サプライ&デマンド・ネットワークにおけるサイバーセキュリティ

JNSA 会長　江﨑　浩

1. サプライ“チェーン”からサプライ＆デマンド“ネットワーク”へ

旧来型の産業構造は、製品を需要家に提供するOEM（Original Equipment Manufacturer）をトップのルート（根）とする排他的なツリー構造のサプライチェーン（＝製品の流通ツリー）を形成していましたが、このような構造は崩壊し、ツリーに属する企業は、多数のOEMツリーに同時に属するように変化・進化しました。さらに、ツリーに属する企業は、多様な“産業”のOEMツリーに属するように変化することになりました。これは、単純な排他的なツリー構造から、ネットワーク型の流通形態へと変化・進化したのです。複数のOEMを出口とするネットワーク内の関係企業が要求する“多様な”サイバーセキュリティのレベルと仕様・統治を各企業は満足しなければならないことを意味します。

2. 紛争や戦争が明らかにしたサプライチェーンの脆弱性

2022年2月に始まったロシアによるウクライナへの侵攻は、現実の戦場での戦闘と並行して、サイバー空間における攻撃が活発に行われた事例として捉えることができます。政府機関や重要インフラなどがサイバー攻撃の標的となり、DDoS攻撃、マルウェア攻撃などが観測されています。サイバー攻撃は、物理的な破壊を伴わないものの、国家・経済・社会の活動を麻痺させることができます。サイバーセキュリティは、企業のみならず、国家安全保障の根幹に関わる重要な課題として捉え、その能力を強化する必要性を強く認識させる契機となりました。各企業の活動も、グローバルなサプライチェーン（正確にはサプライネットワークを形成している）の上に構築されていることが、2020年に発生したコロナ禍が証明し、ウクライナ侵攻によって、グローバルに展開されたサプライチェーンの中のどこかが、サイバー攻撃やサイバーインシデントを含む何らかの原因で機能しなくなることで、甚大で広域に渡る経済損失が発生することが実感・体験されることになりました。

3. データの信憑性と適切なデータ利用

人工知能（AI）の利用が急進展していますが、AIが適切・正確に動作するためには、“正しい”データがAIに提供されなければなりません。データ詐称は、AIへの致命的な誤動作を誘導します。データ詐称は、意図的ではないものと、意図的な攻撃とが存在します。しかも、このAIが利用するデータは、サプライチェーン上で伝搬させられ、各企業・組織で利用されるのです。すなわち、正確なデータの流通と共有が、サプライチェーン上のすべてのステークホルダ組織で実現されなければならないのです。このような環境を実現するために、さまざまなガイドラインや検査／検証システムが作成されています。

4．デジタルツインを基にしたサイバーファーストとロボット前提（OTセキュリティ）

現実世界のすべてのシステムの構造や動き・振舞いがデジタル世界で完全にコピー（Digital Twin）され、さらに、各システムがネットワーク化されることで、デジタル空間（サイバー空間）上に、すべてのシステムが統合化可能なデジタルシステムが構築されることになります。このような、インフラの実現には、「Stove-and-Pipe」と呼ばれる「垂直統合型のサイロ（silo）型のシステム・事業構造を“De-Silo-ing”して、水平統合型あるいはマトリックス型の構造に移行（Migration）させることを目指さなければなりません。

5．AI（人工知能）

人工知能は、システムの運用、さらに設計においても大きな役割を持つように変化し続けています。

(1) サイバー攻撃への防御

サイバー攻撃の検知（と対策）のために、ビッグテックにおいては、スマートNICの導入などを行い、サイバー攻撃のトラフィック解析や、トラフィックの監視・解析による感染の検出を行っています。また、近年では、①各機器の設定情報を用いたAttack Surface Detectionによる未然の攻撃防御（＝ACD; Active Cyber Defense）、あるいは、②LLMを用いた多数の監視ツール群の統合化など、人工知能を用いたサイバー攻撃のReactiveな攻撃防御とProactiveな攻撃防御が広く実装されつつあります。

(2) 稼働状況の把握と管理制御

システムの効率的運用を実現するために、人工知能を用いたデータ駆動型の管理・制御も急速に導入されつつあります。各導入機器の健康診断（＝①故障の予知、②稼働効率）だけではなく、システム全体の健康診断をLLM、さらにLMM（大規模マルチモーダルモデル）を用いて実現する挑戦です。

6．むすび

“サプライチェーン”は、“サプライ&デマンドネットワーク”へ進化、さらに各企業の生産システムおよびすべての機器は、インターネットにCONNECTEDな状況にあることを前提としなければならない状況になり、したがって、“ゼロトラスト“サイバーセキュリティを適用すべき環境にあると認識しなければなりません。Dis-Connectedにしているので大丈夫ということは、事実上存在しない状況にあるのです。疎結合型のオープンアーキテクチャで形成される各データ空間（Data Space）間でのサイバーセキュリティ対策が必須となります。