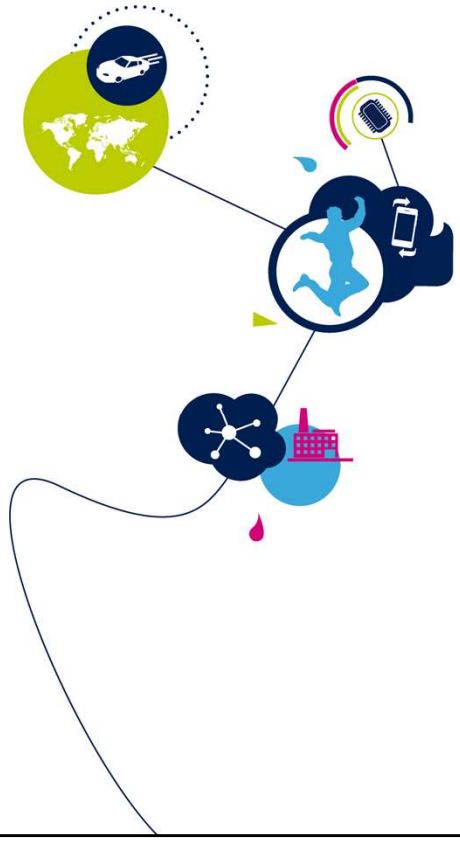
STM32WB MEMPROTECT

メモリ保護機能

1.0 版



life.augmented

STM32 システムメモリ保護のプレゼンテーションにようこそ。
コードやデータを外部や内部の攻撃から保護するさまざまな
手段について説明します。

概要

- 内部の組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込みの保護を提供
  - Flashメモリ
  - SRAM2
  - バックアップレジスタ
- Cortex®-M0+ のコード／データをユーザーアプリケーションから保護

アプリケーション側の利点

- STM32 内の組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、較正データ）
- ワイヤレススタックと RSS の安全な実行を提供

life.augmented

ソフトウェアプロバイダは、悪意のあるユーザや侵入攻撃から自社ソフトウェアの知的財産権を保護する必要がある場合があります。
この目的のため、STM32WB マイクロコントローラには、Flash メモリ、SRAM2、バックアップレジスタにあるコードやデータを保護するためのいくつかの機能が搭載されています。これらの機能によって、JTAG デバッガ、エンドユーザコード、SRAM トロイの木馬コードを通じたコードやデータの読み書きが防止できます。

新しいメモリ保護機能は、Cortex-M0+ 上で動作するルートセキュリティサービス（RSS）とワイヤレススタック専用です。この CPU は保護されたセグメントに対する排他アクセスが可能です。

主な機能

- Cortex-M0+ セキュリティ
  - Cortex M0+ の排他的アクセスのための Flash メモリと SRAM2 の上位部分 の保護
- 読出し保護(RDP)
  - レベル 0:読出し保護なし
  - レベル 1:メモリ読出し保護
  - レベル 2:チップ読出し保護
- 独自仕様コード読出し保護(PcROP)
  - Flash メモリの設定可能な 2 領域
- 書込み保護(WRP)
  - Flash メモリあたり設定可能な 2 領域

life.augmented

- ワイヤレススタックと RSS コード/データはユーザアプリケーションから保護されます。
- JTAG インタフェースからアクセスされた場合や、ブートが Flash メモリではない場合に、Flash メモリコードが保護されます。
- Flash メモリコードは実行可能ですが読出し可能ではありません。
- Flash メモリコードは不要な読み書き操作から保護されます。

コードを保護する目的で以下の手段が提供されます。

- Cortex M0+ セキュア Flash メモリと SRAM2
  Cortex-M4 上で動作するユーザアプリケーションによる RSS とワイヤレススタックのコードとデータへのアクセスを防止します。
  この保護は常に有効です。
- RDP:読出し保護
  JTAG を通じたすべての Flash メモリ領域への Flash メモリアクセスを防止します。
- PCROP:独自仕様コード読出し保護
  悪意のあるサードパーティコード(トロイの木馬)を実行するCPU から行われる、設定可能な Flash メモリ領域の読出しアクセスを防止します。
- WRP:書込み保護
  偶発的あるいは悪意のある書込み/消去操作を防止します。

RDP、PCROP、WRPは STM32WB オプションバイト経由で設定可能です。

Cortex-M0+ セキュリティ(1/2)

- Cortex M0+ セキュリティ
  - CortexM4 とデバッグアクセスからコードとデータを保護
- コードならびに以下の揮発性／不揮発性データの保護が可能
  - ワイヤレススタック（BLE プロトコル、スレッドプロトコル）
  - RSS（セキュアワイヤレススタックアップデート & カスタマキーストレージ）
- Cortex M0+ セキュリティは常に有効（ESE ビット = 1）
  - RDP レベルの回帰（レベル 1 からレベル 0）であっても解除不可

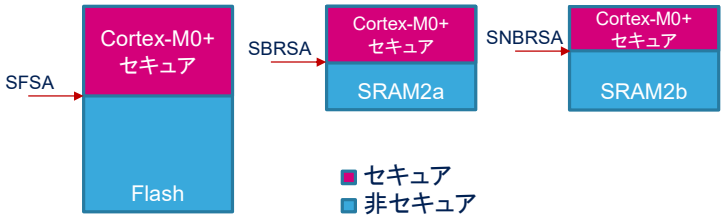
この機能の詳細な説明については、以下の専用トレーニングモジュールを参照してください。
- 「STM32WB- システム-CM0+ セキュリティ」
- 「STM32WB- セキュリティ-ルートセキュリティサービス（RSS）」

life.augmented

Cortex M0+ セキュリティ機能によって、このコア上で動作するファームウェアコードとデータがCortex M4 コア上で動作するユーザアプリケーションから保護されます。
ルートセキュリティサービス（RSS）とワイヤレススタックのセキュアな実行に加えて、デバッグアクセスの防止が保証されます。
CortexM0+ セキュリティ機能は常に有効となっており、RDP レベルの回帰によっても解除できません。
CortexM0+ セキュリティ保護機能または RSS の詳細な説明については、このトレーニングで紹介されている専用モジュールを参照してください。

Cortex-M0+ セキュリティ(2/2)

- 保護は Flash メモリと SRAM2 メモリを対象としています。
  - Flash メモリの上位部分（SFSA オプションバイトにより 4KB 境界で設定）
  - SRAM2a と SRAM2b の上位部分（それぞれ SBRSA と SNBRSA オプションバイトにより 1KB 単位で設定）



- 保護領域のサイズと設定は、ワイヤレススタックのインストール時か更新時に自動的にセットされます。

life.augmented

Cortex-M0+ セキュリティによって、Flash メモリと SRAM2 メモリの上位部分が保護されます。この領域のサイズは、ワイヤレススタックのインストール時か更新時に自動的にセットされます。
セキュア Flash 開始アドレス（SFSA）は、保護される Flash メモリの下位側の境界です。4KB 単位で整列されます。
セキュアバックアップ RAM 開始アドレス（SBRSA）とセキュア非バックアップ RAM 開始アドレス（SNBRSA）は、それぞれ SRAM2a メモリと SRAM2b メモリの保護部分の下位アドレスです。サイズは 1KB 単位で設定可能です。

ただし、これらのオプションバイトの設定は、RSS の責任において行われます。これらは、ワイヤレススタックの初回インストール時または更新時に設定されます。ユーザが修正することはできません。

読出し保護（RDP）

読出し保護機能の詳細についてじっくりと見てみましょう。

読出し保護(1/3)

- 読出し保護レベル 0(保護なし、出荷時デフォルト値)
  - Flash メモリ、SRAM2、バックアップレジスタ上ですべての操作(読出し/書込み/消去)が許可されます。
  - オプションバイトは、どちらの CPU からでも修正できます。
- 読出し保護レベル 1
  - 選択したブートモードがユーザ Flash メモリ(Boot0 = 0)である場合と、デバッガアクセスが検出されない場合 (JTAG なし)
    - Flash メモリ、SRAM2、バックアップレジスタ上ですべての操作(読出し/書込み/消去)が許可されます。オプションバイトは修正可能です。
  - 選択したブートモードがユーザ Flash メモリ(Boot0 = 1)ではない場合と、デバッガアクセスが検出された場合 (JTAG)
    - Flash メモリ、SRAM2、バックアップレジスタに対するすべての操作(読出し/書込み/消去)はブロックされます(ハードフォルトが生成)。オプションバイトは修正可能です。

life.augmented

STM32WB 読出し保護機能は、SRAM2 と Flash メモリのすべてと、バックアップレジスタに対して 3 レベルの保護を提供します。

- レベル 0 は「保護なし」を意味します。 これが出荷時デフォルト値です。読出し、書込み、消去の操作は、SRAM2、Flash メモリとともに、バックアップレジスタにも許可されます。レベル 0 では、オプションバイトは変更可能です。PCROP と CortexM0+ のセキュリティルールが依然として適用されることに注意してください。
- レベル 1 では、チップのメモリ全体に対する読出し保護が保証され、Flash メモリ、バックアップレジスタとともに、STM32 ファミリの新機能である SRAM2 の内容が含まれます。

デバッガアクセスが検出された場合と、ブートモードが Flash メモリ領域に設定されていない場合には、Flash メモリ、バックアップレジスタ、SRAM2 にアクセスすると必ずシステムハードフォルトが生成され、次回のパワーオン・リセットまですべてのコード実行がブロックされます。レベル 1 であればオプションバイトの修正が可能であることに注意してください。

読出し保護(2/3)

- 読出し保護レベル 2(JTAGヒューズ)
  - レベル 1 によるすべての保護がアクティブになります。
  - RAM やシステムメモリ(ブートローダ)からのブートが行えなくなります(ユーザ Flash メモリからのみ可能)。
  - JTAG インタフェースが無効となり、JTAG/SWD 経由のデバッグ／プログラミングは使用できなくなります(JTAG が切断されます)。
    - 工場 FAR が制限され、バックドアがないことが保証されます。
  - 選択されたブートモードがユーザ Flash メモリである場合
    - Flash メモリ、バックアップレジスタ、SRAM2上ですべての操作(読出し／書込み／消去)が許可されます。
  - 内部的にも外部からでも、オプションバイトを変更できなくなります(永久にレベル 2)。

life.augmented

レベル 2 では、レベル 1 に対して説明したものと同じ保護機能が SRAM2、Flash メモリ、バックアップレジスタに提供されます。ただし、大きな違いが 3 点あります。

1. JTAG/SWD デバッガ接続は無効となります(バックドアが存在しないことを保証するため、ST の工場においても同様)。
2. ブート 0/1 設定がどうであれブートモードは強制的にユーザ Flash メモリとなり、永久にレベル 2 となります。ひとたびレベル 2 に設定されると、元に戻す方法はありません。
3. RDP/WRP オプションバイトとともに、その他すべてのオプションバイトを変更できなくなります。

読出し保護(3/3)

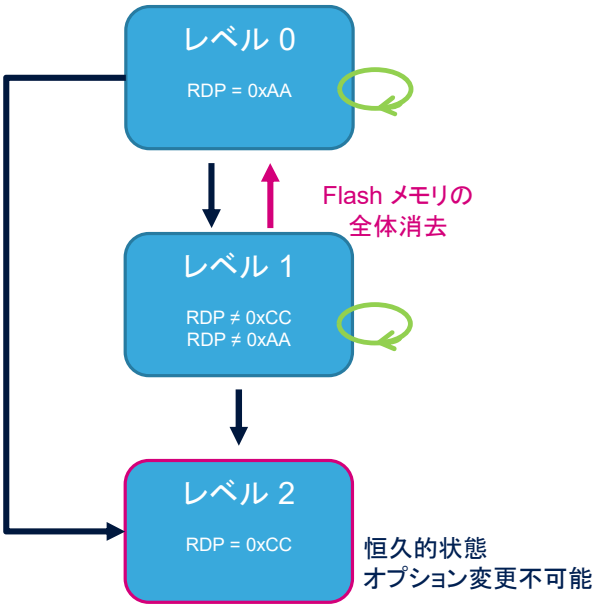
RDP レベル 回帰

- RDP レベル 2 は永久であり、解除することはできません。
- RDP レベル 1 は解除可能であり、レベル 0 に戻すことができますが、以下のような結果となります。
  - Flash メモリの部分消去
    - メモリのユーザ部分が消去されます。
      - PCROP 領域の解除は、設定されている消去ポリシーに依存します。
    - メモリのセキュア部分は変更なく維持されます。
      - CortexM0+ セキュリティは有効のままとなります。
      - ワイヤレススタックと RSS は消去されません。
  - バックアップレジスタと SRAM2 の非セキュア部分は完全に消去されます。

life.augmented

RDP 保護のレベル変更は、現在の保護レベルが ‘1’ であるときのみ許可されます。RDP レベル 2 は恒久的です。
RDP 保護レベルを ‘1’ から ‘0’ に変更すると、Flash メモリ、SRAM2、バックアップレジスタの非セキュア部分が消去されます。Flash のセキュア部分は影響を受けず、セキュア は変更なく維持されます。

RDP の遷移スキーム



- レベル 0
  - 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
  - オプションバイトは修正可能
  - レベル 0 または 2 への遷移が可能
    - レベル 0 → ユーザ Flash メモリ、バックアップレジスタ、SRAM2 の全体消去
- レベル 2
  - オプションバイトは停止
  - 遷移不可能

life.augmented

読出し保護レベル間で可能な遷移について見てみましょう。
すでに説明したように、STM32WB MCU は 3 種類の RDP レベルを備えています。

1. レベル 0 は、メモリ保護が行われず、オプションバイトが修正可能であることを意味します。
   レベル 0 からは、デバイスはレベル 1 またはレベル 2 への遷移が可能です。
2. レベル 1 ではメモリ保護が保証され、デバッグアクセスは有効のままとなります。
   レベル 1 からは、デバイスはレベル 0 またはレベル 2 への遷移が可能です。レベル 0 への回帰を行うと、Flash メモリが全体消去されます。
3. レベル 2 ではレベル 1 と同じメモリ保護が保証されますが、JTAG/SWD デバッグアクセスは完全に無効となります。
   レベル 2 は恒久的状態であり、他の RDP レベルへの遷移は行えません。

アクセスステータスと読出し保護レベルの比較

領域			保護レベル (RDP)	ブート = ユーザ Flash メモリである場合のアクセス権	ブート ≠ ユーザ Flash メモリであるか、デバッグアクセスが検出された場合のアクセス権
Flashメモリ	メインメモリ	非セキュア	1	R/W/E（CPU1&2）	アクセスなし
			2	R/W/E（CPU1&2）	-
		セキュア	1	R/W/E（CPU2）	アクセスなし
			2	R/W/E（CPU2）	-
	システムメモリ		1	R	R
			2	R	-
	オプションバイト		1	R/W/E	R/W/E
			2	R（CPU1） R/W/E（CPU2）	-
	バックアップレジスタ		1	R/W	アクセスなし
			2	R/W	-
	SRAM2	非セキュア	1	R/W（CPU1&2）	アクセスなし
			2	R/W（CPU1&2）	-
		セキュア	1	R/W（CPU2）	アクセスなし
			2	R/W（CPU2）	-

W：書込み
R：読出し
E：消去

life.augmented

この表には、すでに説明したように、読出し保護（RDP）レベル、設定されたブートモードとデバッグアクセスに応じて、Flash メモリ、バックアップレジスタ、SRAM2に対して許可される各種のアクセスタイプがまとめられています。まとめ：

- RDP がレベル 0 に設定されると、保護メカニズムは無効となり、すべてのメモリの読出しと修正が可能です。
- RDP がレベル 0 以外の場合：

ユーザ Flash メモリからのブートにデバイスが設定されている場合：

=> RDP レベルによらず、ユーザ Flash メモリ、バックアップレジスタ、SRAM2 は読出しと修正が可能です。

=> システム Flash メモリは読み出し専用です。

=> RDP がレベル 2 に設定されている場合、オプションバイトは読み出し専用です。

そうではない場合で、ユーザ Flash メモリからのブートにデバイスが設定されていない場合、またはデバッグアクセスが検出されている場合：

=> レベル 1 で読出しのみ可能なシステム Flash メモリと、レベル 1 で読出しと修正が可能なオプションバイトを除く、ほとんどすべてのメモリはアクセス可能ではありません。

独自仕様コード読出し保護（PCROP）

独自仕様コード読出し保護（PCROP）の詳細と、その RDP との違いについてじっくりと見てみましょう。

PCROP を使用する理由

13

RDP レベルによらずソフトウェア IP コードの機密性を保護

- ST やサードパーティは、STM32 MCU 用の固有のソフトウェア IP を開発して販売することがあります。
- ST または OEM のお客様は、自社アプリケーションコードの開発にこれらのソフトウェア IP を使用できます。
- ソフトウェアモジュールの知的財産権は、コードのコピーや「海賊版作成」を行おうとする悪意のあるユーザから保護されなければなりません。

特性／考察

- 悪意のあるソフトウェアまたはデバッガが機密コードを読み出すことを防止します。
- PCROP Flash メモリ領域は実行専用です。
  - R／W／消去操作は許可されません
- PCROP コードは適切なオプション（armcc）でコンパイルされる必要があります。
  - *“–execute_only “*

life.augmented

PCROP とは、独自仕様コード読出し保護のことです。
PCROP を使用する理由
独自仕様コード読出し保護は、RDP レベルの設定に無関係に、サードパーティソフトウェアの知的財産権を保護する基本的な方法です。
サードパーティは、STM32 マイクロコントローラ用の固有のソフトウェア IP を開発して販売することがあります。OEM メーカーは、自社アプリケーションコードの開発時にそれらを使用することがあります。独自仕様コード読出し保護は、サードパーティ IP の機密性を守り、悪意のあるユーザから知的財産権を保護する役に立ちます。
言い方を変えると、PcROP は、悪意のあるソフトウェアまたはデバッガが機密コードを読み出すのを防止することにあります。
保護領域は実行専用であり、STM32 CPU からのみ実行コードとしてアクセス可能ですが、その他すべてのアクセス（DMA、デバッグ、CPU のデータ読出し、書込み、消去）が厳しく禁じられています。すなわち、保護すべきコードは、特定のコンパイラオプションを用いてコンパイルする必要があります。
例：「–execute_only」（Keil ツール用）

PcROP の設定と制約事項

- 設定と制約事項
  - PCROP 領域は、オプションバイト設定を介して定義されます。
  - 2KB単位で 2 つの保護領域を設定できます。
  - PCROP 領域のサイズは、増やすことはできても減らすことはできません。
  - PcROP を無効とする唯一の方法は、レベル 1 からレベル 0 に RDP を遷移させることです。
- オプションビット *PCROP_RDP*
  - 有効になると、RDP 回帰がレベル 1 からレベル 0 となる間に PCROP 領域が消去されるのを防止します。そうでない場合、Flash メモリ全体が消去されます。

life.augmented

Flash メモリの独自仕様コード読出し保護領域は、オプションバイトを介して定義します。
STM32WB デバイスの PcROP 機能は改良されています。分離した 2 つの PcROP 領域が独立して設定可能となりました（バンク当たり 1 個）。それぞれ、開始アドレスと終了アドレスによって定義される 64bit 単位の領域です。 ひとたび PcROP 領域が設定されると、そのサイズは増加だけが可能であることに注意してください。
ひとたび PcROP 領域が定義されると、
この保護機能を無効とする唯一の方法は、RDP 保護レベルを'1'から'0'に変更することですが、これによって Flash メモリ全体が消去されます。

RDP レベル回帰の場合の PCROP 領域の消去ポリシーは、PCROP_RDP オプションビットを介して定義されます。オプションバイトの PCROP_RDP ビットを設定すると、PcROP 領域のコードは失われず、保護が解除されなくなります。

PcROP の「実行のみ」の意味をさらに説明すると、

- PcROP は RDP のサブステートです。PcROP は、STM32 上で実行される他のコードが Flash メモリを読み出すことを防止するように設計されています。これは、保護対象が外界である RDP と同じではありません。PcROP が有効になっていると、AHB は命令バスの動作のみを許可しますので、コードの実行のみが可能となります。データバスは、Flash メモリにアクセスできません。
- ひとたび開発フェーズが完了すれば、PCROP を RDP 設定のレベル 1 に変更できます。この場合、外部からは読出しのみに制限されます。ただし、特定セクターに対する PcROP 設定は、そのコードの読出しを試みるすべてのマスタになおも適用されたままです。

書込み保護機能

次に、STM32WB の書込み保護設定の詳細についてじっくりと見てみましょう。

Flash 書込み保護

- 設定と制約事項
  - 書込み保護領域は、オプションバイトを介して定義されます。
  - STM32WB では、ページ単位（4KB）の 2 つの WRP 領域の設定が可能です。
  - WRP 領域のサイズは、RDP がレベル 2 でない限り修正可能です（オプションバイトを変更）。
- 特性
  - WRP 領域が定義／有効化されている場合、この領域に対する書込み／消去操作は許可されません。

Flash メモリ書込み保護メカニズムは、変化しないブートローダや較正定数などの Flash メモリの定義された領域への不要な書込みアクセスを防止するように設計されています。
書込み保護領域は、オプションバイトを介して定義されます。
ユーザは、異なる書込み保護された Flash メモリ領域を、独立に最高 4 個定義できます（バンク当たり 2 個）。4 個の Flash メモリ領域は、ページ単位（4KB）の開始アドレスと終了アドレスで定義されます。
書込み領域のサイズは、RDP レベルがレベル 2 に設定されていない限り修正可能です。
消去操作は、書込み保護領域への書込み操作として扱われますので、許可されません。

関連ペリフェラル

- 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。
  - STM32WB-メモリ-Flash
    - Flash メモリのアーキテクチャ
  - STM32WB-システム-CM0+ セキュリティ
    - Cortex-M0+ 機能の説明と設定
  - STM32WB-セキュリティ-ルートセキュリティサービス（RSS）
    - RSS 機能の説明（ワイヤレススタックのインストール／更新 & CKS）

life.augmented

このトレーニングに加えて、これら 3 つのトレーニングが役に立つことがわかるでしょう。