

グローバル環境において求められる
IoT セキュリティに関する考察
ー日本製造業に向けてー

一般社団法人セキュア IoT プラットフォーム協議会

理事長 辻井 重男

2020年3月

1. はじめに

グローバル環境において IoT の導入が加速度的に進んでいく中、脆弱性を内在するデバイスも多く、外部からの不正操作、なりすましによる機密情報の搾取やデータの改ざん、デバイスの踏み台化などセキュリティ上の重大な脅威も明確になってきた。特に軍事や重要インフラなどを狙われた場合は、生命や社会生活に大きな影響を与えることが懸念される。

そこで現在の IoT をとりまく状況を「国際協調の視点」、「国際標準化および調達要件の視点」、「グローバルサプライチェーンの視点」で包括的に整理し、その課題を明らかにするとともに、一般社団法人セキュア IoT プラットフォーム協議会(以下、SIOTP 協議会)での取り組みをまとめることとする。

2. IoT を取り巻く環境

【国際協調の視点】

2018 年 10 月 4 日に米国有力シンクタンクであるハドソン研究所でのペンス副大統領の演説が、マスコミでは「新冷戦」と報道され、大きく注目されたのは記憶に新しいところである。この演説の中では、貿易障壁問題だけではなく、国家安全保障の観点での軍事計画も含む知財の窃盗や不当な技術移転の問題を指摘しており、その後のファーウェイ排除に繋がっていることが想定される。

<https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china/>

2019 年 5 月 3 日の「プラハ 5G 会議」では、米国や EU、日本、北大西洋条約機構(NATO)など約 30 カ国・機関が参加し、特定の国や事業者を名指しした指摘はなかったが、サイバー攻撃などのリスク回避に向けて各国が連携を深めるとする議長声明を採択されている。議長声明からは、IoT デバイスの真正性の確保と識別や運用時に脆弱性を早期に発見し、修正プログラムを提供することによりライフサイクルを管理することが含まれていると読み取れる。これは RoT(Root of Trust)による安全な鍵管理や OTA(Over The Air)による確実なファームウェアアップデートなどに繋がるものだと考えられる。

https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf

また、2019 年 6 月大阪で開催された G20 に先立ち、2019 年 3 月にリリースされた「B20 東京サミット共同宣言」では、Society5.0 for SDGs の実現に向け、グローバルなサプライチェーン全体のセキュリティリスクを管理する、一貫性のある、または相互運用可能な枠組みの開発・運用の必要性を指摘されている。

<https://www.keidanren.or.jp/policy/2019/020.html>

これらの動きから、対中国を視野に入れながらも、国際協調によりグローバルなサプライチェーンの中でのセキュリティが大きくクローズアップされていることが理解できる。

【国際標準化および調達要件の視点】

あわせて国際協調の動きと同期を取り、ゼロトラストセキュリティの考え方にに基づき、「IoT デバイスの長期ライフサイクルにわたる識別および保証」を実現する為の国際標準化が進められている。

●IEC 62443

IEC(国際電気標準会議)が定める産業機器の汎用制御システムのセキュリティ規格。

工場、プラント、ビル、発電所などの制御システムにおいてもセキュリティが求められているが、もともと閉じられた世界で運営がされていたため、比較的サイバーセキュリティ対策に対する意識が低く、その対応が遅れている。「IEC62443」では、制御システム機器を製造する“デバイスメーカー”から、機器を組み合わせてシステム構築を行う“システムインテグレータ”そして実際に制御機器を利用する“ユーザー企業”それぞれに適合した規約が設定されている。特に SIOTP 協議会では、システムを構成するコンポーネントのセキュリティを定義する「62443-4 シリーズ」に注目しているところである。

●NIST SP800-171

NIST(アメリカ国立標準技術研究所)が定めた機密情報以外の重要情報（CUI）を扱う民間企業が実施すべきセキュリティ対策をまとめたガイドライン。

一連のサプライチェーンにおいて関連する企業、委託先が一定のセキュリティ基準に基づいて安全性を担保するものであり、その規定対象は、「組織」、「システム」、「コンポーネント」、「技術」と広範囲に渡る。

この「NIST SP800-171」は米国政府調達要件であるが、米国外の企業であっても同盟国などそのサプライチェーンに入っている限り域外適用が求められる。

●FIPS140-3

暗号モジュールの規約として注目されているのが、NIST が発行する米国の連邦情報処理標準「FIPS140-3」である。半導体デバイスにおいて、サービスの上位層を支える厳格なセキュリティ要件を満たす為に、4段階のレベルで、半導体の実装するセキュリティ要件、留意すべき認証テスト要件が規定されている。SSP(Sensitive Security Parameter)管理、物理的改ざん攻撃耐性、非侵襲的セキュリティ、ライフサイクル管理、セルフテスト、RoT(Root of Trust)、セキュアブート、セキュアファームウェアアップデート、鍵やデータの完全な消去等がその要件として明記されている、また FIPS140-3 は米国政府機関だけではなく、世界の商用システムに対する要求にもなることが想定される。

この FIPS140-3 に含まれる「NIST SP800-140」は、2020 年 3 月 22 日にファイナライズされ、認証テスト開始は、2020 年 9 月 22 日を予定している。

このような国際標準化の動きは、実際に施行される法令化にもつながっており、様々な調達基準にも適用され始めている。これらの法律には、セキュリティが担保されていない IoT デバイスについては、「作らせない」、「繋げせない」、「持ち込ませない」という意思が明確に見て取れ、ゼロトラストセキュリティに基づく安全なサプライチェーン構築に向けて動きだしていることが明らかである。

●米国国防権限法 2020(National Defense Authorization Act for Fiscal Year 2020)

米国における国防関連の調達要件として「米国国防法 2020」が 2019 年 12 月 20 日に成立した。

<https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf>

特に sec. 224 において、2023 年 1 月 1 日までリリースされるマイクロエレクトロニクスの製品とサービス対象にサプライチェーンの安全性に係る要件が定義されている。

ここで制定されるセキュリティ基準には、前述の「SP800-171」を中心に「SP800-140」(FIP140-3 に含まれる規格)などの国際標準が調達要件として含まれていくことが予想される。

この要件は、米国内の政府機関、民生産業のみならず、同盟国・パートナー国においても製品とサービスを調達するための基準として使用される。

●カリフォルニア州 IoT セキュリティ法

2020 年 1 月に施行(2018 年 8 月制定)された全米初の IoT デバイスのセキュリティ要件を定義する州法。

ネットワーク接続されるデバイス製造者に対して、デバイス固有のパスワードの付与もしくはデフォルトパスワードの変更を促す機能の追加を義務付けてられている

ここで定義されているセキュリティ要件は厳格なものではないが、IoT セキュリティに関する法令が、実際に施行されたことは注目すべき点だと考える。

日本においても同様の動きがみられる。

IoT はグローバル環境の中で推進しているものであり、今後も国際標準化の動きと同期を取って進められていることが想定される。

●電気通信事業法 技術基準適合認定(技適)

2020 年 4 月 1 日より、「電気通信事業法に基づく通信端末の技術基準適合認定」が変更されます。今回の変更により以下の通り、ネットワークに接続する端末設備のセキュリティ要件が変更される。

http://www.soumu.go.jp/main_content/000615696.pdf

この中では、「アクセス制御機能を持たせること」、「出荷時のデフォルトパスワードの変更を促す機能を含むこと」、「ファームウェアの更新機能を持たせること」の 3 点が技術基準として明記されている。さらに注目すべき点は、アクセス制御に関して、識別符号が安全に保管されていること(RoT: Root of Trust など)やファームウェアの更新に関しては、安全かつ自動で行われること(OTA: Over The Air)など一段高い基準が推奨項目として挙げられていることである。

【グローバルサプライチェーンの視点】

中国武漢を発症地とした新型コロナウイルスの影響が、観光業、小売業のみならず、モノづくりにおいてもグローバル環境でのサプライチェーンに大きな影響を与えたことは周知のとおりである。いかに世界の工場とも呼ばれる中国にモノづくりを依存していたかが改めて認識され、製造業の在り方を再考する機会にもなったとも考えられる。

またヨーロッパもいまや WHO からパンデミックの震源地と位置付けられ、国家非常宣言のもとに経済活動が停止している状態である。米国もニューヨークを中心に同様な状態になりつつある。

一方、日本では公衆衛生の整備状況や医療の高度化により、諸外国に比べると感染がコントロールされている状態であり、医療崩壊も発生していない。安全性に対して高い意識を持つ国民性も有効に機能していると思われる。

今回の新型コロナへの対応を見ても、日本の持つ安全性に対する高い意識、環境、技術は、サイバーセキュリティにおいても世界をリードする立場であることをあらためて実感する。日本製造業の品質の高さや細部にわたるきめ細やかさという強みを活かし、日本製 IoT デバイスの圧倒的な安全性をアピールすることにより、日本製造業のさらなる発展につながることを確信している。

3. セキュア IoT プラットフォーム協議会の取り組み

SIOTP 協議会では、2018 年 4 月に設立以来、「真贋判定こそは個体(デバイス層)から文化層(サービス層)まで貫く理念」を基本方針として、IoT に求められる実装レベルのセキュリティ要件に関する研究を行ってきた。

このような活動を展開してきたのは、様々な標準化の動きを見てもその基準は提示されているものの、「具体的にどうやって実現したらよいのか」という方法論について規定され

ているものが見当たらないためである。

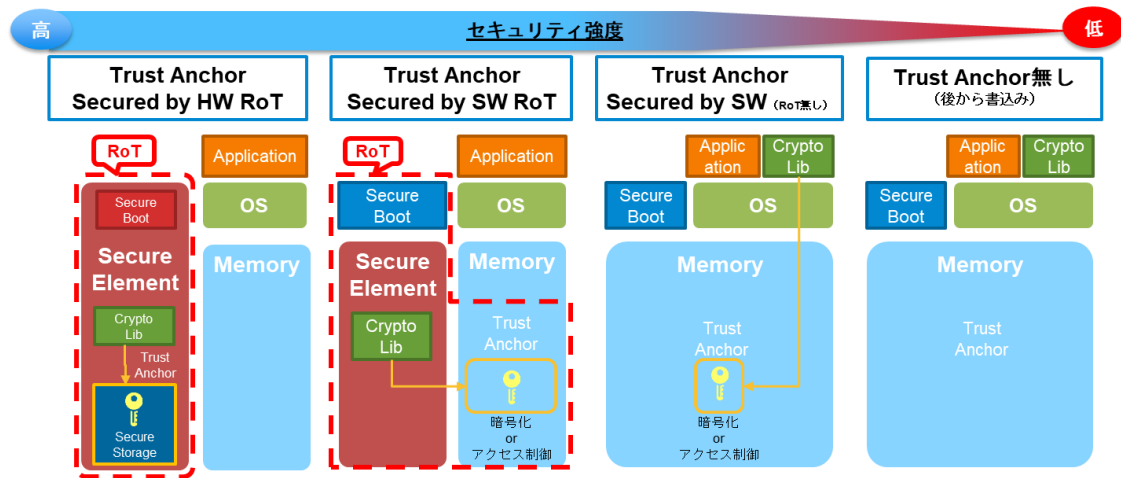
この研究成果は以下の通り学会において発表されている。

- ・「重要 IoT デバイスへの PKI 電子認証の導入 ―セキュア IoT 基盤の確立に向けて―」
電子情報通信学会(ISEC)2018 (2018.11.4 福岡)
- ・「IoT・Big Data・AI 環境における真正性保証・真贋判定の高度化と普及に向けて
―デバイス層から情報サービス層まで―」
電子情報通信学会 暗号と情報セキュリティシンポジウム(SCIS)2019 (2019.1.24 高知)
- ・「重要 IoT デバイスへの PKI 電子認証の実装
―セキュア IoT 基盤が形成するトラストチェーン―」
情報処理学会 コンピュータセキュリティシンポジウム(CSS) 2019 (2019.10.22 長崎)

これらの発表においては、PKI に基づくライフサイクル全体に渡るトラストモデル構築について考察している。

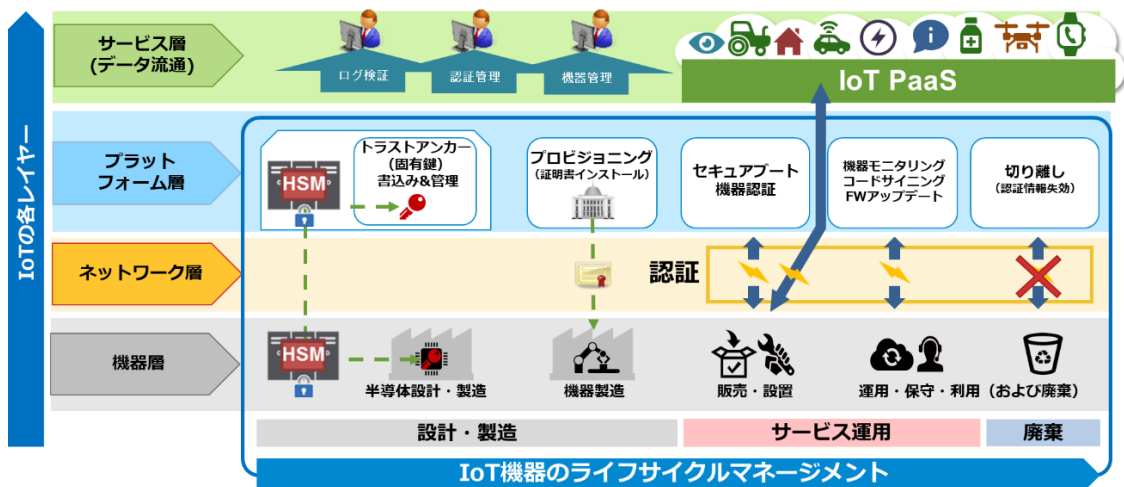
IoT デバイスとして組み立てられる前段階において、各 IoT デバイスに必ず組み込まれる LSI (電子部品)、いわゆる IC チップに普遍的なクレデンシャルを埋め込むことでトレースの信頼度を確実なものにすることを提唱する。この概念を IoT デバイスにおける「RoT: Root of Trust」とする。また RoT に格納されるクレデンシャルとしての「Trust Anchor(固有鍵)」は、PKI のように電子的な証明の立証が連鎖した構造を持つ認証基盤を使うことにより、IoT デバイスのトレースには最も適していると考ええる。

● 「Trust Anchor」 と 「Root of Trust」 イメージ



これらの仕組みにより、IoT デバイスの製造～サービス運用～廃棄にいたるまでライフサイクル全体のトレーサビリティと真贋・真正性の証明を実現するトラストモデルを実現する。

●IoT 機器のライフサイクルマネジメント



今後、SIOTP 協議会では「標準化部会」を立上げ、今まで研究を進めてきた IoT セキュリティの実装手段に国際標準を精査した要素を加えて「SIOTP 協議会セキュリティチェックシート」を策定し、5 月よりまずは会員各社の保有する IoT 関連ソリューションを対象にセキュリティ実装の有効性評価を開始する。

3. まとめ

グローバル環境での大きな流れの中で、もはや我が国の製造業も、やるやらないという次元の問題ではなく、正しいセキュリティ実装を行わない限り、国際社会においてビジネス展開ができない時代に来ていることは明白である。

逆に日本の製造業の品質の高さは、グローバル環境においても大きな武器になり、世界をリードする立場になりうると確信する。Made in Japan の IoT デバイスは、グローバル市場において「世界で最も安全性が担保されている」ことが認識され、大きく成長するチャンスであり、SIOTP 協議会としても実装レベルでの仕様の作成や安全性評価の展開により日本製造業のさらなる成長に寄与したいと考える。