セキュアIoTプラットフォーム協議会
標準化部会

2025年2月18日

標準化部会活動状況

- IoT機器、システムのセキュリティ認証活動を推進している
  - 2021～2023においてIoT機器セキュリティ認証プログラムを発足、
    認証活動を行ってきた。
  - 2024年度からは、活動を産業機器・システムに向けて事例拡大する方向
    産業機器・システムに向けて、鋭意検討中：ー参加奨励ー

具体的状況

ーJASA連携の一層の推進⇒「認証/認定プログラム」の『産業機器・システム』への拡大を図るに当たって、
実地検証のテストベッド協力会社を増やす目的

ーIPA神田委員会への協力⇒4月初に打診あったが、その後接触ない。

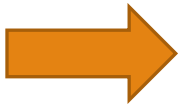
ーデータライフサイクルマネジメント部会発足（推進協力）

ー国際状況の変遷ありー

アクションアイテム

○標準化委員会メンバーの再募集（JASAメンバー、SIOTPメンバー、連携団体・・・）

○脱旧CCの素案
　□制度運用のモディファイ、
　□認証の達成セキュリティレベルのメリハリ
　□上記を一般に共有するためのたたき台



62443ベースのチェックシート（松本版）を元に
　＝制度運用・・・・年限と更新項目
　＝CCとの差異

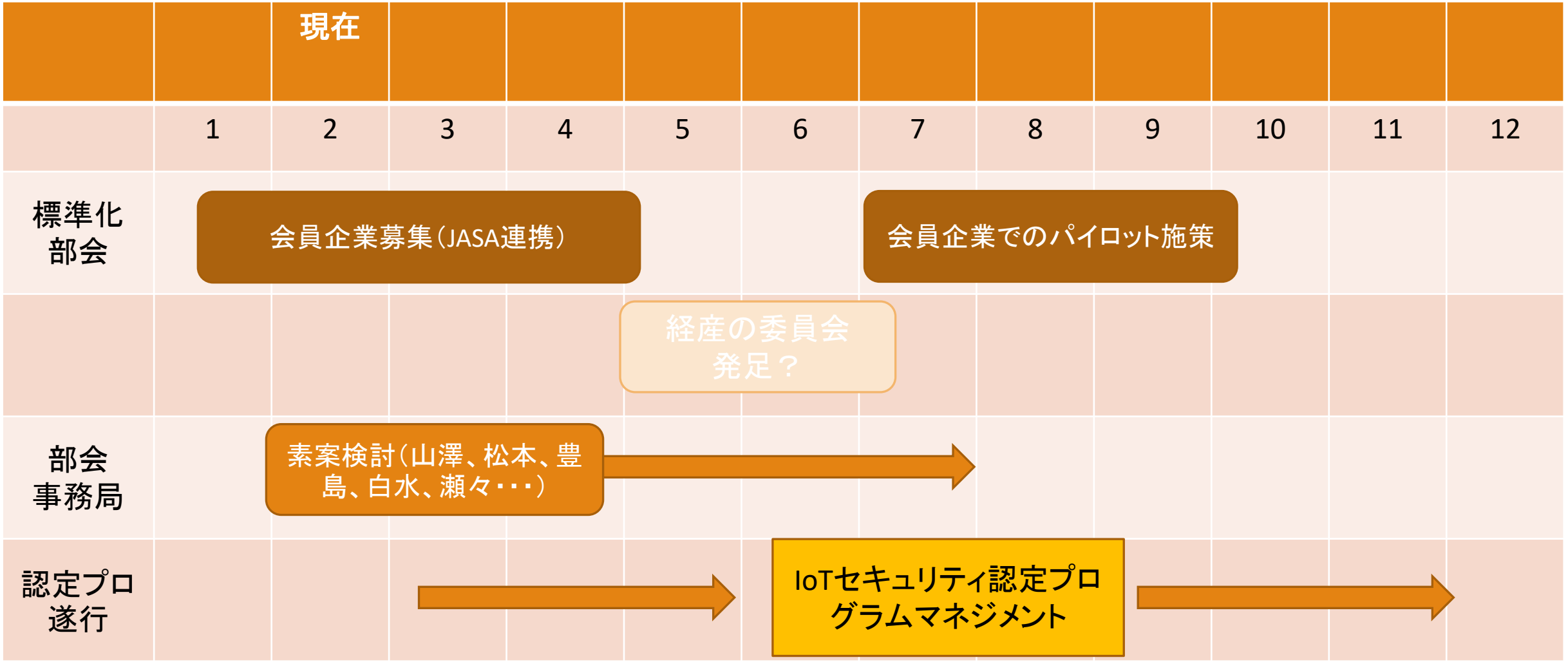
アクションアイテム（続き）

○産業用システム分野における仕様策定のポイント（再掲）

□耐タンパ(鍵管理）、
□ライフサイクル管理(設計・製造、利用、廃棄、リサイクル、データ)
□セキュアアップデート(OTA：Over The Air)

62443ベースのチェックシート（松本版）を元に
＝制度運用・・・・年限と更新項目
＝CCとの差異

標準化部会の年間計画（案）



以上

継続調査アイテム

○標準規格類の調査

- NIST SP800-171,172,53,63,218 etc　:設計、製造、製品、サービスへの適応
- NIST CSF2.0　:組織、サービスへの適応
- CMMC1.0,2.0　:組織、製品、サービスの適合監査
- IEC62443　:工場ラインへのセキュリティマネジメント構築、機能実装

関連法規やガイドライン、諸外国のセキュリティ標準など製造業に求められるセキュリティは多種にわたります。
また、製品へのセキュリティ実装やラインセキュリティへの要求事項も多様です。
標準化部会では、企業や工場におけるセキュリティマネジメントから、IoTセキュリティの製品実装など国際安全基準への対応に関し幅広い情報の収集を継続していきます。

部会活動：標準化部会　IoTセキュリティチェックシート

IEC62443-4-2 check sheet

Target:

classification: ☐H/W ☐S/W ☐cloud system ☐component

Date:

Time:

FR　1 Identification and authentication control (IAC)

SL	原文	和訳	✓	選択理由
SL 1	Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against casual or coincidental access by unauthenticated entities.	簡易な手法もしくは偶発的な不正アクセスから保護		
SL 2	Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.	少ない設備、汎用スキル、低モチベーションの単純な手段を使用した、意図的な不正アクセスから保護		
SL 3	Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.	適度な設備、IACS固有のスキル、悪意のある意図的な不正アクセスから保護（標的型攻撃）		
SL 4	Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.	大規模な設備とIACS固有のスキル、悪意のある意図的な不正アクセスから保護		

SL-C1	CR 1.1
SL-C2	CR 1.1 (1)
SL-C3	CR 1.1(1)(2)
SL-C4	CR 1.1(1)(2)

	要件	和訳	✓	選択した理由	エビデンス
CR1.1	**Human user identification and authentication** Components shall provide the capability to identify and authenticate all human users according to IEC 62443-3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.	**人間のユーザーの識別と認証** コンポーネントは、人間がアクセスできるすべてのインターフェースで、IEC 62443-3-3 SR1.1に従ってすべての人間のユーザーを識別および認証する機能を提供するものとします。この機能は、コンポーネントへの人間のユーザーアクセスを提供するすべてのインターフェイスでそのような識別と認証を実施し、適用可能なセキュリティポリシーと手順に従って職務の分離と最小特権をサポートします。この機能は、コンポーネントによってローカルに提供されるか、システムレベルの識別および認証システムに統合されることに			

「IoTセキュリティ手引書」の
内容をチェックシートに整理
「システム」の構築、運用
のセキュリティ付与の指針に

チェックシートにおける
適用先と
Security Levelの規準

「データ」、「データマネジメント」の真正性

データとデータマネジメントについて、IoTプラットフォームでの考え方を整理し、これまで重視してきたセキュアIoTプラットフォームに関わる国際規格に基づいたライフサイクルマネジメントの考え方（文献[1]）を適用、真正性保証を含んだオペレーション標準化に資することを考える。

[1]セキュアIoTプラットフォーム協議会，「IoTセキュリティ手引書 Ver3.0」，令和5年9月26日．

国際情勢：

STRATEGIC OBJECTIVE 3.2: DRIVE THE DEVELOPMENT OF SECURE IOT DEVICES

この結果、米国はU.S. Cyber Trust Markプログラムを2024年8月末に開始。（NISTのラベリングガイドライン依拠）、他国、シンガポール（Cybersecurity Labelling Scheme）、英国（PSTI法）、EU（CRA法）についてもプログラム運用中。連携、相互認証に向けて国際交渉中（https://www.newton-consulting.co.jp/itilnavi/flash/202410_06.html）

国際情勢：続

STRATEGIC OBJECTIVE 4.1: SECURE THE TECHNICAL FOUNDATION OF THE INTERNET

DNSSEC、RPKI、HTTPS、IPv6

STRATEGIC OBJECTIVE 4.5: SUPPORT DEVELOPMENT OF A DIGITAL IDENTITY ECOSYSTEM

デジタルアイデンティティ
プラットフォーム