「IoTラベリングプログラムが始動！」
～デジタル機器への法規制状況を解説～

2024年3月27日

一般社団法人　重要生活機器連携セキュリティ協議会　代表理事
情報セキュリティ大学大学委員　客員教授

荻野　司　　博士（工学）

CCDSの概要

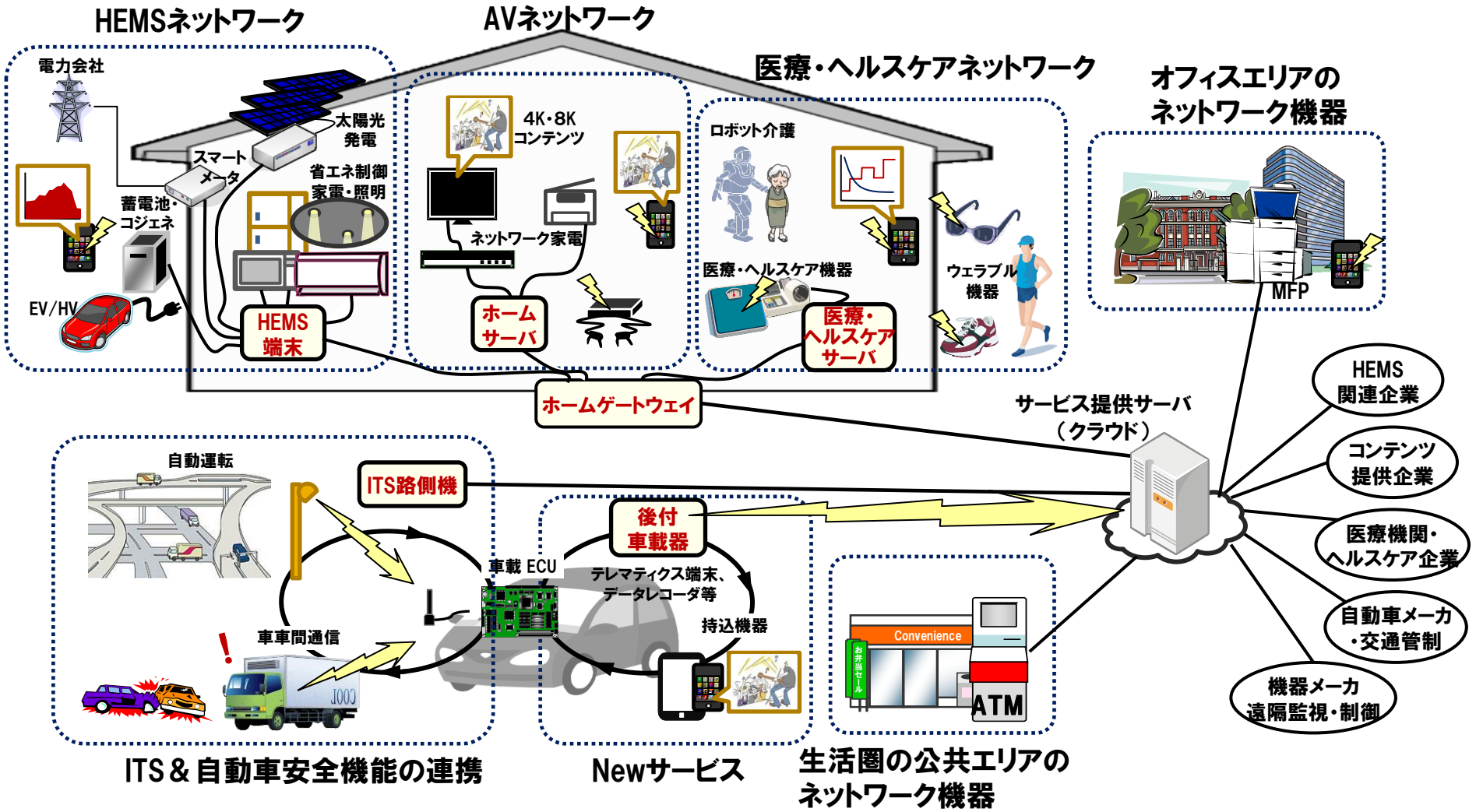
- 名称：一般社団法人 重要生活機器連携セキュリティ協議会
  - ◆ 英名：Connected Consumer Device Security council (CCDS)
- 設立：2014年10月6日
- 会長：徳田英幸（情報通信研究機構　理事長、慶応大学 名誉教授）
- 代表理事：荻野 司（情報セキュリティ大学院大学　客員教授）
- 理事：江崎 浩（東京大学大学院 教授）
  後藤 厚宏（情報セキュリティ大学院大学 学長）
  松本 勉（横浜国立大学先端科学高等研究院 教授）
- 会員数：220（正会員以上：52、一般会員：121、学術系：29、協賛:18）(2023年10月)

- 主な事業：
  1. 生活機器の各分野におけるセキュリティに関する国内外の動向調査、内外諸団体との交流・協力
  2. 生活機器の安全と安心を両立するセキュリティ技術の開発
  3. セキュリティ設計プロセスの開発や検証方法のガイドラインの開発、策定および国際標準化の推進
  4. 生活機器の検証環境の整備・運用管理及び検証事業、セキュリティに関する人材育成や広報・普及啓発活動等

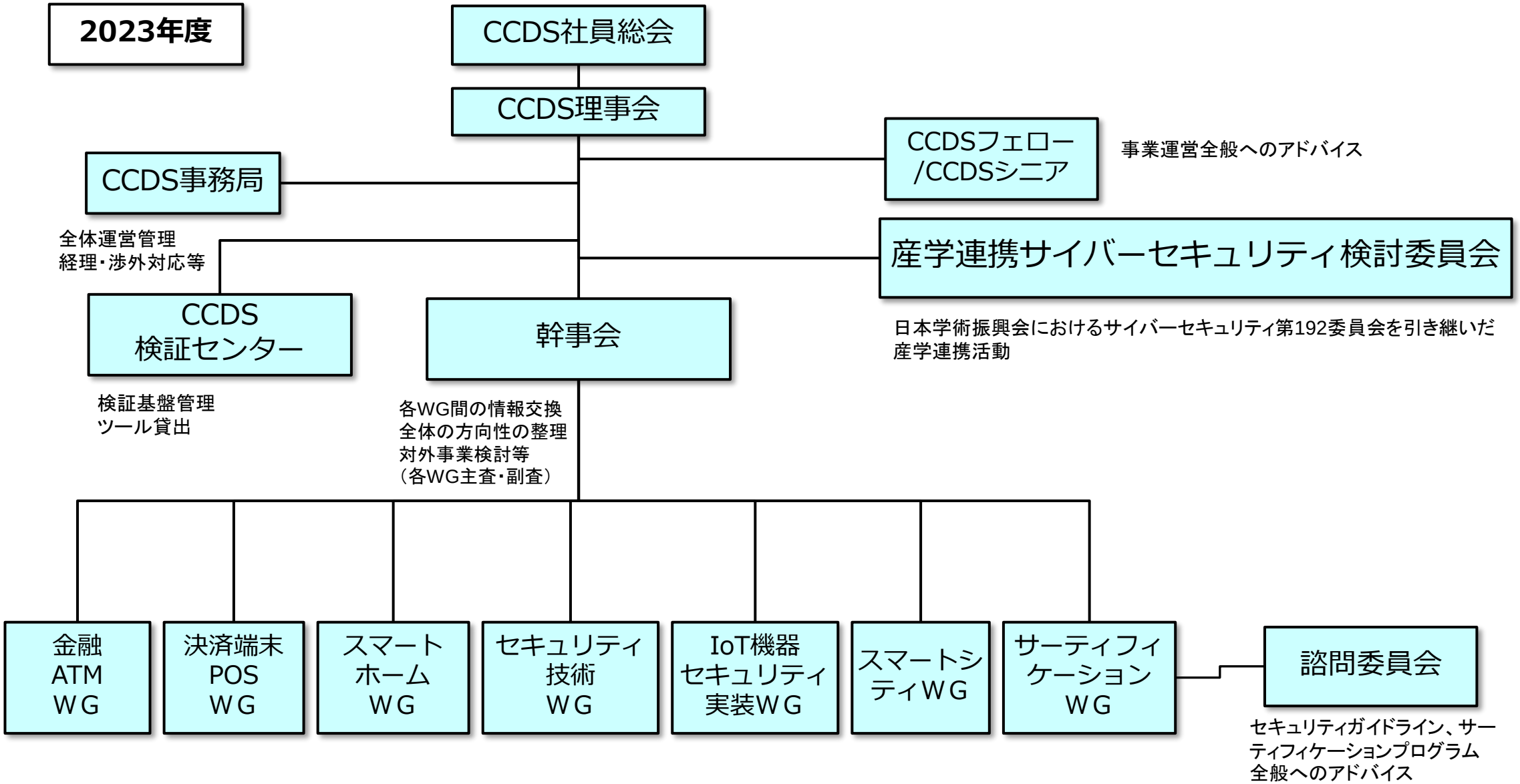
CCDSとは：
重要生活機器におけるセキュリティ事業の創生

一般民生機器など あらゆるモノが繋がる “モノのインターネット”

HEMS、AV家電、医療・ヘルスケア、自動車関連機器（ナビ、AV機器等）製品・サービス



2023年度　運営体制



国内外におけるIoTセキュリティの標準化動向

■2019年以降、日米欧において規格、標準化が加速

法制化関連施策　標準やガイドライン

日本

2017年
- 改正個人保護法施行
- 医療情報システムの安全管理に関するガイドライン第5版

2018年
- 電気通信事業法の技術基準適合認定にセキュリティ要件追加の提案

2019年
- パブコメ募集
- サイバー・フィジカル・セキュリティ対策フレームワーク

2020年
- 技適適合基準施行
  - ４つのセキュリティ要件義務化

2021年
- 5G促進法成立

米国

2017年
- IoT Cybersecurity Act 2017法案提出
  - 政府調達条件を規定

2018年
- NIST IR8200 (草稿)
  - 目的、リスク、脅威の分析、国際標準化状況
- カリフォルニア州 IoT セキュリティ法 成立

2019年
- IoT Cybersecurity Improvement Act 2019法案
- NIST IR 8259 (最終版)
  - 政府調達に適切な管理推奨事項
- カリフォルニア州 SB327 施行
  - 共通の初期パスワード禁止等

2021年
- IoT Cybersecurity Act 2020法
  - 政府調達機器セキュリティ規制強化
- Executive Order 14028
  - サイバーセキュリティ大統領令(コンシューマ機器)

2022年
- 消費者向けIoT製品のサイバーセキュリティラベリング推奨基準
- 消費者向けソフトウェアサイバーセキュリティラベリング推奨基準
  - ラベリング推奨(認証) 基準
- NIST IR8425 (最終版)
  - 消費者向けIoT機器最低限要件

※ NIST: 米国標準技術研究所
※ IR: Internal Report

欧州

2017年
- サイバーセキュリティ認証フレームワーク導入検討を公表
- ENISA IoTベースラインセキュリティ推奨事項を発表

2018年
- EU一般データ保護規則(GDPR)施行

2019年
- 英政府コンシューマIoT向けセキュリティ行動規範13箇条
  - コンシューマ機器の最低限のセキュリティ要件

2020年
- ETSI EN 303 645 Cyber Security for Consumer IoT
  - 英政府行動規範のEU版

2021年
- ETSI TS 103 701
  - EN303 645のテストシナリオ
- ENISA Guidelines for Securing the Internet of Things
  - IoT製品サプライチェーン保護のためのガイドライン

2022年
- 欧州連合官報RED委任規制
  - 無線機器にセキュリティ要件追加
- サイバー・レジリエンス法案
  - ネットワーク接続機器にサイバー攻撃対策を義務化

※ ENISA: 欧州ネットワーク情報セキュリティ庁
※ ETSI:　欧州電気通信標準化機構

NIST IR 8425で定義されたセキュリティ要件①

IoTデバイスの機能要件:IoT Prodduct Capabilities

ID ※当会で付記	要件（邦訳）
#1	**資産の識別：Asset Identification** IoT製品を一意に識別し、IoT製品のすべてのコンポーネントのインベントリを作成することができる。
#2	**製品の構成：Product configuration** IoT 製品の構成は変更可能であり、安全な初期設定を復元する機能があり、あらゆる変更は許可された個人、サービス、および他の IoT 製品のコンポーネントによってのみ実行可能である。
#3	**データ保護：Data Protection** IoT 製品とそのコンポーネントは、保存されたデータ（すべての IoT 製品のコンポーネントにまたがる）および伝送されたデータ（IoT 製品のコンポーネント間および IoT 製品の外部の両方）を不正なアクセス、開示、および修正から保護する。
#4	**インターフェースアクセス制御：Interface Access** IoT製品およびそのコンポーネントは、ローカルおよびネットワークインターフェース、ならびにこれらのインターフェースで使用されるプロトコルおよびサービスへの論理的アクセスを、許可された個人、サービス、およびIoT製品コンポーネントのみに制限する。
#5	**ソフトウェアの更新：Software Update** すべてのIoT製品コンポーネントのソフトウェアは、各IoT製品コンポーネントに適切な、安全で設定可能なメカニズムを使用することによってのみ、権限を有する個人、サービス、および他のIoT製品コンポーネントによって更新することができる。
#6	**サイバーセキュリティの状態認識：Cybersecurity State Awareness** IoT製品は、IoT製品のコンポーネントとそれらが保存および送信するデータに影響を与える、または影響を受けるサイバーセキュリティインシデントの検出をサポートする。

NIST IR 8425で定義されたセキュリティ要件②

IoT製品の製造者に関する非技術的な要件:IoT Product Developer Activities

ID ※当会で付記	要件（邦訳）
#7	**ドキュメンテーション：Documentation** IoT製品開発者は、顧客の購入前、製品の開発とその後のライフサイクルを通じて、IoT製品およびその製品コンポーネントのサイバーセキュリティに関連する情報を作成、収集、保管する。
#8	**情報と問い合わせの受付：Information & Query Reception** IoT製品開発者がサイバーセキュリティに関連する情報を受信し、サイバーセキュリティに関連する情報について顧客等からの問い合わせに対応する能力を有する。
#9	**情報の発信：Information Dissmination** IoT製品開発者は、サイバーセキュリティに関連する情報を（例えば、一般に）公開し、（例えば、顧客またはIoT製品エコシステムの他の人に）配布する。
#10	**製品の教育・啓発：Product Education & Awareness** IoT製品開発者は、IoT製品およびその製品コンポーネントに関連するサイバーセキュリティ関連情報（考慮事項、機能など）について、IoT製品エコシステムの顧客およびその他の人々の意識を高め、教育する。

NIST　認証スキームの提言

NIST IR 8425では削除されたが、"Recommended Criteria"では、IoTラベリング基準に基づく認証スキームについて、以下の検討すべき事項と提言が記載されている。

■ラベリングについての留意事項

・ラベルは消費者のIoT製品の購入意思を支援するものであること（IoT信頼と信用を高める目的で表記される）。
・ラベルデザインは消費者テストによる使い勝手の評価を通して、理解されやすいマークであること。
・サイバーセキュリティの専門的な知識を必要とせず、多様な消費者が利用できること。
・ラベルは、購入前、購入時、購入場所（店舗またはオンライン）、購入後に消費者が利用できるようにすること。
・複数のIoT製品セキュリティ・ステークホルダー（小売業者、メーカー、業界および非営利のセキュリティ団体、学界、または政府など）間で責任を共有すること。
・消費者への教育キャンペーンを伴うこと（ラベルの認知度向上及び、プログラムの重要な側面について消費者に透明性を提供）
  – 製品の基準、専門用語の解説、適合性評価に関する一般的な情報、適合宣言、範囲（製品の種類やラベル付き製品の識別）、消費者への期待、ラベリングプログラムの連絡先や苦情の申立先の情報

■適合性評価の考察

・スキームオーナーは、公的機関である場合もあれば、民間企業である場合もある。
・単一の適合性評価アプローチではなく、IoT製品の範囲、ユースケース別に複数のアプローチが可能である。
・スキームオーナーを定義し、スキームオーナーは以下の対応を行う。
  – 推奨製品の基準を調整
  – 適合性評価要件を定義
  – ラベルと関連情報を開発
  – 関連する消費者アウトリーチと教育を実施
・以下の単独または組み合わせてにより、技術要件への適合を示す。
  – 自己適合宣言
  – 第三者による試験または検査
  – 第三者認証

FCC Proposes Cybersecurity Labeling Program for Smart Devices（2023/8/10）

対象製品：
スマート デバイスまたは製品には、ホームオフィスルーター、デジタルパーソナルアシスタント、ホーム セキュリティシステム、音声起動ショッピング、インターネット接続機器、フィットネス トラッカー、GPS トラッカー、医療機器、ガレージ ドア オープナー、ベビー モニターなど

パブリックコメント：
・CCDSより、13項目の意見を提出

①：有線無線を区別せず対象としてはどうか
②：IoTデバイスだけでなく、IoT製品全体を対象としてはどうか
③：IoT製品で一部のデバイスのみラベルが張られていると消費者は混乱する。IoT製品全体としてラベル付与要件を満たす必要があるでしょう。
④：IoT製品は様々な分野で使用されていいることから、ラベリングプログラムの適応範囲は分野を超えて利用すべきであろう。
⑤：メーカによる自己評価を認めることに賛成でる。
⑥：サポート期間やサポート終了時の対象方法を通知する必要がある。

CCDS パブリックコメント "Cybersecurity Labeling for Internet of Things"

日本国における産学連携団体であるＣＣＤＳは、IoT セキュリティに関するガイドラインや要件について策定、発行を行い、2019 年からサーティフィケーションプログラムを開始している。世界においても産業界主導による IoT 機器認証スキームとしては、最初の取り組みであると考えている。是非、本プログラムの検討において、我々のコメントを参考にして頂ければ幸いである

1．CCDS の概要
・当会は、日本国内の民間企業や学術研究機関等を中心に 200 以上の加入団体を有する。
・IoT 機器のセキュリティに関する技術調査や、標準化、普及啓発、人材育成、
セキュリティ検証、製品・サービスの認証事業など、幅広い事業を展開。

CCDS web site: https://www.ccds.or.jp/english/index.html

2. CCDS のコメント

#	ページ番号	章	該当箇所とコメント	
1	58214	11	該当箇所	たとえば、有線専用 IoT デバイスを除外すると、適切なネットワーク セキュリティ標準を備えた IoT デバイスについて適切に情報を提供するのではなく、このラベリング プログラムの成功、有用性、有効性に影響を及ぼし、消費者を混乱させることになるでしょうか?
			CCDS のコメント	インターネット接続を有する機器を対象とするのであれば、有線無線を区別することなく対象とすべきである。 例えば、無線ブロードバンドルータの場合では、以下の両ケースを想定する必要がある。 1)有線接続によるネットワーク側（WAN 側）からの攻撃（攻撃者にインターネット経由でハッキングされる場合など） 2)無線ブロードバンドルータの配下に無線接続された機器のセキュリティ問題（LAN 側に接続された機器のマルウェア感染など）
2	58214	12	該当箇所	IoT デバイスと、基本的な動作機能を超えて IoT デバイスを使用するために必要な追加の製品コンポーネント（バックエンド、ゲートウェイ、モバイル アプリなど）。委員会は、IoT ラベルの対象となる IoT 製品のこの定義案についてコメントを求めています。
			CCDS のコメント	IoT サービスに含まれる、IoT デバイス単体、連携するモバイルアプリ、ゲートウェアを含め、IoT システム全体をこのラベリング制度の対象とすべきである。 例えば、IoT デバイス単体と連携するモバイルアプリ単体だけをラ 定する必要がある。 参考情報） 日本では、民間団体の CCDS がスマートホーム分野のガイドライ
8	58217	31	該当箇所	特定の IoT デバイスまたは IoT デバイスのクラスに対して、容易に（またはより迅速に）採用できるほどすでに十分に成熟した標準はありますか?

- ISO/IEC 27400　Publication date　2022/6/7
  - ータイトル：IoT security and privacy – Guidelines
  - ー概要：IoTソリューションのセキュリティとプライバシーに関するリスク、原則、コントロール（対策）に関するガイドラインを提供
  - ー対象：IoTサービスプロバイダ、IoTサービス開発者、IoTユーザ
  - ・2017年：総務省・経産省のIoTセキュリティガイドラインv1.0を提案
    上記をベースにプライバシー要件が追加されて標準化
- ISO/IEC 27402（Final Draft）The end of 2023ISO/IEC 27402（Draft）The end of 2023
  - ータイトル： IoT security and privacy –Device baseline requirements
  - ー概要：ベースライン要件を提供する
  - ー対象： IoT機器とその製造者
  - ・2019年：米国発案(NIST IR8259がベースによるIoTセキュリティ要件を定義（後にNIST IR8425）
- ISO/IEC 27404（Approved Work Item）
  - ータイトル： IoT security and privacy — Cybersecurity labelling framework for consumer IoT
  - ー概要：消費者向け IoT のサイバーセキュリティ ラベリング フレームワーク
  - ー対象：消費者、開発者、サイバーセキュリティラベルの発行団体、および独立した試験機関
  - ・シンガポール発案、欧米ともにLabellingに向けた検討

欧州の状況： サイバー・レジリエンス法案

■**概要**

・2022年9月15日に欧州連合（EU）の欧州委員会より、インターネット接続機器に対するサイバーセキュリティ対策を義務化する「サイバー・レジリエンス法案」が提出された。

・メーカやソフトウェアベンダーには、第三者機関による評価が義務付けられ、違反した場合には、最大1500万ユーロもしくは、総売上高の2.5%のうち高い金額を制裁金として科せられる。

※法律発効後24ヵ月で適用、ただし製造業者の報告義務は発効から12ヵ月で適用される。

※脆弱性に気付いた場合やセキュリティ事故が発生した場合には、24時間以内にENISAに報告。

【現在公開されている法案文書と付随文書】

https://www.european-cyber-resilience-act.com/

1_Proposal_for_a_Regulation_on_cybersecurity_requirements_for_products_with_digital_elements__Cyber_resilience_Act

⇒法案文書。法案の目的や法制度の概要を記載

2_Annexes_Proposal_for_a_Regulation_on_cybersecurity_requirements_for_products_with_digital_elements__Cyber_resilience_Act

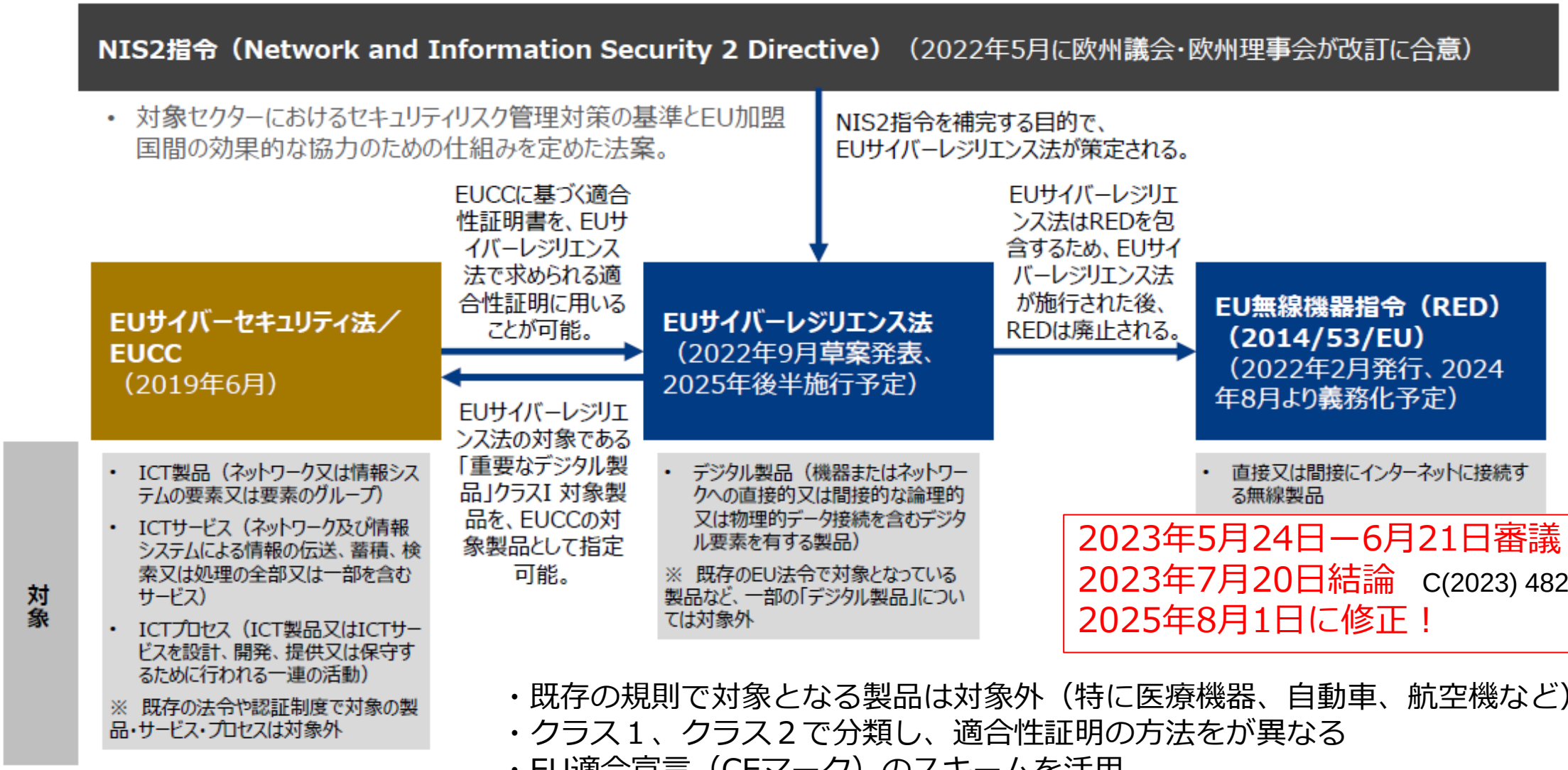
⇒付随文書。遵守すべきセキュリティ要件や、整備しておくべき技術文書などを記載。

参考）サイバー・レジリエンス法案のセキュリティ要件

1. デジタル要素を持つ製品の特性に関するセキュリティ要件	
(1)	デジタル要素を含む製品は、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、生産されなければならない。
(2)	デジタル要素を含む製品は、悪用可能な既知の脆弱性がない状態で提供されること。
(3)	第10条（2）に言及されたリスクアセスメントに基づき、適用される場合、デジタル要素を有する製品は、以下のようにしなければならない。
(a)	デフォルトでセキュアな設定で提供され、製品を元の状態に戻すことが可能であること。
(b)	認証、ID、アクセス管理システムを含むがこれに限定されない適切な管理機構により、不正なアクセスから確実に保護すること。
(c)	保存、送信、またはその他の方法で処理された個人またはその他のデータの機密性を、最新のメカニズムによって静止中または転送中の関連データを暗号化するなどして保護すること。
(d)	保存、送信、またはその他の方法で処理されたデータ、個人またはその他のデータ、コマンド、プログラム、設定の整合性を、ユーザーによって許可されていない操作または修正から保護し、また破損について報告すること。
(e)	個人またはその他のデータを、適切かつ関連性のある、製品の使用目的に関連する必要なものに限定して処理する（「データの最小化」）。
(f)	サービス妨害（DoS）攻撃に対する回復力と軽減を含む、重要な機能の可用性を保護すること。
(g)	他の機器やネットワークが提供するサービスの可用性に及ぼす自らの悪影響を最小限に抑えること。
(h)	外部インタフェースを含む攻撃面を制限するように設計、開発、製造されること。
(i)	適切な悪用防止メカニズムや技術を用いて、インシデントの影響を軽減するように設計、開発、製造されること。
(j)	データ、サービス、機能へのアクセスや変更を含む、関連する内部活動を記録及び／又は監視することにより、セキュリティ関連情報を提供すること。
(k)	脆弱性が、セキュリティ更新（該当する場合、自動更新及び利用可能な更新のユーザへの通知を含む）を通じて対処されることを保証すること。

2. 脆弱性ハンドリング要件	
(1)	製品に含まれる脆弱性とコンポーネントを特定し、文書化する。これには、少なくとも製品のトップレベルの依存関係を網羅する、一般的に使用され機械で読み取り可能な形式のソフトウェア部品表を作成することが含まれる。
(2)	デジタル要素を含む製品にもたらされるリスクに関連して、セキュリティアップデートの提供を含め、脆弱性に遅滞なく対処し、改善すること。
(3)	デジタル要素を含む製品のセキュリティについて、効果的かつ定期的なテストとレビューを適用する。
(4)	セキュリティアップデートが提供された後、修正された脆弱性についての情報（脆弱性の説明、影響を受けるデジタル要素を含む製品を特定できる情報、脆弱性の影響、深刻度、脆弱性を修正するための情報を含む）を一般に公開する。
(5)	脆弱性の協調的な開示に関するポリシーを導入し、実施する。
(6)	デジタル技術を用いた製品およびその製品に含まれる第三者のコンポーネントの潜在的な脆弱性に関する情報の共有を促進するための措置を講じること（デジタル技術を用いた製品で発見された脆弱性を報告するための連絡先を提供することを含む）。
(7)	デジタル技術を用いた製品のアップデートを安全に配布し、悪用可能な脆弱性が適時に修正または軽減される仕組みを提供する。
(8)	特定されたセキュリティ問題に対処するためのセキュリティパッチやアップデートが利用可能な場合、それらが遅滞なく、かつ無料で配布されることを保証すること。

サイバー・レジリエンス法案



2023年5月24日ー6月21日審議
2023年7月20日結論　C(2023) 4823 final
2025年8月1日に修正！

・既存の規則で対象となる製品は対象外（特に医療機器、自動車、航空機など）
・クラス１、クラス２で分類し、適合性証明の方法をが異なる
・EU適合宣言（CEマーク）のスキームを活用

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

CCDS　IoTセキュリティガイドライン整備状況　～社会実装～

CCDS外の動きや国際標準化の動き

提案 → **ISO/IEC 27400提案** IoT security and privacy – Guidelines → 標準化 → **ISO/IEC 27400** IoT security and privacy – Guidelines

提案 → **ISO/IEC 30147** Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes

IoTセキュリティ一般的枠組 **NISC** → 各種ガイドライン（文書）発行

参照

提案 → IoTセキュリティガイドラインV1.0 **IoT推進コンソ 総務省 経済産業省**

医療情報システムの安全管理に関するガイドライン第5版 **厚生労働省**

サイバー・フィジカルセキュリティ対策フレームワーク **経済産業省**

協力 → つながる世界の開発指針 IPA

CCDS認証マーク例

2016年 | 2017年 | 2018年 | 2019年 | 2020年

CCDS内の動きや文書発行

2016年
- 車載機編ガイドライン V1.0
- IoT-GW編ガイドライン V1.0
- ATM編ガイドライン V1.0
- オープンPOS編ガイドライン V1.0
- 分野別ガイドライン V1.0

2017年
- 分野別ガイドライン V2.0
- 分野別ガイドライン V2.0別冊
- 分野別ガイドライン V1.0英語版
- 分野別ガイドライン V2.0英語版
- 評価検証ガイド v1.0

2018年
- IoT分野共通セキュリティ要件ガイドライン_2018年版
- CCDS 調達仕様編 草稿

2019年
- **認証マーク制度運用開始**
- IoT分野共通セキュリティ要件ガイドライン_2019年版
- IoT分野共通セキュリティ要件ガイドライン_2019年_別冊～解説編
- CCDS スマートホーム編 V1.0

2020年
- 認証マーク**制度のサービスへの適用開始**
- IoT機器セキュリティ要件ガイドライン_2021年版
- IoT機器セキュリティ要件ガイドライン_2021年版_別冊～解説編
- IoT機器セキュリティ要件_2021年版_対策方針チェックリスト_v1.0
- CCDS アップデート機能編
- CCDS ATM勉強会報告書

IoT機器セキュリティ認証スキームのポイント

ポイント１：つまるところベースライン要件は、ほぼ変わらい。

ー＞日本案は、日本のメーカや消費者にとって最適に設定すべきであろう
（ETSI,NIST,あまり変わらない）

ポイント２：経年変化するセキュリティなので、要件・適合基準は鮮度が重要。

ー＞柔軟に要件・適合基準をアップデートできる仕組み
（非営利組織で柔軟に動ける体制が寛容）

ポイント３：標準化は、たいていはプロセスチェック重視なのでドキュメント
チェックが多く認証にかかるコストが増大する（重くなる）

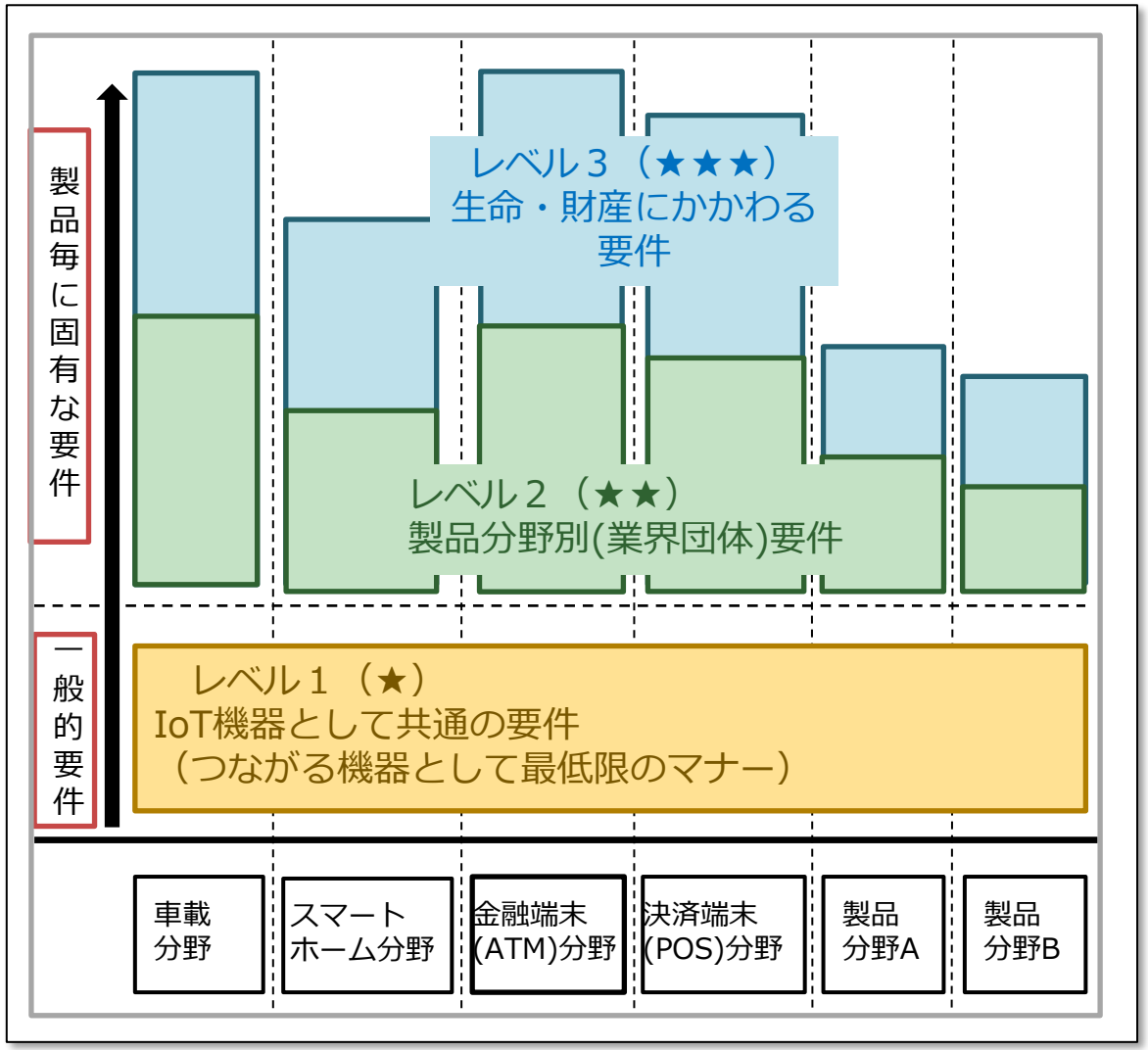
ー＞軽い検査プロセスが重要。
適合基準を我が国として作成することが重要。（経済安全保障）

ポイント４：社会実装：使われることに意味がある。メーカー賛同し消費者が受け入れる

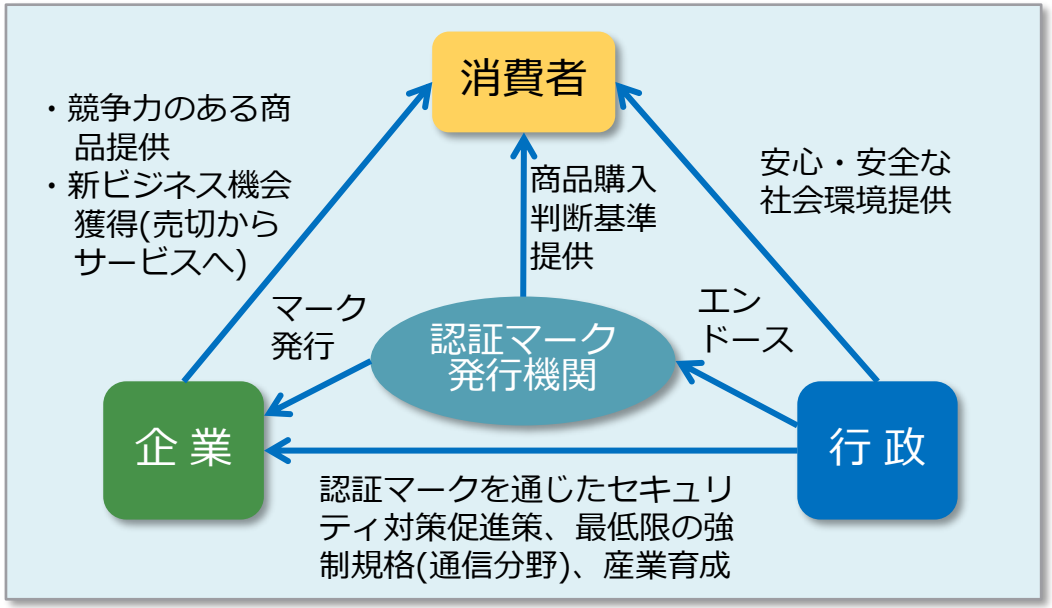
ー＞双方にインセンティブが必要
メーカ：認証にかかるコストを安価に！そして購買意欲につながる！
ユーザー：安心・安全の視覚化、加えて分かるメリットetc.(ex.サイバー保険とか)

CCDSサーティフィケーションプログラムの概要

プログラムのレベル構成



プログラムのスキーム



プログラムのポイント

1. 任意マーク（罰則なし）
2. 自主検査と第三者検査のいずれか選択可能
3. 第三者機関によるマーク付与の意味（検証結果保持と追跡可能）
4. マークの毎年更新（新規攻撃への対応）
5. セキュリティ対策の普及促進策　⇒　例えば税制優遇、助成金

CCDS:IoT機器セキュリティ要件 2023年版

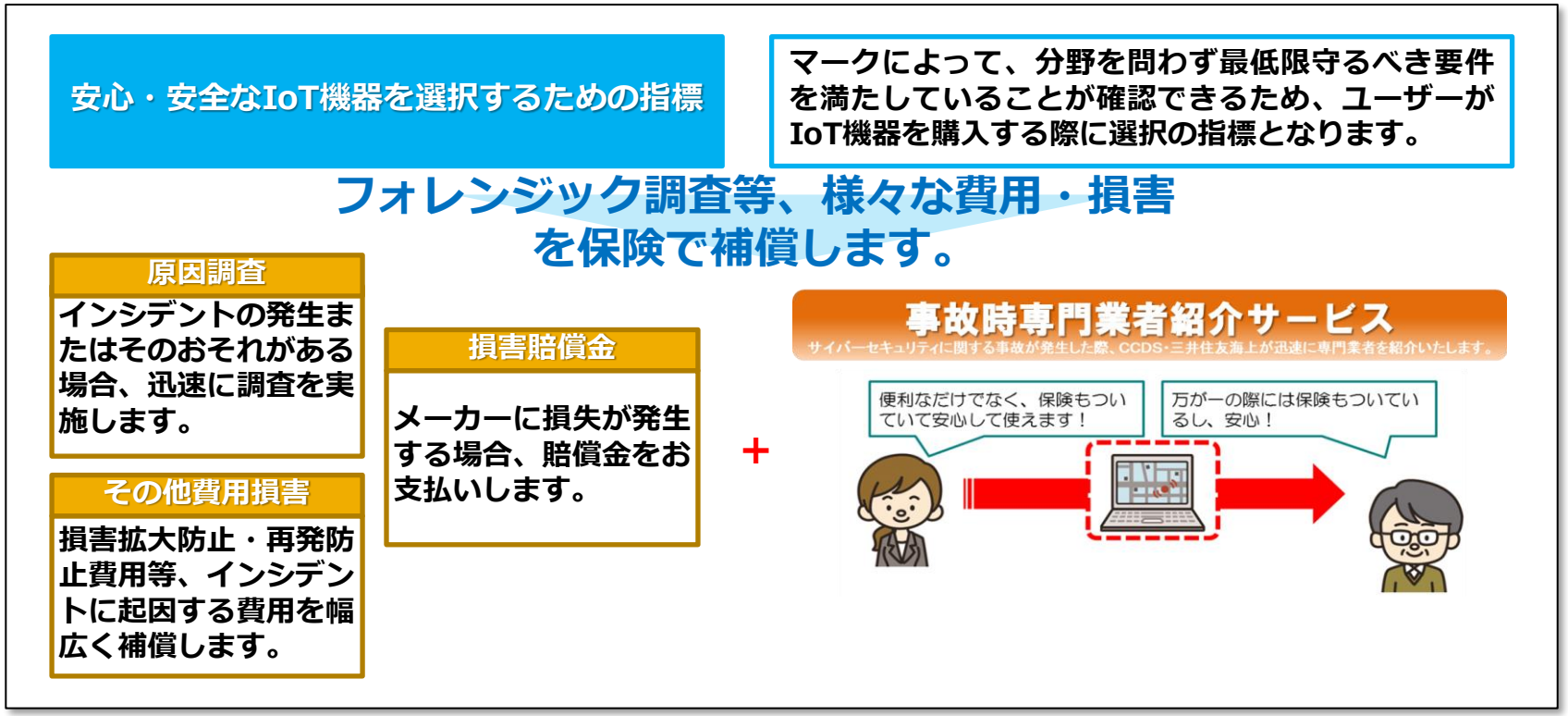
分 類	ID	セキュリティ要件		要件の対象・目的
		サブセットID	サブセットIDに対応するセキュリティ要件	
1）IoT機器の機能要件	1-1	**アクセス制御及び認証**		識別、アクセス制御、構成変更、権限管理、認証
		1-1-1	TCP/UDPポートの無効化	
		1-1-2	認証情報の変更	
	1-2	**データ保護**		データ保護、認証情報・鍵情報保護
		1-2-1	データ消去	
	1-3	**ソフトウェア更新**		運用中インシデント対応
	1-4	**特にインシデントが多く影響度が大きい要件**		発生件数、影響が大きいインシデントへの対応
		1-4-1	Wi-Fiの認証方式	
		1-4-2	Bluetoothの対策	
		1-4-3	USBのアクセス制御	
		1-4-4	インジェクション対策	
2）IoT機器の運用における要件	2-1	**連絡窓口・セキュリティサポート体制**		運用中インシデント対応
	2-2	**製品に関する文書管理**		セキュリティ対応状況の明文化
	2-3	**利用者への情報提供**		運用サポート
3）IoT機器の監査に関する要件	3-1	**ログの記録**		運用中インシデント管理
		3-1-1	時間管理機能	

※ 米国（NIST）、欧州（ETSI）のガイドライン、規格文書を参考に改定（下線赤文字は2021年版からの追加要件）

CCDS:マークに自動付帯するIoTサイバー保険の概要

・マーク取得機器を対象に、IoTサイバー保険が自動付帯される
（保険契約はCCDSが行い、マーク取得者による契約や保険費用負担は不要）

・インシデント発生時に、マーク取得者（ベンダ）の原因調査費用、損害賠償費用、その他費用を補償する。（間接的に機器利用者を保護する）



資料：認証制度のスキーム案

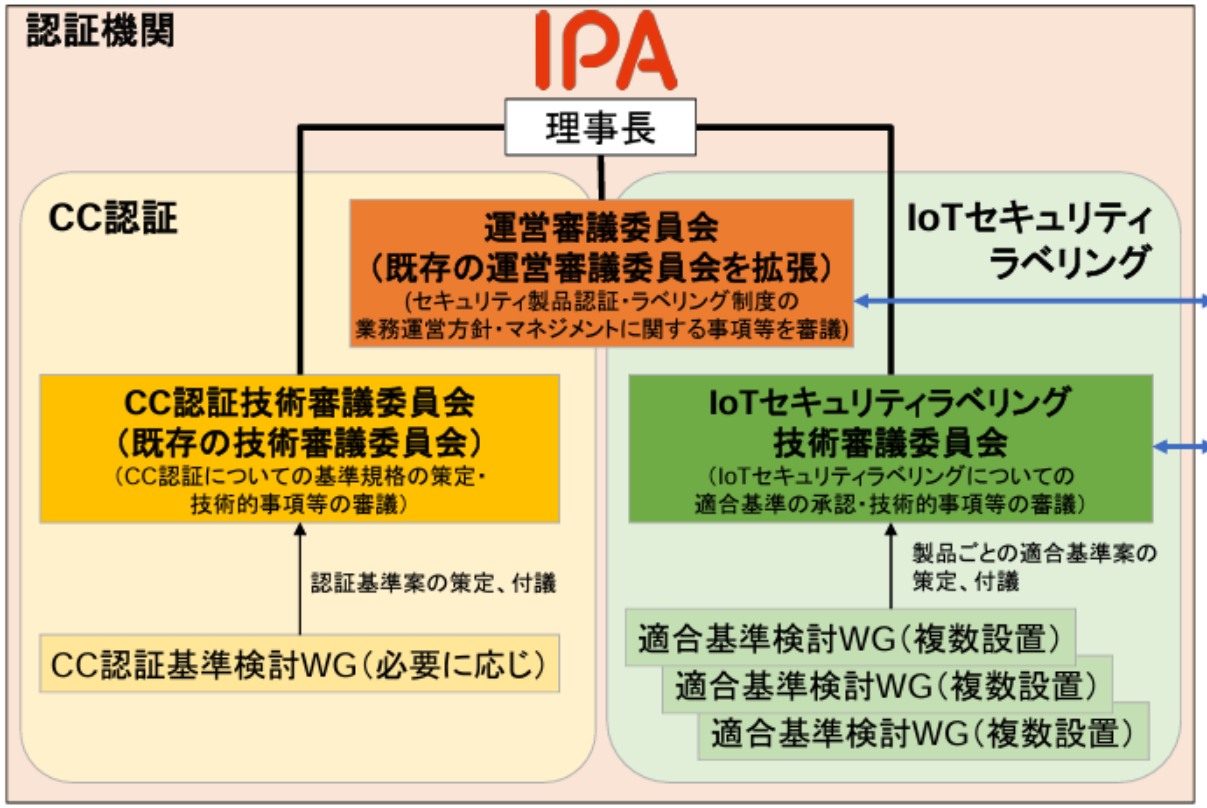
出典:IoT製品に対するセキュリティ
適合性評価制度の構築について,12.12.2023

CCDS

発展JISEC認証スキームの事務局・委員会の体制案

第5回検討会資料P.7を修正

- 現行JISEC制度（CC認証）とIoTセキュリティ適合性評価制度を**発展JISEC制度として、一体となった枠組みで運用**する。
- IoTセキュリティ適合性評価制度は、☆2以上を整備する製品類型の検討、国内既存制度との連携・統合の調整、相互承認等の諸外国との調整などが来年度以降もあるため、**IPAと経産省による運営事務局を設立**し、制度が軌道に乗るまでそれを維持する。



IoTセキュリティ認証制度運営事務局（※）

IPA ＋ 経済産業省

- 制度拡張（☆2以降）の検討
- 国内既存制度との連携・統合検討
- 相互承認等の海外連携の調整
- 政府調達要件等への働きかけ
- 民間企業、一般消費者への制度普及促進
- IoT製品ベンダーへの認証取得促進

など

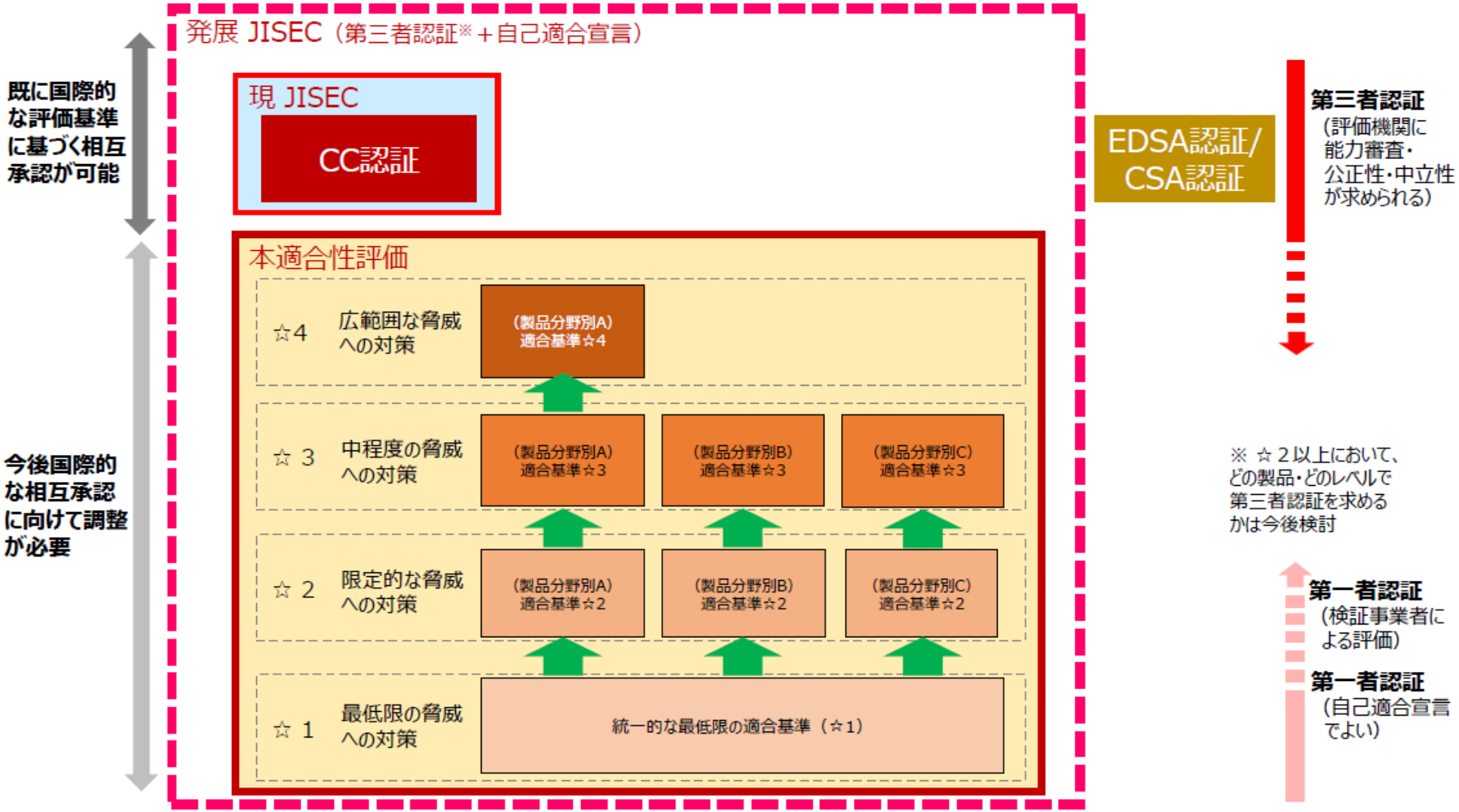
※以下の条件が満たされ、制度が軌道に乗った段階で、IPAによる運営とし、経済産業省は各委員会に委員またはオブザーバーとして関与する。

- 定常的に新規の認証申請がある。
- 主要な製品類型の☆2以降の制度化および既存制度との統合・すみ分けが合意されている。
- 海外の主要国との相互承認等の方向性が合意されている。

資料：既存制度との関係性

出典:IoT製品に対するセキュリティ
適合性評価制度の構築について,7.19.2023

現行のJISEC制度はCC認証のみを対象としているが、本適合性評価制度の構築にあたって、JISEC制度のこれまでの知見やリソースを有効に活用するために、JISEC制度を本適合性評価制度を含む形で拡張する新たな枠組みを立ち上げる。EDSA認証／CSA認証との整理は今後要検討。



9

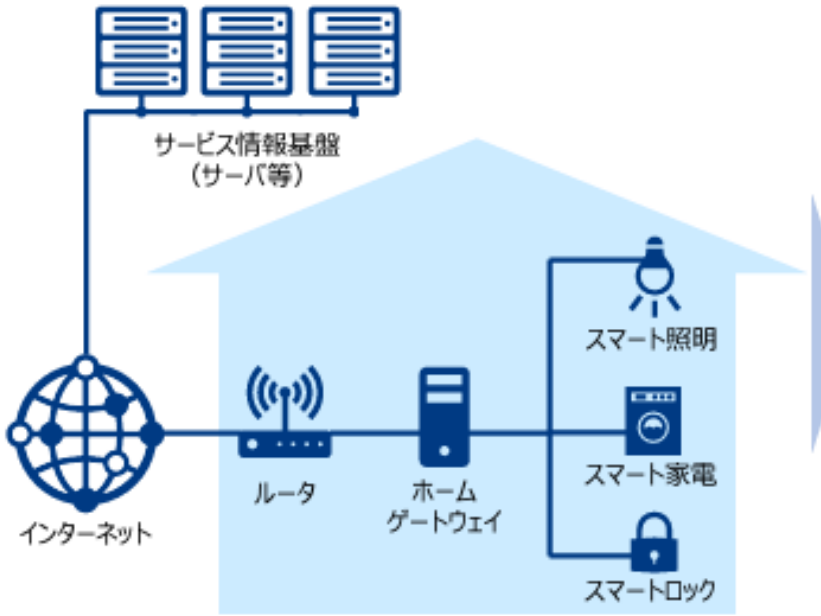
資料：目的②特定分野で使用される IoT機器の最低限のセキュリティ確保

出典:IoT製品に対するセキュリティ適合性評価制度の構築について 12.12.2023

CCDS

- IoT製品は、単体で比較・検討されて調達されるだけではなく、**特定分野のシステムに組み込まれて調達され、利用されるケースもある。**そのようなケースでは、最終調達者（ユーザー）がセキュリティを考慮したIoT製品を直接選定するのではなく、システムに組み込まれる段階で選定・調達される。（例）**スマートホーム、工場システム、ビルシステム**など
- **特定分野のシステムそれぞれの想定するユースケース、守るべき資産、脅威、リスクを定義**し、実施すべき対策のひとつとして、**組み込まれるIoT製品に求めるセキュリティ要件を定める**必要がある。当該要件で、IoT製品類型共通の☆1以上が必要となる場合に、**☆2以上の整備を本制度で検討**する。
- 各業界団体等では、特定分野のシステムのセキュリティに対して、**それぞれの用途や機能を考慮し、組み込むIoT製品のセキュリティ要件として必要な認証・ラベルを指定**する。その他のセキュリティ要件も含めたセキュリティガイドラインの作成や、システム全体としての認証制度等の整備を行い、**その準拠を業界標準とする**ことで、**当該特定分野のシステムにおいて、最低限のセキュリティが確保されたIoT機器のみが採用される**ことを目指す。

【特定分野のシステムのイメージ（スマートホームの例）】



【各IoT製品に求める認証・ラベル指定のイメージ】

IoT製品	認証・ラベル	指定理由（例）
ルータ	☆2以上	・外部からの侵入ルートになる可能性があるため
ホームゲートウェイ	☆2以上	・外部からの侵入ルートになる可能性があるため
スマート照明	☆1以上	・機器単体が侵害を受けても被害は限定的であるため
スマート家電	☆1以上	・機器単体が侵害を受けても被害は限定的であるため
スマートロック	☆2以上	・侵害が受けた場合、人的資産や物理的資産の損害に繋がる恐れがあるため

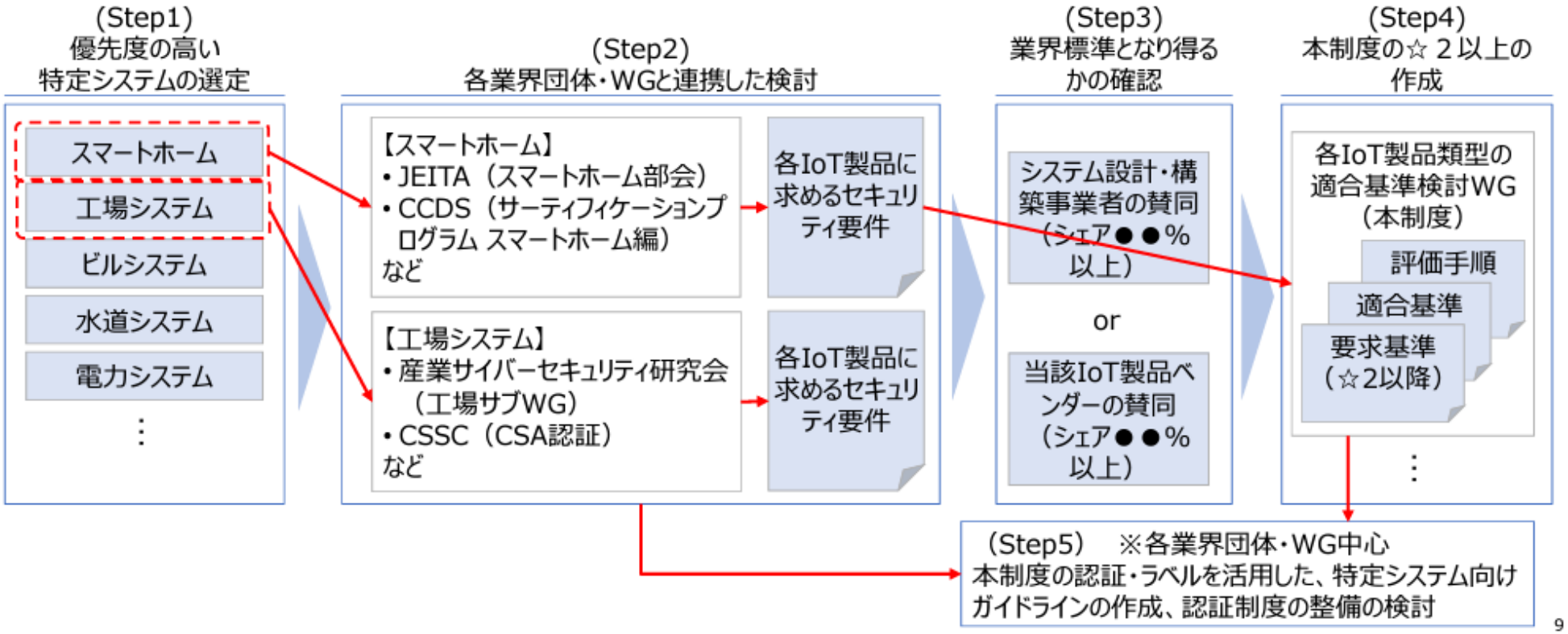
※ システムの重要度・規模やIoT製品の用途で指定する認証・ラベルを分けることもある。

資料：目的②展開戦略と初期ターゲット

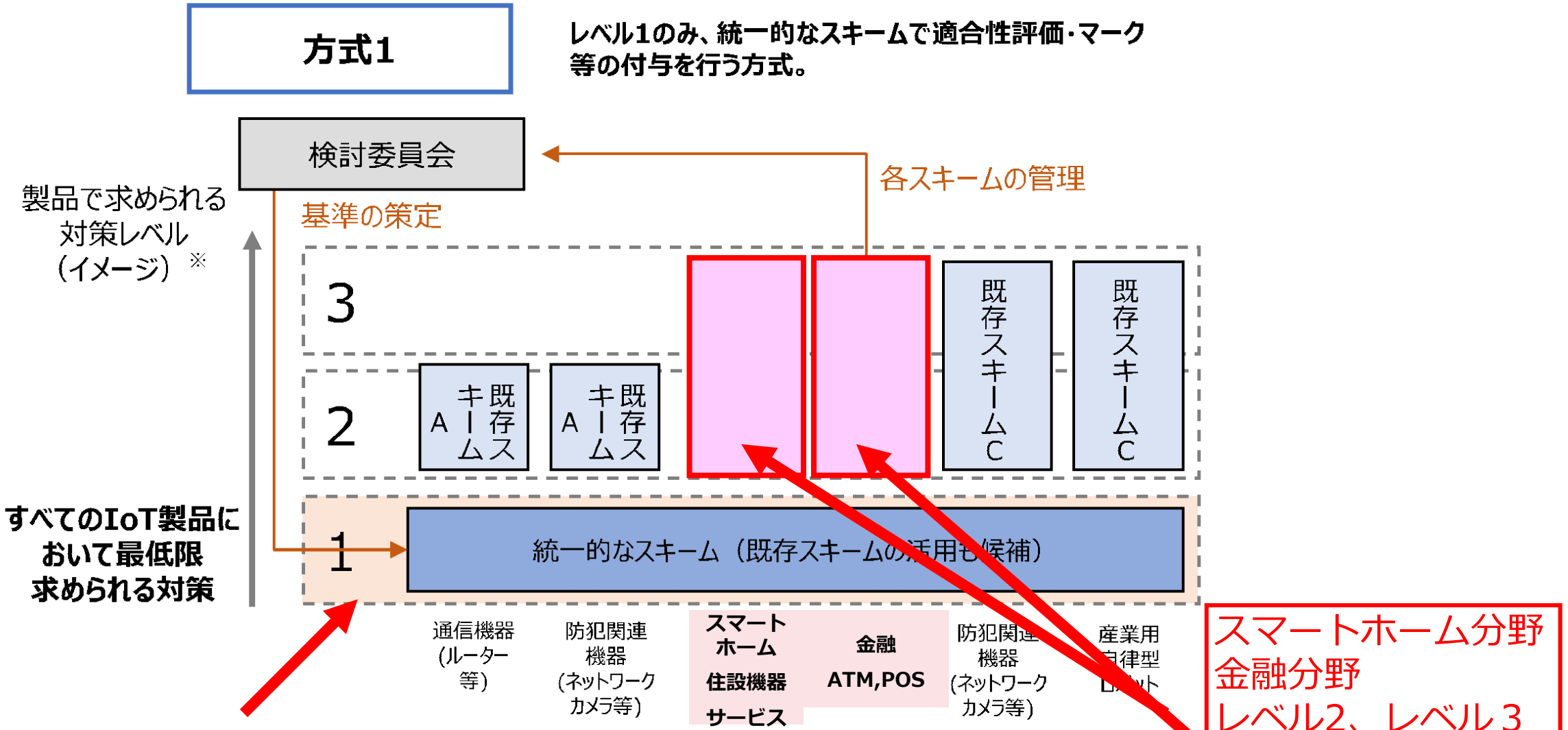
出典:IoT製品に対するセキュリティ
適合性評価制度の構築について,12.12.2023

CCDS

- 検討優先度の高い「特定分野のシステム」を選定し、各システム全体のセキュリティを考えている業界団体やワーキンググループと連携し、各システムに組み込まれるIoT製品に求めるセキュリティ要件を検討する。
- 各特定分野のシステムにおいて、IoT機器を選定する立場の事業者または当該IoT機器を生産するベンダーから、認証・ラベル制度の整備とその活用について一定割合以上の賛同が得られる場合（業界標準となり得ると判断される場合）、本制度として☆2以降の整備を進める。
- 各特定分野のシステム全体のセキュリティガイドラインの作成や、システム全体の認証制度等の整備は、各業界団体やワーキンググループで検討し、本制度はオブザーバーの立場で連携する。（公的機関でのシステム全体の認証制度の整備は、本制度とは分けてその必要性も含めて検討）



適合性評価制度スキーム　CCDSサーティフィケーションプログラム



資料：既存制度との連携・合流（将来像）

出典:IoT製品に対するセキュリティ適合性評価制度の構築について,7.19.2023

CCDS

既存適合性評価スキーム	概要	対象製品	本制度との連携イメージ（将来像）
CCDSサーティフィケーションプログラム （重要生活機器連携セキュリティ協議会(CCDS)）	• CCDSが定める「IoT機器セキュリティ要件ガイドライン」に基づき、指定検査資格者による検査により基準を満たしていると判断された場合、CCDSがマークを付与する仕組み	• インターネットに接続可能な機器及びシステム	• **CCDSサーティフィケーションプログラムを本制度に統合する。** • **策定する適合基準や評価手法について、これまでの検討実績や知見を踏まえ、必要に応じてCCDSとも連携して策定する。** 本制度に統合（適合済み製品には、本制度のマークを付与） 必要に応じてCCDSとも連携して策定 CCDS:CCDSサーティフィケーションプログラム 例）スマートホーム関連機器に関する基準等（☆2以降） 金融関連機器に関する基準等（☆2以降） … ☆1に関する基準等
BMSec（事務機セキュリティプログラム） （ビジネス機械・情報システム産業協会(JBMIA)）	• 「事務機セキュリティガイドライン」に基づきメーカー自身が自己適合宣言を行い、適合結果をJBMIAが確認・公開する仕組み	• エントリークラス/SOHO向けのOA機器	• **事務機の購入／調達者にとってより良い制度という観点でJBMIAにおいても検討を進める。** • **策定するOA機器の適合基準や評価手法について、これまでの検討実績や知見を踏まえ、必要に応じてJBMIAとも連携して策定する。** セキュアな事務機の可視化方法（マーク付与等）について、どのような形が最適かを検討する。 必要に応じてJBMIAとも連携して策定 JBMIA:BMsec OA機器に関する基準等（☆2以降）
RBSS （日本防犯設備協会）	• 防犯機器に必要とされる機器と性能の基準を策定し、その基準に適合した機器を「優良防犯機器」と認定する仕組み	• 防犯カメラとデジタルレコーダ • LED防犯灯	• **RBSSのセキュリティ基準は、本制度で策定した基準を参照するものとする。（具体的な参照方法については継続検討）** 本制度 セキュリティに関する基準の参照 日本防犯設備協会:RBSS （基準に適合した製品については、RBSSのマークが付与される。）

参考）適合基準の公開及びパブリックコメントの実施

実証に関するまとめ・今後の予定

- プレ委員会で議論したセキュリティ要件案・適合基準案・評価手順案に基づき、IoT製品（5ベンダー・10製品）に対して**適合性評価の評価検証を実施**し、**評価工数、基準案・手順案の妥当性、自己適合宣言による評価の妥当性等について確認を行った**。
- また、評価検証で得られた結果を踏まえて**セキュリティ要件案・適合基準案・評価手順案を修正した上で、プレ委員会で修正内容について議論を行った**。
- 今後、**①☆1のセキュリティ要件、②☆1適合基準、③各基準に対してNAとなるための条件の3点についてパブリックコメントを実施**し、**パブリックコメントを踏まえて修正した内容にて、制度を開始する**。なお、パブリックコメントにおいては、これら3点の**英語版も用意し、海外からの意見も受け付ける**。
- 来年度以降、☆2以上のセキュリティ要件、適合基準、評価手順に関する議論・検討を行う。☆2以上については、**優先度の高い製品類型について、関連する業界団体やワーキンググループと連携の上で、具体的な基準等に関して議論・検討を進める**。

パブリックコメントの実施
（3/15開始）

出典）METI適合性評価制度
第7回検討委員会
「資料3　IoT製品に対するセキュリティ適合性評価制度に関する実証について」

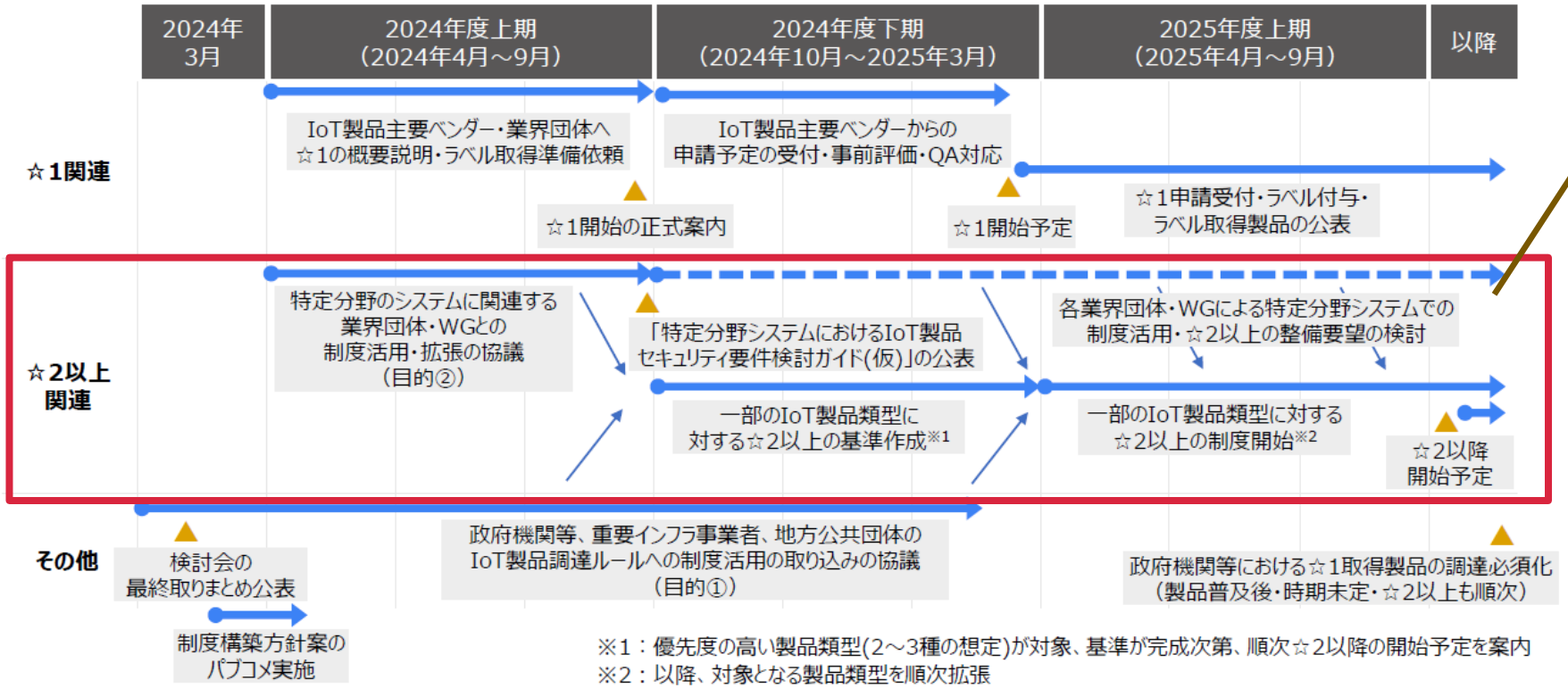
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/007.html

参考）2024年度～2025年度の検討ロードマップ案

IoTセキュリティラベリング制度(仮) ロードマップ案

- **2024年7～9月頃に制度開始の正式案内**を行い、**2024年度中（2025年3月頃）に☆１制度の開始**を目指す。
- ☆2以上は、2024年度の上期に制度活用・拡張の協議を行い、選定した一部のIoT製品類型に対する基準を下期に作成する想定。
  ☆２以上の制度開始は2025年度下期以降となる見込み。
- 並行して、**政府機関等へのラベル取得済みIoT製品調達の必須化**の調整および重要インフラ事業者・地方公共団体へのIoT製品調達ルールへの制度活用の取り込みの働きかけを行う。
- 欧米を含む主要国・地域とは、☆１基準案を共有し議論を進めている。☆１開始の正式案内時に制度が既に導入されているシンガポールと英国については、案内時に相互運用の方向性を提示。正式案内時に制度設計途中の見込みである欧米については、順次公表する。

☆1の制度開始
（2025年3月頃）



※1：優先度の高い製品類型(2～3種の想定)が対象、基準が完成次第、順次☆2以降の開始予定を案内
※2：以降、対象となる製品類型を順次拡張

☆２以降の検討ロードマップ

出典）METI適合性評価制度
第7回検討委員会
「資料4　IoT製品に対するセキュリティ適合性評価制度の構築について」

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/007.html

マーク制度とDX推進

考え方：

１）攻撃者優位のこの時代です！

２）経年劣化します！

３）被害を受けた後の対策を必ず想定しておきましょう！

対策の方針（セキュリティについての調達要件を策定しておく）ー＞マーク製品

１）防御は多層防御の視点で。　（人、組織、モノ、戦略。。。）

２）対策の費用対効果を見積る。　（効果ある対策から）

３）感染してしまった時の対策も考えましょう！　（レジリエンス能力の向上）

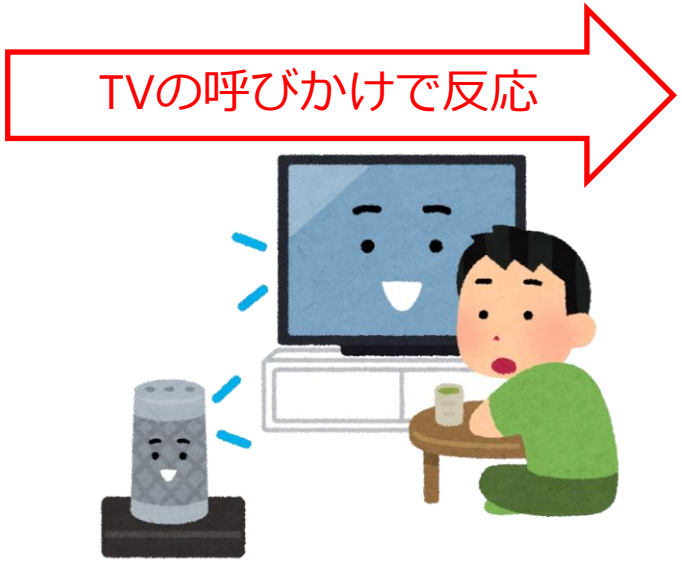
訓練の進め：

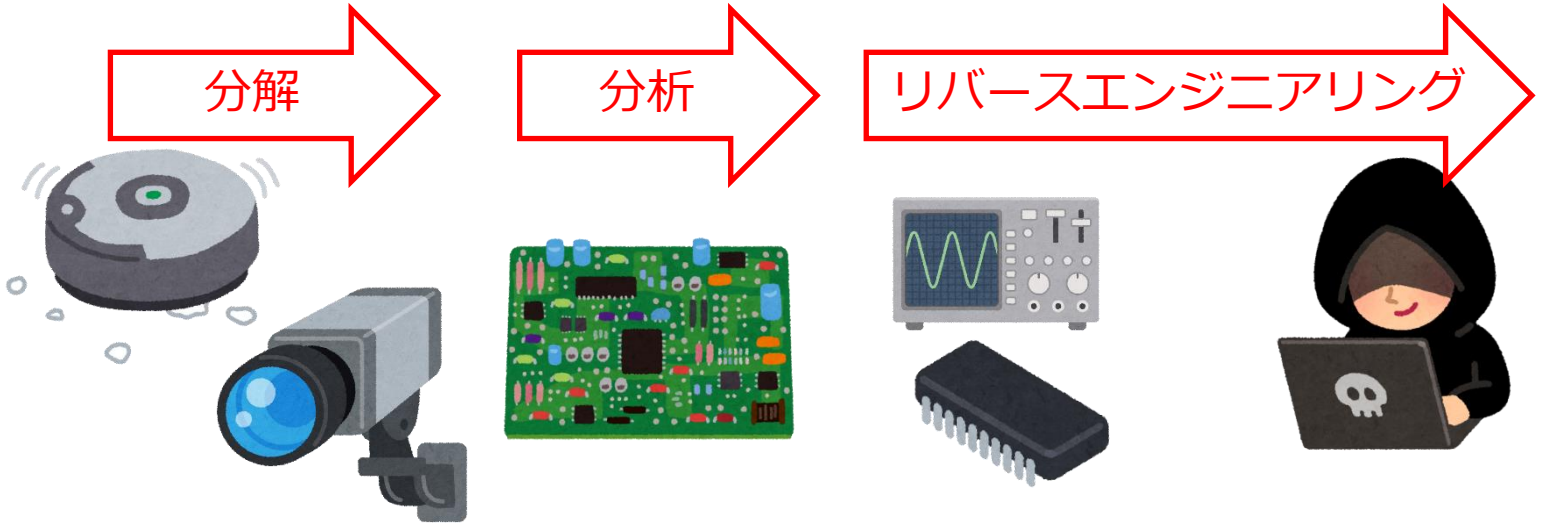
１）インシデント訓練は年1回　（例：バックアップからの復旧
組織の対応内容の実習）

今後に取り組むべき事項（メーカとしてユーザーとして）

セキュリティ要件：
- －サプライチェーン（SBOM?）
- －認証（Authentication）
  - －－暗号

体制・仕組み：
- －経年劣化への対応

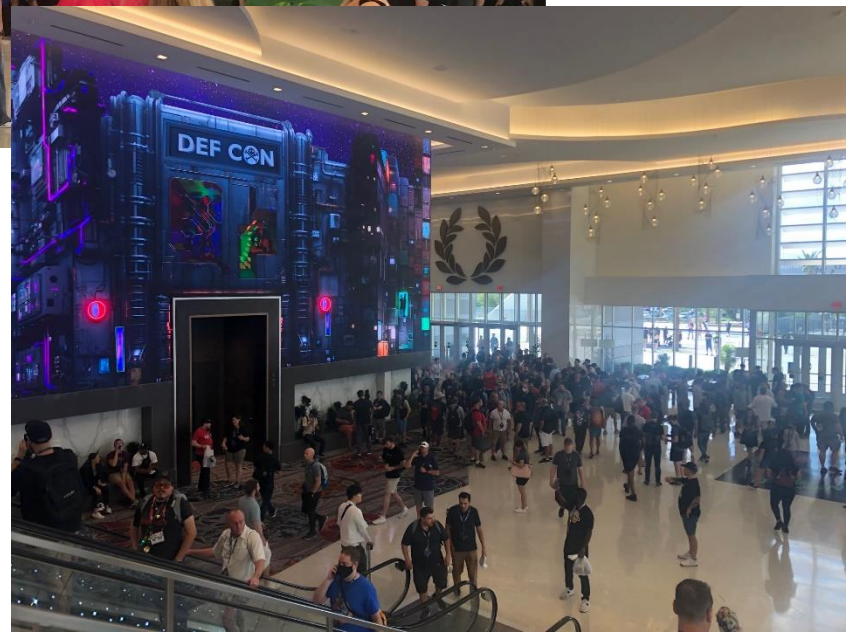




AIハッカーのコミュニティの活性化

DEFCON（2015->2023）

- 会期：2023年8月上旬　（4日間）
- 会場：ラスベガスのホテル会議室・ホール
- 参加者数：2015年：約1.5万人
  2016年：約2.2万人
  2017年：約2.5万人
  2018年：約2.7万人
  2019年：約3.0万人
  2021年：約0.9万人
  2022年：約2.5万人
  ★2023年：約2.5万人
- 参加者：学生から社会人まで

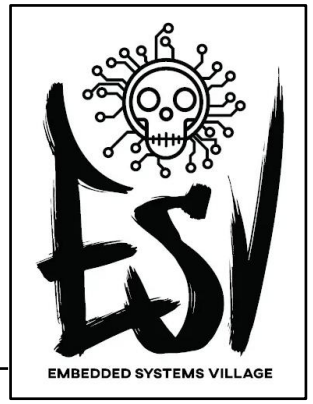


- IoTに留まらず、更に分野が拡大：
  - ◆ ICSビレッジ（2014年）
  - ◆ IoTビレッジ（2015年）
  - ◆ AIビレッジが出現（2018年）
  - ◆ Aerospaceビレッジ（2021年）
  - ◆ XRビレッジ、Embedded Systemビレッジ（2023年）

Village （同好の集まり）：2023年の状況

- 興味を持った人たちが集まって、ミニ講演会やワークショップや展示などを実施
  (下記赤は今年から)

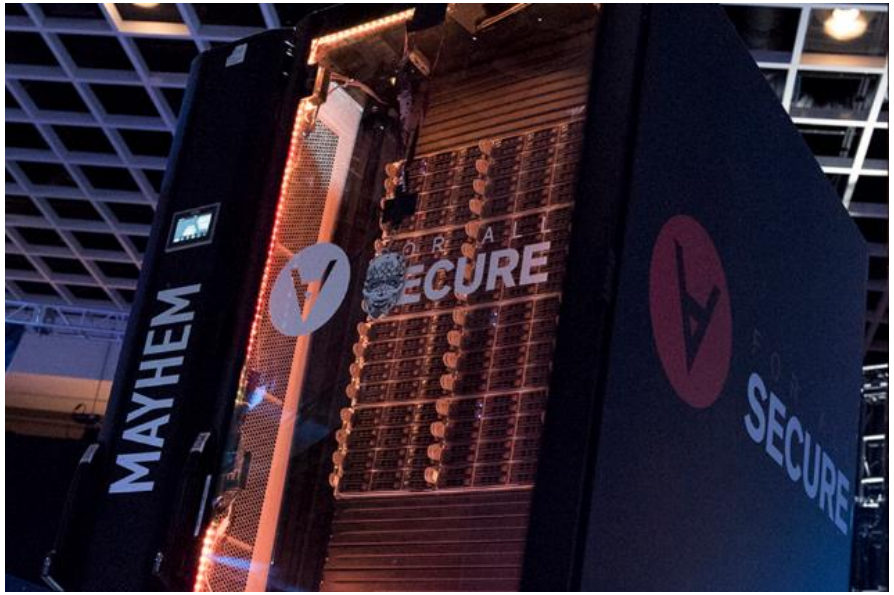
- A.I. Village
- DEFCON GROUPS VR (DCGVR)
- XR Village ★2023年から
- Blue Team Village
- Aerospace Village　★2021年にAviation Villageから拡張
- Biohacking Village
- Crypto & Privacy Village
- Appsec Village
- Blacks In Cyber Village
- Carhacking Village
- Cloud Village
- Data Duplication Village
- Embedded Systems Village　★2023年から
- Ham Radio Village
- Hardware Hacking Village & Soldering Skills Village
- ICS Village　★2014年から



- Lockpick Village
- Misinformation Village
- IoT Village　★2015年から
- Packet Hacking Village
- Payment Village
- Physical Security Village
- Password Village
- Quantum Village
- Policy@DEFCON
- Radio Frequency Village
- Telecom Village
- Tamper Evident Village
- Recon Village
- Red Team Village
- Social Engineering Community Village
- Voting Village

CGC（Cyber Grand Challenge）DARPA 優勝賞金 2 億円

- 機械vs機械（攻撃と防御）
- 環境：
  - ◆ Intel Xeon サーバー（水冷式ラック）
  - ◆ 主催が用意した、プログラム＆サーバ環境
- 脆弱性自動検出ー＞防御パッチ自動生成ー＞
  攻撃コード自動生成
- 優勝：カーネギーメロン大学のForAllSecure チームの「Mayhem」



https://www.cybergrandchallenge.com/

DARPA：人工知能サイバー チャレンジ　賞金総額 1,850 万ドル
The Artificial Intelligence Cyber　Challenge(AIxCC)

バイデン・ハリス政権は、人工知能（AI）を利用して、インターネットや重要インフラの運営に役立つコードなど、米国の最も重要なソフトウェアを保護する2年間にわたる大規模なコンペティションを開始した。

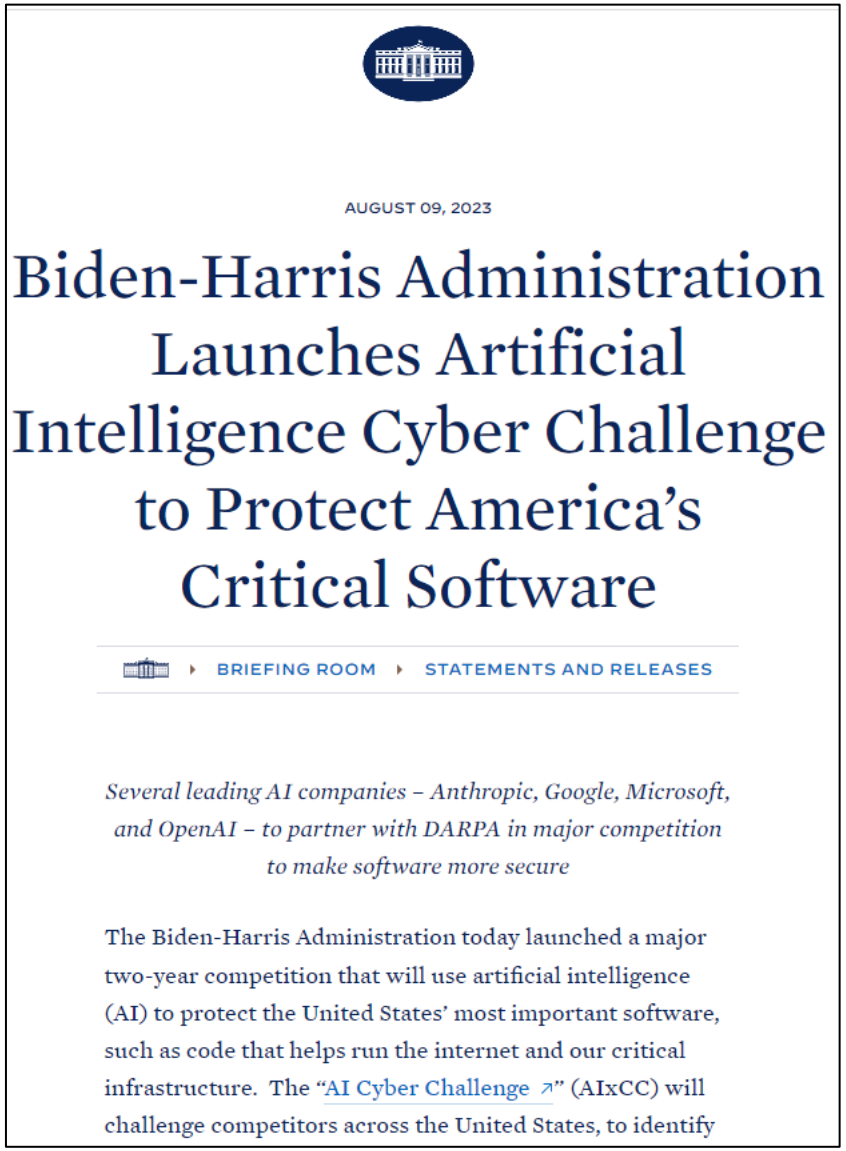
「AIサイバーチャレンジ」」（AIxCC）は、AI を使用してソフトウェアの脆弱性を特定して修正するという課題に挑戦。

Anthropic、Google、Microsoft、OpenAI といったトップ AI 企業数社との協力、専門知識、最先端のテクノロジーを利用できるよう協力

このコンテストは、サイバーセキュリティの最も差し迫った課題の 1 つであるコンピューター コードのセキュリティを急速に向上させるための新技術の開発を促進します。

今年初め、政権は、複数の AI 企業が DEF CON 2023 で大規模言語モデル (LLM) の公開評価に参加するというコミットメントを発表しました。この演習は今週後半（2023年8月）に開始されます。複数の LLM に対する史上初の公開評価は、より安全で透明性の高い AI 開発の推進を目指します。

- https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/biden-harris-administration-launches-artificial-intelligence-cyber-challenge-to-protect-americas-critical-software/



AUGUST 09, 2023

Biden-Harris Administration Launches Artificial Intelligence Cyber Challenge to Protect America's Critical Software

BRIEFING ROOM › STATEMENTS AND RELEASES

Several leading AI companies – Anthropic, Google, Microsoft, and OpenAI – to partner with DARPA in major competition to make software more secure

The Biden-Harris Administration today launched a major two-year competition that will use artificial intelligence (AI) to protect the United States' most important software, such as code that helps run the internet and our critical infrastructure. The "AI Cyber Challenge" (AIxCC) will challenge competitors across the United States, to identify

DARPA：人工知能サイバー チャレンジ　賞金総額 1,850 万ドル
The Artificial Intelligence Cyber　Challenge(AIxCC)

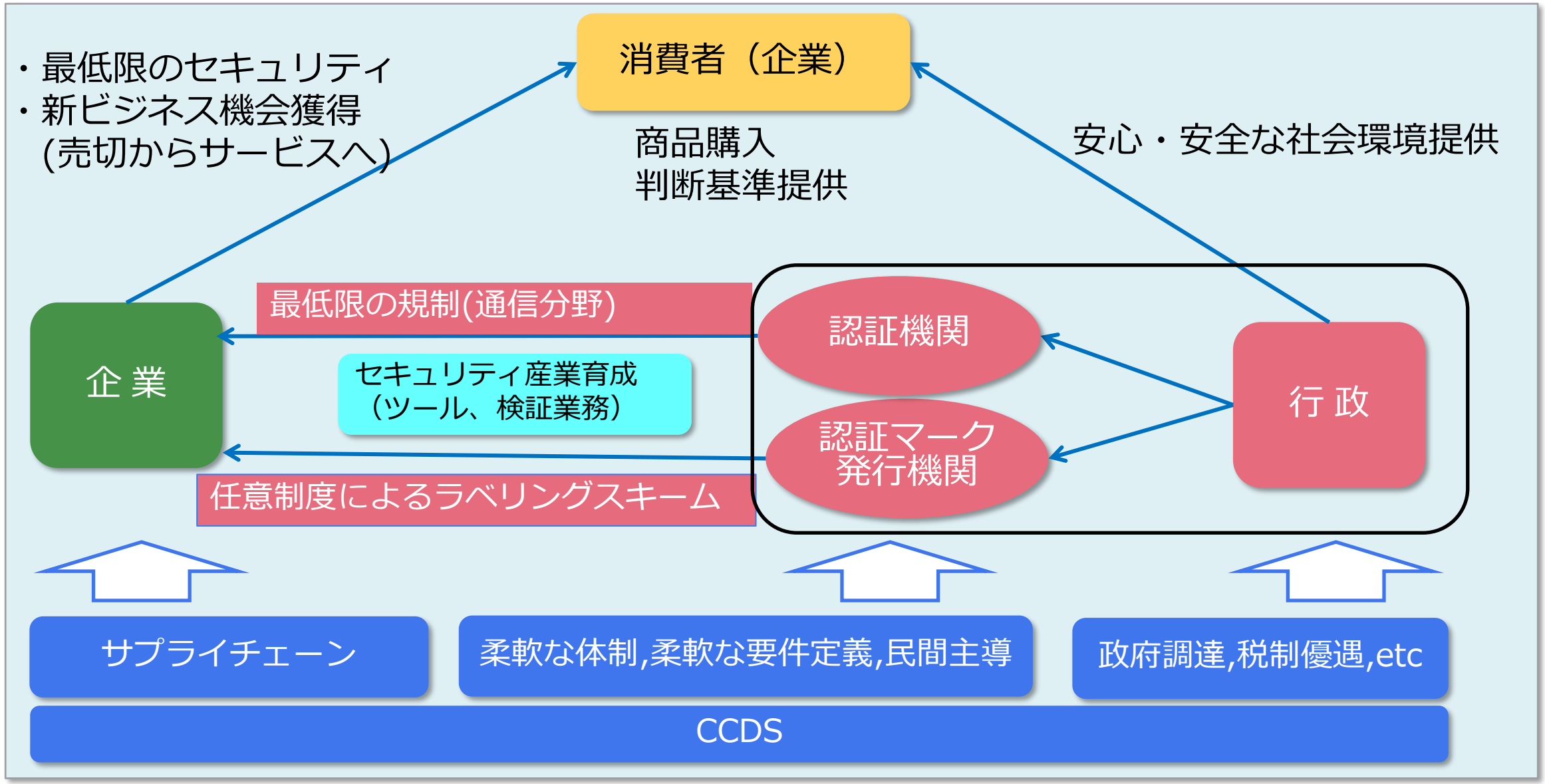
https://aicyberchallenge.com/

- 2023年8月9日　発表
- 2023年8月17日～ 10月3日　資金提供募集
  ー＞100万ドルの支援（7チーム）
- 2023年11月1日～ 12月15日　オープントラック募集
- 2024年2月　キックオフイベント
- 2024年5月　QUALIFYING COMPETITION(AQC)
  20チームを選抜
- 2024年8月　SEMIFINAL COMPETITION(ASC)
  上位５チーム：各200万ドル
- 2025年8月　FINAL COMPETITION(AFC)
  1st:400万ドル, 2nd :300万ドル, 3rdd :150万ドル

- 協賛：Anthropic、Google、Microsoft、OpenAI
- 2 年間のコンテスト

重要なコードを保護するための新しい AI システムの設計

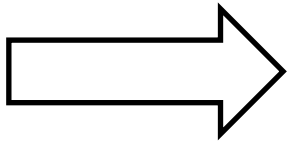
CCDSの活動のポジション（安心・安全な環境に向けて）



GR01-2021

SH02-2021

SH03-2021



GR01-2023

ご清聴ありがとう御座いました

【セキュリティガイドライン】
https://www.ccds.or.jp/public_document/index.html

【サーティフィケーションプログラム】
https://www.ccds.or.jp/certification/index.html

CCDSサーティフィケーション

GR01-2019

■2023年要件の概要

【デバイス側の新設要件】

・要件1-2：データ保護　新設

・要件3-1：ログの記録　新設

【機器メーカ、運用面に対する新設要件】

・要件2-2：製品に関する文書管理

・要件2-3：利用者への情報提供

分野別マーク始動！
IoTサービスへ対象を拡大！

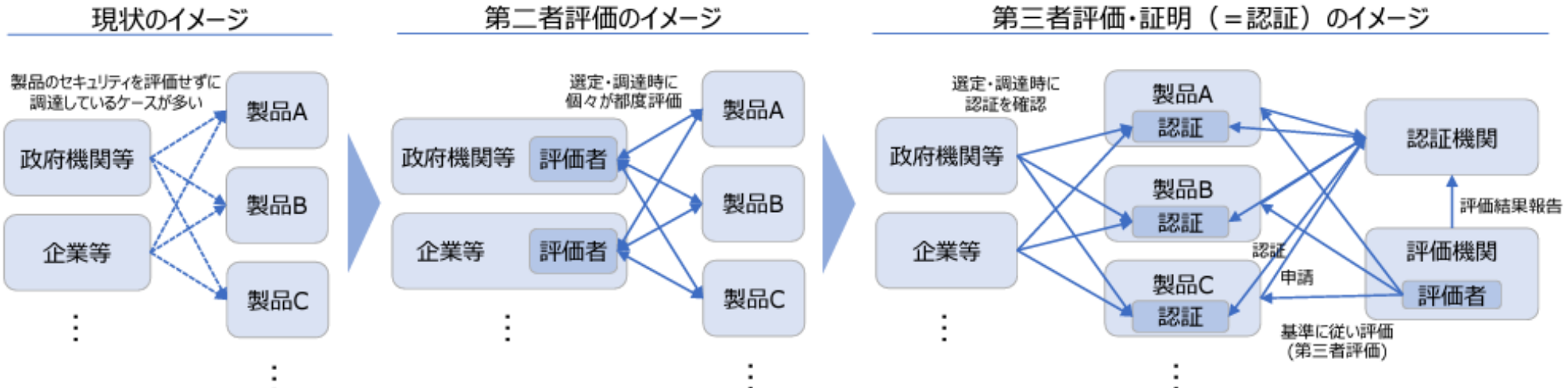
例：リモートロックシステム
・サーバ、ネットワーク、IoT機器への要件を規定

資料：目的①政府機関等・企業等の IoT製品調達ニーズへの対応

出典:IoT製品に対するセキュリティ適合性評価制度の構築について,12.12.2023

CCDS

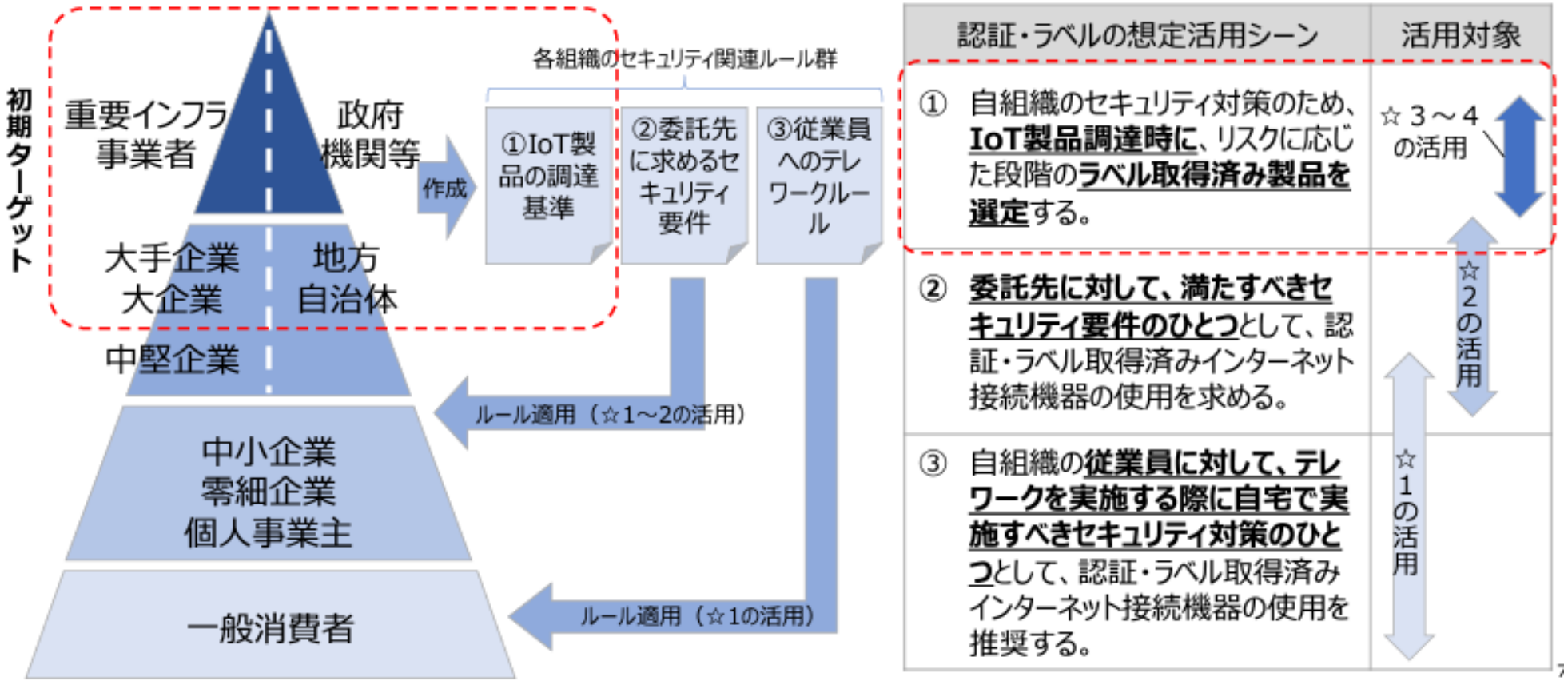
- 政府機関等・企業等のセキュリティ対策において、**調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーンリスク管理の取り組みが広がっている**。
- その際、IoT製品のセキュリティに関して、選定時や調達時に、その**セキュリティ機能や対策状況を自組織で確認すること（第二者評価）が本来必要であるが、そのための確認プロセスを整備できている政府機関等・企業等は少ないのが現状**である。一方、仮に政府機関等・企業等がそのプロセスを整備する場合、調達を行う各組織においてその**確認のための知識と工数が必要**となり、またIoT製品ベンダーは各者から**異なる要件に対して繰り返し回答・対応が求められ**、双方対応しきれなくなる。
- そこで、第二者評価を代替する仕組みとして、**共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度**を整備する。政府機関等・企業等は**認証取得の確認をベースとして活用**しながら、必要な場合に追加的な確認を実施することで、各組織の求めるセキュリティ水準のIoT製品を選定・調達することが可能となる。
- **政府機関等の第二者評価の代替として公平・中立な認証を行うためには公的機関（IPA）が認証機関**となり、制度を維持・運営していくことが望ましい。



資料：目的①展開戦略と初期ターゲット

出典:IoT製品に対するセキュリティ
適合性評価制度の構築について,12.12.2023

- **政府機関等・地方自治体**および**重要インフラ事業者を含む大手企業・大企業を初期ターゲット**とし、セキュリティ関連ルール等に**①のIoT製品調達時の認証取得済み製品の選定を含める**ことをまずは目指す。
- **政府機関等・地方自治体には、強制力を持たせる**ようにNISC・デジ庁・総務省と必要性を合意し、各種基準に盛り込む。
- **重要インフラ事業者には、NISCと協議して行動計画に含め**たうえで、所管省庁・業界団体と連携して取り組みを促す。
- その他の民間企業への直接的な強制・推奨は難しいため、各業界団体や各業種のISAC等と連携して取り組みを促す。

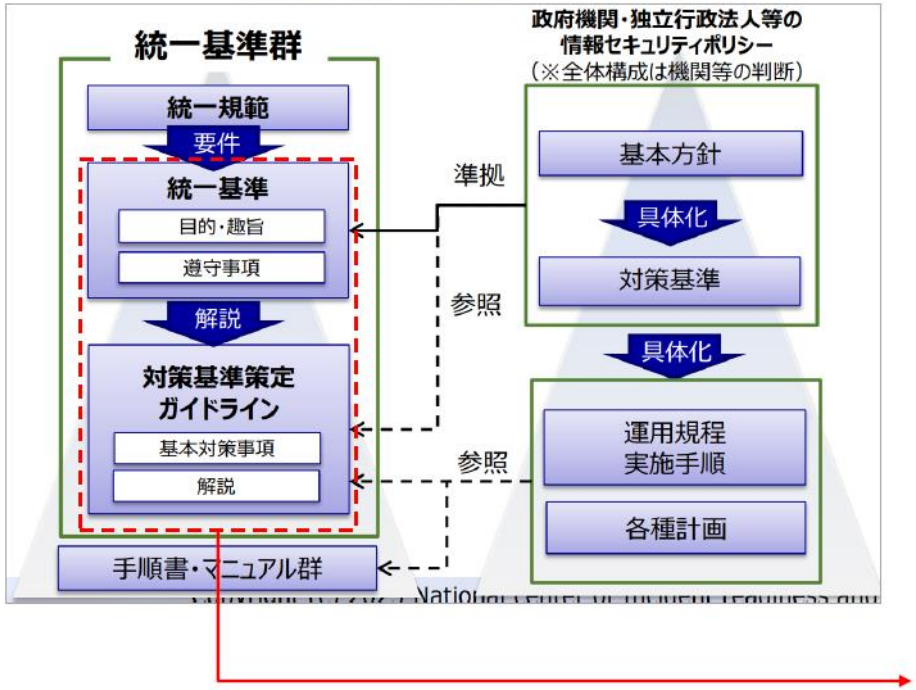


参考）調達基準への追加①（政府機関）

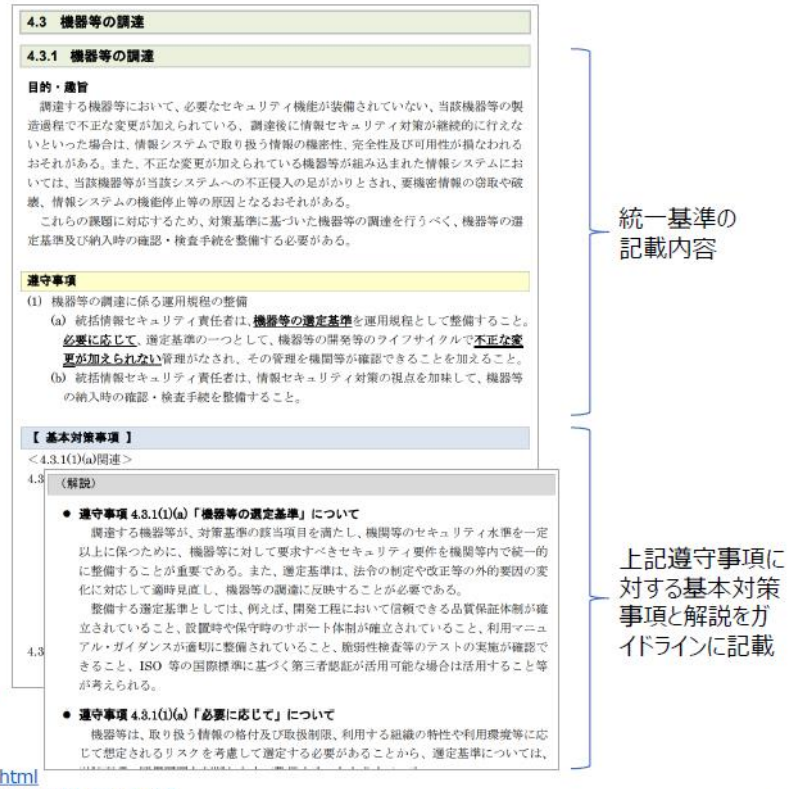
調達者の本制度活用に関する調整状況（政府機関等）

- 政府機関等が遵守すべき事項を定めた「政府機関等のサイバーセキュリティ対策のための統一基準」およびそのガイドラインに、情報システムの重要度に応じ、**「重要度：低」は☆1以上**、**「重要度：高～中」は少なくとも☆3以上のIoT製品を各機関等の選定基準に含める**ことの追加をNISCと検討している。
- ラベル取得済み製品が普及する時期をめどに、政府機関等では**ラベル取得済みIoT製品の調達を必須化する方針**。

統一基準群（令和５年度版）文書体系



対策基準策定ガイドラインの「4.3.1 機器等の調達」の記載


4.3 機器等の調達

4.3.1 機器等の調達

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

これらの課題に対応するため、対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、**機器等の選定基準**を運用規程として整備すること。**必要に応じて**、選定基準の一つとして、機器等の開発等のライフサイクルで**不正な変更が加えられない**管理がなされ、その管理を機関等が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

（解説）

● **遵守事項 4.3.1(1)(a)「機器等の選定基準」について**

調達する機器等が、対策基準の該当項目を満たし、機関等のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を機関等内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。

整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

● **遵守事項 4.3.1(1)(a)「必要に応じて」について**

機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、

統一基準の記載内容

上記遵守事項に対する基本対策事項と解説をガイドラインに記載

出所）NISC「統一基準群改定のポイント（令和５年度版）」https://www.nisc.go.jp/policy/group/general/kijun.html
NISC「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

政府機関の調達基準として追加を検討中。
※「政府機関等の対策基準策定のためのガイドライン」

出典）METI適合性評価制度
第7回検討委員会
「資料4　IoT製品に対するセキュリティ適合性評価制度の構築について」

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/007.ht

参考）調達基準への追加②（地方公共団体）

調達者の本制度活用に関する調整状況（地方公共団体）

- 総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」では、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説されている。
- その中の「情報セキュリティ対策基準」では、IoT機器を含む特定用途機器のセキュリティ管理や情報システムの調達について言及されており、政府統一基準の改定を踏まえ、IoTセキュリティ適合性評価制度のラベルを取得した製品の調達についての追記を検討する。

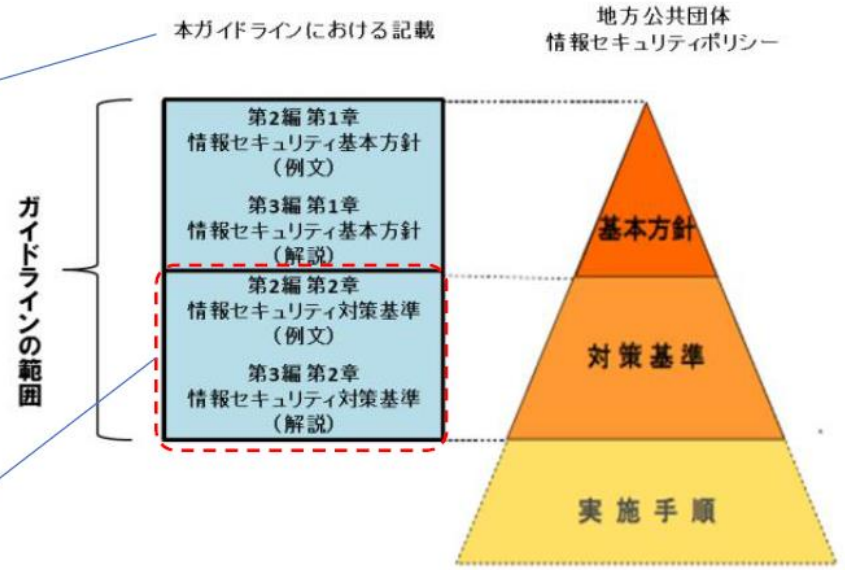
ガイドラインでは以下が示されており、各地方公共団体において、組織の実態に合わせ、必要に応じて推奨事項も含めて、情報セキュリティポリシーを策定することが期待されている。
（第１編 第４章 2.本ガイドラインにおける対策レベルの設定）

- 特段の理由がない限り**対策を講じることが望まれる事項**
  ＋
- **推奨事項**（必要性の有無を検討し、必要と認められる時に選択して実施することが望ましいと考えられる対策事項）

対策基準の以下の関連項目に、IoT製品を選定・調達する際にIoTセキュリティ適合性評価制度を活用することの記載追加を検討したい。（文案は次頁）

- 6.1. コンピュータ及びネットワークの管理
  （１２）IoT 機器を含む特定用途機器のセキュリティ管理
- 6.3. システム開発、導入、保守等
  （１）情報システムの調達

「地方公共団体における情報セキュリティポリシーに関するガイドライン」の構成と地方公共団体情報セキュリティポリシーの対応関係



出所）総務省「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html

地方公共団体の調達基準として追加を検討中。

※「地方公共団体における情報セキュリティポリシーに関するガイドライン」

出典）METI適合性評価制度
第7回検討委員会
「資料4　IoT製品に対するセキュリティ適合性評価制度の構築について」

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/007.ht