参考資料

Application Note

MSPM0 MCU のサイバーセキュリティ・イネーブラ

TEXAS INSTRUMENTS

概要

MSPM0Gxx および MSPM0Lxx マイクロコントローラには、コード、データ、キーなどの資産を保護するためのセキュリティ対策を実装するのに役立つ、さまざまなセキュリティ・イネーブラ・テクノロジーが搭載されています。このドキュメントでは、これらのデバイスに搭載されているイネーブラ、それらの機能と制限、動作方法、基本的な使用事例に合わせた構成方法について説明します。

目次

商標

1 はじめに

産業用、車載、パーソナル・エレクトロニクスのアプリケーションがネットワーク接続され、攻撃者が利用できるツールが増加し続けるのにつれて、組込みアプリケーションでのデバイス・セキュリティの重要性も高まっていきます。テキサス・インスツルメンツの MSPM0 マイクロコントローラには、さまざまなハードウェアおよびソフトウェアのセキュリティ保護を実現するテクノロジーが搭載されており、セキュリティを考慮してアプリケーションを開発する際に活用できます。

1.1 サイバー・セキュリティの目標

一般に、組込みアプリケーションにおけるサイバー・セキュリティの主な目的は、以下の方法で重要な資産を保護することです。

- 機密性 (機密データへのアクセスを制限)
- 完全性 (データを変更から保護)
- 真正性 (すべての当事者が本人であることを保証)
- 可用性 (データや機能を必要なときに使用可能)
- 否認防止 (データの出所や ID を追加の当事者に提示可能)

これらは、多くの場合、以下の状態にある資産に適用されます。

- 休止時 (マイクロコントローラ上のコード、データ、またはキーはアクティブに使用されていない)
- 使用中 (マイクロコントローラ上のコード、データ、またはキーがアプリケーションでアクティブに使用されている)
- 転送中 (マイクロコントローラ上のコード、データ、またはキーが MCU と他のエンティティの間を移動中)

1.2 プラットフォームのセキュリティ・イネーブラ

表 1-1 に、MSPM0 デバイスに搭載されているセキュリティ・イネーブラを示します。さまざまなテキサス・インスツルメンツ製品で利用可能なセキュリティ・イネーブラの完全なリストは、テキサス・インスツルメンツのセキュリティ・ポータルを参照してください。

表 1-1. MSPM0 MCU プラットフォームのセキュリティ・イネーブラ

セキュリティ・イネーブラ	デバイスの機能	MSPM0L	MSPM0G
デバッグのセキュリティ	パスワード認証を使用したデバッグ・アクセス	すべて	すべて
	パスワード認証を使用したブートストラップ・ローダ・アクセス	すべて	すべて
	パスワード認証を使用した MAIN フラッシュ・メモリの一括消去	すべて	すべて
	パスワード認証を使用した完全な工場出荷時リセット	すべて	すべて
	テキサス・インスツルメンツ故障解析 (FA) のイネーブル / ディセーブル	すべて	すべて
	シリアル・ワイヤ・デバッグ (SWD) インターフェイスの完全なハードウェア・ディセーブル	すべて	すべて
	デバイス構成データを永続的にロック可能	すべて	すべて
	エラー耐性のあるデバイス構成データ	すべて	すべて
	パスワード・メモリにハッシュのみを格納 (SHA2-256)	予定	予定
セキュア・ブート	MAIN フラッシュ・メモリを永続的にロック可能 (静的書き込み保護)	すべて	すべて
	CRC-32 検証を使用した MAIN フラッシュ領域	すべて	すべて
	SHA2-256 検証を使用した MAIN フラッシュ・メモリ領域	予定	予定
	ブート時に MAIN フラッシュ・アプリケーションへのエントリ・ポイントを 1 つに制限	すべて	すべて
	ファームウェア・イメージ認証ルーチン (非対称型または対称型)	すべて	すべて
	キーの失効およびロールバック保護のためのロック可能なフラッシュ	予定	予定
	W^X (書き込みまたは実行) SRAM 境界	すべて	すべて

表 1-1. MSPM0 MCU プラットフォームのセキュリティ・イネーブラ (continued)

セキュリティ・イネーブラ	デバイスの機能	MSPM0L	MSPM0G
セキュア・ストレージ	静的フラッシュ・メモリの読み取り / 実行 (RX) ファイアウォール	予定	予定
	IP 保護 (実行のみ) ファイアウォール	予定	予定
	MAIN フラッシュ・バンクに W^X (書き込みまたは実行) を強制	予定	予定
	AES 揮発性キー・ストア (最大 4 つの 128 ビット・キーと 1 つのセッション・キー)	予定	予定
暗号化アクセラレーション機能	ハードウェア AES アクセラレータ (128 ビット / 256 ビット)	予定	オプション
	ハードウェア TRNG	予定	オプション
デバイス ID	固有のデバイス識別子 (96 ビット)	すべて	すべて
物理的なセキュリティ	ブート構成ルーチンによるフォルト注入攻撃への対策	予定	予定

2 デバイス・セキュリティ・モデル

MSPM0 セキュリティ・モデルでは、ブート時に一連のユーザー指定セキュリティ・ポリシーを適用することが基礎となります。このセクションでは、デバイスのブート・プロセスの概要と、さまざまなアプリケーションの使用事例を実現するために設定可能なユーザー指定のポリシーについて説明します。

2.1 ブート時の初期条件

コールド・パワーアップ (POR) 中、デバイスはセキュア状態にリセットされます。デジタル IO ピンは高インピーダンスとなり、すべてのペリフェラル機能が切断され、NRST ピンは NRST モード、シリアル・ワイヤ・デバッグ (SWD) インターフェイス・ピンは SWD モードになります。ブラウンアウト・リセットの解放後、シリアル・ワイヤ・デバッグ・ポート (SW-DP) が最初にイネーブルになり、デバッグ・プローブからデバッグ・サブシステムへの初期接続が確立されます。

ブート・プロセスのこの時点で、デバッグ・プローブからアクセス可能なデバッグ・アクセス・ポート (DAP) は、構成アクセス・ポイント (CFG-AP) とセキュア・アクセス・ポイント (SEC-AP) のみです。CFG-AP は、接続されたデバッグ・プローブで汎用デバイス情報 (デバイスの汎用部品番号など) を読み取るために使用できます。SEC-AP は、ブート構成ルーチンにコマンド・メッセージを渡すために使用できます。デバイスへのアプリケーション・デバッグ・アクセス (AHB-AP、ET-AP、および PWR-AP DAP 経由) は、ハードウェア・ファイアウォールによってブロックされたままです。そのため、デバイスの電源投入時には、デバイス・ハードウェアでプロセッサ、EnergyTrace 状態、または電源構成へのデバッグ・アクセスは許可されません。

ブラウンアウト・リセット (BOR) 後は、ブート・リセット (BOOTRST) が生成され、ブート構成ルーチンの実行が開始されます。

2.2 ブート構成ルーチン (BCR)

MSPM0 デバイスには、読み取り専用メモリ (ROM) に変更不可能な信頼ルート・ブート構成ルーチンが含まれています。ブート構成ルーチン (BCR) は、デバイスの BOOTRST に続いて Cortex-M0+ プロセッサで実行される最初のコードです。BCR は、BSL エントリを認証するために必要なブートストラップ・ローダ (BSL) のソフトウェア起動時にも実行されます。BCR の主な機能は次のとおりです。

1. 適切なデバイス動作に必要なテキサス・インスツルメンツの工場出荷時データを FACTORY フラッシュ・メモリ領域からロジックにロードし、CRC-32 を使用して工場出荷時データ (デバイスのトリム・データを含む) の整合性を検証
2. ユーザー指定のデバイス構成 (セキュリティ・ポリシーを含む) を NONMAIN フラッシュ・メモリ領域からロジックにロードし、CRC-32 を使用してユーザー構成データの整合性を検証
3. シリアル・ワイヤ・デバッグ (SWD) インターフェイス経由で送信されたブート・コマンドを確認し、(該当する場合は) それらを認証して、(認証された場合は) 処理
4. 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は BSL の呼び出し条件を確認し、有効な呼び出しが発生した場合に BSL を開始
5. ユーザー・アプリケーションを開始する前に、MAIN フラッシュ・メモリ領域のユーザー・アプリケーション・コードを含む部分の整合性を確認
6. すべてのブート・エラーを CFG-AP に記録
7. ハードウェアをトリガし、MAIN フラッシュのアドレス 0x0000.0000 からスタック・ポインタを、アドレス 0x0000.0004 からリセット・ベクトルをフェッチして、アプリケーションを開始

BCR の実行中は、AHB-AP、ET-AP、および PWR-AP DAP に SWD インターフェイス経由でアクセスすることはできません。ユーザー指定のセキュリティ・ポリシーによってデバイスへのデバッグ・アクセスが許可されている場合、ハードウェアがユーザー・アプリケーションまたはブートストラップ・ローダを起動したときに、これらの DAP が使用可能になります。

2.3 ブートストラップ・ローダ (BSL)

MSPM0 デバイスには、読み取り専用メモリ (ROM) に変更不可能なブートストラップ・ローダ (BSL) が含まれていることもあります。BSL では、シリアル・ワイヤ・デバッグ (SWD) インターフェイスではなく、標準のシリアル・インターフェイス (UART または I2C) を使用して、デバイス・メモリの内容をプログラムおよび検証できます。

BSL は BCR でのみ起動できます。BCR は、有効な BSL 呼び出し条件 (ソフトウェア起動、IO ピン起動、ブランク・デバイス起動) をチェックし、BSL を起動する前に BSL がイネーブルになっていることを検証します。BSL が終了すると、BCR が再実行され、現在のデバイス・セキュリティ・ポリシーがロードされて、ユーザー・アプリケーションが起動します。

BSL は 256 ビットのユーザー指定パスワードで保護されており、BSL セッションを開始するときに、パスワードを UART または I2C インターフェイス経由で BSL に渡す必要があります。BSL を使用しない場合は、ディセーブルにできます (BSL イネーブル / ディセーブル・ポリシーを参照)。

2.4 ブート・フロー

図 2-1 に、MSPM0 デバイスの大まかなブート・フローを示します。

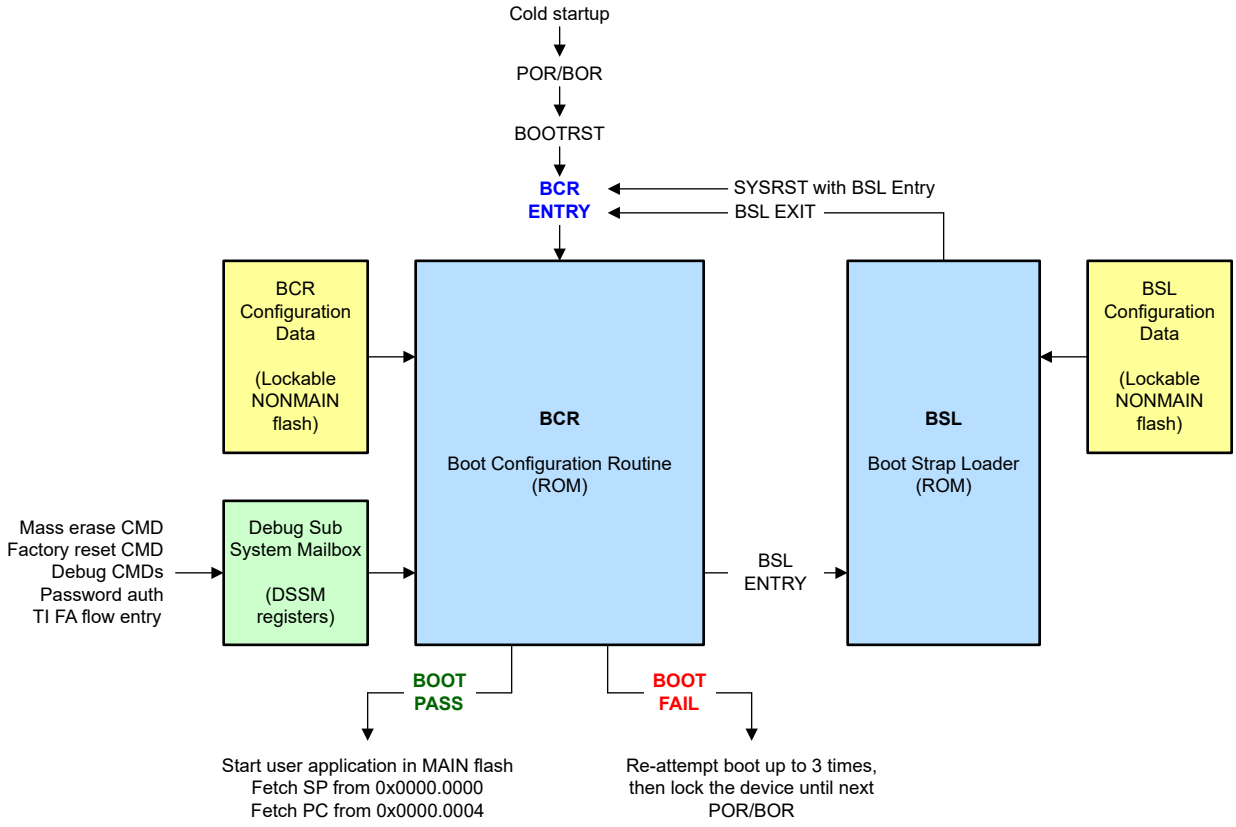

図 2-1. 大まかなブート・フロー

BCR と BSL のどちらにも、ロック可能な NONMAIN フラッシュ・メモリ領域にユーザー指定の構成データ構造が格納されています。これらのデータ構造で指定されているセキュリティ・ポリシーについては、セクション 2.5 を参照してください。

2.5 ユーザー指定のセキュリティ・ポリシー

MSPM0 デバイスには、ユーザー指定のセキュリティおよびデバイス構成ポリシーを保存するための専用のフラッシュ・メモリ領域があります。この領域を NONMAIN フラッシュ領域と呼びます。ブート構成ルーチン (BCR) およびブートストラップ・ローダ (BSL) は、デバイスを動作用に構成するため、NONMAIN フラッシュ領域に保存されているユーザー指定のデータを参照します。

製造時に、デバイスの NONMAIN フラッシュ・メモリ領域に必要なポリシーをプロビジョニングする必要があります。このセクションでは、NONMAIN 構成メモリを使用して構成可能なセキュリティ・ポリシーについて説明します。

NONMAIN フラッシュ領域は、次の 2 つの異なるデータ構造に分割されています。

- BCR 構成 (セクション 2.5.1 を参照):ブート構成のセキュリティ・ポリシーを設定
- BSL 構成 (セクション 2.5.2 を参照):ブートローダのセキュリティ・ポリシーを設定

どちらのデータ構造も、独自の 32 ビット CRC ダイジェストによってバックアップされ、構成データのエラー耐性機能の一部として使用されます。

注

BCR および BSL 構成構造には、このドキュメントに記載されているパラメータ以外のパラメータも含まれています。このドキュメントでは、セキュリティに関連するパラメータに焦点を当てています。NONMAIN フラッシュ・メモリ領域における BCR および BSL 構成構造の詳細な説明は、該当するテクニカル・リファレンス・マニュアルのアーキテクチャの章にあるブート構成のセクションを参照してください。

2.5.1 ブート構成ルーチン (BCR) のセキュリティ・ポリシー

BCR セキュリティ・ポリシーは、BCR によって解釈され、以下のパラメータが含まれます。

- シリアル・ワイヤ・デバッグ関連のポリシー (セクション 2.5.1.1 を参照)
- ブートストラップ・ローダのイネーブル / ディセーブル・ポリシー (セクション 2.5.1.2 を参照)
- フラッシュ・メモリの保護と整合性ポリシー (セクション 2.5.1.3 を参照)

2.5.1.1 シリアル・ワイヤ・デバッグ関連のポリシー

シリアル・ワイヤ・デバッグ関連のポリシーは、デバイスの物理的デバッグ・インターフェイス (SWD) 経由で利用できる機能を構成します。デフォルトでは、MSPM0 デバイスはテキサス・インスツルメンツから無制限の状態で出荷されます。この状態により、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。構成プロセスをシンプルに保ちながら各種のニーズに対応するため、MSPM0 デバイスは、制限なし (レベル 0)、カスタム制限 (レベル 1)、完全制限 (レベル 2) という 3 つの汎用セキュリティ・レベルをサポートしています。表 2-1 に、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・レベルを示します。

SWD インターフェイスには、保護することを考慮する必要がある 4 つの主な用途があります。

- アプリケーション・デバッグ・アクセス。以下のものが含まれます。
  - AHB-AP 経由でプロセッサ、メモリ・マップ、ペリフェラルにフル・アクセス
  - ET-AP 経由でデバイス EnergyTrace+ 状態情報にアクセス
  - PWR-AP 経由でデバッグを行うためのデバイス電源状態制御へのアクセス
- 以下を含む一括消去アクセス:
  - SWD 経由でコマンドを送信して MAIN メモリ領域を消去し、NONMAIN デバイス構成メモリはそのまま保持する機能
- 以下を含む工場出荷時リセットへのアクセス:
  - SWD 経由でコマンドを送信して 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 (レベル 0) にリセットする機能
- 以下を含むテキサス・インスツルメンツ故障解析アクセス:
  - テキサス・インスツルメンツが SWD 経由で故障解析の返却フローを開始する機能 (テキサス・インスツルメンツに FA アクセスが付与される前に、テキサス・インスツルメンツ FA フローにより強制的に工場出荷時リセットが実行されます。これにより、故障解析フローが開始されたときに、デバイスのフラッシュ・メモリに保存されていた独自の顧客情報をテキサス・インスツルメンツが読み取ることができないことが確実になります)。

表 2-1. 汎用セキュリティ・レベル

レベル	シナリオ	SW-DP 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	テキサス・インスツルメンツ FA ポリシー
0	制限なし	イネーブル	イネーブル	イネーブル	イネーブル	イネーブル
1	カスタム制限	イネーブル	イネーブル、パスワードでイネーブル、ディセーブル	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	イネーブル、ディセーブル
2	完全制限	ディセーブル	無関係 (SW-DP が無効な場合はアクセス不可) (1)			

(1) SW-DP ポリシーが **SW-DP ディセーブル**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、BSL を使用して利用可能な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を参照してください。

2.5.1.1.1 SWD セキュリティ・レベル 0

SWD セキュリティ・レベル 0 は、SWD セキュリティ状態のうち最も制限の少ないレベルです。これはテキサス・インスツルメンツの新しいデバイスのデフォルト状態であり、工場出荷時リセットが成功した後のデバイスの状態でもあります。この状態で故障解析を行うため、アプリケーションのデバッグ・アクセス、一括消去、工場出荷時リセットに制限はありません。

この状態を使用する状況

レベル 0 は、デバイス・メモリのプログラミングや、プロセッサとペリフェラルのデバッグが可能なため、プロトタイプ作成や開発に最適です。

この状態を使用するべきでない状況

量産ではレベル 0 を使用しないでください。攻撃者が自由にデバイス・メモリの内容を読み取り、デバイスの実行を操作し、(フラッシュ・メモリの書き込み保護方式に応じて) フラッシュ・メモリの内容を変更できてしまいます。

2.5.1.1.2 SWD セキュリティ・レベル 1

SWD セキュリティ・レベル 1 では、セキュリティ構成をカスタマイズできます。物理的デバッグ・ポート (SW-DP) はイネーブルのままにし、各機能 (アプリケーションのデバッグ、一括消去コマンド、工場出荷時リセット・コマンド、テキサス・インスツルメンツ故障分析) は個別にイネーブル、ディセーブル、または (場合によって) パスワード認証を使用してイネーブルにでき、特定の使用事例に合わせてデバイスの動作をカスタマイズすることが可能です。

この状態を使用する状況

レベル 1 は、制限されたプロトタイプ製作 / 開発シナリオや、特定の SWD 機能 (工場出荷時リセット、テキサス・インスツルメンツ故障解析など) を保持しながら、アプリケーションのデバッグなどの機能をディセーブルにする量産シナリオに最適です。表 2-2 に、レベル 1 のカスタマイズ構成の一般的な例を示します。

表 2-2. レベル 1 構成の例

レベル 1 シナリオ	構成			
	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	テキサス・インスツルメンツ FA
このシナリオでは、ユーザー指定のパスワードを使用してデバッグ・アクセスを制限するが、工場出荷時リセットとテキサス・インスツルメンツ障害解析は使用可能。この構成ではフィールド・デバッグ (パスワードを使用) が可能で、工場出荷時リセットによりデバイスをデフォルトのレベル 0 状態に戻すことも可能。	パスワードでイネーブル	ディセーブル	イネーブル	イネーブル
このシナリオではデバッグは不可。工場出荷時リセットは可能だが、ユーザー指定のパスワードが必要。これにより、MAIN メモリの内容をクリアし、パスワードがわかっている場合はデバイスをレベル 0 状態に戻すことにより、現場でデバイスを開けることが可能。工場出荷時リセット用のパスワードが漏洩した場合でも、攻撃者は MAIN フラッシュ・メモリ内の独自の情報を読み取ることは不可。	ディセーブル	ディセーブル	パスワードでイネーブル	イネーブル
このシナリオでは、デバッグとテキサス・インスツルメンツ故障解析は不可。これにより、ユーザーが FA 用にデバイスをテキサス・インスツルメンツに返却する場合に、ユーザー指定のパスワードを使用して工場出荷時リセットを実行しない限り、テキサス・インスツルメンツがデバイスに対して工場出荷時リセットおよび FA 作業を実行することは不可。	ディセーブル	ディセーブル	パスワードでイネーブル	ディセーブル

注

レベル 1 は、ほとんどの標準的な製造使用事例で推奨される構成です。セキュア・ブートを必要としないアプリケーションでは、製造にレベル 1 を使用し、工場出荷時リセットを (パスワードを指定して) イネーブルにして、テキサス・インスツルメンツ故障解析はイネーブルのままにすることをお勧めします。このような構成では、ユーザー (パスワードを使用) またはテキサス・インスツルメンツ (障害解析の返却フロー) のいずれかによるプロビジョニング後に、デバイスをより制限の少ない状態に回復できます。最大限のセキュア・ブート保護を必要とする使用事例では、製造用により制限の厳しいレベル 1 またはレベル 2 を使用できます。ただし、デバイスをプロビジョニングした後は、より制限の低い状態に回復できない可能性があるというトレードオフがあります。

この状態を使用するべきでない状況

プロトタイプ作成時にデバイスへの完全なアクセスが必要な場合は、レベル 1 を使用せず、レベル 0 を使用してください。

また、最大限の制限が必要で、SWD 機能をイネーブルにしない量産シナリオでも、レベル 1 を使用しないでください。このような場合はレベル 2 を使用して、SWD 物理インターフェイス全体を直接ディセーブルし、誤設定の可能性を最小限に抑える必要があります。

注

アプリケーション・デバッグと工場出荷時リセットをでディセーブルしてデバイスを構成した場合、ユーザーがデバイスへのデバッグ・アクセスを回復する唯一の方法は、ユーザー・アプリケーション・コードで NONMAIN 構成をより制限の少ない状態に変更するメカニズムを提供することです。NONMAIN が静的な書き込み保護によってロックされている場合は、状態を変更できず、ユーザーがデバッグ・アクセスを回復することはできません。

2.5.1.1.3 SWD セキュリティ・レベル 2

SWD セキュリティ・レベル 2 では、デバイスは最大制限状態に設定されます。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、テキサス・インスツルメンツ故障解析) には、個別の構成に関係なく、SWD からアクセスできません。

レベル 2 を選択した場合 (SW-DP がディセーブル)、アプリケーションのデバッグ構成およびテキサス・インスツルメンツ故障解析構成フィールドはデバイス構成には影響を与えません。

BSL がディセーブルの場合、一括消去および工場出荷時リセットの構成フィールドも無関係なフィールドになります。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。

この状態を使用する状況

レベル 2 を量産に使用するのは、SWD 機能にこれ以上アクセスする必要がなく、デバイスに最大のセキュア状態が求められる場合のみにしてください。

この状態を使用するべきでない状況

以下の場合はレベル 2 を使用しないでください。

- 将来のアプリケーションのデバッグや、SWD による再プログラミングが必要になる可能性がある場合
- テキサス・インスツルメンツによるデバイスの故障解析を実行できるようにしたい場合
- SWD 経由で一括消去コマンドまたは工場出荷時リセット・コマンドを送信してフラッシュ・メモリから独自の情報を削除できるようにしたい場合

注

デバイスをレベル 2 (SW-DP ディセーブル) で構成した後は、SWD 経由でデバイスにアクセスすることは**できなくなります**。デバイスを SWD アクセスが可能なレベル 0 またはレベル 1 の状態に戻すことができるのは、BSL と工場出荷時リセットの両方がイネーブル (BSL で工場出荷時リセット・コマンドを送信可能) になっている場合か、またはユーザー・アプリケーション・コードに含まれるメカニズムにより、NONMAIN 構成を制限の少ない状態に変更できる場合のみです。いずれの場合も、NONMAIN が静的な書き込み保護によってロックされている場合は、レベル 2 状態から変更できず、SWD アクセスを回復することはできません。

2.5.1.2 ブートストラップ・ローダ (BSL) のイネーブル / ディセーブル・ポリシー

ブートストラップ・ローダ (BSL) では、シリアル・ワイヤ・デバッグ・インターフェイスではなく、標準のシリアル・インターフェイス (UART または I2C) を使用して、デバイス・メモリをプログラムおよび検証できます。BSL には独自の構成ポリシーがありますが、BSL の起動をイネーブルにするか、ディセーブル (起動不可) にするかは、BCR が決定します。

BSL には追加の攻撃対象領域が存在するため、アプリケーションで BSL を使用しない場合は、ユーザー指定のブート・セキュリティ・ポリシーでディセーブルにできます。BSL をアプリケーションで使用する場合、BSL セキュリティ設定 (BSL アクセス用のパスワードを含む) は BSL 構成ポリシーで管理されます。

2.5.1.3 フラッシュ・メモリの保護と整合性ポリシー

フラッシュ・メモリの保護および整合性ポリシーでは、変更されないようにロックするフラッシュ・メモリのセクタと、ユーザー・アプリケーションを開始する前のブート・プロセス中に整合性をチェックするセクタを指定します。

2.5.1.3.1 アプリケーション (MAIN) フラッシュ・メモリのロック

MSPM0 MCU には、静的書き込み保護方式が実装されており、MAIN フラッシュ領域のユーザー定義セクタを実行時のプログラム / 消去操作からロックアウトできます。目的の静的書き込み保護方式は、NONMAIN フラッシュ領域のブート・セキュリティ・ポリシーの一部として構成されます。

目的

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をフラッシュ・メモリに配置できるようになります。

- プログラムおよびロックされた後は、アプリケーション・コードまたは ROM ブートローダで変更することはできません。
- コードをフラッシュ・メモリの先頭に配置すると、ROM ブート構成ルーチンがユーザー・アプリケーションに実行を移行すると、必ずそのコードが最初に実行されます。

MSPM0 静的書き込み保護は両方の特性をサポートしており、セキュア・ブート・イメージ・マネージャを実装するにはこれらの特性を満たす必要があります。

機能

NONMAIN のセクタが書き込みロックされている場合、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・コードに実行を移行する場合、機能を変更することはできません。静的に保護されたセクタ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。

静的書き込み保護は、アプリケーション・コードまたはブートローダによる変更は防止しますが、SWD インターフェイス経由で送信される一括消去または工場出荷時リセット・コマンドは実行されます。この動作が望ましくない場合は、一括消去または工場出荷時リセットを行う SWD コマンドを固有のパスワードを使用して保護するか、ディセーブルできます (SWD ポリシーを参照)。静的に書き込み保護された MAIN フラッシュ・セクタを変更する手段を完全に削除するには、一括消去および工場出荷時リセット・コマンド (または SW-DP) をディセーブルする必要があります。また、NONMAIN ブート構成メモリを静的に書き込み保護し、アプリケーション・コードが NONMAIN 領域の内容を変更して下位の書き込み保護方式を変更するのを防止する必要があります。これについては、次のセクションで説明します。

2.5.1.3.2 構成 (NONMAIN) フラッシュ・メモリのロック

MSPM0 MCU には、静的書き込み保護機能が実装されており、NONMAIN フラッシュ領域を実行時のプログラム / 消去操作からロックアウトできます。書き込み保護機能は、NONMAIN フラッシュ領域のブート・セキュリティ・ポリシーの一部として構成されます。

目的

テキサス・インスツルメンツのデフォルトでは、NONMAIN 構成メモリ (ユーザー指定のブート・セキュリティ・ポリシーとブートストラップ・ローダ・ポリシーを含む) は書き込み保護の状態になっていません。これにより、プロビジョニング中にユーザーが NONMAIN を消去し、量産時に使用されるユーザー指定のポリシーで再プログラミングすることができます。

多くの場合、構成メモリはプロビジョニング後にロックするのが適切です。構成メモリをロックすると、セキュリティ・ポリシー、ブートストラップ・ローダ・ポリシー、静的書き込み保護ポリシーが、ブートストラップ・ローダまたはアプリケーション・コードによって不正に変更されるのを防止できます。ほとんどのアプリケーションでは、量産デバイスの構成メモリの変更は、デバイスのファームウェアが更新された場合でも必要ありません。

機能

保護するように構成した場合、NONMAIN 領域全体が書き込みロックされ、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・コードに実行を移行したときに、機能を変更することはできません。NONMAIN 領域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。

静的書き込み保護は、アプリケーション・コードまたはブートローダによる変更は防止しますが、SWD インターフェイス経由で送信される工場出荷時リセット・コマンドは実行されます。この動作が望ましくない場合は、工場出荷時リセットを行う

SWD コマンドを固有のパスワードを使用して保護するか、ディセーブルできます (SWD ポリシーを参照)。NONMAIN 構成メモリを変更する手段を完全に削除するには、工場出荷時リセット・コマンドとテキサス・インスツルメンツ FA (または SW-DP) をディセーブルする必要があります。

注

NONMAIN が静的に書き込み保護されており、工場出荷時リセット・コマンドとテキサス・インスツルメンツ FA (または SW-DP) がディセーブルの場合、NONMAIN は変更不可能な読み取り専用メモリと同等であり、いかなる方法でもデバイス構成を変更することはできません。さらに、MAIN メモリ領域セクタのいずれかが静的保護機能を使用して構成されている場合、これらのセクタはいかなる方法でも変更できず、変更不可能とみなすことができます。

2.5.1.3.3 アプリケーション (MAIN) フラッシュ・メモリの整合性の検証

BCR は、BCR (ROM 内) からユーザー・アプリケーション (MAIN フラッシュ・メモリ内) に実行を移行する前に、MAIN フラッシュ・メモリ内のユーザー指定アドレス範囲のデータ整合性をチェックすることをサポートしています。

目的

整合性チェックは、ブート ROM (通常はセキュア・ブート・イメージ・マネージャ) の後に最初に実行されるコードに対して、予測される値と一致する CRC ダイジェストが含まれていることを確認するための追加ステップとして使用できます。この整合性チェックにより、フラッシュ・メモリ内の重要なコード (残りのユーザー・アプリケーション・ソフトウェア・イメージの認証を実行) が破損しているためにセキュリティの脆弱性が発生する可能性が低減されます。

機能

開始アドレス、長さ、および ISO-3309 CRC-32 ダイジェストを、NONMAIN 構成メモリにプロビジョニングできます。ブート・プロセス中に、BCR は MAIN フラッシュ・メモリ内の指定された範囲の CRC-32 ダイジェストを計算し、計算されたダイジェストをプロビジョニングされた (予測される) ダイジェストと比較して検証します。値が一致している場合は、ユーザー・アプリケーションが開始します。値が一致しない場合は、ユーザー・アプリケーションは開始せず、重大なブート・エラーが発生します。

2.5.2 ブートストラップ・ローダ (BSL) のセキュリティ・ポリシー

BSL セキュリティ・ポリシーは、ブートローダが呼び出されたときにブートローダーにより解釈され、次のパラメータが含まれます。

- BSL アクセス・パスワード (セクション 2.5.2.1 を参照)
- BSL 読み出しポリシー (セクション 2.5.2.2 を参照)
- BSL セキュリティ・アラート・ポリシー (改ざん検出) (セクション 2.5.2.3 を参照)

2.5.2.1 BSL アクセス・パスワード

BSL へのアクセスは、ユーザーが指定した 256 ビットのパスワードで保護されます。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。ほとんどの BSL 機能にアクセスできるようにするには、BSL を呼び出した後にパスワードを入力する必要があります。パスワードを入力しない場合、使用できる BSL コマンドは Get Identity および Start Application のみです。

BSL に誤ったパスワードを供給すると、BSL は 2 秒間停止し、その後パスワードを入力し直すことができます。パスワード入力に 3 回失敗すると、セキュリティ・アラート機能がアクティブになります (セクション 2.5.2.3 を参照)。

2.5.2.2 BSL 読み出しポリシー

BSL はオプションで、デバッグや診断の目的でデバイス・メモリの読み出しをサポートできます (パスワードが一致して BSL にアクセスできるようになった後)。デフォルトでは、デバイスから機密コードやデータが抽出されるのを防止するため、この機能はセキュリティ上ディセーブルになっています。BSL 読み出しポリシーがディセーブルの場合、BSL インターフェイス経由でホストに送信できる情報は、最小セグメント長が 1KB であるメモリ・セグメントの CRC32 ダイジェストのみです。デバイス・メモリを直接読み出す必要がある場合は、BSL 構成でイネーブルにできます。

2.5.2.3 BSL セキュリティ・アラート・ポリシー

BSL には、改ざんの疑いがある場合に対処するためのアラート・メカニズムがあります。具体的には、1 つの BSL セッション中に誤ったパスワードが 3 回 BSL に渡された場合、セキュリティ・アラートがアクティブになり、BSL は指定されたセキュリティ・アラート・ポリシーに基づいて、次の 3 つの方法のいずれかで応答します。

1. 工場出荷時リセットの発行 (MAIN フラッシュを消去し、NONMAIN フラッシュ領域をリセット)
2. BSL をディセーブル (MAIN フラッシュはそのままにし、NONMAIN を再構成して BSL アクセスをブロック)
3. 無視 (構成は変更せず、パスワードの試行を継続的に許可)

注

オプション 1 および 2 を選択するには、NONMAIN フラッシュ領域が静的に書き込み保護されていることが必要です (セクション 2.5.1.3.2 を参照)。

オプション 1 を選択した場合、静的に書き込み保護されている MAIN メモリ領域 (セクション 2.5.1.3.1 を参照) は、工場出荷時リセット時に消去されません。

2.5.3 構成データのエラー耐性

MSPM0 デバイスには、NONMAIN 構成メモリにデータ・エラーが発生してセキュリティが失われる可能性を削減するため、複数のメカニズムが備えられています。

2.5.3.1 CRC で保護された構成データ

NONMAIN メモリの BCR 構成データと BSL 構成データ構造には、それぞれの構造の CRC32 ダイジェストに対応する CRC32 値が含まれています。デバイスのブート・プロセス中に、BCR はデータ構造の CRC ダイジェストを計算し、格納されている CRC 値と比較して、構造体内に含まれるデータが信頼できるものかを確認します。

BCR 構成の CRC エラーの処理

ブート中に BCR 構成データ (SWD ポリシー、BSL イネーブル / ディセーブル・ポリシー、フラッシュ・メモリ保護および整合性チェック・ポリシーを含む) 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。

- エラーの原因をブート診断として CFG-AP に記録
- BSL はイネーブルに設定されていても起動しない
- 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

この CRC チェックの利点は、静的書き込み保護構成 (セキュア・ブートの中核) などの構成データに反転ビットがある場合に、それをブート・プロセス中に高い信頼性で検出できることです。エラー処理手順では、BSL およびユーザー・アプリケーションの実行が明示的に防止され、サポートされているオプション (SWD 工場出荷時リセットおよび TI FA) のみが 16 ビットのパターン一致フィールドによって保護されます。

BSL 構成の CRC エラーの処理

BSL 呼び出し中に BSL 構成データ (BSL パスワードおよび BSL ポリシーを含む) 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 はイネーブルに設定されていても起動しない
- 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
- 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

この CRC チェックの利点は、BSL 構成データ内に反転ビットがある場合に、それを起動プロセス中に高い信頼性で検出できることです。このエラー処理手順により、BSL が無効なデータから開始するのを防止できます。無効なデータから開始すると、セキュリティが失われる可能性があります。

テキサス・インスツルメンツの工場出荷時トリム・データの CRC エラー処理

ユーザーが指定した構成データに加えて、ブート中にテキサス・インスツルメンツの工場出荷時トリムの CRC チェックがエラーとなった場合も、致命的なブート・エラーが発生し、以下の制限が発生します。

- エラーの原因をブート診断として CFG-AP に記録
- BSL はイネーブルに設定されていても起動しない
- 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

2.5.3.2 クリティカル・フィールドの 16 ビット・パターン一致

SWD セキュリティ・ポリシーなどの BCR 構成メモリ内の重要なポリシーは、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

これにより、1 ビットの反転によって、デバイスが指定されていたものより低いセキュリティ状態に移行してしまうことが防止されます。

3 セキュア・ブート

MSPM0 デバイスは、ハードウェア機能とソフトウェア機能の組み合わせにより、アプリケーション・ソフトウェア (セキュア・ブート) の認証をサポートしています。非対称型および対称型の認証方式がサポートされていますが、すべての MSPM0 デバイスにソフトウェアの悪用から対称キーを保護するためのセキュア・ストレージが搭載されているわけではありません。

MSPM0 アーキテクチャには、セキュア・ブートを実現するために必要ないくつかの重要なハードウェア機能が含まれています。

- 固定認証ファームウェアと認証キーを格納するためのロック可能なフラッシュ・メモリ
- ブート中のエントリ・ポイントを 1 つにし、セキュア・ブート・イメージ・マネージャが常に BCR の後実行される最初のアプリケーションであることを保証

MSPM0 ソフトウェア開発キット (SDK) には、MSPM0 MCU にセキュア・ブートを実装するためのブート・イメージ・マネージャ (BIM) リファレンス・アプリケーションが含まれています。このリファレンス・アプリケーションは、MSPM0 デバイスに簡単に構成およびプロビジョニングできます。

3.1 セキュア・ブート認証フロー

セキュア・ブートをサポートするデバイスを準備するには、以下のプロビジョニング手順が必要です。

1. ブート・イメージ・マネージャ・ファームウェアは、MAIN フラッシュ・メモリに構成およびプログラムする必要があります。リセット・ベクトルは 0x0000.0004 で、ブート・イメージ・マネージャの開始を指しています。
2. ブート・イメージ・マネージャが必要とするすべての認証キー・マテリアルは、ブート・イメージ・マネージャに隣接する MAIN フラッシュ・メモリにプログラムする必要があります。
3. デバイスの NONMAIN 構成メモリは、次のようにプログラムする必要があります。
   a. ブート・イメージ・マネージャ・ファームウェアと認証キー・マテリアルを含む MAIN フラッシュ・セクタは、変更を防止するため静的書き込み保護として構成する必要があります。
   b. NONMAIN フラッシュ・セクタは、変更を防止するため静的書き込み保護として構成する必要があります。
   c. 一括消去および工場出荷時リセット・コマンドは、パスワード保護またはディセーブルすることを推奨します。上記の構成設定で工場出荷時リセットをディセーブルすると、NONMAIN 構成がブート・イメージ・マネージャおよび認証キーを含むセクタと共に永続的にロックされます。
   d. MAIN フラッシュ・メモリの整合性チェックはイネーブルにし、アドレス範囲をブート・イメージ・マネージャと認証キーを含めるように設定することを推奨します。

プロビジョニングが完了し、署名済みファームウェアがデバイスにプログラムされると、デバイスの電源投入からのセキュア・ブート・フローは次のようになります。

1. 電源投入時、デバイスは最大のセキュア状態になります。BCR がデバイス構成メモリの整合性をチェックし、デバイス構成が有効な場合はそれに応じてユーザー指定のポリシーをロードします。
2. BCR が BIM と認証キー・マテリアルを含む MAIN フラッシュ・メモリに対応する CRC 値を計算します。CRC チェックに成功すると、BCR は最初のユーザー・コード (ブート・イメージ・マネージャ) に実行を移行します。
3. ブート・イメージ・マネージャが、残りのアプリケーション・コードのダイジェストを計算します。
   a. 非対称認証の場合、アプリケーション・コードのセキュア・ハッシュ (SHA2-256) ダイジェストはソフトウェアで計算されます。
   b. 対称型認証の場合、アプリケーション・コードに対応する CMAC メッセージ認証コードは、認証キーを使用して計算されます。
4. ブート・イメージ・マネージャが、供給された署名に対してダイジェストを検証します。
   a. 非対称認証の場合、楕円曲線デジタル署名アルゴリズム (ECDSA) を使用してソフトウェアでデジタル署名が復号化され、その結果が計算されたハッシュと比較されます。
   b. 対称型認証の場合、計算された CMAC がデジタル署名の CMAC と比較されます。
5. アプリケーション・コード・ダイジェストが署名と一致すると、アプリケーション・コードが開始します。一致しない場合は、ユーザー指定のエラー・ハンドラが呼び出されます。

3.2 非対称型と対称型のセキュア・ブート

MSPM0 SDK に搭載されているブート・イメージ・マネージャは、非対称型と対称型のセキュア・ブートをサポートしていますが、2 つの実装の間にはトレードオフが存在します。特定のアプリケーションに対して、これらのトレードオフを注意深く検討する必要があります。表 3-1 に、2 つの方式のトレードオフを示します。

表 3-1. セキュア・ブート・アルゴリズムの比較

パラメータ	非対称型 (SHA2 + ECDSA)	対称型 (CMAC)
認証時間	長い (ソフトウェア・ハッシュの計算と公開キーの演算のため)	短い (アルゴリズムが簡素で、ハードウェア AES アクセラレーションが利用可能な場合に活用できるため)
コードのサイズ	大きい (SHA および ECDSA アルゴリズムのため)	小さい (特にターゲット・デバイスで AES アクセラレーションを利用できる場合)
キーの整合性	公開キーがデバイスにプロビジョニングされ、変更不可能であることが必要	共有キーがデバイスにプロビジョニングされ、変更不可能であることが必要
キーの機密性	公開キーには機密性の要件はなく、公開キーをアプリケーション・コードの脆弱性から保護する必要なし	共有キーは機密情報として保護し、使用しないときには、アプリケーション・コードの脆弱性から保護するため、ラップして静的読み取りファイアウォール (ターゲット・デバイスでサポートされる場合) で保護する必要あり

ほとんどの状況では、非対称型の実装を推奨します。コード・サイズが限られている場合や、認証時間を最小限に抑える必要がある場合には、対称型の実装を使用できます。ただし、共有キーを注意深く管理する必要があります。すべてのデバイスに、ソフトウェアの脆弱性から共有対称キーを保護するためのセキュアなストレージが搭載されているわけではありません。

4 暗号化アクセラレーション機能

一部の MSPM0 MCU には、AES (Advanced Encryption Standard) のハードウェア・アクセラレーション機能と、暗号化目的に真の乱数を生成するためのハードウェア (TRNG) が搭載されています。デバイスに AES アクセラレータまたは TRNG が搭載されているかどうかを確認するには、該当するデバイスのデータシートを参照するか、Appendix A を参照してください。

4.1 ハードウェア AES アクセラレーション

一部の MSPM0 デバイスには、AES (Advanced Encryption Standard) のハードウェア・アクセラレーション機能が備わっています。デバイスに AES アクセラレータが搭載されているかどうかを確認するには、該当するデバイスのデータシートを参照してください。

4.1.1 概要

AES アクセラレータ・モジュールは、AES (Advanced Encryption Standard) に従って 128 ビットまたは 256 ビットのキーをハードウェアに配置し、128 ビットのデータ・ブロックの暗号化と復号化を実行します。AES は、FIPS PUB 197 で規定されている対称キー・ブロック暗号アルゴリズムです。

AES アクセラレータには、次のような機能があります。

- AES 128 ビット・ブロックの暗号化および復号化
- NIST SP 800-38 で定義されている ECB、CBC、OFB、CFB ブロック暗号モードを自動化するための DMA トリガのサポート
- 事前に計算された (nonce || counter) ブロックの暗号化による CTR 暗号モードおよび生成されたキー・ストリームを使用するテキストの XOR の高速化をサポート
- CBC-MAC タグ計算の高速化 (ゼロ初期化ベクトルを使用した CBC DMA モード) をサポート
- 暗号化と復号化のためのオンザフライ方式キー拡張機能
- 復号化用のオフライン・キー生成
- シャドウ・レジスタにすべてのキー長の初期キーを格納
- 8 ビット・バイトまたは 32 ビット・ワードのアクセスにより、キー・データ、入力データ、および出力データを供給
- AES 準備完了割り込み
- RUN モードと SLEEP モードをサポート (デバイスのテクニカル・リファレンス・マニュアルの「動作モード」セクションを参照)

AES アクセラレータ・ハードウェアは、128 ビットのステート・メモリと関連の入出力レジスタ、AES 暗号化 / 復号化コアと制御ロジック、256 ビットの AES キー・メモリと関連の入力レジスタで構成されています。図 4-1 に AES のハードウェアを示します。

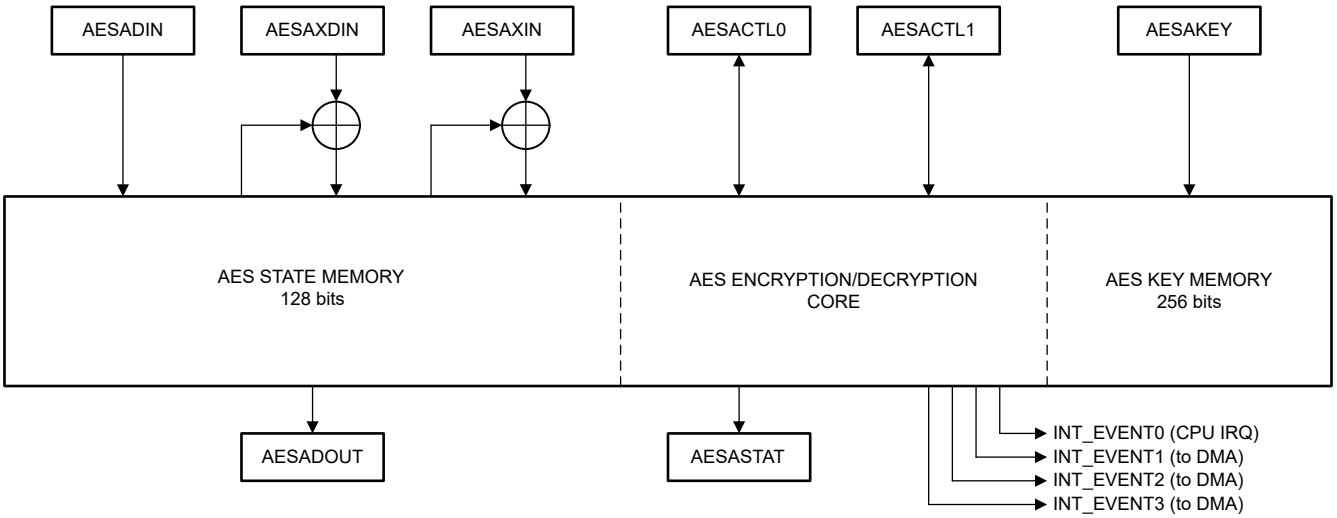

図 4-1. AES アクセラレータのブロック図

4.1.2 AES の性能

AES アクセラレータは、128 ビット・ブロックの高速暗号化と復号化を実現します。表 4-1 に、AES アクセラレータの性能を、ブロック暗号化とブロック復号化 (事前に生成された復号化キーを使用) のサイクル数と実行時間で示します。

表 4-1. AES ハードウェア・アクセラレータの主な性能指標

AES キー長	暗号化 (OPx==0x0)			復号化 (OPx==0x3)		
	サイクル数	時間 (32MHz)	時間 (80MHz)	サイクル数	時間 (32MHz)	時間 (80MHz)
128 ビット	168	5.25µs	2.10µs	168	5.25µs	2.10µs
256 ビット	234	7.31µs	2.93µs	234	7.31µs	2.93µs

4.2 ハードウェア真性乱数生成器 (TRNG)

一部の MSPM0 デバイスには、ハードウェア真性乱数生成器 (TRNG) ブロックが搭載されています。TRNG を使用すると、真の乱数シード値を簡単に生成でき、生成された値を決定論的乱数生成器 (DRBG) のシードとして使用できます。

TRNG モジュールは、デバイス内のデルタ-シグマ変調ベースのアナログ・エントロピー・ソースに基づいて、32 ビットの真性乱数出力を生成します。TRNG には、電力操作攻撃から保護するため、専用レギュレータが付属しています。

内蔵された診断テストにより TRNG のアナログおよびデジタル・コンポーネントのパワーオン・セルフ・テストを実行でき、統計的なセルフ・テストにより連続的な監視が可能になります。

TRNG は、暗号化乱数生成器用の NIST SP800-22 統計テスト・スイートに合格できる TRNG + DRBG システムの作成に適しています。図 4-2 に、TRNG のブロック図を示します。

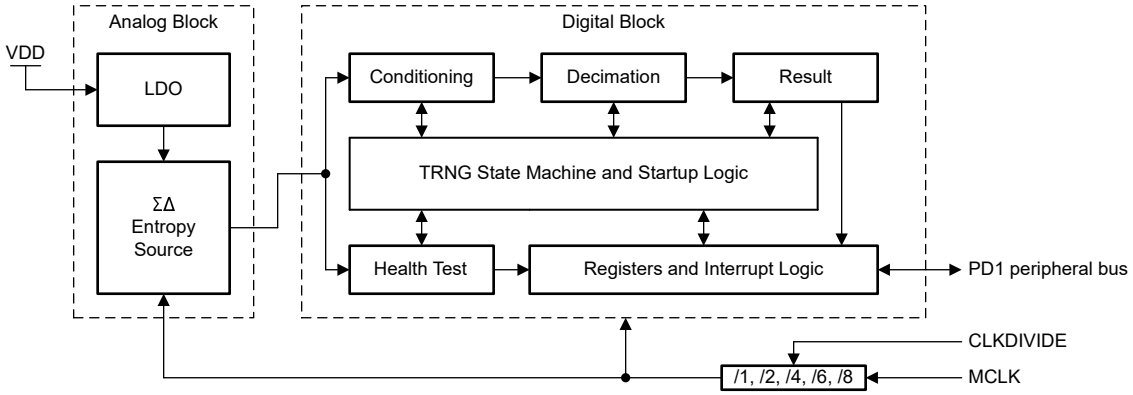

図 4-2. TRNG のブロック図

TRNG の動作の詳細については、デバイス・ファミリのテクニカル・リファレンス・マニュアルを参照してください。

5 デバイス ID

すべての MSPM0 デバイスには、96 ビットのユニット固有識別コード (デバイス ID) が含まれており、アプリケーション・ソフトウェアで読み取ることができます。デバイス ID の詳細については、テクニカル・リファレンス・マニュアルとデバイスのデータシートを参照してください。

デバイス ID は、出荷される各ユニットで固有であり、特定のユニットと他のユニットを識別または区別するために使用できます。デバイス ID は固有ですが、一部のビットは部品番号や製品リビジョンなどのデバイス特性に対応しているため、暗号論的にランダムではありません。

6 まとめ

MSPM0 MCU が提供するセキュリティ・イネーブラは、新しいアプリケーションにサイバー・セキュリティ機能を追加する場合に、機能と価値を提供します。魅力的な価格帯で独自の機能 (パスワード認証を使用した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など) が搭載されているため、構成をシンプルかつ明確なものに維持しながら、さまざまな開発と製造現場で使用できます。

7 関連資料

- テキサス・インスツルメンツ、セキュリティ電子書籍 (SWPB021)
- テキサス・インスツルメンツ、セキュリティ・ポータル (リンク)
- 『MSPM0G テクニカル・リファレンス・マニュアル』(SLAU846)
- 『MSPM0L テクニカル・リファレンス・マニュアル』(SLAU847)

8 改訂履歴

資料番号末尾の英字は改訂を表しています。その改訂履歴は英語版に準じています。

日付	リビジョン	注:
2023 年 1 月	*	初版

A サブファミリ別のセキュリティ・イネーブラ

表 A-1 に、各 MSPM0 サブファミリに含まれるセキュリティ・イネーブラを示します。将来の MSPM0 デバイスに計画されており、表に示すデバイス・ファミリには含まれていない機能があることに注意してください。

表 A-1. MSPM0 サブファミリ別のセキュリティ・イネーブラ

セキュリティ・イネーブラ	セキュリティ・イネーブラ	MSPM0L110x	MSPM0L13xx	MSPM0G110x	MSPM0G150x	MSPM0G3x0x
デバッグのセキュリティ	パスワード認証を使用したデバッグ・アクセス	あり				
	パスワード認証を使用したブート・ストラップ・ローダ・アクセス	あり				
	パスワード認証を使用した MAIN フラッシュ・メモリの一括消去	あり				
	パスワード認証を使用した完全な工場出荷時リセット	あり				
	テキサス・インスツルメンツ故障解析 (FA) のイネーブル / ディセーブル	あり				
	シリアル・ワイヤ・デバッグ (SWD) インターフェイスの完全なハードウェア・ディセーブル	あり				
	デバイス構成データを永続的にロック可能	あり				
	エラー耐性のあるデバイス構成データ	あり				
	パスワード・メモリにハッシュのみを格納 (SHA2-256)	なし				
セキュア・ブート	MAIN フラッシュ・メモリを永続的にロック可能 (静的書き込み保護)	あり				
	CRC-32 検証を使用した MAIN フラッシュ領域	あり				
	SHA2-256 検証を使用した MAIN フラッシュ・メモリ領域	なし				
	ブート時に MAIN フラッシュ・アプリケーションへのエントリ・ポイントを 1 つに制限	あり				
	ファームウェア・イメージ認証ルーチン (非対称型または対称型)	あり				
	キーの失効およびロールバック保護のためのロック可能なフラッシュ	なし				
	SRAM W^X (書き込みまたは実行) 境界の強制	あり				
セキュア・ストレージ	静的フラッシュ・メモリの読み取り / 実行 (RX) ファイアウォール	なし				
	IP 保護 (実行のみ) ファイアウォール	なし				
	MAIN フラッシュ・バンクに W^X (書き込みまたは実行) を強制	なし				
	AES 揮発性キー・ストア (最大 4 つの 128 ビット・キーと 1 つのセッション・キー)	なし				
暗号化アクセラレーション機能	ハードウェア AES アクセラレータ (128 ビット / 256 ビット)	なし			あり	
	ハードウェア TRNG	なし			あり	
デバイス ID	固有のデバイス識別子 (96 ビット)	あり				
物理的なセキュリティ	ブート構成ルーチンによるフォルト注入攻撃への対策	なし				

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、または ti.com やかかる TI 製品の関連資料などのいずれかを通じて提供する適用可能な条項の下で提供されています。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。

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

郵送先住所：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265