IoT機器における サイバーセキュリティ

～最近の日欧米の施策動向について解説する～

JPNIC理事
荻野 司 TSUKASA OGINO

キヤノン株式会社中央研究所を経て、各種製品の研究・開発やISP事業に携わる。2003年～2014年まで株式会社ユビテック代表取締役社長。現在は、ベンチャー支援を担うゼロワン研究所 代表社員。一般社団法人重要生活機器連携セキュリティ協議会（CCDS）では、IoTセキュリティにおける標準化、技術開発を推進。教育活動として、複数の大学でホワイトハッカーのための実践的な演習などIoTサイバーセキュリティ講座を担当。情報セキュリティ大学院大学客員教授（2018～）

■はじめに

IoT（Internet of Things）の普及に伴い、セキュリティの確保がますます重要性を増しています。世界各国で、IoT機器のセキュリティに関する施策が着実に進展しており、その動向を追うことは不可欠です。本稿では、欧州、米国、日本におけるIoT機器セキュリティの最新の施策動向を紹介し、各国が進めるセキュリティ認証スキームのポイントを整理します。各国のこれらの施策は、消費者と企業のデジタル環境をより安全にし、サイバー脅威に対抗するための重要な施策です。

■欧州における施策動向

2019年、英国政府はコンシューマ機器のセキュリティに関する13か条の行動規範を発表しました。これを基に、2020年にはIoTセキュリティ要件として「ETSI EN303 645」が制定されました。2022年には、欧州連合（EU）の欧州委員会は、無線機器指令（RED）にサイバーセキュリティ、個人情報保護、プライバシーの向上を図る新たな要件を追加し、2025年8月1日の施行を目指しています。同年、欧州委員会は、インターネット接続機器に対するサイバーセキュリティ対策を義務化する「サイバー・レジリエンス法案」も提出しました。この法案には、メーカーやソフトウェアベンダーに対して第三者機関による評価を義務付ける規定や、違反した場合の制裁金として最大1,500万ユーロもしくは売上高の2.5%の高額な金額を科す規定が含まれています。また、脆弱性の発見やセキュリティ事故の場合、ENISA（欧州ネットワーク情報セキュリティ機関）に対して24時間以内に報告する義務も規定されています。

■米国における施策動向

2018年、NIST（米国標準技術研究所）は、IoTサイバーセキュリティの目的、リスク、脅威の分析および国際標準化状況を整理したNIST IR8200を草稿として発表。翌年、NIST IR 8259が最終版として公開され、政府調達における適切なセキュリティ管理の推奨事項が示されました。2021年には、コンシューマ機器に焦点を当てた、サイバーセキュリティ大統領令 Executive Order 14028が発行され、翌年NISTは、「消費者向けIoT製品のサイバーセキュリティラベリング推奨基準」の提案。NIST IR 8259をベースにした消費者向けIoT機器のセキュリティベースライン要件もNIST IR 8425として公開しました。2024年4月から春にかけて「消費者向けIoT製品のサイバーセキュリティラベリングスキーム」の実施が予定されています。

■日本における施策動向

IoT機器のセキュリティに関する施策は、2018年から2022年にかけて着実に進展しています。2018年、総務省は、電気通信事業法においてセキュリティ要件の追加を提案。これはIoT機器のセキュリティを向上させる一歩となりました。2019年には、経済産業省よりサイバー攻撃からIoT機器を守るためのガイドライン「サイバー・フィジカル・セキュリティ対策フレームワーク（CSPF）」が公開されました。同年、総務省、NICT、インターネットプロバイダが連携して、悪用されるおそれのあるIoT機器の調査と利用者への注意喚起を行う取り組みが始まっています（NOTICE）。2020年、IoT機器のセキュリティ向上を促進するために、ボット対策（4要件）を追加した技術適合基準が施行され、国際的なリーダーシップを示しています。2022年には、経済産業省がIoT製品に対するセキュリティ適合性評価制度の構築に向けた検討を開始、IoT機器へのラベリングスキーム施策に向けた検討を始めています。

このように、欧州、米国、日本においては、IoT機器へのセキュリティに対する取り組みを一段と強化する方向で検討が進んでいます。国内外でのサイバー脅威に対抗する施策を積極的に検討しています。

■IoT機器セキュリティ認証スキームに関する要点

欧米や日本の進めるセキュリティ対策から、認証スキームにおける重要な四つのポイントを示しておきます。

1）ベースライン要件の安定性：
提案されているベースライン要件（最低限守るべき要件）は、基本的にあまり違いはありませんが、日本のメーカーや消費者に向けて無理のない範囲にすることが肝要です。

2）セキュリティの経年変化と要件の鮮度：
セキュリティは絶えず変化し続けるので、要件や適合基準を柔軟にアップデートできる仕組み、体制が重要です。

3）軽い検査プロセスの必要性：
標準化プロセスは通常、認証にかかるコストが増大する傾向にあります。製品コストを考えると軽い検査プロセスが重要です。

4）社会実装へのインセンティブ：
IoT機器のセキュリティ認証は、実際に使われることが重要です。認証にかかるコストを低く抑え、ユーザには、安心感と安全性の視覚化、さらにはその利点を平易に訴求できることが求められます。

■おわりに

欧米各国や日本は、社会インフラとなったインターネットの健全な環境を維持するため、新たな施策を進めています。ネットワーク資源の管理を行うJPNICは、欠かせない役割を持つ組織です。今後も、会員企業、インターネットを使うユーザ企業とともに、国際的な協調を進めながら安心・安全なインターネット社会基盤に向けた活動が求められています。