IoT・エコシステム時代におけるセキュアコンポーネント ～トラステッドなスマート社会を目指して

日本電信電話株式会社　セキュアプラットフォーム研究所 NTT リサーチプロフェッサー　庭野（にわの）　栄一（えいかず）

1. はじめに

近年IoT環境の進展が著しく、AI/ビッグデータ/クラウド基盤技術と合わせて多様な分野でのデータ利活用・連携によるスマート社会が実現されようとしている。

しかしながら、このような環境においては、IoTデバイスのぜい弱性に起因するインシデント事例が多数報告され始めており、データやデバイスの真正性・トラストをどのように担保してゆくかの検討が正に重要課題となってきている。

このような問題を解決するための手段の一つとして着目されているのが、従来強固なコンシューマ系認証を中心に適用が進んできた「セキュアコンポーネント」である。

本稿では、IoTそしてエコシステム化の進展を背景として出現する超スマート社会において、トラステッドな環境を提供するための技術「セキュアコンポーネント」の現状と将来について述べる。

2. セキュアコンポーネント

さて、セキュアコンポーネントとは何か？セキュアコンポーネントとは一つには現在までに広く普及しているICカードやスマートフォンのSIMなどのような、いわゆる外部からの攻撃に対する強い耐性（耐タンパ性）を有し、1）セキュリティ関連鍵などの機密・機微な情報を管理するセキュアストア、2）認証・署名・暗号化などのセキュリティ機能、そして3）リモートアプリケーション管理機能、などの特徴を有するセキュアチップ（SE：Secure Element）のことである。

近年では、発行後にリモートによる発行者切替えが可能でコネクテッドカーなどへの適用が進んでいるeSIM（embedded SIM）や、最近ではデバイスハードウェアのセキュリティの強化に向けてSoC（System on Chip）にバンドルされるiSIM（integrated SIM）が登場している。そして、このようなSEの種別の拡大のほかに、新たにTEE（Trusted Execution Environment）と呼ばれる通常のOSとは異なるセキュアな実行環境が登場するなど、現在、セキュアコンポーネントの多様化の進展が著しく、ウェアラブルデバイスを含む多様なIoTデバイスへの搭載が期待されている[1]。

特に、エッジデバイス、ゲートウェイ、エッジサーバ、クラウドなど広範なIoTネットワーク環境においてはTPM（Trusted Platform Module）、HSM（Hardware Security Module）のような従来のPC/サーバ系の耐タンパモジュール、そしてセキュアMPU（Micro-Processing Unit）などの関連技術と今後どのように統合連携・棲み分けるかの議論が開始されている。

3. IoT ～デバイス認証・真正性

それではなぜIoT時代においてセキュアコンポーネントが重要となるのか？

多様なエッジデバイスが分散配置、接続されるIoT環境においてはよく指摘されるようにセンサー情報の改ざんのみならず、サイバー・フィジカル結合による物理的デバイスの不正操作(医療機器･自動車等生命に関わるもの等)、ローエンドのIoTデバイスを踏み台としたサイバー攻撃など多数の脅威事例や実証結果が報告され始めている（政府も2019年2月より、NOTICEプログラムによるサイバー攻撃対策に向けたIoT機器の調査を開始)。

人の強固な認証をするためにICカードが普及したように、今後はこのようなインシデントの増加や影響範囲の拡大とともに、デバイスの強固な認証、真正性を保証するための信頼の基点として、デバイスの構成証明（Attestation）／セキュアブート機能をサポートするセキュアコンポーネント[1]への期待が高まってゆくと考えられる。

また、特にIoTデバイスの場合は、保守が困難な場所に対して長期にわたり設置されるケースも多いことから、例えばセキュリティ機能の危殆化対応など耐タンパチップ内の機能をリモートで柔軟に更新・追加できる機能が重要であると、国際標準化組織GlobalPlatform[1]は指摘している。セキュアコンポーネントの最大の特徴は、このようなリモート環境により、後乗せで多様な機能を搭載・追加・変更ができる点にあると言える。

4. エコシステム化の進展～セキュアなIDコンポーネント管理の重要性

さて、「つながる」環境のもう一つの重要な流れがエコシステム化の進展である。

5G/LPWAなど接続環境の高度化を受けて、あらゆるも

のが動的につながる時代が到来してくる。

このような環境下においては、ネットワーク越しに動的に登録生成・接続される、人・もの・システムに対して、その確からしさ（安全性・セキュリティ）と信用（安心性・トラスト）が確認できることが望まれる。

このようなエコシステム環境においては様々な製造者の製品が国を超えて構成され、つながる環境が出現する。ここでは、最近よく議論が開始されている部品のサプライチェーンやデバイスのライフサイクル問題に加え、今後はセキュアコンポーネントと合わせたシステム全体に対するセキュリティ・トラストの保証や評価の考え方がより重要となると考える。

エコシステム化による様々な要素で構成される車、家・ビル、そして都市などSoS（System of Systems）の複雑性の増大と規模の拡大の問題に対して、それぞれ、そしてそれぞれの構成要素のID（識別子だけでなく、構成される実体など多様な属性の正当性含む）をどのように保証・認証してゆくかが鍵となる。

したがって、この極めて複雑な構造を有する「IDコンポーネント」群をどのような単位・関係性で構成・構造化し、それぞれをどのようなセキュアコンポーネント・耐タンパモジュール・セキュアMCUで管理・保証するかが、その真正性や信用を保証する上で非常に重要となると考える。

すなわち、人、もの、システム、SoS及びその構成要素に対するIDコンポーネント、そして信頼の基点としてのセキュアコンポーネント（その他耐タンパモジュール、セキュアMPU等）の関係を整理し、そのセキュリティ・トラストを評価・保証する仕組み、そしてそのためのセキュリティバイデザインが今後の重要な課題である。

5. トラステッドなスマート社会

現在、有望なIoT及びIoTセキュリティ分野のほか、その中で有望なセキュアコンポーネントの適用分野・ユースケースについての議論が開始されている。

述べてきたセキュアコンポーネントと合わせた、実体の構成保証を含むIDコンポーネント群の管理問題を小さなところから検討してゆくことで、最終的には「安心・安全に」多業種・多分野データ連携が行える超スマート社会、それを支えるトラステッドスマートシティの実現につながってゆくのではないかと考える。

そのための重要な鍵として、多様なレベルでの構成要素の社会的信用の検討も重要となるであろう[2]。

6. おわりに

現在、IoT×セキュリティ×セキュアコンポーネントに関しては、本格的な標準化の検討が開始されたばかりであると言える。

国際的な団体としては、GlobalPlatformとGSMA[3]、OneM2M[4]が連携して標準を定めている。ETSIは2019年2月コンシューマ系IoT向けのサイバーセキュリティ文書でeUICC/TEEなどを利用してセキュリティサービスを管理する記述を含む技術仕様をリリースした[5]。また、同様に米国NIST、欧州ENISA、国内ではIPA、IoT推進コンソーシアムにてもサイバーセキュリティ／IoT関連のガイドラインにて耐タンパモジュールやセキュアコンポーネントについての言及が見られる。

今後は、開始されているGlobalPlatformとTPMの標準化組織であるTCG（Trusted Computing Group）など耐タンパチップ関連団体の連携強化、このような耐タンパチップ関連団体とIoT関連団体の連携拡大、さらには将来に向けてITU-T SG20などスマートシティ関連の団体との協調に期待するとともに、その一助になれば幸いである。

参考文献

[1] 庭野栄一、「GlobalPlatformの最新標準化動向― IoT時代のセキュアコンポーネント」NTT技術ジャーナル、2018 Vol.30 NO.12

[2] Eikazu NIWANO, “From Secure to Trusted Smart Cities”, Global Forum 2015, 2015.9.29

[3] “GSMA Remote Provisioning Architecture for Embedded UICC”, Technical Specification Version 3.2, June 2017

[4] OneM2M TECHNICAL SPECIFICATION, TS-0003-V2.124.1, Security Solutions, March 2018

[5] “CYBER；Cyber Security for Consumer Internet of Things”, Provision 4.4-1, ETSI TS 103 645 V1.1.1（2019-02）