2018 年 3 月 5 日
大日本印刷株式会社
NTT コミュニケーションズ株式会社

安全な IoT ソリューションを提供可能とする「セキュリティ SIM」を共同開発

～DNP が IC カード事業で培ったセキュリティ技術と、NTT Com が香港に構築した MVNO 基盤を活用～

大日本印刷株式会社(以下:DNP)とNTTコミュニケーションズ株式会社(以下:NTT Com)は共同で、IoT (Internet of Things：モノのインターネット)機器がモバイル回線を利用する際に必要な SIM (Subscriber Identity Module)に、通信データの暗号化など IoT 機器のセキュリティを向上する機能を追加した、新たな SIM および eSIM※1(以下:「セキュリティ SIM」)の開発を、2018 年 3 月より実施します。「セキュリティ SIM」を IoT 機器に組み込むと、1 個のチップで、モバイル回線の利用とセキュリティの向上を同時に実現することができます。

DNP は、「セキュリティ SIM」の開発において、IC カード事業などで培ったセキュリティ技術や基盤を活用します。また NTT Com は、香港で実証実験を行っている SIM の発行や運用ノウハウを用いることで、日本の MVNO として初めて「セキュリティ SIM」の発行に取り組みます。

1. 開発の背景

近年、工場やオフィスなどのさまざまな機器がインターネットに接続され、IoT を活用したサービス・技術の高度化やビジネスモデルの変革が進みつつあります。現在は、自社の機器のみがつながるクローズドな環境における IoT が主流ですが、今後さらに IoT が浸透していくことによって、他社の機器との連携も含めたオープンな環境において IoT を活用する事例の増加が予想されます。一方で昨今、IoT 機器を対象としたサイバー攻撃も数多く報告されるようになっており、オープンな環境でも安全に運用を行うため、IoT 機器のセキュリティを高めたいというニーズが高まっています。

DNP と NTT Com は、このようなニーズに応えるため、NTT Com が香港で行っている eSIM の実証実験の基盤と、DNP のセキュリティ基盤とを連携させることで、1 枚の SIM でモバイル回線の利用と IoT 機器のセキュリティ向上を同時に実現する実験に成功しました。これを踏まえ、今回の実用化に向けた共同開発を行うこととなりました。

2. 機能と特長

「セキュリティ SIM」は、モバイル回線の加入者認証を行う機能に加えて、暗号鍵などのデータを用いた IoT 機器の識別や認証、通信データの暗号化と真正性の確認、ソフトウェア改ざんなどの不正検知を行うセキュリティ機能を備えています。また、フラッシュメモリではなく IC チップ内にセキュリティ機能を実装することで、物理攻撃やサイドチャネル攻撃※

[2] に対するきわめて高い耐タンパ性※3 の確保を実現しています。

(1) 暗号鍵などのデータを用いた IoT 機器の識別および認証を行う機能

ID・暗号鍵・電子証明書などのデータを用いて、クラウドに接続する IoT 機器が正当なものかどうかの識別および認証を行うことができます。

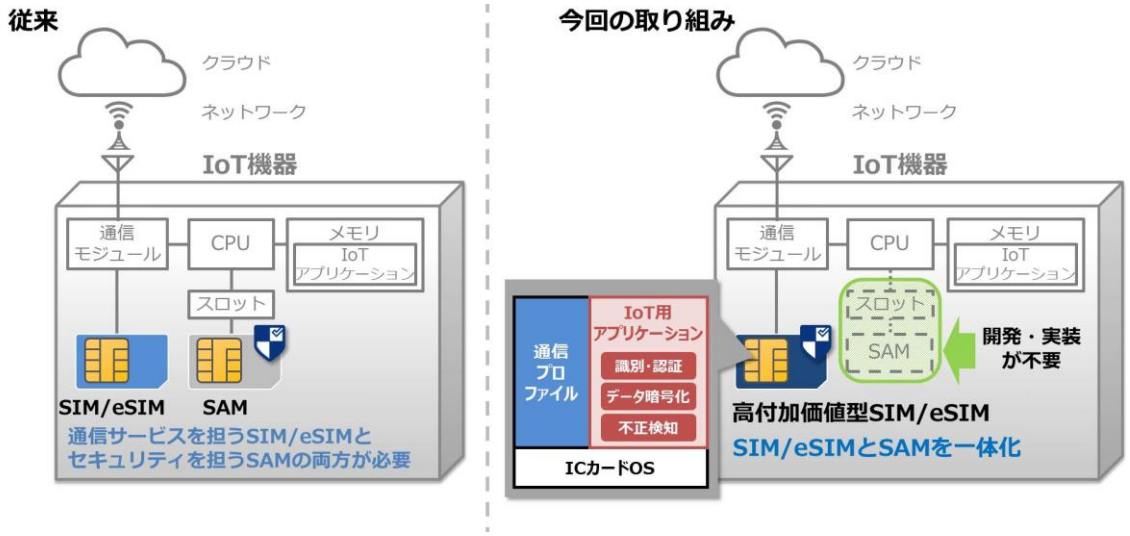
(2) 通信データの暗号化と真正性の確認機能

通信するデータの暗号化および復号を SIM チップ内部で行います。DNP が IC カード事業で培った情報セキュリティ技術を応用して提供する、IoT 環境のセキュリティレベルを高めるサービス「IoST (Internet of Secure Things)プラットフォーム」を利用することで、データを IoT 機器で暗号化してクラウドに送ることができるほか、クラウドから送られてきたデータを IoT 機器で復号することが可能です。このため、オープンな通信経路であっても、IoT で用いるデータをエンド・ツー・エンドで保護して、データの真正性を確保することができます。暗号アルゴリズムは、2030 年以降も利用可能な※4 共通鍵暗号、公開鍵暗号、ハッシュ関数を搭載しています。

(3) 機器のソフトウェア改ざんなどの不正検知機能 (予定)

IoT 機器に搭載する OS やアプリケーションの改ざんを防止するために、SIM チップ内で管理する秘密鍵やホワイトリストを用いて、署名検証や IoT 機器のセキュアブート※5 の機能を実現します。

これらの機能を実現するために、従来は「SAM (Secure Application Module)」や「TPM (Trusted Platform Module)」と呼ばれるセキュアな IC チップを、SIM とは別に IoT 機器に組み込む必要がありました。本製品は SIM と SAM の機能を 1 つのセキュアな IC チップ内に一体化しているため、3G/LTE などの SIM が利用できる通信モジュールを備えた機器に、「セキュリティ SIM」を動作させる専用のソフトウェアを組み込めば、新たにハードウェアセキュリティ対策のための開発・実装を行うことなく、IoT 機器にモバイル通信回線に加えて高いセキュリティを提供することが可能になります。



＜「セキュリティ SIM」概要＞

3. 今後の取り組み

DNP と NTT Com は、共同で「セキュリティ SIM」に関する市場調査や検証を進めていきます。

DNP は実用化の際に、「IoST プラットフォーム」を活用して、SIM 製造時に暗号鍵、電子証明書を初期発行するとともに、運用中にセキュリティ向上のためインターネット経由にて定期的に更新する機能を実装します。

また NTT Com は、お客さまの IoT に最適なモバイル回線と、モノから集まるデータを蓄積・可視化・分析する IoT プラットフォームサービス「Things Cloud」などの提供実績を活かし、「セキュリティ SIM」を用いたより安全な IoT ソリューションを提供していく予定です。

※1：eSIM とは、embedded SIM の略。遠隔で通信プロファイルを書換えすることができる SIM のこと。
※2：サイドチャネル攻撃とは、暗号を不当に解読する方法の一つ。機器や回路が暗号を処理する際の物理的な兆候、例えば電磁波や温度の変化、処理時間の違いなどを外部から観察することにより分析する。
※3：耐タンパ性とは、外部から、機器内部のハードウェアやソフトウェアの構造を不当に解析・改ざんする行為(英語で tamper)に対する耐性のこと。
※4：米国の国立標準技術研究所(NIST)が公表している、長期的に見た場合のアルゴリズムと鍵長の安全性に関する指標において、2030 年以降も利用できるかどうかが分水嶺となっている。
※5：セキュアブートとは、IoT デバイス起動時に、ブートローダ(OS を読み込んで起動させるプログラム)と OS のデジタル署名を検証し、正式なデジタル署名のない OS では起動させないことで、改ざんを防止する機能。