IoT、無線とセキュリティ

Mike Violette
Washington Laboratories/American Certification Body

1. はじめに

この記事では、コネクテッドな世界（インターネットに常時接続された世界）を保護するための国際的、国内的な取り組みの概要を説明する。世界が複雑化してリスクがたかまり、さまざまな脅威にさらされるようになるにつれて、このような努力は永続的に続くと思われる。

2. 大西洋の向こうで（欧州）

EU（および英国）は、無線機器指令（RED：Radio Equipment Directive）に規定されている無線機器のセキュリティに積極的に取り組んでいる。電子機器に影響を与える多くの指令の1つであるこの指令には、ごく近い将来に制定される予定の特定条項がある。

メーカーと試験所（および Notified Body※1）は、RED の重要な条項を管理するための準備が必要である。

その必要性は明らかである。というのも、このコネクテッドな世界では、多くの IoT※2 機器がネットワークやその他デバイス、重要なインフラストラクチャに接続されているからである。そして IoT 機器は、インターネットのあらゆる方面からの攻撃に対して、ますます脆弱になってきている。例えば実際の仕事では、ほぼ全ての機器に無線機能が搭載され、Wi-Fi や Bluetooth、レーダー、センシング、その他の電磁波利用などあらゆる種類の IEEE 802.11 規格を実装している。

2021 年 5 月 10 日、悪質業者による Colonial Pipeline 社ハッキング事件が発生し、このような激動と困難の時代でもあり、米国連邦政府は緊急事態宣言を発した。このことは、業界の他の研究者が行った調査と相まって、ネットワークへの侵入が目新しいものではなく、インフラストラクチャが脆弱であることを示している。

他にも、世界中そしてサイバー空間全体に、驚くような事例が多く存在する。2021 年 4 月、New Yorker 誌は、銀行や企業などの機関から数 10 億ドルを搾り取る北朝鮮の国営ハッキングおよび恐喝作戦に関して、驚くべき暴露記事を発表した。北朝鮮政府は、継続的な取り組みとして有能なプログラマーを募集し集中的なトレーニングをした上で、ターゲットを絞った恐喝キャンペーンを実行し、プログラマーが成果を上げない場合は、家族や身近な人への脅迫など厳しい対応が待っているという。

そこで、ネットワークを守る方法について多くの業界で頻繁に議論が行われている。米国では、国立標準技術研究所（NIST：National Institute of Standards and Technology）がサイバーセキュリティリスクを管理する規格、ガイドライン、ベストプラクティスを使用して（連邦および民間産業レベルの両方の）組織にガイダンスを提供するサイバーセキュリティ・フレームワークを作った。現時点では義務化されていないが、連邦政府の購買ガイドラインにはいくつかの例外があり、知的財産の盗難やその他の信用侵害に関与した特定の企業からの製品取得が禁止されている。

構成に無線を追加すると、セキュリティという壁に生じたヒビが広がる。

現在、EU は無線機器のセキュリティ対策を実施しており、RED

[訳者注]
※ 1 . EU指令および規則に基づき適合性評価を行う機関
※ 2 . Internet of Things：モノのインターネット