資料8

我が国のサイバーセキュリティ政策の今後への提案

慶應義塾大学
村井純

１．サイバーセキュリティに「ロボット」を対象とした領域を加えるべき

企業や組織、個人が攻撃されるというモデルに加えて、インフラの制御システム、無人運転のドローンや自律運転の車やロボットなど、従来「IoT のサイバーセキュリティ」として狭義に捉えられていた、スマート化されたシステムが攻撃されるというモデルも考え直さなければならない。これらの技術は社会の中に急速に展開し始めている。しかし、これらがサイバーセキュリティの主戦場として捉えられてはいない。この体制整備は急務である。

２．デジタル国家推進においてこそ、サイバーセキュリティがコア政策であるとの位置づけを明確にする

DX の対象がすべての産業領域に拡がり、地域的にも全国への拡がりを前提とすると、サイバーセキュリティ政策の対象は、行政や産業の分野を横断する水平的な守備範囲を確実にしなければならないことに加えて、国全体の垂直的な守備範囲も重要となる。このような「サイバーセキュリティ全体構造」を担う政策的な責任と役割を明確にする必要がある。また、その考え方が、国土全体と国民を守り、発展する DX 政策を先導する。

３．AI の具体的な展開を視点としたサイバーセキュリティ政策のあり方

デジタルデータを利用し、全国に分散する学習としての計算拠点があり、推論を担う機能がすべてのデバイスに組み込まれる、というのが AI を前提としたサイバー空間のインフラ構造である。安全なデータの共有、安全なデータの利用から、停止しないデジタルインフラサービスこそが、サイバーセキュリティの新しい責任のモデルである。サイバーセキュリティ政策の戦略は AI を前提とした新しいコンピュータ・アーキテクチャに基づいて発展する必要がある。

４．グローバルに通用するサイバーセキュリティ標準化技術への積極的な役割と先導性の発揮

サイバーセキュリティの適切な整備と運用は、バラバラに提案される手法を導入して追従するだけでは、膨大な初期費用と運用コストがかかる。この問題を解決するのが正しいグローバル標準技術の確立と発展である。標準技術によるセイバーセキュリティの整備は低コストで安全な運用を可能とする。PQC（量子コンピュータの出現により弱体化する現用暗号の次を担う暗号技術）など、サイバーセキュリティに関する技術は世界で標準化が提案され検証されている。このような技術体系が共通の標準化として広く使われるための国際的な協力と、標準化技術プロセスへの積極的な参加、先導的な役割を果たせるための戦略的アプローチを考える必要がある。