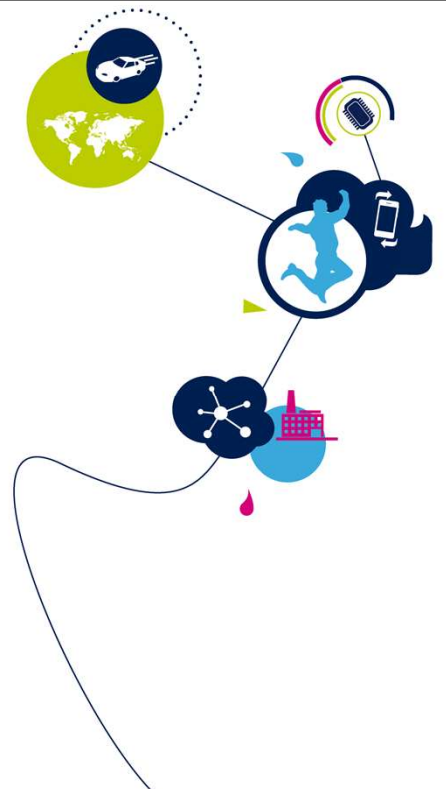


STM32G4 - MEMPROTECT

メモリ保護機能

1.0版



STM32システムメモリ保護のプレゼンテーションによろこそ。
コードやデータを保護するさまざまな手段について説明します。

• 目的:

1. 内部の組み込みソフトウェアやそれに含まれるデータに読出しと書き込みの保護を提供:
 - Flashメモリ
 - コア結合メモリ(CCM)SRAM
 - バックアップ・レジスタ
2. 機密性の高いファームウェアの安全な実行を提供

アプリケーション側の利点

- STM32内の組み込みソフトウェアの知的財産権を保護
- JTAGインタフェースその他の外部攻撃手段を通じたコードのハッキングやコードのダンプを防止
- 不要/偶発的な消去からコード/データを保護(ローダ、校正データ)
- セキュア・アプリケーションの開発(セキュア・ブートまたはセキュア・ファームウェア更新)を可能に



メモリ保護は、さまざまな目的のために設計されています。保護メモリは、Flashメモリ、コア結合メモリ(またはCCM)SRAM、およびバックアップレジスタです。

たとえば、読取り保護は、外部アクセスを通じて埋め込みソフトウェアコードをダンプすることを防ぎ、開発者の知的財産を保護します。

書き込み保護は、ソフトウェアまたはデータ更新手順でのオーバーフローによって、特定のFlashセクタが誤って消去されることを防ぎます。

STM32G4マイクロコントローラは、Flashメモリおよびバックアップレジスタにあるコードとデータを保護するためのいくつかの機能を提供します。

これらの典型的なメモリ保護に加えて、STM32G4は、機密性の高いファームウェアの安全な実行を保証する新しいメカニズムも導入しています。

以下のスライドでは、これらすべての保護機能について説明します。

• 読出し保護(RDP)

- 外部アクセスに対してFlashメモリ、CCM SRAM、バックアップレジスタをグローバルに保護
- ブートがユーザのFlashメモリ内からと異なる場合、メモリとレジスタはSWD/JTAGアクセスから保護
- 保護なし、から永続的かつ完全な保護までの、3つのRDPLレベルを定義



• 独自仕様コード読出し保護(PCROP)

- ソフトウェアIPの読出しおよび書込みアクセスに対するFlashメモリ領域の保護
- PCROP属性を持つFlashメモリコードは実行のみ可能



リクエスト	アクセス許可
読出し	不可
書込み	不可
実行	可能



コード保護のために以下の手段が提供されます。:

RDP: 読出し保護 (ReadOut Protection)

PCROP: 独自仕様コード読出し保護 (Proprietary Code ReadOut Protection)

WRP: 書込み保護 (Write Protection)

セキュアなユーザメモリ保護は、STM32G4マイクロコントローラの新機能です。コードとデータ保護に加えて、機密性の高いアプリケーションを安全に実行可能です。

読み出し保護(RDP)は、Flashメモリ、オプションバイト、CCM SRAMとバックアップレジスタへの外部読み取りアクセスを防ぐグローバルメカニズムです。外部アクセスは、JTAGコネクタ、シリアルワイヤポート、またはSRAMに組み込まれたブートソフトウェアを使用してデータを取得しようとするアクセスです。

RDP保護の3つのレベルは、全く保護を提供しないレベル0から永続的かつ完全な保護を備えたレベル2まで定義されます。

保護レベルは、次のスライドで説明します。

PCROPは、コードダンプに対するメモリアクセス保護です。コードの知的財産を保護するために使用されます。

保護されたファームウェアは実行可能なままですが、悪意のあるサードパーティコード(トロイの木馬など)を実行しているCPUによって実行される読み取りおよび書き込みアクセスを防止します。

• 書込み保護(WRP)

- Flashメモリセクタによる書込み/消去/プログラム・アクセスに対する保護
- 書込み保護属性を持つFlashメモリコードは、不要な書込みまたは消去の操作から保護される



リクエスト	アクセス許可
読出し	可能
書込み	不可
実行	可能

• セキュア・ユーザメモリ保護

- 感度の高いファームウェア実行のため、特定のアクセスメカニズムによるFlashメモリ領域保護
- この領域のコードとデータはリセット後にのみアクセス可能
- コードは他のプロセスの前に実行される
- 実行されると、保護領域は閉じられ、次のリセットまでアクセス出来なくなる



リクエスト	アクセス許可
セキュア読出し	可能
非セキュア読出し	不可
セキュア書出し	可能
非セキュア書出し	不可
セキュア実行	可能
非セキュア実行	不可



書込み保護メカニズムは、偶発的または悪意のある書込み/消去操作を防ぎます。

セキュア・ユーザメモリは、コードおよびデータ保護に加えて、機密ファームウェアのセキュアな実行を保証する特定の保護メカニズムを備えたFlashメモリ領域です。

すべての保護メカニズムは、STM32G4オプションバイトを介して設定可能です。セキュアブートが実行されると、次のリセットまで、ユーザの安全なメモリにアクセスできなくなることに注意してください。

STMG43X/4XとSTM32G47X/8Xの違い

5

	STM32G43X/4X (カテゴリ2)	STM32G47X/8X(カテゴリ3)	
		FLASH_OPTR[DBANK]=0 (シングルバンク)	FLASH_OPTR[DBANK]=1 (デュアルバンク)
バンク数	1	1	2
ページサイズ	2キロバイト	4キロバイト	2キロバイト
書き込み保護領域(WRP)	2	4	2 / バンク
独自仕様コード読出し保護(PCROP)	1	2	1 / バンク
セキュリティ保護可能なメモリ領域	1	2	1 / バンク



このスライドでは、カテゴリ2マイクロコントローラと呼ばれるSTM32G43X/4Xと、カテゴリ3マイクロコントローラと呼ばれるSTM32G47X/8Xの実装されたFlashメモリに関する違いについてハイライトします。

DBANKオプションビットに応じて、カテゴリ2のバンクの数は1つ、カテゴリ3の場合は1つ、または2つです。

最小の消去の粒度になるページサイズは、カテゴリ2では2キロバイト、カテゴリ3はシングルバンクの場合は4キロバイト、デュアルバンクを持つカテゴリ3の場合は2キロバイトです。

保護機能に関して、カテゴリ2のマイクロコントローラは1つの書き込み保護領域、1PCROPおよび1つのセキュリティ保護可能なメモリ領域を有し、カテゴリ3のマイクロコントローラには2つの書き込み保護領域、2つのPCROPsおよび2つのセキュリティ保護可能なメモリ領域を持ちます。

保護レベル0、および1

- RDPLレベル0
 - 保護が設定されておらず、Flashメモリ、CCM SRAM、およびバックアップレジスタですべての操作（読出し/書込み/消去）が許可されている
 - オプションバイトの変更が可能
- RDPLレベル1
 - デバッグポートが接続されている間、またはRAMもしくはシステムFlashメモリ・ブートローダから起動した場合、Flashメモリおよびバックアップレジスタへのアクセス（読出し/消去/プログラム）は実行できない
 - 読出しまたは書込みリクエストでバスエラーが生成
 - ユーザがプログラムしたFlashメモリから起動するとき、ユーザコードから保護されたメモリへのアクセスが許可
 - オプションバイトの変更は可能で、レベル0への保護レベルへの変更は可能だが、Flashメモリ、CCM SRAM、バックアップレジスタが全消去される



最下位のRDPLレベル0が設定されている場合、デバイスは保護されません。Flashメモリ上のすべての読出しまたは書込み操作（書込み保護が設定されていない場合）は、すべてのブート構成（Flashユーザブート、デバッグ、RAMからのブートなど）でCCM SRAMとバックアップレジスタを実行できます。

オプションバイトもこのレベルで変更可能です。

レベル0は工場出荷時のデフォルトレベルです。

レベル1では、読出し保護はFlashメモリ、CCM SRAM、およびバックアップレジスタに設定されます。

このレベルでは、保護されたメモリは、Flashメモリのユーザコードから起動するときのみアクセス可能です。

デバッグからのアクセスが検出されるか、ブートがユーザのFlashメモリ領域に設定されていない場合、保護されたメモリへのアクセスは、システムのハードフォルトを生成し、次の電源投入がリセットされるまですべてのコード実行をブロックします。

オプションバイトはこのレベルでは変更可能なため、保護を解除できます。このメカニズムについては、次のスライドで説明します。

レベル回帰と保護レベル2

- レベル1からレベル0への保護レベルの回帰
 - Flashメモリ、CCM SRAM、バックアップ・レジスタの全消去
 - 保護領域 (PCROPおよびセキュア・ユーザメモリ) は、消去ポリシーに依存する
 - オプションバイトおよびOTPバイトは消去されない
- RDPLレベル2
 - レベル1によって提供されるすべての保護が、アクティブかつ永久
 - オプションバイトは、内部から、または外部からも変更出来ない
 - SWD/JTAGは無効
 - RAMまたはシステムメモリ(ブートローダ)からのブートは許可されない
 - ユーザFlashメモリでのみブートが許可され、Flashメモリとバックアップ・レジスタ上のすべての操作(読出し/書込み/消去)が有効になる



前のスライドでは、レベル1でオプションバイトを変更することが可能であることを確認しました。保護レベルをレベル0に変更することで、保護を解除できます。

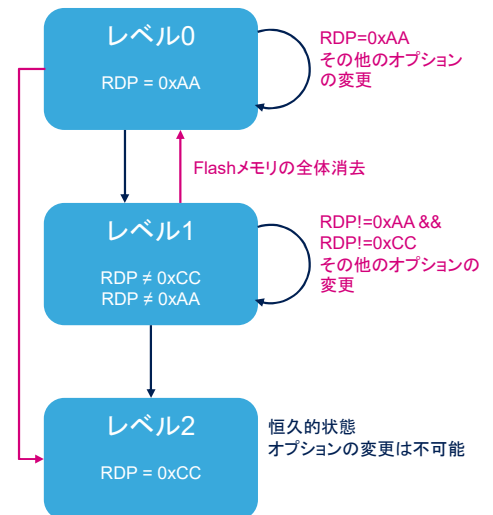
この保護レベルの回帰により、Flashメモリ、CCM SRAM、およびバックアップレジスタが一括で全消去されます。PCROPによって保護されるか、またはセキュア・ユーザメモリとして構成されたFlash領域は、消去ポリシーの設定に応じて消去または変更されないままにすることができます。

読み出し保護レベル2はレベル1と同じ保護を提供しますが、永久に保護されます。オプションバイトは変更できなくなるため、RDP保護がこのレベルに設定されると、それを変更する方法はなく、全消去メカニズムによるレベル回帰は不可能になります。このレベルは、開発段階が完了した場合にのみ最終製品で考慮する必要があります。

この保護はST工場でも解除できないことに注意してください。

遷移スキーム

- レベル0 / RDP = 0xAA
 - オプション・バイトは修正可能
 - レベル1または2への遷移が可能
- レベル1 / RDP != (0xAA | 0xCC)
 - オプション・バイトは修正可能
 - ユーザFlashメモリ、バックアップ・レジスタ、CCM SRAMの全体消去でレベル0に移行
 - 永続的な保護(レベル2)への遷移が可能
- レベル2 / RDP = 0xCC
 - オプション・バイトが固定される
 - 他のレベルへの遷移不可能



このスライドでは、各読出し保護レベル間の可能な遷移を示します。保護レベルを上げることは常に可能ですが、回帰はレベル1とレベル0の間でのみ可能です。

RDPがレベル1からレベル0に遷移するように値0xAAに再プログラムされると、Flashメインメモリの全体消去が実行されます。バックアップレジスタとCCM SRAMも消去されます。OTP領域は、全体消去の影響を受けず、変更されません。

FLASH_PCROP1ERレジスタのビットPCROP_RDPがクリアされると、完全な一括消去は、PCROPによって保護されているページを除いて、PCROPがアクティブなバンクでの連続したページ消去である部分的な一括消去に置き換えられます。これはPCROPコードを保持するために行われます。

RDPレベルは1つのオプションバイトでコーディングされています。レベル0は0xAA値でコーディングされ、レベル2は0xCC値でコーディングされ、レベル1は0xAAまたは0xCC以外の値でコーディングされます。

サマリー

エリア	保護レベル (RDP)	ユーザFlashメモリでブートするときのアクセス権	RAMからのブートか、ブートローダまたはデバッガからのアクセスでブートした場合のアクセス権
メインFlashメモリ	1	R/W/E	アクセスなし
	2	R/W/E	N/A、ユーザFlashメモリ内での起動のみが許可される
システムFlashメモリ (ブートローダ)	1	R	R
	2	R	N/A、ユーザFlashメモリ内での起動のみが許可される
オプション・バイト	1	R/W/E	R/W/E
	2	R	N/A、ユーザFlashメモリ内での起動のみが許可される
バックアップ・レジスタ	1	R/W	アクセスなし
	2	R/W	N/A、ユーザFlashメモリ内での起動のみが許可される
CCM SRAM	1	R/W	アクセスなし
	2	R/W	N/A、ユーザFlashメモリ内での起動のみが許可される
OTP	1	R/W	アクセスなし
	2	R/W	N/A、ユーザFlashメモリ内での起動のみが許可される



W:書込み R:読出し E:消去

この表は、前のスライドで見られるように、読出し保護(またはRDP)レベル、構成されたブートモード、およびデバッグアクセスに従って、Flashメモリとバックアップレジスタに対して、認可されているさまざまなアクセスの種類をまとめたものです。

ソフトウェアIPコードの機密性を保護

• ソフトウェアの知的財産保護

- STまたはサードパーティは、STM32マイコン用の特定のソフトウェアIPを開発および販売することが出来る
 - これらのIPは、さらなるアプリケーション開発のために使用され、不正コピーから保護する必要がある
- PCROP機能により、内部(悪意のあるファームウェア)または外部Flashメモリ・アクセス(デバッグ・ポート)からのダンプに対するソフトウェアIP保護が保証される

• PCROPの特性

- PCROP領域は実行専用
 - 読出し/書込み/消去の操作は許可されていない
 - PCROPコードは、このメモリ属性に準拠するために適切なオプション(armcc) “-execute_only”を使用してコンパイルする必要がある
- RDPLレベルに関係なく保護が有効



PCROPは、独自のコード読み出し保護を意味します。

サードパーティは、STM32マイクロコントローラ用の特定のソフトウェアIPを開発および販売する場合があります。相手先ブランド機器メーカーは、独自のアプリケーションコードを開発する際に使用することができます。ソフトウェアの知的財産(またはIP)を保護するために、コードをコピーまたは読み取りしないでください。PCROPの目的は、サードパーティ製ソフトウェアの知的財産コードの機密性を、RDPLレベルの設定に依存しない悪意のあるユーザから保護することです。

保護されたファームウェアはCortex®-M4コアによってのみ実行できます。その他のアクセス(DMA、デバッグ、データの読出し、書込み、消去など)は厳しく禁止されています。

この制約に準拠するには、ファームウェアを適切なコンパイルオプションでコンパイルする必要があります。たとえば、「-execute_only」(Keilツールの場合)。このオプションを指定しないと、リテラルプールと呼ばれる読み取り専用セクションの関数と定数がインターリーブされます。

Cortex-M4 MPUは、実行のみのアクセス許可をサポートしていません。

設定/設定解除

• 設定

- 各PCROP領域は、16バイトまたは32バイトからフルバンクまでの物理Flashバンクベースアドレスに関連する開始ページオフセットと終了ページオフセットによって定義される
- PCROP領域はオプションバイトレジスタを介して定義される

• 設定解除

- PCROPを非アクティブ化する唯一の方法は、RDPLレベルのレベル1からレベル0への回帰
 - この回帰レベルは、Flashメモリの全消去の操作をトリガ
- 追加オプション・ビット(PCROP_RDP)を使用すると、RDP保護がレベル1からレベル0に変更されたときに、PCROP領域を選択して消去することが可能



Flashメモリ内の独自のコード読出し保護領域は、オプションバイトを使用して定義されます。

各PCROP領域は、16バイトまたは32バイトのフルバンクまでの物理Flashバンクベースアドレスに関連する開始ページオフセットと終了ページオフセット、カテゴリ2デバイスの場合は16バイト、デュアルバンクを持つカテゴリ3デバイスの場合は32バイト、シングルバンクを持つカテゴリ3デバイスの場合は32バイトで定義されます。

これらの領域は、データアクセスから保護されます。

PCROP機能で保護されたセクタも書込みアクセスから保護され、不要なセクター書込み操作や消去操作に対する保護を提供します。

PCROP保護は、RDPLレベル回帰でレベル1からレベル0に対してのみ削除できます。このメカニズムを実行すると、Flashメモリの完全な一括消去がトリガされます。

RDP保護がレベル1からレベル0に変更されると、PCROP_RDPオプション・ビットに応じて、PCROP領域は消去されます。

不要な消去や偶発的な消去からコードとデータを保護

- 保護属性への書込み
 - 保護されたセクタは消去またはプログラムできない
- セット/リセット
 - 保護は、Flashメモリの各ページに対して個別に設定
 - 保護はオプション・バイト・レジスタで設定
 - 書込み保護はRDPLレベル0およびレベル1でリセット可能
 - RDPLレベル2では変更できない
 - 書込み保護されたページがある場合、レベル回帰メカニズムは機能しない
 - 書込み保護は、レベル回帰によるFlashメモリの一括消去の前に削除する必要がある



書込み保護により、コードや不揮発性データを不要な消去や偶発的な消去から保護します。

この保護はFlashメモリでのみ使用できます。書込み保護は、選択したFlashメモリページのみに設定できます。

ページが保護されている場合、ページを消去またはプログラムすることはできません。セクタへの書込みアクセスを試みると、Flashメモリエラーが発生します。

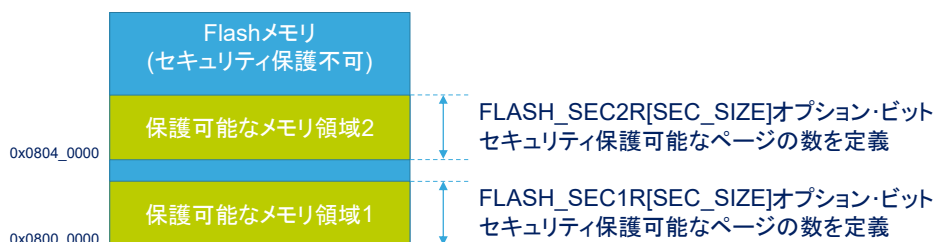
少なくとも1つのページが書き込み禁止の場合、Flashメモリの一括消去は実行できません。保護を最初に削除する必要があります。

セキュリティ保護可能なメモリ領域

13

イントロダクション

- セキュリティで保護可能なメモリ領域の主な目的は、望ましくないアクセスからFlashメモリの特定の部分を保護するため
 - これにより、安全なキー・ストレージや安全なブートなどのソフトウェア・セキュリティ・サービスを実装可能



- FLASH_SECiR[SEC_SIZE]オプション・ビットが0の場合、セキュリティ保護可能なメモリは実装されない
 - このフィールドはRDPLレベル0でのみ変更可能



セキュリティで保護可能なメモリの目的は、ブート時に使用できるコードとデータを格納し、ブートプログラムがコントロールビットを設定するとアクセスできなくなることにあります。

通常のユースケースは、セキュリティ保護可能なメモリに含まれる暗号キーを使用して、Flashメモリに存在するソフトウェアイメージの認証と、場合によっては復号化を実行する場合があります。認証プログラムと復号化プログラムも、セキュリティ保護可能なメモリに格納されます。

オプションビットは、セキュリティ保護可能なメモリのサイズをページ単位で設定するために使用できます。ベースアドレスは、Cortex-M4リセットベクタに対応する、セキュリティ保護可能なメモリ領域1に対して常に0x0800_0000になります。

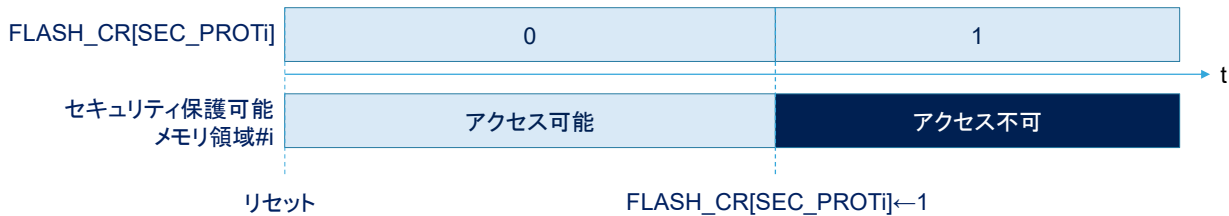
セキュリティ保護可能なメモリ領域2はアドレス0x0804_0000から始まります。

オプションバイトのSEC_SIZEフィールドがゼロの場合、セキュリティ保護可能なメモリは実装されません。

このフィールドはRDPLレベル0でのみ変更可能です。

セキュリティ保護可能なメモリ領域

14



- 既定では、リセット後、セキュリティ保護可能なメモリにアクセス可能
 - SEC_PROTiビットがレジスタFLASH_CRに設定されると、次のリセットまで、確保可能なメモリ番号#iにアクセスできなくなる
 - リセットのみがSEC_PROTiビットをクリア可能



ソフトウェアがFLASH_CRレジスタにSEC_PROTiビットを設定すると、セキュリティ保護可能なメモリ番号#iはアクセスできなくなります。

イメージ認証と復号化を実行するために使用されるセキュアブートの場合、SEC_PROTiビットは、認証が成功したときに、イメージの最初の命令に分岐する直前に1に設定されます。

SEC_PROTiビットが設定されると、ソフトウェアでクリアすることはできません。このビットをクリアする唯一の方法は、リセットすることです。

セキュリティ保護可能なメモリ領域

15

- セキュリティ保護可能なメモリの内容は、PCROPページと重なっていても、RDPLレベル1からレベル0に変更すると消去される

セキュリティ保護可能なメモリ・サイズ (SEC_SIZE[6:0])	セキュリティ保護可能なメモリ?	PCROP_RDP	消去されるページ
0	NO	1	すべて(全(マス)消去)
0		0	PCROP以外のすべて
>0	YES	1	すべて(全(マス)消去)
>0		0	PCROP以外すべてのセキュリティ保護可能なメモリ領域

- PCROP_RDPのレベルがレベル1からレベル0に回帰した場合にPCROPを保持するかどうかをビット制御
=0:PCROPは消去されない
=1:PCROPは消去される



もちろん、セキュリティ設定可能なメモリに存在するコードは、一部またはセキュリティ保護可能なメモリを消去場合があります。

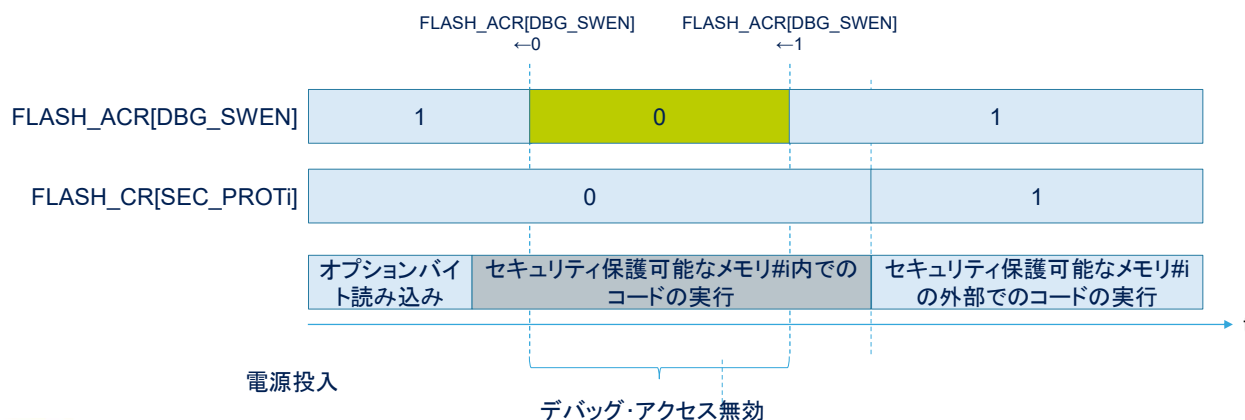
さらに、Flash読出し保護レベルをレベル1からレベル0に変更すると、セキュリティ保護可能なメモリの消去がトリガされます。セキュリティ保護可能領域に存在するコードは、独自仕様コード読出し保護(またはPCROP)領域にマッピングすることで、読出しおよび書込みアクセスから保護することもできます。

RDPLレベルをレベル1からレベル0に回帰すると、PCROP_RDPビットの値にかかわらず、これらのPCROP領域が消去されます。セキュリティで保護可能なメモリアドレス範囲の外側にあるPCROP領域の内容だけが保持されます。

コア・デバッグ・アクセスの無効化

16

- 機密コードの実行や、セキュリティ保護可能なメモリ領域での機密データの操作を行う場合、コアへのデバッグ・アクセスは一時的に無効にすることが可能



デバッガを使用してのCortex-M4を制御することは、DBG_SWEN制御ビットを適切にプログラミングすることによって一時的に無効にすることができます。たとえば、セキュアブートでは、認証/復号化を実行する前にこのビットをクリアし、認証が成功した後にこのビットを1つに設定して、デバッガによるデバッグを再度有効にできます。

- STM32G4ブート・メモリ:
 - 組み込み型SRAM
 - システムメモリ(ブートローダ)
 - メインFlashメモリ
- セキュリティを強化し、信頼のチェーンを確立するために、FLASH_SECRLレジスタのBOOT_LOCKオプション・ビットでは、他のブート・オプションに関係なく、システムがメインFlashメモリから強制的に起動することを許可する
 - BOOT_LOCKビットを設定することは常に可能
 - このビットをリセットする条件:
 - RDPはレベル0に設定されている。もしくは
 - RDPはレベル1に設定されており、レベル0が要求され、完全なマス消去が実行された時



STM32G4では、組み込みSRAMから起動、システムメモリから起動、メインFlashメモリから起動する3つの異なるブートモードを選択できます。

セキュア・メモリからセキュア・ブートを実行すると、ブート領域はFlashメモリになります。他のブート領域を無効にするには、FLASH_SECRLレジスタでBOOT_LOCKオプションビットを設定する必要があります。

このオプションビットは常に設定できます。ただし、RDPレベルが0の場合、またはRDPがレベル1からレベル0に回帰され、完全なマス消去が発生した場合にのみ、リセットが可能です。

- この機能に関連した以下のトレーニング資料を参照してください。
 - STM32G4-Flashメモリ



メモリアーキテクチャ、オプションバイト、Flashメモリの操作の詳細については、Flashメモリのトレーニングを参照してください。