経済安全保障への対応
～国際安全基準へ適合したセキュリティ対応とは～

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

２０２４年 ４ 月

1. はじめに

国際状況の状況変化に伴い、ネットワークに接続される機器やサービスにおいて法令化が進み、国際安全基準が各国の調達基準に適用され、義務化の流れが明確になってきた。
国内においてもこの動きと同調する形で、経済安全保障に対する動きが活発化してきた。
今回はその動向と具体的な対応策について考察を行った。
また当協議会では過去にも経済安全保障をテーマに様々な考察を発行してきたので、参考にして欲しい。

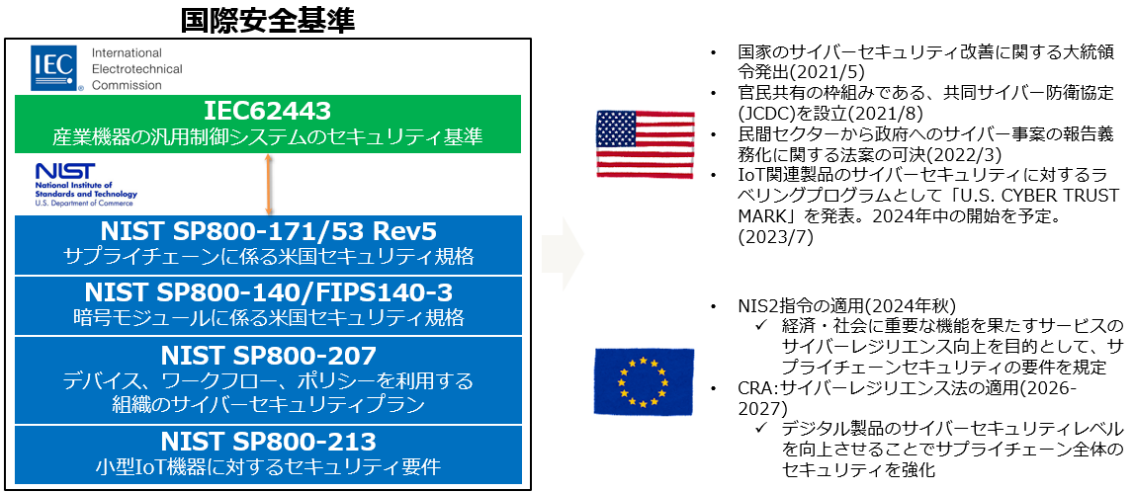
日付	タイトル	URL
2022/1/14	経済安全保障への対応： ハードウェア ルートオブトラストの 重要性についての考察	https://www.secureiotplatform.org/static/images/report_20220114.pdf
2022/4/25	経済安全保障への対応：～日本製造業に向けて～	https://www.secureiotplatform.org/static/images/report_20220425.pdf
2022/8/25	経済安全保障への対応 ～オープンソースセキュリティの動向～	https://www.secureiotplatform.org/wp-content/uploads/report_20220825.pdf
2022/11/22	経済安全保障への対応 ～次世代半導体開発への期待～	https://www.secureiotplatform.org/wp-content/uploads/report_20221122.pdf
2023/1/12	経済安全保障への対応 ～国際連携におけるサイバーセキュリティ対策の推進～	https://www.secureiotplatform.org/wp-content/uploads/report_20230112.pdf
2023/5/15	IoTセキュリティ観点におけるChatGPTに対する考察	https://www.secureiotplatform.org/wp-content/uploads/report_20230515.pdf
2023/6/21	FIPS140-3を取り巻く環境に対する考察	https://www.secureiotplatform.org/wp-content/uploads/report_20230621.pdf

2. 海外の動向

バイデン政権はサイバーセキュリティを国家安全保障にかかわる最優先事項と位置付け、国際協調のもと、大統領令を発布してきている。
また 2024 年中には、IoT 関連機器に対する、サイバーセキュリティ対応を認証・明示するラベリングプログラムとして「U.S. CYBER TRUST MARK」の開始が予定されている。

また欧州においてはサイバーレジリエンス法(CRA)の適用が迫ってきており、その前段となる NIS 2 指令が今年度からスタートする。特に CRA においては欧州でビジネスを行う上では適合が義務付けられ、高額な罰則規定まで設けられている。

いよいよ IEC62443 や NISTSP800 シリーズなどの国際安全基準が各国の調達基準に採用され始めてきており、日本の経済安全保障で求められるセキュリティ要件についても、国際安全基準への準拠が求められ始めている。



3. 国内の動向

日本においても海外の動きと同期をとって、経済安全保障にかかわる動きが加速してくることが予想される。

例えば、2024 年 2 月 16 日に「特定社会基盤事業者」が公示され、具体的に重要インフラ事業者が特定された。
https://www.cao.go.jp/keizai_anzen_hosho/infra.html
https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_jigyousya.pdf

また 2024 年 2 月 27 日には「重要経済安保情報の保護及び活用に関する法律案」が閣議決定し、国会に提出され、セキュリティークリアランス(適性評価制度)の創設の議論が開始され始めたところである。
https://www.cas.go.jp/jp/houdou/240227keizaianzenhosyo.html

さらに経済産業省では 2024 年 3 月 15 日に IoT 機器のラベリング制度となる「IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会最終とりまとめ」が発表され、今後パブリックコメント募集を経て、2024 年度中に一般コンシューマ機器を対象とした☆1 から、ラベル付与が開始される予定である。
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240315_report.html

4. 重要インフラに求められるセキュリティ要件

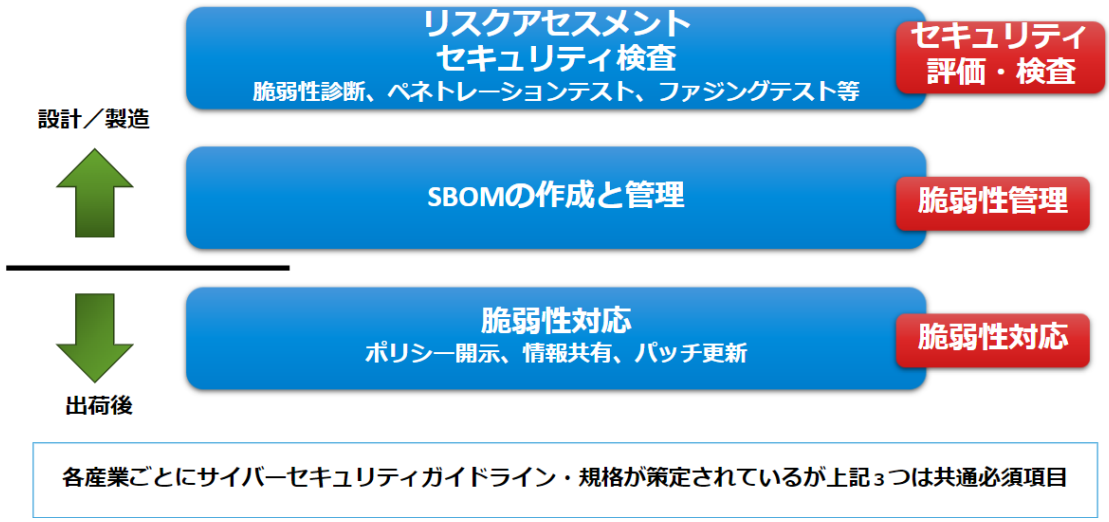
そのため重要インフラ、政府調達案件で使用されるシステムを中心に、国際標準に準拠した対策が急務となってきている。

具体的には、①PKI ベースの電子認証による識別とアクセス制御、②機器認証のための厳格な鍵管理、③セキュアアップデートなど安全な運用支援のための脆弱性管理の仕組みの実装が求められる。

これは当協議会が一般社団法人組込みシステム技術協会(JASA)と共同で推進する「セキュア IoT プログラム」の検証項目として掲げている要件とも合致する。
また長期的な運用を視野に入れたシステムの選定も重要である。いまや重要インフラにおいても当たり前に使用されるオープンソースにおいては、長期的にサポートが提供されることが重要となってきている。

5. 必要となる対策

ここでは日本の製造業が業界横断で実施すべき対策を考える。
設計製造から運用に至るまでのライフサイクル全体の安全性を確保することを考えると、以下の 3 点必要となる。



まず設計/製造段階において、製品やサービスに脆弱性が含まれていないことを検査し、確認することが必要である。そのために設計・製造時において、セキュリティ検査(脆弱性診断、ペネトレーションテスト、ファジングなど)を実施し、リスクアセスメントを行うことが必要である。

さらに国際的なセキュリティ規格に適合するためにも SBOM(Software Bill Of Materials: ソフトウェア部品表)を整備することが必須となる。

出荷後においては、新たに見つかった脆弱性に迅速に対応するために、セキュリティポリシ

ーの開示、情報開示、パッチの更新など脆弱性管理が求められる。

6. 具体的な対策

セキュリティベンダー各社からもセキュリティ検査や脆弱性管理についてサービス提供が開始されている。
ここでは参考として、当協議会のセキュア IoT プログラムに検査機関として登録している会員企業のサービスを紹介する。

・サイバートラスト株式会社
https://www.cybertrust.co.jp/iot/iot-security-consulting.html

・株式会社 SYNCHRO
サイバーセキュリティ対策センター（CSCC）
https://www.udc-synchro.co.jp/service/cscc/

・ベルウクリエイティブ株式会社
https://belue-c.jp/

7. まとめ

いよいよ国際安全基準への対応について、国内外の動きが具体化し、調達要件に採用され、義務化の動きが出てきた。しかし製造業の皆様にとっては、自社の製品やサービスがその要件に適合しているかどうかわからない/またどのように対応したらよいか不明という点が課題であった。

それに対する回答として、各社よりそれに対応するセキュリティ診断や脆弱性管理サービスがリリースされている。ぜひ皆様のビジネスを維持拡大するためにも、ぜひこのようなサービスを活用して欲しい。