経済安全保障への対応
ハードウェア ルートオブトラストの重要性
についての考察

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

２０２２年1月

1. はじめに

近年、世界各国で発電所やプラント、石油パイプライン、食肉工場など国民生活や社会経済活動に大きな影響を与える重要インフラをターゲットにしたセキュリティ攻撃が多発している。以前より「重要インフラ 14 分野」と指定し、重点的に障害に対する対策を徹底し、持続的に安全な環境を実現することを目指してきました分野でもある。

発生時期	インシデント事例	概要
2021/5	コロニアルパイプライン	米国東海岸の50%の燃料供給を占めるコロニアルパイプラインがランサムウェアの攻撃を受け、6日の操業停止が発生。 米国の大動脈を狙われた為、社会的な大混乱に。 ロシアのハッカー集団「ダークサイド」による犯行。 ビットコインによる440万ドルの身代金が要求されたが、後日ほとんど回収。
2021/5	JBS	ブラジルの世界最大の食肉加工会社がランサムウェアの攻撃を受け、米国・豪州・カナダの向上が操業停止に。 サプライチェーンが分断され、価格が高騰し、社会生活に大きな影響が発生。 ロシアのハッカー集団「レビル（ソディノキビ）」が関与？
2021/2	フロリダ水道局	水道システムの管理システムがハッキングされ、水処理に使われる水酸化ナトリウムの濃度設定を通常時の100倍に設定された。 オペレーターが事前に気が付いたため事故にはつながらなかったが、住民に対する大きな健康被害につながる恐れがあった。

このような重要インフラをターゲットしたセキュリティインシデントの増大に対応するために、サイバーセキュリティの観点も「国家安全保障」から「経済安全保障」へ拡大しているように見受けられる。この動きをリードしている米国の動向をみると、安全保障に関する議論は超党派で進められており、民主党のバイデン政権に代わっても、続々と関連する大統領令の発布進められている。この動きは、当然米国だけではなく国際協調の中で進められている。

2. 経済安全保障を守る仕組み

経済安全保障に対する取り組みは日本においても進んでおり、岸田政権発足時にあらたに経済安全保障担当大臣のポストが制定され、小林鷹之大臣が就任されている。また「特許の公開制限」、「サプライチェーンの強靭化」、「先端技術の研究開発支援」、「重要インフラの安全確保」を骨子とする経済安全保障推進法案の制定が始まっており、また 2021 年 11 月 19 日には岸田首相を議長とする経済安全保障推進会議も開催され、2022 年の通常国会に経済安保推進法案の提出が予定されている。

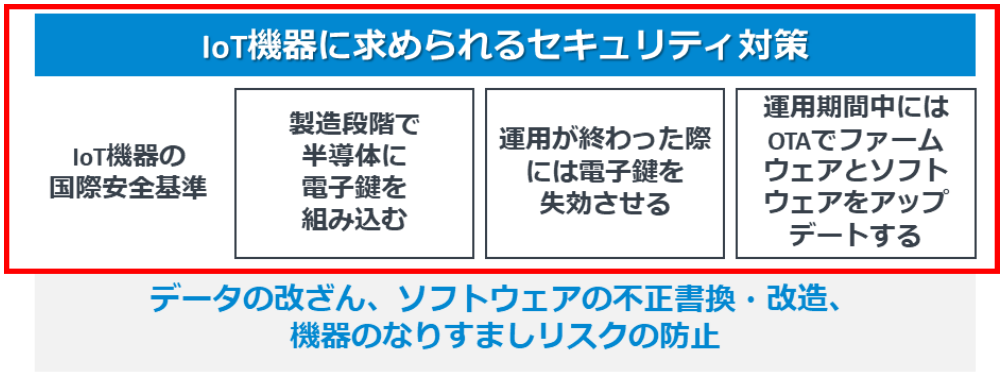
なかでも我々が注目しているのが半導体を中心とした「サプライチェーンの強靭化」である。あらゆる電子機器に使用される半導体不足により製造業に大きなインパクトが発生しており、あらゆる産業において製品開発や製品出荷の遅延など我々の経済活動にも大きな影響が出てきている。また各国とも半導体確保に動いており、我が国においても台湾 TSMC 熊本工場の誘致が報道されている。

現状においては、我が国のサプライチェーンの議論では未だ半導体の量の確保の議論が中心であるが、今後、国内、グローバル市場を問わず国際標準に適合させたルートオブトラストによるトラストチェーンの実装が可能な半導体が求められることになり、我が国とし

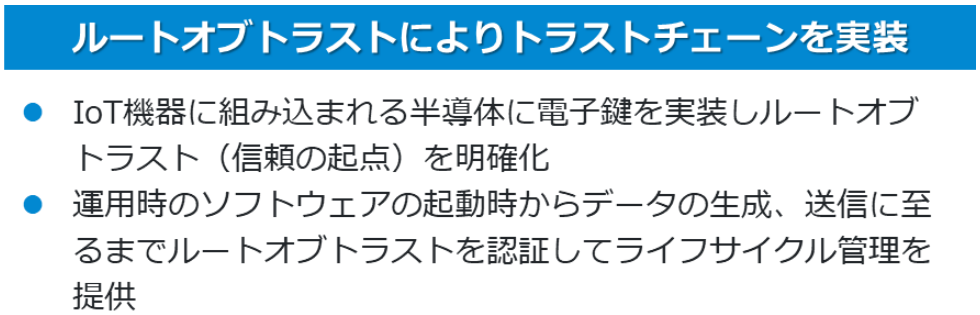
ても積極的に取り組むべきである事は間違いないと考える。

3. 経済安全保障に対する SIOTP 協議会の取組み

SIOTP 協議会では、経済安全保障を念頭においた安全な社会を実現するために、PKI に基づくトラストモデル構築を提唱している。このモデルにおいては、①IoT デバイスの真正性の確保と識別、②設計・製造から廃棄にいたるプロダクトライフサイクル管理、③適切なファームウェアアップデートをセキュリティ要件として満たすトラストチェーンの実装を実現する。



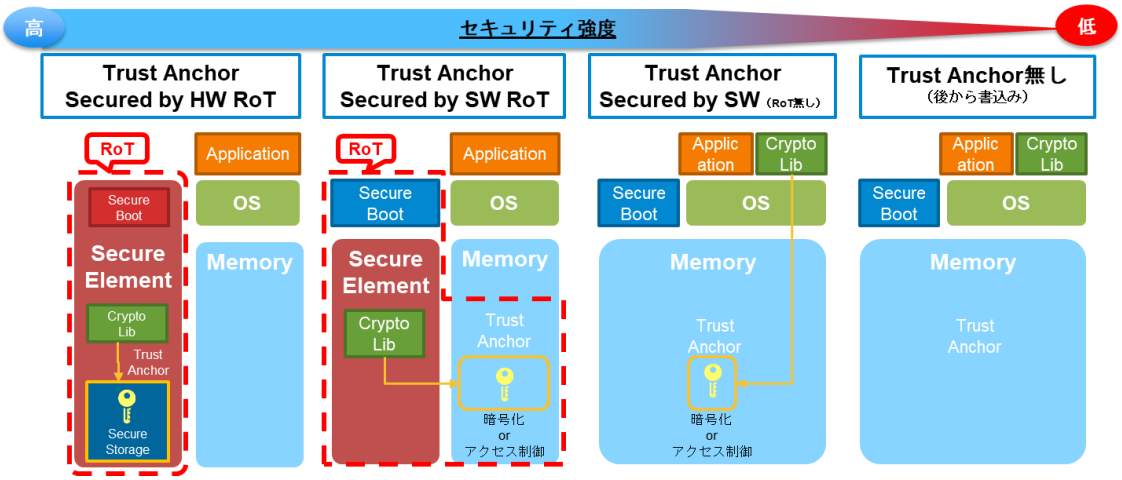
SIOTP 協議会では、ネットワークに接続される IoT 機器が組み立てられる前段階において必ず組み込まれる LSI（電子部品）、いわゆる IC チップに普遍的なクレデンシャルを埋め込むことでトレースの信頼度を確実なものにすることを提唱する。この概念を「ルートオブトラスト: Root of Trust（RoT）」とする。また RoT に格納されるクレデンシャルとしての「トラストアンカー：Trust Anchor（固有鍵）」は、PKI のように電子的な証明の立証が連鎖した構造を持つ認証基盤を使うことにより、IoT デバイスのトレースには最も適していると考える。



経済安全保障を考えると、高度なセキュリティが求められる重要インフラにおいては、ここで説明したような、よりセキュリティ強度が高いハードウェアレベルでのルートオブト

ラストの実装が望ましいと考える。

●「トラストアンカー」と「ルートオブトラスト」のイメージ



尚、これらの暗号モジュールに関するセキュリティ要件は、NIST（National Institute of Standards and Technology：米国国立標準技術研究所米国連邦標準規格）が制定するFIPS140-3（SP800-140）で仕様が定義され、事実上の国際標準として注目されている。。

4. まとめ

昨今の重要インフラや産業機器などをターゲットにした攻撃が増え、経済安全保障を脅かす状況が増加している。そのため重要インフラを守り、経済安全保障を確保するためには、半導体サプライチェーンを議論する際には、供給量の確保という視点だけではなく、半導体の実装する機能にも着目し、重要インフラに対応するセキュリティ要件が実装されている半導体の開発や製造にも目を向ける必要があると考える。