経済産業省

IoT製品に対するセキュリティ適合性評価制度について

2025年 2月18日

経済産業省 商務情報政策局 サイバーセキュリティ課

サイバーセキュリティ戦略専門官
山田　剛人

1. サイバーセキュリティを取り巻く現状

2. 経済産業省のサイバーセキュリティ政策

3. IoT製品に対するセキュリティ適合性評価制度の概要

（１）IoTセキュリティの重要性

（２）制度の概要

（３）制度普及に向けた取組み

（４）今後のスケジュール

サイバー攻撃の現状

- 「**ランサムウェア攻撃**」や「**サプライチェーンの弱点を悪用した攻撃**」により、甚大な影響が生じている。また国家支援型の攻撃集団等が特定の企業を執拗に狙う「**標的型攻撃**」も大きな課題。
- 社会のデジタル化は進展する一方、AI等のデジタル技術の発展や地政学情勢の不安定化の影響もあり、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれ**。

情報セキュリティ10大脅威 2024

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

（出典）（独)情報処理推進機構(IPA)、2024.1.24

デジタル技術の発展によるサイバーリスクの増加の例

- 情報システムの利用拡大やクラウド等の活用拡大、インターネットに接続されるIoT製品の急増（2019年：231億台⇒ 2024年：399億台）など**サイバー空間の利用拡大**等に伴い、サイバー攻撃を受ける**システム側の侵入口が増加**。
- スピアフィッシングやビジネスメール詐欺等の実行を支援する**サイバー犯罪用の生成 AI ツールも登場**。

- NICTER において2023年に観測した**サイバー攻撃関連通信数は増加傾向**であり、約6,197億パケット（2018年の約３倍）。中でも、**IoT機器を狙った攻撃関連通信が多い**。
- フィッシング対策協議会によると、2023年における**フィッシングの報告件数は100万件超**（2019年の約20倍まで増加）。

（出典）総務省「令和 5 年度版情報通信白書データ集」、(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2024」解説書、(国研)情報通信研究機構「NICTER観測レポート2023」、フィッシング対策協議会「月次報告書」 等

サイバーセキュリティ政策に関する国際的な動向

- **欧米中心に、重要インフラ事業者等におけるサイバーセキュリティ対策の強化に関する制度整備が加速**。
- **セキュア・バイ・デザイン**＊1**の概念が国際的に支持**＊2**を集める**など、企業は自社をサイバー攻撃から守ることのみならず、**自社が提供する製品のサイバーセキュリティ対策についても問われる時代に**なりつつある。

重要インフラ事業者等に関する制度整備

*1 IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。
*2 日米含む13か国の政府機関等が2023年10月にセキュア・バイ・デザイン等の実践に向けた推奨事項をまとめたガイダンスに共同署名。

重要インフラに係るサイバーインシデント報告法（Cyber Incident Reporting for Critical Infrastructure Act of 2022）	• 米国の16の「重要インフラ」セクターに対し、①**重大なサイバーセキュリティインシデント**について発生を認知後**72時間以内**、②**ランサム支払い**について支払い後**24時間以内に米CISAに報告すること等を義務付け**。 • 2022年3月に成立、2024年4月に規則案のパブコメ開始。施行は2025年秋を想定。
米国証券取引委員会開示規則（SEC Form 8-K）	• 登録企業に対し、①サイバーセキュリティインシデントに重要性があると判断してから**4営業日以内に、当該インシデントの性質、影響等の開示**、②**リスク管理、戦略、ガバナンスの年次開示等を義務付け**。 • 2023年7月に採択、2023年12月18日より運用開始。
NIS 2指令（Directive (EU) 2022/2555）	• **2016年NIS指令から対象セクターを拡大**の上、対象「主要エンティティ」、「重要エンティティ」に対し、①**サイバーセキュリティ・リスクマネジメントの強化**、②**重大なサイバーセキュリティインシデントについて**発生を認知後**24時間以内に早期警告、72時間以内にインシデント通知をCSIRT又は管轄省庁に報告すること等を義務付け**。 • **2023年1月発効、2024年10月18日より執行予定**、それまでに加盟国が国内法に反映予定。

セキュア・バイ・デザインの要請

PSTI法（Product Security and Telecommunication Infrastructure Act）	• **消費者向けIoT機器の製造者に対し**、デフォルトパスワードを使用しない等の**最低減のセキュリティ基準への自己適合宣言を義務化**。 • 2022年12月に国王裁可し、下位法制定を経て**2024年4月29日より施行予定**。
サイバーレジリエンス法案（Cyber Resilience Act）	• **デジタル要素を備えた全ての製品（ソフトウエア含む）の製造者に対し、**①セキュリティ特性要件に従った**上市前の設計製造**、② **上市後に積極的に悪用された脆弱性、インシデント**について**認識後24時間以内の早期警告通知**、**72時間以内の通知をCSIRTに報告すること等を義務付け。** • 2023年11月に暫定合意。**報告義務の運用開始は2025年秋～冬、その他は2027年夏頃運用開始を想定。**

（出典）各種公開情報に基づき経済産業省作成

国家安全保障戦略に基づく政府の検討の方向性

現在の課題

- 我が国に対する**安全保障上の懸念となる重大なサイバー攻撃のおそれ**がある場合、これを**未然に排除し、または既に発生した被害の拡大を防止する必要**があるが、このための**制度や体制が整備されていない。**
- このままでは、海外の脅威主体等からの重大なサイバー攻撃により**社会インフラの機能の停止や重大な犯罪被害が発生**し、**有事の際の対応にも支障を来す**可能性がある。

国家安全保障戦略の記述

- **武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入**する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

（ア）重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

（イ）**国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

（ウ）**国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

- 能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する**。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。

⇒現在、内閣官房サイバー安全保障体制整備準備室において必要な法案の検討作業を実施中。
NISCについては今夏、次官級ポストの設置など順次組織を拡大。

1. サイバーセキュリティを取り巻く現状

2. 経済産業省のサイバーセキュリティ政策

3. IoT製品に対するセキュリティ適合性評価制度の概要

（１）IoTセキュリティの重要性

（２）制度の概要

（３）制度普及に向けた取組み

（４）今後のスケジュール

経済産業省におけるサイバーセキュリティ政策の全体像

- サイバー攻撃の高度化・多様化が生じている現状を認識しつつ、我が国**産業界へのサイバー攻撃を抑制・防御**し、事業活動への影響を最小化する。そのための政策を企画・実行する。
- その上で、各種の取組を、**我が国産業競争力の強化**につなげる。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

サイバーセキュリティ CSお助け隊

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

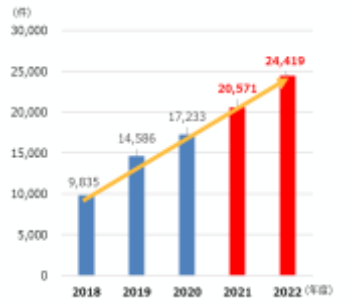
②国際連携を意識した認証・評価制度等の立上げ

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

③政府全体でのサイバーセキュリティ対応体制の強化

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃被害情報の共有促進に向けた検討

サイバー攻撃事案の調整件数（年度集計）



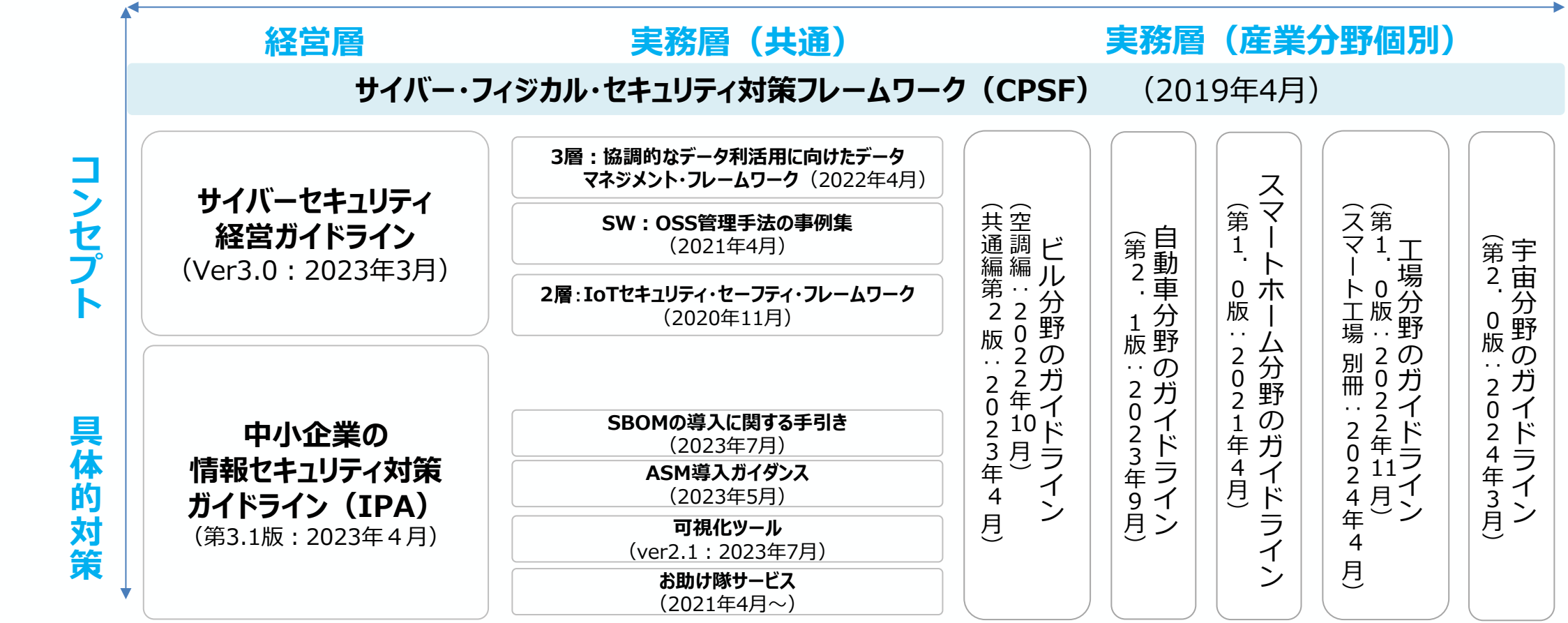
④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業振興）

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討

CPSFを軸とした各種取組

- CPSFに沿って、**対象者や具体的な対策を整理**し、実践的なガイドラインを整備。

主なガイドラインや対策ツール



中小企業向けセキュリティ対策

- **中小企業の情報セキュリティ対策ガイドライン（第3.1版 2023年4月）**

  中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、を実践する際の手順や手法をまとめたもの。
  付録としてクラウドサービスの安全利用やセキュリティインシデント対応に関する手引きなどがある

中小企業の情報セキュリティ対策ガイドライン

経営者向けの解説
経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説
企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

付録6、8:クラウドサービス安全利用の手引き、セキュリティインシデント対応手引き

【クラウドサービス導入時の考慮ポイントの例】

- ✓ 選択時のポイント（利用業務の明確化、取り扱う情報の重要度確認、クラウドサービスの安全・信頼性確認　等）
- ✓ 運用時のポイント（管理担当者、利用者範囲の決定　等）
- ✓ セキュリティ管理のポイント（利用者サポート体制の確認、利用終了時のデータ確保、適用法令や契約条件の確認　等）

【セキュリティインシデント対応時等の例】

- ✓ インシデント対応の基本ステップ（ステップ１　検知・初動対応、ステップ２　報告・公表、ステップ３　復旧・再発防止）に関する具体例
- ✓ インシデント発生時の相談窓口・報告先　等

- **「SECURITY　ACTION」**

  中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。30万者を超える中小企業が宣言。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

- **サイバーセキュリティお助け隊サービス**

  相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など各種サービス内容を要件としてまとめた基準を満たすワンパッケージサービス。（2024年４月時点で40事業者）

サイバーセキュリティ お助け隊

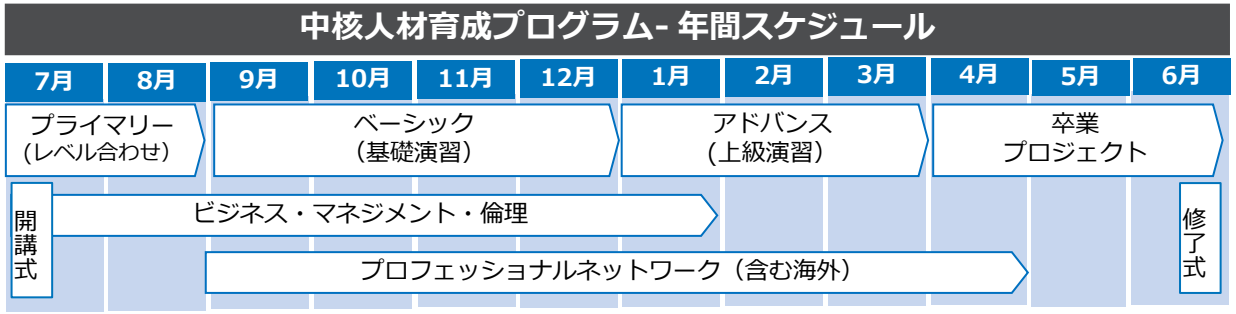
IT導入補助金に
「セキュリティ推進枠」創設

IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人）



- **IT系・制御系に精通した専門人材の育成**
- **模擬プラントを用いた対策立案**
- **実際の制御システムの安全性・信頼性検証等**
- **攻撃情報の調査・分析**

現場を指揮・指導するリーダーを育成

□　米・英・仏等の海外とも協調したトレーニングを実施

➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

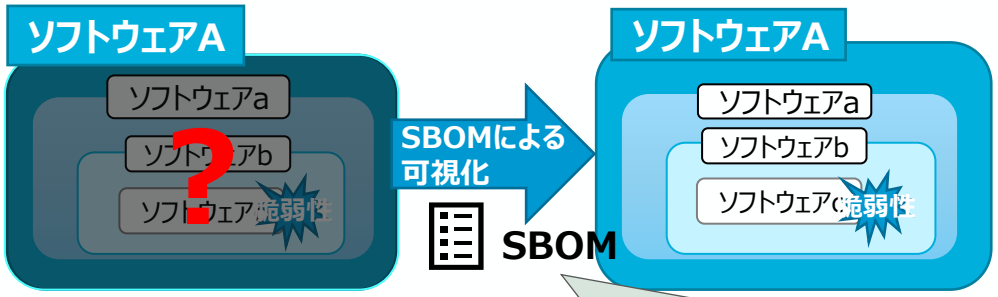
➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

など

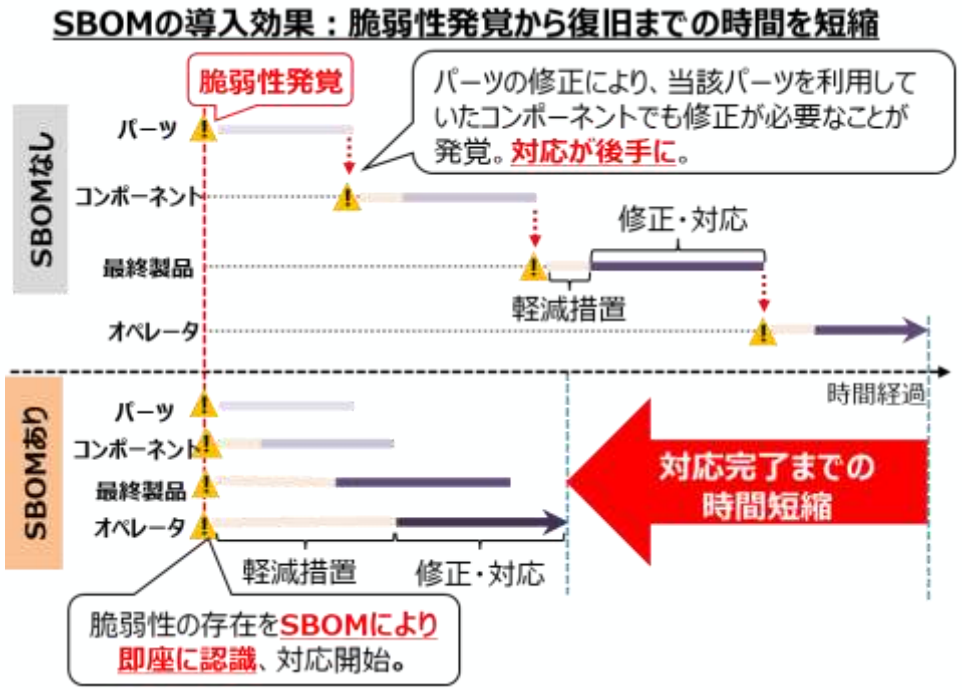
ソフトウェア・セキュリティ確保手段としてのSBOM

- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。
- SBOMにより脆弱性情報の即時の特定が可能である一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示した**「ソフトウェア管理に向けたSBOMの導入手引き」を公表。2024年8月29日に改訂版を公表。**

＜SBOMイメージ＞



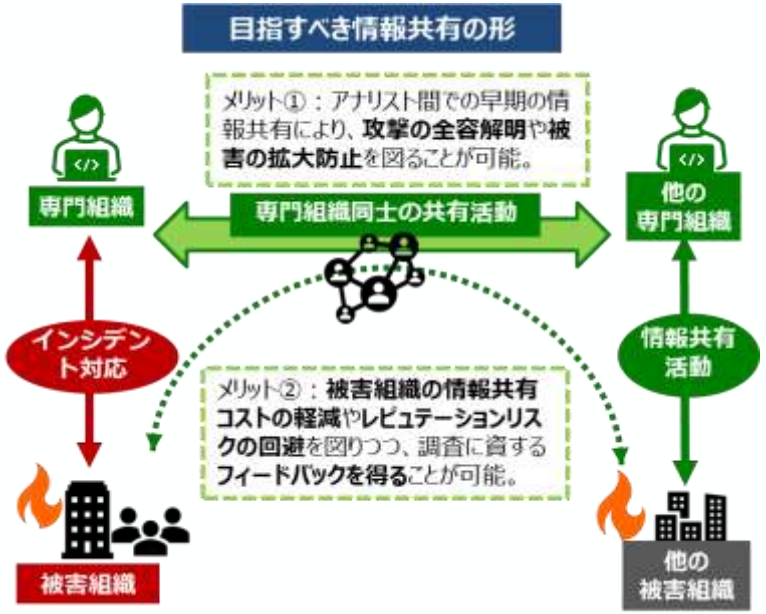
サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…



サイバー被害情報の情報共有の更なる促進に向けた対応
（専門組織間の情報共有）

- サイバー攻撃が高度化する中、攻撃の全容の把握や被害の拡大を防止する等の観点から、**被害組織を直接支援する専門組織を通じたサイバー被害に係る情報の速やかな共有が重要**。
- これまで、**被害組織における情報共有・公表**及び**専門組織を通じた速やかな情報共有**について、それぞれの組織において**実務上参考となるガイダンスや手引き等を整備**。今後、これら成果物に関し**専門組織やユーザー企業の経営層への意識啓発も含めた周知・啓発活動を行う。**

＜参考＞専門組織を通じた速やかな情報共有の促進に向けた対応



- 最終報告書において、**被害組織の同意を個別に得ることなく専門組織間で速やかに情報共有することが可能な情報として「攻撃技術情報」※を整理**し、そうした考え方に基づく専門組織間での円滑な情報共有を提言。
  ※通信先情報やマルウェア情報などから被害組織が推測可能な情報を非特定化したもの。
- 最終報告書の**提言を補完する２つの文書**（以下①②）**を提示。**
  ① 専門組織向けに、**効果的な共有対象となる情報や非特定化加工の方法**といった専門組織同士の情報共有における論点について、複数のユースケースも用いつつ解説した**手引き**
  ② 被害組織と専門組織が共通の認識を持ち、情報共有について合意するための**秘密保持契約に盛り込むべきモデル条文**
- さらに、最終報告書では、専門組織同士の情報共有促進だけでは解消されない**今後の課題として、情報共有に向けた官民連携のあり方 、サプライチェーンにおけるベンダ等の役割について提言。**

先進的サイバー防御機能・分析能力強化のための研究開発

- 経済安全保障重要技術育成プログラムにおいて、**サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等の研究開発を実施予定（320億円を超えない範囲／5年）。
- 2023年10月に具体的な研究開発の構想を決定。これに基づき、同年12月に公募を開始し、外部有識者による審査等も踏まえた上で、実施事業者を採択。**昨年７月から研究開発を開始**。

目的

- サイバー空間において提供される多様なサービスが複雑化するに伴い、サイバー空間内やサイバーとフィジカルの垣根を超えた主体間の「相互連関・連鎖性」が一層深化。近年では、**人工知能（AI）**を活用した攻撃に代表される**新たなサイバー攻撃のリスク**や、**量子計算機の活用**の広がりに伴う**既存暗号の危殆化によりデータが漏洩するリスク**が顕在化。
- **サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等を開発し、我が国のサイバー領域における状況把握力・防御力を飛躍的に向上させることを目的とする。

実施内容

（１）サイバー空間の情報を収集・調査する状況把握力の向上

- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

（２）サイバー攻撃から機器やシステムを守る防御力の向上

- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

（３）共通基盤の整備

- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

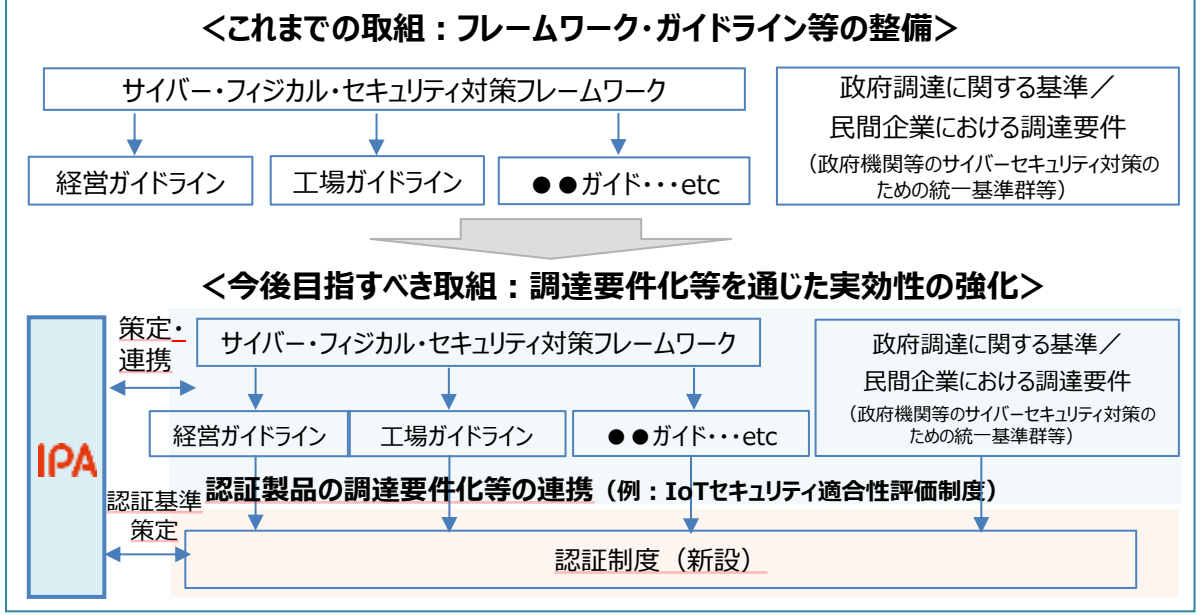
（４）セキュアな量子情報通信技術の開発

- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発

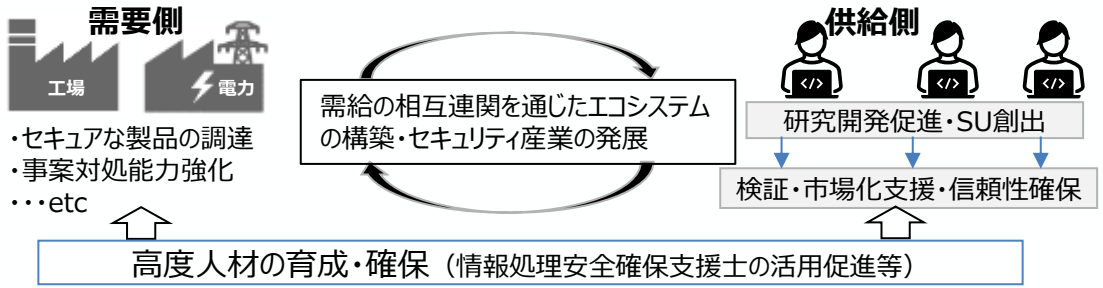
新たなサイバーセキュリティ政策の方向性

- サプライチェーン全体での対策強化に向け、これまでソフトロー・アプローチとして、経営層の意識改革の促進、各種のフレームワーク・ガイドライン等の策定を実施。
- 今後、関係省庁と連携し、**政府調達等への要件化を通じた実効性の強化、国産製品の開発・普及促進や高度人材の育成・確保**、サイバー安全保障の実現に向け**官民のサイバー状況把握力・対処能力向上に向けた取組**を進める。　※十分なリソースの確保が困難な中小企業等に対しては、支援策を一層強化。

サイバーセキュリティ対策の実効性強化



セキュリティ市場の拡大に向けたエコシステムの構築



サイバー情勢分析能力の強化

官民の情報ハブとしてのIPAの強みを活かし、地政学等の情勢と産業界（エンドポイント）から得られるサイバー攻撃情報の集約・分析を一層推進。攻撃者の意図を把握し、攻撃の対象や手法を予見して効果的な防御策を講じる。

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

1. サイバーセキュリティを取り巻く現状

2. 経済産業省のサイバーセキュリティ政策

3. IoT製品に対するセキュリティ適合性評価制度の概要

（１）IoTセキュリティの重要性

（２）制度の概要

（３）制度普及に向けた取組み

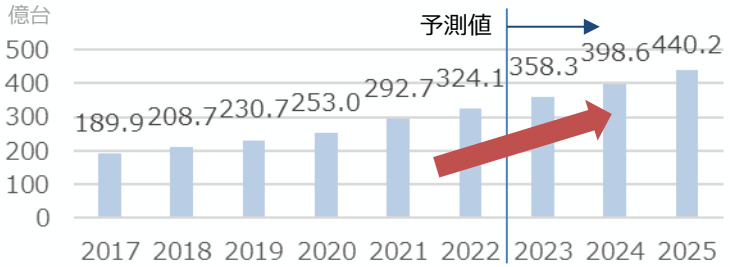
（４）今後のスケジュール

IoT機器の利用拡大に伴い増加するリスク・経営への影響

- IoT機器の増加に加え、IoT機器を狙った攻撃も多く、IoT機器の脆弱性を狙ったサイバー脅威が高まってきており、経営に影響を与えるセキュリティインシデントも起きている。

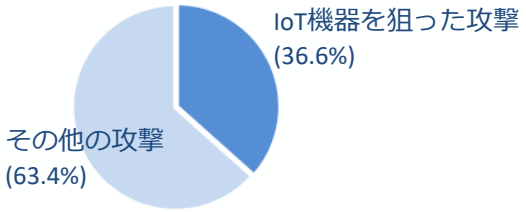
IoT機器の増加

〔IoT機器の増加〕



世界のIoT機器数の推移及び予測(※1)

〔IoT機器を狙った攻撃の割合〕



ダークネットにおける年間観測パケット数の割合(※2)

IoTのセキュリティインシデントによる経営への影響(※3)

操業停止や逸失利益の発生を含む事業への直接的な影響

半導体製造工場の制御装置に対する攻撃によって、**3日間の操業停止、営業機会損失が発生(売上高(四半期)の3%損失)**[台湾:2018]

石油化学工場の安全計装システムを対象とした攻撃による**操業停止。プラント爆発のおそれ**[サウジアラビア:2017]

脆弱性対応や損害賠償を含む追加費用の発生

脆弱性発見による自動車140万台のリコールの発生。脆弱性等の対応で、**2億9900万ユーロ(約394億円)の赤字を計上**(四半期の最終損益) [米国:2015]

評判の低下等より生じる競合優位性の低下

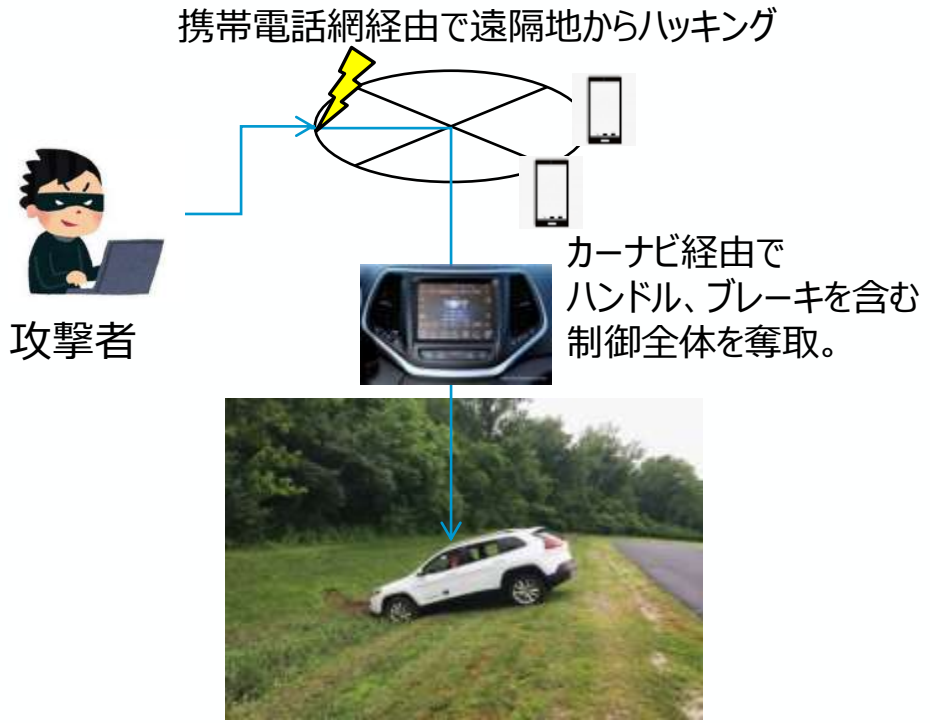
高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下**[オーストリア: 2017]

(※1)総務省「情報通信白書令和4年版 データ集」、「情報通信白書令和5年版 データ集」の「3章関連データ」より作成
(※2)NICT「NICTER観測レポート2023」の1年間にダークネットで観測されたTCPとUDPの攻撃パケット(調査目的を除く)の上位10種類のポートから、主にIoT機器に関連したポート(23/TCP、22/TCP、8080/TCP、5555/TCP、37215/TCP、5060/UDP)のパケットを集計
(※3)各種公開情報に基づき経済産業省作成

（事例）IoTの不正操作によるセキュリティインシデント

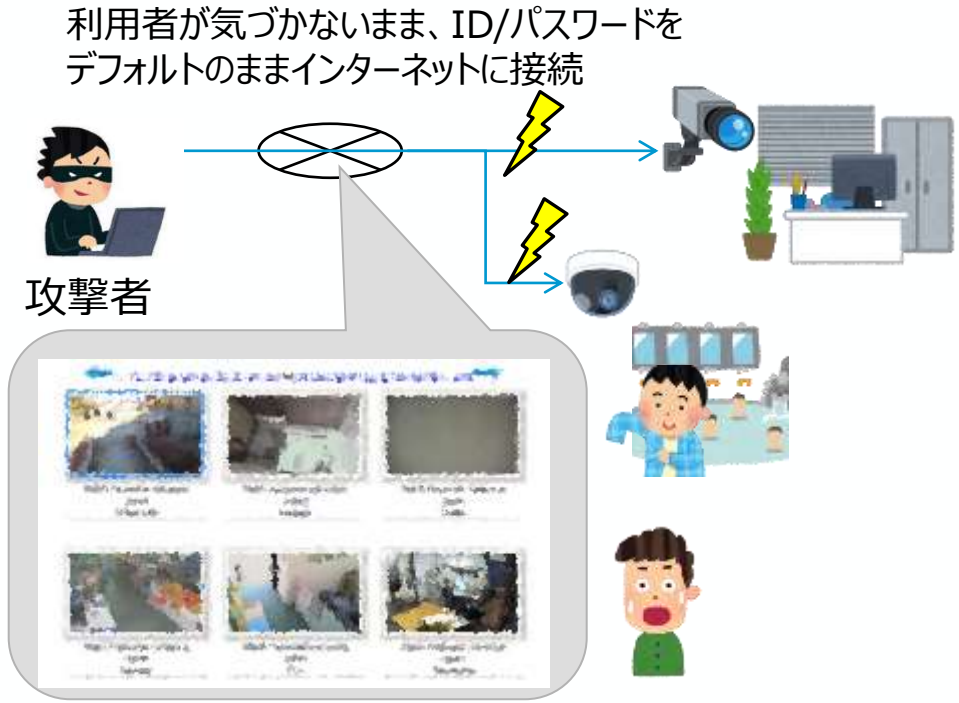
- 自動車やカメラなどの機器が、Wi-Fiや携帯電話網などを介してインターネットに接続されることによってサイバー攻撃の新たな対象となり、不正操作などのリスクが顕在化。

自動車へのハッキングよる遠隔操作



人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開



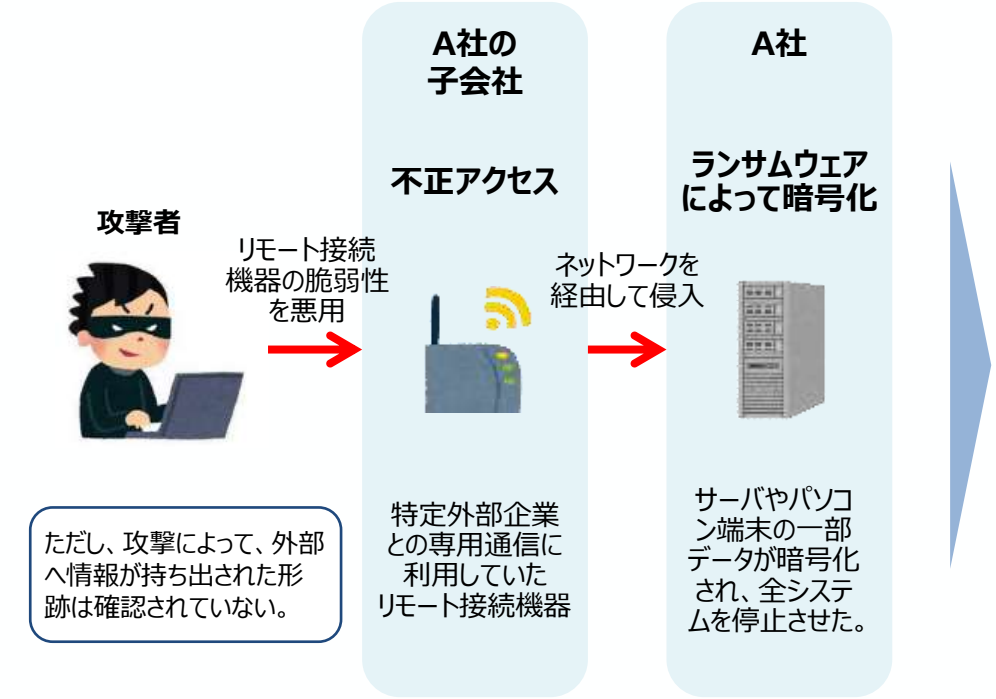
セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。

（出典）各種公開情報に基づき経済産業省作成

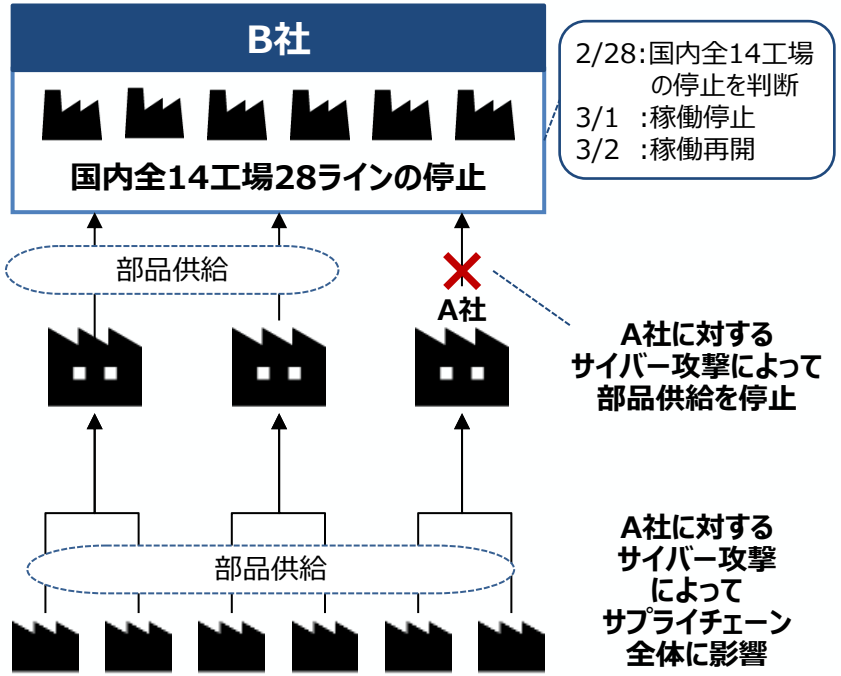
（事例）中小企業のIoT製品への不正アクセスが全体に波及

- B社に部品を納入しているA社は、子会社のリモート接続機器の脆弱性を悪用された不正アクセスから、ランサムウェアの被害を受け全システムを停止させた。
- A社の被害によりB社の国内生産ラインも停止し、サプライチェーン全体へ被害が波及した。

子会社のIoT製品への不正アクセスからのランサムウェア感染



サプライチェーン全体への波及



（出典）各種公開情報に基づき経済産業省作成

1. サイバーセキュリティを取り巻く現状

2. 経済産業省のサイバーセキュリティ政策

3. IoT製品に対するセキュリティ適合性評価制度の概要

　（１）IoTセキュリティの重要性

　（２）制度の概要

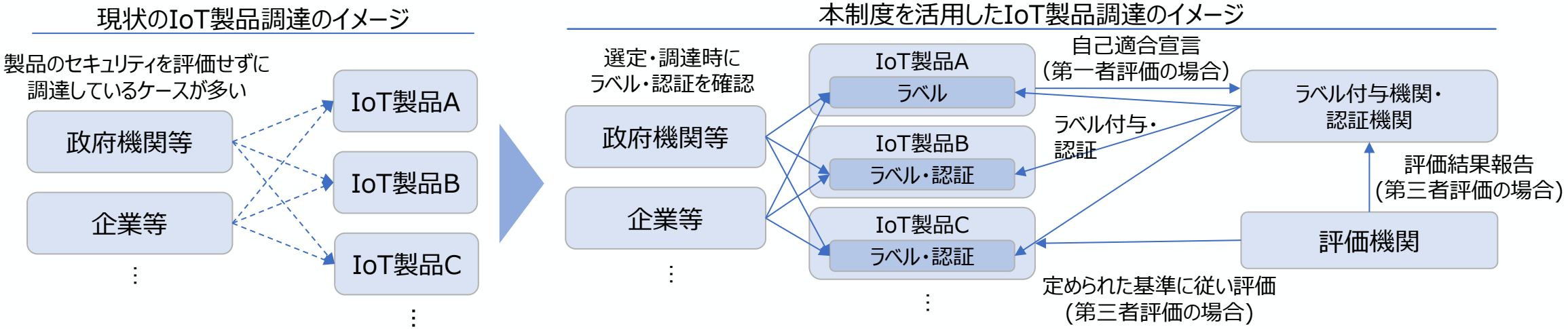
　（３）制度普及に向けた取組み

　（４）今後のスケジュール

IoTセキュリティ適合性評価制度の目的と位置付け

- IoT製品に対するセキュリティ適合性評価制度を国内で構築し、そのラベル・認証を広く普及させ、社会に浸透させるため、まずは**調達者が自身を守るために、求めるセキュリティ水準のラベルが付与された製品を優先的に選択**できるようにする。（調達ニーズへの対応）
- そのうえで、**IoT製品ベンダーが積極的にラベル取得するインセンティブ**を与える。

調達ニーズへの対応		ラベル取得のインセンティブ		
主目的① 【調達要件】	**政府機関や企業等で調達する製品**について、**共通的な物差しでIoT製品のセキュリティを評価・可視化できるようにする**ことで、各組織の求めるセキュリティ水準を満たしたIoT製品の選定・調達を容易にする。	左記に加え	主目的③ 【相互承認】	**諸外国の制度と協調的な制度を構築し、相互承認を図る**ことで、IoT製品を海外に輸出する際に求められる適合性評価にかかるIoT製品ベンダーの負担を軽減する。
主目的② 【業界標準】	特定分野のシステムにて調達・利用されるIoT製品に対し、必要な認証・ラベルを各業界団体等で指定できるようにし、当該**特定分野において必要なセキュリティが確保されたIoT製品のみが採用される**ようにする。			



IoT製品に対するセキュリティ適合性評価制度の概要

- 2022年11月より検討会(※1)を開催し、2024年3～4月のパブコメを経て、8月に制度構築方針を公表。**9月30日にIPAから「JC-STAR」という制度名にて制度開始の案内**(※2)を実施。
- **★１については2024年度中の制度開始**を予定。**政府調達等の要件**等とすべく関係省庁と議論中。**米欧等の諸外国との制度調和**を図るため議論中。

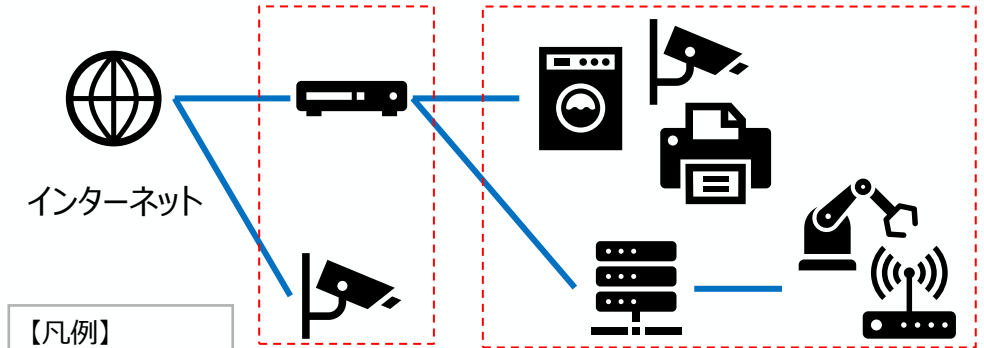
制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

JC-STAR

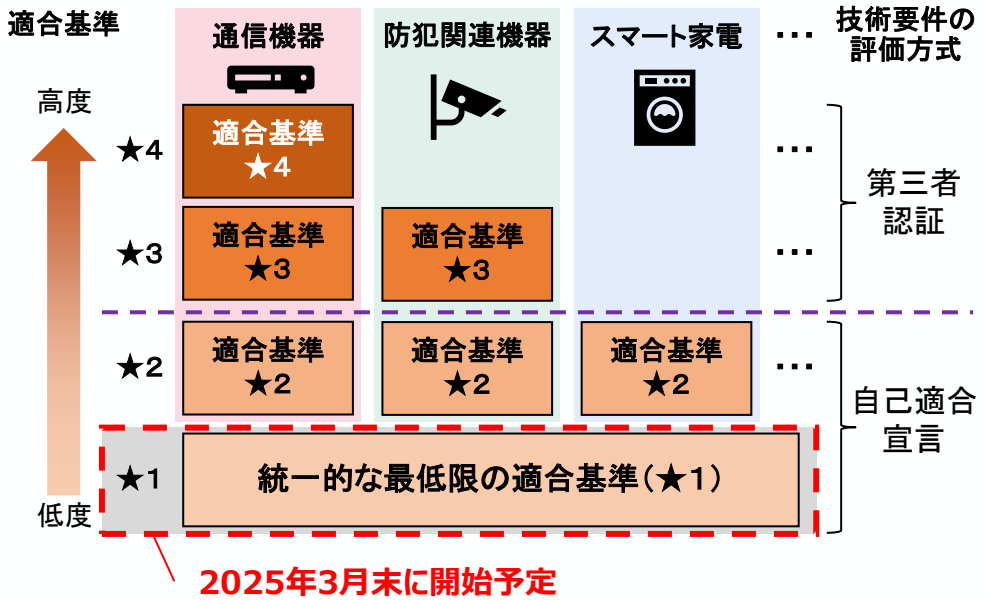
JAPAN CYBERSECURITY LABEL
★★★★
JC-STAR
Registered ID: 0123456789012345

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



(※1)経済産業省「ワーキンググループ3（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）」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
(※2)IPA「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」https://www.ipa.go.jp/pressrelease/2024/press20240930.html

IoTセキュリティ適合性評価制度について諸外国との比較

- 諸外国でも同様の制度検討が進んでいる。国内IoT製品ベンダーの負担を抑えるため、主要国制度の基準も参考にしながら本制度の基準を検討し、**相互承認の調整**を図る方針。
- 日米（首脳級）、日EU（閣僚級）、G7（首脳級）等にて、相互承認に向けて取組む旨合意。

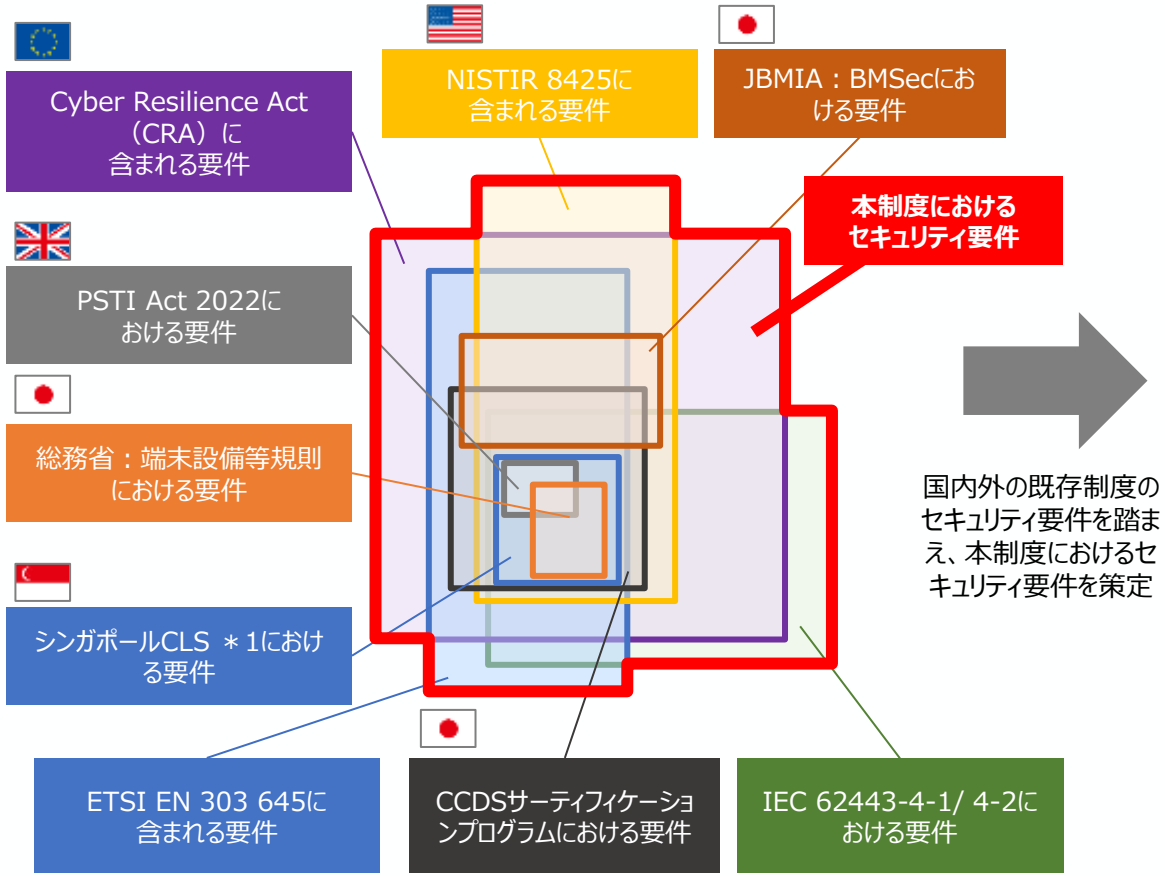
国・地域	日本	シンガポール	英国	米国	EU
制度名	JC-STAR （Japan Cyber STAR）	Cybersecurity Labelling Scheme （CLS）	Product Security and Telecommunication Infrastructure Act （PSTI法）	U.S. Cyber Trust Mark	Cyber Resilience Act （CRA）
開始時期	• ★1：2025年3月開始予定 • ★2以上：2025年度下期以降開始予定	2020年10月制度開始	2024年4月施行	2024年中に開始予定 （なお、基準策定は2025年に後ろ倒しとなる見込み）	• 報告義務：2026年9月 • その他：2027年12月
任意/義務	任意	任意	義務	任意	義務
対象	IoT製品	消費者向けIoT機器	消費者向けIoT製品	消費者用無線IoT製品	デジタル要素を含む製品
適合基準	★1：ETSI EN 303 645及びCLSの記載内容を中心に検討（ただし、総務省技適の要件、CCDSの要件も参照のほか、事務局にて記載内容を検討）	• ＊1：ETSI EN 303 645の基準の一部(※1) • ＊2：＊1の基準に加え、ETSI EN 303 645の基準の一部(※2) • ＊3及び＊4：＊2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NISTIR 8425をベースとした基準となる見込み	• 製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける内容 • 12月10日に発効予定。発効後、基準策定機関に対して法案に伴う基準の策定が命じられる予定。
評価方法	• ★1、★2：自己適合宣言 • ★3以上：第三者	• ＊1及び＊2：自己適合宣言 • ＊3及び＊4：自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	• 基本デジタル製品：自己適合宣言 • 重要デジタル製品クラスⅠ（低リスク）でEUCCやEN規格の対象外の製品及びクラスⅡ（高リスク）：第三者認証

(※1) ETSI EN 303 645のサイバーセキュリティ規定5.1-1、5.1-2、5.1-3、5.1-4、5.1-5、5.2-1、5.3-2、5.3-3、5.3-7、5.3-8、5.3-10、5.3-13、5.3-16
(※2) ETSI EN 303 645のサイバーセキュリティ規定5.4-1、5.4-2、5.4-3、5.4-4、5.5-5、5.5-7、5.5-8、5.6-1、5.6-2、5.6-4、5.8-2、5.8-3、5.11-1、5.13-1及びデータ保護規定6.1、6.2、6.3、6.5

セキュリティ要件（全体リスト）の整理

- 本制度で使用するセキュリティ要件は、ETSI EN 303 645、NISTIR 8425、EU-CRA等の**国内外のセキュリティ要件の全体をカバー**するように整理し、作成した。（全101項目）

諸外国制度において求められるセキュリティ要件の関係性イメージ



本制度におけるセキュリティ要件（全体リスト）のイメージ

セキュリティ要件案	
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。
	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。
	1-3. 製品に対してユーザを認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる技術を使用していなければならない。
	1-4. 製品に対するユーザ認証において、製品は使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。
	1-5. 製品が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。
2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない ・問題を報告するための連絡先情報 ・以下のタイムラインに関する情報 1) 最初の受領確認 2) 報告された問題が解決されるまでの状況の更新
	・・・
・・・	・・・

☆１セキュリティ適合基準

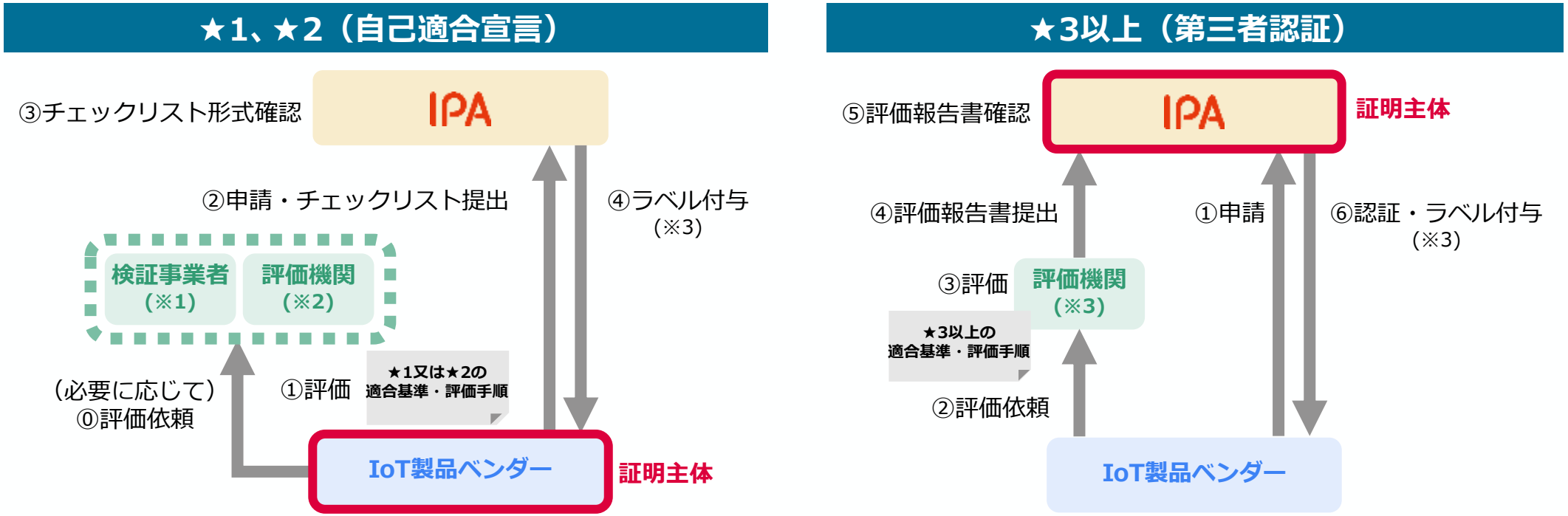
- ☆1で守るべき資産やアタックサーフェスから検討した想定脅威に対して、☆1で対応するセキュリティ要件を全体リストから抽出し、**16項目の適合基準を作成**。

★1で考慮する主な脅威			脅威に対抗するために★1で求める適合基準(※1)			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御** (2)**容易に推測可能なデフォルトパスワードの禁止** (3)パスワード等の認証値の変更機能 (4)ネットワーク経由のユーザ認証に対する**総当たり攻撃からの保護**	情報提供	(16)ユーザへの**セキュアな利用・廃棄方法に関する情報提供**(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能 (7)**容易かつ分かりやすいアップデート手順** (8)アップデート前のソフトウェアの完全性の確認機能 (10)ユーザが型式番号を認識可能とする記載・機能	情報・問い合わせの受付、情報提供	(5)連絡先・手続き等の**脆弱性開示ポリシーの公開** (9)セキュリティアップデートの優先度決定方針の文書化
	③未使用インタフェースの有効化により、		インターフェイスへの論理アクセス	(13)**不要かつリスクの高いインタフェースの無効化**(物理的・論理的な通信ポート等)	–	–
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(**保存データの暗号化、匿名化**等)	–	–
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(**通信の暗号化、保護された通信環境の利用**等)	–	–
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)**製品内に保存される守るべき情報の削除機能**	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の**認証情報やソフトウェア設定の維持**(初期状態に戻らないこと)	–	–

(※1)IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR） > ★1（レベル1）適合基準・評価ガイド」https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html

技術要件の評価方式

- 制度を広く普及させるため☆**1、☆2は自己適合宣言**による技術評価とし、高い信頼性が求められる☆**3以上は独立した第三者による技術評価を受ける第三者認証**とする。



(※1)情報セキュリティサービス基準への適合性について審査及び登録する情報セキュリティサービス基準審査登録制度の機器検証サービス（2023年9月より募集開始）にサービスが登録されている事業者を「検証事業者」とする。
(※2)製品評価技術基盤機構（NITE）の製品評価技術基盤機構認定制度(ASNITE)の中に、本制度の★3以上の評価を行える事業者についてISO/IEC17025に基づく評価機関認定制度を設け（2024年度以降、別途検討）、適切な能力及び体制を整備した事業者を「評価機関」として認定する。
(※3) IPAは、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

1. サイバーセキュリティを取り巻く現状

2. 経済産業省のサイバーセキュリティ政策

3. IoT製品に対するセキュリティ適合性評価制度の概要

（１）IoTセキュリティの重要性

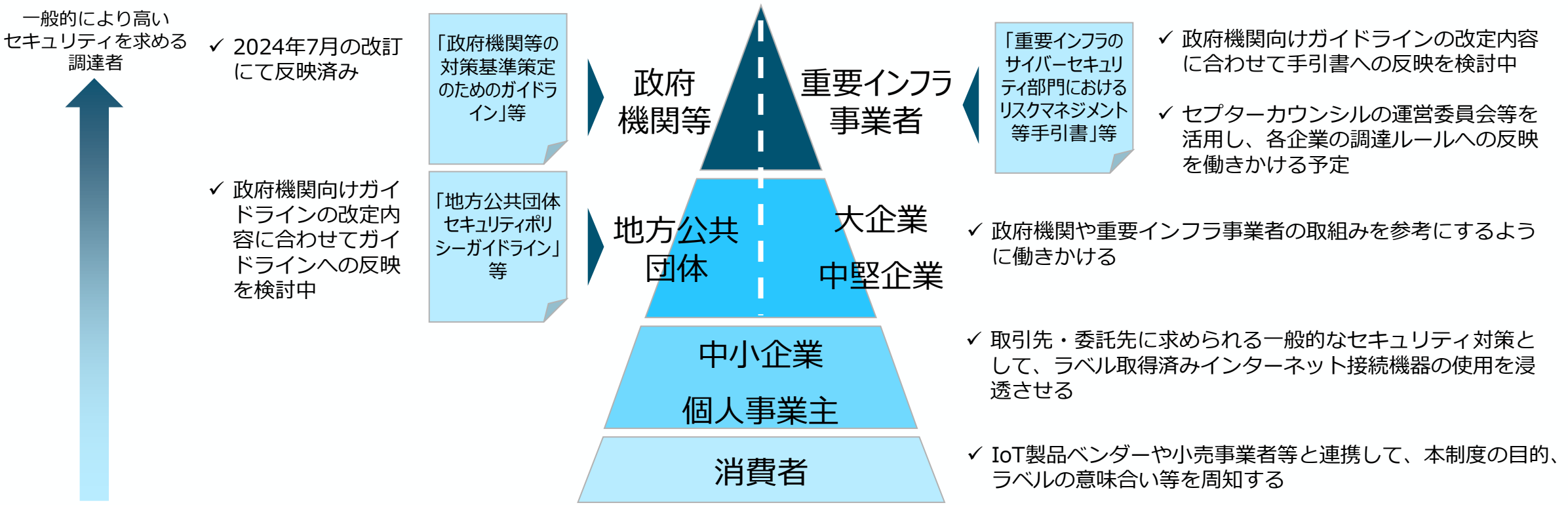
（２）制度の概要

（３）制度普及に向けた取組み

（４）今後のスケジュール

調達者への制度展開戦略と初期ターゲット

- 今年度、**政府機関等、重要インフラ事業者、地方公共団体**向けの各ガイドライン類に本制度の**ラベル付与製品の調達に関する方針を盛り込む**よう協議を進める。
- 併せて、IoT製品ベンダー・団体等にラベル取得を働きかけ、および民間企業・消費者に本制度の目的やラベルの意義等の周知を行い、ラベル取得製品の調達・購入を浸透させていく。



政府統一基準群のガイドラインへの反映

- 2024年7月に公開された政府統一基準群のガイドラインに、今後の本制度活用を反映済み。

「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）の一部改定（令和６年７月）」（抜粋）

4.3　機器等の調達

4.3.1　機器等の調達

（解説）

本制度☆１適合基準相当の内容

- **基本対策事項 4.3.1(1)-2「必要なセキュリティ機能が適切に実装されていること」について**

　必要なセキュリティ対策を実施するためには、機器等に必要なセキュリティ機能が適切に実装されていることが求められる。例えば、IoT 機器等に必要なセキュリティ機能の具体例としては、少なくとも以下の内容が考えられる。

  - 容易に推測可能な初期パスワードの設定禁止
  - 主体認証のネットワークを介した総当たり攻撃対策
  - 容易に行えるソフトウェアの脆弱性対策（アップデート等）
  - 機器内のセキュリティパラメータの保護
  - 安全な通信の確保
  - 利用者が作成したデータの容易な消去
  - 利用しない機能や通信ポートの無効化

本制度の活用方針

　機器等に必要な情報セキュリティ対策が適切に実装されていることを確認するには、機器等の仕様書の確認、製造者へのヒアリングの実施のほか、次の「IoT 製品のセキュリティ適合性評価制度」の活用が考えられる。

　IoT 機器等に対する要求すべきセキュリティ要件に関連して、2024 年度中（2025 年３月頃）に「IoT 製品に対するセキュリティ適合性評価制度」の☆１のラベル付与が開始される予定であり、今後の調達における活用が考えられる。☆１は機器等共通の最低限満たすべきセキュリティ項目を満たしていることを製造業者が自己で評価し、その適合性を宣言することで取得可能となるものである。☆１の取得を確認することで、上記に記載しているセキュリティ機能の実装状況の確認の代用とすることができる。

　また同制度では、製品種別毎により高度なセキュリティ適合基準に対する評価を行う☆２（自己適合宣言）、☆３以上（第三者認証）が順次整備される予定である。制度整備の状況を踏まえつつ、2025 年度中に同制度の☆１以上を取得していることを機器等の選定基準に含めるとともに、以降も、☆２、☆３以上の対象機器の拡充に応じて選定基準への反映を順次行っていく予定である。

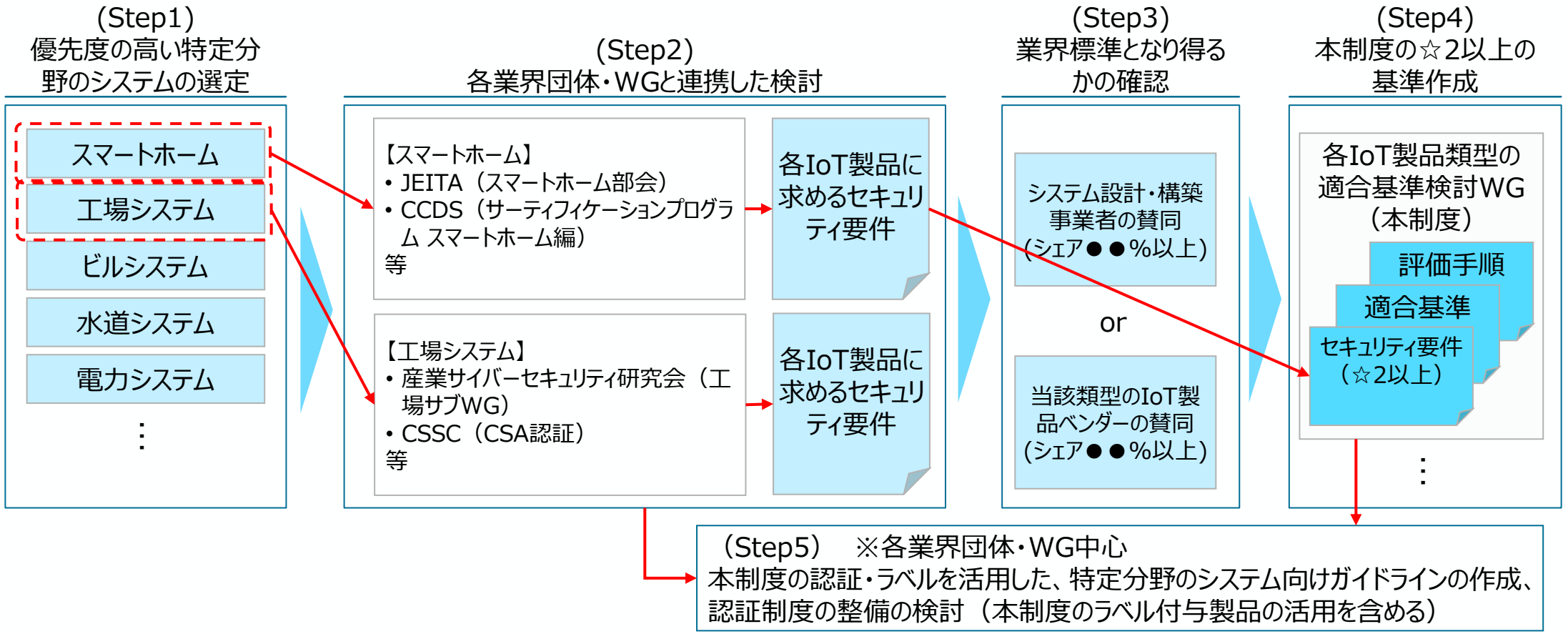
　情報システムの重要度に応じて「重要度：低」は☆１以上、「重要度：高～中」は少なくとも☆３以上の IoT 機器等を各機関等の選定基準に含めることの追加を検討している。なお、ラベル付与製品が普及する時期をめどに、政府機関等では求めるセキュリティ水準に応じたラベル付与製品の調達を必須化する方針である。

参考：経済産業省「IoT 製品のセキュリティ適合性評価制度構築方針」
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html）

（出典）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）の一部改定（令和６年７月）」（https://www.nisc.go.jp/pdf/policy/general/guider6.pdf）

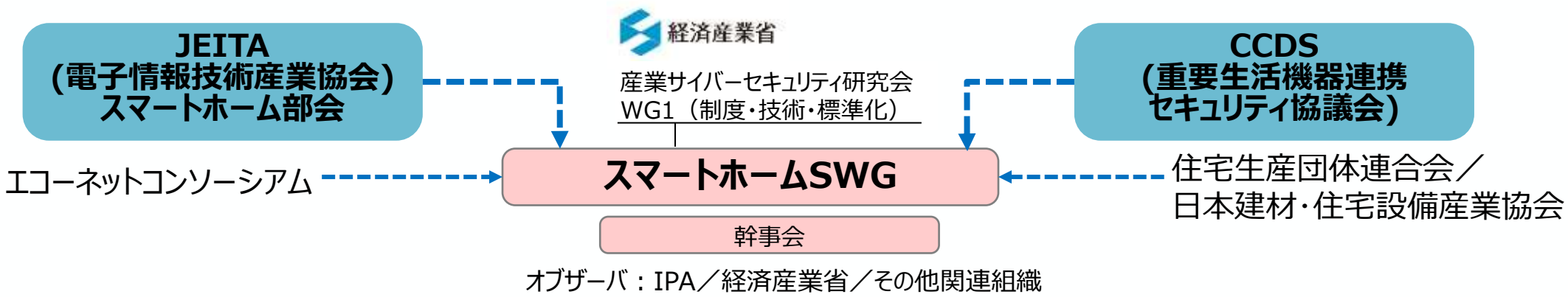
特定分野のシステムに関する業界団体・WGとの連携

- 製品単体で比較されず、特定分野のシステムに組み込まれて調達されるIoT製品について、検討優先度の高い分野の業界団体等と連携し、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や☆2以上の適合基準をその必要性も含めて検討する。



スマートホームサブワーキンググループとの連携

- **スマートホーム分野は消費者向けのIoT製品の利用が拡大**している優先分野として、JEITA、CCDS等の関係者と連携し、2024年7月よりスマートホームSWGを拡大し、検討を開始。



主査：JEITA/CCDSから選出、共同主査形式
委員：JEITA/CCDSの両会員企業から、IoT製品メーカ、ユーザを中心に委員を招聘する。
主な活動内容：
- **評価基準検討**
  - ースマートホームの定義
  - ースマートホームで実施すべきセキュリティ対策の検討
  - ースマートホーム関連の各IoT製品類型におけるIoTセキュリティラベル☆１の活用及び☆２以上の整備要否の検討
  - ー☆２以上の整備のIoTセキュリティ適合性評価制度（IPA+経産省）への依頼
- **普及促進検討**
  - ースマートホームの普及・セキュリティ対策状況の現状確認、セキュリティを考慮した普及促進策の検討
  - ーIoT製品の販売・購入の促進施策の検討、IoT製品類型の活用に関する製品ベンダー、調達関係者との合意

（出典）2024年度第1回スマートホームSWG資料に基づき経済産業省作成

1. サイバーセキュリティを取り巻く現状

2. 経済産業省のサイバーセキュリティ政策

3. IoT製品に対するセキュリティ適合性評価制度の概要

（１）IoTセキュリティの重要性

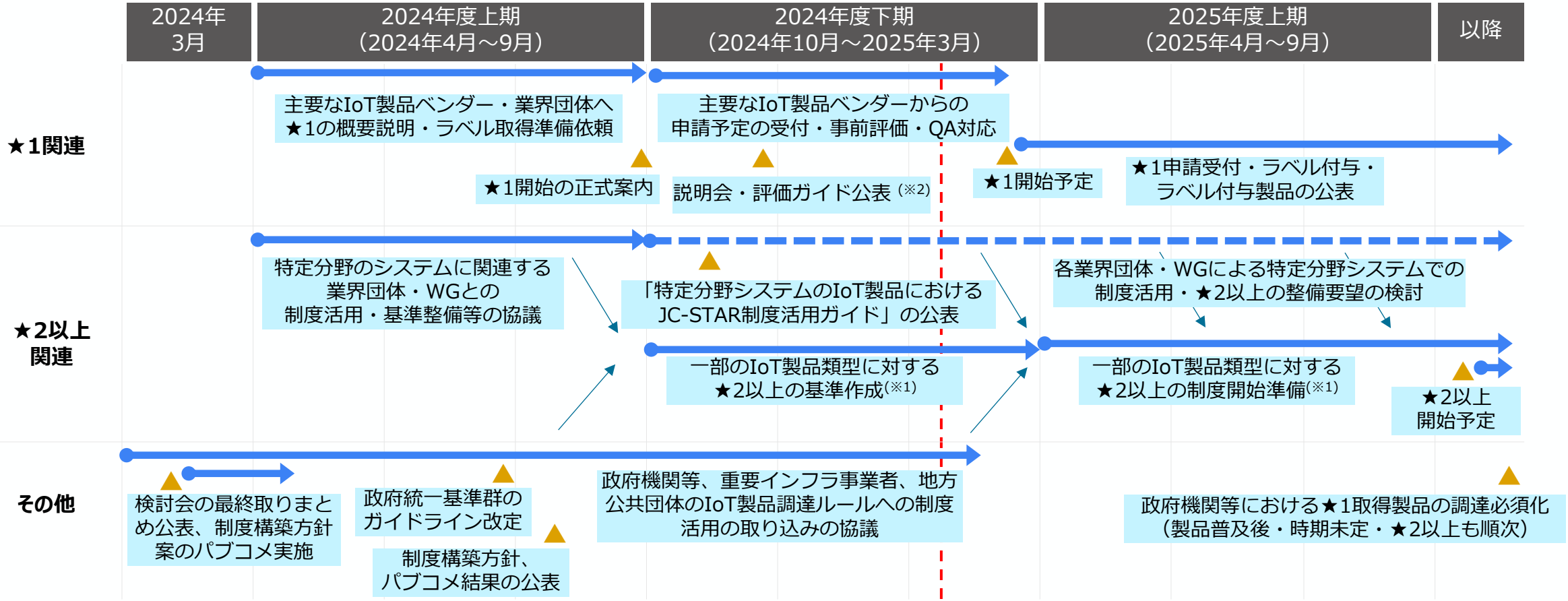
（２）制度の概要

（３）制度普及に向けた取組み

（４）今後のスケジュール

今後のスケジュール

- 2024年9月30日にIPAから制度開始の正式案内を実施。2025年3月末に★１を開始予定。
- ★2以上はNWカメラと通信機器を対象に、基準検討WGを開始。2025年度4Qの開始予定。



(※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以上の開始予定を案内。以降、対象となる製品類型を順次拡張。
(※2)IPA「JC-STAR制度説明会資料（2024年11月28日、12月2日、12月6日開催）」 https://www.ipa.go.jp/security/jc-star/material.html

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html