IoT製品のセキュリティ確保に向けて
～セキュリティ要件適合評価及びラベリング制度（JC-STAR*）の紹介～

* JC-STAR: Labeling scheme based on Japan Cyber-Security Technical Assessment Requirements

（独）情報処理推進機構セキュリティセンター

IPA Better Life with IT

IPAが運営するセキュリティ製品認証制度

ITセキュリティ評価及び認証制度（JISEC）

国際標準ISO/IEC 15408（Common Criteria）に基づき、IT製品・システムのセキュリティ機能の適切性・正確性を客観的に評価・認証する日本の制度

- 必要なセキュリティ機能がライフサイクル全般に渡って適切に設計され、正しく実装されていることを客観的に検査
- 評価検証の深さに依存してEAL1～EAL7まで設定
- CC認証承認アレンジメント（CCRA）加盟31ヶ国間で相互承認

NEW

セキュリティ要件適合評価及びラベリング制度（JC-STAR）

ETSI EN 303 645やNISTIR8425等とも調和しつつ、独自に定める適合基準（セキュリティ技術要件）に基づき、IoT製品等に対する適合基準への適合性を確認・可視化する日本の制度

- セキュリティ技術要件で求めたセキュリティ機能を正しく実装していることの適合性を自己宣言又は客観的に評価
- セキュリティ技術要件の違いに依存して★1～★4まで設定。★1と★2は自己宣言、★3と★4は客観的評価による
- 相互承認については、類似スキームをもつ各国と協議予定

暗号モジュール試験及び認証制度（JCMVP）

国際標準ISO/IEC 19790に基づき、暗号モジュールのセキュリティ機能等の確実性・安全性を客観的に試験・認証する日本の制度

- 承認されたセキュリティ機能（暗号アルゴリズム等）が正しく実装され、セキュリティ重要情報を適切に保護していることを客観的に試験
- 試験する攻撃耐性に依存して保護レベルをLev1～Lev4まで設定
- 相互承認スキームはない

本日説明する内容

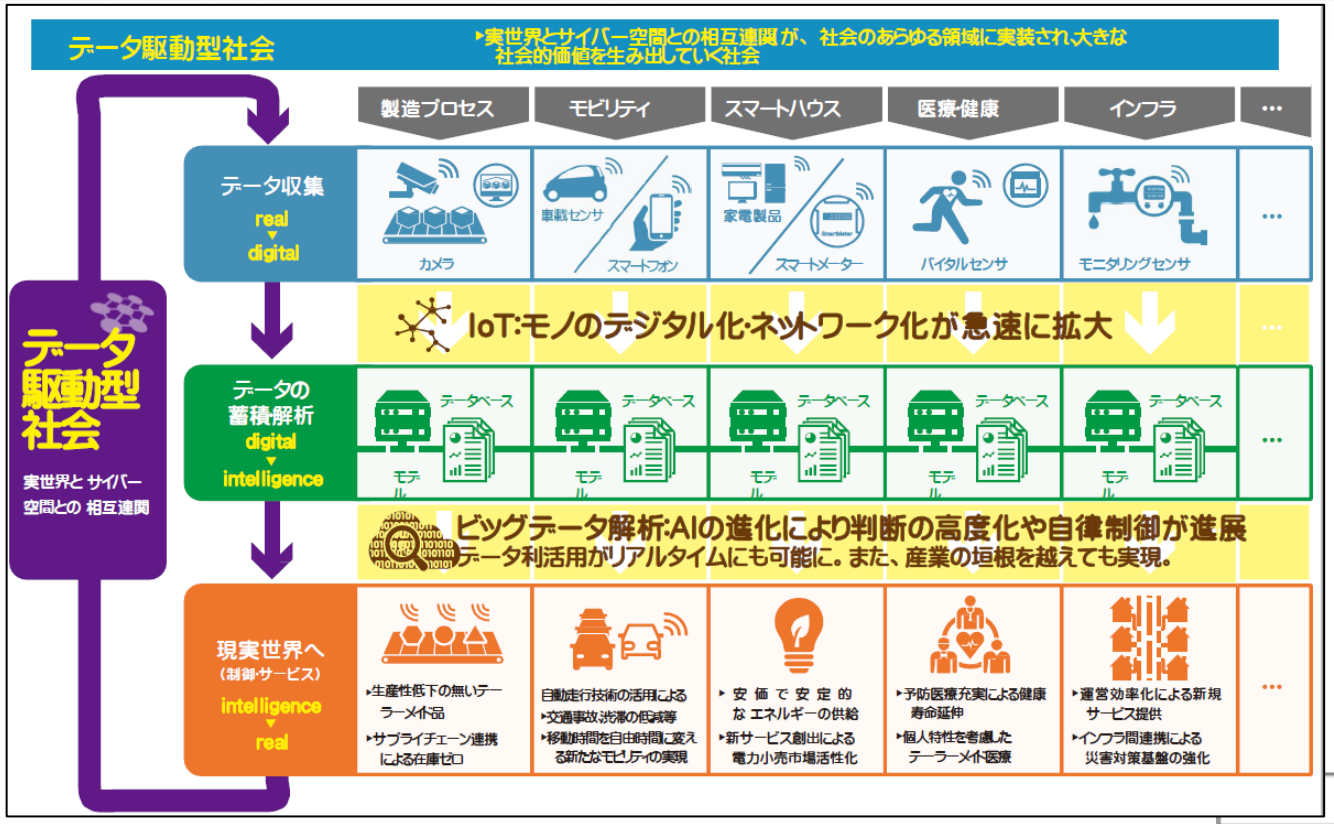
IoT製品に対するセキュリティ要件（適合基準）への適合性を自己適合宣言又は客観的評価に基づき可視化するラベリング制度の運用を2025年3月から開始します！

本制度の概要

- IoT製品が具備するセキュリティ機能として満たしてほしい水準にあることを確認するための制度です。
- 求められるセキュリティ要件への適合を満たしたIoT製品に、二次元バーコード付き適合ラベルが付与されます。
- 調達者・消費者は製品詳細や適合評価、セキュリティ情報・問合せ先等の情報を簡単に取得でき、セキュリティ要件を満たした安全なIoT製品を選びやすくなります。

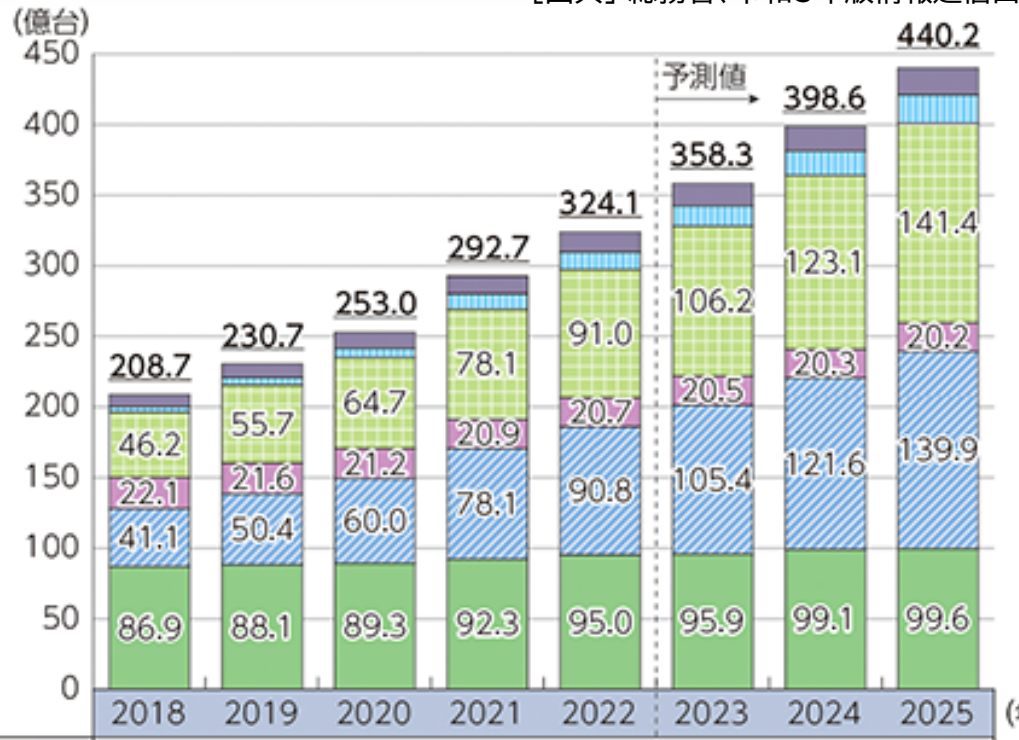
JC-STAR制度発足の背景

IoT製品の普及が進んでいる



［出典］経済産業省、第四次産業革命に向けた商務情報政策局の取組（2016）

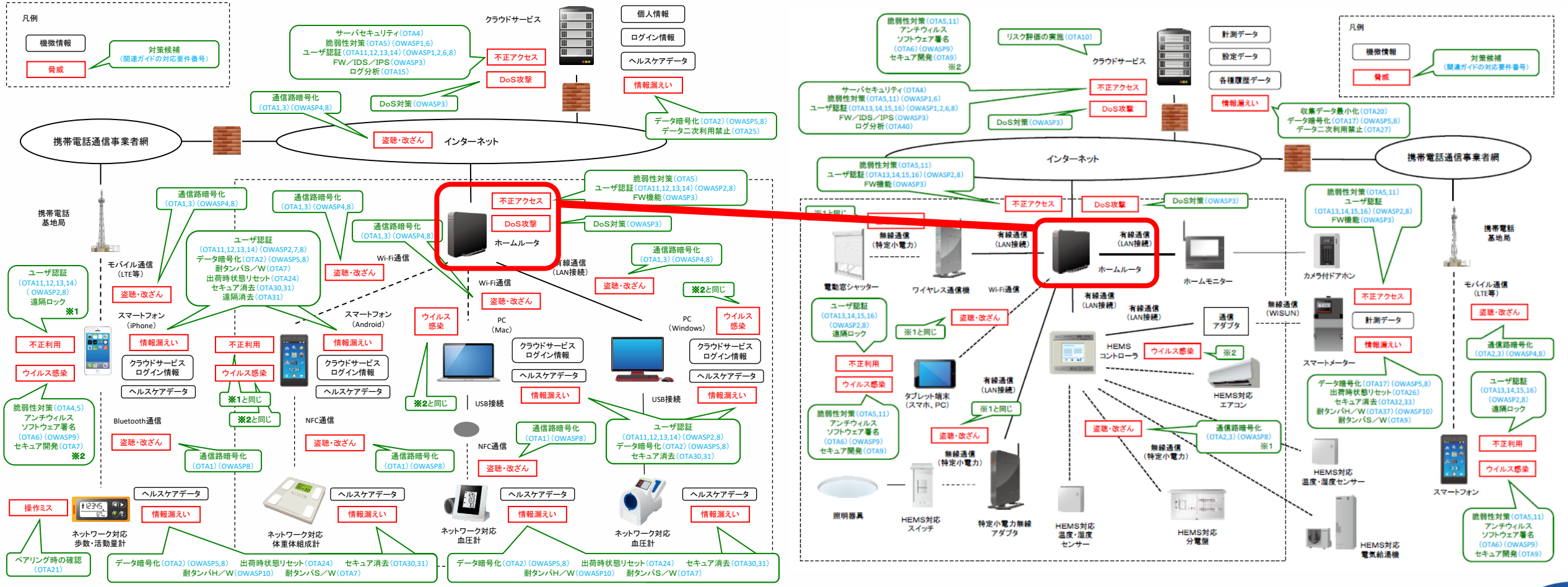
［出典］総務省、令和5年版情報通信白書



	2018	2019	2020	2021	2022	2023	2024	2025
合計	208.7	230.7	253.0	292.7	324.1	358.3	398.6	440.2
自動車・宇宙航空	8.5	9.8	11.3	12.7	14.2	15.7	17.3	18.9
医療	4.0	5.1	6.5	10.7	12.5	14.6	17.2	20.2
産業用途	46.2	55.7	64.7	78.1	91.0	106.2	123.1	141.4
コンピュータ	22.1	21.6	21.2	20.9	20.7	20.5	20.3	20.2
コンシューマ	41.1	50.4	60.0	78.1	90.8	105.4	121.6	139.9
通信	86.9	88.1	89.3	92.3	95.0	95.9	99.1	99.6

IoTになって便利になった･･･けれども

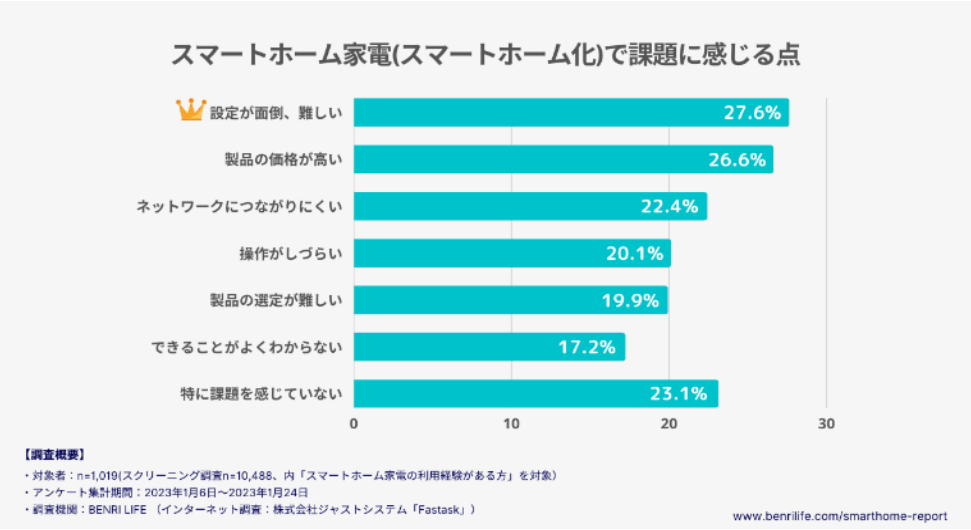
■ 結果として、インターネットから攻撃できる場所がいたるところに存在



［出典］ IPA、「IoT開発におけるセキュリティ設計の手引き」

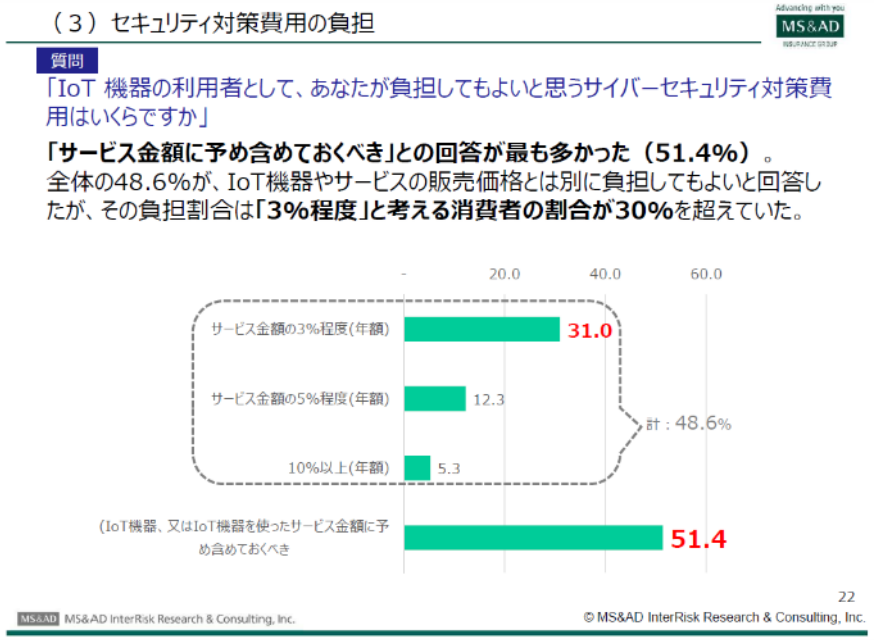
IoTになって便利になった・・・けれども

- **安いモノ、便利なモノ**ほど売れる
  - セキュリティは二の次。簡単につなげられる、すぐに使えることが重要
    - 繋がらないとクレームになる
    - デフォルトでは貧弱なアクセス制御／ログイン管理しかしていない
    - IoT機器ならではのリスクに対する知識を持たない人たちが利用する可能性もある



［出典］BENRI LIFE, 日本におけるスマートホーム市場の動向とその発展の歴史、および今後の予測に関して（2023年版）

- コストを安くすることが重要
  - 少数のIoT向けライブラリやオープンソースが多くの機器に使われている
  - リソースが限られているIoT機器ではセキュリティ対策を適用するのが困難なこともある



［出典］MS&ADインターリスク総研, 個人向けIoT機器に関するサイバーセキュリティ対策の意識調査報告書

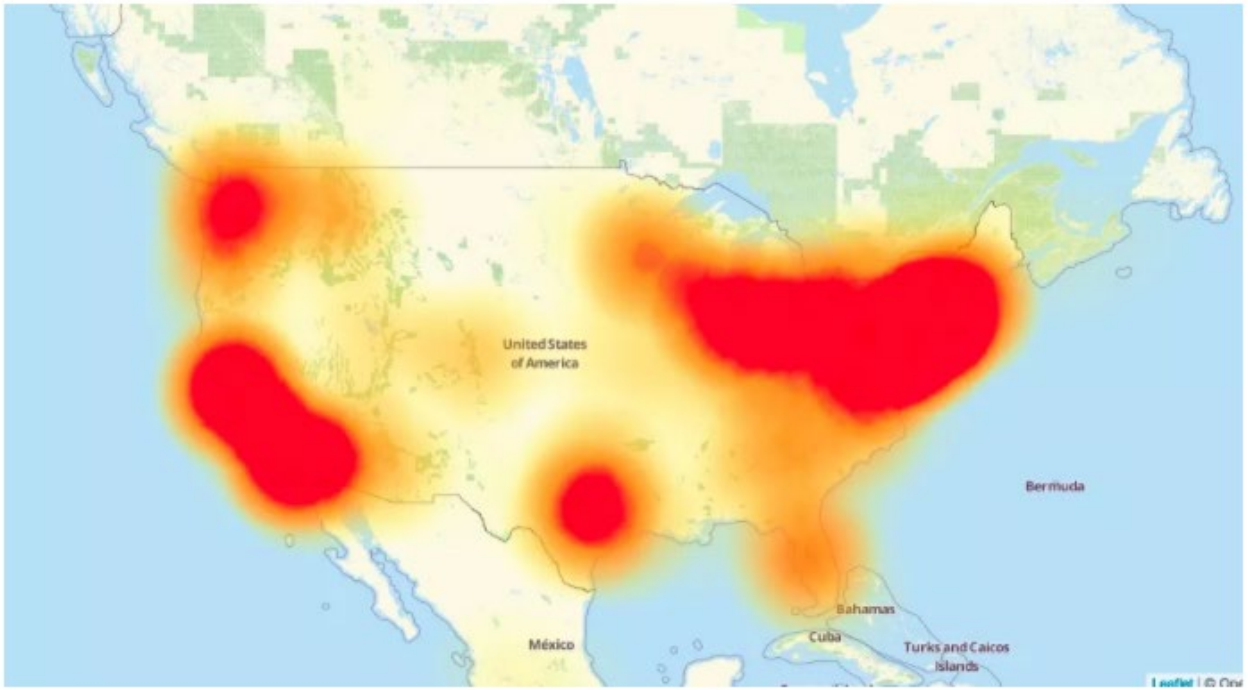
IoTになって便利になった･･･けれども

- **想定しないつながり**が発生する
  - 汎用のOSや通信インタフェース（標準プロトコル）を利用している
  - 開発者が想定していなかった接続が行われる可能性がある
  - 貧弱なアクセス制御／ログイン管理から変更しない
- **予想しない機能**がデフォルトでついていることがある
  - データを収集してクラウドに自動送信
  - サーマルカメラでの画像記録
- **管理されていない**モノでもつながる
  - 機器の管理担当者がいない／はっきりしない
  - 発見された脆弱性に対して修正パッチの適用困難＆そもそも修正パッチが作られない
  - 10年以上の長期、かつメンテナンスフリーで使われるような機器もたくさんある
  - 機器の廃棄手順がはっきりしない
- 問題が発生しても**ユーザに分かりにくい**
  - 物理的な異常が発生しない限り、設定ミスやマルウェア感染、不正アクセスが起きていても気が付かない可能性が高い
- ネット接続していることで新たに脅威にさらされ、**時間とともに脅威が高度化**

➡リスクが放置される危険性

IoT製品の普及に伴うリスク

- 情報セキュリティ10大脅威で「IoT」が最初に取り上げられたのは2017年
  - IoT機器にウイルス感染　⇒　DDoS攻撃用のボットネット化



A map of the internet outage as it affected website access in the US at 11:30 a.m. Pacific Time on Friday.

Screenshot by Laura Hautala/CNET

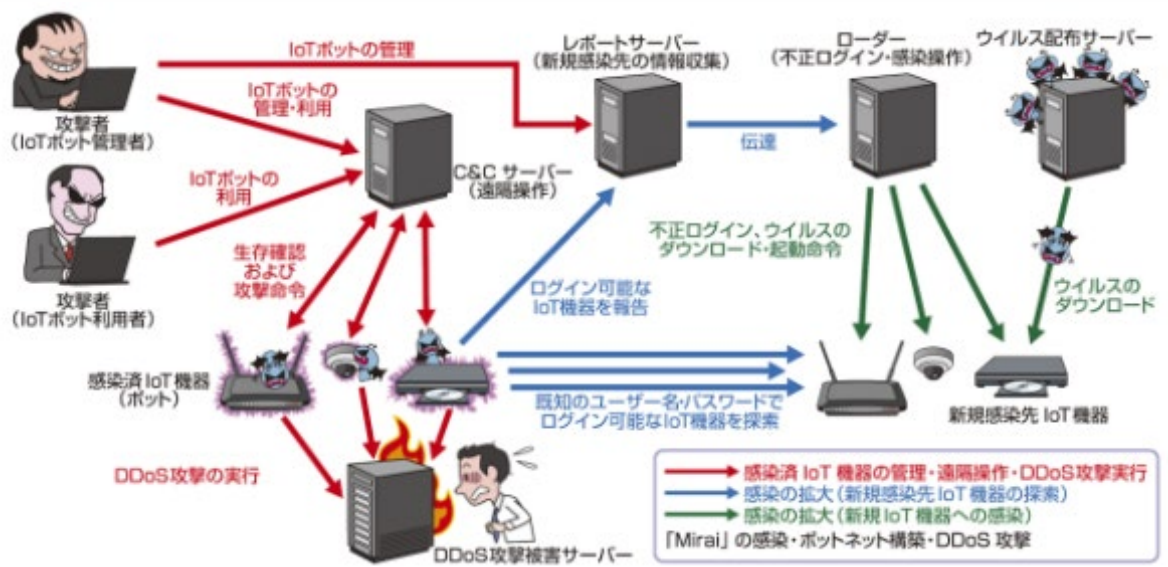
[URL] https://www.cnet.com/how-to/what-is-a-ddos-attack/

2016年10月21日

- Amazon・GitHub・Twitter・Netflix等の有名サイトを含めた多くのサイトがアクセス不能
- Miraiに感染したIoT機器によるボットネットからの攻撃と推定
- 500Gbps～1000Gbpsにも達するトラフィックを発生

Mirai(2016)

- Linuxで動作するコンピュータを遠隔操作できるボット化するマルウェア
  - 主要ターゲットはネットワークカメラや家庭用ルータなどのオンライン機器(IoTデバイス)
  - ランダム検出したIPアドレスを経由してデバイスを検索
  - IoTデバイスの基本機能は維持されるので、感染しても気が付かない可能性が高い
- **工場出荷時設定のまま**になっている脆弱なIoTデバイスに感染
  - 工場出荷時に**共通なユーザーネームとパスワード**のテーブルを使って感染させるためにログイン
- ボットネットを形成、C&Cサーバ指令で大規模・破壊的なDDoS攻撃実行
- ソースコードがオープンソースとして公開



[出典] IPA、情報セキュリティ10大脅威 2017

日本では

- 国内におけるIoT機器のマルウェア感染急増(2017年)
  - NICTERセンサへの国内のIPアドレスからのアクセス(＝マルウェア感染)が急増
    - Mirai亜種「Satori/Okiru」
    - Miraiと比べても20倍以上、約4万台程度が感染したと推測
  - 脆弱性(CVE-2014-8361)を有する国内メーカ製無線LAN BBルータが多く感染
    - **4年前にすでに更新ファームウェアが公開**されたが適用が徹底されていなかった

図5: 23/TCP に対する日本国内からの攻撃元 IP アドレス数統計

[出典] NICT, NICTERレポート2016&2017

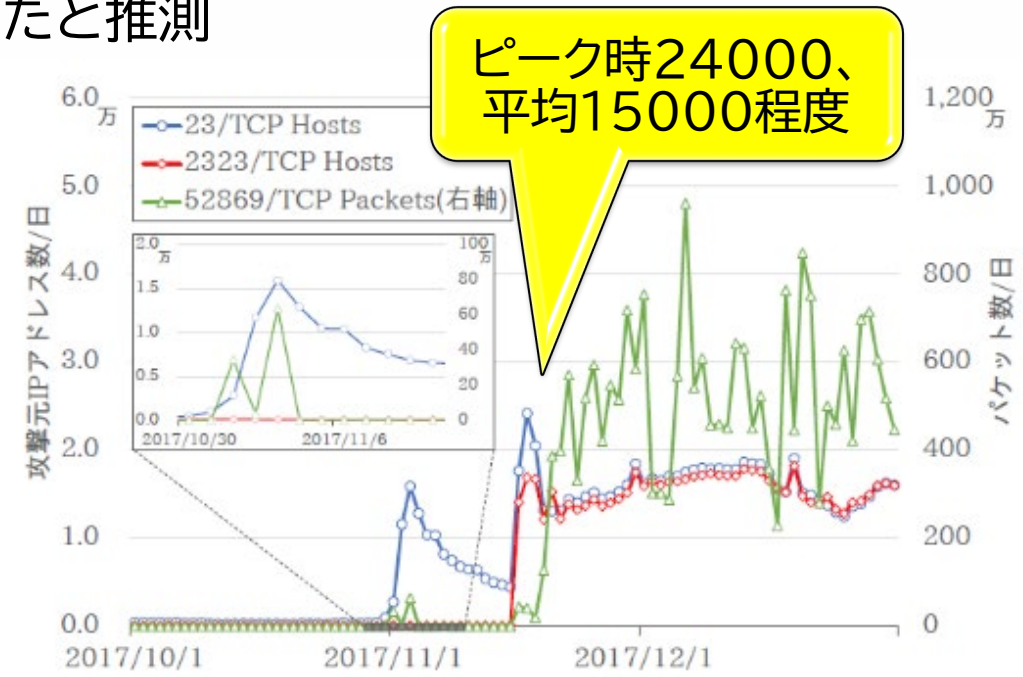
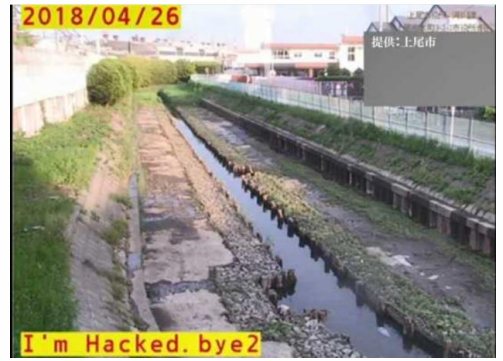


図6: Telnet 宛ての攻撃ホスト数（日本）と 52869/TCP 宛てのパケット数の推移

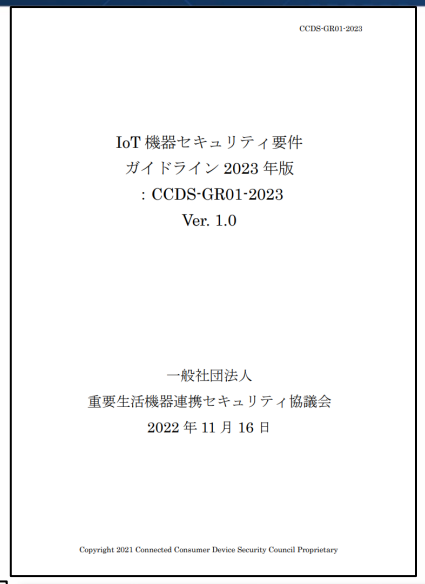
IoT製品の普及に伴うリスク

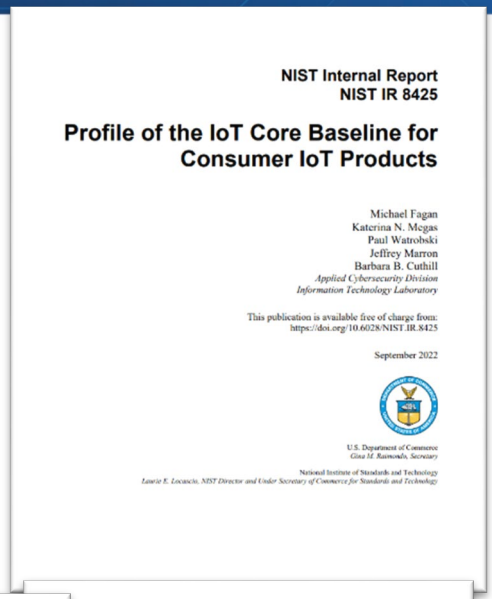
- 個人宅に設置されたネットワークカメラ乗っ取り（2017年）
  - 売れ筋ランキング＆注目度ランキング1位の並行輸入品
  - **複数の脆弱性**が存在
    - 電子回路基板上プログラムに認証情報漏えいの脆弱性（CVE-2017-8225）
    - パスワードを初期値から変更しても第三者による不正操作が可能
    - 出荷時停止のTelnetを外部から起動可能（＝バックドア）
- 全国各地の国内ベンダ―製監視カメラが不正アクセス被害（2018年）
  - 全国で60台以上のカメラに及ぶとみられる
  - **パスワードが初期設定**のままだったこと等が原因とみられる

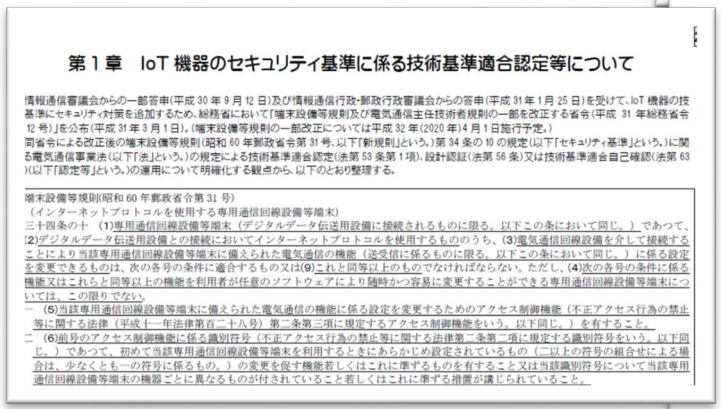


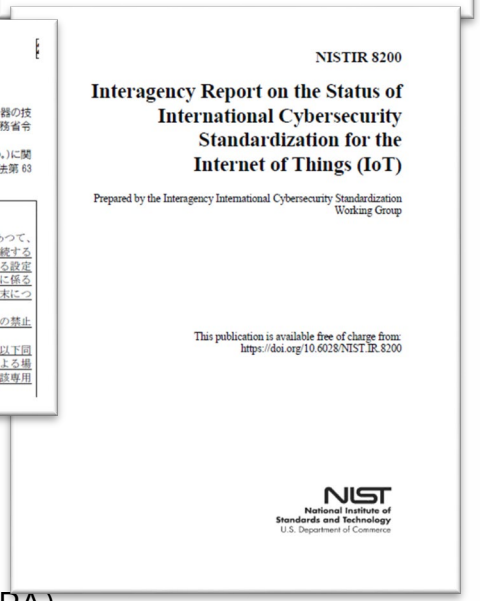
- 重要インフラ等で利用されるIoT機器の調査（2017～2018年）
  - 150件の脆弱な重要IoT機器（消費電力監視装置、水位監視装置、防災設備制御装置、ガス観測警報通知装置等）を検出
  - **パスワード設定が適切にされていない**ものが27件、パスワード設定はされているが認証画面がインターネット上で公開されていたものが9件
- 世界中の監視カメラ映像をリアルタイムで覗き見
  - **パスワード設定なし**の監視カメラが狙われる。日本では、629台が登録（2023/12/05時点）

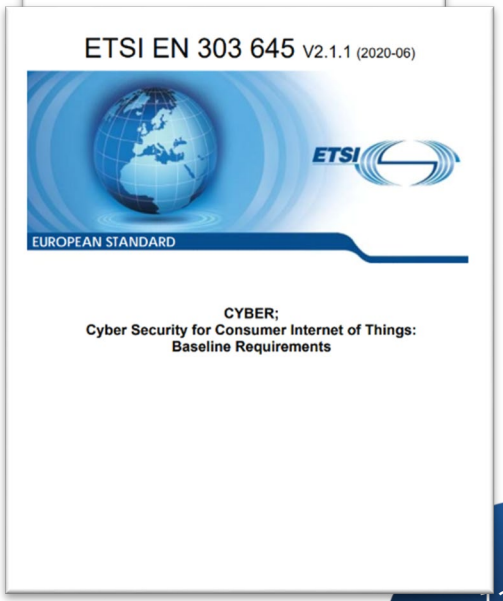
IoT製品の設計ガイドライン・規範などが公開



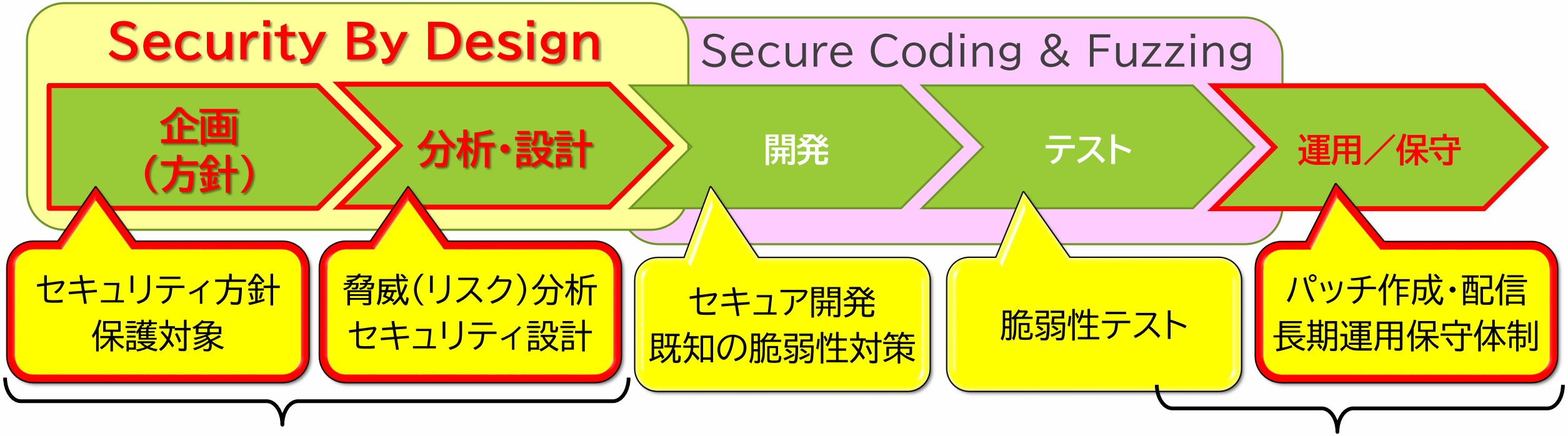








IoT製品のライフサイクル



設計段階からセキュリティを考慮

- システムの全体構成の明確化
- 保護すべき情報・機能・資産の明確化
- 「脅威分析」：保護対象に対する想定脅威の明確化
- 「対策検討」：対策候補の洗い出し、脅威・被害・コスト等を考慮した選定

セキュリティ対策の継続的サポート

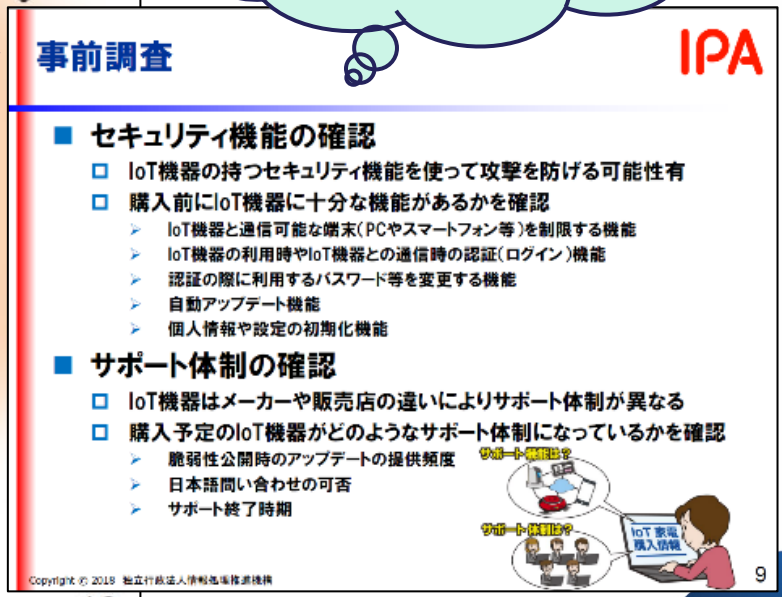
- 脆弱性対応
- ソフトウェア更新

IoT製品の利用者への対応策として

■ 情報セキュリティ対策の基本　IoT機器(情報家電)編公開(2018)

[URL] https://www.ipa.go.jp/security/10threats/ps6vr7000000bjc5-att/000066221.pdf

でもどうやって？



現実は厳しい

[出典] IPA、「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」(2018年)

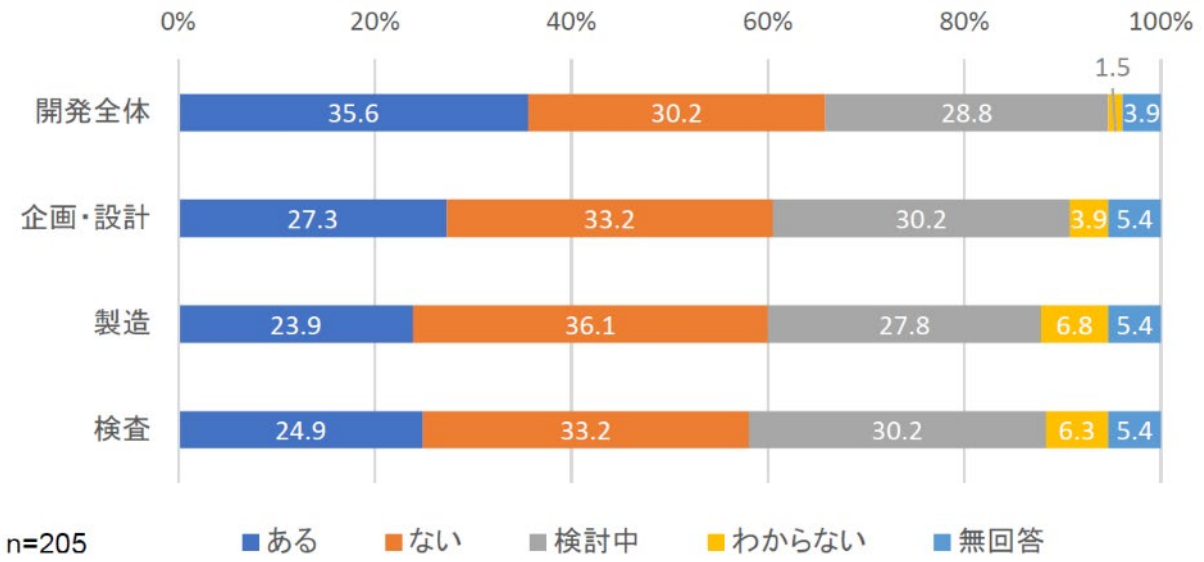


図 3.33 開発段階のセキュリティ方針・基準

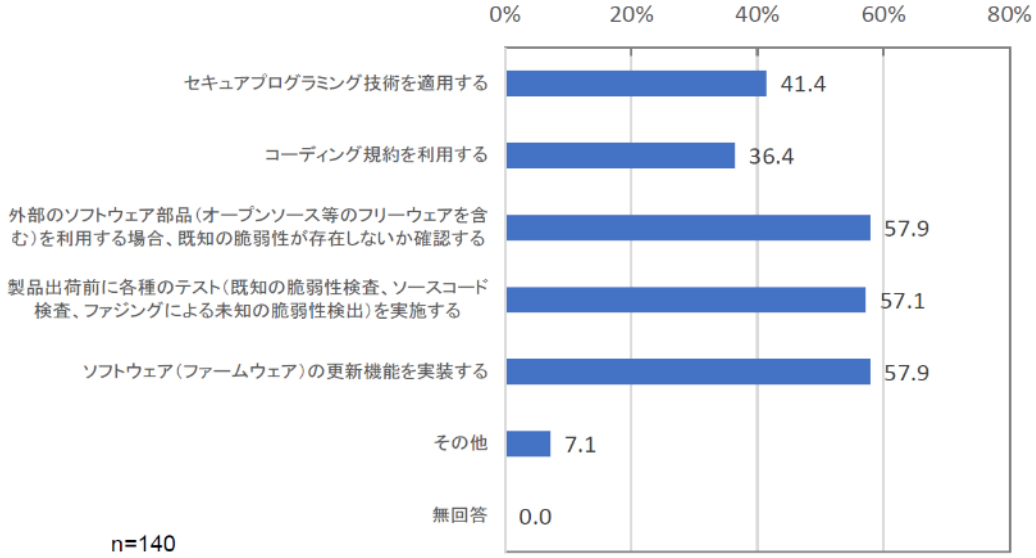


図 3.37 開発段階の脆弱性対策の考慮内容

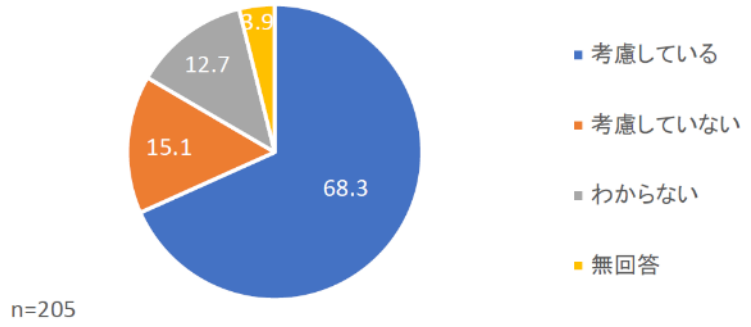


図 3.36 開発段階の脆弱性対策の考慮

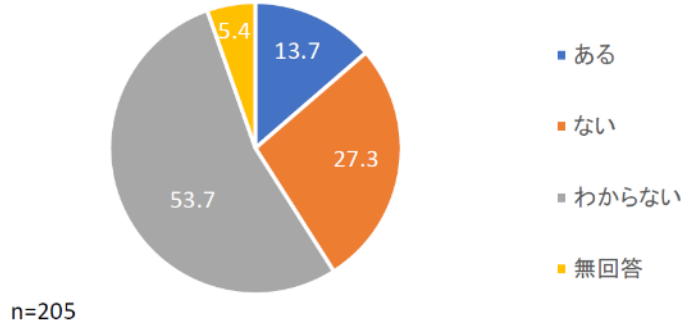


図 3.47 脆弱性対策が不可能な場合

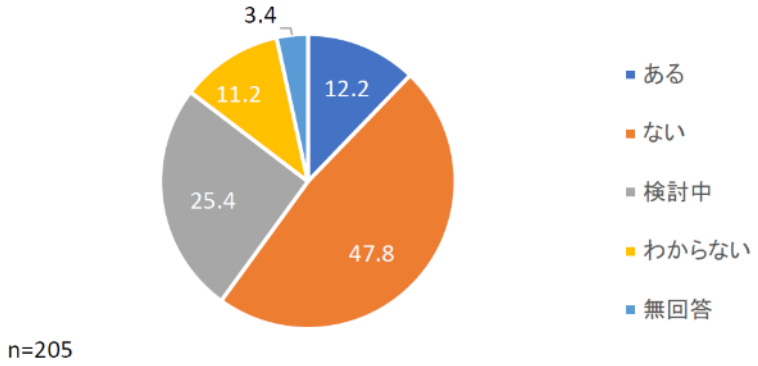


図 3.50 サポート終了後の脆弱性対応方針

NOTICEプロジェクトを知っていますか？

- IoT機器のセキュリティ対策向上により、サイバー攻撃の発生や被害を未然に防ぐためのプロジェクト

[出典] NICT、NOTICEプロジェクト（https://notice.go.jp/）

報道資料

令和6年3月29日

IoT機器のセキュリティ向上を推進する新しい「NOTICE」を開始

サイバー攻撃手段の高度化による新たな脅威の登場などの環境変化によりIoT機器を悪用したサイバー攻撃の発生が継続していることを踏まえ、IoT機器のセキュリティ向上を推進するプロジェクトとして、新しい「NOTICE(National Operation Towards IoT Clean Environment)」を開始します。

1 背景

IoT機器を悪用したDDoS攻撃※1などのサイバー攻撃が引き続き発生しています。こうした事態に対応するため、令和6年度からID・パスワードに脆弱性があるIoT機器の調査に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とする、サイバーセキュリティ対策助言等業務を新設※2し、新しい「NOTICE」を開始します。

※1 ルーターやネットワークカメラ等のIoT機器が第三者に乗っ取られ、複数の機器から大量のデータを攻撃先に送信するDDoS攻撃の発生源となる事例が多数報告されています。DDoS攻撃が発生するとネットワークの輻輳による通信速度の低下などの被害が生じます。

※2 国立研究開発法人情報通信研究機構法の一部を改正する等の法律（令和5年法律第87号）による新設。

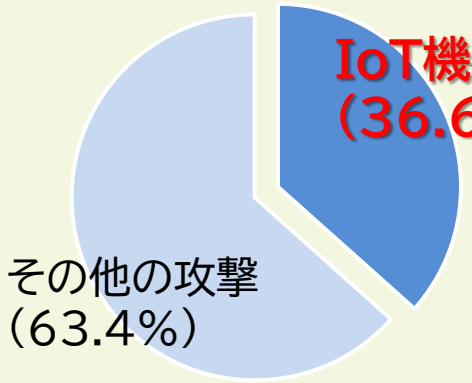
2 新しい「NOTICE」の概要

IoT機器の悪用によるサイバー攻撃の発生・被害を抑制するため、具体的には以下の取組を実施します。

- IoT機器の悪用を予防する安全管理対策の広報活動を強化します。
- 国立研究開発法人情報通信研究機構（NICT）が令和5年度末までに限り行うこととされていたID・パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）を令和6年度以降も継続し、「NOTICE」の枠組みを通じた注意喚起を継続します。
- 新たに「ファームウェアに脆弱性があるIoT機器」の調査をNICTの業務として位置付け、「NOTICE」の枠組みを通じた注意喚起を実施します。
- 「既にマルウェアに感染しているIoT機器」の情報提供をNICTの業務として位置付け、「NOTICE」の枠組みを通じた注意喚起を継続します。
- 従来から協力関係にあるインターネットサービスプロバイダ（ISP）に加え、IoT機器のメーカーやその他セキュリティ関係機関等との連携を強化します。

IoT製品セキュリティラベリング制度構築に向けて

IoT機器の**脆弱性を狙った**サイバー脅威が高まってきている



IoT機器を狙った攻撃（36.6%）

不審な通信のうち1/3以上はIoT機器を狙った攻撃

その他の攻撃（63.4%）

ダークネットにおける年間観測パケット数の割合

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

諸外国でもIoT製品セキュリティ対策に関する**適合制度の検討**が進展

共通的な物差しでIoT製品のセキュリティ機能を評価・可視化し、適切なセキュリティ対策が講じられているIoT製品が広まる仕組みの構築が必要

- 経済産業省は、2022年11月より「IoT機器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」を開催

経済産業省のパブリックコメント

経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大 | アクセシビリティ閲覧支援ツール

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策について

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2023年度3月一覧 ▶ 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の最終とりまとめを公表し、制度構築方針案に対する意見公募を開始しました

English

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の最終とりまとめを公表し、制度構築方針案に対する意見公募を開始しました

2024年3月15日

▶ 安全・安心

【2024年3月15日発表資料差し替え】関連資料「IoT製品に対するセキュリティ適合性評価制度構築方針案（概要説明資料）」につきまして、誤植がございましたので差し替えました。
IoT製品の脆弱性を狙ったサイバー脅威が高まっていることを踏まえ、経済産業省では、2022年11月よりIoTセキュリティ適合性評価制度構築に関する検討会を開催し、今般、最終とりまとめを策定しました。

まずは2025年3月頃にIoT製品共通の最低限の脅威に対応するための基準（☆1）に対する自己適合宣言の受付及びラベル付与の開始を目指し、政府機関や重要インフラ事業者等の調達ルールに本制度が活用されるよう働きかける予定です。

1. 背景・趣旨

近年、デジタル化の進展に伴い、IoT製品の数が急速に増加するとともに、IoT製品を狙った攻撃も増加傾向にあるなど、IoT製品の脆弱性を狙ったサイバー脅威が高まってきています。こうした背景を踏まえ、諸外国ではIoT製品のセキュリティ対策に関する制度検討が進んでいます。

諸外国の取組も踏まえつつ、我が国においても適切なセキュリティ対策が講じられているIoT製品が広まる仕組みを構築することを目指し、経済産業省は、2022年11月に「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」（以下「検討会」という。）を設置し、議論を進めてきました。

国内で構築するIoT製品に対するセキュリティ適合性評価制度（以下「本制度」という。）を、広く普及させ、そして社会に浸透させるために、IoT製品の調達者が自組織の資産をサイバー脅威から保護するべく適切なセキュリティ水準を満たした製品（ラベルが付与された製品）を優先的に選択するように促すと同時に、IoT製品ベンダーが積極的にラベルを取得することを促すことが必要です。このため、検討会では、以下の三点を主目的として制度を検討してきました。

1. 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（特に初期ターゲットとして、政府機関等、重要インフラ事業者、地方公共団体を設定）。
2. 特定分野のシステムに組み込まれて調達・利用されるIoT製品に求められるセキュリティ要件を定め、必要な認証・ラベルを各業界団体等で指定できるようにする（業界標準としての活用）。
3. 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。

今般、経済産業省は、検討会としての最終とりまとめを策定しましたので、公表します。最終とりまとめでは、構築すべきセキュリティ適合性評価制度の目的と位置付けや、制度の運用体制や対象とする製品範囲などの制度詳細、制度の発展に向けた施策等について、検討会で頂いた主な御意見及びそれを踏まえて構築すべき制度を示しています。併せて、経済産業省は、最終とりまとめを踏まえた本制度の制度構築方針案を作成し、意見公募を開始（2024年3月15日～4月15日）しました。

e-GOV パブリック・コメント

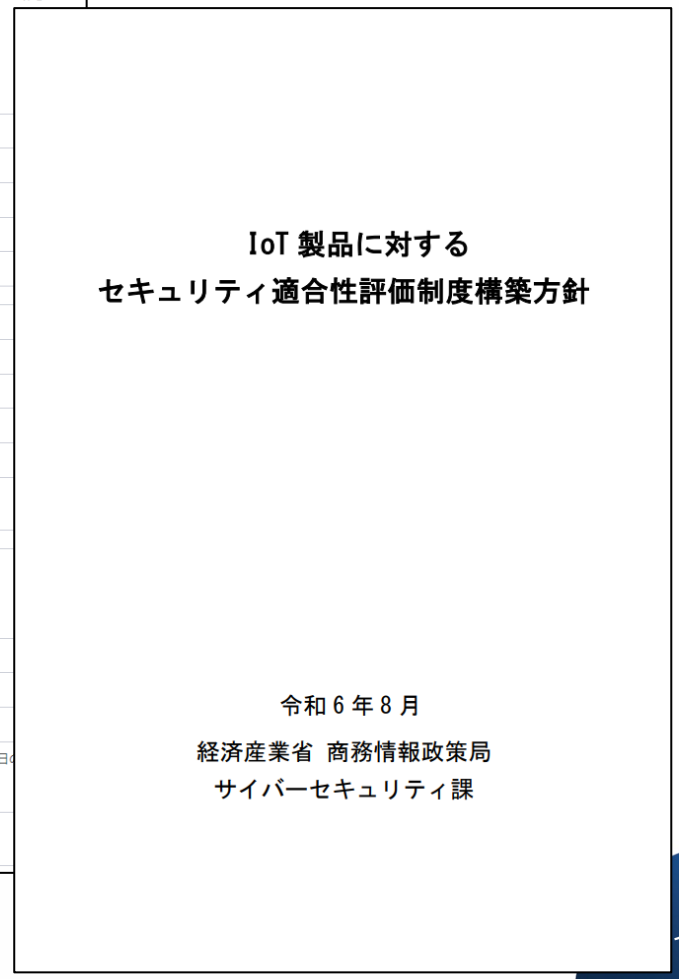
トップ | パブリック・コメント制度について | 案件一覧 | ヘルプ

トップ ＞ 案件一覧 ＞ IoT製品に対するセキュリティ適合性評価制度構築方針案に対する意見公募手続の結果について

IoT製品に対するセキュリティ適合性評価制度構築方針案に対する意見公募手続の結果について

カテゴリー	IT社会化推進
案件番号	595224006
定めようとする命令などの題名	
根拠法令条項	特になし
行政手続法に基づく手続か	任意の意見募集
案の公示日	2024年3月15日
受付締切日時	2024年4月15日23時59分
結果の公示日	2024年8月23日
対象が定められた日	2024年8月23日
提出意見数	37
提出意見を踏まえた案の修正の有無	有
結果概要 提出意見 意見の考慮 結果・理由等	IoT製品に対するセキュリティ適合性評価制度構築方針案に対する意見公募手続の結果について PDF （別紙）提出意見に対する考え方 PDF IoT製品に対するセキュリティ適合性評価制度構築方針 PDF IoT製品に対するセキュリティ適合性評価制度構築方針 別添 ☆1セキュリティ要件・適合基準 PDF
その他	IoT製品に対するセキュリティ適合性評価制度構築方針（概要説明資料） PDF
公募時の内容	公募時の画面
資料の入手方法	
備考	「IoT製品に対するセキュリティ適合性評価制度構築方針 別添 ☆1セキュリティ要件・適合基準」は、2024年3月15日の 募版から変更なし。 産業サイバーセキュリティ研究会WG3 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
問合せ先 （所管省庁・部局名等）	経済産業省 商務情報政策局 サイバーセキュリティ課

[URL]
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf



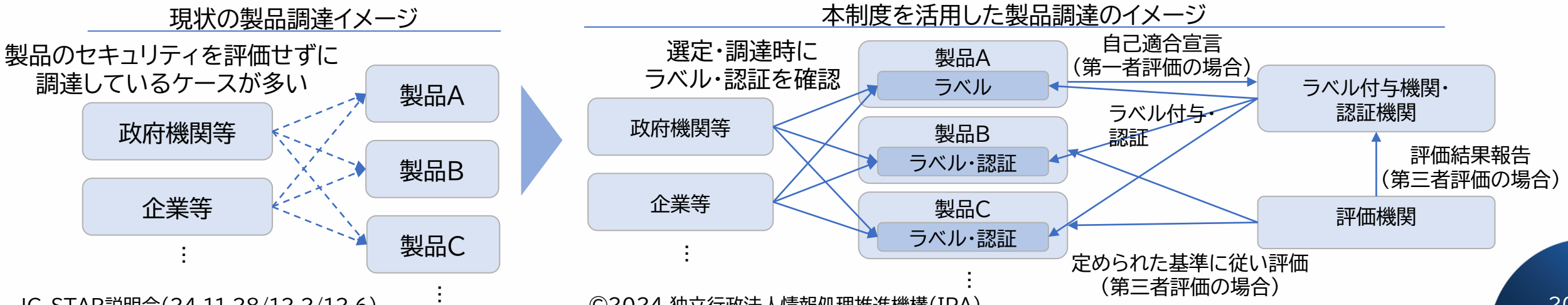
IoT 製品に対する
セキュリティ適合性評価制度構築方針

令和 6 年 8 月

経済産業省 商務情報政策局
サイバーセキュリティ課

制度の目的と位置づけ

- 調達者・利用者が求めるセキュリティ水準のラベルが付与されたIoT製品を優先的に選択することの意義
  - ① 政府機関や企業等で調達するIoT製品について、共通的な物差しでセキュリティを評価・可視化することで、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
  - ② 特定分野のシステムに組み込まれて調達・利用されるIoT製品に必要なラベルを付与し、各業界団体等で指定できるようにすることで、当該特定分野において求められる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

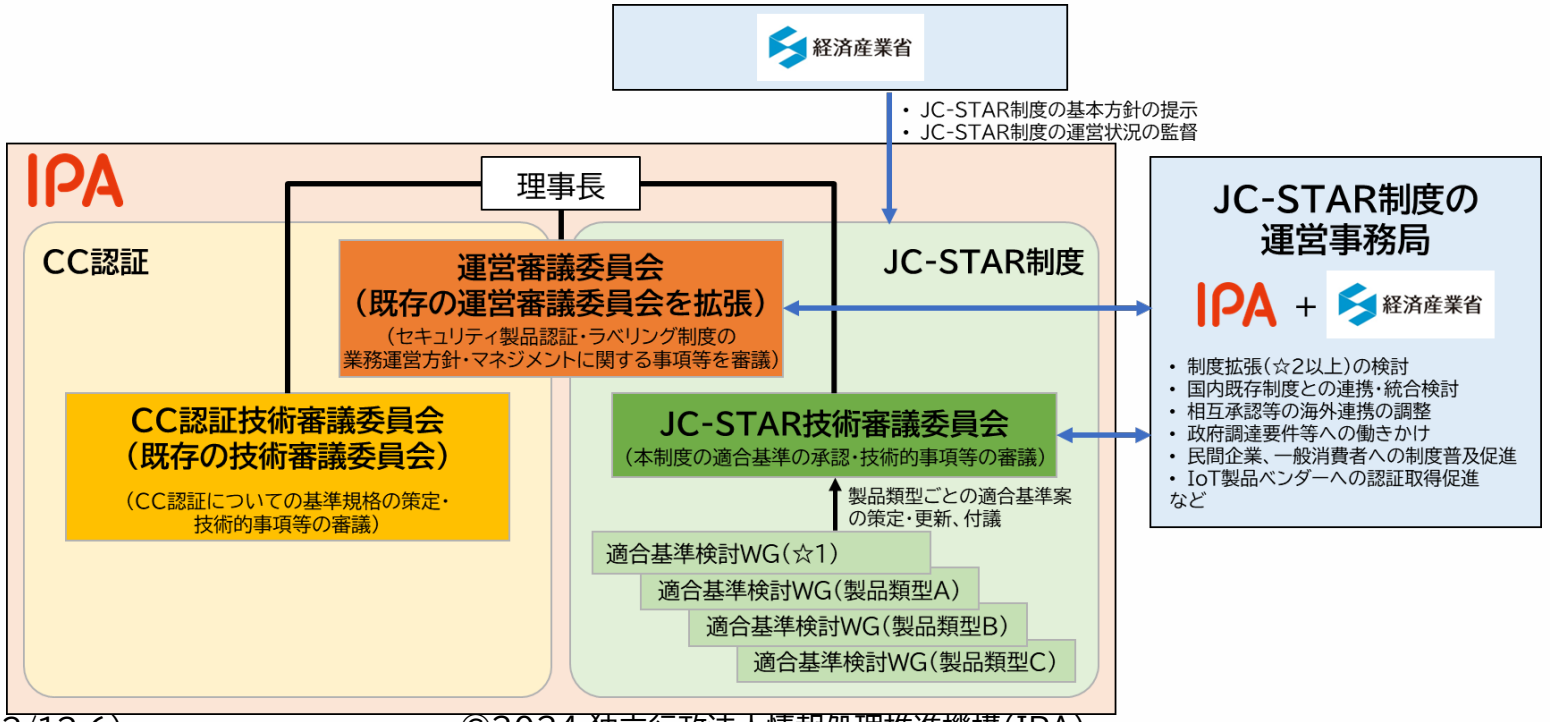


制度に対するインセンティブ

- セキュリティ要件に応じたラベルを付与することで、IoT製品ベンダへのインセンティブ、IoT製品の付加価値向上に繋げる
  - ① 政府機関等、重要インフラ事業者、地方公共団体等の社会的にセキュリティリスクが高く確かな制度利用が見込まれる組織のIoT製品の調達要件の中にラベルが付与された製品の選定を含めることを働きかけ
    - **「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」・ガイドライン（反映済）**
    - 「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針・手引書
    - 地方公共団体セキュリティポリシーガイドライン
  - ② 業界標準としてIoT製品ベンダと調達者・利用者が、ラベルが付与された製品の製造・販売と選定・調達する分野を確保
    - 政府機関等で主に調達されるIoT製品を中心に、関連団体・業界団体と連携
    - 積極的なラベル取得の働きかけを行うことに賛同していただいている**賛同団体：5団体**
  - ③ 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製品ベンダの負担を軽減

制度の運営体制

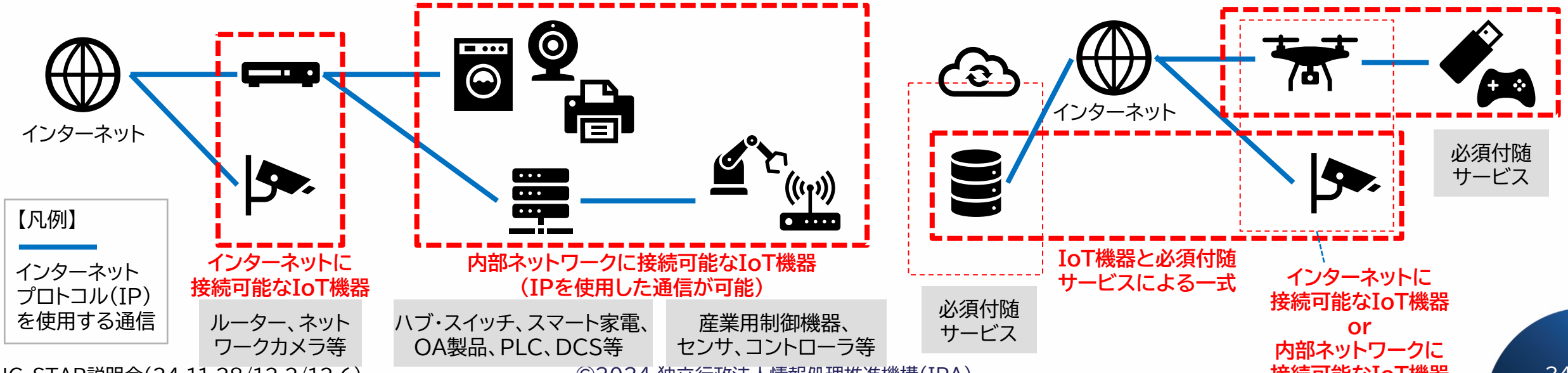
- 経済産業省の示す制度構築方針に従い、同省の監督のもと、本制度を構築・運営するスキームオーナーをIPAとする。IPAが運営するJISEC制度を、CC認証から本制度を含む形に拡張させる枠組みとする
- 技術審議委員会は、プレ委員会を引き継ぐ形で新設し、適合基準の承認・技術的事項等を審議する
- 各製品類型ごとの適合基準案の策定は、技術審議委員会の配下に設置する適合基準検討WGにて行う。各WGは、当該製品類型のIoT製品ベンダーや主な調達組織、それらの関連機関・団体を中心に構成予定
- 経済産業省も運営事務局に加わり、制度の拡張・普及や海外との相互承認・連携等について推進



JC-STAR制度の概要説明

適合ラベルの対象範囲

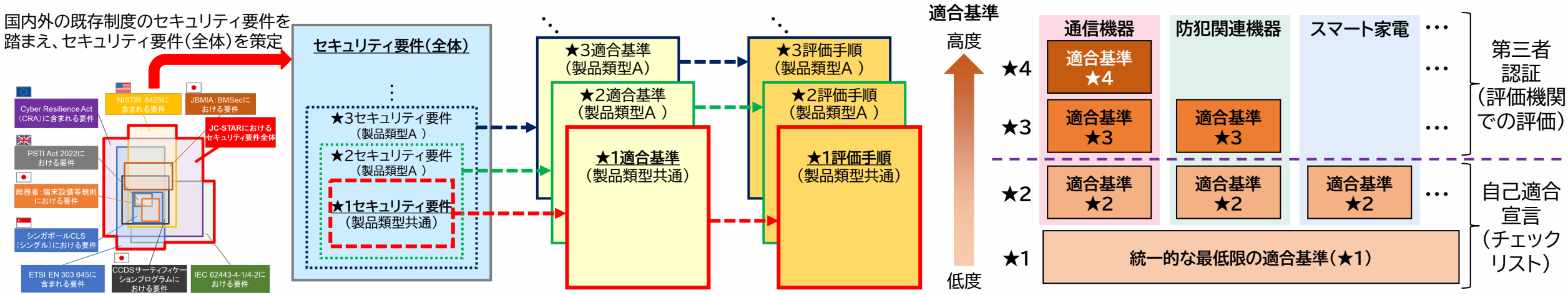
- **IoT製品**：供給者による販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独のIoT機器、又はIoT機器と必須付随サービスとで構成される一式
  - ① **機器**が含まれている（機器に対してラベルが付与される）
  - ② **インターネットプロトコル（IP）を使用したデータの送受信機能を持つ**
  - ③ **直接・間接を問わず、インターネットにつながる（可能性がある／否定できない）**
  - ④ **購入時に具備されているセキュリティ機能を利用し、アップデート以外で（調達者・利用者が自らの意志で）後からセキュリティ機能を追加することが困難／できない**



適合ラベルの適合基準・評価手順

ETSI EN 303 645やNISTIR8425等とも調和しつつ、独自に定める適合基準（セキュリティ技術要件）に基づき、IoT製品に対する適合基準への適合性を確認・可視化する日本の制度

- **求められるセキュリティ水準に応じたセキュリティ技術要件**として、最低限の脅威に対応するための製品共通の適合基準・評価手順（★1）と製品類型ごとの特徴に応じた適合基準・評価手順（★2～★4）を設定

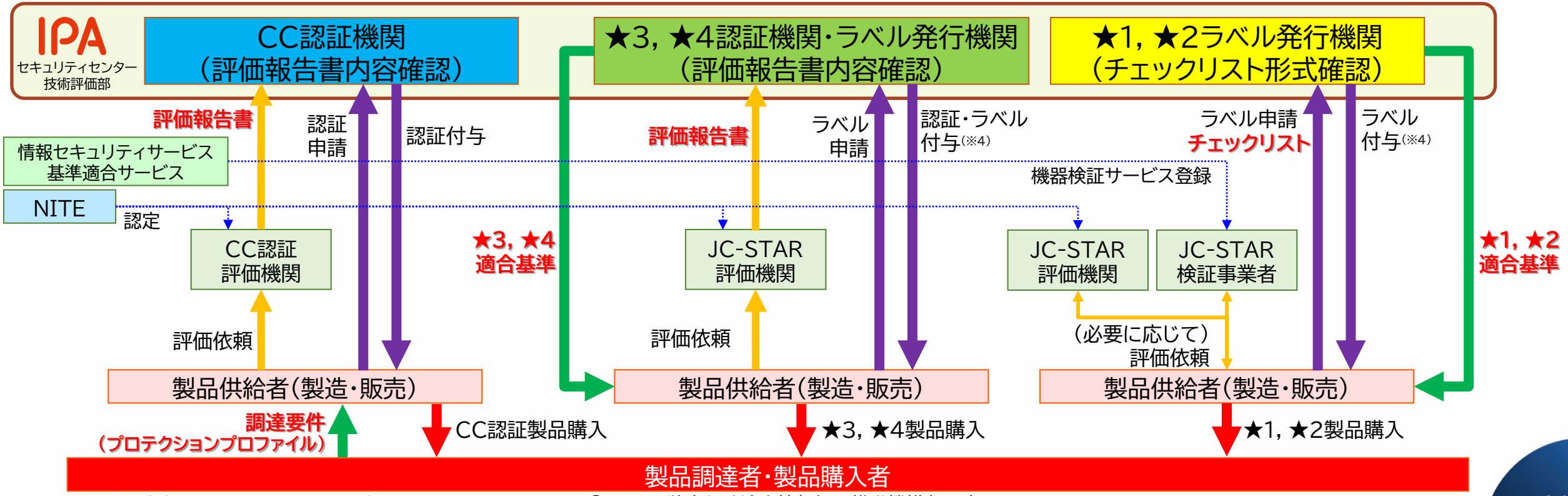


レベル	位置付け	適合基準	評価方式
★4 ★3	政府機関等や重要インフラ事業者、地方自治体、大企業の重要なシステムでの利用を想定した製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの	製品類型別	第三者認証
★2	製品類型ごとの特徴を考慮し、★1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの		自己適合宣言
★1	製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの	製品類型共通	

ラベリング制度スキーム

- **★1、★2は自己適合宣言によるラベル付与**、高い信頼性が求められる**★3、★4は第三者認証**とする
  - ★1、★2はIoT製品ベンダの自己評価のほか、**有資格者(※1)、検証事業者(※2)、評価機関等への評価委託も可能**
  - ★3、★4は**ISO/IEC17025に基づく本制度の評価機関認定(※3)を受けた評価機関による評価**を求める

(※1)指定資格の保有者(情報処理安全確保支援士等)が、IoTセキュリティ評価に関する研修受講完了又は評価ガイドラインを理解していることの宣誓したうえで、評価又は評価結果の確認を実施した場合に「有資格者」による評価とする。
(※2)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。
(※3)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。
(※4) 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。



JC-STARにおける★1の位置付け

★1では、以下の3点を最低限実現することが求められる

- ★1の適合基準への適合により、**最低限の脅威に対抗**できる
  - ✓ 特定の製品類型に絞らず、**広範なIoT製品を対象とした、最低限の脅威に対抗するための統一的な基準**とする
- ★1の適合基準への**評価は、低コストかつ自己適合宣言で対応**できる
  - ✓ ベンダ自身による**自己適合宣言を許容**する
  - ✓ 検証や評価を行う担当者が、**チェックリストや評価ガイドを見て低コストで自己評価可能なレベル**とする
  - ✓ **適合性評価チェックリストの申請に基づきラベルを付与**する（IPAはチェックリストの内容確認は実施しない。）
- ★1の適合基準は、**海外制度と国際連携可能な基準**とする
  - ✓ シンガポールCLS＊1要件や英国PSTI法など、**海外制度と国際連携可能な要件**とする

★1で実現したいセキュリティ水準の考え方

① **マルウェアに感染してボット化するのを防ぐ**。とりわけ、感染した機器からの感染拡大を防止する

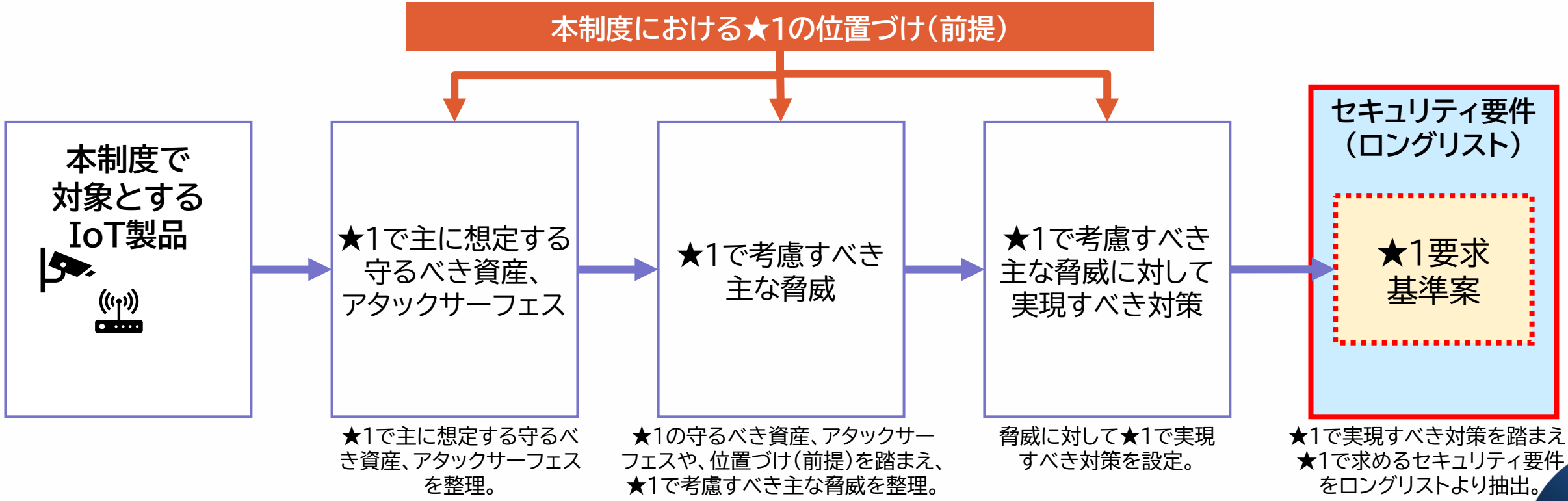
② インターネット側からの遠隔攻撃を主に想定し、スクリプトキディレベル（限定的な専門知識のみを有し、インターネットやダークウェブなどで公開されているクラックツール等を用いてシステムの脆弱性を利用して攻撃するレベル）の攻撃（不正アクセスや盗聴など）に対して**実用的な耐性を持たせる**

③ 製品不具合や脆弱性に対する**対応・サポート方針を明確化**し、適合ラベル有効期間内の**サポート（アップデートファイルの提供等）が確実に提供**されるようにする

④ 廃棄前に、運用中に生成されたデータを**適切に削除することができる**

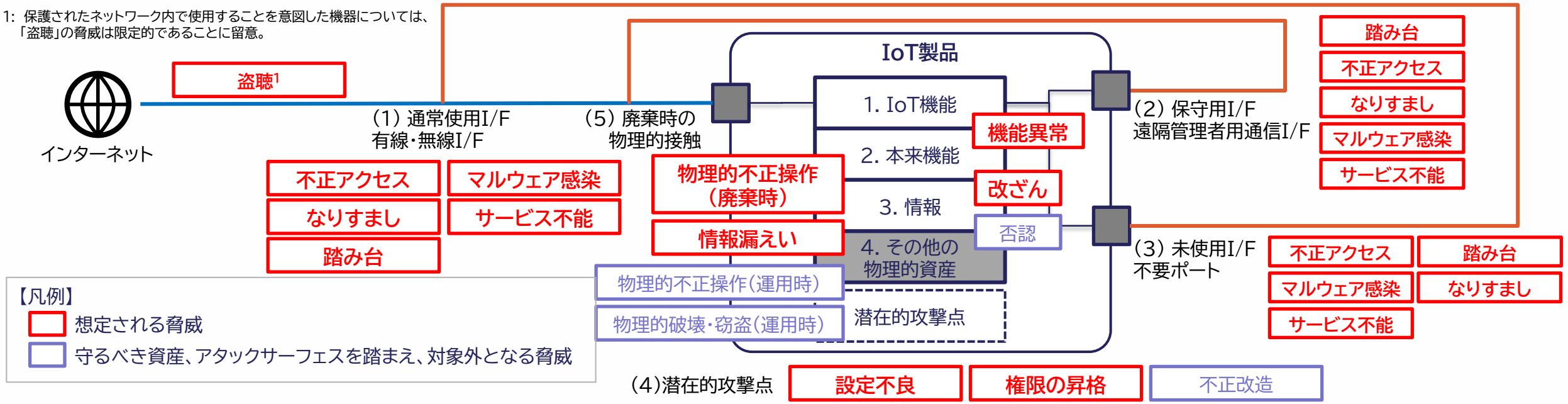
★1におけるセキュリティ要件の抽出について

1. セキュリティ要件全体のリスト(ロングリスト)より、本制度の**★1で設定するセキュリティ要件を抽出**
2. この抽出に向け、まず本制度における**★1の位置づけ(前提)を整理**するとともに、対象製品において★1で主に守るべき資産、アタックサーフェスを整理
3. これらの項目を踏まえ、**★1で考慮すべき主な脅威を整理**した上で、**当該脅威に対して★1で実現すべき対策を整理**し、当該対策を実現するための**セキュリティ要件をロングリストより抽出**



★1で想定される脅威

- ★1で想定する守るべき資産及びアタックサーフェスを踏まえ、IoT製品に対して想定される脅威を以下のようにマッピング。なお、脅威は、IPA文書及びCCDS文書を参照して整理
  - ✓ 「製品運用時の物理的接触」と「製品開発・調達等のサプライチェーンにおける接触」のアタックサーフェスを想定しないため、「物理的不正操作（運用時）」「物理的破壊・窃盗（運用時）」「不正改造」の脅威は対象外
  - ✓ STRIDEモデルでは「否認」が一つの脅威として挙げられているが、★1で想定する守るべき資産として「否認」の影響を受ける資産を考慮していないため、当該脅威は対象外



出所）IPA つながる世界の開発指針 第2版 https://www.ipa.go.jp/publish/qv6pgp000000114a-att/000060387.pdf
IPA IoT開発におけるセキュリティ設計の手引き https://www.ipa.go.jp/security/iot/ug65p90000019832-att/ssf7ph0000002vih.pdf
CCDSサーティフィケーションプログラム IoT機器に対するリスク分析のガイド https://www.ccds.or.jp/certification/document/ccds_risk-analysis-process.pdf

脅威に対抗するために★1で実現すべき対策

★1で考慮すべき主な4つの脅威に対し、★1の位置付けや海外制度の基準等を踏まえ、製品／製品ベンダにおいて実現すべき対策を以下のとおり選定

★1で考慮すべき主な脅威			脅威に対抗するために★1で実現すべき対策			
			製品における対策		製品ベンダにおける対策	
			カテゴリ	対策	カテゴリ	対策
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	• 容易に推測できるパスワードが設定できない仕組みを導入する • セキュアな認証の仕組みを提供する • ブルートフォースによる認証試行を防ぐ仕組みを提供する	情報提供	• セキュアな利用方法に関する情報を提供する
	②脆弱性の放置により、		脆弱性対策、ソフトウェアの更新	• 深刻度の高い既知の脆弱性及び主要なCWEに対する対策を行う • ソフトウェアコンポーネントがアップデート可能な仕組みを導入する	情報・問い合わせの受付、情報提供	• 製品に関する情報及び脆弱性に関する情報を提供する • セキュリティパッチの適用方法に関する情報を提供する
	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	• 不要なインタフェースを無効化する	―	―
			データ保護	• 機器が保有する守るべき情報を保護するための機能を提供する（①～③の脅威に共通する対策）	―	―
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	• インターネット経由で伝送される守るべき情報を保護するために情報の漏えいや変更に対する保護対策を実装する	―	―
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	• 機器の利用中に機器内に保存された守るべき情報を製品本体や関連サービスを介して削除できる機能を提供する • 機器に当初から搭載されている守るべき情報を保護するための機能を提供する	情報提供	• セキュアな廃棄方法に関する情報を提供する
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			レジリエンスの向上	• ネットワーク切断や停電等の事象が発生し、復旧した場合でも、認証情報やソフトウェア設定は初期状態に戻らず、電源OFF前の状態を提供する	―	―

★1のセキュリティ要件・適合基準

★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			
			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**[1-3,5-5] (2)**容易に推測可能なデフォルトパスワードの禁止**[1-2,1-1] (3)パスワード等の認証値の変更機能[1-4] (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**[1-5]	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)[17-12,17-3,17-5,17-8,17-10]
	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[3-1,3-2] (7)**容易かつ分かりやすいアップデート手順**[3-3] (8)アップデート前のソフトウェアの完全性の確認機能[3-7,3-2,3-10] (10)ユーザが製品型番を認識可能とする記載・機能[3-16]	情報・問合せの受付、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**[2-1] (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[3-8]
	③未使用インタフェースの有効化により、		インタフェー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)[6-1]	―	―
	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、物理的保護による保存、OSセキュア管理**等)[4-1]	―	―
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)[5-1,5-7]	―	―
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**[11-1] ※(11)も含む	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)[9-1]	―	―

※「適合基準の概要」欄の末尾の"[N-N]"は対応するセキュリティ要件の項目番号(複数の場合、代表的な要件を先頭に記載)を示す。セキュリティ要件は17個の大項目に分類
※ 複数の脅威に対応するための適合基準もあるが、代表的なものにマッピングしている。

適合ラベル

- 適合ラベルは定められた**適合基準への適合**を示す目印として付与
  - IoT製品が予め具備するセキュリティ機能として満たしてほしい水準にあることを確認できる
  - 完全・完璧なセキュリティが確保されていることを保証するものではない

IoT製品が取得した適合ラベルのレベルを表現しています。
★一つがレベル1を、★四つがレベル4を表します。

適合ラベルを取得したIoT製品情報を確認するため、IPAが管理する「適合ラベル取得IoT製品情報ページ」にリンクします。
このページは登録番号ごとに用意されます。

適合ラベルを取得したIoT製品の登録番号です。

- ラベル付与製品毎の情報提供ページのURLを埋め込んだ**二次元バーコード**を掲載
  - 情報提供ページで「適合ラベルのステータス表示」と「セキュリティ情報・問合せ先の一元表示」を実現
- ラベル付与製品に対して事後的に**検査やサーベイランスを行える**権利をIPAは有する
  - ★1、★2では、適合ラベル交付時に定められた適合基準に適合しているかどうかをIPAは確認しない（評価の信頼性はベンダーの信頼性に依存）
  - 証跡の保管義務をIoT製品ベンダに課す
  - 適合基準への適合に疑義が生じた場合に、必要に応じ、証跡提出の要求やサーベイランスを実施
  - サーベイランスの結果次第では「適合ラベル取消し」も有り得る

製品公開情報(イメージ)

二次元バーコード付適合ラベルを添付してプロモーション可能
常時、最新の適合ラベルステータス(有効、有効期限切れ、取消し等)+セキュリティ情報を提供

■適合ラベル情報

ラベルステータス	有効(Active)
ラベル登録番号	0123456789012345
適合性評価レベル	Star 1(★)
適合基準バージョン	JST-CR-01-01-2024
有効期間	20yy年mm月dd日
後継製品	なし
最新更新日	20yy年mm月dd日
適合評価方法	自己適合評価
チェックリスト	Checklist-N.pdf
評価完了日	20yy年mm月dd日
初回発行日	20yy年mm月dd日
適合評価方法	JC-STAR検証事業者
チェックリスト	Checklist-1.pdf
評価完了日	20yy年mm月dd日

JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN(IPA)

有効期間は2年が基本。
延長申請可

適合ラベルのステータス	概要
有効(Active)	適合ラベルが有効期間内にあり、**失効・取消しに該当する事由がない**状態
失効猶予(延長申請中(Extension procedure in progress))	適合ラベルの有効期間が満了しているが、**有効期間の延長申請手続きが行われている**状態
失効(有効期限切れ(Expired))	適合ラベルの有効期間が満了した後、**有効期間の延長が行われていない**状態
失効(自主取下げ(Withdrawn))	適合ラベルの有効期間内に、**IoT製品ベンダーからの申し出により、適合ラベルの効力を失効**させた状態
取消し(Revoked)	適合ラベルの有効期間内に、適合ラベルの取消し事由に該当する事象が発生し、定められた期間内にその事由を解消するための是正がなされなかった場合に、**IPAが強制的に適合ラベルの効力を停止**させた状態

■製品情報

適合ラベル取得事業者	●●●●株式会社
製品類型	通信機器
製品名称	△×ルータ
製造事業者	●●●●株式会社
製品型番	RT-■■■■
ファームウェアバージョン	FW-〇〇〇〇〇〇
サポート期間	20yy年mm月dd日以降(終了日未定)

有効期間内はアップデートサポートを義務付け

製品概要	….
製品ホームページ	https://….
製品に関する問合せ窓口	….@…
不具合・脆弱性届出窓口	….@…
技術基準適合認定番号等	電気通信事業法に基づく技術基準適合認定番号等
他認証の認証番号等	JC-STAR以外のサイバーセキュリティ関連認証の取得実績・認証番号

■セキュリティ情報

脆弱性開示ポリシー	https://….
アップデート情報	20yy年mm月dd日 FW-◆◆◆◆◆◆
当該製品に関わる重要なセキュリティ情報	重要なセキュリティ情報
その他セキュリティ関連情報	他セキュリティ関連情報

適合ラベルの失効・取消し

「低コストかつ短期間で適合ラベルを取得可能」と、「有効期間の導入」と「疑義が生じた場合に、事後的に検査やサーベイランスを実施し、その結果次第で適合ラベル取消しも有り得る」仕組みを入れることで適合ラベルの信頼性のバランスを確保

適合ラベルの失効	● 有効期間満了に伴うもの（表示としては【有効期間切れ（Expired）】） ● 登録者からの自主取下げ申請によるもの（表示としては【自主取下げ（Withdrawn）】）
適合ラベルの取消し	● **取消事由（以下のようなもの：例示）に該当すると判断されたもので、指定された期間内に是正措置が取られなかった場合（表示としては【取消し（Revoked）】）** ➢ **サーベイランスの結果、申請内容、自己適合宣言の内容、ラベル取得要求事項で定められた条件に反していない旨の自己宣言の内容又は適合評価・認証等に関して違反や虚偽があると認められた** ➢ **重大な脆弱性が検知された後、適切な期間内に当該脆弱性に対する適切な対応がなされなかった** ➢ 適合ラベルの維持申請が認められなかった ➢ 適合ラベルの承継が認められなかった ➢ 適合ラベルの信頼性を著しく損なうような行為等が認められた

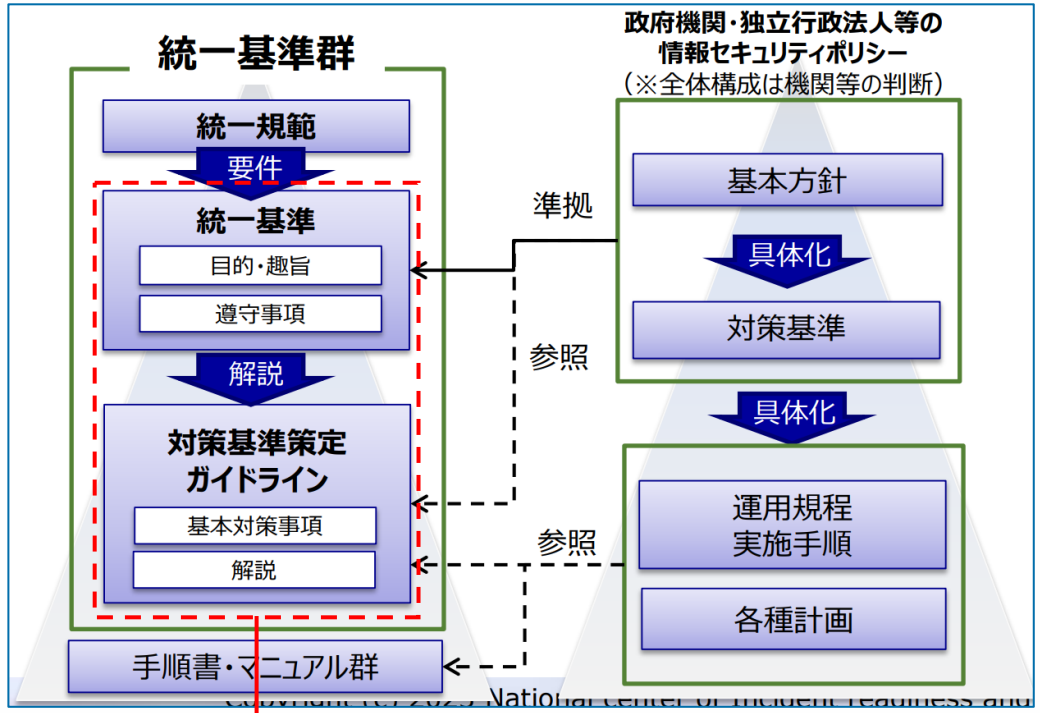
制度に対するインセンティブ（再掲）

- セキュリティ要件に応じたラベルを付与することで、IoT製品ベンダへのインセンティブ、IoT製品の付加価値向上に繋げる
  - ① 政府機関等、重要インフラ事業者、地方公共団体等の社会的にセキュリティリスクが高く確かな制度利用が見込まれる組織のIoT製品の調達要件の中にラベルが付与された製品の選定を含めることを働きかけ
    - **「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」・ガイドライン（反映済）**
    - 「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針・手引書
    - 地方公共団体セキュリティポリシーガイドライン
  - ② 業界標準としてIoT製品ベンダと調達者・利用者が、ラベルが付与された製品の製造・販売と選定・調達する分野を確保
    - 政府機関等で主に調達されるIoT製品を中心に、関連団体・業界団体と連携
    - 積極的なラベル取得の働きかけを行うことに賛同していただいている**賛同団体：5団体**
  - ③ 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製品ベンダの負担を軽減

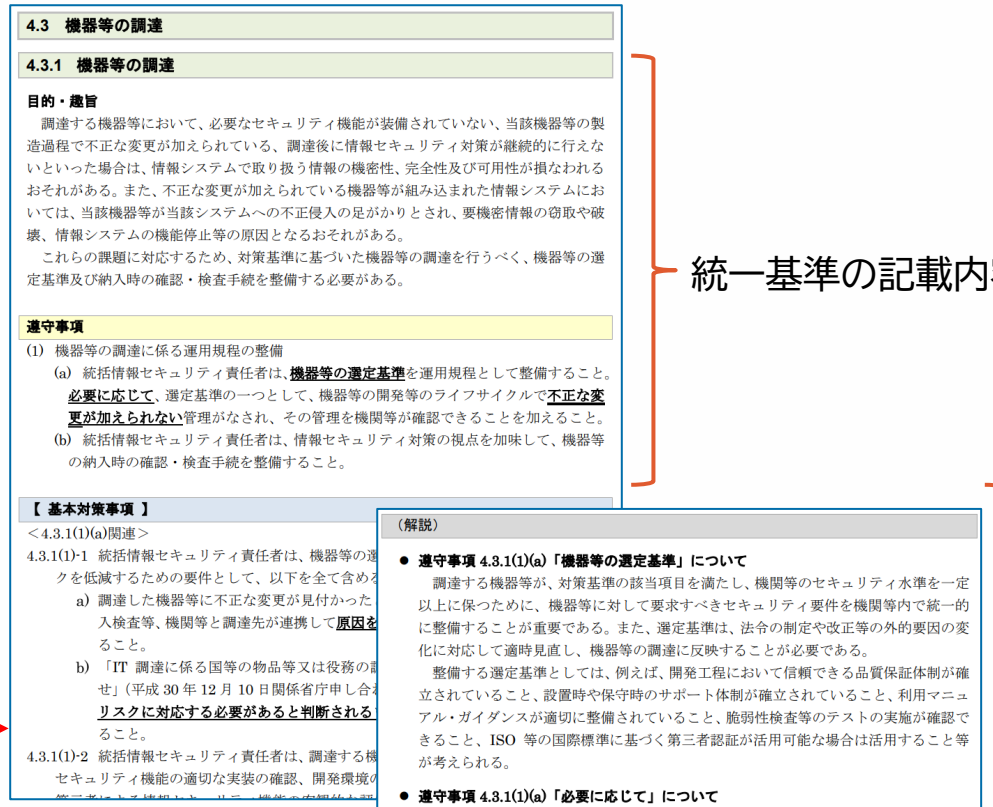
本制度活用に関する調整状況（政府機関等）

- 「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と検討中（一部改定されたガイドラインに方向性が明記された）
- 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＞

4.3.1(1)-1 統括情報セキュリティ責任者は、機器等の選

クを低減するための要件として、以下を全て含めて

a) 調達した機器等に不正な変更が見付かった

入検査等、機関等と調達先が連携して**原因を**

ること。

b) 「IT 調達に係る国等の物品等又は役務の

せ」（平成 30 年 12 月 10 日関係省庁申し合

リスクに対応する必要があると判断され

ること。

4.3.1(1)-2 統括情報セキュリティ責任者は、調達する

セキュリティ機能の適切な実装の確認、開発環境

（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、

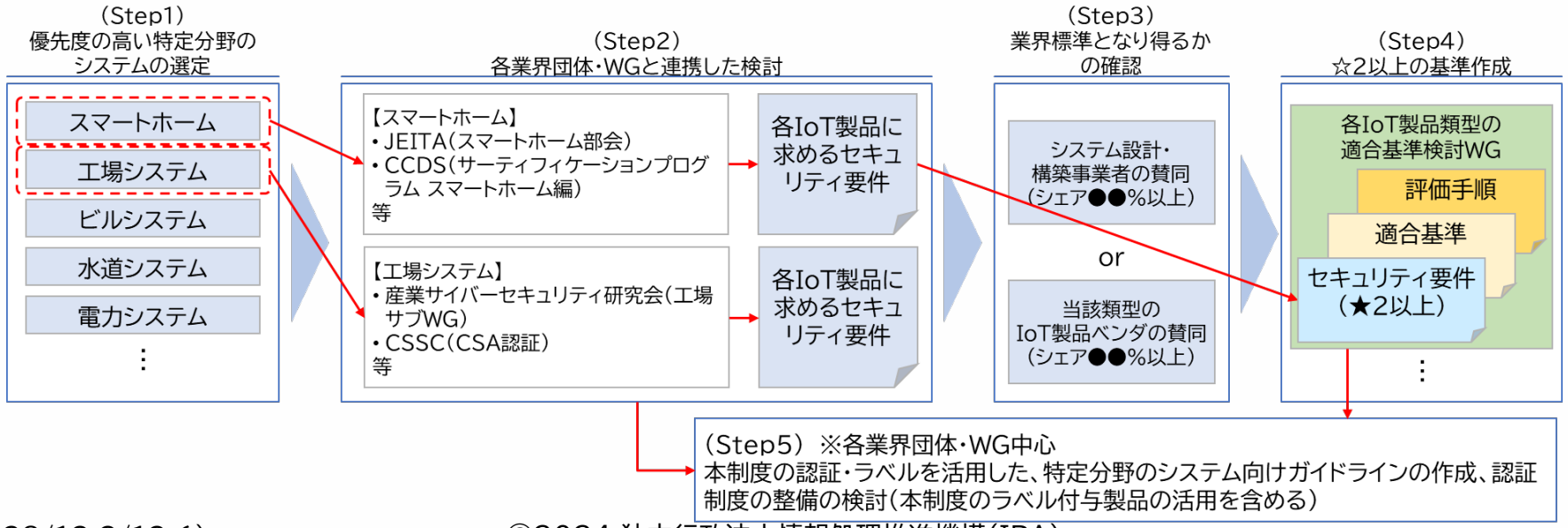
統一基準の記載内容

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）一部改定」
https://www.nisc.go.jp/pdf/policy/general/guider6.pdf

本制度活用に関する調整状況(重フラ・自治体等)

- 重要インフラ事業者、地方公共団体におけるIoT製品調達時に、用途やそのリスクに応じてラベル付与製品を選定・調達することを求めていくように、関係者と調整を進める
  - 「重要インフラのサイバーセキュリティに係る行動計画」に紐づく安全基準等策定指針および手引書
  - 地方公共団体セキュリティポリシーガイドライン
- 政府機関等で主に調達されるIoT製品を中心に、その関連団体に対して、本制度との連携や会員企業への積極的なラベル取得の働きかけの賛同を図る
- 優先度の高い特定分野のシステムに対して業界団体やワーキンググループと連携する



賛同団体一覧

各業界団体やIoT製品を製造しているベンダーも参画し、JC-STAR制度の連携や会員企業への積極的なラベル取得の働きかけを行うことに賛同していただいている団体

（五十音順）

名称	会員数	主なIoT製品類型
情報通信ネットワーク産業協会（CIAJ）	会員数：153社・団体（2024年8月現在） （正会員86社・団体、賛助会員48社・団体、名誉友好会員19団体）	情報通信関連機器
デジタルライフ推進協会（DLPA）	会員数：12社（2024年9月現在） （正会員7社、賛助会員5社）	ネットワーク機器（主に消費者向け）
電子情報技術産業協会（JEITA）	会員数：387社・団体（2024年2月14日現在） （正会員350社・団体、賛助会員37社・団体）	スマートホーム関連機器、ヘルスケア関連機器
日本防犯設備協会（SSAJ）	会員数：274社・団体（2023年7月現在） （正会員73社、準会員151社、賛助会員5団体、特別会員45団体）	防犯カメラ、デジタルレコーダ（防犯用）、その他防犯設備機器
ビジネス機械・情報システム産業協会（JBMIA）	会員数：39社・団体（2024年9月現在） （正会員20社、準会員17社・団体、賛助会員2社）	プリンター・複合機、データプロジェクター、その他事務機

諸外国制度との連携

シンガポール、英国、米国、EUの各国担当機関との間で相互承認に向けた交渉中

（仮訳）

ファクトシート：岸田総理大臣の国賓待遇での米国公式訪問
2024年4月10日

本日、バイデン大統領は、日米両国の深く歴史的な絆を祝福するため、岸田日本国内閣総理大臣を公式訪問及び公式晩餐会に迎えた。今回の訪問はまた、日米同盟が将来の進歩と繁栄という共通のビジョンを促進するグローバルなパートナーシップへと進化していくに当たり、その上昇軌道を反映している。両首脳の野心的な取組は、同盟の深さと広さに及んでおり、防衛・安全保障、宇宙、先端技術及び経済協力、外交及び開発並びに人と人とのつながりにおける協力を含むものである。

この二国間で調整されたファクトシートは、公式晩餐会を含む公式訪問において確認又は再確認された政治的見解及び日米間の更なる協力活動の計画の概観を提示するものである。

情報保全及びサイバーセキュリティに関する協力の深化：日米両国は、同盟が情報・コミュニケーション技術（ICT）分野において増大する脅威に先んじ、強じん性を構築することを確保するため、情報保全及びサイバーセキュリティに関する協力を引き続き深化させていくことを誓約する。日米両国はまた、重要インフラの防護に関する協力を強化していく計画である。日米両国は、IoT（Internet of Things）のサイバーセキュリティ・ラベリング制度の相互承認を達成するための行動計画を策定するため、関連する専門家による作業部会を設置する予定である。

[URL] https://www.mofa.go.jp/files/100652150.pdf

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme（CLS）	Product Security & Telecommunication Infrastructure Act（PSTI法）	U.S. Cyber Trust Mark	Cyber Resilience Act（CRA）
開始時期	2020年10月開始	2024年4月施行	2024年中開始予定	未定（2027年開始想定）
任意/義務	任意	義務	任意	義務
対象	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	デジタル製品
適合基準	• ＊1：ETSI EN 303 645の基準の一部 • ＊2：＊1の基準に加え、ETSI EN 303 645の基準の一部 • ＊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」等を義務付ける予定
評価方法	• ＊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	• 「重要なデジタル製品」以外の製品：自己適合宣言 • 「重要なデジタル製品」のクラスⅠ（EUCCやEN規格の対象外の製品を除く）及びクラスⅡの製品：第三者認証

JC-STAR説明会（24.11.28/12.2/12.6）

今後のスケジュール予定