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5回（最終回） イーサ/USB/SD/デバッグ・ポート…外部からの盗み見を防ぐメモリ保護ユニットMPU

中森 章

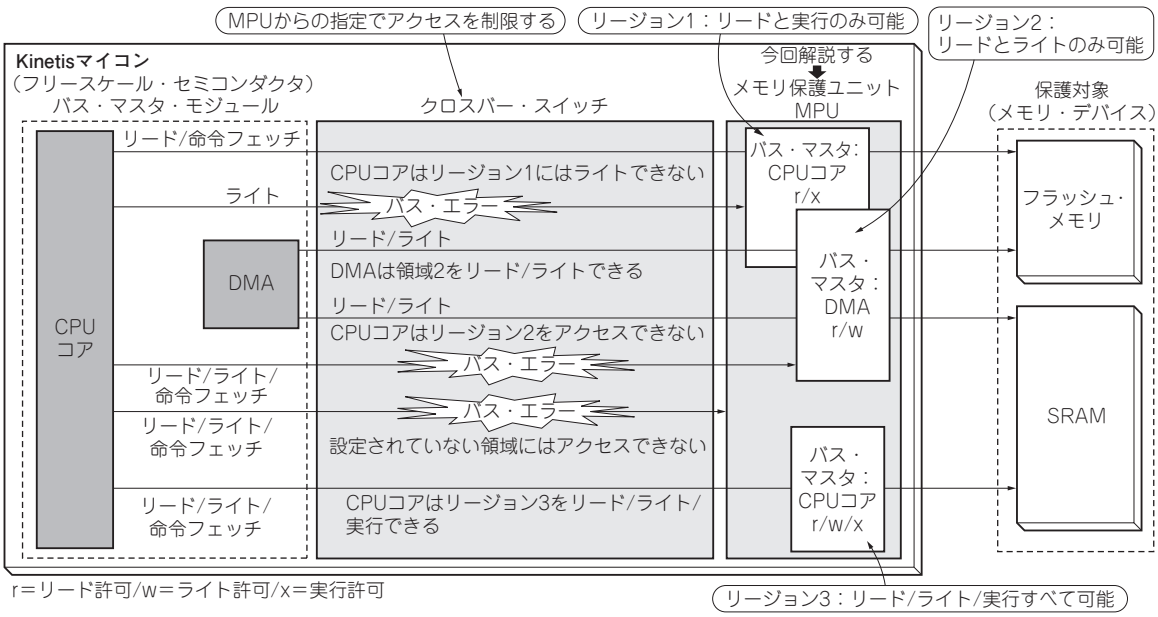

図1　メモリへのアクセスを制限! 内容の盗み見を防ぐ Memory Protection Unit（MPU）
メモリ保護はクロスバー・スイッチでメモリへのアクセスを制限することによって行う

本稿ではCortex-Mマイコン Kinetis（フリースケール）の周辺機能として実装されているメモリ保護ユニットMPU（Memory Protection Unit）について解説します.

Cortex-Mシリーズの CPUコアにもMPUが内蔵されていますが，本稿で説明するMPUとは別物です．しかし，提供している機能は，メモリ保護という観点では，同様です．しかし，CPU内蔵のMPUは，CPUというバス・マスタからのアクセス保護しか実現できません.

Kinetisでは周辺機能としてMPUを実装することで，CPUからのメモリ保護のほかに，CPU以外のバス・マスタ，すなわちイーサネットやDMAからのメモリ保護を実現します.

● デバッグ・ポートやSD，イーサネットなど外部からの侵略行為にも有効!

Kinetisが備えるMPUの保護対象は，フラッシュ・メモリやSRAM，あるいはFlexBus（メモリに接続することを仮定）などのメモリ領域です．外部からの侵略行為に対してメモリ内容を保護する意味があります．これは耐タンパ機能そのものです.

これらのメモリを盗み見する場合，侵略者はデバッグ・ポートやイーサネットなどのバス・マスタを経由して侵入することが考えられます．Kinetisの提供するMPUにはこれらのバス・マスタからメモリ領域を保護する機能を第一に考えられています．これはCPUコアのみを対象としているCortex-Mシリーズ CPU内蔵のMPU機能とは一線を画する機能です.

メモリ保護ユニット MPU

● メモリ保護方法…クロスバー・スイッチでアクセスを制限

MPUはMCUのクロスバー・スイッチに対して，

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）