2024 年 8 月 30 日

「経済安全保障の時代における情報セキュリティ」シンポジウム事務局
日本アイ・ビー・エム株式会社
公益財団法人日本国際問題研究所

「経済安全保障の時代における情報セキュリティ」シンポジウム　報告書

1. シンポジウム概要

2024 年 8 月 28 日（水）、霞山会館(東京都千代田区)において、日本アイ・ビー・エム株式会社と公益財団法人日本国際問題研究所の共催により、「経済安全保障の時代における情報セキュリティ」シンポジウムが開催された。

2. オープニング対談：経済安全保障の時代における情報セキュリティ

本対談では、昨今の経済安全保障情勢に関する情勢認識について意見交換が行われた。経済安全保障リスクの高まりの要因として、デジタル・トランスフォーメーション（DX）の進展が指摘された。行政、医療、教育を含む社会全体が電子制御社会へと移行するに伴い、情報窃取に要する労力が大幅に減少し、その結果として社会の直面するリスクが飛躍的に増大している。また、この状況は、データを取り扱うデバイスを構成する半導体の国内生産能力の強化が必要とされる背景にもなっている。ＤＸ、半導体戦略、経済安全保障は密接に関連しており、これらを体系的に法制化したのは世界で日本が初めてであるとの認識が示された。

官民連携では信頼関係の醸成が不可欠であるが、そのためには、企業側がインシデント情報を報告する利点を感じられる仕組みなどが必要であり、報告窓口のワンストップ化や報告に対して適切な助言が得られる環境を整備することなどが挙げられた。経済安全保障は経営リスクになりうるものであり、リスクを最小化しつつビジネス成長を実現するためには、産官学連携による課題や解決策のオープンな議論が重要であることが共有された。

3.　セッション１：地政学的視点

　経済安全保障政策の究極の目的は、日本の経済成長の持続・強靭化であり、そのために諸政策が位置付けられていることが整理された。また、米中間の技術覇権競争が激化する現状を踏まえ、経済インテリジェンスの観点から、最先端技術に関する国内外の状況を収集・分析し、他国から情報を得るのみならず、相手国が求める情報を提供できる体制を構築することの必要性についても示された。

　上記背景のもと、政府側からは、不十分な政策で課題を解決できないことがないよう、積極的な施策が必要であるとの考え方が示されるとともに民間企業に対しては、経済安全保障を国からの規制に基づいて実行するものと捉えるのではなく、自ら危機意識を持ち対応すべきとの議論がなされた。リスクの例としては、サプライチェーンの単一供給源への依存やコア技術のみならず周辺技術が他国に奪われ市場を席巻される可能性が挙げられた。

　民間企業からは、「事業」視点で日本の仕組みを比較し、技術開発における産学連携の希薄さや選択と集中といったガバナンスが適切に行われていないこと、産業界からの提案力の欠如と社会実装の低調さなどが課題として挙げられた。

　こうした問題を解決するため、日本全体として、官民で合意された一貫した経済安全保障戦略の明確化が必要であるとの認識が示された。さらに、官民の役割分担の考え方にも再検討が必要であるとの意見が示された。研究開発から事業化に至るパイプラインをシームレスにつなぐため、従来の役割分担論から相互に一歩踏み出した関係性が必要であるという意見や、分担というコンセプトを超えて、「大きな目的を共有した上で、それぞれが持ち場で最善を尽くす」というより踏み込んだ協働のコンセプトへの転換が必要であるとの意見が示された。

4. セッション２：技術的視点

冒頭、各企業の経済安全保障の取組が紹介された。経済安全保障推進法や外為法などの法令順守を基盤としつつ、さらに踏み込んだ対応として、自主的なリスクチェックや中立機関のオーディットの受入、社内の疑似攻撃部隊（レッドチーム）による模擬訓練、スパイ行為を持ちかけられた場合の窓口設置、社員向け教育の徹底や違反時の解雇規程まで含む誓約書への署名等の措置・事例が説明された。

経済安全保障やサイバーセキュリティに関わる業界全体の対応例として、金融業界における耐量子計算機暗号対応の推進事例が紹介された。技術的・資金的に恵まれた大企業だけでなく、中小企業も含めたエコシステム全体で防御体制を強化する必要があり、業界および監督当局が一体となって対応が進められている事例が説明された。

官民連携の具体的なあり方と課題について、サイバーセキュリティ分野では、実際のインシデントの情報共有が他者の役に立つケースは稀でないかということ、したがって真にアクショナブルな情報共有は何かを現場の意見を聞いて定めることが必要であるとの認識が示された。官民対話の重要性については、官民双方の立場から指摘され、非公式な場を含めた情報交換を通じて、課題を共有しリスクマネジメントに対する官民の認識を相互に理解することが、国家的な戦略目標を共有し協働していく上で必要と認識された。

また、今後の経済安全保障を考えていく上で、データ保護の重要性が指摘された。先ずは、日本として真に保護すべき情報やデータの特定が必要である。企業側でも個人情報など法令で定められたデータの取り扱いは徹底されているが、経済安全保障の文脈での洗い出しは依然として不十分であり、今後そのような議論が必要であるとされ、要すれば現行の法制議論に追加すべきとの議論が行われた。

会場からは、耐量子計算機暗号の対応推進の必要性について質問があり、パネリストからは、米国が標準化や国策としての対応を進めている現状を踏まえ、実際の対応には時間を要することから、将来の追加コストを最低限に抑えるためにもリスクアセスメントと対応計画の立案は迅速に着手すべきであるとの回答がなされた。

最後に、デジタル技術の発展と国際政治上のリスクの高まりが重なり、社会構造の全体的な建直しが進む中、民主的アプローチと中央集権的アプローチが各国で各々進展しているとの認識が共有された。民主的アプローチでの建直しを日本が推進すべく、様々な産学官の対話が継続されるべきであるとの意見で締めくくられた。