2. IoT 製品に対するセキュリティ適合性評価制度『JC-STAR』の開始

要約

- 独立行政法人 情報処理推進機構（IPA）は、IoT 製品のセキュリティ適合要件を評価する制度『JC-STAR』を 2025 年 3 月から開始すると公表した。
- JC-STAR で付与される適合ラベルにより、ユーザーは購入する IoT 製品が国で定めたセキュリティの適合基準を満たしているかどうかを容易に確認することができる。

概要

IPA は 2024 年 9 月 30 日、IoT 製品に対するセキュリティ適合性評価制度となる『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）』（以下、「本制度」という。）の開始について公表しました(*1)。本制度は、2024 年 8 月に経済産業省が示した『IoT 製品に対するセキュリティ適合性評価制度構築方針』(*2)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、共通的な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。

セキュリティ対策が不十分な IoT 製品がサイバー攻撃によってマルウェアに感染する事例が相次ぐ中、本制度により、ユーザーは一定のセキュリティ要件を満たした安全な IoT 製品を調達しやすくなります。本制度は 2025 年3月から開始される予定で、適合基準を満たす製品には適合ラベルが付与されることとなります。

本制度のロゴ

適合ラベル（イメージ）

出典：IPA「IoT 製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」(*3)から転載

本制度の対象機器、適合基準

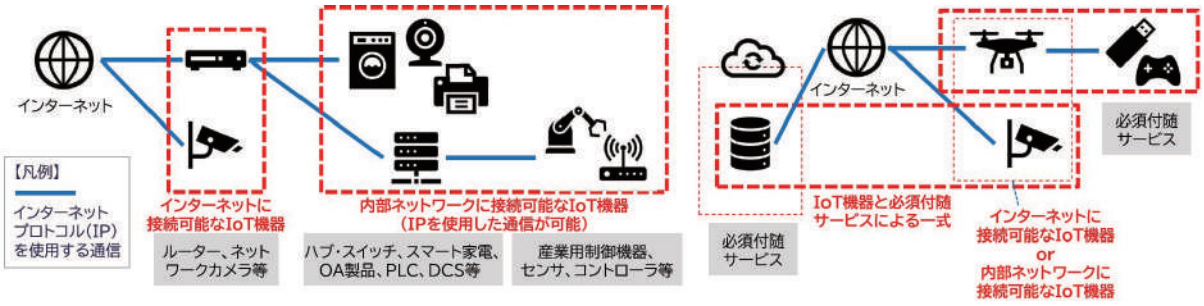
本制度で適合ラベルの対象となる機器は、インターネットプロトコル（IP）を使用したデータの送受信機能を持つものであって、ルーター、ネットワークカメラ、スマート家電、産業用制御機器などの他、これら機器と一体で提供することが必須となるものも含まれます。

また、本制度の適合基準は4段階のレベル（★1～4）が設けられており、レベルが高くなるほど求められるセキュリティ要件の項目が多くなります。★1 は全ての IoT 製品に共通の統一的な最低限の適合基準が設けられていますが、★2 以上では、通信機器やスマート家電といった製品類型ごとの特徴や利用形態、脅威なども考慮され、同じレベルであっても製品類型によって異なる適合基準が設定されています。

(*1) IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」

(*2) 経済産業省「IoT 製品に対するセキュリティ適合性評価制度構築方針」

(*3) IPA「IoT 製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」

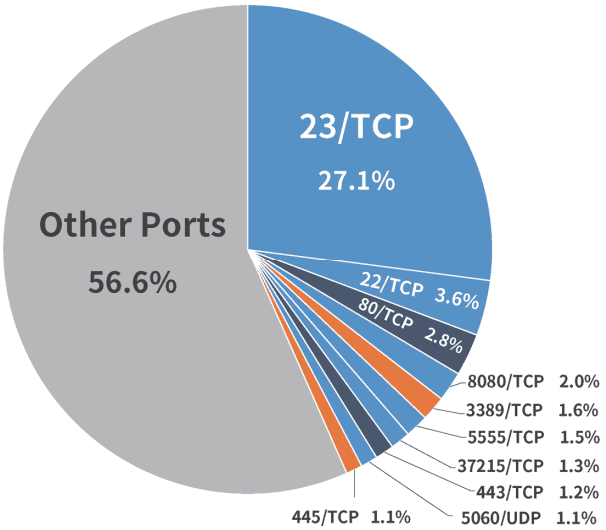


本制度で適合ラベルの対象となる機器（赤枠部分）

出典：IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」(*1)から転載

本制度創設の背景

本制度創設の背景には、近年のデジタル化の進展に伴い IoT 機器が急速に増加し、これらの脆弱性を狙ったサイバー攻撃の脅威が高まっていることがあげられます。国立研究開発法人情報通信研究機構（NICT）が 2024 年 2 月 13 日に公表した『NICTER 観測レポート 2023』(*2)によれば、2023 年にインターネット上で観測された主な攻撃対象（宛先ポート番号）の上位 10 位のうち、六つが IoT 機器に関連しており、その通信量は全体の 36.6%を占めていました。



宛先ポート番号別パケット数分布（水色の箇所が IoT 機器に関連するもの）

出典：NICT『NICTER 観測レポート 2023』(*2)から転載

宛先ポート	攻撃対象
23/TCP	Telnet（ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Webサーバ）
8080/TCP	HTTP（Web管理画面）
3389/TCP	Remote Desktop
5555/TCP	ADB（Android）
37215/TCP	Huawei 製ルータ
443/TCP	HTTPS（Webサーバ）
5060/UDP	SIP
445/TCP	Windows SMB

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

これらの IoT 機器を狙った攻撃により、インターネットに接続された IoT 機器が知らぬ間にマルウェアに感染し、新たな攻撃の踏み台としての悪用や、情報が窃取される被害が多発しています。このような現状から、IoT 機器へのセキュリティ対策が求められる一方で、製品ベンダーはセキュリティ対策の取り組みをユーザーに効果的に伝えることが難しく、ユーザー側も製品のセキュリティ対策が適切かどうかを判断するのが困難という課題がありました。本制度ではこれらの課題を解決し、ユーザーが製品の詳細や適合評価、セキュリティ情報、問い合わせ先などの情報を容易に取得できるようにしています。

最後に

本制度では、諸外国における IoT 製品の適合性評価制度設立の動向も踏まえ、各国の制度との連携を図り、相互承認することも目指しており、現在、シンガポール（Cybersecurity Labelling Scheme）、英国（PSTI 法）、米国（U.S. Cyber Trust Mark）、EU（CRA）の各国担当機関との間で相互承認に向けた交渉を行っています。EU（CRA）については、本冊子 P.11 で紹介していますのでご参照ください。

（横平　健）

(*1) IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」

(*2) NICT「NICTER 観測レポート 2023 の公開」