

# サイバー・サプライチェーン・セキュリティの法政策的研究

■ 社会環境学部 社会環境学科 准教授 橘 雄介

○ 研究分野：情報法、知的財産法、人権法

○ キーワード：情報セキュリティ、サプライチェーン・リスクマネジメント

## I 研究概要

### 1. 研究背景

近時、サプライチェーン(供給網)を利用したサイバー攻撃が相次いでいる。たとえば、直近では、米国や欧州の政府機関などで広く使われている SolarWinds 社のソフトウェア「Orion」への攻撃が世界に衝撃を与えた。攻撃者は、まず、SolarWinds 社のネットワークに侵入し、Orion に悪意のあるソフトウェアを注入した。次に、顧客がそのソフトウェアをダウンロードし、攻撃者が顧客のネットワークに侵入可能となった(同種の事件として、富士通 ProjectWEB 事件)。サプライチェーンの弱いところが狙われているのである。

### 2. 研究内容

サイバー・サプライチェーン・セキュリティとは情報及び運用技術(IT/OT)に関するサプライチェーンのセキュリティ確保の取組みを指す。サプライチェーンの情報セキュリティ水準については、従来、どのようなセキュリティ対策を実施するかを事業者委ねるアプローチが採用され、一律の義務が課されているわけではなかった。このような中、「任意のアプローチからの転換」を目指しているのが米国である。米国は国防事業について、従来、セキュリティ対策について請負人が自ら履行を申告することのみが求められていたのに対して、近時、これを第三者機関による認証の対象とした(Cybersecurity Maturity Model Certification: CMMC)。他方で、こういった「アクセル」に対して「ブレーキ」のあり方が問題となっている。すなわち、サプライチェーンから排除される事業者をどうするかという問題である。

本研究では「アクセル」と「ブレーキ」のバランスを法学、法政策及び実務の観点から探求するものである。たとえば、セキュリティ水準を高くしすぎて、中小事業者などが対応できず、官公庁の入札やサプライチェーンから排除されてしまえば元も子もない(そうでなければ、一部の企業の寡占を招き、消費者に害悪となる)。そこで、この競争的なサプライチェーンという観点から我が国の政策を提言する。また、社会実装(実務)としては中小事業者も履行可能なガイドラインの整備を提言する。

### I 利点特徴

- ・IT機器などについて**安全な**サプライチェーンの構築へ寄与する
- ・中小事業者なども参入可能な、**競争的な**サプライチェーンの構築へ寄与する
- ・欧米の動向も踏まえ、**国際的な**サプライチェーンの構築へ寄与する

### I 応用分野

私は日本企業が直面するサプライチェーンに関する法的・政策的・実務的課題を研究しており、本研究もその一環である。そのため、本研究は以下の分野に応用可能である。

- ・サプライチェーン・リスクマネジメント
- ・営業秘密の保護
- ・消費者の保護(情報漏洩の防止や製造物責任の回避など)

