ご購入はこちら

IoT時代の必読！ 押さえておこう！技術仕様の基本

インターネット・プロトコル教科書

第5回 IoT時代！センサ・ネットワークのセキュリティ・プロトコルSPINS

笠野 英松

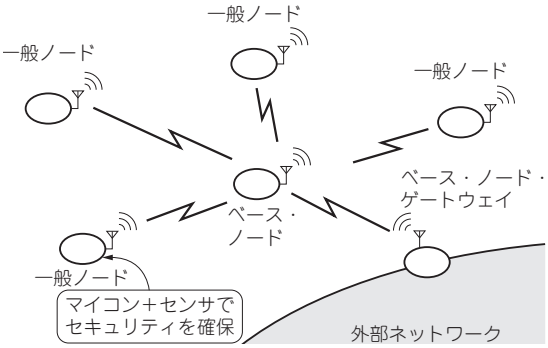

図1　センサ・ネットワークの一般的な構成

モノのインターネットIoT（Internet of Things）や，センサ・ネットワークなどの機械間ネットワークM2M（Machine to Machine）では，その中を流れる情報のセキュリティ保持が最も重要です．しかし，このセキュリティ保持は，従来のセキュリティのしくみでは対応しきれません．そのため，新しい考え方が提案されています．

今回は，センサ・ネットワーク向けに研究されているしくみSPINSを紹介します．同じような標準化であるIEEE 802.15.4/ZigBeeなどはここでは割愛します．

センサ・ネットワークの心配ごと

M2Mの代表的なものが（ワイヤレス）センサ・ネットワークです（**図1**）．マルチホップのワイヤレス通信を使うセンサ・ネットワークではセキュリティが最重要な課題になっています．

● 低消費電力＆低計算能力なのにセキュリティを確保しないといけない

センサ・ネットワークで使われる，センサ・デバイスの電力および計算能力は一般に低めです．それらを使ってセキュリティを確保するにはそれなりの工夫が必要です．

センサ・ネットワークはかなり前から広がっていますが，セキュリティはあまり強調されていませんでした．それが，時代の流れでセンサ・ネットワークでもセキュリティが主要な関心事になってきました．

しかし，計算能力やメモリ，通信帯域，消費電力などの制約がある場合，アドホック（直接接続）/マルチホップのワイヤレス通信をサポートしつつ，セキュリティを確保するのは簡単ではありません．

デスクトップ環境であればこれらについては深く考慮する必要はありませんが，リソースが制限された環境では，これらが死活的な条件です．

● セキュリティ・プロトコルSSL/TLSを拡張しないといけない

IoTネットワークの標準化はIEEE 802.15.4（下位層）やZigBee（中位層）などで行われていますが，セキュリティについてはIETFのTCP/IPのTLS階層がベースです．従来は，アプリケーション・レベルではSSL（Secure Sockets Layer）/TLS（Transport Layer Security）を使用したTCPベースのものでした．すべての「モノ」に対応するためにはUDPへの対応やSSL/TLSの拡張が必要です．実際にこれらはRFC化されています．

マイコン向けの研究！セキュリティ・プロトコルSPINS

今回紹介するのは，低コスト，低消費電力でセキュリティを確保できるSPINS（Security Protocols For Sensor Networks）です[注1]．SPINSは，この条件を重視して進められた研究です．

■ 想定している構成

● ハードウェア

SPINSが想定するハードウェア構成は，外部ネッ

注1：SPINS：Security Protocols For Sensor Networks．米国郵政公社USPS，米国国防高等研究計画局DARPA，米国国立科学財団NSFからのサポートをもとにした，UCB（University of California, Berkeley）/SmartDustプログラムのAdrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygarによるセンサ・ネットワークのセキュリティ研究．

第1回　ネットを使うときの隠れ常識！技術文書RFC（2015年9月号）
第2回　考えとかないとマズい！ IPv6プロトコルの全体像（2015年10月号）
第3回　IPv6プロトコルこれだけは…パケット/アドレス/ソケット（2015年11月号）