「セキュアIoT認定プログラム」紹介資料

2023年3月1日

一般社団法人 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
（中央大学大学研究開発機構）
副座長　松本 義和
（サイバートラスト株式会社）

「セキュアIoTプログラム」とは

インターネット上に接続されるIoTシステムの脆弱性を基点にしたサイバー攻撃が増加しています。
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ますが、脆弱性の放置は致命的なリスクです。
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)

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。

【プログラム概要】プログラム構成

セキュアIoT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
- 真正性の担保 (耐タンパ：鍵管理)
- 認証と識別
- セキュアアップデート (OTA)

✓ 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。

【プログラム概要】Goldグレード Class

Class	対象
Class1	プライバシー情報を扱わない機器またはシステム
Class2	安全性や機密性、プライバシーへの影響が少ない機器またはシステム
Class3	安全性・機密性・プライバシー保護が求められる機器またはシステム
Class4	安全性・機密性・プライバシー保護が厳密に求められる機器またはシステム（重要インフラ）

【プログラム概要】認定対象

認証対象	具体例
ハードウェア	IoTデバイス、入出力デバイス、電子回路（ボード）、電子部品など
ソフトウエア	OS、アプリケーション、ファームウェアなど
システム	認証局、OCSP、ライフサイクル管理システム、鍵管理システム、OTAシステムなど

【プログラム概要】認定有効期間・提供物

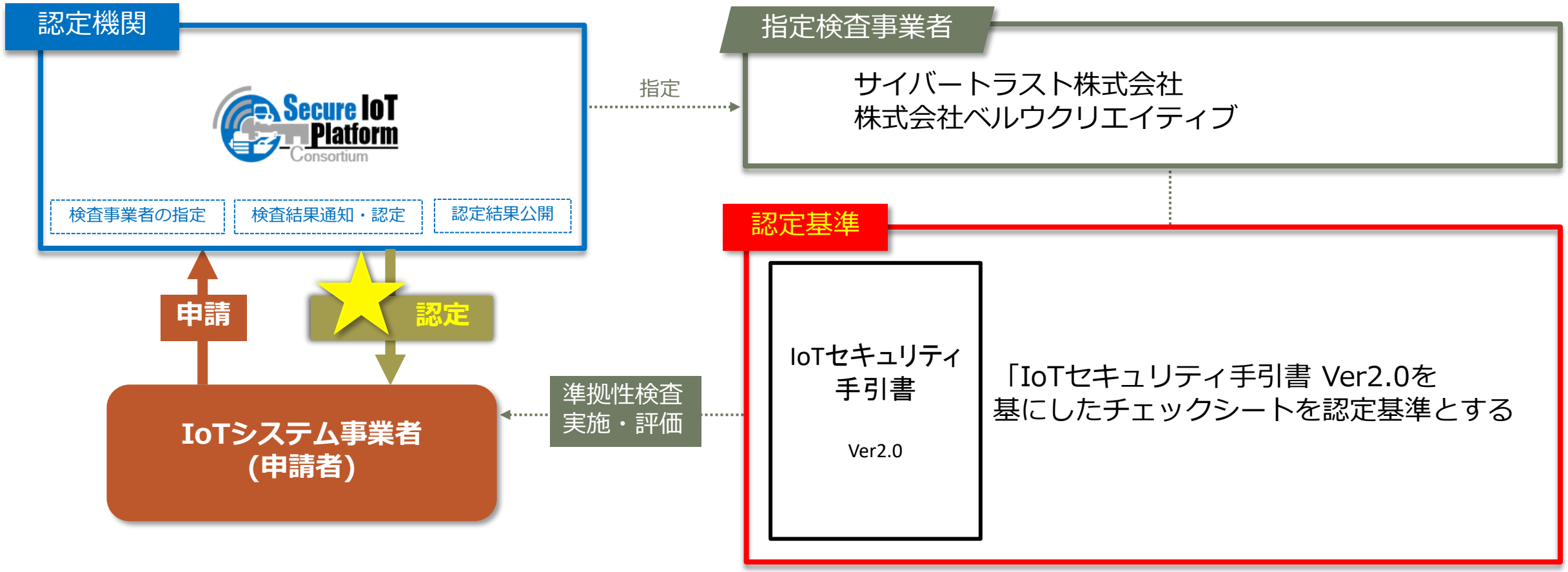
- 認定有効期間：認定日より5年間
- 発行物：認定証書、認定マーク

●認定マーク

【プログラム概要】費用

・400万円～/件
(IoTセキュリティ検査、脆弱性検査、認定費用含む)

認定スキーム


認定機関
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
指定検査事業者
サイバートラスト株式会社
株式会社ベルウクリエイティブ
準拠性検査
実施・評価
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

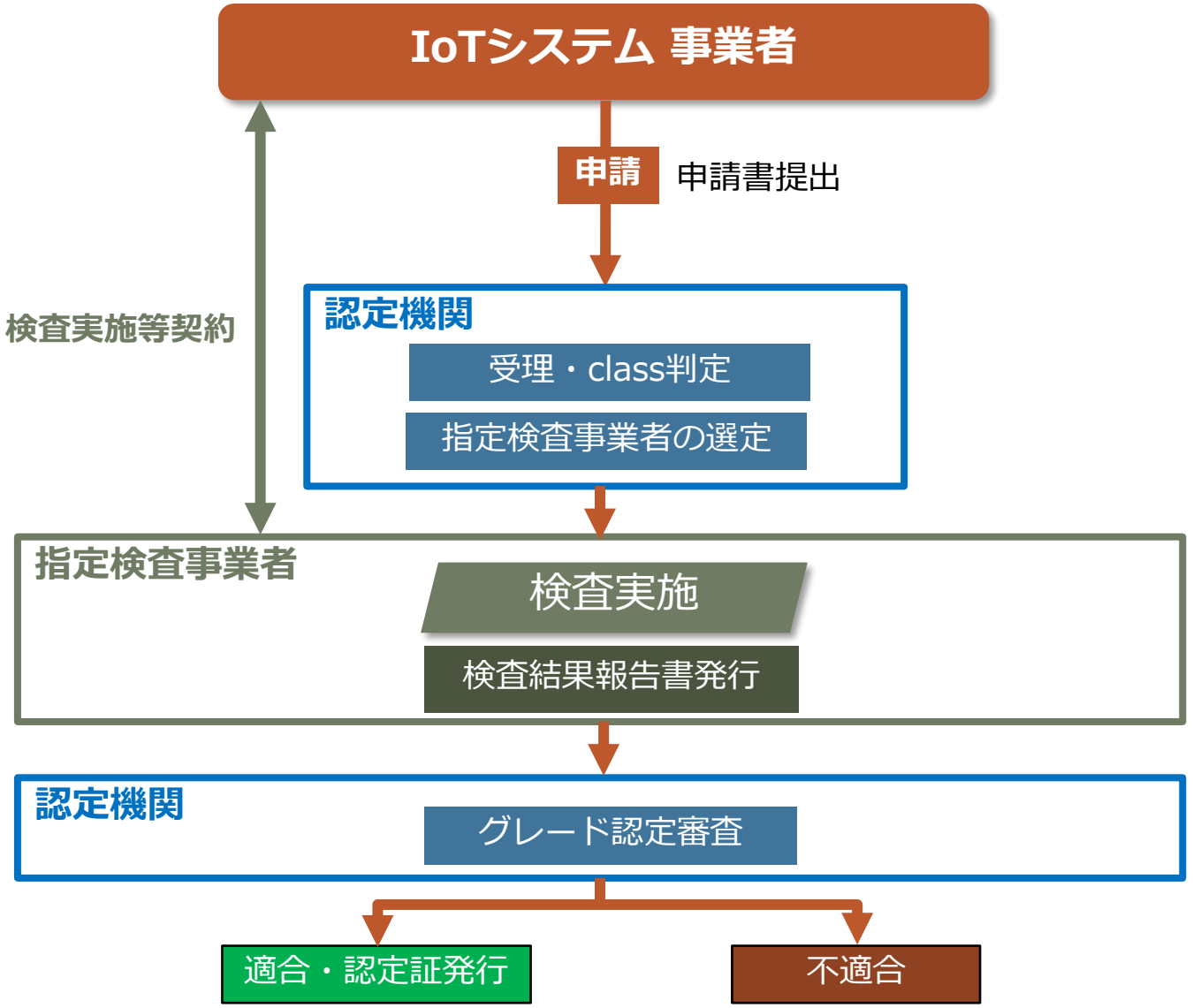
検査事業者指定要件

指定基準（次の全てを満たすこと）

【基準】

- ISO/IEC 27001（JIS Q 27001）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」に適合する事業者であり、IPAが公開する「情報セキュリティサービス基準適合サービスリスト」の情報セキュリティ監査サービスと脆弱性診断サービスの両方のリストに掲載されている事業者。
- 以下に示す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が検査に従事すること。
  - 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
- 脆弱性診断については、検査事業者の技術と評価の公平性を保つため、検査事業者に拠らず認証機関が提供する共通検査ツールを利用すること。

申請フロー


IoTシステム 事業者
申請
申請書提出
検査実施等契約
認定機関
受理・class判定
指定検査事業者の選定
指定検査事業者
検査実施
検査結果報告書発行
認定機関
グレード認定審査
適合・認定証発行
不適合