第2章 プログラムの性能や効率向上に役立つ

Armv8-Mアーキテクチャ徹底解説

金丸 敦礼

表1 Armv8-Mアーキテクチャを構成する各種要素

#	各種要素	概 要
1.	動作モードと特権レベル	CPUが持つ2つの動作モードと2つの特権レベル
2.	汎用レジスタ	データやアドレスを格納する32ビット幅の汎用レジスタ
3.	特殊レジスタ	CPUの設定レジスタやステータス・レジスタなどの特殊レジスタ
4.	FPUとFPU用レジスタ	浮動小数点演算を行うFPU(Floating Point Unit)とそのレジスタ
5.	セキュリティ・ステート	Armv8-Mの新機能であるセキュリティ拡張(TrustZone)を実現するために実装されている2つのセキュリティ・ステート
6.	例外モデル	CPUが持つ例外タイプとその優先度,ベクタ・テーブル,スタック・フレーム,不要なスタック・フレームの生成をスキップするテールチェイニングとレイトアライバル,割り込みコントローラであるNVIC(Nested Vector Interrupt Controller)
7.	メモリ・モデル	CPUが持つ32ビット(4Gバイト)のメモリ・マップ,各メモリ領域が持つ3種類のメモリ属性,CPUがサポートしているデータ・タイプ,メモリ・エンディアン,指定したメモリ領域へのアクセスを制御するMPU(Memory Protection Unit)とSAU(Security Attribution Unit)
8.	電力管理	CPUが持つ省電力モード
9.	システム・タイマ	OSへの定期的な割り込み生成などに用いられるシステム・タイマ
10.	その他の機能	ディジタル信号処理向けの演算に特化したDSP(Digital Signal Processing),コプロセッサやアクセラレータと連携するためのコプロセッサ・サポート,独自のカスタム命令を追加できるカスタム・データ・パス拡張

本章では,**表1**に挙げた,Armv8-Mアーキテクチャを構成する各種要素の仕様について説明します.

ソフトウェア開発者は,これらのArmv8-Mアーキテクチャの仕様を正確に理解することで,プログラムの動作に問題が生じる可能性を低くできます.また,性能や効率が向上する可能性もあります.

これらの要素については,特に注釈がない限りセキュリティ拡張(TrustZone)が搭載されている場合の仕様を説明します.

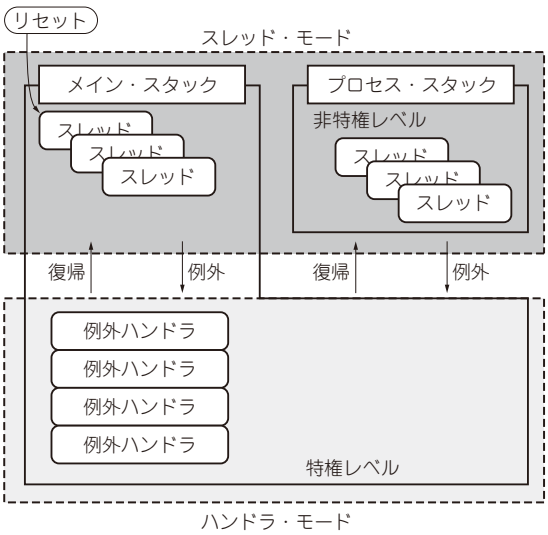

図1 Armv8-Mの動作モード

1. 動作モードと特権レベル

● 動作モード間の遷移と特権・非特権レベルの分離

Armv8-Mには,スレッド・モードとハンドラ・モードの2種類の動作モード(Processor modes)が存在します.通常のソフトウェアが動作するモードがスレッド・モードで,例外処理などが発生したときハンドラ・モードに入ります.また,特定のシステム・リソースへのアクセス権を持っている特権レベル(Privileged)と,それを持たない非特権レベル(Unprivileged)が設定されています(**図1**).セキュリティ拡張(TrustZone)が搭載されている場合,後述する2種類のセキュリティ・ステートごとにこれらの