工場システムのサイバーフィジカルセキュリティ

◆活発化するサプライチェーン攻撃

2023年2月、IPA（情報処理推進機構）は情報セキュリティ10大脅威2023を公開した。この資料では、22年に発生したセキュリティ事故や攻撃の状況から選出された脅威が順位付けされている。企業組織の立場から見た脅威では、「サプライチェーンの弱点を悪用した攻撃」が13年から2位以上を維持していた「標的型攻撃による機密情報の窃取」を抑えて2位に順位を上げた。なお、1位は「ランサムウェアの被害」である。サプライチェーンは商品の企画から、調達、製造、在庫管理、物流、販売まで一連の商流に関わる組織群を指す。サプライチェーンの脆弱性を突いたサイバー攻撃では、攻撃者はセキュリティが堅牢な大企業を直接狙わず、その企業と業務上や製品調達上の関係があり、かつセキュリティが脆弱な企業（調達先、業務委託先、協力企業の子会社、海外拠点）を最初の標的とし、そこを踏み台として顧客や上流プロセスの関連企業の本命の標的を攻撃する。対策として、自組織だけでなく、調達先、業務委託先など取引先を適切に管理することが重要になる。具体的には、情報管理規則の徹底、インシデント発生時の情報セキュリティ上の責任範囲の明確化、定期的にセキュリティ対策状況と情報資産管理の実態の把握を契約に取り込むことが有効である。

◆各国で強化される産業サイバーセキュリティ政策

22年に日本の大手企業がサプライチェーン攻撃によって被害を受けた事例を表1に整理した。どの事例も海外拠点、子会社など、セキュリティが脆弱な企業がランサムウェアとみられる被害を受けたことが起点となって、最悪、工場の生産停止にまで被害が拡大した。サイバー空間（仮想世界）の攻撃がフィジカル空間（現実世界）に影響を及ぼすようになっている。こうした状況を踏ま

表1 サプライチェーン攻撃を受けた事例（ARCまとめ）

時期	企業名	概要
2022年 2月	ブリヂストン	南北アメリカ地域の事業統括会社で被害。ITシステムを遮断した影響で生産に一時支障。
	小島プレス工業	子会社のネットワークを起点に不正侵入され、システムに障害が発生。取引先のトヨタ自動車などの生産が一時停止。
3月	デンソー	ドイツの現地法人が被害。データを暴露される。
	森永製菓	社内サーバーに不正アクセスあり。製造ライン支援システムが被害に遭い、生産に影響が出た。
4月	パナソニック	カナダ子会社が被害。データを暴露される。

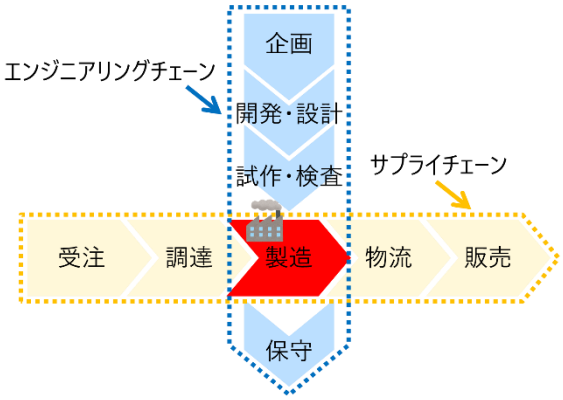

図1　製造を中心とするスマート製造（ARC作成）

え、産業分野のサイバーセキュリティ強化に向けた取組が各国で加速している。

今後も産業分野のDX推進でデジタル化の流れは止まらず、サイバー空間とフィジカル空間の融合は進む。そして、サイバー・フィジカル融合によりデータの流通・活用の自律的なサイクルが構成され、市場動向リスク、地政学リスク、災害リスクの外部環境に起因する需要変動に対して柔軟かつ動的に追従できるスマート製造が可能になる。スマート製造では、製造（スマート工場）を中心としてエンジニアリングチェーンとサプライチェーンの情報を統合し、複雑化する事業環境に柔軟に対応することで事業プロセス全体の付加価値向上を図る（図1）。スマート工場では、生産性向上を目指したデジタル技術の活用が進み、IoT化、OT（Operational Technology）機器の自動化によって、さまざまなデバイスが工場ネットワークに接続する。これは、工場内のデジタル資産というサイバー攻撃対象の増加と、外界とのネットワーク接続という侵入経路の増加につながるため、外部からサイバー攻撃を受けるリスクが高まっていく。

◆スマート工場の土台を支えるサイバーセキュリティ対策

22年11月、経済産業省は工場システムのセキュリティ対策ガイドラインを発表した。米国や欧州を始めとして、工場の製品や製造プロセスに関わるセキュリティ対策を要求する取引先や製品ユーザが増えてきており、その基準となる標準規格が整備されつつある状況の下、本ガイドラインは海外規格と整合性の取れた日本のスタンスを示した形となっている。

今後、スマート工場の工場システムは5G、ローカル5Gの情報通信技術でロボットの自動化技術を活用した設備やセンサなどのIoT機器とつながるだけでなく、情報システムやインターネットと接続し、他事業所・他拠点と連携する機会が増えていく。同時に、サイバーセキュリティの担う役割はより大きくなる。サイバーセキュリティ人材は一日にして成らず。社内での継続的なサイバーセキュリティ人材の育成や確保が求められる時代になってきた。　【永田紘基】