第3部

第3章 LPC55Sxxのセキュリティ機能

TrustZoneに対応したNXPマイコンのセキュリティ

浜野 正博

表1 LPC5500シリーズの一覧
LPC55の次に「S」が付く型番がセキュリティ対応（例：LPC55S16）で，「S」が付かない型番がセキュリティ非対応（例：LPC5516）

ファミリ	CPUコア	特　徴	パッケージ
LPC55（S）0x	Arm Cortex-M33	低価格	HTQFP64, HVQFN48
LPC55（S）1x	Arm Cortex-M33	USBおよびCAN-FD搭載	HLQFP100, VFBGA98, HTQFP64
LPC55（S）2x	Arm Cortex-M33（TrustZone非搭載）	USB搭載，大容量メモリ	HLQFP100, VFBGA98, HTQFP64
LPC55（S）3x	Arm Cortex-M33	高度なアナログ機能	HLQFP100, HTQFP64
LPC55S6x	Arm Cortex-M33	高効率，デュアルコア	HLQFP100, VFBGA98, HTQFP64

本章では，TrustZoneに対応した，NXPセミコンダクターズのCortex-M33マイコン「LPC55Sxx」シリーズのTrustZoneとの連携や暗号化アクセラレータに関するセキュリティ機能について解説します．

Cortex-M33を初めて採用したLPC5500シリーズ

● LPC5500シリーズは全てCortex-M33

LPC55S69は，2018年に初めてArm Cortex-M33およびTrustZone技術を採用したマイコンです．最高150MHz動作のCortex-M33コアを2個搭載し，32μA/MHzの電力効率で動作します．TrustZoneに加え，セキュア・ブートやセキュア・デバッグ，鍵の管理，暗号化アクセラレータなど，さまざまなセキュリティ機能が搭載されています．

LPC5500シリーズは5つのファミリを持つ汎用マイコンです．全ての製品がCortex-M33コアを搭載していますが，LPC55（S）2xファミリのみTrustZone非搭載です（**表1**）．これらは全て共通のアーキテクチャで設計されており，ソフトウェア互換かつピン互換で利用できます．

LPC55Sxxファミリはさまざまな攻撃から組み込み機器を守れるよう，セキュリティ機能をサポートします．LPC55Sxxのセキュリティ・サブシステムでサポートされるセキュリティ機能には，次のものがあります．

- TrustZone（LPC55S2x除く）
- SRAM PUF（Physically Unclonable Function：物理的に複製不可の機能）
- デバッグ認証（Debug Auth.）
- リアルタイム暗号化/復号（PRINCE）
- 乱数発生器（RNG）
- セキュア・ブート（Secure Boot）
- SHA-2，AES-256
- フラッシュ保護領域（PFR）

また，**図1**にLPC55S3xの機能ブロック図を示します．

LPC55Sxxのセキュリティ機能

● LPC55Sxxのセキュリティ・ブロック

LPC55SxxシリーズはTrustZoneによるTrusted Execution Environment（TEE）のサポートと同時に，ブート時やランタイム時に要求される各種ハードウェア・セキュリティ機能を包括的にサポートすることを基本設計としています（**図2**）．

LPC55Sxxのセキュリティは，TrustZoneとセキュリティ・ハードウェアを組み合わせたものです．TrustZoneによるセキュア領域とノンセキュア領域のより完全な分離をサポートするため，セキュリティ属性ユニット（Security Attribution Unit：SAU）に加え，セキュア・バス・コントローラ，セキュアDMA，セキュアGPIOをハードウェアで実装します．このハードウェアによる分離は，セキュアなリソースとノンセキュアなリソースへのアクセス・パスを分けることで，信頼できる安全な実行環境を実現します．

● ROMファームウェア

LPC55Sxxの内蔵ROMには書き換えできないブート・コードが書き込まれており，認証処理や復号，セキュアなプログラム・フローやセキュリティの状態設定を行います．Cortex-M33コアはリセット後に内蔵ROMからコード実行を開始します．このROMによ