

# 「IoTサプライチェーンのセキュリティ対策セミナー」を開催

総務省東海総合通信局(局長 吉武 久)は、令和元年10月29日(火)、ホテルメルパルク名古屋において、東海情報通信懇談会(会長 稲垣 康善 名古屋大学名誉教授)との共催により、「IoTサプライチェーンのセキュリティ対策セミナー」を開催し、通信、放送関係企業を中心に170名が参加しました。

当日は、情報セキュリティ大学院大学学長・教授で、政府のサイバーセキュリティ戦略本部員でもある後藤 厚宏氏より、「Society5.0の価値創造を支えるIoTサプライチェーンのセキュリティ対策」と題してご講演いただきました。

はじめに、「身代金」を要求する不正プログラムであるランサムウェアに感染した欧州企業からサプライチェーン経由で日本企業へ感染した事例や台湾の金融機関の海外支店がネットワーク侵入の切り口となった事例を紹介。生産・流通プロセス(サプライチェーン)は多くの事業者により構成され国をまたぐことも珍しくない。部品の製造・出荷、部品の組立、製品の出荷・流通、消費の各段階で最も脆弱な部分を狙って攻撃されるため、国レベルやシステムレベルでそれぞれのサプライチェーンで利用されるインフラの特性(新旧設備混在、大規模・広域の別等)を踏まえたセキュリティ対策が必要となっている。アジア、日本、米国、欧州では、ガイドラインの策定、技術の標準化や制度の検討がグローバルに進められていると紹介されました。

モノがインターネットにつながるIoT社会においては、脆弱性のあるIoT機器に対する攻撃が増えており、IoT車載器搭載の車がブレーキ不能で事故につながった事例も紹介されました。IoTリスクとサプライチェーンリスクは喫緊の課題であり、サイバー(仮想空間)とフィジカル(実空間)における両面でのセキュリティ対策を確実に実施し、製造、流通、構築、運用の各段階における「信頼チェーン」を構築、維持していくことが重要と力説されました。(別添参照)

参加者からは、製造業における海外の生産拠点におけるサイバー攻撃に対する具体的な対策や企業におけるセキュリティ人材の育成方法についての質問があるなど、関心の高さが伺えました。

お問い合わせ先: 情報通信部情報通信連携推進課

052-971-9313



情報セキュリティ大学院大学 後藤学長



セミナー会場の様子

