

**32 ビット RISC マイクロコントローラー
リファレンスマニュアル**

**セキュリティー機能
(SECG2-A)**

Revision 1.0

2026-01

東芝デバイス&ストレージ株式会社

目次

序章	3
関連するドキュメント	3
表記規約	4
1. 概要	6
2. 構成	6
3. 機能説明	7
3.1. チッププロテクト(CPRO)	7
3.1.1. 機能	7
3.1.2. 動作説明	7
3.2. セキュアアクセスメモリー(SAM)	9
3.2.1. 機能	9
3.3. 解除不能フラッシュプロテクト(NRFP)	10
3.3.1. 機能	10
3.3.2. 動作説明	10
3.4. 東芝テストモード制御(TCON)	10
3.4.1. 機能	10
3.4.2. 動作説明	10
3.5. RAM 転送コマンド(シングルブートモード)	11
3.5.1. 機能	11
3.5.2. 動作説明	11
4. 使用方法の例	12
5. 改訂履歴	14
製品取り扱い上のお願い	15

図目次

図 2.1 セキュリティー機能	6
-----------------------	---

表目次

表 3.1 チッププロテクトの対象	7
表 5.1 改訂履歴	14

序章

関連するドキュメント

文書名
データシート
クロック制御と動作モード
例外
セキュアアクセスメモリー
フラッシュメモリー

表記規約

- 数値表記は以下の規則に従います。
16 進数表記: 0xABC
10 進数表記: 123 または 0d123 (10 進表記であることを示す必要のある場合だけ使用)
2 進数表記: 0b111 (ビット数が本文中に明記されている場合は「0b」を省略可)
- ローアクティブの信号は信号名の末尾に「_N」で表記します。
- 信号がアクティブレベルに移ることを「アサート(assert)」アクティブでないレベルに移ることを「デアサート(deassert)」と呼びます。
- 複数の信号名は[m:n]とまとめて表記する場合があります。
例: S[3:0]は S3、S2、S1、S0 の 4 つの信号名をまとめて表記しています。
- 本文中[]で囲まれたものはレジスターを定義しています。
例: [ABCD]
- 同種で複数のレジスター、フィールド、ビット名は「n」で一括表記する場合があります。
例: [XYZ1]、[XYZ2]、[XYZ3] → [XYZn]
- 「レジスター一覧」中のレジスター名でユニットまたはチャネルは「x」で一括表記しています。
ユニットの場合、「x」は A、B、C、...を表します。
例: [ADACR0]、[ADBCR0]、[ADCCR0] → [ADxCR0]
チャネルの場合、「x」は 0、1、2、...を表します。
例: [T32A0RUNA]、[T32A1RUNA]、[T32A2RUNA] → [T32AxRUNA]
- レジスターのビット範囲は[m:n]と表記します。
例: [3:0]はビット 3 から 0 の範囲を表します。
- レジスターの設定値は 16 進数または 2 進数のどちらかで表記されています。
例: [ABCD]<EFG> = 0x01 (16 進数)、[XYZn]<VW> = 1 (2 進数)
- ワード、バイトは以下のビット長を表します。
バイト: 8 ビット
ハーフワード: 16 ビット
ワード: 32 ビット
ダブルワード: 64 ビット
- レジスター内の各ビットの属性は以下の表記を使用しています。
R: リードオンリー
W: ライトオンリー
R/W: リード/ライト
- 断りのない限り、レジスターアクセスはワードアクセスだけをサポートします。
- 本文中の予約領域「Reserved」として定義されたレジスターは書き換えを行わないでください。
また、読み出した値を使用しないでください。
- Default 値が「-」となっているビットから読み出した値は不定です。
- 書き込み可能なビットフィールドと、リードオンリー「R」のビットフィールドが共存するレジスターに書き込みを行う場合、リードオンリー「R」のビットフィールドには Default 値を書き込んでください。
Default 値が「-」となっている場合は、個々のレジスターの定義に従ってください。
- ライトオンリーのレジスターの Reserved ビットフィールドには Default 値を書き込んでください。
Default 値が「-」となっている場合は、個々のレジスターの定義に従ってください。
- 書き込みと読み出しで異なる定義のレジスターへのリードモディファイライト処理は行わないでください

本資料に記載されている社名・商品名・サービス名などは、それぞれ各社が商標として使用している場合があります。

1. 概要

本製品は、内部のデータ、製品の制御などの資産の保護を目的としたセキュリティ機能を搭載しています。

機能分類	機能	動作説明
通信の遮断	チッププロテクト(CPRO)	以下の機能を禁止または制限します。 ・デバッグツール(JTAG/SW) ・RAM モニターツール(NBDIF) ・フラッシュ書き込みツール(フラッシュライターモード時)
メモリーへのアクセス制御	セキュアアクセスメモリー (SAM)	バスマスターからメモリーへのアクセスを制御します。 3つのステートを持ち、各ステートでアクセス可能な領域が定義されます。 シングルブートモードは動作しません。
フラッシュメモリーの書き込み/消去禁止	解除不能フラッシュプロテクト (NRFP)	フラッシュメモリーの消去/書き込みを禁止します。 有効にすると、解除することはできません。 シングルブートモードおよびフラッシュライターモードは動作しません。
テストモード制御	東芝テストモード制御(TCON)	当社のテストモードへの遷移を禁止します。 フラッシュライターモードは動作しません。
パスワード認証	シングルブートモード RAM 転送コマンド	シングルブートモードにて、RAM 転送コマンドを実行する場合には 255 バイトのデータ長のパスワード認証が必要です。

2. 構成

製品とセキュリティ機能の関係の概略を示します。点線枠がセキュリティ機能による保護を表しています。

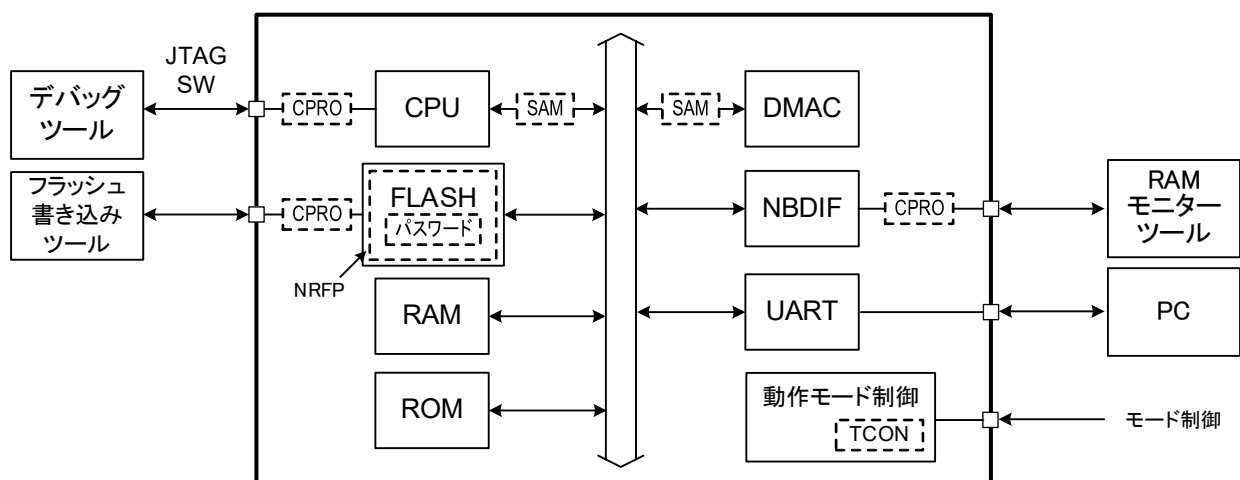


図 2.1 セキュリティ機能

3. 機能説明

本章内に記載されているフラッシュコマンドとレジスターについては、リファレンスマニュアル「フラッシュメモリー」を参照してください。

3.1. チッププロテクト(CPRO)

3.1.1. 機能

チッププロテクトはデバッグツールおよびフラッシュ書き込みツールの機能を禁止または制限します。チッププロテクトの対象を表 3.1 に示します。

表 3.1 チッププロテクトの対象

対象	機能
デバッグツール	JTAG またはシリアルワイヤ(SW)経由の通信を禁止
RAM モニターツール	NBDIF 端子経由の通信を禁止
フラッシュ書き込みツール	フラッシュライターモードでのフラッシュメモリーの読み出し、書き込みを禁止 セキュアアクセスメモリーが有効な場合はフラッシュライターモードを禁止

フラッシュライターモードの仕様は非公開です。

ノンブレイクデバッグインタフェースは製品によって搭載しない場合があります。製品の搭載機能は「データシート」で確認してください。

3.1.2. 動作説明

チッププロテクトは、チッププロテクトビットとチッププロテクトマスクレジスター`[FCCPROMR]`で構成されます。チッププロテクトビットとチッププロテクトマスクレジスターの両方が"1"の場合にチッププロテクトが有効になります。チッププロテクトの状態は、チッププロテクト/東芝テストモードステータスレジスター`[FCCPROTCONSR]` `<CPROSTA>`で確認します。

3.1.2.1. チッププロテクトビット

チッププロテクトビットはフラッシュメモリー内の不揮発ビットで、直接アクセスすることはできません。チッププロテクトビットの操作はフラッシュコマンドで行います。

チッププロテクトを有効にするには、チッププロテクトビットを"1"にする必要があります。出荷時のチッププロテクトビットは"0"です。

3.1.2.2. チッププロテクトマスクレジスター(`[FCCPROMR]`)

`[FCCPROMR]` `<CPROMSK>`はチッププロテクトビットを一時的にマスクする(無効にする)ことができます。"1"がマスクしていない状態、"0"がマスク状態です。

`[FCCPROMR]` `<CPROMSK>`の書き換えは以下の手順で行います。

- (1) `[FCKCR]`に"0xA74A9D23"を書く。
- (2) (1)の書き込みから 16 クロック以内に`[FCCPROMR]` `<CPROMSK>`に書く。

`[FCCPROMR]` `<CPROMSK>`は POR と PORF でのみ初期化されます。初期化後の値は"1"です。

3.1.2.3. チッププロテクトの一時解除

[FCCPROMR]/<CPROMSK>の設定を変更することで、チッププロテクトを一時的に解除することができます。

チッププロテクトが有効な状態で[FCCPROMR]/<CPROMSK>を"0"に設定すると、チッププロテクトが解除されます。

注) セキュアアクセスメモリーが有効な場合、App ステートでは[FCCPROMR]/<CPROMSK>に書き込みできません。

3.1.2.4. チッププロテクトビットの操作

チッププロテクトビットを"1"にするには、自動 CPRO プログラムコマンドを実行します。

チッププロテクトビットを"0"にするには、自動 CPROTCN 解除コマンドを実行します。

自動 CPROTCN 解除コマンドを実行する場合、[FCCPROMR]/<CPROMSK>の値によって動作が異なります。

(1) [FCCPROMR]/<CPROMSK>が"0"の場合(チッププロテクト一時解除状態)

チッププロテクトビットが"0"になるとともに、東芝テストモード制御が無効になります。

(2) [FCCPROMR]/<CPROMSK>が"1"の場合(チッププロテクト状態)

フラッシュメモリーの全データを消去後、チッププロテクトビットが"0"になるとともに、東芝テストモード制御が無効になります。

ただし、解除不能フラッシュプロテクトが有効な場合、自動 CPROTCN 解除コマンドは無視されます。

自動 CPRO プログラムおよび自動 CPROTCN 解除コマンド実行後、リセットが発生するまでチッププロテクトビットの値は反映されません。

3.2. セキュアアクセスメモリー(SAM)

セキュアアクセスメモリーの概要を説明します。詳細は、リファレンスマニュアル「セキュアアクセスメモリー」を参照してください。

セキュアアクセスメモリーを使用する際はチッププロテクト機能も有効にし、外部からの不正なアクセスを遮断することを推奨します。

3.2.1. 機能

セキュアアクセスメモリーはバスマスターからのフラッシュメモリーと RAM のアクセスを制御する機能です。以下の3つのステートを持ち、ステートごとにアクセス可能な領域を指定します。

- Boot ステート
スタートアッププログラムが動作するステート。
- App ステート
アプリケーションプログラムが動作するステート。
- Lib ステート
アプリケーションプログラムから分離された状態でプログラムが動作するステート。

各ステートで許可されていない領域をアクセスすると SAM リセットが発生します。

Boot ステートおよび Lib ステート中の NMI は、SAM リセットとして扱われます。

App ステートでは **[FCCPROMR]**<CPROMSK>に書き込みできません。

自動 SAMNRFP プログラムコマンドのロック設定により自動 SAMNRFP 解除コマンドが無効になります。このため、セキュアアクセスメモリーと解除不能フラッシュプロテクトが無効にすることができなくなります。

セキュアアクセスメモリーを有効にすると、以下のモードは動作しません。

- シングルブートモード

3.3. 解除不能フラッシュプロテクト(NRFP)

3.3.1. 機能

指定したフラッシュメモリー領域の書き込み/消去を禁止します。フラッシュプロテクト(FPRO)と異なり、ロック設定により解除ができなくなります。ただし、故障解析時には当社のテストモードで解除が可能です。(東芝テストモード制御が無効の場合)

フラッシュプロテクト機能についてはリファレンスマニュアル「フラッシュメモリー」を参照してください。

対象とするフラッシュメモリー領域は、ブロック 0 から連続した領域をブロック単位で指定します。最大で、ブロック 0~31 を指定することができます。解除不能フラッシュプロテクトを指定したブロックに対する書き込み/消去のフラッシュコマンドは無視されます。

解除不能フラッシュプロテクトを有効にすると、以下のモードは動作しません。

- シングルブートモード
- フラッシュライターモード

また、チッププロテクトが有効(チッププロテクトビットと`[FCCPROMR]<CPROMSK>`の両方が"1")な場合、自動 CPROTCON 解除コマンドは無視されます。

3.3.2. 動作説明

解除不能フラッシュプロテクトの領域設定、有効設定、ロック設定は、フラッシュコマンドの自動 SAMNRFP プログラムで行います。ロック設定されていない場合、領域設定と有効設定は自動 SAMNRFP 解除コマンドで解除できます。ロック設定によって自動 SAMNRFP 解除コマンドが無効になり、解除不能フラッシュプロテクトとセキュアアクセスメモリーが解除不能になります。

解除不能フラッシュプロテクトの領域設定、有効設定の状態は、解除不能フラッシュプロテクトステータスレジスター`[FCNRFPSR]`で確認できます。

ロック設定は、ロックステータスレジスター`[FCLOCKSR]<LOCKSTA>`で確認できます。

3.4. 東芝テストモード制御(TCON)

3.4.1. 機能

東芝テストモード制御を有効にすると、当社のテストモードおよびフラッシュライターモードの起動が禁止されます。出荷時には東芝テストモード制御は解除されています。

3.4.2. 動作説明

東芝テストモード制御を有効にするには、フラッシュコマンドの自動 TCON プログラムを実行します。解除するには自動 CPROTCON 解除コマンドを実行します。自動 CPROTCON 解除コマンドを実行する場合、`[FCCPROMR]<CPROMSK>`の値によって動作が異なります。「3.1.2.4 チッププロテクトビットの操作」を参照してください。

東芝テストモード制御の状態は、チッププロテクト/東芝テストモード制御ステータスレジスター`[FCCPROTCONSR]<TCONSTA>`で確認できます。

3.5. RAM 転送コマンド(シングルブートモード)

シングルブートモードの RAM 転送コマンドの詳細は、リファレンスマニュアル「フラッシュメモリー」を参照してください。

3.5.1. 機能

シングルブートモードで RAM 転送コマンドを実行する際、パスワードによる認証が行われます。

3.5.2. 動作説明

パスワードとしてフラッシュメモリー内の連続する 255 バイトのデータが使用されます。

RAM 転送コマンドを実行する際、パスワードのスタートアドレスと 255 バイトのパスワードデータの入力が求められます。

4. 使用方法の例

セキュリティ機能を使用する際のデバッグツール接続について説明します。

- ユーザーによる開発

アプリケーションソフトウェアの開発中は、デバッグツールを使用するためにチッププロテクトは無効とします。

セキュアアクセスメモリーを使用する場合、各ステートの領域を定義するとともに、起動用の **Boot** ステートプログラム、通常動作用の **App** ステートプログラム、必要に応じて **Lib** ステートプログラムを作成します。

セキュアアクセスメモリーの動作確認後、その他のセキュリティ機能と合わせて動作確認を行います。

セキュアアクセスメモリーと合わせてチッププロテクトを使用することを推奨します。

解除不能フラッシュプロテクトと東芝テストモード制御は必要に応じ有効にします。これらの機能を有効にした場合、故障解析をする際に制約があります。

セキュアアクセスメモリー、解除不能フラッシュプロテクトを使用する場合はロック設定を行います。

必要なすべてのセキュリティ機能を設定した状態で、最終的な動作確認を行います。

- ユーザーによる故障解析

故障解析でデバッグツールを使用するためにチッププロテクトを解除するには以下の方法があります。

- CPU のプログラム実行による解除

外部からの通信等をトリガーとして以下の操作を行うことで、デバッグツールが使用できるようになります。

- チッププロテクトの一時解除

[FCCPROMR]/<CPROMSK>を"0"にすることでチッププロテクトが一時解除されます。

- チッププロテクトの解除

自動 **CPROTCN** 解除コマンドを実行することで、チッププロテクトおよび東芝テストモード制御が解除されます。

- 強制 **CPROTCN** 解除

セキュアアクセスメモリーが有効で解除不能フラッシュプロテクトが無効の場合、強制 **CPROTCN** 解除が使用可能です。

シングルブートモード起動の操作(**BOOT_N** 入力を"Low"として **RESET_N** 端子によるリセット)で強制 **CPROTCN** 解除が実行され、フラッシュメモリーのデータの消去、チッププロテクトの解除および東芝テストモード制御の解除を行います。

強制 **CPROTCN** 解除については、リファレンスマニュアル「セキュアアクセスメモリー」を参照してください。

- フラッシュメモリー消去コマンド(シングルブートモード)

シングルブートモードのフラッシュメモリー消去コマンドを実行すると、フラッシュメモリーのデータの消去、チッププロテクトの解除、東芝テストモード制御の解除およびフラッシュプロテクトの解除を行います。

ただし、セキュアアクセスメモリーまたは解除不能フラッシュプロテクトが有効な場合、シングルブートモードは起動しません。

- 東芝による故障解析
東芝テストモード制御が有効な場合、当社のテストモードによる解析はできません。
当社に故障解析を依頼する場合は、東芝テストモード制御を解除した状態にしてください。

5. 改訂履歴

表 5.1 改訂履歴

Revision	Date	Description
1.0	2026-01-30	・新規作成

製品取り扱い上のお願い

株式会社東芝およびその子会社ならびに関係会社を以下「当社」といいます。

本資料に掲載されているハードウェア、ソフトウェアおよびシステムを以下「本製品」といいます。

- 本製品に関する情報等、本資料の掲載内容は、技術の進歩などにより予告なしに変更されることがあります。
- 文書による当社の事前の承諾なしに本資料の転載複製を禁じます。また、文書による当社の事前の承諾を得て本資料を転載複製する場合でも、記載内容に一切変更を加えたり、削除したりしないでください。
- 当社は品質、信頼性の向上に努めていますが、半導体・ストレージ製品は一般に誤作動または故障する場合があります。本製品をご使用頂く場合は、本製品の誤作動や故障により生命・身体・財産が侵害されることのないように、お客様の責任において、お客様のハードウェア・ソフトウェア・システムに必要な安全設計を行うことをお願いします。なお、設計および使用に際しては、本製品に関する最新の情報（本資料、仕様書、データシート、アプリケーションノート、半導体信頼性ハンドブックなど）および本製品が使用される機器の取扱説明書、操作説明書などをご確認の上、これに従ってください。また、上記資料などに記載の製品データ、図、表などに示す技術的な内容、プログラム、アルゴリズムその他応用回路例などの情報を使用する場合は、お客様の製品単独およびシステム全体で十分に評価し、お客様の責任において適用可否を判断してください。
- 本製品は、特別に高い品質・信頼性が要求され、またはその故障や誤作動が生命・身体に危害を及ぼす恐れ、膨大な財産損害を引き起こす恐れ、もしくは社会に深刻な影響を及ぼす恐れのある機器（以下"特定用途"という）に使用されることは意図されていませんし、保証もされていません。特定用途には原子力関連機器、航空・宇宙機器、医療機器（ヘルスケア除く）、車載・輸送機器、列車・船舶機器、交通信号機器、燃焼・爆発制御機器、各種安全関連機器、昇降機器、発電関連機器などが含まれますが、本資料に個別に記載する用途は除きます。特定用途に使用された場合には、当社は一切の責任を負いません。なお、詳細は当社営業窓口まで、または当社 Web サイトのお問い合わせフォームからお問い合わせください。
- 本製品を分解、解析、リバースエンジニアリング、改造、改変、翻案、複製等しないでください。
- 本製品を、国内外の法令、規則及び命令により、製造、使用、販売を禁止されている製品に使用することはできません。
- 本資料に掲載してある技術情報は、製品の代表的動作・応用を説明するためのもので、その使用に際して当社及び第三者の知的財産権その他の権利に対する保証または実施権の許諾を行うものではありません。
- 別途、書面による契約またはお客様と当社が合意した仕様書がない限り、当社は、本製品および技術情報に関して、明示的にも黙示的にも一切の保証（機能動作の保証、商品性の保証、特定目的への合致の保証、情報の正確性の保証、第三者の権利の非侵害保証を含むがこれに限らない。）をしておりません。
- 本製品、または本資料に掲載されている技術情報を、大量破壊兵器の開発等の目的、軍事利用の目的、あるいはその他軍事用途の目的で使用しないでください。また、輸出に際しては、「外国為替及び外国貿易法」、「米国輸出管理規則」等、適用ある輸出関連法令を遵守し、それらの定めるところにより必要な手続を行ってください。
- 本製品の RoHS 適合性など、詳細につきましては製品個別に必ず当社営業窓口までお問い合わせください。本製品のご使用に際しては、特定の物質の含有・使用を規制する RoHS 指令等、適用ある環境関連法令を十分調査の上、かかる法令に適合するようご使用ください。お客様がかかる法令を遵守しないことにより生じた損害に関して、当社は一切の責任を負いかねます。