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
神田　雅透

セキュリティ製品対策の急速な強化の必要性

- 一言で言えば「信頼できるセキュリティ製品を使わないと危ない」時代になってしまったから
  - 色々なものがインターネットにつながる時代
  - サイバーでの出来事がリアルな社会に深刻な影響を与える時代
  - サイバー攻撃の激化（犯罪集団の分業化・専業化・ビジネス化、国家ぐるみの諜報戦・破壊戦、グレーゾーン紛争・ハイブリッド攻撃）
  - サプライチェーン問題

一つの製品におけるサイバーセキュリティインシデントが組織全体やサプライチェーン全体に影響を及ぼす可能性、内部市場の境界を越えた拡散につながる可能性

IoT製品セキュリティラベリング制度（JC-STAR）

2025年3月25日、IoT製品のセキュリティを見える化するラベリング制度の運用開始！
～ セキュリティ対策されたIoT製品を選びやすく！ ～

どの製品のセキュリティ対策が適切か判断できない

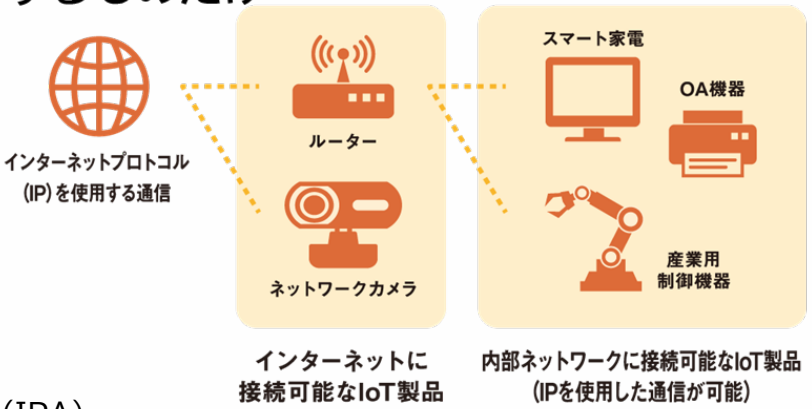
JC-STAR適合ラベル

セキュリティ対策の取組をアピールすることが難しい

対象とするIoT製品例

購入時から安全なIoT製品を選ぶことが重要

- 筐体がある（ソフトウェアやサービスではない）
- インターネット側からの通信を受信する可能性がある
- 使えるセキュリティ機能は製品の製造ベンダが提供するものだけ



アジェンダ

1. JC-STARがつくられた背景や目的

2. JC-STARの概要

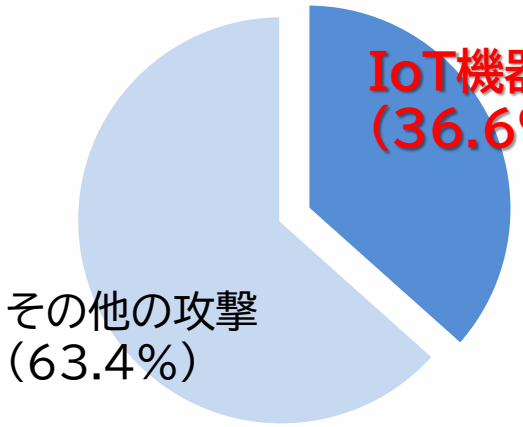
3. JC-STARの今後に向けて

4. 参考：ビルディングオートメーションでの取扱いに向けて

使っているIoT製品がサイバー攻撃にあうか？

サイバー攻撃の対象になるのは、政府とか企業とかでしょう？
IoT製品に大事なデータとか入れていないし・・・

IoT製品は世界中から無作為に狙われています。ざっくりいうと、1日600回以上攻撃されています



不審な通信のうち
1/3以上はIoT機器を
狙った攻撃

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

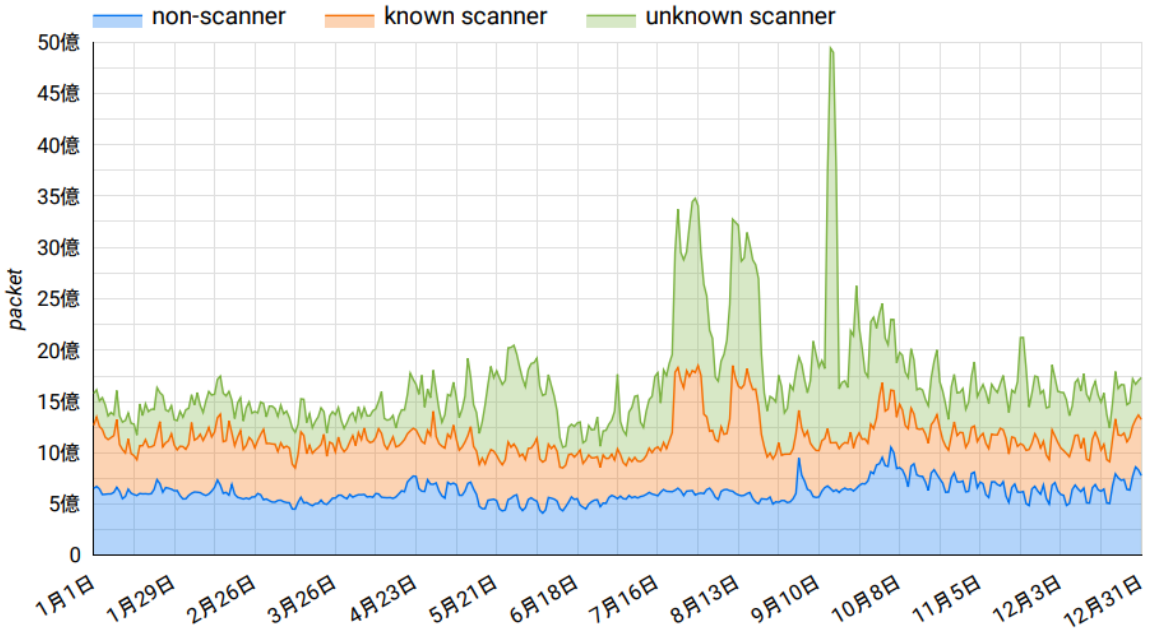


図1: ダークネットにおける日ごとの観測パケット数の推移（積み上げグラフ）
NICT「NICTER観測レポート2023」の1年間にダークネット（約29万観測アドレス）で観測された攻撃パケット数の日ごとの合計

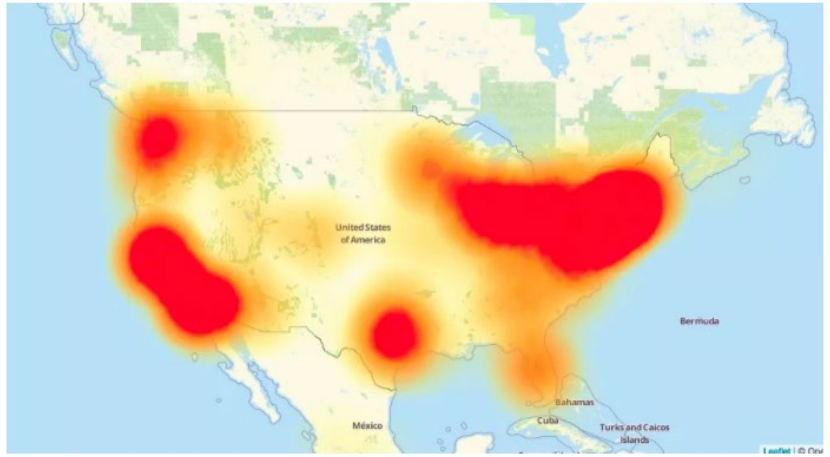
IoT製品のインシデント事例

■ 情報セキュリティ10大脅威で「IoT」が初登場（2017年）

● IoT機器にウイルス感染　⇒　DDoS攻撃用のボットネット化

2016年10月21日

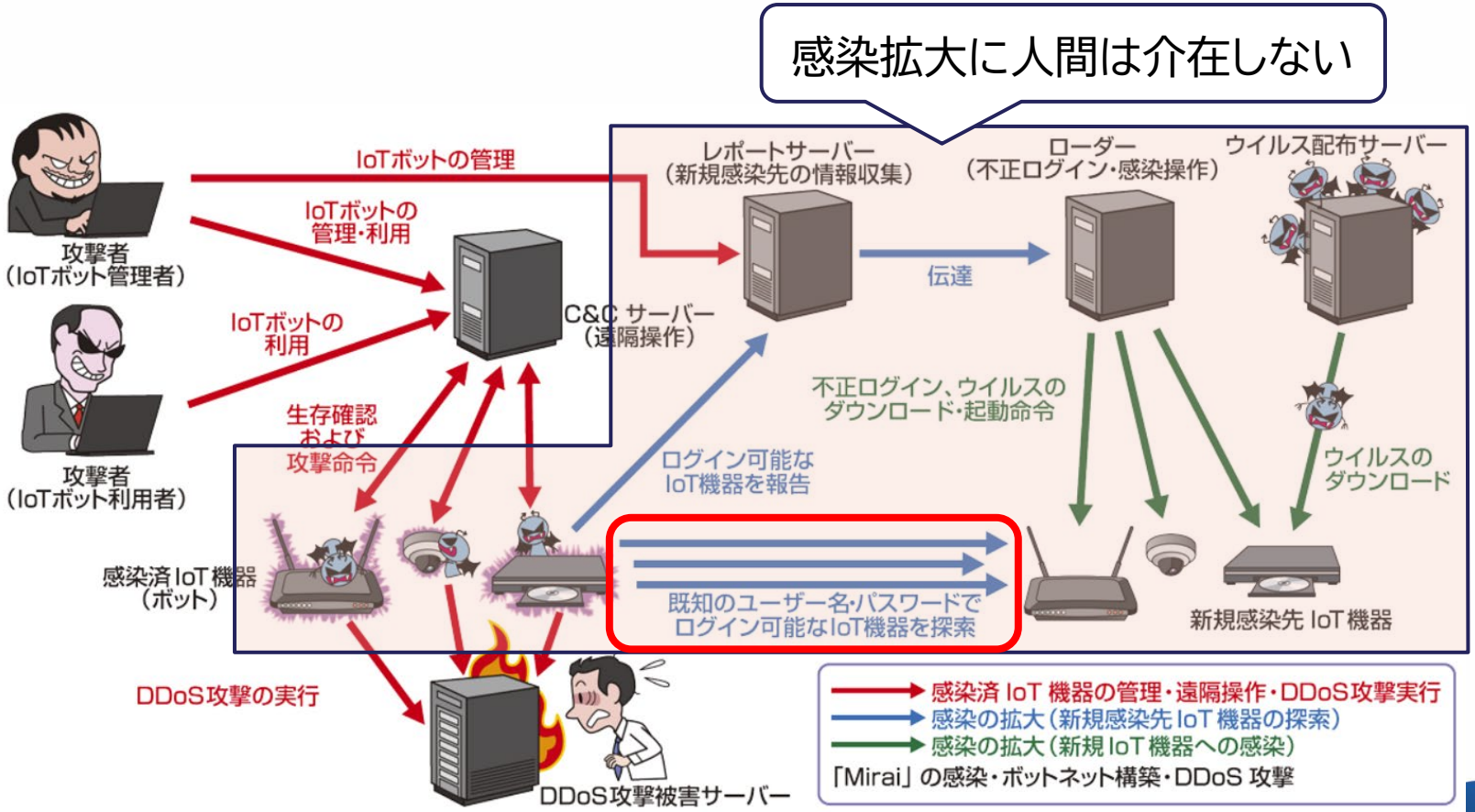
- Amazon・GitHub・Twitter・Netflix等を含めた多くのサイトがアクセス不能
- Miraiに感染したIoT機器によるボットネットからの攻撃と推定
- 500Gbps超にも達するトラフィックを発生



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/



[出典] IPA、情報セキュリティ10大脅威 2017

BA講演会（2026.03.18）

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)を有する国内ベンダ製無線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

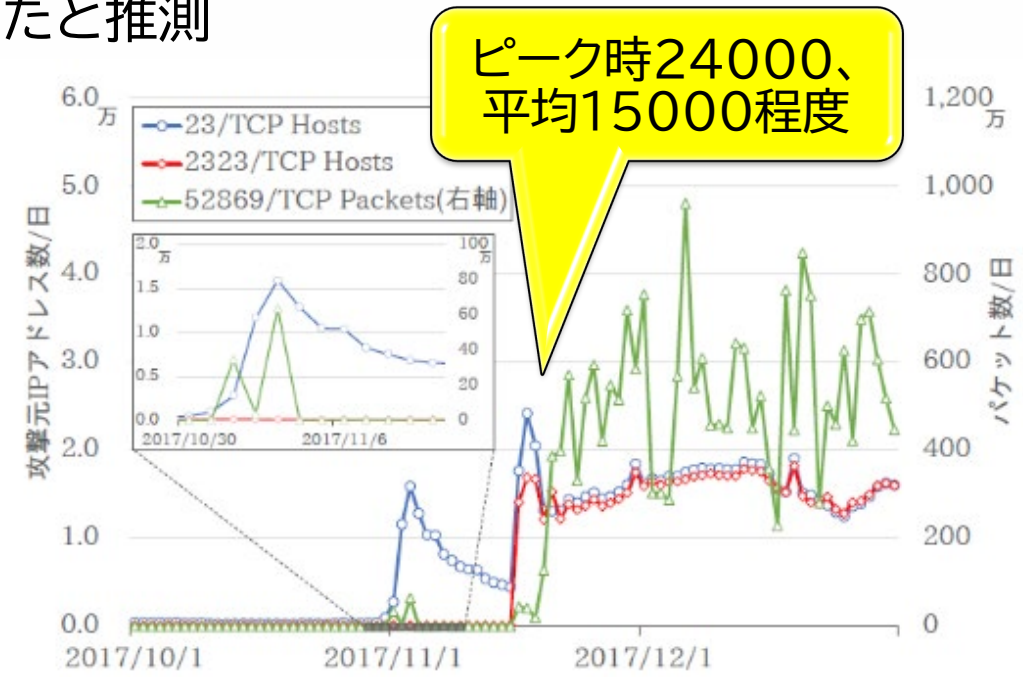


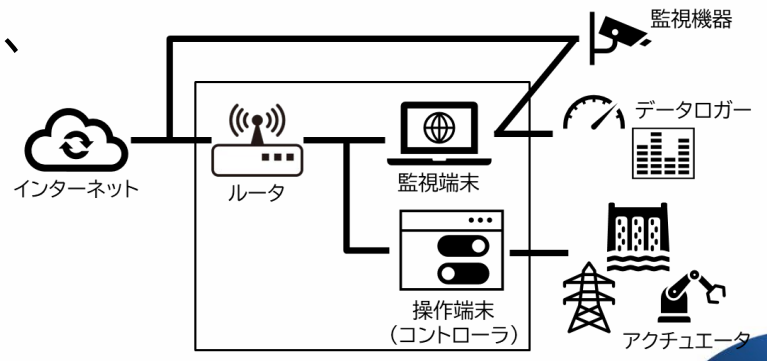
図6: Telnet 宛ての攻撃ホスト数（日本）と 52869/TCP 宛てのパケット数の推移

IoT製品のインシデント事例

- **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。しかも、ハードコードされている部分があり**アップデートが事実上不可能**
    - 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

最近（2025.11）も読売新聞で報道あり
「保育園や工場の防犯カメラ映像、
500件が海外サイト流出…設定に不備」

- **重要インフラ等で利用されるIoT機器の調査（2017, 2020, 2023年度）**
  - 2,883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
    - データロガー、カメラなどの接続機器の起動停止制御用が多数
    - 河川や水道などの水処理施設や太陽光発電を含む発電設備の遠隔監視の目的で設置
  - 90%超が「**インターネット上から確認できることを意図していない**」



IoT製品のインシデント事例

- **家庭用セットトップボックス（STB）乗っ取り・踏み台攻撃（2025年）**
  - IoT機器に**ウイルス感染** ⇒ マネーロンダリングの踏み台攻撃
- **900万台以上の家庭用デバイスの強制切断（2026年; Wall Street J.報道）**
  - Google Threat Intelligence Groupが、家庭用デバイス900万台以上を悪用し、サイバー攻撃の中継点（レジデンシャルプロキシ）として転売していた世界最大級の住宅用プロキシネットワーク「IPIDEAプロキシネットワーク」をテイクダウン
  - 2024年以降のボットネットのテイクダウン・捜査の過程で巧妙化された**不正SDKの存在**を発見
  - IPIDEAプロキシネットワークに関与するものが、安価なルーターやIoT機器の製造、無料アプリ（VPNや節約ツールなど）の開発で利用するSDK（開発キット）にバックドアやプロキシ化するための機能を密かに組み込んで、複数のデベロッパーに提供 ⇒ 製品**出荷時点ですでにボットネット**組込み
- **中国の太陽光発電インバーターに不正な通信機器を搭載（2025年; ロイター報道）**
  - 中国製ソーラーインバーターから製品仕様書に記載されていない不正な通信機器やバッテリーから未登録の携帯電話用無線機が発見
  - 米国は「信頼できる機器」の電力網への統合に向けた取り組みを推進

IoTになって便利になった・・・けれども

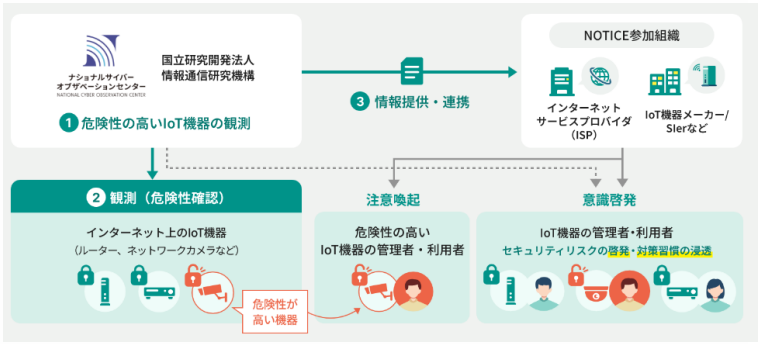
リスクが放置された（気づかない）状態で利用している危険性あり

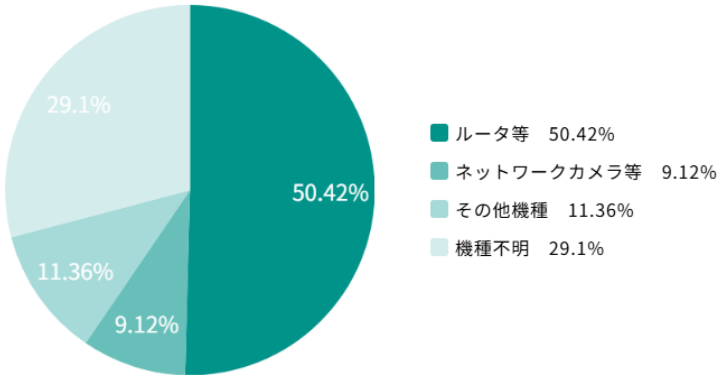
- **想定しないつながり**が発生するリスク
  - 汎用のOSや通信インタフェース（標準プロトコル）を利用するようになった
  - 貧弱なアクセス制御／ログイン管理から変更しない
- **予想しない機能がデフォルトオン**になっているリスク
  - 他社製品やOSSをブラックボックス利用していることによるサプライチェーンリスク
  - セキュア・バイ・デザインが徹底されていない
- **管理されていない**モノでもつながるリスク
  - 機器の管理担当者がいない／はっきりしない
  - 脆弱性に対して修正パッチの適用困難＆そもそも修正パッチが作られない
- 問題が発生しても**ユーザに分かりにくい**リスク
  - 物理的な異常以外は、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付かない
  - 画面がないことによって異常・警告通知の手段が制約される

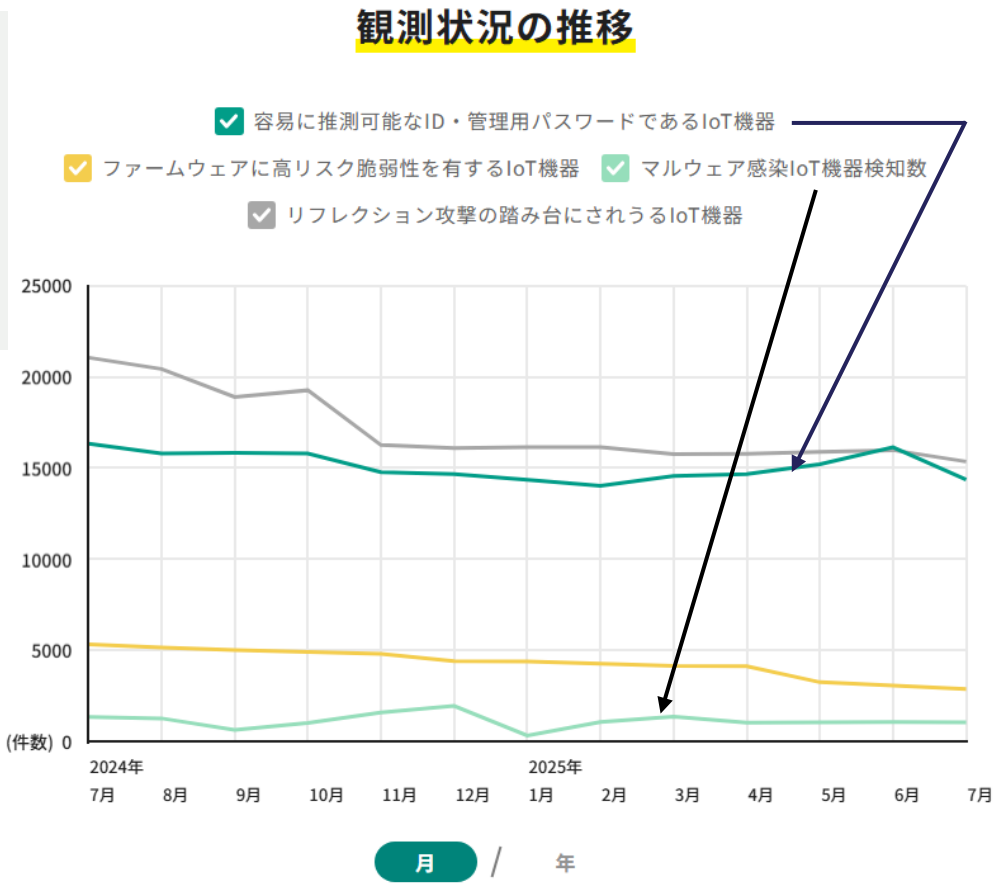
NOTICEプロジェクトを知っていますか？

- 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

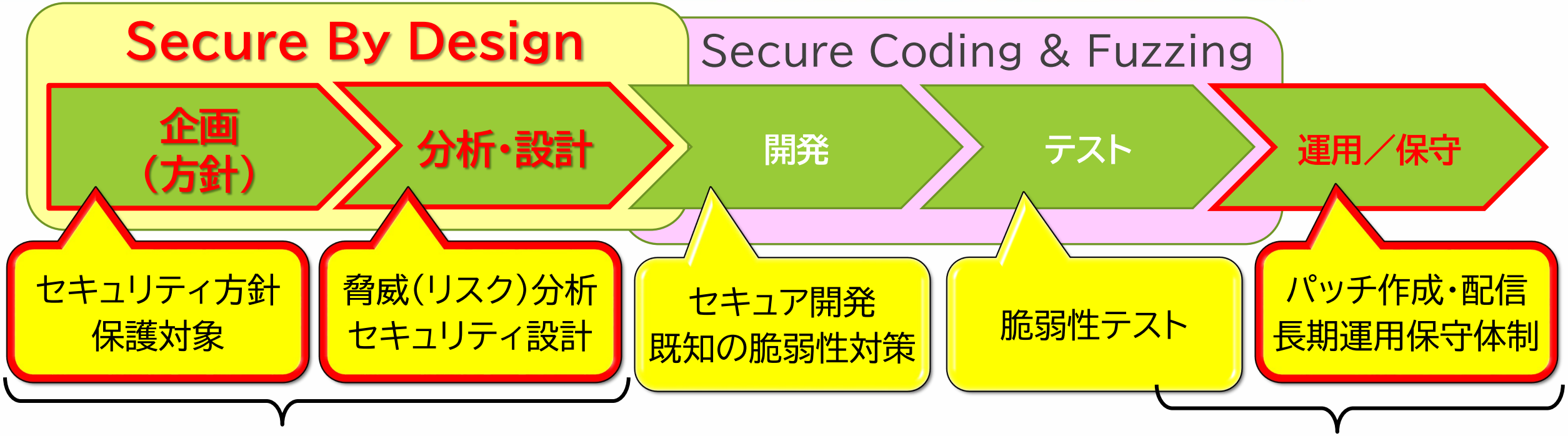
［出典］NICT、NOTICEプロジェクト（https://notice.go.jp/）







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

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)

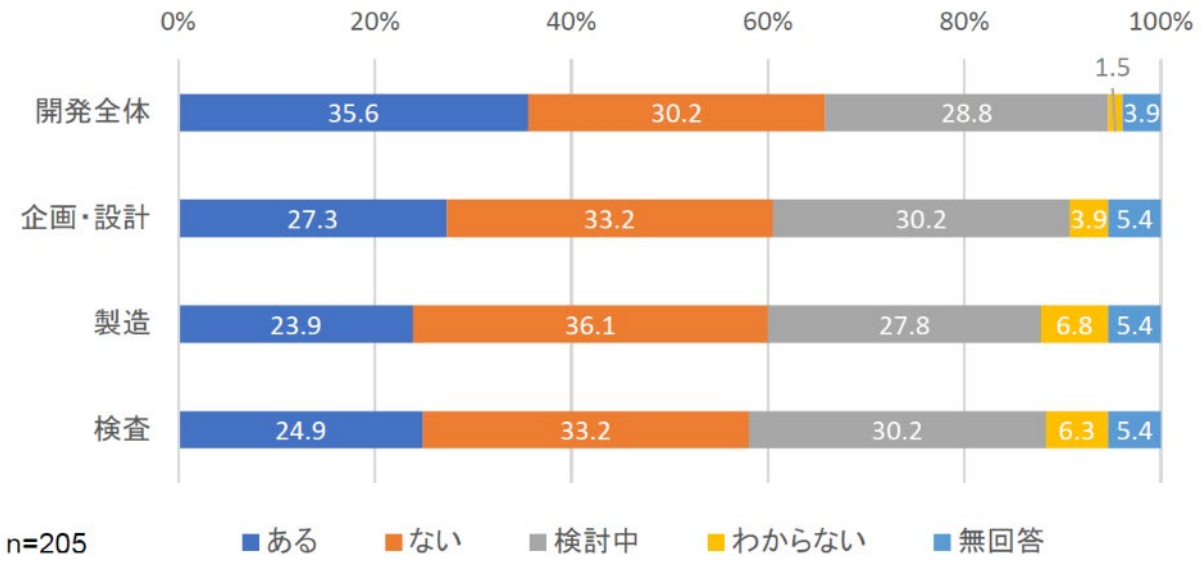


図 3.33 開発段階のセキュリティ方針・基準

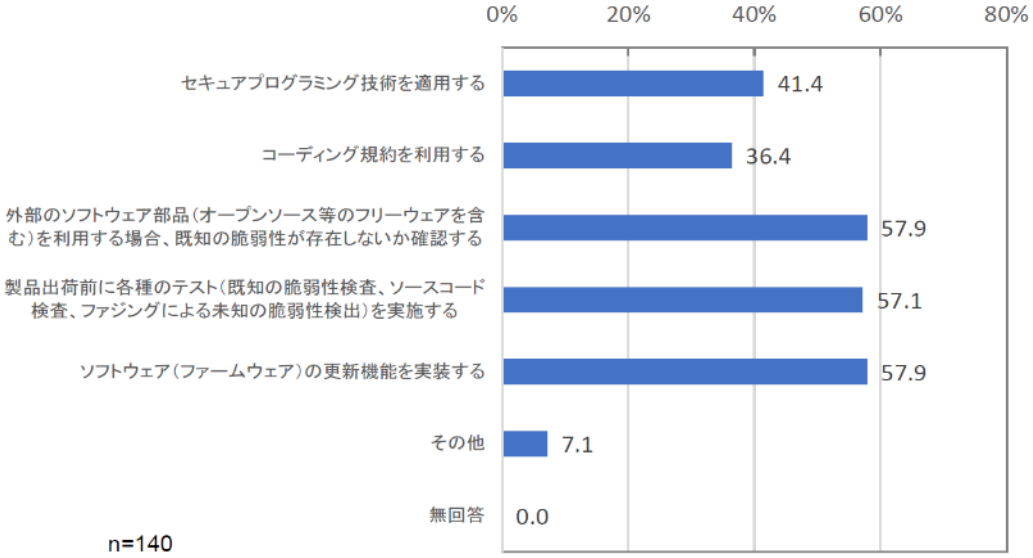


図 3.37 開発段階の脆弱性対策の考慮内容

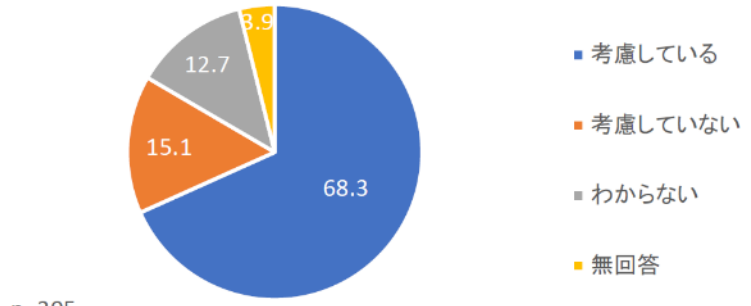


図 3.36 開発段階の脆弱性対策の考慮

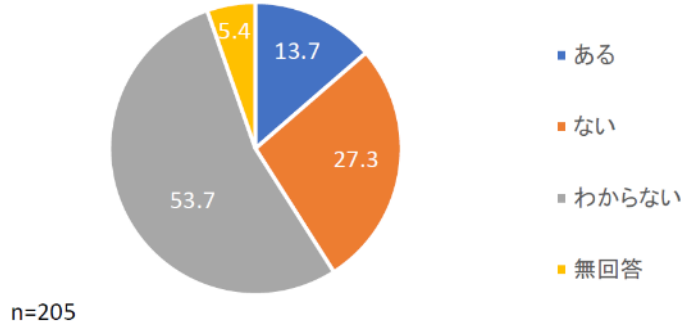


図 3.47 脆弱性対策が不可能な場合

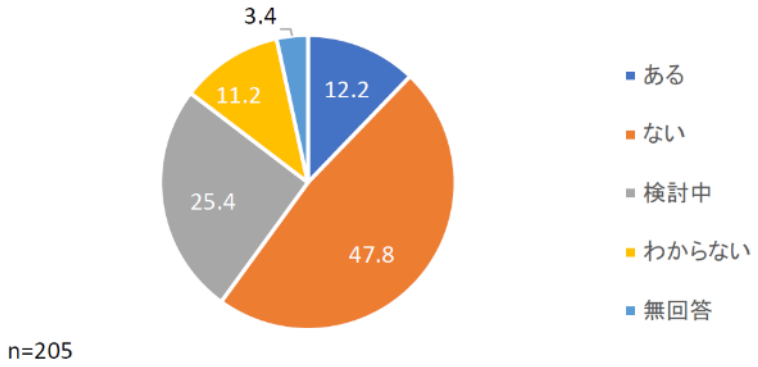


図 3.50 サポート終了後の脆弱性対応方針

「セキュリティ対策してくれる」と期待してよいか？

■ 総務省：令和5年度無線LAN利用者実態調査 [URL] https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

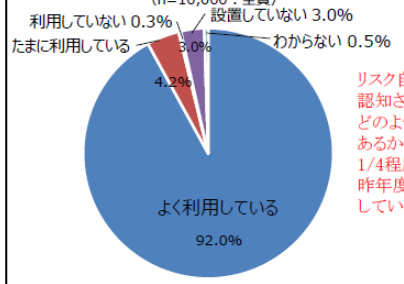
無線LAN利用者実態調査①

1

➢ 無線LANに対するセキュリティ意識等を把握するための調査をWebアンケートにより実施。
期間：2024.3.5-3.8 調査数：1,422（うち無線LAN利用者1,000をスクリーニング（性別・年代・エリアを偏りがないように割り付け））

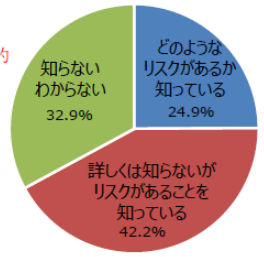
自宅に設置する無線LAN（その１）

自宅無線LANの利用有無
（n=10,000：全員）

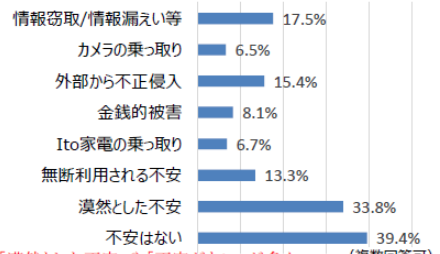


リスク自体は比較的認知されている。どのようなリスクがあるかを知る人は1/4程度であるが、昨年度より増加している。

無線LAN利用時におけるセキュリティ上のリスク認知
（n=10,000：全員）



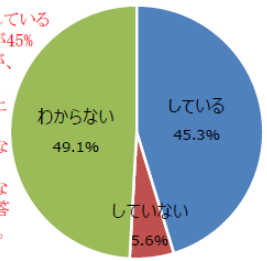
自宅無線LANでのセキュリティ上の不安
（n=961：自宅無線LANの利用者）



「漠然とした不安」や「不安がない」が多く、具体的なリスクを把握している利用者が少ない。

自宅無線LANの暗号化
（n=961：自宅無線LANの利用者）

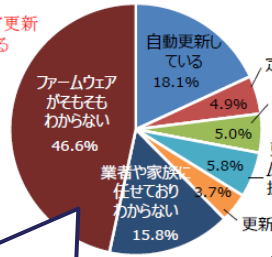
暗号化している利用者が45%程度だが、一方で半分以上が「わからない」、「していない」と回答している。



自宅無線LANのファームウェア更新
（n=961：自宅無線LANの利用者）

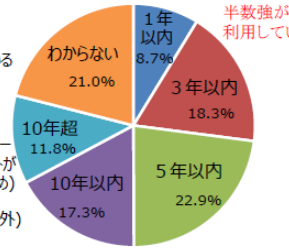
ファームウェア更新を実施している利用者は4分の1程度である。

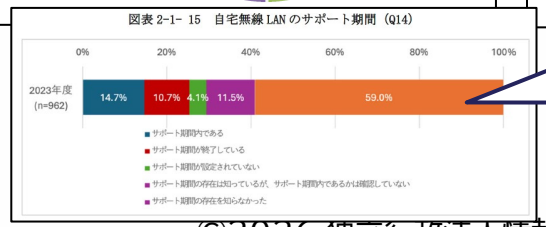
6割強が存在を把握していない



自宅無線LANの購入時期
（n=961：自宅無線LANの利用者）

半数強が3年以上利用している。





アップデートしてといってもファームウェアそのものがわからない

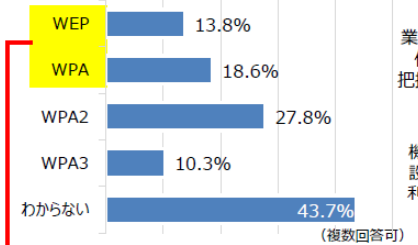
サポート期間の存在を知らなかった

無線LAN利用者実態調査②

2

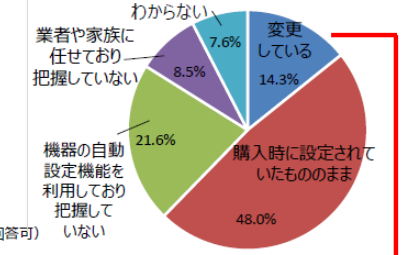
自宅に設置する無線LAN（その２）

自宅無線LANのセキュリティ方式
（n=435：自宅無線LANを暗号化している利用者）



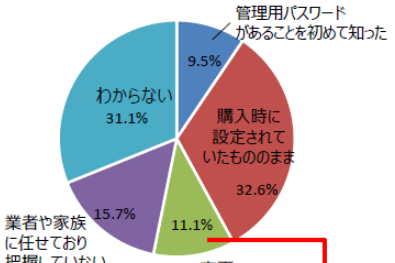
WEPやWPAを利用する人が3割おり方式を把握していない人も半数近く存在。昨年よりWPAが若干減り、WPA3が増えている。

自宅無線LANの暗号化パスワード
（n=435：自宅無線LANを暗号化している利用者）



購入時設定のまま利用している人が多数であり、自ら変更している人は15%程度である。

自宅無線LANの管理用パスワード
（n=961：自宅での無線LAN利用者）

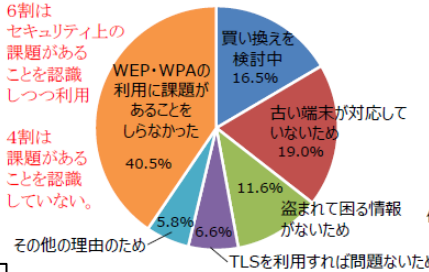


購入時設定のまま利用している人が多数
1割は管理用パスワードの認識がない。

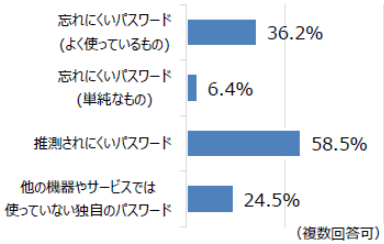
WEP・WPAを利用する理由
（n=121：自宅無線LANでWEP・WPAを用いている利用者）

6割はセキュリティ上の課題があることを認識しつつ利用

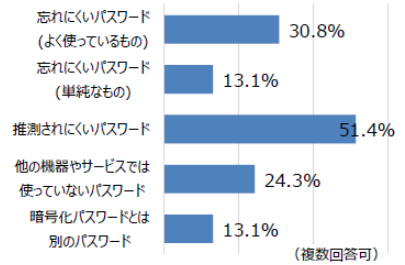
4割は課題があることを認識していない。



暗号化パスワード設定の留意点
（n=94：暗号化パスワードを変更している利用者）



管理用パスワード設定の留意点
（n=107：管理用パスワードを変更している利用者）



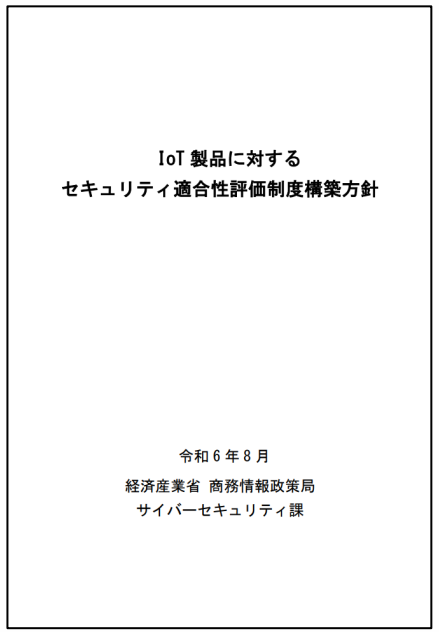
パスワードは変更せずに利用しているのが最多

JC-STARの目的

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

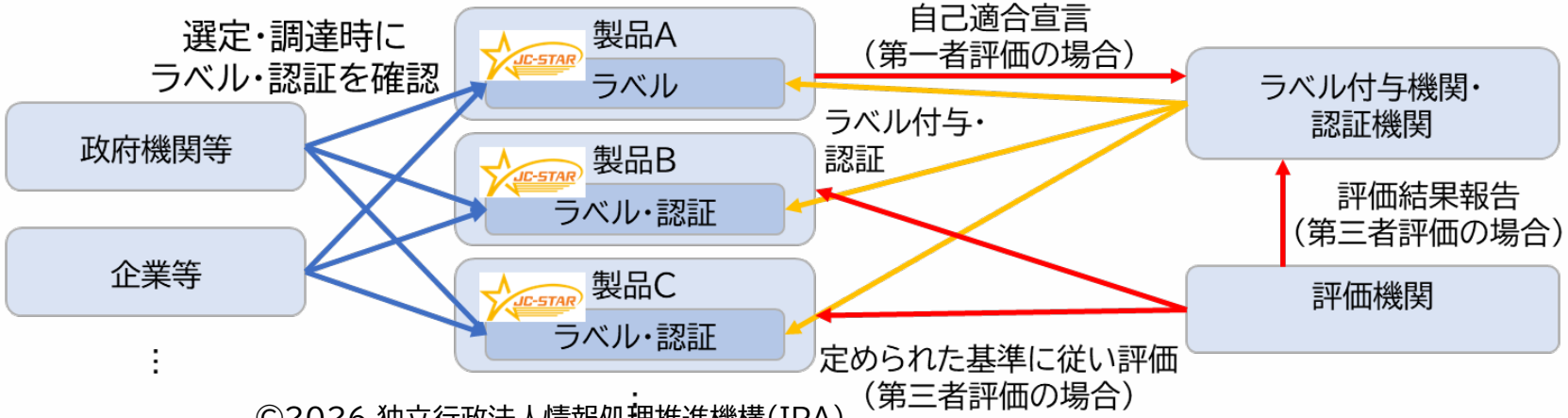
調達者・利用者に適合ラベルが付与されたIoT製品を購入・利用してもらうことで、セキュリティ対策の促進をつなげる


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

- 経済産業省の示す制度構築方針に従い、IPAが制度を構築・運営
- 経済産業省も一緒に制度拡張・普及や海外相互承認・連携等を推進

本制度を活用した製品調達のイメージ



アジェンダ

1. JC-STARがつくられた背景や目的

2. JC-STARの概要

3. JC-STARの今後に向けて

4. 参考：ビルディングオートメーションでの取扱いに向けて

適合ラベルの対象範囲

■ 購入時から安全なIoT製品を選ぶことが重要な範囲を想定

筐体がある（ソフトウェアやサービスではない）

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）

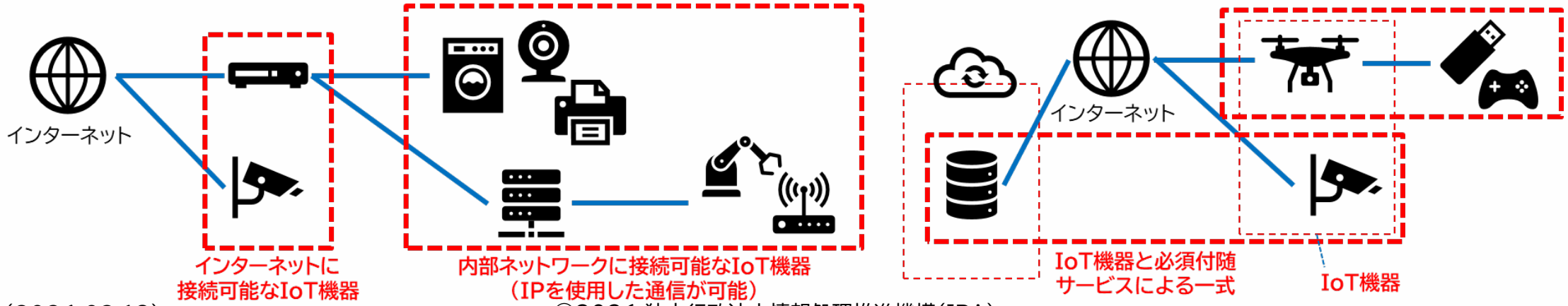
インターネット側からの通信を受信する可能性がある

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）

使えるセキュリティ機能は製品の製造ベンダが提供するものだけ

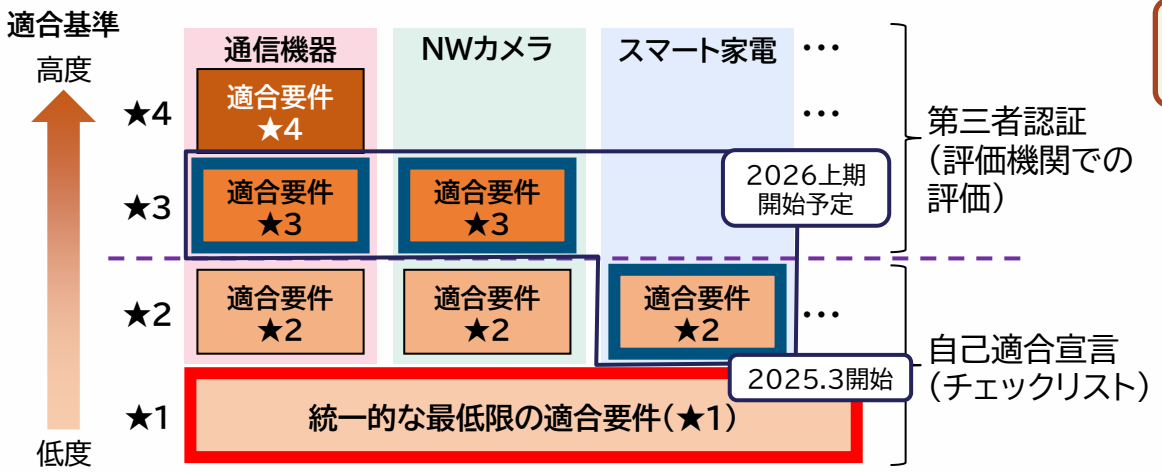
④ 購入時に具備されているセキュリティ機能を利用し、アップデート以外で後からセキュリティ機能を追加することが困難／できない



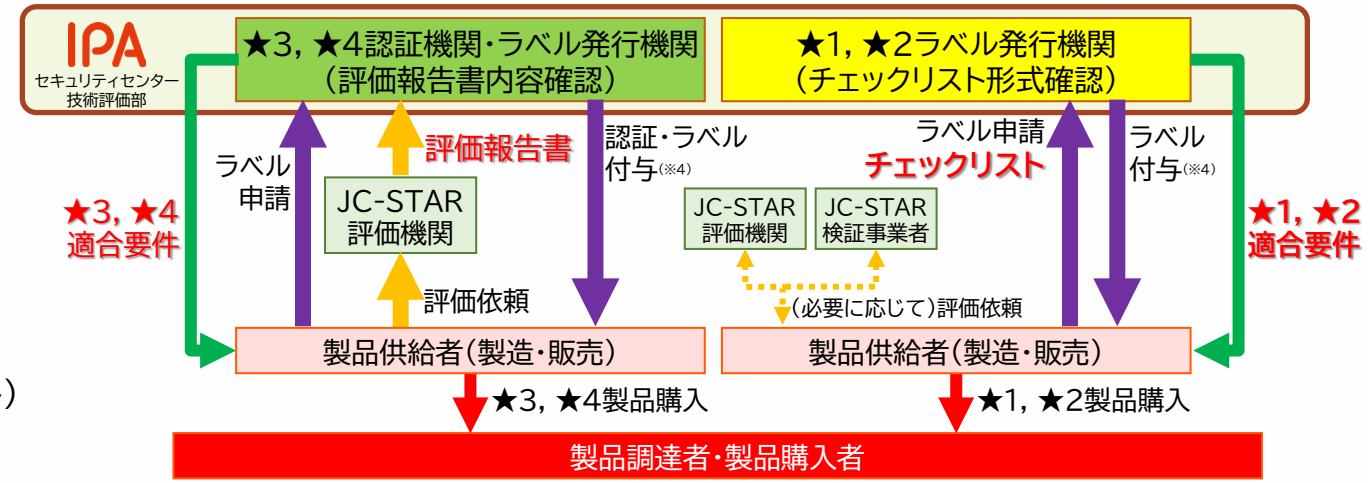
適合ラベルの適合要件

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

適合基準レベル（イメージ）



スキーム

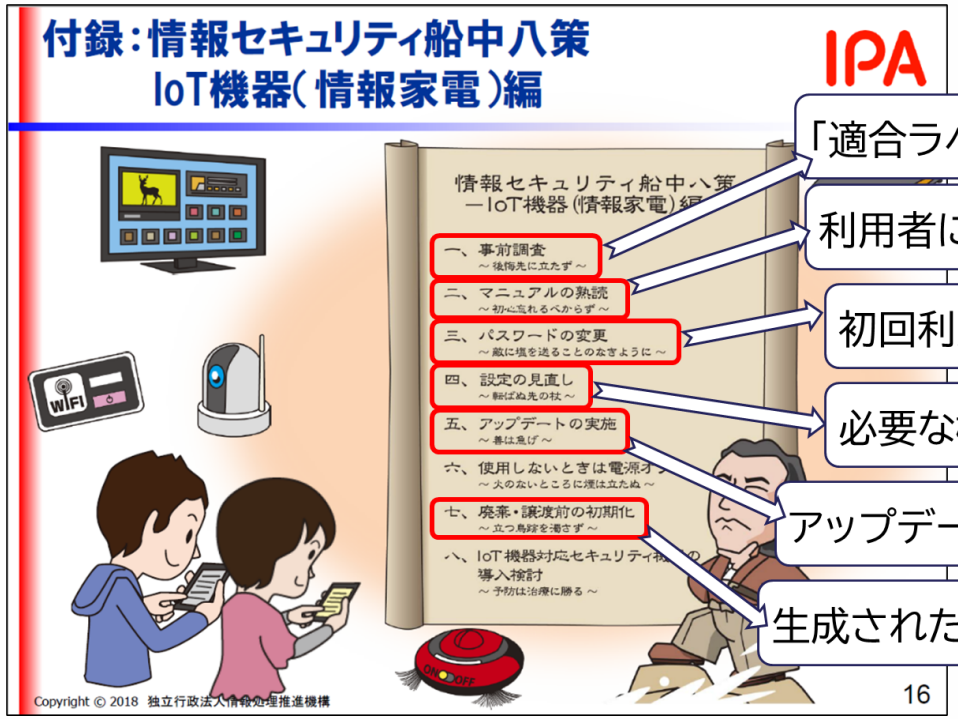


レベル	位置付け	適合基準	評価方式
★4 ★3	政府機関等や重要インフラ事業者、地方自治体、大企業の重要なシステムでの利用を想定した製品類型ごとに★1、★2に追加して汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの	製品類型別	第三者認証
★2	製品類型ごとの特徴を考慮し、★1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの	製品類型別	自己適合宣言
★1	製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの	製品類型共通	自己適合宣言

JC-STARにおける「★1」で目指していること

★1の適合要件への適合により、**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要件
  - 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
  - ② インターネット側からの遠隔攻撃を想定し、**スクリプトキディレベルの攻撃に対して実用的な耐性**を保持
  - ③ 脆弱性に対するサポート方針を明確化し、適合ラベル有効期間内の**サポートを確実に提供**
  - ④ 廃棄前に、運用中に**生成されたデータを適切に削除**可能



「適合ラベル取得製品情報ページ」に必要な情報が掲載

利用者に注意喚起させる情報は必ずマニュアル等に記載

初回利用時に強制的にパスワード変更を要求

必要な機能のみ「デフォルトオン」設定し、安全性を確認

アップデートサポートの提供義務化と自動的／容易なアップデートを実現

生成されたユーザデータの消去機能の搭載義務化

★1のセキュリティ要件・適合要件

★1で考慮する主な脅威			脅威に対抗するために★1で求めるセキュリティ要件			
			IoT製品に対する適合要件		IoT製品ベンダーに対する適合要件	
			対策種別	適合要件の概要	対策種別	適合要件の概要
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]	―	―

※「適合要件の概要」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要件もあるが、代表的なものにマッピングしている。

★1適合ラベル

3月25日★1受付開始。5月21日★1適合ラベル第1陣発行(11社26申請)
2月26日時点で適合ラベル発行数65社158申請(製品型番数1,000超)

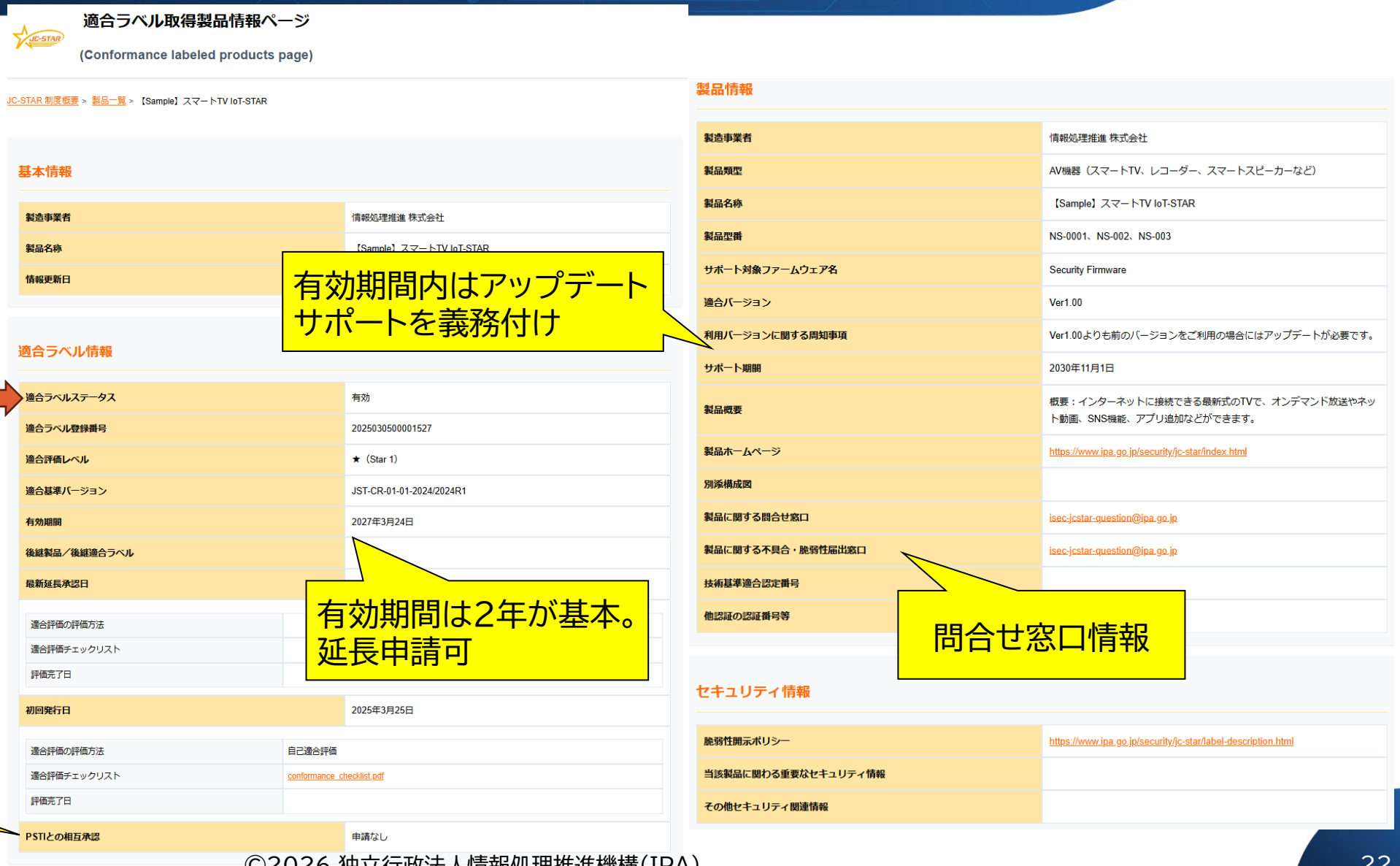
- 適合ラベルは定められた**適合要件への適合**を示す目印として付与
  - IoT製品が予め具備するセキュリティ機能として満たしてほしい水準にあることを確認できる
  - 完全・完璧なセキュリティが確保されていることを保証するものではない
  - 情報提供ページで「適合ラベルのステータス表示」と「セキュリティ情報・問合せ先の一元表示」を実現
  - ★1、★2では適合要件に適合しているかどうかをIPAは確認しない(評価の信頼性はベンダーの信頼性に依存)

- 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
  - 証跡の保管義務をIoT製品ベンダに課す
  - 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

適合ラベル取得製品情報ページ

JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
JC-STAR
Registered ID: 2025030500001527
Information-technology Promotion Agency, Japan (IPA)

- 有効(Active)
- 失効猶予(延長申請中(Extension procedure in progress))
- 失効(有効期限切れ(Expired))
- 失効(自主取下げ(Withdrawn))
- 取消し(Revoked)



適合ラベル取得製品情報ページ
(Conformance labeled products page)

JC-STAR 制度概要 > 製品一覧 > 【Sample】スマートTV IoT-STAR

基本情報

製造事業者	情報処理推進 株式会社
製品名称	【Sample】スマートTV IoT-STAR
情報更新日	

適合ラベル情報

適合ラベルステータス	有効
適合ラベル登録番号	2025030500001527
適合評価レベル	★（Star 1）
適合基準バージョン	JST-CR-01-01-2024/2024R1
有効期間	2027年3月24日
後継製品／後継適合ラベル	
最新延長承認日	
適合評価の評価方法	
適合評価チェックリスト	
評価完了日	
初回発行日	2025年3月25日
適合評価の評価方法	自己適合評価
適合評価チェックリスト	conformance_checklist.pdf
評価完了日	
PSTIとの相互承認	申請なし

製品情報

製造事業者	情報処理推進 株式会社
製品類型	AV機器（スマートTV、レコーダー、スマートスピーカーなど）
製品名称	【Sample】スマートTV IoT-STAR
製品型番	NS-0001、NS-002、NS-003
サポート対象ファームウェア名	Security Firmware
適合バージョン	Ver1.00
利用バージョンに関する周知事項	Ver1.00よりも前のバージョンをご利用の場合にはアップデートが必要です。
サポート期間	2030年11月1日
製品概要	概要：インターネットに接続できる最新式のTVで、オンデマンド放送やネット動画、SNS機能、アプリ追加などができます。
製品ホームページ	https://www.ipa.go.jp/security/jc-star/index.html
別添構成図	
製品に関する問合せ窓口	isec-jcstar-question@ipa.go.jp
製品に関する不具合・脆弱性届出窓口	isec-jcstar-question@ipa.go.jp
技術基準適合認定番号	
他認証の認証番号等	

セキュリティ情報

脆弱性開示ポリシー	https://www.ipa.go.jp/security/jc-star/label-description.html
当該製品に関わる重要なセキュリティ情報	
その他セキュリティ関連情報	

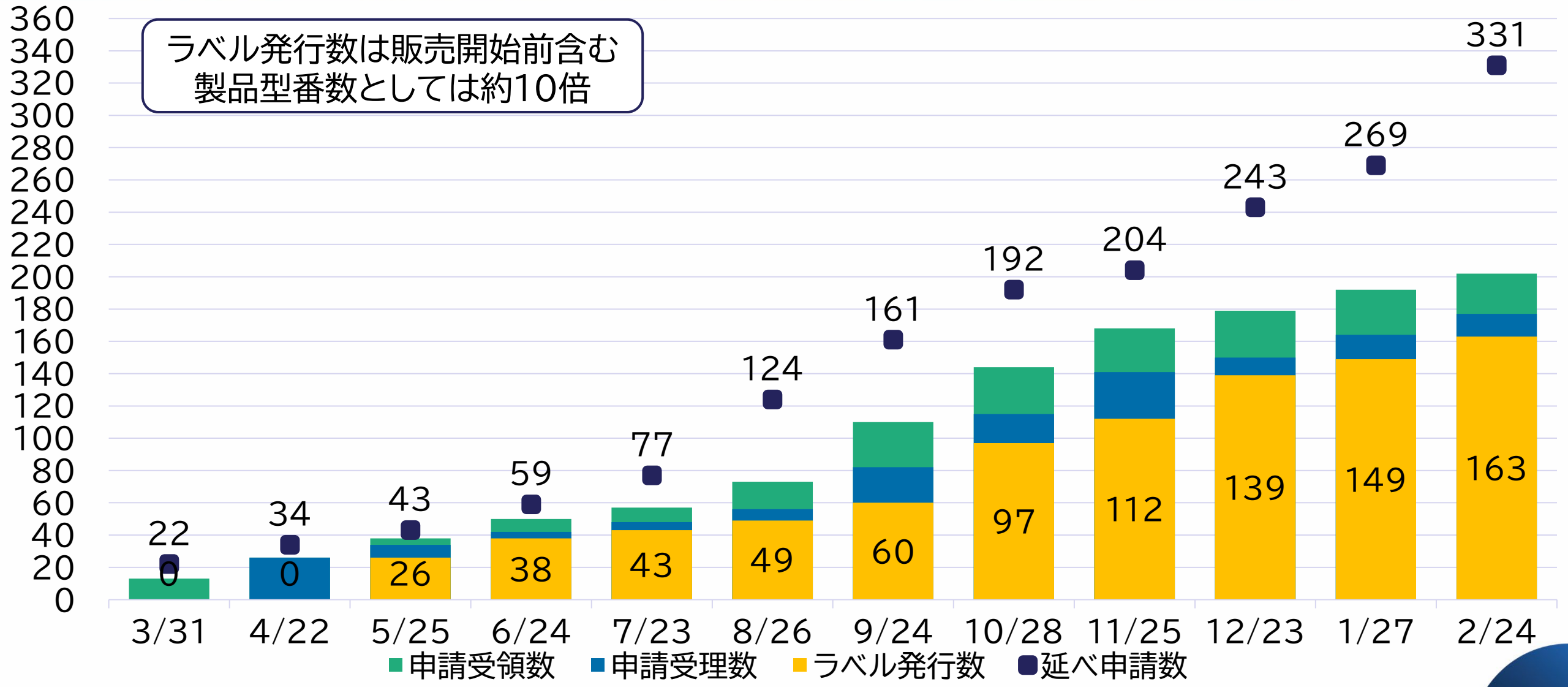
有効期間内はアップデートサポートを義務付け

有効期間は2年が基本。延長申請可

問合せ窓口情報

PSTI法適合確認欄

申請実績推移



アジェンダ

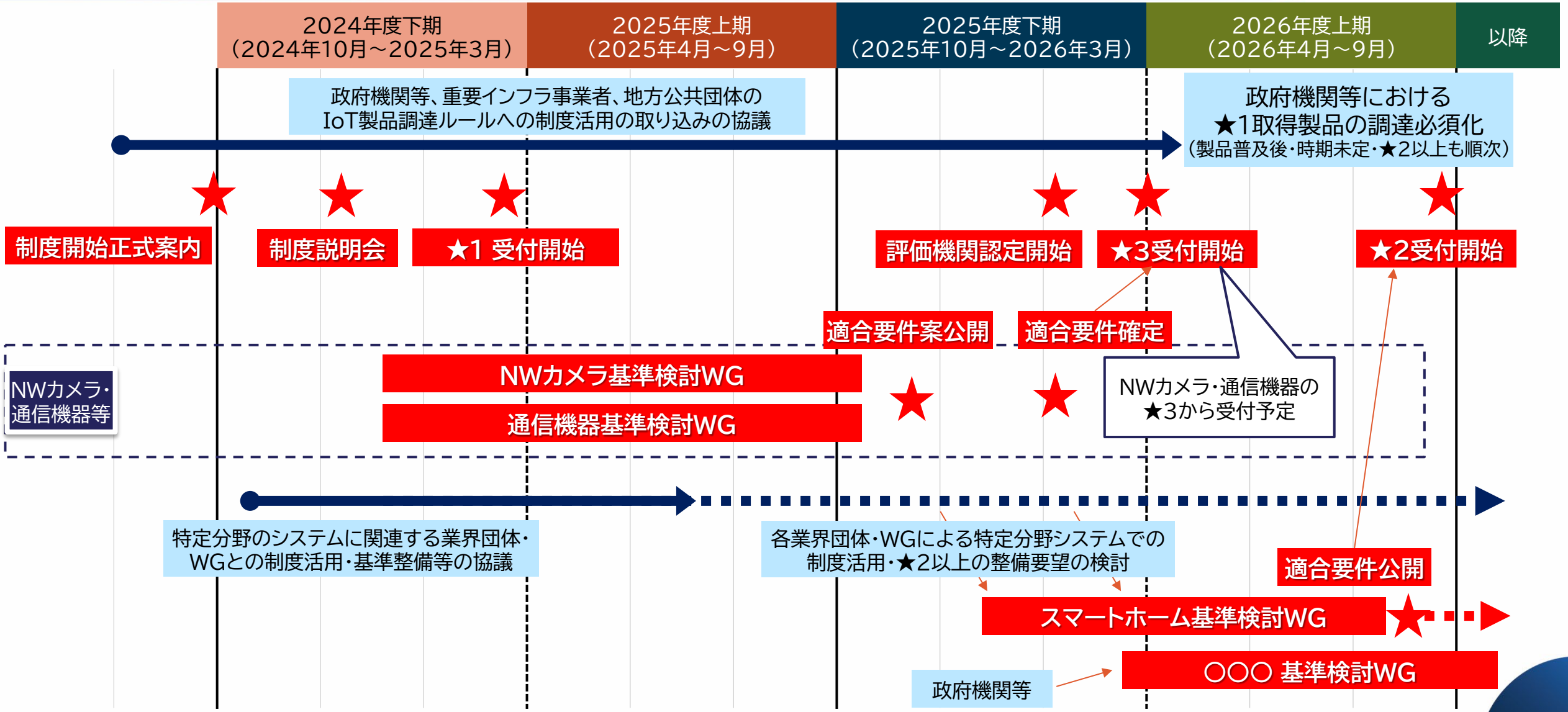
1. JC-STARがつくられた背景や目的

2. JC-STARの概要

3. JC-STARの今後に向けて

4. 参考：ビルディングオートメーションでの取扱いに向けて

今後のスケジュール予定



JC-STARの今後に向けて

① 政府機関、重要インフラ事業者、地方公共団体等での調達要件に適合ラベル付与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（9月5日改定！）
- 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（令和7年3月版）
- エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドラインVer3.0

ガイドライン（令和７年度版）一部改定の主なポイント

国家サイバー統括室 National Cybersecurity Office

- 直近に発生した重大インシデントからの教訓・対策や最近の技術動向等を反映し、必要な改定を行うもの。

ポイント	内容
1．セキュリティ要件適合評価及びラベリング制度（JC-STAR）の運用開始	➢ JC-STARの運用開始に伴う、JC-STARの機器等の選定基準への反映
2．情報セキュリティサービス審査登録制度の新たなサービスの開始	➢ 情報セキュリティサービス審査登録制度のペネトレーションテスト（侵入試験）サービスが開始
3．キッティングイメージの厳格な管理	➢ 端末キッティングイメージ（端末をユーザがすぐに使える状態にするドライブイメージのこと。）を最新に保ち、盗難・紛失がないよう厳格に管理
4．多要素主体認証（２つ以上の認証方式（例えば、指紋認証とパスワード認証）を用いた認証）の導入促進	➢ 厳格な主体認証が必要な場合以外にも、多要素主体認証方式等の導入を前提に検討し、導入を促進
5．ドメインネームシステム（DNS）の対策	➢ DNSの対策（ドメイン乗っ取り攻撃対策）の記載見直し

1

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

4.3.1(1)-2 統括情報セキュリティ責任者は、機器等の選定基準に、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**を含めること。また、IoT 機器等については、対象機器の「**セキュリティ要件適合評価及びラベリング制度（JC-STAR）**」の登録状況と以下の観点を踏まえて、当該制度を選定基準に含めること。

a) 「重要度：低」に分類された情報システムの IoT 機器等については、★１（レベル１）ラベルを取得した製品群からの選定等、**当該制度の★１ラベル取得に求められるセキュリティ適合基準**の機能が実装された機器等とすること。

b) 「重要度：中～高」に分類された情報システムの IoT 機器等については、★１ラベル以上を取得した製品群から選定するなどして、**当該制度の★１ラベル取得に求められるセキュリティ適合基準**に加えて、情報システムの重要度に即したより高度なセキュリティ機能が実装された機器等とすること。

「★3」適合要件

カテゴリ	★3	
	★1	追加
1.脆弱な認証・認可メカニズム(例: 汎用のデフォルトパスワード、脆弱なパスワード)を使用しない	✓ 実機テスト	✓ 実機テスト
2. 脆弱性の報告を管理するための手段を導入する	✓	✓
3. ソフトウェアを最新の状態に保つ	✓ 実機テスト	✓ 実機テスト SBOM
4. 機密セキュリティパラメータをセキュアに保存する	✓	✓
5. セキュアに通信する	✓	✓ 実機テスト
6. 露出した攻撃面を最小化する	✓ 実機テスト	✓ 実機テスト
7. ソフトウェアの完全性を確実にする		✓
8. 個人データがセキュアであることを確実にする		✓

カテゴリ	★3	
	★1	追加
9. 停止に対してレジリエントなシステムにする	✓ 実機テスト	✓ 実機テスト
10. システムのテレメトリデータを検証・保護する		✓ 実機テスト
11. ユーザが簡単にデータを消去できるようにする	✓ 実機テスト	
12. 製品の設置及びメンテナンスを容易にする		✓ 実機テスト
13. 入力データの妥当性を確認する		✓ 実機テスト
14. 個人データを適切に処理する		✓ 実機テスト
16. 脅威を特定しテストする		✓ ペネトレーションテスト
17. 製品に関する情報提供を行う	✓	✓
19. 製品の可用性を確実にする		✓ 実機テスト
21. ハードウェアの完全性を確実にする		✓

JC-STARの今後に向けて

② 業界標準としてIoT製品ベンダと調達者・利用者が協力して適合ラベル付与製品の製造・販売と選定・調達する分野を確保

- 情報機器販売時のガイドライン(JCSSA)にて、「販売店がIoT機器を販売する場合は、JC-Star制度を活用することの考慮を推奨」

(出典) https://www.jcssa.or.jp/wp-content/uploads/2025/05/guideline_ver1.1.pdf

賛同団体名称	主なIoT製品類型	会員数
情報通信ネットワーク産業協会(CIAJ)	情報通信関連機器	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)
デジタルライフ推進協会(DLPA)	ネットワーク機器(主に消費者向け)	会員数:12社(2024年9月現在) (正会員7社、賛助会員5社)
電子情報技術産業協会(JEITA)	スマートホーム関連機器、ヘルスケア関連機器	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)
日本自動販売システム機械工業会(JVMA)	自動販売機、券売機、自動精算機、ATM、入出金機、出納機、両替機、キャッシュレス決済端末他	会員数:89社(2025年9月現在) (正会員 52社、賛助会員 37社)
日本防犯設備協会(SSAJ)	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	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)
ビジネス機械・情報システム産業協会(JBMIA)	プリンター・複合機、データプロジェクター、その他事務機	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)

BMSecはJC-STARに制度移行

「スマートホーム分野」の「★2」適合要件の作成開始

JC-STARの今後に向けて

③ 諸外国制度との相互承認を図ることで、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

- 日英両国間で「JC-STARと英国PSTI法の相互承認に関する協力覚書」に署名（11.06）
- グローバル・サイバーセキュリティ・ラベリング・イニシアティブ（GCLI）共同声明を発表（10.23）

国・地域	英国	多国間	米国	EU	シンガポール
制度名	Product Security & Telecom. Infrastructure Act（PSTI法）	Global Cybersecurity Labeling Initiative（GCLI）	U.S. Cyber Trust Mark	Cyber Resilience Act（CRA法）	Cybersecurity Labelling Scheme（CLS）
マーク	ステッカーのみ		U.S. CYBER TRUST MARK	CE	CYBERSECURITY LABEL CSA/IOTWABCD
相互承認	2026年1月1日開始		–	–	–
開始時期	2024年4月施行	2025年10月発足（11ヶ国参加）	2027年1月開始予定	• 報告義務: 2026年9月 • その他: 2027年12月	2020年10月開始
任意/義務	義務	–	任意	義務	任意
対象	消費者向けIoT製品 エンタープライズ向けも検討中	–	消費者用無線IoT製品	デジタル製品	消費者向けIoT機器
適合基準	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	IoT製品のサイバーセキュリティ・ラベリング制度の推進と国際協力を目的とした世界的な枠組み	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	• ＊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
評価方法	自己適合宣言	–	第三者認証	• クリティカル製品:第三者認証 • クラスⅠ・Ⅱの製品:第三者認証 • 上記以外の製品:自己適合宣言	• ＊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

JC-STARの今後に向けて

消費者にも必要性・有用性を伝えるためのプロモーション
～ そして、実際に購入してもらえるようにするために ～

アジェンダ

1. JC-STARがつくられた背景や目的

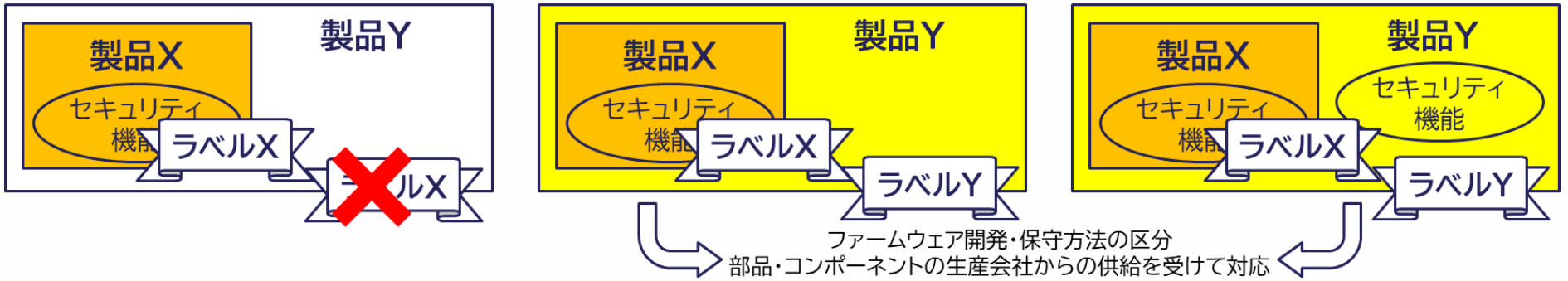
2. JC-STARの概要

3. JC-STARの今後に向けて

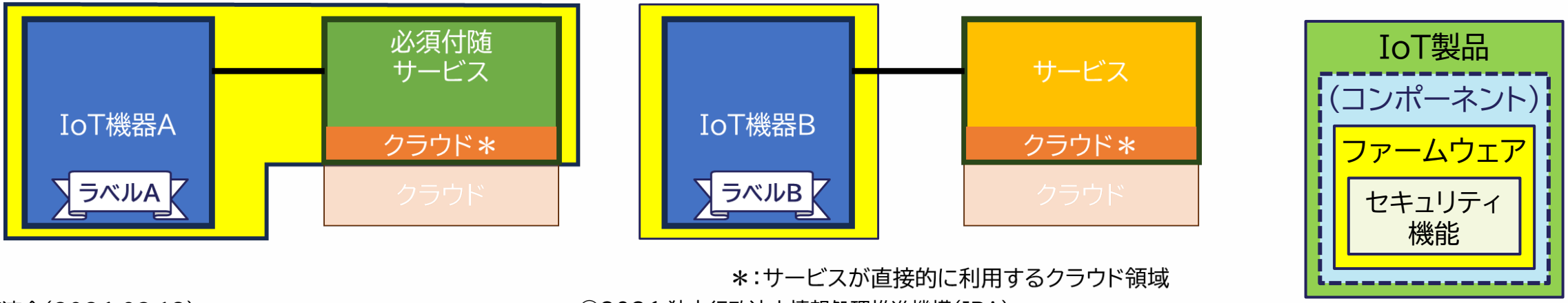
4. 参考：ビルディングオートメーションでの取扱いに向けて

適合ラベルの前提

- 「**製品ブランド名**」の保有会社が「**申請会社**」



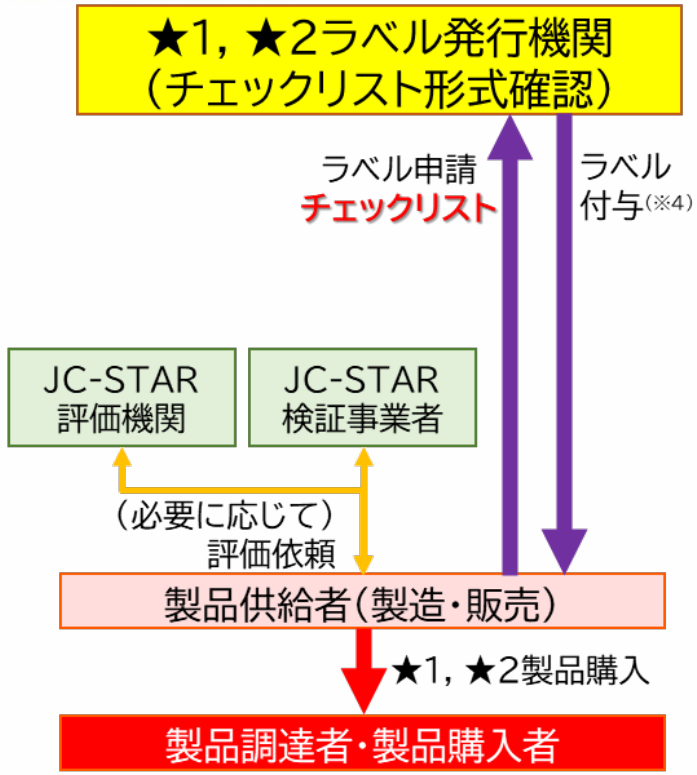
- 「**機器**」を含む「**製品型番**」で規定される「**製品**」に対して適合ラベルが交付
- 「適合要件を満たすために必要なセキュリティ機能を提供する**ファームウェア（コンポーネント）の保守**」が「**サポート対象＝申請会社の責務**」



＊：サービスが直接的に利用するクラウド領域

★1適合ラベルの申請方法

1. IoT製品ベンダ（事前準備）
   - ★1適合要件・評価手順に従って自ら評価を行い、**チェックリストを作成**
   - 必要に応じて、JC-STAR評価機関・検証事業者等に評価を依頼可
2. IoT製品ベンダ（申請）
   - 事前にJC-STAR申請担当にメールし、**申請番号を取得**
   - **申請書類一式とチェックリストを、取得した申請番号を本文に記載したメールに添付**して、IPAにラベル申請
   - チェックリストの提出に当たり、IPAへの証跡提出は不要
   - 適合ラベルの有効期間中は証跡の保管義務があることに留意
3. IPA 【確認作業が順調に進めば、申請後**最短ケースで2週間程度**を想定】
   - 申請書類一式とチェックリストについて、経済産業省とともに必要な確認作業を行ったうえで、内容に不備がなければラベル申請を受理
   - **申請内容によっては確認作業に時間がかかるケースもある**ので注意
4. IoT製品ベンダ
   - 申請が受理されたら、新規申請手数料（198,000円）をIPAに支払い
5. IPA 【支払確認後、おおむね2週間程度を想定】
   - そのIoT製品に対する適合ラベルを付与



- 申請書類形式確認
- チェックリスト形式確認
- 申請書内容（製造情報）確認

「適合ラベルの利用ガイダンス」に従って
プロモーションに利用可能

対象外としている「システム」としての扱い

- 現状では対象外としている複数「IoT機器」を組み合わせる「システム」をどうするか？

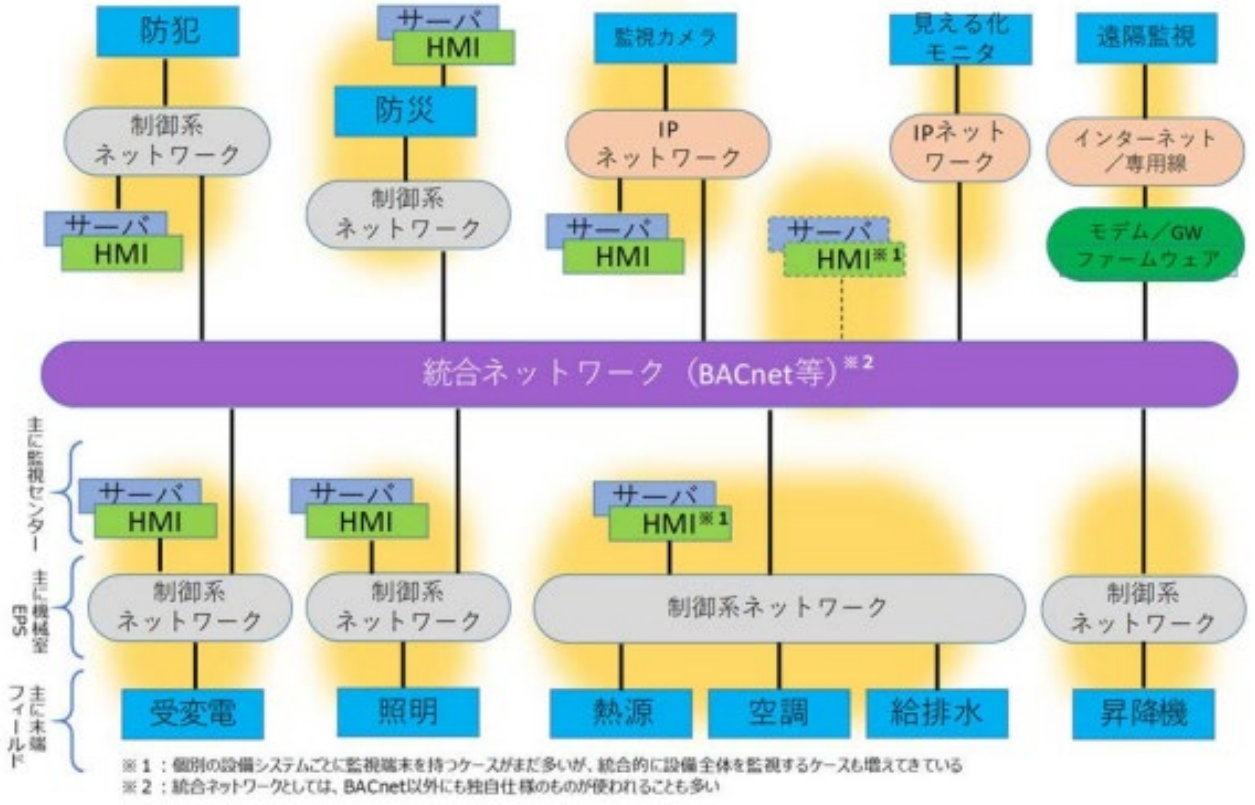


図 3-3 ビルシステムの標準的なモデル（全体像）

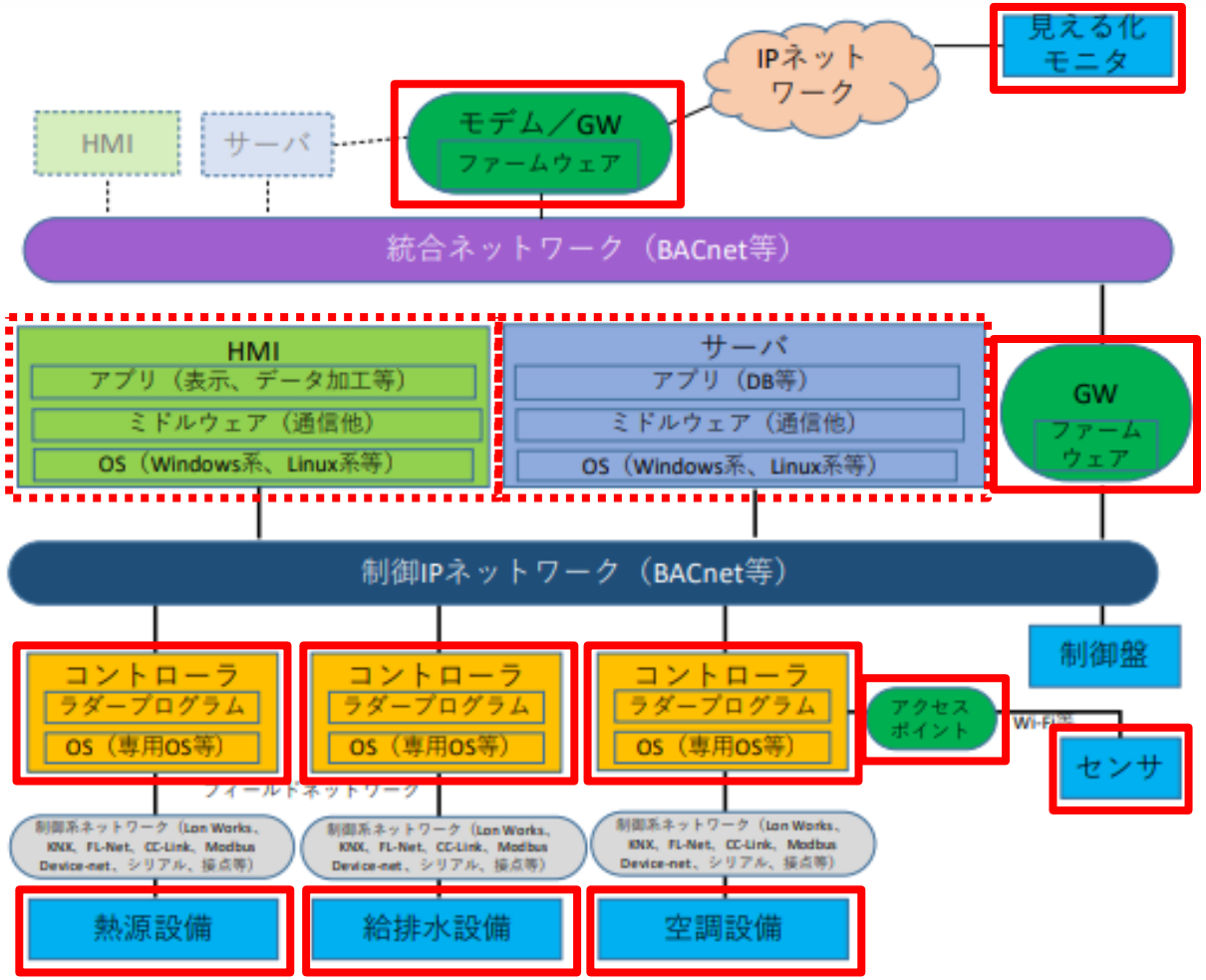


図 3-6 熱源・空調・給排水システムの標準的なモデル

【出典】 経済産業省、「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版」

詳しくは以下を参照ください

https://www.ipa.go.jp/security/jc-star/material.html