セキュアIoTプラットフォーム協議会

セキュアIoTプログラムについて

2024年3月6日(水) 16:05～16:20

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**
副座長　**松本　義和**

標準化部会のご紹介

- 標準化部会：なにを目指すか
  - 対象：**産業用システムや業務システム**を中心に、最終的なIoT機器や、IoT機器を構成する**部品やソフトウェア、システム**を対象。
  - 活動：仕様検討部会でまとめた「IoTセキュリティ手引書」の実装性を検証し「標準的プラクティス」を作成する活動。
  - 社会貢献：「セキュアIoTプログラム」の発信、遂行。
    - **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)**

IoTセキュリティ：とりまく状況

- セキュリティリスク
  - 個体数、管理問題、ネットワーク化、不正アクセス、BOT化問題・・・
- セキュリティガイドライン
  - ＮＩＣＴ、総務省、ＩＰＡ、医療情報システム・・・
- セキュリティ基準
  - ISO/IEC・・・、NIST・・・、ENISA・・・
- 法規制
  - サイバーセキュリティ基本法、技適・・・
- 認証プログラム・・・
  - CC、技適、CCDS機器認証・・・・

IoTセキュリティ：とりまく状況：補足

- 認証プログラム・・・
  - CC、技適、CCDS機器認証・・・

- 経産省の

『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』

2023年度　標準化部会　活動状況

- 2022年度末～2023年度初頭
  - セキュアIoTプログラムを開始
  - 「セキュアIoT認定(Gold)」をサイバートラスト、SYNCHROの2社/6件に授与 <https://japansecuritysummit.org/2023/02/6256/>
- 2023年度初頭~
  - セキュアIoTプログラムプロモーション
  - JASA（一般社団法人組込みシステム技術協会）との協業調整

「セキュアIoTプログラム」推進の背景認識

- ネット上のIoTシステムの脆弱性を基点にしたサイバー攻撃が増加。
- 経済安全保障の議論においても「サプライチェーンの強靭化」や「基幹インフラ安全性強化」がトピックに上げられていて、脆弱性の放置は致命的なリスク。
- これに起因するセキュリティ事故を未然に防ぐには、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。

セキュアIoTプログラムをリリース

- 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」および、その検査結果をもとに、
- その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。
- 【検査ポイント】
  - ①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
  - ②認証と識別 (設計・製造、利用、廃棄、リサイクル)
  - ③セキュアアップデート (OTA：Over The Air)
- 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。

全体構成

セキュアIoT認定プログラム

IoTセキュリティ検査

●検査項目：ライフサイクル管理
- ・認証/識別
- ・鍵管理 (RoT)
- ・セキュアアップデート

✓ 対象となるIoTシステムに求められるセキュリティ強度によりclass1～4の基準を選択し、適合する検査を実施

脆弱性検査※

- ・ソースコード解析
- ・ファームウェア解析
- ・ネットワークスキャン
- ・既知脆弱性診断　など

セキュアIoT認定

●認定基準

✓ 一定基準の「脆弱性検査」をクリア
- ・Bronze: 80%以上
- ・Silver: 90%以上
- ・Gold: 95%以上

✓ 加えてGoldの場合は、該当するclassの「IoTセキュリティ検査」要件クリア*

＊ 認定対象の利用用途や目的によって適切なclassを認定機関が決定します。

検査基準

- 「IoTセキュリティ手引書 Ver 2.0」をベースにしたチェックシート(IEC62443-4準拠)

  - 「IoTセキュリティ手引書」とは
    国際標準をベースにIoTデバイスに求められる実装レベルのセキュリティ仕様をまとめたドキュメント（仕様検討部会のアウトプット）

検査認定対象

- 産業用システム、業務システム、コンシューマ機器
- 上記機器を構成する
  - ハードウェア
  - ソフトウェア
  - システム

認定グレード

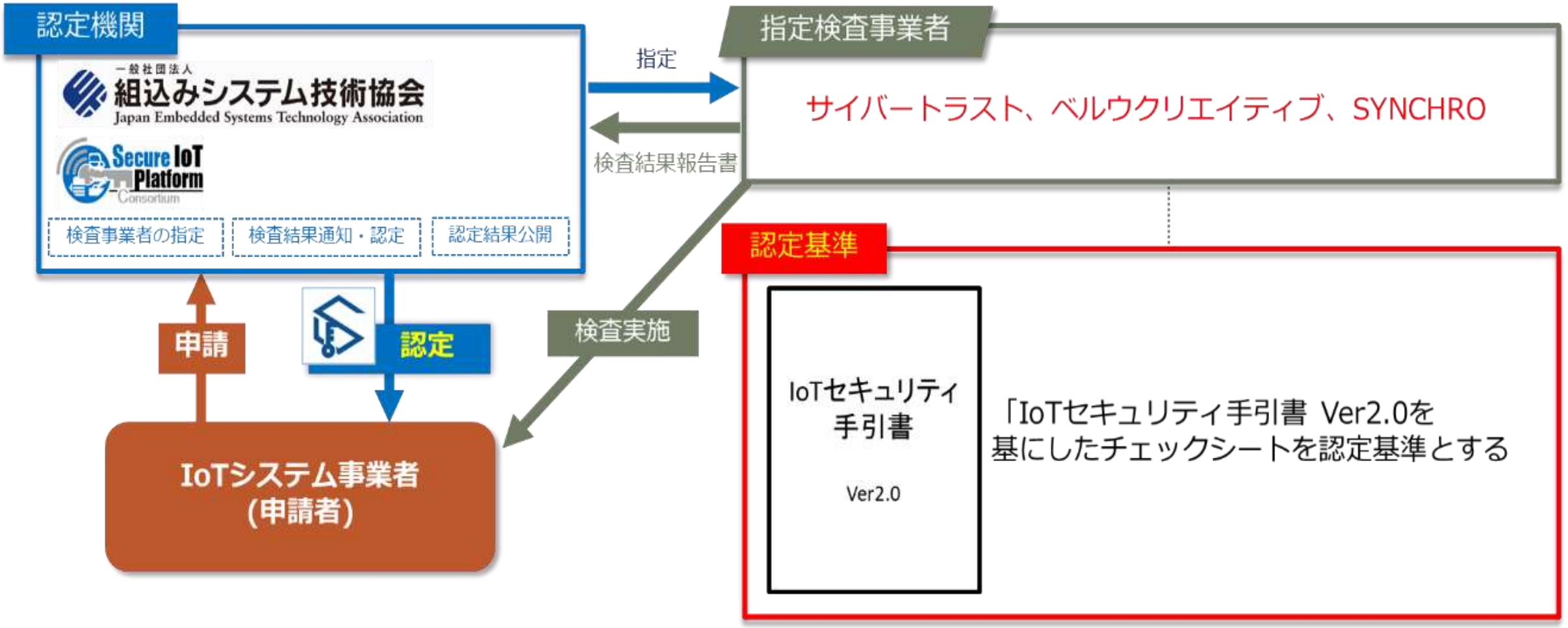
- 産業用システム、業務システム、コンシューマ機器
- 上認定要件に対する適合度により、
  - 『Gold』
  - 『Silver』
  - 『Bronze』

  の3段階のグレードで認定

認定の費用、有効期間、認定マーク

- 400万円～（税別）IoTセキュリティ検査、脆弱性検査、認定費用含む
- 有効期間：5年間
- 認定マーク：

認定体制


認定機関
一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association
Secure IoT Platform
Consortium
検査事業者の指定
検査結果通知・認定
認定結果公開
申請
認定
IoTシステム事業者
(申請者)
指定
検査結果報告書
検査実施
指定検査事業者
サイバートラスト、ベルウクリエイティブ、SYNCHRO
認定基準
IoTセキュリティ
手引書
Ver2.0
「IoTセキュリティ手引書 Ver2.0を
基にしたチェックシートを認定基準とする

指定検査事業者要件

- ISO/IEC 27001（JIS Q 27001）等の認証取得企業
- 経済産業省「情報セキュリティサービス基準適合サービスリスト」登録企業
- 以下に例示する内容相当の資格を保有し、かつ監査・診断において一定の実務経験がある技術者を擁する企業
- 公認情報セキュリティ監査人、公認システム監査人、CISA、システム監査技術者、情報処理安全確保支援士、CEH、CISSP、CISM、GIAC等

2023年度　標準化部会　活動まとめ

- 2022年度末～2023年度初頭
  - セキュアIoTプログラムを開始
  - 「セキュアIoT認定(Gold)」をサイバートラスト、SYNCHROの2社/6件に授与<https://japansecuritysummit.org/2023/02/6256/>
- 2023年度初頭~
  - セキュアIoTプログラムプロモーション
  - JASA（一般社団法人組込みシステム技術協会）との協業調整

ご清聴ありがとうございました

2024年度もよろしくお願い申し上げます。

- セキュアIoTプログラムプロモーション
- IoTプラットフォーム・セキュリティ・エンハンス
- さらなる標準的プラクティスの追求