IoT時代はデータ漏えいの危険がいっぱい…
ワンチップCortex-Mでここまで!

マイコン内蔵最新セキュリティ機能の研究

第4回　侵略行為に対する保護機能

中森 章

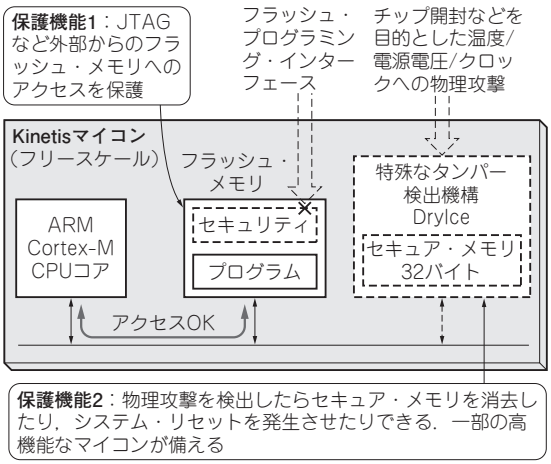

図1　プログラムへの侵略行為に対するマイコンの保護機能のイメージ

Cortex-M搭載Kinetisマイコンが備える機能の例．DryIceの代わりにリアルタイム・クロック・モジュールRTCに同様の特殊なタンパー検出機構を備えているタイプもある．DryIceについては，対応マイコンのリファレンス・マニュアルRev3からNDA事項になっている

MCU内部の情報をチップ開封などにより盗み見る侵略行為のことをタンパーといいます．

組み込み制御向けのマイコン（MCU）の多くは，タンパーを検出すると内蔵している秘密情報を消去して無意味なものにしてしまう機能を備えています．本連載のターゲットCortex-M搭載Kinetisマイコン（フリースケール）もこの例にもれません．

Kinetisでは，もっと概念を拡張してクロック，電源，温度の異常などのMCUが正常動作できなくなるような状況もタンパーと呼んでいるようです．チップ内情報を取り出すための開封作業などの侵略行為の副作用でクロック，電源，温度に変化があった場合の対処だと思われます．

Kinetisの耐タンパー機能には，主に**図1**に示す二つがあります．

- フラッシュ・メモリのセキュリティ
- 特殊なタンパー検出機構DryIce

DryIceについては，対応マイコンKinetis K70のリファレンス・マニュアルRev2に記載されていたのですが，Rev3からはNDA事項となりましたので，詳細な解説は差し控えます．リファレンス・マニュアル以外の文献などで記載されている一般的な記述から，最低限の概要について紹介したいと思います．

保護機能1：フラッシュ・メモリのセキュリティ

フラッシュ・メモリのセキュリティは耐タンパー機能の一種ですが，他の耐タンパー機能とは少ししくみが異なります．基本的にはリセット後にフラッシュ・メモリに書き込まれているアプリケーション・プログラムからのビット・イメージへのアクセスを制限します．フラッシュ・メモリの保護機能とよく似ています．

通常のフラッシュ・メモリの保護機能は，正式な（安全が確定している）アクセスを行っている場合にプログラムの予期しない暴走を避けるためのものです．一方，セキュリティ機能は外部からの予期しないアクセスからフラッシュ・メモリへのアクセスを保護します．

フラッシュ・メモリに格納されるアプリケーション・プログラムはIP（Intellectual Property：知的所有物）の宝庫ですので，他人（外部からの侵略）に中をのぞかれるのは好ましいことではありません．

こういったセキュリティ機能はフラッシュ・メモリを内蔵するデバイスには必須ですから，全Kinetisマイコンに搭載されています．

● セキュリティ制御用FSECレジスタ

フラッシュ・セキュリティにかかわる情報が格納されている0x400番地から0x40F番地は，フラッシュ・メモリ・コンフィグレーション・フィールドと呼ばれます（**表1**）．

KinetisにはFSEC（Flash Security）レジスタが用意されており，フラッシュ・メモリのセキュリティを制御します．**表2**にFSECレジスタのビット割り当てを示します．

FSECレジスタのSECビットがセットされている場合は，フラッシュ・メモリに対するアクセスやコマン

第1回　通信の認証などによく使う/暗号高速化ユニットCAU（2015年3月号）
第2回　暗号化通信に欠かせない！乱数生成器RNG（2015年4月号）
第3回　エラー検出によく使うCRC（2015年5月号）