経済安全保障とサイバーセキュリティ

大澤淳

はじめに

経済安全保障推進法案の検討がいよいよ大詰めを迎えつつある。2021 年 11 月 26 日に始まった内閣官房の「経済安全保障法制に関する有識者会議」は、計 4 回の全体会合と計 8 回の分科会会合（4 分科会で各 2 回）の討議を終え、22 年 2 月 1 日に「経済安全保障法制に関する提言」を発表した。提言では、地政学的な緊張が高まる中、科学技術・イノベーションが国家間の覇権争いの中核になっている、という問題意識の下で、①サプライチェーンの強靭化、②基幹インフラ機能の安全性・信頼性の確保、③官民技術協力、④特許出願の非公開化、の四分野について政策対応や立法措置の枠組みの方向性が示された。

本稿では、このような「経済安全保障」の概念が、2018 年以降急速に注目されるようになった国際政治上の背景を第 1 項で、サイバー空間における経済安全保障上の課題を第 2 項で、サイバーセキュリティ確保を含む経済安全保障法制議論の推移と課題を第 3 項で取り上げる。

1　経済安全保障のナラティブ（国際政治上の背景）

経済安全保障を巡る議論が、2019 年以降日本国内で急速に進んだ背景には、国際政治上の大きな構造変動があり、その文脈で経済安全保障のナラティブを理解する必要がある。

第 2 次大戦後の国際政治では、米ソの冷戦が 1946 年から 1989 年（ソ連崩壊の 91 年とする場合もある）まで約 40 年間継続した。冷戦の特徴は、ソ連を中心とした社会主義体制と米国を中心とした民主主義自由経済体制間の、いわゆる生き残りをかけた「体制間競争」であり、経済論理よりも安全保障の論理が優先された。この「体制間競争」の認識は、西側では 1946 年 3 月の英国のウィンストン・チャーチル首相（演説は首相退任後）による「鉄のカーテン演説」と、米国のジョージ・ケナン（当時註ソ臨時代理大使）による「長文電報」により象徴的に形成されており、ケナンの「長文電報」は後にフォーリン・アフェアーズ誌に著者名を伏して「X 論文」として掲載された。

1989 年に冷戦が終焉してから 2019 年頃までの約 30 年は、ソ連の崩壊による米国一強体制の成立と、2008 年のリーマンショックを境目とした多極化の時代に分けることができる。この時代は、国際政治上の大きな緊張が解け、安全保障の論理よりも経済の論理が優先され、ヒト・モノ・カネが活発に国境を越えて自由に移動するグローバリゼーションが特徴であった。

しかし、このグローバリゼーションの時代が、中国の台頭と共に終焉を迎えつつある。エコノミック・ステイトクラフトや貿易管理の厳格化などのいわゆる「経済安全保障」を巡る議論が諸外国で活発化してきたのも、中国の台頭により、再び国際政治が「体制間競争」に向かうというナラティブが形成されているからである。中国を競争相手と認識し、冷戦期のような「体制間競争」が再び起こるとの認識の変化の潮目となったのは、2018 年 10 月に米国のペンス副大統領（当時）がハドソン研究所で行った対中戦略演説である。同演説でペンス副大統領は、中国が政治、経済、軍事的手段とプロパガンダを用いて米国に対する影響力と干渉を強め、人権や宗教でも自由を抑圧しているとして、中国との長期戦を覚悟し、経済・戦略的関係をリセットすることを示唆した。演説後、ペンス演説は米中新冷戦の開始を暗示する、とメデ

ィアでは評価がなされている。

さらに、2021 年には、冷戦期のケナンの「長文電報」にあたる論文が、米国のシンクタンクアトランティック・カウンシルのホームページに掲載された。同論文は、「より長い電報：アメリカの新対中戦略に向けて」と題するもので、ケナンの「長文電報」を意識して米国の元政府関係者が匿名で執筆し、米国を凌駕しようという中国の長期戦略に対抗する米国の新対中戦略を同盟国と共に実施すべき、と訴えている。

このように形成されてきた中国との「体制間競争」とも言える「新冷戦」であるが、一朝一夕には終わりそうにない。中国経済は 2030 年頃米国を上回ると分析されており、人口減少による経済減速で再び米国経済が中国を逆転する 2050 年頃まで、中国が世界経済のトップである状態が継続する。少なくともこの 30 年間は、中国型社会主義とデジタル監視社会を併せ持つ権威主義体制と米国を中心とした自由民主主義体制が、「体制間競争」を繰り広げることになる。かつての冷戦が 40 年続いたことを考えれば、この競争も 2060 年頃まで継続しても不思議では無い。「新冷戦」でも、かつての冷戦期と同じように、経済論理よりも安全保障の論理が優先されることとなる。そのようなナラティブで経済安全保障を考える必要がある。

では、米国ではどのように中国との「新冷戦」を戦うつもりなのであろうか。米国の軍人や安全保障を学ぶ者は、国益を実現する戦略を DIME を組み合わせて考えるように教育される。この DIME は、外交(Diplomacy)の D、情報(Information/Intelligence)の I、軍事(Military)の M、経済(Economy)の E を組み合わせたものである。生存をかけた体制間競争は、この DIME をすべて動員しての真剣勝負となる。日本では「経済安全保障」という言葉がもてはやされているが、すべての政策を動員する DIME の E だけを議論しているに過ぎないことを認識する必要がある。米国ではバイデン政権下で策定が急がれている次期国防戦略で、“integrated deterrence”というキーワードが据えられ、DIME をすべて動員した whole-of-government アプローチで、安全保障戦略を実施することが検討されている。従来の外交と軍事に偏った安全保障から、すべての手段を使った安全保障に変わりつつあるという米国の現状を知ることが、「経済安全保障」のナラティブを理解する上でもう一つの重要な側面である。

2　サイバー空間における情報窃取型サイバー攻撃と経済安全保障上の焦点

先に述べた 2018 年のペンス演説では、「中国共産党は「中国製造 2025」計画によって、ロボット、バイオテクノロジー、人工知能など最先端産業の 90%を支配することを目指しており、（中略）米国の知的財産をあらゆる手段を用いて手に入れるように指示してきた」との警戒感が示されている。実際にサイバー空間において顕著となっている米中対立の焦点は、米国の技術力・経済力の基盤である知的財産を中国がサイバー攻撃で窃取している点にある。

「中国製造 2025」 は、2015 年 5 月に中国政府が発表した中長期の産業育成政策で、中国が「製造強国」となるために、①次世代情報技術、②新エネ自動車、③航空・宇宙、④海洋工学（ハイテク船舶）、⑤先進鉄道、⑥ロボット・工作機械、⑦電力設備、⑧新素材、⑨バイオ医薬・医療機器、⑩農業機械、の 10 重点産業育成分野を定めている。サイバー空間においては、「中国製造 2025」の重点分野に掲げられた企業に対する、情報窃取型のサイバー攻撃が多数発生している。中国のサイバー攻撃者がターゲットとしているのは、「中国製造 2025」で重点育成分野として定められた①次世代情報技術、②新エネ自動車、③航空・宇宙、④海洋工学、⑤新素材、⑥電力設備、といった産業と一致している。

このようなサイバー攻撃は、攻撃による結果として、先進国の保有する技術の不公正な強制移転をもたらし、先進国の技術優位を脅かす。また、安全保障上の問題のみならず、自由貿易体制の大きな脅威にもなっている。このような不公正な手段で入手した技術を用いて、途上国向けの製品を中国企業が製造して輸出している事例も発生しており、自由で公正なルールに基づく自由貿易体制の信頼を揺るがすことになりかねない。

中国による情報窃取型サイバー攻撃の一例として、2013 年 1 月に発覚した中国人民解放軍によるサイバー攻撃作戦がある。この攻撃を分析した米国のセキュリティ企業マンディアント社の報告書によれば、サイバー攻撃作戦を行った「APT1」と名付けられたグループは、人民解放軍(PLA)総参謀部第三部第二局（当時）傘下の第 61398 部隊であり、この攻撃グループは 2006 年以降 7 年以上の長期にわたって、米国のメディアだけでなく、幅広い産業を標的としたサイバー攻撃を行っていた。標的となった産業は、情報、運輸、ハイテク、金融、法律事務所、エンジニアリング、メディア、食糧・農業、宇宙、衛星通信、化学、エネルギー、医療、など広範囲に渡っている。

先進国の技術を狙う同様なサイバー攻撃グループとして「APT10」が知られている。「APT10」は、英国・米国の司法当局によって、中国の国家安全部と密接な関係がある攻撃グループであることが明らかになっている。「APT10」は、政府機関のみならず、製薬、鉱業、エネルギー、金属、エンジニアリング、工業生産、技術産業、小売など多岐にわたる先進国の産業を標的として「情報窃取型」サイバー攻撃を繰り返している。

APT1 や APT10 のように先進国の先端産業を攻撃対象とする中国のサイバー攻撃グループは、サイバーセキュリティの関係者で知られているだけでも数十におよび、投資制限条項や様々な政策による外国企業に対する技術移転の強制、最先端技術を有する外国企業の買収による技術の獲得と並んで、ビジネス秘密や知的財産を窃取し外国企業から技術を獲得する中国政府の重要な手段となっている。

我が国でも、2021 年 4 月に航空・宇宙分野の技術窃取を狙ったとみられるサイバー攻撃が発覚している。警視庁は、同月中国共産党員の男を私電磁的記録不正作出・同供用の疑いで書類送検した。この男は、日本国内でレンタルサーバーを借りていたが、この男が契約したレンタルサーバーは、宇宙航空研究開発機構(JAXA)をはじめ三菱電機や IHI など、防衛・航空宇宙関連の約 200 の企業や研究機関へ行われたサイバー攻撃で使われていた。

サイバー空間では、中国の国家機関が関与するこのようなサイバー攻撃を阻止していくことが、先進国の技術・経済力を守るために不可欠となっている。米国はこのようなサイバー攻撃に対して、攻撃者の攻撃コストを増加させ行動を抑止する積極的サイバー防御(ACD)を実施している。ACD は、誰が攻撃を行っているのかをアトリビューション（帰属性の解決）に基づいて特定し、外交的圧力、司法訴追、経済制裁、サイバー反撃を含むあらゆる政策を動員して攻撃側の負荷を増大させ、攻撃に対抗措置を取る政策である。先に述べた“integrated deterrence”戦略による、DIME をすべて動員した whole-of-government アプローチを具体化したものとなっている。今後我が国のサイバーセキュリティでも、中国による情報窃取型のサイバー攻撃を防ぐために、積極的サイバー防御のオペレーションを行うことを、経済安全保障政策の一環として検討する必要がある。

3　経済安全保障法制への道のり

経済安全保障の議論の推移を振り返ると、2014 年 1 月に内閣官房に国家安全保障局が設置されて以

降、外国人による土地取得問題、外国資本の日本企業への投資・買収問題による技術移転問題、外国人による大学や企業からの技術流出問題等が浮上していた。

このような安全保障上懸念される問題や次世代技術、国際規格ルール策定などを検討する必要があるとして、甘利明衆議院議員を会長に「ルール形成戦略議員連盟」が 2017 年に発足した。同議員連盟は、2019 年 3 月 20 日に『国家経済会議(日本版 NEC)創設』と題する政策提言を発表した。同提言では、①米中競争の激化が技術・資源・ルール形成をめぐる対立に発展、②ハイテク摩擦、データ（デジタル）覇権争いが米中間で発生しインテリジェンスを駆使した諜報活動が活発化、③エコノミック・ステイトクラフト（経済的手段による国益の追求）が激しさを増している、が情勢認識として提示され、中国のエコノミック・ステイトクラフトに対抗するため「国家経済会議(日本版 NEC)」創設の必要性を提唱した。具体的には、戦略的外交・経済政策を策定する「国家経済会議」を創設し、最先端技術の輸出規制強化、外国企業の投資監視強化、経済制裁、知的財産管理、国際標準のルール形成に取り組むことが必要である、としている。

この提言を一部反映する形で、翌 2020 年 4 月 1 日に国家安全保障局内に経済班が設置された。経済班は、①技術安全保障： 輸出管理、外国からの直接投資規制、技術移転規制、サプライチェーンリスクなど、②サイバーセキュリティ：次期移動体通信基盤（5G）のセキュリティ 、サイバーセキュリティ、サイバーセキュリティの情報共有、データセキュリティなど、③国際協力：各国のインフラ整備への国際協調、ハイテクの技術開発に関わる国際協調、④新型コロナ対応：人の移動規制（国境)、医療機器の調達などを担当すると、報道されている。

政府内外での一連の議論を受けて、立法面では、2020 年 6 月に、外国為替及び外国貿易法の改正法の施行ならびに関連政省令・告示の全面適用が行われた。外国為替法の改正では、国の安全等を損なう恐れのある投資への適切な対応として、上場会社の取得時の事前届けの閾値引き下げ（10%から 1%に)、取締役や監査役等の役員の就任ならびに安全保障上重要な指定業種に属する事業の譲渡・廃止および非公開技術・情報へのアクセスに際して事前届け出制度の導入が行われた。また、外国人等が防衛施設周辺や国境離島の土地等を取得し、安全保障上の懸念事項となっている問題に関して、議員立法による「国家安全保障上重要な土地等に係る取引等の規制等に関する法律」が 2021 年 6 月に可決成立した。同法では、①防衛施設、原子力施設など国家安全保障上重要な施設の敷地及び周辺区域、②国境離島の区域のうち、国家安全保障上支障となる恐れのある地域について、総理大臣が重要国土区域に指定し、土地取引の届け出および国による買い取りや収用などが規定されている。

現在の経済安全保障法制の土台を形成したのは、自民党内での動きである。先に述べた「ルール形成戦略議員連盟」の活動を受ける形で、2020 年 6 月 4 日、当時の岸田政務調査会長のもとに、政務調査会長直轄の「新国際秩序創造戦略本部」が設立され、座長に甘利明議員が就任した。同戦略本部は、2020 年 12 月 22 日「『経済安全保障戦略』策定に向けて」と題する提言を発表している。

同提言は、経済安全保障戦略策定の必要性、経済安全保障の定義、各国の経済安全保障環境、基本方針、重点的に取り組み課題、の 5 章で構成されている。第 1 章の戦略策定の必要性では、①経済的手段を自国の利益追求の「武器」として利用する国の出現、②DX が進む中で、国家の独立と生存、普遍的価値の維持、同盟国の連携のための戦略的発想が必要、③経済安全保障戦略策定が必要、との情勢認識が示されている。第 2 章で、経済安全保障を「我が国の独立と生存及び繁栄を経済面から確保すること」定義し、経済安全保障確保の基本的考え方として「戦略的自律性と戦略的不可欠性」を初めて提示した。第 4 章の

基本方針では、①戦略的自律性の維持・強化のために脆弱性の把握、強靱性の向上、依存の低減を行うこと、②戦略的不可欠性の獲得のために優位を持つ産業の維持・発展のための環境整備を行うこと、③自律性・不可欠性を有する技術の特定、保全・育成を行うこと、が示され、2022 年の通常国会で「経済安全保障一括推進法（仮称）」の制定を目指す、との提言がなされた。

自民党の「新国際秩序創造戦略本部」の提言では、経済安全保障を実現するために幅広い分野での俯瞰的、総合的対応の必要性が示されているのが特徴である。この提言では具体的に、資源・エネルギー確保、海洋開発、食料安全保障強化、金融インフラ整備、情報通信インフラ整備、宇宙開発、サイバーセキュリティ強化、データ利活用、サプライチェーンの多元化・強靱化、技術優越確保・維持、イノベーションの向上、土地取引、大規模感染症対策、インフラ輸出、国際ルール形成への関与、経済インテリジェンス能力強化、の 16 分野が列挙されている。

この自民党の提言を受けて、内閣官房に「経済安全保障法制に関する有識者会議」が設置されたのであるが、自民党の提言が 16 分野の取り組みを提唱しているのに対して、政府の有識者会議の提言では、先に述べたように 4 分野と大幅に縮小されている。また、政府の有識者会議の提言の 4 分野は、ほぼ経済産業省所管事項と一致しているなど、自民党の提言からの大幅な後退が見られる。「経済安全保障推進法案」は 22 年 2 月末頃閣議決定を予定しているとされるが、今後経済安全保障の推進が 4 分野に留まってしまうのか、それとも徐々に拡大されて、自民党の提言のような総合的な経済安全保障法制が形成されていくのか、今後注視が必要である。

サイバーセキュリティの分野では、サイバーセキュリティに留意して、我が国の基幹インフラ機能の維持等に関わる安全性/信頼性を確保することが、経済安全保障推進法案の 2 番目の柱として掲げられている。しかし、第 2 項で述べたような、知的財産の窃取を防ぐ手立てについては、サイバーセキュリティ上の対処は何ら盛り込まれておらず、かろうじて秘密特許の導入が 4 番目の柱に入れられている。今後、推進法案の改定の中で、積極的サイバー防御を実現し、サイバーによる情報窃取を防ぐ法整備が望まれる。

（中曽根平和研究所主任研究員）