第4章 IoT時代の不安解消! セキュリティ対応TrustZoneのためにゴッソリ作り替え

超最新! マイコン用ARMv8-Mアーキテクチャの研究

中森 章

特徴

● 基本はセキュリティ機能TrustZoneを追加しただけ

ARM社は2015年11月10日，マイコン向け最新アーキテクチャARMv8-Mを発表しました(ARM TechCon 2015, 米国カリフォルニア州サンタクララ)．Cortex-Aプロセッサ向けARMv8-AやCortex-Rプロセッサ向けARMv8-Rはすでに発表されていたので，ARMv8-Mもそろそろと筆者は推測していました．しかし，基本的に追加点が，従来プロセッサ向けに提供されていたセキュリティ機能TrustZoneをマイコンにも対応しただけということに驚きました．TrustZoneに応じて各種機能の強化が行われていますが，信頼性を追加するだけでこんなに改変が必要なのかという感じです．

ARMv8-Mの「売り」はとにかくTrustZoneです．幾つかの命令拡張が行われていますが，それらのほとんどはTrustZoneの実現を前提としたもののようです．Cortex-A(ARMv7-A/ARMv8-A)のTrustZoneは，構想が大き過ぎて，聞いても「モヤモヤ」したものが残っていました．ハイパーバイザ不要のARMv8-MのTrustZoneは，感覚的に理解のしやすいものになっています．

本章では，ARMv8-Mの特徴とTrustZone，ARMv8-Mで強化された特徴のうち幾つかを説明していきます．

● 拡張された命令

最初に，ARMv8-Mとその前身である，ARMv6-M，ARMv7-Mとの関係を**図1**に示します．なお，ARMv8といっても64ビット・アーキテクチャではなく，ARMv8-Rと同様に，32ビット・アーキテクチャを維持しています．

ARMv8-Mアーキテクチャはさまざまな応用分野に対応できるように2種類のプロファイル(実装形態)をもっています．それが，ベースライン(基本線)とメインライン(本線)です．それぞれには**表1**に示すような特徴があります．

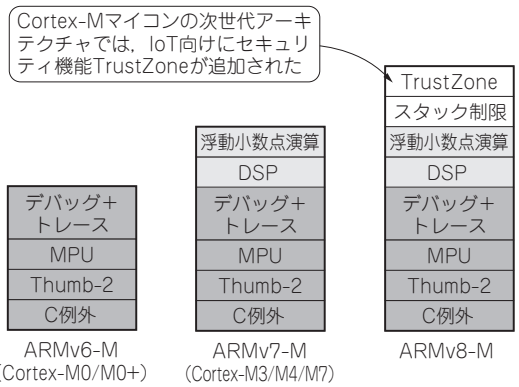

図1[3] IoT用途向けにセキュリティ機能を追加した新しいマイコン用アーキテクチャARMv8-M

ARMv8-Mの目玉! セキュリティ機能TrustZone

● セキュリティ状態の定義

ARMv8-MのTrustZoneはCortex-Mプロセッサの実行状態に「セキュア」と「非セキュア」という新しい状態を追加して実現します．これらの状態は，従来の「スレッド」，「ハンドラ」状態と直交します．つまり，

- セキュア・ハンドラ
- セキュア・スレッド
- 非セキュア・ハンドラ
- 非セキュア・スレッド

の4状態が定義されます．

スレッド状態には正確には「特権」と「非特権」の2種類があるので6状態です．ハンドラ状態は特権のみです．

● 基本機能…非セキュア状態からセキュア命令は実行できない

セキュア状態からはセキュアな情報と非セキュアな情報の両方をアクセスできますが，非セキュア状態からは非セキュアな情報しかアクセスできません．この