資料88-4

JC-STARの紹介と端末機器の技術基準等への適合性に係るセキュリティ基準の見直しについて

（独）情報処理推進機構
神田　雅透

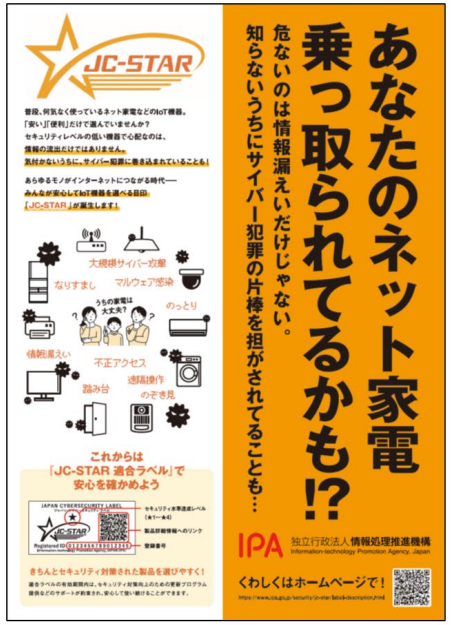
IPA Better Life with IT

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レベルを見える化するラベリング制度の運用開始！

～　きちんとセキュリティ対策されたIoT製品を選びやすく！　～

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



どのIoT製品のセキュリティ対策が適切か否か判断できない

適合ラベルを目印に製品購入することでセキュリティ向上

JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
Registered ID: 20250305000001527
Information-technology Promotion Agency, Japan (IPA)

適切なセキュリティ対策が講じられている製品を示す目印

セキュリティ対策の取組についてアピールすることが難しい

JC-STAR適合ラベル

取得した適合基準のレベルを表現

「適合ラベル取得製品情報ページ」へのリンク
登録番号ごとに用意

適合ラベル取得製品の登録番号

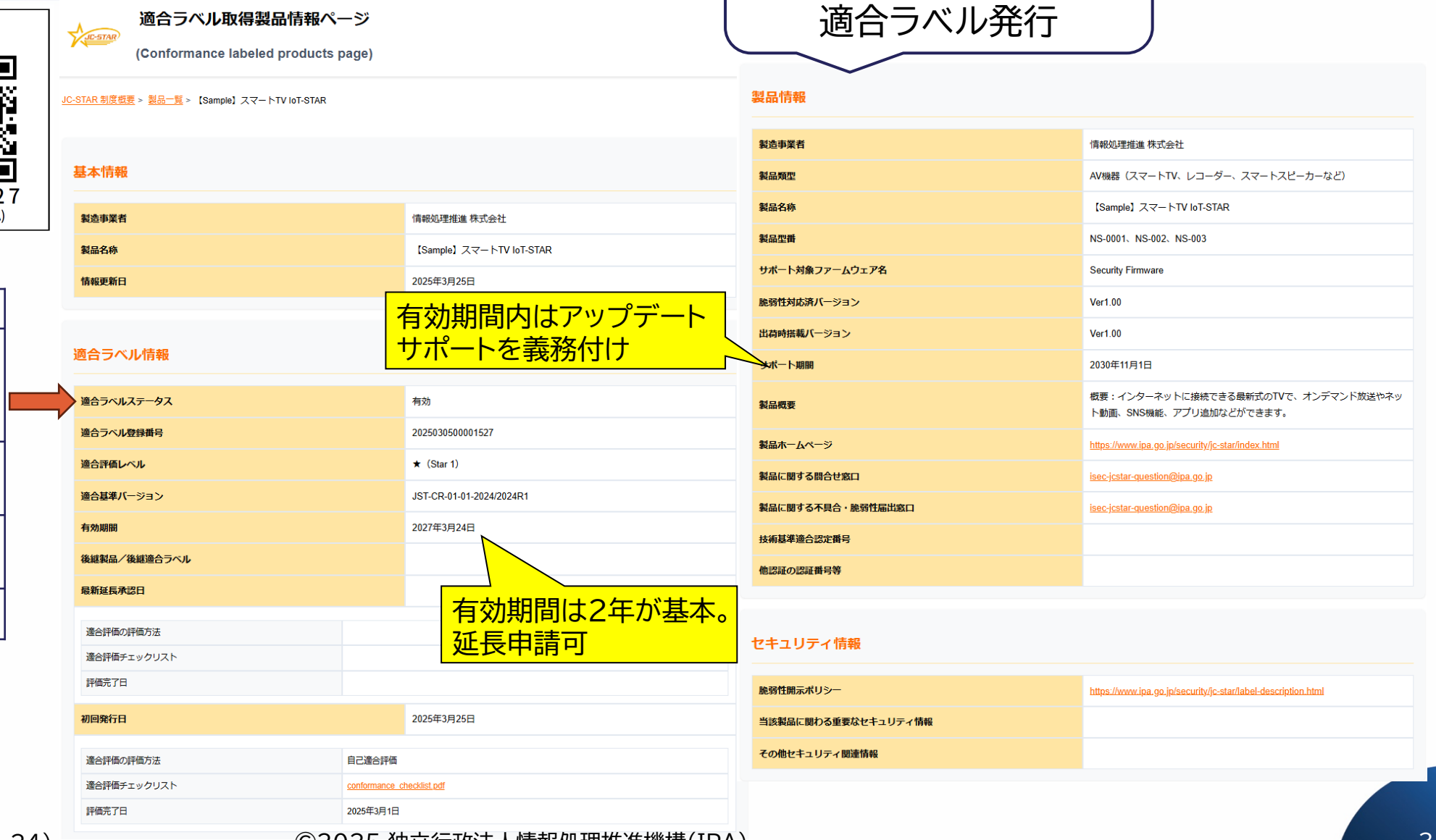
IPネットワーク設備委員会資料（25.06.24）

適合ラベル取得製品情報ページ

2025年5月21日時点で
11社26申請に対して
適合ラベル発行

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失効(自主取下げ(Withdrawn))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	2025年3月25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	2025年3月1日

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

製品情報

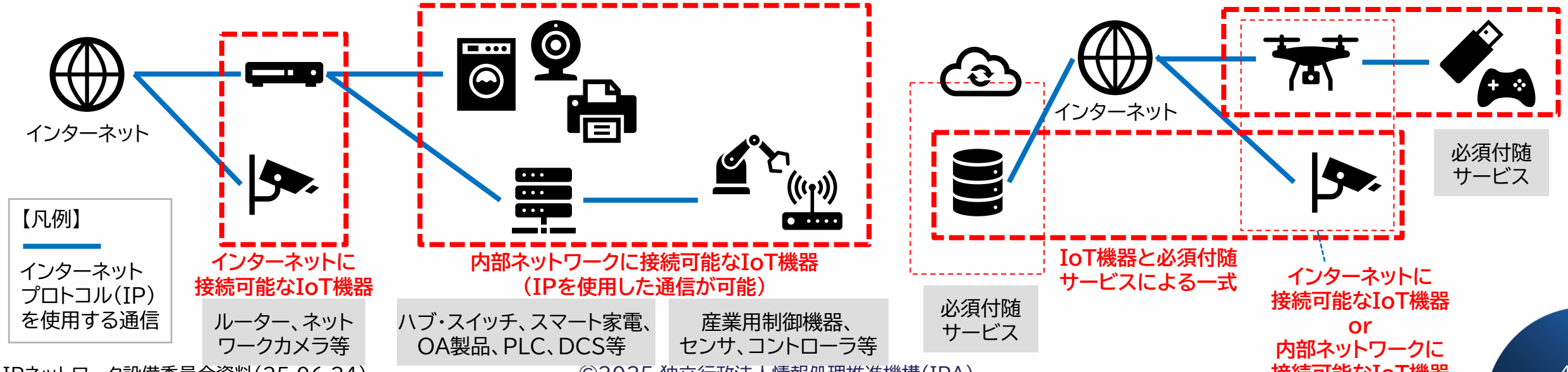
製造事業者	情報処理推進 株式会社
製品類型	AV機器（スマートTV、レコーダー、スマートスピーカーなど）
製品名称	【Sample】スマートTV IoT-STAR
製品型番	NS-0001、NS-002、NS-003
サポート対象ファームウェア名	Security Firmware
脆弱性対応済バージョン	Ver1.00
出荷時搭載バージョン	Ver1.00
サポート期間	2030年11月1日
製品概要	概要：インターネットに接続できる最新式のTVで、オンデマンド放送やネット動画、SNS機能、アプリ追加などができます。
製品ホームページ	https://www.ipa.go.jp/security/jc-star/index.html
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	

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**

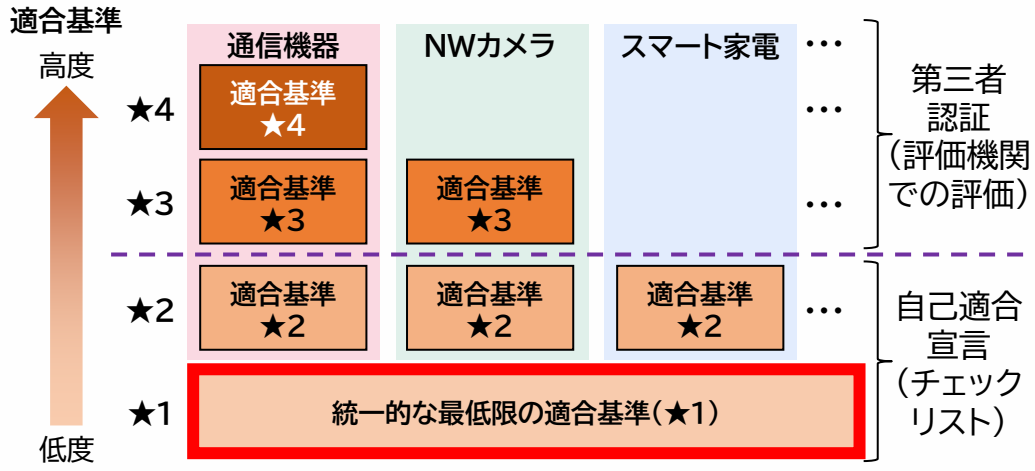


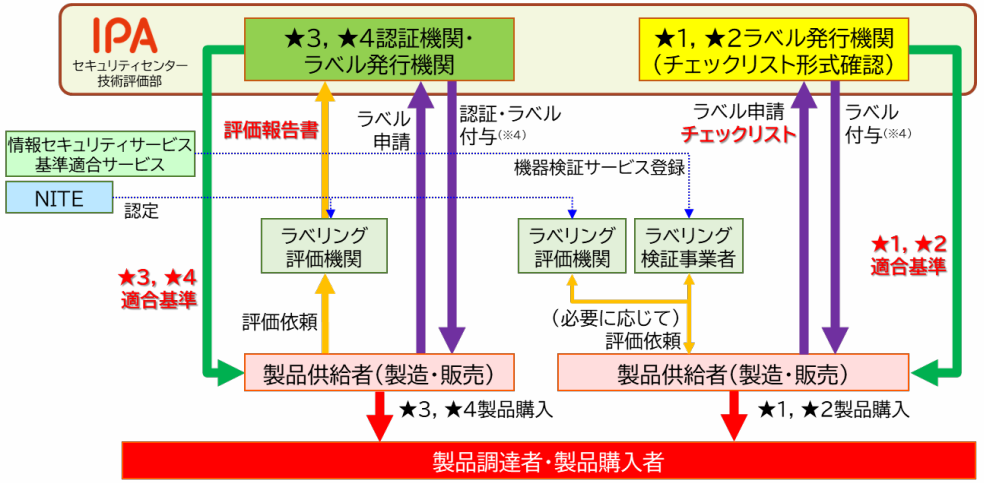
IPネットワーク設備委員会資料（25.06.24）

適合ラベルの適合基準

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		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	

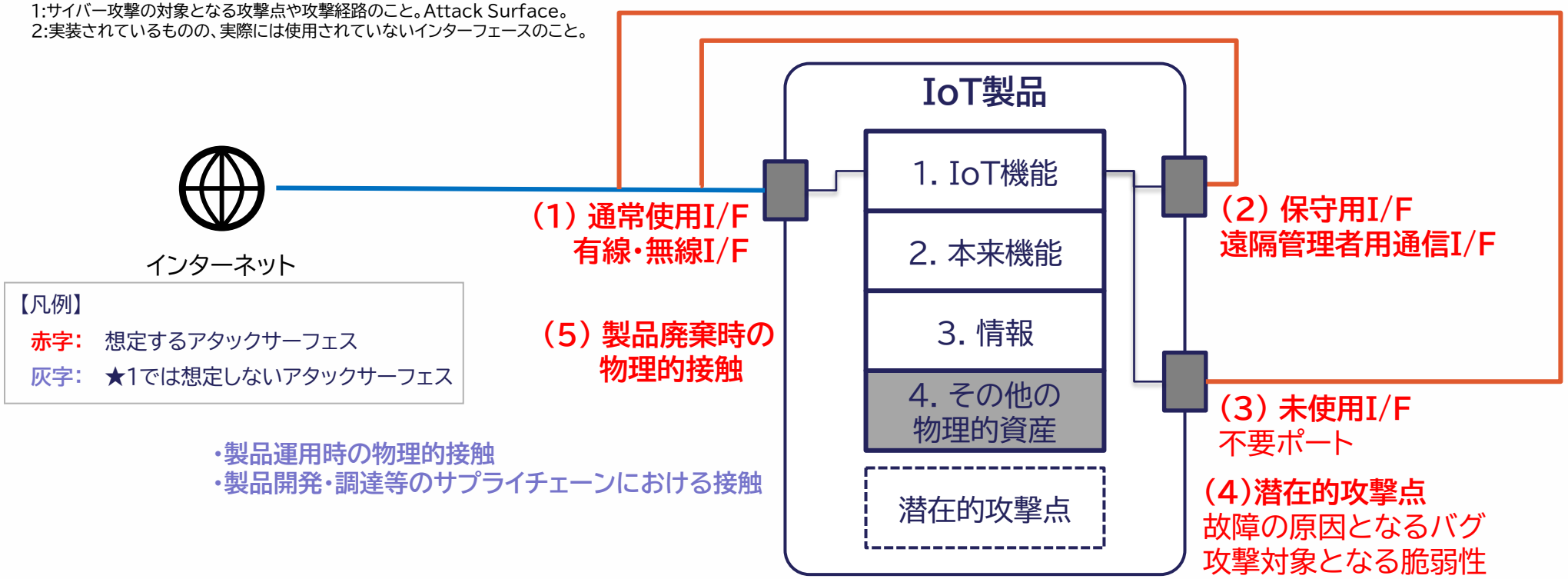
JC-STARにおける「★1」で目指していること

- ★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製品を対象とした統一的な基準とする
    - 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持たせる
    - 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
  - ✓ 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
  - ✓ ベンダ自身が実施した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
- ★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で想定するアタックサーフェス

- IPA文書及びCCDS文書を踏まえ、★1取得が想定される製品におけるアタックサーフェス[1]としては、「(1) 通常使用I/F」、「(2) 保守用I/F」、「(3) 未使用I/F[2]」、「(4) 潜在的攻撃点」、「(5) 製品廃棄時の物理的接触」の5つのアタックサーフェスを想定
  - ✓ ★1で対抗する脅威のレベルを踏まえ、「製品運用時の物理的接触」や「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は★1では想定しない

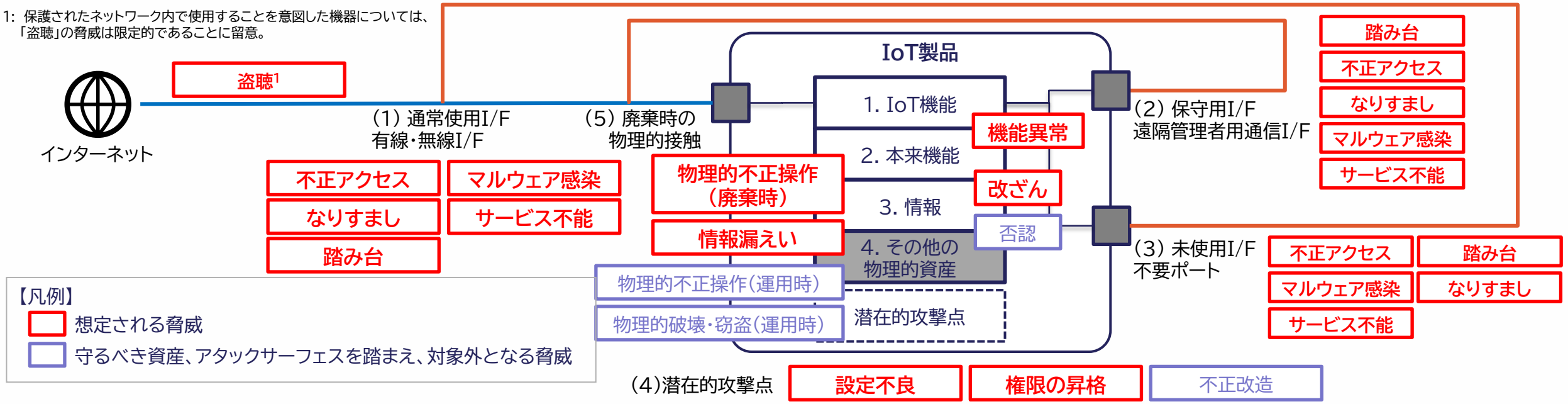
1:サイバー攻撃の対象となる攻撃点や攻撃経路のこと。Attack Surface。
2:実装されているものの、実際には使用されていないインターフェースのこと。



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
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

★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。

JC-STAR★1の更新後のパスワードの規定(8桁以上)について、機器又はユーザーのどちらに担保させるのか

IPA

- ★1においての取扱いは以下の通り
  - ドキュメント評価
  - 評価項目1、2のいずれかを満たす実装
    - [評価項目1] デフォルトパスワードは、IoT機器毎に異なる一意で、以下のA)～D)のいずれにも該当しない、6文字以上のパスワードであること。
      ⇨ **ベンダーの責任で設定**
    - [評価項目2] デフォルトパスワードは、初回起動時にユーザによるパスワード変更を必須とする機能を実装し、8文字以上のパスワードを強制させる。
      ⇨ **ユーザーの責任で設定。「8文字以上」以外の制約条件はない**

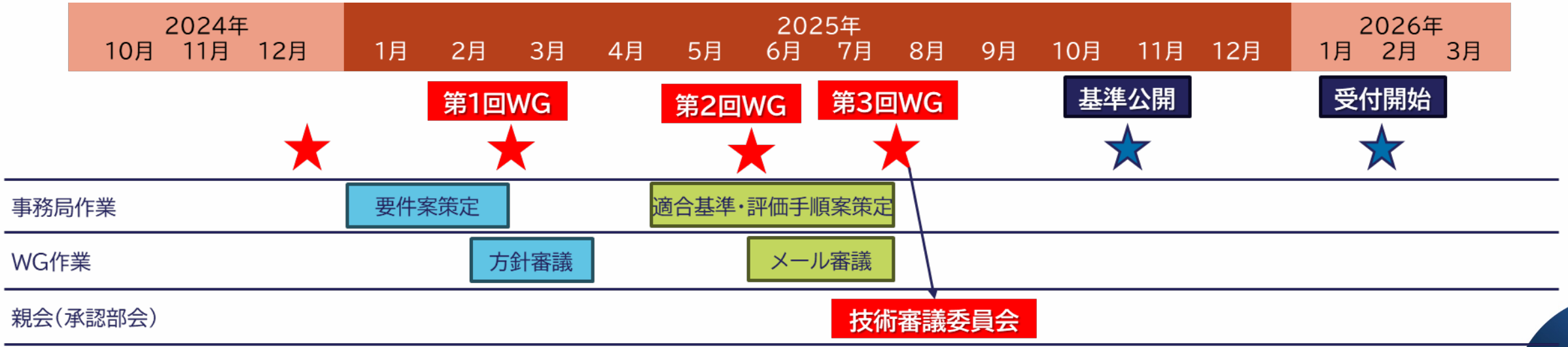
A) 共通する文字列や単純なパターンが存在するパスワード(例:"admin"、"root"、"QWERTY"など)
B) 覚えやすい有名な固有名詞や、人名、地名などを利用したパスワード(例:"baseball"、"mustang"、"michael"など)
C) 増加するカウンターに基づくパスワード(例:"123456"、"aaaaaaaa"、"1234abcd"、"password1"など)
D) MAC アドレス、Wi-Fi の SSID、IoT 製品のシリアル・型番・名前(略称)などの公開情報に基づくパスワード

- ★2以上においての検討課題は以下の通り
  - 実機テスト確認をするかどうか
  - デフォルトパスワード長: 6文字以上 → 8文字以上 or 15文字以上
  - 変更パスワード長: 8文字以上 → 15文字以上
  - 変更パスワード強度確認:
    強度推定メーター or 脆弱なパスワード設定拒否機能 or 自動生成機能(+パスワード管理機能)

NIST SP800-63B-4 (2nd Draft)
- Verifiers and CSPs SHALL require passwords to be a **minimum of eight characters** in length and SHOULD require passwords to be a **minimum of 15 characters** in length.
- Estimating the **entropy for user-chosen passwords is challenging**, and past efforts to do so have not been particularly accurate. For this reason, a different and somewhat more **straightforward approach based primarily on password length** is presented herein.

通信機器における★3適合基準の策定に向けて

- ★3としての代表的な脅威に対抗するためのセキュリティ機能や脆弱性への対応等
  - MiraiやMirai亜種による攻撃（BoT化リスクへの対応）
  - 自動化された攻撃によるマルウェア感染（悪意のあるコードの混入リスクへの対応）
  - 正規のID・パスワードを用いた侵入（内部ネットワークへの侵入リスクへの対応）
  - 踏み台による他の機器への攻撃（踏み台となるリスクへの対応）
  - 既知及び未知の脆弱性を悪用した攻撃（脆弱性対応・脆弱性検査不備リスクへの対応）
  - 政府・自治体・企業を標的としたサービス不能攻撃（悪意のある攻撃リスクへの対応）
  - サプライチェーンにおけるバックドアを仕込んだ攻撃（サプライチェーンリスクへの対応）



「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/

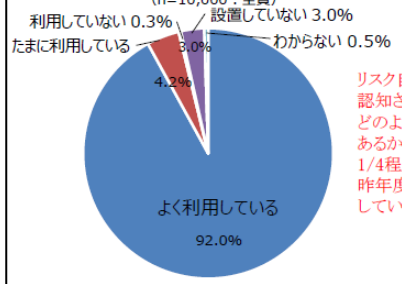
無線LAN利用者実態調査①

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））

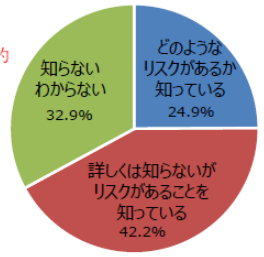
自宅に設置する無線LAN（その１）

自宅無線LANの利用有無
（n=10,000：全員）

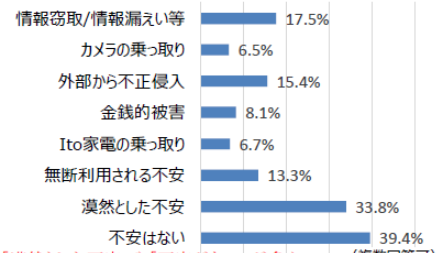


リスク自体は比較的認知されている。どのようなリスクがあるかを知る人は1/4程度であるが、昨年度より増加している。

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）



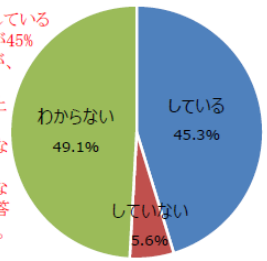
自宅無線LANでのセキュリティ上の不安
（n=961：自宅無線LANの利用者）



「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）

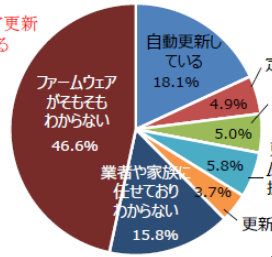
暗号化している利用者が45%程度だが、一方で半分以上が「わからない」、「していない」と回答している。



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）

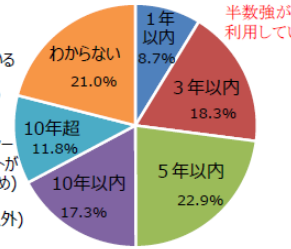
ファームウェア更新を実施している利用者は4分の1程度である。

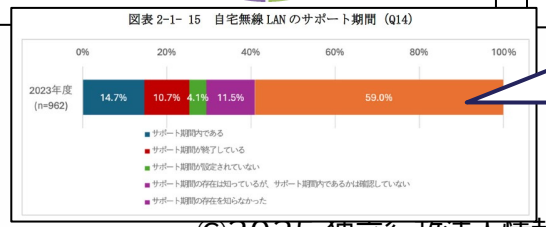
6割強が存在を把握していない



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。





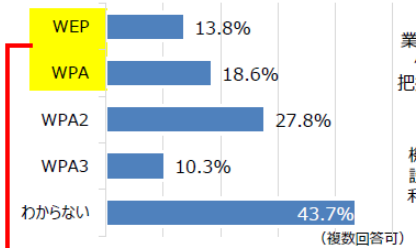
サポート期間の存在を知らなかった

無線LAN利用者実態調査②

2

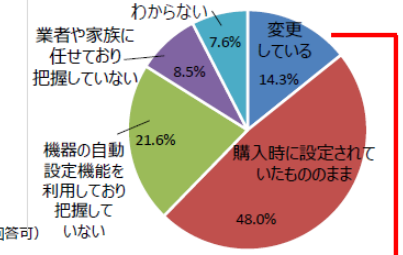
自宅に設置する無線LAN（その２）

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）



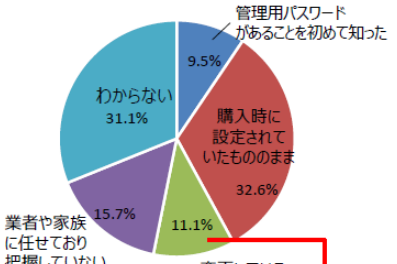
WEPやWPAを利用する人が3割おり方式を把握していない人も半数近く存在。昨年よりWPAが若干減り、WPA3が増えている。

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）

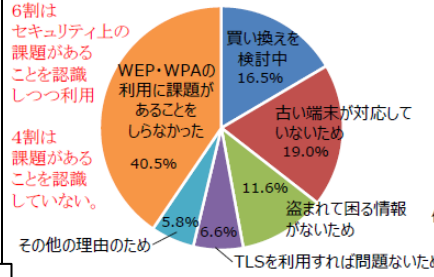


購入時設定のまま利用している人が多数
1割は管理用パスワードの認識がない。

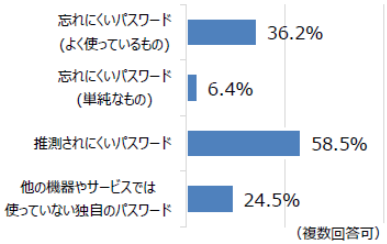
WEP・WPAを利用する理由
（n=121：自宅無線LANでWEP・WPAを用いている利用者）

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

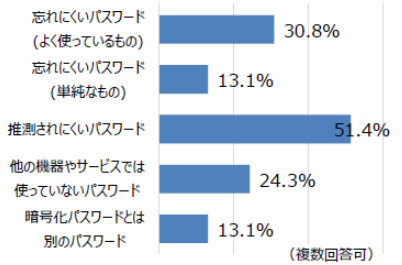
4割は課題があることを認識していない。



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）



端末機器の技術基準等への適合性に係るセキュリティ基準の見直しに向けて　－　JC-STARを開始して気が付いたこと

- 対象範囲を広げるほどいろいろなケースを考慮する必要がある
  - 同じ基準であっても、製品の利用形態やベンダの実装方法の違いによって適用できるのかどうかの個別判断が必要になることもある
- 相互承認（同種評価の重複回避）への期待はやはり大きい
  - 少なくとも同一の要件は同一の基準にしておきたい
  - 法令規格と任意規格での評価方法・評価結果の取扱いの違いをどう考えるか
  - 自己適合評価（自己宣言）と第三者検証の違いをどう考えるか
- どこまでユーザーの自由度を認めるかを考慮する必要がある
  - ユーザーが脆弱なパスワードを設定することを認めるのかどうか、注意喚起するのかどうか
  - ファームウェア更新を自動設定させるのかどうか
- ファームウェア更新範囲をどう考えるかを決める必要がある
  - 脆弱性対策としてファームウェア更新と、機能拡張・改善のためのファームウェア更新の区別が必要
- インタフェースの無効化はどのように確認するかも考える必要がある
  - 検査ツールをどのように指定しておくか
- サポート期間の周知／有効期間を導入するかを考慮する必要がある