敵対的な OS からソフトウェアを保護するプロセッサアーキテクチャの実装

春木洋美　橋本幹生（東芝）

近年、コンピュータソフトウェア、及び、コンピュータシステムで扱われる著作物に対する著作権侵害が問題となっている。とりわけ、利用者端末のOS がマルチベンダ・マルチタスクのオープンシステムであるとき、この問題は深刻となる。これを解決するため、我々は、ソフトウェアベンダの立場からは利用者端末の OS が信頼できないことを前提として、マルチベンダ・マルチタスクのシステムにおいて、アプリケーションプログラムを解析や改ざん から守ることのできるプロセッサハードウェアアーキテクチャ L-MSP（License-controlling Multiparty Secure Processor）を提案した[1]。L-MSP では、マルチタスク OS に必要な資源管理機能と、アプリケーション保護のための秘密保護機能とを分離することにより、信頼できないOS を持つ端末においても安全なライセンス管理を実現するソフトウェア実装の枠組みを提供している。

我々は、L-MSP の機能検証、及び、評価のために、MeP(Media Embedded Processor)[2]に改造を施して L-MSP で提案した保護機能を実現するハードウェアを設計し、FPGA 上に実装した。このハードウェアは、プログラム、データ、コンテキストの保護を実現し、共通鍵暗号 に AES、公開鍵暗号に RSA を内蔵している。同時に、μITRON をベースとしたオープンソースソフトウェア TOPPERS/JSP カーネル[3]に対して、L-MSP で提案した保護メカニズムをサポートするための改造を施した。今回、これらの改造を行った CPU、及び、OS を用いて、個々に暗号化された複数のプログラムがμITRON 上のマルチタスク環境で動作するデモを展示する。 本デモシステムでは、複数の平文／暗号プログラムの共存が可能であり、かつ、プログラムを保護するための秘密を OS に埋め込む必要がなく、プロセッサ内部にある秘密鍵によってプログラムを保護する。図１のように、FPGA の外部信号とデモ用に取り出した内部信号を対比することによって、内部メカニズムと保護メカニズムの動作を可視化できる。

[1] 橋本、春木、“敵対的なOS からソフトウェアを保護するプロセッサアーキテクチャ”、コンピュータシステムシンポジウム 2003、2003

[2] MeP、http://www.mepcore.com/

[3]TOPPERS/JSP, http://www.toppers.jp/

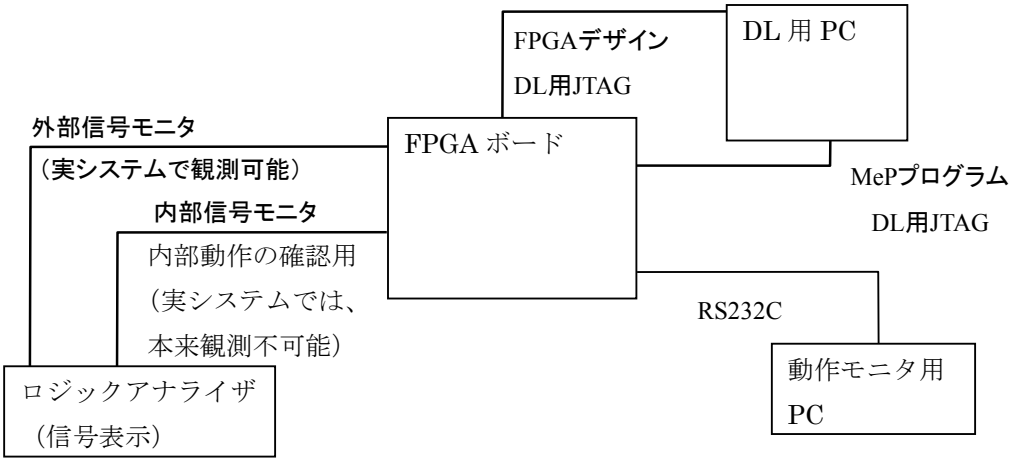

図 1　L-MSP デモシステム構成