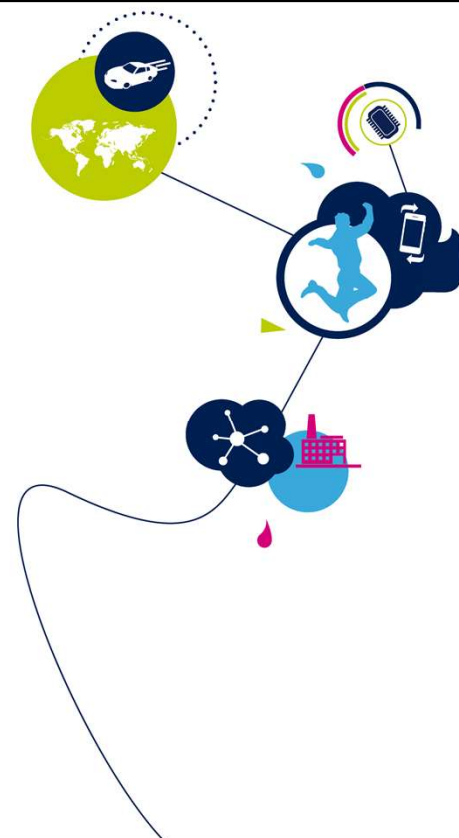


# STM32G4 – Flash

内蔵Flashメモリ

0.1版



こんにちは、STM32G4マイクロコントローラファミリや、すべての製品に含まれている組み込みFlashメモリのプレゼンテーションへようこそ。

- STM32G4は、デュアルバンク・アーキテクチャを備えた最大512キロバイトのFlashメモリを内蔵
- Flashメモリインタフェースは、すべてのアクセス（読出し、プログラミング、削除）、メモリ保護、セキュリティ、およびオプション・バイト・プログラミングを管理

### アプリケーション側の利点

- 高性能で低消費電力
- 書込み中読出し機能
- 小さな消去粒度
- 短いプログラミング時間
- デュアルバンク・ブート
- セキュリティと保護



STM32G4マイクロコントローラは、デュアルバンクアーキテクチャを備えた最大512キロバイトのFlashメモリを内蔵しています。

Flashメモリインタフェースは、すべてのメモリアクセス（読出し、プログラミング、および削除）だけでなく、メモリ保護、セキュリティ、オプションバイトを管理します。

このFlashメモリインタフェースを使用するアプリケーションは、低電力アクセスと共にその高パフォーマンスという利点を活用できます。それは書込み中での読出（RWW）サポート、消去の単位が小さく、プログラミング時間も短く、デュアルバンクブートを可能にします。

コードとデータ、読出しや書込みアクセスに対して、さまざまなセキュリティと保護メカニズムを備えています。

# STM32G43X/4XとSTM32G47X/8Xの違い

3

	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)
サイズ	128キロバイト	512キロバイト	
バンク数	1	1	2
データ幅	64ビット	128ビット	64ビット
ページサイズ	2キロバイト	4キロバイト	2キロバイト
Flash構成	64ページ	128ページ	128ページ
書込み保護領域(WRPs)	2	4	2/バンク
独自仕様コード読出し保護領域(PCROPs)	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Flashメモリの実装に関する相違点をハイライトしています。

Flashメモリのサイズは、カテゴリ2の場合は128キロバイト、カテゴリ3の場合は512キロバイトです。

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、カテゴリ3の場合は1、または2です。書込み中読出し機能(RWW)は、デュアルバンクアーキテクチャがアクティブな場合にのみサポートされます。これにより、一方のバンクをプログラミングまたは削除し、もう一方のバンクからのコードを実行できます。

最小の消去の単位を提供するページサイズは、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、デュアルバンクの場合は2キロバイトです。

ページ数はカテゴリ2の場合は64ページ、カテゴリ3の場合は128ページです。

保護機能に関しては、カテゴリ2のマイクロコントローラは2つの書込み保護領域、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4つの書込み保護領域、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があります。

- ページ消去、バンク消去、マス消去
- 高速消去 (22ms) と高速プログラミング時間 (ダブルワードで82 $\mu$ s)
- 2つのプログラミングモード:
  - 標準 (メインメモリおよびOTP用)
  - 高速 (メインメモリのみ)
    - Flashのベリファイ確認無しでプログラム64ダブルワード
- エラーコード訂正 (ECC): 64ビットダブルワードで8ビット
  - シングルビット・エラーの検出と訂正、マスク可能な割込みによる通知
  - ダブルビット・エラーの検出と通知、NMIIによる通知



Flashメモリは、ページ消去、バンク消去、およびマス消去をサポートします。

ページ、バンク、またはマス消去の操作は22msしか必要とされず、ダブルワードの場合、プログラミング時間は82 $\mu$ sです。

高速プログラミングモードは、64個のダブルワードを連続して書き込み、ページプログラミング時間を短縮して、各ダブルワードアクセスのFlashのベリファイを確認する必要をなくし、さらに、ダブルワード書き込みごとに高電圧の立ち上がり時間と立ち下がり時間を回避します。

プログラムするダブルワードに8ビットECCコードが追加されます。読み取り時にチェックされ、シングルビットエラーを検出して修正し、ダブルビットエラーを検出します。

修正できないエラーが発生した場合、Flashメモリコントローラは、マスク不可割り込み (NMI) をCortex®-M4に通知します。

- ART Accelerator™ (命令キャッシュ、データ・キャッシュ、プリフェッチ・バッファ)は周波数に対して線形の性能を実現
- 保護:
  - 書込み保護領域
  - 独自仕様コード読出し保護領域
  - WPR領域、2つのPCROP領域、2セキュリティ保護可能なメモリ領域
  - デュアルバンク・モード:バンクごとに2WPR領域、バンクごとに1つのPCROP領域、バンクごとに1つのセキュリティ保護可能なメモリ領域



適応型リアルタイムメモリアクセラレータ (ART Accelerator) は、命令キャッシュ、データキャッシュ、プリフェッチバッファを備えており、周波数に対して線形のパフォーマンスを実現します。また、Vcoreパワードメインに属する電力消費の低減にも貢献します。

以下の保護メカニズムがサポートされています。

- 不要な書き込み操作から保護するために使用される書き込み保護領域。
- 独自仕様コード読出し保護領域 (またはPCROP): Flashメモリの一部を第三者からのアクセスから保護することができます。
- 保護領域は実行専用であり、命令コード域としてSTM32 CPUのみ読み取り可能ですが、他のすべてのアクセス (DMA、デバッグ、およびCPUデータとしての読み取り、書き込み、消去) は厳しく禁止されています。
- セキュリティ保護可能なメモリ領域は、新しいリセットが発生しない限り、ブート時に1度だけ実行できるコード領域を定義します。

Flashメモリは次のように構成されている:

- 64ページまたは128ページを含むメインメモリ・ブロック
  - シングルバンクを持つカテゴリ3デバイスの場合、ページサイズは4キロバイト
    - 各ページは、512バイトの8行で構成される
  - カテゴリ2デバイスとデュアルバンクを備えたカテゴリ3マイクロコントローラの場合、ページ・サイズは2キロバイト
    - 各ページは、256バイトの8行で構成される
- 情報ブロックは次を含む:
  - STブートローダ用に予約済みのシステムメモリ
  - ユーザ・データに使用する1キロバイト(128ダブルワード)のOTP(ワンタイム・プログラマブル)領域
    - OTP領域のデータは消去不能、ダブルワードを1回だけ書き込める
  - ユーザ設定のオプション・バイト



メインメモリは、マイクロコントローラのカテゴリに応じて64または128ページが含まれます。

シングルバンクアーキテクチャを持つカテゴリ3の場合、ページサイズは4キロバイト、各ページは512バイトの8行で構成されます。デュアルバンクアーキテクチャを持つカテゴリ3とカテゴリ2の場合、ページサイズは2キロバイトで、各ページは256バイトの8行で構成されます。

メインFlashメモリに加えて、STM32G4は:

- STブートローダを含む28キロバイトのシステムメモリ
- 消去または変更してはならないユーザデータを格納するために使用できる1キロバイトのOTPメモリ。ダブルワードの1つのビットを“0”に設定すると、ダブルワード全体はオールゼロ以外の値を書き込めなくなります。
- システムオンチップ内のIPを設定するためのデフォルト設定を含むオプションバイト。これらは、電源投入リセット後に自動的にロードされます。

## Flashメモリの構成 (2/2)

7

Flash領域		Flashメモリ・アドレス (カテゴリ3、デュアルバンク)	サイズ	名前	オペレーション	粒度
メイン メモリ	バンク1	0x0800_0000 – 0x0800_07FF	2キロバイト	ページ0	プログラミング	8バイト
		...	...	...	高速プログラミング	512バイト行
		0x0803_F800 – 0x0803_FFFF	2キロバイト	ページ127	消去	マス、バンク、ページ
	バンク2	0x0804_0000 – 0x0804_07FF	2キロバイト	ページ0	セキュリティ保護可能なメモリ	ページ
		...	...	...	書込み保護	
		0x0807_F800 – 0x0807_FFFF	2キロバイト	ページ127	読込み保護	グローバル
インフォメーション ブロック	0x1FFF_0000 – 0x1FFF_6FFF	28キロバイト	システムメモリ	独自仕様コード読出し保護領域	クワッドワード(カテゴリ3シングルバンク)もしくは、ダブルワードアライメント	
	0x1FFF_7000 – 0x1FFF_73FF	1キロバイト	OTPエリア			
	0x1FFF_7800 – 0x1FFF_787F	48バイト	オプションバイト			



life.augmented

左の表は、メインFlashメモリの領域のデュアルバンクアーキテクチャを持つカテゴリ3マイクロコントローラと、インフォメーションブロックに基づくメモリ構成を詳述しています。

右の表は、Flashメモリへのオペレーションを詳しく示しています。

- プログラミングは8バイトのダブルワードで行われる
- 高速プログラミングは512バイトの行で行われます
- 消去は、グローバルに(大量消去)するか、バンクまたはページの単位で行われます。
- セキュリティ保護可能なメモリはページ上に配置されます。
- 書込み保護はページごとに行われます
- 読取り保護はグローバル単位です
- 独自仕様コード読出し保護領域は、クワッドワードまたはダブルワードのいずれかの整列されたプログラム可能な開始アドレスと終了アドレスに基づいています。



## 書き込み中の読出し、およびデュアルバンクブート機能

- ユーザ・オプションのバイト・オプションDBANKは、デュアルバンク・モードを選択
- デュアルバンク・ブート機能を備えたデュアルバンクFlashメモリ
  - ユーザ・オプション・バイトのオプションBFB2
    - BFB2 = 1、有効なバンクに応じて、バンク2またはバンク1からデバイスが起動
    - BFB2 = 0、バンク1のみでのデバイスが起動
- 書き込み中の読出し
  - デュアルバンク機能により、一方のバンクから読み取り、もう一方のバンクをプログラミング/消去することが可能
    - Flashメモリがプログラムが書かれているときにコード実行が停止されない
  - 同じバンクでデータをプログラミング/消去する場合: AHBはプログラム/消去操作が進行中で停止



DUALBANK (DBANK) オプションは、カテゴリ3デバイスに対してシングル・バンクまたはデュアル・バンクのいずれかを選択するために使用されます。

Flashメモリは、2つのバンクをサポートするように設定でき、書き込み中の読出し機能とデュアルバンクブート機能を備えており、バンク1またはバンク2から起動できます。

ユーザオプションバイトのBFB2オプションは、デュアルバンクブートモードを選択するために使用されます。BFB2オプションが設定されている場合、デバイスは有効なバンクに応じてバンク2またはバンク1から起動します。BFB2オプションをオフにすると、デバイスは常にバンク1から起動します。



## 170MHzで213DMIPS

- 適応型リアルタイム・アクセラレータ (ART Accelerator™) は、Flashメモリのアクセス時間に関係なく、周波数に対して線形パフォーマンスを実現

ウェイト状態 (WS) (Flash遅延)	HCLK (MHz)		
	V <sub>CORE</sub> レンジ1 ブースト・モード	V <sub>CORE</sub> レンジ1 ノーマル・モード	V <sub>CORE</sub> レンジ2
0 WS	≤ 34	≤ 30	≤ 8
1 WS	≤ 68	≤ 60	≤ 16
2 WS	≤ 102	≤ 90	≤ 26
3 WS	≤ 136	≤ 120	-
4 WS	≤ 170	≤ 150	-

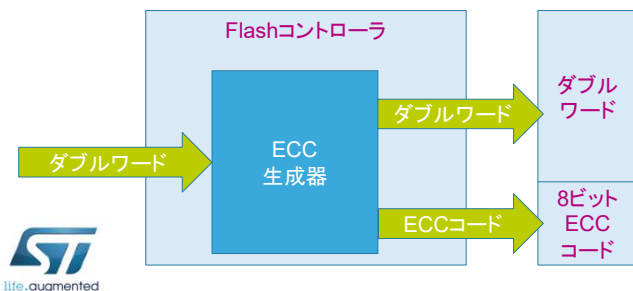


Flashメモリを読み取るためには、クロック周波数に応じて、読出しアクセスに挿入されるウェイト状態の数を設定する必要があります。待機状態の数も電圧スケーリング範囲によって異なります。レンジ1では、Flashメモリは4つのウェイト状態で最大170MHzにアクセスできます。0のウェイト状態で34MHzまでアクセスできます。レンジ2の場合、26MHzまで、ウェイト状態が2です。適応型リアルタイムアクセラレータ、ARTアクセラレータにより、プログラムはクロック周波数に依存しない0待ち状態で実行することができます。これは周波数170MHzに対して、213Dhrystone MIPSのベンチマークの結果に関連してほぼ線形性能を提供します。

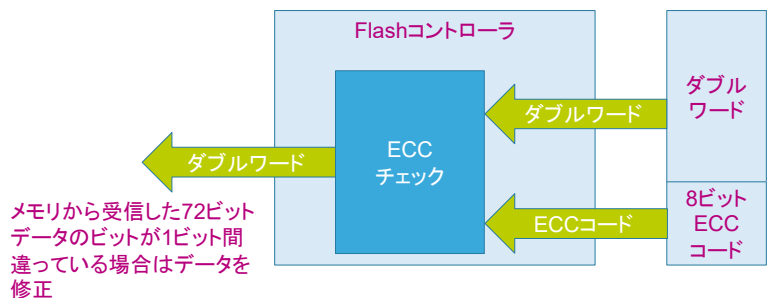
## 堅牢なメモリの完全性と安全性

- **ECC(エラーコード訂正):64ビットワードの場合、8ビットの長さ**
  - シングルビット・エラー訂正:FLASH\_ECCRで設定されたECCCビット、オプションの割込み生成
  - ダブルビット・エラー検出:ECCDビットセットFLASH\_ECCR => NMI
  - FLASH\_ECCRレジスタにエラー・アドレスが保存

## プログラミング



## 読出し



Flashメモリワードデータは72ビット幅で、各ダブルワード(64ビット)ごとに8ビットが追加されます。ECCメカニズムは以下をサポートします

- 1ビットのエラー検出と修正
- 2ビットのエラー検出

1ビットのエラーが検出されて修正されると、ECCCフラグ(ECC訂正)がFlash ECCレジスタにセットされます(FLASH\_ECCR)。また割込みを生成できます。

2ビットのエラーが検出されると、Flash ECCレジスタ(FLASH\_ECCR)にECCDフラグ(ECC訂正)がセットされます。この場合、NMIが生成されます。

## 堅牢なメモリの完全性と安全性

- プログラミングの単位は64ビット(実際は8ビットECCを含む72ビット)
  - シングルバンクのカテゴリ3デバイスの場合は144ビット(72ビットx2)
- 2つのプログラミング・モード:
  - 標準(メインメモリおよびOTP用)
  - 高速(メインメモリのみ)
    - Flashメモリのベリファイを確認せずに64ダブルワードでプログラム



高速プログラミングにより、256バイトの行をプログラミングが出来ます。通常のプログラミングは8バイト単位となります。

高速プログラミングの主な目的は、ページ単位のプログラミング時間を短縮することです。高速モードでは、アドレス位置の内容はプログラミング前にチェックされません。ダブルワードごとの電圧の上げ下げを節約できます。

# プログラミング/消去時間

12

短いプログラミングと消去時間&小さいページサイズ  
→データEEPROMエミュレーションの利点

パラメータ	標準値
64ビットプログラミング時間	82μs
1行(256バイト)のプログラミング時間	標準モード:2.61ms 高速モード:1.91ms
1ページ(2キロバイト)のプログラミング時間	標準モード:20.91ms 高速モード:15.29ms
バンク・プログラミング時間	標準モード:2.68s 高速モード:1.96s
ページ(2キロバイト)の消去時間	22.02ms
マス消去時間	22.13ms



- プログラム操作と消去操作は、電圧スケーリングのレンジ1でのみ可能

高速プログラミングは、標準モードプログラミングより3分の1高速です。

512キロバイトの消去操作のマス消去時間は、ページ消去とほぼ同じ時間を要します。

# 行(64ダブルワード)高速プログラミング

13

- 高速プログラミングでプログラムできるのはメインメモリのみ
  - OTPバイトもオプション・バイトも不可
- プログラミング前に、ハードウェアによるFlashロケーションの検証はしない
- 64のダブルワードは連続して書く必要がある
  - すべてのプログラミングのため、Flashメモリには高電圧が維持される
  - 連続した2つのダブルワード書込みリクエスト間の最長時間は、プログラミング時間(50 $\mu$ s前後)で規定される=>ただし、割込みは無効にする
- Flashクロック周波数(HCLKS)は少なくとも8MHzとする必要がある



高速プログラミングと標準プログラミングでは

- メインFlashメモリのどこにでも位置する8バイトのダブルワードの代わりに512バイトがプログラムされる
  - 8バイトのプログラミングは、検証手順により信頼性が高い
- 2つの連続したダブルワードの間の最大時間は約50  $\mu$ sであることに注意してください。この遅延の後に2番目のダブルワードが到着すると、高速プログラミングは中止され、エラーフラグがセットされます。したがって、この遅延を超えないように、割込みを無効にする必要があります。

# プログラミング・モード: 標準vs高速

14

	プログラミング・モード	
	標準	高速
対象	メインメモリ+OTPエリア	メインメモリのみ
粒度	8バイト	256バイト
固有の制限	なし	アドレス位置のチェックなし Flashクロック周波数 $\geq$ 8MHz 割込み禁止
256バイトのプログラムに要する時間	2.61ms	1.91ms



このスライドは、標準プログラミングモードと高速プログラミングモードの比較を示しています。

- デザイン上の期待値

耐久性	40°C~+105°Cで最低10000回書き換え
データ保持	55°Cで10000回書き換え後30年 85°Cで10000回書き換え後15年 105°Cで10000回書き換え後10年
	85°Cで1000回書き換え後30年 105°Cで1000回書き換え後15年 125°Cで1000回書き換え後7年



それぞれプログラム/消去の操作は、Flashメモリセルを劣化させます。

プログラム/消去サイクルを何度も行うとメモリセルは、メモリエラーを引き起こし、機能しなくなる可能性があります。

耐久性とは、Flashメモリが信頼性に影響を与えることなくサポートできる消去/プログラミングシーケンスの最大数です。

データ保持は、指定された期間、特定のデータパターンを保持すると定義されます。

保持は、プログラム/消去サイクルの数と温度によって異なります。

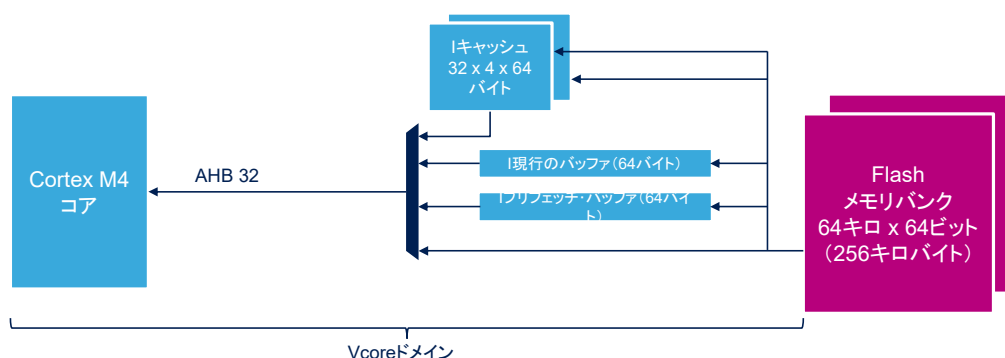


# 適応型リアルタイム・メモリアクセラレータ (ART Accelerator™)

16

## 優れたパフォーマンスと低消費電力

- 命令キャッシュ: 32ラインの4x64ビット(1キロバイト)、命令用
- データ・キャッシュ: 8ラインの4x64ビット(256バイト)、リテラルプール用
- プリフェッチ・バッファ: 64ビット1ライン
- 最高のトレードオフ キャッシュ・サイズ、パワー、パフォーマンス



ARTアクセラレータは、優れた性能を発揮し、動的消費電力を低減します。

1キロバイトの命令キャッシュ、256バイトのデータキャッシュ、およびプリフェッチバッファで構成されます。

命令キャッシュには32ラインの4つのダブルワードが含まれ、データ・キャッシュには8ラインの4つのダブルワードがあります。

命令キャッシュ・メモリ・ラインがすべて満杯になると、LRU(最も使用されにくい)ポリシーを使用して、命令メモリ・キャッシュ内で置き換えるラインを判別します。

この機能は、ループを含むコードの場合に特に有益です。

このアーキテクチャは、キャッシュサイズ、消費電力、パフォーマンスの間で最良のトレードオフを実現するために選択したものです。

キャッシュミスが発生する度に、キャッシュは要求されたダブルワードによってのみ更新されます。そうすることで、Flashへのアクセスを制限し消費電力を抑えることができます。ライン内の4ダブルワードは全て有効であるとは限りません。

キャッシュミスの場合、Cortex M4コードはFlashメモリから直接命令を取得します。

並行して、64ビットのラインが有効化された現行バッファと有効化されていれば命令キャッシュにコピーされます。従って、次のシーケンシャルアクセスは現行バッファから直接行なわれます。

プリフェッチが有効な場合、さらに64ビットのFlashメモリアccessが行なわれ、プリフェッチバッファはシーケンシャルデータで満たされます。

データが現行バッファにある場合、CPUは現行バッファを読み出します。

その次のシーケンシャル読出しはプリフェッチバッファにて行なわれ、同時に現行バッファにコピーされるため、次のシーケンシャルデータを格納するためのスペースが確保できます。

データが現行バッファになく、プリフェッチバッファにあればそこから読み出されます。

プリフェッチバッファになければ、キャッシュヒットしている場合、命令キャッシュから読み出されます。そうでない場合、Flashアクセスが行なわれます。

消費電力とパフォーマンスの結果は、アプリケーション・コードに依存  
ほとんどの場合、キャッシュがONかつプリフェッチがOFFの条件でエネルギー効率は最高

- プリフェッチがON: ARTの命令キャッシュは分岐キャッシュのように動作
  - キャッシュは処理フロー内で分岐/ジャンプが発生するたびに更新
  - シーケンシャル・アクセスは、現行命令バッファ+プリフェッチバッファにより発行
  - プリフェッチ・バッファがアクセスされるたびに、その内容が現行命令バッファに転送され、プリフェッチバッファを満たす新しいFlashアクセスが行われる
    - したがって、キャッシュ内容は変更されない
- プリフェッチがオフ(リセット値): ARTのキャッシュは普通のキャッシュのように動作
  - プリフェッチバッファが無効なので、シーケンシャルアクセスでもキャッシュ・コンテンツが変更される



命令キャッシュは、プリフェッチバッファが有効か無効かによって動作が異なります。

プリフェッチバッファが有効な場合、ARTの命令キャッシュは分岐キャッシュのように動作します。

キャッシュは処理フロー内で、分岐、または、ジャンプが発生するたびに変更されます。

シーケンシャルアクセスは現行命令バッファとプリフェッチバッファにより発行されます。プリフェッチバッファがアクセスされるたびに、その内容は現行命令バッファに転送され、プリフェッチバッファにデータを満たすための新しいFlashアクセスが行なわれます。この場合、キャッシュの内容は変更されません。

プリフェッチバッファが無効になっている場合、ART命令キャッシュは普通のキャッシュのように動作します。

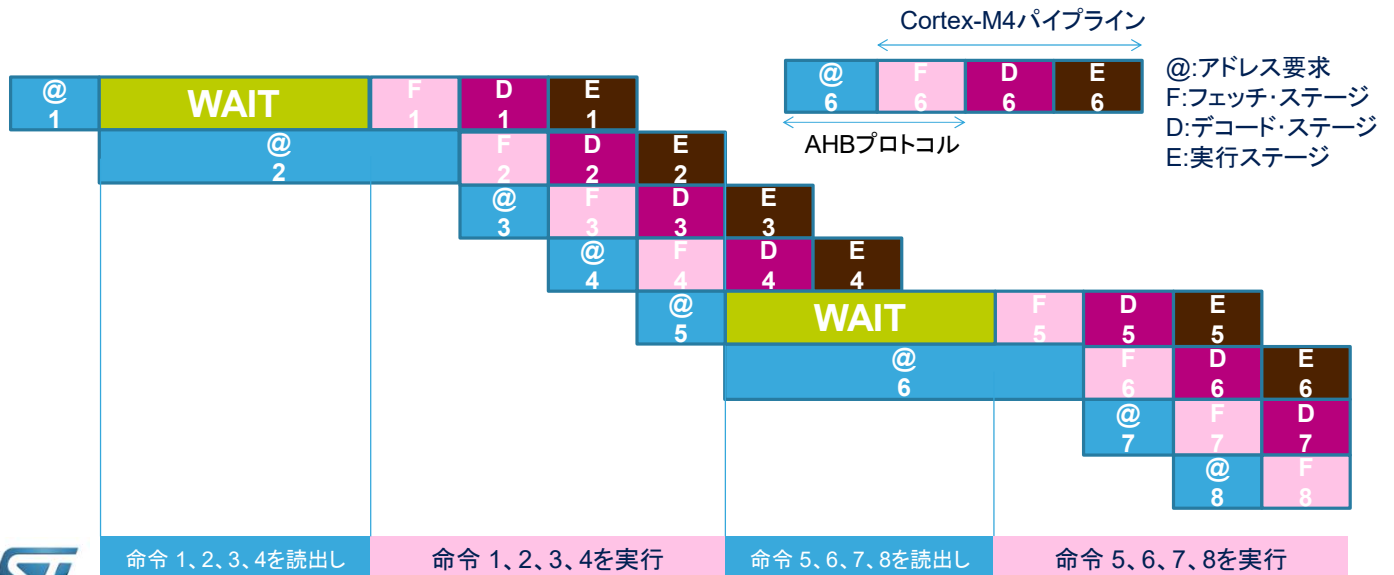
プリフェッチバッファは無効なので、シーケンシャルアクセスでもキャッシュの内容が変更されます。

消費電力とパフォーマンスのトレードオフは、アプリケーションごとに評価し、プリフェッチバッファの有効、無効を判断する必要があります。

ほとんどのアプリケーションでは、プリフェッチバッファを有効にすることでパフォーマンスが若干向上しますが消費電力が増えます。

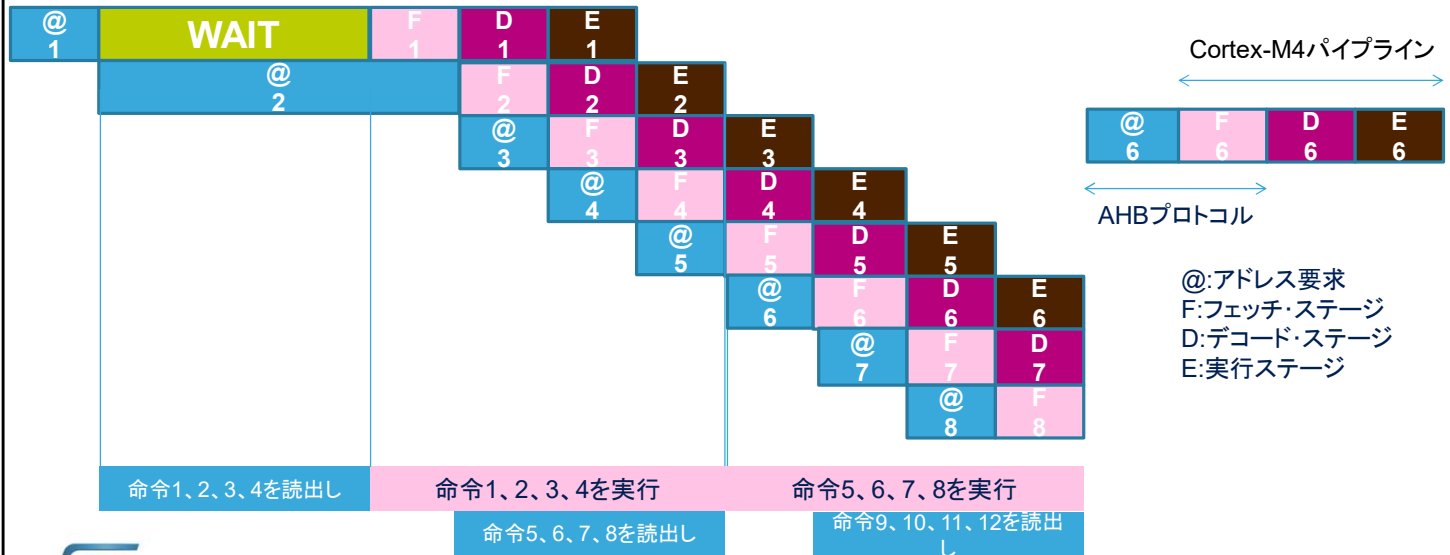
一般的に、Flashアクセスの数が減るため、キャッシュが有効になり、プリフェッチバッファが無効になっている場合、一般的に最適なエネルギー効率が提供されます。

# シーケンシャル16ビット命令の実行(3WS) プリフェッチ無し



本スライドは、Flashメモリへのアクセスに3ウェイト状態必要な場合で、プリフェッチ無効時にシーケンシャル16ビット命令の実行に必要なサイクル数を示しています。各Flashアクセスにより64ビットまたは4命令を取得できます。これにより、各Flashアクセスにおいて、4命令ごとに3ウェイト状態が挿入されます。

# シーケンシャル16ビット命令の実行(3WS) プリフェッチ有効



本スライドは、Flashメモリへのアクセスに3ウェイト状態が必要な場合で、プリフェッチ有効時にシーケンシャル16ビット命令の実行に必要なサイクル数を示しています。各Flashアクセス後に、次のFlashアクセスを行ないプリフェッチバッファを満たすことができます。

従って、現行バッファから全ての命令がフェッチされた後、次のシーケンシャル命令はプリフェッチバッファより読み出され、命令フローが順番に処理される限り、ウェイト状態は挿入されません。

## アプリケーションでの必要性に応じた柔軟なFlashメモリ保護機能

- 読出し保護(RDP)
  - SRAMからのブート時、ブートローダの選択時、またはデバッグ・インタフェース(JTAG/SWD)によるFlash/SRAM/バックアップ・レジスタへのアクセスを禁止
- 独自仕様コード保護(PCROP)
  - 読出し、または書込みアクセスから特定のコード域を保護するために使用
    - コードの実行のみ可能
- 書込み保護(WRP)
  - 不要な書込みアクセスおよび消去から特定のコード領域を保護するために使用



life.augmented

オプションバイトを使用して、複数のFlashメモリ保護オプションを設定できます。

読出し保護は、Flashメモリ、オプションバイト、内部CCM SRAMおよびバックアップレジスタの内容を、デバッガやソフトウェアの読み取りによって要求された読出しから保護することを目的としています。

Flashメモリからのブートのみが、これらのメモリの内容を読出すことを許可されます。

独自仕様コードの保護は、Flashメモリの一部を実行専用としてマークする方法です。この種のアクセス許可は、Cortex®-M4コアに存在するメモリ保護ユニットではサポートされないことに注意してください。

PCROP領域は、Flashメモリの一部だけをサードパーティの読み取りから保護するのに役立ちます。

書込み保護により、Flashメモリの一部が消去および再プログラムされるのを防ぐことができます。

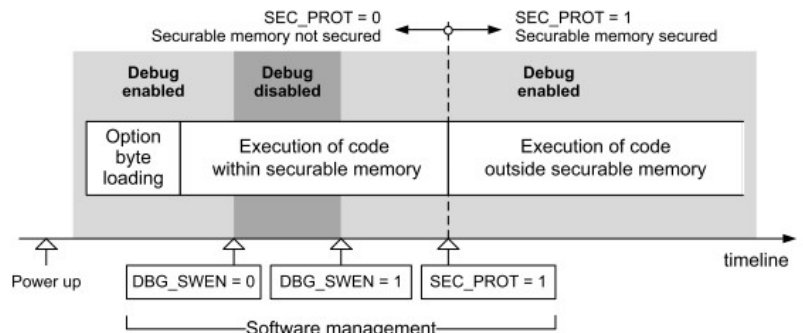
## アプリケーションでの必要性に応じた柔軟なFlashメモリ保護機能

- セキュリティ保護可能なメモリ領域

- アクティブ化すると、セキュリティ保護可能なメモリ領域へのアクセス(フェッチ、読み出し、プログラミング、消去)が拒否され、バス・エラーが発生

- コアデバッグ・アクセスの無効化

- セキュリティ保護可能なメモリ領域でコードを実行する際のデバッグ・アクセスの時間的な無効化



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ことです。これにより、イメージ認証を担当するセキュアキーストレージやセキュア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できます。プロセッサがセキュリティ保護可能なメモリを出ると、Flashメモリのこの部分にはアクセスできなくなります。

保護可能な領域は、デバイスをリセットすることによってのみ保護を解除できます。

セキュリティ保護可能なメモリ領域のサイズは、ページ上で調整されます。

さらに、セキュリティ保護可能なメモリから実行されたコードは、デバッグアクセスを一時的に無効にする可能性があります。

- ユーザ・オプション・バイトは次の場合に読み込まれる
  - 電源リセット後 (BORまたはSTANDBY/SHUTDOWNの終了)
  - Flash制御レジスタ (FLASH\_CR) のOBL\_LAUNCHビットがセットされたとき

オプション	説明	コメント
BOR_LEV[2:0]	ブラウンアウト・リセットの閾値レベル	STM32G4の新機能
nRST_STOP; nRST_STDBY; nRST_SHDW	STOP/STDBY/SHUTDOWNモード終了時のリセットの生成/リセットの 不生成	STM32F3と同じ
WWDG_SW; IDWG_SW IWDG_STOP; IWDG_STDBY	ハードウェア/ソフトウェア・ウィンドウのウォッチドッグ/独立型ウォッチ ドッグSTOP/STANBYモード時の、独立型ウォッチドッグのカウンタ停止 の有無	STM32F3と同じ
BFB2	デュアルバンク・ブートの有効化/無効化	STM32G4の新機能
DBANK	128ビットデータ読み取り幅のシングルバンク・モードと64ビットデータ読み 取り幅のデュアルバンク・モード間の選択	STM32G4の新機能
nBOOT1	ブート設定 (BOOT0ピンと一緒に)	STM32F3と同じ
nSWBOOT0	オプションビットnBOOT0から取得されたBOOT0	STM32G4の新機能
nBOOT0	またはPB8/BOOT0ピンから	STM32G4の新機能
CCM SRAM_RST	システムリセット時、CCM SRAM消去	STM32G4の新機能
SRAM_PE	SRAM1およびCCM SRAMパリティチェックを使用可能	STM32F3と同じ



オプションバイトは、Cortex®-M4を起動する前に、システムオンチップを早期に設定するために使用されます。これらは48バイトあります。

電源リセット後、またはFLASH\_CRレジスタにOBL\_LAUNCHビットのセットに応じて、自動的に読み込まれます。この機能は、デバイスをリセットせずに新しい設定を適用するために必要です。このスライドと次の2つのスライドでは、オプションバイトの各種フィールドについて説明します。



オプション	説明	コメント
BOOT_LOCK	設定すると、メインFlashメモリから強制的にブートする	STM32G4の新機能
SEC_SIZE1[7:0] SEC_SIZE2[7:0]	バンク1の確保可能なメモリ領域のサイズ バンク2の確保可能なメモリ領域のサイズ	STM32G4の新機能 STM32G431はSEC_SIZE2なし
IRHEN	内部リセット・ホルダ・イネーブル・ビット	STM32G4の新機能
NRST_MODE	PG10/NRST機能選択	STM32G4の新機能



Bootlockは、他のブートオプションに関係なく、システムをメインFlashメモリから強制的に起動させます

# ユーザ・オプションバイト(セキュリティ)

オプション	説明	コメント
RDP[7:0]	読出し保護レベル	STM32F3と同じ
PCROP1_STRT[14:0] PCROP1_END[14:0] PCROP2_STRT[14:0] PCROP2_END[14:0]	バンク1 PCROP エリア開始オフセットアドレス バンク1 PCROP エリア終了オフセットアドレス バンク2 PCROP エリア開始オフセットアドレス バンク2 PCROP エリア終了オフセットアドレス	STM32G4の新機能
PCROP_RDP	RDP レベルが低下した場合に保持される PCROP 領域	STM32G4の新機能
WRP1A_STRT[6:0] WRP1A_END[6:0] WRP1B_STRT[6:0] WRP1B_END[6:0] WRP2A_STRT[6:0] WRP2A_END[6:0] WRP2B_STRT[6:0] WRP2B_END[6:0]	バンク1 書き込み保護領域 A 開始 オフセットアドレス バンク1 書き込み保護領域 A 終了 オフセットアドレス バンク1 書き込み保護領域 B 開始 オフセットアドレス バンク1 書き込み保護領域 B 終了 オフセットアドレス バンク2 書き込み保護領域 A 開始 オフセットアドレス バンク2 書き込み保護領域 A 終了 オフセットアドレス バンク2 書き込み保護領域 B 開始 オフセットアドレス バンク2 書き込み保護領域 B 終了 オフセットアドレス	STM32F3では、書き込み保護は2ページの単位で実装され、2ページごとに1つのオプション・ビットがある



読出し保護レベルにより、Flashメモリ全体の読出し保護が可能:

- レベル0:保護なし
- レベル1:読出し保護
- レベル2:デバッグ不可

レベル0からレベル1、部分的または一括消去を意味するレベル1からレベル0、レベル0からレベル2、レベル1からレベル2までの遷移がサポートされます。

- PCROPA\_STRTとPCROPA\_ENDは、独自のコード読出し保護アドレス範囲Aを定義します。
- PCROPB\_STRTとPCROPB\_ENDは、独自のコード読出し保護アドレス範囲Bを定義します。
- PCROP\_RDPは、RDP保護がレベル1からレベル0に変更されたときにPCROP領域を消去するか、または消去しないかの選択を行うことができます。

割込みイベント	説明
操作終了	1つまたはそれ以上のFlashメモリの操作(プログラム/消去)が正常に完了するとハードウェアによってセット
操作エラー	Flashメモリの操作(プログラム/消去)が正常に完了しなかったときに、ハードウェアによってセット
読出しエラー	読み取るアドレスがFlashの読取り保護領域に属している場合はハードウェアによってセット(PCROP保護)
書出しエラー	消去/プログラムされるアドレスがFlashメモリの書き込み保護された部分(WRP、PCROPまたはRDPLレベル1)に属している場合、ハードウェアによってセット
サイズ・エラー	プログラムまたは高速プログラム・シーケンス中に、アクセスのサイズがバイトまたはハーフワードである場合に、ハードウェアによってセット ダブルワード・プログラミングのみ可能
プログラミング・エラー	プログラムされるダブルワード・アドレスが、書き込むデータが0x0000_0000の場合を除いて、プログラミング前に0xFFFF_FFFFとは異なる値が含まれている場合に、ハードウェアによってセット
プログラミング・シーケンスエラー	Flashメモリへの書き込みアクセスが実行される場合、ハードウェアによってセット PGまたはFSTPGが以前に設定されていない間にコードを記述 以前のプログラミング・エラーにより、PROGERR、SIZERR、PGAERR、WRPERR、MISSERRまたはFASTERRが設定されている場合も、ハードウェアによってセット

Flashメモリコントローラは、このスライドと次のスライドに示されているように多くの割込みソースをサポートしています。操作が正常に終了すると、割込みをアサートできます。プログラム/消去操作中にエラーが発生した場合、割込みをアサートすることもできます。保護違反によっても割込みが発生する可能性があります。サイズエラーは、プログラムするデータがワードアラインドでない場合に発生します。プログラムの操作が、事前にFlashメモリを消去していないときに、エラーが発生します。

割込みイベント	説明
プログラミング・アライメントエラー	通常プログラミングの場合、同じダブルワード(64ビット)Flashメモリにデータを含めることができない場合、または高速プログラミング中にページの変更がある場合、ハードウェアによってセット
高速プログラミング中のデータミス・エラー	新しいデータが時間内に存在しない場合は、ハードウェアによってセット
高速プログラミング・エラー	高速プログラミングシーケンス(FSTPGによってアクティブ化)がエラーのために中断された場合、ハードウェアによってセット
オプションの有効性エラー	読み取ったオプションがユーザーによって設定されたものではない場合がある
ECC訂正	1ビットのECCエラーが検出され、修正された場合、ハードウェアによってセット
<b>マスク出来ない割込み (NMI)</b>	
ECC検出	2ビットのECCエラーが検出された場合、ハードウェアによってセット



プログラミングのアライメントエラーは、通常プログラムの操作を開始する前に完全なダブルワードが指定されていない場合、または高速プログラミング操作を開始する前に完全な行が記述されていない場合に発生します。

高速プログラミングシーケンス中にデータが時間内に書き込まれていない場合、高速プログラミング中のデータミスエラーが発生します。

シングルビットECCエラーが検出され修正されると、割込みをアサートできます。

ダブルビットECCエラーが検出されると、NMIがアサートされます。

## SRAMからのコード実行時の消費電力の最適化

- RUN／低電力RUN、SLEEP／低電力SLEEPの各モード時に、Flashへのクロック供給をゲートオフできる
  - Flashクロックは、リセットおよびクロック・コントローラ(RCC)で設定
  - Flashクロックはデフォルトで有効
- SLEEP／低電力SLEEPモード時のFlashメモリをパワーダウン・モードに設定できる
- RUN／低電力RUNモード時のFlashメモリをパワーダウン・モードに設定できる



Flashメモリからのコードを実行していない場合、Flashメモリ分の消費電力を下げるすることができます。

Flashクロックは、RUN／低電力RUNモード時にゲートオフすることができます-またSLEEP／低電力SLEEPモード時にも、Flashクロックをゲートオフすることができます。Flashクロックはリセットおよびクロックコントローラにより設定します。Flashクロックはデフォルトで有効です。

SLEEP／低電力SLEEPモード時のFlashメモリをパワーダウンモードに設定できます。

コードがSRAMから実行されているとき、RUN／低電力RUNモード時のFlashメモリもまたパワーダウンモードに設定できます。

クロックのゲーティングおよびFlashメモリをパワーダウンモードに設定することで、消費電力を大幅に低減できます。

モード	説明
RUN	有効 コードがSRAMから実行され、Flashメモリがパワーダウン・モードの場合、Flashクロックを無効にできる
SLEEP	有効 SLEEPモード時にFlashクロックを無効にできます。Flashメモリをパワーダウン・モードにすることができる
低電力RUN	有効 コードがSRAMから実行され、Flashメモリがパワーダウン・モードの場合、Flashクロックを無効にできる
低電力SLEEP	有効 低電力SLEEPモード時にFlashクロックを無効にできます。Flashメモリをパワーダウンモードにすることができる
STOP0/STOP1	Flashメモリのクロック・オフ ペリフェラル・レジスタの内容は保持され、Flashメモリは、パワーダウン・モードにすることができる
STANDBY	パワーダウン状態 Flashメモリ・インタフェースは、STANDBYモード終了後に再び初期化する必要がある
SHUTDOWN	パワーダウン状態 Flashメモリインタフェースは、SHUTDOWNモード終了後に再び初期化する必要がある



Flashメモリモジュールは、次の低電力機能をサポートします。

- クロック・ゲーティング
- Flashメモリのパワーダウンモード
- モジュール全体への電力ゲーティング:Flashメモリとコントローラ

RUN、SLEEP、低電力RUN、低電力SLEEPスリープモードではクロックのゲーティング、パワーダウンモードがサポートされています。SRAMからコードを実行する際に使用できます。

STOP0とSTOP1では、クロックはゲートされ、Flashメモリはパワーダウンモードに入ります。

SHUTDOWNモードでは、Flashメモリとコントローラの両方に対して、Flashメモリモジュールの電源がゲートされます。クロックをゲーティングし、Flashメモリをパワーダウンモードに設定すると、消費電力が大幅に削減されます。

# Flashメモリのパフォーマンス

29

3.36Coremark / MHz

- ARTアクセラレータにより、Flashメモリのパフォーマンスは周波数に対してほぼ線形的に変化
- 3.36CoreMark / MHz(シングルバンク、キャッシュオン、プリフェッチオン) => 571CoreMark @170MHz

CoreMark / MHz	ARTオン I-キャッシュオン D-キャッシュオン プリフェッチオン		ARTオン I-キャッシュオン D-キャッシュオン プリフェッチオフ		ARTオフ	
	デュアルバンク	シングルバンク	デュアルバンク	シングルバンク	デュアルバンク	シングルバンク
	3.26	3.36	3.23	3.32	1.05	1.47



ここでは、EEMBC CoreMarkベンチマークを実行しながら、170MHzでのコード実行パフォーマンスを比較します。コードがSRAM1にあるデータをCCM SRAMで実行されると、最大パフォーマンスに達します。170MHzでFlashメモリから実行すると、ARTアクセラレータが有効の場合CoreMarkの最大パフォーマンスに達し、170MHzで7つのウェイトを必要とするFlashアクセス時間によるパフォーマンスの低下はほとんどありません。



- このペリフェラルにリンクされている他のペリフェラルのトレーニングを参照してください。
  - システム設定コントローラ(SYSCFG)
  - リセットおよびクロック・コントローラ(RCC)
  - 電源コントローラ(PWR)
  - 割込み(NVIC)
  - メモリ保護



Flashメモリモジュールは、次の他のモジュールとの関係を持っています。

- システム設定コントローラ(SYSCFG)
- リセットおよびクロックコントローラ(RCC)
- 電源コントローラ(PWR)
- 割込み(NVIC)
- メモリ保護

- 詳しくは、以下の関連資料を参照してください。
  - AN2606: STM32 microcontroller system memory boot mode – Application note



life.augmented

詳しくは、STM32マイクロコントローラのシステムメモリブートモードに関するアプリケーションノート、AN2606を参照してください。