参考資料

User's Guide

MSPM33 NONMAIN フラッシュメモリ構成ガイド

Utkarsh Kripashankar and Yuhao Zhao

概要

MSPM33 NONMAIN は、チップの起動と拡張機能の選択に関連するパラメータを設定する専用フラッシュメモリ領域です。このドキュメントでは、NONMAIN 領域の構成について詳しく説明し、アプリケーションで使用するための設定ガイダンスを提供します。

目次

概要 1
1 概要 2
1.1 用語 3
2 NONMAIN アーキテクチャ 4
2.1 MSPM33 ファミリの概要 4
2.2 NONMAIN 構成の概要 4
2.3 NONMAIN メモリ 7
3 NONMAIN 構成 9
3.1 BCR の構成 9
3.2 BSL の構成 18
4 SysConfig を使用した NONMAIN 構成 22
4.1 SysConfig の概要 22
4.2 SysConfig を使用した BCR の構成 22
4.3 SysConfig を使用した BSL の構成 29
5 アプリケーション コードでの NONMAIN 構成 32
6 IDE ツールを使用した NONMAIN 動作 33
6.1 NONMAIN 構成ファイル 33
6.2 プロジェクトの消去プロパティ 33
6.3 パスワードで保護されたデバッグ 37
7 プログラマ ツールを使用した NONMAIN 動作 39
7.1 UniFlash を使用した NONMAIN 動作 39
7.2 J-Flash を使用した NONMAIN 動作 40
8 よくある質問 (FAQ) 41
8.1 マイコン ロック状態分析 41
8.2 MSPM33 デバイスのロック解除 43
8.3 デバッグ エラーの概要 44
8.4 MSPM33 ブート診断 46
9 まとめ 47
10 参考資料 48

商標

Code Composer Studio™ is a trademark of Texas Instruments.
J-Flash™ and J-Link™ are trademarks of SEGGER MICROCONTROLLER GMBH & CO. KG.
Arm®, Cortex®, and Keil® are registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere.
IAR Embedded Workbench® is a registered trademark of IAR Systems AB.
すべての商標は、それぞれの所有者に帰属します。

Copyright © 2026 Texas Instruments Incorporated

1 概要

図 1-1 に、すべての MSPM33 デバイスが共有する共通プラットフォーム メモリ マップを示します。マップには 4 つの異なるメモリ領域があります。

- MAIN フラッシュ
- NONMAIN フラッシュ
- FACTORY リージョン
- ROM

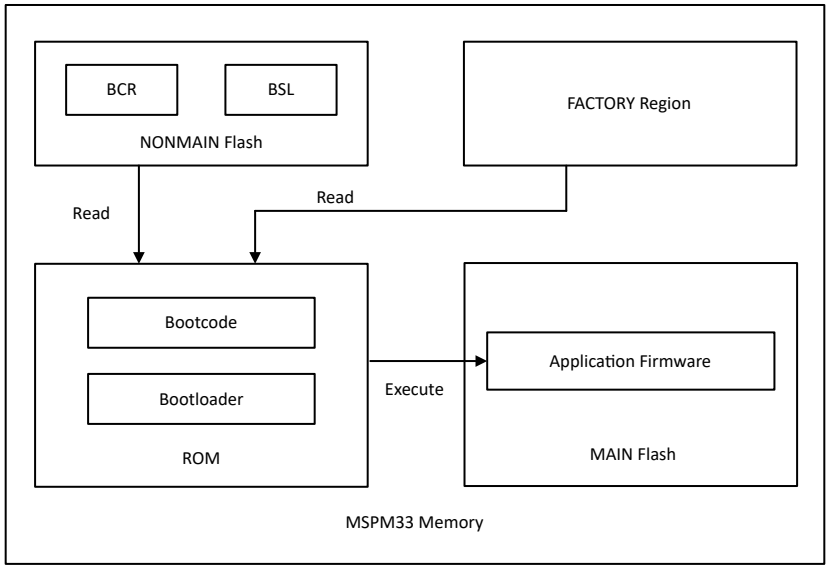


図 1-1. MSPM33 メモリ マップ

MAIN フラッシュは、実行可能コードとデータを格納するために使用されるメモリです。MSPM33 デバイスは、シングル バンクまたはデュアル バンクの MAIN フラッシュをサポートしています。詳細については、デバイス固有のデータシートを参照してください。

NONMAIN フラッシュは、デバイスをブートするためにブート構成ルーチン (BCR) とブートストラップ ローダ (BSL) 構成が使用する構成データを格納する、フラッシュ メモリの専用領域です。BCR と BSL にはも構成ポリシーがあり、NONMAIN フラッシュ領域にプログラムされた値を変更することで、デフォルト値 (開発および評価時の標準値) をそのままにするか、特定の目的 (量産プログラミング時の標準値) に変更することができます。

注

NONMAIN フラッシュを消去した後で、適切な値が NONMAIN フラッシュにロードされていることを確認します。負荷を検証しないと、次の BOOTRST の後にデバイスが永続的にロックされます。

すべてのデバイスは、アプリケーション ソフトウェア用に、デバイスの機能を説明する読み出し専用データと、工場から提供された調整情報とを、メモリ内に割り当てられた FACTORY 領域に格納しています。

読み取り専用メモリ (ROM) は、変更不可能な信頼ルートブート構成ルーチン (BCR) とブートストラップ ローダ (BSL) で構成されています。BCR は、メイン アプリケーションが開始する前に、デバイスの BOOTRST に続いて Arm® Cortex®-M33 プロセッサで実行される最初のコードです。BCR は、ハードウェアまたはソフトウェアによるブートストラップ ローダー (BSL) の呼び出しを通じて動作し、BSL エントリを認証します。図 1-2 に、MSPM33 デバイスの高レベルのブート フローを示します。詳細については、『MSPM33C セキュリティ ユーザー ガイド』を参照してください。

Copyright © 2026 Texas Instruments Incorporated

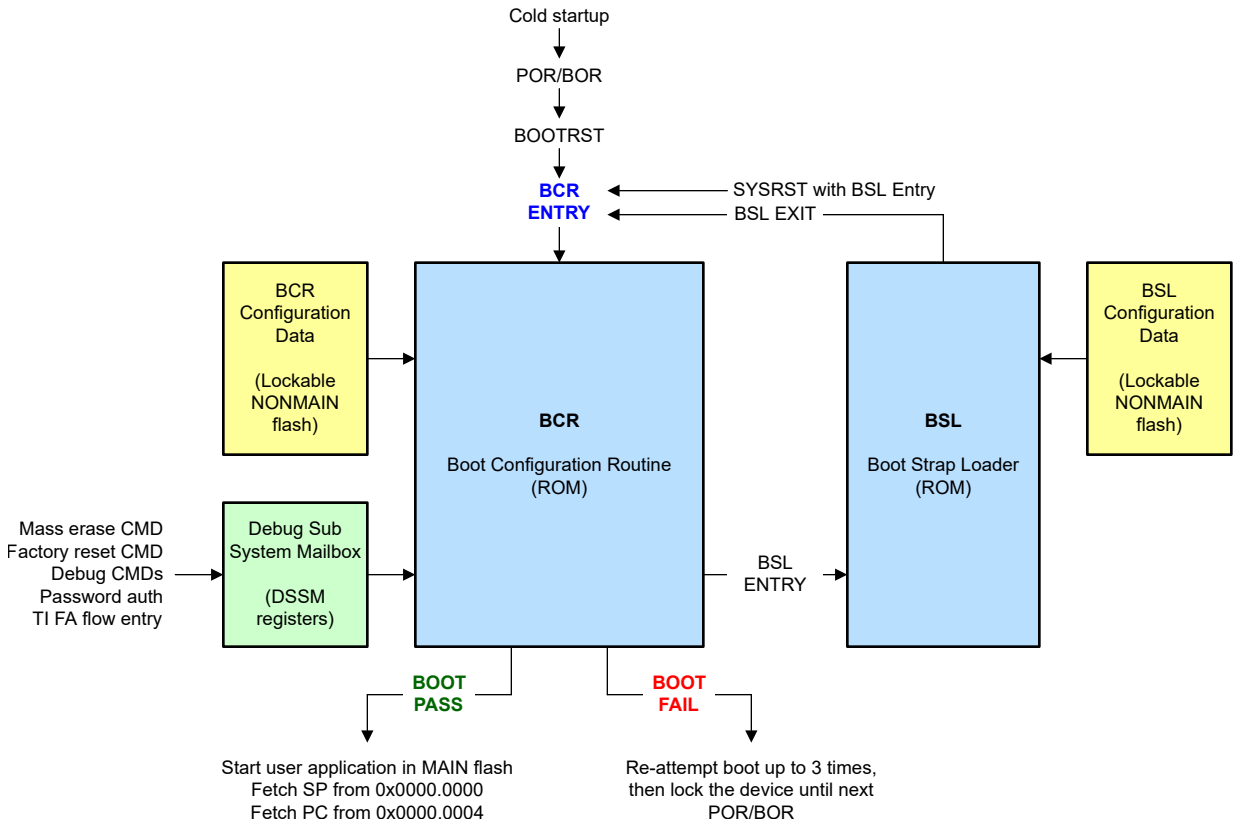


図 1-2. MSPM33 のブート フロー

BCR は、デバイスのセキュリティ ポリシーをセットアップし、デバイスが動作するように構成を行うほか、BSL がトリガーされた場合には、必要に応じて BSL を起動します。BCR が BSL を起動した場合は、その BSL を使用して、標準シリアル インターフェース (UART、I2C、または CAN) 経由でデバイス メモリ (フラッシュおよび SRAM) のプログラミングや検証を行います。

1.1 用語

ブートコード (BCR)	BOOTRST の後で実行されるスタートアップ ルーチンで、アプリケーションを実行するためにデバイスを構成します。
NONMAIN フラッシュ	NONMAIN フラッシュは、デバイスをブートするためにブート構成ルーチン (BCR) とブートストラップ ローダ (BSL) 構成が使用する構成データを格納する、フラッシュ メモリの専用領域です。
FACTORY フラッシュ	FACTORY 領域は、メモリ内に割り当てられた フラッシュ領域であり、アプリケーション ソフトウェア用に、デバイスの機能を説明する読み出し専用データと、工場から提供された調整情報を格納しています。
BCR の構成	NONMAIN フラッシュ メモリに置かれている、ユーザーが構成可能なすべてのブートコード パラメータを含む構成構造です。
ブートストラップ ローダ (BSL)	データをデバイスのメモリにロードするために使用されるブート ルーチンです。
BSL の構成	NONMAIN フラッシュ メモリに置かれている、ユーザーが構成可能なすべてのブートストラップ ローダのパラメータを含む構成構造。
カスタマ セキュア コード (CSC)	このコードは、テキサス・インスツルメンツのブート コードの後に実行され、フラッシュ メモリ上で動作して、追加のセキュリティ要素を設定します。詳細については、セキュア ブート ユーザー ガイドを参照してください

Copyright © 2026 Texas Instruments Incorporated

2 NONMAIN アーキテクチャ

このセクションでは、NONMAIN 構造、サポートされている機能、さまざまな NONMAIN 構成のアプリケーションについて詳しく説明します。

2.1 MSPM33 ファミリの概要

MSPM33 ファミリは、NONMAIN 構成でサポートされている機能を制限する、さまざまな種類の NONMAIN レイアウトをサポートしています。

表 2-1 に、どの NONMAIN レイアウト タイプをどのデバイスで使用するかを示しています。詳細については、セクション 10 にリンクされている、デバイス固有のテクニカル リファレンス マニュアルの「ブート構成」セクションを参照してください。

表 2-1. NONMAIN レイアウト タイプ

NONMAIN レイアウト タイプ	サポート対象のデバイス	概要
タイプ A	MSPM33C32xx	• CSC サポートを含む • SHA256 ハッシュ形式でのパスワード保存 • アプリケーション整合性チェックで、CRC32 または SHA256 ハッシュ オプションを使用 • システム PLL の構成 • フラッシュ セキュリティの構成 • UART のデフォルト ボーレート構成 • ROM BSL のみをサポート • デバイス構成用の OTP 領域をサポート

2.2 NONMAIN 構成の概要

MSPM33 NONMAIN フラッシュ メモリは、さまざまな種類の構造レイアウトを備えています。一部のレイアウト タイプでは、一部の機能が縮小またはサポートされていません。

Copyright © 2026 Texas Instruments Incorporated

表 2-2. NONMAIN 構成パラメータ

構成パラメータ			レジスタ フィールド	NONMAIN レイアウト タイプ
				A
BCR	BCR の構成 ID		BCRCONFIGID	✓
	SWD (シリアル ワイヤ デバッグ) ポリシーの構成	アクセス ポリシー	BOOTCFG0	✓
		デバッグ ポリシー		
		デバッグ パスワード	DEBUG_LOCK	✓
			DEBUG_NS_LOCK	✓
	SWD ロック、工場出荷時リセットの構成	工場出荷時リセット アクセス プロパティ	BOOTCFG4	✓
		工場出荷時リセット パスワード	MASS_ERASE_y	✓
	SWD 一括消去の構成	一括消去アクセス プロパティ	BOOTCFG4	✓
		パスワードの一括消去	FACTORY_RESET_y	✓
	フラッシュ セキュリティの構成	Bank0 メイン FLASH 書き込み消去保護	BANK0_WRITE_ERASE_PROTECTION_A BANK0_WRITE_ERASE_PROTECTION_B	✓
		Bank0 メイン FLASH セキュリティ保護	BANK0_SECURITY_PROTECTION_A BANK0_SECURITY_PROTECTION_B	✓
		Bank0 メイン FLASH 特権保護	BANK0_PRIVILEGE_PROTECTION_A BANK0_PRIVILEGE_PROTECTION_B	✓
		Bank1 メイン FLASH 書き込み消去保護	BANK1_WRITE_ERASE_PROTECTION_A BANK1_WRITE_ERASE_PROTECTION_B	✓
		Bank1 メイン FLASH セキュリティ保護	BANK1_SECURITY_PROTECTION_A BANK1_SECURITY_PROTECTION_B	✓
		Bank1 メイン FLASH 特権保護	BANK1_PRIVILEGE_PROTECTION_A BANK1_PRIVILEGE_PROTECTION_B	✓
		データ FLASH 書き込み消去保護	DBANK_WRITE_ERASE_PROTECTION	✓
		データ FLASH セキュア保護	DBANK_SECURITY_PROTECTION	✓
		データ FLASH 特権保護	DBANK_PRIVILEGE_PROTECTION	✓
		NONMAIN 静的書き込み保護	BANK0_NM_USER_CONFIG	✓
	SYSPLL の構成	ブート時のシステム PLL の構成	BOOTCLK0 BOOTCLK1	✓
	不正なデバイス変換	不正なデバイス変換パスワード	BAD_CONV_y	✓
	カスタマ セキュア コード (CSC)	CSC ポリシー	BOOTCFG2	✓
		フラッシュ バンク スワップ方針		✓
		デバッグ ホールド	BOOTCFG1	✓

Copyright © 2026 Texas Instruments Incorporated

表 2-2. NONMAIN 構成パラメータ (続き)

構成パラメータ			レジスタ フィールド	NONMAIN レイアウト タイプ
				A
BCR	高速ブート モード		BOOTCFG3	✓
	アプリケーション ダイジェスト チェックの構成	アプリケーション ダイジェスト チェック ポリシー	SECURE_BOOT_MODE	✓
		アプリケーションの開始アドレス	USER_SECURE_APP_START_ADDR	
		セキアプリケーションの長さ	USER_SECURE_APP_LENGTH	
		アプリケーション チェックサム	USER_SECURE_APP_HASH_y	
	BSL ポリシー	ピン チェックの呼び出しを有効にします	BOOTCFG1	✓
		イネーブル BSL モード	BOOTCFG3	
	BCR チェックサム	CRC32-ISO3309	BCRCRC	✓
BSL	BSL の構成 ID		BSLCONFIGID	✓
	BSL ピン構成	ピン構成を起動	BSLCONFIG0	✓
	UART インターフェイスの構成	ピン構成	BSLPINCFG0	✓
		ボーレートの設定	BSLCONFIG1	✓
	I2C インターフェイスの構成	ピン構成	BSLPINCFG1	✓
		ターゲット アドレス構成	I2C_SLAVE_ADDR	✓
	CAN インターフェイスの構成	ピン構成	BSLPINCFG2	✓
	BSL セキュリティの構成	BSL アクセス パスワード	PASSWORD_y	✓
		BSL 読み出し機能	BSLCONFIG0	
		BSL アラート構成	BSLCONFIG1	
		アプリの整合性チェック	APP_REV_POINTER	
	BSL チェックサム	CRC32-ISO3309	BSLCRC	✓
デバイス構成	顧客キー構成	キー カウント	KEY_COUNT	✓
		キー リビジョン	KEY_REV	
		セキュア ブートのアクティブ キー	MPUK_ACTIVE	
		DSSM のアクティブ キー	DSSM_ACTIVE	
	ライフサイクル管理	顧客コードがプロビジョニングされました	CODE_PROVISION	✓
		障害分析が有効です	FAILURE_ANALYSIS	
		廃止が有効です	DCOM	
	HSSE デバイスのハードウェアで保護されたフラッシュ セキュリティ構成	Bank0 メイン FLASH 書き込み消去保護	BANK0_WRITE_ERASE_PROTECTION_A BANK0_WRITE_ERASE_PROTECTION_B	✓
		Bank0 メイン FLASH セキュリティ保護	BANK0_SECURITY_PROTECTION_A BANK0_SECURITY_PROTECTION_B	✓
		Bank0 メイン FLASH 特権保護	BANK0_PRIVILEGE_PROTECTION_A BANK0_PRIVILEGE_PROTECTION_B	✓

Copyright © 2026 Texas Instruments Incorporated

表 2-2. NONMAIN 構成パラメータ (続き)

構成パラメータ			レジスタ フィールド	NONMAIN レイアウト タイプ
				A
デバイス構成	HSSE デバイスのハードウェアで保護されたフラッシュ セキュリティ構成	Bank1 メイン FLASH 書き込み消去保護	BANK1_WRITE_ERASE_PROTECTION_A BANK1_WRITE_ERASE_PROTECTION_B	✓
		Bank1 メイン FLASH セキュリティ保護	BANK1_SECURITY_PROTECTION_A BANK1_SECURITY_PROTECTION_B	✓
		Bank1 メイン FLASH 特権保護	BANK1_PRIVILEGE_PROTECTION_A BANK1_PRIVILEGE_PROTECTION_B	✓
		データ FLASH 書き込み消去保護	DBANK_WRITE_ERASE_PROTECTION	✓
		データ FLASH セキュア保護	DBANK_SECURITY_PROTECTION	✓
		データ FLASH 特権保護	DBANK_PRIVILEGE_PROTECTION	✓

注

NONMAIN レイアウトの種類によって、レジスタ アドレス オフセットが異なる可能性があります。詳細については、セクション 10 にリンクされている、デバイス固有のテクニカル リファレンス マニュアルを参照してください。

注

デバイス構成 (Device Config) は、MSPM33 がライフサイクルを維持するために使用する OTP 領域です。HSSE は MSPM33 のライフサイクル ステータスの 1 つです (他のステータスは HSKP、HSFS、HSFA)。詳細については、『MSPM33C セキュリティ ユーザーガイド』または『MSPM33 C3 シリーズ 160MHz マイコン テクニカル リファレンス マニュアル』を参照してください

2.3 NONMAIN メモリ

表 2-3 に、NONMAIN フラッシュの全体的なメモリ セクションを示します。レジスタ メモリ マップは、NONMAIN レイアウト タイプによって異なります。詳細については、セクション 10 にリンクされている、デバイス固有のテクニカル リファレンス マニュアルを参照してください。

表 2-3. NONMAIN メモリ マップ

NONMAIN セクション	開始アドレス	終了アドレス
デバイス構成 (OTP)	8010、1000h	8010、17FFh
BCR の構成	8010.1800h	8010.1BFFh
BSL の構成	8010.1C00h	8010.1FFFh

MSPM33 デバイスは、NONMAIN メモリ内に OTP 領域 (2KB) をプロビジョニングします。この領域には、以下の制限があります。

- この領域は決して消去できません (工場出荷時リセットや一括消去操作を含みます)。
- この領域は、HSFS、HSKP、HSSE、HSFA を含むすべてのライフサイクル ステータスで記述できます。

この OTP 領域には、ROM ブートで使用されるデバイス構成が含まれています。この構成は、MSPM33 キープロビジョニング、ライフサイクルの維持、HSSE デバイスのハードウェア保護されたセキュアおよび特権属性構成に関連しています。

Copyright © 2026 Texas Instruments Incorporated

また、未使用の OTP 領域にハードウェアベースの単調カウンタ機能を実装することもできます。このセクタは追記のみでプログラムされるため、この機能は実質的には不揮発性のアップカウンタ (ソフトウェアでの解釈によってはダウンカウンタ) として動作します。

デバイスが NONMAIN メモリ内の OTP 領域をサポートしているかどうかを確認するには、デバイス固有のデータシートを参照してください。

注

OTP 領域を消去して再プログラムすることはできません。定義された OTP 領域 (テキサス・インスツルメンツが定義したレジスタ) へのプログラミングが誤っていると、顧客のキー、ライフサイクルのメンテナンス、フラッシュのセキュアおよび特権属性に回復不可能な誤った設定が発生し、マイコンのロックにつながる可能性があります。

Copyright © 2026 Texas Instruments Incorporated

3 NONMAIN 構成

このセクションでは、BCR 構成と BSL 構成を含む、NONMAIN 構成について詳しく説明します。

3.1 BCR の構成

ブート構成ルーチン (BCR) は、BOOTRST の後でデバイス上で実行される最初のファームウェアです。ユーザーは、ブートのスタートアップ段階でデバイスにさまざまなプロパティを設定できます。

テキサス・インスツルメンツでは、SysConfig ツールを使用して BCR 構成をカスタマイズすることを推奨しています。詳細については、『SysConfig を使用した BCR の構成』を参照してください。

3.1.1 BCR の構成 ID

TI は、さまざまなタイプの NONMAIN レイアウト向けにデフォルトの BCR 構成 ID を定義しています。ユーザーは、アプリケーション用途に応じて構成 ID を上書きできます。デフォルトの BCR 構成 ID を復元回復するには、工場出荷時リセットを実行します。

表 3-1 に、各デバイスのデフォルト値を示します。

表 3-1. デフォルトの BCR 構成 ID

NONMAIN レイアウト タイプ	デバイス ファミリ	デフォルト値
タイプ A	MSPM33C321A	0x05000000

3.1.2 SWD (シリアル ワイヤ デバッグ) ポリシー

シリアル ワイヤ デバッグ (SWD) 関連のポリシーは、デバイスの物理的デバッグ インターフェイスで使用可能な機能を構成します。MSPM33 デバイスは、制限なし、カスタム制限、完全制限という 3 つの汎用セキュリティ シナリオをサポートしています。表 3-2 に、各レベルの違いを含め、最も制限の少ないものから最も制限の厳しいものの順に、3 つの汎用セキュリティ シナリオを示します。

表 3-2. 汎用セキュリティ レベル

シナリオ	SW-DP アクセスポリシー	アプリケーション デバッグ ポリシー	一括消去ポリシー	工場出荷時のリセット ポリシー
制限なし	EN	L0 – フル アクセス	EN	EN
カスタム制限	EN	L0 – フル アクセス L1 - PW 付き EN セキュア、EN 非セキュア L2 - PW 付き EN セキュア、PW 付き EN 非セキュア DIS - 無効	イネーブル、パスワードでイネーブル、ディセーブル	イネーブル、パスワードでイネーブル、ディセーブル
完全制限	DIS	無関係(1) (SW-DP が無効な場合はアクセス不可)		

(1) SW-DP ポリシーが「SW-DP ディスエーブル」の場合、SWD インターフェイスの観点からは、一括消去と工場出荷時リセットのポリシーは関係ありません。ただし、ブートストラップ ローダ (BSL) がイネーブルになっている場合、一括消去および工場出荷時リセットのポリシーは、利用可能な BSL 機能に影響を及ぼします。BSL のセキュリティ保護の詳細については、BSL セキュリティのセクション (セクション 3.2.4) を参照してください。

デフォルトでは、TI は無制限の状態で MSPM33 を提供します。この無制限の状態により、製造時のプログラミング、評価、開発が容易になります。ただし、この無制限の状態では、大きな攻撃対象領域が存在したままになるため、量産では推奨されません。

保護の必要性を判断する際、考慮すべき SWD インターフェイスの主な用途は 3 つあります。

- アプリケーション デバッグ アクセス: IDE ツールでのデバッグ
- 一括消去アクセス: MAIN メモリ領域を消去
- 工場出荷時リセットへのアクセス: MAIN メモリ領域を消去し、NONMAIN デバイス構成メモリをテキサス・インスツルメンツの工場出荷時デフォルト (制限なし) にリセット

Copyright © 2026 Texas Instruments Incorporated

SWD セキュリティ ポリシーは、NONMAIN メモリ内の 16 ビット パターン一致フィールドとして実装され、以下の特徴があります。

- より低いセキュリティ状態をイネーブルにするにはパターンが正確に一致することが必要
- 16 ビット フィールドのいずれかの値が定義されたパターンに正確に一致しない場合、対応するパラメータが最大のセキュア状態になる

また、SWD は 8 セットのパスワード (合計 128 ビット) のカスタマイズもサポートしており、デバッグ サブシステム メールボックス (DSSM) コマンドを使用してデバイスのロックを解除するために使用できます。詳細な手順については、『MSPM0 用ハードウェア プログラミングおよびデバッガ ガイド』アプリケーション ノートを参照してください。

3.1.2.1 アクセス ポリシー

BCR は、デバイスを最大制限状態に設定する BOOTCFG0.SWDP_MODE フィールドによる SWD アクセス ポリシーの変更をサポートしています。

このフィールドがディセーブル (SW-DP がディセーブル) の場合、物理デバッグポート (SW-DP) は完全にディセーブルになり、SWD でアクセス可能なすべての機能 (アプリケーションのデバッグ、一括消去、工場出荷時リセット) には、個別の構成に関係なく、SWD からアクセスできません。

BSL がイネーブルの場合は、BSL インターフェイスから送信される一括消去または出荷時リセットのコマンドを認証するため、BSL は引き続き一括消去および工場出荷時リセットの構成フィールドを使用します。詳しくは、セクション 3.2 を参照してください。

3.1.2.2 デバッグ ポリシー

SWD アクセス ポリシーをイネーブルのままにすると、ユーザーは BOOTCFG0.DEBUGACCESS フィールドを使用して SWD デバッグ ポリシーをさらに変更できます。

MSPM33 は、4 段階の SWD アクセス ポリシー (フル アクセス、すべてディセーブル、128 ビットパスワードによるセキュア デバッグでの暗号化、2 つの 128 ビット パスワードによるセキュア デバッグおよび非セキュア デバッグでの暗号化) をサポートしています。MSPM33 は、セキュア デバッグと非セキュア デバッグに異なるパスワードを適用できます。デバイスは、ブート段階でのみパスワードを検証します。ユーザは、SWD インターフェイスのロックを解除するためのリセット動作を含むパスワード認証用の DSSM コマンドを生成します。

MSPM33 は、SHA2-256 ダイジェストでパスワードを保存できます。SHA2-256 ダイジェスト ストレージ パターンでは、128 ビットのパスワードが NONMAIN メモリ領域に直接保存されることはありません。代わりに、ユーザーは 128 ビットのパスワードから 256 ビットのハッシュ値を生成し、ハッシュ値を NONMAIN 領域に格納して、パスワード ストレージのセキュリティを強化します。このハッシュ値は、DEBUG_LOCK フィールドと DEBUG_NS_LOCK フィールドに保存されます。

以下は、ユーザーが SHA2-256 ダイジェスト パスワードを生成して設定する方法です。

1. SWD インターフェイスのロックを解除する 128 ビットパスワードを決定します。4 つの 32 ビット パスワードを形成するために、パスワードを 32 ビット アライメントに設定します。
2. SHA が 8 ビットのアドレス指定形式を使用するため、4 つの 32 ビットパスワード エンディアンを反転します。
3. ハッシュ値を計算するときは、反転された 4 つの 32 ビット パスワードを 1 つの文字列として結合します。
4. 入力文字列の SHA256 値を計算します。
5. 出力された SHA256 値を、8 つの 32 ビット ワードに分割します。
6. SHA2-256 計算では 8 ビットのアドレス指定形式を使用するため、8 つの 32 ビット ワードの出力のエンディアンを反転します。
7. 反転したパスワードを、DEBUG_LOCK フィールドまたは DEBUG_NS_LOCK フィールドに順番に保存します。

注

パスワードの *0* の値は重要です。計算中に *0* の値を削除しないでください。

このフローは、次のような 256 ビット SHA2-256 ダイジェストパスワード生成をサポートするすべてのデバイスに対して設計されています。

- SWD アクセスを実現

Copyright © 2026 Texas Instruments Incorporated

- 工場出荷時リセット
- 一括消去
- 不正なデバイス変換
- BSL アクセス (256 ビットのパスワード)

セクション 4.2 に、SysConfig ツールを使用してパスワードを設定する方法を示します。セクション 6.3 に、CCS ツールを使用してデバイスのロックを解除する方法を示します。

3.1.2.2.1 SHA2-256 パスワードの例

以下は、ユーザーが 128 ビットパスワードを *0123456789ABCDEF67452301EFCDAB89* に設定した場合の SHA2-256 ダイジェストパスワードの計算例です。

1. パスワードを 32 ビット アライメント (0x01234567、0x89ABCDEF、0x67452301、0xEFCDAB89) に設定します
2. SHA2-256 の計算はバイト単位で行われるため、パスワードのエンディアンを反転させます:0x67452301、0xEFCDAB89、0x01234567、0x89ABCDEF
3. 反転された 4 つの 32 ビット パスワードを 1 つの文字列として結合します:
   67452301EFCDAB890123456789ABCDEF
4. SHA2-256 の値を計算します (入力エンコードとして 16 進数を選択):
   8420347FCB0F019E15564A0F65B8E197ECDF9F92D1ECA2BBAB1B8CB314C763DA (SHA256 オンライン ツール)
5. SHA2-256 値を 8 つの 32 ビットワード に分割します:0x8420347F、0xCB0F019E、0x15564A0F、0x65B8E197、0xECDF9F92、0xD1ECA2BB、0xAB1B8CB3、0x14C763DA
6. 出力エンディアンを反転させます:0x7F342084、0x9E010FCB、0x0F4A5615、0x97E1B865、0x929FDFEC、0xBBA2ECD1、0xB38C1BAB、0xDA63C714
7. 8 つの 32 ビット パスワードを、DEBUG_LOCK フィールドまたは DEBUG_NS_LOCK フィールドに順に保存します

3.1.2.3 一括消去と工場出荷時リセット ポリシー動作

SWD 一括消去は、MAIN フラッシュ領域のみの消去であり、ここには通常はユーザー アプリケーションが格納されています。NONMAIN フラッシュ領域に格納された BCR および BSL ポリシーは、一括消去の影響を受けません。一括消去は、デバイスの NONMAIN 構成を残しながら、すべてのアプリケーション コードとデータを消去する場合に便利です。

SWD 工場出荷時リセットでは、MAIN フラッシュ領域の消去と、NONMAIN フラッシュ領域のデフォルト値へのリセットを行います。このような消去は、アプリケーション コードとデータを消去するだけでなく、BCR および BSL デバイスのブート ポリシーを完全にリセットする場合に便利です。

BCR 構成は、DSSM を使用して、デバッグ プローブから SWD インターフェイス経由でデバイスに送信されるコマンドにより、一括消去および工場出荷時リセット機能を提供します。これらのコマンドは、SWD が完全に制限されている場合は利用できません (SW-DP が無効)。デバイスが、完全に制限された SW-DP 無効状態に設定されていない場合、一括消去および工場出荷時リセットのコマンドに対して、「有効」、「固有の 128 ビット パスワードで有効」、または「無効」の 3 つの構成状態を選択できます。

注

「工場出荷時リセット」または「一括消去」が個別に無効に設定されている場合、BSL は工場出荷時リセット コマンドまたは一括消去コマンドを実行できません。

サポートされている 128 ビットのパスワード保存パターン (SHA2-256) については、デバイス固有のデータシートを参照してください。SHA2-256 ダイジェスト パスワードの計算手順についてはセクション 3.1.2.2 を、SWD 一括消去または工場出荷時リセットを生成するフローについてはセクション 8.2 を参照してください。

3.1.3 フラッシュ セキュリティの構成

フラッシュ セキュリティの構成ポリシーでは、変更されないようにロックするフラッシュ メモリのセクタ、セキュリティ保護に設定されるセクタ、権限保護に設定されるセクタを指定します。保護には、静的書き込み消去保護、セキュリティ保護、および特権保護の 3 種類があります。

Copyright © 2026 Texas Instruments Incorporated

静的書き込み消去保護は、MAIN フラッシュ メモリ、DATA フラッシュ メモリ、NONMAIN フラッシュ メモリに適用できます。静的書き込み保護により、次の特性を持つ固定のユーザー定義アプリケーション、データ、または NONMAIN 構成をフラッシュ メモリに配置できるようになります。

1. 一度プログラムされてロックされると、ロックされたセクタはアプリケーション コードや ROM ブートローダーによって変更することはできません。
2. アプリケーションがフラッシュ メモリの先頭に配置されている場合、ROM ブート構成ルーチンが実行をユーザー アプリケーションに移した際に、このアプリケーションが最初に実行されるコードになります。

注

DSSM コマンドによって一括消去または工場出荷時リセットが生成されると、このコマンドは指定された静的書き込み保護ポリシーよりも優先されます。これに対して、BSL コマンドはオーバーライドを生成せず、対応する保護されたフラッシュ領域は変更されません。

セキュリティ保護と特権保護は、MAIN フラッシュ メモリとデータ フラッシュ メモリにのみ適用できます。セキュリティ保護は、保護領域の範囲を定義します。セキュア領域内のすべてのコードおよびデータは、非セキュア領域から保護されます。特権保護は、特権領域の範囲を定義します。特権領域内のすべてのコードおよびデータは、非特権領域から保護されます。

注

MSPM33 上のセキュアおよび非セキュア パーティションの場合、final secure 属性は GSC 構成だけでなく SAU および IDAU の設定にも依存します。詳細な構成については、『MSPM33 マイコンにおけるセキュア アプリケーション用 Trustzone のイネーブル』を参照してください。

3.1.3.1 MAIN フラッシュ セキュリティの構成

バンク 0 の静的書き込み保護の場合、BANK0_WRITE_ERASE_PROTECTION_A および BANK0_WRITE_ERASE_PROTECTION_B フィールドは 512KB のメモリ全体を保護します。値 *0* は、対応するセクタに書き込み保護が適用されることを示します。BANK0_WRITE_ERASE_PROTECTION_A の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。BANK0_WRITE_ERASE_PROTECTION_B の場合、1 ビットはフラッシュ メモリ (16KB) の 8 セクタを表します。

バンク 1 の静的書き込み保護の場合、BANK1_WRITE_ERASE_PROTECTION_A および BANK1_WRITE_ERASE_PROTECTION_B フィールドは 512KB のメモリ全体を保護します。値 *0* は、対応するセクタに書き込み保護が適用されることを示します。BANK1_WRITE_ERASE_PROTECTION_A の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。BANK1_WRITE_ERASE_PROTECTION_B の場合、1 ビットはフラッシュ メモリ (16KB) の 8 セクタを表します。

バンク 0 のセキュリティ保護のため、BANK0_SECURITY_PROTECTION_A および BANK0_SECURITY_PROTECTION_B フィールドでは、512KB メモリ全体のセキュア領域が定義されています。値 *0* は、対応するセクタがセキュアであることを示します。BANK0_SECURITY_PROTECTION_A の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。BANK0_SECURITY_PROTECTION_B の場合、1 ビットはフラッシュ メモリ (16KB) の 8 セクタを表します。

バンク 1 のセキュリティ保護のため、BANK1_SECURITY_PROTECTION_A および BANK1_SECURITY_PROTECTION_B フィールドでは、512KB メモリ全体のセキュア領域が定義されています。値 *0* は、対応するセクタがセキュアであることを示します。BANK1_SECURITY_PROTECTION_A の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。BANK1_SECURITY_PROTECTION_B の場合、1 ビットはフラッシュ メモリ (16KB) の 8 セクタを表します。

バンク 0 の特権保護のため、BANK0_PRIVILEGE_PROTECTION_A および BANK0_PRIVILEGE_PROTECTION_B フィールドでは、512KB メモリ全体の特権領域が定義されています。値 *0* 値は、対応するセクタが特権を持つことを示します。BANK0_PRIVILEGE_PROTECTION_A の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。BANK0_PRIVILEGE_PROTECTION_B の場合、1 ビットはフラッシュ メモリ (16KB) の 8 セクタを表します。

Copyright © 2026 Texas Instruments Incorporated

バンク 1 の特権保護のため、BANK1_PRIVILEGE_PROTECTION_A フィールドと BANK1_PRIVILEGE_PROTECTION_B フィールドでは、512KB メモリ全体の特権領域が定義されています。値 *0* 値は、対応するセクタが特権を持つことを示します。BANK1_PRIVILEGE_PROTECTION_A の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。BANK1_PRIVILEGE_PROTECTION_B の場合、1 ビットはフラッシュ メモリ (16KB) の 8 セクタを表します。

3.1.3.2 DATA フラッシュ セキュリティの構成

データ フラッシュの静的書き込み保護のため、DBANK_WRITE_ERASE_PROTECTION フィールドは、データ バンク メモリ全体を保護します。値 *0* は、対応するセクタに書き込み保護が適用されることを示します。DBANK_WRITE_ERASE_PROTECTION の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。

データ フラッシュのセキュリティ保護のため、DBANK_SECURITY_PROTECTION フィールドでは、データ バンク メモリ全体のセキュア領域が定義されています。値 *0* は、対応するセクタがセキュアであることを示します。DBANK_SECURITY_PROTECTION の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。

データ フラッシュの特権保護のため、DBANK_PRIVILEGE_PROTECTION フィールドは、データ バンク メモリ全体の特権領域が定義されています。値 *0* 値は、対応するセクタが特権を持つことを示します。DBANK_PRIVILEGE_PROTECTION の場合、1 ビットはフラッシュ メモリ (2KB) の 1 セクタを表します。

3.1.3.3 NONMAIN フラッシュ静的書き込み保護

NONMAIN 領域に静的書き込み消去保護を適用するように BANK0_NM_USER_CONFIG を構成すると、NONMAIN 領域全体が書き込みロックされます。このロックは、ブート構成ルーチンがブートストラップ ローダまたは MAIN フラッシュ内のユーザー アプリケーション コードのいずれかに実行を移行する場合、当該リージョンを機能的に変更不可能な状態にします。NONMAIN リージョンをアプリケーション コードまたはブートストラップ ローダでプログラムまたは消去しようとすると、ハードウェア フラッシュ動作エラーが発生し、セクタは変更されません。

3.1.4 ブート時の SYSPLL 構成

デフォルト構成では、ROM ブートは 32MHz MCLK を使用して実行され、SYSOSC をソースとし、SYSPLL はありません。ブート プロセスを高速化するため、ユーザーはクロック ソースだけでなく SYSPLL も構成できます。ユーザーは、次の設定を構成できます。

- SYSPLL 事前分周器 (PDIV) および SYSPLL 帰還分周器 (QDIV)
- クロックソースの選択 - SYSOSC (32MHz) または HFXT (20MHz または 40MHz)

NONMAIN フラッシュ メモリの BOOTCLK0 および BOOTCLK1 フィールドを使用して SYSPLL 構成を設定します。

3.1.5 カスタマ セキュア コード (CSC)

カスタマ セキュア コード (CSC) は、テキサス・インスツルメンツのブート コードの後に実行されるコードです。CSC はフラッシュ メモリから実行され、追加のセキュリティ要素を設定します。CSC は顧客が所有するセキュア ソフトウェアであり、CSC が 0x0 アドレスにあることを確認する必要があります。図 3-1 に、CSC 実行の概略フローを示します。

Copyright © 2026 Texas Instruments Incorporated

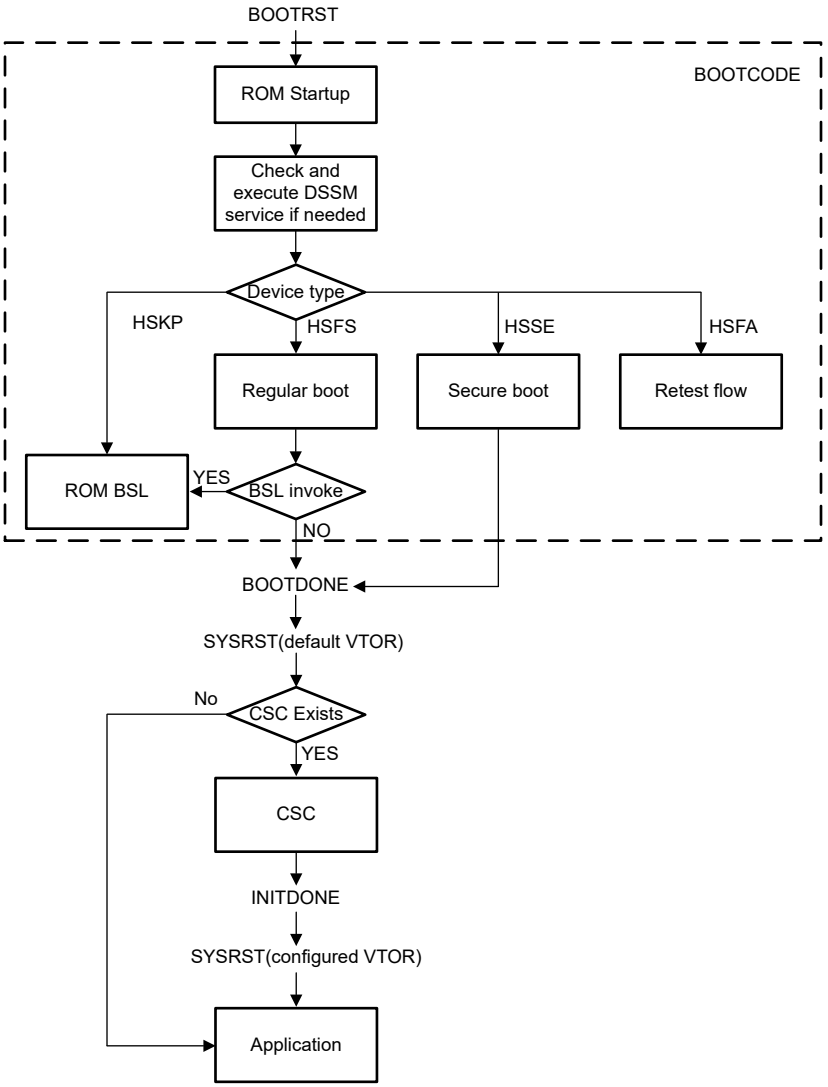


図 3-1. セキュア ブートとスタート シーケンス

テキサス・インスツルメンツのセキュリティ モデルの概念では、TI のブートコードと CSC の両方が信頼の対象となります。CSC を信頼するために、TI では、デバッグ ホールドとフラッシュ メモリの静的書き込み保護をイネーブルにすることを推奨しています。CSC への実装については、『MSPM33 マイコンにおける顧客セキュア コードの評価』を参照してください

注

フロー内では、デバイス タイプ HSKP、HSFS、HSSE、HSFA が MSPM33 デバイスのライフサイクル ステータスです。詳細については、『MSPM33C セキュリティ ユーザーガイド』または『MSPM33 C3 シリーズ 160MHz マイコン テクニカル リファレンス マニュアル』を参照してください

3.1.5.1 CSC ポリシー

デフォルトでは、CSC は無効になっています。ユーザーは、BOOTCFG2.CSCEXISTS フィールドを使用して CSC を有効にします。CSC の実行が完了すると、システムは構成済みの VTOR を用いて 2 番目の SYSRST を実行し、その後メイン アプリケーションが起動します。

Copyright © 2026 Texas Instruments Incorporated

3.1.5.2 フラッシュ バンク スワップ方針

複数のバンク デバイスでは、バンク スワップはデフォルトでディスエーブルになっています。

ユーザーは、BOOTCFG2.FLASHBANKSWAPPOLICY フィールドを使用してバンク スワップをイネーブルできます。ブート コードはこの構成を読み出し、適切なキー (0xCA) を使って SYSCTL.SECCFG.FLBANKSWPPOLICY に書き込みます。ハードウェアのデフォルトでは、スワップ可能な設定はイネーブルになり、下位バンクは論理バンク 0 として使用されます。BOOTCFG2.FLASHBANKSWAPPOLICY フィールドのデフォルト値は、バンク スワップ ポリシーをディスエーブルにします。

バンク スワップの動作は CSC ステージで発生し、デバイスが INITDONE を発行した後の動作は有効になります。CSC は、どのバンクを論理バンク 0 として決定するかを決めるため、適切なキー (0x58) を使用して SYSCTL.SECCFG.FLBANKSWP に書き込みます。

1. 下位バンクが論理バンク 0 の場合、下位バンクと上位バンクのアドレスは変更されません。
2. 上位バンクが論理バンク 0 の場合、下位バンクと上位バンクのアドレスが交換されます。

このメカニズムは、INITDOWN を発行した後のポリシーを適用します。一般に、実行バンクは論理バンク 0 (下位アドレス) で、ファームウェア更新のための保存場所を論理バンク 1 (上位アドレス) にします。

注

上位バンクを論理バンク 0 としてバンク スワップすると、アドレスのみがスワップされます。下位バンクおよび上位バンクのデータは転送されません。

注

バンク スワップが有効かどうかにかかわらず、複数のバンクは、異なるメモリ アドレスで同じプロパティ (書き込み、読み取り、実行) を持ちます。

バンク スワップ機能の詳細については、『MSPM33 マイコンにおける顧客のセキュア コードの評価』を参照してください。

3.1.5.3 デバッグ ホールド

CSC 機能をサポートするデバイスでは、BCR 構成により、CSC 実行中に SWD インターフェイスをロックできます。CSC の末尾で INITDOWN が発行されるまで、デバイスはデバッグ アクセスを解放しません。

デバッグ ホールド機能はデフォルトでディスエーブルになっています。テキサス・インスツルメンツでは、アプリケーションのデバッグ中はこの機能をディセーブルにしておくことを推奨しています。CSC がイネーブルになって製品が量産段に入る場合、BOOTCFG1.DEBUGHOLD フィールドを使用してデバッグホールドをイネーブルにして、CSC をアクセス不可能な状態に保護することを推奨します。

3.1.6 高速ブート モード

高速ブート モードを有効にすることで、BCR の実行時間を短縮できます。高速ブート モードでは、次の方法でブート プロセスが高速化されます。

- BSL エントリを制限：高速ブート モードをイネーブルにすることで、SYSCTL レジスタを用いた呼び出しメソッドと DSSM を用いた呼び出しメソッドのみを使用してブートローダーに移行します。
- アプリケーションのダイジェスト チェックが有効になっている場合でも、そのチェックをバイパスします。詳細については、セクション 3.1.7 を参照してください。

NONMAIN フラッシュメモリの BOOTCFG3.FASTBOOTMODE フィールドを使用して、高速ブート モードをイネーブルに設定します。

3.1.7 アプリケーションのダイジェスト チェック

BCR は、ユーザー アプリケーションを開始する前のブート プロセス中に、MAIN フラッシュ領域に含まれるアプリケーション コードおよびデータの完全な CRC32 または SHA2-256 整合性チェックを実行できます。アプリケーションのダイジェスト チェックは、アプリケーション コードとデータを実行する前に、一部またはすべての整合性を確認するのに役立ちます。

Copyright © 2026 Texas Instruments Incorporated

アプリケーションのダイジェスト チェックを有効にするには、次の手順を実行します。

1. アプリケーションの ダイジェスト チェック ポリシーを選択します。このポリシーは、CRC32 または SHA2-256 (SECURE_BOOT_MODE フィールド) として設定できます。
2. アプリケーションのダイジェスト チェックの 32 ビット開始アドレス (USER_SECURE_APP_START_ADDR フィールド) を設定します。
3. CRC または SHA ダイジェスト チェックが適用されるアプリケーションの長さ (バイトで指定) (USER_SECURE_APP_LENGTH フィールド) を設定します。
4. 特定のデータ (バイトで指定) を使用して、CRC32 または SHA2-256 の値を計算します。
5. 事前計算された CRC32 または SHA2-256 の値を 32 ビット形式に分割し、その値を BCR 構成 (USER_SECURE_APP_HASH_y フィールド) に保存します。

ブート時にアプリケーションのダイジェスト チェックが失敗した場合、MAIN フラッシュ内のアプリケーションは開始されません。BSL が有効である場合、BSL が起動します。BSL が有効でない場合、ブートは失敗します。

3.1.7.1 CRC32 ダイジェスト チェックの例

図 3-2 は、ユーザーが開始アドレスを 0x0001.0000、長さを 8 バイトに設定した場合の、CRC32 整合性チェックの計算例です。アプリケーションデータはセクション 3.1.7 を参照します。

	32-bit Hex	*8-bit Hex*
0x0001.000 :	0x01234567	67 45 23 01
0x0001.004 :	0x89ABCDEF	EF CD AB 89

図 3-2. CRC32 ダイジェスト チェックのサンプル データ

計算モデルとして *JAMCRC* を選択し、CRC32 の出力値を取得します。*JAMCRC* CRC モデルには逆入出力ビットがあり、0x04C11DB7 の多項式 (初期値 0xFFFFFFFF、出力 XOR 値 0x00000000) を使用します。

以下の手順に従って、CRC32 値の例を計算します。

1. アプリケーション ダイジェストの確認ポリシーとして、「CRC による確認」(SECURE_BOOT_MODE = Abhor) を選択します。
2. アプリケーション ダイジェスト チェックの 32 ビット開始アドレスを設定します (USER_SECURE_APP_START_ADDR = 0001.0000h)。
3. CRC ダイジェストチェックが適用されるアプリケーションの長さ (バイトで指定) を設定します (USER_SECURE_APP_LENGTH = 8h)。
4. 指定された入力を使用して、CRC32 出力を計算します。
   a. CRC32 は次の 8 ビット形式を使用して計算されるため、入力されたデータ エンディアンを反転させます:67、45、23、01、EF、CD、AB、89。
   b. 入力された 8 ビット データを 1 つのストリングとして結合します:67452301EFCDAB89。
   c. CRC32 値を計算します (入力エンコードに *HEX* を選択、モデルに *JAMCRC* を選択):0x24648719 (CRC32 オンライン ツール)。
5. CRC32 出力値を BCR 構成 (USER_SECURE_APP_HASH_1 = 2464.8719h) に登録します。USER_SECURE_APP_HASH_y レジスタが複数ある場合、CRC32 にはダイジェストの最初の 32 ビット ワードのみが使用されます。

注

アプリケーション CRC32 ダイジェスト チェックの長さが偶数であることを確認します。

Copyright © 2026 Texas Instruments Incorporated

3.1.7.2 SHA2-256 ダイジェスト チェックの例

図 3-3 は、ユーザーが開始アドレスを 0x0001.0000、長さを 8 バイトに設定した場合の、SHA2-256 整合性チェックの計算例です。図 3-3 にアプリケーション データの例を示します。

	32-bit Hex	*8-bit Hex*
0x0001.000 :	0x01234567	67 45 23 01
0x0001.004 :	0x89ABCDEF	EF CD AB 89

図 3-3. SHA2-256 ダイジェスト チェックのサンプル データ

以下の手順に従って、SHA2-256 値の例を計算します。

1. アプリケーション ダイジェスト チェック ポリシーとして SHA2-256 (SECURE_BOOT_MODE = CCDDh) を選択します。
2. アプリケーション ダイジェスト チェックの 32 ビット開始アドレスを設定します (USER_SECURE_APP_START_ADDR = 0001.0000h)。
3. SHA2-256 ダイジェスト チェックが適用されるアプリケーションの長さ (バイトで指定) を設定します (USER_SECURE_APP_LENGTH = 8h)。
4. 指定された入力を使用して、SHA2-256 出力を計算します。
   a. SHA2-256 の計算はバイト単位で行われるため、入力された 32 ビット データのエンディアンを反転させます: 67、45、23、01、EF、CD、AB、89。
   b. 入力された 8 ビット データを 1 つのストリングとして結合します:67452301EFCDAB89。
   c. SHA2-256 の値を計算します (入力エンコードとして 16 進数を選択)。FDD232547CEEE35ADD35783CA7D518D2A49ABCCD0B60B028C8A9C629EBA6201F (SHA2-256 オンライン ツール)。
   d. SHA2-256 の値を 8 つの 32 ビット ワードに分割します:0xFDD23254、0x7CEEE35A、0xDD35783C、0xA7D518D2、0xA49ABCCD、0x0B60B028、0xC8A9C629、0xEBA6201F。
5. 32 ビットの出力ワード エンディアンを反転させます:0x5432D2FD、0x5AE3EE7C、0x3C7835DD、0xD218D5A7、0xCDBC9AA4、0x28B0600B、0x29C6A9C8、0x1F20A6EB。
6. 8 つの 32 ビット SHA2-256 チェックサムを USER_SECURE_APP_HASH_y フィールドに次の順序で保存します。

3.1.8 BSL ポリシー

ROM BSL をサポートするデバイスでは、テキサス・インスツルメンツは BSL インターフェイスを介してデバイス メモリへのアクセス機能を提供しています。デフォルトの BSL 起動ピンは、BSL のハードウェア起動に使用されます。詳細については、セクション 3.2.2 を参照してください。

ユーザーは、BOOTCFG3.BOOTLOADER_MODE フィールドを使用して BSL を無効化できます。このフィールドでは、BSL モードは完全に無効化させます。(SYSRST 経由) BSL ソフトウェア起動もブロックされます。

または、BOOTCFG1.BSL_PIN_INVOKE フィールドを使用して BSL 起動ピンチェックを無効化すると、BSL ハードウェア エントリがブロックされます。起動ピン チェックを無効化した後、デバイスはブート時に呼び出しピンのステータスをチェックしないため、BSL ハードウェア エントリが無効化されます。ユーザーは、アプリケーション コードのソフトウェア呼び出しメソッドを使用して BSL を入力できます。

3.1.9 BCR チェックサム

MSPM33 デバイスは、ブート段階の間に BCR 構成データの CRC チェックを行います。デバイスが CRC32-ISO3309 をサポートしている場合、32 ビットの CRC ダイジェストが適用されます。

CRC 計算用の構成を以下に示します。

Copyright © 2026 Texas Instruments Incorporated

- 事前に選択された CRC 規格 (CRC32-ISO3309) を持つ多項式を選択します
- 入力値と出力値を反映します
- 初期値は 0xFFFFFFFF (または 0xFFFF) に設定されます
- 最終的な XOR 値は 0x00000000 (または 0x0000) に設定されます

テキサス・インスツルメンツでは、SysConfig ツールを使用して BCR チェックサムを自動的に計算することを推奨しています。詳細については、セクション 4.2 を参照してください。

3.1.9.1 CRC チェック エラーの処理

呼び出し中に BCR 構成データの CRC チェックがエラーとなった場合、致命的なブート エラーが発生し、以下の制限が課されます。

- このエラーの原因をブート診断として CFG-AP に記録
- BSL がイネーブルに設定されていても BSL は起動しない
- ユーザー アプリケーションを開始しない
- アプリケーションのデバッグ アクセスはすべてディセーブル
- 保留中の SWD 工場出荷時リセット コマンドがイネーブルの場合、またはパスワードを使用してイネーブルになった場合は、それを実行
- 保留中の テキサス・インスツルメンツ故障解析フロー エントリがイネーブルの場合は適用
- ブート プロセスを最大 3 回再試行
  - 2 回目または 3 回目の試行で成功した場合、デバイスを通常どおり起動
  - 3 回目の試行に失敗した場合、次に BOR または POR が実行されるまで、それ以上のブート試行は許可しない

3.2 BSL の構成

ブートストラップ ローダ (BSL) ルーチンは、デバイスのメモリにデータをロードするために使用される ROM ベースのファームウェアです。ユーザーは、NONMAIN 領域の BSL 構成を使用して、BSL のエントリと実行にさまざまなプロパティを設定します。

TI は、BSL の設定をカスタマイズする際に、SysConfig ツールを使用することを推奨しています。詳細についてはセクション 4.3 をご確認ください。

3.2.1 BSL の構成 ID

TI は、異なる NONMAIN レイアウト向けにデフォルトの BSL 構成 ID を定義しています。ユーザーは、アプリケーション用途に応じて BSL ID を上書きできます。デフォルトの BSL 構成 ID を復元回復するには、工場出荷時リセットを実行します。

デフォルトの BSL 構成 ID に、各デバイスのデフォルト値を示します。

表 3-3. デフォルトの BSL 構成 ID

NONMAIN レイアウト タイプ	デバイス ファミリ	デフォルト値
タイプ A	MSPM33C321A	0x05000000

3.2.2 ピン構成を起動

ブートローダーは、GPIO を使用した BOOTRST 後のハードウェア起動をサポートしています。TI のデバイスは、特定の GPIO と極性で構成されています。デフォルトの起動ピン割り当てについては、デバイス固有のデータシートを参照してください。

ユーザーは、BSLCONFIG0 フィールドを使用して、デフォルトの呼び出しピンを変更します。起動ピンの設定には、以下のものが含まれます。

- パッド
- ポート
- ピン
- 極性

Copyright © 2026 Texas Instruments Incorporated

回路図設計のデフォルトの起動ピンの初期ステータスが、起動ピン構成と一致している場合、デバイスは電源投入後に BSL へ移行し、アプリケーションコードが実行されることはありません。

3.2.3 ROM ベースの通信インターフェイス

MSPM33 は、構成可能な I2C、UART、またはシリアルワイヤ BSL インターフェイスとして CAN をサポートしています。ROM ベースの BSL では、UART、I2C、または CAN のピンをカスタマイズできますが、通信インターフェースのインスタンス (例えば UC0 から UC1) を含めることはできません。UART、I2C、CAN のピンのいずれかをカスタマイズできます。デフォルトのピン割り当てについては、デバイス固有のデータシートを参照してください。

USB インターフェイスを備えたデバイスの場合、ROM ベースのインターフェイスはさらにデバイス ファームウェア アップグレード (DFU) オプションもサポートしています。

3.2.3.1 UART インターフェイス

ROM BSL をサポートするデバイスでは、UART インターフェイスを使用できます。BSL の構成では、BSLPINCFG0 フィールドを使用して UART ピン (pad および MUX) の構成を変更することができます。UART インスタンスが変更されないため、デバイス ピンの属性プロパティによって、使用可能なピンが制限されます。使用可能なピンについては、デバイス固有のデータシートを参照してください。

UART のデフォルトのボーレートは 9600 です。BSL コマンドで UART 通信ボーレートを動的に変更できます (コマンドは 9600 ボーレートで送信されます)。さらに、NONMAIN 領域のレイアウトは、BSLCONFIG1.UART_BAUD_RATE フィールドによって変更されるデフォルトのボーレートに対応しています。

3.2.3.2 I2C インターフェイス

ROM BSL をサポートするデバイスでは、I2C インターフェイスを使用できます。BSL の構成では、BSLPINCFG1 フィールドを使用して I2C ピン (pad および MUX) の構成を変更することができます。デバイス ピンの属性プロパティは、特定の I2C インスタンスで使用可能なピンを制限します。使用可能なピンについては、デバイス固有のデータシートを参照してください。

I2C のデフォルトのターゲット アドレスは 0x48 です。MSPM33 は、I2C_SLAVE_ADDR フィールドを介して、ターゲット アドレスの変更をサポートしています。最大 7 ビットのターゲット アドレスに対応しています。

3.2.3.3 CAN インターフェイス

ROM BSL をサポートするデバイスでは、CAN インターフェイスを使用できます。BSL の構成では、BSLPINCFG2 フィールドを使用して CAN ピン (pad および MUX) の構成を変更することができます。デバイス ピンの属性プロパティは、特定の CAN インスタンスで使用可能なピンを制限します。使用可能なピンについては、デバイス固有のデータシートを参照してください。

デフォルト モードは、1Mbps (公称値とデータ) の CAN-FD です。デフォルトのサンプリング ポイントは 80% です。使用可能な MCAN プロトコル ID は 0x3 または 0x5 です。

BSL UART、I2C、CAN インターフェイスの詳細については、『MSPM33 ブートローダー ユーザー ガイド』を参照してください。

3.2.4 BSL セキュリティの構成

BSL コアは、潜在的な攻撃を防止するためのさまざまなセキュリティ機能を備えています。

- アクセス パスワード
- 読み出し
- Alert
- アプリケーションの整合性チェック

セキュリティ機能は、ROM BSL で常に有効になります。

3.2.4.1 アクセス パスワード

ユーザー指定のパスワードにより、ROM BSL アクセスが保護されます。パスワードは PASSWORD_y フィールドにあります。BSL アクセスのパスワードをディセーブルするオプションはありません。

Copyright © 2026 Texas Instruments Incorporated

正しいパスワードを BSL コアに送信して BSL のロックを解除する前は、BSL のほとんどの機能にアクセスすることはできません。詳細については、『MSPM33 ブートローダー (BSL) ユーザー ガイド』を参照してください。BSL に誤ったパスワードを供給すると、BSL は 2 秒間停止します。その後、正しいパスワードを再送信してください。パスワード入力に 3 回失敗すると、セキュリティ アラート機能 (セクション 3.2.4.3) がアクティブになります。

BSL アクセス パスワードは 256 ビット SHA 暗号化に対応しています (元のパスワードの長さは 256 ビット)。SHA2-256 の計算フローについてはセクション 3.1.2.2 を参照してください。BSL 構成には、パスワードのハッシュ値が保存されます (256 ビット、256 ビット データから計算され、すべてのバイトは 0xFF)。

3.2.4.2 読み出し機能

ROM BSL 対応デバイスは、BSL 構成内に、BSL インターフェイス経由でデバイス メモリを読み戻せる構成可能なプロパティを備えています。すべてのフラッシュ メモリは、BSL ホストから完全にアクセスできますが、一部の SRAM メモリはアクセス制限されています。詳細については、『MSPM33 ブートローダー (BSL) ユーザーガイド』の「SRAM メモリの使用」セクションを参照してください。

デフォルトでは、読み出し機能は安全のためディスエーブルになっています。ユーザーは、BSL 構成の BSLCONFIG0.READOUT フィールドを使用して、読み出し機能をイネーブルできます。

3.2.4.3 アラート機能

3 つを超える BSL パスワード チェックが行われる場合、ROM BSL でアラート機能が適用されます。デフォルトでは、セキュリティ アラートが発生しても、デバイスは追加のアクションを実行しません。ユーザーは、BSLCONFIG1.SECURITY_ALERT_LEVEL フィールドを使用して、アラート動作を構成できます。

BSL の構成では、次の 2 つの追加アラート動作がサポートされています。

- BSL の工場出荷時リセットをトリガします。MAIN または NONMAIN フラッシュのセクタが静的書き込み保護されている場合、セクタは BSL の工場出荷時リセットの影響を受けません。
- BSL をディセーブルにするには、NONMAIN 領域を再構成します。NONMAIN フラッシュが静的書き込み保護されている場合、再構成はサポートされません。

特定の MAIN フラッシュ メモリまたは NONMAIN フラッシュ メモリ全体を保持するように、フラッシュ メモリの静的書き込み保護 (セクション 3.1.3) を設定します。

3.2.4.4 アプリケーションの整合性チェック

BSL は、BSL インターフェイス経由でアプリケーションのバージョン番号を返すことをサポートしています。これにより、BSL ホストはファームウェアを読み出さずに、ファームウェアのバージョンを照会できます。バージョン フィールド アドレスの長さは 32 ビットです。対応する MAIN フラッシュのバージョン値をプログラムします。

APP_REV_POINTER フィールドを使用して、アプリケーション バージョン ワードのアドレスを設定します。バージョン データは、指定されたアドレスが有効なフラッシュ メモリ アドレスに対応している場合にのみ返されます。指定されたフラッシュ アドレスがプログラムされていない場合、ROM BSL は 0h を返します。

3.2.5 BSL チェックサム

MSPM33 デバイスは、ブート段階の間に BSL 構成データの CRC チェックを行います。BSL の CRC チェックサムは、BCR チェックサムと同じ計算フローを共有しています。詳細については、セクション 3.1.9 を参照してください。

テキサス・インスツルメンツでは、SysConfig ツールを使用して BSL チェックサムを自動的に計算することを推奨しています。詳細については、セクション 4.3 を参照してください。

3.2.5.1 CRC チェック エラーの処理

BSL の起動時に BSL 構成データの CRC チェックがエラーとなった場合、致命的なブート エラーが発生し、以下の制限が課されます。

- このエラーの原因をブート診断として CFG-AP に記録
- BSL がイネーブルに設定されても BSL は起動しない
- ユーザー アプリケーションを開始しない
- アプリケーションのデバッグ アクセスはすべてディセーブル

Copyright © 2026 Texas Instruments Incorporated

- ブート プロセスを最大 3 回再試行
  - 2 回目または 3 回目の試行で成功した場合、デバイスを通常どおり起動
  - 3 回目の試行に失敗した場合、次に BOR または POR が実行されるまで、それ以上のブート試行は許可しない

Copyright © 2026 Texas Instruments Incorporated

4 SysConfig を使用した NONMAIN 構成

このセクションでは、テキサス・インスツルメンツのグラフィカル構成ツール SysConfig を使用して、NONMAIN メモリのさまざまな機能オプションを構成する方法を説明します。

4.1 SysConfig の概要

SysConfig ツールは、ピン、ペリフェラル、サブシステム、他のコンポーネントを構成するための、直感的で包括的なグラフィカル ユーティリティのコレクションであり、ユーザーは競合を視覚的に管理、表面化、解決することができます。その結果、アプリケーションの作成により多くの時間を費やすことができます。SysConfig の出力ファイルには、ソフトウェア開発キット (SDK) サンプルと組み合わせて使用したり、カスタム プロジェクトを構成したりするためのヘッダ ファイルとソース ファイルが含まれています。

SysConfig ツールは、スタンドアロン インストーラとして提供されます。インストーラを TI の Code Composer Studio™ (CCS) ソフトウェア、IAR Embedded Workbench® (IAR)、または Keil® に手動でリンクするか、クラウド ツールポータルを使用します。テキサス・インスツルメンツのエコシステムの一部として、CCS にはデフォルトで SysConfig が統合されています。詳細については、『SysConfig ユーザー ガイド』を参照してください。

図 4-1 に、NONMAIN 領域を構成するツールの一部を示します。各コンポーネントに関する詳細については、疑問符を選択して確認できます。

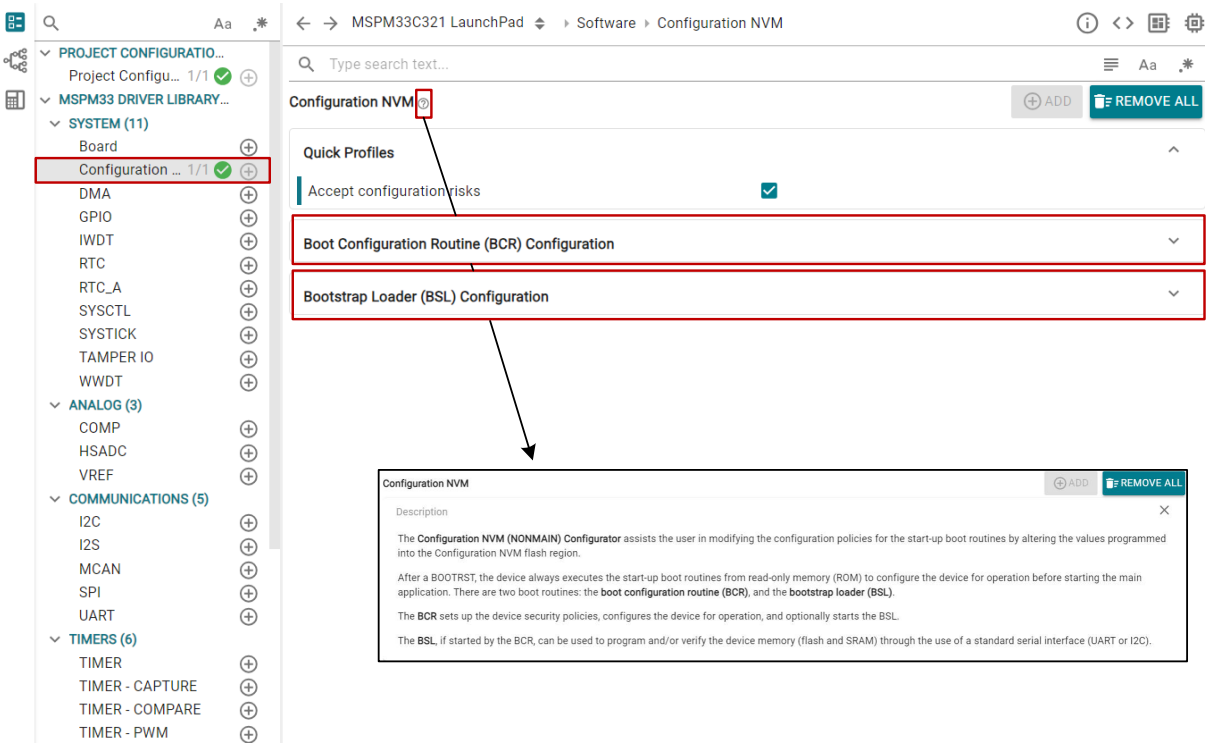


図 4-1. SysConfig ツール：NVM を構成

4.2 SysConfig を使用した BCR の構成

図 4-2 は、MSPM33C321A デバイスの BCR 構成 (Type-A レイアウト) を示しています。BCR の構成に従い、アクセス ポリシー、デバッグ ポリシー、一括消去、工場出荷時リセットに関するポリシーを、各種セキュリティ シナリオに合わせて設定できます。詳細については、セクション 3.1.2 を参照してください。BCR 構成 ID はデフォルト値で使用され、ツールでの変更はサポートされていません。CRC チェックサムは、カスタマイズされた BCR 構成に基づいて自動的に計算されます。

Copyright © 2026 Texas Instruments Incorporated

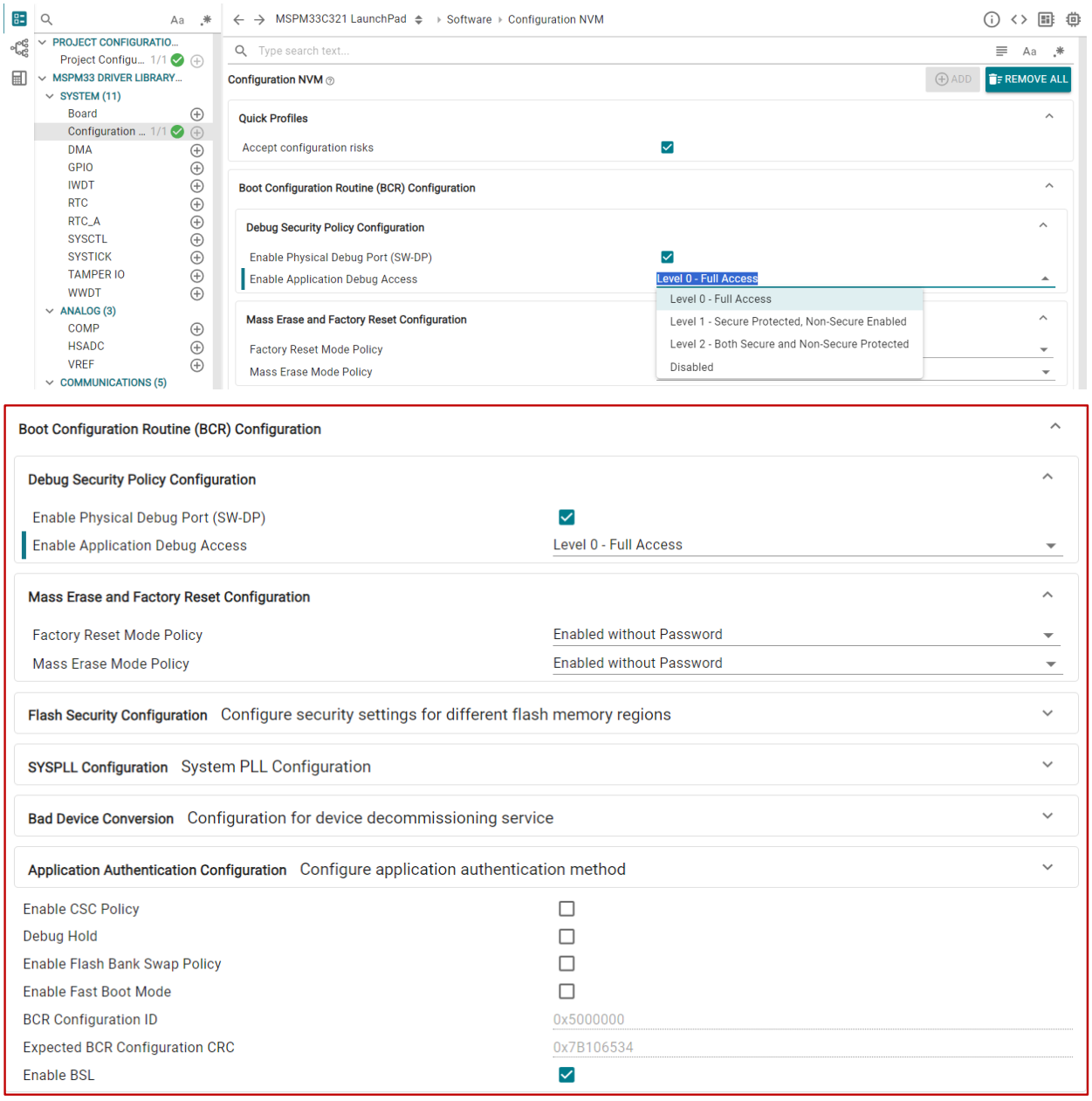


図 4-2. BCR の構成

4.2.1 パスワードの設定

SHA2-256 パスワードをサポートするデバイスでは、NONMAIN BCR 構成で 256 ビットの暗号化パスワードを設定します。図 4-3 は、MSPM33C321A デバイス (Type-A) の SWD パスワード構成を示しています。

English Document: SDAA228
Copyright © 2026 Texas Instruments Incorporated

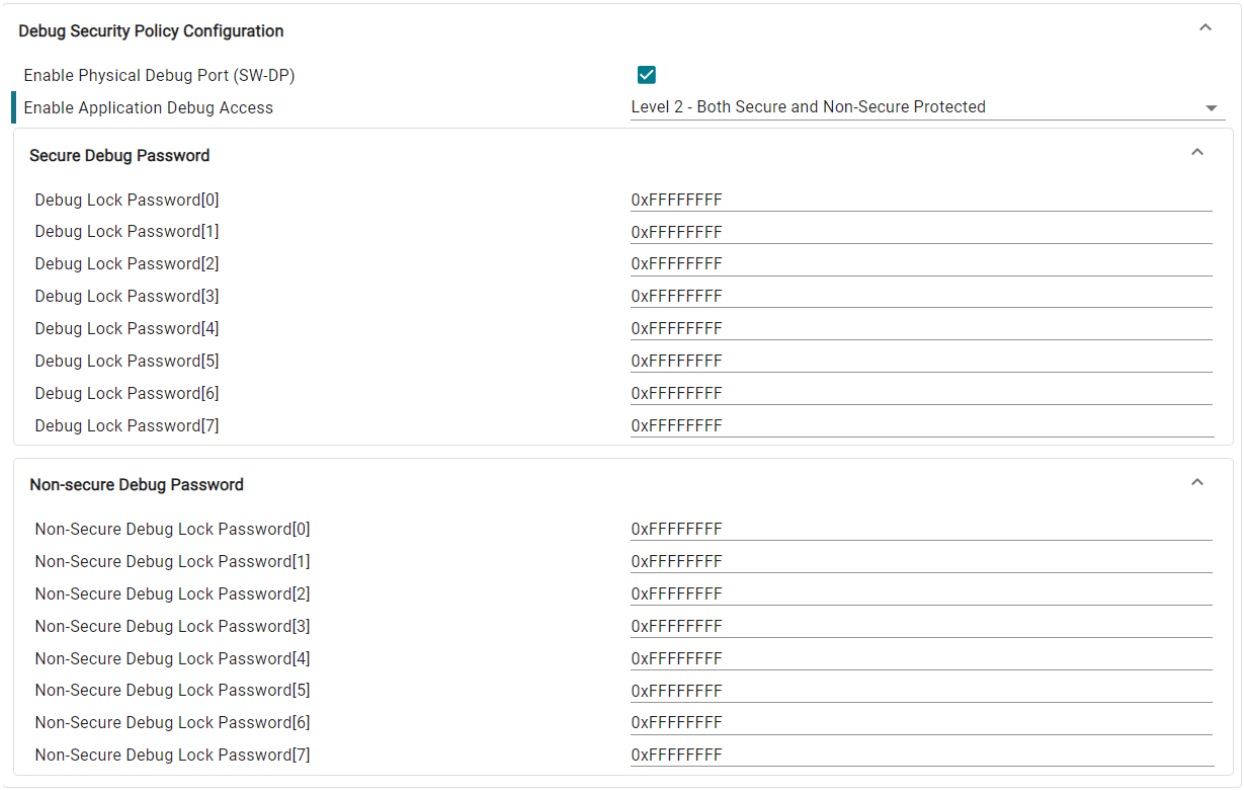


図 4-3. SHA2-256 SWD パスワードの設定

SysConfig ツールは、SHA2-256 パスワード生成フロー (図 4-4 として示される) を統合しています (セクション 3.1.2.2 を参照)。デバイスが SHA2-256 パスワードをサポートしている場合は、「セキュア デバッグ パスワード」の横にある疑問符を選択して、プロセス フローの例を表示してください。この例では、SHA256 オンライン ツールも紹介されています。

サンプル フローは、次のような 256 ビット SHA2-256 パスワード生成すべてに対して設計されています。

- デバッグ アクセス
- 工場出荷時リセット
- 一括消去
- 不正なデバイス変換
- BSL アクセスを実現

Copyright © 2026 Texas Instruments Incorporated

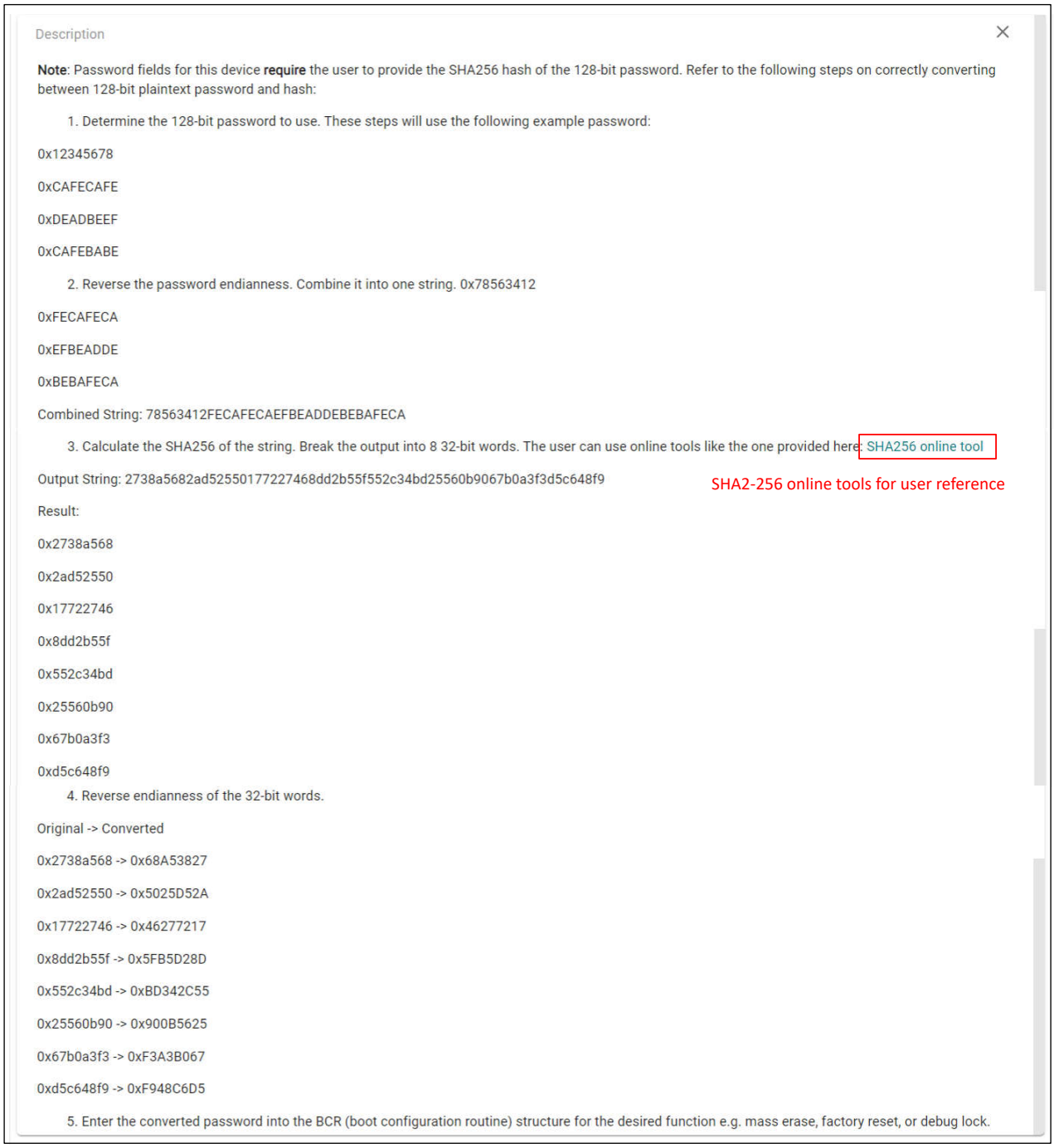


図 4-4. SHA2-256 パスワード生成フロー

4.2.2 SYSPLL の構成

SysConfig ツールを使用すると、図 4-5 に示すように、3 レベルの SYSPLL 動作モードを構成できます。

- NOPLL - PLL は使用しない
- PLL_80 - PLL は 80MHz 動作用に構成されている
- PLL_CUSTOM - PLL はカスタム構成を使用する

Copyright © 2026 Texas Instruments Incorporated

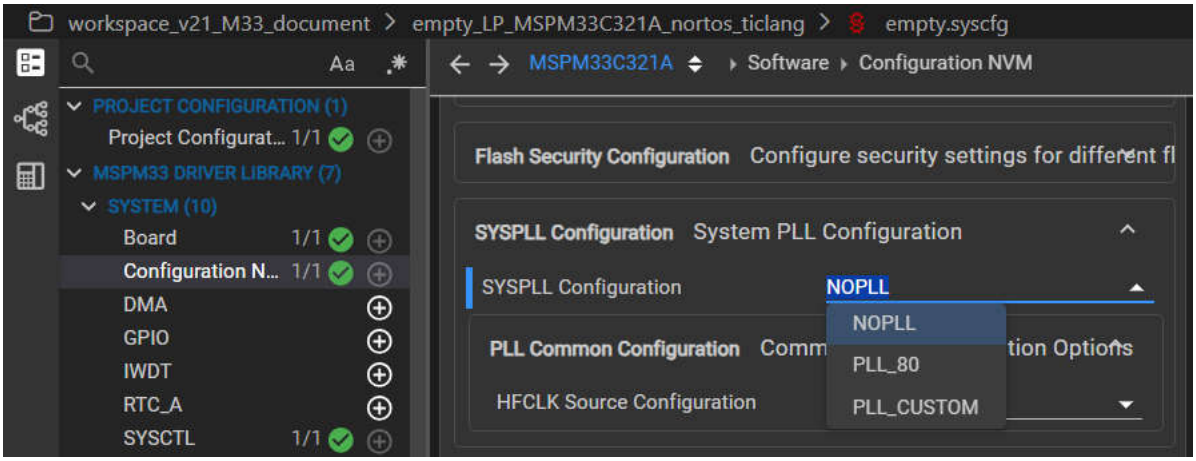


図 4-5. SYSPLL の構成

また、PLL が有効のときはシステム PLL への入力として使用でき、PLL が無効のときは HFCLK として直接使用できる高周波クロック ソースを構成することもできます。図 4-6 に示すように、ソースは以下の 3 つのオプションに構成できます。

- デフォルト (0xFF):SYSOSC (16MHz) を使用
- HFXT_20MHZ (0xAA):20MHz HFXT 水晶振動子を使用
- HFXT_40MHZ (0xBB):40MHz HFXT 水晶振動子を使用

この構成は、PLL の入力ソース (PLL がイネーブルのとき)、直接 HFCLK ソース (PLL がディセーブルのとき)、MCAN クロック ソース構成に影響を及ぼします。

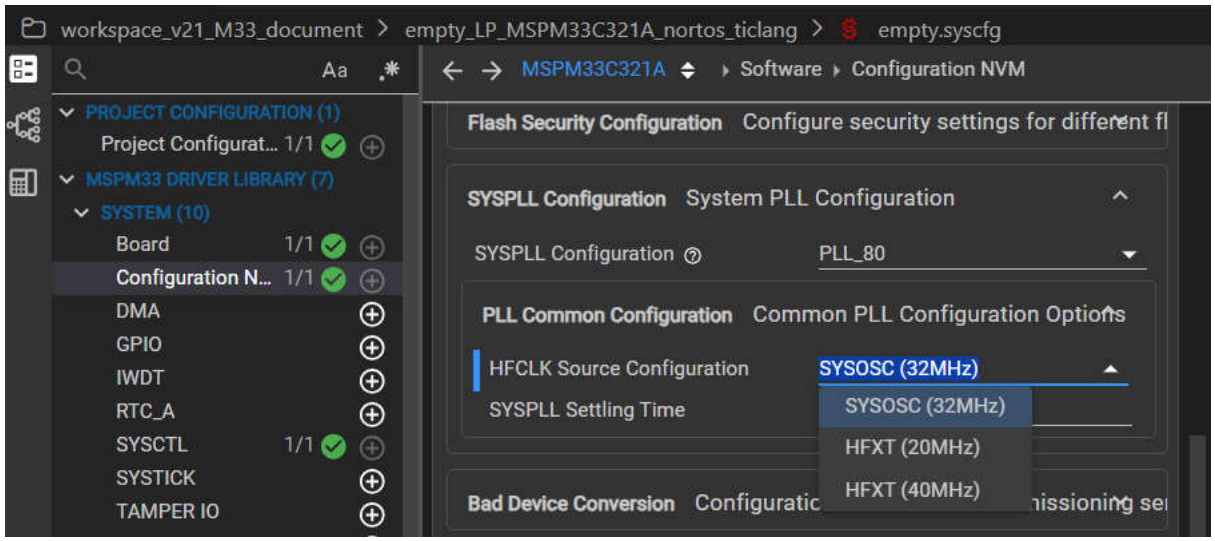


図 4-6. HFCLK ソース構成

4.2.3 フラッシュ セキュリティの構成

静的書き込み保護、セキュリティ保護、または特権保護をイネーブルにするには、関連するフィールドのビットを 0 に設定します。最小メモリ範囲は 2KB (1 セクタ) または 16KB (8 セクタ) で、保護されているセクタの順序によって異なります。詳細については、セクション 3.1.3 を参照してください。

SysConfig ツールを使用すると、ユーザーは特定のセクタを選択して、静的書き込み保護、セキュリティ保護、特権保護を適用できます。

図 4-7 に MSPM33C321A デバイスの MAIN FLASH bank0 の静的書き込み保護を構成する方法を示します。最初の 32 セクタでは、各セクタ (2KB) に個別に書き込み保護を適用できます。残りのセクタでは、各ブロック (8 セクタ) に書き込み保護を個別に適用できます。

Copyright © 2026 Texas Instruments Incorporated

図 4-8 に MSPM33C321A デバイスの MAIN FLASH bank1 のセキュリティ保護を構成する方法を示します。最初の 32 セクタでは、各セクタ (2KB) に個別にセキュリティ保護を適用できます。残りのセクタでは、各ブロック (8 セクタ) にセキュリティ保護を個別に適用できます。

図 4-9 に MSPM33C321A デバイスの DATA FLASH の特権保護を構成する方法を示します。最初の 32 セクタでは、各セクタ (2KB) に個別に特権保護を適用できます。残りのセクタでは、各ブロック (8 セクタ) に特権保護を個別に適用できます。

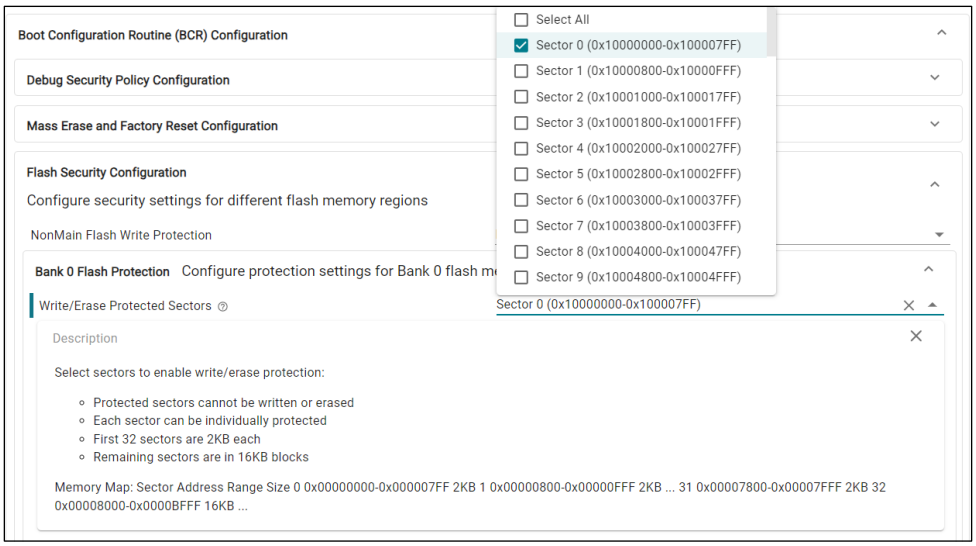


図 4-7. フラッシュの静的書き込み保護

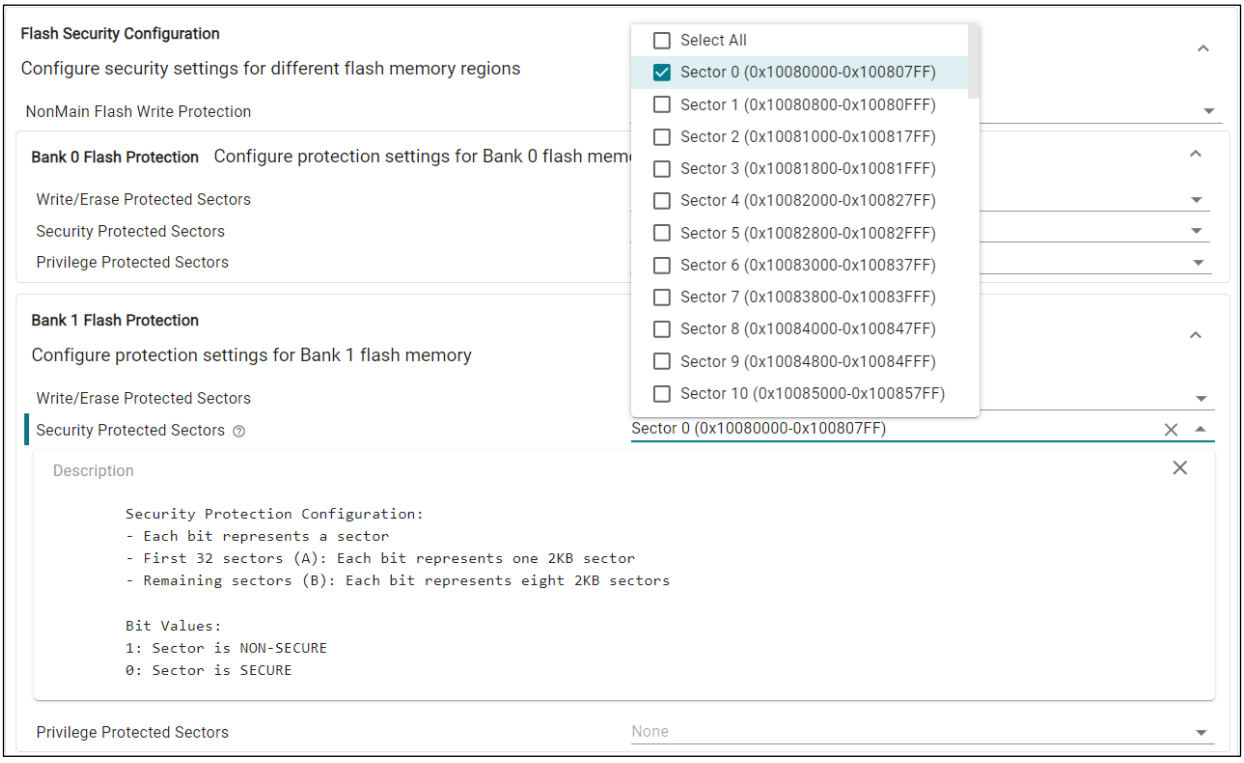


図 4-8. フラッシュ セキュリティ保護

Copyright © 2026 Texas Instruments Incorporated

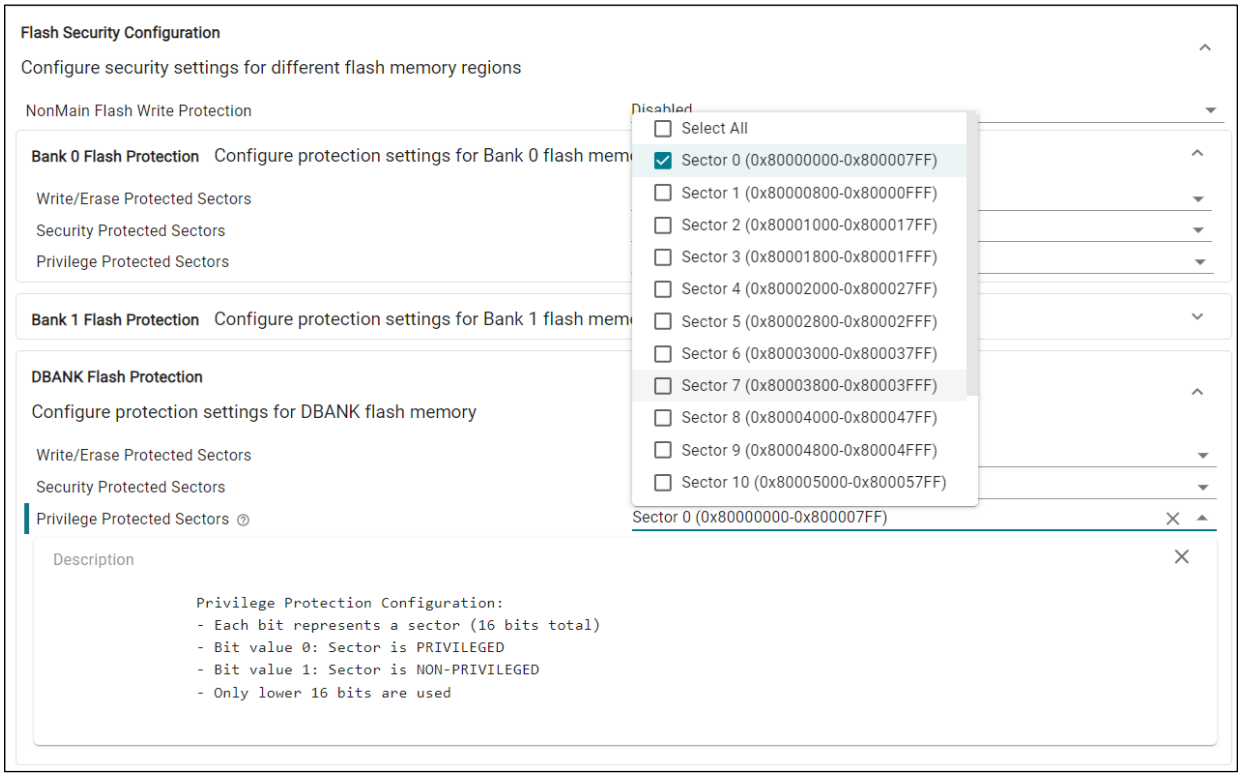


図 4-9. フラッシュ特権保護

SysConfig ツールは、NONMAIN 静的書き込み保護もサポートしています。デバイスが NONMAIN 領域で書き込みおよび消去動作をロックすると、NONMAIN 領域は変更不可能になります。NONMAIN は、DSSM コマンドを使用して生成された工場出荷時リセットによってのみ復元できます。

4.2.4 アプリケーションのダイジェスト チェック

アプリケーションのダイジェスト チェックでは、ユーザーは NONMAIN BCR 構成で CRC32 ダイジェスト チェックまたは SHA2-256 ダイジェスト チェックを設定できます。

図 4-10 に、セクション 3.1.7.1 の設定に基づく MSPM33C321A (TYPE-A) の CRC32 ダイジェスト チェック構成を示します。例となるデータ図 3-2 は、0x00010000 に配置されています。

図 4-11 に、セクション 3.1.7.2 の設定に基づく MSPM33C321A (TYPE-A) の SHA2-256 ダイジェスト チェック構成を示します。例となるデータ図 3-3 は、0x00010000 に配置されています。

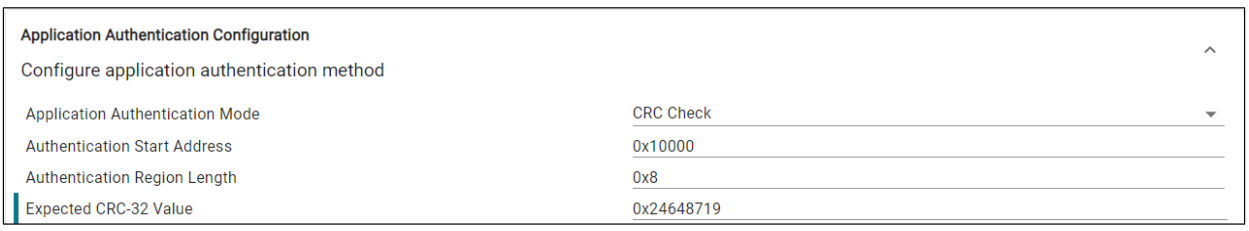


図 4-10. CRC32 ダイジェスト チェックの構成

Copyright © 2026 Texas Instruments Incorporated

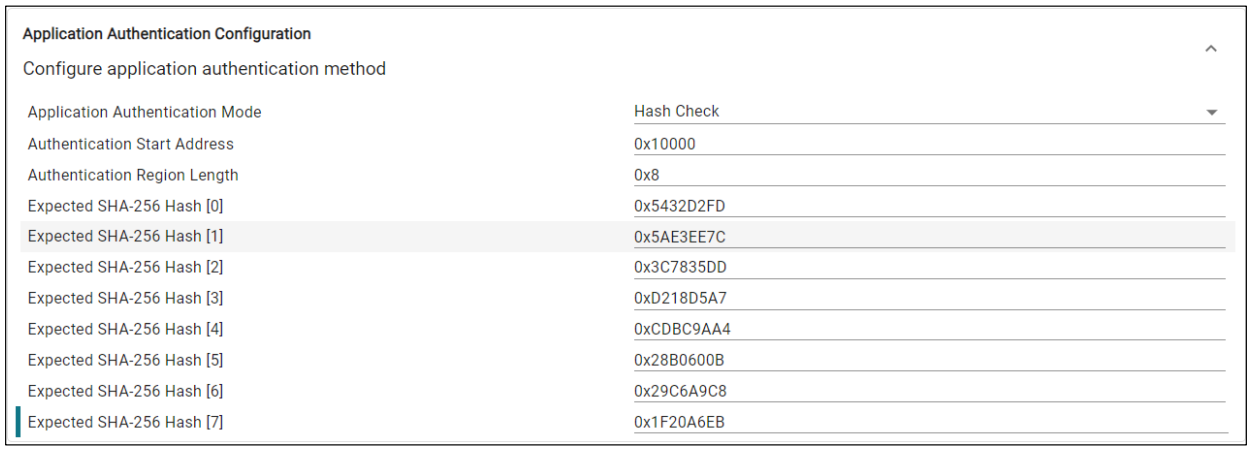


図 4-11. SHA2-256 ダイジェスト チェックの構成

4.2.5 その他の BCR 構成

SysConfig の一部の BCR 構成は単純であり、以下のものを含め、有効または無効にできます。

- 高速ブート モードを有効化
- デバッグ ホールドを有効化
- CSC ポリシーを有効化
- フラッシュ バンク スワップ ポリシーを有効化
- イネーブル BSL モード
- BSL 起動ピンのチェックを有効化
  - SysConfig ツールの、「BCR の構成」ではなく、「BSL の構成」には「BSL 起動ピンチェックを有効化」の選択項目や、その他の BSL GPIO 起動構成が含まれています。

4.3 SysConfig を使用した BSL の構成

図 4-12 は、MSPM33C321A デバイスの BSL 構成 (Type-A レイアウト) を示しています。



図 4-12. BSL の構成

Copyright © 2026 Texas Instruments Incorporated

4.3.1 BSL アクセス パスワード

デバイスが ROM BSL をサポートする場合、256 ビットの BSL アクセス パスワードは常にイネーブルです。パスワードは SHA2-256 暗号化され、元のパスワードはすべて 0xFF (256 ビット) なので、SysConfig ツールは、生成された SHA2-256 の値を PASSWORD_y フィールドに保存します。

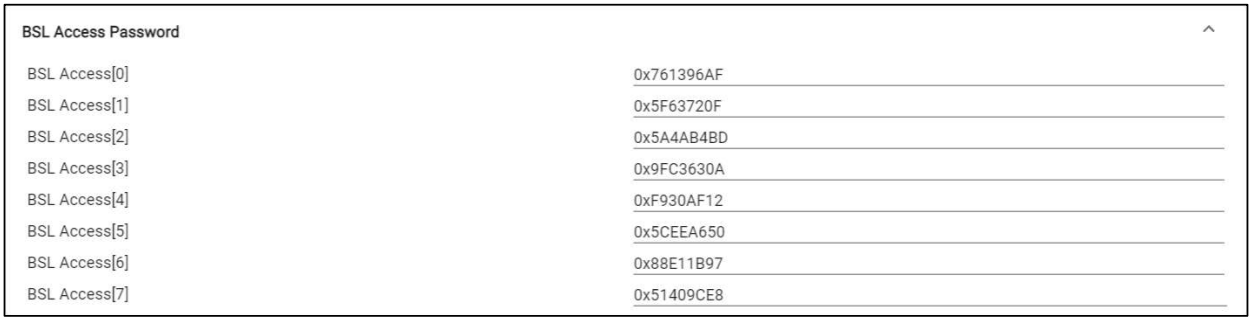


図 4-13. SHA2-256 BSL デフォルト アクセスパスワード

4.3.2 BSL 起動ピンの構成

このデバイスは、カスタマイズした起動ピン プロパティを使用して ROM BSL をサポートしています。セクション 4.3 に、構成の詳細を示します。



図 4-14. BSL 起動ピン

BSL の構成で BSL 起動ピン チェックをディスエーブルにすると、BCR はハードウェアピンによる起動チェックをスキップしますが、ソフトウェアによる BSL 起動は引き続き利用可能です。無効化後、SysConfig ツールでは BCR 構成の BOOTCFG1.BSL_PIN_INVOKE フィールドがディスエーブルに設定されますが、BSL ピンの構成は変更されません。

4.3.3 BSL 通信インターフェイス

ROM BSL をサポートするデバイスでは、I2C、UART、CAN の各インターフェイスは、共通の BSL インターフェイスとして提供されています。USB ペリフェラルをサポートするデバイスには、DFU をサポートする USB インターフェイスが BSL インターフェイスとして適用されます。

セクション 4.3 に示すように、BSL の構成を使用すると、BSL インターフェイスを柔軟にカスタマイズできます。デフォルトでは、BSL 構成はピンの選択、I2C ターゲットアドレスの変更、UART のボーレートの変更をサポートしています。

Copyright © 2026 Texas Instruments Incorporated

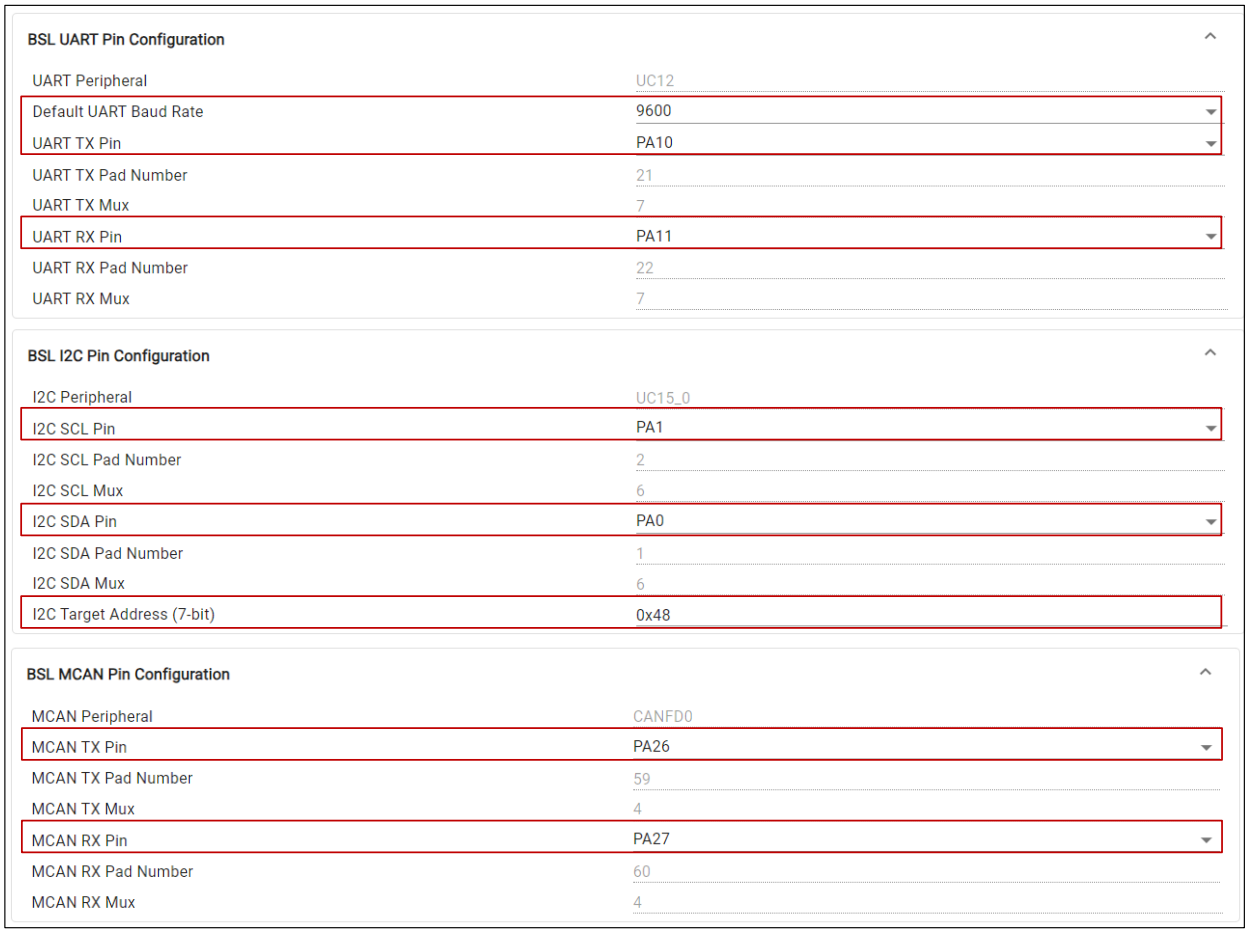


図 4-15. BSL 通信インターフェイス

4.3.4 その他の BCR 構成

BSL 構成 ID 以外にも、図 4-12 に示すように、SysConfig ツールを使用したカスタマイズをサポートする機能がいくつかあります。

- BSL アプリケーションのバージョン
- BSL 読み取りを有効化
- BSL セキュリティ アラート構成

BSL の構成が変更されるたびに、SysConfig ツールが CRC チェックサム値を自動的に計算します。そのため、ユーザーはカスタマイズされた BSL 機能のみに注目し、NONMAIN ファームウェア ファイルを簡単に生成できます。

Copyright © 2026 Texas Instruments Incorporated

5 アプリケーション コードでの NONMAIN 構成

NONMAIN 領域は、アプリケーション コードおよびカスタマイズされたブートローダーで広く使用されている FLASHCTL による動的変更もサポートしています。図 5-1 および SDK の例では、ユーザーの参考用として、アプリケーション コードで NONMAIN フラッシュ フィールドを変更するための一般的なフローを提供します。

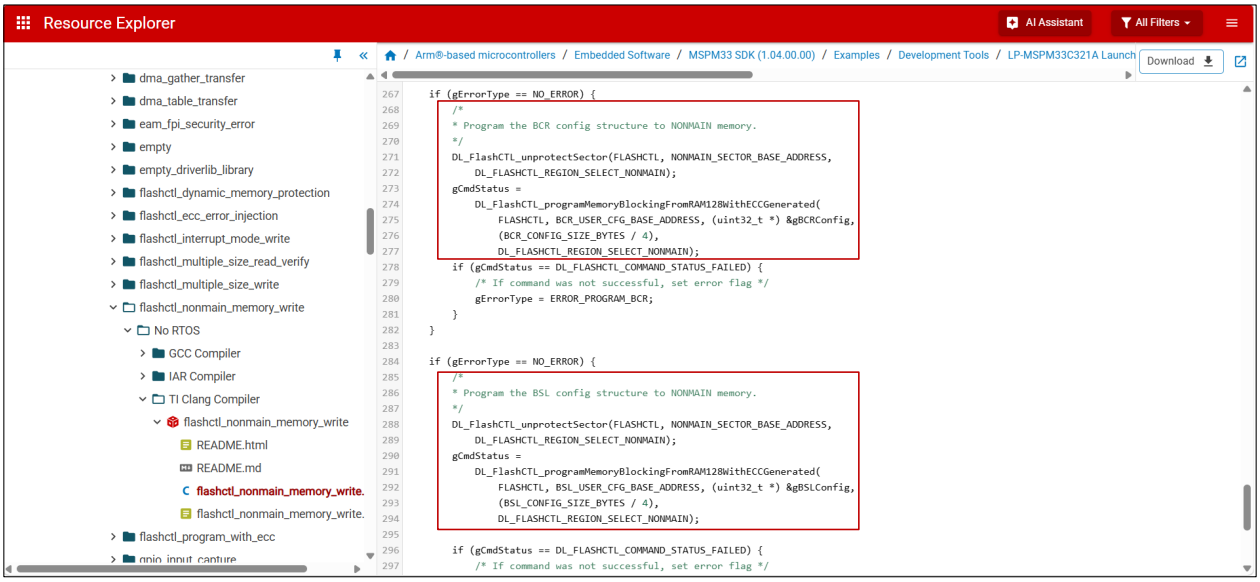


図 5-1. NONMAIN 修正を使用したプロジェクト例

ブート コードは ECC チェックで NONMAIN メモリを読み取るため、ECC は NONMAIN メモリをプログラムする必要があります。NONMIAN レジスタを変更するたびに、NONMAIN セクタ全体を消去し、NONMAIN 構成レジスタ全体の新しい値をロードする必要があります。

テキサス・インスツルメンツは、安全状態で NONMAIN フィールドを消去およびプログラミングすることを推奨します。アプリケーション コードの NONMAIN 構成が頻繁に更新されると、NONMAIN フィールドが空になるリスクが発生します (電源の不安定さなどがその要因)。

Copyright © 2026 Texas Instruments Incorporated

6 IDE ツールを使用した NONMAIN 動作

テキサス・インスツルメンツは、NONMAIN 構成を管理するために SysConfig ツールを使用することを推奨しています。SysConfig ツールは、TI Code Composer Studio™ (CCS) ソフトウェアに統合されています。テキサス・インスツルメンツは、Keil® や IAR® など他の IDE ツールと組み合わせて使用するための SysConfig ツールのスタンドアロン バージョンを提供しています。別の IDE ツールで SysConfig を使用する方法の詳細については、セクション 10 を参照してください。

6.1 NONMAIN 構成ファイル

図 6-1 に、SysConfig ツールが、NONMAIN フラッシュ メモリを構成するために 2 つのファイル (boot_config.c および boot_config.h) を生成することを示します。

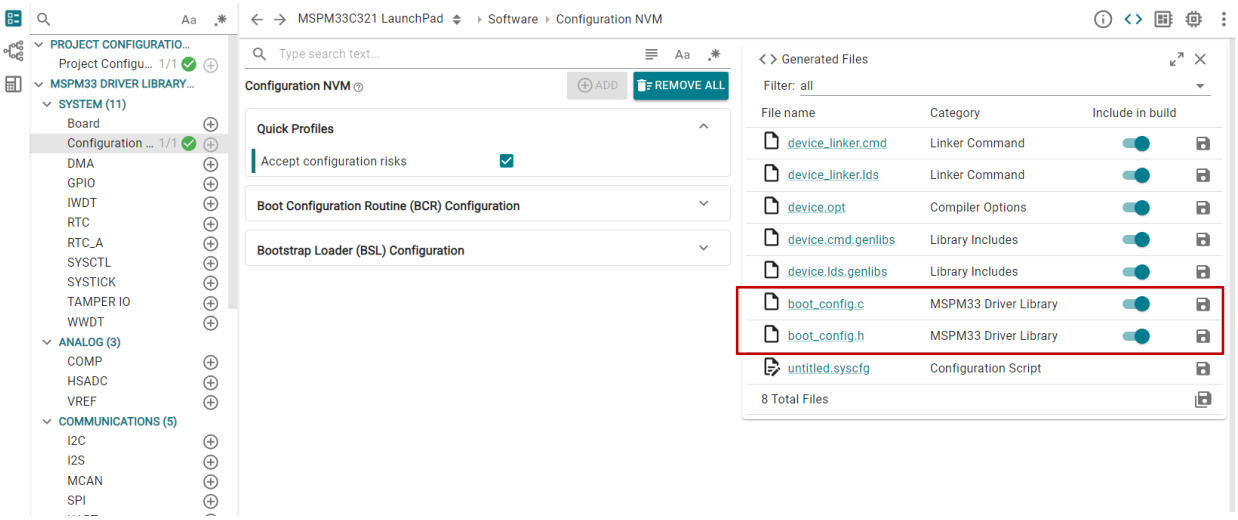


図 6-1. 構成ファイル

boot_config.c ファイルには、NONMAIN 構造体のすべての構成が含まれており、構成は自動的に出力ファイルにコンパイルされます。boot_config.c ファイルには、SysConfig ツールで設定されたデフォルト値が含まれています。SysConfig ツールがファイルを管理および上書きするため、ユーザーはこれら 2 つのファイルを手動で変更することはできません。NVM コンポーネント内でプロジェクト固有の .syscfg ファイルを変更した後、これら 2 つのファイルが再生成され、最新の構成に更新されます。

SysConfig ツールを使用して追加の変更を実行するには、「ビルドに含む」ボタンをチェック解除し、2 つのファイルをビルドから除外します。これにより、SysConfig で生成されたファイル (boot_config.c と boot_config.h) がコンパイルされなくなるため、ユーザーはファイルをプロジェクトに手動で追加して、追加の変更を行うことができます。

6.2 プロジェクトの消去プロパティ

NONMAIN フラッシュ領域は不揮発性メモリで、新しい値を書き込む前に消去動作が必要です。NONMAIN 領域のファームウェアをデバイスに正常にロードするには、erase プロパティを設定して NONMAIN を消去します。

Code Composer Studio™ studio の場合、プロジェクトを右クリックし、プロジェクト プロパティを開きます。図 6-2 に詳細を示します。

Copyright © 2026 Texas Instruments Incorporated

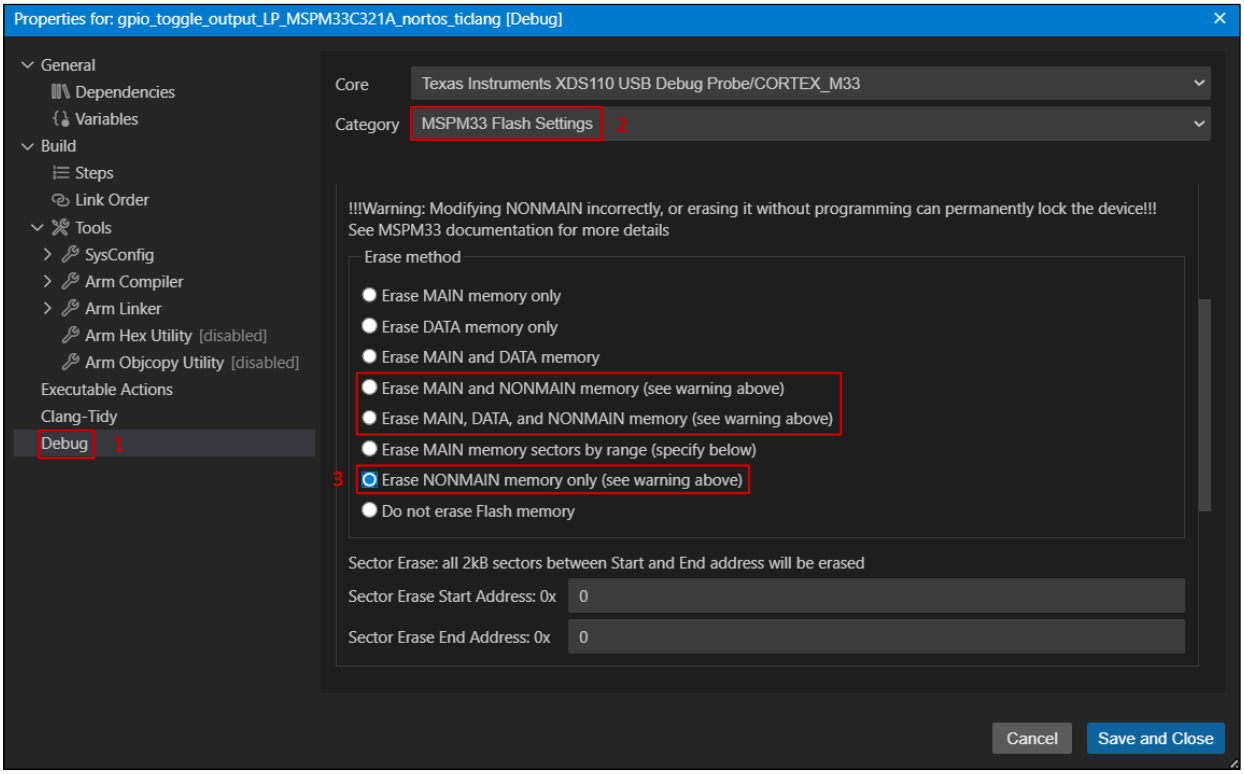


図 6-2. CCS 消去プロパティの設定

Keil® では、ターゲットのオプションを選択して開き、デバッグ設定に NONMAIN を追加します。図 6-3 に、Keil 消去プロパティの設定を示します。

Copyright © 2026 Texas Instruments Incorporated

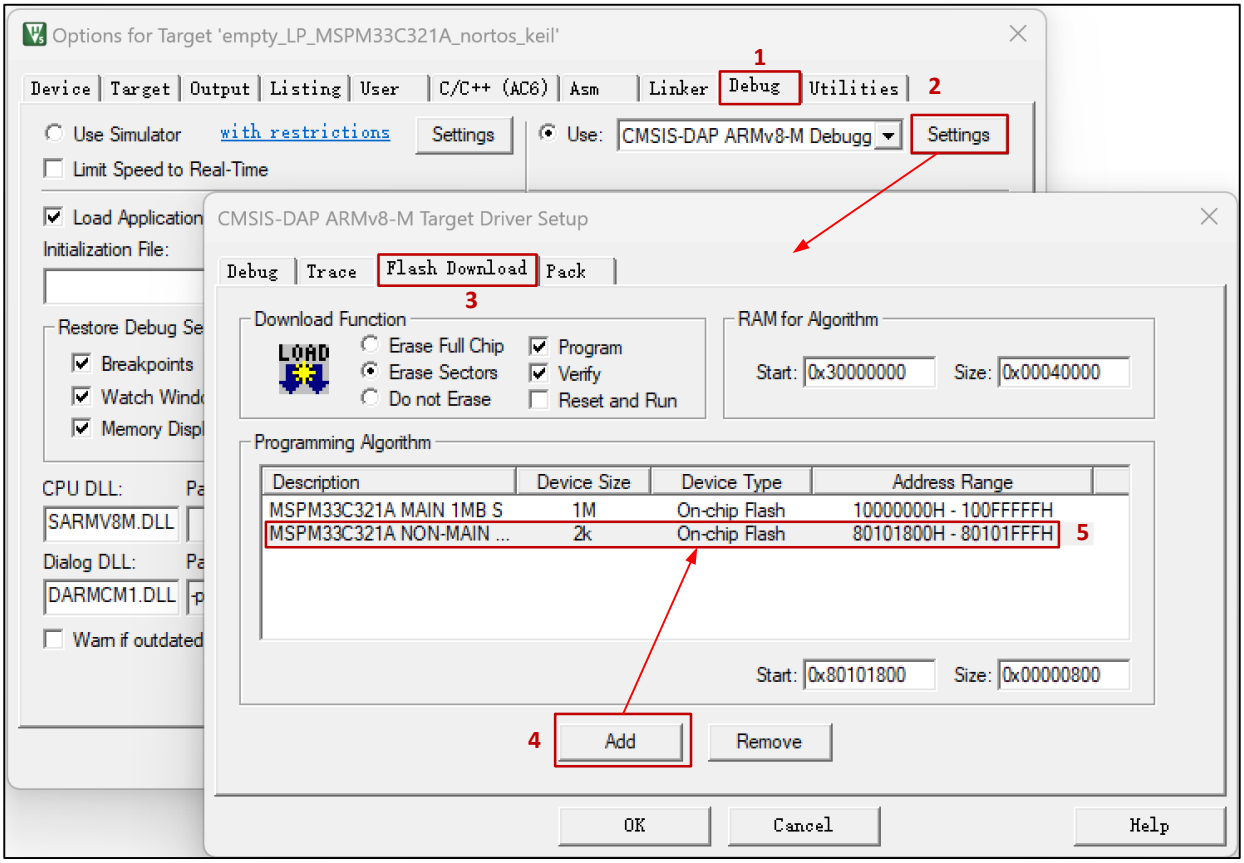


図 6-3. Keil 消去プロパティの設定

IAR® の場合は、プロジェクトを右クリックしてオプションを開きます。メイン以外の領域がパラメータを伴って追加されていることを確認します。図 6-4 に、IAR 設定を示します。

Copyright © 2026 Texas Instruments Incorporated

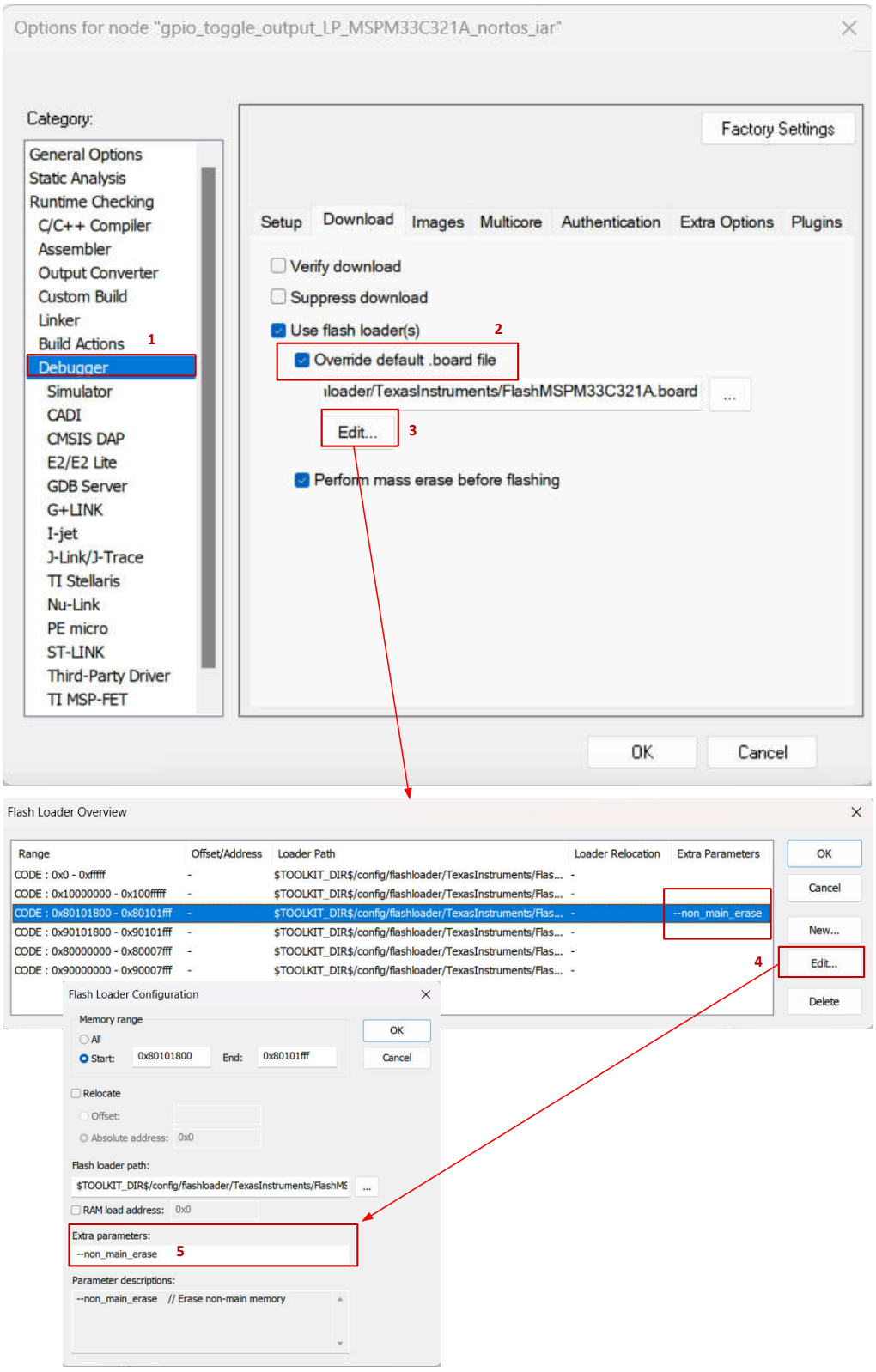


図 6-4. IAR 消去プロパティの設定

Copyright © 2026 Texas Instruments Incorporated

NONMAIN 構成が完了してプログラムされた後、毎回同じ値で NONMAIN を再プログラムすることを避けるため、NONMAIN フィールドを削除することを推奨します。

6.3 パスワードで保護されたデバッグ

SWD デバッグ ポリシーがパスワードを使用して暗号化として設定されている場合は、新しいファームウェアをデバッグまたはダウンロードする前に、SWD パスワード認証用の DSSM コマンドを生成します。

TI は、XDS110 ツールで MSPM33 デバッグ構成用の .ccxml ファイルを提供しています。図 6-5 に、次の DSSM コマンドの 128 ビット パスワードを設定する手順を示します。

1. *targetConfigs* フォルダにある *.ccxml* ファイルを開きます。
2. 「詳細設定」を選択して、XDS110「ターゲット構成」を開きます。
3. 「MSPM33 デバイス」を選択して、「デバイスのプロパティ」ページを開きます。
4. SWD パスワードボックスに 128 ビットのパスワードを入力します。

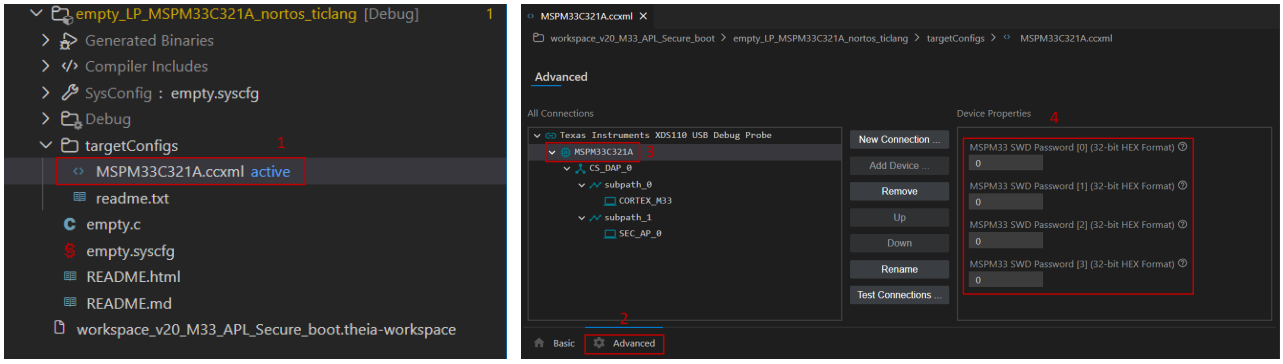


図 6-5. .ccxml ファイルを使用してパスワードを設定

注

.ccxml ファイルで設定されたパスワードは、SWD アクセス、工場出荷時のリセット、一括消去など、すべての DSSM 操作用パスワードに適用されます。

正しいパスワードを設定したら、DSSM スクリプトを実行して SWD インターフェイスのロックを解除します。図 6-6 にそのプロセスを示します。

1. プロジェクトで *targetConfigs* を見つけ、*.ccxml* ファイルを選択します。
2. .ccxml ファイルを右クリックし、「プロジェクトレス デバッグを開始」を選択します。
3. 上部メニューで「スクリプト」を選択し、「MSPM33 デバイス コマンド」を選択します。
4. DSSM コマンドを選択して生成します。
5. SWD インターフェイスのロックを解除するには、*DebugAccessPasswordAuthentication_Auto* を選択します。
6. コマンドの実行が正常に完了したら、トップ メニューを見つけます。「実行」を選択して、プロジェクトをデバッグするか、プロジェクトをフラッシュします。

Copyright © 2026 Texas Instruments Incorporated

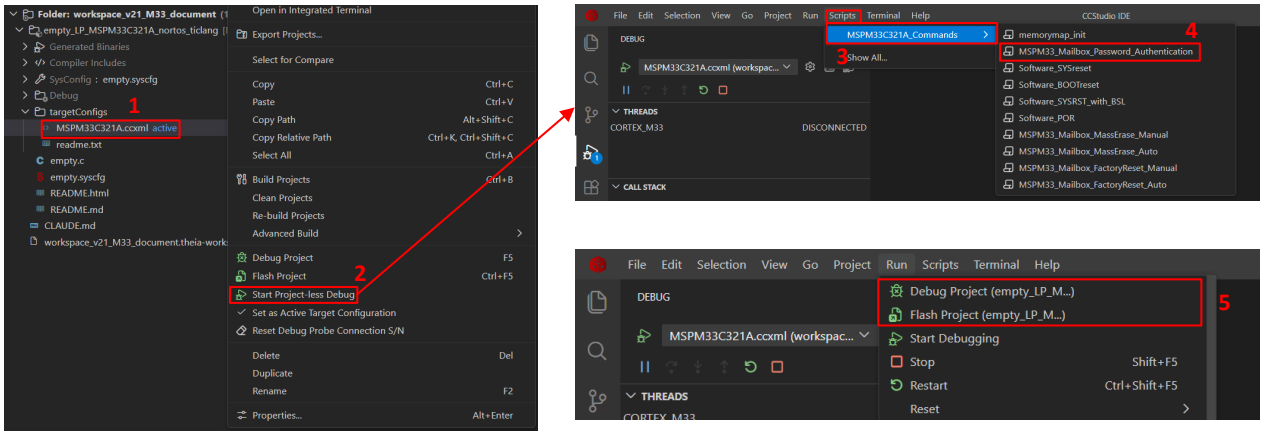


図 6-6. CCS v21 を使用した DSSM コマンド

注

デバッグ アクセスのためのパスワード認証シーケンスが正常に実行された後、デバイスは次の BOOTRST までロック解除状態のままになります。

Copyright © 2026 Texas Instruments Incorporated

7 プログラマ ツールを使用した NONMAIN 動作

NONMAIN は、デバイスをブートするために BCR と BSL が使用する構成データを格納する、フラッシュ メモリの専用領域です。この領域は、他の目的では使用されません。ブート構成のパラメータを変更するには、NONMAIN セクタ全体を消去し、目的の設定で BCR と BSL の両方の構成構造を再プログラムします。

空の NONMAIN フィールドがデバイスを恒久的にロックするリスクについては、NONMAIN 領域が空のままとなる時間を短縮し、新しいデータがロードされるまで待つことを推奨しています。2 種類のアプローチを推奨します。

- 既存の NONMAIN を個別に消去し、直ちに新しい NONMAIN をロードします。
- MAIN と NONMAIN を一緒に消去し、NONMAIN と MAIN を順番に書き込みます。
  - プログラマが消去とプログラムの順序に確信を持てない場合は、MAIN ファームウェアと NONMAIN ファームウェアを個別にロードします。

7.1 UniFlash を使用した NONMAIN 動作

UniFlash は、テキサス・インスツルメンツのマイコンやワイヤレス コネクティビティ デバイスに搭載されしているオンチップ フラッシュと、テキサス・インスツルメンツ製プロセッサ向けのオンボード フラッシュに対してプログラミング (書き込み) を行うためのソフトウェア ツールです。Uniflash は、グラフィカル インターフェイスとコマンドライン インターフェイスの両方を採用しています。

NONMAIN フラッシュ メモリをプログラムするには、NONMAIN メモリを含む消去プロパティを選択します。図 7-1 にこのプロセスを示します。

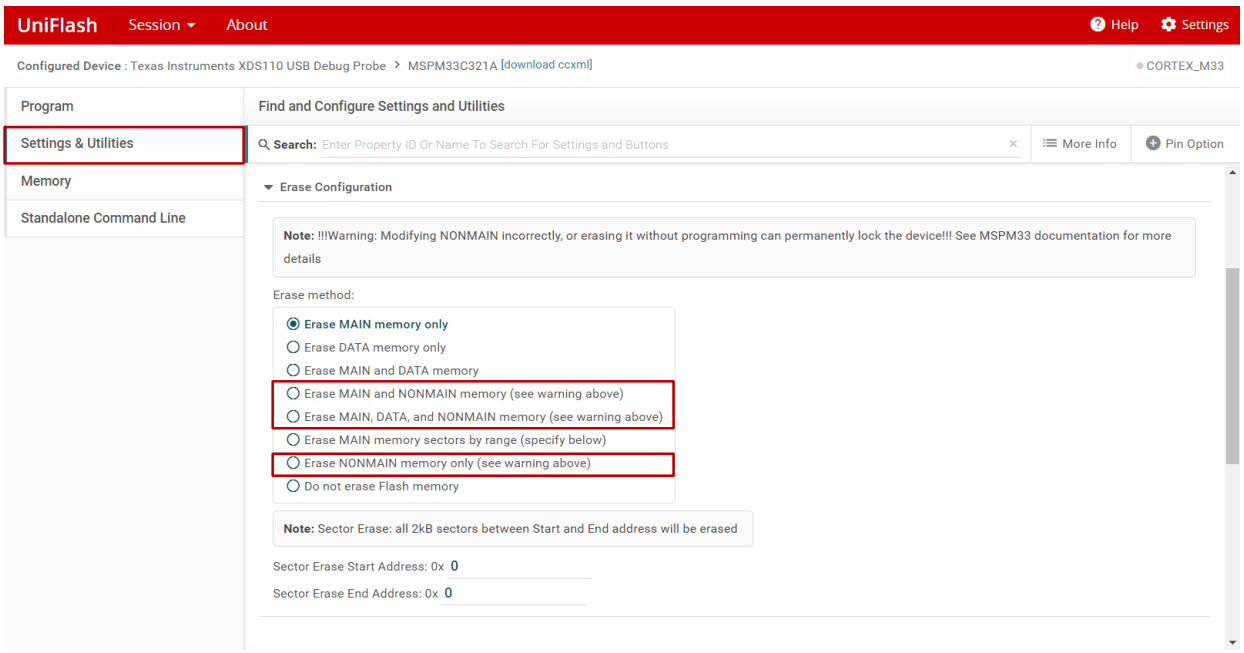


図 7-1. UniFlash を使用した NONMAIN 動作

NONMAIN をプログラムするには、以下の手順に従います。

1. NONMAIN 領域ファームウェアのみが含まれるようにファームウェアを準備します。TI-Hex または Intel-Hex 形式を使用すると、NONMAIN 領域のファームウェアを、簡単に切り離して処理することができます。
2. 消去プロパティとして「NONMAIN メモリのみを消去」を選択します (上記の警告を参照)。
3. デバイスをプログラムします。NONMAIN のみが消去され、再プログラムされます。

Copyright © 2026 Texas Instruments Incorporated

7.2 J-Flash を使用した NONMAIN 動作

J-Flash™ は、SEGGER によるフラッシュ プログラミング ソフトウェアで、ユーザーは組み込みマイコンの内部および外部フラッシュ メモリをプログラムできます。GUI (J-Flash) またはコマンド ライン インターフェイスを使用して、J-Flash を制御します。

NONMAIN フィールドをプログラムするには、NONMAIN バンクを有効にし、erase プロパティを選択して NONMAIN フィールドを含めます。図 7-2 に、J-Flash を使用した NONMAIN 動作を示します。

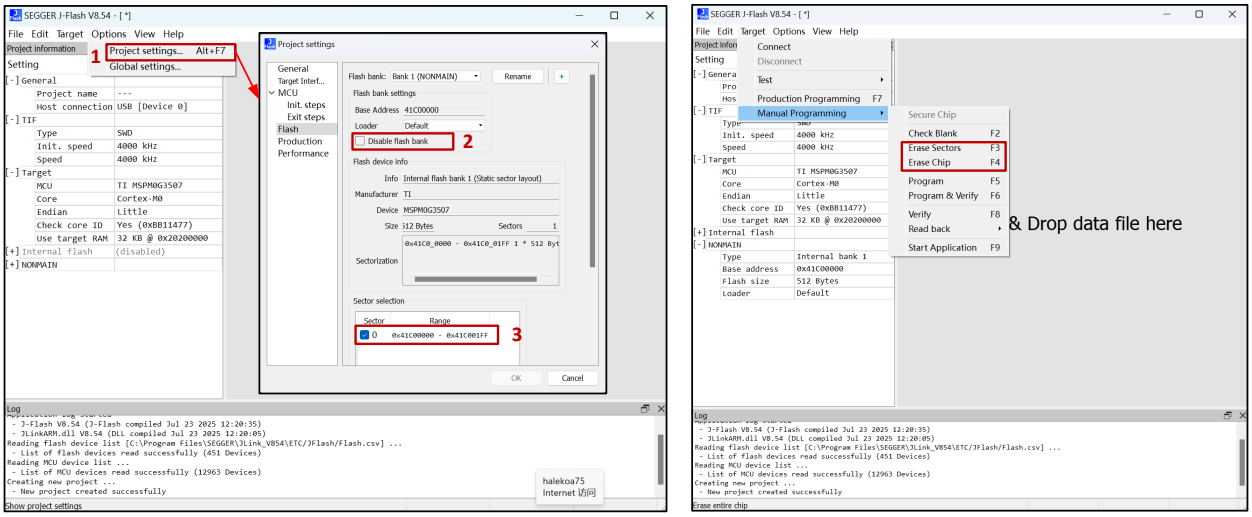


図 7-2. J-Flash を使用した NONMAIN 動作

手動プログラミング方法を選択する場合は、新しい NONMAIN ファームウェアをロードする前にデバイスがリセットされていないことを確認してください。デバイスがリセットされた場合、空の NONMAIN はデバイスを永続的にロックします。

注

TI は、新しい MSPM33 デバイスには最新の J-Flash バージョンの使用を推奨します。

NONMAIN のみをプログラムするには、以下の手順に従います。

1. NONMAIN 領域ファームウェアのみを含むファームウェアを準備します。
2. MAIN フラッシュ メモリを除外するには、ERASE プロパティを選択します (MAIN フラッシュを無効にする、または MAIN フラッシュ セクタをいずれも選択しない)。
3. 消去セクタを使用してデバイスをプログラムします。NONMAIN フィールドのみが消去および再プログラムされます。

Copyright © 2026 Texas Instruments Incorporated

8 よくある質問 (FAQ)

8.1 マイコン ロック状態分析

MSPM33 デバイスがロック状態になると、MSPM33 は SWD インターフェイス経由で接続できない可能性があります。このセクションでは、マイコンがロックされている一般的な理由について説明します。

8.1.1 ハードウェア問題の分析

次のハードウェア要因によって、デバイスがロックアップすることがあります。

- ハードウェア回路設計の欠陥です
- デバッガへの接続中に問題が発生しました
- 周期的な外部リセット信号 (NRST へ)

8.1.1.1 ハードウェア回路設計

MSPM33 デバイスを安定動作させるため、指定の電源ピンに正しい容量の外付けコンデンサが配置されていることを確認します。回路が VDD、Vcore (サポートされている場合)、NRST ピン、およびピンの電圧に接続されていることを確認します。

デバイス固有のデータシートの「基本アプリケーション回路図」セクションで、リファレンス回路を検索します。Vcore 電圧 (サポートされている場合) は 1.35V (標準値) であれば、デジタル コア機能用の内部 PMU 回路が正常に動作していることを示します。

8.1.1.2 デバッガ接続

スタンドアロン デバッガを使用して MSPM33 デバイスをデバッグする場合は、ハードウェア ピンの割り当てを確認します。デバイスを正常に接続するために、SWDIO と SWCLK が正しい順序で適切に接続されていることを確認してください。場合によっては、デフォルトでデバッガがデバイスに電力を供給しないことがあります。オンボードまたは外部電源レールを使用して、デバイスに適切に電力が供給されていることを確認してください。

ノイズの多い環境で MSPM33 デバイスをデバッグする場合は、より低いデバッグレートを試すか、SWCLK および SWDIO ピンと並列に小型のコンデンサを追加してください。

8.1.1.3 外部リセット信号

外部リセット信号が NRST ラインに接続されている場合は、reset 信号をディセーブルにするか、MSPM33 デバイスのデバッグ時に信号を High に維持します。NRST ピンにリセット信号 (Low アクティブ) が生成され、SWD 接続を切断します。連続的なリセット信号を挿入すると、デバイスがロック状態に移行する可能性があります。

8.1.2 ソフトウェア問題の分析

次のソフトウェア要因によって、デバイスがロックアップすることがあります。

- CPU がフォルト状態に移行
- BCR の構成
- 低消費電力モード (STOP または STANDBY)
- シャットダウン IO 状態
- SWD IO (SWCLK または SWDIO) 機能がディセーブル
- WDT または IWDT リセット (アプリケーション コードでイネーブルの場合)
- ソフトウェア POR または BOOTRST

8.1.2.1 CPU がフォルト状態に移行

CPU がフォルト状態に移行すると、CPU がそのフォルト状態から抜けるまで、Arm® デバイスは自動的にセルフリセットを継続します。無効なアドレス変更やペリフェラルの誤設定といった CPU の不正な動作により、ネストされた例外 (ダブルハード フォルトや NMI など) が発生し、CPU がフォルト状態に移行します。

CPU がフォルト状態に移行すると、連続リセット動作によって SWD 接続が切断され、デバイスはロック状態に移行します。

Copyright © 2026 Texas Instruments Incorporated

8.1.2.2 BCR の構成

BCR の構成が SW-DP ディセーブルまたは SWD アクセス ディセーブルに設定されている場合、デバイスはデバッグ モードでロック状態に移行します。BCR の構成が SWD アクセス暗号化に設定されている場合、誤ったパスワードがロードされると、デバイスはデバッグ モードで ロック状態に移行します。

さらに、誤った NONMAIN 構成をロードすると、デバイスが永続的にロック状態になる可能性があります。

8.1.2.3 低消費電力モード (STOP または STANDBY)

デバイスが STOP モードまたは STANDBY モードに移行すると、Arm® Advanced High-performance Bus Access Port (AHB-AP、Arm デバッグ) コアは検出できず、デバイスはロック状態に移行します。AHB-AP にアクティブに接続するには、デバッガが最初に PWR-AP を接続していることを確認します。詳細については、『MSPM0 用ハードウェアプログラミングおよびデバッガガイド』アプリケーション ノートを参照してください。

XDS110 は、STOP モードまたは STANDBY モードでのデバイスの接続をサポートしています。J-Link™ のような他のサードパーティー デバッガを使用する場合は、この低消費電力モードのデバッグに関する問題を解決する最新のソフトウェア バージョンをお試しください。

8.1.2.4 シャットダウン IO 状態

デジタル IO ピンの状態は、シャットダウンに移行するとラッチされ、保持されます。デジタル IO ピンの状態は次のとおりです。

- 出力 Low または high
- プルアップまたはプルダウン
- 入力イネーブルまたは出力イネーブル
- ドライブ構成

SHUTDOWN モードから復帰した後、IO はアプリケーション ソフトウェアが SHDNIOREL レジスタの RELEASE ビットを適切な KEY 値と共に設定して解除するまで維持されます。

SHUTDOWN モードから復帰するときは、シリアル ワイヤ デバッグ (SWD) ピンも、アプリケーション ソフトウェアが RELEASE ビットを設定するまでの間、ロックされたままになります。そのため、SHUTDOWN モードから復帰する際、アプリケーション ソフトウェアによって IO が解放されるまでは、デバッグ接続を確立できません。

TI デバッグ ツール - XDS110 - 現在は、SHUTDOWN モードからのデバイスのウェークアップを直接デバッグする機能をサポートしています。

8.1.2.5 SWD IO 機能

POR の後、ブート プロセスが完了して CPU がアプリケーションを開始すると、シリアル ワイヤ デバッグ (SWD) IO が SWD モードに設定されます (SWDIO が High になり、SWCLK が Low になります)。

デバッグのサポートが不要になった場合にアプリケーションでこれらのピンを使用できるように、ソフトウェアで SWD ピンを汎用入出力 (GPIO) として再構成することができます。SWD の機能をディスエーブルにするには、SYSCTL の SWDCFG レジスタの DISABLE ビットを KEY (62h) とともに設定します。

SWD ピン機能がディセーブルになると、デバイスはロック状態のままで、SWD ピンの機能は POR をトリガしてのみ再度イネーブルにできます。

8.1.2.6 WDT または IWDT リセット

WDT または IWDT が正しい時間ウィンドウ内に供給されない場合、リセットが発生し、デバイスがロック状態に移行する可能性があります。

通常、デバッガは SYSCTL 経由で SYSRST を生成し、WDT を無効化します。リセットが生成されない場合、または CPU レベルのリセットとして設定されている場合、WDT によりデバイスがロック状態に移行し、SWD 接続段中にリセットをアサートする場合があります。

IWDT ペリフェラルを含む MSPM33 デバイスの場合、デバッガは LFSS リセットまたは IWDT リセットを生成して IWDT を無効化します。それ以外の場合、SYSRST は IWDT を含む LFSS コンポーネントをリセットしないため、デバイスはロック状態に移行できます。

Copyright © 2026 Texas Instruments Incorporated

8.1.2.7 ソフトウェア POR または BOOTRST

ソフトウェアによる POR や BOOTRST は SWD 接続を切断します。この切断が SWD 接続の確立中に発生した場合、デバイスがロック状態に移行する可能性があります。

ソフトウェア POR と BOOTRST をディスエーブルにして MSPM33 デバイスを安定的にデバッグします。

8.2 MSPM33 デバイスのロック解除

このセクションでは、ソフトウェアの問題が原因でデバッグ アクセスに失敗した場合のデバイスのロック解除について説明します。

8.2.1 強制的にマイコンを BSL モードに移行

BSL をサポートしており、BSL がイネーブル (デフォルトはイネーブル) に設定されているデバイスでは、ハードウェア起動メソッドを使用してマイコンに強制的に BSL モードに移行させます。その後、マイコンは ROM 内で BSL コードを実行し、アプリケーション コードは実行しません。このデバイスは、BSL モードでは SEC_AP および CS_DAP コアに接続されたままです。

注

マイコンが BSL モードに入ると、BSL はデフォルトでデバッグできないため、ユーザーは Arm® Cortex®-M33 コアに接続できません。ただし、CS_DAP コアを接続に使用できるため、ユーザーは DSSM コマンドを送信できます。

BSL モードでは、BSL コマンドをセクション 8.2.2 として、または DSSM コマンドをセクション 8.2.3 として送信して、デバイスを復旧させることができます。このアプローチにより、ソフトウェアの問題によってマイコンがロック状態に移行した場合にデバイスのロックを解除できます。

マイコンを強制的に BSL モードに移行させるための推奨方法を以下に示します。

- BSL 起動ピン (デフォルトは PA18) を VCC (プルアップ抵抗あり / なし) に接続します。デバイスの電源を入れ直します。
- BSL 起動ピン (デフォルトは PA18) を VCC (プルアップ抵抗あり / なし) に接続します。POR をトリガするために、NRST を 1 秒以上強制的に Low にします。

注

BSL 接続コマンドが UART、I2C、または CAN インターフェイスに 10 秒以内に送信されない場合、マイコンが BSL モードに移行すると、マイコンは STANDBY0 モードに移行します。

このアプローチは、次の状況では実行できません。

- NONMAIN 構成で CRC チェックに失敗しました。
- NONMAIN 構成は、SWD インターフェイスをディスエーブルするか、デバッグ アクセスをロックします。
- IWDT は、VBAT 機能をサポートするデバイスによってイネーブルになります。IWDT をディスエーブルするには VBAT を手動でオフにする必要があります。
- BSL ハードウェア起動メソッドはディセーブルです。

8.2.2 BSL コマンドを送信

NONMAIN 構成で SWD インターフェイスをディスエーブルにするか、デバッグ アクセスをロックする場合、BSL モードに移行した後に BSL コマンドを送信してデバイスのロックを解除します。

BSL 通信インターフェイス (セクション 3.2.3 を参照) が適用されて、BSL コマンドが送信されます。ROM BSL コアは、工場出荷時リセット コマンドをサポートしており、デフォルトの NONMAIN 構成に復元できます。詳細については、『MSPM33 ブートローダー ユーザー ガイド』を参照してください。

このアプローチは、次の状況では実行できません。

- BCR の構成により、工場出荷時リセットが無効に設定されている。
- BCR の構成により、NONMAIN 静的書き込み保護が無効に設定されている。
- BCR の構成で、BSL が無効に設定されている。

Copyright © 2026 Texas Instruments Incorporated

8.2.3 DSSM コマンドを生成

MSPM33 デバイスは、一括消去や工場出荷時リセットを含む DSSM コマンドをサポートしています。DSSM コマンドはブート コードで実行されます。セクション 6.3 を参照してください。CCS ツールで DSSM コマンドを使用する方法を示す例として、DebugAccessPasswordAuthentication_Auto コマンドを使用します。他の DSSM コマンド (工場出荷時リセットまたは一括消去) も同じ方法を使用しており、これには、.ccxml ファイルの同じ場所に 4 つの 32 ビット パスワードを設定することも含まれます。

CCS ツールでは、次のコマンド リストがサポートされています。

- DebugAccessPasswordAuthentication_Auto
- FactoryReset_Auto
- FactoryReset_Manual
- FactoryResetPasswordAuthentication_Auto
- FactoryResetPasswordAuthentication_Manual
- MassErase_Auto
- MassErase_Manual
- MassErasePasswordAuthentication_Auto
- MassErasePasswordAuthentication_Manual

テキサス・インスツルメンツは、FactoryReset_Auto を使用してデバイスのロックを解除することを推奨します。FactoryReset_Auto コマンドは、NRST ピンでリセット信号を生成し、デフォルトの NONMAIN 構成を復元できます。

ソフトウェアの問題が工場出荷時リセット プロセスを中断した場合 (通常はソフトウェア リセットが原因)、FactoryReset_Manual を選択して、次の手順に従ってデバイスのロックを解除します。

1. セクション 6.3 の手順に従って、プロジェクトレス デバッグを開始します。
2. NRST ラインを Low 状態に維持します (GND に接続)。
3. FactoryReset_Manual を使用して DSSM コマンドを生成します (NRST 行を Low のままにします)。
4. CCS コンソール ウィンドウに「リセット ボタンを押下」とが表示されたら、NRST ラインをリリース離します (GND から切断)。
5. 工場出荷時リセット コマンドが実行されます。

FactoryReset_Manual によるデバイスのロック解除が失敗した場合は、BSL 起動ピンを VCC に接続して強制的にマイコンを BSL モードにし (BSL モードが存在し、かつイネーブルの場合)、FactoryReset_Auto コマンドを生成します。コマンドの実行中は、デバイスがアプリケーション コードを実行しないように、BSL 起動ピン (デフォルトは PA18) を VCC に接続したままにしてください。

このアプローチは、次の場合には実行できません。

- NONMAIN 構成によって SWD 工場出荷時リセットコマンドがディスエーブルになっている。
- VBAT 機能をサポートするデバイスで IWDT がイネーブルになっており、IWDT をディスエーブルにするために VBAT を手動でオフにする必要がある。

さまざまなツールを使用して工場出荷時リセットを生成するには、『[FAQ] MSPM33C321A: 工場出荷時リセットでデバイスを回復』を参照してください。

8.3 デバッグ エラーの概要

このセクションでは、CCS ツールを使用したときに発生する一般的なデバッグ エラーと、考えられるリカバリ方法について詳しく説明します。

8.3.1 エラーコードなし: DAP 接続エラー

考えられる根本原因:

- SWD の接続の問題。
- MSPM33 デバイスが破損。
- CPU がフォルト状態に移行。
- 接続中にソフトウェア (POR または BOOTRST) またはハードウェア リセットが発生。

Copyright © 2026 Texas Instruments Incorporated

考えられるリカバリ方法:

- SWD ハードウェア接続を確認します。
- VCC、NRST、Vcore (サポートされている場合) がデータシートの仕様範囲内であることを確認します。
- NRST を強制的に Low にして、デバイスを再接続します。DAP 接続エラーが表示されない場合は、セクション 8.2 に示す方法を試してください。

8.3.2 エラー コードなし:MSPM33 コアへの接続に失敗しました

考えられる根本原因:

- NONMAIN 構成は、SWD インターフェイスをディスエーブルまたは暗号化します。
- CPU がフォルト状態に移行。
- 接続中にソフトウェア (POR または BOOTRST) またはハードウェア リセットが発生。

考えられるリカバリ方法:

- NRST ラインで Low パルスが発生していないことを確認します。
- SWD インターフェイスが暗号化されている場合は、DSSM による SWD アクセス パスワード認証を生成します。
- セクション 8.2 の手順に従ってください。

8.3.3 エラー - 6305:PRSC モジュールがルーチン レジスタの書き込みに失敗しました

セクション 8.3.2 を参照してください。

8.3.4 エラー - 260:XDS110 への接続に失敗しました

考えられる根本原因:

- XDS110 が接続されていない、または占有されていない。
- 無効な XDS110 ファームウェア、無効な XDS110 シリアル番号など。

考えられるリカバリ方法:

- XDS110 に電力を再供給し、USB 接続を確認します。
- XDS110 ファームウェアをリセットします。

8.3.5 エラー - 261:XDS110 から無効な応答

考えられる根本原因:

- XDS110 デバッガがフォルト状態に移行。
- CPU がフォルト状態に移行。

考えられるリカバリ方法:

- XDS110 デバッガに電力を再供給する。
- セクション 8.2 の手順に従ってください。

8.3.6 エラー - 615:ターゲットが、正しくフォーマットされた SWD ヘッダーを識別できません

セクション 8.3.5 を参照してください。

8.3.7 エラー - 1001:要求された操作はこのデバイスでサポートされていません

考えられる根本原因:

- ソフトウェア リセットまたはハードウェア リセットが発生。
- CPU がフォルト状態に移行。

考えられるリカバリ方法:

- NRST ラインで Low パルスが発生していないことを確認します。
- デバイスがロック状態に移行する場合は、セクション 8.2 の手順に従ってください。

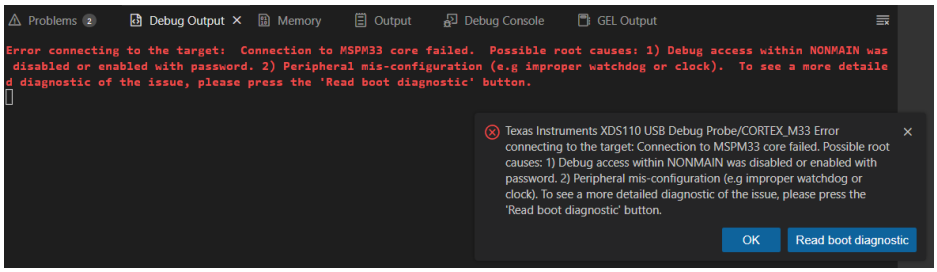
Copyright © 2026 Texas Instruments Incorporated

8.3.8 エラー - 2131 : デバイス レジスタにアクセスできません

セクション 8.3.7 を参照してください。

8.4 MSPM33 ブート診断

デバイスがロック状態に移行し、DAP が接続されたままになると、図 8-1 に示すように、CCS ツールは MSPM33 デバイスのブート診断を読み取ることができます。



CCS Version 20.x

図 8-1. CCS ツールを使用してブート診断を読み取る

表 8-1 に、一般的なブート診断読み取り値を示します。

表 8-1. 一般的なブート診断読み取り値

デバイス診断の読み取り	詳細説明
0x0000.0000	起動に失敗しました。原因として、NRST ラインが Low に保持されているか、クロック電源が無効であることが考えられます。
0x0800.0007	起動に成功。アプリケーション コードが実行され、デバイスはロックアップ状態になります。
0x0800.0016	起動に失敗しました。原因として、NONMAIN CRC チェックサム検証が失敗したことが考えられます。
0x0804.004C	起動に失敗しました。セキュア ブートはフラッシュに格納されているアプリケーション イメージを認証しようとしましたが、認証に失敗しました。
0x0804.110A	起動に成功。BSL が起動され、実行されます。
0x0807.0000	起動に失敗しました。NMI エラーはブート コード内でトリガされます。

Copyright © 2026 Texas Instruments Incorporated

9 まとめ

このユーザー ガイドでは、MSPM33 ファミリの NONMAIN 構成の概要と、NONMAIN レジスタを構成するための手順を説明しています。この資料には、基本的な知識に加えて、ユーザー向けの参考資料や補足資料も記載されています。

English Document: SDAA228
Copyright © 2026 Texas Instruments Incorporated

10 参考資料

- テキサス・インスツルメンツ、『MSPM33 C3 シリーズ 160MHz マイコン テクニカル リファレンス マニュアル』
- テキサス・インスツルメンツ、『MSPM33 ブートローダー ユーザー ガイド』
- テキサス・インスツルメンツ、『MSPM33C セキュリティ ユーザー ガイド』
- テキサス・インスツルメンツ、『MSPM33 マイコンにおける顧客セキュア コードの評価』
- テキサス・インスツルメンツ、『MSPM33 マイコンにおけるセキュア アプリケーション用 Trustzone のイネーブル』
- テキサス・インスツルメンツ、『Code Composer Studio 用クイック スタート ガイド』
- テキサス・インスツルメンツ、『IAR 用 MSPM33 SDK クイックスタート ガイド』
- テキサス・インスツルメンツ、『Keil 用 MSPM33 SDK クイックスタート ガイド』ユーザー ガイド
- テキサス・インスツルメンツ、*UniFlash フラッシュ プログラミング ツール*
- テキサス・インスツルメンツ、*C-GANG 設計および開発ツール*
- *SEGGER Microcontroller GmbH*、*J-Flash プログラム内部および外部マイコン フラッシュ ツール*
- *Emn178.Github.io*、*CRC32*、*SHA256 オンラインツール*

Copyright © 2026 Texas Instruments Incorporated

重要なお知らせと免責事項

TI は、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、 TI の販売条件 、 TI の総合的な品質ガイドライン 、 ti.com または TI 製品などに関連して提供される他の適用条件に従い提供されます。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。 TI がカスタム、またはカスタマー仕様として明示的に指定していない限り、TI の製品は標準的なカタログに掲載される汎用機器です。

お客様がいかなる追加条項または代替条項を提案する場合も、TI はそれらに異議を唱え、拒否します。

Copyright © 2026, Texas Instruments Incorporated

最終更新日：2025 年 10 月