FERI INFORMATION

経済安全保障とサイバーセキュリティ及び量子技術に関する所見

渡辺 秀明
（SBI 金融経済研究所顧問 / 前防衛装備庁長官）

本年 2 月、ロシアはウクライナに対し軍事侵略を開始した。国際法に違反する暴挙であり、自由民主主義陣営（日本を含む西側諸国）は、SWIFT（国際銀行間通信協会）からのロシアの排除を始め、幅広い分野で制裁措置を導入した。経済安全保障が急激にクローズアップされたわけである。また、ロシアは、明確な意思表示は示していないが、経済制裁への報復措置として西側諸国へのサイバー攻撃を強めている。我が国も例外ではない。松野博一官房長官は 3 月 1 日午前の記者会見で、「ウクライナ情勢を含む昨今の情勢からサイバー攻撃のリスクは高まっている」として、企業などに注意を呼びかけた。

バイデン米大統領は 3 月 21 日、声明を発表し、米国などが「ロシアに前例のない経済的代償を負わせた」ことを受けて、ロシア政府がサイバー攻撃を仕掛ける可能性があると警戒を呼び掛けた。こうした現下の情勢を踏まえ、日本政府は、3 月 24 日、政府機関や重要インフラ事業者（金融機関を含む）をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めると共に所要の措置を講ずるように呼びかけた。

このような中、我が国では折しも、経済安全保障が新たな日本政府の方針として示され、経済安全保障推進法案が今国会にて審議されている。この法案の目的は、一言で述べると経済と安全保障を共に強化することである。従って、その法案では、以下の4つの柱が示されている。

1. サプライチェーンの強靭化
2. 基幹インフラの安全性・信頼性の確保
3. 先端技術開発の促進（官民技術協力）
4. 非公開特許制度の確立（国家安全保障上機微な先端技術の流出防止）

このうち、基幹インフラの安全性・信頼性確保の要は、サイバーセキュリティ対策の強化であり、現下の状況を乗り越えるためにも大変重要な施策である。

先端技術は近年、安全保障及び経済（産業競争力）の観点から、米国、中国、欧州を中心として、大規模な予算が計上され、急速に強化が図られている。具体的には、先端技術のうち、量子技術、AI（人工知能）、自律化技術（ロボット・自動運転等）、バイオテクノロジー、宇宙、サイバーなどが注目を集めている。

ここでは、4 つの柱のうち、2 番目の「基幹インフラの安全性・信頼性の確保」及び 3 番目の「先端技術開発の促進」の双方に関わる量子技術を例として説明したい。

量子コンピュータの研究について、米国ではグーグル、IBM などの民間会社を中心として研究開発が進んでいる。2019 年にグーグルが発表した量子超越性は、防衛のみならず、社会全体に大きな衝撃を与えるものであった。量子超越性とは、プログラム可能な量子デバイスが、どの様な古典コンピュータでも実用的な時間では解決できない問題を解決できることを、問題の有用性に関係なく証明することである。グーグルは、独自に開発した量子コンピュータが、スーパーコンピュータが 1 万年かかる計算をわずか 200 秒で解いたとし、量子超越性が証明されたとしている。

中国では、約1兆円かけて 2017 年に設立した量子技術に関する国家研究機関（合肥市）を中心として研究が進められている。2020 年 12 月、中国科学技術大学は光子を用いた量子コンピュータ「九章」が、世界最速（当時）のスーパーコンピュータである富岳では 6 億年かかる計算を 200 秒で実行したと発表し、中国が米国に次いで量子超越性を達成したと主張した。

量子コンピュータの実現は、4～5 年前からサイバーセキュリティの問題としても、にわかに脚光を浴びるようになってきた。NIST（米国立標準技術研究所）が、世界中で広く用いられている RSA 暗号（公開鍵暗号方式）が、量子コンピュータの実現により、無力化される恐れがあるため、2030 年までに新しい暗号システムに乗り換える必要があると発表したことが背景にある。

各国は、新しい暗号システムに真剣に取り組んでいる。 我が国は、東京大学、NICT（情報通信研究機構）、NTT 等関連企業を中心に、新しい暗号として、量子鍵配送方式（QKD:Quantum Key Distribution）に関する研究を 30 年以上前から取り組んでいたが、近年、中国の研究グループに実用化研究で一歩先を越された状況にある。これを受け、今般政府は、経済安全保障の目玉として、QKD 事業への本格的な支援を決めた。

しかし、米国では、日本や中国が取り組む QKD ではなく、耐量子暗号（量子コンピュータによって解析できない暗号）が、次世代公開鍵暗号として最適であるとして、NIST により標準化作業が進められている。また、暗号に関し、世界的に最も権威のある機関として有名な NSA（米国国家安全保障局）は、「安全保障の観点から QKD を（現時点では）採用すべきでない。」と結論づけている。同様の判断が、英国及びフランスの国家サイバーセキュリティの専門機関によってなされており、QKD は欧米の政府機関から否定された格好となっている。日本政府としても、QKD の国際的な立ち位置を十分に認識し、米国等と情報交換を十分行いながら、我が国が取るべき方策を検討していく必要がある。

ウクライナへのロシアの進攻に伴い、冒頭でも述べたように世界中でサイバー攻撃が蔓延し日本の企業が被害に遭うことも多くなってきている。金融ネットワークも例外ではない。日本政府は、サイバー攻撃に対する警告を発信するだけではなく、国家として何か抜本的な対策を講じる必要

がある。参考ではあるが、米国や欧州各国は、サイバーセキュリティの拠点を有しており、教育・研究さらにサイバーインシデント対応も行われている。日本がサイバーセキュリティの教育研究拠点を整備するのであれば、サイバーセキュリティと関連の深い量子技術及び AI との研究と合わせて整備することで、よりシナジー効果が発揮できる拠点構築が可能となろう。

本年は、国家安全保障戦略の見直しを行うことを岸田総理は再三発言しているが、経済安全保障について、もう一段踏み込んだ施策の実現のため、先端技術として、量子技術、AI、サイバーセキュリティに関する抜本的な制度や組織の見直しを行うことは重要である。