安全で容易なIoT構築を支援する「TrustZone セキュアシステム」の取り組み

IoT機器の急増に伴い、これを狙った外部攻撃も増えています。いまやIoT機器への万全のセキュリティ対策は不可欠と言えるでしょう。当社は、ARM「TrustZone」を利用したIoT向けプラットフォーム「TrustZone セキュアシステム」の提供を開始しました。お客様が容易に重要なデータをより安全に管理できるよう、機能拡張などの環境の提供に向けて取り組みを進めています。

外部攻撃に脅かされるIoT機器

日常生活や産業のいたるところであらゆるモノがネットワークに繋がるIoT時代を迎えています。IHS Technologyの推定によれば、インターネットに繋がるIoTデバイスの数は、2020年までに約304億個にまで増大するとされています。一方で、2012年にはCarnaボットネットが世界中で約42万台のIoT機器にウイルスを感染させたり、2016年にはIoT機器を標的としたマルウェア「Mirai」によって世界で約50万台が被害を被ったりするなど、外部からのサイバー攻撃による被害は極めて深刻なものになってきました。

外部からの攻撃は、通信路を傍受して機密データを不正に入手したり、もしくはデータを改ざんしたりするものから、ルータやIPカメラ、ストレージなどネットワークに繋がった機器そのものを攻撃するものまで広範囲に及びますが、セキュリティの仕組みはまだ整っていないのが実状であり、IoT機器のセキュリティ対策は急務となっています。

当社では、こうした喫緊の課題に対応できるソリューション開発の取り組みを進めてきました。現状のIoT機器におけるセキュリティ対策は、通信路の攻撃に対してはTLSなどの標準プロトコルの使用、機器の攻撃には機密データの暗号化などが挙げられますが、これらに共通する重要課題として暗号に使用する「秘密鍵」の保護の問題があります。セキュリティチップなどで秘密鍵を保護すれば、ハードウェアコストが増加します。また、ハードウェア固有のIDなどで秘密鍵を暗号化しても、一時的にRAM上に展開されるため100％安全とは言えません。このような課題をすべて解決する結論として当社が導き出したのが、ARM TrustZoneを使用したプラットフォームです。

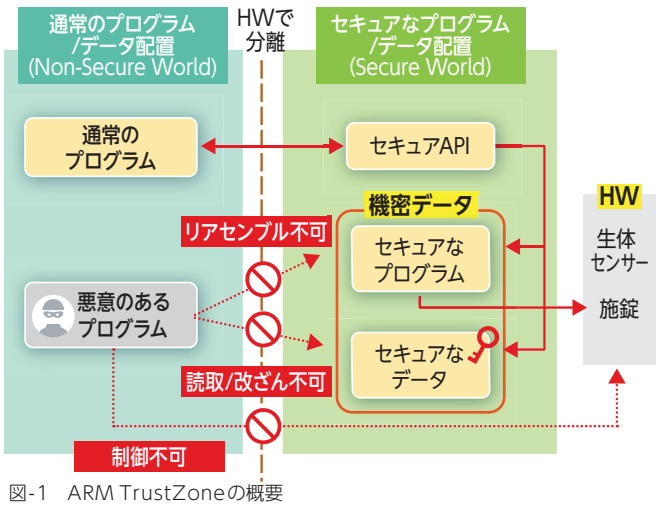

図-1　ARM TrustZoneの概要

IoTに最適な低電力チップ＋万全のセキュリティ

ARM TrustZoneは、ARMのプロセッサコアに搭載されるセキュリティ機能です。追加ハードウェアが不要で、通常プログラムからセキュアデータへのアクセスをハードウェアレベルで制御するため、ソフトウェアによる攻撃から守ることが可能です**(図-1)**。また、認証のためのセンサー(指紋などの生体センサー)や施錠など重要度が高いハードウェアの制御を不正なプログラムから隔離することにより、安全な環境を構築することが可能です。

当社ではIoT向けの新しい低消費電力チップであるARM Cortex-M23/M33(ARMv8-M)に着目し、そこに搭載されているセキュリティ機能(TrustZone)を容易に利用できるプラットフォーム(セキュアプラットフォーム)を提供します。セキュアプラットフォームでは、通常プログラムに対し、セキュアな領域にアクセスするためのAPI(セキュアAPI)を提供することで、センサー操作、Crypto(暗号)といったセキュア機能を簡単に利用できるようになります。また当社は、APIをC言語で開発し、インタフェースをTrusted Execution Environment(TEE)[注1]に準拠することで、よりお客様に使いやすいものとなるように心がけています。

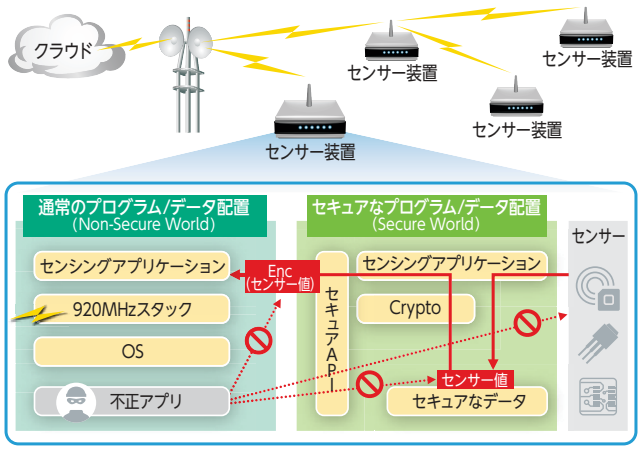

図-2 「TrustZoneセキュアシステム」を利用したセンサー装置を使ったソリューション例

当社はセキュアプラットフォームの提供だけではなく、それを利用したIoTセキュリティソリューションの開発も進めています。近年自然災害が各地で頻発しており、また橋梁、道路、トンネルやビルなど社会インフラの老朽化が深刻化しています。IoT機器(センサー装置)を用いることにより、社会インフラや自然環境の状態を広範囲に渡ってセンシングしデータを収集することで、災害予測や発生時の被害拡大防止に寄与することができます。しかし、これを実現するにはいくつもの障壁があります。まず、センサーが設置される場所の多くは、橋梁やトンネルの高所部分など、人が容易に立ち入ることができない場所です。そのような場所では、有線ネットワークの場合は通信線が劣化・破損する危険性もあります。さらに広い範囲の監視が不可欠であり、しかも異変を見逃さずキャッチできる確実なデータ収集が求められます。その上で、不正なデータや悪意のあるデータによる誤検知を防ぐ必要もあります。

こうした課題の解決策として、次のようなアプローチが考えられます。

(1) 設置やメンテナンスの手間の軽減・撤廃

センサー装置の無線化と電池駆動によるケーブルレス化がポイントとなります。通信線や電源線をなくすことで設置が容易となり、敷設ケーブルのメンテナンスから解放されます。できる限り省電力化を図ることで電池交換のメンテナンスを軽減することも重要です。

(2) 広範囲の安定的な監視

無線マルチホップネットワークの採用により、受信したデータをバケツリレー方式で中継しながら送信することが可能となります。安価な無線センサー装置を使って数kmに及ぶ広域での監視が実現できます。

(3) データの信頼性確保

センサー装置の認証とデータの完全性を確保することで、収集したデータから確実な統計情報を算出することが可能となります。

セキュアプラットフォーム×メッシュネットワーク

このような観点から、当社が取り組みを進めているのが、センサー装置をターゲットとしたプラットフォームです**(図-2)**。通信に関しては、IoT用途に最適な(株)東芝独自の920MHzプロトコルスタックを採用しました。このプロトコルスタックは、メッシュネットワークを自動形成するためネットワーク設定は不要です。また独自アルゴリズムにより、当社のシミュレーションでは電池のみで10年駆動を実現し、低消費電力かつ容易にIoT機器を使った監視システムを構築することが可能です。

もちろん、小さなセンサー機器あるいは無線のデータを盗聴や改ざんなど外部攻撃から守るため、暗号化および安全な場所への保持など万全なセキュリティの仕組みを導入しています。

当社は2017年9月から「TrustZone セキュアシステム」としてセキュアプラットフォーム、およびIoTセキュリティソリューションの提供を開始しました。IoTセキュリティソリューションは、センサー装置向けにセンシングするサンプルアプリケーションを付属しているため、すぐに利用いただけます**(図-3)**。

IoTの用途によってセンサーを選び、TrustZone セキュアシステムを導入するだけで、収集したデータを安全にかつ容易に送る仕組みを提供します。現在はサーバ連携なども進めているほか、多くのIoT機器の暗号鍵をいかに管理していくか、さらにはIoT機器以外への適用などにも取り組んでいるところです。お客様のセキュアなIoT実現を支援できるよう、さらなる取り組みを進めていきます。

(エンベデッドシステム事業部　清水 豊、加藤 雪子)

注1) Trusted Execution Environment(TEE) : GlobalPlatform (https://www.globalplatform.org/) が策定したガイドラインです。

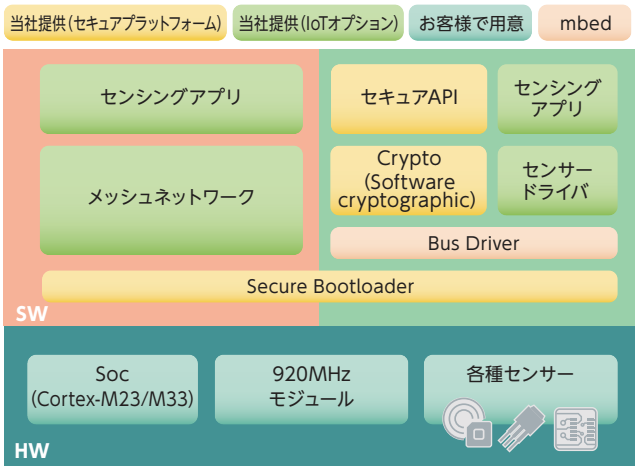

図-3 当社が提供する機能