IoTセキュリティWGのご紹介
～ 絶賛メンバー募集中 ～

2025年 7月23日

IoT セキュリティWGの活動を振り返る

2014年～2024年までの活動の振り返り

2014年4月に発足

［目的］

IoTの市場調査・アーキテクチャとセキュリティ範囲検討・脅威の洗い出しと調査と報告書の取りまとめ

［市場調査］

- 対象となる領域（ネットワーク接続可能な機器）があまりにも広すぎることが当初から課題に
- ひとまず、アーキテクチャとセキュリティ範囲について、先達の成果物を参照（IoT-A Project, OWASPなど）することから整理を進める。

https://www.iot-a.eu

https://owasp.org/www-project-internet-of-things/

2016年、ガイドを発行

- 「コンシューマ向け」としたのは、業務用や産業用など、企業や社会インフラで利用されるIoT製品は、産業用制御システム向けのISO/IEC62443 といった国際規格などの登場により、サイバーセキュリティ対策の標準化が行われ始めていたことや、国内ではNISCを中心とした業界団体と監督官庁によるサイバーセキュリティ対策への取り組み（セプターカウンシル）が始まっていたことから、それらの業種の製品は除外することとし、サイバーセキュリティが求められているものの十分な対処が困難な、コンシューマ向け製品の開発者や利用者に向けたガイドとなることを目指した。
- 10年を経た現在、英国のPSTI、EUのCRA、米国のCyber Trust Mark、日本ではIoTラベリングなどの取り組みが端緒についたばかりで、問題は山積したまま。

http://www.jnsa.org/result/iot/

他の文書には無い視点を導入

ライフサイクルについて
＊ベンダーの製品提供と保証

製品保証期間 → セキュリティ更新の提供期間

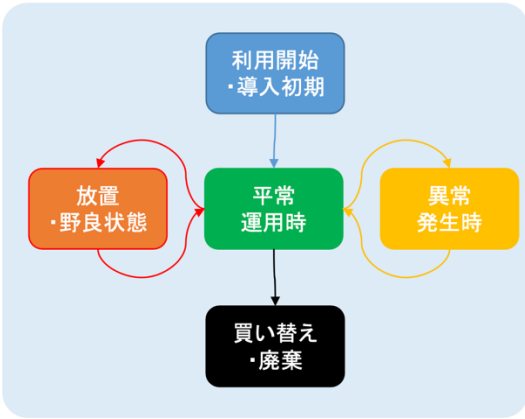
- 個人向け IoTデバイスは、任意の利用目的で所有、利用するものであるため、製品の保証期間をベンダーが定めたとしても実際に稼働する期間を厳密に定義することはできない
- このため、セキュリティ含め、安全に利用することのできる期間を設定する必要がある
- 上記の「製品保証期間」は製品の保証を提供する期間で、製品の不具合（ハードウェアの材質上や製造上の瑕疵など）について保証を提供する期間は、通常1年程度とされる
- 「セキュリティ更新の提供期間」とは、製品保証期間を過ぎてもユーザーが使い続けることを想定し、製品に対するセキュリティの更新を提供する期間である
- この期間を過ぎた場合ユーザーには「廃棄」することを勧めるなどの対応が望ましいと考えられる

※経済産業省ではベンダー（事業者）に対して「製品安全に関する事業者ハンドブック 」を発行している

http://www.meti.go.jp/product_safety/producer/jigyouhandbook.pdf

ライフサイクルについて
＊ユーザーによる製品の利用

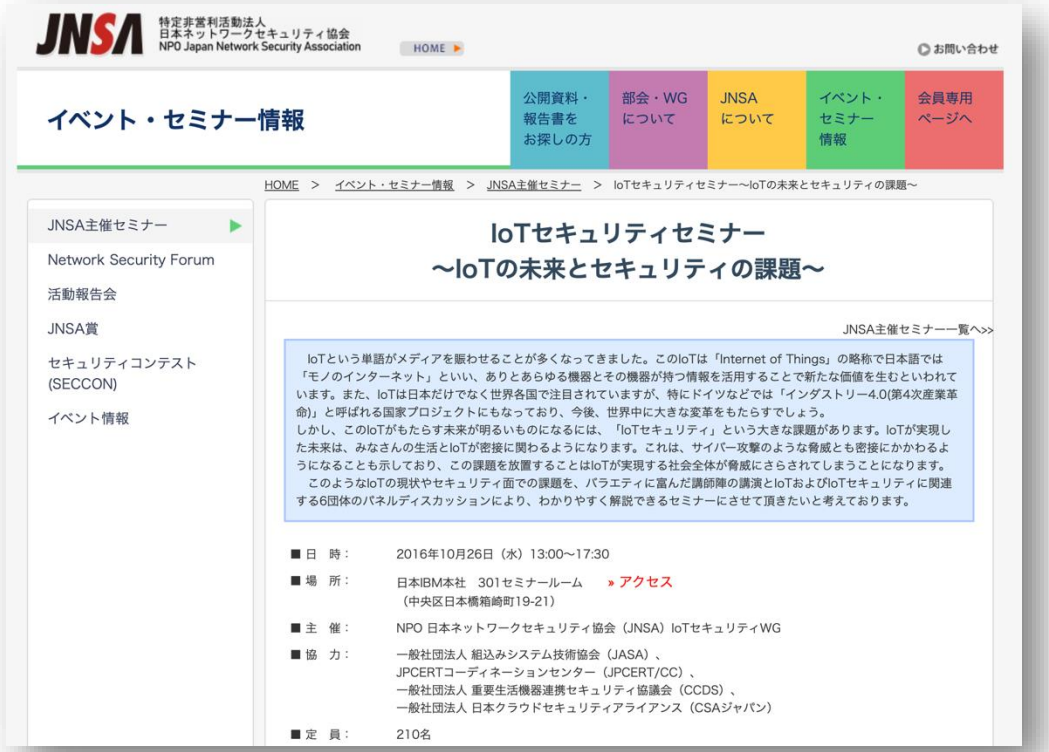
- 利用開始の際に、デバイスの導入設定がユーザーにとって複雑でなく、初期設定に必要な情報などを第三者が再利用することのできない仕組みを提供することが望ましい。
- 利用を開始した後、デバイスに異常が発生した場合、異常を解消して復旧する必要がある
- 利用開始後、長期間にわたって使用せずに稼働させたまま放置することで第三者がデバイスにアクセスすることが可能な状態を「野良」と呼ぶが、セキュリティ上は好ましくない。
- デバイスが不要となる場合には、記録・保存されたデータの消去や初期化についての手順が準備され、ユーザーが対処するか、ユーザーが対処せずともよいような仕組みがあることが望ましい



2016-17年、ガイドの認知度向上と啓蒙活動

2016年10月26日

IoTセキュリティセミナー　～IoTの未来とセキュリティの課題～ の開催



https://www.jnsa.org/seminar/2016/1026/index.html

https://xtech.nikkei.com/it/atcl/column/17/052900219/

2018年、ハンドブックを作成・公開

- 2016年に「コンシューマ向け IoTセキュリティガイド」を公開した後、世界ではIoTセキュリティに関連する様々な文書が公開され、国際的な標準化の動きもある中、WGとして新しいガイドの作成ではなく、発行された大量の文書の要点をまとめ、文書の概要を把握する助けとなるハンドブックを作成、公開した。

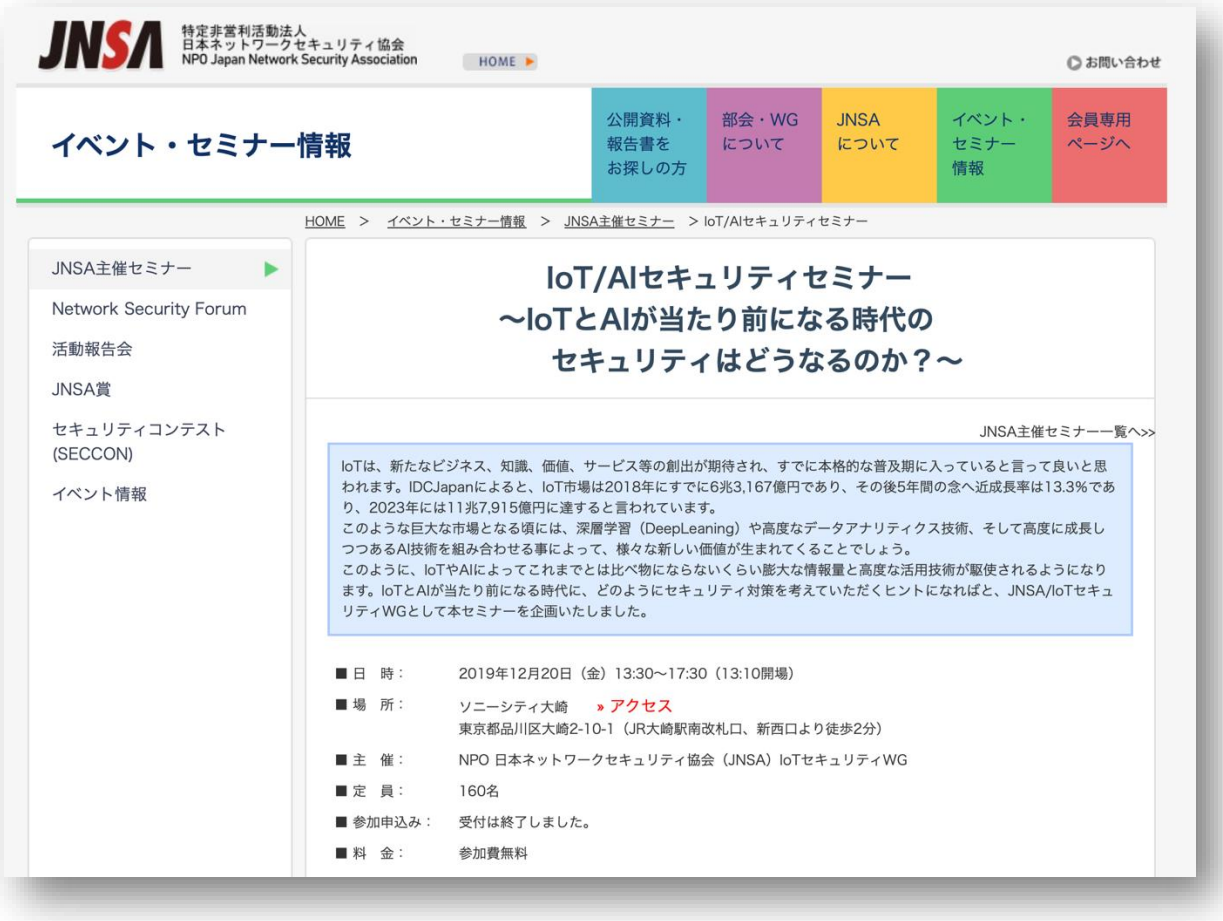
本ハンドブックに掲載しているガイドライン等の一覧

No	組織	名称
1	DHS	STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS
2.1	ENISA	Security and Resilience of Smart Home Environments
2.2	ENISA	Security and Resilience of Intelligent Public Transport. Good practices and recommendations
2.3	ENISA	Cyber security for Smart Cities
2.4	ENISA	Cyber security and resilience for Smart Hospitals
2.5	ENISA	Securing Smart Airports
2.6	ENISA	Cyber Security and Resilience of smart cars
2.7	ENISA	Baseline Security Recommendations forIoT
3	FTC	Internet of things Privacy & Security in a Connected World FTC Staff Report JAN 2015
4	IETF	Best Current Practices for Securing Internet of Things (IoT) Devices
5	IIC	Industrial Internet Security Framework
6	IoT推進コンソーシアム	IoTセキュリティガイドライン
7.1	IPA	IoT開発におけるセキュリティ設計の手引き
7.2	IPA	つながる世界の開発指針
7.3	IPA	安全なIoTシステムのためのセキュリティに関する一般的枠組
8	ISACA	INTERNET OF THINGS：RISK AND VALUE CONSIDERATIONS
9	ITU-T	Y.4806
10	NIST	SP800-160 Systems Security Engineering
11	OTA	IoT Trust Framework(V2)
12	OWASP	OWASP IoT Security Guidance

https://www.jnsa.org/result/iot/2018.html

2019年、IoT周辺の新しい技術「AI」の調査

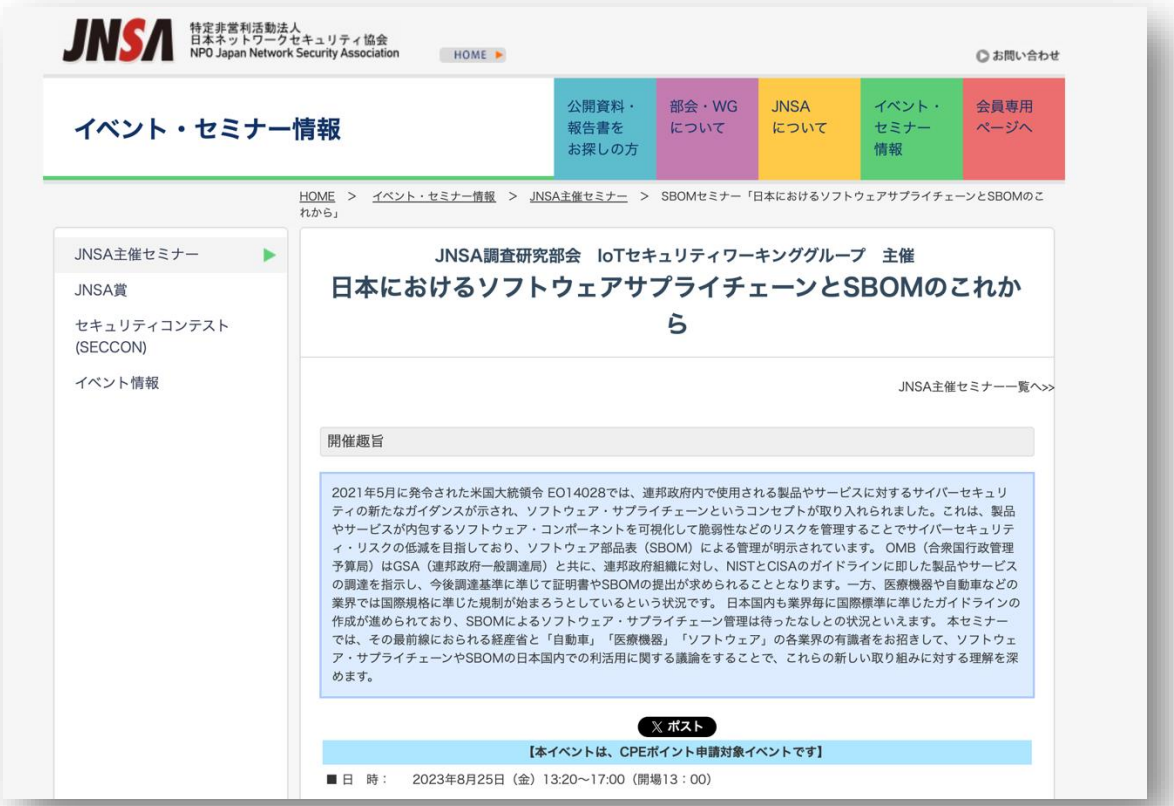
- AI技術のコンシューマ製品での採用が増加傾向にある中、IoTとの組み合わせによる新たなリスクの登場に関して専門家の意見を伺う機会としてのセミナーを実施した。



https://www.jnsa.org/seminar/2019/1220/

2023年、「SBOM」の調査

- 2021年の米国大統領令EO14028以降、FDAの市販前申請、EUのCyber Resilience Actなどで明示され、提出が求められるソフトウェア部品表（SBOM）は、技術的な成熟度が高く無いにものの、脆弱性をソフトウェアのリスクをサプライチェーン上で共有するための手段として急速に利用が拡大しつつある。
- そこで、他業界に先行してSBOMの検討と採用が進みつつある自動車業界と医療機器業界、そしてSBOMの採用を推進する経産省からご講演いただいた。



https://www.jnsa.org/seminar/2019/1220/

そうです、IoT製品は規制の対象です

- 2027年から施行されるEU CRAによって、デジタル要素を備えた製品（Products with Digital Elementsと総称されるソフトウェアおよびハードウェア）に対する規制が始まる。

- 2023年、米国FDAのガイダンスによる医療機器に対する規制、UNR-155/156では2022年から段階的に自動車に対する規制が、その他にも5G、ICSなどは業界や利用分野に応じた規制が始まりつつある。

- 要点は、ソフトウェアの透明性（製品によってはハードウェアも）を担保するための「SBOM」、リスク分析を始点とするセキュリティテスト、脆弱性報告などの要求がおよそ全ての業界で求められる。

2023年、セミナー登壇者

経済産業省 商務情報政策局 サイバーセキュリティ課

飯塚 智 様

一社） Japan Automotive ISAC 技術委員会 委員長

山﨑 雅史 様

一社） 電子情報技術産業協会 ヘルスケアインダストリ部会　医療用ソフトウェア専門委員会 委員長

松元 恒一郎 様

一社） ソフトウェア協会 Software ISAC 副委員長

鈴木 康弘 様

セミナーで何が議論されたか？

- なぜSBOMを導入するのか？
- SBOMをどのように導入するのか？
- 医療機器、自動車の各業界で苦労していること。
- 既存の資産や製品をどうするのか？
- サイバーセキュリティの専門家が足りないことの問題。
- サプライチェーンにおける契約の問題でもある。

EU CRA：欧州市場と消費者の保護

- EU CRA はデジタルコンポーネントを備えたソフトウェアまたはハードウェア製品を購入する消費者と企業の保護を目的としている。

- この規制は、既存の規則で既にカバーされている特定のオープンソースソフトウェアまたはサービス製品（医療機器、航空機、自動車など）を除き、他のデバイスまたはネットワークに直接的または間接的に接続されるすべての製品に適用される。

- デジタルコンポーネントを含む製品のサイバーセキュリティ基準を強化し、製造業者と小売業者に製品のライフサイクル全体にわたってサイバーセキュリティを確保することを義務付けている。

EU CRA：主な要求事項1/2

- 製造業者は、脆弱性分析を容易にするためにSBOMを作成するなど、製品に含まれるコンポーネントを特定して文書化する必要がある

- 製造業者は、第三者からの直接的・間接的な脆弱性の報告を容易にするために、脆弱性開示ポリシーを導入する必要がある

- 製造業者は、製品に含まれる積極的に悪用された脆弱性を認識した場合、コーディネーターとして指定されたCSIRTとENISAに、不当な遅延なく、いかなる場合も製造業者が認識してから 24 時間以内に同時に通知する

EU CRA：主な要求事項2/2

- 製品の設計・開発段階で、サイバーセキュリティ機能を考慮する義務があり、サイバーセキュリティ対策を製品開発プロセスに組み込み、効果的かつ定期的なテストとレビューを適用する必要がある。

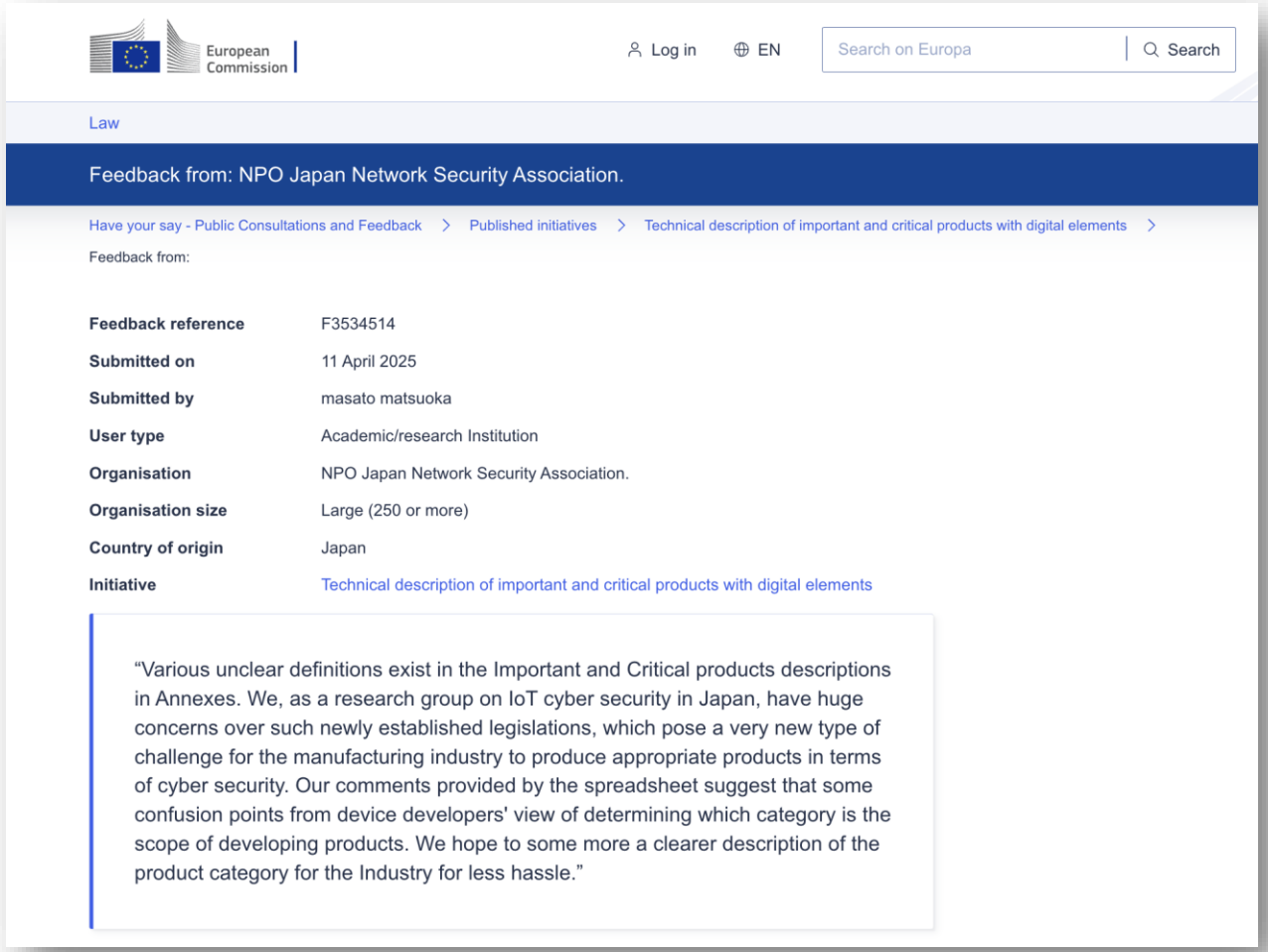
- 設計およびデフォルトのセキュリティ、リスク管理、インシデント管理、個人データの保護（GDPRと密接に関連）に関連する規定を含む、CRAで指定されたセキュリティ要件を製品が満たしていることを確認する必要がある。

- 製品の使用条件に基づくサイバーセキュリティのリスク分析を含むリスク評価を文書化。

2025年、 EU CRA Draftへのコメントの送付

- JNSA名で、製品カテゴリーの記述への修正を２点送付

- 採択については12月に発行される技術要件などの内容を読み解く必要がある



European Commission | Log in | EN | Search on Europa | Search

Law

Feedback from: NPO Japan Network Security Association.

Have your say - Public Consultations and Feedback > Published initiatives > Technical description of important and critical products with digital elements >

Feedback from:

Feedback reference	F3534514
Submitted on	11 April 2025
Submitted by	masato matsuoka
User type	Academic/research Institution
Organisation	NPO Japan Network Security Association.
Organisation size	Large (250 or more)
Country of origin	Japan
Initiative	Technical description of important and critical products with digital elements

"Various unclear definitions exist in the Important and Critical products descriptions in Annexes. We, as a research group on IoT cyber security in Japan, have huge concerns over such newly established legislations, which pose a very new type of challenge for the manufacturing industry to produce appropriate products in terms of cyber security. Our comments provided by the spreadsheet suggest that some confusion points from device developers' view of determining which category is the scope of developing products. We hope to some more a clearer description of the product category for the Industry for less hassle."

IoTの課題、一緒に調査研究を！

国際法規、SBOM、ガイドライン、ラベリング制度、サイバーセキュリティ対策、業界動向などについて、

インタビュー、調査レポート、セミナー、勉強会など、

やりたいことやアイデアを持ち込んで一緒に実現しましょう！