証明書、サービス プロバイダ証明書、ローカル システム オペレータ証明書（使用する場合）、補助デバイス証明書を含む証明書チェーンの一部として、これらの証明書を検証する必要があります。これらの証明書を使用して、PacketCableシステムのさまざまなサーバを識別します。たとえば、フェーズ1 IKEの交換に署名するか、PKINIT 交換の認証にこれらを使用できます。ローカル システム名はオプションですが、ローカル システムの CA 証明書に署名するときに必須です。標準的なドット付き10進表記で2IPアドレスを指定する必要があります。例；245.120.75.22。DNS名の値は、完全修飾ドメイン名（FQDN）として指定する必要があります。例：device.packetcable.com。

次の表は、PacketCable サーバ証明書に関連する値を示します。

表 *12 : PacketCable* サーバ証明書

PacketCable サーバ証明書		
件名フォーム		ヨーロッパ仕様 PacketCable C=*Country* O=*Company* OU = ヨーロッパ仕様 PacketCable [OU=*Local System Name*] OU=*Sub-system Name* CN=*Server Identifier*[:*Element ID*] commonName 追加仕様については、[PKT-SP-SEC-IO8-030415] を参照してください。

PacketCable サーバ証明書		
	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 またはコロン（:）にする必要があり、オプションでコロンに続き、前後にスペースを入れない要素 ID です。 *Element ID* は請求イベント メッセージに表示する ID です。イベント メッセージを生成可能なすべてのサーバの証明書に含める必要があります。これには、CMS、CMTS、および MGC が含まれます。[8] は 5 オクテットの右揃え、スペース埋め込み、ascii 文字エンコード、数字の文字列として要素 ID を定義します。証明書で使用するための要素 ID を変換するとき、スペースを ASCII ゼロ（0x48）に変換する必要があります。 たとえば、要素 ID 311 および IP アドレス 123.210.234.12 を持つ CMTS は、共通名「123.210.234.12: 00311」があります。 *Sub-System Name* の値は、次のいずれかである必要があります。 • 境界プロキシ：bp • ケーブル モデム終端シス	

PacketCable サーバ証明書		
	テム：CMTS • コール管理サーバ：CMS • メディア ゲートウェイ：mg • メディア ゲートウェイ コントローラ：MGC • Media Player：mp • メディア プレーヤー コントローラ：mpc • プロビジョニング サーバ：ps • 記録保持サーバ：RKS • ゲートウェイのシグナリング：sg	
使用目的	これらの証明書を使用して、PacketCable システムのさまざまなサーバを識別します。たとえば、フェーズ 1 IKE の交換に署名するか、PKINIT 交換のデバイス認証にこれらを使用できます。	
署名者	テレフォニー サービス プロバイダ証明書またはローカル システム証明書	
有効期間	MSO ポリシーによる設定	
係数長	2048	
拡張機能	keyUsage[c,o](digitalSignaturekeyEncipherment) authorityKeyIdentifier [n、m] (keyIdentifier*subjectKeyIdentifier* が *CA* 証明書から値を =) subjectAltName [n、m] (dNSName =*DNSName* | iPAddress =*IP* 「*addressname*」) KeyUsage タグはオプションです。使用する際に、重大としてマークする必要があります。後述のようにしない限り、subjectAltName 拡張には、件名の [CN] フィールドで指定された対応する名前値を含む必要があります。	

CMS 証明書の CN 属性値は、要素の ID である必要があります。SubjectAltName 拡張には、IP アドレスまたは CMS の FDQN のどちらかを含む必要があります。CMTS 証明書の CN 属性値

は、要素 ID である必要があります。SubjectAltName 拡張には、IP アドレスまたは CMTS の FDQN のどちらかを含む必要があります。

MGC 証明書の CN 属性値は、要素 ID である必要があります。SubjectAltName 拡張には、IP アドレスまたは MGC の FDQN のどちらかを含む必要があります。

証明書の失効

この時点で PacketCable の範囲外です。

ケーブル検証証明書階層

CableLabs Code Verification Certificate (CVC) PKI は、本来一般的であり、CVC が必要なすべてのすべての CableLabs プロジェクトに適用されます。これは、基本的なインフラストラクチャがあらゆる CableLabs プロジェクトの再利用できることを意味します。各プロジェクトに必要なエンドエンティティ証明書に違いがある可能性がありますが、エンドエンティティ証明書が重複する場合、エンド エンティティ証明書を重複のサポートのために使用可能です。

CableLabs CVC 階層は、eMTAs には適用されません。

共通 CVC 要件

次の要件は、すべてのコード検証証明書に適用します。

- 証明書は、DER エンコードが行われる必要があります。
- 証明書は、バージョン 3 である必要があります。
- 証明書は、次の表で指定される拡張機能を含め、追加の拡張機能は含まないようにする必要があります。
- [Public exponent] は F4 である必要があります（65537 10 進数）。

CableLabs Code Verification Root CA Certificate

CableLabs コード検証ルート CA 証明書、CableLabs コード検証 CA、コード検証証明書を含む証明書チェーンの一部として、この証明書を検証する必要があります。証明書を検証する方法についての詳細は、『証明書の検証』を参照してください。

次の表は、CableLabs コード検証ルート CA 証明書に関連する値を示します。

表 *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		
件名フォーム	PacketCable c=US O = CableLabs CN=CableLabs CVC Root CA	ヨーロッパ仕様 PacketCable C = BE O = tComLabs CN = tComLabs CVC Root CA
使用目的	この証明書は、コード検証CA証明書の署名に使用されます。この証明書は、製造時にS MTA の不揮発性メモリに含める必要があります。	
署名者	Self-signed	
有効期間	20 年以上	
係数長	2048	
拡張機能	KeyUsage [c,m] (keyCertSign, cRL Sign) subjectkeyidentifier [n,m] basicConstraints [c,m](cA=true)	

CableLabs Code Verification CA Certificate

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、CableLabs コード検証証明書を含む証明書チェーンの一部として検証する必要があります。証明書を検証する方法についての詳細は、『証明書の検証』を参照してください。1 つ以上の CableLabs コード検証 CA がある可能性があります。S-MTA は一度に 1 個の CableLabs CVC CA をサポートする必要があります。

次の表は、CableLabs コード検証 CA 証明書に関連する値を示します。

表 *14 : CableLabs* コード検証 *CA* 証明書

CableLabs コード検証 CA 証明書		
件名フォーム	PacketCable c=US O = CableLabs CN=CableLabs CVC CA	ヨーロッパ仕様 PacketCable C = BE O = tComLabs CN = tComLabs CVC CA
使用目的	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。この証明書は、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 の不揮発性メモリに含める必要があります。	
署名者	CableLabs コード検証ルート CA	

CableLabs コード検証 CA 証明書	
有効期間	CableLabs ポリシーにより設定
係数の長さ	2048
拡張機能	KeyUsage [c,m] (keyCertSign, cRL Sign) subjectKeyIdentifier [n,m] authorityKeyIdentifier [n,m] basicConstraints [c,m](cA=true, pathLenConstraint=0)

Manufacturer Code Verification Certificate

CableLabs コード検証 CA は、承認済みの各製造元にこの証明書を発行します。安全なソフトウェア ダウンロードのケーブル オペレータにより、ポリシー設定で使用されます。

次の表は、製造元コード検証証明書に関連する値を示します。

表 *15 :* 製造業者コード検証証明書

製造元コード検証証明書		
件名フォーム	PacketCable C=*Country* O=*Company Name* [ST=*State/Province*] [L=*City*] CN=*Company Name* Mfg CVC	ヨーロッパ仕様 PacketCable C=*Country* O=*Company Name* [ST=*state/province*] [L=*City*] CN=*Company Name* Mfg CVC
使用目的	CableLabs コード検証 CA は、承認済みの各製造元にこの証明書を発行します。安全なソフトウェア ダウンロードのケーブル オペレータにより、ポリシー設定で使用されます。	
署名者	CableLabs コード検証 CA	tCableLabs コード検証 CA 証明書
有効期間	CableLabs ポリシーにより設定	
係数の長さ	1024、1536、2048	
拡張機能	extendedKeyUsage [c,m] (id-kp-codeSigning) authorityKeyIdentifier [n,m]	

組織内の会社名は、共通の会社名と異なる可能性があります。

サービス プロバイダ コード検証証明書

サービス プロバイダ 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、サービス プロバイダ コード検証証明書を含む証明書チェーンの一部

として検証する必要があります。証明書を検証する方法についての詳細は、『証明書の検証』を参照してください。

次の表では、サービス プロバイダ コード検証証明書に関連する値を示します。

表 *16*：サービス プロバイダ コード検証証明書

サービス プロバイダ コード検証証明書		
件名フォーム	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
使用目的	CableLabs コード検証CA は、承認済みの各サービス プロバイダにこの証明書を発行します。安全なソフトウェア ダウンロードのケーブル オペレータにより、ポリシー設定で使用されます。	
署名者	CableLabs コード検証 CA	tCableLabs コード検証 CA 証明書
有効期間	CableLabs ポリシーにより設定	
係数の長さ	1024、1536、2048	
拡張機能	extendedKeyUsage [c,m] (id-kp-codeSigning) authorityKeyIdentifier [n,m]	

組織内の会社名は、共通の会社名と異なる可能性があります。

Certificate Revocation Lists for CVCs

S-MTA は、CVC の証明書失効リスト（Crl）をサポートする必要はありません。