

IoT機器のサイバーセキュリティ対策について

2017年12月11日（月）

一般社団法人 電子情報技術産業協会

一般社団法人 電子情報技術産業協会 (JEITA) の概要

- ◆ JEITAは国内外で約36兆円の規模を持つIT・エレクトロニクス産業を担うわが国最大級の業界団体
- ◆ 設 立：2000年11月1日(EIAJとJEIDAが統合)
- ◆ 会員数：382社(正会員275社 賛助会員107社 2017年10月25日現在)
- ◆ 会 長：長榮 周作 パナソニック株式会社 取締役会長
- ◆ 目 的：電子機器、電子部品の健全な生産、貿易及び消費の増進を図ることにより、
電子情報技術産業の総合的な発展に資し、わが国経済の発展と文化の興隆に寄与する
- ◆ 領 域：電子機器、電子部品/材料、電子デバイス、ITソリューション・サービス等

◆ 基本方針 Society 5.0の推進

高度な情報活用による世界に先駆けた「超スマート社会」の実現 (Society 5.0) に向け、異業種、ベンチャー、海外等とも連携し、成長分野に関わる課題の検討や政府への提言など、会員の新たな取組みを促進するための活動にスピード感を持って取り組む。

また、会員の競争力強化のため、規制・制度改革や税制改正要望等の事業環境整備に着実に取り組んでいく。これらの事業を推進することにより、IT・エレクトロニクス産業ならびにわが国の経済・社会の発展に貢献していく。

◆ 主な事業活動

政策提言: CPS/IoTの推進
税制改正/規制改革

調査統計: 幅広い製品分野の動向把握

課題解決: 社会的要請や業界共通課題解決に向けた取組み

市場創出: 共創と競争によるイノベーションを促し、新たな市場創出のための事業。
「CPS/IoTの総合展」CEATEC JAPAN開催など

JEITAのサイバーセキュリティ対策

■ JEITAとしての取組み

IoT技術によるデータ連携により、技術革新が急激に進展し、新たなサービス創出が期待されている。一方で、各対象分野共通で、機器/サービスの信頼性確保上、サイバーセキュリティ対策は最も重要な課題と認識し、以下の活動を行っている。

- ①パブコメを通じた、業界意見の提出
- ②サイバーセキュリティ関連ガイドラインの周知
- ③CEATEC等を活用し、有識者等のセミナー主催、サイバーセキュリティ対策重要性の周知
- ④海外の関連団体とも連携した諸外国におけるサイバーセキュリティ関連動向把握、ルール整備への対応
- ⑤「IoTセキュリティガイドライン」(IoT推進コンソーシアム IoTセキュリティWG策定)に基づく各社対応

今後「セキュリティ対策検討WG」を設置し、自主的な取り組みの推進を図っていく。

- ＜主な活動案＞
- ①対象機器に対するサイバーセキュリティ対策の検討
 - ②業界(各社)のサイバーセキュリティ対策の周知

JEITAのサイバーセキュリティ対策

■IoT機器のサイバーセキュリティに対する考え方

1. IoTのセキュリティ対策は、ネットワーク全体、個々の対象機器、運用等、極めて幅広く影響が及ぶが、一律的な対策を避け、重要度や各機器の特性に応じたメリハリある対策を講じるべき。
2. 国境を越えるサイバー空間において、サイバー攻撃はグローバルに展開されるため、サイバーセキュリティ確保のためには、国際連携が不可欠である。また、市場のグローバル展開が加速しているなか、日本独自の施策、対応は市場の成長を損なう。国際的な基準や諸外国の制度とのすり合わせ、連携などによる取組みが必要である。
3. 今後、産業界としてもサイバーセキュリティ対策を自主的に推進することが重要と考える。また政府も、官民による検討の場を設けるなどして、サプライチェーン全体、国際的な動きを見据えた合理的な施策を検討頂きたい。

JEITAのサイバーセキュリティ対策

■IoT機器のサイバーセキュリティに関する自主的取組みについて

IoTの進展により、産業構造や社会構造が大きく変わりつつあるなか、当協会は、高度な情報活用による世界に先駆けた「超スマート社会」の実現(Society 5.0)に向け、異業種、ベンチャー、海外等とも連携し、新たなビジネスの創出に取り組んでいる。

IoTは社会のあらゆる分野に浸透しつつあり、これまで接続されていなかった機器が、インターネットに接続され、DDoSのようなサイバー攻撃等、新たな脅威が発生している。当協会では、セキュリティ対策が産業界共通の重要課題と認識しており、IoT推進コンソーシアム IoTセキュリティWG策定の「IoTセキュリティガイドライン」に沿い、IoT機器のセキュリティ対策に取り組んでいる。

今後、ユーザーにセキュリティの確保された製品を提供するために、当協会は所管するIoT機器について、取り組みの可視化も含めて具体的な自主的対応策を検討する。

なお、サイバー脅威は、DDoSのようなものに限られるわけではなく、様々なレベルのものがある。重要システムについては、サプライチェーン全体でサイバーセキュリティを確保する動きもあり、今後、国際標準も踏まえつつ官民で連携して検討することが必要である。総務省、経済産業省にも一層の対策をお願いしたい。