

AI・IoTによるイノベーションを支える暗号技術によるトラスト

セコム株式会社 IS 研究所
JNSA PKI 相互運用技術 WG リーダー
松本 泰

1. はじめに

Society5.0が目指す超スマート時代において、AI・IoTによるイノベーションが期待されている。IoTは、繋がることによる価値の創造が求められており、また、AIは、IoTの吐き出すビッグデータを処理するといったことにより様々な産業におけるイノベーションが期待されている。

AI・IoTによるイノベーションが期待されている分野に自動車、医療デバイス等があるが、これらの分野においては、従来からの法的な規制がある。これらの規制が必要な分野において、ソフトウェアや機械学習済みデータの更新が行われるAIエッジを想定した場合、利用時の規制が強化される方向に向かうと考えられる。

利用時の規制を考えた場合、製品プロバイダー・サービスプロバイダーは、利用時における個々のデバイスのトレーサビリティ／トラッキングを確実に実行する必要に迫られる。また、サイバーセキュリティ上だけでなく、セーフティやプライバシーについてもそのインシデントに対するアカウントビリティが強く求められることになるが、これらの対応に暗号技術によるトラストが非常に重要な役割を果たす。

このようにAI・IoTによるイノベーションに対応するAIエッジは、暗号技術によるトラストの実現が重要になる。こうしたことに対応するために、暗号技術とハードウェアセキュリティをベースにしたデバイス自体のアーキテクチャ変革が必要であり、こうした技術をベースにしたIoTデバイスが、超スマート時代の産業競争力に結びつくと考えられる。

2. AI・IoTによるイノベーションと規制

AI・IoTによるイノベーションでは、リアル空間に大量に配置されたIoTデバイスが、大量のデータをサイバー空間に吸い上げ学習し、その学習結果をAIエッジに反映するといったモデルが考えられている。このようなAIエッジの考え方が社会に大きなインパクトを

与えると考えられている分野／製品に、自動運転などを目指す自動車や、AI医療診断等に利用する医療デバイスがある。

このような自動車や医療デバイスなどは、従来からの「モノ」としての規制が存在する。例えば自動車であれば、車種に対して型式認証と呼ばれる法規・技術要件・安全性を満たした製品に与えられる認証を取得し、この型式認証を取得した車種の個々の車が、法的に要求される出荷検査を経た後に初めて公道を走ることができる。また、医療デバイスであれば、医薬品と同様に、臨床実験において、その効果と安全性が証明された後、承認というフェーズを経て初めて製品の出荷が可能となる。

しかし、AI・IoT等技術の発展と、これらのイノベーションの期待等を背景に、この規制のあり方に変化が見られる。例えば、米国における医療の規制管轄官庁であるFDA（米国食品医薬品局）では、2017年からデジタルヘルスソフトウェア事前認証プログラム（Digital Health Software Precertification (Pre-Cert) Program）を開始しているが、ここでは、新たな製品出荷後の規制、すなわち利用時の規制のあり方が示されている。

同様のことは、自動運転への期待が高まる自動車においても起きている。2019年5月、「道路交通法の一部を改正する法律案」が可決し成立した。これは、国連配下の自動車基準調和世界フォーラム（WP29）において自動運転車の国際基準作りに向けた作業の反映でもあるが、この法律の大きな主旨のひとつは「自動運行装置等に組み込まれたプログラムの改変による改造等に係る許可制度」になる。

このような規制が必要な分野におけるAIエッジでは、従来からの「モノ」としての規制だけではなく、利用時の規制、サービスとしての規制が求められることになる。この際、製品プロバイダー・サービスプロバイダーは、AIエッジの利用時における、確実なトレーサビリティ／トラッキング、そして、インシデントなどに対応するアカウントビリティが強く求められることになる。

図1に、これらの関係を示す。

3. 利用時の規制に対応した暗号技術によるトラスト

AIエッジとなる医療デバイスや自動車等において、利用時のソフトウェアや機械学習済みデータの更新が出来ることは、社会を変革させる可能性があるが、これらには、利用時の規制が求められる。

利用時における規制的要求は、概ねセーフティ、プライバシー、セキュリティの確保になると考えられるが、これらの規制に対応するためには、個々のデバイス（医療デバイス、個々の自動車、および、自動車内の個々のECU等）が、確実に個体識別でき、その状態が（リモートから）把握でき、更にセキュアなソフトウェアと学習済みデータ等の更新が可能であることが求められる。また、強い規制という観点からは、これらの客観的な説明、および、証明できることが非常に重要になる。

こうした利用時の規制に対応するAIエッジの実装への要求は、トレーサビリティ・トラッキング、アカウントビリティ等に対応する何らかの説明および証明の仕組みになるが、この証明の仕組みは、「トラスト」と言い換えることができる。

このような説明／証明、すなわちトラストには、情報セキュリティで言われるところのCIA 中のI(インテグリティ)を継続的に、また効率的に可能とする実

装が重要になる。そして、このインテグリティを効率的に実現するためには、暗号技術、とくデジタル署名技術が、重要な役割を果たす。

規制における重要な視点は、一般的には、セーフティに対する規制の対応が重要であり、セキュリティの対応だけを意味する訳ではないことに注意する必要がある。このように暗号技術によるトラストの実装は、セーフティに対する規制への対応でもある。

AI・IoTによるイノベーションにとって、利用時のソフトウェアと学習済みデータの更新が重要だと考えると、そもそものビジネスモデルが売り切りの製品販売から、利用時重視のサービス中心のビジネスモデルに変化していく。サービスの視点、特にサブスクリプションモデルなどのビジネスモデルを想定した場合、大量のAIエッジの効率的な管理の観点が欠かせないが、ここにも暗号技術によるトラストが大きな役割を果たす。確実なトレーサビリティ・トラッキングの仕組みなしには、サービス時の何らかの課金の仕組みは難しい。すなわち、ビジネス的観点からも暗号技術によるトラストが必要になる。

4. 暗号技術によるトラストの実装および標準化動向

このような利用時の規制に対応するAIエッジにお

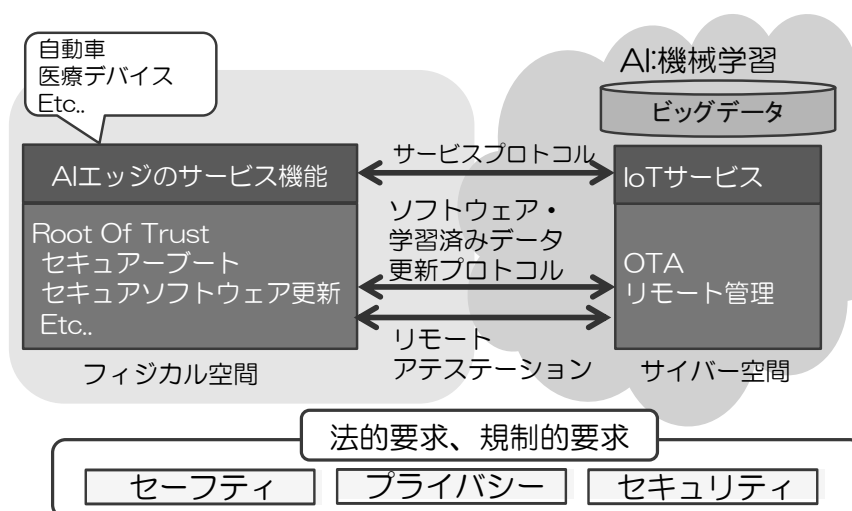


図1. AIエッジ、機械学習、規制の関係

ける「証明の仕組み」すなわち「暗号技術によるトラスト」は、AIエッジの信頼の起点(Root of Trust)、デバイスIDの一意性、耐タンパ性の確保等がベースとなって構築されることは想像難くない。こうした暗号技術によるトラストを実現するアーキテクチャは、ここ10数年でスマートフォンという形で非常に進化してきた。そして現在、これらスマートフォンで培われてきた技術が、様々なIoTデバイス・AIエッジに適用されつつある。

ここでの技術的に重要なキーワードとして、TEE (Trusted Execution Environment) とアテステーションがある。TEEは、概ね、一般のアプリケーションと分離された実行環境 (Execution Environment) になるが、この実行環境においてトラストが要求されるアプリケーションが実行される。TEEの実装には、様々なアーキテクチャが提案され、また実装されているが、TEEを利用するAPIはGlobal Platformにおいて標準化されており、これらがIoTデバイスに実装されつつある。また、TEEが組み込まれることを想定したIoTデバイス向け半導体、SoC (System-on-a-chip) が、数多く開発されている。

一方、IoTデバイス・AIエッジをリモートから管理するアテステーションの標準化が進んでいる。IETFでは、2019年3月に開催されたIETF104プラハから、リモート・アテステーション・プロシージャ (Remote Attestation Procedures - RATS) がワーキンググループとして活動を始めているが、このRATSは、リモート環境のIoTデバイスの正当性の確認・証明等、すなわちリモート・アテステーションに使われていくことが想定されている。

参考文献

PKI day 2019 午前の部 IoTのトラスト
<https://www.jnsa.org/seminar/pki-day/2019/>

FDA Digital Health Software Precertification (Pre-Cert) Program
<https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program>

IETF: Remote ATtestation ProcedureS (rats)
<https://datatracker.ietf.org/wg/rats/>

このアテステーションという概念は、従来からPCに内蔵されたTPM等を利用して実装されてきたが、それほどブレイクしたとはいえないところがあった。PCの場合、PCの管理を利用する人に頼っていた側面があったためと考えられる。

これに対して、現在、膨大な数のIoTデバイスを人手に頼らずにリモート管理するといった要求からリモート・アテステーションが俄然注目を浴びている。こうした仕組みの標準化が出来れば、多様なIoTデバイスを、大量にかつ効率的にリモート管理が可能になり、すなわち低コストでIoTデバイスを保守することが可能になる。そして、こうしたことがイノベーションにつながる。

トラストなアテステーションを生成しようとした場合には、ハードウェアセキュリティ、Root of TrustやTEEなどに依存することになるが、このトラストなアテステーションは、「利用時の規制」や、サブスクリプションモデルのビジネスにおけるIoTデバイス・AIエッジにとって非常に重要な役割を果たすことになる。

5. おわりに

既存の法規制等が、AI・IoTによるイノベーションを阻害していると考えられる一方、本質的に規制が必要な分野においては、規制のパラダイムシフトが起こりつつある。こうした分野においては、新たな法規制などに対応できるIoTデバイス・AIエッジの暗号技術によるトラストが重要となり、これらが低コストで実現できることが、今後の超スマート社会における競争力の源泉ともなる。