

セキュリティ要件適合評価及びラベリング制度 (JC-STAR*)の紹介と最新動向 ～ セキュアなIoT製品の普及を目指して ～

* 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



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！ ～

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



インターネットに接続可能なIoT製品

内部ネットワークに接続可能なIoT製品 (IPを使用した通信が可能)

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

1. JC-STARがつけられた背景や目的

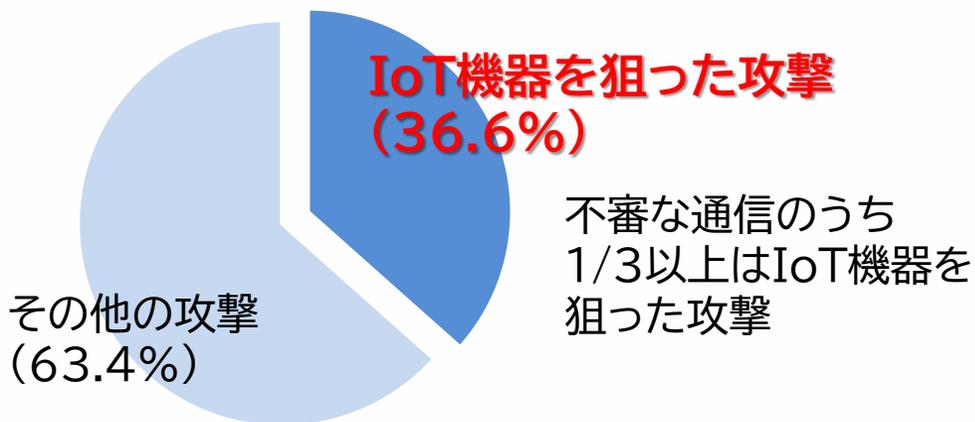
2. JC-STARの概要

3. JC-STARの今後に向けて

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か？
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



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

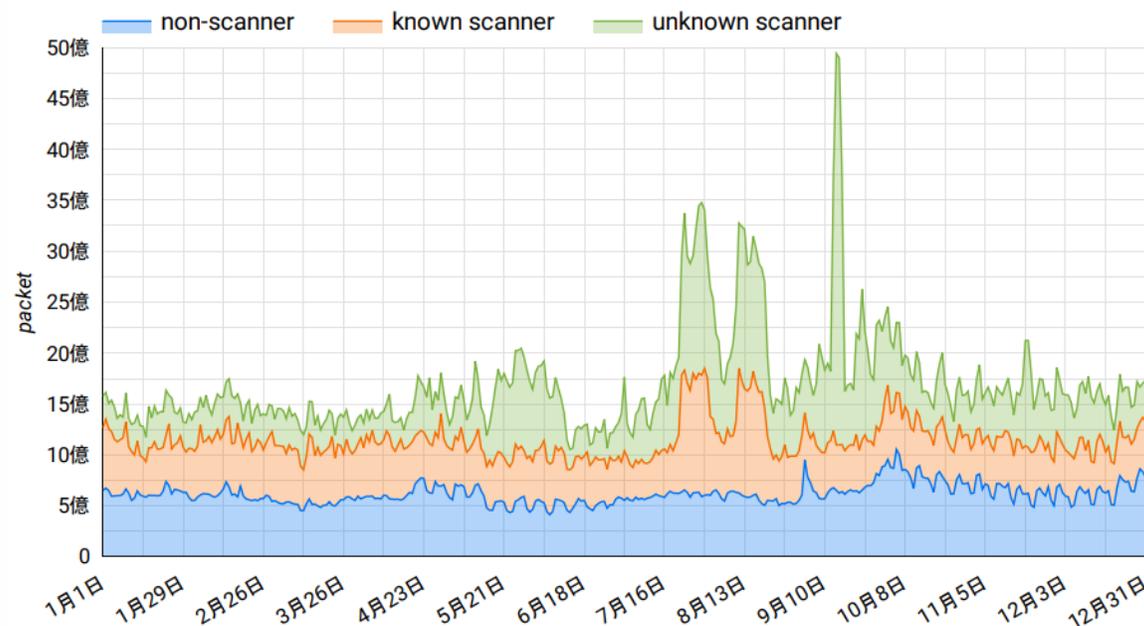


図1: ダークネットにおける日ごとの観測パケット数の推移(積み上げグラフ)
NICT「NICTER観測レポート2023」の1年間にダークネット(約29万観測アドレス)で
観測された攻撃パケット数の日ごとの合計

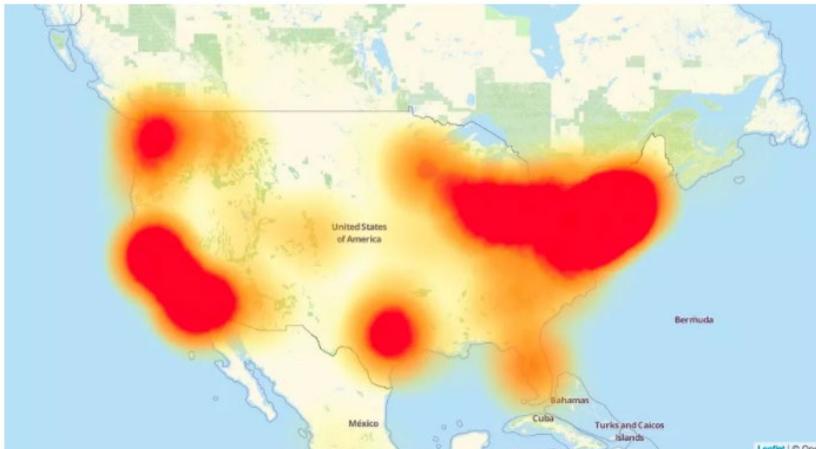
IoT製品のインシデント事例

■ 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

2016年10月21日

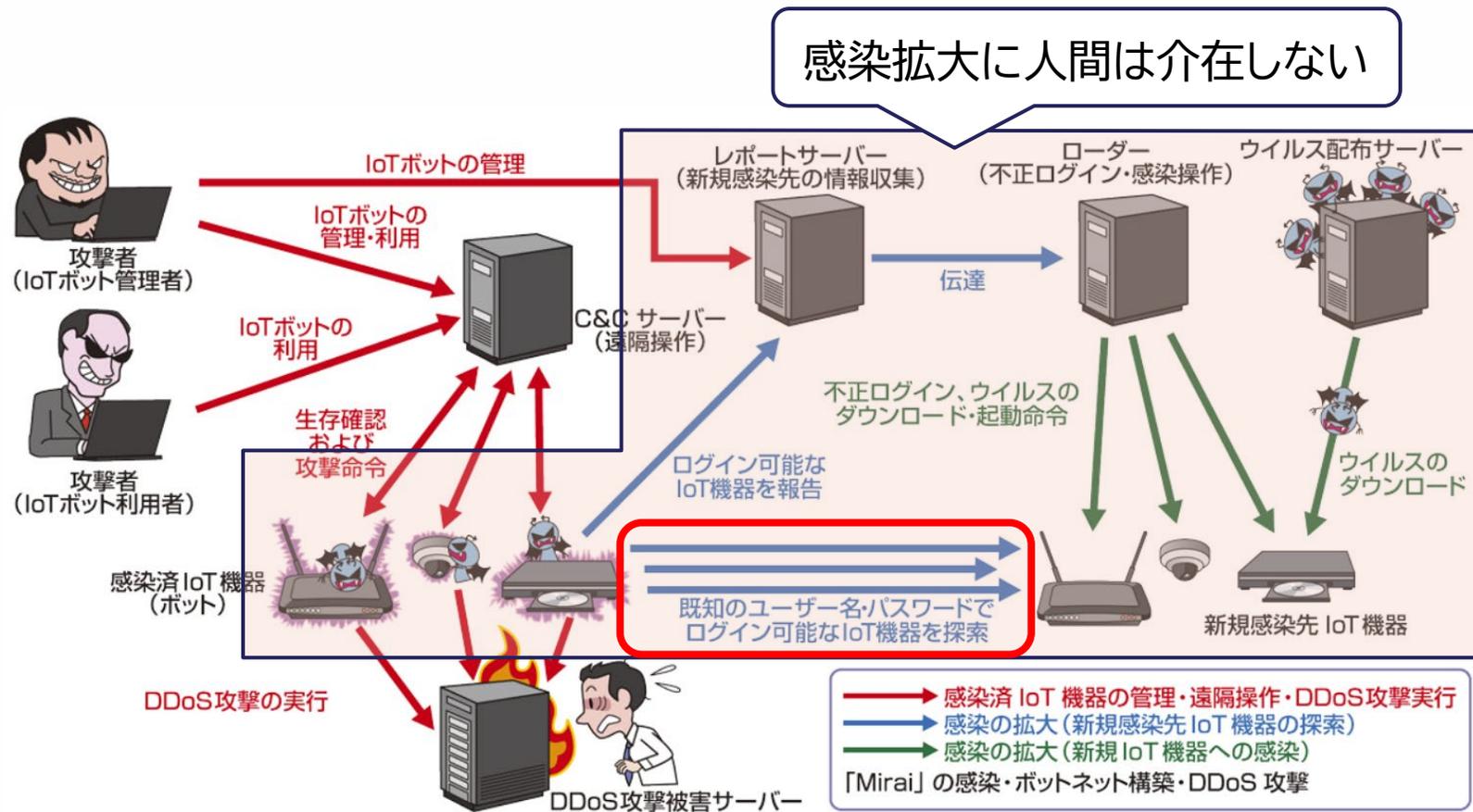
- Amazon・GitHub・Twitter・Netflix等を含めた多くのサイトがアクセス不能
- Miraiに感染したIoT機器によるボットネットからの攻撃と推定
- 500Gbps超にも達するトラフィックを発生



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/>
エコネットシンポジウム(2026.03.05)



[出典] IPA、情報セキュリティ10大脅威 2017

©2026 独立行政法人情報処理推進機構(IPA)

IoT製品のインシデント事例

- 国内におけるIoT機器のマルウェア感染急増(2017年)
 - 4年前に公開された**更新ファームウェアの適用が未徹底**だった無線LAN BBルータが多く感染
- 個人宅に設置されたネットワークカメラ乗っ取り(2017年)
 - **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**
- 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)
 - **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
 - 不正アクセスできるNWカメラを集めたサイトもあり
- 重要インフラ等で利用されるIoT機器での脆弱性調査(2017, 2020, 2023年度)
 - 2023年度は2,883件の脆弱な重要IoT機器を検出
 - 検知された脆弱な機器の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**」
- 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)
 - 安価なルーターや無料アプリに「**不正SDK**」が利用 ⇒ 製品**出荷時点ですでにボットネット**組込み

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」

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/はつきりしない
 - 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/>)

2025年7月時点のIoT機器観測状況

観測概要

IoT機器観測総数

月 **1.24** 億件

参加インターネットサービスプロバイダ (ISP) のIPアドレスに対して観測している総数

容易に推測可能なID・パスワードであるIoT機器

月 **14,370** 件



容易に推測可能なIDやパスワードを使用しているため、攻撃者によって管理権限を乗っ取られたり、サイバー攻撃に追加させられる危険性がある機器

ファームウェアに高リスク脆弱性を有するIoT機器

月 **2,865** 件



第三者に不正利用される危険性があるファームウェア脆弱性を有するIoT機器

マルウェア感染IoT機器検知数

最大 **1,024** 件/日

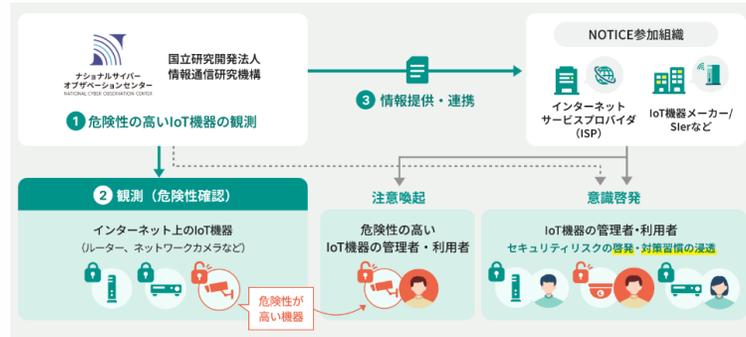


Miraiに既に感染していると推定されるIoT機器。サイバー攻撃に追加させられている可能性がある。
※IPアドレスが変動している場合は、重複して計上している場合があります
※当月1日あたりの最大値を掲載しています

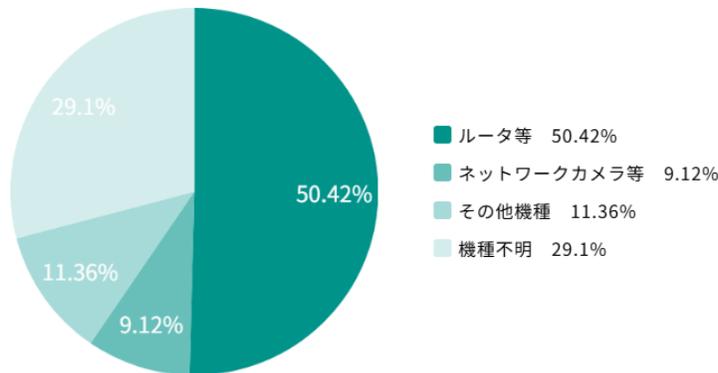
リフレクション攻撃の踏み台にされるIoT機器

月 **15,353** 件

リフレクション攻撃の踏み台にされる可能性のあるIoT機器だと検知した数

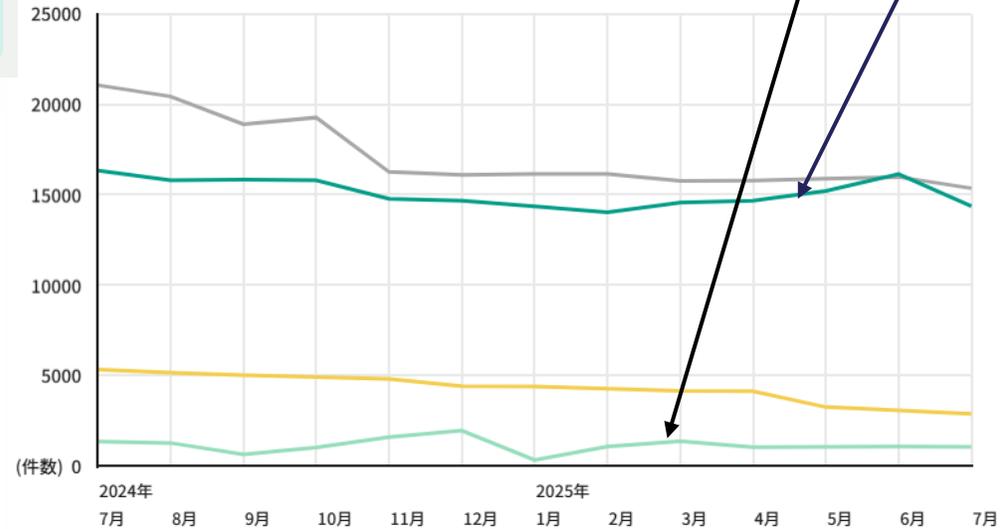


容易に推測可能なID・パスワードであるIoT機器の種類



観測状況の推移

- ✓ 容易に推測可能なID・管理用パスワードであるIoT機器
- ✓ ファームウェアに高リスク脆弱性を有するIoT機器
- ✓ マルウェア感染IoT機器検知数
- ✓ リフレクション攻撃の踏み台にされるIoT機器



月 / 年

IoT製品のライフサイクル

Secure By Design

Secure Coding & Fuzzing

企画
(方針)

分析・設計

開発

テスト

運用／保守

セキュリティ方針
保護対象

脅威(リスク)分析
セキュリティ設計

セキュア開発
既知の脆弱性対策

脆弱性テスト

パッチ作成・配信
長期運用保守体制

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

JC-STARの目的

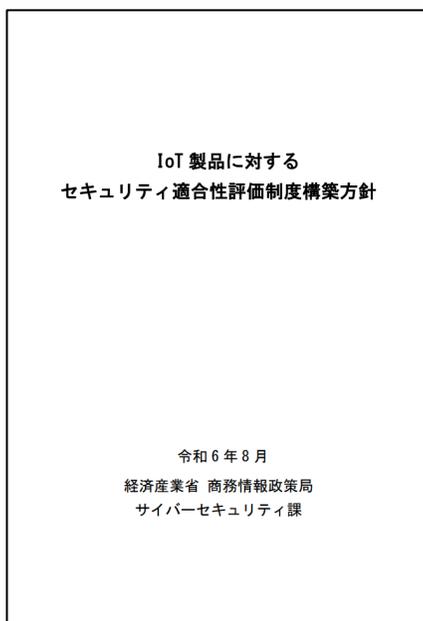
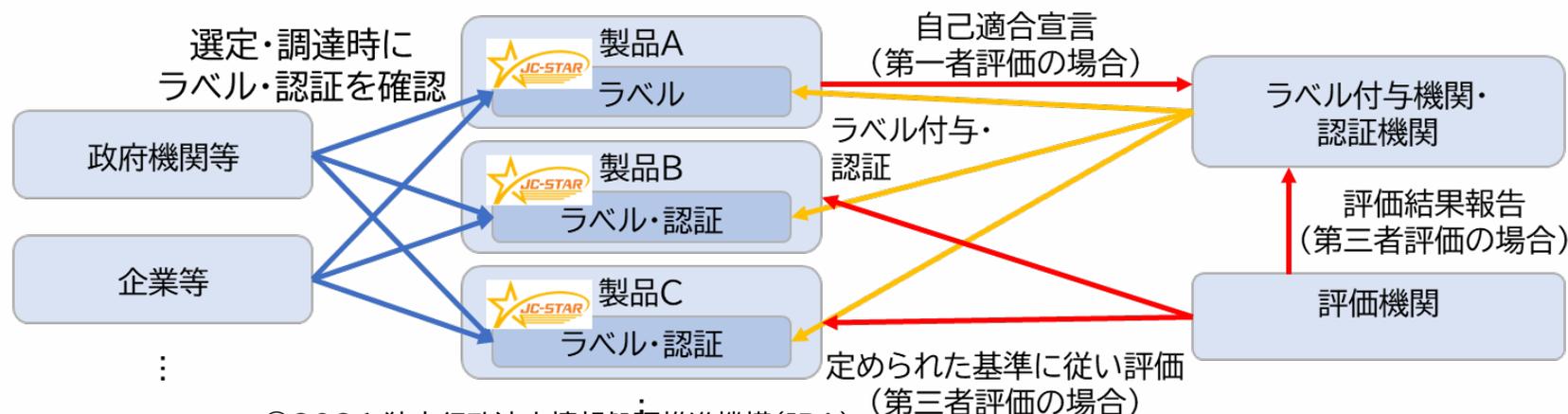
共通的な物差しでIoT製品のセキュリティ機能を評価・可視化し、適切なセキュリティ対策が講じられているIoT製品が広まる仕組みの構築が必要

- 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

- 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



1. JC-STARがつけられた背景や目的

2. JC-STARの概要

3. JC-STARの今後に向けて

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)

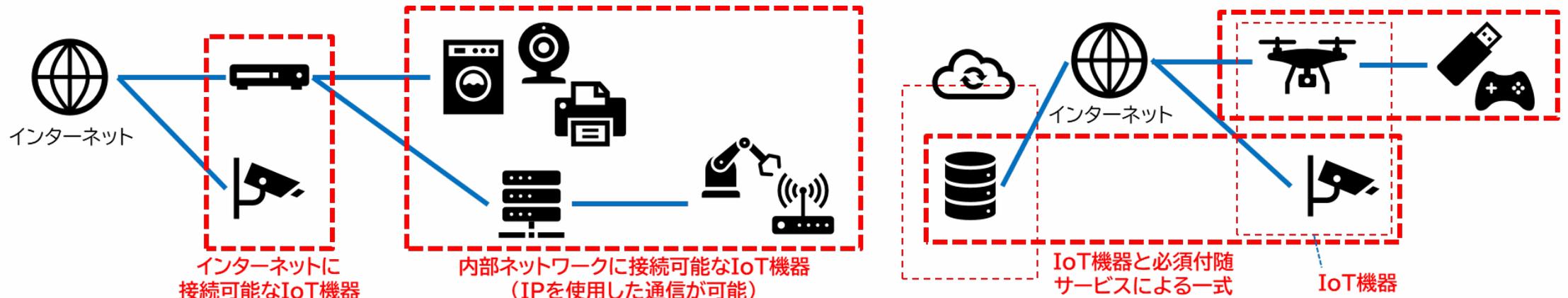
インターネット側からの通信を受信する可能性がある

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

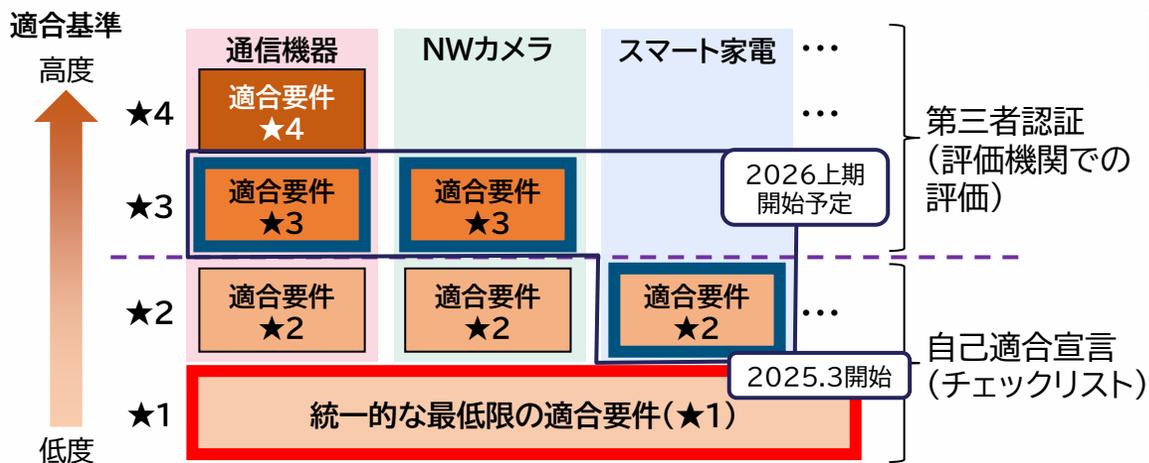
④ 購入時に具備されているセキュリティ機能を利用し、アップデート以外で後からセキュリティ機能を追加することが困難/できない



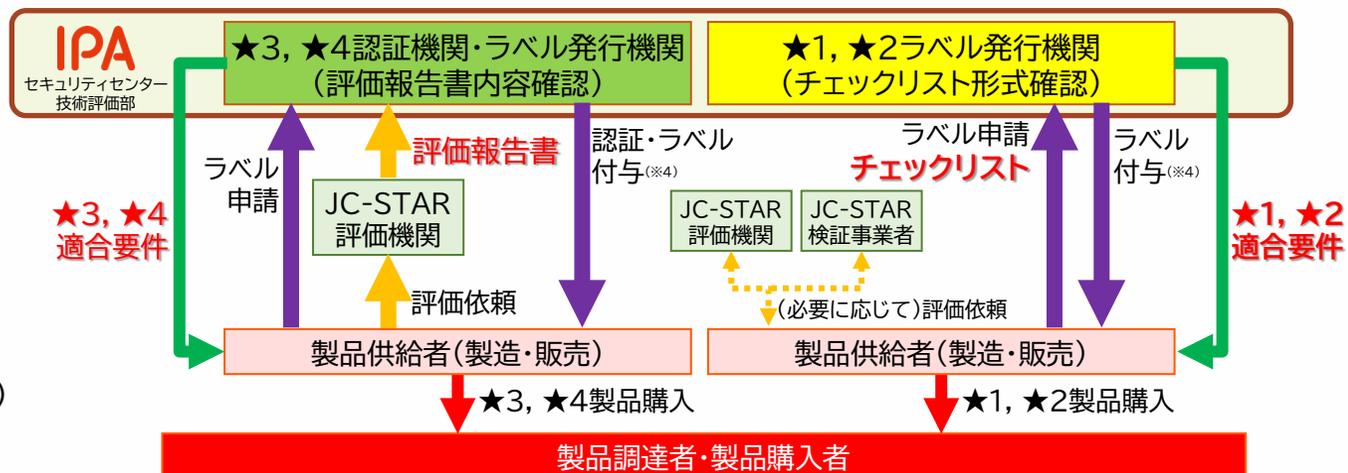
適合ラベルの適合要件

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



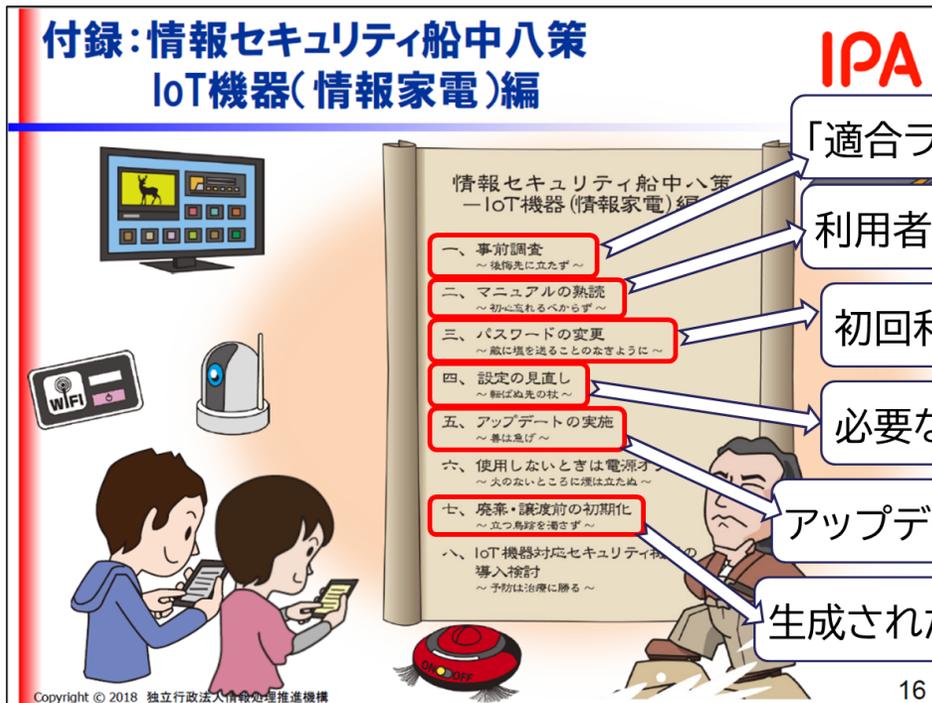
レベル	位置付け	適合基準	評価方式
★4	政府機関等や重要インフラ事業者、地方自治体、大企業の重要なシステムでの利用を想定した製品類型ごとに★1、★2に追加して汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの	製品類型別	第三者認証
★3			
★2	製品類型ごとの特徴を考慮し、★1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの	製品類型共通	自己適合宣言
★1	製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの		

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、**スクリプトキテ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**



★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20日時点で適合ラベル発行数65社157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)

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

■ ラベル付与製品に対して事後的に**検査やサーバイランスを行える**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
- サバ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



Registered ID: 2025030500001527
Information-technology Promotion Agency, Japan (IPA)



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	

有効期間内はアップデートサポートを義務付け

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	

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-001, 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	

問合せ窓口情報

- 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)

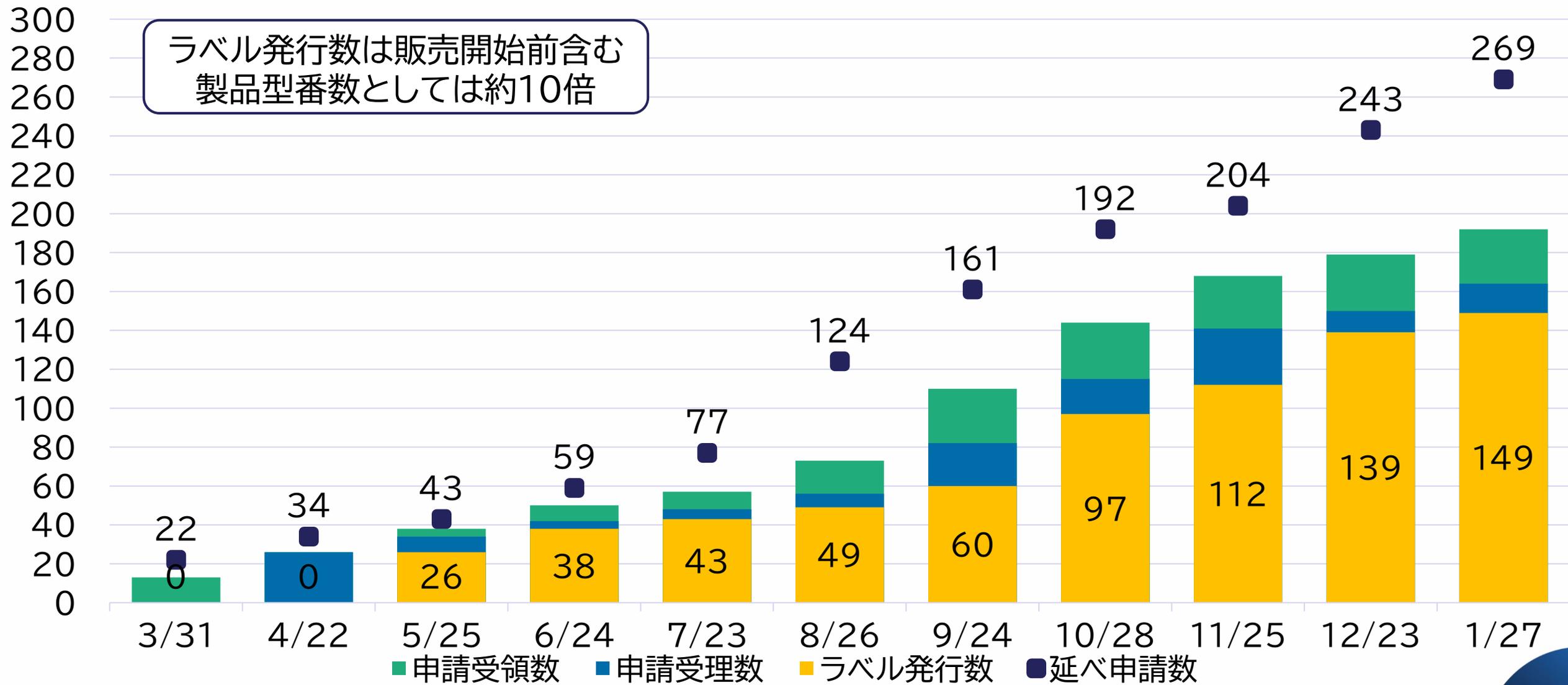
PSTI法適合確認欄

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	
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

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	

申請実績推移

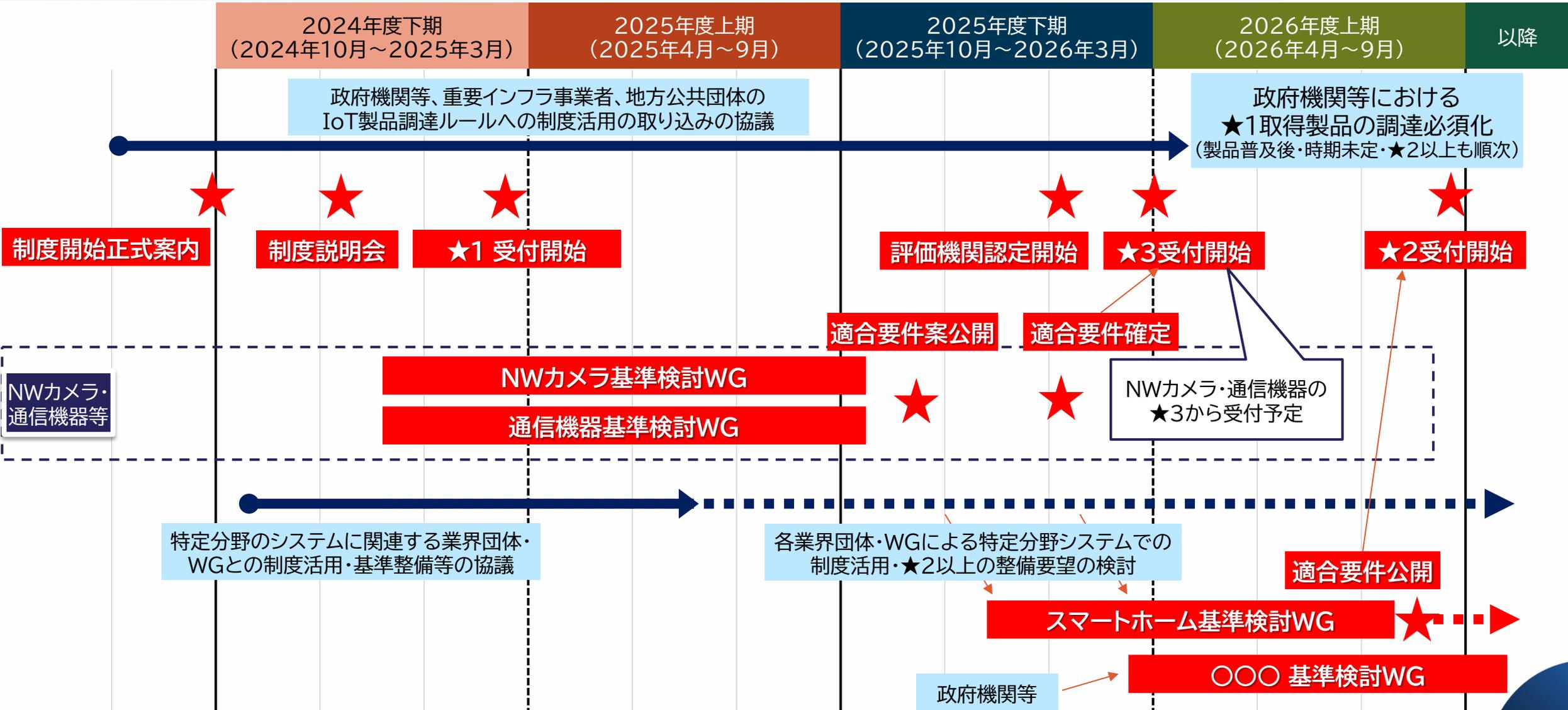


1. JC-STARがつけられた背景や目的

2. JC-STARの概要

3. JC-STARの今後に向けて

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



➤ 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. キットティングイメージの厳格な管理	➤ 端末キットティングイメージ（端末をユーザがすぐに使える状態にするドライバイメージのこと。）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

【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。

- 「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。
- 「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

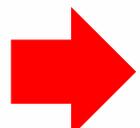
② 業界標準としてIoT製品ベンダと調達者・利用者が協力して適合ラベル付与製品の製造・販売と選定・調達する分野を確保

➤ 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				
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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> *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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> *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ようようにするために ～



そのネット家電、乗っ取られてるかもしれません。

情報漏えい、大規模サイバー攻撃、マルウェア感染、のぞき見、不正アクセス、踏み台、のっとり

あなたのネット乗っ取られてる知らないうちにサイバー犯罪の片棒を担が

危険なのは情報漏えいだけじゃない。

「安心」「便利」だけで選んでいませんか？
セキュリティレベルの高い機器で心配なのは、情報の流出だけではありません。
気がないうちに、サイバー犯罪に巻き込まれていることも！

あらゆるモノがインターネットにつながる時代—
みんなが安心してIoT機器を選ぶ目印—
「JC-STAR」が誕生します！

Q. セキュリティ対策が必要な家電はどれでしょう？

01 冷蔵庫 02 洗濯機 03 テレビ 04 洗濯機
05 冷蔵庫 06 監視カメラ 07 無線LANルーター 08 テレビ

A. 全部

インターネットにつながる電化製品一制製品は、外見からの判断が難しく、家電店の店頭、メーカーのウェブサイトなど、暮らしをより便利にしてくれます。

ですがインターネットにつながることは、知らず知らずのうちに外部との間に「見えにくい穴」を作ってしまったというところ。

家の広間に鍵をかけるように、ネット家電の見えない穴に鍵を、それが、これからの家電選びの要諦です。

では、セキュリティ対策された安心ネット家電を選ぶには？

これからのネット家電選びは、この星を目印に。

マークで見分ける安心家電

あらゆるものがインターネットにつながる時代に誰もが安心してネット家電を選ぶ目印。それが「JC-STAR」です。

ネットワークカメラの映像を盗み見られたり、電化製品を遠隔操作されたりすることがないように。「星」を確かめて選ぶことで、便利さに「安心」をプラス。

スマートな暮らしを、安心して楽しむために。次の一台は、JC-STAR適合ラベル付き製品を。



JAPAN CYBERSECURITY LABEL

セキュリティ水準適合レベル (★1～★4)
製品詳細情報へのリンク
登録番号

星のラベルの二次元コードをスマホで読み取り、セキュリティ情報をリアルタイム&かんたんチェック！

適合ラベルの有効期間内は、セキュリティ対策向上のための更新プログラム提供などのサポートが約束され、安心して使い続けることができます。有効期限切れなどの情報も、簡単に確認できます。

IPA 独立行政法人情報処理推進機構
Information Technology Promotion Agency, Japan
くわしくはホームページで！
<https://www.ipa.go.jp/security/jcstar/label-description.html>

JAPAN CYBERSECURITY LABEL

セキュリティ水準適合レベル (★1～★4)
製品詳細情報へのリンク
登録番号

ラベルの二次元コードをスマホで読み取り、セキュリティ情報をリアルタイム&かんたんチェック！

適合ラベルの有効期間内は、セキュリティ対策向上のための更新プログラム提供などのサポートが約束され、安心して使い続けることができます。有効期限切れなどの情報も、簡単に確認できます。

IPA 独立行政法人情報処理推進機構
Information Technology Promotion Agency, Japan
くわしくはホームページで！
<https://www.ipa.go.jp/security/jcstar/label-description.html>

詳しくは以下を参照ください

IPA 独立行政法人 情報処理推進機構

IPAについて お問い合わせ English 公式SNS 検索 目的別に探す

情報セキュリティ 試験情報 デジタル人材の育成 社会・産業のデジタル変革

情報セキュリティ

トップページ > 情報セキュリティ > セキュリティ要件適合評価及びラベリング制度 (JC-STAR)

セキュリティ要件適合評価及びラベリング制度 (JC-STAR)

[ENGLISH]

こちらから →

「制度ロゴ」 「適合ラベル」

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) とは、ETSI EN 303 645やNISTIR 8425等の国内外の規格とも調和しつつ、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、我が国の制度です。

本制度の概要

本制度は、2024年8月に経済産業省が公表した「IoT製品に対するセキュリティ適合性評価制度構築方針」に基づき構築された制度で、インターネットとの通信が行える幅広いIoT製品を対象として、共通の物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的としています。

従来、IoT製品におけるセキュリティ対策の取組については、ベンダー側が調達者・消費者にアピールすることが難しく、調達者・消費者から見ても、製品のセキュリティ対策が適切か否か判断できないという課題がありました。また、政府機関や企業等でのセキュリティ対策において、調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーン・リスク管理の取組が広がる中、本来自組織が実施すべき、製品のセキュリティ機能や対策状況を確認するプロセスを定選・調達時に実行することが難しい現状があります。

本制度では、これらの課題を解決するため、求められるセキュリティ水準に応じて、IoT製品共通の最低限の脅威に対応するための適合基準である★1 (レベル1) とIoT製品類型ごとの特徴に応じた適合基準である★2 (レベル2)、★3 (レベル3)、★4 (レベル4) を定め、適合が認められた製品には、二次元バーコード付きの適合ラベルを付与することで、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調達者・消費者が簡単に取得できるようにしています。

「IoT製品に対するセキュリティ適合性評価制度構築方針」については、経済産業省のページを参照ください。

- 情報セキュリティ
- 重要なセキュリティ情報
- 脆弱性対策情報
- 情報セキュリティ10大脅威
- ビジネスメール詐欺 (BEC) 対策
- 中小企業の情報セキュリティ
- 制御システムのセキュリティ
- IoTのセキュリティ
- 情報セキュリティ関連ガイド
- Emotet (エモテット) 関連情報
- 協定・地域との連携
- 情報セキュリティ安心相談窓口
- サイバーレスキュー隊 J-CRAT (ジェイ・クラート)

IPA 独立行政法人 情報処理推進機構

情報セキュリティ

トップページ > 情報セキュリティ > セキュリティ要件適合評価及びラベリング制度 (JC-STAR) > JC-STAR制度説明資料集

JC-STAR制度説明資料集

最終更新日：2025年1月30日

JC-STAR制度説明会資料 JC-STAR制度説明会質疑応答

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)

- 第一部 (JC-STAR制度の説明) (PDF:9.0 MB)
- 第二部 (JC-STAR制度へのよくある質問について) (PDF:3.9 MB)
- 第三部 (★1 (レベル1) 適合基準・評価ガイドの説明) (PDF:8.0 MB)

「★1 (レベル1) 適合基準・評価ガイドの説明について」は、「★1 (レベル1) 適合基準・評価ガイド」もあわせてご確認ください。

[★1 \(レベル1\) 適合基準・評価ガイド](#)

JC-STAR制度説明会質疑応答

[会場での質疑応答\(PDF:309 KB\)](#)

オンラインでの質疑応答 注：後日公開予定

- 情報セキュリティ
- 重要なセキュリティ情報
- 脆弱性対策情報
- 情報セキュリティ10大脅威
- 情報セキュリティ安心相談窓口
- ビジネスメール詐欺 (BEC) 対策
- サイバーレスキュー隊 J-CRAT (ジェイ・クラート)
- サイバー情報共有イニシアティブ J-CSIP (ジェイシップ)
- 攻撃情報の調査・分析事業

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

IPA