# 米中体制間競争と経済安全保障
## ―背景にある国際関係論の考え方と安全保障戦略―

大澤　淳

# U.S.-China Competition and Economic Security
## ―National Security Strategy and International Relations Theory as a Background

Jun OSAWA

### はしがき

2023年5月に広島で開催されたG7サミットでは、初めて経済安全保障が議題として取り上げられた[1]。サミットでの議論を受け、G7首脳は「経済的強靭性と経済的安全保障」というコミュニケを採択した。首脳コミュニケでは、中国を名指しすることを慎重に避け、デカップリングではなく、多様化、パートナーシップの深化、そして「デリスキング」に基づく経済の強靭性と経済安全保障へのアプローチにおいて協力することを確認した[2]。「デリスキング」は、それまで使用されていた「デカップリング」よりも軟らかい表現であるが、中国に対して、経済的関係を断ち切る（デカップリング）ことはしないまでも、これまでよりも厳しいアプローチを取ろうとしていることは明らかであり、経済安全保障を強化することで中国との地政学的競争を乗り切ろうとしているG7の苦悩が見て取れる言葉である。この首脳コミュニケでは、「経済的強靱性及び経済安全保障をグローバルに確保することは、経済的な脆弱性の武器化に対する我々の最善の防御となり続ける」との表現が盛り込まれ、経済安全保障を強化するため、7つの具体的方策が示された[3]。

相互依存が進んだグローバル経済の中で、経済的な脆弱性の武器化（経済的威圧）に対する懸念は、日本では2010年に尖閣列島を巡る中国との対立において、中国からレアアースの輸出規制をうけたことにより、急速に広まった。日本が輸出規制を受けたのと同じ2010年に、中国の民主化運動に参加した中国人作家の劉暁波氏へのノーベル平和賞授与に反発した中国が、ノルウェーに対してサーモンの輸入禁止措置を行ったが、中国の経済的威圧に対する認識は、欧米では2020年頃まで高まらなかった。欧米の対中認識は、習近平政権の2期目（2018年）以降に中国政府の対外的な経済的威圧の事例[4]が急速に増えたことによって徐々に厳しくなってきたが、欧米で中国に対する警戒感が一気に高まったのは、米国のトランプ政権下で、中国に対する懸念が安全保障上の問題として示された2017年末の国家安全保障戦略（NSS2017）[5]であった。NSS2017では、アメリカの安全保障と繁栄に挑戦する国家として中国とロシアが位置づけられ[6]、特に中国は数千億ドルの米国の知的財産を不正に盗み続けている国と位置づけられ[7]ている。このよ

---

[1] 外務省、“G7 Leaders’ Statement on Economic Resilience and Economic Security,” May 20, 2023. https://www.mofa.go.jp/mofaj/files/100506767.Pdf

[2] 外務省、“G7 Hiroshima Leaders’ Communiqué,” May 20, 2023, Ministry of Foreign Affairs, https://www.mofa.go.jp/mofaj/files/100506875.pdf

[3] Ibid., p.18.

[4] このような事例として、2019年にカナダに対する菜種輸入停止（HUAWEIの孟晩舟CFOの拘束がきっかけ）、2020年のオーストラリアに対するワイン・石炭の輸入制限（コロナウィルスの発生源を巡る豪政府の究明要求がきっかけ）、2021年の台湾に対するパイナップルの輸入停止（中国と距離を置く蔡英文政権への圧力）がある。

[5] The White House, *National Security Strategy of the United States of America*, December 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[6] Ibid., p.2.

うな安全保障上の挑戦国（Challenger）としての中国の位置づけの変更は、国際政治上の大きな視点の転換[8]であり、今般の経済安全保障の議論につながる分水嶺であった。

本稿では、新たな政策論点として生起してきた経済安全保障の背景としての米中間競争に注目し、この競争がどのような歴史的経緯で登場したのか、米国において米中間競争はどのようにとらえられているのか、この米中間競争に端を発する経済安全保障は国際関係論（IR）の観点からどのような意味を有しているのか、について検討を行う。経済安全保障を巡る議論は、2019年以降日本国内で急速に進展したが、その要因として、NSS2017の見方に代表されるような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しておく必要がある。

経済安全保障のナラティブとして、国際関係論の分析枠組みから国際政治上の背景を第1節で概観する。その上で、国家の力の源泉とも言える技術を巡る問題、なかんずく知的財産の強制移転に対して、米国が中国にどのように対処しているのかをサイバー空間を事例として第2節で概観する。最後に、国際関係論の分析枠組みを踏まえ、米国の対中国戦略のなかで、経済安全保障が、どのように位置づけられているのか、また日本での経済安全保障の政策について第3節で取り上げる。

## 第1節　経済安全保障の国際政治上の背景

### 1. 国際政治の覇権交代論

国際関係論では世界秩序の構造に大きな変動をもたらす要因は、1）覇権国（hegemon）の力の衰退、2）新興国の台頭、と分析されている。それらの結果、世界の大国間の力関係（バランス・オブ・パワー）に大きな構造変化が生じ、国際政治のガバナンスに空白が生まれ、最終的には経済的な危機ないし大きな戦争を契機として新たな世界秩序の構造に入れ替わるという道筋[9]を歴史は歩んできた。

このような長期のサイクル論の代表的な論者であるジョージ・モデルスキーは、グローバル政治の長期サイクルを、①グローバル戦争、②世界大国の登場、③大国の正当性の喪失、④大国の力の分解の4つのフェーズに分け、世界的に力を持つ大国（hegemon）の栄枯盛衰を歴史的に分析している[10]。

また、ロバート・ギルピンは、長期の国際政治の変動を分析する枠組みである覇権交代論の一つとして、覇権安定論（Hegemonic stability）を提唱している[11]。ギルピンは、国際システムの動態は、①国家のパワーとその分布の形態が国際システムの動きと安定を形作り、②覇権国が強力であるときには国際システムは安定し、覇権国が弱体してくると国際システムは不安定になる、③覇権国は、成長と対外的拡大、平衡状態（覇権安定）、衰退というライフサイクルをたどり、覇権戦争を経て覇権国の交代が生じる、と述べており、国際システムを変化させることが利益になると考える国が存在しない場合、国際システムは安定しているが、ひとたび、国際システムを変化させることから得る利益（期待利得）がコスト（期待費用）を上回り、国際システムを変化させようという試みる国が出てきた場合には、国際システムが不安定になると分析している。

直近では、このような覇権交代の分析枠組みを用いて、ハーバード大学のグレアム・アリソンが、覇権国米国と台頭する中国の相克を分析し、両国が「トゥキディテスの罠」に陥る可能性があると分析している[12]。「トゥキディテスの罠」とは、紀元前5世紀のスパルタとアテネの「ペロポネソス戦争」を記録した歴史家トゥキディテスの分析にちなむ言葉で、「新興国が覇権国に取って代わろうとするとき、国際関係に構造的な摩擦が起こり、暴力的な衝突が発生する」というものである。台頭しつつある中国も、この「トゥキディテスの罠」を意識しており、2017年2月に習近平主席がジュネーブの国連事務局で行った演説の中では、「諸国が和すれば世界は安定し、諸国が闘えば世界は乱れる。紀元前のペロポネソス戦争から2度の世界大戦まで、さらに40余年続いた冷戦まで、教訓はにがくて大きい」[13]と述べられている。

### 2. 覇権国の要件としての経済力と長期の経済循環

国際関係論で、覇権国や覇権に挑戦する新興国の台頭の要因とされているのが、当該国による資源の囲い込みや新技術による経済成長である。中国の台頭で再び注目されるようになった覇権国と挑戦国の対立であるが、国

---

[7] Ibid., p.21.

[8] 国際政治上の意味合いについて例えば、森（2018）30–31ページおよび、船津（2020）35ページを参照。

[9] 大国の興亡と世界経済の関係については以下を参照。Kindleberger（1996）およびKennedy（1989）。

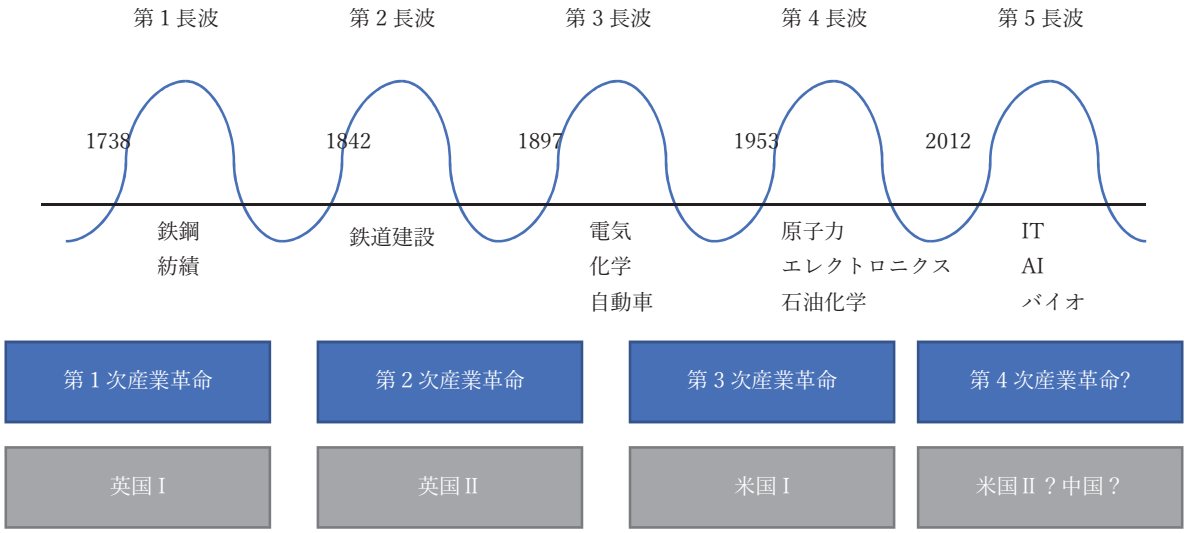
[10] Modelski（1987）。

[11] Gilpin（1981），p.10。

[12] Allison（2017）。

[13] 中華人民共和国駐日本国大使館「習近平主席の国連ジュネーブ事務局における講演全文（仮訳）」2017年2月。http://jp.china-embassy.gov.cn/jpn/jzzg/201702/t20170210_2062970.htm

**第１図　コンドラチェフの長期サイクルと覇権国**




（資料）著者作成。

際関係論では、日本が著しい経済成長によって台頭し、米国の挑戦国と見なされるようになった 1980 年代に、経済成長との関係で注目されるようになった。

例えば、1980 年代にベストセラーとなったポール・ケネディの『大国の興亡』で、ケネディは、過去 500 年の近代国家の歴史の中で、主要大国の盛衰は相対的な経済力の地位と共に変化してきたと述べており、平時における大国の経済成長の速度の差が、相対的な関係の中でそれぞれの国の興亡を決定する、と分析している[14]。

また、国際関係論の中で経済成長と国家の競争が分析の焦点となった 1980 年代に、その先駆けとなったのがイマニュエル・ウォーラスティンである。彼は、国際システムにおける国家間の競争と経済の長期サイクルとが密接な関係にあると指摘し、資本主義の成長と停滞という循環の中で、覇権国の交代が発生すると分析した[15]。彼の分析は、資本主義の成長と停滞のサイクルをもたらす長期の景気循環に関する経済学をもとにしており、特に数十年の景気循環をもたらすコンドラチェフ・サイクルに注目していた。

ロシアの経済学者コンドラチェフの提唱した 50 年にわたる長期の景気循環を研究したヨーゼフ・シュンペーターは、経済変動の要因として技術革新を指摘し、このような技術革新は、集中的かつ断続的に発生（産業クラスター化）する特徴を持ち、そのような集中的な技術革新が継続的な景気の上昇を可能にすると共に、そのような技術革新が発生した国の地位を急速に押し上げることとなると述べている[16]。

このコンドラチェフ・サイクルは、経済の大きな波動であり、その原因は、産業革命、蒸気機関、電気・科学、自動車の発明といった技術革新群を原因としている。実際にシュンペーターの議論に基づいて覇権国の推移を見てみると、第１図のように産業クラスターの形成による産業革命と覇権国の台頭の時期はほぼ一致し、長期のコンドラチェフ・サイクルを生み出す景気循環の長波に乗っかる形で覇権国が台頭していることがわかる。

以上見てきたように、国際関係論では覇権国の盛衰のメカニズムの大きな要因として、技術革新を出発点とする長期の経済成長があると考えられており、今般の米中の体制間競争でも、先端技術の囲い込みやその時代の産業の基幹製品の輸出制限などが、経済安全保障を確保する上での焦点となっている。それが故に、中国による資源の囲い込みや新技術の取り込みに対して、後のサイバーの節でも述べるように、ワシントンは神経質になっていると言えよう。

また、技術革新だけでなく、国力を決定づける要素として、資源の囲い込みや資本市場の支配、市場の確保なども重要と位置づけられている。覇権国のグローバル経済での要件を検討したロバート・コヘインは、国家が世界政治経済において覇権的であるためには、国家は、①重要な原材料に対するアクセスを持ち、②資本の主要な源泉を支配し、③大きな輸入市場を維持し、④相対的に高い賃金と利潤を生む高付加価値産業に比較優位を持たなければならない、と指摘している[17]。

### 3. 第二次大戦後の覇権を巡るサイクル：2050 年までの展望

現在の米中間競争に至るまでの、第二次世界大戦後の

[14] Kennedy（1989）。
[15] Wallerstein（1979）。
[16] Schumpeter（1939）。
[17] Keohane（1984）。

約 80 年間の国際政治では、どのような歴史的文脈が語られており、国際政治の中で、どのような価値が重視されてきたのであろうか。ざっくりと結論を先取りするならば、第二次大戦後の国際政治のシステムの中では、経済重視か安全保障重視かによって、約 40 年のサイクルがあることがわかる。

第 2 次大戦後の国際政治では、1946 年から 1989 年までの 40 年間、ソ連を中心とする社会主義陣営と、アメリカを中心とする民主主義・自由経済陣営の間で、生き残りをかけた「戦略的競争」が繰り広げられた。この大国間競争の認識は、ウィンストン・チャーチル英首相による 1946 年 3 月の「鉄のカーテン演説」[18] と、ジョージ・ケナン駐ソ米国臨時代理大使による「The Long Telegram（長文電報）」により形成された。このケナンの「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」[19] として掲載され、広く外交／安全保障の当局者・専門家の中で認識されるようになった。この大国間競争は 40 年近く続き、その間、国際関係の基調は安全保障の論理が経済の論理に優先された。

次の期間、すなわち 1989 年の冷戦終結から 2019 年頃までの 30 年間は、国際政治における大きな緊張が収まり、安全保障の論理よりも経済の論理が優先され、ヒト・モノ・カネが国境を越えて活発に移動したグローバリゼーションの時代であった。1989 年の冷戦終焉により、ソ連を中心とした陣営は崩壊し、米国一極体制が成立した。この米国一極体制は長続きせず、2008 年のリーマンショックを境目として、多極化の時代に入ることとなる。

しかし、この経済論理優先の時代は、中国の台頭によって終焉を迎えた。中国の台頭が、国際政治が再び“戦略的競争”に向かっているという物語（ナラティブ）を形成しつつあるからだ。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、再び国際政治が「体制間競争」に向かうというナラティブに影響を受けている。

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、マイク・ペンス米副大統領（当時）のハドソン研究所での演説である[20]。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、米メディアはペンスの演説が米中間の新たな冷戦の開始を暗示していると評価した[21]。

2021 年には、冷戦期のケナンの「X 論文」にあたる分析が、米国のシンクタンク大西洋評議会のウェブサイトに掲載された。同論文は、ケナンの「長文電報」を意識して、「Longer Telegram（より長い電報）：アメリカの新対中戦略に向けて」[22] というタイトルが付与されていた。この論文は、ケナンの「ロング・テレグラム」を参考に元米政府高官が匿名で書いたもので、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、と提言している。

中国経済は、2030 年頃に米国経済を抜いて世界一になり[23]、2050 年頃まで発展を続けるが、人口減少で減速し始め、米国経済が 2050 年頃中国経済を再び追い抜くと予測[24] されている。したがって、米国と中国との「体制間競争」とも言える「新冷戦」は、一朝一夕には終わりそうにない。少なくとも今後の約 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する自由民主主義陣営との「戦略的競争」が続くことになる。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

---

[18] Winston Churchill, “The Sinews of Peace,” at Westminster College, Fulton, Missouri, March 5, 1946. https://www.nationalarchives.gov.uk/education/resources/cold-war-on-file/iron-curtain-speech/

[19] Kennan（1947）。

[20] “Vice President Mike Pence’s Remarks on the Administration’s Policy Towards China,” at Hudson Institute, October 4, 2018. https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018

[21] 例えば、“Pence’s China Speech Seen as Portent of ‘New Cold War’,” New York Times, October 5, 2018. https://www.nytimes.com/2018/10/05/world/asia/pence-china-speech-cold-war.html

[22] Anonymous, “Longer Telegram: Toward a new American China strategy,” Atlantic Council Strategy Paper, January 27, 2018. https://www.atlanticcouncil.org/wp-content/uploads/2021/01/The-Longer-Telegram-Toward-A-New-American-China-Strategy.pdf

[23] CEBR, “World Economic League Table 2022,” December 2021. https://cebr.com/wp-content/uploads/2021/12/WELT-2022.pdf

[24] JCER, “China’s GDP will not surpass that of the US,” JCER Medium-Term Forecast of Asian Economies, December 15, 2022. https://www.jcer.or.jp/jcer_download_log.php?f=eyJwb3N0X2lkIjo5OTUxNSwiZmlsZV9wb3N0X2lkIjoiOTk1MjUifQ==&post_id=99515&file_post_id=99525

では無い。今後30年間は、冷戦時代と同様、経済の論理よりも安全保障の論理が優先される「新冷戦」の時代となるだろう。

我々は、このような長期の国際政治を巡る変動の認識の元に、今日の戦略環境認識が醸成され、経済安全保障の議論が形成されてきたことに、注意を払う必要がある。

## 第2節　サイバー空間における技術窃取と米国の対応

### 1. 中国による情報窃取型攻撃による技術窃取

中国との戦略競争が米国の安全保障にとって重大な懸念となり、トランプ政権下のNSS2017で中国が米国の挑戦国であると認定されたことは先に述べたが、2018年のペンス演説ではより具体的に、「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[25]。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。

中国の攻撃グループは、知的財産やビジネス秘密の窃取を目的に、先進国の民間企業、研究所、大学などへの情報窃取型サイバー攻撃を多数実施している[26]。このようなサイバー攻撃は、先進国の保有する先端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しつつある。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見られるようになっており、自由で公正なルールに基づく自由貿易体制の信頼も揺るがしつつある。

中国のサイバー攻撃者が標的としている産業・企業を分析すると、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、といった分野が集中的に狙われている[27]。これらの産業は、いずれも中国国務院が2015年5月に発表した10カ年の産業育成戦略が定められている「中国製造2025」[28]に掲載されている分野である。「中国製造2025」の序文では、国際競争力のある製造業こそが、中国の国力を増大させ、国家安全保障を確かにし、世界の強国として中華民族が復興するために欠かせない、と述べられており、製造強国の実現に向けて、具体的に10の重点産業育成分野が定められている。それらは、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農業機械となっている。

このようなサイバー攻撃による技術窃取例としては、「APT1」と名付けられたサイバー攻撃主体による米国への広範な情報窃取型サイバー攻撃作戦がある。このサイバー攻撃作戦を行ったAPT1は、人民解放軍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[29]。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た。

また、中国国家安全部と関わりの深いサイバー攻撃主体として、クラウドサービスなどを提供する会社を標的として攻撃し、その顧客である政府機関・企業の機微情報・知的財産の窃取を行っている「APT10」と名付けられたグループも存在する。英国の大手防衛産業BAEとPWCは、2017年4月、「APT10」が行っている「情報窃取型」サイバー攻撃に関して報告書を公表した[30]が、「APT10」の標的は、公的機関、医薬健康、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っていた。

このように中国による知的財産を狙った情報窃取型サイバー攻撃は、国家が関与して行われており、先に述べた「中国製造2025」と密接な関係がある。サイバー手段を用いた情報収集活動は中国の技術獲得の中核に据えられていると言われている[31]。そのため、中国が自国の5カ年計画の重点分野に沿ってサイバー窃取を行ってい

---

[25] Ibid., “Pence’s China Speech”, 2018.

[26] 大澤（2021）。

[27] 大澤（2022）。

[28] 中国国務院「**国务院关于印发**《中国制造2025》的通知」（2015年5月8日）。https://www.jst.go.jp/crds/pdf/2015/FU/CN20150725.pdf

[29] Madiant, “APT1 : Exposing One of China’s Cyber Espionage Units”（2013.2）. https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

[30] PWC/BAE, “Operation Cloud Hopper : Exposing a systematic hacking operation with an unprecedented web of global victims”, April, 2017. ＜https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf＞

[31] 例えば、以下を参照。Hannas, Mulvenon and Puglisi（2013）。

る、と米国政府は疑っている[32]。これらのサイバー手段を用いた情報窃取は、中国の技術力を強化し、中国の国力を増大させる。中長期的には、国家間の力関係に重大な影響を及ぼし、中国を覇権国として押し上げるのではないかとの危機感が米国内では広がってきている。

### 2. 米国の FDO の一環としての能動的サイバー防御による対応

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。米国では、中国の国家機関が関与するサイバー攻撃に対して、攻撃者の行動を抑止する柔軟抑止戦略（Flexible Deterrence Option：FDO）の一環として能動的サイバー防御（Active Cyber Defense：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手段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。

米司法当局は 2014 年 5 月、米国のウェスティングハウス社（原子炉）、ソーラーワールド社（太陽光発電）、US スティール（鉄鋼）などのネットワークに情報を窃取する目的で侵入し、情報を窃取した疑いで、攻撃グループ「APT1」の実行犯として、人民解放軍 61398 部隊に所属する将校五名を訴追した[33]。

また、「APT10」に対しても、米国は英国などの同盟国とともに攻撃者を特定し[34]、攻撃者のうちの 2 名が、中国の国家安全部と関係があることを明らかにしている。米司法省は、2018 年 12 月、クラウドサービスなどを提供する会社への不正アクセスを通じて、45 以上の企業の技術情報を窃取したとして、Zhu Hua、Zhang Shilong の中国人ハッカー 2 名を訴追したと発表した[35]。訴追状によれば、この 2 名は中国天津のテクノロジー企業の社員であり、国家安全部天津支局と協力して、2006 年から 2018 年にかけて、少なくとも 12 カ国の多岐にわたる企業から情報を窃取していた[36]。

米国司法省や FBI による司法訴追やサイバー攻撃実行犯の指名手配も、このような FDO 政策の一環として行われており、米国では、上記の 2 例を含め、2014 年から 2020 年までの 6 年間で、人民解放軍の将兵 5 名、国家安全部の高官 2 名を含む、中国の軍や情報機関の協力者 20 名以上を特定して司法訴追している。過去 5 年にわたって行われた米国の司法訴追や指名手配による積極的サイバー防御では、サイバー攻撃グループの活動を 1 年から 2 年抑止することに成功しており、国家が関与するサイバー攻撃に対して一定の効果をあげている。

## 第 3 節　日米の新国家安全保障戦略と経済安全保障

### 1. 米国の新安全保障戦略と経済安全保障の位置づけ

米国は 2022 年に国家安全保障戦略を改定した。米国バイデン政権の新しい国家安全保障戦略[37] は、安全保障を達成する手段として統合抑止（integrated deterrence）に焦点を当てている。統合抑止戦略は、すべてのドメインを動員した whole-of-government アプローチで、安全保障戦略を実施するという考え方である。whole-of-government アプローチとは、安全保障政策の執行に当たり、外交（Diplomacy）の D、情報（Information/Intelligence）の I、軍事（Military）の M、経済（Economy）

---

[32] Gina Chon & Charles Clover 'US spooks scour China's 5-year plan for hacking clues'（Financial Times, November 25, 2015） http://www.ft.com/intl/cms/s/0/40dc895a-92c6-11e5-94e6-c5413829caa5.html

[33] US Department of Justice, "U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage", May 19, 2014. https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and

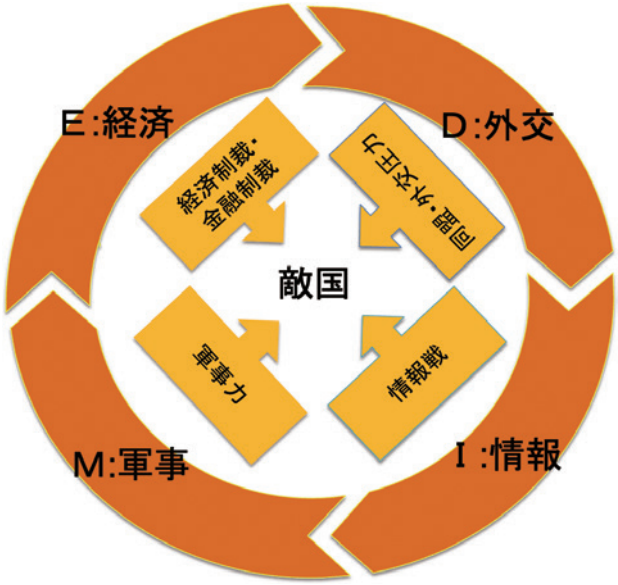
[34] UK Government, "UK and allies reveal global scale of Chinese cyber campaign", December 20, 2018. https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign

[35] US Department of Justice, "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information", December 20, 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[36] ニューヨーク州南地区裁判所「アメリカ合衆国対朱および**张**」訴追状 https://www.justice.gov/opa/press-release/file/1121706/download

[37] White House, National Security Strategy, October 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

**第２図　統合抑止戦略による安全保障**




（資料）著者作成

という、DIME をすべて動員して、中国との大国間競争の真剣勝負をしようというものである[38]。米国では、従来の外交と軍事に偏った安全保障から、情報と経済を加えたすべての手段を使った安全保障政策に変わりつつあるというのが重要な点である。米国はこの統合抑止戦略を、同盟国とともに実際に柔軟抑止戦略（FDO: Flexible Deterrence Option）のオペレーションとして行おうとしており、米国の考える経済安全保障政策は、このような国家安全保障の考え方の一領域として行われていると理解する必要がある。

生存をかけた大国間競争は、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。

## 2. 日本での経済安全保障議論の推移と新安全保障戦略

日本での経済安全保障論議の変遷を振り返ると、2014 年 1 月に内閣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、外資による日本企業への出資・買収を通じた技術移転、外国人による大学や企業からの技術流出といった問題が議論されてきた。

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 年に設立された。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[39]が、その提言の中では、①米中間の競争激化は、技術、資源、ルール作りをめぐる対立に発展している、②米中間のハイテク摩擦やデータ（デジタル）覇権争いが発生し、諜報活動が活発化している、③経済ステイトクラフト（経済手段による国益追求）が激しさを増している、という状況認識が示されている。

この自民党の提言を反映し、2020 年 4 月 1 日、国家安全保障局内に経済安全保障班が設置された。同班は、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、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。

さらに、2022 年 5 月 11 日、経済安全保障推進法案が参議院本会議で賛成多数で可決され、5 月 18 日に施行された。同法案は、4 つの柱で構成されており、①重要物資の安定供給、②重要インフラの安全確保、③最先端重要技術の開発支援、④秘密特許制度からなる。内閣官房が発表した文書では、法案の趣旨について、「複雑化する国際情勢を踏まえ、安全保障を確保するための経済対策を総合的かつ効果的に推進するための基本的な方針

[38] bid, “National Security Strategy,” p.22.

[39] ルール形成戦略議員連盟「提言『国家経済会議（日本版 NEC 創設）』」（2019 年 3 月 20 日）https://amari-akira.com/02_activity/2019/03/20190320.pdf

及び体制を確立すること」と説明されている。

日本でも 2022 年 12 月に「国家安全保障戦略」をはじめとする「安保 3 文書」が改定された。新国家安全保障戦略では、米国と同様に、サイバー安全保障分野で「能動的サイバー防御（アクティブ・サイバー・ディフェンス、以下 ACD と略す）」が採用された。2022 年の安保 3 文書での記述では、より踏み込んだ形での ACD の実施が謳われており、「国家安全保障戦略」では、「安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」との表現が盛り込まれた。また、自衛隊の役割についても、「今後、おおむね 10 年後までに、（中略）自衛隊以外へのサイバーセキュリティを支援できる態勢を強化する」との文言が「国家防衛戦略」に入り、自衛隊自身のネットワーク防衛のみならず、我が国全体のサイバー空間の防衛にも一定の役割を果たす事が示された。これらを受けて、具体的な「防衛力整備計画」では、2027 年度を目処に、自衛隊サイバー防衛隊等のサイバー関連部隊を約 4,000 人に拡充し、サイバー要員を約 2 万人体制に強化するとともに、サイバー・スレット・ハンティング（脅威追跡）機能を強化し、重要インフラ事業者及び防衛産業などの民間との連携強化を行うことが述された。

今後日本において米国と同じように、能動的サイバー防御（ACD）によって先端技術の防護をサイバー空間で行うためには、国際法上の合法性の立ち位置の確認や国内法の改正、体制整備が必要となる[40]。

**参考文献**


大澤淳（2020）、「米中サイバー戦争の様相とその行方」川島真・森聡編『UP plus アフターコロナ時代の米中関係と世界秩序』東京大学出版会。

大澤淳（2021）、「産業競争力を奪うサイバー攻撃の脅威」産経新聞社『正論』2021 年 7 月号。

大澤淳（2022）、「情報窃取型サイバー攻撃の脅威―国の競争力を奪う中国による標的型攻撃」立花書房『治安フォーラム』第 28 巻第 9 号。

舟津奈緒子（2020）、「トランプ政権の対中認識」日本国際問題研究所『トランプ政権の対外政策と日米関係』。

森聡（2018）、「2017 年国家安全保障戦略に見るトランプ政権の世界観」日本国際問題研究所『トランプ政権の対外政策と日米関係』。

Allison, Graham (2017), Destined for War : Can America and China Escape Thucydides' Trap, Scribe Publication.

Gilpin, Robert (1981), War and Change in World Politics, Cambridge University Press.

Hannas, William C., Mulvenon, James and Puglisi, Anna B. (2013), Chinese Industrial Espionage, Routledge.

Kennan, George F. (1947), "The Sources of Soviet Conduct," Foreign Affairs, Vol.25, No.7, pp.566-582.

Kennedy, Paul (1988), The Rise and Fall of the Great Powers, HarperCollins.〔鈴木主税訳（1988）『大国の興亡』草思社。〕

Kindleberger, Charles P. (1996), World Economic Primacy, 1500-1990, Oxford University Press.

Keohane, Robert (1984), After Hegemony : Cooperation and Discord in the World Political Economy, Princeton University Press.

Modelski, George (1987), Long Cycles in World Politics, Houndmills/London : Macmillan.〔浦野起央、信夫隆司訳（1991）、『世界システムの動態：世界政治の長期サイクル』晃洋書房。〕

Schumpeter, Joseph (1939), Business cycles : a theoretical, historical, and statistical analysis of the capitalist process, McGraw-Hill Book Company.

Wallerstein, Immanuel (1979), The Capitalist World-Economy, Cambridge University Press.


[40] 佐藤謙・大澤淳「激化するサイバー戦に無力の日本：法と体制整備を急げ」『Wedge』2022 年 8 月号。