

CEC173x 評価用ボード ユーザガイド

EV42J24A



はじめに

EV42J24A CEC173x 評価用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。この最新ボードは、製造を終了した EV19K07A 評価用ボードの後継品です。新しい EV42J24A ボードは、簡素化された設定変更用ジャンパのセットと SPI フラッシュメモリ デバイス用ソケットを備え、プログラミング インターフェイスは SF600 DediProg 向けにアップグレードされています。本ボードでは CEC1736 または CEC1734 デバイスの 84 ピン バージョンが使えます。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開発するための各種ハードウェア(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。ボード上の SPI ソケットを介して 3.3V と 1.8V の SPI メモリチップをサポート可能です。

本評価用ボードは Microchip 社の TPDS (Trust Platform Design Suite)の使用を前提に設計されており、CEC173x-TFLX および CEC173x-TCSM デバイスの能力を評価可能な複数のユースケースを備えています。

- 下記の 4 種類の CEC173x TrustFLEX™ および TrustCUSTOM™ デバイスのサンプルパック(各パックは 3 個のデバイスを含む)

CEC1736-TFLX-PROTO、CEC1736-TCSM-PROTO、CEC1734-TFLX-PROTO、CEC1734-TCSM-PROTO

- ボードの初期使用および検証用の CEC1736 デモサンプル
 - ユーザ固有のユースケースまたはアプリケーション開発には適さず
 - 最新の Soteria-G3 ファームウェア リリースがプログラミング済み
- MEC1723 (アプリケーション プロセスとしてエミュレート)
 - MEC1723 サンプル ファームウェアが書き込み済みで、TPDS ツールの一部としてアップグレード可能
- CEC173x ソケット
 - CEC173x-TFLX または CEC173x-TCSM を使ってユーザ固有の回路向けに各種セキュリティ機能の設定をカスタマイズ可能

図 1. CEC173x 評価用ボード



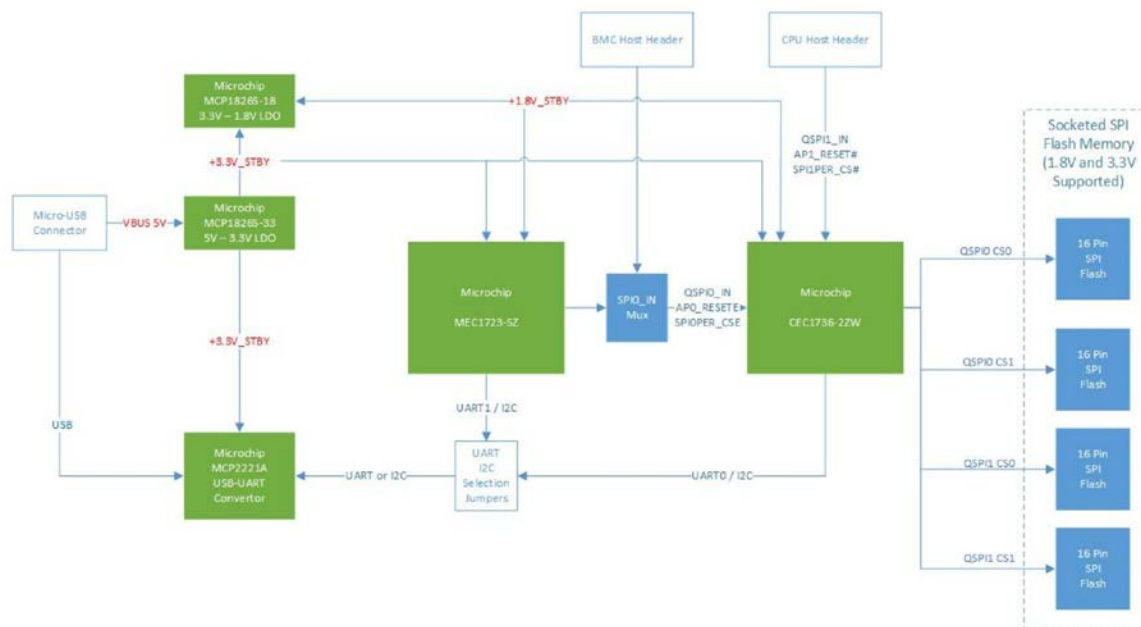
目次

はじめに	1
1. 特長	3
1.1 CEC173x 評価用ボードのブロック図	3
1.2 ハードウェアの特長	3
1.3 CEC173x 評価用ボードのレイアウト	4
2. 推奨ツールおよびアクセサリ	6
3. ボードの動作と設定	7
3.1 CEC173x 評価用ボードへの給電	7
3.2 ジャンパ オプション	8
3.3 外部 SPI フラッシュ ファームウェアの更新	11
3.4 SPI0PER フィルタ コンデンサ	15
4. 開発キットの動作	19
4.1 ボードの検証	19
4.2 Trust Platform Design Suite (TPDS)	21
5. 改訂履歴	23
Microchip 社の情報	24
商標	24
法律上の注意点	24
Microchip 社のデバイスコード保護について	24

1. 特長

1.1 CEC173x 評価用ボードのブロック図

図 1-1. ブロック図



1.2 ハードウェアの特長

- 84 ピン CEC173x 向けソケット
- 4x 16 ピン 256 Mbit/3.3V SPI フラッシュ (ソケットに実装、通常動作向け)
- 1x USB-UART/I²C ポート(CEC173x 向け)
- 1x USB-UART ポート(MEC1723 向け)
- BMC ホストヘッダ
- CPU ホストヘッダ
- 1x デバッグ/プログラミング用 1x8 PICKIT4 ヘッダ(CEC173x 向け)
- 1x デバッグ/プログラミング用 1x8 PICKIT4 ヘッダ(MEC1723 向け)
- オプションのカスタマイズ開発向け GPIO/I²C ヘッダ
- ボードには Micro-USB ケーブルまたは+5V 電源アダプタから給電可能(これらは評価用ボードキットに含まれず)

ボードの検証用に CEC1736 デバイスが本ボード上のソケットに実装済みです。加えて、本キットにはアプリケーション開発用に以下の CEC173x サンプルパックが含まれます。

- CEC1736-TFLX-PROTO
- CEC1736-TCSM-PROTO
- CEC1734-TFLX-PROTO
- CEC1734-TCSM-PROTO

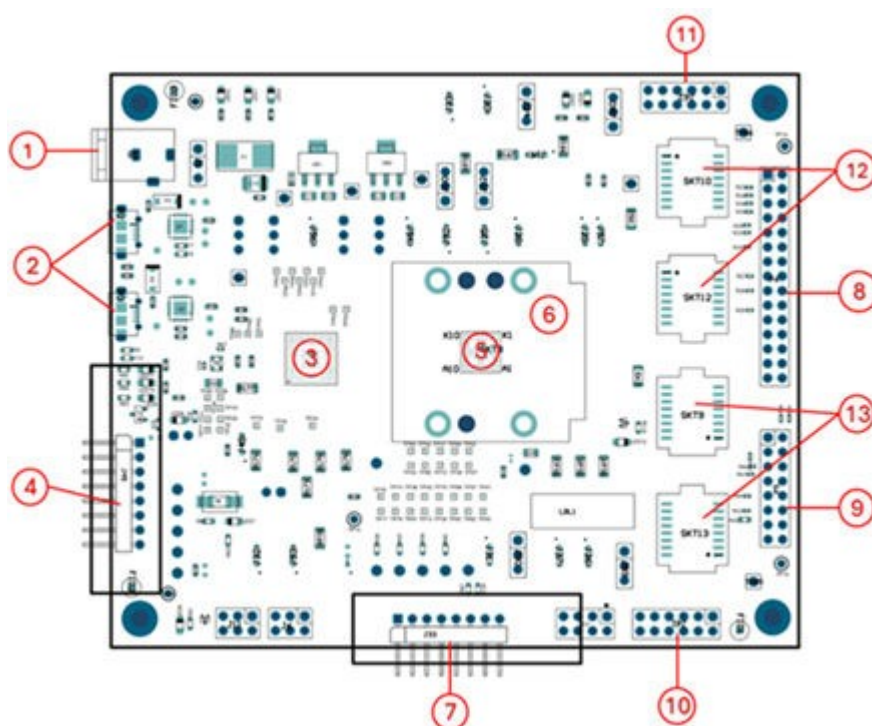
各サンプルパックには 3 個のデバイスが含まれます。

**重要:**

デバイス上面のマーキングでデバイスのタイプ(CEC1734 または CEC1736)を識別することはできますが、TFLX と TCSM を見分ける事はできません。デバイスの識別には注意が必要です。TFLX と TCSM は TPDS を使って識別できます。TPDS ツールはプログラミングの前にデバイスのタイプを確認します。

1.3 CEC173x 評価用ボードのレイアウト

図 1-2. ボードのレイアウト



1. 電源アダプタプラグ(P1) - 外部+5V 電源アダプタから給電する場合に使用
2. USB micro-B コネクタ(P2、P3) - ボードへの電源と、CEC173x (P2)および MEC1723 (P3)へのシリアル入力または I²C 向けインターフェイスを提供(Microchip 社の MCP2221A USB-to-UART/I²C シリアルコンバータを使用)
3. Microchip 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. MEC1723 向け Microchip PICKIT4 1x8 ヘッダ(J45)
5. Microchip CEC1736-S0-I/2ZW デモデバイス(U3 ソケットに実装済み)
6. 84 ピン 2ZW パッケージ ソケット(U3)
7. MEC172x 向け Microchip PICKIT4 1x8 ヘッダ(J33)
8. BMC ホスト接続ヘッダ(P4)

9. CPU ホスト接続ヘッダ(P5)
10. DediProg SF600 SPI フラッシュ プログラミング ヘッダ(J61) - U9 または U13 のプログラミング用
11. DediProg SF600 SPI フラッシュ プログラミング ヘッダ(J62) - U10 または U12 のプログラミング用
12. ソケット上の SPI フラッシュ(U10、U12) - CEC173x QSPI1 チャンネル
13. ソケット上の SPI フラッシュ(U9、U13) - CEC173x QSPI0 チャンネル

2. 推奨ツールおよびアクセサリ

CEC173x 評価用ボードを使った開発には以下のツールを推奨します。

推奨ハードウェア

1. Microchip MPLAB® X v6.20 以上
2. XC32 Pro Compiler v2.50 以上 - Soteria ソフトウェアをカスタマイズする TrustCustom ユーザ向け
3. PICKIT™ 4/PICKIT 5 インサーキット デバッガ(直接プラグイン)
4. [Aardvark I2C/SPI ホストアダプタ](#)
5. [DediProg SF600Plus-G2 プログラマ](#) (推奨)または DediProg SF100 外部 SPI フラッシュ プログラマ

推奨ソフトウェア

EV42J24A 評価用ボードには以下のソフトウェアを推奨します(もしくは使う必要があります)。

1. Microchip 社の Trust Platform Design Suite (TPDS) (詳細は「[Trust Platform Design Suite \(TPDS\)](#)」参照)
2. [MPLAB X IDE](#) のインストール
 - MPLAB バージョン 6.20 と PICKIT5 を使用する場合、ツールパック バージョン 2.5.391 と CEC DFP バージョン 2.0.261 がインストールされている必要があります。
 - TPDS 内で MPLAB X パスを設定(メニュー選択: File -> Preferences -> MPLAB X Path)
3. [FTDI4222H ドライバ](#)のインストール
4. [Aardvark I2C/SPI ホストアダプタ ドライバ](#)のインストール
5. DediProg SF600Plus-G2 向け [SF ソフトウェア](#)と [USB ドライバ](#)のインストール([Support]タブから)
6. Tera Term v4.106 以上(または同等のツール) - UART デバッグログ用

参考資料

CEC173x 製品に関連する多くの文書と開発ボードには NDA(機密保持契約)が必要です。これらは [myMicrochip](#) から入手できます。詳細は、[Accessing Microchip's Secure Documents via myMicrochip](#) を参照してください。

- [CEC1736 製品ページ](#)
- [CEC1734 製品ページ](#)
- [CEC1736-TFLX 製品ページ](#)
- [CEC173x サマリ データシート](#) (myMicrochip から包括的なデータシートが入手可能、要 NDA)
- 追加のボード関連資料(回路図、Gerber ファイル、BOM)とその他の技術資料が myMicrochip から入手可能です(要 NDA)。

ご不明の点は Microchip 社正規代理店にお問い合わせください。

3. ボードの動作と設定

3.1 CEC173x 評価用ボードへの給電

USB-シリアル コンバータの USB micro-B ポート(P2 または P3 もしくはその両方) から CEC173x 評価用ボードへ直接給電できます。USB 電源からの 5V 入力は、MCP1826S 電圧レギュレータにより 3.3V に調整されます。

または、外部電源から電源プラグ(P1)を介して CEC173x 評価用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、5V が 3.3V に調整されます。このオプションはジャンパ J1(ピン 1-2)により選択します。既定値(ピン 2-3)は USB 経由の給電です。

USB micro-B ポートからの給電時は、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。

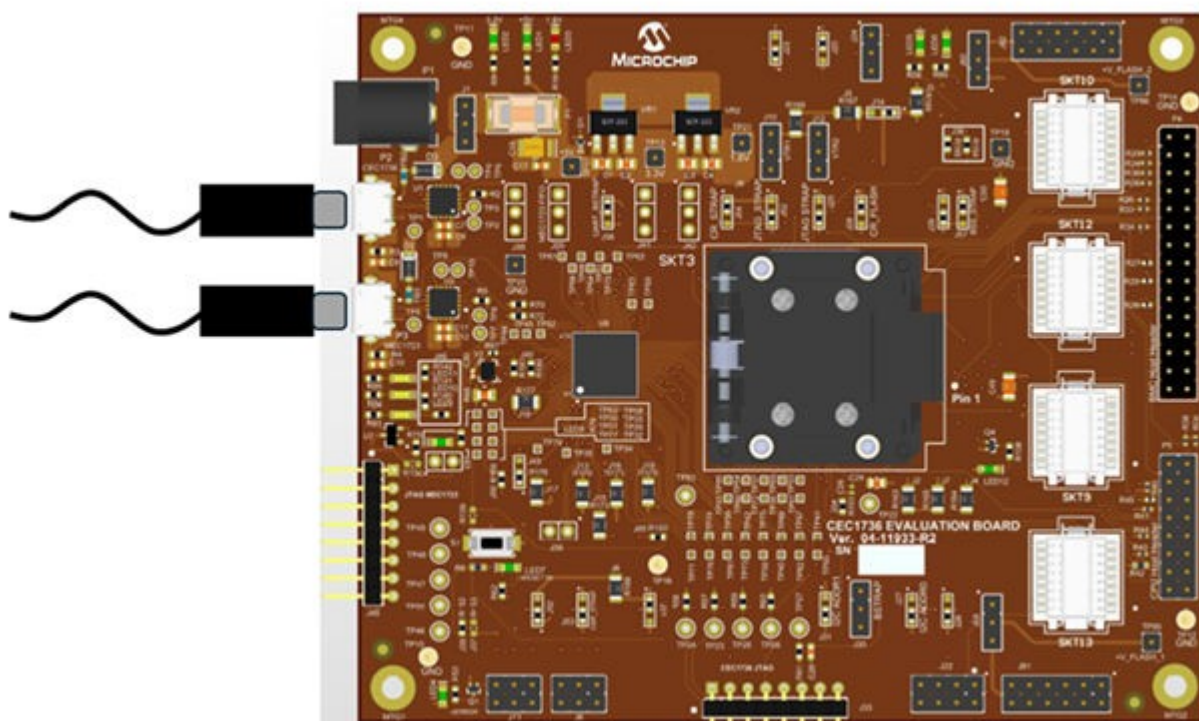
ボードが給電されている時に LED1 (+5V)、LED2 (+3.3V)、LED3 (+1.8V) が点灯する必要があります。

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 が点滅する事があります。これは 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。

本ボードへの電源接続を図 3-1 に示します。

図 3-1. ボードへの電源接続



3.2 ジャンパオプション

CEC173x 評価用ボードは各種の設定用ジャンパを備えています。

基板上のジャンパとヘッダには「J」で始まる識別名が割り当てられています。一部のジャンパは、基板トレースによって既定値設定に固定接続されています。図 3-2 に、そのようなジャンパの例としてジャンパ J23 を示します。これらのジャンパの設定を変更するには、既定値トレースを切断して異なるピンとの間に抵抗を実装する必要があります。J23 の場合、ピン 1 とピン 2 の間のトレースを切断し、ピン 2 とピン 3 の間に 0603 表面実装ゼロオーム抵抗を実装します。このタイプのジャンパは、表 3-1 内の「ジャンパタイプ」列に「トレース接続」として示されます。

トレース接続の代わりにゼロオーム抵抗の実装によるジャンパも存在します。これらのジャンパでは、抵抗の実装(表 3-1 では「IN」と表記)または非実装(同じく「OUT」と表記)によりオプションを設定します。このタイプのジャンパは、表 3-1 内の「ジャンパタイプ」列に「ゼロオーム短絡」として示されます。その他のジャンパでは、デバイスを既定値動作に設定するために通常のジャンパプラグを既定値位置のジャンパピン間に装着する必要があります。このタイプのジャンパは、表 3-1 内の「ジャンパタイプ」列に「標準」として示されます。

図 3-2. トレース接続ジャンパ

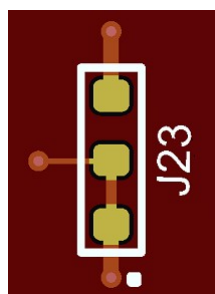


表 3-1 のジャンパー一覧は、前製品の EV19K07A 評価用ボードに基づきます。ジャンパタイプに関係なく、ジャンパの名称は元の EV19K07A から変更していません。ジャンパの種類を識別しやすくするため、この表には「ジャンパタイプ」列を追加しています。ジャンパは以下のタイプに識別されます。

1. **標準** – 回路を変更するためにジャンパプラグを使う標準タイプのジャンパです。
2. **ゼロオーム短絡** – ジャンパプラグの代わりに 1 つまたは複数のゼロオーム抵抗を実装しています。表 3-1 内の「補足」列に抵抗のシルク部品名を記載しています。
3. **トレース接続** – 既定値設定となるよう特定ピン間が基板トレースで固定接続されています。
4. **ヘッダ** – 外部へ接続するためのヘッダです。ジャンパではありません。
5. **未実装** – 元の EV19K07A ボードには存在しましたが、EV42J24A ボードには実装していません。

表 3-1. ジャンパオプションとヘッダの一覧

記号	用途	ジャンパタイプ	補足
J1	ボード電源の選択	標準	1-2: 外部 5V アダプタ(P1) 2-3 (既定値): micro-USB ポート(P2、P3)
J2	CEC173x への VTR 電源	ゼロオーム短絡	R163 IN (既定値): VTR 電源を接続 OUT: VTR 電源を遮断
J3	MEC1723 への+3.3V 電源	ゼロオーム短絡	R166 IN (既定値): +3.3V 電源を接続 OUT: +3.3V 電源を遮断
J4	CEC173x への VTR_PLL 電源	ゼロオーム短絡	R164 IN (既定値): VTR_PLL 電源を接続 OUT: VTR_PLL 電源を遮断
J5	MEC1723 への+1.8V 電源	ゼロオーム短絡	R167 IN (既定値): +1.8V 電源を接続 OUT: +1.8V 電源を遮断
J6	MCP2221A への CEC173x I ² C SCL 選択	標準	1-2: I ² C10 3-4 (既定値) I ² C06 5-6: I ² C00

.....続き

記号	用途	ジャンパタイプ	補足
J7	CEC173x への VTR_ANALOG 電源	ゼロオーム短絡	R165 IN (既定値): VTR_ANALOG 電源を接続 OUT: VTR_ANALOG 電源を遮断
J8	CEC173x への +3.3V 電源	ゼロオーム短絡	R168 IN (既定値): +3.3V 電源を接続 OUT: +3.3V 電源を遮断
J9	CEC173x への +1.8V 電源	ゼロオーム短絡	R169 IN (既定値): +1.8V 電源を接続 OUT: +1.8V 電源を遮断
J10	CEC173x 向け VTR1 電源の選択	標準	1-2 (既定値): +3.3V 電源を接続 3-4: +1.8V 電源を接続
J11	MCP2221A への CEC173x I ² C SDA の選択	標準	1-2: I ² C10 3-4 (既定値): I ² C06 5-6: I ² C00
J12	CEC173x 向け VTR2 電源の選択	標準	1-2 (既定値): +3.3V 電源を接続 3-4: +1.8V 電源を接続
J13	MEC1723 への VTR_REG 電源	ゼロオーム短絡	R170 IN (既定値): VTR_REG 電源を接続 OUT: VTR_REG 電源を遮断
J14	MEC1723 向け VTR2 電源の選択	トレース接続	1-2 (既定値): +3.3V 電源を接続 3-4: +1.8V 電源を接続
J15	MEC1723 への VTR_PLL 電源	ゼロオーム短絡	R173 IN (既定値): VTR_PLL 電源を接続 OUT: VTR_PLL 電源を遮断
J16	MEC1723 への VTR_ANALOG 電源	ゼロオーム短絡	R175 IN (既定値): VTR_ANALOG 電源を接続 OUT: VTR_ANALOG 電源を遮断
J17	MEC1723 への VTR1 電源	ゼロオーム短絡	R176 IN (既定値): VTR1 電源を接続 OUT: VTR1 電源を遮断
J18	MEC1723 への VBAT 電源	ゼロオーム短絡	R177 IN (既定値): VBAT 電源を接続 OUT: VBAT 電源を遮断
J19	MEC1723 への VTR3 電源	ゼロオーム短絡	R178 IN (既定値): VTR3 電源を接続 OUT: VTR3 電源を遮断
J20	CEC173x GPIO012/nEXTRST プルアップ/ダウ選択	トレース接続	1-2 (既定値): VTR_REG ヘブルアップ 2-3: ブルダウ
J21	CEC173x GPIO106/AP0_nRESET プルアップ/ダウ選択	トレース接続	1-2 (既定値): VTR_REG ヘブルアップ 2-3: ブルダウ
J22	CEC173x GPIO ヘッダ	ヘッダ	デバッグ用
J23	CEC173x GPIO1316/AP1_nRESET プルアップ/ダウ選択	トレース接続	1-2 (既定値): VTR_REG ヘブルアップ 2-3: ブルダウ
J24	CEC173x nRESET_IN ピン	標準	1-2 (既定値): 通常動作 2-3: CEC1736 をリセット状態に保持
J25	CEC173x JTAG _STRAP ピン	トレース接続	1-2: バウンダリ スキャンモードに設定 2-3 (既定値): 通常動作
J26	CEC173x GPIO055 ストラップオプション	トレース接続	1-2 (既定値)
J27	CEC173x I ² C_ADDR0 ストラップ	トレース接続	1-2: VTR_REG ヘブルアップ 2-3 (既定値): ブルダウ
J28	CEC173x CR_FLASH ストラップ	トレース接続	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	CEC173x GPIO124 ストラップオプション	トレース接続	1-2 (既定値)
J30	CEC173x BSTRAP ストラップ	標準	1-2 (既定値): 通常動作 2-3: I ² C または UART クライシスポートからブート
J31	CEC173x I ² C_ADDR1 ストラップ	トレース接続	1-2: VTR_REG ヘブルアップ 2-3 (既定値): ブルダウ

.....続き

記号	用途	ジャンパタイプ	補足
J32	CEC173x RESET_IN#遅延回路の電源	トレース接続	1-2 (既定値): +3.3V 電源を接続 2-3: VTR_REG 電源を接続
J33	CEC173x PICKIT4 1x8 ヘッダ	ヘッダ	デバッグ用
J34	CEC173x 32 kHz シングルエンド信号源	ゼロオーム短絡	R151 IN (既定値): オシレータを接続 OUT: オシレータを切断
J35	CEC173x RESET_IN#遅延回路	ゼロオーム短絡	R152 IN (既定値): 遅延回路を接続 OUT: 遅延回路を切断
J36	CEC173x GPIO157/LED1 および GPIO156/LED0 ピンの接続	ゼロオーム短絡	R154 1-2 (既定値): GPIO157 を LED5 へ接続 R155 3-4 (既定値): GPIO156 を LED6 へ接続
J37	CEC173x RESET_IN#ピン グランド	ゼロオーム短絡	IN: CEC1736 をリセット状態に保持 R153 OUT (既定値): 通常動作
J38	CEC173x UART0 デバッグヘッダ	標準	デバッグ用
J39	MEC1723 テストクロック出力ヘッダ	標準	デバッグ用
J40	MEC1723 32 KHz シングルエンド入力 の選択(オプション)	ゼロオーム短絡	クロック源の選択用に R180、R181、R67 を使用
J41	MEC1723 I ² C02 チャンネルヘッダ	標準	デバッグ用
J42	MEC1723 I ² C07 チャンネルヘッダ	標準	デバッグ用
J43	MEC1723 RESET_IN#遅延回路	標準	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	ゼロオーム短絡	IN: MEC1723 をリセット状態に保持 R156 OUT (既定値): 通常動作
J45	MEC1723 PICKIT4 1x8 ヘッダ	ヘッダ	デバッグ用
J46	MEC1723 GPIO156/LED0、 GPIO157/LED1、 GPIO153/LED2 ピンの接続	ゼロオーム短絡	R140 (既定値): GPIO156 を LED9 へ接続 R141 (既定値): GPIO157 を LED10 へ接続 R142 (既定値): GPIO153 を LED11 へ接続
J47	Dediprog SPI プログラミング ヘッダ	ヘッダ	本リビジョンでは未実装
J48	U8 SPI フラッシュ電源の選択	未実装	本リビジョンでは U8 と J48 は未実装
J49	MEC1723 XTAL2 の選択	トレース接続	1-2 (既定値): 2 ピン水晶振動子へ接続 2-3: シングルエンド 32 kHz 信号源へ接続
J50	MEC1723 XTAL1 の選択	ゼロオーム短絡	R159 IN (既定値): 2 ピン水晶振動子へ接続 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	未実装	本リビジョンでは未実装
J52	MEC1723 JTAG_STRAP ピン	トレース接続	1-2: バウンダリ スキャンモードに設定 2-3 (既定値): 通常動作
J53	MEC1723 の CMP_STRAP ピン	トレース接続	1-2 (既定値)
J54	MEC1723 の CR_STRAP ピン	トレース接続	1-2 (既定値): CEC1736 経由で 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 UART0 デバッグヘッダ	標準	デバッグ用
J56	MEC1723 UART_BSTRAP ピン	トレース接続	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 BSS_STRAP ピン	トレース接続	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	CEC173x QSPI0 CS0 成功/失敗ケース の選択(デモ用)	未実装	本リビジョンでは未実装
J59	CEC173x フラッシュバス 1 電源の選択	標準	1-2 (既定値): ボード電源へ接続 2-3: Dediprog 電源を接続
J60	CEC173x フラッシュバス 2 電源の選択	標準	1-2 (既定値): ボード電源へ接続 2-3: Dediprog 電源を接続

.....続き

記号	用途	ジャンパタイプ	補足
J61	Dediprog SPI プログラミング ヘッダ	ヘッダ	U9 または U13 SPI フラッシュのプログラミング用
J62	Dediprog SPI プログラミング ヘッダ	ヘッダ	U10 または U12 SPI フラッシュのプログラミング用
J63	U9/U11 または U13 SPI フラッシュ プログラミングの選択	未実装	本リビジョンでは未実装
J64	U10 または U12 SPI フラッシュ プログラミングの選択	未実装	本リビジョンでは未実装
J65	CEC173x AP0_RESET# の MEC1723 RES の接続	ゼロオーム短絡	R150 IN (既定値): 接続 OUT: 切断

3.3 外部 SPI フラッシュ ファームウェアの更新

EV42J24A 評価用ボードはクワッド SPI インターフェイスを持つ 4 個の外部 NOR フラッシュ SPI デバイスを実装しています。これらの SPI デバイスは、チャンネルあたり 2 つのフラッシュ デバイスを持つ 2 つの SPI チャンネル上に配置されます。

大量のメモリを要求するユーザ アプリケーションでは、最大で 4 個のデバイスの全てを使う事ができます。以下では、SPI フラッシュ デバイス ファームウェアの更新方法について説明します。

3.3.1 DediProg SF600 を使ったプログラミング

EV42J24A 上の SPI NOR フラッシュ デバイスは、DediProg 社の SF600 レベルのインシステム プログラマを使ってプログラミングする事を推奨します。このプログラマは、リボンケーブルを介して EV42J24A 上の 2x6 ヘッダに直接接続します。本ボードには 2 つのプログラミング ヘッダが存在し、各ヘッダから 2 つの SPI チップへアクセスできます。プログラマを接続した後に、Dediprog ソフトウェアを使ってそれらのメモリデバイスをプログラミングします。このソフトウェアは適切なチップセレクトを自動的にアサートするため、チップセレクト ラインの接続を手動で変更する必要はありません。各ヘッダは 2 つの SPI NOR フラッシュチップへ接続されており、2 つのヘッダは互いに独立しています。

SPI チップをプログラミングするには、USB ケーブルを P2 と P3 に接続する事によって本ボードに電源を投入しておく必要があります。ジャンパ J1 が USB ケーブルからの給電(既定値)に設定され、ボードに電源が投入されている事を確認します。DediProg ヘッダをプログラミング ヘッダの 1 つに接続します。図 3-3 に、本ボードにプログラマを接続した状態を示します。プログラミング ケーブルとボードコネクタのピン 1 マークの位置に注意してください。

図 3-3. DediProg SF600 の接続



SF600 プログラミング ソフトウェアは SF600 プログラマ、プログラミングする SPI チップ(これにより正しいチップセレクトが選択される)、メモリデバイスのメーカーとデバイス番号を選択するようユーザ

に要求します。加えて、プログラミング速度と動作モード(シングル、デュアル、クワッド I/O SPI モード)を選択する必要があります。次に、ユーザはロードするファームウェアを選択する事ができます。その後に、ボードをプログラミングするためのバッチ プログラミング メニューアイテムをクリックします。成功すると出力ログが表示されます。図 3-4 にログの例を示します。さらに、残りのデバイスに対して上記の手順を繰り返す事ができます。

図 3-4. SF600 の出力ログ

```

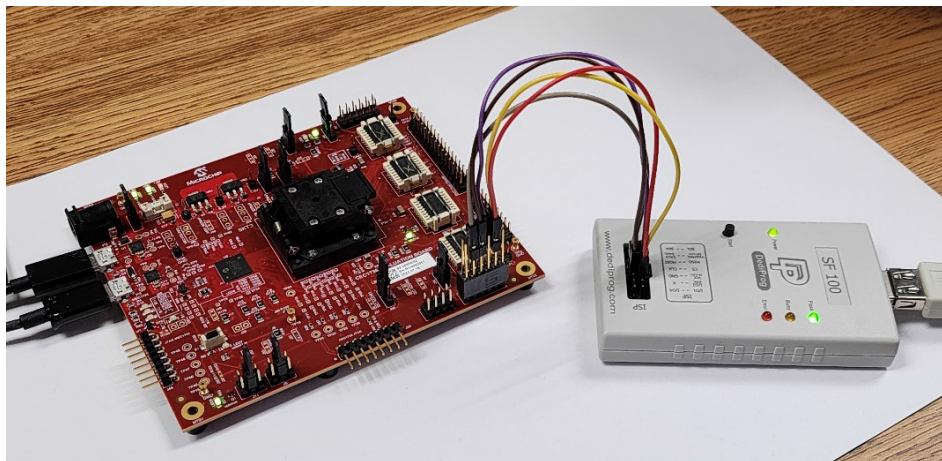
2022-Jun-30 11:02:28: 0.464 seconds elapsed.
2022-Jun-30 11:04:47: Programming parameters:
2022-Jun-30 11:04:47: Source File: spi_image_port_0_comp_0.bin(0x2000000 bytes)
2022-Jun-30 11:04:47: ATE Region: [0, 0x2000000]
2022-Jun-30 11:04:47: Spare Memory Region: leave as being erased.
2022-Jun-30 11:04:47: Truncate-File-To-Fit-Memory Disabled.
2022-Jun-30 11:04:47: Erasing a whole chip ...
2022-Jun-30 11:05:51: A whole chip erased
2022-Jun-30 11:05:51: Programming ...
2022-Jun-30 11:05:51: Programming parameters:
2022-Jun-30 11:05:51: Source File: spi_image_port_0_comp_0.bin(0x2000000 bytes)
2022-Jun-30 11:05:51: ATE Region: [0, 0x2000000]
2022-Jun-30 11:05:51: Spare Memory Region: leave as being erased.
2022-Jun-30 11:05:51: Truncate-File-To-Fit-Memory Disabled.
2022-Jun-30 11:07:54: Programming OK.
2022-Jun-30 11:07:55: Programming parameters:
2022-Jun-30 11:07:55: Source File: spi_image_port_0_comp_0.bin(0x2000000 bytes)
2022-Jun-30 11:07:55: ATE Region: [0, 0x2000000]
2022-Jun-30 11:07:55: Spare Memory Region: leave as being erased.
2022-Jun-30 11:07:55: Truncate-File-To-Fit-Memory Disabled.
2022-Jun-30 11:07:55: Reading From Address [0, 0x2000000] ...
2022-Jun-30 11:08:48: Verify OK.
2022-Jun-30 11:08:48: Operation completed.
2022-Jun-30 11:08:48: 241.346 seconds elapsed.

```

3.3.2 DediProg SF100 を使ったプログラミング

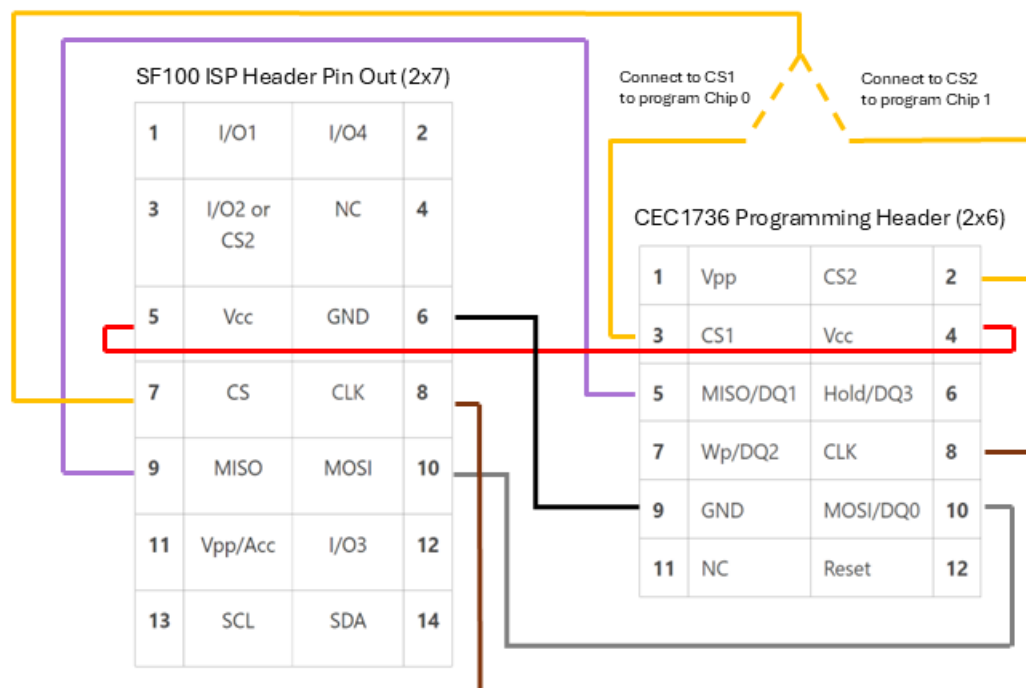
「DediProg SF600 を使ったプログラミング」で説明した通り、EV42J24A 上の SPI NOR フラッシュチップのプログラミングには DediProg SF600 レベルのインシステム プログラマを推奨します。しかし、SF100 レベルのプログラマしか利用できないユーザも多数存在します(以前のボードは SF100 のみサポート)。新しい EV42J24A ボードでは、図 3-5 に示すジャンパ線接続により SF100 プログラマを使う事ができます。この場合、プログラマ側と EV42J24A 側のピン間をジャンパ線で接続します。

図 3-5. ジャンパ線による SF100 プログラマと EV42J24A の接続



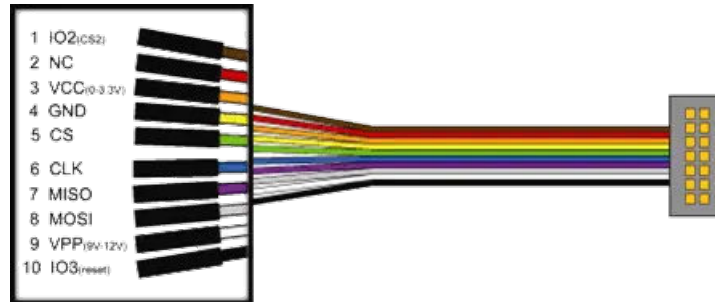
この接続の詳細を図 3-6 に示します。プログラミング手順は基本的に SF600 と同じです。プログラマからボードに給電されるようにジャンパを設定する事を推奨します。SF600 とは異なり、SF100 はチップセレクト ラインを 1 つしか提供しません。このため SF100 を使って両方の SPI チップをプログラミングするには、チップセレクト接続ワイヤの接続先をヘッダ上の 2 本のチップセレクト ピンの間で手動によって変更する必要があります(図 3-6 内の橙色のライン)。4 個のデバイスの全てをプログラミングするには、最初に SF100 をヘッダ J61 (SPI チャンネル 0 へ接続)に接続し、チップセレクト信号を CS1 と CS2 に順次手動で接続する必要があります。次に SF100 をヘッダ J62 (SPI チャンネル 1 へ接続)に接続し、同じ手順で各チップセレクト ピンに接続します。

図 3-6. SF100 と CEC1736 プログラミング ヘッダ間のジャンパ線接続



DediProg 社は ISP-SP-CB フライワイヤ ケーブルを提供しています。このケーブルと 2x6 ヘッダソケットを使うと、容易にプログラミング ケーブルが作れます。

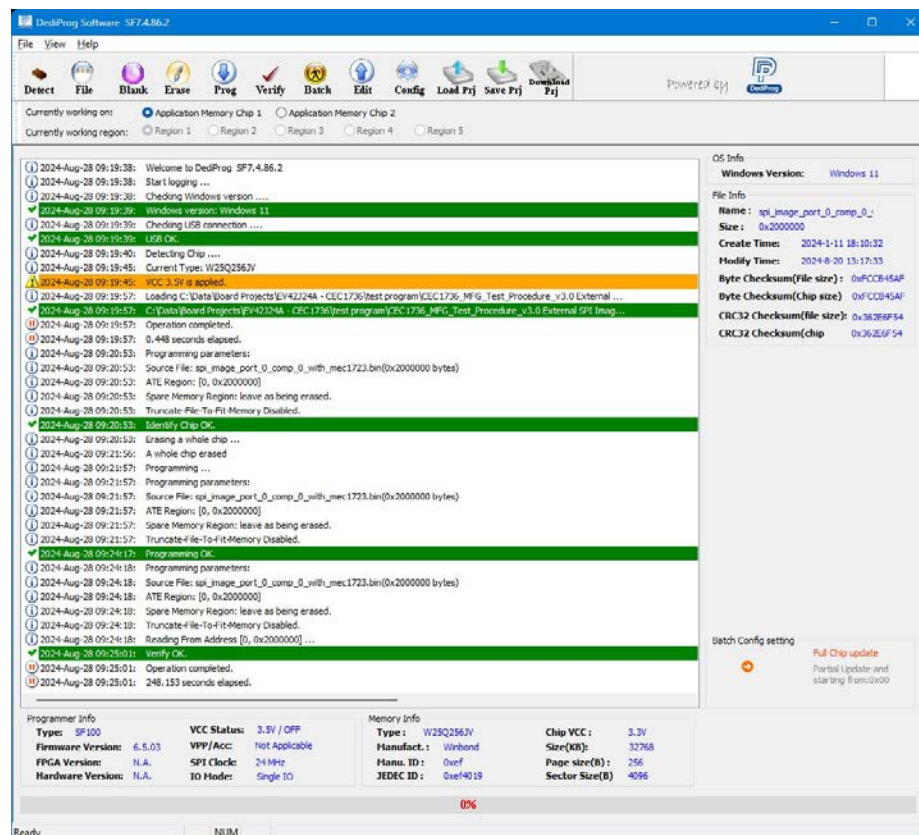
図 3-7. Dediprog 社製 ISP-SP-CB フライワイヤ ケーブル



Dediprog ISP-SP-CB 10 ピン スプリット ケーブルは、SF100 ISP ヘッダに直接接続できる 14 ピンヘッダを備えています(10 ピンのみ ISP スプリット ケーブル用に使用)。各ケーブルは色分けされてピン名が表記されているため、容易に識別できます。

図 3-8 に、SF100 プログラマをフライワイヤ ケーブルで接続した場合のプログラミング ログを示します。このセットアップは 1 つの I/O しかサポートしませんが、24 MHz でプログラミングする事に注意してください。これらの設定は、[Config]ボタン→[Miscellaneous]セクションでの設定に基づきます。

図 3-8. SF100 プログラマを使った場合のプログラミング ログ



3.3.3 SPI フラッシュメモリ デバイスの交換

EV42J24A 評価用ボードのフラッシュメモリ ソケットには 4 個の 3.3V クワッド SPI メモリデバイスが実装済みです。それら他メーカーの SPI フラッシュまたは 1.8V デバイスと交換する場合、お客様の責任で互換性を確認する必要があります。

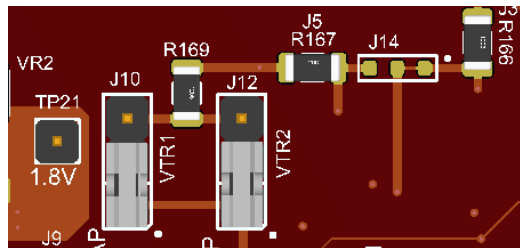
3.3V SPI フラッシュ デバイス

他メーカーの 3.3V デバイスに交換する場合、ボードの電源を遮断し、既存の SPI フラッシュ デバイスを取り外して新しいメモリデバイスと交換します。前述の手順に従ってボードに電源を投入し、DediProg プログラムを使ってフラッシュ デバイスをプログラミングします。

1.8V SPI フラッシュ デバイス

1.8V SPI フラッシュ デバイス向けにボードを設定するために、一部のジャンパ設定を変更する必要があります。これらの変更を行う前に、ボードへの電源を全て遮断します。ボードの設定を 3.3V フラッシュ デバイス向けの既定値モードから 1.8V デバイス向けモードへ変更するには、3 つのジャンパ設定を変更する必要があります。ジャンパ J10 と J12 は、ジャンパプラグを移動させる事により変更できます。J14 はトレース接続ジャンパであるため、トレースを切断する必要があります。

図 3-9. 1.8V SPI 向けのジャンパ設定



CEC1736 は、最大 2 つのチップのそれぞれで 2 つの SPI バンクをサポートします。各バンクは 1.8V または 3.3V の SPI チップをサポート可能です。ジャンパ J10 と J12 では、各チャンネルの電圧(SPI チャンネル 0 に対して VTR1、SPI チャンネル 1 に対して VTR2)を選択します。CEC1736 はフロースルーデータパスであるため、サポートするアプリケーション プロセッサ インターフェイスも、選択された SPI デバイスと等しい電圧信号を提供する必要があります。EV42J24A ボード向けのサポート アプリケーション プロセッサ(MEC1723) の電源電圧はトレース接続ジャンパ J14 により制御されます。このジャンパの既定値設定は 3.3V です。これを 1.8V へ変更するには、トレース接続を切断して 0603 ゼロオーム抵抗を J14 のピン 2-3 に実装します。

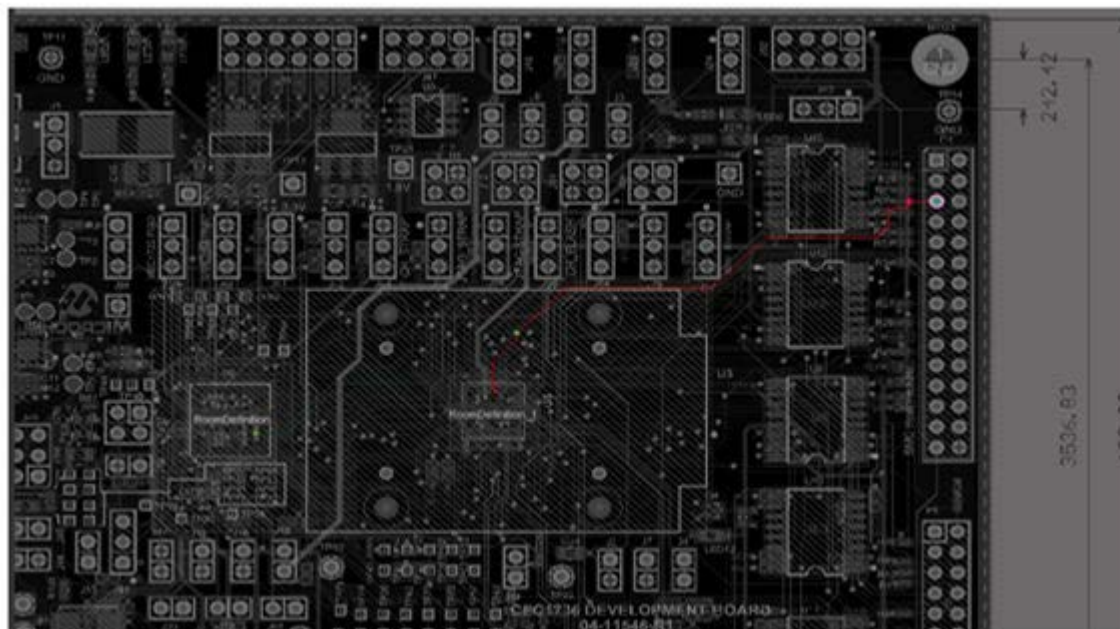
ジャンパ設定を変更した後に、前述の手順でボードに電源を投入し、DediProg プログラムでフラッシュ デバイスをプログラミングします。

3.4 SPI0PER フィルタ コンデンサ

一部の開発ユースケースでは、外部ボードへ接続する必要があります。その場合、SPI0PER チップセレクト ラインに小容量のフィルタ コンデンサを追加する事によってインターフェイスの性能を改善できます。図 3-10 に、評価時に考慮すべきトレースとして BMC コネクタへの SPI0PER トレースを赤で示します。

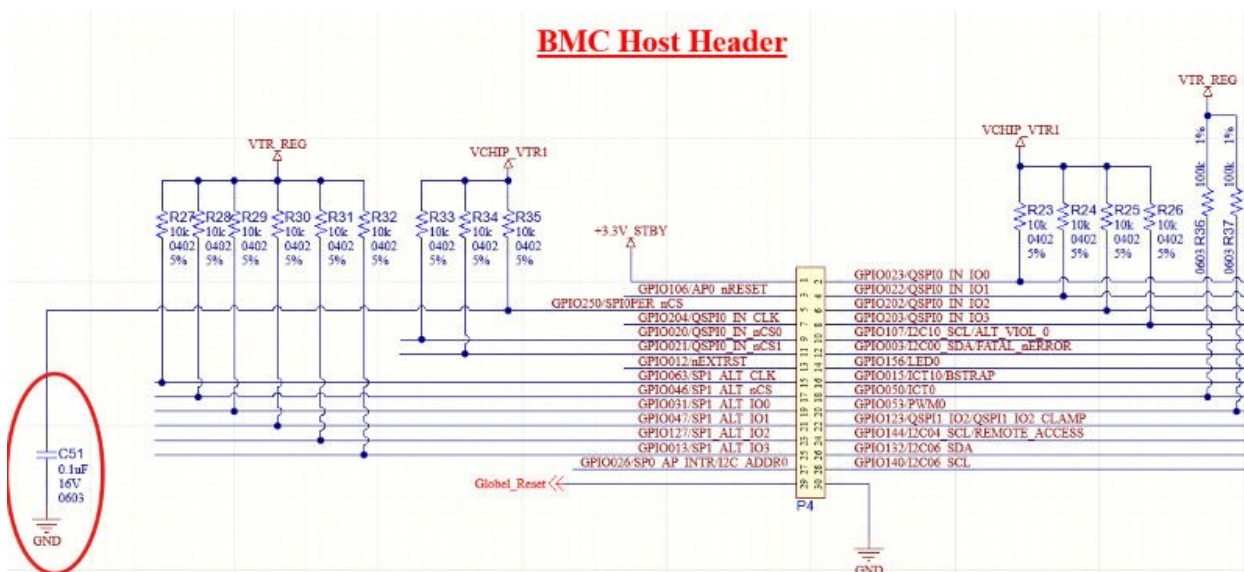
100 nF コンデンサが CS ライン(GPIO250/SPI0PER_nCS)とグラウンドの間に追加されています(Glacier ASIC の近くにあるビアパッドを使用)。これにより、SPT は最高 30 MHz まで確実に動作し、駆動強度は最大 16 mA まで試験されました。

図 3-10. フィルタ コンデンサの実装位置考慮用の SPI0PER トレース



回路図上のコンデンサの実装位置を図 3-11 に示します。コンデンサ C51 は GPIO250/SPI0PER_nCS ラインと GND の間に追加されています。

図 3-11. 回路図上のコンデンサの実装位置



C51 の最適な実装位置は、CEC173x デバイスの直下の基板裏面です(図 3-12 参照)。この図は、以前の評価用ボードの裏面を示しています。最新の評価用ボードでも、この位置はほぼ同じです。

図 3-12. フィルタ コンデンサの取り付け位

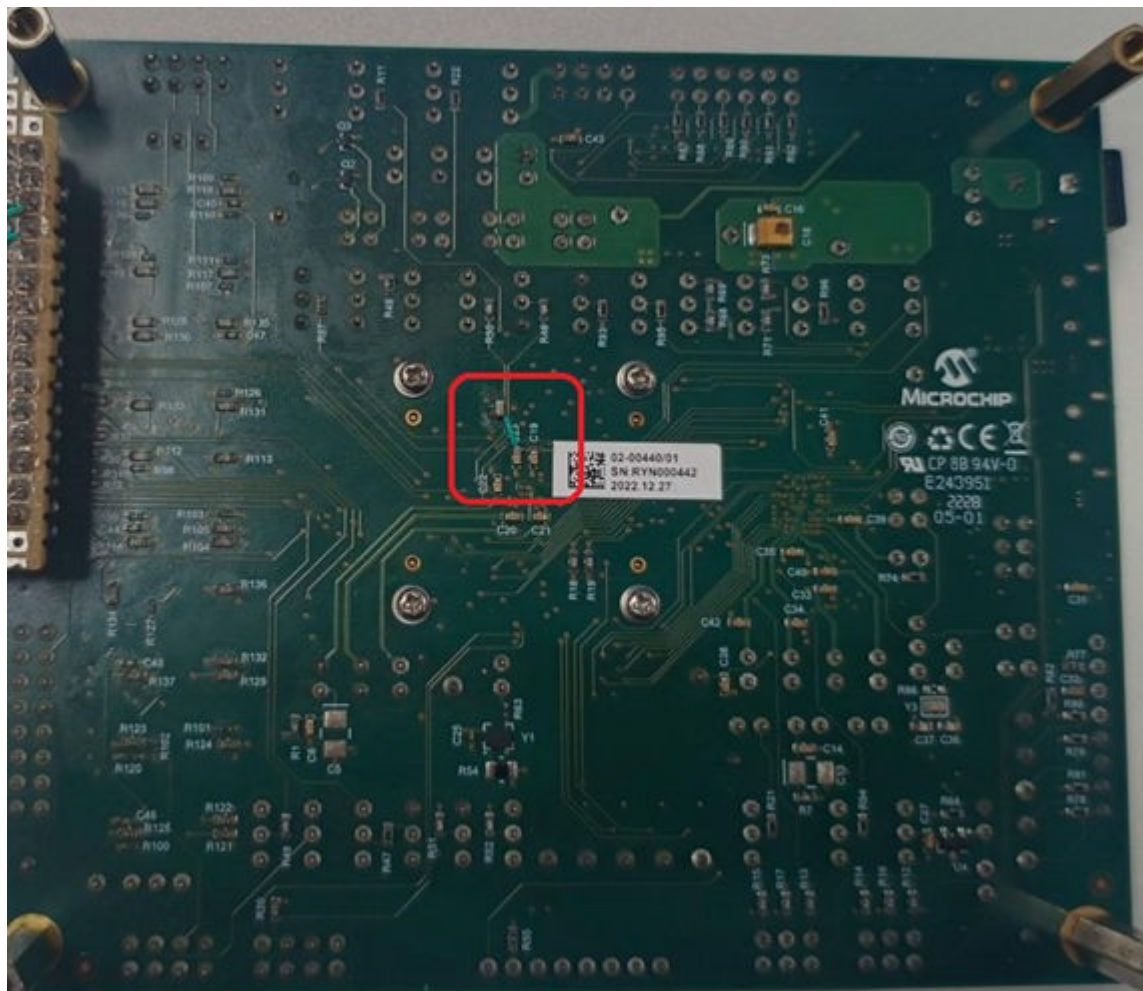
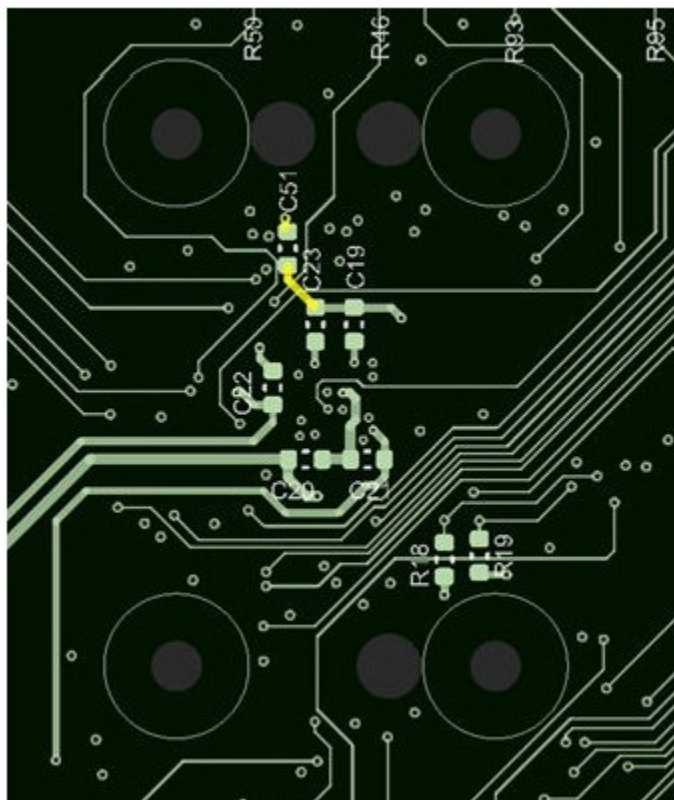


図 3-13 に、設計ツールに表示された変更箇所の詳細を示します。これは、最新評価用ボードのデータに基づきます。黄色のトレースは、変更するために必要なはんだ付けまたはワイヤの追加位置を示しています。

Note: コンデンサの一方のリードはビアパッドに直接はんだ付けします。他方のリードは、短いワイヤを介してグランドに接続します。

図 3-13 フィルタ コンデンサを取り付けるための改造



4. 開発キットの動作

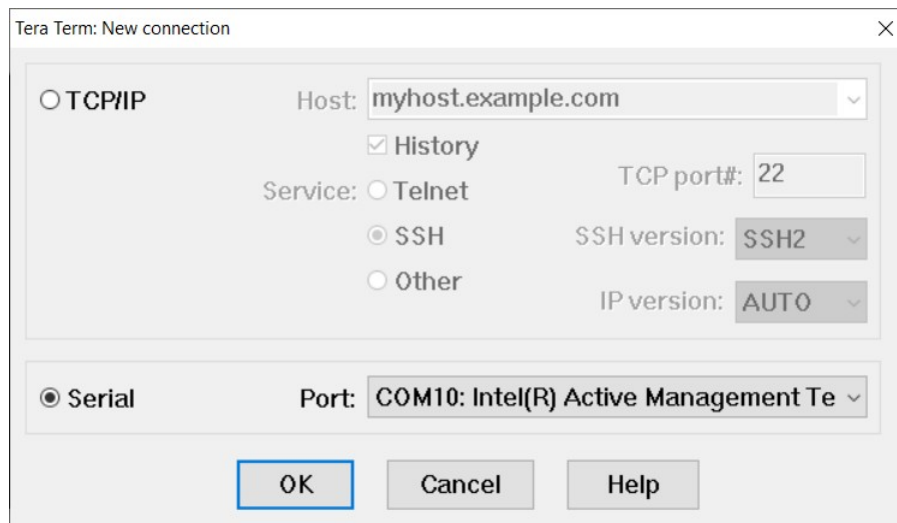
以下では、各種ハードウェアおよびソフトウェア ツールを使って本評価用ボードを動作させる方法を詳細に説明します。これには、評価用ボードへの電源投入方法、オプションのジャンパ設定、外部プログラマを使ったクワッド SPI フラッシュメモリのプログラミング方法、ボードのクイック検証、Microchip Trust Platform Design Suite (TPDS)ツールの概略使用方法が含まれます。

4.1 ボードの検証

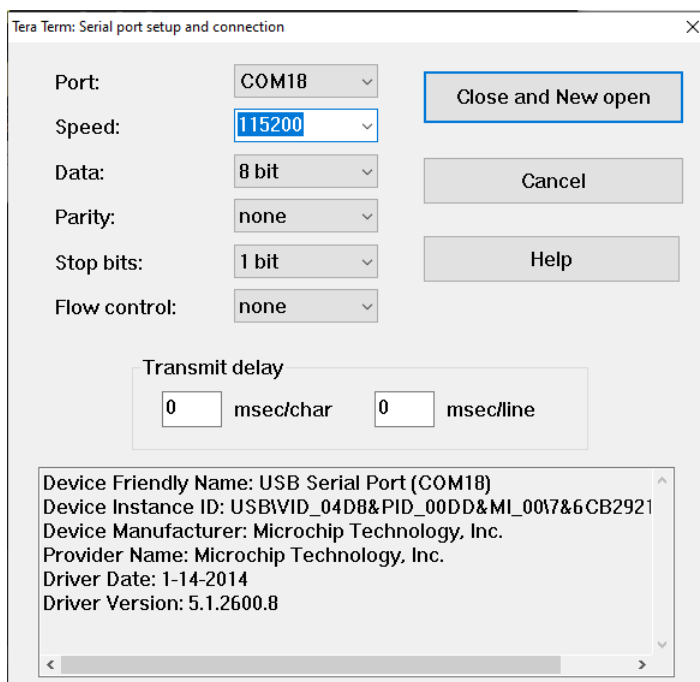
EV42J24A 評価用キットは、定義済み OTP 設定と Soteria-G3 ファームウェア SPI イメージが書き込まれた CEC1736 デバイスを実装しています。このデバイスを使って、ボードが正しく動作している事を確認するための簡単な検証を実行できます。

以下の手順により、ボードの動作を検証できます。

1. ジャンパが全て前述の既定値状態である事を確認します。
2. PC にターミナル ウィンドウ ソフトウェアがインストールされ、マルチウィンドウ モードで実行可能である事が必要です。本書の試験には Tera Term を使用しました。
3. micro-USB ケーブルをコネクタ P2 および P3 と PC に接続します。これらの USB 接続によりボードが給電されると共に、CEC173x と MEC1723 の出力を監視する事が可能になります。
4. 1 つめの[Tera Term]ウィンドウを開き、「Serial」で新しい COM ポート(例:COM10)を設定および選択します。



5. [Setup] -> [Serial port]と操作し、「115200-8-n-1-n」を選択します。



6. 手順 4 と 5 を繰り返して、2 つめの[Tera Term]ウィンドウを設定します。両方ともシリアルポートの baud レートを 115200 に設定する必要があります。
7. EV42J24A 評価用ボード上のリセットボタン S1 を押します。ボードは内部プログラミングされたルーチンに従い、表 4-1 に示す Tera Term 出力ログを生成します。

表 4-1. ボード検証の出力ログ

CEC1736 シリアル ログ出力	MEC1723 シリアル ログ出力

8. カーソルを MEC1723 出力ログ上へ移動し、任意のキーを押します。全てが正しく動作していれば、図 4-1 に示す出力が表示されます。

図 4-1. 最終的な MEC1723 出力ログ

```
COM8 - Tera Term VT
File Edit Setup Control Window Help
Hit a key to begin...

*****
* Soteria Gen-3 Secureboot Application Demo *
*****
* SG3 build version : 0x0D04                *
* Demo version      : 1.6                  *
*****

*****
* AP Image authentication status             *
*****
=> Active APCFG table : APCFG_0
=> AP0 component 0: PASS
=> AP0 component 1: PASS
=> AP1 component 0: PASS
=> AP1 component 1: PASS

*****
* SG3 Image authentication status           *
*****

Menu:
-----
1. Recovery of AP image (Demo code image)
2. Recovery of SG3 TAG0 image
3. SPIMON opcode violation
4. SPIMON runtime violation
5. SPIMON runtime authentication
6. Read I2C violation address qmspi0 and VIOLATION LOG Reg STATUS qmspi0

Select a demo [1-6] and press enter:
```

NOTICE

上図のログはあくまでも一例です。実際の結果は試験環境と使用した Soteria-G3 ファームウェアのリリース バージョンに応じて異なる可能性があります。上図は、本開発キットのリリース時点で Tera Term ソフトウェアと CEC1736 デバイスを使って得られた結果です。TPDS を使ってデバイスをプログラミングした場合、既定値テストイメージが上書きされ、ログは上図と同じになりません。

検証を実行する事により、デバイスとボードが Trust Platform Design Suite (TPDS) ツールを使って動作する事を確認できます。

4.2 Trust Platform Design Suite (TPDS)

CEC173x-TFLX および CEC173x-TCSM デバイスは、Microchip 社の Trust Platform Design Suite (TPDS)の使用を前提に設計されています。TPDS は、Microchip 社ウェブサイトから Windows、Linux、Mac 向けにダウンロードできます。TPDS 上の CEC173x-TFLX/TCSM コンフィグレータは、各種の CEC173x Trust バージョンを有効化および設定するための使い易いグラフィカル ユーザーインターフェイスを提供します。このコンフィグレータにより、試作と量産の両方のフロー向けにパッケージを生成できます。ユーザは、テスト用に CEC173x-TFLX-PROTO および CEC173x-TCSM-PROTO デバイスをプログラミングできます。

TPDS ツールを使うには Microchip MPLAB® X をインストールする必要があります。

CEC173x コンフィグレータは、目的とするユースケース向けに CEC173x Trust Platform デバイスを評価するために必要な暗号アセットを生成およびプロビジョニングするための各種ツールとユーティリティで構成されます。コンフィグレータは OTP、鍵、証明書チェーン、内部および外部フラッシュ デバイス向け複合 SPI イメージを生成およびプロビジョニングするための各種ユースケースとパラメータを表示します。

TPDS ベース パッケージは、Microchip 社ウェブサイトから無償でダウンロードできます。CEC173x の TPDS 拡張には、myMicrochip アカウントと NDA(機密保持契約)が必要です。デバイスの TFLX バージョンと TCSM バージョン向けに別々の拡張が存在します。TPDS ツールを使って完全なソリューションを生成するには、ベース パッケージと適切な拡張パッケージの両方が必要です。

- [TPDS ベース パッケージ](#)
- [CEC1736 TFLX または TCSM TPDS 向け拡張パッケージ](#)

NOTICE

推奨ハードウェアおよびソフトウェア ツールと追加の技術資料については、[「推奨するツールとアクセサリ」](#)を参照してください。

TPDS の使用

TPDS ツールは、ツール機能を強化すると共に、各製品に関連するユースケースを追加するために、常に進化しています。ベース TPDS ツールをダウンロードしてインストールした後に、CEC173x 拡張パッケージと MPLAB® X IDE ツールの起動が可能になります。

開発する CEC173x Trust 製品を選択し、サンプルデバイスの 1 つを EV42J24A 評価用ボード上の SKT3 CEC1736 ソケットに実装します。本製品がお客様の要件を満たしているかどうかを判断するために、CEC173x-TFLX デバイスを使って評価を始める事を推奨します。より柔軟性が必要であれば、CEC173x-TCSM デバイスに変更できます。

TPDS ツールを起動した後に、CEC173x コンフィグレータと適切な CEC173x Trust 製品を選択します。オプションを変更する前に、1 つまたは 2 つのデモ プロジェクトを実行して TPDS ツールと利用可能オプションを熟知する事を推奨します。それらを熟知して独自のアプリケーションを開発できるよう準備するために、ツールに組み込まれたガイダンスと技術資料が役立ちます。



注意: TPDS ツールは、製造時に SPI フラッシュメモリに書き込まれた既定値イメージを上書きします。TFLX デバイスと TCSM デバイスではイメージも異なります。

5. 改訂履歴

リビジョン B (2025 年 1 月)

- 外部ボードと接続するアプリケーション向けのコンデンサに関する項目として「[SPI0PER フィルタ
コンデンサ](#)」に追加しました。

リビジョン A (2024 年 10 月)

- 本書の初版です。

Microchip 社の情報

商標

Microchip 社の名称とロゴ、「M」ロゴ、その他の名称、ロゴ、ブランドは米国および/またはその他の国における Microchip Technology Incorporated またはその支社および/または子会社の登録または未登録商標です。これらの Microchip 社商標に関する情報は、<https://www.microchip.com/en-us/about/legal-information/microchip-trademarks> でご覧になれます。

ISBN:979-8-3371-1356-2

法律上の注意点

本書および本書に記載されている情報は、Microchip 社製品を設計、テスト、お客様のアプリケーションと統合する目的を含め、Microchip 社製品に対してのみ使う事ができます。それ以外の方法でこの情報を使用する事はこれらの条項に違反します。デバイス アプリケーションの情報は、ユーザの便宜のためにのみ提供されるものであり、更新によって変更となる事があります。お客様のアプリケーションが仕様を満たす事を保証する責任は、お客様にあります。その他のサポートについては、弊社または代理店にお問い合わせになるか、www.microchip.com/en-us/support/design-help/client-support-services をご覧ください。

Microchip 社は本書の情報を「現状のまま」で提供しています。Microchip 社は、明示的、暗黙的、書面、口頭、法定のいずれであるかを問わず、本書に記載されている情報に関して、状態、品質、性能、商品性、特定目的への適合性をはじめとする、いかなる類の表明も保証も行いません。

いかなる場合も Microchip 社は、本情報またはその使用に関連する間接的、特殊的、懲罰的、偶発的、または必然的損失、損害、費用、経費のいかににかかわらず、また Microchip 社がそのような損害が生じる可能性について報告を受けていた場合あるいは損害が予測可能であった場合でも、一切の責任を負いません。法律で認められる最大限の範囲を適用しようとも、本情報またはその使用に関連する一切の申し立てに対する Microchip 社の責任限度額は、使用者が当該情報に関連して Microchip 社に直接支払った額を超えません。

Microchip 社の明示的な書面による承認なしに、生命維持装置あるいは生命安全用途に Microchip 社の製品を使う事は全て購入者のリスクとし、また購入者はこれによって発生したあらゆる損害、クレーム、訴訟、費用に関して、Microchip 社は擁護され、免責され、損害をうけない事に同意するものとします。特に明記しない場合、暗黙的あるいは明示的を問わず、Microchip 社が知的財産権を保有しているライセンスは一切譲渡されません。

Microchip 社のデバイスコード保護について

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。