注意： この日本語版文書は参考資料としてご利用ください。最新情報は必ずオリジナルの英語版をご参照願います。

CEC1736 開発ボード ユーザガイド

#EV19K07A

CEC1736開発ボード ユーザガイド

Microchip 社製品のコード保護機能について以下の点にご注意ください。

- Microchip 社製品は、該当する Microchip 社データシートに記載の仕様を満たしています。
- Microchip 社では、通常の条件ならびに動作仕様書の仕様に従って使った場合、Microchip 社製品のセキュリティ レベルは、現在市場に流通している同種製品の中でも最も高度であると考えています。
- Microchip 社はその知的財産権を重視し、積極的に保護しています。Microchip 社製品のコード保護機能の侵害は固く禁じられており、デジタル ミレニアム著作権法に違反します。
- Microchip 社を含む全ての半導体メーカーで、自社のコードのセキュリティを完全に保証できる企業はありません。コード保護機能とは、Microchip 社が製品を「解読不能」として保証するものではありません。コード保護機能は常に進化しています。Microchip 社では、常に製品のコード保護機能の改善に取り組んでいます。

商標

ISBN: 978-1-6683-1702-0

Microchip 社の品質管理システムについては www.microchip.com/quality をご覧ください。

CEC1736 開発ボード ユーザガイド

目次

序章

お客様へのご注意

どのような文書でも内容は時間が経つにつれ古くなります。本書も例外ではありません。Microchip 社のツールとマニュアルは、お客様のニーズを満たすために常に改良を重ねており、実際のダイアログやツールの内容が本書の説明とは異なる場合があります。最新文書は Microchip 社のウェブサイト (www.microchip.com) をご覧ください。

文書は「DS」番号によって識別します。この識別番号は各ページのフッタのページ番号の前に表記しています。DS 番号「DSXXXXXA」の「XXXXX」は文書番号、「A」はリビジョンレベルを表します。

開発ツールの最新情報は MPLAB® IDE のオンラインヘルプでご覧になれます。[Help] メニューから [Topics] を選択すると、オンラインヘルプ ファイルのリストが表示されます。

はじめに

本書では、Microchip 社の CEC1736 開発ボードの使い方とデモの準備と実行について説明します。

本章には、CEC1736 開発ボードを使い始める前に知っておくと便利な一般情報を記載しています。主な内容は以下の通りです。

- 本書の構成
- 本書の表記規則
- Microchip 社ウェブサイト
- 開発システムのお客様向け変更通知サービス
- カスタマサポート
- 改訂履歴

本書の構成

本書は、Microchip 社の CEC1736 開発ボードを使って CEC1736 のデモを実行しようとする人向けに書かれています。以下に本書の構成を示します。

- **第 1 章「はじめに」** - 本ガイドの目的と範囲を説明します。
- **第 2 章「特長」** - ボードの特長とレイアウト情報を示します。
- **第 3 章「推奨ツールおよびアクセサリ」** - デモに使う推奨ツールについて説明します。
- **第 4 章「CEC1736 開発ボードへの給電」** - デモを実行する手順を図入りで説明します。
- **第 5 章「ジャンパ オプション」** - ボードのジャンパ設定情報を示します。
- **第 6 章「OOB(アウトオブ ボックス) デモコードの実行」** - 本開発ボードに付属するアウトオブ ボックス デモについて説明します。
- **第 7 章「開発の準備」** - ユーザ カスタマイズされた開発を行うための手順を説明します。

本書の表記規則

本書には以下の表記規則を適用します。

本書の表記規則

表記	適用	例
Arial、MS ゴシックフォント		
二重かぎカッコ : 『』 太字	参考資料	『MPLAB® IDE ユーザガイド』
	テキストの強調	... は**唯一の**コンパイラです ...
角カッコ : [ ]	ウィンドウ名	[Output] ウィンドウ
	ダイアログ名	[Settings] ダイアログ
	メニューの選択肢	[Enable Programmer] を選択
かぎカッコ : 「 」	ウィンドウまたは ダイアログのフィールド名	「Save project before build」
右山カッコ (>) で区切り、 角カッコ ([ ]) で囲んだ 下線付きテキスト	メニュー項目の選択	[File] > [Save]
角カッコ ([ ]) で囲んだ太字の テキスト	ダイアログのボタン	**[OK]** をクリックする
	タブ	**[Power]** タブをクリックする
N'Rnnnn	Verilog 形式の数値 (N は総桁数、R は基数、 n は各桁の値)	4'b0010, 2'hF1
山カッコ (< >) で囲んだ テキスト	キーボードのキー	<Enter>、<F1> を押す
Courier New フォント		
標準の Courier New	サンプル ソースコード	`#define START`
	ファイル名	`autoexec.bat`
	ファイルパス	`c:\mcc18\h`
	キーワード	`_asm, _endasm, static`
	コマンドライン オプション	`-Opa+, -Opa-`
	ビット値	`0, 1`
	定数	`0xFF, 'A'`
斜体 Courier New	変数の引数	*`file.o`* (*`file`* は有効な任意のファイル名)
角カッコ : [ ]	オプションの引数	`mcc18 [options]` *`file`* `[options]`
中カッコとパイプ 文字 : {	}	どちらかの引数を選択する場合 (OR 選択)	`errorlevel {0|1}`
省略記号 : ...	繰り返されるテキスト	`var_name [, var_name...]`
	ユーザが定義するコード	`void main (void) { ... }`

Microchip 社ウェブサイト

Microchip 社はウェブサイト (www.microchip.com) でオンライン サポートを提供しています。当ウェブサイトでは、お客様に役立つ情報やファイルを簡単に見つけ出せます。インターネット ブラウザから以下の内容がご覧になれます。

- **製品サポート** - データシートとエラッタ、アプリケーション ノートとサンプル プログラム、設計リソース、ユーザガイドとハードウェア サポート文書、最新のソフトウェアと過去のソフトウェア
- **一般的技術サポート** – よく寄せられる質問 (FAQ)、技術サポートのご依頼、オンライン ディスカッション グループ、Microchip 社のコンサルタント プログラム メンバーの一覧
- **Microchip 社の事業** – プロダクト セレクタガイドとご注文案内、プレスリリース、セミナーとイベントの一覧、営業所の一覧

開発システムのお客様向け変更通知サービス

Microchip 社のお客様向け変更通知サービスは、お客様に Microchip 社製品の最新情報をお届けするサービスです。ご興味のある製品ファミリまたは開発ツールに関する変更、更新、リビジョン、エラッタ情報をいち早くメールにてお知らせします。

Microchip 社のウェブサイト (www.microchip.com) にアクセスし、[Customer Change Notification] からご登録ください。

開発システム製品のカテゴリは以下の通りです。

- **コンパイラ** - Microchip 社の C コンパイラ、アセンブラ、リンカ、その他の言語ツールの最新情報を提供します。これには MPLAB C コンパイラ全製品、MPLAB アセンブラ全製品 (MPASM アセンブラを含む)、MPLAB リンカ全製品 (MPLINK オブジェクト リンカを含む)、MPLAB ライブラリアン全製品 (MPLIB オブジェクト ライブラリアンを含む) が含まれます。
- **エミュレータ** - Microchip 社のインサーキット エミュレータの最新情報です。これには MPLAB REAL ICE と MPLAB ICE 2000 インサーキット エミュレータが含まれます。
- **インサーキット デバッガ** - Microchip 社のインサーキット デバッガに関する最新情報を提供します。これには MPLAB ICD 3 インサーキット デバッガと PICkit 3 Debug Express が含まれます。
- **MPLAB IDE** - Microchip 社の MPLAB IDE(開発システムツール向け Windows 統合開発環境) の最新情報です。これには MPLAB IDE、MPLAB IDE プロジェクト マネージャ、MPLAB エディタ、MPLAB SIM シミュレータと一般的な編集 / デバッグ機能が含まれます。
- **プログラマ** - Microchip社のプログラマの最新情報を提供します。これにはMPLAB REAL ICE インサーキット エミュレータ、MPLAB ICD 3 インサーキット デバッガ、MPLAB PM3 デバイス プログラマ等の量産プログラマが含まれます。また、PICSTART Plus や PIC-kit 2/3 等、量産向けではない開発用プログラマも含まれます。

カスタマサポート

Microchip 社製品をお使いのお客様は、以下のチャンネルからサポートをご利用頂けます。

- 正規代理店
- 技術サポート

サポートは正規代理店にお問い合わせください。

技術サポートは以下のウェブページからもご利用になれます。
http://www.microchip.com/support

改訂履歴

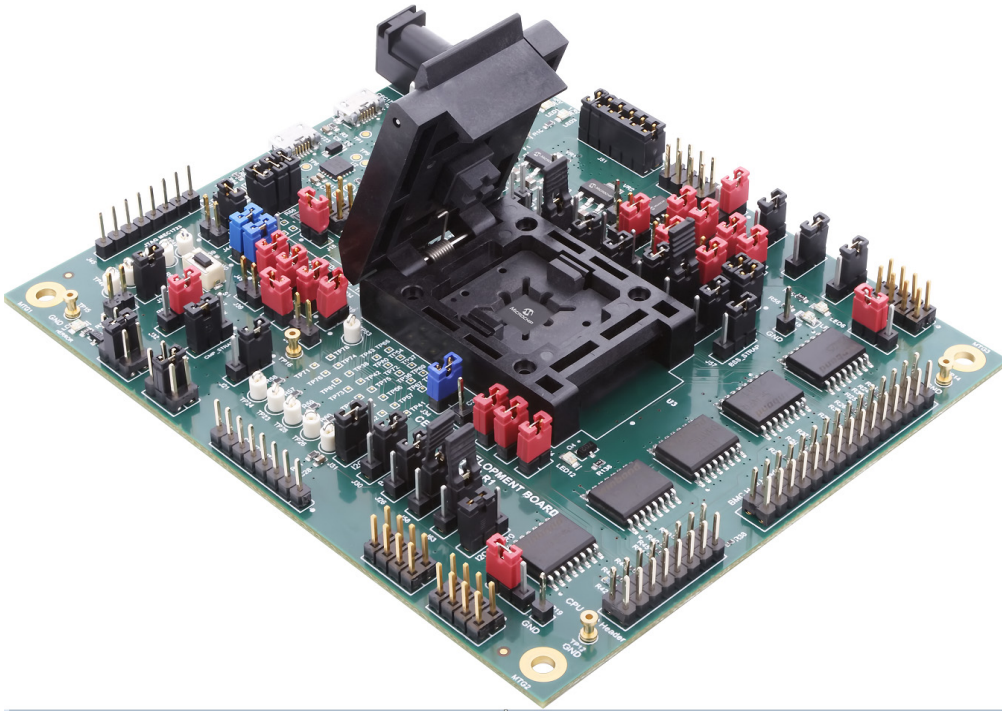
リビジョン	セクション / 図 / 項目	改訂内容
DS50003324A (05-06-22)	本書は初版です。	

第 1 章 はじめに

CEC1736 開発ボードは、データセンター、通信、ネットワーク、産業用、組み込みコンピューティング市場のリアルタイム プラットフォーム ルートオブ トラスト アプリケーション向けのデモ、開発、テスト用プラットフォームです。本ボードは、リアルタイム プラットフォーム ルートオブ トラスト アプリケーションのプロトタイプを迅速に製作、開発できる各種ハードウェア (電源、ユーザ インターフェイス、シリアル通信、拡張ヘッダ等) を備えています。

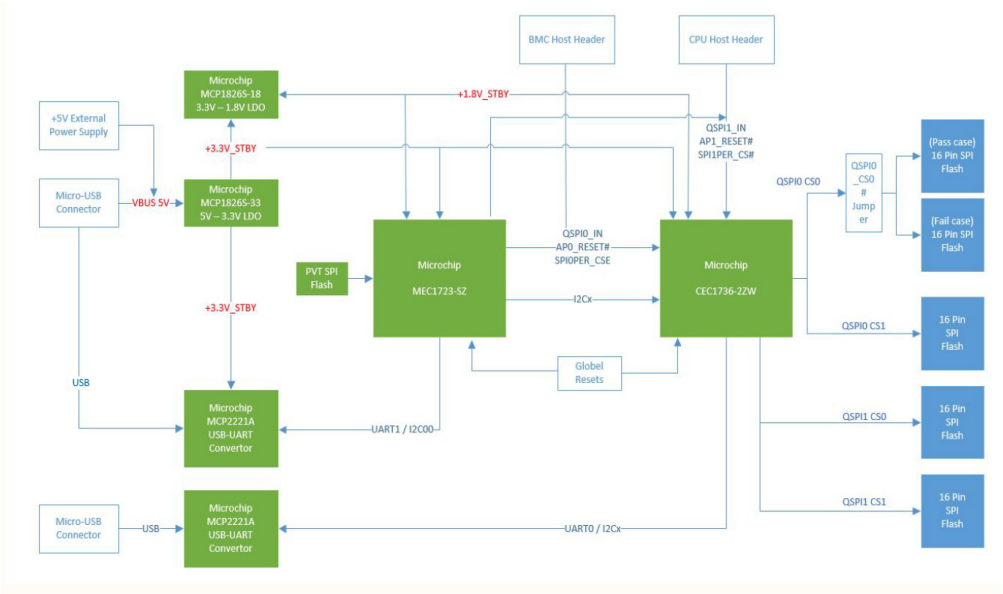
本開発ボードは以下のように設計されているため、すぐに使い始める事ができます。

- CEC1736 OTP - デモサンプルをサポートする事前定義された OTP 機能を書き込み済みです。
- CEC1736 内部 SPI フラッシュ - 最新の Soteria-G3 ファームウェア リリースを書き込み済みです。
- MEC1723(アプリケーション プロセスとしてエミュレート) - 追加設定なしで動作するサンプル ファームウェアの MEC1723 が含まれており、デモ用にアップグレード可能です。
- CEC1736 ソケット - 量産品の CEC1736 を使って特定の設計のための独自の OTP 機能を開発できます。



第 2 章 特長

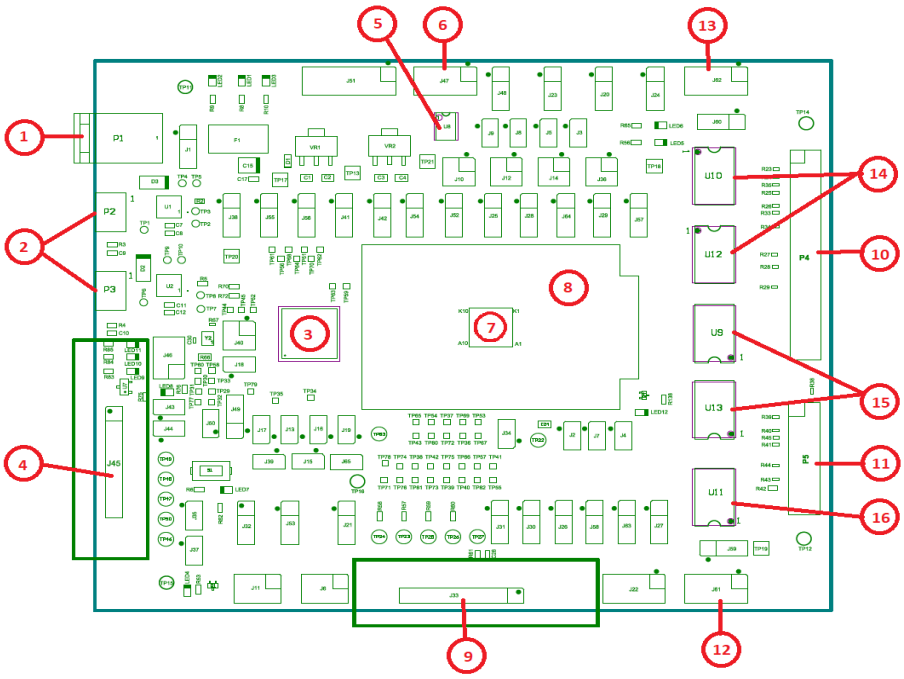
2.1 CEC1736 開発ボードのブロック図



2.2 ハードウェアの特長 :

- CEC1736 84 ピン用ソケット
- 4 x 16 ピン 256 Mbit SPI フラッシュ (通常動作用)
- 1 x 16 ピン 256 Mbit SPI フラッシュ (失敗ケースデモ用)
- 1 x CEC1736 用 USB-UART/I2C ポート
- 1 x MEC1723 用 USB-UART ポート
- BMC ホストヘッダ
- CPU ホストヘッダ
- 1 x デバッグおよびプログラミング用の CEC1736 用 1x8 PICKIT4 ヘッダ
- 1 x デバッグおよびプログラミング用の MEC1723 用 1x8 PICKIT4 ヘッダ
- オプションのカスタマイズ開発用 GPIO/I2C ヘッダ
- ボードには Micro-USB ケーブルまたは +5 V 電源アダプタ (どちらも開発ボードには同梱されていません) を使って給電可能

2.3 CEC1736 開発ボードのレイアウト



1. 電力アダプタプラグ (P1) — 外部 +5 V 電源アダプタによるもう 1 つの給電方法を提供します。
2. USB micro-B コネクタ — ボードへの給電、Microchip 社 MCP2221A USB-to-UART/I2C シリアル コンバータを使った CEC1736 (P2) と MEC1723 (P3) とのシリアル入出力 (I2C) インターフェイスを提供します。
3. Microchip 社の MEC1723N-B0-I/SZ (U6) - アプリケーション プロセッサとしてエミュレート
4. Microchip 社の MEC1723 用 PICKIT4 1x8 ヘッダ (J45)
5. Microchip 社の MEC1723 のプライベート フラッシュブート用 SST26VF040A SPI フラッシュ (U8)(オプション)
6. U8 への Dediprog SF100/SF600 SPI フラッシュ プログラミング ヘッダ (J47)

Note: J47 のピン 7 とピン 8 は接続されていますが、Dediprog の動作に影響を与える可能性があります。障害が発生した場合、SFxxx からヘッダへのピン 7 とピン 8 の接続を切断してください。

7. Microchip 社の CEC1736-S0-I/2ZW (U3 ソケットに取り付け)
8. 84 ピン 2ZW パッケージ ソケット (U3)
9. Microchip 社の CEC1736 用 PICKIT4 1x8 ヘッダ (J33)
10. BMC ホスト接続ヘッダ (P4)
11. CPU ホスト接続ヘッダ (P5)
12. U9、U11、または U13 への Dediprog SF100/SF600 SPI フラッシュ プログラミング ヘッダ (J61)
13. U10 または U12 への Dediprog SF100/SF600 SPI フラッシュ プログラミング ヘッダ (J62)
14. CEC1736 の QSPI1 チャンネル上の SPI フラッシュ (U10、U12)
15. CEC1736 の QSPI0 チャンネル上の SPI フラッシュ (U9、U13)
16. CEC1736 の QSPI0 CS0# チャンネル上の SPI フラッシュ (U11)(失敗ケースデモ専用)

第 3 章 推奨ツールおよびアクセサリ

CEC1736 開発ボードを使った開発では以下に示すツールを推奨します。

1. Microchip 社 MPLAB®X (v6.00 以上)
2. XC32 Pro コンパイラ (v2.50 以上)
3. 直接プラグイン用 PICKit4 インサーキット デバッガ
4. ICD4 インサーキット デバッガ + デバッガ アダプタボード (mD# AC102015)
5. UART デバッグログ用 Tera Term v4.106 以上 (またはお好みの同等のツール)
6. (オプション) 外部 SPI フラッシュ プログラミング用の Dediprog SF100 または SF600(またはお好みの同等のツール)

EV19K17A (CEC1736 開発ボードの技術文書) を守秘義務契約 (NDA) の下、Microchip 社正規代理店経由でリクエストして頂けます。

- Altium 設計ファイル
- ガーバーファイル
- 回路図
- Bill of Material: 部品表

その他ご不明な点がありましたら、Microchip 社正規代理店にお問い合わせください。

第 4 章 CEC1736 開発ボードへの給電

CEC1736 開発ボードへは USB- シリアル コンバータの USB micro-B ポート (P2 および / または P3) から直接給電できます。USB 電源からの 5 V 入力は、MCP1826S 電圧レギュレータにより 3.3 V に調整されます。

または、外部電源から電源プラグ (P1) を通して CEC1736 開発ボードへ給電する事もできます。USB micro-B ポートを使う場合と同じく、5 V が 3.3 V に調整されます。このオプションは J1 の 1 ～ 2 で選択します。既定値は 2 ～ 3 の USB 経由の給電です。

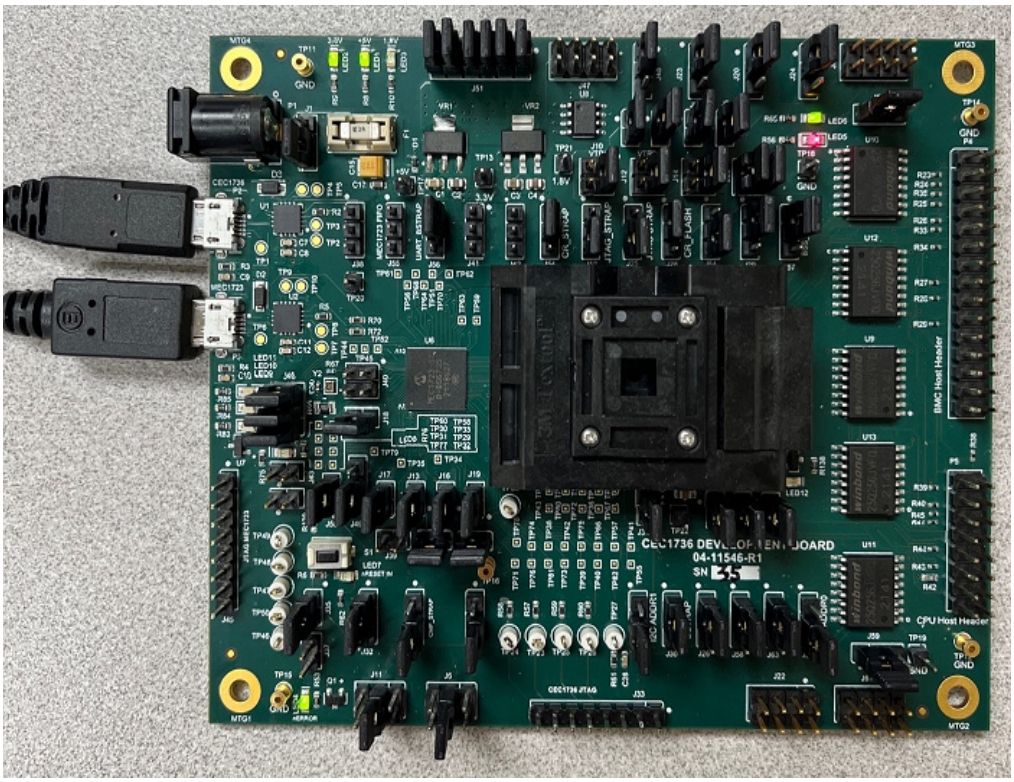
USB micro-B ポート使用時は、シャント ダイオード (D1) で総システム消費電力を計測できます。外部電源使用時は、ジャンパ (J1) で総システム消費電力を計測できます。

ボードに電源が投入された後、LED1 (+5 V)、LED2 (+3.3 V)、LED3 (+1.8 V) が ON になる必要があります。

MEC1723 のファームウェア アプリケーションに応じて LED9、LED10、LED11 が点滅する事があります。これは MEC1723 のファームウェアがロードされて実行中である事を示します。

LED4、LED5、LED6、LED12 が点滅する場合は CEC1736 の Soteria ファームウェアがロードされて実行中である事を示します。

以下に示すように電源を投入します。



第 5 章 ジャンパ オプション

下表に、CEC1736 開発ボードのジャンパについてまとめます。

ジャンパ オプション

ジャンパ	説明	詳細
J1	ボードの電源選択	1 ～ 2: 外部 5 V アダプタ (P1) により給電 **2 ～ 3(既定値)**: Micro-USB ポート (P2、P3) により給電
J2	CEC1736 への VTR 電源	**IN(既定値):** VTR 電源を接続 OUT: VTR 電源を切断
J3	MEC1723 への +3.3 V 電源	**IN(既定値):** +3.3 V 電源を接続 OUT: +3.3 V 電源を切断
J4	CEC1736 への VTR_PLL 電源	**IN(既定値):** VTR_PLL 電源を接続 OUT: VTR_PLL 電源を切断
J5	MEC1723 への +1.8 V 電源	**IN(既定値):** +1.8 V 電源を接続 OUT: +1.8 V 電源を切断
J6	MCP2221A への CEC1736 I2C SCL 選択	1 ～ 2: I2C10 **3 ～ 4(既定値):** I2C06 5 ～ 6: I2C00
J7	CEC1736 への VTR_ANALOG 電源	**IN(既定値):** VTR_ANALOG 電源を接続 OUT: VTR_ANALOG 電源を切断
J8	CEC1736 への +3.3 V 電源	**IN(既定値):** +3.3 V 電源を接続 OUT: +3.3 V 電源を切断
J9	CEC1736 への +1.8 V 電源	**IN(既定値):** +1.8 V 電源を接続 OUT: +1.8 V 電源を切断
J10	CEC1736 の VTR1 電源選択	**1 ～ 2(既定値):** +3.3 V 電源を接続 3 ～ 4: +1.8 V 電源を接続
J11	MCP2221A への CEC1736 I2C SDA 選択	1 ～ 2: I2C10 **3 ～ 4(既定値):** I2C06 5 ～ 6: I2C00
J12	CEC1736 の VTR2 電源選択	**1 ～ 2(既定値):** +3.3 V 電源を接続 3 ～ 4: +1.8 V 電源を接続
J13	MEC1723 への VTR_REG 電源	**IN(既定値):** VTR_REG 電源を接続 OUT: VTR_REG 電源を切断
J14	MEC1723 の VTR2 電源選択	**1 ～ 2(既定値):** +3.3 V 電源を接続 3 ～ 4: +1.8 V 電源を接続
J15	MEC1723 への VTR_PLL 電源	**IN(既定値):** VTR_PLL 電源を接続 OUT: VTR_PLL 電源を切断
J16	MEC1723 への VTR_ANALOG 電源	**IN(既定値):** VTR_ANALOG 電源を接続 OUT: VTR_ANALOG 電源を切断
J17	MEC1723 への VTR1 電源	**IN(既定値):** VTR1 電源を接続 OUT: VTR1 電源を切断
J18	MEC1723 への VBAT 電源	**IN(既定値):** VBAT 電源を接続 OUT: VBAT 電源を切断
J19	MEC1723 への VTR3 電源	**IN(既定値):** VTR3 電源を接続 OUT: VTR3 電源を切断
J20	CEC1736 の GPIO012/nEXTRST のプルアップ / ダウン選択	**1 ～ 2(既定値):** VTR_REG にプルアップ 2 ～ 3: プルダウン

ジャンパ オプション

ジャンパ	説明	詳細
J21	CEC1736 の GPIO106/AP0_nRESET のプルアップ / ダウン選択	**1 ～ 2(既定値):** VTR_REG にプルアップ 2 ～ 3: プルダウン
J22	CEC1736 の GPIO ヘッダ	デバッグ用
J23	CEC1736 の GPIO1316/AP1_nRESET の プルアップ / ダウン選択	**1 ～ 2(既定値):** VTR_REG にプルアップ 2 ～ 3: プルダウン
J24	CEC1736 の nRESET_IN ピン	**1 ～ 2(既定値):** 通常動作 2 ～ 3: CEC1736 をリセット状態に保持
J25	CEC1736 の JTAG _STRAP ピン	1 ～ 2: バウンダリ スキャンモードに移行 **2 ～ 3(既定値):** 通常動作
J26	CEC1736 の GPIO055 ストラップ オプション	ドントケア
J27	CEC1736 の I2C_ADDR0 ストラップ	1 ～ 2**:** VTR_REG にプルアップ **2 ～ 3(既定値)**: プルダウン
J28	CEC1736 の CR_FLASH ストラップ	**1 ～ 2(既定値):** 通常動作 2 ～ 3: クライシス リカバリ フラッシュ コンポーネントからブート
J29	CEC1736 の GPIO124 ストラップ オプション	ドントケア
J30	CEC1736 の BSTRAP ストラップ	**1 ～ 2(既定値):** 通常動作 2 ～ 3: I2C または UART クライシスポートからブート
J31	CEC1736 の I2C_ADDR1 ストラップ	1 ～ 2**:** VTR_REG にプルアップ **2 ～ 3(既定値)**: プルダウン
J32	CEC1736 の RESET_IN# 遅延回路電源	**1 ～ 2(既定値):** +3.3 V 電源を接続 2 ～ 3: VTR_REG 電源を接続
J33	CEC1736 の PICKIT4 1x8 ヘッダ	デバッグ用
J34	CEC1736 の 32 KHz シングルエンド信号源	**IN(既定値):** オシレータを接続 OUT: オシレータを切断
J35	CEC1736 の RESET_IN# 遅延回路	**IN(既定値):** 遅延回路を接続 OUT: 遅延回路を切断
J36	CEC1736 の GPIO157/LED1 と GPIO156/LED0 間のピン接続	**1 ～ 2(既定値):** GPIO157 を LED5 に接続 **3 ～ 4(既定値):** GPIO156 を LED6 に接続
J37	CEC1736 RESET_IN# ピングランド	IN: CEC1736 をリセット状態に保持 **OUT(既定値):** 通常動作
J38	CEC1736 の UART0 デバッグヘッダ	デバッグ用
J39	MEC1723 テストクロック出力ヘッダ	デバッグ用
J40	MEC1723 の 32 KHz シングルエンド入力選択 (オプション)	1 ～ 2: 32KHZ_IN ピンに接続 2 ～ 3: XTAL2 に接続
J41	MEC1723 の I2C02 チャンネルヘッダ	デバッグ用
J42	MEC1723 の I2C07 チャンネルヘッダ	デバッグ用
J43	MEC1723 の RESET_IN# 遅延回路	IN: 遅延回路を接続 **OUT(既定値)**: 遅延回路を切断
J44	MEC1723 RESET_IN# ピングランド	IN: MEC1723 をリセット状態に保持 **OUT(既定値):** 通常動作
J45	MEC1723 の PICKIT4 1x8 ヘッダ	デバッグ用
J46	MEC1723 の GPIO156/LED0、GPIO157/LED1、GPIO153/LED2 間のピン接続	**1 ～ 2(既定値):** GPIO156 を LED9 に接続 **3 ～ 4(既定値):** GPIO157 を LED10 に接続 **5 ～ 6(既定値):** GPIO153 を LED11 に接続
J47	Dediprog SPI プログラミング ヘッダ	U8 PVT SPI フラッシュのプログラミング用
J48	U8 SPI フラッシュ電源選択	**1 ～ 2(既定値):** ボードの +3.3 V 電源に接続 2 ～ 3: Dediprog +3.3 V 電源を接続
J49	MEC1723 の XTAL2 選択	**1 ～ 2(既定値):** 2 ピン水晶振動子に接続 2 ～ 3: シングルエンド 32 KHz 信号源

ジャンパ オプション

ジャンパ	説明	詳細
J50	MEC1723 の XTAL1 選択	**IN(既定値):** 2 ピン水晶振動子に接続 OUT: シングルエンド 32 KHz 信号源を使用、フローティング状態
J51	U8 SPI フラッシュ絶縁ジャンパ	**1 ～ 2(既定値):** U8 SPI_CLK を接続 **3 ～ 4(既定値):** U8 SPI_IO0 を接続 **5 ～ 6(既定値):** U8 SPI_IO1 を接続 **7 ～ 8(既定値):** U8 SPI_CS# を接続 **9 ～ 10(既定値):** U8 SPI_IO2 を接続 **11 ～ 12(既定値):** U8 SPI_IO3 を接続
J52	MEC1723 の JTAG _STRAP ピン	1 ～ 2: バウンダリ スキャンモードに移行 **2 ～ 3(既定値):** 通常動作
J53	MEC1723 の CMP_STRAP ピン	ドントケア
J54	MEC1723 の CR_STRAP ピン	**1 ～ 2(既定値):** CEC1736 を介して SHD_SPI フラッシュからブート 2 ～ 3: PVT_SPI フラッシュ (U8) からブート
J55	MEC1723 の UART0 デバッグヘッダ	デバッグ用
J56	MEC1723 の UART_BSTRAP ピン	**1 ～ 2(既定値):** 通常動作 2 ～ 3: UART クライシスポートからブート
J57	MEC1723 の BSS_STRAP ピン	**1 ～ 2(既定値):** 通常動作 2 ～ 3: このアプリケーションではブートしない
J58	CEC1736 の QSPI0 CS0 成功 / 失敗ケース選択 (デモ用)	**1 ～ 2(既定値):** U9 による通常の成功ケース 2 ～ 3: U11 によるデモ失敗ケース
J59	CEC1736 のフラッシュバス 1 電源選択	**1 ～ 2(既定値):** ボードの +3.3 V 電源に接続 2 ～ 3: Dediprog +3.3 V 電源を接続
J60	CEC1736 のフラッシュバス 2 電源選択	**1 ～ 2(既定値):** ボードの +3.3 V 電源に接続 2 ～ 3: Dediprog +3.3 V 電源を接続
J61	Dediprog SPI プログラミング ヘッダ	U9、U11、または U13 SPI フラッシュ プログラミング用
J62	Dediprog SPI プログラミング ヘッダ	U10 または U12 SPI フラッシュ プログラミング用
J63	U9/U11 または U13 SPI フラッシュ プログラミング選択	**1 ～ 2(既定値):** U9/U11 に接続、J58 で選択 2 ～ 3: U13 に接続
J64	U10 または U12 SPI フラッシュ プログラミング選択	**1 ～ 2(既定値):** U10 に接続 2 ～ 3: U12 に接続
J65	CEC1736 AP0_RESET# の MEC1723 RESET_IN# への接続	**IN(既定値):** 接続 OUT: 切断

第 6 章 OOB(アウトオブ ボックス) デモコードの実行

本 CEC1736 開発ボードは、アウトオブ ボックスですぐに主要な CEC1736 の特長をお試し頂けるように設計されています。

そのため、本開発ボードには、事前定義された OTP 設定と Soteria-G3 ファームウェア SPI イメージがインストールされた書き込み済みの CEC1736 が付属しています。

現在のデモには以下が含まれます。その他にもデモを作成中で、ファームウェアのアップグレードにより利用可能になる予定です。

1. イメージ認証のデモ
   - **AP イメージ**

     MEC1723 は CEC1736 に、AP イメージの認証、現在のステータスの表示、UART ログへの出力を行うよう I2C コマンドを送信します。次に、不正なイメージ格納先を設定し、CEC1736 をリセットします。認証は失敗し、ゴールデンイメージのリカバリを実行します。以上全てのステップとステータスが UART ログに出力されます。

   - Soteria-G3 イメージ

     MEC1723はCEC1736に、Soteria-G3イメージ認証ステータスを取得してUART ログに出力するよう、I2C コマンドを送信します。次に、CEC1736 に不正なイメージ位置を設定した TAG0 を設定し、CEC1736 をリセットします。TAG0 の不正なイメージの認証は失敗し、Soteria-G3 ファームウェア TAG1 の適切なイメージが読み込まれます。以上全てのステップとステータスが UART ログに出力されます。

2. SPI MON(監視) フィルタ処理のデモ
   - オペコード違反

     AP_CFG ポストブート オペコード設定で読み / 書きパーミッションを付与し、消去アクセス権パーミッションは付与しないよう設定します。次に、MEC1723 (AP ホスト) が AP0 SPI フラッシュの任意のメモリ位置に対して消去動作を実行します。CEC1736 はオペコード違反を検出し、MEC1723 をリセットします。以上全てのステップとステータスが UART ログに出力されます。

   - ランタイム違反

     AP_CFG 設定のメモリ領域保護で読み出し動作をブロックするよう設定します。次に、MEC1723 (AP ホスト) が AP0 SPI フラッシュ上のこの保護領域に対して読み出し動作を実行します。CEC1736 はこの読み出し介入ランタイム違反を検出し、MEC1723 をリセットします。以上全てのステップとステータスが UART ログに出力されます。

   - ランタイム認証

     AP_CFG プリブート オペコード設定で読み / 書き / 消去パーミッションを付与します。次に、MEC1723 (AP ホスト) が AP0 SPI フラッシュにバイト値一致イメージを読み込んだ後、非クリティカル ハッシュ値一致イメージを読み込むと、イメージ検証ステータスは「Good to Go」として読み取られます。その後、非クリティカル ハッシュ値一致イメージを破損させてから、イメージ検証ステータスを再度読み取ります。今回は「FW is bad」が読み取られます。以上全てのステップとステータスが UART ログに出力されます。

- 証明 (SPDM) のデモ

  MEC1723 は CEC1736 に一連の I2C コマンドを送信する事で、内部フラッシュから認証チェーン全体を取得、検証を実行、CEC1736 に「チャレンジ認証」を送信して NONCE データとその署名を得てから、NONCE データの署名を検証します。以上全てのステップ、ステータス、データが UART ログに出力されます。

3. 無効化のデモ
   - 鍵の無効化

     このデモでは、鍵が無効化された後、MEC1723 がイメージの読み込みに失敗する事を確認できます。全てのステップとステータスが UART ログに出力されます。

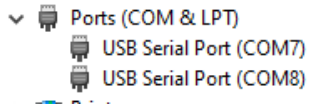
   - ロールバック保護

     このデモでは、FW のリビジョンが更新された後、MEC1723 が旧イメージの読み込みに失敗する事を確認できます。全てのステップとステータスが UART ログに出力されます。

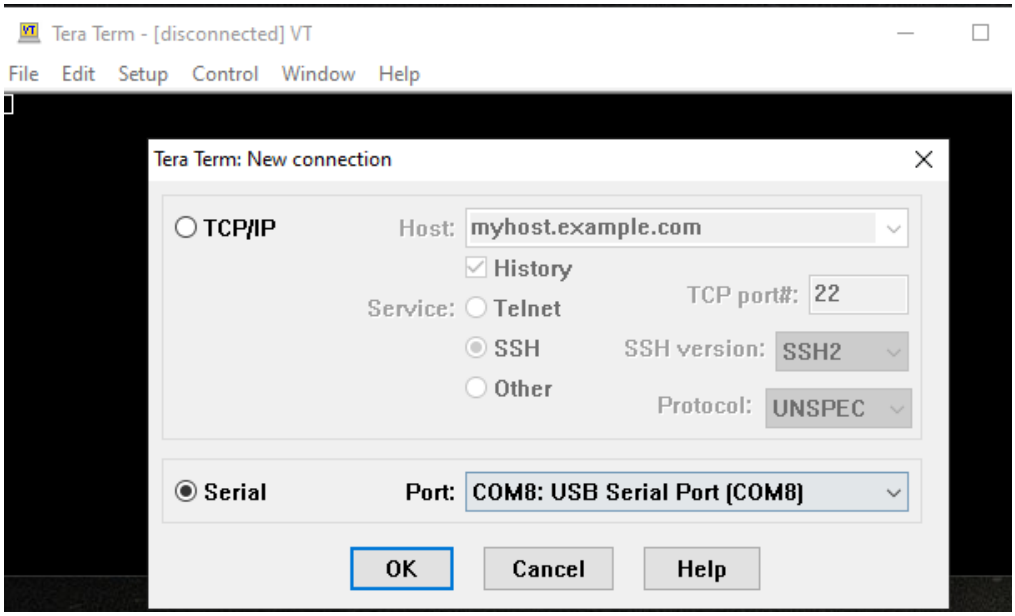
Note:	デモ #1 のデモは開発ボードに含まれる (プログラムされる) 予定です。デモ #2、#3、#4、その他の今後開発されるデモは、公開次第、SDE でリリースされる独立した OOB ホスト サンプルコード パッケージに同梱される予定です。
Note:	詳細は、OOB デモコード リリース パッケージのアプリケーション ノートを参照してください。
Note:	最新情報は Microchip 社の正規代理店にお問い合わせください。

以下のステップごとの例では、本開発ボードの初期電源投入後の CEC1736 のシリアル UART ログを示しています。

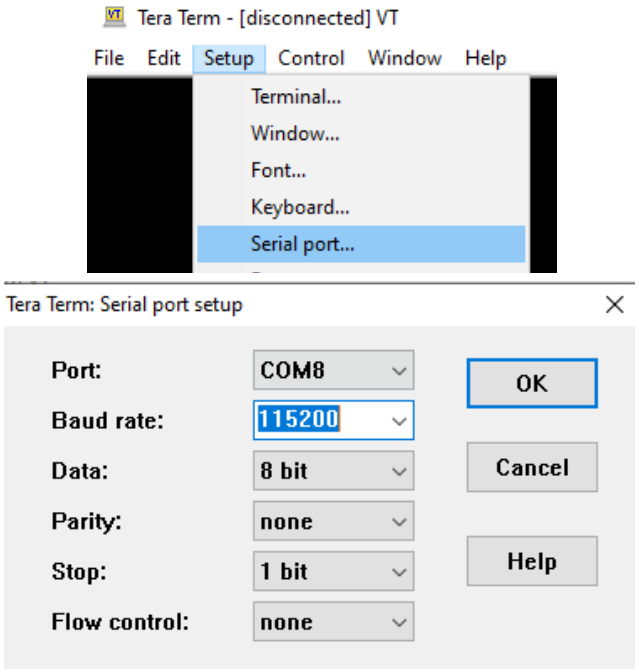
1. Micro-USB ケーブルを使って、PC の USB ポートと第 4 章に示す CEC1736 開発ボードの CEC1736 用 Micro-USB ポート (P2) をつなぎます。
2. 別の Micro-USB ケーブルを使って、PC の USB ポートと第 4 章に示す CEC1736 開発ボードの MEC1723 用 Micro-USB ポート (P3) をつなぎます。
3. 接続された PC の Windows の [デバイス マネージャー] には USB シリアルポートが 2 つ (以下の図の COM7、COM8 等) 検出されます。



4. Tera Term ターミナルを開き、名前に「Serial」とある新しい COM ポート (例 : COM8) を選択します。

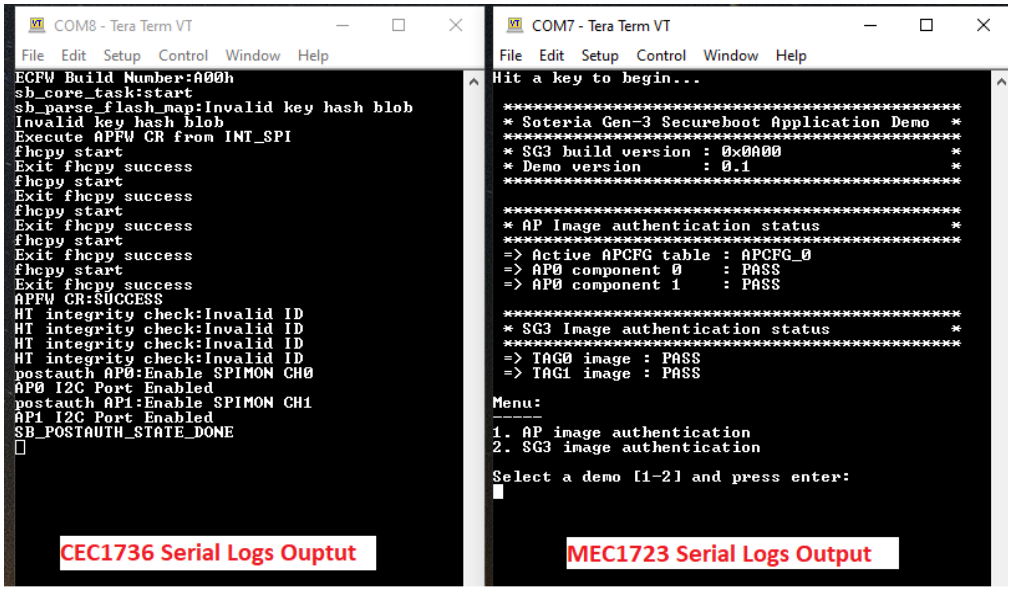


5. [設定] > [シリアルポート] に移動し、「115200-8-n-1-n」を選択します。



6. もう 1 つ Tera Term を開き、COM7 にも同じ設定「115200-8-n-1-n」を行います。
7. ボード電源投入時に CEC1736 Soteria-G3 ファームウェアが既に実行されていたため、上記設定後、最初の UART ログが欠落していました。S1 スイッチを使って CEC1736 をリセットすると、以下の図に示すように対応する UART ログが表示されます。

Note: 以下のログは一例です。実際の結果は使われているテスト環境と Soteria-G3 ファームウェア リリース バージョンによって異なります。

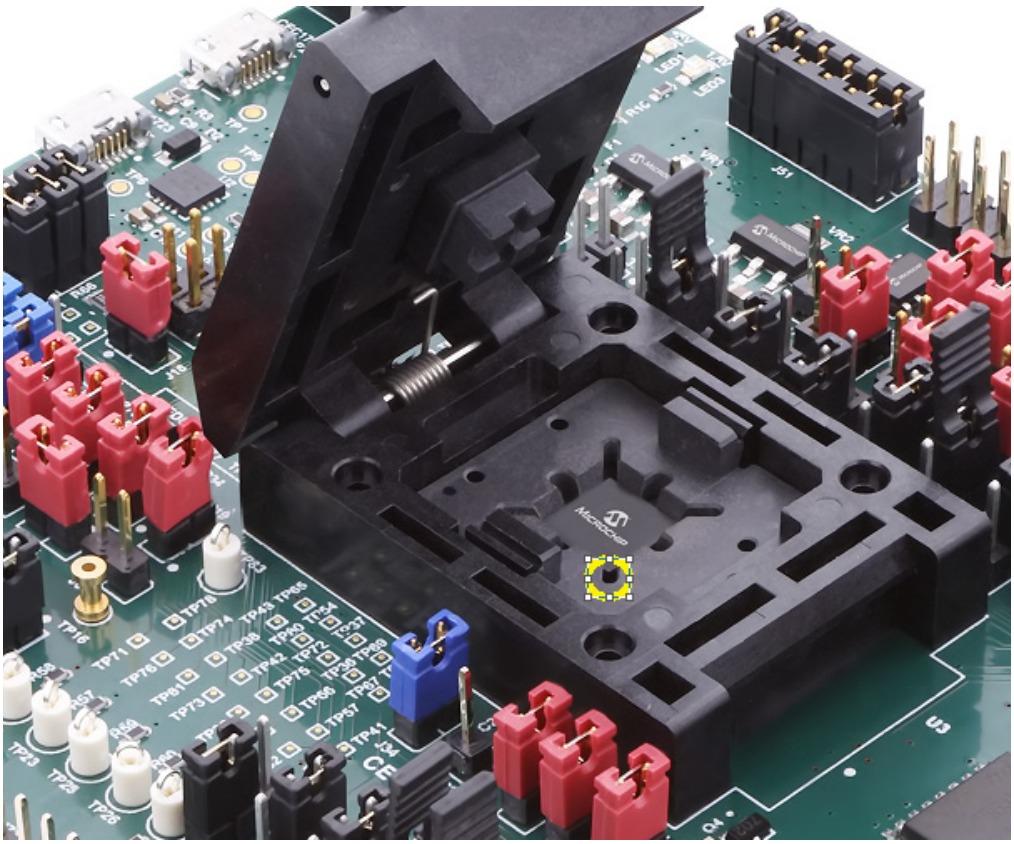

COM8 - Tera Term VT
File Edit Setup Control Window Help
ECFW Build Number:A00h
sb_core_task:start
sb_parse_flash_map:Invalid key hash blob
Invalid key hash blob
Execute APFW CR from INT_SPI
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
fhcpy start
Exit fhcpy success
APFW CR:SUCCESS
HT integrity check:Invalid ID
HT integrity check:Invalid ID
HT integrity check:Invalid ID
HT integrity check:Invalid ID
postauth AP0:Enable SPIMON CH0
AP0 I2C Port Enabled
postauth AP1:Enable SPIMON CH1
AP1 I2C Port Enabled
SB_POSTAUTH_STATE_DONE
CEC1736 Serial Logs Ouptut
COM7 - Tera Term VT
File Edit Setup Control Window Help
Hit a key to begin...
* Soteria Gen-3 Secureboot Application Demo *
* SG3 build version : 0x0A00 *
* Demo version : 0.1 *
* AP Image authentication status *
=> Active APCFG table : APCFG_0
=> AP0 component 0 : PASS
=> AP0 component 1 : PASS
* SG3 Image authentication status *
=> TAG0 image : PASS
=> TAG1 image : PASS
Menu:
1. AP image authentication
2. SG3 image authentication
Select a demo [1-2] and press enter:
MEC1723 Serial Logs Output

第 7 章 開発の準備

デモと評価の段階を終えた後、この開発ボードはセキュリティ機能をカスタマイズするために使う事ができます。

量産バージョンの CEC1736-S0-I/2ZW (84 ピンパッケージ) デバイスの注文をリクエストするには、まず独自の QTP パッケージを作成する必要があります。

その後、新しいカスタムの CEC1736 を開発ボードのソケットに差し換えられます。以下の図の黄色い印で示すように、デバイス上の小さな黒い突起がソケットピン 1 を向いている事を確認してください。



- 残りの開発ステップと動作の詳細は、Microchip 社 TPDS (Trust Platform Design Suite)とCEC1736対応バージョンのパッケージを参照してください。
- CEC1736 をプロビジョニングするツールの使い方の詳細は、『Trust Platform Design Suite Quick Start Guide』を参照してください。
- CEC1736 の周辺モジュール (UART、SPI、LED、PWM 等) を開発しカスタマイズするためのツールの使い方の詳細は『MPLAB Harmony v3 User Guide』を参照してください。
- TPDS (Trust Platform Design Suite)、MPLAB Harmony v3、関連するユーザガイドを入手するには、最寄りの Microchip 社正規代理店にお問い合わせください。NDA(守秘義務契約) の締結が必要です。

7.1 ユーザシステムによる CEC1736 の評価

さらなる評価と製品開発のため、CEC1736 開発ボードをシステムに接続する事を検討できます。

CEC1736 開発ボードは、以下を変更する事で MEC1723 を無効にできるように設計されています。

- J65 を取り外して、CEC1736 の AP0_RESET# ピンと MEC1723 の RESET_IN# ピン間を切断する
- J43 と J44 をジャンパで結合して MEC1723 をリセット状態に保持すると、接続されている全てのピンが 3 ステートの入力モードとなる
- P4 (BMC ホストヘッダ) をプラットフォームの AP0 インターフェイスに接続する
  - CEC1736 の QSPI0_IN バスから AP0 の QMSPI バスへ
  - CEC1736 の AP0_RESET# から AP0 のリセットピンへ
  - CEC1736 の I2C チャンネルから AP0 の I2C チャンネルへ
  - 設計で必要なその他のオプション機能用信号
- デュアル チャンネルを使う場合、P5 (CPU ホストヘッダ) をプラットフォームの AP1 インターフェイスに接続する
  - CEC1736 の QSPI1_IN バスから AP1 の QMSPI バスへ
  - CEC1736 の AP1_RESET# から AP1 のリセットピンへ
  - 設計で必要なその他のオプション機能用信号

各国の営業所とサービス

南北アメリカ

本社
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
技術サポート :
http://www.microchip.com/support
URL:
www.microchip.com

アトランタ
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

オースティン、TX
Tel: 512-257-3370

ボストン
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

シカゴ
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

ダラス
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

デトロイト
Novi, MI
Tel: 248-848-4000

ヒューストン、TX
Tel: 281-894-5983

インディアナポリス
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

ロサンゼルス
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

ローリー、NC
Tel: 919-844-7510

ニューヨーク、NY
Tel: 631-435-6000

サンノゼ、CA
Tel: 408-735-9110
Tel: 408-436-4270

カナダ - トロント
Tel: 905-695-1980
Fax: 905-695-2078

アジア / 太平洋

オーストラリア - シドニー
Tel: 61-2-9868-6733

中国 - 北京
Tel: 86-10 -8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重慶
Tel: 86-23-8980-9588

中国 - 東莞
Tel: 86-769-8702-9880

中国 - 広州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 香港 SAR
Tel: 852-2943-5100

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青島
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 瀋陽
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 蘇州
Tel: 86-186-6233-1526

中国 - 武漢
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦門
Tel: 86-592-2388138

中国 - 珠海
Tel: 86-756-3210040

アジア/太平洋

インド - バンガロール
Tel: 91-80-3090-4444

インド - ニューデリー
Tel: 91-11-4160-8631

インド - プネ
Tel: 91-20-4121-0141

日本 - 大阪
Tel: 81-6-6152-7160

日本 - 東京
Tel: 81-3-6880-3770

韓国 - 大邱
Tel: 82-53-744-4301

韓国 - ソウル
Tel: 82-2-554-7200

マレーシア - クアラルンプール
Tel: 60-3-7651-7906

マレーシア - ペナン
Tel: 60-4-227-8870

フィリピン - マニラ
Tel: 63-2-634-9065

シンガポール
Tel: 65-6334-8870

台湾 - 新竹
Tel: 886-3-577-8366

台湾 - 高雄
Tel: 886-7-213-7830

台湾 - 台北
Tel: 886-2-2508-8600

タイ - バンコク
Tel: 66-2-694-1351

ベトナム - ホーチミン
Tel: 84-28-5448-2100

欧州

オーストリア - ヴェルス
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

デンマーク - コペンハーゲン
Tel: 45-4485-5910
Fax: 45-4485-2829

フィンランド - エスポー
Tel: 358-9-4520-820

フランス - パリ
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

ドイツ - ガーヒンク
Tel: 49-8931-9700

ドイツ - ハーン
Tel: 49-2129-3766400

ドイツ - ハイルブロン
Tel: 49-7131-72400

ドイツ - カールスルーエ
Tel: 49-721-625370

ドイツ - ミュンヘン
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

ドイツ - ローゼンハイム
Tel: 49-8031-354-560

イスラエル - ラーナナ
Tel: 972-9-744-7705

イタリア - ミラノ
Tel: 39-0331-742611
Fax: 39-0331-466781

イタリア - パドヴァ
Tel: 39-049-7625286

オランダ - ドリューネン
Tel: 31-416-690399
Fax: 31-416-690340

ノルウェー - トロンハイム
Tel: 47-7288-4388

ポーランド - ワルシャワ
Tel: 48-22-3325737

ルーマニア - ブカレスト
Tel: 40-21-407-87-50

スペイン - マドリッド
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

スウェーデン - ヨーテボリ
Tel: 46-31-704-60-40

スウェーデン - ストックホルム
Tel: 46-8-5090-4654

イギリス - ウォーキンガム
Tel: 44-118-921-5800
Fax: 44-118-921-5820