第2章 Cortex-M0＋の後継者

ちょっとした用途向き Cortex-M23入門

中森 章

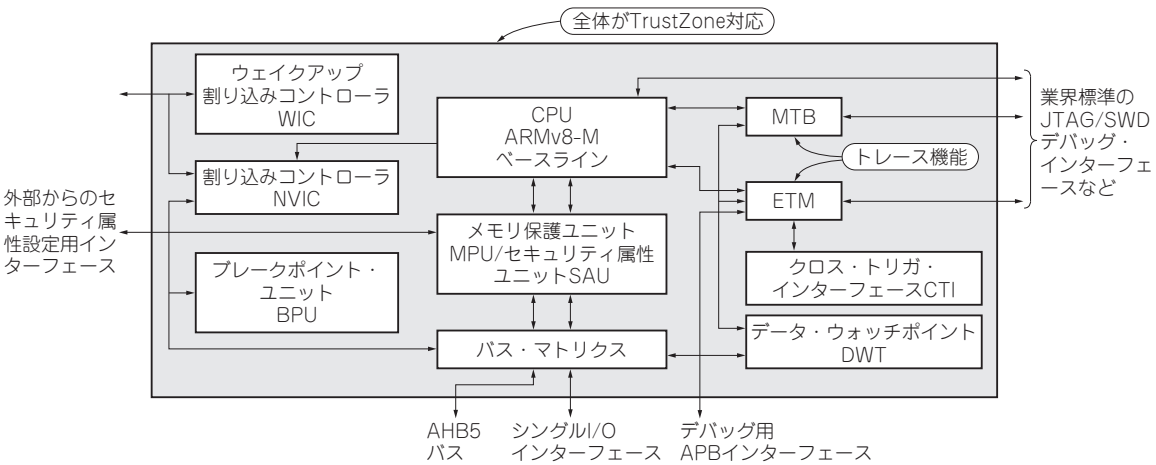

図1　ちょっとした用途向きCortex-M0＋の後継者！ Cortex-M23の回路構成

以降で，ARMv8-Mアーキテクチャを実装する新しいCortex-M23とCortex-M33の特徴を示していきます．まず本稿ではCortex-M23を紹介します．

とてもシンプルな回路構成

まずCortex-M23の特徴を一言でいうと，TrustZoneを備えた，小さくてエネルギー効率に優れるプロセッサといえます．命令セットはARMv8-MのBaseline（サブセット）で，ARMによると「効率の良いセキュリティが要求され，かつ使用制限の多い（constrained）組み込みアプリケーションに最適」とのことです．

図1にCortex-M23の回路ブロックを示します．「APBインターフェース」は，ETM（Embedded Trace Macrocell）としかつがなっていないので，ETMの設定を行うためのデバッグ・インターフェースだと思われます．

以下にCortex-M23の特徴的な5つの項目について説明します．

特徴1：セキュリティ基本機能 TrustZone

● IoTやセキュリティ用途などに使える

Cortex-M23は，ハードウェアにより，ソフトウェアを「信頼された世界（トラステッド）＝セキュアな世界」と「信頼されない世界（ノン・トラステッド）＝非セキュアな世界」に分離します．

従来は，これを実現するために2つのプロセッサが必要でしたが，TrustZoneを使えば1つのプロセッサ上に2種類のセキュリティ属性（トラステッドとノン・トラステッド）を使って世界を構築できます．

Cortex-M23は，1つのプロセッサで，デバイス認識管理，機密性の高いファームウェアの保護，アプリケーション・ソフトウェアの認証，セキュリティ・ブートなどに要求される諸々のセキュリティを兼ね備えた用途に使うことが可能になるのです．

ちなみに，TrustZoneはオプション機能です．TrustZoneを持たないCortex-M23は，デバッグ機能などが強化された，高性能で低消費電力なCortex-M0+（相当品）として使用できます．