## 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1回　通信の認証などによく使う！暗号高速化ユニットCAU

中森 章

表1　連載で紹介するKinetisマイコン（フリースケール）が備えるセキュリティ機能

| シリーズ | 暗号化機能 | | | フラッシュ・メモリのセキュリティ（耐タンパーなど） | その他セキュリティ機能 | |
|---|---|---|---|---|---|---|
| | 暗号高速化ユニットCAU | 乱数生成器RNG | CRC | | ユニークID | メモリ保護ユニット（MPU） |
| K | K11，K21，K52，K53，K6*x*，K70 | | ○ | ○ | 128ビット | ≧100MHz |
| L | — | — | — | ○ | 80ビット | — |
| M | — | — | ○ | ○ | 128ビット | ○ |
| W | — | KW2*x* | ○ | ○ | KW2x：128ビット<br>Kw01：80ビット | — |
| E | — | — | ○ | ○ | 64ビット | — |
| V | — | — | ○ | ○ | KV1：48ビット<br>KV3/KV4：96ビット | — |

さまざまな装置をインターネット接続するIoT（Internet of Things）時代になると，データベースを管理するクラウド・サーバだけでなく，サーバと通信を行う末端のセンサ機器などにもセキュリティ機能が要求されます．セキュリティ機能を内蔵したワンチップ・マイコンも数多くあります．

本稿では，多くのセキュリティ機能を備え，LAN通信搭載mbed互換ボードが4000円程度で入手できて実験に使いやすい，ARM Cortex-M内蔵Kinetis（フリースケール）を例に，ワンチップ・マイコンの最新セキュリティ機能を紹介していきます．

## マイコンの主なセキュリティ機能

一口にセキュリティといってもいろいろありますが，本稿ではKinetisマイコンに内蔵された暗号化支援機能と耐タンパー機能を中心に紹介していきます．

**表1**にKinetisシリーズのセキュリティ機能を示します．この中でMPU（Memory Protection Unit）はCPUの機能とは別物で，システム・バス（クロスバー・スイッチ）に付加されています．

**▶その1：認証などに使われる暗号化支援機能**

通信の認証などに使われる暗号化の支援機能には，以下のものがあります．

- 暗号高速化ユニットCAU（Cryptographic acceleration unit）
- 乱数生成器RNG（Random number generator）
- 巡回冗長検査回路CRC（Cyclic Redundancy Check）

**▶その2：直接攻撃対策…耐タンパー機能**

タンパーとはMCU内部の情報をチップ開封などによって盗み見る侵略行為のことです．耐タンパー機能は次のものがあります．

- タンパー検出モジュールTDM（Tamper Detection Module）

TDMはKinetisではDryIce（ドライアイス）とも呼ばれます．これは熱（侵害）を加えると（解析したい機能が）蒸発して消えて無くなってしまうという意味に由来しているのだと思われます．

**▶公開可能な範囲で解説していきます**

ちなみに，セキュリティ機能の解説には注意が必要です．たとえば，耐タンパー機能はKinetis K6*x*シリーズのリファレンス・マニュアルではNDA事項になっていますが，Kinetis K70シリーズのリファレンス・マニュアルでは公開機能になっています．フリースケールの担当者もNDAが必要なのはCAUの機能であり，タンパー検出は特に秘密ではないといっていました．連載では，このあたりも気をつけながら解説していきたいと思います．