第32回公開シンポジウム 基調講演

産業分野におけるサイバーセキュリティ政策

Cybersecurity Policy for Industry Sector in Japan

鴨田 浩明

Hiroaki Kamodai

経済産業省 商務情報政策局 サイバーセキュリティ課 企画官
Ministry of Economy, Trade and Industry

第32回公開シンポジウム「統一論題：Society5.0 実現に向けた課題と展望—サイバーフィジカルシステムと監査—」の基調講演として、経済産業省の鴨田 浩明氏に、「産業分野におけるサイバーセキュリティ政策」と題してご講演をいただいた。

産業分野のさまざまなシステムにおいてサイバーセキュリティの脅威が増大する中、経済産業省が取り組んでいる政策を中心に話をいただいた。鴨田氏の講演要旨を以下に報告する。

1. サイバー攻撃の動向

世界経済フォーラムが発表している『グローバルリスク報告書2019』によれば、リスクの発生可能性のランキングで、“サイバー攻撃”および“データの不正利用または窃盗”が、“自然災害”や“異常気象”と並んでトップ5に入っている。

また、IPAが発表している『情報セキュリティ10大脅威2019』では、“ランサムウェアによる被害”、“IoT機器の脆弱性の顕在化”などは毎年のように入っているが、2019で初めて“サプライチェーンの弱点を悪用した攻撃の高まり”がいきなり第4位に入った。産業分野のシステム環境は、クラウド利用も含めてグローバルなサプライチェーンを組んでいるものが多く出現しており、日本国外で発生したサイバー攻撃の影響が日本国内の企業のシステム環境に及ぶ例も発生している。

IoTの進展に伴う脅威の拡がりも深刻である。自動車、航空機、監視カメラ、ドローンなどさまざまなIoT機器が繋がるようになり、そうした機器を通して産業分野のシステムにサイバー攻撃が

加えられるリスクも大きくなっている。

リスク（脆弱性）の発生件数も増大しており、致命的な脆弱性だけで平均して1日に5～6件新たに見つかっているという報告もある。

2. 産学官の検討体制の構築～産業サイバーセキュリティ研究会

最近のサイバー攻撃の動向を踏まえ、産業分野のシステム環境での対策を検討する目的で、経済産業省主導で産学官の代表で構成する「産業サイバーセキュリティ研究会」を立ち上げ、2018年12月から活動を開始した。

アクションプランとして、サプライチェーン強化パッケージ、経営強化パッケージ、人材育成・活躍推進パッケージ、およびビジネスエコシステム創造パッケージの4つの柱を提示し、アクションプランを実現するためのワーキンググループ(WG)を3つ設けた。WG1がサプライチェーン強化パッケージを、WG2が経営強化パッケージと人材育成・活躍推進パッケージを、WG3がビジネスエコシステム創造パッケージを検討することとし、活動を進めている。さらに、アクションプランの実現を加速化する3つの指針として『グローバル』をリードする、『信頼の価値』を創出する、『中小企業・地域まで』展開する、を提示した。

3. WG1:「Society5.0」において必要なセキュリティ対策～サイバー・フィジカル・セキュリティ対策フレームワークの策定

WG1の取組みの一つは『サイバー・フィジ

カル・セキュリティ対策フレームワーク』(CPSF)の策定である。“Society5.0”でのサプライチェーン構造の変化として、データの流通・活用を含む、より柔軟で動的なサプライチェーンの構成が可能となる。一方、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要となる。この状況に対応するためのモデルとして、CPSFでは三層構造(企業間のつながり、フィジカル空間とサイバー空間のつながり、サイバー空間におけるつながり)と6つの構成要素(ソシキ、ヒト、モノ、データ、プロシージャ、システム)で構成されるモデルを提示した。CPSFで提示している標準モデルおよび対策フレームワークを基に産業分野ごとの個別セキュリティガイドラインを策定すべく、ビル、電力、防衛産業、自動車産業、スマートホームの5つのサブWGが活動を行っている。

4. WG2：サイバーセキュリティ対策の基盤整備～経営、人材育成、中小企業

CPSFは、Society5.0における産業社会でのセキュリティ対策の全体的枠組みを提示した。WG2ではその全体的枠組みに沿って、対象者や具体的な対策を整理し、次のような取組みを行った。

- 以前からあった経営者向けの『サイバーセキュリティ経営ガイドライン』の改訂版としてver2.0を発表し、経営者がリーダーシップをもって取り組むことを認識すべき三原則と、経営者がサイバーセキュリティ対策の実施責任者となるCISO等に指示すべき重要10項目を提示した。
- 『サイバーセキュリティ経営ガイドラインver2.0実践のためのプラクティス集』を作成し、企業における具体的な取組事例を紹介した。
- 中小企業に対する具体的支援として、事前支援策としてIPAが中心となつての『中小企業の情報セキュリティ対策ガイドライン』の作成、「セキュリティアクション自己宣言」(現時点で約8万社超が宣言)、情報処理安全確保支援士等による対策支援を実施している。また、事後支援策として「サイバーセキュリティお助け隊」によるセキュリティ対策についての相談対応、事故発生時の復旧対応等を行うとともに、中小企業向けのサイバーセキュリティ保険のあり方について検討を行っている。

• IPAの中に「産業サイバーセキュリティセンター(ICSCoE)」を設置し、IT系・制御系に精通した専門人材、サイバーセキュリティ経営を進める戦略マネジメント層の育成に取り組んでいる。サプライチェーンは海外企業にも拡大していることから、ICSCoEと米国の専門家による制御システムのサイバーセキュリティに関する演習を、インド太平洋地域向けに14の国と地域が参加して2019年9月に実施した。来年以降も実施を計画している。

5. WG3：サイバーセキュリティビジネスの創出～エコシステムの創出

「情報セキュリティサービス審査登録制度」をスタートした。一定の品質を維持・向上するための要件を定めた『情報セキュリティサービス基準』を策定し、基準に適合するサービスを提供する企業のリストを審査登録機関およびIPAから公開する仕組みである。『情報セキュリティサービス基準』には情報セキュリティ監査サービス、脆弱性診断サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービスの4つのサービスに関する基準が定められており、2019年9月現在、合計119のサービスが登録されている。

この後、会場からの質問に丁寧に回答していただき、鴨田様の講演は終了した。

私にとって、産業分野の事業活動におけるサイバー攻撃の脅威、脅威を抑え込むための経済産業省主導の多様な取組みについての話が伺え、非常に有意義な講演であった。

(小野 修一 記)
(2019年10月25日開催)