第4部

第4章 FreeRTOSとAzure RTOSを動かす

Cortex-M33上で体験するRTOS

宮田 賢一

Cortex-M33のTrustZone

Cortex-M33の特徴の1つであるTrustZoneの実力の一端を，実験を通して体験してみます．

● Cortex-M33の目玉機能TrustZone

大規模化・複雑化する組み込み機器の中心として動作するマイコンでは，システムが安定して動作するためのセキュリティ確保が必要となっています．そのような背景のなかArmは，新しいプロセッサ・アーキテクチャArmv8-Mを2015年に発表しました．そしてArmv8-Mを初めて実装したプロセッサ・コアがCortex-M33およびCortex-M23です．

Armv8-Mの最大の特徴はTrustZoneと呼ぶセキュリティ機構をアーキテクチャの中に組み込んだことです．なおCortex-A系のプロセッサ・アーキテクチャであるArmv8-AにもTrustZoneの機能が組み込まれていますが，Armv8-Mのものとは異なるものです．以降，Armv8-M向けのTrustZoneを単にTrustZoneと呼ぶことにします．

● TrustZoneによるセキュリティ

TrustZoneを備えたプロセッサに，命令の実行状態としてセキュア（Secure）と非セキュア（Non Secure）という2つのセキュリティ状態が新たに加わりました．またArmv8-M以前からある動作モード（ハンドラ・モード，スレッド・モード）と特権実行レベル（特権レベル，非特権レベル）も，引き続きArmv8-Mにも存在します．

▶動作モード

プロセッサがアプリケーション・コードを実行しているのか，割り込み発生時のハンドラを実行しているのかを区別するのが動作モードです．スレッド・モードとハンドラ・モードがあります．

スレッド・モードは，アプリケーション・コードを実行している状態で，プロセッサは特権レベルまたは非特権レベルのいずれかで動作します．一方，ハンドラ・モードでは常に特権レベルとなります．

▶特権実行レベル

プログラムからアクセスできる範囲を規定するのが特権実行レベルです．特権レベルと非特権レベルがあります．

プロセッサが特権レベルにあるとき，プログラムは全ての命令を実行でき，全てのリソースにアクセスできます．それに対して非特権レベルでは，プログラムはプロセッサの状態を変更する命令へのアクセスが制限されます．例えばシステム・タイマや特定のレジスタ，特権アクセスしか許されていないメモリや周辺機器へのアクセスはできません．

▶セキュリティ状態

ペリフェラルやメモリ領域をセキュアと非セキュアに分割し，それぞれのどちらにアクセスできるかを制御するのがセキュリティ状態です．セキュア状態と非セキュア状態があります．

プロセッサがセキュア状態にある場合，プロセッサは全てのリソースと全てのメモリ領域にアクセスできます．一方，非セキュア状態にある場合は，あらかじめアクセスを許可するよう定義されたリソースにのみアクセスできます．これにより，例えばマイコンが持つ特定のGPIOピンや機能ブロックのアクセスを制限し，ハードウェアを無闇に制御されるのを防ぎます．

● TrustZoneの状態遷移

動作モード，特権実行レベル，セキュリティ状態の関係と状態遷移を**図1**に示します．

①初期状態

プロセッサがリセットされると，まずセキュア状態となり，特権モードを持つスレッド・モードとして命令の実行を開始します．

②スレッド・モードとハンドラ・モードの遷移

スレッド・モードで割り込みが発生するとハンドラ・モードに遷移します．その後割り込みハンドラの実行を終了すると再びスレッド・モードに復帰します．

③特権実行レベルの変更

特権実行レベルを変更するには特別なレジスタに規