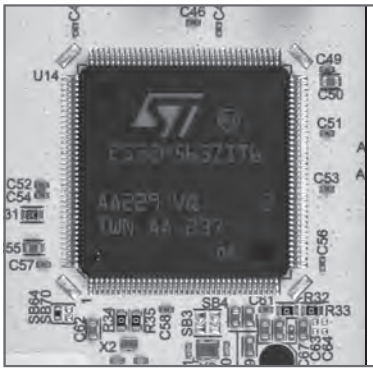

第4章 これからのキー・テクノロジ…TrustZone &セキュア・プログラミング入門

高性能Cortex－M33実力研究！ GPIOハッキング阻止実験

宮田 賢一 Kenichi Miyata

本章では，Cortex-M33のセキュリティ機能であるTrustZoneを実際に動かしてみます．実験では，STM32H563ZIを搭載するNUCLEO-H563ZIを使用し，オンボードのLEDやスイッチをセキュリティで保護する手法を紹介します(**写真1**)．

マイコンのセキュリティの基本

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不可欠となっています．セキュリティが弱いとクラッキングの脅威にさらされる危険性を常に抱えていることになり，情報の漏洩やシステム全体のダウンといった問題を発生させてしまう恐れがあります．

マイコンをセキュリティ的な脅威から保護する技術には，以下のようなものがあります．

● 通信路暗号化

マイコンと外部ネットワークとの間の通信路に流れるデータを暗号化し，第三者が通信傍受することによるデータ漏洩を防止します．

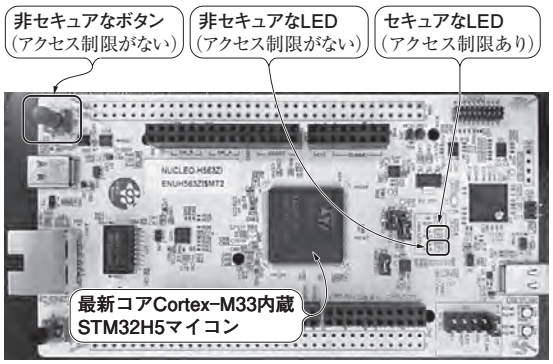

写真1　本稿ではArmのセキュリティ機能TrustZoneに対応した最新コアCortex-M33によるGPIOのセキュリティ保護実験を行う
アクセス権限のない非セキュアなプログラムからはセキュア設定したLEDをチカチカできない

● 格納データ暗号化

マイコンに保持するデータを暗号化して，データを取り出すには秘密の鍵情報を要求することで，マイコンが盗難されときのデータ漏洩を防止します．

● 分離/隔離

実行するソフトウェアやハードウェアを複数の領域に分離/隔離し，ある領域が改ざんされて不正な挙動をしたとしても，ほかの領域に影響を与えないように制御して，不正動作の影響を最小限にします．

本章で解説するTrustZoneは，このうちの隔離に該当する技術です．

● タンパリング検知

システムを不正に改ざんする行為(タンパリング)を検知し，システムを保護する技術です．マイコンへの侵入を検知すると，特別な割り込みを発生させて実行中のプログラムに通知したり，メモリ内容を消去したりといった対応を実施します．

Armのセキュリティ機能 TrustZone

Arm Cortex-M33のTrustZone技術は，メモリとペリフェラルを保護します．これらの保護は，信頼できるセキュアなコードと，信頼できない非セキュアなコードのそれぞれの実行環境を物理的に分離することにより行われます．以下にTrustZoneの特徴を挙げます．

● メモリ保護

TrustZoneは，メモリ領域をセキュアと非セキュアに分離します．セキュアなメモリ領域にはセキュア・コードとデータが配置され，これらは非セキュア・コードからアクセスできません．これにより，重要な情報が悪意の有無にかかわらず改ざんされるのを防ぎます．