JNSA ワーキンググループ紹介

IoT セキュリティ WG

リーダー：松岡　正人（日本シノプシス合同会社）

ソフトウェア開発におけるサプライチェーンと サイバーセキュリティリスク管理

2022年にEUがドラフト版を発行したCyber Resilience Act（以下CRA）が国内の製造業を中心に関心が高まっている。CRAは罰則規定付きであるだけでなく、EU域内に提供されるネットワーク接続可能な機器のソフトウェアの脆弱性管理とインシデントが発生した際の対処が要求される法案だからでCRA適合の有無が欧州ビジネスに大きな影響があるかもしれないからである。

一方で、すでに世界的に規制の始まった業界がある。ひとつは自動車業界で、UNECE（国連欧州経済委員会）の作業部会WP29（自動車基準調和世界フォーラム）が策定し、2020年6月に採択されたのがUNECE規則の「サイバーセキュリティ（UN-R155）」、「ソフトウェアアップデート（UN-R156）」である。EUは2024年7月にはすべての新車を対象にUN-R155とUN-R156の義務化を予定している。

いまひとつは、医療機器である。International Medical Device Regulators Forum（以下IMDRF）が2020年4月に最初のガイドラインを発行しており、厚生労働省はIMDRFサイバーセキュリティガイダンスの国内導入を進めており、日本語訳のガイドラインの公開などを2020年以降順次行っている。

これらの取り組みは、いずれの場合もサイバーセキュリティ対策の枠組みに、ソフトウェアサプライチェーンという考え方を取り込み、自動車や医療機器で用いられるソフトウェアの構成を把握し、リスク分析による適切なサイバーセキュリティ対策の選択と適用を製品のライフサイクル全体で考慮して実践できるようにすることを目指している。これらの取り組みに共通なのは、開発した製品に含まれるあらゆるソフトウェアコンポーネントの構成をソフトウェア部品表（Software Bill of Materials：SBOM）としてライフサイクルを通じて管理すること、製品の脆弱性を管理し当局に報告することが求められており、CRAでは報告の遅延などは罰則の対象となっている。そして運用する機器やシステムを駆動するソフトウェアの部品表に基づいたリスク分析によって、的確な対策がより早期に可能になると考えられるとしている。

そこで、IoTセキュリティWGでは「機器」のセキュリティの観点からこの課題について先行して取り組んでいるいくつかの団体から講師を招いてセミナーを開催した。

日本国内での産業界を跨いだ取り組みについては、経済産業省 商務情報政策局サイバーセキュリティ課課長補佐飯塚智氏にご説明いただき、自動車業界からは、一社）Japan Automotive ISAC 技術委員会委員長の山﨑雅史氏、医療機器業界からは、一社）電子情報技術産業協会 ヘルスケアインダストリ部会 医療用ソフトウェア専門委員会委員長の松元恒一郎氏、そしてSoftware ISAC OSS委員会副委員長の鈴木康弘氏の3名の方に各業界が直面しているソフトウェアサプライチェーンの課題を、規制のあらましや業界での対策や活動、インシデントの事例などをそれぞれの視点で解説していただいた。

最後に1時間少々のパネルディスカッションを実施したが、聴講者と講演者の間で活発な議論が行えたことは大きな収穫であったと思う。

プロアクティブなサイバーセキュリティ対策の手法として、これからソフトウェアサプライチェーンという考え方や取り組みが展開されていく際の課題や問題を浮き彫りにできたように思う。また、松元氏が「医療機器では患者の生命が最も優先される」と述べたように、業種や機器によって優先順位や目的も異なるであろうこと、セキュアなソフトウェアの提供に向けてITやOTだけでなく、ソフトウェア開発やソフトウェアのサプライチェーンについて、自動車ではサプライヤとの契約面も含めて考慮すべき事柄があるということを認識させてくれる良い機会となったと思う。

講演資料は以下のイベントページからダウンロードできるので、ぜひ読んでみていただきたい。

JNSA調査研究部会　IoTセキュリティワーキンググループ　主催
「日本におけるソフトウェアサプライチェーンとSBOMのこれから」
https://www.jnsa.org/seminar/2023/iot/index.html