Joint OECD-EC conference on IoT, AI and product safetyにてスマートホームのサイバーセキュリティ確保に向けたあり方を提言

2018年11月14日（水）に欧州議会（ベルギー／ブリュッセル）にてIoT/AI時代の製品安全に関するOECD/EC合同の国際会議が開催され、JEITAよりスマートホーム部会 スマートホームサイバーセキュリティWG（主査：小松崎 常夫 セコム株式会社 顧問）が出席し、スマートホームにおけるセキュリティ対策確保に向けた活動を紹介しました。

会場となった欧州議会

IoT/AI時代における製品安全

IoTやAIといった新たな技術により、イノベーティブなビジネスモデルが多数生まれている中で、製品の安全の在り方についても大きな曲がり角に来ています。

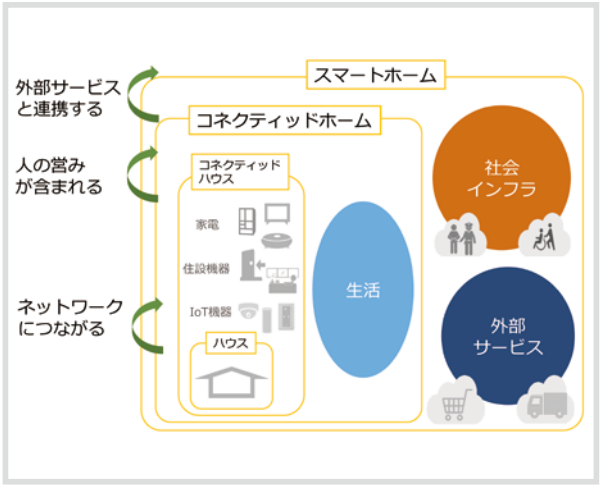
テクノロジーと政策展開のギャップを埋めていき、国際ハーモナイゼーションを確保する必要から、この度、OECD/EC（欧州委員会）合同にて国際会議が開催されました。当局からの要請により、スマートホームのセキュリティ対策確保に向けたJEITAスマートホーム部会で議論されている取り組みについて紹介しました。

JEITAが目指すスマートホームビジョン

「スマートホーム」というと、スマートフォンで家電を操作するようなイメージが想定されますが、JEITAスマートホーム部会が目指す「スマートホーム」は、住む人の“想い”や“わけ”に応える、新しい社会システムサービスのプラットフォームの構築です。

JEITAスマートホーム部会では、スマートホームビジョンを、以下の図の通り示しています。

【スマートホームビジョン】



住む家に、家電・住設機器・IoT機器といった様々な機器を導入し、単にネットワークにつなげるだけの状態は「コネクティッドハウス」としています。

この「コネクティッドハウス」に人の営みを入れ、人間中心に考えると「コネクティッドホーム」になります。

そして、「コネクティッドホーム」にさまざまな外部サービスや社会インフラまでをも含めて連携させ、限られた社会のリソースを共有し、社会の全体最適を促す家、これがJEITAが目指す「スマートホーム」となります。

スマートホームが設置される「家庭」の特性と特有の脅威

この「スマートホーム」が設置される「家庭」には以下のような特性と特有の脅威があります。

❶膨大な攻撃対象
（日本の世帯数はおよそ5300万世帯）

スマートホームを構成するシステムは世帯の数だけ存在し、セキュリティレベルは一部でも低いところがあれば、全体のレベルはその一番低いレベルになってしまう。

❷マネジメント不在に起因する脆弱性
（選定、設置、保守、破棄に対する妥当性のチェックが働きにくい）

家庭では、スマートデバイスの導入や利用に計画性がないことも多く、どんな機器をつないでいるか把握し、ファームウェア更新の保全をしているか等、運用をチェックする機構が働かない。

❸利用者側のリテラシー不足による
想定外のインシデント

家庭では、子供や高齢者等様々な人が暮らしており、誤使用によるインシデント発生の可能性があり、機器単体のセキュリティ対策だけでは不十分である。

会議においては、上記の特性を踏まえ、スマートホームという新たな社会システム構築のためには、従来型のサイバーセキュリティ対策では不十分であり、新たな枠組み構築に向けた活動を紹介し、具体的な産業界の取り組みとして高く評価されました。

スマートホーム部会において議論すべき論点

IoT/AIが搭載された製品が市場に出た時には、従来の製品の安全品質の確保に加えて、ソフトウェアのバグの可能性、また、それに伴う消費者の安全性の確保のための施策についても考えていく必要があります。

一方で、AI搭載の製品は黎明期にある状況であり、世界各国の規制当局はどのように政策展開できるか、また消費者への啓もうを如何に展開していくのかについて活発な議論も行われています。

AIやIoT技術は国境を越えて利用されているために、国際的な協力やチャレンジが必要であり、デジタル経済の安全性確保に向け、あらゆるステークホルダーが連携するための活動が活発化することが見込まれ、JEITAスマートホーム部会としても、安心・安全な社会を支えるための、官民一体となった製品安全・セキュリティ対策を継続して検討していきます。

会議の様子