セキュアIoTプラットフォーム協議会

標準化部会活動報告

2026/02

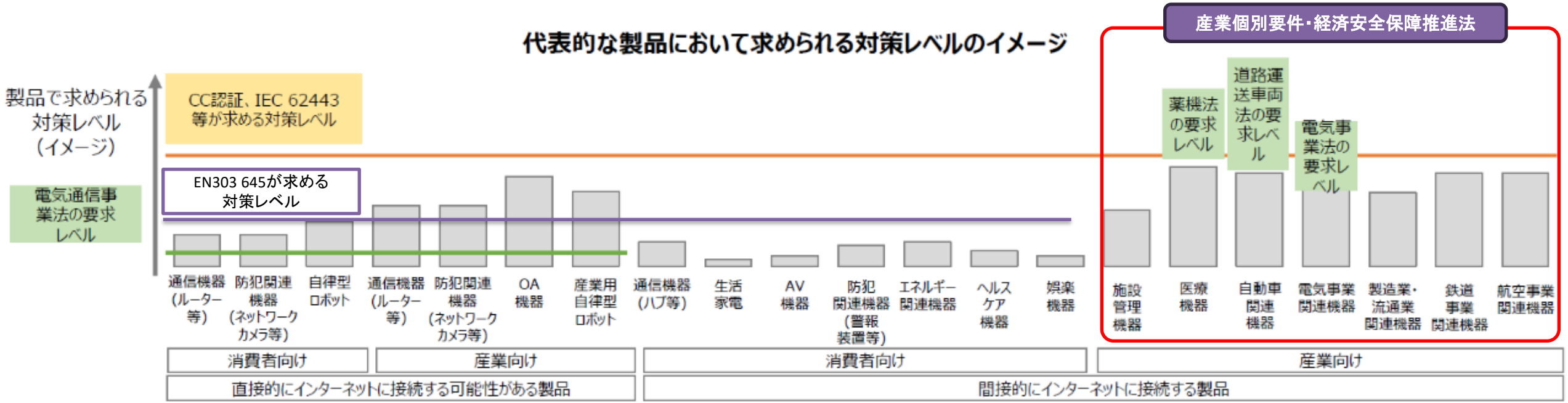
セキュアIoTプラットフォーム協議会　標準化部会
座長　山澤　昌夫

欧米英における主なセキュリティ標準／規制（2026年1月時点）

主要各国にてサイバーセキュリティ標準／規制が策定され、相互承認する方向（各国共通規定）

国、地域	標準／規制	主な対象	運用開始	備考
	**PSTI 法**	消費者向け、且つ インターネット接続可能な （有線/無線)製品	**2024年4月29日～開始**	ETSI EN 303 645
	**サイバーレジリエンス法 （CRA）**	デジタル要素を含む ソフトウェア、ハードウェア製品	**2027年12月全面施行予定**	ETSI EN303 645 IEC62443
	**NIST SP800s**	デジタル要素を含む ソフトウェア、ハードウェア製品	**-**	NIST SP800-171 NIST SP800-53 NIST SP800-207
	**JC-STAR**	消費者機器向け☆1から重要インフラ☆4まで 4段階に分けて制度設計	**2025年3月～☆1開始 ☆2以上順次開始予定**	**英PSTIと相互承認開始**

民生品・産業製品それぞれのセキュリティ標準規格の対策レベル



国際協調で進むサイバーセキュリティ規制規制（各国のラベリング制度）

- **日本：JC-STAR（EN303 645相当）★１が運用スタート / ★3順次整備**
- **米国： NIST SP800-171･53 、**Cyber Trust Mark（NIST SP800-213 / NIST IR 8259）
- **欧州：CRA（EN303 645 / IEC 62443） ※罰則規定あり**

各国とも同等のサイバーセキュリティ規制を準備中
欧州のCRAが最も厳しい規制になると考えられる。

経産省　IPA　JC-STAR

経済産業省が運用を開始したJC-STARは、共通的な物差しでIoT製品に具備されているセキュリティ機能を評価・可視化し、政府機関、民間企業から一般消費者まで、IoT製品の購入者・調達者が、本制度のラベルを確認することで、**自らが求めるセキュリティ水準の製品を容易に選択できるようにすること**を目的としています。現時点では★１が開始され、★２以降が今後、順次公開される予定です。

■今後、製造業者に求められること
- 自社製品の適用吟味
  →通信機能の有無
  →組み込み資材としての判断
  →消費者への対応
- 適合レベルの判断
- 認証取得に関するコスト算出　等

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html

SIOTP協議会：「セキュアIoT認定プログラム」について

IoTの脆弱性に起因するセキュリティ事故を未然に防ぐために、大企業から中堅・中小企業にいたるまで、IoTシステムの製造事業者、運営事業者に対する脆弱性検査の普及促進が重要だと考えます。

そこでセキュアIoT協議会では、検査を受ける動機づけとなる「認定」を付加価値要素とする、セキュリティ検査の仕組み「セキュアIoTプログラム」をリリースし、我が国における脆弱性検査の普及に貢献します。

今回のプログラムでは、IoTシステムの脆弱性の有無を確認する「脆弱性検査およびIoTセキュリティ検査」に加えて、その検査結果をもとに特に重要と考える以下の3項目において国際標準(IEC62443)への適合性を確認する「セキュアIoT認定」を組合わせて提供します。

【検査ポイント】

■ライフサイクル管理

- **真正性の担保と識別 (耐タンパ：鍵管理)**
- **認証と識別 (設計・製造、利用、廃棄、リサイクル)**
- **セキュアアップデート (OTA：Over The Air)**

セキュアIoT認定

本プログラムでは、産業用システムや業務システムを中心に、最終的なIoT機器だけではなく、IoT機器を構成する部品やソフトウェア、システムも認定対象とします。

ご清聴ありがとうございました。