

IPv6に対応した組み込みシステム用IPSecモジュールの開発

Development of an IPSec Module for the IPv6 Network of Embedded Systems

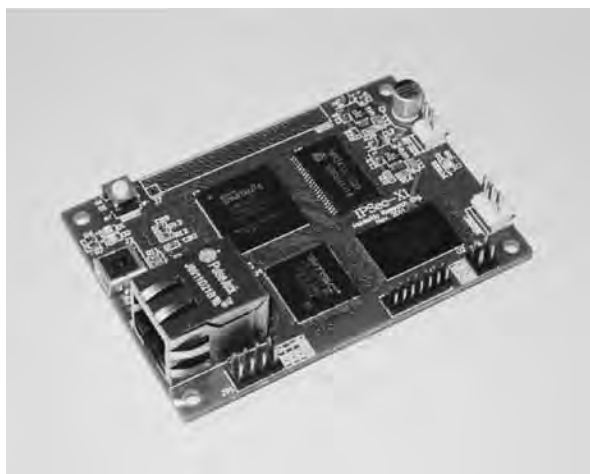
ものづくり支援センター 堤 大祐
情報システム部 大村 功

■研究の背景

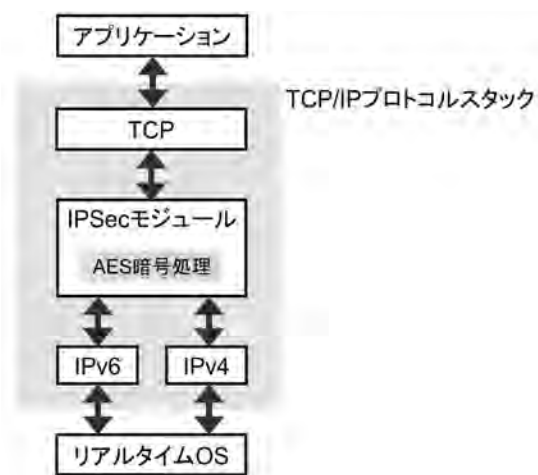
組み込みシステムのネットワーク環境はIPv4アドレスの枯渇問題によるIPv6への移行や、暗号化などによる通信の保護が必要となっています。本研究では通信の安全性を確保するためのセキュリティ・プロトコルであるIP Security Protocol (IPSec) をIPv6およびAdvanced Encryption Standard (AES) に対応させたIPSecモジュールの開発に取り組みました。

■研究の要点

1. ソフトウェアによるAES暗号処理機能の開発
2. Field Programmable Gate Array (FPGA) を用いたハードウェアによるAES暗号処理機能の開発
3. IPv6/IPv4に対して同時通信できるデュアルスタック・サポート対応機能の開発
4. 小型ボードの開発と、上記機能の動作検証



開発した小型ボード



IPSecモジュールのブロック図

■研究の成果

1. リアルタイムOS (TOPPERS/ASPカーネル) と苫小牧高専が開発したTCP/IPプロトコルスタック (TINET) 上で動作するソフトウェアによるAES暗号処理機能を開発しました。
2. AES処理の一部をハードウェア・モジュール化し、独自仕様の小型CPUで制御したハードウェアによるAES暗号処理機能を開発しました。
3. IPv6/IPv4のどちらのプロトコルにおいても動作するAES暗号処理機能を実現しました。
4. 小型ボードを開発し、IPv6/IPv4のプロトコルにおけるIPSec通信の動作検証を行いました。

※本研究の一部は総務省の戦略的情報通信研究開発推進制度 (SCOPE) の委託研究に基づく結果による。

苫小牧工業高等専門学校 北海道苫小牧市字錦岡443番地 Tel. 0144-67-8937