

技術保護と経済安全保障の諸課題

齊藤孝祐（上智大学）
saitouk@sophia.ac.jp

イントロダクション

政府・企業・大学といった「当事者」が抱える課題を整理する。

● 目的と概要

- 先端技術や科学知の管理が強く求められるようになるなか、その実効性や功罪をめぐる政策論争が活発化してきている。本報告では、経済安全保障推進法案の経緯に触れながら、政府・企業・大学といった「当事者」が抱える課題を整理する。

● 経済安全保障の基本的な理解について

- 経済的利益を国家の中心的な価値の一つとして保護していく
- 総体的な国益の保護 = 安全保障を経済的な側面から高めるための政策（取り組み）
- エコノミックステイトクラフト：経済的手段（輸出管理／制裁／関税など）を用いた他国への戦略目標の強制

● 科学技術をめぐる問題

- 安全保障、経済、産業、社会を含む諸分野で影響力を拡大する科学技術
- 分散する技術資源をいかに管理するか

I. 経済安全保障をとりまく文脈



経済安全保障推進法の成立①

「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（2022年5月）

- (1) 自民党提言「経済安全保障戦略策定」に向けて（2020年12月）
 - ・ 「『国家安全保障戦略』で定義された国益を経済面から確保するもの」
 - ・ 「わが国の独立と生存および繁栄を経済面から確保すること」
 - ・ そのために必要な「戦略的自律性」と「戦略的不可欠性」
- (2) 経済安全保障推進法の成立と四本の柱
 - ・ サプライチェーン強靱化
 - ・ 基幹インフラの安定供給
 - ・ 先端技術の官民協力
 - ・ 非公開特許制度
- (3) 大まかな特徴
 - ・ 基本的には「守り」の色彩の強い法律
 - ・ 具体的な対象分野や管理手続きはこれから明確化
 - ・ 重要物資指定にあたっては関係事業者や団体の意見を考慮

経済安全保障推進法の成立②

四本柱の概要

● サプライチェーン強靱化

- 重要物資の指定と関連企業の認定・支援
- 罰則規定の削除

● 基幹インフラの安定供給

- 電気/ガス/石油/水道/鉄道/貨物自動車輸送/外航貨物/航空/空港/電気通信/放送/郵便/金融/クレジット決済
- 停止した場合に国民生活に影響のある企業の指定・審査

● 先端技術の官民協力

- 「特定重要技術」への資金・制度的支援/シンクタンク機能も。
- 秘密保持義務と罰則。

● 非公開特許制度

- 公開により安全が損なわれる特許の公開保留。
- 指定特許の外国出願の禁止、損失補填と罰金。

注目すべき大きな文脈

なぜ経済安全保障が重視されるようになってきたのか？

こうしたなかで政府・民間セクター・個人はいかにふるまうか？

- 産業・研究開発における「境界」のあいまい化
 - ・ 担い手における官民境界のあいまい化
 - ・ 科学技術をめぐる国境のあいまい化（グローバル化）
 - ・ 技術の効果のあいまい化（いわゆる「新興技術」への対応）
- 米中関係の展開
 - ・ 相互依存関係がもたらすリスクの顕在化・政治化・武器化
 - ・ 西側諸国間の政策協調をめぐる課題
- ロシア・ウクライナ戦争
 - ・ エネルギー・食料安全保障への注目
 - ・ 制裁のあり方をめぐる問題提起
- その他：日本固有の文脈
 - ・ 産業競争力の後退？
 - ・ 科学研究能力の後退？
 - ・ 安全保障をめぐる意識の変化？

参考：経済安全保障をめぐるリスク類型の一例

リスク・アーキタイプ	定義
唯一（sole）のソース（サプライヤー）	必要な能力を供給することのできるサプライヤーが一件しかない状態
単一（single）のソース（サプライヤー）	必要な能力を供給する資格を与えられたサプライヤーが一件しかない状態
脆弱な（fragile）サプライヤー	特定の（重要な）サプライヤーが財政危機に陥る、または困難に直面している状態
脆弱な（fragile）市場	構造的な弱さを抱えた産業経済、国内産業が壊滅する可能性
市場の影響による能力制約	市場における需要の競合によって、必要な供給量や納期を満たすことができない
対外依存	国内の産業では生産できない、または十分な量を生産できない状況
サプライヤーの縮小と素材の不足	関連サプライヤーの撤退によって製品や素材の陳腐化を招く状況
人材不足	産業に必要な技術を備えた労働者を国内で十分に雇用・維持できない状況
インフラ喪失	組み立てや製造、能力維持に必要な特殊資本設備の喪失
製品の安全性	サイバーおよび物理的な防護能力の欠如による、健全性や信頼性、競争的優位の喪失

Donald J. Trump, "Presidential Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," Executive Order 13806, July 21, 2017 ;Office of the Under Secretary of Defense for Acquisition and Sustainment, and Office of the Deputy Assistant Secretary of Defense for Industrial Policy, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency: Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806*, September 2018.

重要技術への投資指針

2500億円の技術投資

成果の「民生利用」と「公的利用」を想定

- 統合イノベーション戦略2021（2021年6月）

- 「経済安全保障の確保・強化のため、宇宙、量子、AI、スーパーコンピューター、半導体、原子力、先端材料、バイオ、海洋等の先端分野における重要技術について、関係省庁と大学、研究機関、企業等の密接な連携の下、実用化に向けた強力な支援を行う新たなプロジェクトを創出」

- 経済安全保障重要技術育成プログラム

- 日本が確保すべき応用レベル、ニーズを踏まえたシーズベースの先端重要技術の研究開発を促進
- 内閣府、経産省、文科省：助成機関としてNEDO、JSTが所掌し、それぞれ1250億円の予算
- 研究成果を民生利用のみならず、関係府庁で「公的利用」することを想定
- 適切な技術流出対策を導入

参考：米国ECRA14項目とC&ET20項目

ECRA	C&ET
バイオテクノロジー（合成生物学、ゲノム工学等）	バイオテクノロジー
人工知能（AI）および機械学習技術	人工知能
測位（PNT）技術	＜宇宙技術
マイクロプロセッサ技術	半導体・微細電子工学
先端コンピュータ技術	先端コンピュータ技術
データ分析技術	データサイエンス・ストレージ
量子情報・センシング技術（量子コンピュータ、量子暗号等）	量子情報科学 ＜先端センシング
輸送技術	
3Dプリンティング	＜先端製造
ロボティクス（マイクロドローン、スウォーム技術等）	＜自律化技術
ブレイン・コンピュータインターフェース	＜ヒューマン・マシン・インターフェース
極超音速	＜航空エンジン技術
先端素材	先端エンジニアリング素材
先端監視技術	＜通信・ネットワーク技術
	医療・公衆衛生技術
	エネルギー技術
	分散型台帳技術
	先端通常武器技術
	農業技術
	CBRN緩和技術

参考：2022年度米国C&ET戦略の対象項目

C&ET戦略の更新リスト（2022）	サブカテゴリー
Advanced Computing	• Supercomputing • Edge computing • Cloud computing • Data storage • Computing architectures • Data processing and analysis techniques
Advanced Engineering Materials	• Materials by design and material genomics • Materials with new properties • Materials with substantial improvements to existing properties • Material property characterization and lifecycle assessment
Advanced Gas Turbine Engine Technologies	• Aerospace, maritime, and industrial development and production technologies • Full-authority digital engine control, hot-section manufacturing, and associated technologies
Advanced Manufacturing	• Additive manufacturing • Clean, sustainable manufacturing • Smart manufacturing • Nanomanufacturing
Advanced and Networked Sensing and Signature Management	• Payloads, sensors, and instruments • Sensor processing and data fusion • Adaptive optics • Remote sensing of the Earth • Signature management • Nuclear materials detection and characterization • Chemical weapons detection and characterization • Biological weapons detection and characterization • Emerging pathogens detection and characterization • Transportation-sector sensing • Security-sector sensing • Health-sector sensing • Energy-sector sensing • Building-sector sensing • Environmental-sector sensing
Advanced Nuclear Energy Technologies	• Nuclear energy systems • Fusion energy • Space nuclear power and propulsion systems
Artificial Intelligence (AI)	• Machine learning • Deep learning • Reinforcement learning • Sensory perception and recognition • Next-generation AI • Planning, reasoning, and decision making • Safe and/or secure AI
Autonomous Systems and Robotics	• Surfaces • Air • Maritime • Space
Biotechnologies	• Nucleic acid and protein synthesis • Genome and protein engineering including design tools • Multi-omics and other biometrology, bioinformatics, predictive modeling, and analytical tools for functional phenotypes • Engineering of multicellular systems • Engineering of viral and viral delivery systems • Biomanufacturing and bioprocessing technologies
Communication and Networking Technologies	• Radio-frequency (RF) and mixed-signal circuits, antennas, filters, and components • Spectrum management technologies • Next-generation wireless networks, including 5G and 6G • Optical links and fiber technologies • Terrestrial/undersea cables • Satellite-based communications • Hardware, firmware, and software • Communications and network security • Mesh networks/infrastructure independent communication technologies
Directed Energy	• Lasers • High-power microwaves • Particle beams
Financial Technologies	• Distributed ledger technologies • Digital assets • Digital payment technologies • Digital identity infrastructure
Human-Machine Interfaces	• Augmented reality • Virtual reality • Brain-computer interfaces • Human-machine teaming
Hypersonics	• Propulsion • Aerodynamics and control • Materials • Detection, tracking, and characterization • Defense
Quantum Information Technologies	• Quantum computing • Materials, isotopes, and fabrication techniques for quantum devices • Post-quantum cryptography • Quantum sensing • Quantum networking
Renewable Energy Generation and Storage	• Renewable generation • Renewable and sustainable fuels • Energy storage • Electric and hybrid engines • Batteries • Grid integration technologies • Energy-efficiency technologies
Semiconductors and Microelectronics	• Design and electronic design automation tools • Manufacturing process technologies and manufacturing equipment • Beyond complementary metal-oxide-semiconductor (CMOS) technology • Heterogeneous integration and advanced packaging • Specialized/tailored hardware components for artificial intelligence, natural and hostile radiation environments, RF and optical components, high-power devices, and other critical applications • Novel materials for advanced microelectronics • Wide-bandgap and ultra-wide-bandgap technologies for power management, distribution, and transmission
Space Technologies and Systems	• On-orbit servicing, assembly, and manufacturing • Commoditized satellite buses • Low-cost launch vehicles • Sensors for local and wide-field imaging • Space propulsion • Resilient positioning, navigation, and timing (PNT) • Cryogenic fluid management • Entry, descent, and landing

II. 技術保護の当事者性と課題



「当事者」の課題：政府

経済的機会・学術的機会と安全保障上の要請のバランス

コストの増大：政策の継続性の問題

- 政策を主導する立場としての政府
 - ・ 合理的な範囲をどのように定めるか
 - ・ 自力では定めがたい「政策のゴール」：何を、いつ、どこまでやれば十分なのか。
- 経済と安全保障のバランス
 - ・ リスクがある場合にどちらを優先するか
 - ・ 経済的利害や学術的機会を低下させることも国益の損失
 - ・ それだけでなく、軍事安全保障の能力低下にもつながりうる
- 政策の負担
 - ・ 「カネのかかる」経済安全保障の取り組み
 - ・ 技術投資／重要分野の特定・審査の負担（cf. CFIUS）
- 経済安全保障政策の動向に関わらず生じていた関連課題
 - ・ 科学技術基盤の縮小
 - ・ 防衛産業基盤の縮小
 - ・ 軍事セクターのオープン化問題

「当事者」の課題：民間セクター①

誰がリスクを判断し、誰がコストを引き受けるのか

- 対象事業・技術を抱える組織
 - ・ 自社の事業が規制や支援の対象となる取引・技術を含むかどうか
 - ・ 指定の物資を扱う組織への取引先・連携先の制限の可能性
- 対象事業を含まない場合に、経済安全保障に基づく対応をすべて免れうるか
 - ・ 目まぐるしく変化する国際情勢
 - ・ 「新興技術」が定義上はらむそもそもの曖昧さ：安全保障上、経済社会上の重要性や用途の想定が困難な技術群
 - ・ 後からリスクを認められるようになる可能性
 - ・ 事業リスク、レピュテーションリスク
- 組織の情報収集・判断能力
 - ・ 規制対応（情報管理等）・能力構築のためのコスト負担

「当事者」の課題：民間セクター②

これまでの政策課題との関連

- 学術研究と安全保障の接近をめぐる問題
 - 安全保障技術研究推進制度の実施に伴う、いわゆる「軍事研究」問題
 - 経済安全保障重要技術育成プログラムにおける「公的利用」の意味合い
 - （政策上の必要性は別にして）こうした取り組みへの受容の問題
- 技術流出への対応としての規制強化
 - 国際共同研究の相手先選定をめぐる問題
 - 研究者・学生の移動規制問題
 - 外部資金資金をめぐる「リサーチインテグリティ」＝科学者が遵守すべき研究公正の概念をいかにして拡張する（しない）かという問題
- さらなる「選択と集中」への対応？
 - 2500億円の基金に基づく研究開発
 - cf. ムーンショット型研究開発は800億円（2018年）

まとめ・論点

一意には決まらない、複合的政策の「意義」：経済的合理性・安全保障上の要請双方の文脈の考慮

● 法的規制と自主規制のバランス

- まずは具体的な事業・技術指定の推移の確認
- 政府の明確な指針提示と民間セクターの理解の双方がなければ規制の実効性は高まらない
- 政府が全てを管理できるわけではないし、そうすべきでもない
- 調査能力の重要性：自組織の事業・技術がもたらす社会的帰結に注意を払う必要性の（ますますの）拡大

● 今後の追加的な論点

- 国家と事業者のリスク・コストバランス
- 「守る」ことが中心の政策／「攻める」ことがどこまで政策の射程に入ってくるか：人権問題や重大な国際法違反への対応など
- サプライチェーンを「向こうに切られる」のではなく、「こちらから切りに行く」ケースをどう考えるか