

エネルギー安全保障に関する国際問題の諸相

— 2019～2020年度 エネルギー安全保障に関する国際問題検討班報告書 —

2 0 2 6 年 6 月

日本エネルギー法研究所

は し が き

この報告書は、2019年度から2020年度にかけて開催した「エネルギー安全保障に関する国際問題検討班」での研究会報告を基礎として、各担当者が改めて論点を補強し、分担執筆した論考を集成したものである。

エネルギーをめぐる環境変化の影響は、国内のみならず、新たな世界的潮流として多くの国に及ぶようになってきている。例えば、原子力の平和的かつ安全な利用のように、一国のみによる対応では十分な解決策を得ることができず、関係する国々の協力がなければ、本来の目的を達成できない場面が増えている。これまでの研究会においては、2016年5月に発効した「核物質の防護に関する条約の改正」等の国際取決めや、諸外国における具体的な訴訟事例・法制度等を広く研究の対象としてきたが、国際動向はますます流動的になっており、これに迅速かつ適切に対応することが、より一層求められる現状にある。

また、我が国特有の課題として、海外のエネルギー資源への高い依存度を背景に、資源調達における交渉力の限界や、資源国やシーレーンにおける情勢変化の影響等による供給不安に直面するリスクを常に抱えていることから、エネルギー安全保障の確保は依然として大きな課題であり続けている。

以上の現状認識を前提に、本研究班では、エネルギーをめぐる国際的な環境変化が日本のエネルギー安全保障に与える影響についての観点を中心に据え、国際的な指針・基準・動向等を広く対象とし、その法的諸問題について検討を重ねてきた。

本報告書は、日本関係船舶の安全確保のための自衛隊の中東派遣をめぐる法的諸問題、ハイジャック航空機によるテロへの対応、外国為替及び外国貿易法（外為法）における「中核的な基盤(critical infrastructure)」の位置づけ、EU構成国間の投資協定とエネルギー憲章条約、クラウドサービスと競争法、サイバー攻撃に対する国際法の適用、行政法の域外適用と執行管轄権、通商協定における労働条項の法的機能といった、国際法、国際経済法、EU法、国内行政法など、広範な法分野に係る論考で構成されている。

本報告書の作成にさいしては、幹事を務めた研究員が、テーマの企画、調整、総括をはじめ、編集全般にわたり、きめ細かい配慮を重ねて下さった。研究班の主査として心より御礼申し上げたい。

2026年6月

森 川 幸 一

エネルギー安全保障に関する国際問題検討班主査
専 修 大 学 教 授

エネルギー安全保障に関する国際問題検討班名簿

(2019年4月～2021年3月)

主 査	森 川 幸 一	専修大学教授
研 究 委 員	斎 藤 誠	東京大学教授
	酒 井 啓 亘	京都大学教授
	中 西 優美子	一橋大学教授
	林 秀 弥	名古屋大学教授
	西 村 弓	東京大学教授
	原 田 大 樹	京都大学教授
	伊 藤 一 頼	東京大学教授
研 究 員	羽 鳥 洋 一	日本エネルギー法研究所 (2020年3月まで)
	高 橋 一 正	日本エネルギー法研究所 (2019年7月まで)
	阿 部 桜 子	日本エネルギー法研究所 (2019年7月から12月まで)
	橋 本 侑 磨	日本エネルギー法研究所 (2020年11月から)
	井 熊 良	日本エネルギー法研究所 (2020年10月まで)
	菱 田 欣 矯	日本エネルギー法研究所 (2020年11月から)
	勢 藤 耕 平	日本エネルギー法研究所 (2020年9月まで)
	井 上 元 太	日本エネルギー法研究所 (2020年10月から)
	井 上 大 樹	日本エネルギー法研究所 (2020年8月まで)
	堀 雅 晃	日本エネルギー法研究所 (2020年1月まで)
	林 洋 志	日本エネルギー法研究所 (2020年2月から)
	森 実 慎 二	日本エネルギー法研究所 (2020年2月まで)
	高 尾 宗士朗	日本エネルギー法研究所 (2020年3月から)
	城 野 智 慧	日本エネルギー法研究所 (2020年7月まで)
	上 野 佑 太	日本エネルギー法研究所 (2020年8月から)

※肩書きは、特に示さない限り、研究会当時のものである。

研 究 活 動 記 録

<2019年度>

- | | |
|--------|--|
| 第1回研究会 | 2019年4月19日
2019年度研究テーマについて
原子力損害の民事責任に関する条約について
(城野研究員) |
| 第2回研究会 | 2019年5月17日
超越的情報流通をめぐる法制度とエネルギー安全保障
(伊藤研究委員) |
| 第3回研究会 | 2019年6月28日
EUの投資に関する法的問題
(中西研究委員) |
| 第4回研究会 | 2019年7月19日
プラットフォーム事業者に対する競争法的規律
ードイツの連邦カルテル庁・Facebook決定をめぐってー
(林研究委員) |
| 第5回研究会 | 2019年10月18日
エネルギーと安全保障～問題提起として
(経済産業省通商政策局通商法務官 米谷三以様
経済産業省貿易経済協力局貿易振興課長 福永佳史様) |
| 第6回研究会 | 2019年11月15日
サイバー攻撃に対する国際法の適用
(西村研究委員) |
| 第7回研究会 | 2019年12月20日
日本が締結した二国間投資協定 (BIT) における安全保障例外について
(酒井研究委員) |
| 第8回研究会 | 2020年1月10日
日本関係船舶の安全確保のための自衛隊の中東派遣をめぐる法的諸問題
(森川主査) |
| 第9回研究会 | 2020年2月3日
エネルギー安全保障行政法
(原田研究委員) |

<2020年度>

- 第10回研究会 2020年6月26日
対内直接投資を巡る最近の動向～エネルギー産業を中心に～
（電力中央研究所社会経済研究所スタッフ副研究参事 丸山真弘様）
- 第11回研究会 2020年7月29日
外国住民・外国自治体による国内行政訴訟の提起
—エムスランド事件からの考察
（斎藤研究委員）
- 第12回研究会 2020年8月28日
法制度の変更に関する投資協定上の評価
—再生可能エネルギー支援策の縮小をめぐる投資紛争を素材として—
（伊藤研究委員）
- 第13回研究会 2020年9月14日
日米欧のマージン（プライス）・スクイーズ規制
—エネルギー市場への示唆—
（林研究委員）
- 第14回研究会 2020年10月16日
サイバー攻撃への対処措置の国際法上の位置づけ
（西村研究委員）
- 第15回研究会 2020年11月17日
安全保障例外条項における「安全保障上の重大な利益」概念について
（酒井研究委員）
- 第16回研究会 2020年12月18日
日本関係船舶の安全確保のための自衛隊の中東派遣をめぐる法的諸問題
—海上警備行動の国際法上の根拠を中心に—
（森川主査）
- 第17回研究会 2021年2月24日
エネルギー安全保障と国内行政法—公権力の行使と執行管轄権
（原田研究委員）
- 第18回研究会 2021年3月30日
外国大規模施設に対する国内裁判所への出訴と条約の関係
—ザルツブルク空港事件をめぐって
（斎藤研究委員）

※肩書きは、研究会当時のものである。

なお、本報告書の執筆は以下の通り分担して行った。

- 第1章 日本関係船舶の安全確保のための自衛隊の中東派遣をめぐる法的諸問題
森川 幸一 主査
- 第2章 ハイジャック航空機によるテロへの対応
—ドイツ判例からの考察，原発防護を念頭において—
斎藤 誠 研究委員
- 第3章 外国為替及び外国貿易法（外為法）における「中枢的な基盤(critical infrastructure)」の位置づけ—地域的な包括的経済連携協定（RCEP 協定）の安全保障例外との関係を手がかりに—
酒井 啓亘 研究委員
- 第4章 EU 構成国間の投資協定とエネルギー憲章条約—Komstroy 事件判決を中心に—
中西優美子 研究委員
- 第5章 クラウドサービスと競争法
林 秀弥 研究委員
- 第6章 サイバー攻撃に対する国際法の適用
西村 弓 研究委員
- 第7章 行政法の域外適用と執行管轄権
原田 大樹 研究委員
- 第8章 通商協定における労働条項の法的機能
—資源・エネルギー産業への経済的・政策的示唆—
伊藤 一頼 研究委員

目 次

第1章 日本関係船舶の安全確保のための自衛隊の中東派遣をめぐる法的諸問題	森川 幸一	1
Ⅰ はじめに.....		3
Ⅱ 派遣の経緯とその後の展開.....		5
1. 自衛隊の中東派遣の経緯.....		5
2. その後の展開.....		7
Ⅲ 情報収集活動.....		9
1. 情報収集活動の内容と実績.....		9
2. 派遣根拠としての防衛省設置法上の「調査・研究」.....		9
3. 情報収集活動の地理的範囲.....		11
4. 情報収集活動に従事する部隊の武器使用権限.....		14
Ⅳ 海上警備行動.....		15
1. 保護対象.....		15
2. 発令要件.....		15
3. 措置をとり得る相手.....		16
4. とり得る措置と国際法上の根拠.....		16
Ⅴ 海上警備行動の国際法上の根拠.....		17
1. 公海上で旗国以外の国がとり得る措置とその対象.....		17
2. SUA条約および改正議定書.....		19
3. 海上警備行動でとり得る措置と旗国主義.....		20
Ⅵ むすびにかえて.....		22
第2章 ハイジャック航空機によるテロへの対応ードイツ判例からの考察, 原発防護を念頭において.....	斎藤 誠	25
Ⅰ はじめに.....		27
Ⅱ 原子力発電所の防護ーこれまでの経緯から.....		28
Ⅲ ドイツにおける軍・警察の分離原則とその変容.....		31
1. 分離原則とその淵源.....		31
2. ハイジャック機への武器使用と分離原則ー連邦憲法裁判所判決を巡って.....		32
Ⅳ 比較の視座からの若干の考察.....		36
1. 比較の前提.....		36

2. 根拠法の明確性, 法令の整合性及び体系的解釈を求める姿勢	36
3. 固有武器使用の可否	36
4. 緊急時の決定権限－大臣権限と合議体としての政府の権限	37
V 自衛隊と法執行組織（広義の警察。海保も含む）の分離原則	39
VI むすび	39
 第3章 外国為替及び外国貿易法（外為法）における「中核的な基盤(critical infrastructure)」の 位置づけ－地域的な包括的経済連携協定（RCEP 協定）の安全保障例外との関係を 手がかりに－	酒井 啓亘 45
I はじめに	47
II RCEP 協定における「中核的な公共基盤」の取扱い	48
1. RCEP 協定の概要	48
2. 例外条項と「中核的な公共基盤」規定	50
III 日本における対内直接投資規制と「中核的な基盤」の関係	55
1. 日本が締結した経済関係協定における例外規定と「中核的な基盤」	55
2. 外為法における「中核的な公共基盤」の位置づけ	65
IV おわりに	75
 第4章 EU 構成国間の投資協定とエネルギー憲章条約－Komstroy 事件判決を中心に－	中西 優美子 79
I 背景	81
1. 気候変動対処とエネルギー憲章条約	81
2. EU 法の自律性と EU 構成国間の投資協定	82
II Komstroy 事件（Case C-741/19, 2021 年 9 月 2 日 EU 司法裁判所の先決裁定）	85
1. 事実概要	85
2. 判決	86
III 判決の評価・影響	90
 第5章 クラウドサービスと競争法	林 秀弥 95
I はじめに	97
II 電力事業におけるクラウドサービスの重要性	98
III クラウドサービスの経済的特徴：経済的視点	99
1. 規模の経済	101
2. ネットワーク効果	102

3. 大手 CSP の垂直統合	103
4. 参入障壁	103
5. 高い乗り換えコスト／ベンダーロックイン	105
IV 競争法の文脈でのクラウドサービスの市場研究・規制事例	107
V クラウドサービスに関する EU 法の展開	112
1. データ法 (DA)	113
2. デジタル市場法 (DMA)	117
3. DMA によるクラウドサービス規制への批判	118
4. クラウドサービスに関する DA と DMA の相互作用に関する潜在的問題点	119
VI 課題と展望	120
VII 結語	123
第 6 章 サイバー攻撃に対する国際法の適用	西村 弓 125
I はじめに	127
II サイバー攻撃の法的評価と対応措置	130
1. 既存の国際法の適用の適否	130
2. 武力攻撃／武力行使に該当するサイバー攻撃への対応	132
3. 国家による武力行使に至らないサイバー攻撃への対応	134
4. 非国家主体によるサイバー攻撃への対応	135
III サイバーセキュリティの回復措置	138
IV むすびに代えて	139
第 7 章 行政法の域外適用と執行管轄権	原田 大樹 143
I はじめに	145
II 公権力の行使の外延	146
1. 一般性と個別性	146
2. 法的行為と事実行為	146
III 執行管轄権の内包	147
1. 執行概念の複合的性格	147
2. 観念的な実力行使?	148
IV 公権力の行使と執行管轄権	149
1. 立法と規律	149
2. 規律と実現	151
V おわりに	152

第8章 通商協定における労働条項の法的機能

－資源・エネルギー産業への経済的・政策的示唆－	伊藤 一頼	155
I	はじめに	157
II	通商協定における労働条項の系譜	157
1.	WTO 協定	157
2.	二国間ないし地域的な通商協定	158
III	通商協定における労働条項の下での紛争処理	160
1.	北米労働協力協定 (NAALC)	160
2.	環境分野における私人申立の仕組み（参考）	163
3.	TPP 協定の労働章における紛争処理手続	164
IV	労働条項に基づく仲裁事例　－米国対グアテマラ事件－	164
1.	事案の背景	164
2.	仲裁パネルの判断	165
V	おわりに	172

第 1 章

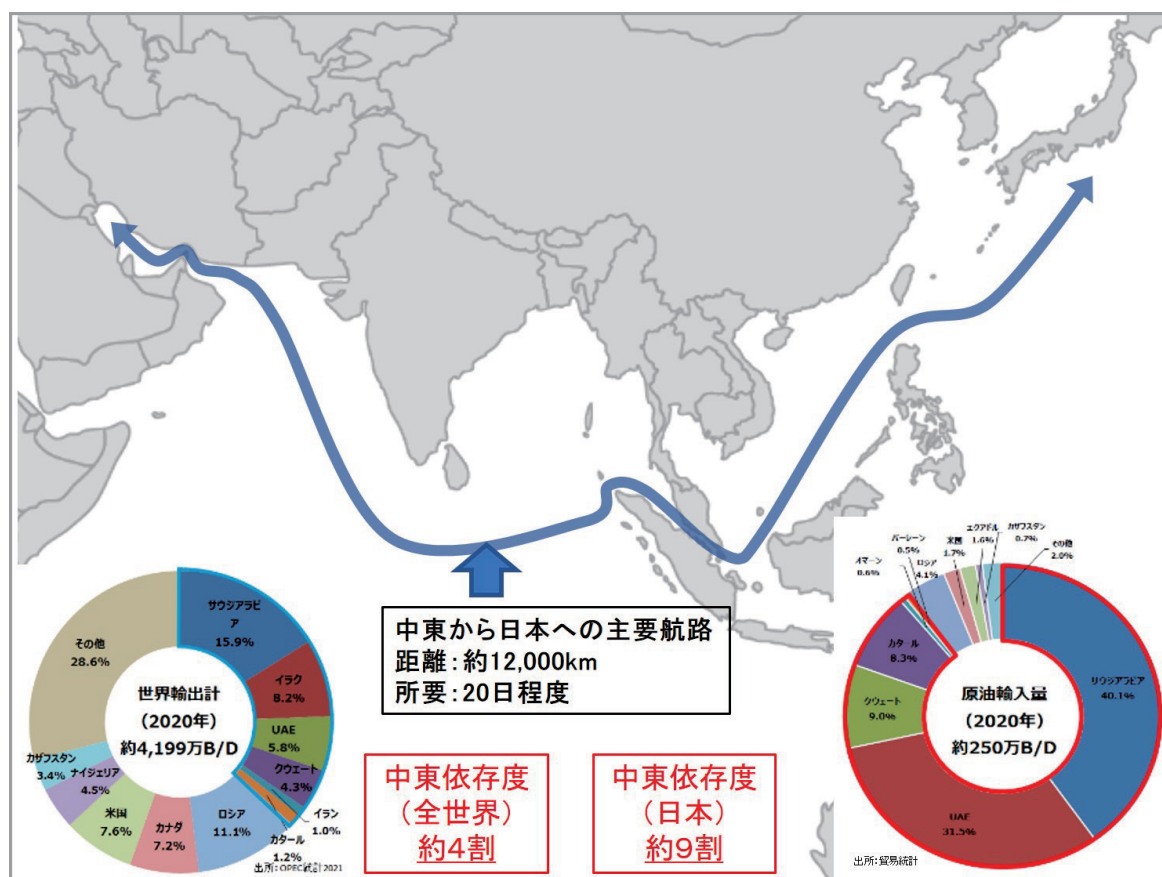
日本関係船舶の安全確保のための 自衛隊の中東派遣をめぐる法的諸問題

専修大学教授
森川 幸一

I はじめに

中東地域は、世界の石油埋蔵量の約 5 割、天然ガス埋蔵量の約 4 割を占める世界最大のエネルギー資源の供給地であるとともに、地政学上も、アジア、欧州、アフリカの結節点かつシーレーンの要衝という極めて重要な地域となっている。とりわけ、エネルギーの多くを海外からの輸入に依存し、原油の 9 割以上を同地域から輸入する日本にとって、同地域における平和と安定やシーレーンの確保は、エネルギー安全保障の観点からも、極めて重要であるとされている¹。

中東から日本までの航路は約 12,000km あり、主にペルシャ湾内で原油を積載したタンカーは、ホルムズ海峡、アラビア海、インド洋、東南アジアのマラッカ・シンガポール海峡を航行し、20 日程度かけて日本に到着する（下図参照）²。



出典：防衛省 HP

2019 年 12 月 27 日、日本政府は、中東地域で航行する日本関係船舶の安全確保のための情

¹ 藤生将治「外交・安全保障に関する調査会 3 年目の調査—外交・安全保障に関する調査報告の概要—」立法と調査 No.476 (2025 年 7 月) 4 頁。

² 防衛省「中東地域における日本関係船舶の安全確保に関する政府の取組」(令和 7 年 11 月 7 日更新) https://www.mod.go.jp/j/approach/defense/m_east/index.html (以下、各サイトの最終閲覧日はいずれも 2026 年 2 月 15 日)。

報収集を目的として、海上自衛隊の護衛艦と哨戒機を派遣することを閣議決定した³。同閣議決定は、一部変更を加えつつ、これまで 6 回にわたって更新され、最新のものは 2025 年 11 月 7 日に行われたものである⁴。

同閣議決定によると、中東地域では高い緊張状態が継続する中、船舶を対象とした攻撃事案が生起しており、米国をはじめとする各国も、同地域で艦船、航空機などを活用した航行の安全確保に取り組んでいる。このように、国際社会において、多様な手段で船舶の航行の安全のための情報を収集し、あるいは安全確保に万全を期すという取組が行われている状況にあることに鑑みて、中東地域における平和と安定及び日本関係船舶の安全の確保のため、日本独自の取組として、①中東の緊張緩和と情勢の安定化に向けた更なる外交努力、②関係業界との綿密な情報共有をはじめとする航行安全対策の徹底、③情報収集態勢強化のための自衛隊の艦艇及び航空機の活用について、政府一体となった総合的な施策を関係省庁が連携して実施するとされている。

このうち、③の自衛隊による情報収集活動は、「日本関係船舶の安全確保に必要な情報を収集するものであり」、これは、「不測の事態の発生など状況が変化する場合への対応として」「自衛隊法（昭和 29 年法律第 165 号）第 82 条に規定する海上における警備行動（以下「海上警備行動」という。）に関し、その要否に係る判断や発令時の円滑な実施に必要である」とされている。

情報収集活動に従事する自衛隊の部隊の装備は、当初は、護衛艦を新規に 1 隻派遣するとともに、海賊行為の処罰及び海賊行為への対処に関する法律（平成 21 年法律第 55 号。以下「海賊対処法」という。）第 7 条第 1 項の規定による海賊対処行動に現に従事する自衛隊の部隊（以下「海賊対処部隊」という。）の固定翼哨戒機 P-3C を活用するとされていた。もっともその後、2021 年 12 月 24 日の閣議決定⁵では、専従の護衛艦の派遣の期限を再延長せず、代わりに、海賊対処法第 7 条第 1 項の規定による海賊対処行動に現に従事する自衛隊の部隊の護衛艦及び固定翼哨戒機 P-3C を活用することへと変更された。

上記自衛隊の部隊は、オマーン湾、アラビア海北部及びバブ・エル・マンドブ海峡東側のアデン湾の 3 海域の公海（沿岸国の排他的経済水域を含む。）において、船舶の航行の安全に直接影響を及ぼす情報その他の航行の安全確保に必要な情報の収集を行うこととされている。

また、不測の事態が発生するなど状況が変化する場合への対応として、自衛隊による更な

³ 外務省「中東地域における日本関係船舶の安全確保に関する政府の取組」

https://www.mofa.go.jp/mofaj/fp/nsp/page1_000986.html。

⁴ 外務省「中東地域における日本関係船舶の安全確保に関する政府の取組の一部変更について」

<https://www.mofa.go.jp/mofaj/files/100941317.pdf>。

⁵ 外務省「中東地域における日本関係船舶の安全確保に関する政府の取組の一部変更について」

https://www.mofa.go.jp/mofaj/fp/nsp/page25_002071.html。

る措置が必要と認められる場合には、自衛隊法第 82 条の規定に基づき、海上警備行動を発令して対応する。当該発令に際しては、迅速な意思決定に努めることとする。また、海上警備行動に際してとり得る措置は、旗国主義の原則をはじめとする国際法を踏まえ、保護対象船舶が日本籍船か外国籍船かの別、侵害の態様といった個別具体的な状況に応じて対応することになるという。

本稿は、2019 年 12 月 27 日の閣議決定に基づき中東地域に派遣され、現在までその活動が継続されている、日本関係船舶の安全確保のための自衛隊の活動について、その派遣の経緯とその後の展開を概観したのち（Ⅱ）、活動の内容やその国内法上、国際法上の根拠について、主に政府の説明に即して整理する（Ⅲ、Ⅳ）。さらに、それを踏まえたうえで、特に海上警備行動に焦点を絞り、その国際法上の根拠について考察する（Ⅴ）ことを目的とする。

Ⅱ 派遣の経緯とその後の展開

1. 自衛隊の中東派遣の経緯

2015 年 7 月、イランと米・英・独・仏・中・ロとの間で結ばれた核合意「包括的共同作業計画(JCPOA)」によって、イランが核開発を大幅に制限すること（高濃縮ウランや兵器級プルトニウムを 15 年間生産しないことや、ウラン濃縮に使われる遠心分離機の大幅削減等）の見返りとして、米・欧はイランに対する金融制裁や原油取引制限などの制裁措置を緩和することになった。

しかし、2017 年 1 月に就任したトランプ大統領は、核開発の制限に期限が設けられていないことや核兵器を運搬する弾道ミサイル開発の制限が盛り込まれていないとして、2018 年 5 月、JCPOA から一方的に離脱し、イランへの制裁を段階的に再開した。2019 年 5 月にはイラン産原油の全面禁輸が始まり、イランは歳入の 6 割を占める原油収入が激減して経済的困窮に陥った⁶。

こうした中、ホルムズ海峡周辺では、航行中の商船が妨害活動を受ける事案が多発し、2019 年 5 月 12 日、オマーン湾に面したフジャイラ沿岸で、フジャイラ港で給油を受けるためアラブ首長国連邦の領海に停泊していたサウジアラビア船籍の石油タンカー 2 隻、ノルウェー船籍の石油タンカー 1 隻と、アラブ首長国連邦船籍のバンカー船（給油船）1 隻が被害を受ける事件が発生した。2019 年 6 月 13 日には、日本の国華産業が所有するパナマ船籍のケミカルタンカー、コクカ・カレイジャス号がホルムズ海峡付近のオマーン湾で何者かによって攻撃を受け火災が発生するという事件が起きた（下図参照）⁷。米国政府は、コクカ・

⁶ JCPOA 及び第 1 次トランプ政権による対イラン経済制裁について詳しくは、杉田弘毅「アメリカの対イラン外交—経済制裁を軸に考える」安全保障研究第 2 巻 2 号（2020 年 6 月）31-45 頁参照。

⁷ 防衛省・前掲注(2)参照。

カレイジャス号に対する攻撃は、イラン革命防衛隊によるリムペット機雷⁸を使った犯行であると主張し、イランはこれを否定したが、日本政府は攻撃主体について特定はしなかった⁹。



出典：防衛省 HP

こうした事態を受けて、7月9日、ダンフォード米統合参謀本部議長（当時）は、ホルムズ海峡及びイエメン沖のバブ・エル・マンデブ海峡での航行の自由を確保するため、多国間の有志連合の結成を検討していることを明らかにした。米軍は、この有志連合への参加国間の調整等を通じて、参加国の艦艇が自国籍船舶の護衛を行うことを可能にすることを想定し、この護衛作戦を「オペレーション・センチネル(Operation Sentinel)」と名付けた。7月19日の米中央軍声明¹⁰で、米軍は、この作戦の目標として、アラビア海、ホルムズ海峡、バブ・エル・マンデブ海峡及びオマーン湾全域の国際水域(international waters)における海洋の安定

⁸ リムペット機雷(Limpet mines)は、工作員が直接目標船舶の船底に装着し時限式で爆発させる方式のもので、1985年7月10日、環境NGOグリーンピースが所有するレインボー・ウォーリア号が、ムルロワ環礁でのフランスの核実験に抗議するため、ニュージーランドのオークランド港に停泊していたところ、仏諜報機関部員によって仕掛けられたリムペット機雷によって爆破され沈没し、乗組員であるオランダ人カメラマンが溺死した「レインボー・ウォーリア号事件」で使用されたものが有名である。なお、エネルギー海上輸送の安全確保の観点から機雷をめぐる法的論点を論じたものとして、森川幸一「エネルギー海上輸送の安全確保と機雷をめぐる国際法・国内法上の諸問題」日本エネルギー法研究所編『エネルギー資源確保に関する国内外の法的問題の諸相—2015～2016年度 エネルギー資源確保に関する国際問題検討班報告書—JELI R No.148』（2021年）3-15頁がある。

⁹ ポンペオ米国務長官（当時）がイランの責任に言及したことについて、菅義偉官房長官（当時）は、「予断をもって発言することは控えたい」と述べたとされる。朝日新聞朝刊（2019年6月15日）。

¹⁰ U.S. Central Command Statement on Operation Sentinel, July 19, 2019, U.S. Central Command, <https://www.centcom.mil/MEDIA/STATEMENTS/Statements-View/Article/1911282/us-central-command-statement-on-operation-sentinel/>.

の促進、安全な航行の確保及び緊張緩和を挙げている。

このように米国は、「海洋安全保障イニシアティブ(Maritime Security Initiative: MSI)」の名の下、「国際海洋安全保障構成体(International Maritime Security Construct: IMSC)」という枠組みを設立して¹¹、11月にバーレーンに司令部を開設し活動を開始した。現在IMSCには、米国に加え、英国、バーレーン、サウジアラビア、UAE、アルバニア、リトアニア、エストニア、ルーマニア、セーシェル、ラトビア、ヨルダンの計12か国が参加している¹²。

日本については、2019年8月7日に開催された日米防衛相会談において、エスパー米国防長官(当時)より、IMSCへの参加要請があったとされるが¹³、日本政府は伝統的に友好関係にあるイランへの配慮や法的制約などから、結局、IMSCへの参加を見送り、独自派遣を行うこととなった。それが冒頭の2019年12月27日の閣議決定である。中東地域への自衛隊の独自派遣については、それに先立つ12月21日の安倍晋三首相(当時)とイランのロハニ大統領(当時)との首脳会談の中で説明され、ロハニ大統領は「自らのイニシアティブで航行の安全確保に貢献する日本の意図を理解している」と述べたと報道されている¹⁴。

その後2020年1月2日には、米軍が、イラン革命防衛隊「コッズ部隊」のソレイマニ司令官をイラクのバグダッド国際空港近くでドローンによって殺害するという事件が起きた。イラン国民に絶大な人気を誇っていたスレイマニ司令官の標的殺害に対してイランは態度を硬化させ、1月5日には、核開発につながるウラン濃縮の制限撤廃を宣言した。1月7日には、弾道ミサイル10数発を、米軍と有志連合軍が駐留するバグダッド西方のアサド空軍基地とイラク北部クルド人自治区のアルビルにある基地に撃ち込んだ。

このように、米・イラン関係が派遣決定時に比べて極度に悪化する中、菅義偉官房長官(当時)は、1月8日の記者会見で、中東地域への自衛隊派遣を予定通り行う方針を改めて示した¹⁵。派遣日程も変更せず、1月11日にはP-3C哨戒機を、2月2日には護衛艦「たかなみ」が日本を出発し、中東地域での情報収集の任務に就いた。

2. その後の展開

2023年10月7日、パレスチナ武装勢力(ハマス及びイスラム聖戦)がガザ地区からイスラエルに数千発のロケット弾を発射するとともに、1500人規模の戦闘員がイスラエル領内に侵入し、イスラエル軍兵士のほか、外国人を含む多数の民間人を殺害・拉致した。これに対してイスラエルは、同日ガザ地区への空爆を、また同月27日以降、ガザ地区内において大

¹¹ IMSCの設立の経緯及び国際法上の位置付けについては、佐藤量介「ホルムズ海峡と有志連合」国際法学会エキスパート・コメントNo.2019-10, <https://jsil.jp/archives/expert/2019-10>を参照。

¹² 防衛省・前掲注(2)参照。

¹³ 東京新聞朝刊(2019年8月8日)。

¹⁴ 毎日新聞朝刊(2019年12月21日)。

¹⁵ 朝日新聞朝刊(2020年1月9日)。

規模な地上作戦を開始し、中東地域の緊張は一挙に高まった¹⁶。

イスラエル・パレスチナ間の紛争は、ガザ地区でのハマスとイスラエル間の戦闘に止まらず、中東の周辺地域にまで拡大している。ハマスとイスラエルとの戦闘が開始されて以降、ハマスへの連帯を示す親イラン武装勢力の活動が中東地域で活発化し、特にイエメンの反政府武装組織ホーシーは民間船舶を狙った攻撃も行っている。ホーシーによる民間船舶への攻撃は、イスラエル船舶のみならず同国と何らかの関係を有する船舶を標的に行われており、2023年11月19日にはイエメン沖の紅海を航行中の日本郵船が運航するバハマ船籍の自動車運搬船ギャラクシー・リーダー号¹⁷が、所有する英国企業の株主にイスラエルの富豪が含まれているという理由で拿捕され、その影響は日本関係船舶にも及んでいる。

こうした事態に対応して、2023年12月、米国は、紅海からアデン湾にかけての海洋安全保障と能力構築のための活動を任務とする第153連合任務群(CTF153)の傘下に多国籍安全保障作戦である「繁栄の守護者作戦 (Operation Prosperity Guardian: OPG)」を立ち上げ、紅海、アデン湾における巡回任務などを行っている¹⁸。

2024年1月12日、米英軍は、カナダ、オランダ、オーストラリア、バーレーンの支援を受け、ホーシー派の軍事拠点などを攻撃した。以降も、米軍は、英軍との共同攻撃を含め、継続的にホーシー派の軍事拠点などを攻撃した。また、ホーシー派と対立するイスラエルも散発的にホーシー派の拠点に対する空爆を実行している¹⁹。

他方で、フランス、イタリア、スペインなどのEU諸国は、当初、米国主導のOPGへの参加を表明していたが、1月12日の米・英によるイエメン領域への攻撃に反発し、米・英の行動と分離する態度を明確に示すために、OPGへの参加を翻して欧州連合海軍部隊の下にEU独自の「アスピデス作戦(Operation Aspides: OA)」を結成した。海上では護衛、パトロール、監視、迎撃の任務のみで活動することを強調しているという²⁰。

このように、2023年10月7日のハマス等によるイスラエルに対するテロ攻撃以降、中東

¹⁶ 防衛省『令和7年版 日本の防衛—防衛白書—』(2025年6月)160頁。なお、イスラエル・パレスチナ紛争をめぐる国際法上の論点については、「焦点：イスラエル・パレスチナ紛争に見る国際法の課題」国際問題 No.722 (2024年12月)所収の各論考を参照。

¹⁷ ギャラクシー・リーダー号は、トルコ西部のキョルフエズを出港し、スエズ運河を経由して紅海に入り、インド西部ピパバブへ向かっていたが、バブ・エル・マンデブ海峡に近い紅海の出口付近にあるイエメン西部ホデイダ沖を航行中に拿捕されたという。拿捕はヘリコプターから降下したホーシー構成員によって行われた。乗員はウクライナやフィリピンなど多国籍の25人で、日本人やイスラエル人は含まれていなかったという。朝日新聞朝刊 (2023年11月21日)。

¹⁸ 防衛省・前掲注(16)188頁。

¹⁹ 上掲書188頁。なお、ホーシーの船舶攻撃に対する米国の対応については、R. Pedrozo, “Houthi Maritime Terrorism: Severing the Iranian Lifeline,” *International Law Studies*, Vol.106 (2025) pp.392-414 に詳しい。

²⁰ 中村進「ウクライナとガザにも繋がる第三の戦場—紅海・アデン湾—商船攻撃を続けるフーシ派 vs 商船保護作戦で対抗する諸外国海軍部隊」国際情報ネットワーク分析 IINA, https://www.spf.org/iina/articles/nakamura_12.html。

地域では、単にガザ地区での戦闘の激化に止まらず、周辺海域での船舶への攻撃事案が多発し、2023年11月19日には、派遣自衛隊部隊の活動海域外であるとはいえ、バブ・エル・マンドブ海峡に近い紅海の出口付近で日本関係船舶がホーシーによって拿捕される事件も起きている。これに対応して、米国をはじめとする各国も新たなオペレーションを立ち上げるなど対応を強化している。

これに対して日本では、先に見た閣議決定で「情勢に顕著な変化があった場合は、国家安全保障会議において対応を検討する」となっており、2024年11月5日の閣議決定²¹、2025年11月7日の閣議決定²²と、2度の閣議決定の機会があったにもかかわらず、「中東地域においては、日本関係船舶の防護の実施を直ちに要する状況にはない」という派遣当初の認識が繰り返され、自衛隊の装備、活動の地理的範囲、不測の事態の発生など状況が変化する場合への対応につき、派遣当時の条件に変更は加えられていない状況にある。

Ⅲ 情報収集活動

1. 情報収集活動の内容と実績

中東地域に派遣された自衛隊の部隊による情報収集活動は「日本関係船舶の安全確保に必要な情報を収集するもの」であり、具体的には、活動海域を航行する船舶の船種、船籍、位置、針路、速力などを確認し、不審な船舶の存在や不測事態の兆候といった、船舶の航行の安全に直接影響を及ぼす情報やその他必要な情報を収集しているとされる。こうして防衛省・自衛隊が収集した情報は、内閣官房、国土交通省、外務省をはじめとする関係省庁に共有しているほか、官民連絡会議などを通じて関係業界にも共有するなど、政府としての航行安全対策に活用されているという²³。

2025年3月31日までの活動実績としては、水上部隊（2022年2月以降、派遣海賊対処行動水上部隊が兼務）が、オマーン湾の公海とアラビア海北部の公海において確認した船舶数は累計で95,444隻、また、航空隊（派遣海賊対処行動航空隊）が、アデン湾の公海とアラビア海北部の西側の公海において確認した船舶数は累計で88,365隻に及んでいるという²⁴。

2. 派遣根拠としての防衛省設置法上の「調査・研究」

2019年12月27日の閣議決定によると、自衛隊の中東地域への派遣は、日本関係船舶の安全確保に必要な情報収集活動を行うためのものであり、その国内法上の根拠は防衛省設置法第4条第1項第18号の規定に基づくものとされる。同法第4条第1項は「防衛省は、次に掲

²¹ 外務省「中東地域における日本関係船舶の安全確保に関する政府の取組」
<https://www.mofa.go.jp/mofaj/files/100756491.pdf>。

²² 外務省・前掲注(4)。

²³ 防衛省・前掲注(16)，263頁。

²⁴ 上掲書，263頁。

げる事務をつかさどる」として、その第 18 号に「所掌事務の遂行に必要な調査及び研究を行うこと」を掲げている。

海上自衛隊が日常的に実施している護衛艦や哨戒機による日本周辺海域での警戒監視活動は、自衛隊法には明記されておらず、この規定を根拠としているという²⁵。また、この規定を根拠とした自衛隊の海外派遣の前例としては、2001 年の米同時多発テロ後に横須賀基地からペルシャ湾に向けて出港した米空母キティホークに海上自衛隊の護衛艦を随伴させた例や、同年 11 月、テロ対策特別措置法に基づく活動の前に、佐世保基地から護衛艦をインド洋に先行派遣した例があるという²⁶。

今回の自衛隊の中東派遣に関しては、なぜ自衛隊法ではなく防衛省設置法の「調査・研究」を根拠として自衛隊を派遣できるのかとの質問に対して、政府は「従来より、この情報収集あるいは平素から行っております警戒監視の根拠についてでございますけれども、これらの活動につきましては、それ自体が実力行使を行うものではなく、公権力の行使を伴うものではございません。そうしたことから、その根拠につきましては、この設置法の防衛省の所掌事務の遂行に必要な調査研究ということで従来より解しているものでございます」²⁷として、情報収集活動それ自体が、実力の行使や公権力の行使を伴うものでないことをその理由に挙げている。

また、第 18 号は「所掌事務の遂行に必要な」調査・研究を行うとしており、今回の派遣はどのような所掌事務に必要なものとして調査・研究を行うのかという点について、政府は、「まず、所掌事務については、……自衛隊の行動に関することを考えております。その行動とは具体的には何かということでございますけれども、……状況が変化した場合に、我が国に関係する船舶の安全を確保するための自衛隊の措置を検討するというふうにしてございまして、……現時点において、この行動としては海上警備行動というのが考えられるんだと思います」²⁸として、同号に言う自衛隊の所掌事務として想定されているのは、自衛隊法第 82 条に規定する海上警備行動であると答えている。

加えて、自衛隊の行動として想定しているのは海上警備行動のみかという質問に対しては、「防衛出動等を想定しているわけではございませんで、現時点において、このかかる措置について、海上警備行動以外に具体的に想定している行動はございません」²⁹と答えている。

こうした質疑応答を経て、2019 年 12 月 27 日の閣議決定では、所掌事務の遂行の必要性に

²⁵ 中島明彦防衛省運用企画局長答弁『第 186 回国会参議院外交防衛委員会会議録』第 21 号（平成 26 年 6 月 5 日）5 頁。

²⁶ 朝日新聞朝刊（2019 年 10 月 22 日）。

²⁷ 榎道明宏防衛省防衛政策局長答弁『第 200 回国会参議院外交防衛委員会会議録』第 2 号（令和元年 11 月 7 日）3 頁。

²⁸ 上掲会議録 5 頁。

²⁹ 上掲会議録 5 頁。

つき、今回の情報収集活動は、「日本関係船舶の安全確保に必要な情報を収集するものであり」、これは、「不測の事態の発生など状況が変化する場合の対応として」「海上警備行動に関し、その要否に係る判断や発令時の円滑な実施に必要である」との整理が行われた。

3. 情報収集活動の地理的範囲

2019 年 12 月 27 日の閣議決定によると、派遣される自衛隊の情報収集活動の地理的範囲は、オマーン湾、アラビア海北部及びバブ・エル・マンデブ海峡東側のアデン湾の三海域の公海（沿岸国の排他的経済水域を含む。）とされている。

米国が主導する「海上安全保障イニシアティブ(MSI)」の活動の地理的範囲が、アラビア海、ホルムズ海峡、バブ・エル・マンデブ海峡及びオマーン湾全域の国際水域(international waters)とされているのに対して、自衛隊の活動の地理的範囲からはホルムズ海峡が除外されているのはなぜか。

この点と関連して、防衛省設置法上の「調査・研究」には地理的要件や安全性という要件は課されているのかという質問に対して政府は、「……情報収集を行う場合には、その根拠は一般的に防衛省設置法の第 4 条第 1 項第 18 号における調査研究ということになります。そこにおいては、地理的な要件や、……安全性といった要件が法律上規定されているわけではございません」として、国内法上は、情報収集活動に地理的な制限は設けられていないとの解釈を示している³⁰。

活動の地理的範囲を上記のように限定したのが国内法上の制約によるものではないとする、それはいかなる制約によるものか。その理由についての政府の説明は以下の通りである。

「我が国は、米国と同盟関係にあり、同時にイランと長年良好な関係を維持するなど、中東の安定に関係する各国と良好な関係を築いています。これを生かし、中東の緊張緩和と情勢の安定化に向け、更なる外交努力を行うこととしています。自衛隊による情報収集活動については、外交努力と調和を図りながら取り組む必要があります。

また、いずれの国も、広大な海域を自国のアセットのみによりカバーすることは困難です。自衛隊による情報収集活動についても、船舶の通航量や関係国の取組の状況等を踏まえて効率的に実施することが必要です。

このような基本的な考え方の下、自衛隊の情報収集活動の地理的範囲について政府として検討を行った結果、ホルムズ海峡からペルシャ湾に至る海域において日本関係船舶の航行が集中する分離航路帯は主にイラン、オマーンを含む沿岸国の領海内であること、もとより、領海における船舶の安全な航行の確保には領海に主権を有する沿岸国が大きな役割を有していること、また、領海内における情報収集活動は沿岸国から無害通航に該当しな

³⁰ 榎道明宏防衛省防衛政策局長答弁『第 200 回国会衆議院外務委員会議録』第 2 号（令和元年 10 月 23 日）12 頁。

いと主張され得ること、ペルシャ湾及びホルムズ海峡の情報については米国や沿岸国を含む関係各国との連携を通じて一定の情報収集が可能であると見られることを総合的に勘案し、ペルシャ湾、ホルムズ海峡においては自衛隊の情報収集を行わないこととしたものがあります。」³¹

ここから、伝統的な友好国であるイランに対する外交的配慮、米国や沿岸国を含めた関係各国との連携を通じた効率的な情報収集の可能性といった要因に加えて、ホルムズ海峡の通航に関する国際法上の制約がその理由になっていることがわかる。

ホルムズ海峡において情報収集活動を実施することはできるかとの質問に対して政府は、「……自衛隊が他国の領海において情報収集活動を行うためには、航行が継続的かつ迅速に行われ、沿岸国の平和、秩序又は安全を害しないものを除いては、沿岸国の同意が必要であると考えております」、「自衛隊が他国の領海で活動する場合、沿岸国との関係で同意を取り付ける場合もあれば、無害通航という形で行う場合も考えられます。無害通航という形で行う場合には、国連海洋法条約に照らして、自衛隊の活動が無害の通航という形で行われる必要がございます」³²と答弁している。

これらの答弁から、日本政府はホルムズ海峡をイラン、オマーンの領海とみなし、その通航には無害通航権の要件を満たすか沿岸国の同意が必要であるとの認識を示している。これに対して米国の声明では、ホルムズ海峡を含む MSI の活動海域は、国際水域(international waters)とされている。このような認識の違いはどこから生じたのか。

国連海洋法条約は、「公海又は排他的経済水域の一部分と公海又は排他的経済水域の他の部分との間にある国際航行に使用されている海峡」(第 37 条)で、「すべての船舶及び航空機は、……通過通航権を有するものとし、この通過通航権は、害されない。」(第 38 条第 1 項)と規定し、国際海峡における通過通航権という新たな制度を創設した。なお、国連海洋法条約以前の 1958 年の「領海及び接続水域に関する条約(領海条約)」では、「外国船舶の無害通航は、公海の一部と公海の一部又は外国の領海との間における国際航行に利用される海峡においては、停止してはならない」(第 16 条第 4 項)として、いわゆる「強化された無害通航権」を定めていた。

国連海洋法条約上の通過通航権は、領海における無害通航権と比較すると、①通航の無害性が要件とされない、そのため、無害でない通航に対して認められる沿岸国の保護権は適用されず、通過通航を否定したり妨害したりすることはできない、②上空飛行の自由が認められる、③潜水艦の潜水航行が認められるなど、外国船舶や航空機の航行・飛行の自由が広く認められる制度である。国連海洋法条約で領海が以前の 3 カイリから 12 カイリに拡大され

³¹ 安倍晋三内閣総理大臣答弁『第 201 回国会参議院会議録』第 2 号(令和 2 年 1 月 23 日) 8 頁。

³² 河野太郎防衛大臣答弁『第 200 回衆議院安全保障委員会議録』第 6 号(令和元年 11 月 15 日) 11 頁。

ることにより、それまで公海部分を残していた国際航行に使用されている海峡の多くが沿岸国の領海になることで、軍艦や軍用航空機の移動の自由が制約されることを危惧した米・ソなどの軍事大国の要求を入れる形で設けられた。

さて、ホルムズ海峡は、イランとオマーンの間に位置し、ペルシャ湾とアラビア海を結ぶ海峡で、最も狭い海域部分は 21 カイリであり、イランとオマーンのそれぞれ 12 カイリの領海が重なり合っている。米国とイランはともに国連海洋法条約の非締約国であり、オマーンは締約国である。他方で、米国とイランは領海条約の締約国であるが、オマーンは非締約国である。イランは、国連海洋法条約の署名時に解釈宣言を行い、国際海峡における通過通航権についてその国際慣習法性を否定し、国連海洋法条約の締約国のみがその創設した権利から利益を享受できるとの立場である³³。

他方で、オマーンも国連海洋法条約の批准時に、オマーンの領海を通航する軍艦について「海洋法条約は、オマーンが自ら平和と安全の利益を保護するために必要な適当な措置をとることを妨げない」旨の解釈宣言を行っているが、国際海峡における通航にはあえて触れていないことから、この沈黙は、オマーンが通過通航権に関する自らの立場を国連海洋法条約の規定に調和させようとしたものとの解釈も存在する³⁴。

また、米国は、国連海洋法条約の非締約国ではあるが、国際海峡における通過通航権は、単に条約上認められるだけではなく、国際慣習法上の権利でもあると主張している³⁵。MSI の活動の地理的範囲にホルムズ海峡を加え、それを含めて「国際水域(international waters)」と呼んでいるのは、米国のこうした解釈の表れであると考えられる。1990 年代初頭以降のホルムズ海峡における国家実行では、通過通航が実際に行使されていることを示していると解されている³⁶。

ホルムズ海峡において情報収集活動を実施することはできるかとの質問に対する答弁を見ると、日本政府としてはホルムズ海峡を領海としてとらえ、そこでの情報収集活動には、沿岸国の同意を得るか、領海における無害通航権の要件を満たす必要があるとして、米国とは異なる認識を示しているように思われる。

日本が実際に行っている情報収集活動や米国をはじめとする MSI のオペレーションが、領海における無害通航権の要件を満たし得る場合があるのか、仮にそれが認められないとして、領海条約上の「強化された無害通航権」としては認められる余地はあるのか、また、国際海峡に適用される通過通航権としてなら認められるのか、を逐一検討してみる必要があるが、おそらく日本政府としては、イランの立場を前提としたとしても、日本として国際法上問題

³³ 坂元茂樹『日本の海洋政策と海洋法〔増補第 2 版〕』（信山社、2019 年）78-79 頁。

³⁴ S. Mahmoudi, “Transit Passage,” R. Wolfrum (ed.) *The Max Planck Encyclopedia of Public International Law*, Vol. IX (Oxford, 2012) p.1039.

³⁵ 坂元・前掲注(33) 79-80 頁。

³⁶ Mahmoudi, *supra* note (34) pp.1039-40.

ないと主張できる安全な海域として、今回の派遣海域を選定したのではないかと考えられる。

4. 情報収集活動に従事する部隊の武器使用権限

情報収集活動に従事する部隊の武器使用権限について、政府は「情報収集を行うという場合において、情報収集の目的として武器を使用するということは認められておりませんので、我々が情報収集を命じるに当たりましては、そうしたことも勘案しながら、その活動の範囲ですとか任務の内容について大臣から御命令いただくということになるかと思います」³⁷と答弁しており、この点は、情報収集活動それ自体が、実力の行使や公権力の行使を伴うものでないとする先に言及した答弁³⁸とも整合している。

もっとも情報収集活動に従事している自衛隊の部隊に対して侵害行為が発生するような場合については、「……あくまで一般論として申し上げれば、防衛省設置法に基づく調査研究に従事している自衛隊部隊に対して侵害行為が発生した場合でございますが、そうした場合には、自衛隊法第 95 条に基づきまして、我が国の防衛力を構成する重要な物的手段である武器等を防護するため、当該武器等を職務上警護する自衛官が、その事態に応じて合理的に必要と判断される限度で武器を使用することができるということになっているところでございます」³⁹として、武器使用が可能との見解が示されている。

自衛隊法第 95 条は、自衛隊の武器等の防護のための武器の使用に関する規定で、「自衛官は、自衛隊の武器、弾薬、火薬、船舶、航空機、車両、有線電気通信設備、無線設備又は液体燃料（以下「武器等」という。）を職務上警護するに当たり、人又は武器等を防護するため必要であると認める相当の理由がある場合には、その事態に応じ合理的に必要と判断される限度で武器を使用することができる。ただし、刑法第三十六条又は第三十七条に該当する場合のほか、人に危害を与えてはならない。」と規定している。

この規定にあるように、武器を使用できるのは、「職務上」武器などの警護に当たる自衛官に限られることから、「調査・研究」に従事する部隊の隊員がそうした権限を付与されることのないままに、例えば攻撃から自らの護衛艦を防護するために第 95 条を根拠に武器使用を行うことはできないと考えられる。

中東海域に派遣された海上自衛隊の部隊の隊員は、設置法第 4 条第 1 項第 18 号の規定に基づき派遣された以外に、自衛隊法第 95 条に基づく武器等防護の任務を付与されているのかについては、2019 年 12 月 27 日の閣議決定でも国会答弁でも、必ずしも明らかではない。

³⁷ 榎道明宏防衛省防衛政策局長答弁『第 200 回国会衆院外務委員会議録』第 2 号（令和元年 10 月 23 日）12 頁。

³⁸ 榎道・前掲注(27) 3 頁。

³⁹ 榎道・前掲注(37) 5 頁。

IV 海上警備行動⁴⁰

1. 保護対象

自衛隊法第 82 条は、「海上における人命若しくは財産の保護」や「治安の維持」のため特別の必要がある場合に、防衛大臣が内閣総理大臣の承認を得て自衛隊の部隊に海上警備行動を発令できる旨を規定している。

この規定でいう「海上における人命若しくは財産」とは、基本的には日本国民の生命又は財産を意味すると解されており、2019 年 12 月 27 日の閣議決定では、その航行の安全を確保する対象となる「日本関係船舶」は、①日本籍船、②日本人が乗船する外国籍船、③我が国船舶運航事業者が運航する外国籍船、④我が国の積み荷を輸送している外国籍船であって我が国国民の安定的な経済活動にとって重要な船舶とされている。

このうち④について、政府は「一般に、当該船舶が輸送している我が国の積荷の内訳等を踏まえつつ、個別具体的な状況に応じて判断する必要がある」として、「当該外国船が輸送する全ての積荷が我が国を仕向地とするものでなければならない等の基準を設けているわけではない」とした上で、「原油等のエネルギー資源を積荷として我が国に輸送する外国籍船については、これらの積荷が我が国国民の安定的な経済活動にとって重要であることを踏まえ」、基本的には「我が国国民の安定的な経済活動にとって重要な船舶」に該当し得るとしている⁴¹。

2. 発令要件

海上警備行動が発令される「不測の事態」とはどのような場合かについて、政府は、「…日本関係船舶に対する侵害行為の発生が迫っている場合、あるいは侵害行為が発生した場合など、航行の安全に危険が生ずるような場合を想定しているところでございます」⁴²としていることから、日本関係船舶に対して実際に「侵害行為が発生した場合」のみならず、「侵害行為の発生が迫っている場合」を含め、広く、日本関係船舶の「航行の安全に危険が生ずるような場合」を想定していると言える。

⁴⁰ 2019 年 12 月 27 日の閣議決定で想定されていた自衛隊の「海上警備行動」をめぐる法的問題について、筆者は既に、2021 年 5 月段階で明らかだった事実や研究状況を基に、「海上警備行動の国際法上の根拠についての一考察—海上自衛隊の中東地域派遣をめぐる議論を手掛かりに—」柳原正治ほか編『（間宮勇先生追悼）国際秩序とグローバル経済』（信山社、2021 年 9 月）33-65 頁で詳細な検討を行っている。本稿の海上警備行動に係る部分の記述は、同論文の内容を簡素化しつつ、その後の事実の変化や研究状況の進展を踏まえて、内容を補足・修正したものである。

⁴¹ 『中東地域における日本関係船舶の防護と国際法上の旗国主義に関する質問に対する答弁書』（内閣参質 201 第 60 号）（令和 2 年 3 月 10 日）1 頁。

⁴² 河野太郎防衛大臣答弁『第 201 回国会衆議院安全保障委員会議録』第 2 号（令和 2 年 4 月 2 日）3 頁。

3. 措置をとり得る相手

海上警備行動に基づき措置をとり得る相手について、政府は「……あくまで一般論として申し上げますと、海上警備行動は、海上における人命若しくは財産の保護又は治安の維持を目的として、いわゆる警察権の行使として行うものでございます」、「海上警備行動を命ぜられた自衛官による武器使用につきましては、その相手方が武力攻撃を行っている国又は国の組織（「国に準ずる組織」の誤りか―筆者）であることが明らかな場合には、警察権の範囲を超え、認められないものであろうというふうに理解をしております」⁴³としている。

4. とり得る措置と国際法上の根拠

海上警備行動が発令された場合にとり得る措置とその国際法上の根拠について、日本政府の立場⁴⁴を整理すると、以下のようになる。

(1) 日本籍船に対する侵害の場合

公海上で日本船籍に対する侵害行為が発生した場合には、侵害の程度に応じて、武器の使用を伴わない措置をとることが可能になる。また、自衛隊法第 93 条第 1 項で準用する警察官職務執行法第 7 条に基づき、その事態に応じ合理的に必要と判断される限度で武器の使用が認められる。国際法上も、これを排除するためにほかに適当な手段がない場合に、このような武器の使用が認められる⁴⁵。

(2) 日本船籍でない日本関係船舶、外国籍船に対する侵害の場合

他方で、日本船籍でない日本関係船舶、あるいは外国船籍の場合には、個別具体的な状況に応じて判断せざるを得ないが、（日本船籍でない）日本関係船舶の場合には、呼びかけや近接といった実力の行使を伴わない措置を行うことができ、（日本関係船舶でない）外国船籍の場合にも、通報あるいは人命救助といった人道上必要とされる措置は行い得る⁴⁶。

(3) 国際法上の根拠

日本籍船と外国籍船の場合とでこのような違いが出るのは、公海上における外国籍船の防護については、国際法上、一般的には当該船舶への排他的管轄権を有する旗国がその責任のもとに行うべきとの旗国主義の考えに基づき対処することが基本であるから⁴⁷とされる。

⁴³ 樋道明宏防衛省防衛政策局長答弁『第 200 回国会参議院外交防衛委員会会議録』第 2 号（令和元年 11 月 7 日）6 頁。なお、「国に準ずる組織」について政府は、「国家に準ずる組織については、国際法上、確立された定義があるわけではありませんが、他方で、従来から、政府としては、国家に準ずる組織について、国家そのものではないがそれに準ずるものとして国際紛争の主体たり得るものとして用いてきております」と答弁している（茂木敏充外務大臣答弁『第 200 回国会衆議院安全保障委員会会議録』第 9 号（令和 2 年 1 月 17 日）10 頁）。

⁴⁴ この点に関する政府の具体的な答弁内容については、森川・前掲注(40) 41-42 頁を参照。

⁴⁵ 河野太郎防衛大臣答弁『第 201 回国会衆議院予算委員会会議録』第 2 号（令和 2 年 1 月 27 日）15 頁。

⁴⁶ 上掲会議録 15 頁。

⁴⁷ 安倍晋三内閣総理大臣答弁『第 201 回国会衆議院本会議録』第 3 号（令和 2 年 1 月 23 日）20 頁。

以上のように、政府の説明によると、保護対象船舶が日本籍船か、外国籍船かによって海上警備行動としてとり得る措置に違いが生じること、また、そうした違いは、「旗国主義の原則をはじめとする国際法」を踏まえた結果であるとされる。

V 海上警備行動の国際法上の根拠

1. 公海上で旗国以外の国がとり得る措置とその対象

山本草二教授によると、「公海上の船舶に対する管轄権は、国際慣習法によればその旗国に専属的に帰属すること（旗国管轄）を原則とし、少なくとも執行・司法管轄権については、そうである。外国船舶が域外で行う犯罪その他の違法行為に対して、旗国以外の国が各種の基準（属地主義、国籍主義、受動的属人主義、保護主義）を用いて内国刑事法令（立法管轄権）の域外適用をはかることは許容される場合があるにしても、強制措置を伴う執行・司法管轄権そのものは、当該容疑船舶の旗国に専属するのが原則だからである。……このような旗国管轄の原則の重要な例外・補完をなすものとしては、海賊の規制がある。この場合には、旗国以外の一般の第三国に対して公海上で広範な海上執行措置（臨検、拿捕、抑留、押収、逮捕、引致）の行使が認められ、さらにその起訴・処罰についての司法管轄権も与えられる」⁴⁸という。

これまで海上自衛隊に海上警備行動が発令された事例⁴⁹のうち、2009年のソマリア海賊事案は、国際慣習法上も旗国主義の例外とされる海賊の規制に関するものであった。海賊を対象とするものであれば、たとえ措置の対象となる船舶が他国を旗国とするものであったとしても、海上警備行動として、公海上で広範な海上執行措置の行使が可能となる。しかし、当初は海上警備行動としてソマリア沖に派遣された海上自衛隊の活動は、海賊対処法が制定されたことにより、海上警備行動としてではなく、海賊対処法第7条と自衛隊法第82条の2に基づく海賊対処行動として行われることになった。

海賊対処法第7条第1項は、海賊対処行動が発令された場合には、海上警備行動に関する自衛隊法第82条の規定は適用しないとしているが、その趣旨は、海賊対処行動が発令されている活動については、海上警備行動を根拠にすることはできないということであり、海賊対処行動が発令されていない活動については、その国内法上の根拠が自衛隊法第82条の海上警備行動である場合であっても、国際法上は海賊対処に当たる活動まで排除されているわけではないと考えられる。

現在中東地域に派遣されている自衛隊の護衛艦は、当初は海賊対処行動に従事する自衛隊の護衛艦とは別途に、防衛省設置法に基づく「調査・研究」を根拠に派遣されていた。しか

⁴⁸ 山本草二「海上執行をめぐる国際法と国内法の相互関係」山本草二編集代表『海上保安法制』（三省堂、2009年）11頁。

⁴⁹ これまで海上警備行動が発令された事例について詳しくは、森川・前掲注(40) 47-52頁参照。

し、2021 年 12 月 24 日の閣議決定以降は、既に海賊対処行動に従事している自衛隊の護衛艦に、併せて「調査・研究」権限が付与されて情報収集活動に従事している。そうだとすると、情報収集活動に従事する自衛隊の護衛艦が不測の事態に直面した場合であっても、措置をとり得る相手が海賊である限り、新たに海上警備行動の発令を行うことなく、国際法上は、公海上で広範な海上執行措置をとり得ることになるのか。

この点に関しては、海賊対処行動が認められている活動海域と、情報収集活動が認められている活動海域の違いを考慮に入れる必要がある。前者については、ソマリア沖及びアデン湾に限定されており⁵⁰、情報収集活動の認められる海域と一部重なるものの、後者の活動海域であるオマーン湾及びアラビア海北部は、前者の活動海域に入っていない。したがって、活動海域が重なる海域については、措置をとり得る相手が海賊である限り、新たに海上警備行動の発令を行うことなく、国際法上は、海賊対処を根拠に公海上で広範な海上執行措置をとり得ることになるが、それ以外の海域では、不測の事態が生じた場合、海賊対処行動ではなく、新たに海上警備行動の発令を待たなくてはならないことになる。その際、相手が最初から海賊であることが明らかであれば、海賊対処行動の活動範囲を拡大することで対処することも可能であるが、2021 年 12 月 24 日の閣議決定以降の閣議決定においても、「不測の事態の発生など状況が変化する場合への対応」として想定されているのは、海上警備行動である。そうだとすると、日本関係船舶への侵害行為として想定されているのは、第一義的には、海賊対処行動としての対処が可能な海賊行為ではないと考えられる。

この点に関連を有すると考えられるのは、2015 年 5 月 14 日の「公海上で我が国の民間船舶に対し侵害行為を行う外国船舶を自衛隊の船舶等が認知した場合における当該侵害行為への対処について」という閣議決定⁵¹である。この閣議決定は、自衛隊の船舶または航空機による警戒監視等の活動中に、公海上で日本の民間船舶（日本の船籍を有する民間船舶）に対して海賊行為その他日本に対する外部からの武力攻撃に該当しない不法な暴力行為、抑留または略奪行為を行う外国船舶を認知した場合の対処を定めたもので、こうした侵害行為に対して海上保安庁では対応できない場合に、自衛隊の部隊に海上警備行動や海賊対処法に基づく海賊対処行動を発令して対処することを定めている。この閣議決定にいうところの海賊行為以外の「その他日本に対する外部からの武力攻撃に該当しない不法な暴力行為、抑留または略奪行為」として、いかなる違法行為が想定されているのか、また公海上でかかる違法行為に海上警備行動として対処する際の国際法上の根拠は何かということが問題となる。

⁵⁰ 防衛省「海賊対処行動に係る内閣総理大臣の承認について（令和 6 年 11 月 5 日閣議決定）」
https://www.mod.go.jp/j/approach/kokusai_heiwa/somaria/pdf/20241105a.pdf。

⁵¹ 内閣官房「公海上で我が国の民間船舶に対し侵害行為を行う外国船舶を自衛隊の船舶等が認知した場合における当該侵害行為への対処について」
<https://www.cas.go.jp/jp/gaiyou/jimu/pdf/senpakusingaikouitaisho.pdf>。

2. SUA 条約および改正議定書

(1) 1988 年の SUA 条約

海賊行為以外の海上における違法行為への管轄権の行使を広く認める条約としては、海洋航行不法行為防止条約（1988 年の SUA 条約）⁵²がある。同条約は、伝統的な海賊行為概念の類推に困難を生じさせる海上暴力行為⁵³のうち、不法かつ故意に行われる、暴力等を用いて船舶を奪取・管理する行為（第 3 条第 1 項(a)）、船舶の安全な航行を損なうおそれがある当該船舶内の人に対する暴力行為（同項(b)）、船舶を破壊したり、船舶・積荷に当該船舶の安全な航行を損なうおそれがある損害を与えたりする行為（同項(c)）など、特に海洋航行の安全を害する犯罪について、裁判管轄権の設定と国際協力を通じて、犯人の処罰を確実なものにするための多数国間条約である。

この条約によると、犯罪行為が、自国を旗国とする船舶に対して（客観的属地主義）、またはその船舶内で行われた場合（旗国主義）に限らず、自国民によって行われた場合（能動的属人主義）にも裁判管轄権を設定しなければならず（義務的管轄）、また、犯罪が自国民に対して行われた場合（受動的属人主義）にも裁判管轄権を設定することが認められる（任意的管轄）。もちろん、こうした立法管轄権を基礎として、海上警察機関がそれを執行するために、他国を旗国とする船舶に執行管轄権を行使できるかは別の問題であり、1988 年の SUA 条約では、この点について一般法を修正する条約上の仕組みはなんら導入されなかった。

(2) 2005 年の改正議定書

これに対して、2005 年の SUA 条約改正議定書⁵⁴は、締約国に対して条約に規定する不法な行為を防止し、抑止するための協力義務を課し（第 8 条の 2、第 1 項）、そのための具体的な執行措置の内容や手続きを定めている点に最大の特徴がある。すなわち、① 締約国（要請国）の法執行機関が、領海外において、他の締約国（国籍被表示国）の旗を掲げる船舶に遭遇し、条約の対象犯罪に関与し、または関与しようとしていると疑うに足る合理的な根拠があり、かつ乗船を希望する場合には、要請国は国籍被表示国に対して、国籍確認を要請し、

⁵² 正式名称は、「海洋航行の安全に対する不法な行為の防止に関する条約(Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation)」。1988 年 3 月に作成、1992 年 3 月に発効。2025 年 12 月現在、締約国は 166 カ国。日本は 1998 年 4 月に同条約に加入、同年 7 月に日本について発効した。

⁵³ 海賊行為概念の類推に伴う困難としては、①海賊行為は、行為が遂行される場所や容疑船舶を拿捕できる場所が、「公海その他のいずれの国の管轄権にも服さない場所」に限られるため、内水や領海など沿岸国の管轄権が及んでいる場所で生じた暴力行為やそこに逃げ込んだ海賊船舶に対して、沿岸国に取締りを行う意思や能力が欠けている場合には、有効な規制が期待できないこと、②海賊行為は、複数の船舶間で外部から行われる侵害行為であるため、船舶内部にいる乗組員や旅客よる船舶の不法奪取（シージャック）は海賊行為には該当しないこと、③海賊行為は、「私的目的のために行われる」行為であることから、政治的目的の実現を標榜する海上テロ行為へは適用できない可能性があること、などが挙げられる。この点について詳しくは、森川幸一「海上暴力行為」『海上保安法制』295-298 頁を参照。

⁵⁴ 2005 年 10 月に作成、2010 年 7 月に発効。2025 年 12 月現在、締約国は 54 ヶ国。日本は未批准。

対象犯罪への関与を決定するために行われる乗船、搜索等についての授權を要請する（第 8 条の 2、第 5 項(a)）。② 国籍が確認された場合、旗国はこれに対して可能な限り迅速に回答する義務を負い、(i) 授權を与える、(ii) 自国で執行する、(iii) 共同で執行する、(iv) 授權を拒否する、のいずれかの回答を行う（第 8 条の 2、第 5 項(c)）。③ 条約を締結する際（またはその後）に、各締約国は、国際海事機関（IMO）事務局長に対して、国籍確認の要請に 4 時間以内に回答がない場合、要請国に対して、対象犯罪への関与を決定するために行われる乗船、搜索等の権限が与えられることを通知できる（第 8 条の 2、第 5 項(d)）、というものである。

こうした公海上の他国を旗国とする船舶に対する執行措置に関する規定は、1988 年の SUA 条約には見られなかったもので、2005 年の SUA 条約改正議定書は、締約国が自国の旗を掲げる船舶について、国籍確認要請の受領から 4 時間以内に回答がない場合に、要請国が乗船等を行うことを授權する通知を予め行っておくための手続き（第 8 条の 2、第 5 項(d)）を定めるなど、要請国が国籍被表示国から授權を受けることを容易にする仕組みを提供している点で、伝統的な旗国主義の問題を克服するための工夫が施されている。しかし、そうした事前の包括的授權を行っていない締約国に対しては、なお個別の授權を得る必要があり、要請国は旗国の明示的な同意なしに乗船等を行うことができない旨が明記されている（第 8 条の 2、第 5 項(c)）。この点、旗国の同意を得ることなく臨検が可能な海賊行為の場合とは異なり、伝統的な旗国主義の原則はここでも堅持されている。

2015 年 5 月 14 日の「公海上で我が国の民間船舶に対し侵害行為を行う外国船舶を自衛隊の船舶等が認知した場合における当該侵害行為への対処について」という閣議決定では、海上警備行動を発令して日本籍船を防護する際の具体的な措置については言及されていなかったが、本稿の IV で明らかにしたように、現在、中東地域に派遣されている自衛隊の護衛艦に海上警備行動が発令された際に、侵害行為が日本籍船に対するものである場合には、侵害の程度に応じて、武器の使用を伴わない措置から、その事態に応じ合理的に必要と判断される限度で武器の使用も認められるとされている。しかし、そのような措置を外国を旗国とする船舶に対して公海上でとり得る国際法上の根拠はどこに求められているのであろうか。最後にこの点について検討してみる必要がある。

3. 海上警備行動でとり得る措置と旗国主義

国連海洋法条約は、「船舶は、一の国のみの旗を掲げて航行するものとし、……公海においてその国の排他的管轄権に服する」（第 92 条）とした上で、「いずれの国も、自国を旗国とする船舶に対し、行政上、技術上及び社会上の事項について有効に管轄権を行使し及び有効に規制を行う」と規定している（第 94 条）。旗国主義とは、公海上で、自国を旗国とする船舶に対しては、他国の干渉を排除して、旗国のみが有効に管轄権を行使し有効に規制を行

い得ることを定めた原則である。

確かに、公海上で、①外国籍船から日本籍船に対して武力攻撃に該当しない不法な暴力行為等が行われる場合、②外国籍船の乗組員が日本籍船に乗り込んで不法な暴力行為を行う場合、③日本人の船員に対して同様な行為を行う場合は、それぞれ客観的属地主義、旗国主義、受動的属人主義を根拠として、公海上にも立法管轄権を域外適用して、容疑者の身柄を確保できれば、日本で裁判管轄権を行使できることは確かである。

これに対して、被害船舶が外国籍の日本関係船舶である場合は、被害者が日本人である場合（受動的属人主義）を除けば、被害船舶の旗国に管轄権があり、日本として裁判管轄権を行使できないという違いがある。そのような意味では、国際法上の旗国主義を根拠として、被害船舶が日本籍船である場合と外国籍の日本関係船舶の場合とで、とり得る措置が異なるとすることに、まったく理由がないわけではない。しかし、こうした違いは、あくまで立法管轄権上の違いであり、執行管轄権については、被害船舶が日本籍船か外国籍の日本関係船舶かの区別とは無関係に、加害船舶の旗国との関係で、被害船舶の安全を確保するために加害船舶に対して執行措置をとれるかどうかが問題となる。

海上警備行動が発令される「不測の事態」とはどのような場合かについて、政府は、日本関係船舶に対して実際に「侵害行為が発生した場合」や「侵害行為の発生が迫っている場合」を含め、広く、日本関係船舶の「航行の安全に危険が生ずるような場合」を想定しているとしている。

このうち「侵害行為が発生した場合」としては、例えば、外国籍の加害船舶の乗組員が被害船舶に乗り込んできて不法な暴力行為等を行う場合が考えられる。このような場合には、被害船舶が日本籍船であれば、その船内に日本の執行管轄権も及んでいるので、海上自衛官が被害船舶に乗り込んで不法な暴力行為等を行う容疑者を拘束することも可能である。しかし、被害船舶が外国籍の日本関係船舶の場合には、当該被害船舶の旗国の同意がない限り、そうした執行措置を執ることはできない。こうした場合については、執行措置についても、被害船舶が日本籍船か外国籍船かで違いが出ることもについても旗国主義によって説明可能であろう。

他方で、「侵害行為が発生した場合」のうち、加害船舶から被害船舶へ不法な発砲や体当たりが行われることにより被害船舶の「航行の安全に危険が生ずるような場合」については、海上自衛官は、「海上における人の生命若しくは身体に対する危険又は財産に対する重大な損害を及ぼすおそれがある行為を制止する」（自衛隊法第93条第2項、海上保安庁法第18条第1項）ための措置を加害船舶に対してとることになると思われる。

また、日本関係船舶への不法行為を未然に防止するという観点からはより重要だと思われる「侵害行為の発生が迫っている場合」、例えば、不審な外国船舶が日本関係船舶に接近してくるような場合には、当該不審船舶に対して、停船命令、立入検査、職務質問、制止等の

措置をとること（自衛隊法第93条第2項、海上保安庁法第17条）が予想され、上記「侵害行為が発生した場合」の対応を含め、これらの職務の執行には、警察官職務執行法第7条の規定が準用されることになる（自衛隊法第93条第1項）⁵⁵。

これらいずれの場合にも、日本の国内法上は海上警備行動として対応が可能であるが、国際法上は、当該加害船舶や不審船舶が、海賊対処法が適用されるような海賊ではなく、また日本籍船でもないことを前提とすると、その旗国の同意があるか、他に条約上の根拠がない限り、かかる執行措置をとることはできないことになる。この点では、加害船舶の船籍こそが重要であり、被害船舶や被害を受けるおそれのある船舶が、日本籍船か外国籍船かの区別は重要な意味を持たない。

2005年のSUA条約改正議定書は、海洋航行の安全を害する犯罪について、1988年のSUA条約を補完し、執行措置の面で伝統的な旗国主義を修正しようとしたものであり、その限りでは、公海上での海上警備行動で想定されている外国を旗国とする加害船舶や不審船舶に対する執行措置の国際法上の根拠を強化するものになり得るものと考えられるが、日本はこの改正議定書を批准していない。

V むすびにかえて

自衛隊の護衛艦が初めて公海上での本格的な海上警備行動を実施したソマリア海賊事案では、海上警備行動によって保護の対象となる「海上における人命若しくは財産」は、基本的には日本国民の生命または財産と解されていたため、日本籍船のみならず外国籍船であっても日本関係船舶であれば、その保護の対象となると考えられていた⁵⁶。また、そこで想定されていた日本関係船舶への侵害行為は、国際慣習法上、旗国以外の第三国に対して公海上で広範な海上執行措置の行使が認められている海賊行為であったため、日本が実施した海上警備行動の国際法上の根拠は、当時まったく問題とはならなかった。

それに対して、今回の中東地域への自衛隊の護衛艦等の派遣は、現時点ではそうであるよ

⁵⁵ ちなみに海賊対処法では、警察官職務執行法第7条の規定に基づく武器の使用が認められる以外にも、現に行われている海賊行為のうち他の船舶への著しい接近、つきまとい、進路妨害に係るもの（海賊対処法第2条第6号）の制止に当たり、当該海賊行為を行っている者が、他の制止の措置に従わず、なお船舶を航行させて当該海賊行為を継続しようとする場合、「当該船舶の進行を停止させるために他に手段がないと信じるに足る相当な理由のあるとき」には、「その事態に応じ合理的に必要と判断される限度において」武器を使用することが認められる（同第6条）として、新たに「停船射撃」が認められたが、海上警備行動では認められないと解される。

⁵⁶ 2009年当時の政府の整理では、外国籍の船舶も含めて日本関係船舶を広く武器の使用が可能な海上警備行動の対象にしたのに対して、今回想定されている海上警備行動については、日本関係船舶がその保護の対象であるとする見解を維持しながらも、政府が「旗国主義」を根拠に、襲撃に対する武器の使用は日本籍船に限られ、外国籍の日本関係船舶は他の外国籍船と同様に実力の行使を伴わない措置に留まるという解釈を示した点に、疑問を呈する見解もある。中村進「日本は国際海運の保護にどう向き合うのか（後篇）—フーシ派の無差別攻撃が示唆する日本の商船保護の現状と課題」国際情報ネットワーク分析 IINA, https://www.spf.org/iina/articles/nakamura_13.html。

うに、実力の行使を伴わない「調査・研究」にとどまっている間は国際法上の問題は生じないとはいえ、今後不測の事態が生じて、それが海上警備行動に切り替えられた場合、本稿で検討してきたように、そこでの執行措置の国際法上の根拠が問われることになる。

不測の事態が生じた場合の対応として、海賊対処行動ではなく海上警備行動が予定されていることからすると、中東地域で日本関係船舶の航行の安全を侵害する行為として想定されているのは、ソマリア周辺海域でのような身代金目当ての海賊ではないということになるだろう。他方で、国や国に準ずる組織による侵害行為も想定されていないとなると、考えられるのは、国や国に準ずる組織でもないような武装組織による侵害行為である。政府は、イラン革命防衛隊は国軍の一部であるとしているものの⁵⁷、米国がテロ組織として再指定した⁵⁸、親イランの武装組織であるイエメンのホーシーについては、「現時点において政府として、国家に準ずる組織であるか否かについて判断を行っておりません」⁵⁹と述べるにとどまり、その可能性を否定してはいない。

こうした武装組織を、仮に国や国に準ずる組織ではなく私的な犯罪集団とみなすのであれば、これらの組織による公海上での日本関係船舶への侵害行為は、基本的には 1988 年の SUA 条約とそれを執行措置の面で強化した 2005 年の SUA 条約改正議定書に基づき対処すべきものということになるだろう。もっとも既に見たように、日本は未だ改正議定書を批准しておらず、また仮に批准したとしても、締約国が 54 ヶ国にとどまっている現状では、締約国間で働く簡便な授權手続は適用されず、結局は旗国の個別の授權を得られない限り、外国船舶を使用したこれら武装集団の侵害行為に対して有効な執行措置はとれないことが予想される。

それではこうした武装組織による暴力行為と海賊行為との区別はどのようにして可能になるのか。周知のように国際法上の海賊行為とは、私有の船舶が「私的目的」⁶⁰のために行う「不法な暴力行為、抑留又は略奪行為」とされ（国連海洋法条約第 101 条）、日本の海賊対処法も同様に「私的目的」を海賊行為の要件としている（第 2 条）。もっとも SUA 条約が対象にしているような海上テロリズム行為を「私的目的」によるものではないとして海賊行為から除外すべきかについては、国際法学上賛否両論があることも、また事実である⁶¹。

⁵⁷ 茂木敏充外務大臣答弁『第 200 回国会参議院予算委員会会議録』第 1 号（令和 2 年 1 月 29 日）33 頁。

⁵⁸ Pedrozo, *supra* note (19), pp.403-408.

⁵⁹ 茂木敏充外務大臣答弁、前掲注(57) 10 頁。

⁶⁰ 国際法上の海賊行為概念に係る「私的目的」要件について詳しくは、森田章夫「国際法上の海賊（Piracy *Jure Gentium*）—国連海洋法条約における海賊行為概念の妥当性と限界—」国際法外交雑誌第 110 巻 2 号（2011 年）1-24 頁を参照。

⁶¹ 奥脇直也「海上テロリズムと海賊」国際問題 No.583（2009 年 7・8 月）20-33 頁、特に注(15)参照。もっとも奥脇教授自身は、海上テロリズムはある場合には海賊の要件に形式的には当てはまるようにみえる場合があるが、海賊による普遍的管轄権は海賊による通商破壊から海上交通・国際交易の安全を確保するためのものであるのに対して、SUA 条約は船舶の運航支配を奪取したり船舶を破壊し

このように「私的目的」によるものか否かを判断するための基準についても争いがあるとすると、現に日本関係船舶が侵害を受けている現場で、海賊行為かそれ以外の暴力行為かを判断することは、実際には至難の業であるように思われる。そうだとすると、現場でそうした侵害行為に直面した海上自衛官は、まずはその行為を国際法上の海賊行為とみなして、それを制止させるための執行措置をとることも考えられないわけではない。中東地域に派遣されている自衛隊の部隊は、派遣当初はそうでなかったとはいえ、2021年12月24日の閣議決定以降は、既に海賊対処行動を命じられている護衛艦によって情報収集活動を兼務している。したがって、海賊対処行動の活動海域である限りでは、情報収集活動を行っている自衛隊の護衛艦が不測の事態に直面した場合、新たに海上警備行動の発令を待つことなく即応できるというメリットもある。またそれ以外の海域では、なお、海上警備行動の発令が必要になるが、海賊対処行動が発令されていない海域であれば、海上警備行動を国内法上の根拠として、国際法上は海賊対処を行うことも、海賊対処法7条1項の解釈上は可能であると考えられる。

日本政府はそうのように特定していないとはいえ、イラン革命防衛隊によるものと思われるコクカ・カレイジャス号爆破事件が起きた2019年時点と、ホーシーによるギャラクシー・リーダー号拿捕事件が起きた2023年以降では、本稿のⅡでも概観してきたように、中東地域の海洋安全保障環境も大きく変化してきている。そうした中で、日本関係船舶の安全確保をいかに万全に図っていくか、海賊対処行動で対応できない場合に想定し得る海上警備行動の国際法上の根拠の明確化に向けた一層の検討が必要だと思われる⁶²。

【付記】本稿脱稿後の2026年2月28日、米国とイスラエルはイランに大規模な軍事攻撃を行い、イランはこの攻撃に対する自衛措置として、イスラエルや、米軍基地のある湾岸諸国に軍事攻撃を行うとともに、ホルムズ海峡を事実上閉鎖する措置に及んでいる。そのため米国はペルシャ湾やホルムズ海峡を通航する船舶の安全確保のために諸国に艦船を派遣することを求めているという。本稿が対象とした既に中東に派遣されている自衛隊の護衛艦は、ペルシャ湾やホルムズ海峡をその活動海域に含んでおらず、また仮に海上警備行動を発動したとしても、イランの国軍である革命防衛隊を対象とすることはできない。その意味で、日本が自衛隊の護衛艦を派遣するためには、その法的枠組みは、別途考察されなければならない。

たりする行為について処罰を確保することにより、船舶の安全な運航を確保するものであり、両者の法制はその保護法益が異なるゆえにまったく異なる、との立場である。

⁶² ホーシーによる船舶攻撃に見られるような「紅海危機」を念頭に、日本の自衛隊がとり得る実力措置としての海上警備行動と海賊対処行動の意義と限界を検討した論考として、石井由梨佳「船舶を防護する権利—紅海危機における各国の対応を手がかりに」国際問題 No.722（2025年12月）50-63頁がある。また、本稿とは別の切り口ながら、国連海洋法条約には合法的な海洋の利用に対する妨害への法的対処の根拠となる権利が万全に設定されていないとはいえ、このような法的対処の権利を総称して「海洋の利用を保護する権利（「保護権」）」と呼び、その理論的な枠組みの構築を試みた興味深い論考として、A. Kanehara, “The Houthi Rebels’ Attack against Japan-Related Vessel in the Red Sea—An Idea of ‘the Right to Protect Uses of Sea’—”, Canon Institute for Global Studies, https://cigs.canon/updates/2024/12/paper_kanehara_241213.pdf がある。

第 2 章

ハイジャック航空機によるテロへの対応
ードイツ判例からの考察，原発防護を念頭においてー

東京大学大学院教授
斎 藤 誠

I はじめに

2022年3月、ロシアによるウクライナ・ザポリージャ原子力発電所への攻撃は、原子力発電所のセキュリティ・セーフティ両面での安全性に、衝撃をもたらした。従来、あり得るリスクとして、そのような事態は机上では議論され「想定外」ではなかったにせよ、現実のものとなるとフェーズはまた異なる。分断と対立が深まる世界において、その修復の道を模索し続けることは不可欠であるが、このようなリスクへの備えもまた切実な課題となった。

国際班においても、既に、2023年初頭に森川主査、原田研究委員の報告がなされたところである¹。また、2023年2月24日には、笹川平和財団 安全保障研究グループ「核不拡散・核セキュリティ研究会」（座長 鈴木 達治郎氏）による政策提言「原子力施設の保護と日本の役割～ロシアによるウクライナ侵攻と原発攻撃をうけて～」が公表されている²。

以下、まず、国際的な対応策を示す素材として、この提言を掲出する。

提言1：戦時下における原子力施設の保護に関する提言

「戦時下の原子力施設の保護は万全ではない。国連安全保障理事会が本来の機能を果たせず、結果として原子力施設の保護に関与できない事態が起きている。そのため、国際原子力機関(IAEA)が戦争当事国および周辺国と協議し、原子力施設の保護を支援する仕組みを新たに構築する必要がある。例えば、IAEAが提唱している「原子力安全保護地帯」(Nuclear Safety and Security Protection Zone)の設立、戦時下の活動で実績がある国際赤十字委員会(ICRC)との協力、さらには安保理が機能しない場合に備え、国連総会決議による「国連緊急原子力安全ミッション」(Nuclear Emergency Safety Mission: NESM)の派遣などの仕組みを検討することを提言する。国際社会で早期にこうした仕組みづくりに関する議論をスタートさせ、日本がその議論を主導するべきである」

提言2：原子力施設の保護強化への国際法の改正など将来の取り組みに関する提言

「今後、原子力施設を有する国やその周辺国が戦争当事国になった場合を想定し、原発への攻撃を原則禁じているジュネーヴ条約や原子力に関する国際条約の改正や追記により、原子力施設への軍事行動を全面的に防止すべく、実現への課題を含め国際社会は早急に話し合

¹ それぞれの報告のアウトラインについては、日本エネルギー法研究所季報 280 号 12 頁の「研究班の動き」欄を参照。

² 公益財団法人笹川平和財団 安全保障研究グループ 核不拡散・核セキュリティ研究会「原子力施設の保護と日本の役割～ロシアによるウクライナ侵攻と原発攻撃をうけて～」(2023 年 2 月 24 日)、https://www.spf.org/global-data/user26/20230224_PolicyRecommendation.pdf (最終閲覧日：2024 年 1 月 9 日)。なお、この提言に先行して、同研究会は、公益財団法人笹川平和財団 安全保障研究グループ 核不拡散・核セキュリティ研究会「緊急提言 ロシアによるウクライナ侵攻：原子力民生利用の諸課題と日本の役割」(2022 年 7 月 1 日)、<https://www.spf.org/global-data/user26/Proposals.pdf> (最終閲覧日：2024 年 1 月 9 日) を公表している。

いを進める必要がある。日本は国際条約の改正作業や国際原則の確立に向けて、原子力民生利用の先進国として具体策を示しながら、各国間の議論を先導するべきである」

この提言が述べるような、国際的な協議・協力とそれに基づく「仕組みづくり」と関連条約の改正、そして「原子力施設への軍事行動全面禁止」にかかる「国際原則の確立」は、ロングスパンでみれば実効的であり、実現に向けての取り組みが希求される。それと並行して、国内的にはどのような対応策が考えられ、その課題は何か。

本稿では、そのような視点で、これまでの経緯を振り返るとともに、ドイツにおけるハイジャック航空機への対応にかかる判例を比較の素材として考証を加える。国際的な対応策や、国内における今後の具体的な制度設計に論が及ばないという意味で、後衛の位置からの検討にとどまることを予めおことわりしておきたい。

II 原子力発電所の防護－これまでの経緯から

筆者は、2005年に「核物質防護条約」(Convention on the Physical Protection of Nuclear Material)改正案の採択がなされ、なおかつ日本がまだ批准していなかった段階で、原子力発電所の防護の問題を採り上げたことがある。グローバル化と地方自治の関係に関する考察の一環であるが、往時の課題とその後の変化を確認するために、再掲する³。

「＜改正「核物質防護条約」(Convention on the Physical Protection of Nuclear Material)と地方公共団体＞

核物質の盗取や犯罪利用を防止する目的を持つ「核物質防護条約」(1987年発効。以下「PP条約」という)も、旧ソ連・東欧諸国における核物質の不適切な管理への懸念や9.11テロを契機に、条約の強化が図られ、2005年7月に改正案が採択された⁴(日本はまだ批准していない)。

改正PP条約の主たる改正点は、従来、締約国が条約によって、犯罪化措置を取らなければならなかった保護の対象が、国際輸送中の核物質だけであったのに対して、国内で使用、貯蔵、輸送中の核物質、及び原子力施設に対象を拡大したことである。従来は、このような域内における規制は、原子力の平和利用にかかわる国家主権事項として捉えられてきた⁵。そ

³ 斎藤誠「グローバル化と地方自治」自治研究 87 巻 12 号 (2011 年) 24 頁以下。二重下線は今回付した。以下 4～9 の注も原論考に記載のものであるが、原注と番号は異なる。

⁴ 改正にいたる経緯につき、兼原敦子「核物質防護条約の改正を巡る議論の意義」日本エネルギー法研究所編『核物質の国際移転に関する国際法と国内法(JELI R-No.93)』(日本エネルギー法研究所、2002 年) 93 頁以下を参照。

⁵ 現行 PP 条約の前文は、「条約の締約国は、平和的目的のために原子力を開発し、及び応用する全ての国の権利並びに原子力の平和的応用から得られる潜在的な利益に対する全ての国の正当な権利を認め…」という。また、原子力の安全に関する条約(Convention on Nuclear Safety)の前文(iii)は、Safety

うした理解自体が、テロ対策についての国際的な環境変化によって、揺らぎつつある。

締約国は、新たに原子力施設に対する各種の攻撃行為を犯罪と位置付けなければならない。改正条約においてそれは明確な義務である（7条2項。Article 7.2. Each State Party shall make the offences described in this article punishable ...）。

それに加えて、改正PP条約は、核物質防護に関する多くの基本原則（fundamental principles）を明文化した（2A条3項の基本原則A～L、国際輸送時の引継ぎの責任、許可・検査などの法令上の枠組みの整備と維持、所管官庁の指定など）。これらの基本原則は、従来は国際原子力機関（IAEA）の勧告（ガイドライン，guideline）において記述されてきたものである⁶。

核物質の防護制度の確立と実施及び維持とそのための組織整備等は、改正PP条約において一般的な形式で義務化されているが（2A条1～2項）、それをより具体化した位置付けの基本原則については、犯罪化措置の場合とは異なり、締約国は合理的かつ実行可能な範囲でそれを適用すれば良い（Each State Party shall ... apply insofar as is reasonable and practicable the Following Fundamental Principles ...）。締約国が国内化措置を行うか否かは、その立法裁量に大幅に委ねられている（各基本原則においては、The State should ... という表現が採用されている）。しかし他方で、基本原則が条約のなかに位置付けられたことで、法的拘束力が無いことが明らかなガイドライン・勧告との差異が生じたことは否定できない⁷。締約国間の国際協力の場合などで、基本原則の遵守を求める要請は強まるのであろう。日本の場合には、改正条約に先行し、なおかつ詳細な内容を定めるガイドラインに「自発的に」対応して、原子炉等規制法の改正を行っているが⁸、それでもなお、同条約を批准する場合には、原子力施設への攻撃を防止することの実効性という観点から、基本原則の遵守⁹のために、地方公共団体に対する新たな義務付けの議論がなされることも想定される。

例えば、現在のところ、原子力発電所の防護については、原子炉等規制法の規制によって

（事故等からの安全）に関してではあるが、「原子力の安全に関する責任は原子力施設について管轄権を有する国が負うことを再確認し...」とする。

⁶ 核物質防護措置に関する現行ガイドラインは、1999年改定の INFCIRC/225/Rev. 4 である。また、法令上の枠組みを定める責任が国にあること（基本原則 C）や、原子力の規制機関・任務と利用・促進機関・任務の独立性確保措置の要請（基本原則 D）のように、類似の規定が、原子力安全（safety）の基本原則を定めたインセンティブ条約である、原子力の安全に関する条約に置かれているものもある（同条約 7、8 条を参照。使用済み燃料管理及び放射性廃棄物管理の安全に関する条約にも同趣旨の規定がある、同条約 19 条、20 条）。

⁷ ただし、核物質防護に関するガイドラインが、協定や条約で援用される場合には、スタンドアローンのガイドラインとは異なる法効果を持ち得る（核テロ防止条約 8 条や日米原子力協定実施取極 6 条におけるガイドラインへの言及を参照）。

⁸ INFCIRC/225/Rev. 4 が、防護システムを設計する場合に基礎とすべき脅威（設計基礎脅威，DBT）を国が設定するという考え方を示し、併せて、DBT も含め機密情報保護制度の必要性を勧告したことを受けて、2005 年原子炉等規制法改正で、「核物質防護検査制度」（12 条の 2、43 条の 2 等で準用、核物質防護検査官につき 67 条の 2）、事業者等の機密保持義務と罰則による担保規定（68 条の 2、78 条 31 号）が新たに設けられた。

⁹ 例えば、基本原則 F「セキュリティ文化（の醸成と維持）」、基本原則 I「多重防護」。

民間事業者に「核物質防護規定」の制定をはじめとする防護措置を義務付けているが（12条の2、43条の2等）、行政の側では、国内法上は一般的な警察権限により、都道府県警察及び海上保安庁が警備にあたっている。原子力発電所のある海岸について、海岸管理者としての地方公共団体は特別の規制を行ってはいない。

条約上の基本原則は特定の措置を締約国に義務付けるものではないが、現在の防護の仕組みが安全確保の上で十分かどうかについての国内での法政策上の議論において、改正PP条約が「援用」されることは十分あり得よう。」

その後の経緯について、以下略記しておく¹⁰。日本は、2014年（平成26年）6月4日、改正PP条約が国会承認され、同月27日にIAEA事務局に受諾書が寄託された。日本も含め締約国の批准が進んで、締約国の3分の2の批准という発効条件を満たして、2016年5月8日に、改正PP条約は発効した。

日本における国内（化）措置としては、先に述べた改正PP条約7条2項、すなわち、新たに締約国に原子力施設に対する各種の攻撃行為を犯罪化することを義務付けた規定を受けて、「放射線を発散させて人の生命等に危険を生じさせる行為等の処罰に関する法律」（放射線発散処罰法）が制定された。しかし、その余の新規定、すなわち、施設の防護措置にかかる規定についての新規立法は、政省令レベルのものも含め、なされなかった。

それは、既に、改正PP条約の基本原則の内容を、より具体的に記述したIAEAの勧告文書INFCIRC/225/Rev. 5（2011年3月公表）に対応した措置を省令改正によって実施しているという理由による。具体的には、「実用発電用原子炉の設置、運転等に関する規則」の改正による、①立入制限区域の設定（同年12月）、②監視機能と連絡機能の二重化などその他の勧告内容への対応（2012年3月、実用炉以外の原子力施設についての省令改正による勧告内容への対応等）である。これらの対応は、2011年3月11日の東日本大震災による福島原発事故を受けての、セーフティ面での規制強化と並行してなされたものである。

そして、外国の軍隊によるミサイル攻撃など、「武力紛争における軍隊の活動」であって「国際人道法によって規律されるもの」は、改正PP条約の対象とならないところ（改正PP条約2条4項(b)）¹¹、ロシア軍によるウクライナ原発の攻撃という、かつてない事態の発生によって、日本においても、有事における原発防護のあり方が、冒頭に掲げた研究グループによる提言に見られるように、様々に議論されている。

¹⁰ 条約改正及び日本の対応については、森川主査による詳細な論究がある。森川幸一「改正核物質防護条約の国内実施と実効性強化に向けた国際的試み」『エネルギーに関する国際取決めの法的問題の諸相—2017～2018年度エネルギーに関する国際取決めの法的問題検討班報告書—(JELI R-No.154)』（日本エネルギー法研究所、2023年）1-22頁。以下の概観に当たっても参照した。

¹¹ また、同条項により、国の軍隊が公務の遂行に当たって行う活動で、他の国際法の規則によって規律されるものには、改正PP条約の規律が及ばない。

本章においては、このような状況だからこそ、基本的な事項に立ち戻っての考察も重要であると考え、ハイジャック航空機による原子力発電所など国内インフラへの攻撃への国内的な対応について、ドイツの法制・判例を参考に、若干の検討を試みる¹²。

Ⅲ ドイツにおける軍・警察の分離原則とその変容

1. 分離原則とその淵源

合衆国における2001年の9.11テロのような、平時であり、なおかつ外国軍隊によるものではない、ハイジャック機による攻撃についても、一般に、事態の性質上、自国軍の出動が必要となることが想定される。そして、そのような事態において、軍と警察の連携・共同行動が必要となる場合もあろう。

かかる状況に関する法的論点として、ドイツにおいては、軍と警察の組織及び任務の分離と連携について、「分離原則(Trennungsprinzip)」ないし「分離命令(Trennungsgebot)」という法的要請が、学説のみならず立法実務上も通用してきた¹³。分離原則は「安全の担い手の分離(Trennung der Sicherheitsgewährleister)」とも言われるように、具体的には、軍(Streitkräfte)、警察(Polizei)、秘密情報機関(Nachrichtendienste)¹⁴、3者間の組織と任務に関する分離をその中心とする¹⁵。

そして、分離原則の歴史的な淵源としては、第二次大戦後の占領法規¹⁶の一種である軍の指令、具体的には、1949年4月14日に連合軍軍政官から（憲法制定の審議機関である）議会評議会議長宛で出された、いわゆる「警察書簡(Polizei Brief)」に集約される一連の指令が第一に挙げられる。そこでは、一方で、連邦政府に対する破壊活動に関する情報機関の設置が、当該機関は警察権限を保持しないという制限の下で認められた。他方で、警察については、軍事的、ないし軍事に類した性格を持つこと、或いは警察任務とは異なる軍事任務を遂行す

¹² 以下、ⅢからⅤの行論の一部は、斎藤誠「海上保安庁と自衛隊の海上警備行動における連携——国内法的側面」奥脇直也・坂元茂樹編『海上保安法制の現状と展開 多様化する海上保安任務』（有斐閣、2023年）244～268頁をベースに、この問題設定の下で、改稿を加えたものである。

¹³ Dorn, A., Das Trennungsgebot in verfassungshistorischer Perspektive, 2004, Thiel, M., Zur Theorie der neuen Sicherheitsarchitektur und Sicherheitsinfrastruktur, in: Stober, R., (hrsg.), Stand und Perspektiven des Sicherheitswirtschaftsrechts, 2013, S.21.

¹⁴ 現在は、具体的には、ボン基本法 87 条 1 項所定の情報中央官庁を指す。

¹⁵ その他にも、連邦と州、それぞれの安全所管官庁の間（垂直的な分離原則）、警察（官庁）と他の秩序行政（官庁）の間など、様々な場面で、分離原則が語られ、多義性を免れない。なお、警察行政と他の秩序行政の分離（いわゆる脱警察化）の歴史と理論については、米田雅宏『「警察権の限界」論の再定位』（有斐閣、2019年）45頁以下が詳細である。

¹⁶ 筆者は、相異なる層に属する法相互間の関係、特に法の「転換」という観点について、連合国のドイツ占領法に若干の検討を加えたことがある。斎藤誠「条約の国内『実施』と『転換』——若干の考察」『エネルギーをめぐる国内外の法的問題の諸相——2013～2015年度エネルギーに関する国際問題検討班報告書一(JELI R-No.138)』（日本エネルギー法研究所、2018年）25-36頁。

るように、組織、武装し、また育成されることが禁止された¹⁷。

この淵源からも容易に推測できるように、各組織とその作用双方の分離を求める分離原則は、一方では、戦前期と戦時下におけるナチスによる警察権限の肥大化と濫用—「警察の軍事化」という言葉に象徴される—、他方では、ナチス以前、第二帝政期に遡る、国内治安維持を目的とした軍の過大な投入の歴史、それぞれに対するアンチテーゼという面が大きい¹⁸。警察書簡は占領解除後には効力を失ったが、法治主義及び権力分立という憲法原則や、各機関の権限に関する連邦憲法条項（ボン基本法73条1項10号、87条1項2文）から、法的要請として分離原則が存在することは、（原則の位置付けや強度には議論もあるものの）広く認められてきた。特に、軍の防衛出動以外の任務での出動を、ボン基本法が明文で認めているものに限定する同法87a条2項は、分離原則の主要な内容を直接に表現したものとされる。

しかし、今世紀に入って、ドイツもまた、「国際テロリズム」によって市民生活が実際に脅かされ、安息の時代は過去のものとなってしまった。分離原則についても、連邦・州の警察権限の垂直的な分離について、州警察で対応が困難な場合等を対象に、国際テロリズムへの対処について連邦刑事庁の権限を認める憲法改正がなされた¹⁹。軍・警察・情報機関の間においても、種々の連携や任務の新設が図られている。例えば、この憲法改正を受けて、連邦刑事庁法が改正され、同庁における秘密情報の収集や他官庁及び外国機関への情報提供等の新規権限が認められた。

2. ハイジャック機への武器使用と分離原則—連邦憲法裁判所判決を巡って

立法及び行政実務との関係で、現在判例・学説上最も議論があるのは、警察・情報機関間の関係、特にその情報の共有の問題である²⁰。しかし、軍と警察の関係についても、合衆国における9.11テロを受けて、ハイジャックされた航空機によるテロを防止するため、ドイツ国内において空軍による当該航空機撃墜を認めた改正航空安全法（2005年）に対して大きな

¹⁷ Dorn, a. a. O. (Anm.13).同著には「警察書簡」（ドイツ語版）も所収（Dorn, a. a. O. (Anm.13), S. 195f.）。Thiel, a. a. O. (Anm.13), S. 31.軍の国内出動にかかる規定の変遷については、松浦一夫『立憲主義と安全保障法制 同盟戦略に対応するドイツ連邦憲法裁判所の判例法形成』（三和書籍、2016年）343頁以下も参照。

¹⁸ 軍と警察の関係一般に立ち入る紙幅はないが、ドイツでの脱警察化の占領期以前の文脈については、米田・前掲注(15)、日本については、仲野武志『法治国原理と公法学の課題』（弘文堂、2018年）176頁以下を参照。

¹⁹ この憲法改正については、上代庸平「テロ対策権限の垂直的配分——ドイツ基本法73条1項9a号と連邦国家制の変容」大沢秀介・小山剛編『自由と安全—各国の理論と実務』（尚学社、2009年）238頁を参照。

²⁰ 例えば、対テロデータファイル法における警察・情報機関間の情報共有についてのBVerfGE, 133, 277, Urteil vom 24. 4. 2013, 入井凡乃「情報機関・警察の情報共有と情報自己決定権—テロ対策データファイル法判決—」ドイツ憲法判例研究会編『ドイツの憲法判例IV』（信山社、2018年）46頁、連邦刑事庁が収集した情報の他官庁、外国機関への提供等につき、BVerfGE 141, 220, Urteil vom 20. 4. 2016, ドイツ憲法判例研究会「ドイツ憲法判例研究(206)」自治研究94巻7号（2018年）145頁。

議論が巻き起こった。国内における軍の出動に対して、従来の立法実務が、前記の歴史を踏まえ、また憲法上の限定もあって、謙抑的な立場をとってきたこともその背景にある。

当該法改正に対して提起された訴訟（憲法異議）²¹につき、2006年2月15日連邦憲法裁判所第一法廷は、撃墜を認める航空安全法14条3項を、無辜の乗客・乗員を犠牲にするものであり、人間の尊厳条項（ボン基本法1条1項）及び生命権条項（同2条）に違反するとして違憲であると判断した。他方で、ハイジャック犯のみが乗っている旅客機の撃墜は同条項違反ではないとしたが、この場合も、軍固有の武器の使用はできないとした²²。この判決によれば、空軍機によるハイジャック機への対応は極めて限定的・抑制的なもののみが可能ということになる。

しかし、同法改正の違憲を争う抽象的規範統制訴訟が別途に提起された同裁判所第二法廷において、同法廷が、連邦の立法権限と武器使用等の争点につき、第一法廷の判断と異なる解釈を採る必要があると判断したので、当該争点につき両法廷の合同法廷(Plenum)による審理が求められた。そして、2012年7月3日合同法廷決定は、第一法廷とは異なる解釈を示し、連邦憲法裁判所としての統一的判断を下した。以下、本章の問題設定に関わる部分を中心に、同決定につき略説する²³。

(1) 連邦の立法権限

第一法廷は、ハイジャック航空機撃墜にかかる連邦の立法権限は、ボン基本法35条2項2文及び同条3項であるとした。当該規定は、自然災害及び重大な災難事故の場合の、他州の警察、国境警備隊及び軍の出動についての実体規定である。しかし、合同法廷は、この規定はハイジャック航空機撃墜に軍を出動させる連邦権限の根拠にはならないとした。ボン基本法7章（70条以下）の連邦立法権限規定の外にある実体規定に、「書かれざる権限規定」を求めることは「連邦制の権限秩序」と相容れない(Rn.16)。

それに代えて、合同法廷は、「航空交通」を連邦の専属立法管轄として規定する同70条6号の「付随的権限」(Annexkompetenz)として、航空交通から生ずる危険防御のための規制権限が連邦に帰属するとした(Rn.18)。

²¹ 憲法異議は、原告の権利の侵害ないしそのおそれを理由とする主観訴訟であり、実際に航空機を利用している国会議員が原告となった。

²² BVerfGE 115, 118.同判決は、旅客機乗客とテロで想定される被害者、それぞれの権利保護につき、撃墜を認めると前者を後者救済の為の手段に使うことになり、人間の尊厳条項に違背するとした。同判決は、この判断部分を中心に、日本においても広く紹介されている。嶋崎健太郎「航空安全法判決」ドイツ憲法判例研究会・前掲注(20)81頁、小野寺邦広「テロ攻撃撃退のための軍隊出動についての合同部決定—『航空安全法』合同部決定—」ドイツ憲法判例研究会・前掲注(20)366頁及びそれぞれに掲記の文献を参照。特に、松浦・前掲注(17)331頁以下が、航空安全法の立法経緯、同判決、合同法廷判決、それを受けた第二法廷判決について詳細に詳細・分析している。ここでは本文に記したように、主として軍と警察の権限と連携手続の関係から検討する。

²³ BVerfGE 132, 1.文末番号は判例集記載の段落番号であるが、項目の番号とタイトルは筆者が便宜上付したものである。下線も筆者による。

(2) 出動要件と軍固有の武器の使用

a. 出動要件論一般

ハイジャックされた航空機を撃墜するには、一般には警察機関が保持していない武器によらねばならないところ、第一法廷は、前記35条は、特別に重大な災難事故 (*besonderes schweren Unglücksfalls*) の場合も含め、軍固有の武器の使用を認めていないとした。それに対して、合同法廷は、同条は軍固有の武器の使用を原則として排除していないが、そのような軍の出動は、87a条4項が定める国内緊急事態での軍出動についての厳格な要件が迂回されないように、狭い前提条件が満たされる場合にのみ許容されるとした (Rn.24)。当該条件は、91条が規定する、他州警察及び国境警備隊の出動が許容される国内緊急事態²⁴の状態ですぐに充足されるものではなく、また「警察が、公共の安全と秩序の維持と回復という一般的目的について過大な負担の下にある、ということで常に充足されるものではない」 (Rn.25)。

b. 軍固有の武器の使用

他方で、35条各条項を適用する場合に、軍が使用できる手段は、軍が出動する州の危険防除に関する法令によって警察が使用できる手段には限定されない。35条の当該条項の文言、立法経緯 (Rn.32.33) に加えて、法体系上も、87a条4項1文は、組織され軍事的に武装した暴動の鎮圧につき、州及び連邦の警察を「支援するため」の軍出動と固有の武器使用を認めているのだから、35条2項及び同条3項においても、軍の使用手段は、支援される警察が使用できる手段には限定されない。実効的な危険除去に向けられた規律の目的と、「効果的な対処の必要性」をいう91条からもこの解釈が支持される (Rn.29)。

c. 「特別に重大な災難事故」の解釈

合同法廷は、このように武器の使用については、軍固有のものを認める立場に立ったが、他方で35条2項2文の「特別に重大な災難事故」については、上記87a条における制限の迂回にならないよう限定的な解釈を示した (87a条の「遮断効果」)。「破局的な次元の事件」 (*Ereignisse von katastrophischer Dimension*) だけがそれに該当し、州警察によって統制不能な危険状況というだけでは不十分である。災難事故は既に存在しなければならず、国家によらない攻撃から来る国内的不安の除去といった状況も対象外であり、デモによる生命・身体の危険も含まれない。既に損害が発生していることは要求されないが、破局的損害発生が切迫し、直接見込まれる場合に限られる。軍固有の武器の使用は、そのような危険に対する最終手段であり、軍による、航空安全に対する包括的な危険防除を同条項は認めていない (Rn.43～49)。

²⁴ 同条は、連邦ないし州に、その存立または自由で民主的な基本秩序に対する差し迫った危険を防止するための、連邦政府の各州警察に対する指揮権及び連邦国境警備隊の出動を定めている。同条の改正 (1968 年) も含め、国内緊急事態への軍出動にかかる憲法改正については、松浦・前掲注(17)3 頁以下が詳細である。

この説示からすると、航空機がハイジャックされたというだけでは、「破局的な次元の事件」には該当せず、既に（ハイジャック犯だけが乗った）同機が目標に向かって接近しつつあるなど、極めて限定的な場合にのみ軍固有の武器使用が認められることになる。

（3）国防大臣の緊急権限

改正航空安全法は、ハイジャック機によるテロの危険も含め、州を超えた重大な災難事故の緊急事態において、（内務大臣と協議の上での）国防大臣単独での命令権限を認めたが、第一法廷はこれを違憲とし、合同法廷も以下のように合議体としての連邦政府（Bundesregierung）の決定（日本でいうところの閣議決定）が必要であるとして、この判断を維持した。

ボン基本法は、体系的に大臣権限と連邦政府の権限を区別しており、連邦政府の権限を個々の大臣に委任する権限は政府には無い。国防大臣の軍指揮権、国家の保護義務による実効的危険防止といった論拠で他の解釈を採ることもできない上に、原則として議会に属する権限について、連邦政府への例外的な帰属を認めた連邦憲法裁判所の諸判例も、ここでは論拠にならない。それらは、いずれもボン基本法が明示的に規律していない決定権限に関するものだからである（Rn.55～58）²⁵。判決は、憲法上の連邦における権限配分規定の解釈によって、本事案で想定される緊急の状況においても、合議体による決定という慎重な手続を経ることを求めたことになる。

＜Gaier裁判官の反対意見＞

合同法廷判決には、(2)の説示に対して、「軍固有の武器を使用する軍の出動」を認めないとするGaier裁判官の反対意見が付されている。同意見は、歴史的解釈として、憲法制定権者は、1956年の再軍備に関する改正、1968年の緊急事態条項に関する改正のいずれにおいても、軍の国内出動は、民主制と自治に対する特別な危険と結びついており、厳格かつ明確な限界を必要とすると認識していたとし、また明文化された「国内緊急事態」とそうでない「破局的緊急事態」を明確に区別していたとする。このように、軍と警察の分離、そして前者を警察任務に出動させることの抑制についての歴史的意義を同意見は強調する。

また、体系的解釈としても、連邦政府の合議権限を前提にして、「破局的緊急事態」においては、災害事故ないし自然災害の結果除去だけが可能であり、それは時間を要するものであることからすると、その任務は軍の出動とは相容れない。「破局的かつ直接的な被害が目前にある」場合という、合同法廷多数意見の基準は不明確であり、実務による主観的判断を免れず、国内政策的な目的での出動への拡張が排除できない、とGaierは批判する。

²⁵ 本決定を受けた第2法廷の決定（2013年3月20日，BVerGE,133,241）は、(1)～(3)の判断を維持し、(3)によって、航空安全法13条3項2、3文を違憲無効とした。

IV 比較の視座からの若干の考察

1. 比較の前提

本件は、ドイツ国内における軍の出動に関する事案であり、そこには当然ながら固有の法体系と史的前提がある。その差を踏まえた上で、比較検討の対象となるのは、日本においては、対処すべき事態の近接性からいえば、1)領空侵犯に対する措置（自衛隊法84条）であるが²⁶、2)治安出動（同法78条）、3)海上警備行動（同法82条）も対象となろう。治安出動については、海上警備行動にはない国会承認手続が課されるなど、自衛隊の出動と武器使用について、彼の地と同様に、やはり国民の自由と民主制の観点からの配慮が規定に看取される。

それに対して、海上警備行動の場合、海という場の特性に加え、なおかつ、現在日本で主に想定されるケースは、外国の船舶が対象であることも考慮する必要がある²⁷。もっとも、海上上空からのハイジャック機の接近に対して、海上における人命・財産の保護のため、警備行動で対応することもあり得よう²⁸。

以下、1)～3)に通底する、通常の警察組織・権限では対応できない事案への対応という、より一般的な次元で、参考になる点を掲げる。

2. 根拠法の明確性、法令の整合性及び体系的解釈を求める姿勢

軍固有の武器使用を認めるか（合同法廷意見、第二法廷判決）否か（第一法廷意見、Gaier反対意見）に関わりなく、根拠法の明確性、法令間の整合性、そして体系的解釈を求める姿勢がまず挙げられる。合同法廷意見が、連邦権限規定上の根拠を必要とした、(1)の争点に対する判断が典型であるが、軍固有武器の使用についても、軍出動を許容する他の憲法条項との整合性を含め、法令の体系的解釈が強調されている。

3. 固有武器使用の可否

それでもなお、固有武器使用の可否について、第一法廷意見、合同法廷の法廷意見、反対意見の分岐が示すように、解釈に幅がある。このことは、軍の出動について、一義的にその要件を法令で事前設定できるのか、そして設定すべきなのか、という問題の存在にも注意を

²⁶ 領空侵犯に対する措置においては、2)、3)とは異なり警察官職務執行法7条が明文で準用されていないが、行政実務においては、退去ないし着陸させるための武器の使用は排除されていないとの解釈が採られている。黒崎ほか『防衛実務国際法』（弘文堂、2021年）194頁、仲野武志『防衛法』（有斐閣、2023年）415頁以下を参照。民間航空機に対しては、国際民間航空条約3条の2により、武器使用は原則として禁止される。

²⁷ もちろん、海上警備行動も、漁業への影響など国民生活と直結する場面もあるし、陸域・空域で別途とられる措置とあいまって、ケースによっては、自由と民主制への懸念も想定されるが、概括的にいえば、本文のような対比もできよう。

²⁸ ただし、原発は海岸近くに設置されている場合も含め、陸域に存在するので、原発のセキュリティ確保を目的に、ハイジャック機に対して海上警備行動を実施することは、82条及び84条の解釈上難しいといえよう。

促す。

第一法廷判決の後、連邦議会の与野党及び学界では、ハイジャック旅客機の撃墜権限につき、ボン基本法（連邦憲法）に規定するという改正案が複数提示されたが、実現には至らなかった²⁹。現行ボン基本法を前提に事案の解決を求められる裁判所の解釈として、どの意見が妥当なのか。

この点、「軍・警察分離原則」との関係で、合同法廷判決を論じたThielは、以下のよういう³⁰。テロへの対応など、軍の国内での防衛以外の任務への投入に積極的な諸議論や端緒一軍の騎兵隊化(Konstabilisierung)という評語がある一の文脈に本判決を位置付けることができる。軍固有の武器使用を（限定された条件の下ではあれ）認める合同法廷多数意見は、防衛以外の国内出動では、軍は警察と同様の手段しか認められないという従来の考え方ー「予備的な警察部隊」(Polizeitruppen auf Vorrat)という評語がある一からすると、「分離原則」の壁を破っているようにも見える。

Gaier反対意見は、そのような認識を基礎に、1968年憲法改正による国内緊急事態条項の導入においては、一定の軍出動を認めたにせよ、その例外的性格によって、同様の出動にかかる法解釈には抑制が求められるとした。しかし、Thiel自身は、現実的に考えるのであれば、「特別に重大な災難事故」において軍の出動を認めるのであれば、軍は実効的武器を手にする方が望ましいとして、Gaierの結論には賛同できないとする。

むしろ、多数意見の問題は、「特別に重大な災難事故」とはどのようなものを曖昧なままにしたことである。同意見は、デモや、武装反乱による不安がこれに該当せず、事故は既に存在しなければならないことなどをいうが（上記(2) c）、「特別に重大な災難事故」の積極的な法律構成を示していない。ゆえに、Thielは同判決における「分離原則」の「破棄」は、それが緊急事態においては、例外的状況ゆえに破棄できる場合がある、という仮定的なものにとどまるとする³¹。

もともと、仮定的かつ厳格な要件の下ではあっても、明文の憲法改正がなされなかった状況下で、武器使用について6年前の判例の解釈変更を行ったこと³²は、時代状況及び歴史との関係での分離原則の位置付けにも再度の考慮を促すものではある。

4. 緊急時の決定権限ー大臣権限と合議体としての政府の権限

この争点については、第一法廷判決の意見を是認した合同法廷判決によって、ドイツにおいては、連邦憲法規定との関係で、法律による国防大臣への緊急時の単独権限付与に限界が

²⁹ 松浦・前掲注(17)391頁以下が詳細である。

³⁰ 以下の3段落は、Thiel, a. a. O. (Anm.13), S. 25ff.からの要約である。

³¹ Thiel, a. a. O. (Anm.13), S. 26.

³² 裁判所の「解釈改憲」であるとの議論につき、松浦・前掲注(17)438頁以下、小野寺・前掲注(22)368頁以下を参照。

あることが確認された。例えば、日本における海上警備行動の場合、自衛隊法82条は、内閣総理大臣の承認を得て、防衛大臣がこれを発動する手続になっている。そして、この承認権限は、合議体としての内閣に行政権が属する日本国憲法のシステムにおいては（同65条、66条3項）、内閣の首長（内閣法2条）としての内閣総理大臣の権限であり、権限行使には閣議決定が必要である（同法4条）。閣議にかけて決定した方針に基づいて、内閣総理大臣は行政各部を指揮監督する（同法6条）。

実際に、海上警備行動の発動初例（能登沖不審船事件）においては、それぞれ持ち回りの安全保障会議と閣議を経て承認がなされている。緊急時の単独権限行使に憲法上の制約がかかるという面でドイツの法状況と類縁性がある。そして、この制約のなかで、内閣による判断の迅速性と的確性を確保するための実務的慣行も蓄積されている。その一つは、「閣議にかけた方針」については、予め一般的な方針を定めておけば、個別の案件ごとに閣議は必要としないという解釈である³³。そして、「我が国の領海及び内水で潜没航行する外国潜水艦への対処について」（平成8年（1996年）12月24日閣議決定）は、当該艦船を対象に海上警備行動を発令する場合について、この一般的方針を定めたものである。

実際に、2004年11月10日の、中国潜水艦による領海内潜航航行事件においては、この閣議決定を基に、小泉内閣総理大臣の承認を得て、大野防衛庁長官が、本邦2例目となる海上警備行動を発令した。しかし、この事件においても、潜水艦の侵入状況の確認から発令まで相当の時間がかかった（哨戒機による確認は同日早朝、発令は午前8時45分）ことから、事件後、潜航潜水艦が領海内に侵入した場合には、上記閣議決定を基に、特段の事情がない限り直ちに海上警備行動を発令する旨を含む、対処方針が策定されている。

また、潜航潜水艦以外の外国軍艦については、平成27年に対処についての閣議決定がなされたが、そこでは、基本的に、事態発生毎に、緊急の場合で全員が参集しての閣議が困難なときは首相が主宰して電話等により各大臣の了解を得て閣議決定を行い、それを経て承認するという手続が予定されている³⁴。基本的には、（オンライン環境の進捗はあるにせよ）能登沖事件の際の手続と同様であり、潜航潜水艦の場合に対比すると、慎重性の確保に重きが置かれている。

そして、弾道ミサイル等に対する破壊措置（82条の3）においても、内閣総理大臣の承認が必要とされるのに対して、領空侵犯に対する措置（84条）には、承認手続は規定されておらず、防衛大臣が単独で措置を講じさせることができる。

³³ 阪田雅裕編著『政府の憲法解釈』（有斐閣、2013年）187頁。

³⁴ 「我が国の領海及び内水で国際法上の無害通航に該当しない航行を行う外国軍艦への対処について」（平成27年5月14日閣議決定）の3.（1）。併せて、発令に際して、安全保障会議の審議等を行う場合も、電話等により行うことができる旨をいう（同（2））。

V 自衛隊と法執行組織（広義の警察。海保も含む）の分離原則

次に、ドイツの法制・議論としての「分離原則」を参考に、対比・類比を試みると、日本の場合にも、防衛・警察の「分離原則」は、実定法の法体系において、組織と権限の構成原理として語り得ると考えられる。日本国憲法においては、ドイツ・ボン基本法とは異なり、自衛隊と警察（広義）の組織・権限、そして、その調整に関する明文の規定は存在しない。しかし、憲法9条の下で一定の限界をもって認められている対外的な防衛の組織・作用と、国内における公共の福祉（憲法12条、13条）の一環としての「公共の安全と秩序」の確保³⁵のための警察の組織・作用は、憲法上区別されていると解される。そして、法律レベルにおいてこれを受けとめて、自衛隊、都道府県等警察、そして海上保安庁麾下の組織と作用は、それぞれ独立したものとして規定されている。なおかつ、海上保安庁法25条「この法律のいかなる規定も海上保安庁又はその職員が軍隊として組織され、訓練され、又は軍隊の機能を営むことを認めるものとこれを解釈してはならない。」は、分離原則の包含する内容の一つを法律レベルで確認したものとして特筆されよう。

その上で、日本の法体系上、分離原則は、例外を許容しない固いルールではない。自衛隊と都道府県等警察、海上保安庁、各組織の連携、そして、防衛権限と警察権限の組織上の交差も認められている。海上警備行動は、両組織が連携し、かつ権限の交差が認められている具体例である。

VI むすび

以上、不十分ながらドイツのハイジャック航空機対応立法にかかる判例及び分離原則についての議論を比較の素材として、防衛・警察両組織の緊急事態対処のあり方を検討してきた。

ハイジャック機も含め、航空機等による意図的攻撃に対する原発防護という具体論へと議論を展開するには、更に様々な要素を考慮しなければならない。要素の一端を示すことでむすびとしたい。

<国際民間航空条約（シカゴ条約）との関係>

同条約3条の2(a)は以下のように規定する。

「締約国は、各国が飛行中の民間航空機に対して武器の使用に訴えることを差し控えなければならない及び、要撃の場合には、航空機内における人命を脅かし又は航空機の安全を損なつてはならないことを承認する。この規定は、国際連合憲章に定める国の権利及び義務を修正するものと解してはならない」

(b) 以下略

³⁵ これに対応した、法律レベルでの表現として、例えば「公共の安全と秩序」の維持（警察法1条、2条）、「海上の安全及び治安の確保」（海上保安庁法2条）が挙げられる。

本条は、「国際民間航空条約の改正に関する千九百八十四年五月十日にモントリオールで署名された議定書」により条約に追加されたものである。

この議定書は、「昭和59年（1983年）に大韓航空機が撃墜された事件を踏まえ、同様の事件の再発を防止するため、国際法の原則である民間航空機に対する武器の不使用をシカゴ条約上の義務として明文化すること等を内容とするものである」³⁶。日本では、平成10年（1998年）5月22日に国会承認、6月23日に批准の閣議決定、26日に批准書寄託、という過程を経て、10月1日に日本も含め効力が発生、同15日に条約第14号として公布された。

なお、日本において、批准までに長い時間を要しているが（事件発生及び議定書採択から15年）、政府の説明は、同条c項が規定した、自国の民間航空機が、外国領空において、無許可飛行など法令違反をしている場合に、「重い制裁を課す」ことについての慎重な検討が必要であったとする。

また、この間議定書に未加入であったことについては、議定書前文が「民間航空機に対して武器を使用しないとの原則を再確認する」とあるように、民間航空機に対する武器不使用は、一般国際法上の原則であり、日本はこれを遵守しており、他国もこれを遵守する義務があるという説明がなされている³⁷。

日本の場合、そもそも国内的な法政策として、セキュリティ面での原発防御は、本章Ⅱで振り返ったように、事業者にも物理的な面も含め防護措置を義務付け、一般的な警察権限の行使の範囲内で、都道府県警察と海上保安庁が警備を行っている。しかし、もし仮に、ハイジャックされた民間航空機に対して、ドイツ航空安全法のような対応を検討するとすれば、この条項との関係が問題になる。そして、シカゴ条約3条の2(a)は、武器不使用の例外として、自衛権による措置としての武器使用を認める趣旨で規定されたものではあるが、本章で想定しているようなケースが自衛権の発動に該当する場合は、極めて限定的であろう。

そして、日本の国内法として、想定ケースに直接に関わる措置を規定するのは、自衛隊法84条の「領空侵犯に対する措置」である。

＜領空侵犯に対する措置と民間航空機への対応及び自衛権との関係＞

自衛隊法84条は、以下のように定める。

「防衛大臣は、外国の航空機が国際法規又は航空法（昭和二十七年法律第二百三十一号）その他の法令の規定に違反してわが国の領域の上空に侵入したときは、自衛隊の部隊に対し、これを着陸させ、又はわが国の領域の上空から退去させるため必要な措置を講じさせることができる」

同条の解釈にかかる議論の整理と分析は他日を期さざるを得ない。ここでは、①同条は、

³⁶ 同議定書の国会審議に当たり、議定書に説明のため付された（参考）の記述。

³⁷ 第142回国会 衆議院 外務委員会「会議録 第11号」（1998年5月13日）を参照。

「外国の航空機」と規定することから、日本の民間航空機は、ハイジャックされたとしても同条の措置の対象にはなり難いこと、②同条の「必要な措置」については、やはり上記シカゴ条約3条の2(a)との関係で、民間航空機に対する武器使用は原則としてできないと解されていること³⁸を指摘するにとどめる。

なお、本章で紹介検討した、ドイツ連邦憲法裁判所合同法廷判決においては、シカゴ条約3条の2(a)と航空安全法との関係は論じられていない。各法廷から回付された憲法上の論点を扱うのが合同法廷の役割であるからでもあるが、航空安全法の立法に当たっては、その作用の位置付けは、自衛権による措置ではなく、危険防除のための警察活動であるとされていた³⁹。そして、各連邦憲法裁判所判決もそれを前提に、連邦憲法上、自然災害及び重大災害事故の場合に「軍隊による警察活動」を一定範囲で認めるボン基本法35条が、航空安全法による武器使用の作用法上の根拠となるか、また、他の既存の「軍隊による警察活動」にかかる連邦憲法関係諸規定と航空安全法の整合性を問題としたことを再度強調しておきたい。

＜戦時、軍隊による攻撃に対する防御＞

戦時、軍隊による攻撃への防御、特にそれを未然に防止するための対応については、ウクライナで起きた事態を受けて、①知事会の政府に対する緊急要請「原子力発電所に対する武力攻撃に関する緊急要請」（令和4年3月30日）⁴⁰、②国際条約の改正等を中心とした前記笹川平和財団の提言がある。

①は、以下に掲げるように、外交等を通じた武力攻撃の抑止(1)と併せ、武力攻撃事態における原子力発電所の停止等(2)、ミサイル攻撃に対する防衛(3)という、直接の防御にかかる内容からなっている。

1 他国の領土や主権の侵害は何の利益も生まず、自らの国益を大きく毀損するとの認識を国際社会において確立することこそが、ミサイル発射などの武力攻撃に対する最大の抑止力であり、国においては、今般のような事案が起きた場合には、国際社会と協調した経済制裁措置の実施など、外交等を通じて毅然として対処すること。

³⁸ 仲野・前掲注(26)418頁。シカゴ条約3条の2の存在から、憲法98条2項により民間航空機に対する武器使用は禁止されるとする。

³⁹ 松浦・前掲注(17)336頁以下が詳細である。また、同法は、9.11テロ後の危険への対応を図った2002年12月16日の欧州航空安全規則(Verordnung (EG) Nr. 2320/02 des Europäischen Parlaments und des Rates vom 16. Dezember 2002)の要請による法改正の一環でもあるが、同規則は軍隊の利用については関説していない。この点についても、松浦・前掲注(17)334頁以下を参照。なお、同規則の要請による空港リスク管理強化に関しては、ドイツにおける関連事業者や旅客の基本権等との関係で訴訟も提起されているが、Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Beschluss vom 14. April 2005, juris Logo.はその一例である。

⁴⁰ 全国知事会 HP に所収、

https://www.nga.gr.jp/item/material/files/group/2/01_2022033001_siryo_nc_ver2.pdf（最終閲覧日：2024年1月9日）。この要請については、②においても紹介がなされている。

（武力攻撃事態における原子力発電所の停止等）

2 原子力発電所への武力攻撃などが懸念されるような事態となった場合には、国は、国民保護法に基づき、原子力事業者に対し運転停止を命ずるなど、迅速に対応すること。

また、突発的な武力攻撃の発生に備え、原子力事業者が、特に緊急を要する場合には国からの命令を待たず直ちに運転を停止できるよう、国は、平時から事業者の体制の確認・徹底を指導すること。

（ミサイル攻撃に対する防衛）

3 万が一、原子力発電所に対するミサイル攻撃等が行われるような事態になった場合に、迅速に対応できるよう、自衛隊による迎撃態勢及び部隊の配備に万全を期すこと。

また、②においては、提言2の解説に、以下の記述がある（下線は本章筆者による）。

「まず、今回のザポリージャ原発への攻撃、占拠の教訓を踏まえ、ジュネーヴ諸条約第一追加議定書が定める原発への攻撃や占拠の原則禁止について、あらためて各国で協議し、条約の改定や解釈の統一に向けた努力を開始するべきである。具体的には、原発を含むすべての原子力施設に対する軍事行動を全面的に防止するための話し合いを進める必要がある。その場合、この合意を隠れ蓑として利用し、軍事施設を原子力施設周辺に設置する国が出てくる可能性がある。そのような行動を防ぐためにも、原子力施設を保有している国は、当該施設を隠れ蓑として軍事拠点としないことを確約する必要がある。また、戦時下においては、当該施設が軍事施設でないことを明示することにより、攻撃のリスクを低減できる。」

そして、下線部に付された注において、以下が指摘されている。

「現在、原子力施設の保護対策として、対空ミサイルの設置などが検討されているが、その措置は、原子力施設が軍事拠点とみなされる恐れがあり、かえって攻撃の正当性を与えてしまうことになりかねない」⁴¹。

「戦時」の攻撃を想定したとしても、その未然防止も含めた方策には種々の課題があることが、現場の声も反映された上記①②の記述からも読み取れる。そして、ウクライナだけでなく、中東においても新たに憂慮すべき事態が生じた今日において、戦時と平時（のテロ）、サイバーとリアル、更に言えばセキュリティとセーフティなど、生起する危険の「区分」は容易ではない。

そうすると、一方で、テロについては、施設のハード・ソフト両面での嚴重化、戦時においては、国民保護も含めた「有事」法制、という二分論での対応を維持できるのかが問われる。他方で、他の場面も含め、シームレスな対応の必要性も強調されているが、そちらはそ

⁴¹ 同提言注(18)。記述の典拠は、笹川平和財団「第13回核不拡散・核セキュリティ研究会」〔真山全・大阪学院大学教授講演〕(2022年11月16日)。

ちらで、シームレス化と「分離原則」及びそれを支える思考の整合性も十分考慮しなければならない。

危険の種類ごとに、長短両面での事前の対応、攻撃が迫った段階、そして攻撃を受けた段階での対応を設計・運用する必要もあるが、長い目でみれば、知事会の緊急要請がまず言及するように、外国との関係での防護の根本は「外交」であることも強調しておきたい。

第 3 章

外国為替及び外国貿易法（外為法）における
「中枢的な基盤(critical infrastructure)」の位置づけ
—地域的な包括的経済連携協定（RCEP協定）の
安全保障例外との関係を手がかりに—

京都大学大学院教授
酒井 啓亘

I はじめに

2022年12月に日本政府は国家安全保障戦略を閣議決定し、その中で経済安全保障の重要性を指摘している¹。ただし、経済安全保障がいかなるものなのかについては確固たる定義があるわけではなく、国家安全保障戦略では「我が国の平和と安全や経済的な繁栄等の国益を経済上の措置を講じ確保すること」が経済安全保障であるとされるだけである。また、2022年8月に施行された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（令和4年法律第43号）（以下「経済安全保障推進法」という）においても経済安全保障についての確たる定義は置かれていない²。このため、経済安全保障とはいかなるもので、それをいかに実現するかということについては、輸出入規制や対内・対外投資規制、技術・情報保護、インフラ・通信・個人情報・先端技術に関する民間取引制限など、広範な経済活動に対する予防的制限措置を個別的に検討し、その法的規律の在り方を模索することが依然として必要となろう³。

本稿では、こうした経済安全保障の実施に位置づけられる措置の中でも、重要インフラや戦略的インフラとも呼ばれる「中枢的な基盤(critical infrastructure)」をめぐる措置に焦点を当て、特に対内直接投資と「中枢的な基盤」との関係に関する国際的・国内的規律について整理することを試みる⁴。この検討においては、「中枢的な基盤」に属する業種を規律する日本の外資規制に関する国内法制が、一方において安全保障例外条項や一般的例外条項を含む経済関係協定との関連でいかなる特徴を有するのか、そして他方において、「安全保障」概念の観点から「中枢的な基盤」を捉える傾向が強い諸外国の国内法制と比較して、改善すべき余地はないのかということに焦点を当てる。具体的には、国際レベルでは、日本が締結した二国間投資協定(BIT)や自由貿易協定(FTA)、経済連携協定(EPA)のうち、「中立的な公共基盤(critical public infrastructure)」概念を導入して、近年、日本についても効力が発生した地域的な包括的経済連携協定(RCEP協定)を取り上げるとともに、日本の国内レベルにおいて、対内直接投資に関する審査メカニズムを定める外国為替及び外国貿易法（昭和24年法

¹ 令和4年12月16日国家安全保障会議決定・閣議決定「国家安全保障戦略」、<https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf>。

² 阿部克則「国際経済法秩序と経済安全保障」日本国際経済法学会年報33号（2024年）43頁。

³ 伊藤一頼「経済安全保障における法の役割——企画趣旨と論点」法律時報96巻1号（2024年）4-9頁参照。

⁴ なお、「中枢的な基盤」とは何か、そしてそれに係る業種は何かということがそもそも問題となる。その内容自体が各国の裁量的な判断に基づくものであり、ここでの検討対象となろう。ちなみに、経済開発協力機構(OECD)によれば、「中枢的な基盤」とは、「現代の相互に接続された各社会の機能の基幹を構成する」ものとされ、それには電気通信サービス、水道やエネルギー供給、運送や金融システムが含まれ、その途絶は、市民の福利に重大な被害をもたらす、直接被害を受けた地域だけにとどまらない経済的な悪影響をもたらす可能性があるという。OECD, Good Governance for Critical Infrastructure Resilience (OECD, 2019), p.18.

律第228号) (以下「外為法」という) 第27条の概要を確認し、国際規範と諸外国の関連国内法制との比較を通じてその評価と課題を検討することにする。

Ⅱ RCEP協定における「中枢的な公共基盤」の取扱い

1. RCEP協定の概要

(1) RCEP 協定の法的地位と目的

RCEP協定は、2022年1月1日にその効力が発生した東アジアで初めてのメガFTAである。きっかけは、2011年にASEANが後にRCEP協定となる自由貿易地域構想を提案したことであった。その後、2012年11月に、ASEAN10か国と、日本、中国、韓国、オーストラリア、ニュージーランド、そしてインドの計16か国が交渉の立ち上げを宣言し、ほぼ8年の交渉期間を経て、2019年11月以降は交渉から離脱したインドを除く15か国が2020年11月に署名を行うに至っている⁵。

RCEP協定第20.6条第2項によると、少なくともASEAN構成国10か国中の6か国と、ASEAN構成国以外の少なくとも3か国が署名国となり、批准書、受諾書又は承認書を寄託者であるASEAN事務局長に寄託した日の後60日で、寄託したこれらの署名国について効力が生ずるとされている。この規定に従い、RCEP協定を署名した15か国のうち、日本のほか、ブルネイ、カンボジア、ラオス、シンガポール、タイ、ベトナム、オーストラリア、中国及びニュージーランドについて2022年1月1日にRCEP協定に効力が発生した⁶。さらに、同条第3項に従って、同年2月1日には韓国について、同年3月18日にはマレーシアについて、翌2023年1月2日にはインドネシアについて、そして同年6月2日にはフィリピンについて、それぞれ効力が発生し、その結果、署名15か国のうち、ミャンマーを除く14か国がRCEP協定の締約国となっているのが現状である⁷。

⁵ なお、インドが RCEP 協定交渉から離脱した理由について、see, P.Gaur, “India’s Withdrawal from RCEP: neutralising national trade concerns”, *Journal of the Asia Pacific Economy*, Vol.22, No.2 (2022), pp.277-281. See also, D.Chakraborty, J.Chaisse & X.Qian, “Is It Finally Time for India’s Free Trade Agreements? The ASEAN “Present” and the RCEP “Future””, *Asian Journal of International Law*, Vol.9 (2019), pp.359-391.

⁶ ASEAN, “RCEP Agreement enters into force” (January 1, 2022), <https://asean.org/rcep-agreement-enters-into-force/>.

⁷ 外務省「RCEP 協定の概要」(令和 5 年 6 月), <https://www.mofa.go.jp/mofaj/files/100284650.pdf>.

RCEP 協定第 20.6 条は以下のとおり。

「1 この協定は、署名国により、それぞれの関係する国内法上の手続に従って批准され、受諾され、又は承認されなければならない。署名国の批准書、受諾書又は承認書は、寄託者に寄託する。

2 この協定は、少なくとも六の ASEAN の構成国である署名国及び少なくとも三の ASEAN の構成国でない署名国が批准書、受諾書又は承認書を寄託者に寄託した日の後六十日で、批准書、受諾書又は承認書を寄託したこれらの署名国について効力を生ずる。

3 この協定が効力を生じた日の後は、この協定は、2 に規定する署名国以外の署名国が批准書、受諾書又は承認書を寄託者に寄託した日の後六十日で、当該署名国について効力を生ずる。」

RCEP協定は、日本が提起したASEAN+6による東アジア包括的経済連携構想(CEPEA)と、ASEAN+3による東アジア自由貿易圏構想(EAFTA)との間において、ASEAN周辺地域である東アジアでの広域な地域経済統合を目指す動きとその対立を前に、ASEANが自ら中心となって広域経済統合を早く進めるべきとの立場から構想・促進された交渉の結果である⁸。したがって、RCEP協定締結に向けた交渉の当初から、その目的にはASEAN中心性の尊重が強調されていたことが、2012年8月に開催されたASEAN+FTAパートナー諸国経済大臣会合で採択された「RCEP交渉の基本指針及び目的」という文書でも確認された。その他、RCEP交渉を立ち上げる目的として、ASEAN構成国とASEANのFTAパートナー諸国との間において、現代的で包括的な、しかも質が高くかつ互恵的な経済連携協定を達成することも明記されている⁹。

RCEP協定署名直前の2019年時点において、RCEP参加15か国のGDPの合計は25.8兆ドルで、世界全体の29%を占めており、参加国の貿易総額（輸出額ベース）は55兆ドル、世界全体の29%に相当していた。また、人口の合計は約22.7億人で、世界全体の30%を占めていたという。このように、地域的に広い範囲にわたり、大規模な経済的影響力を有することになる地域経済統合を目指し、RCEP協定は、地域の貿易や投資の促進及びサプライチェーンの効率化に向けて、市場アクセスを改善し、発展段階や制度の異なる多様な国々の間で知的財産、電子商取引等の幅広い分野のルールを定立することを目的とするものであった¹⁰。

(2) RCEP 協定の主な内容

RCEP協定は、第1章「冒頭の規定及び一般的定義」、第2章「物品の貿易」、第3章「原産地規則」、第4章「税関手続及び貿易円滑化」、第5章「衛生植物検疫措置」、第6章「任意規格、強制規格及び適合性評価手続」、第7章「貿易上の救済」、第8章「サービスの貿易」、第9章「自然人の一時的な移動」、第10章「投資」、第11章「知的財産」、第12章「電子商取引」、第13章「競争」、第14章「中小企業」、第15章「経済協力及び技術協力」、第16章「政府調達」、第17章「一般規定及び例外」、第18章「制度に関する規定」、第19章「紛争解決」、第20章「最終規定」の全20章と、21の附属書からなる。

そこで定められているRCEP協定の内容は、環太平洋パートナーシップに関する包括的及び先進的な協定(CPTPP)ほどの水準ではないとされる。しかし、東アジア地域における貿易と投資の自由化を促進し、市場アクセスを改善しつつ、経済開発段階と国内体制の異なる多

⁸ 篠田邦彦「RCEPと日本—交渉の歩みと日本のFTA戦略」石川幸一・清水一史・助川成也編著『RCEPと東アジア』（文眞堂、2022年）27-29頁参照。

⁹ “Guiding Principles and Objectives for Negotiating the Regional Comprehensive Economic Partnership”, <https://asean.org/wp-content/uploads/2012/05/RCEP-Guiding-Principles-public-copy.pdf>.
日本語訳については、外務省「東アジア地域包括的経済連携(RCEP)交渉の基本指針及び目的（仮訳）」を参照、https://www.mofa.go.jp/mofaj/press/release/24/11/pdfs/20121120_03_04.pdf.

¹⁰ 外務省・財務省・農林水産省・経済産業省「地域的な包括的経済連携(RCEP)協定に関するファクトシート」（令和3年4月）2頁参照、<https://www.mofa.go.jp/mofaj/files/100115475.pdf>.

様な諸国の間で、物品やサービス貿易だけでなく、知的財産や電子商取引を含めて、広範な分野を規律するメガFTAとしての意義は重要である。とりわけRCEP協定において最大の成果といわれているのは、共通特惠原産地ルールの導入であった¹¹。

その他、物品貿易については、その自由化のために多くの規定が定められた。多数の品目の関税が、既存のASEAN+1のFTAを超えて撤廃されるほか、日中や日韓のように、これまでFTAが存在しなかった諸国間でFTAが構築されることになり、最終的に締約国間での関税撤廃率は品目ベースで91%にもなるという。サービス貿易については、既存のASEAN+1のFTAで採用されているポジティブリスト方式のほかに、ネガティブリスト方式も採用され、特定分野につきポジティブリストを採用した諸国も一定の期間内にネガティブリスト方式への転換が求められて、サービス貿易の自由化が促進されることになったのである。投資に関しては、その保護・自由化・促進・円滑化を対象として、既存のASEAN+1や貿易に関連する投資措置に関する協定（TRIMS協定）に基づく措置を上回る水準のパフォーマンス要求の禁止等が定められた。また、知的財産についても、知的所有権の貿易関連の側面に関する協定（TRIPS協定）よりも高水準の知的財産権の保護が認められている¹²。

他方で、RCEP協定はその効力が発生してから5年ごとに「一般的見直し」が行われる予定とされており、その過程で内容の質の向上を図り、より高い水準の自由化やルールの整備が求められるという見方もあり、CPTPPや他の二国間・多数国間EPAとの連携も含め、そのさらなる発展の可能性も期待されている¹³。

2. 例外条項と「中核的な公共基盤」規定

(1) RCEP 協定の例外条項

本稿で検討する「中核的な公共基盤」という用語がRCEP協定で登場するのは、その第17章「一般規定及び例外」の中にある例外条項の第17.13条においてである。「安全保障のための例外」と題する第17.13条は、以下のように規定する。

「この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。

- (a) 締約国に対し、その開示が自国の安全保障上の重大な利益に反すると当該締約国が認める情報の適用を要求すること。

¹¹ 柳赫秀「RCEPと日中韓」日本国際経済法学会年報30号（2021年）130、139-140頁参照。

¹² その他の規定の内容も含め、清水一史「RCEPの意義と東アジア経済統合」石川ほか編著・前掲注(8)13-16頁参照。

¹³ 篠田邦彦「RCEPの今後の課題と日本の役割」馬田啓一・浦田秀次郎・木村福成編著『変質するグローバル化と世界経済秩序の行方 米中対立とウクライナ危機による新たな構図』（文眞堂、2023年）141-145頁参照。

(b) 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを妨げること。

(i) 核分裂性物質若しくは核融合物質又はこれらの生産原料である物質に関する措置

(ii) 武器、弾薬及び軍需品の取引並びに軍事施設に供給するため直接若しくは間接に行われるその他の貨物及び原料の取引に関する措置又は軍事施設のため直接若しくは間接に行われるサービスの提供に関する措置

(iii) 通信、電力及び水道の基盤を含む中枢的な公共基盤（注）を防護するためにとる措置

注 中枢的な公共基盤は、公有のものであるか私有のものであるかを問わない。

(iv) 国家の緊急時又は戦時その他の国際関係の緊急時にとる措置

(c) 締約国が国際の平和及び安全の維持のため国際連合憲章に基づく義務に従って措置をとることを妨げること。」¹⁴

RCEP協定第17章「一般規定及び例外」には、RCEP協定に横断的に適用される一般規定のほか、同協定上の義務を免除される事由となるいわゆる一般的例外と安全保障例外の規定がそれぞれ置かれている¹⁵。その中で、第17.12条が一般的例外条項であり¹⁶、上記の第17.13条が

¹⁴ RCEP 協定第 17 章の和文テキストについては、外務省ホームページを参照、

<https://www.mofa.go.jp/mofaj/files/100129075.pdf>。

RCEP 協定第 17.13 条の正文（英語）は次の通りである。

“Article 17.13: Security Exceptions

Nothing in this Agreement shall be construed:

(a) to require any Party to furnish any information the disclosure of which it considers contrary to its essential security interests;

(b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests:

(i) relating to fissionable and fusionable materials or the materials from which they are derived;

(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials, or relating to the supply of services, as carried on directly or indirectly for the purpose of supplying or provisioning a military establishment;

(iii) taken so as to protect critical public infrastructures⁷ including communications, power, and water infrastructures;

⁷ For greater certainty, this includes critical public infrastructures whether publicly or privately owned.

(iv) taken in time of national emergency or war or other emergency in international relations; or

(c) to prevent any Party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.”

RCEP 協定の英文についても外務省ホームページを参照のこと、<https://www.mofa.go.jp/files/100129124.pdf>。

¹⁵ RCEP 協定第 17 章「一般規定及び例外」の概要については、外務省「地域的な包括的経済連携協定の要約（仮訳）」を参照、<https://www.mofa.go.jp/mofaj/files/100114949.pdf>。

¹⁶ 一般的例外を規定した RCEP 協定第 17.12 条は次の通りである。

「1 第二章（物品の貿易）、第三章（原産地規則）、第四章（税関手続及び貿易円滑化）、第五章（衛生植物検疫措置）、第六章（任意規格、強制規格及び適合性評価手続）、第十章（投資）及び第十二章（電子商取引）の規定の適用上、千九百九十四年のガット第二十条の規定は、必要な変更を加えた上で、この協定に組み込まれ、この協定の一部を成す。（注）

注 締約国は、千九百九十四年のガット第二十条(b)に規定する措置には、人、動物又は植物の生命又は健康の保護のために必要な環境に関する措置が含まれること並びに同条(g)の規定が有限天然資

安全保障例外条項とされている。したがって、「中枢的な公共基盤」という用語が出てくるのは、安全保障例外条項の中においてということになる。

例外（条項）とは、条約の当事国が、そうでなければ当該条約上の実体義務と両立しない行動を適法にとることを認める根拠・規定であり、なかでも、安全保障例外（条項）は、そうした行動が安全保障上の理由からとられるというものである¹⁷。その典型例としては、関税及び貿易に関する一般協定（GATT）第21条やサービスの貿易に関する一般協定（GATS）第14条の2、TRIPS協定第73条があるが、こうしたいわゆる世界貿易機関（WTO）協定以外の、二国間投資協定（BIT）や自由貿易協定（FTA）、経済連携協定（EPA）などの経済関係条約にも、この種の安全保障例外条項が様々なかたちで挿入されている¹⁸。特にGATT第21条は、経済関係協定において最も早く定式化された安全保障例外条項であり、その形式においてもその具体的な事由においても、後に取り入れられた他の経済関係協定における安全保障例外条項に大きな影響を与えてきた。

実際、RCEP協定の第17.13条に規定された安全保障例外事由も、GATT第21条の形式と内容を基礎にしている。例えば、第17.13条(a)はGATT第21条(a)に、RCEP協定第17.13条(b)(i)、(b)(ii)、(b)(iv)はGATT第21条(b)(i)、(b)(ii)、(b)(iii)に、そしてRCEP協定第17.13条(c)はGATT第21条(c)に、それぞれ対応している。

これに対して、GATTの安全保障例外には含まれていない事項でRCEP協定第17.13条に定められたのは、第17.13条に新たに入れられた同条(b)(iii)の規定と、同条(b)(iv)の冒頭の「国家の緊急時(national emergency)」である。すなわち、GATTやGATSのいずれにも規定されていない、「中枢的な公共基盤」の防護のための措置及び「国家の緊急時」の措置がRCEP協定第17.13条には付加されており、結果としてこの条項はWTO協定の場合よりも広い範囲を安全保障例外として認めているということになる¹⁹。特に前者の第17.13条(b)(iii)の規定に本稿で検討の素材としている「中枢的な公共基盤」という用語が含まれていることがここでは重要である。これに関しては、以下の2つの点を指摘することができるであろう。

源（生物資源であるかどうかを問わない。）の保存に関する措置について適用されることを了解する。

2 第八章（サービスの貿易）、第九章（自然人の一時的な移動）、第十章（投資）及び第十二章（電子商取引）の規定の適用上、サービス貿易一般協定第十四条（注を含む。）の規定は、必要な変更を加えた上で、この協定に組み込まれ、この協定の一部を成す。（注）

注 締約国は、サービス貿易一般協定第十四条に規定する措置には、人、動物又は植物の生命又は健康の保護のために必要な環境に関する措置が含まれることを了解する。」

¹⁷ 拙稿「GATT/WTO 体制における『安全保障例外』の審査可能性とその意義」日本エネルギー法研究所編『エネルギー資源確保に関する国内外の法的問題の諸相—2015～2016 年度エネルギー資源確保に関する国際問題検討班報告書—（JELI-R-No.148）』（2023 年）83-84 頁。

¹⁸ S.Mantilla Blanco & A.Pehl, National Security Exceptions in International Trade and Investment Agreements. Justiciability and Standards of Review (Springer, 2020), p.2.

¹⁹ 日本関税協会『RCEP コメンタール』（日本関税協会，2022 年）235-236 頁。謝笠天（石川義道・濱田太郎訳）『国際経済法における新アジア地域主義』（信山社，2024 年）85-86 頁参照。

第一に、「中枢的な公共基盤」は、第17.12条の一般的例外ではなく、あくまで安全保障例外の文脈において規定されており、その防護のための措置が例外事由となるということである。特に例示として挙げられている通信、電力及び水道について、これらに関する中枢的な基盤を防護することが安全保障を理由とした例外事由の枠内に位置づけられていることは、後にみるように、これを安全保障例外ではなく一般的例外の事由とみなしているように思われる規定を有する条約もあるだけに、ここで確認しておく必要がある。

第二に、RCEP協定の安全保障例外の事由がWTO協定の場合よりも広がっており、「中枢的な公共基盤」を防護する措置がその事由の1つであるということの意味である。すなわち、「中枢的な公共基盤」を防護する措置がGATTやGATS、TRIPS協定、そして政府調達協定のようなWTO協定の安全保障例外条項に明示的には含まれていないため、安全保障例外条項に関するWTOの紛争解決手続でのパネルの判断は、この「中枢的な公共基盤」自体の文言の解釈や「中枢的な公共基盤」を防護する措置の内容について直接参考となるようなものとはならない。各種経済関係協定の安全保障例外条項の多くはGATT第21条を参考にして作成されており、その限りでは、当該協定の紛争解決手続において判断された安全保障例外条項の解釈・適用を通じて「中枢的な公共基盤」をめぐる紛争において参考となるような基準が提供されることは期待しにくいということになる。

(2) RCEP 協定における「中枢的な公共基盤」の意味

RCEP協定の安全保障例外条項に定められた「中枢的な公共基盤」に係る事由は、この協定で突然登場したものではない。特にASEANが締結した経済関係協定では、「中枢的な公共基盤」に関する条文が安全保障例外条項に含められているものがある。

RCEP協定締結前のそのような協定としては、例えば、2009年にASEANとインドの間でASEAN・インド包括的経済協力枠組条約が締結され、この枠組条約の下に置かれた物品貿易協定第13条に安全保障例外が規定された例がある。その第1項は、「この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。」としたうえで、b号で、「締約国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを定めること」が該当するとして、その措置の中には、「中枢的な通信基盤を無力化し又は劣化させることを意図した故意の試みから当該基盤を防護するためにとる行動」が含まれるとした（13条1項(b)(iii)）。すなわち、ここでは、RCEP協定の場合と同様に、公共基盤の中でも特に通信施設を防護するためにとられる措置が安全保障例外として認められているのである²⁰。

²⁰ ASEAN・インド包括的経済協力枠組条約下の物品貿易協定(https://commerce.gov.in/wp-content/uploads/2020/06/MOC_636205354502532516_ASEAN-India_Trade_Goods_Agreement.pdf)第13条第1項(b)(iii)は次の通りである。

“Article 13 Security Exceptions

Nothing in this Agreement shall be construed:

ASEANが締結した同時期の条約としては、2009年のASEAN・韓国包括的経済協力枠組協定(AKFTA)の下で締結されたサービス貿易協定第14条第1項(b)(iii)、物品貿易協定第12条(b)(iii)、及び投資協定第21条第1項(b)(iv)があり、その安全保障例外条項はほぼ同様に「中核的な公共基盤」という文言が含まれている²¹。同じく2009年のASEAN・オーストラリア・ニュージーランド自由貿易協定(AANZFTA)第15章第2条第1項(b)(iii)もまた、RCEP協定第17.13条(b)(iii)と同一の文言である²²。さらにこれもまた2009年に締結されたASEAN包括的投資協定第18条(b)(iv)にも、「中核的な公共基盤」という文言が含まれる同趣旨の規定が定められている²³。

(b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests, including:

(iii) action taken so as to protect critical communications infrastructure from deliberate attempts intended to disable or degrade such infrastructure;”

また、同枠組条約下でそれぞれ2014年に締結されたサービス貿易協定(https://commerce.gov.in/wp-content/uploads/2020/12/MOC_636040205325835433_ServicesAgreement.pdf)第13条第1項(b)(iii)及び投資協定(https://commerce.gov.in/wp-content/uploads/2020/05/MOC_636040211593720663_InvestmentAgreement.pdf)第22条第1項(b)(iv)の場合は、同枠組条約下の物品貿易協定第13条第1項(b)(iii)の規定と類似しているが、“critical communications infrastructure”が“critical public infrastructure”とされているほか、“including communication, power and water infrastructures”という文言が新たに挿入されている。

²¹ AKFTA サービス貿易協定第12条第1項(b)(iii)は以下の通りである。

“Article 12 Security Exceptions

1. Nothing in this Agreement shall be construed: ...

(b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests, including but not limited to: ...

(iii) action taken so as to protect critical public infrastructures including communications, power and water infrastructures from deliberate attempts intended to disable or degrade such infrastructures;...”

AKFTA 投資協定第21条第1項(b)(iv)ほぼ同一、AKFTA 物品貿易協定第12条(b)(iii)では“critical communications infrastructure”のみで電気・水道は含まれていないが、それ以外はほぼ同じである。Malaysia’s Free Trade Agreements: ASEAN-Korea, <https://fta.miti.gov.my/index.php/pages/view/asean-korea?mid=37>.

²² AANZFTA 第15章第2条第1項(b)(iii)は以下の通りである。

“Article 2 Security Exceptions

1. Nothing in this Agreement shall be construed: ...

(b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests: ...

(iii) taken so as to protect critical public infrastructures³ including communications, power and water infrastructures from deliberate attempts intended to disable or degrade such infrastructures;

³ For clarity, this includes critical public infrastructures whether publicly or privately owned. ...”

Australia, ASEAN-Australia- New Zealand Free Trade Area, <https://www.dfat.gov.au/trade/agreements/in-foc/rce/aanzfta/official-documents/Pages/official-documents>.

²³ ASEAN 包括的投資協定第18条(b)(iv)は以下の通りである。

“Article 18 Security Exceptions

Nothing in this Agreement shall be construed: ...

(b) to prevent any Member State from taking any action which it considers necessary for the protection of its essential security interests, including but not limited to: ...

(iv) action taken so as to protect critical public infrastructure, including communication, power and water infrastructures, from deliberate attempts intended to disable or degrade such infrastructure; ”

ASEAN Comprehensive Investment Agreement, <https://investasean.asean.org/asean-comprehensive-investment-agreement-acia---section-a/view/799/newsid/841/article-18--security-exceptions.html>

これらの規定に共通するのは以下の2点である。第一に、上記のいずれの規定も安全保障例外規定の一部として位置づけられている。すなわち、「中枢的な公共基盤」を防護する措置は、「締約国が自国の安全保障上の重大な利益のために必要であると認める」措置とされているのである。安全保障例外の特徴の1つは、「締約国が…必要であると認める」という「自己判断的な」性格を有する文言から、これを援用する締約国の裁量が広範に認められることであり、したがって、「中枢的な公共基盤」を防護する措置についても、「自国の安全保障上の重大な利益」のための必要性という観点からこうした裁量が締約国に認められるということになる。

第二に、「中枢的な公共基盤」の例として、「通信、電力及び水道」といったインフラが挙げられ例示されているという点である。すなわち、「中枢的な通信基盤」と規定することで「中枢的な基盤」を「通信」に特化したASEAN・インド包括的経済協力枠組条約下の物品貿易協定第13条第1項(b)(iii)の場合を除き、それ以外の「中枢的な公共基盤」と規定する協定では、この「中枢的な公共基盤」に「通信、電力及び水道」というインフラが含まれるだけでなく、それ以外にも「中枢的な公共基盤」とみなされるインフラの存在が排除されていない。しかも、先に述べたように、この「中枢的な公共基盤」を安全保障例外に位置づけることで、「中枢的な公共基盤」の内容とそれを防護するための措置について当該措置をとる締約国に広範な裁量が認められることから、「中枢的な公共基盤」にどのような業種が含まれるかということについても、「安全保障」概念に関係する限り様々な業種が含まれる可能性が生じ、同概念が拡大すれば「中枢的な公共基盤」概念も拡大するという状況が発生するのである。

RCEP協定における「中枢的な公共基盤」規定も、まさに上記のようなこうした特徴を有している。このような規定を締約国が国内で実施するためには、それぞれの国内法制において受け皿を用意しておかなければならない。日本の場合、「中枢的な（公共）基盤」に関する規定を含んだ経済関係協定に対してどのように対応してきたのであろうか。そして、特に外資規制のためにいかなる国内法制の下で、こうした「中枢的な（公共）基盤」をめぐる規則がどのように実施されるのであろうか。

Ⅲ 日本における対内直接投資規制と「中枢的な基盤」の関係

1. 日本が締結した経済関係協定における例外規定と「中枢的な基盤」

(1) 一般的例外事由としての「中枢的な基盤」規定

日本がそれまでの方針を変更してBITやFTA・EPAの締結に積極的な姿勢を示すようになったのは2000年初頭以降のことであった²⁴。そして、日本が締結した2002年以降のほとんどの

²⁴ 小寺彰「国際投資法の発展－現状と課題」日本国際経済法学会編『国際経済法講座Ⅰ 通商・投資・競争』（法律文化社、2012年）284-285頁。

BITやEPAには、一般的例外とともに、安全保障例外が規定として含まれるようになっている²⁵。

他方、日本が締結した経済関係協定の中で、RCEP協定第17.13条(b)(iii)の規定のように、「中枢的な（公共・通信等）基盤」という語句を含む条項を取り入れているものは、RCEP協定以外では3つしかない。その1つで、この語句を例外条項に含めた最初の協定は、日本が締結した最初のEPA協定でもある2002年の日本・シンガポールEPAであった²⁶。同協定の第4条は、「安全保障のための例外及び一般的な例外」という表題の下、以下のような内容を定めている。

「1 この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない。

(a) 締約国に対し、その開示が自国の安全保障上の重大な利益に反すると当該締約国が認める情報の提供を要求すること。

(b) 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを妨げること。

(i) 核分裂性物質若しくは核融合性物質又はこれらの生産原料である物質に関する措置

(ii) 武器、弾薬及び軍需品の取引並びに軍事施設に供給するため直接または間接に行われるその他の貨物及び原料の取引に関する措置

(iii) 軍事施設のため直接又は間接に行われるサービスの提供に関する措置

(iv) 武器、弾薬若しくは軍需品の調達又は国家の安全保障のため若しくは国家の防衛上の目的のために不可欠な調達に関連する措置

(v) 戦時その他の当該締約国又は国際関係の緊急時にとる措置

(c) 締約国が国際の平和及び安全の維持のため国際連合憲章に基づく義務に従って措置をとることを妨げること。

2 1の規定の適用に当たり、適当な場合には、世界貿易機関設立協定中の関連規定の解釈及び運用を考慮する。

²⁵ 安全保障例外条項が含まれていないのは、日本・パプアニューギニア BIT(2011)、日本・イラク BIT(2012)及び日本・サウジアラビア BIT(2013)のみである。以上について、拙稿「日本が締結した経済関係協定における安全保障例外条項について」日本エネルギー法研究所編『エネルギーに関する国際取決めの法的問題の諸相—2017～2018年度エネルギーに関する国際取決めの法的問題検討班報告書—(JELI-R-No.154)』(2023年)54-58頁参照。

²⁶ 日本がEPAを締結する相手国をシンガポールに選んだ理由や両国間の交渉内容、締結されたEPAの成果と特徴などについては、渡邊頼純監修・外務省経済局EPA交渉チーム編著『解説 FTA・EPA交渉』(日本経済評論社、2007年)45-67頁参照。

- 3 この協定のいかなる規定も、締約国が中枢的な通信基盤を不法な行為から防護するために必要な措置をとることを妨げるものと解してはならない。」²⁷

本稿の目的から注目されるのは、言うまでもなく、この第4条のうち、その第3項となる。ここでは、「中枢的な通信基盤(communication infrastructure of critical importance)」を不法な行為から防護するための必要な措置が予定されており、この措置を行うに当たり、これを例外事由として、締約国は日本・シンガポールEPA上の義務を免れることが可能となるのである。

この第4条第3項の規定に関連して留意しなければならないことは、この規定が安全保障例外の事由としてではなく、それ以外の一般的例外事由に該当するという点であろう。第4条の表題は「安全保障のための例外及び一般的な例外」とあり、その内容は、安全保障例外と一般的例外の2種類の例外事由で構成されることが示されている。第4条は3つの項からなるが、第4条第1項は、その規定振りから、GATT第21条とGATS第14条の2という安全保障例外条項を参照して作成されていることが明らかであり、このため第4条第1項は安全保障例外の規定であると考えられる。また、第2項の規定も、「1の規定を適用するにあたり、」とあることから、第1項の安全保障例外の規定の解釈に際してはWTO協定における安全保障例外条項の解釈・適用を考慮する趣旨であり、したがって、安全保障例外に属する規定である。このように、第1項も第2項も安全保障例外に関する規定だとすると、残る第3項は、第4条の表題「安全保障のための例外及び一般的な例外」からみて、安全保障例外ではなく、一般的例外と位置付けられなければならない。すなわち、日本・シンガポールEPAは、「中枢的な通信基盤」を不法な行為から防護するために必要な措置をとることを一般的例外に位置づけているということになる。このことは、先にみたような、RCEP協定を含め、その後に締結さ

²⁷ 日本・シンガポール EPA 第4条の英文は以下の通りである。

“Article 4 Security and General Exceptions

1. Nothing in this Agreement shall be construed:

(a) to require a Party to furnish any information the disclosure of which it considers contrary to its essential security interests;

(b) to prevent a Party from taking any action which it considers necessary for the protection of its essential security interests:

(i) relating to fissionable and fusionable materials or the materials from which they are derived;

(ii) relating to traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;

(iii) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment;

(iv) relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes;

(v) taken in time of war or other emergency within that Party or in international relations; or

(c) to prevent a Party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

2. In the application of paragraph 1 above, the relevant interpretations and operation of the WTO Agreement shall, where appropriate, be taken into account.

3. Nothing in this Agreement shall be construed to prevent a Party from taking any action necessary to protect communications infrastructure of critical importance from unlawful acts against such infrastructure.”

れた協定が、「中核的な公共基盤」を防護する措置をとることを安全保障例外に含めていることと好対照をなす。

なぜ、日本・シンガポールEPAでは、「中核的な通信基盤」に関する規定が安全保障例外に分類されなかったのであろうか。実は、「中核的な（通信・公共）基盤」という語句が経済関係協定に規定されたのは、管見の限り、この日本・シンガポールEPAが初めてであった。このため、その位置づけについて先例がなかったということも関係しているのではないかとと思われる。また、この協定では、「中核的な公共基盤」というより一般性を纏う用語ではなく、「中核的な通信基盤」という通信分野が特に対象であったということにも留意しなければならない。安全保障例外条項がようやく経済関係協定にも含まれるようになってきたこの時期において、当該条項が対象とする事項に何が含まれるかについては、先行するGATT第21条の規定が参照されたであろうと推測すると、「通信」分野に関する措置が、軍事的な活動に関係する事項に対応した安全保障例外とは異なるものと考えられたと推測することもできよう。

さらに、日本にとっては、自らが締結した経済関係協定において初めて安全保障例外条項が規定されたのも、この日本・シンガポールEPAであった。日本は、1980年代まで、通信を含め、航空運送や海運、放送などに関する対内直接投資の規制について、1961年のOECD資本移動の自由化に関する規約（OECD資本移動自由化規約）第3条(ii)にいう「当該加盟国の安全保障のための実質的な利益を保護する」ために必要な措置とみなしていた。しかし、1990年から91年にかけてのOECDの審査により、通信に係る対内直接投資の規制については、同規約の安全保障例外に関する第3条(ii)に根拠を置くのではなく、第2条a号にいう自由化措置に関する義務への留保として扱われるべきとの指摘を受けたが²⁸、こうしたことも、日本・シンガポールEPAの例外条項の規定作成に何らかの影響を及ぼしていたと考えられる。OECD資本移動自由化規約第3条(i)にいう「公の秩序」に該当する事項には、電力、ガス、熱供給、通信、放送、旅客運送、鉄道などが含まれるのに対して、同条(iii)の「安全保障」には、武器、航空機、原子力、宇宙開発など分野に関連するとされており、通信分野が日本・シンガポールEPAでは安全保障例外ではなく、一般的例外に位置づけられることになったのは、GATTの一般的例外及び安全保障例外の諸規定のほか、こうしたOECD資本移動の自由化に関する規約（OECD資本移動自由化規約）の適用をめぐる日本の立場の変化も作用していることが予想される²⁹。ここには、一般的例外と安全保障例外の区別という問題のほ

²⁸ 中谷和弘『経済安全保障と国際法』（信山社、2024年）47頁。

²⁹ 実際にも、同EPA第8章のいわゆる投資章に適用される例外規定には国家安全保障への言及はなく、「公衆の道徳の保護または公の秩序の維持のために必要な措置」がとり得ることが規定されており（第83条第1項(a)）、これは安全保障例外ではなく、一般的例外だけが投資章には、すなわち外国投資に適用されることを示すものである。

か、「公の秩序(public order)」と「国家安全保障(national security)」の区別とその基準という問題が伏在しているのである。

(2) 安全保障例外事由としての「中枢的な公共基盤」規定

日本・シンガポールEPAでは一般的例外の事由として「中枢的な通信基盤」が盛り込まれたが、それ以降、日本が締結した経済関連協定に「中枢的な（公共・通信等）基盤」という語句が盛り込まれることはそれほど多くはなく、RCEP協定締結までの間では2つの例があるにすぎない。しかも、この語句が例外として含まれる場合でも、日本・シンガポールEPAの場合と異なり、一般的例外ではなく、安全保障例外として位置付けられてきたことが注目される。

その一例が、2008年に日本がASEANとの間で締結した日本・ASEAN包括的経済連携協定(AJCEP)である。2002年に日本・シンガポールEPAが締結されてから2008年のAJCEPの締結まで、日本は4本のBITと7本のEPAに署名したが³⁰、そのいずれにおいても「中枢的な公共基盤」に関する規定が盛り込まれることはなかった。さらに、その間、日本が締約国ではない経済関係協定でも、「中枢的な公共基盤」に言及があったものは、2005年のインド・シンガポール包括的経済協力協定(CECA)のみであり³¹、AJCEPはそれに続く3例目ということになる。

「中枢的な公共基盤」を含むAJCEP第8条は、以下のように規定する。

「第8条 安全保障のための例外

³⁰ 日本・韓国(2002)、日本・ベトナム(2003)、日本・カンボジア(2007)、日本・ラオス(2008)の各BITと、日本・メキシコ(2004)、日本・マレーシア(2005)、日本・フィリピン(2006)、日本・チリ(2007)、日本・タイ(2007)、日本・ブルネイ(2007)、日本・インドネシア(2007)の各EPAである。

³¹ インド・シンガポールCECAでは第6.12条の第1項(b)(iv)に「中枢的な公共基盤」への言及がある。同条は以下の通りである。

“Article 6.12 Security Exceptions

1. Nothing in this Chapter shall be construed:

(a) to require a Party to furnish any information, the disclosure of which it considers contrary to its essential security interests; or

(b) to prevent a Party from taking any action which it considers necessary for the protection of its essential security interests

(i) relating to fissionable and fusionable materials or the materials from which they are derived;

(ii) in time of war or other emergency in international relations;

(iii) relating to the production or supply of arms and ammunition; or”

(iv) to protect critical public infrastructures, including communication, power and water infrastructures, from deliberate attempts intended to disable or degrade such infrastructures; or

(c) to prevent a Party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.”

第6.12条は安全保障例外条項で、防護措置の対象となる「中枢的な公共基盤(critical public infrastructure)」はその第1項(b)(iv)において言及があり、その例として、「通信、電力及び水道の基盤(communication, power and water infrastructures)」が挙げられている。<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/2707/download>。

この協定のいかなる規定も、次のいずれかの事項を定めるものと解してはならない。

- (a) 締約国に対し、その開示が自国の安全保障上の重大な利益に反すると当該締約国が認める情報の提供を要求すること。
- (b) 締約国が自国の安全保障上の重大な利益の保護のために必要であると認める次のいずれかの措置をとることを妨げること。
 - (i) 核分裂性物質又はその生産原料である物質に関する措置
 - (ii) 武器、弾薬及び軍需品の取引並びに軍事施設に供給するため直接又は間接に行われるその他の貨物及び原料の取引に関する措置
 - (iii) 通信、電力及び水道の基盤を含む中枢的な公共基盤を使用不能にし、又は破壊することを意図した計画的な企てから、当該公共基盤を防護するためにとる措置
 - (iv) 国内における緊急時又は戦時その他の国際関係の緊急時にとる措置
- (c) 締約国が国際の平和及び安全の維持のため国際連合憲章に基づく義務に従って措置をとることを妨げること。」³²

この第8条の(b) (iii)には、「通信、電力及び水道の基盤を含む」「中枢的な公共基盤」を防護するためにとる措置が締約国により認められる安全保障例外事由として掲げられており、それによりAJCEP上の義務の免除が認められることが認められている。すなわち、「中枢的な公共基盤」の防護措置は、一般的例外ではなく、「自己判断的な」性格の文言を擁する安全保障例外とされていること、そしてこの「中枢的な公共基盤」には、日本・シンガポールEPAの場合のように通信だけではなく、電力と水道の基盤が含まれ、さらにこれらに限られない業務も該当する余地があることが示されているのである³³。

³² AJCEP 第8条の英文は以下の通りである。

“Article 8 Security Exceptions

Nothing in this Agreement shall be construed:

(a) to require any Party to furnish any information, the disclosure of which it considers contrary to its essential security interests; or

(b) to prevent any Party from taking any action which it considers necessary for the protection of its essential security interests:

(i) relating to fissionable materials or the materials from which they are derived;

(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;

(iii) taken so as to protect critical public infrastructure, including communications, power and water infrastructures, from deliberate attempts intended to disable or degrade such infrastructure;

(iv) taken in time of domestic emergency, or war or other emergency in international relations; or

(c) to prevent any Party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.”

³³ なお、2008年に締結されたAJCEPについては、その後、2019年にその第一改正議定書が締結され、安全保障例外条項である第8条も改正された。しかし、「中枢的な公共基盤」に関係する例外事由に関しては、文言に変更はなく、そのままのかたちで第8章第1項(b) (iv)に規定されている（同議定書第3条参照）。外務省「日・ASEAN 包括的経済連携(AJCEP) 協定第一改正議定書」、https://www.mofa.go.jp/mofaj/gaiko/fta/j_asean/page23_002962.html。

また、「中核的な公共基盤」という用語を含むもう1つの例は、2011年に締結された日本・インド包括的経済連携協定(CEPA)の第11条である。その第1項、第2項及び第3項は以下のよう

「第11条 例外

- 1 この協定（第六章及び第九章を除く。）の適用上、千九百九十四年のガット第二十条及び第二十一条の規定は、必要な変更を加えた上で、この協定に組み込まれ、この協定の一部を成す。
- 2 第六章及び第八章の規定の適用上、サービス貿易一般協定第十四条及び第十四条の二の規定は、必要な変更を加えた上で、この協定に組み込まれ、この協定の一部を成す。
- 3 この協定のいかなる規定も、締約国が、通信、電力及び水道の基盤を含む中核的な公共基盤を使用不能にし、又は破壊する計画的な企てから当該公共基盤を防護するという自国の安全保障上の重大な利益の保護のために必要であると認める措置をとることを妨げるものと解してはならない。

注釈 この3の規定は、世界貿易機関設立協定に基づく両締約国の権利を害し、及び義務を免れさせるものと解してはならない。」³⁴

この規定もまた、AJCEP第8条の規定と同様に、「中核的な公共基盤」には「通信、電力及び水道の基盤」も含まれることを確認すると同時に、この「中核的な公共基盤」に係る規定が安全保障例外に該当することを明らかにしている。同条第3項は、「通信、電力及び水道の基盤を含む中核的な公共基盤」という文言を用いて、その防護措置が「自国の安全保障上の重大な利益の保護のために必要であると認める措置」であるとしているからである。この規定はその文言から「自己判断的な」性格を有し、「中核的な公共基盤」を防護する措置は、それを行う国が自国の安全保障上の重大な利益のために必要であると判断すればとることができる措置だとされている。

(3) 日本が締結した経済関係協定における「中核的な公共基盤」の特徴

³⁴ 日本・インド CEPA 第 11 条の第 1 項から第 3 項までは以下の通りである。

“Article 11 Exceptions

1. For the purposes of this Agreement except Chapters 6 and 9, Articles XX and XXI of the GATT 1994 are incorporated into and form part of this Agreement, *mutatis mutandis*.

2. For the purposes of Chapters 6 and 8, Articles XIV and XIV bis of the GATS are incorporated into and form part of this Agreement, *mutatis mutandis*.

3. Nothing in this Agreement shall be construed to prevent a Party from taking any action which it considers necessary for the protection of its essential security interests to protect critical public infrastructure, including communications, power and water infrastructure, from deliberate attempts to disable or degrade such infrastructure.

Note: Nothing in this paragraph shall be construed so as to derogate from the rights and obligations of the Parties under the WTO Agreement.”

このように、日本が締結した50本以上の経済関係協定で「中核的な公共基盤」に言及したものは、これまでのところ、日本・シンガポールEPA(2002)、AJCEP(2008)、日本・インドCEPA(2011)、そしてRCEP協定(2020)の4本に限られる。その意味では、BITやEPAなどの経済関係協定に「中核的な公共基盤」の防護に言及した条項を入れることが日本の実行として定着しているわけではなく、むしろ、交渉の相手国が「中核的な公共基盤」に言及する条文の規定を求めたことで、こうした協定が締結されたということが推測されるであろう。

そこで締約国に目を移すと、上記協定について日本の相手方締約国となったのは、ASEANとその構成国のほかにインドといった諸国であった。シンガポールは、すでに述べたように2002年の日本との間のEPAにおいて最も早く「中核的な（通信）基盤」に関する条項を導入した後、インド、台湾、イラン、EU、インドネシア、そしてミャンマーとの間で締結した各協定に「中核的な公共基盤」の規定を置き、これをいずれも安全保障例外条項の中に位置づけた³⁵。ASEANについては、日本との間でAJCEPを締結した後、インド、韓国、オーストラリア・ニュージーランド、中国、香港とそれぞれ締結した協定において「中核的な公共基盤」に関する規定を安全保障例外条項に含めている³⁶。ASEAN構成国としては、先に述べたようにインドネシアとミャンマーが同じASEAN構成国のシンガポールとそれぞれ協定を締結しているほか、マレーシアがオーストラリアと、カンボジアが韓国と、そしてタイがスリランカと締結した協定において、それぞれ「中核的な公共基盤」の規定を安全保障例外条項においている³⁷。また、ASEAN諸国以外では、インドもまた、安全保障例外条項に「中核的な公共基盤」という用語を含めた協定を比較的に数多く締結しているのが注目される

³⁵ シンガポール・インド CECA(2005)第 6.12 条第 1 項(b)(iv)、シンガポール・台湾 EPA(2013)第 16.3 条(b)注 29、シンガポール・イラン BIT(2016)第 14 条(c)、シンガポール・EU 投資保護協定(2018)第 4.5 条(b)(iv)、シンガポール・インドネシア BIT(2018)第 40 条注 25、シンガポール・ミャンマーBIT(2019)第 30 条注 16 がそれぞれ該当する規定である。

³⁶ ASEAN・インド包括的経済協力枠組み協定(CECFA)物品貿易協定(2009)第 13 条(b)(iii)、ASEAN・インド CECFA サービス貿易協定(2009)第 13 条第 1 項(b)(iii)、ASEAN・インド CECFA 投資協定(2009)第 22 条第 1 項(b)(iv)、ASEAN・韓国 CECFA 投資協定(2009)第 21 条第 1 項(b)(iv)、ASEAN・オーストラリア・ニュージーランド FTA(AANZFTA)第 15 章第 2 条第 1 項(b)(iii)注 3、ASEAN・中国 CECFA 投資協定(2009)第 17 条(b)(iii)、ASEAN・インド CECFA 投資協定(2014)第 22 条第 1 項(b)(iv)、ASEAN・香港投資協定(2017)第 8 条第 1 項(b)(iv)である。

³⁷ それぞれ、マレーシア・オーストラリア FTA(2012)第 18.2 条第 1 項(b)(iii)注 39、カンボジア・韓国 FTA 第 9.2 条第 1 項(b)(iii)、タイ・スリランカ FTA(2024)第 9.20 条第 1 項(b)(iii)である。なお、ASEAN 諸国は 2009 年に ASEAN 包括的投資協定を締結しており、安全保障例外条項であるその第 18 条(b)(iv)でも「中核的な公共基盤」の防護への言及がある。

38. もっとも、ASEAN諸国とインドが締約国である場合を除けば、「中核的な公共基盤」の防護を例外に位置づける規定が定められた経済関係協定はほとんど存在しない³⁹。

このようにしてみると、ASEAN諸国やインドとの間で経済関係協定を締結する場合には、「中核的な公共基盤」に関する規定を盛り込むことが、常にではないにしても多くの場合に実行として行われてきたことがわかる。実際、日本が締結した上記4本の協定も、相手方締約国（の一部）がシンガポール、インド及びASEAN諸国であることから、こうした実行の一部を構成していることになるのである。

以上のような「中核的な公共基盤」規定を含む経済関係協定を概観した場合、次のような特徴があることに留意しなければならない。第一に、これら経済関係協定に規定された「中核的な公共基盤」は、日本・シンガポールEPAの場合を除いてすべて安全保障例外条項に位置づけられているということがある。日本・シンガポールEPAはこうした特徴を有する協定が主流となる前に締結されたことや、「中核的基盤」が通信分野に限定されていたことも、この特徴に該当しない理由となるであろう。「中核的な公共基盤」の対象分野ということであれば、第二に、「中核的な公共基盤」の内容について、関係する協定のほとんどが「通信、電力及び水道基盤を含む(including communication, power and water infrastructures)」というように、通信・電力・水道の各インフラを代表例として、その対象となるインフラをそれらに限定しないような規定振りとなっていることが挙げられる⁴⁰。しかも、「中核的な公共基盤」が

38 先に示したシンガポールとの CECA (2005) や日本との CEPA (2011) のほか、インド・韓国 CEPA 第 6.15 条第 1 項 (b) (iv)、インド・マレーシア FTA (2011) 第 12.2 条第 1 項 (b) (iv) がある。さらに、2015 年には、2003 年のモデル BIT を改訂して、新たに安全保障例外条項とそこに「中核的な公共基盤」に言及した規定（第 33 条第 1 項 (ii) (d)）を含めたモデル BIT を定めて以降、インド・ベラルーシ BIT (2018) 第 33 条第 33.1 項 (ii) (d)、インド・キルギスタン BIT (2019) 第 33 条第 33.1 項 (ii) (d)、インド・ブラジル BIT (2020) 第 24 条 (b) (iv)、インド・モーリシャス経済協力連携協定 (CECPA) (2021) 第 6.21 条第 1 項 (b) (iv)、インド・アラブ首長国連邦 (UAE) CEPA (2022) 第 16.2 条第 1 項 (b) (iv)、インド・オーストラリア経済協力貿易協定 (ECTA) (2022) 第 11.2 条第 1 項 (b) (v)、インド・UAEBIT (2024) 第 34 条第 34.1 項 (ii) (d) に、それぞれ「中核的な公共基盤」に関する規定が定められている。

39 太平洋諸島フォーラム (PIF) 加盟国の中で 11 か国（オーストラリア、クック諸島、キリバス、ナウル、ニュージーランド、ニウエ、サモア、ソロモン諸島、トンガ、ツバル、バヌアツ）が経済と貿易に関する統合協定として 2017 年に締結した太平洋諸島経済緊密化協定 (PACER Plus) が数少ない例であり、その第 11 章第 2 条第 1 項 (b) (iii) 注 4 に「中核的な公共基盤」の防護を安全保障例外事由とする旨の規定が定められている。その他では、西アフリカ諸国経済共同体 (ECOWAS) が、域内のすべての投資活動に関する法的制度的枠組みを調和させ、それによって投資、持続可能な開発、外国直接投資の誘致、域内の貿易・投資関係を促進することを目的として、2019 年に ECOWAS 共通投資コード (ECOWIC) を定め、その第 9 条 (2) (b) (iv) が「中核的な公共基盤」の防護のための行動を安全保障例外事由としていることが注目される。

40 さらに、シンガポール・台湾 EPA (2013) 第 16.3 条 (b) 注 29、シンガポール・インドネシア BIT (2018) 第 40 条注 25 及びシンガポール・ミャンマー BIT (2019) 第 30 条注 16 では、通信・電力・水道インフラのほかに、運送 (transportation) の追加も明記している。こうした注はその対象である条文の適用範囲を拡大させる締約国の意図を明確化させている。P. Accaoui Lorfing, “The International Legal Framework for Foreign Investment Control”, in J. Hillebrand Pohl, Th. Papadopoulos & J. Wiesenthal (eds.), *National Security and Investment Control* (Springer, 2024), p. 135. 他方で、インド・韓国 CEPA (2009) 第 6.15

「公的所有か私的所有かにかかわらず (whether publicly or privately owned)」という規定がある場合もあり⁴¹、安全保障例外の特質から、協定締約国が「中枢的な公共基盤」概念を柔軟に解し、その範囲を広げる余地を残すかたちとなっているのである。

もつとも、何が具体的に「中枢的な」インフラに該当するのかについて、協定には例示されていることが多い一方、公共基盤の中枢性 (criticality) の基準が関連協定中に明記されているわけではない⁴²。また、「中枢的な公共基盤 (critical public infrastructure)」は、そのほとんどが安全保障例外条項の中に位置づけられているとはいえ、例示されたインフラにみられるように、必ずしも軍事的な利益と関連するものばかりではなく、それ自体では「安全保障上の重大な利益 (essential security interests)」に正確な意味を与えることにはならない。むしろ、「中枢的な」や「基盤」といった曖昧な用語が用いられることで、解釈上の不明確さがさらに残る結果となりかねないとの指摘もある⁴³。

こうした「中枢的な公共基盤」規定の特徴は、日本が締結した経済関係協定の「中枢的な公共基盤」規定についても、最初期の日本・シンガポールEPAの場合を除き、他の3本の事例に当てはまる。すなわち、「中枢的な公共基盤」は、通信・電力・水道の各インフラを典型例として、公的私的施設を問わず、それ以外のインフラも含まれることを許容し、安全保障例外条項の一部として、何が「中枢的な公共基盤」に含まれる施設なのかについての決定も含めて、締約国の広範な裁量の下に置かれる規定とされているのである。

「中枢的な公共基盤」規定を含む経済関係協定は必ずしも多いとはいえないが、ASEAN構成国やインドが締約国となる場合には規定が置かれることもある。日本は、ASEAN構成国やインドとの間でEPAやBITをすでに数多く締結しており⁴⁴、新規に締結する機会はいま

条第1項(b)(iv)では、「通信、電力及び水道供給についての (for communication, power and water supply)」 「中枢的な公共基盤」とされており、通信・電力・水道インフラが例示規定とはされていない。また、ASEAN・インド CECFA 物品協定 (2009) 第13条(b)(iii)、ASEAN・中国 CECFA 投資協定 (2009) 第17条(b)(iii)、カンボジア・韓国 FTA (2021) 第9.2条第1項(b)(iii)には、「中枢的な公共基盤」の例を示す文言が含まれていない。しかし、これらの規定は締約国の裁量を広範に認める安全保障例外条項の一部であることからすると、「中枢的な公共基盤」の分野を厳格に限定するものと解する必要はないであろう。

⁴¹ AANZFTA (2009) 第15章第2条第1項(b)(iii)注3、マレーシア・オーストラリア FTA (2012) 第18.2条第1項(b)(iii)注39、PACER Plus (2017) 第11章第2条第1項(b)(iii)注4、インド・オーストラリア ECTA (2022) 第11.2条第1項(b)(v)参照。

⁴² いかなる施設や資産が国家の重大な利益にとって決定なのかという「中枢性」の基準について、そのインフラが公益にとってどれだけ重要であるかどうかだけでなく、そのインフラによる物品やサービスの供給が数時間でも中断するだけで人々の生命を危機に陥らせることになるように、そのような供給の継続がきわめて必要であることも基準となるという見解として、see, W.Zwartkruis, “Foreign Direct Investment and Security: What is Actually the Problem?” in Hillebrand Pohl *et al.*, (eds.), *supra* note 40, pp.34-35.

⁴³ Ch.Bian, “The Essential Security Interest Exception Clause in International Investment Agreements and Arbitration: From an Exception to a Norm?” in Y.Li, F.Lin & Ch.Bian (eds.), *National Security in International and Domestic Investment Law. Dynamics in China and Europe* (Routledge, 2024), p.33.

⁴⁴ 日本はASEAN構成国のすべてと個別に次のような経済関係協定を締結している。日本・ベトナム BIT (2003)、日本・マレーシア EPA (2005)、日本・フィリピン EPA (2006)、日本・タイ EPA (2007)、

ど多くはないであろうが、新たに締結する際に「中核的な公共基盤」規定をいれることになるのであれば、上記の特徴に留意する必要がある。もっとも、現実において、むしろより重要なのは、こうした「中核的な公共基盤」規定を国内で実施する際に、日本の国内法の関連規定がこの規定の特徴に適合的な内容を有していなければならないということであろう。例えば、RCEP協定上、「中核的な公共基盤」を防護する方策の1つとして、外国投資の「中核的な公共基盤」への制限を実施するのであれば、日本の関連国内法である外為法の制度がこれに対応できるような建付けとなっている必要があるはずである。日本の外為法は、果たしてこの要請に応えるような制度となっているのであろうか。

2. 外為法における「中核的な公共基盤」の位置づけ

(1) 「安全(security)」に関する対内直接投資規制の評価基準

a. 外為法における対内外国投資規制の制度的枠組み

RCEP協定などに規定されている「中核的な公共基盤」を防護するためにとられる措置には様々なものが想定されるが、その1つとして、こうした「中核的な公共基盤」に対する対内直接投資等の規制措置という手段が挙げられる。これを法的に規律しているのが主として外為法である。

外為法は、その第5章に位置する第26条から第30条にかけて、対内直接投資等を規律する規則を定めており、これを受けて、外為法の下位規範として対内直接投資等に関する政令（昭和55年政令第261号）（以下「直投令」という）、さらに対内直接投資に関する命令（昭和55年総理府・大蔵省・文部省・厚生省・農林水産省・通商産業省・運輸省・郵政省・労働省・建設省令第1号）（以下「直投命令」という）がその規律を詳細に定めるかたちとなっている。こうした法令による現行の制度では、1991年の外為法の改正により、対内直接投資等は原則として事後報告とするものとし、一部の業種についてだけ事前届出の対象とされている⁴⁵。

なかでも対内直接投資に対する審査については外為法第27条が定めている。この外為法第27条及び直投令第3条第2項によると、外国投資家が対内直接投資等を行う際に事前届出が必要とされるのは、その投資が、①国の安全を損ない、公の秩序の維持を妨げ、又は公衆の安全の保護に支障をきたすことになるおそれのあるもの、②我が国の経済の円滑な運営に著しい悪影響を及ぼすおそれのあるもの、③我が国との間に対内直接投資等に関する国際約束等がないことにより相互主義が確保されていない国の外国投資家が行うもの、④財務大臣の許

日本・カンボジア BIT(2007)、日本・ブルネイ EPA(2007)、日本・インドネシア EPA(2007)、日本・ラオス BIT(2008)、日本・ベトナム EPA(2008)、日本・ミャンマーBIT(2013)で、いずれにも「中核的な公共基盤」規定は含まれていない。

⁴⁵ 貞嘉徳・高田翔行『経済安全保障×投資規制・貿易管理 外為法 Q&A』（中央経済社、2023年）18頁。

可を要する資本取引に係るもののいずれかに該当する場合である⁴⁶。このうち、①と②については、直投命令第3条第3項に従い、財務大臣と事業所管大臣が告示（指定業種告示）を通じて特定の業種を指定し、この指定業種に係る対内直接投資等については原則として事前届出を必要とするものとされた⁴⁷。特に外為法第27条第3号第1号イには、「国の安全」、「公の秩序」及び「公衆の安全」という3つの概念が明記され、これらがそれぞれどのような機能を有するかについては、下位規範に当たる直投令第3条第2項第1号イや直投命令第3条第3項第3項によりさらに詳しく規定されるという構造となっているのである。

2002年には、直投命令第3条第3項に基づき、対内直接投資等に関する命令第三条第三項の規定に基づき財務大臣及び事業所管大臣が定める業種を定める件（平成26年3月6日内閣府、総務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省告示第1号）が公表され、そこでは、別表第一及び別表第二などにおいて、事前届出や事後報告の対象となる業種とその理由についての対応関係が記された。

それによれば、別表第一に規定される業種では事前届出の対象となる業種が列挙され、主に「国の安全」に係る業種が挙げられている。この業種には、当初は、武器、航空機、原子力、人工衛星及びロケットやその活動に関連する物・ソフトウェアの製造業や、軍事転用の蓋然性が高い汎用品の製造業及びそれらの設計・製造の技術を保有するソフトウェア業などが含まれていたが、2017年には、各原材料物資の金属鋼業が別表第二から別表第一に写され、原子力発電所を保有するものに限る電気等の業種が新規に追加されるなど、その内容は随時更新されている。また、別表第二には、事前届出ではなく事後報告のみが求められる対象業種が挙げられている。そのうち、「公の秩序」に係る業種として、電気・ガス、熱供給、通信、放送、水道、鉄道、旅客運送が、「公衆の安全」に係る業種として、生物学的製剤（ワ

⁴⁶ 対内直接投資等に関する政令第3条第2項は以下の通りである。なお、「法」とは外為法を表す。

2 法第二十七条第一項に規定する審査が必要となる対内直接投資等に該当するおそれがあるものとして政令で定めるものは、次の各号のいずれかに該当する対内直接投資等とする。

一 イ又はロのいずれかに該当する業種として主務省令で定める業種に係る対内直接投資等（カッコ内略）

イ 国の安全を損ない、公の秩序の維持を妨げ、又は公衆の安全の保護に支障を来すことになるおそれがある対内直接投資等に係る業種

ロ 我が国が経済協力開発機構の資本移動の自由化に関する規約第二条bの規定に基づき留保している対内直接投資等に係る業種

二 法第二十七条第三項第二号に掲げる対内直接投資等に該当するおそれがあるものとして主務省令で定める対内直接投資等

三 外国為替令（昭和五十五年政令第二百六十号）第十一条第一項の規定による財務大臣の指定に係る資本取引に当たるおそれがあるものとして主務省令で定める対内直接投資等

⁴⁷ さらに、そうした指定業種のうち、国の安全等の観点から慎重な取扱いが必要とされる業種がコア業種と呼ばれ、直投令第3条の2第2項第3号及び直投命令第3条の2第3項により、財務大臣と事業所管大臣により指定されている。指定業種の説明については、財務省『外為法・投資審査制度アニュアル・レポート 年次報告書（2023年度）』7頁参照、

https://www.mof.go.jp/policy/international_policy/gaitame_kawase/fdi/annual_report2023.pdf。

クチン）製造及び警備業がそれぞれ明記されている⁴⁸。さらに、別表第二には、安全保障の観点からサイバーセキュリティの重要性が増してきたことを理由として、「国の安全」に係る業種として、サイバーセキュリティ関連業（集積回路、記録メディア、通信機械器具、電子計算機製造、ソフトウェア、情報処理サービス、インターネット利用サービス業等）が2019年に追加された⁴⁹。

このように、外為法第27条の規定に基づく対内直接投資の規制に関する運用としては、「国の安全」、「公の秩序」及び「公衆の安全」を独立した3つの概念として整理され、それぞれに対応して関連業種が規制対象として割り当てられている。逆に言えば、この運用では、第27条の規定全体を貫く包括的な概念が存在するわけではなく、3つの概念それぞれについて個別にその内容が想定され、それに応じて適的な業種が検討されているということになる。したがって、以上のような制度の下で、RCEP協定等に規定された「中核的な公共基盤」に該当するインフラが、その何らかの意味での重要性を理由として、別表においてどのように位置づけられて規制が行われるべきなのかが検討されなければならないのである。

b. 国際規範における「安全保障」と「公の秩序」の区別とその国内的実施

このように、「国の安全」、「公の秩序」及び「公衆の安全」という概念に基づき規制対象や規制手段を区別する手法は、必ずしも外為法の関連規定に限られない。諸外国でも後述のようにこれらの概念の区別が導入されているが、国際レベルでの貿易・投資活動等の規律を対象とした経済関連協定でも、こうした区別に言及がなされる場合がある。近年のこうした協定には安全保障例外条項が挿入されることが多くなっていることはすでに指摘したが、GATTやBITにみられる安全保障例外と一般的例外の区別は、「安全保障」上の利益とそれ以外の利益との区別を前提していることに留意しなければならない。とりわけGATSにおける安全保障例外と一般的例外との区別とそこで規定されている内容は示唆的である。というのも、GATSは、その第14条の2において締約国が「自国の安全保障上の重大な利益(its essential security interests)のために必要であると認める」例外的な措置を許容する一方、第14条では一般的例外が規定され、そのなかで、GATT第20条と同様に「公衆の公德(public morals)」の保護が例外事由として挙げられるほか、さらに「公の秩序(public order)」が追加され、その維持に必要な措置を採用・実施することが認められている（GATS第20条(a)）からである⁵⁰。

⁴⁸ その他別表第二には、「我が国経済の円滑な運営」（外為法第27条第3項第1号ロ）に係る業種として、農林水産業・石油業・皮革・航空運送・海運といった業種が掲載されている。これは、後述するOECD資本移動化自由規約第2条で日本が留保した業種に該当する。OECD Code of Liberalisation of Capital Movements (OECD, 2011), p.97.

⁴⁹ 貞ほか・前掲注(45)61頁。

⁵⁰ GATS第20条(a)には「公の秩序」について注が付けられており、「公の秩序を理由とする例外は、社会のいずれかの基本的な利益に対し申請かつ重大な脅威がもたらされる場合に限り、適用する」となされている。

外為法第27条における「国の安全」、「公の秩序」及び「公衆の安全」の区別に直接影響を与えたのは、法的拘束力を有するOECD資本移動自由化規約である。日本は1964年にOECDに加盟したが、それにより、OECDが設立された1961年と同じ年にOECD理事会で採択されたこの規約上の法的義務に従うことが求められたからである。

OECD加盟国間の資本移動に関する制限を漸進的に撤廃することを目的としたこの規約には、一般的約束（第1条）や自由化措置とそれに対する留保（第2条）、公の秩序と安全保障を理由とした措置（第3条）、免除条項（第7条）などの実体規定や、加盟国による通告・情報提供（第11条）、第2条bの規定に基づく留保の通告（第12条）などの手続規定、貿易外取引委員会の任務（第18条・第19条）といった付託事項規定のほか、自由化措置の対象となり得る全てのクロスボーダー取引を定めた資本移動自由化リスト（附属書A）と、同規約の締約国であるOECD加盟国がOECDに通告している自由化措置の留保項目が国別に羅列されている資本移動自由化規約留保項目（附属書B）などの附属書が含まれている。この規約のスキームによると、OECD加盟国は、実効的な経済協力のために必要な限度まで、資本移動に関する制限を互いに漸進的に撤廃するという一般的約束を負い、それにもかかわらず対内直接投資の規制を実施するためには、自由化措置に対して第2条bに基づく留保を付すか、第3条の公の秩序や安全保障を理由とした規制を行うかのいずれかを選ばなければならない⁵¹。

そのなかでも第3条は次のような規定である。

「第3条 公の秩序と安全保障

この規約の規定は、加盟国が、次のいずれかのことのために必要と認める措置を執ることを妨げるものではない。

- (i) 公の秩序を維持し、又は公衆の衛生、道徳及び安全を保護すること。
- (ii) 当該加盟国の安全保障のために実質的な利益を保護すること。
- (iii) 国際の平和及び安全に関する当該加盟国の義務を履行すること。」⁵²

すなわち、第3条(i)がGATTやGATS、BIT、EPAなどで規定される一般的例外に該当する事由であるのに対して、同条(ii)は、他の経済関係協定においては安全保障例外に該当する

⁵¹ なお、同規約第3条のコメンタリーによれば、国家安全保障上の懸念から規制を導入する際には、第3条の適用により同規約の規律の外でその規制を維持するよりも、第2条に基づき留保を付すことが奨励されてきたという。OECD, *OECD Codes of Liberalisation of Capital Movements and Current Invisi-ble Operations: User's Guide* (OECD, 2003), p.34.

⁵² 第3条の規定の英文は以下の通りである。

“Article 3 Public order and security

The provisions of this Code shall not prevent a Member from taking action which it considers necessary for:

- (i) the maintenance of public order or the protection of public health, morals and safety;
- (ii) the protection of its essential security interests;
- (iii) the fulfilment of its obligations relating to international peace and security.”

事由であるということが言えるであろう。なお、同条(iii)は、主として国連の集団安全保障上の措置である非軍事的な強制措置の実施が念頭にあると考えられる。

日本は、こうした国際規範の枠内で、外為法に基づき、国の政策上重要と考えられる一定の業種の国内企業への外国投資家による投資等に関して審査付きの事前届出制を導入している⁵³。OECD資本移動自由化規約第3条柱書に「必要と認める」とあるように、いかなる業種が同条(i)～(iii)に定める外資規制を実施し得る事由に該当するかどうかを判断するのはOECD加盟国自身である。このいわゆる「自己判断的な」性格を有する規定に基づき、日本もまた同条に該当する行動かどうかを裁量的に判断できることになる。ただし、実際には、OECDにおいていかなる業種が特に(i)と(ii)のいずれかに関連するののかについて「一定の相場観」が形成されているという。こうした「相場観」に導かれるかのように、日本政府がこれまで第3条(ii)に基づき安全保障を理由に説明してきた航空運送・海運・通信・放送の各業種について、OECD国際投資・多国籍企業委員会はこれを安全保障上の自由ではなく第2条bに基づく自由化への留保を行うようにという勧告がなされた。そしてこれを受けて日本政府は、1992年2月に、すでに第2条bに基づき留保していた農林水産業・鉱業・石油業・皮革／皮革製品製造業に加えて、航空輸送業・海運業・投資信託業を留保業種に追加することになったという⁵⁴。

こうした経緯の結果、外為法に基づく対内直接投資の規制に係る業種の分類としては、OECD資本移動自由化規約第3条(i)の中で「公の秩序」に係る業種としては、電力・ガス、熱供給、通信事業、放送事業、水道・鉄道・旅客運送が、また「公衆の安全」に係る業種としては、生物学的製剤製造業、警備業が該当する一方、同条(ii)の「国の安全」に係る業種としては、武器、航空機、原子力、宇宙関連、軍事転用可能な汎用品の製造業、サイバーセキュリティ関連、感染症に対する医薬品に係る製造業、高度管理医療機器に係る製造業が該当するものとされている⁵⁵。

このように見ていくと、対内直接投資の規制との関係で「中枢的な基盤」に係る業種が通信・電力・水道などを含むことを想定するならば、外為法第27条による規制ではこれらが「公の秩序」に係る業種に該当するということになる。これは、「中枢的な通信基盤」を一般的例外に位置づけた日本・シンガポールEPAはこれと整合的にとらえられるとしても、「中枢的な基盤」規定を有するそれ以外の協定では「中枢的な基盤」規定が安全保障例外として位置づけられていることからすると、国際義務の国内的实施という観点からこれらの協定と国内法制との間では齟齬が生じているのではないかという疑念が生じることになる。

(2) 「中枢的な基盤」と「国の安全」及び「公の秩序」との関係

⁵³ 中崎隆編著『詳説 外為法・貿易関係法』（中央経済社、2021年）123頁。

⁵⁴ 以上について、中谷・前掲注(28)47頁。

⁵⁵ 今村英章・桜田雄紀編著『詳解外為法 対内直接投資等・特定取得編』（商事法務、2021年）9頁。

a. 外資規制の国内法制における「中枢的な基盤」の位置づけ

以上みてきたように、日本では、外為法に基づく対内直接投資の規制に係る業種の観点から「中枢的な基盤」を捉えた場合、同法第27条の建付けからすると、「国の安全」よりも「公の秩序」に関連する業種に含まれるものがほとんどということになる。もっとも、OECD資本移動自由化規約第3条(i)及び同条(ii)にいう「公の秩序」と「国の安全」の区別に従ってある業種がいずれのカテゴリーに該当するかについては、必ずしも固定的に考えられているわけではない⁵⁶。例えば電力事業は一般に「公の秩序」に関わるが、電力の中でも原子力発電事業については「国の安全」に関わるというように、当該業種のどの側面に焦点を当てるかにより相対的な判断結果となるようにも思われる。

他方で、当然のことながら、諸外国においても「中枢的な基盤」についてはこれに対する外国投資を規律する関連法制の中で一定の位置づけが試みられている。参考のためにここで主要国の状況を概観しておこう。

米国は、2007年7月に外国投資及び安全保障法(FINSA)を制定し、その中で、2001年の同時多発テロ事件直後に制定された愛国者法の文言をそのまま「中枢的な基盤」の定義として採用した。それによれば、「物的であるか否かにかかわらず、米国にとって重要なシステムや資産であって、そのシステムの不能や破壊が安全保障の弱体化をもたらすもの」とされている⁵⁷。さらに、外資による米国内への投資を審査する対米外国投資委員会(CFIUS)の権限を強化することを目的として2018年に制定された外国投資リスク審査現代化法(FIRRMA)では、「中枢的な技術(critical technology)」、「機微な個人情報であるデータ(sensitive personal data)」と並び、「中枢的な基盤」がTID米国事業(TID U.S. Business)に含められて引き続きCFIUSの審査対象となった。この「中枢的な基盤」には、インターネット・プロトコル・ネットワーク、情報通信、海底ケーブル、電気エネルギーの発電・送電・配電・貯蔵のためのシステム、石油・ガス州際パイプライン、水道、衛星システム、鉄道、金融市場など28種類

⁵⁶ OECD 資本移動自由化規約第3条にいう「公の秩序」と「国の安全」の区別についてはそれぞれの概念の明確化が必要であるが、「公の秩序」の定義について OECD 加盟国間では多様に解釈されていて一元的な概念で説明することが困難ではあるが、日本の国内法制では「公の秩序」を「国家及び社会の一般的利益」を意味するものと理解するのが一般的であるとされる一方、「国の安全」については、「国家安全保障上不可欠な利益」、すなわち安全保障上重要な技術の流出防止、国内の防衛生産・技術基盤の維持、国内の安全を損なう国内活動の防止の3つで構成されるという。藤田輔「OECD 投資委員会の活動—FOI プロジェクトに焦点を当てて—」外務省調査月報 2009 年度 3 号(2010 年) 16-17 頁参照。

⁵⁷ 50 U.S.C. App. §2170(a)(6) こうした基盤には、国土安全保障省の見解によると、農業及び食糧供給、水の供給、公衆衛生、緊急サービス供給、防衛基幹産業、電気通信産業、エネルギー産業、運輸業、金融業、化学産業、郵便及び配送業、そして情報技術産業という 12 の産業が該当するとされた。渡井理佳子『経済安全保障と対内直接投資—アメリカにおける規制の変遷と日本の動向—』(信山社, 2023 年) 56-57 頁。

のインフラが指定されたのである⁵⁸。現在では、これらをダム、エネルギー、金融、食糧・農業、情報技術、原子炉・核物質・核廃棄物、運輸システムなど16の部門にまとめて「中核的な基盤」に含めている⁵⁹。すなわち、米国の外資関連国内法制では、「中核的な基盤」を安全保障上の利益の観点から保護することが試みられているのである。

欧州ではEUが2019年に初めて外国直接投資を審査する規則を制定した⁶⁰。EU構成国は、この規則に基づき、透明性、無差別、機密性、及び法的救済と迂回防止という4つの原則に従って外国投資の審査を行うものとされたが、いかなるメカニズムにより審査を行うかについては構成国に委ねられている。また2019年EU規則第4条は、外国直接投資が安全保障や公の秩序に影響を与える可能性があるかどうかについて構成国当局並びに欧州委員会が検討する分野を5種類例示しており、その1つに「中核的な基盤(critical infrastructure)」が挙げられている。そして、この「中核的な基盤」には、エネルギー、運輸、水道、健康、通信、メディア、データ保護・保有、航空宇宙、防衛、選挙・財政インフラ、機微な施設、及びこれらインフラの利用に不可欠な土地や不動産が含まれるとされている⁶¹。

こうしたEU規則の制定を受けて、EU構成国の多くがそれに関連して国内法整備が行われている。フランスでは、「中核的な基盤」に関連する規則に限っていえば、外資規制の対象となる活動が、金融財政法典(*le code monétaire et financier*)第R.151-3条に従って、①性質上対内直接投資規制の対象となる活動(武器・弾薬、軍事目的の爆発物、戦争物資など)、②一定の指標に基づき重大性を示す基準を満たして対内直接投資規制の対象となる活動(エネルギー、水道、輸送ネットワーク、電気通信、公衆衛生、農産物など)、③調査・開発活動に関連して対内直接投資規制の対象となる活動(中核的な技術や軍民両用の物品・技術など)に分類されている。このうち本稿で扱う「中核的な基盤」に該当する活動の多くは②の活動になるが、そこでは、他のカテゴリーと同様に、国家防衛の利益、「公の秩序」及び「公の安全」を害するおそれのある活動とされており、①～③が保護される利益により分類されて

⁵⁸ 31 C.F.R. § 800.212. F.Jalinous & T.Sensenig, “Keeping up with CFIUS: A Practitioner’s Reports on National Security Trends in the United States”, *Erasmus L.R.*, 2022, nr.4, p.271. 龍野滋幹・水本啓太「グローバル情勢における安全保障上の懸念を踏まえた、外資による投資・買収規制の最新動向 [第1回] 米国(上)」*Business & Law* (公開日 2023年2月15日), <https://businessandlaw.jp/articles/a20230215-1/>.

⁵⁹ America’s Cyber Defense Agency, “Critical Infrastructure Sectors”, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

⁶⁰ Regulation 2019/452.

⁶¹ 「中核的な基盤」以外の4種類は、人工知能、半導体、サイバーセキュリティなど「中核的な技術及び適切な利用品目(critical technologies and due use items)」, エネルギーや原材料、食糧安全保障などの「中核的な入力の供給(supply of critical inputs)」, 個人データやそうしたデータをコントロールする能力などの「機微情報へのアクセス(access to sensitive information)」, 及び「メディアの自由と多様性(the freedom and pluralism of the media)」である。Y.Li, “Europeanization of Foreign Direct Investment Screening: A Spotlight on the EU Regulation”, in Y.Li, F.Lin & Ch.Bian (eds.), *National Security in International and Domestic Investment Law. Dynamics in China and Europe* (Routledge, 2024), pp.82-88.

いるわけではない⁶²。すなわち、問題となる投資が「国の安全」を害するのか、それとも「公の秩序」を害するのかということは、当該活動に関する上記の分類で決定されるわけではなく、別の基準によるものと考えられる。しかし、重要なのは、「中枢的な基盤」に該当する業種・分野が安全保障上の観点から規制の対象となることが一定の場合に許容されていることである。

また、ドイツの場合、外国投資規制は外国貿易法(AWG)と外国貿易令(AWV)により規律されており、「中枢的な基盤」の決定においては、連邦情報セキュリティ庁法(BSIG)及び中枢的な基盤の認定に関する命令(BSI-KritisV)が決定的な役割を果たすとされる。そして、特定の業種については連邦経済・気候保護省(BMWK)に届出を行うことがAWVにより義務付けられているが、そのほとんどは「中枢的な基盤」に係る業種であるという。上記命令によると、「中枢的な基盤」には、エネルギー、水道、情報テクノロジー・電気通信、金融・保険、健康、運送並びに食糧の各分野が含まれる。なお、これらの分野で「公の秩序又は安全(öffentlichen Ordnung oder Sicherheit)」が害されるおそれがある際の考慮要素としては、投資により資産を取得する者が第三国の政府により直接又は間接に支配されているかどうかといったことが挙げられているが、ここでは「公の秩序」と「国の安全」を区別する基準が明確に定められているわけではないことに留意しなければならない⁶³。

最後に中国についても触れておきたい。中国は、2019年に、同国における初めての外国投資法に関する法典となる外国投資法を公布し、同法の効力はその実施規則とともに2020年1月に発生した。同法は国家安全保障審査(NSR)メカニズムを規定しており、その対象となる分野については、軍事関連分野と特定の主要分野とを区別している。後者の特定の主要分野の例として、重要な農産物、エネルギー・資源、重要なインフラ、情報テクノロジー、インターネットサービス、金融サービスなどが挙げられており、こうした国家安全保障に関連する重要な分野の定義については中国政府の裁量によるところとされている⁶⁴。したがって、中国における「中枢的な基盤」に該当する分野での外国投資に対しては、「国の安全」の観点から審査が行われる手続が準備されているのである⁶⁵。

⁶² Ch.Miles, “Foreign Investment Screening Mechanism in France”, in Li, Lin & Bian (eds.), *supra* note 61, pp.132-134.

⁶³ J.Hörnig, S.Kirwitzke & F.Schöning, “Foreign Direct Investment Screening in Germany”, in Li, Lin & Bian (eds.), *supra* note 61, pp.156-161.

⁶⁴ 中国の外国投資審査メカニズムは米国のCFIUSを参考に造られてきたが、中国の「国家安全保障」概念は米国の「国家安全保障」概念よりも相当広いという。Ch.Huang, “China’s Take on National Security and Its Implications for Evolution of International Economic Law”, *Legal Issues of Economic Integration*, Vol.48, no.2 (2021), p.130.

⁶⁵ NSRメカニズムに服する安全保障審査の範囲は、こうした外国投資が行われる業種が中国国内にある場合だけでなく、投資により取得された財産が外国投資家により「支配」されている場合も含まれるように拡大しているという。M.Ruhl, “The National Security Review in China’s New Foreign Investment Legal Regime”, in Li, Lin & Bian (eds.), *supra* note 61, p.116.

以上のように、主要な外国の外資規制国内法制においては、「中枢的な基盤」に該当する分野・業種が安全保障上の利益を保護する目的で規制の対象となる場合がほとんどであることが確認される。その背景には、国家の防衛に関わる安全保障概念が、科学技術の発展や国家・国民の保護法益の拡大から、単に軍事的側面に限定されるのではなく、その侵害が国民の安全・生活に深刻な被害を及ぼしかねない領域へと拡大していることが挙げられよう⁶⁶。こうした安全保障概念の拡大は、そこに含まれる具体的な分野について、保護法益の拡大に関する今後の展開に対応できるように柔軟かつ裁量をもって国家が判断するように要請することにつながっているのである⁶⁷。

b. 外為法における「中枢的な基盤」の位置づけとその課題

以上のような諸外国の外資規制に関する国内法制と日本の外為法の関連規定とを比較した場合、次の点を指摘しておく必要がある。すなわち、すでに確認したように、外為法第27条において「国の安全」、「公の秩序」及び「公衆の安全」の保護というそれぞれの観点からなされた業種の分類は、OECD資本移動自由化規約に定められた分類に比較的厳格に従ったものである一方、諸外国の国内法制では同規約の規定に沿った分類が必ずしも行われているわけではないということである⁶⁸。いずれにおいても「国の安全」（「安全保障」）や「公の秩序」といった抽象的な概念が用いられることにより、実質的には各国の行政庁に裁量的な判断権が与えられているという点では共通していることに留意しなければならないが⁶⁹、特に「中枢的な基盤」に関する外資規制について日本の外為法は、これを主として「公の秩序」の維持の枠組み内に位置づけており、この点において、米国や中国のように「安全保障」の観点

⁶⁶ とりわけ人工知能(AI)については、近年において軍民両用(dual-use)で利用される機会が増大してきたため、国家安全保障上の利益保護を目的に、当該AIへの外国投資を審査する方向に各国の政策が転換してきたという。その状況と影響について、see, OECD, *AI in Business and Finance. OECD Business and Finance Outlook 2021* (OECD, 2021), pp.149-161.

⁶⁷ 米国や中国は国内法で「安全保障」概念の定義を明らかにしていない一方、フランスやドイツは「安全保障」上の重大な利益を他の利益と国内法上区別はしつつ、その定義には広い裁量の余地が残されているが、いずれの場合においても、外国投資の審査システムにおいて「国家安全保障」概念が意図的に定義されず、実行上規制についてかなりの程度の自律性を維持しようとしている。すなわち「国家安全保障」概念は、審査対象となる取引の特徴に応じて、国内当局によりケース・バイ・ケースで解釈されるのである。Ch.Bian, “Foreign Direct Investment Screening and National Security: Reducing Regulatory Hurdles to Investors Through Induced Reciprocity”, *Journal of World Investment & Trade*, Vol.22 (2021), p.570.

⁶⁸ しかも、これら概念の分類において何らかの一般的な基準が明記されているわけではない。例えば「公の秩序」をどのようにとらえるかについて各国の実行が統一されているわけではないため、こうした国内の「公の秩序」概念の内容を国際規範のレベルに持ち込んでその内容を明確にすることは困難であり不適切であろう。W.W.Burke-White & A.von Staden, “Investment Protection in Extraordinary Times: The Interpretation and Application of Non-Precluded Measures Provisions in Bilateral Investment Treaties”, *Virginia Journal of International Law*, Vol.48 (2008), pp.357-361.

⁶⁹ 伊藤一頼「国有企業・政府系ファンドに対する諸国の外資規制—開放性と安全保障の両立をいかにして図るか—」*RIETI Discussion Paper Series 15-J-059* (2015年) 39頁。

を重視したり、フランスやドイツのように「安全保障」と「公の秩序」の双方に関連付けたりするような諸外国の関連国内法制とは異なる特徴を有しているということが言えよう。

それでは、「中枢的な基盤」に対する外国投資について、その規律の正当化自由を「国の安全」ではなく「公の秩序」の侵害のおそれにとどめておくことに不都合は生じないのであろうか。確かにこれまでは、例えば日本の電力会社である電源開発株式会社（以下「Jパワー」という）の株式を英国の投資ファンド(TCI)が20%取得しようとしたことが日本の「公の秩序」の維持を妨げるおそれがあるとして日本政府により中止命令が発せられた2008年のJパワー事件のように⁷⁰、電力事業を含む「中枢的な基盤」への外国投資の規律を「公の秩序」の維持の観点から国内法上正当化することはそれほど困難ではなかったかもしれない。しかし、国家により「安全保障」概念が広くとらえられるようになってきた現代においては、必ずしもそうとは限らなくなっているであろう。外国投資の規制においては、軍事戦略産業はもちろんのこと、軍事的側面が主たる側面とはいえないハイテク産業や天然資源開発産業などもまた、その「中枢的な基盤」を外国投資家が支配することにより、国家安全保障や安全保障上の重大な利益に対する脅威が生じ得るという認識が広まっているからである。

確かに、2000年代初頭くらいまでは、各国において「中枢的な基盤」に数えられていたものが国家安全保障と常に関係づけられていたわけではなく、むしろその内容としては「公の秩序」や「公衆の安全」との関連のほうが強かった⁷¹。しかし、米国や中国のように、現代において「中枢的な基盤」を外国投資との関連で国家安全保障上の利益と直接結びつける動きが出てきたのは、「中枢的な基盤」としての性格を有する産業において投資財産の所有権が外国人に移転することにより国民生活のみならず国家の存立に対して重大な影響が及ぼされるという国家安全保障観の展開があったからに他ならない。ここには、国家安全保障と外

⁷⁰ 古城誠「TCI ファンドによるJパワー株式の取得－外為法と外資規制」『法学教室』第337号

(2008年) 8-12頁参照。See also, K.Nakatani, “Restrictions on Foreign Investment in the Energy Sector for National Security Reasons: The Case of Japan”, in A.McHarg, B.Barton, A.Bradbrook & L.Godden (eds.), *Property and the Law in Energy and Natural Resources* (Oxford U.P., 2010), pp.311-325.

⁷¹ 例えば2010年頃までの「中枢的な基盤」の定義の例として、「経済及び福祉のために、公衆の安全のために、そして主要な政府の責任の実現のために不可欠な支援を提供するインフラ」(OECD, *Protection of ‘Critical Infrastructure’ and the Role of Investment Policies Relating to National Security*, 2008), 「物理的施設, サプライチェーン, 情報テクノロジー及びコミュニケーション・ネットワーク」(Australian Government, *Critical Infrastructure Resilience Strategy*, 2010), 「国の機能, 及び英国での日常生活が依存している不可欠なサービスの供給にとって必要な施設, システム, 用地及びネットワーク」(United Kingdom, Cabinet Office, *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, 2010), 「その機能の不全や低下が持続的供給の不足, 公共の安全の重大な崩壊, あるいはその他の劇的な結果をもたらすような, 国民社会と経済にとってきわめて重要な組織的物理的構造と施設」(Germany, Federal Ministry of the Interior, *National Strategy for Critical Infrastructure Protection*, 17.06.2009), 「重要な社会的機能, 人々の健康, 安全(safety), 保安(security), 経済的社会的安寧の維持にとり不可欠であり, その混乱や破壊がそうした機能を維持不能とする結果として構成国に重大な影響を及ぼすような, 構成国に所在する資産, 施設及びその一部」(EU, Council Directive 2008/114/EC)などが挙げられる。

国資本の関係が軍事的戦略的レベルで再解釈されるとともに、安全保障も経済的政治的社会的観点から問われ直さなければならないとする国家安全保障概念の動態的性格が色濃く反映されていると見ることもできるであろう⁷²。

現代の「中枢的な基盤」をめぐる外資規制に関しては、一方では、「中枢的な基盤」がその具体的内容として物理的インフラのみならず、情報・データを含む無形の資産、コミュニケーション・ネットワークの創設・維持も含めるように広く解釈され、他方で、そうした「中枢的な基盤」に及ぶリスクの形態次第では、それに対する外国投資の規律の根拠が「国の安全」と「公の秩序」の維持のいずれかに関連することになる。こうした状況の下で、既存の外為法第27条における対内直接投資の規制枠組みは十分かどうかということが、現在問われているのである。すなわち、「国の安全」、「公の秩序」、そして「公衆の安全」を独立した3つの概念として整理してそれぞれについて対応する業種を規制対象として定め、「中枢的な基盤」については、これに関連する業種やそれに対するリスク形態別に「国の安全」か「公の秩序」か、それとも「公衆の安全」なのかを分類し逐次見直していくという従来の方法が、こうした「国家安全保障」概念の展開に対して十分に対応できるかが課題となっている。これら3つの類型を相互に独立したものとみるだけでなく、場合によっては重なり合うこと可能性も検討されなければならないのである⁷³。

IV おわりに

本稿では、RCEP協定の安全保障例外条項に定められているような「中枢的な（公共）基盤」に関する規定が、外資規制の文脈において、日本の外為法によりどのように実施されるのかについて検討を進めた。その結論として、RCEP協定にみられるような「中枢的な（公共）基盤」の位置づけと日本の外為法におけるその位置づけとの間にはギャップが存在するということである。

すなわち、RCEP協定において「中枢的な公共基盤」は安全保障例外に位置づけられているのに対して、対内直接投資を規律する外為法第27条を中心としたスキームでは、OECD資本移動自由化規約第3条(i)の分類に従って「国の安全」、「公の秩序」及び「公衆の安全」という概念ごとに関連業種が結びつけられており、これらのうち、「中枢的な基盤」に該当する業種は「公の秩序」に含まれている。確かに「公の秩序」は、二国間投資協定において、一般的例外条項だけでなく、安全保障例外条項中にも、また両者のハイブリッドな形式の条項にも含まれるといわれるが⁷⁴、諸外国では「中枢的な基盤」に係る事業を「安全保障」上

⁷² C.Esplugues, *Foreign Investment, Strategic Assets and National Security* (Intersentia, 2018), pp.82-112.

⁷³ 本郷隆「外資規制法の構造分析—安全保障を理由とする投資規制の比較法的分析と事例研究—」東京大学法科大学院ローレビュー6号（2011年）162頁。

⁷⁴ L.Sabanogullari, *General Exception Clauses in International Investment Law. The Recalibration of Investment Agreements via WTO-Based Flexibilities* (Nomos, 2018), pp.260-261.

の利益の保護という観点から外国投資規制を実施したり、「安全保障」概念そのものを拡大させて「中核的な基盤」へのリスクをそこに含めたりする傾向があることを踏まえると、外為法において「中核的な公共基盤」を「公の秩序」のカテゴリーにとどめておくことが適当かあらためて確認する必要があるように思われる。「中核的な基盤」の保護のために経済関係協定上の義務に反する措置をとらざるを得ない場合に、「公の秩序」の維持がその協定の安全保障条項に含められていないのであれば、この例外条項を援用することは困難となるおそれがあるなど、「中核的な基盤」を過度に「公の秩序」と結びつけることで不都合が生じることがあるからである。

そうした齟齬を正す方策としては、「中核的な基盤」に係る業種を「公の秩序」から「国の安全」に移行するように外為法とその下位規範を改正することがあり得るであろう。しかし、そのような対応では、安全保障例外条項そのものを含まない経済関係協定が問題となる場合に一般的例外条項さえ援用できないという隘路に陥ることになりかねない⁷⁵。むしろ、「国の安全」と「公の秩序」の双方にかかわるように分類し直し、一定の考慮要素に基づきケース・バイ・ケースで「国の安全」に関わるのか、それとも「公の秩序」の問題にとどまるのかを判断する方が望ましいのではなかろうか⁷⁶。適当な場合には措置を行う国に比較的広い裁量が認められる安全保障例外が援用できるように、「中立的な基盤」を「国の安全」に係る業種とみなす実行を積み重ねていくことが重要であろう。その際には、そこで考慮される要素を明確化するとともに、できる限り対外的に公表して、外国投資家の投資意欲をそがないように手続の透明性を高める努力も併せて行う必要がある⁷⁷。

⁷⁵ 既存の経済関係協定の安全保障例外条項の中には、締約国に対して、サイバー安全保障上の脅威や「中核的な基盤」のような主要な部門からの脅威に対応するための行動を可能とするような柔軟性を提供していないものもあるとの指摘として、see, O.Hrynkiv, “Legal and Policy Responses to National Security Measures in International Economic Law”, *Georgetown Journal of International Law*, Vol.54 (2023), p.229.

⁷⁶ 例えば英国では、2022年国家安全保障・投資法に従い、一定の条件を満たした企業や資産の支配・取得について、国家安全保障への脅威が合理的に疑われる場合には内閣府の担当大臣が審査を開始することができるとされており、この国家安全保障への脅威は定義されていないものの、3つの判断要素、すなわち①ターゲットリスク（対象となる資産等が国家安全保障への脅威として利用されるおそれがあるかどうかなど）、②取得者リスク（取得者が、その業種や技術力、国家安全保障上の脅威となり得る国家や組織との関係性等から国家安全保障に脅威をもたらし得るかどうかなど）、③支配リスク（取得者が対象となる資産の支配をどの程度取得するかなど）を考慮して、審査を開始するかどうかをケース・バイ・ケースで判断するとされていることが参考になろう。National Security and Investment Act 2021: Statement for the purposes of section 3 - 2021 version (updated 21 May 2024), paras.16-32. See, A.Spano, “The National Security and Investment Act 2021: Assessing the UK’s New Approach to Investment Screening”, in Li, Lin & Bian (eds.), *supra* note 61, pp.246-247. 龍野滋幹・内藤央真・中林憲一「グローバル情勢における安全保障上の懸念を踏まえた、外資による投資・買収規制の最新動向〔第3回〕英国」*Business & Law*（更新日 2024/05/07），<https://businessandlaw.jp/articles/a20230509-1/>。

⁷⁷ 現行の外為法の運用においても、対内直接投資が事前届出の対象となるかどうかを判断する際に、考慮すべき要素として、「外為法に基づく対内直接投資等の事前届出について財務省及び事業所管省庁が審査に際して考慮する要素」が2017年に公表され、2020年に外為法改正にあわせて、12項目にわたる詳細な内容に変更されている。

「中枢的な基盤」の性格付けについて、こうした柔軟な捉え方を国内法制に持ち込むことは、経済安全保障推進法のように、外為法以外の他の国内法令において、「重要インフラ」や「基幹インフラ」というような「中枢的な基盤」に類似する概念が用いられる場合もあることから⁷⁸、国内における実施を目的としたその統一的な運用に向けて国内法制を整備しなければならないであろう。それとともに、「中枢的な基盤」を特に「国の安全」の枠内に位置づける可能性を認めたうえで、国家安全保障上の利益の保護が通商上の取引を阻害し、その結果として資本移動の自由や市場経済が損なわれることを念頭に置きつつ、国家による「国の安全」概念の裁量的な判断を維持しながら、外国投資の審査をめぐる基準の明確さや透明性を通じてその判断の恣意性を最小限に狭めて外国投資の設立を奨励するというバランスをとらなければならない。すなわち、国家安全保障上の利益の保護と投資の自由化という2つの価値が対立する中で、「中枢的な基盤」の規律においても、これら相対立する2つの利益を調和させるような政策的な決定が求められるのである⁷⁹。

(2025年1月17日脱稿。本稿中にあるウェブサイトは同日付ですべて確認済み)

https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/recent_revised/gaitame-hou_20200508.htm。「国の安全」に係る判断についても同様に一定の考慮事項が準備されることで、基準や手続の客観性・透明性が担保されることになるはずである。

⁷⁸ 経済安全保障推進法における「基幹インフラ」の問題については、蔦大輔・新井雄也「基幹インフラ審査制度ーサプライチェーン・サイバーセキュリティ」ジュリスト1601号(2024年)33-40頁参照。また、重要インフラ施設に係る取組において、安全保障に関係が深い措置として「能動的サイバー防御」の導入が検討されており、国内法令の整備が進んでいる。風木淳『経済安全保障と先端・重要技術 実践論』(信山社、2023年)51頁参照。

⁷⁹ Ch.Bian, *National Security Review of Foreign Investment. A Comparative Legal Analysis of China, the United States and the European Union* (Routledge, 2020), p.214.

第 4 章

EU構成国間の投資協定とエネルギー憲章条約

—Komstroy事件判決を中心に—

一橋大学大学院教授
中西 優美子

I 背景

本稿で中心的に取り上げるEU司法裁判所のKomstroy事件判決¹は、二つの文脈で捉えることでよりよく理解できると考える。すなわち、Komstroy事件は、エネルギー憲章条約という文脈とEU法の自律性という文脈の両方の文脈にかかわる。また、同時にそれら二つの文脈がISDS（Investor-State Dispute Settlement、投資家対国家の紛争解決）にかかわっている。一つは、環境との関係でエネルギー憲章条約をEUにおいてどのように取り扱うべきかという問題と、もう一つは、EUがISDSに代えて、紛争解決制度として投資裁判所の設立を目指していると事情である。このような中で、Komstroy事件は、EU司法裁判所が積極的に管轄権を自らに認め、進んで判断を示したとも捉えられる事件でもある。

1. 気候変動対処とエネルギー憲章条約

世界における大きな流れとして、気候変動問題への対処がある。国家や企業がその政策において方向転換を迫られている。エネルギー憲章条約（Energy Charter Treaty：ECT）は、1994年にポルトガルリスボンで調印されて1998年に発効した。ソ連の崩壊に伴い、1991年、旧ソ連、東欧を含む欧州諸国、アメリカ、カナダ、オーストラリア及び日本は、旧ソ連及び東欧諸国におけるエネルギー分野の市場原理に基づく改革の促進、並びに、エネルギー分野における企業活動（貿易及び投資）を全世界的に促進する宣言を行い、その内容を実施するための法的枠組みとして、同条約が作成された²。同条約は、エネルギーの原料・製品の貿易及び通貨の自由化並びにエネルギー分野の投資の保護等を定めている。日本は、2002年に同条約に加入している。調印時から約30年が経過し、同条約も環境問題への意識の高まり等の世界情勢の変化に直面している。また、環境NGOから、エネルギー憲章条約が時代遅れであるという指摘もあった。

このような中で、2017年11月、ECT締約者は、欧州委員会を中心とした近代化の議論を開始することに合意し、2020年7月にその交渉を開始した。15回の交渉を経て、2022年6月24日に近代化案に合意がなされ、その骨子が公表された。もっとも、EUでは近代化案に合意がなされず、ストップすることになった³。近代化を求めていたEU自体が脱退を決定したが、その後、2024年12月3日、最終的に近代化案に合意がなされ、条文が確定した⁴。

また、紛争の内容につき、再生可能エネルギーに関係するものが増えてきており、加えて、EU構成国で生じるものが増えてきていた。ECTには個人対国家の紛争解決方法、ISDS条項

¹ Case C-741/19 *République de Moldavie v Komstroy LLC*, Judgment of 2 September 2021, ECLI:EU:C:2021:655.

² エネルギー憲章条約の概要については、外務省の Web サイトを参照。

<https://www.mofa.go.jp/mofaj/gaiko/energy/charter.html>（最終閲覧日：2025年5月28日）

³ <https://www.energychartertreaty.org/modernisation-of-the-treaty/>（最終閲覧日：2025年5月28日）

⁴ Decision of the Energy Charter Conference, CCDEC202414, 3 December 2014, Entry into Force and Provisional Application of Amendments to the Energy Charter Treaty and Changes and Modifications to its Annexes.

が規定されており、国家のエネルギー政策の変更のために投資家より訴えられるというケースが増えてきた。国家にとっては、エネルギー憲章条約に入っていることで、そこからのメリットよりもリスクを背負う可能性が高くなってきた。2022年11月22日、条約署名及び締約当事者数は、一時は50を超えていた⁵。現在は、脱退する国が増えている。条約当事者として、EU、Euratom及び全EU構成国が加入していたが、2014年に、イタリアは脱退の意思を通知した。また、フランス、ドイツ及びポーランドが2022年に脱退の通知を行った。さらに、EUとEuratom自身も脱退することを決定した⁶。加えて、他のEU構成国もこれらに続くことになる。

Komstroy事件は、2019年10月8日にEU司法裁判所に付託が受理され、2021年9月2日に判決が下された。このような変動期に下されたKomstroy事件は、事件そのものを見るだけではなく、流れの中で捉えると理解が深まる。

2. EU法の自律性とEU構成国間の投資協定

Komstroy事件にかかわる、もう一つの文脈がEU構成国間の投資協定をめぐるEU法の自律性の問題である。まず、Komstroy事件判決にとって大きな意味を持っているのがAchmea事件⁷と言われる事件である。同事件はドイツから先決付託がなされ、EU司法裁判所が2018年3月6日に先決裁定を下した。Achmea事件では、構成国間の投資協定とEU法の両立性が問題となり、大きな関心呼んだ。1991年にEUに加盟する前のチェコスロバキアがオランダと投資保護協定を締結した。この協定の8条は、外国投資家と締約国の間で紛争が生じた場合には仲裁裁判所に服するというISDS仲裁条項を含んでいた。現在、スロバキアは、EUの構成国であるが、問題となる投資協定が結ばれたときは、まだチェコとスロバキアはチェコスロバキアという一つの国で、かつ、EUの構成国ではなかった。EU加盟後、スロバキアが保険制度改革を行い、民間疾病保険サービス市場を開放した。そのことを受けて、オランダの保険会社のAchmeaが、スロバキアに子会社を設立し、サービスを開始した。しかし、その後、スロバキアは、この保険市場の自由化の一部を変更したことで、民間疾病保険業務から生じた利益配分が禁じられる措置の採択に至った。Achmeaは、この措置を受けて、当時のチェコスロバキアとオランダの投資協定の8条には、ISDS条項があり、それに基づいて仲裁手続に訴えた。ドイツのフランクフルトにある仲裁裁判所は、中間判決でAchmea方の主張を認めて、スロバキアに損害賠償の支払いを命じた。スロバキアは、自国がEU構成国になったことで、仲裁裁判所が、管轄権を有さないのではないかという点を争った。スロバキアは、

⁵ エネルギー憲章条約の Web サイトで条約締約者を確認することができる。

⁶ Council Decision (EU) 2014/1638 of 30 May 2014 on the withdrawal of the Union from the Energy Charter Treaty.

⁷ Case C-284/16 Slowakische Republik v Achmea BV, Judgment of 6 March 2018, ECLI:EU:C:2018:158; 中西優美子「EU 構成国間の投資協定と EU 法の自律性」自治研究 95 巻 1 号 (2019 年) 98-110 頁。

ドイツ上級裁判所に仲裁判断の破棄を求めたが、破棄され、その後、ドイツ連邦通常裁判所に上訴した。ドイツ連邦通常裁判所は、国内では最終審の裁判所になるため、EU運営条約267条に基づいて、先決付託をEU司法裁判所にしなければならないことから、先決裁定をEU司法裁判所に求めた。EU司法裁判所は、以下のように判示した。まず、たとえ仲裁裁判所が投資協定の違反に関してのみ判断することを求められるとしても、当該投資協定8条に従い、関連する当事国で効力のある法及び締約国間の関連する協定を考慮に入れなければならないという事実は残るという指摘をした。EU司法裁判所は、仲裁裁判所がEU法、とりわけ開業の自由及び資本の自由を含む基本的自由に関する規定を解釈することになり、実際に適用することを求められる可能性があるというような判断をした。しかし、その仲裁裁判所は、これまでの判例法からEU運営条約267条の意味における構成国の裁判所には当たらないことから、仲裁裁判所が先決裁定を求めないということは、EU司法裁判所の解釈がなされることなく、仲裁裁判所がEU法の解釈をすることになるということが認定された。仲裁裁判所を含む投資協定を締結することで、EU構成国は、紛争がEU法の解釈、または、適用に関係する場合に、EU法の十分な実効性を確保することを妨げるISDS制度を設定したものと捉えられると認定し、EUではなくて、構成国によって締結された協定に基づく仲裁裁判所が、EU法を解釈する可能性が存在するとした。当該投資協定8条が、構成国間相互信頼の原則のみならず、先決裁定により確保されているEU基本条約により設定されている法の特質の維持に疑問を投げかけることになり、誠実協力原則に合致しないというように判決して、最終的に問題となっている投資協定の8条は、EU法の自律性に悪影響を有すると結論付けた。これによって、構成国間での仲裁裁判所を含む投資協定 (intra-EU bilateral investment treaties) は、EU法に違反するということが明確化された。

このAchmea事件判決後、まず2019年1月15日にAchmea事件判決の法的結果及びEUにおける投資保護に関する構成国政府代表の宣言⁸が出された。この前文では以下のようなことが書かれている。

EU法は構成国間で締結された二国間投資協定に優立する。その結果、同二国間協定に含まれるすべてのISDS仲裁条項は、EU法に違反し、適用不可能である。ISDS条項を基礎として設立された仲裁裁判所は、管轄権を有さない。エネルギー憲章条約を含むEUによって締結された国際協定は、EU法秩序の一部であり、EU基本条約と合致しなければならない。

仲裁裁判所は、エネルギー憲章条約を構成国間に適用可能なISDS条項を含むものとして解釈してきた。そのように解釈されると、EU基本条約と合致せず、不適用とならなければ

⁸ Declaration of the Representatives of the Governments of the Member States of 15 January 2019 on the legal consequences of the Judgment of the Court of Justice in Achmea and on investment protection in the European Union.

ならないだろう。

ここでは、不適用とならなければならないだろう (would have to be disapplied) とされ、断定形にはなっていない。これは、宣言であり、別にEU司法裁判所の判決ではないため、このような形で文言が用いられたと考えられる。

この前文の後にくる宣言の中で、ECTについて構成国は、欧州委員会とともに遅滞なく、ECTのEU構成国、EU内での適用に関して、Achmea事件判決からの結果に対処するのに追加的な措置が必要か否かを議論すると述べられた。そのため、この段階ではECTのISDS条項がEU法に違反するかどうかは、まだ不明な状況であった。

この宣言の後、2019年10月24日に、構成国は、構成国間の2国間の投資条約 (Bilateral investment treaties, BITs) の終了のための協定に同意した。2020年5月3日に正式に構成国間のBITsの終了のための協定、終了協定 (Termination Agreement)⁹と言われるものに署名がされた。EUは27か国でその全加盟国が署名しているのではない。もっとも署名している国は、ベルギー、ブルガリア、クロアチア、キプロス、チェコ、デンマーク、エストニア、フランス、ドイツ、ギリシャ、ハンガリー、イタリア、ラトビア、リトアニア、ルクセンブルク、マルタ、オランダ、ポーランド、ポルトガル、ルーマニア、スロバキア、スロベニア、スペインの23か国である。他方、スウェーデン、フィンランド、アイルランド、オーストリアの4か国は署名していない。そして2020年8月29日にこの協定が発効した。

同終了協定の前文にECTへの言及がある。そこでは、同終了協定は、EU構成国二国間の投資協定 (intra-EU bilateral investment treaties) を対象としており、ECT26条に基づくEU間の訴訟手続 (intra-EU proceedings) を対象としていないと述べている。ECT26条は、ISDS条項を定めている。すなわち、この終了協定では、ECTのISDS条項が対象とはなっていないということが明らかにされた。したがって、ECTのISDS条項がEU法に違反するかどうかは不明なままであった。

加えて、同終了協定の前文には、EUと構成国は、後にこの事項を取り扱うと述べられていた。このことは、この点が不明であり、EU側も構成国側もそれを認識していたことが、この条約の前文から分かる。この頃、ECTの近代化のための交渉がなされていた。交渉がうまくいかないことで、EUの中には、もうECTから脱退すべきという声もあった。そのような中でKomstroy事件判決が出された。

なお、上述したAchmea事件判決後、動きがあった。ドイツの連邦通常裁判所がEU司法裁判所のAchmea事件判決(先決裁定)を受け、仲裁判決は無効であるという判決を下した¹⁰。その後、その判決に不服であるとして、申立人はドイツ連邦憲法裁判所に憲法異議を提訴した。

⁹ Agreement for the termination of Bilateral Investment Treaties between the Member States of the European Union, OJ of the EU 2020 L169/1.

¹⁰ BGH (I.Zivilsenat), Beschluss vom 31.10.2018, I ZB2/15.

最終的に、憲法裁判所は、仲裁判決が無効であると判断されたことは憲法違反ではないと判示した¹¹。

II Komstroy事件 (Case C-741/19, 2021年9月2日EU司法裁判所の先決裁定)

1. 事実概要

1999年に、電気の発電の会社、配電の会社、その供給を受ける会社間で、電気に関する一連の契約が締結された。それらの契約により、Ukrenergo発電会社（以下、「U会社」という。）というウクライナの発電会社が、電気を配電会社であるウクライナのEnergoalian会社（以下、「E会社」という。）に電気を販売し、販売された電気がさらにBritish Virgin Islandsに登録されているDerimen会社（以下、「D会社」という。）に再販売され、その電気がモルドバの公営企業であるMoldtranselectro会社（以下、「M会社」という。）に売られた。電気の供給は、U会社からM会社になされた。契約に従い、D会社は、E会社に代金支払いを滞りなく行った。しかし、電気の供給を受けたM会社は、金額の一部のみをD会社に支払い、残りは債務不履行という状況になった。そこでD会社は、自分の債権をE会社に譲渡した。E会社がM会社を相手に訴えを起し、債務履行を求めた。E会社は、このM会社を相手取りモルドバの裁判所、それからウクライナの裁判所に提訴したりしたが、埒があかないという状況に陥った。そこで、E会社は、モルドバの行動がECTの重大な違反であると考え、ECT26条4項(b)に定められるアドホック仲裁手続を開始した。2013年10月25日に、この紛争を解決するために、パリで設置されたアドホック仲裁裁判所は、この紛争に関し管轄権があるとしたうえで、モルドバが国際的な取決めに遵守しなかったと考え、ECTに基づきE会社に代金を支払うようにモルドバに命じる仲裁判決を下した。2013年11月25日、モルドバは、民事手続法典1520条に従い、強制的な公共政策規定、すなわち、仲裁裁判所の管轄権規定の違反であるとして、同仲裁判決取消しを求めて、パリ上訴裁判所に訴訟を提起した。2016年4月12日の判決により、パリ上訴裁判所は、仲裁裁判所が管轄権を有するとしたのは誤りであったとして、同仲裁判決を取り消した。事実、同裁判所によると、E会社とモルドバ間の紛争は、電気販売の事項のみにかかわり、ECTの意味における「投資」にはかかわらないとした。その後、訴訟が長期化したこともあり、Komstroy会社（以下、「K会社」という。）がE会社の権利を継承した。K会社は、パリ上級裁判所の判決に不服であり、フランスの最終審の裁判所である破棄院(cour de cassation)に上告した。そこで、破棄院は、2018年3月28日に、パリの上訴裁判所の判決を破棄して差し戻すという判決を下した。差し戻されたパリの上訴裁判所が2019年9月24日にEU司法裁判所に先決裁定を求めるということを決定し、付託した。その先決付託を受けて、2021年9月2日にEU司法裁判所が先決裁定を下した。これが本先決裁定である。

¹¹ BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 23. Juli 2024, 2 BvR 557/19; 中西優美子「EU構成国間の投資協定に関する Achmea 先決裁定とドイツ連邦憲法裁判所」自治研究 101 巻 6 号 2025 年 104-115 頁。

2. 判決

本件の争点は、大きく分けて二つに分かれる。一つ目は、そもそもEU司法裁判所が管轄権を有するのか否かという点である。K会社は、ウクライナの会社であり、モルドバはEUの構成国ではないため、ISDSの当事者である投資家も国家も、EUとは関係しないという点で、果たしてEU司法裁判所が管轄権を有するかという問題である。二つ目は、もともと、仲裁裁判所の判決が取り消された理由は、仲裁裁判所が管轄権を持たないこと、すなわち電気契約というのは、投資に当たらない、ということ、から始まっているため、ECTにおける「投資」の概念が問題になった。

(1) EU 司法裁判所の管轄権

それでは、EU司法裁判所がどのように自らの管轄権を理由付けたか。一つ目は、本判決は先決裁定であるため、EU運営条約267条がかかわってくる。同条はEU条約及びEU運営条約の解釈と、それからEUの機関が採択したEU法行為の有効性と解釈について管轄権を有すると定めている。まず、問題は、ECTがEU機関の法行為に当たるか否かである。EU司法裁判所は、EUが締結する国際条約のEUにおける批准は、EU機関の行為、理事会決定(decision)による承認という形で行われるため、国際協定はEU法の一部であるとする判例¹²に従い、EU司法裁判所はそのような国際協定を解釈する管轄権を有するとした¹³。ECTについてもEUが加入する際に、理事会決定によりECTを承認しているため、ECTもEU機関の理事会の行為に当たると解釈された。今回のECTは、日本も加盟しているように、多数国間条約になっている。さらに、EUのみではなくてEUの構成国も締結しており、混合協定の形になっている。たとえ混合協定だとしても、EUの管轄権を否定するものではないと司法裁判所は判示した¹⁴。

加えて、本件では「投資」が問題となった。EU司法裁判所は、直接投資についてはEUが排他的権限をEU運営条約207条で付与されているため、EUは外国直接投資に対して排他的権限を持つことと、直接投資でないものは、共有権限であることを確認した¹⁵。そのうえで、裁判所は、EU法の対象とならない文脈で国際協定が適用される場合は、国際協定を解釈する管轄権は持たないという原則を確認した¹⁶。さらに、特に、非EU構成国の投資家と、非

¹² Case 181/73 R. & V. Haegeman v Belgian State, Judgment of 30 April, ECLI:EU:C:1974:41, paras. 2-4; Case C-321/97 Ulla-Brith Andersson and Susanne Wåkerås-Andersson v Svenska staten (Swedish State), Judgment of 15 June 1999, ECLI:EU:C:1999:307, para. 26; Case C-83/17 KP v LO, Judgment of 7 June 2018, ECLI:EU:C:2018:408, para. 24.

¹³ 本判決理由 23 段。

¹⁴ 本判決理由 24 段。

¹⁵ 本判決理由 25 段。

¹⁶ 本判決理由 28 段。

EU構成国間の紛争の場合は、そのようなケースに当たるとした¹⁷。しかし、EU司法裁判所は、このような原則は確認したものの、本件においては、この原則を適用せず、自己の裁判管轄権を肯定した。EU司法裁判所は、これにつき二つの理由を挙げた。一つは、国際協定の規定がEU法の範囲に入る状況、及び、EU法の対象とならない状況の場合の両方に適用される場合、解釈における将来生じるかもしれない相違を避けるために、適用される状況が何であれ規定が統一的に解釈されるべきことはEUの利益であるとした¹⁸。つまり本件は、非EU構成国の投資家と非EU構成国間の紛争であり、EUは関係してこないが、将来発生し得る状況にEU法がかかわるかもしれないので、そういった場合にEU法の統一的解釈が必要となるから、本件において当該事項につき解釈をすることがEUの利益となるという理由である。

もう一つの理由は、原訴訟（パリの上訴裁判所）における紛争の当事者が、ECT26条4項(b)に従って、UNCITRALの仲裁ルールを基礎に設定される仲裁裁判所をパリに設定したという点に、裁判所は注目すべきだとした。

EU司法裁判所は、仲裁裁判所が管轄権を欠いたために、フランスの裁判所は、フランスの民事訴訟法1520条の下で、フランスでなされた仲裁判決を破棄する訴訟を付託される場合、管轄権を有することを確認した¹⁹。EU構成国の領域に仲裁の場所を設定したことは、必然的にEU法の適用を伴うことになり、その事件を付託される裁判所は、EU条約19条に従って、EU法の遵守を確保するように要請される²⁰。

このようにEU法の統一適用の利益と、仲裁裁判所が設定されたのがパリだったという二つの点からEU司法裁判所は、先決付託問題に回答する管轄権を有すると判断した。

(2) 本案

a. EU法の自律性

本案の問題は、「投資」の概念であるが、その投資の概念に行くまでのところ、この前提問題というところが実は重要な問題となった。EU司法裁判所は、ある当事国と別の当事国の投資家の紛争がECT26条²¹に従って、仲裁裁判所に提訴ができるか否かを明確にしなけれ

¹⁷ 本判決理由 28 段。

¹⁸ 本判決理由 29 段。

¹⁹ 本判決理由 33 段。

²⁰ 本判決理由 34 段。

²¹ エネルギー憲章条約 26 条（投資家と締約国との間の紛争の解決）「(1)締約国の地域における他の締約国の投資家の投資財産に関する当該締約国と当該他の締約国の投資家との間の紛争であって、第三部の規定に基づく当該締約国の義務の違反であると申し立てられるものについては、可能な限り、友好的に解決する。

(2)(1)に規定する紛争がいずれか一方の紛争当事者が友好的な解決を要請した日から三箇月以内に(1)の規定に従って解決されない場合には、紛争当事者である投資家は、当該紛争を解決するために次のいずれの手続を選択することができる。

(a)紛争当事者である締約国の裁判所又は行政裁判所に当該紛争を付託すること。

(b)あらかじめ合意した適用可能な紛争解決手続に従って当該紛争を付託すること。

(c)(3)から(8)までの規定に従って当該紛争を付託すること。

ばならないとした²²。また、ECT26条2項(c)に基づく紛争が第三国の事業者(operator)と別の第三国間の紛争にかかわるという事実は先決付託に回答するEU司法裁判所の管轄権を排除するものではないが、ECT26条があるEU構成国の事業者と別のEU構成国間の紛争にも適用されると推定されえないとした²³。EU司法裁判所は、これまでの判例法を以下のように確認した²⁴。国際協定は、EU基本条約に定められる権限配分、EU法制度の自律性に影響を与えることはできない。その原則は、とりわけEU運営条約344条に規定されており、それによると、構成国はEU基本条約の解釈または適用に関する紛争を条約に規定されている以外の紛争解決制度に訴えることができない。

EU司法裁判所は、以下のようにEU法の自律性にフォーカスしていく²⁵。このような確立された判例法によると、構成国法及び国際法に対するEU法の自律性は、EUとEU法の本質的な特徴、とりわけEUの憲法上の構造及びEU法のまさに本質により正当化されるとする。また、EU法は、EU法が独立した法源、EU基本条約から生来しているという事実、EU法の国内法に対する優位並びに構成国の国民及び構成国に適用可能な一連のEU法規定の直接効果によって特徴付けられる。これらの特徴は、EU及び構成国を相互に拘束する、構造化された諸原則、ルール及び相互に依存する法的関係のネットワークに昇華してきた。

従って自律性は、EUがそれに唯一である憲法枠組みを所有しているという事実から生じる。この枠組みは、とりわけEU基本条約の規定（特に権限付与や権限配分に関するルール、EU機関及び司法制度がどのように働くべきかを規律するルール、EU条約1条2項に定められる統合過程の実施に寄与するような形に構造化された、特定の分野における基本的なルール）

...

(4)投資家は、(2)(c)の規定に基づく解決のために紛争を付託することを選択した場合には、当該紛争を次のいずれかに付託することについて書面により同意を与える。

(a)(i) 投資家が属する締約国及び紛争当事者である締約国の双方が、1965年3月18日にワシントンで署名のために開放された国家と他の国家の国民との間の投資紛争の解決に関する条約（以下「ICSID条約」という。）の締約国である場合には、ICSID条約に基づいて設立された投資紛争解決国際センター

(ii)投資家の属する締約国及び紛争当事者である締約国のいずれか一方のみがICSID条約の締約国である場合には、ICSID条約に基づいて設立された投資紛争解決国際センター（この場合には、投資紛争解決国際センターの事務局が手続を実施するための追加的な制度を規律する規則（以下、「追加的制度規則」という。）に従って付託される。）

(b) 国際連合国際商取引法委員会（以下、「UNCITRAL」という。）の仲裁規則に基づいて設置される単独の仲裁人又は仲裁裁判所

(c)ストックホルム商工会議所の仲裁機関の仲裁手続

...

(6) (4)の規定に基づいて設置される裁判所は、この条約並びに国際法の適用可能な規則及び原則に従って紛争の争点について決定を行う。

...」

²² 本判決理由 40 段。

²³ 本判決理由 41 段。

²⁴ 本判決理由 42 段。

²⁵ 本判決理由 43-44 段。

を対象とする。

このようにEU法の自律性を強調したうえで、EU司法裁判所と国内裁判所の役割、先決裁定手続の役割に言及した²⁶。EUの特質及び法秩序の自律性が維持されるように、EU基本条約はEU法の一貫性及び統一性を確保することを意図した司法制度を設定した。EU条約19条に従って、EU法の十分な適用が構成国で確保されるように、また、個人の権利の効果的な司法的救済を確保するのは、国内裁判所とEU司法裁判所である。その際、EU司法裁判所は、EU法の決定的な解釈を与えるのに排他的権限を有する。このため、EU運営条約267条に定められている先決裁定手続制度が存在する。EU司法裁判所と構成国裁判所間の対話を設定することによって、司法制度の要である、先決裁定手続はEU法の統一的解釈を確保する目的を持ち、それによって、EU法の一貫性、その実効性、自律性、ひいてはEU基本条約により設定される法の特質を確保している。

EU司法裁判所は、これらを前提として、構成国と他の構成国の投資家間の紛争がECT26条2項(c)の下での仲裁に服しうるか否かという問題が審査されなければならないとした²⁷。

b. ECT26 条の下での仲裁裁判所

まず、EU司法裁判所は、ECT26条6項に言及されるような仲裁裁判所がEUの司法制度に入るか否かを審査した²⁸。EU司法裁判所は、ECT26条6項に言及される仲裁裁判所は、EU法を解釈し、適用することを要請されたとした。それゆえ、そのような仲裁裁判所がEUの司法制度、とりわけEU運営条約267条の意味における裁判所とみなされるか否かが確認されなければならないとした。この確認は、EU司法制度に入る構成国により設立された裁判所であれば、同裁判所の判決は、EU法のルール of の十分な実効性を確保できるメカニズムに服することになるためである。

EU司法裁判所は、Achmea事件判決で問題となった二国間投資協定に定められる仲裁裁判所がEU構成国の国内裁判所の司法制度の構成要素とならないのと同じように、ECT26条6項に言及される仲裁裁判所ともならないとした²⁹。仲裁裁判所の特徴から、EU運営条約267条の構成国の裁判所という裁判所とはみなされない。従って、仲裁裁判所は、先決裁定を求める権利もないし、求める義務もなく、逆に、そのような仲裁裁判所がEU法を解釈する可能性があることを指摘した³⁰。

EU司法裁判所は、EU法の十分な実効性が保障されなくなるため、国際的な事項におけるEUの権限の行使は、国際協定において、構成国の投資家と他の構成国間の紛争がEU法の司

²⁶ 本判決理由 46 段。

²⁷ 本判決理由 47 段。

²⁸ 本判決理由 50-51 段。

²⁹ 本判決理由 52 段。

³⁰ 本判決理由 52-53 段。

法制度から取り除かれるような国際協定に及ぼすことはできないとした³¹。つまり、EU構成国の投資家と他の構成国間の紛争が、仲裁裁判所に付託されることになったら、EU司法裁判所の管轄権は及ばないことになってしまうため、そういった可能性のある国際協定をEUは結ぶことができないとした。そのうえで、国際協定は一般的に多角的な性質を持つにもかかわらず、ECT26条のような規定は、当事者間の二者間の関係を規律しており、それは二国間の投資協定の規定と類似すると認定した³²。結論として、EU司法裁判所は、ECT26条2項(c)は、EU構成国と他のEU構成国の投資家の紛争に適用できないと解釈されなければならないとした³³。

EU司法裁判所は、Achmea事件では、構成国二国間の投資協定はEU法に違反すると判示したが、Komstroy事件では、たとえ多数間協定であっても、EU構成国とEU構成国の投資家間の条文が入っている場合は、EU法違反になると解釈されなければならないという判示をした。本当は本案の問題は投資であるが、この投資については、ECT1条6項の投資の概念が問題となって、二つの条件が満たされてなければならないとした³⁴。一つは、投資家によって直接または間接に所有または管理されている財産であること。もう一つは、同規定の(a)から(f)までに列挙されている業種の一つを含んでいるということとした。EU司法裁判所はこの条文を解釈し、結果的に、電気供給契約は、ECT1条6項の投資には当たらないと判示した³⁵。

Ⅲ 判決の評価・影響

Komstroy判決（先決裁定）の仲裁プラクティスに与える影響は多大であり、この判決によりECT26条に定められるISDS条項がEU法違反とみなされ、EU構成国の投資家と別のEU構成国間の紛争では適用できなくなった。本件で最初に疑問がわくのは、なぜEU司法裁判所は本件で自己の管轄権を認めたのかという点である。なお、本判決に先立ち、本件の法務官 Szpunarは、EU司法裁判所の管轄権がないとも解されるという可能性を示しながらも、EU司法裁判所の管轄権を認めたうえで、投資には当たらないと結論付けた³⁶。本件の原訴訟では、権利を譲り受けた投資家Komstroyとモルドバ間の紛争、すなわち、EU構成国ではないECT加盟国と構成国と別のECT加盟国の投資家間の紛争であり、EU構成国にもEU構成国の投資家にも直接関係していない。唯一のEUとの接点は、KomstroyがECT26条の下での仲裁手続に訴

³¹ 本判決理由 61 段。

³² 本判決理由 64 段。

³³ 本判決理由 66 段。

³⁴ 本判決理由 69 段。

³⁵ 本判決理由 84 段。

³⁶ Case C-741/19 *République de Moldavie v Komstroy LLC*, Opinion of Advocate General Szpunar delivered on 3 March 2021, ECLI:EU:C:2021:164.

え、その際にEU構成国フランスのパリの仲裁裁判所を用いたということである。もし、Komstroyがパリの仲裁裁判所でなく、非EU構成国の仲裁裁判所に訴えを起こしていたら、そもそもこの事件は起こらなかった。加えて、EU司法裁判所は、パリの通常裁判所からは単に投資の概念をどのように解釈するかということのみが聞かれており、全くEU構成国ではないECT加盟国と他のECT加盟国の投資家間の紛争(ISDS)にかかわる事項がEU法違反になるか否かということは、同通常裁判所の先決付託の質問の中に入っていなかった。これらにもかかわらず、本件に対する裁判管轄権を認め、さらに先決裁定の判決理由の中でECT26条に関する箇所にも多くの段落が割かれた。

訴訟参加した者について、当然先決裁定であるため、原訴訟の当事者（モルドバとKomstroy）は参加したが、その他にEU構成国のフランス、ドイツ、スペイン、イタリア、ハンガリー、オランダ、ポーランド、フィンランド、スウェーデン、EU機関のEU理事会と欧州委員会が参加した。

EUとEuratomは、1994年12月17日にECTに調印し、1998年4月16日にEUにおいて効力を発生した。ECTは、EUが締結した国際条約であり、条約の批准が理事会決定というEU機関の行為とみなされるため、EU運営条約267条1項定められる先決裁定³⁷の対象となりうる。EUがECTに加入してから20年余り経っているが、本件までECT規定の解釈がEU司法裁判所に求められることはなかった。これは、偶然ではなくて、ECTの下での投資家対国家間紛争は仲裁廷に求められ、構成国の裁判所に提訴されることがまれであったためとされる³⁸。先決裁定手続では、EU司法裁判所は、架空の事例には回答できず、常に国内裁判所に事件が係属していることが必要となる。上述したように、Achmea事件ではEU構成国間の投資協定に規定されるISDS条項がEU法違反とされ、その後、構成国による宣言が出されたが、その中で、多数国間協定であるECTに規定されるISDS条項がEU法違反であるとは断定されなかった。また、上述した構成国間の終了協定では投資協定の終了はあくまでも二国間の投資協定の終了であり、多国間協定であるECTは対象としていないとされた。それゆえ、本件に至るまで、ECTのISDS条項がEU法違反であるか否かは不明のままであった。そのようななかで、EU司法裁判所がECT26条6項におけるISDS条項が、EU法違反であるか否かを判断する機会を得た。そして、本件において、EU司法裁判所は、ECTのISDS条項がEU法に違反するということを明確にした。すなわち、最初に紹介したAchmea事件は、構成国間、2国間でのISDS条項を含む投資協定がEU法違反であるとしたが、その際の理由付けが、今回の多数国間条約であるECTも拡大されて、EU構成国間の紛争(intra EU dispute)には、今後、ECT26条を用いること

³⁷ 先決裁定手続では、EU条約及びEU運営条約の解釈並びにEU機関の行為の効力及び解釈につきEU司法裁判所に質問をすることができる。

³⁸ Bianca Böhme, “The future of the Energy Charter after *Moldova v. Komstroy*”, *Common Market Law Review*, vo. 59, 2022, p. 853.

はEU法違反になるとされた。

この判決後、どのようになったか。本先決裁定により、EU法の下ではECTのISDS条項はEU法違反とされた。しかし、このことは、ECTのISDS条項が国際法違反ということは意味しない。確かにEU構成国では、もはや仲裁裁判所を設立することは難しくなる。しかし、仲裁廷をEU構成国以外の場所に設定すれば、EU法秩序の外にあり、EU司法裁判所の判決の効果が及ばない³⁹。それゆえ、EU構成国以外の場所が仲裁廷として選択されることになる。ドイツのエネルギー会社、RWEやUniperは、オランダの法律、地球温暖化対策のための法律の改正で石炭事業が廃止に追い込まれて損害を受けた。そこで、オランダの法律が改正されたことに対して、補償を求めるという状況がある。この紛争は、EU構成国とEU構成国の投資家間の紛争となり、この場合、オランダは仲裁決定の無効を求めなければならない、欧州委員会は*amicus curiae*を通じて本判決を防衛するだろうという見解が示された⁴⁰。

EUでは、本先決裁定後、本先決裁定の法的効果を明確化するために、Komstroy事件判決の法的結果とEU間の仲裁(Intra-EU Arbitration)の基礎としてのECT26条の不適用に関する共通の了解についての宣言がEU構成国とEUにより2024年6月26日に公表された⁴¹。そこでは、以下のようなことが宣言されている。共通了解として、ECT26条がEU域内の仲裁手続の根拠として適用されることはなく、また適用されるべきでもなかったこと。EU法の国内法に対する優位から、ECT26条は、EU域内の仲裁手続の基礎として適用できず、適用できなかったこと。EU域内の仲裁手続の法的基礎がない結果、脱退に関するECT47条3項は、拡大できず、また、拡大できなかったということ。ECT26条は、EU域内仲裁手続の基礎として適用されず、この点に関してECT47条3項はEU域内関係において法的効果を生み出さないこと。この宣言により、ECTのISDS条項はEU法違反であり、投資家はそれを援用できないことが明らかにされた。また、この宣言の前文では、第三国での仲裁決定が執行手続の対象となっており、仲裁廷がその管轄権を否定せず、仲裁機関が新たな仲裁手続を登録し、許容されない(inadmissible)と却下しないことは遺憾であると述べられている。本先決裁定やこの宣言の法的効果はあくまでもEU法秩序においてであり、国際法の観点からは必ずしも貫徹されるものになっていない。

ECTは、旧ソ連国家への投資を保護するために採択されたが、現在、ECTは石油燃料産業が気候変動対処のためにとられた法律の実施を遅らせたり、妨げたりする手段になっている

³⁹ Böhme, note (35), p. 868.

⁴⁰ Cf. ClientEarth, “The Future of Arbitration under the Energy Charter Treaty”, December 2021, p. 7 and p. 14; Böhme, note (35), p. 868.

⁴¹ Declaration on the legal consequences of the Judgment of the Court of Justice in *Komstroy* and common understanding on the non-applicability of Article 26 of the Energy Charter Treaty as a basis for intra-EU arbitration proceedings.

という指摘がある⁴²。本先決裁定は、ISDS条項がEU法の統一的な解釈を損なうリスクという狭い事項ではなく、環境保護の観点から語られるECTの近代化交渉という文脈からも捉えることが重要である。結局、EUは、2024年6月27日に脱退の意思を通知し、2025年6月28日に正式に脱退となった。

⁴² Christina Eckes and Laurens Ankersmit, “Komstroy: the beginning of the end for the Energy Charter Treaty?”, *European Law Blog*, 4 October 2021.

第 5 章

クラウドサービスと競争法

名古屋大学大学院教授
林 秀 弥

I はじめに

2023年、最も著名なM&A案件の1つは、マイクロソフトによるアクティビジョン・ブリザードの買収案件¹であろう。当該承認のために当事会社は各国の競争当局に届出を行った。欧州委員会(EU)、国家市場監督管理総局(中国)、日本公正取引委員会(日本)など、ほとんどの競争当局が早期に承認したのとは対照的に、競争市場庁(英国)および連邦取引委員会(米国)は、2020年代にも繁栄が続くと推定されるクラウドゲーム市場²における競争への合併の影響について懸念を示している。クラウドゲーミングは、ダウンロードやインストールを必要とせず、クラウドゲーミングサーバーから自分のデバイスにゲームを「ストリーミング」する機能をプレイヤーに提供する。これは、クラウド・コンピューティングの概念と関連技術の賜物である。

クラウド・コンピューティングは、インターネット経済におけるほとんどのデジタルサービスの競争基盤を築いている。ゲーム会社を含む企業に、必要なインフラ、プラットフォーム、ソフトウェアへのアクセスを“サービスとして”提供する。米国国立標準技術研究所の定義によると、次のようになる。

「クラウド・コンピューティングとは、設定可能なコンピューティング・リソース(ネットワーク、サーバー、ストレージ、アプリケーション、サービスなど)の共有プールへの、ユビキタスで便利なオンデマンド・ネットワークアクセスを可能にするモデルであり、最小限の管理労力やサービスプロバイダーとのやり取りで、迅速にプロビジョニングとリリースを行うことができる。」³

クラウド・コンピューティングとは、簡単に言えば、インターネット上でコンピューティング・リソースをサービスとしてオンデマンドで提供するサービスのことである。従来、企業は自社でコンピューティング・リソースを手配、整備、管理する必要があった。しかし、

※本稿は、日本エネルギー法研究所の2019～2020年度エネルギー安全保障に関する国際問題検討班の研究報告書として提出するものであるが、本稿執筆時点(2024年12月)の最新の状況を織り込んで執筆しているため、前提となっている情報や課題設定は2019年～2020年のものではない。

¹ マイクロソフトは2023年10月13日にアクティビジョン・ブリザードの買収を完了した。

<https://www.sec.gov/ix?doc=/Archives/edgar/data/0000789019/000119312523255762/d537928d8k.htm> (最終閲覧日: 2025年1月13日)(以下同じ)。しかし、米国では、第九巡回区裁判所が2023年7月にFTCの上訴中の差し止め命令を求める申し立てを却下したにもかかわらず、FTCの行政訴訟は行政法判事の下で係争中である。USFTC, Order Returning Matter to Adjudication, In the Matter of Microsoft Corp. and Activision Blizzard, Inc., Docket No. 9412 (Sep. 26, 2023).

² CMA, Anticipated acquisition by Microsoft of Activision Blizzard, Inc., Final report (Apr. 26, 2023), paras 8.1-8.442; USFTC, Administrative Complaint, In the Matter of Microsoft Corp. and Activision Blizzard, Inc., Docket No. 9412 (Dec. 8, 2022), paras 96-119.

³ Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing Recommendations of National Institute of Standards and Technology, NIST Special Publication 800-145 (Sept. 2011), p 2.

クラウド・コンピューティングの台頭により、ランニングコストの低さ、柔軟性、高度なITソリューションへのアクセスのしやすさなどを考慮し、自社でオンプレミスのサーバーを配置し、そこでソフトウェアを稼働させるよりも、サードパーティのクラウドサービスプロバイダー（以下「CSP」という）が提供するクラウドサービスを採用する傾向が強まっている。このように、CSPはデジタル分野において重要な役割を担っており、CSPがどのように競争を強化し、あるいは歪める可能性があるかは、より注目されるべきものである。以下では、基本的に、上記クラウド・コンピューティングのことを指して、単に「クラウドサービス」という。

実際、クラウドサービスは、高い市場集中や支配的なクラウドプロバイダーが採用する物議を醸す慣行など、競争上の懸念があるとして、最近、世界中の競争当局によって標的とされている⁴。しかし、クラウドサービスをめぐる競争は、ケースバイケースで関連市場の観点から評価されるだけでなく、エコシステムの観点からも評価されるべきであり、エコシステムには複数の種類のクラウドサービスや非クラウドサービスも含まれる可能性があることに留意すべきである⁵。実際、CSPの中には、顧客がCSPのソフトウェア製品やサービスを以前から利用していたことにより、現在の市場ポジションを獲得した企業もある⁶。さらに、以下の段落で言及されているすべての市場調査で示されているように、クラウドサービス市場における現在の高い市場集中が構造的要因に起因するものであるかどうか、競争法の介入の必要性、比例性及び有効性を判断する上で重要な問題である。

II 電力事業におけるクラウドサービスの重要性

2016年に、一般家庭も含めて電気事業が全面自由化され、顧客自らが小売電気事業者を選べるようになり競争が激化した。いわゆる旧一般電気事業者のなかには多くの顧客を失うも

⁴ 最近の例では、2024年9月、公正取引委員会が、クラウドシステムとサービス管理ソフトウェアで世界的に知られるCSPである「VMware」（アメリカの大手半導体メーカー「ブロードコム」の日本法人で、東京に拠点を置くソフトウェア会社）の東京オフィスに対し、抱き合わせ販売と優越的地位の濫用の疑いで立ち入り検査を行ったことが報道された。NHKの報道を参照、NHK「ブロードコム 日本法人に立ち入り 一方的に契約変更か 公取委」（2024年9月25日）、<https://www3.nhk.or.jp/news/html/20240925/k10014591481000.html>。このような反競争的行為は、クラウド展開におけるベンダーロックイン効果（次項で説明）の結果であると考えられる。また、株式会社MCデータプラスに対する排除措置命令（公取委命令令和6年12月24日・令和6年(措)第20号）もあわせて参照。本件は、クラウド関連の取引で行政処分を行った、初めての事案である、公取委は「データ囲い込み行為について違反になることを示した前例のない事案だ。引き続きデジタル分野での妨害行為に対し、厳正かつ的確に対処する」と記者会見で表明している。
<https://www3.nhk.or.jp/news/html/20241224/k10014677781000.html>

⁵ Gary Biglaiser, Jacques Crémer and Andrea Mantovani, The Economics of Cloud, TSE Working Paper, n. 24-1520 (Mar. 2024), p 12.

⁶ Jigsaw Research, Cloud Services Market Investigation Qualitative Customer Research Final Report (May 2024), para 7.3.1., https://assets.publishing.service.gov.uk/media/664f02634f29e1d07fadc56/Cloud_Services_Market_Investigation_Qualitative_Customer_Research_Final_Report_.pdf.

のもあった。ところが、22年ごろからいわゆるウクライナ戦争等に起因して世界的に燃料費が高騰し、電気の市場価格も高騰した。このため、今度は逆に、最終的な電気の供給保障を担う旧一般電気事業者の契約に戻る顧客が多くなった。このような市場の変遷は、特別高圧・高圧電力の供給を受ける法人顧客のニーズにも変化があった。以前は安価な電気こそが最大の価値であったが、近時は、少し価格が高くてもボラティリティーの小さい電気を好む顧客であったり、逆にボラティリティーは大きくても市場価格に合わせて価格水準が変わる料金メニューを選びたいなど、新しいニーズが生まれてきている状況にある。また、カーボンニュートラルも大きなトレンドである。電気以外の化石燃料系エネルギーを電化したい、環境価値が証書化されたエネルギーを活用したいといったニーズも高まっている。

このような様々なニーズの高まりに応じて、旧一般電気事業者のなかには、市場連動型メニュー⁷を導入して顧客のニーズにきめ細かく応えられるよう工夫しているところも表われてきている⁸。このように、電力小売業務に必要な機能をワンストップで提供したり、使用量や料金計算のデータを自動でチェックしたり、あるいは制度変更や業界潮流に伴う機能拡張を提供したりできるクラウド型電力システムは、省エネ・節電や、新電力業界の発展を支援するなどの目的で近時使用が広がっている。このように、電力事業の将来⁹においては、クラウドサービスの存在を抜きには考えられないことは明らかである。

デジタル分野におけるクラウドサービスの重要性に鑑み、本章ではクラウドサービスに関連する競争問題に重点を置く。まず、クラウドサービスの経済的特徴を概観し、クラウドサービス市場における高い市場集中の理由を説得力を持って説明する。第二に、クラウドサービスに関連する最近の市場研究をレビューし、競争当局間のコンセンサスを探る。第三に、市場調査において広範かつ徹底的に分析されてきたクラウドサービス市場における伝統的競争法の適用の可能性を分析する代わりに、クラウドサービス市場を事前規制や分野別規制によって規制する傾向を理解するために、最近のEUの法律に焦点を当て、そのような規制の導入後に生じると予想される潜在的な問題を指摘している。最後に、VIでは、主な調査結果のまとめと展望を述べて、本章を締めくくる。

Ⅲ クラウドサービスの経済的特徴：経済的視点

一般的に、クラウドサービスはサービスモデルによって、IaaS (Infrastructure as a Service),

⁷ 市場連動型メニューとは、スポット市場価格の変動に連動する料金プランのことである。スポット市場価格として参照する価格は、顧客の電気の使用場所が属する供給区域を基に卸電力所が公表した値が用いられている。

⁸ 例えば、東京電力の取組みとして、以下を参照。東洋経済オンライン「社長対談『東京電力がクラウド導入』実施の狙い」(2024年8月28日)、<https://toyokeizai.net/articles/-/789677>。

⁹ 電力事業に限った話ではなく、ガス事業やその他のエネルギー事業においても同じ事がいえよう。クラウドを活用した集中監視による自動検針、残ガス量管理、消し忘れ通報や使用量の見える化など、さまざまな局面で、ガス供給サービスにおいてクラウドの利用が想定されている。

PaaS(Platform as a Service), SaaS(Software as a Service)の3つに分類される。その名前が示すように、これらは異なるサービスモデルを表している¹⁰。

そもそもIaaSサービスモデルでは、CSPはインターネットを通じて、ワークロードを処理しデータを保存するためのコンピューティング・リソースを顧客に提供する。これらのコンピューティング・リソースは「インフラストラクチャー」と呼ばれ、CSPが所有・管理するサーバーやネットワーク機器の形で提供される。顧客は、これらの基盤となるクラウド・インフラストラクチャーを管理・制御することはないが、自らデプロイ(deploy)¹¹したオペレーティング・システム、データベース、アプリケーションを制御することができる。

次に、PaaSサービスモデルでは、CSPは、顧客がアプリケーションを開発、テスト、デプロイ、および実行できるように、「プラットフォーム」と理解される仮想開発・デプロイ環境へのアクセスをインターネット経由で提供する。これには、アプリケーション開発用コンピューティング・プラットフォームや、顧客がそこで完全なアプリケーションを構築・管理するために使用できる、事前構築済みのアプリケーション・コンポーネントやツールが含まれる。このモデルでは、CSPは基盤となるクラウド・インフラストラクチャー、運用システム、ミドルウェア・プラットフォーム（アプリケーション開発ツール、データベース、データ分析など）の管理に責任を負う。一方、顧客（通常はアプリケーション開発者）は、インストールされたアプリケーションとその構成設定のみを管理する。

最後に、SaaSサービスモデルでは、CSPはCSPのサーバー上でホストされるクラウドアプリケーションへのアクセスを顧客に提供する。顧客は、クラウド・インフラ上で稼働するCSPのアプリケーション（ソフトウェア）をダウンロードやインストールすることなく利用できる。このモデルでは、顧客は基盤となるクラウド・インフラストラクチャー、ミドルウェア・プラットフォーム、個々のアプリケーションを制御・管理することはない。SaaSサービスの提供に関連する基盤となるクラウド・インフラストラクチャーとデプロイされたソフトウェアはすべてCSPによって管理される。SaaSサービスのよく知られた例としては、オンライン・コミュニケーション・サービス（GmailやMessengerなど）やオンライン生産性ソフトウェア（Microsoft Office 365など）がある。

CSPは顧客とのコミュニケーションにおいて、自社のサービスをこれら3つのタイプに分類するのが一般的であるが、各サービス間の正確な線引きは容易ではないことを認識することが重要である。これらの分類は、クラウドサービスの概念全体を理解する上では有用であ

¹⁰ サービスの詳細な定義と例については、Jigsaw Research・前掲注(6)2.2.7項を参照のこと。

¹¹ deploy とは、システムやソフトウェアを開発環境から本番環境に配置し、実際に使用できる状態にするプロセスのことをいう。

るが、確固とした区別というよりはスペクトルのようなものである¹²。つまり、競争法の観点からは、各サービスモデルはそれだけで関連市場を構成するとは限らない。各サービスには、オン・ザ・クラウドであるか否かを問わず、他の有効な代替品が存在する可能性があり、また、それらは相互に代替し合う可能性さえある。これは、英国競争市場庁（CMA）の最近のワーキングペーパー¹³で分析されている問題である。競争法および競争政策の観点からクラウドサービス市場をよりよく理解するために、以下では、クラウドサービスの経済的特徴をいくつか挙げてみたい。

1. 規模の経済

CSPがどの種類のクラウドサービス（IaaS, PaaS, SaaS, またはそれらの混合）を提供したいかにかかわらず、CSPは事業活動を実現するためにサーバー、ネットワーク機器、その他のインフラを必要とする。SaaSやPaaSのCSPは、自社で構築したインフラの代替として、他のCSPのIaaSサービスを利用してサービスを提供することがある程度可能である。一方、IaaS型CSPは一般的に、自社でデータセンターを構築し、そこで独自のクラウド・コンピューティング・インフラを運用する必要がある。したがって、CSPの立場からすれば、クラウドサービスの提供にはインフラが不可欠であることは疑いの余地がない。

データセンターの建設と維持にかかるコストは高い。これには、用地買収のコスト、物理的なコンピューティング・リソースのコスト、オペレーションコスト、エネルギーコストなどが含まれる。クラウドサービス市場における規模の経済は、このように様々な方法で達成される。供給サイドの規模の経済については、CSPはエネルギーコスト、クラウド・インフラの稼働に必要な人件費、セキュリティ、信頼性、購買力の増大¹⁴における規模の経済の恩恵を受ける。また、コンピューティング、ストレージ、ネットワークのリソースを共有できる仮想化技術のおかげで、同じワークロードを処理するのに必要なサーバーの台数が少なくて済むという需要サイドの規模の経済も享受している¹⁵。

コンピュータリソースに関連する規模の経済とは別に、クラウドサービスのニーズが高まっていることから、CSPは既存のクラウドサービスを改善したり、新しいクラウドサービスを開発したりするために、研究開発（R&D）に大規模な投資を行っている。クラウドサービスが仮想化されカスタマイズ可能であることから、CSPが提供するクラウドサービスの範囲は、

¹² Alex Gaynor, Transcript of the FTC Panel Event on Cloud Computing : Taking Stock and Looking Ahead (May 11, 2023), p 3., https://www.ftc.gov/system/files/ftc_gov/pdf/cloud-computing-taking-stock-and-looking-ahead-may-11-2023.pdf.

¹³ CMA, Cloud services market investigation: Competitive landscape working paper (23 May, 2024), para 9.11. この見解の詳細な説明については, see id, paras 4.18-4.29.

¹⁴ Rolf Harms and Michael Yamartino, The Economics of Cloud, Microsoft White Paper (Nov. 2010), pp 3-4., <https://news.microsoft.com/download/archived/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf>.

¹⁵ Ibid, pp 4-8.

その競争力に大きな影響を与える。また、サービス範囲を拡大するために、企業買収を通じて多額の投資を行うCSPも存在することが確認されている¹⁶。このことは、研究開発への投資によって規模の経済が達成できることを示唆している。クラウドサービス分野でのアイデアやプロジェクトの開発には高い研究開発費がかかるが、いったん開発に成功すれば、限界費用は研究開発費に比べて相対的に低くなる¹⁷。さらに、新しく優れたサービスはより多くの顧客を惹きつけ、より多くの顧客を抱えるCSPほど、研究開発コストを分散し、規模の経済により魅力的な価格でサービスを提供することができる。

2. ネットワーク効果

一般的に、直接的なネットワーク効果は、同じCSPが提供する同じクラウド・インフラをより多くの企業が利用することによって生じる。間接的なネットワーク効果は、クラウド・インフラの大規模なユーザーベースが、CSPが物理的なインフラとソフトウェアをクラウド向けに最適化するインセンティブを与えることで生じる¹⁸。

前述したように、クラウド・インフラはあらゆる種類のクラウドサービスにとって不可欠な基盤である。したがって、企業がB2Bクラウドサービスを、最も多くのビジネスユーザーを抱える支配的なCSPのインフラ上で展開することを選好するのは理にかなっている。具体的には、このような選好は、いくつかの理由が絡み合って生じる可能性がある。第一に、B2Bサービスの役務提供市場（マーケットプレイス）の規模は、支配的なCSPのクラウドエコシステムにおいて最も大きい。第二に、例えば金融業界をターゲットとしたタイムクリティカルなサービスやデータ伝送サービスなど、自社のサービスが伝送速度に大きく依存している場合、その潜在的な顧客も支配的なCSPのサービスを利用している可能性が高いため、当該伝送に要する時間を最小限に抑えるために、支配的なCSPを開発プラットフォームとして選択する傾向がある可能性がある。第三に、様々なCSPのクラウドサービスが必ずしも相互運用可能であるとは限らないが、全てのCSPが同じCSPプラットフォーム上でクラウドサービスを開発している場合、理論的にはCSP間の相互運用性を実現しやすくなる。したがって、潜在的な顧客がクラウドサービスの購入を検討する際、サードパーティのソフトウェアベンダーが提供するサービスが、クラウドサービスの大半を購入しているCSPが提供するサービスと組み合わせれば、顧客にとって付加価値がある^{19 20}。

¹⁶ Autoriteit Consument & Markt (ACM), Market Study Cloud services, ACM/INT/440323 (Sep 5, 2022), p 47., <https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf>.

¹⁷ Id.

¹⁸ Biglaiser et al, supra note 5, pp 40-41.

¹⁹ ACM, supra note 16, pp 47-48.

²⁰ 公正取引委員会（公取委）が公表した報告書では、間接的なネットワーク効果は、さらに導入支援事業者への影響とサードパーティソフトウェアベンダーへの影響の2種類に分類されている。公取委「クラウドサービス分野の取引実態に関する報告書（デジタルプラットフォーム事業者の取引慣行等

3. 大手CSPの垂直統合

アマゾン、マイクロソフト、グーグルといった大手CSPは、さまざまなクラウドサービス(IaaS, PaaS, SaaS)を統合したパッケージを提供している。例えば、アマゾンはクラウドサービス、すなわちアマゾン・ウェブ・サービス(AWS)をIaaSサービスとして開始し、徐々にPaaSやSaaSサービスへとサービスを拡大してきた。対照的に、マイクロソフトは、オンライン生産性ソフトウェアなどのSaaSサービスで長らく市場で確固たる地位を築いてきたが、その後、PaaSサービスやIaaSサービスへとサービスを拡大してきた。

通常、顧客がさまざまな種類のクラウドサービスを統合する必要がある場合、次の2つの選択肢がある。①すべてのサービスを相互運用可能にして、これらのクラウドサービスが連携して接続できるようにする方法と、②単一のCSP²¹が提供するサービスとして利用する方法である。しかし、後者の場合、すべてのCSPが提供するサービスのAPIや標準を開示しているわけではないため、相互運用性が必ずしも保証されるとは限らない。また、APIや標準規格が提供されていても、接続の問題への対応に手間がかかり、エラーや互換性の問題が発生するリスクもある。このような場合、単一のCSPから統合サービスを購入することが、実現可能で現実的な解決策である。さらに、単一のCSPから複数のクラウドサービスを購入すれば、顧客は割引を受けられる可能性がある。このような顧客のワンストップショッピングに対するニーズが、CSPの垂直統合に寄与している。

また、垂直統合により、CSPは市場における顧客を通じて、競争上重要なデータを含むより多くの情報を収集することができる²²。CSPは、自社で開発したかサードパーティのCSPが開発したかにかかわらず、自社のインフラ上で稼働するあらゆるクラウドサービスに関する利用指標について直接情報を得ることができる。サードパーティのCSPの観点からは、クラウド・インフラを提供するCSPがこの情報を利用して、どの種類のクラウドサービスを取得するか、または複製して自社で提供するかに関するビジネス上の意思決定を行う可能性があるため、懸念が生じる。

4. 参入障壁

参入障壁に関しては、CSPがどのようなサービスモデルを提供するかによって、初期コストは大きく異なる。しかし、多くの場合、顧客は、様々なサービスを提供しているCSPか

に関する実態調査報告)」参照、

<https://www.jftc.go.jp/houdou/pressrelease/2022/jun/digital/hontai.pdf>。

²¹ ACM, *supra* note 16, pp 20-21.

²² Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary of the House of Representatives, Investigation of competition in digital markets: Majority Staff Report and Recommendations (Jul., 2022), p 100., <https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf>.

らクラウドサービスを購入することを好む。その主な理由は、他のクラウドサービスを購入する必要があり、その後に様々なクラウドサービスを、上記で説明したような相互運用性の問題に直面することなく接続したいと考えるからである。新規参入企業にとって、クラウドサービス市場において、ゼロからスタートし、既存のCSPとすべてのレイヤー（ソフトウェア、プラットフォーム、インフラ）で同時に競争することは非現実的であろう。

SaaSサービスの場合、SaaSサービスはそもそも同質化されておらず、新規参入企業は市場で競合他社のSaaSサービスと差別化できるため、基本的に参入障壁は比較的低い。SaaSサービスの性質を考慮すると、SaaSサービスの提供に注力するCSPは、他のCSPのPaaSサービスやIaaSサービスを購入して、SaaSサービスの開発に必要なクラウド・インフラを入手することができる。多くの場合、クラウド・インフラの利用は従量課金制であるため、初期の設備投資は少なく済む²³。しかし、CSPがSaaSサービスを開発し、すでに競合するSaaSサービスが提供されている市場に参入することは、依然として難しいかもしれない。このような場合、ロックイン効果、ブランド認知の程度、先行者利益が市場参入の主な障害となる²⁴。さらに、競合するSaaSサービスが垂直統合型CSPによって提供されている場合、垂直統合型CSPの抱き合わせやバンドル割引などの反競争的慣行により、市場参入が困難になる可能性がある。

PaaSサービスに関しては、ウェブデプロイメント、モバイルデプロイメント、機械学習²⁵など、特定の開発形態にフォーカスしていることが多い。PaaSサービスは、アプリケーションとクラウド・インフラを接続するという技術的な性質から、SaaSサービスよりも多様性に乏しく、SaaSサービスと比べて差別化やイノベーションの余地が少ない。PaaSサービスは一般的に異なるサービスのチェーンの一部として利用されるため、PaaSサービスでは異なるサービス間の相互運用性が最も重要である。これは、クローズドなAPIや標準が採用されている場合や、PaaSのCSPが他のCSPのインフラがどのように動作しているかについての情報が不足している場合に特に当てはまる。また、同じ理由から、CSPはPaaSサービスを含む統合クラウドサービスを提供するのが一般的であり、そのような統合CSPはPaaSサービスのみを提供するCSPと比較して、PaaSサービスを提供する上で競争優位性を持っている。このような競争優位性は、高い相互運用性だけでなく、規模の経済性にも起因する。クラウド・インフラを他のIaaS型CSPから「購入」できることから、PaaSサービスの参入コストはIaaSサービスと比べて比較的低いが、SaaSサービスの場合と同様に、クラウド・インフラを所有する

²³ これは、ユーザーが使用するコンピュータリソースに対してのみ支払えばよいという柔軟な価格設定モデルを意味する。CSPは多くの場合、従来のIT業界で使用されていた、ライセンスの前払いを必要とする料金モデルではなく、従量課金モデルに従ってサービスを課金するビジネスモデルである。

²⁴ ACM, *supra* note 16, p 52.

²⁵ *Ibid*, p 53.

統合型CSPがライバルとなる場合、非統合型PaaS型CSPにはコスト競争上の優位性はない。

最後に、IaaSサービスに関しては、3つのタイプの中で最も均質なサービスである。IaaS CSP間の競争は、理論的には主に価格である。前述したように規模の経済により、グローバルに展開する大手CSPの存在は市場参入を困難にしている²⁶。規模の経済以外にも、技術的リーダーシップや評判、乗り換えのコストやセキュリティリスクも高い参入障壁につながる²⁷。しかし、比較的小規模なニッチ市場に新規参入することは可能である²⁸。

5. 高い乗り換えコスト／ベンダーロックイン²⁹

クラウドサービスの顧客は、オンプレミスからクラウド環境に移行することを決めた後、CSPを変更することはほとんどないことが観察されている³⁰。この「ロックイン」の背景にある洗練された理由は、技術的な切り替え障壁と金銭的な切り替え障壁の2種類に分類できる。

技術的なスイッチング障壁に関しては、相互接続の困難性、異なる製品提供、データポータビリティの問題、マルチクラウド³¹という4つの状況から構成される。まず、相互接続の困難性とは、顧客が使用しているすべてのクラウドサービスの相互接続を作成または維持するためにコードを書き直したり、新しいCSPに乗り換えたい場合に元のサービスと新しいサービス間の通信がどのように設定・管理されるべきかを理解するためにクラウドサービスを担当する従業員を教育したりすることに時間を費やさなければならない状況を指す。相互接続されているクラウドサービスが多ければ多いほど、関係するレイヤーにかかわらず、切り替えはより複雑で時間がかかる。第二に、提供する製品が異なるということは、CSP間の機能的な類似性があるにもかかわらず、CSPの提供する製品には常に技術的な違い、例えば技術

²⁶ Kamila Benzina, Cloud Infrastructure-as-a-Service as an Essential Facility : Market Structure, Competition, and the Need for Industry and Regulatory Solutions, Berkeley Technology Law Journal, Vol.34 (2019), pp 130-131.

²⁷ Ibid, pp 131-133.

²⁸ ACM, supra note 16, pp 51-52. 特に、サービスはクラウドを通じて提供されるため、データセキュリティとサービスの信頼性は顧客から高く評価される。しかし、新規参入企業は通常、業界固有の規制に準拠した信頼性の高いサービスを提供できることを潜在顧客に納得させるだけの実績を持っていない。

²⁹ ベンダーロックインとは、そのCSP固有の技術や、すでにクラウドサービス上に構築された複雑なシステムを利用しているために、顧客が他のCSPが提供する同種のクラウドサービスに乗り換えることが困難な状況を指す。

³⁰ 公取委の前出の市場調査では、すべてのクラウドサービスが仮に5～10%値上げされた場合、オンプレミスに戻ると回答したのはわずか4%だった。公取委・前掲注(20)37-38頁を参照。さらに、クラウドサービスが仮に5～10%値上げされた場合、回答者の85.9%は同じサービスを使い続け、他のクラウドサービスやオンプレミスに切り替えるとは回答したのはわずか14.1%であった。同報告書49-50頁を参照。日本のクラウドサービス市場にロックイン効果が存在することは、経験的に明らかであるように思われる。

³¹ ACM, supra note 16, pp 55-57.

的なセキュリティやプライバシーの基準が異なることを意味する。このことは、顧客が利用するクラウドサービスに対して、常に代替手段が用意されているとは限らないことを意味する。第三に、データのポータビリティの問題は、元のCSPや新しいCSPがクローズドなAPI(application protocol interface)や標準、互換性のないデータ形式を使用している場合に存在する。最後に、マルチクラウドとは、顧客が異なるCSPが提供する類似のクラウドサービスを並行して利用する状況を示す。マルチクラウドは、顧客にとって異なるCSP間の切り替えの可能性を提供するが、必ずしもロックイン効果を効果的に緩和するとは限らない。逆に、異なるCSPのクラウドサービス間の相互運用性が不十分な場合、マルチクラウドは最終的に複数のクラウドへの事実上のロックインをもたらす可能性がある³²。このような状況では、単一のCSPが主に利用され、他のCSPのサービスは相互接続が不要な特定のサービスにのみ利用される。

一方、金銭的なスイッチング障壁には、主にエグレスフィー(Egress fee)とディスカウント(クレジット込み)の2種類がある。エグレスフィーは、顧客がCSPのクラウドからデータを外部へ転送する際に発生する料金のことを指す。具体的には、クラウドプロバイダー(例えば、Amazon Web Services, Microsoft Azure, Google Cloud等)から、ユーザーのオンプレミスの環境や他のクラウドサービス、インターネット上の他の場所へデータを転送する際に発生する費用のことである。CSPは、データセンターのネットワーク帯域を維持するためにコストを負担している。ユーザーが大量のデータを外部に送ると、その分帯域が使われるため、その使用料として料金を課す仕組みとして、普及してきた。エグレスフィーは特に、動画配信やAI、ビッグデータ解析といった大規模なデータを扱う企業にとって、運用コストの大きな部分を占める可能性があるため、米国連邦取引委員会(FTC)やEU競争当局は、CSPによるエグレスフィーが公正な競争を阻害しているのではないかと調査を進めている。現在、主要なCSPは顧客に対してエグレス料金を課していないが、CSPの無料ティア(一定の条件内で無料で利用できる利用枠)³³を超えた場合、自社のクラウドから転送されたデータ量に応じてエグレスフィーを請求している。顧客が新しいCSPに乗り換えたい場合、まず元のCSPのサーバーから新しいCSPのサーバーにデータを転送する必要がある。顧客はこの転送費用を「エグレスフィー」という名目で支払わなければならないが、これは顧客がCSPのコンピュータリソースを使用する際に支払う料金とは別に請求される。このような現行の料金体系により、CSPのクラウドサービスを購入し、そのクラウドにデータを保存する障壁は低い。しかし、顧客が元のCSPのクラウドに保存するデータの量によっては、元のCSPのクラウドか

³² 一方、複数のパブリッククラウドを利用する場合、オープンなAPIが用意されているため、統合が容易であり、顧客が直面する課題が少なかったケースもある。See CMA, Cloud services market investigation : Technical barriers working paper (Jun. 6, 2024), para 4.14.

³³ エグレスフィー体系の発展の歴史については、see, ACM, supra note 12, pp 58-59.

らのデータ移行にコストがかかる可能性がある。通常、顧客によって保存されるデータ量は時間の経過とともに増加するため、エグレスフィーの総額も時間の経過とともに上昇する³⁴。このように、クラウドからデータを移動させるとエグレスフィーのために高くつくという料金体系が、顧客の乗り換えを阻害している。

もう1つの金銭的なスイッチングの障壁は、顧客にCSPのクラウドサービスの長期利用を約束させる目的でCSPが提供する割引である。割引を提供するビジネス慣行は、利用ベースであれ、料金ベースであれ、あるいはその両方の混合であれ、クラウドサービス市場³⁵で広く行われている。このような割引は、他の乗り換え阻害要因（例えば、退出手数料など）と相まって、顧客が割引を受けるために1つのプロバイダーにビジネスを集中させることを促し、その結果、小規模なCSPの参入障壁や事業拡大障壁を高めることになる。したがって、割引の存在は顧客のスイッチング行動に影響を与える。また、顧客がCSP間の料金プランを直接比較することが困難であるため、割引額の計算が複雑であることも、乗り換えに関する顧客の意思決定にとって不都合である。

上記のようなクラウドサービスの経済的特性は、大規模なCSPに有利であり、クラウドサービス市場の高度集中構造につながっている³⁶。クラウドサービス市場で観察されるように、こうした特性は、大手CSPが統合されたエコシステムを提供し、異なる技術標準に基づいて競争する市場競争につながる。クラウドサービス市場はまだ急速な拡大期にあるが、大手CSPによる構造的要因と潜在的な反競争的慣行は、多くの競争当局の注目を集めている。IVでは、クラウドサービスに関する競争当局の市場調査と、クラウドサービス市場における競争問題に対処するために導入された既存の法律を概略的に紹介する。

IV 競争法の文脈でのクラウドサービスの市場研究・規制事例

クラウドサービス市場は近年、明らかに上昇傾向にある。例えば、Synergy Research Groupによると、2024年第2四半期の世界クラウド市場において、IaaS型CSPの上位3社（アマゾン、マイクロソフト、グーグル）の世界市場シェアは66%（それぞれ32%、23%、12%）を占めている³⁷。米国、英国、オランダ、フランス、日本を含む多くの競争当局は、クラウドサービス市場の現在の寡占的な市場構造を一因として、クラウドサービスに関する市場調査を最近実施している。クラウドサービス市場の競争状況は国によって異なるため、これらの市場調査の調査対象や勧告の内容には若干の違いがあるものの、共通して、そこでの反競争的慣

³⁴ Jigsaw Research, *supra* note 6, para 5.2.4. et seq.

³⁵ 主要なCSPの割引戦略については、see, CMA, *Cloud services market investigation: Committed spend agreements working paper* (May 23, 2024), paras 1.23-1.34.

³⁶ Daniel Schnurr, *Switching and Interoperability Between Data Processing Services in Proposed Data Act*, CERRE (Dec. 2022), pp 8-9.

³⁷ Synergy Research Group, *Cloud is a Global Market - Apart from China* (Aug. 21, 2024), <https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china>.

行に対する競争当局の懸念が表明されている。これらの市場調査とは別に、EUでは、クラウドサービス市場を含むデジタル市場における競争問題に取り組むための新たな規制が採択された。しかし、これらの規制は、とりわけ、クラウドサービスをコア・プラットフォーム・サービスの一種として列挙している点³⁸や、明確性を欠いている点³⁹について批判されている。以下では、まず競争当局や規制当局が実施した市場調査の概要を説明し、クラウドサービスに関連するEU規制について議論する。

米国では、下院司法委員会の反トラスト・商法・行政法小委員会の多数派スタッフが、2020年のデジタル市場における競争に焦点を当てた調査報告書を発表した。この著名な報告書の中で、クラウド・コンピューティングも対象市場の1つに含まれている⁴⁰。しかし、その焦点は主にIaaSサービスに当てられており、特に市場やデータの反競争的な利用について焦点が当てられている。この報告書の後、FTCは2023年の競争とデータセキュリティに影響を与える可能性のあるCSPのビジネス慣行についてパブリック・コメントを求めた。パネル・ディスカッション⁴¹を開催した後、FTCは2023年11月のブログ記事⁴²において、いくつかの重要なテーマを指摘し、いくつかの質問を投げかけている。競争に関して、FTCは、ソフトウェアのライセンス慣行、エグレスフィー、最低利用契約という3つの問題に焦点を当てた。米国反トラスト法の文脈では、クラウドサービスの市場構造よりもむしろ、潜在的な反競争的行為に注目が集まっているように見受けられる。その後の展開として、FTCは2025年1月に、大手CSP（Alphabet, Amazon, Microsoft）とAI開発企業（OpenAI, Anthropic）との間の企業提携・投資に関する6(b)報告書を公表し、これらのパートナーシップがコンピューティングリソースへのアクセスに影響を与え、AI開発パートナーの乗り換えコストを増大させ、CSPパートナーに競争上重要な情報へのアクセスを提供する可能性があるとは指摘した。さらに、FTCは2024年11月以降、マイクロソフトに対するクラウド・コンピューティングおよびAI分野における包括的な反トラスト調査を本格化させ、2026年2月には少なくとも6社の競合他社に対してもCIDを発出し、ライセンス規則、相互運用性の制限、AI・セキュリティソフトウェアのバンドリング慣行に関する情報を求めている。

³⁸ Konstantina Bania and Damien Geradin, The regulation of cloud computing: why the European Union failed to get it right, *Information & Communications Technology Law*, Vol.1 (2024), pp 104-106.

³⁹ Ibid, pp 110-111.

⁴⁰ Supra note 22, pp 91-100.

⁴¹ USFTC, Cloud Computing: Taking Stock and Looking Ahead (May 11, 2023), <https://www.ftc.gov/news-events/events/2023/05/cloud-computing-taking-stock-looking-ahead>.

⁴² USFTC, Cloud Computing RFI: What we heard and learned (Nov. 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned>.

欧州⁴³、オランダ⁴⁴、フランス⁴⁵の各国政府も、2022年と2023年に市場調査を実施している。オランダの競争当局であるAutoriteit Consument & Markt (ACM) は、その報告書の中で、IaaS、PaaS、SaaSの各レイヤーを含むクラウドサービスセクター全体を分析し、特に、マルチクラウド戦略を採用する顧客の動機に関連する、顧客の最初のCSP選択に関する競争と、様々な種類のスイッチング障壁に起因するベンダーロックインの問題という2つの側面を強調している。フランスの競争当局であるAutorité de la concurrenceは、主にIaaSとPaaSサービスに焦点を当て、支配的なCSPがその市場力を活用できる3種類の関連分野、すなわちデータセンターのコロケーションサービス、オンプレミスのソフトウェア、クラウドソリューションのコンサルティングと統合の仲介を分析した。

他方、英国の通信業界の規制当局である英国情報通信庁 (Office of Communications, Ofcom) は、2023年10月にクラウドサービス市場レポートを発表した⁴⁶。Ofcomはまた、クラウド・インフラストラクチャー・サービス (IaaSとPaaS) に焦点を当て、顧客がマルチクラウドを乗り換えたり利用したりするための競争は、エグレスフィー、相互運用性とデータポータビリティに関する技術的制限、コミットメント・ディスカウントなど、CSPの商業的・技術的慣行によってある程度制限されていることを明らかにした。Ofcomは、英国のパブリック・クラウド・インフラ・サービス市場を競争市場庁 (CMA) に照会し、市場調査を実施している。CMAは2025年1月に暫定決定報告書を公表し、同年7月31日に最終決定報告書を公表した。最終報告書において、CMAは、英国のパブリック・クラウド・インフラ・サービス市場が十分に競争的に機能していないとの判断を示した。具体的には、AWSとマイクロソフトがそれぞれ30～40%の市場シェアを有し、高度に集中した市場構造が形成されていること、技術的・商業的な乗り換え障壁（エグレスフィー、相互運用性の制限、コミットメント・ディスカウント等）やマイクロソフトのソフトウェア・ライセンス慣行が顧客の選択を制限していること、両社が資本コストを大幅に上回る持続的な収益を得ていることを認定した。CMAは、2024年デジタル市場・競争・消費者法 (DMCCA) に基づく戦略的市場地位 (SMS) 調査をAWSおよびマイクロソフトに対して実施するよう勧告した。もっとも、CMAの理事会 (Board) は、2026年初頭に、両社が自主的にエグレスフィーの削減やEUデータ法の基準の英国への適用拡大等の措置を講じたことを考慮し、SMS調査の即時開始ではなく「参加型対

⁴³ EU レベルでは、欧州議会が欧州委員会に対し、単一市場における高度に集中した市場構造を踏まえ、デジタル市場法に基づきクラウドサービス分野の市場調査を開始することを検討するよう求めた。See, European Parliament, Competition policy: annual report 2023 (2023/2077(INI)), (Jan. 16, 2024), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0011_EN.html.

⁴⁴ ACM, *supra* note 16.

⁴⁵ Autorité de la concurrence, Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector (Jun. 2023), https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2023-09/23a08_EN.pdf.

⁴⁶ Ofcom, Cloud services market study: Final report (Oct. 5, 2023), <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-3-4-weeks/244808-cloud-services-market-study/associated-documents/cloud-services-market-study-final-report.pdf>.

話（participative dialogue）」を通じた対応を選択したため、本勧告の実施に関しては今後の動向を注視する必要がある⁴⁷。

アジアに目を転じると、日本の公取委は2022年、日本のクラウドサービス分野における支配的なCSPによる取引慣行と競争状況を明らかにすることを目的として、クラウドサービス市場における取引慣行に関する調査を実施した。その報告書⁴⁸において、公取委は、クラウドサービス市場における価格及び品質に関する競争は一定の水準にあることが確認されたものの、同市場は将来的に非競争的な構造に変化する可能性が高いことを指摘している⁴⁹。潜在的な反競争的行為について、公取委の報告書は、CSPの退出料、異なる機能の統合、CSPによるソフトウェアライセンスの自己優遇（self-preferencing）、独占的パートナーの優遇措置などを分析している。他の競争当局の市場報告書と比較して、公取委の報告書は、独占禁止法に基づき、CSPの「マーケットプレイス」⁵⁰で行われるいくつかの反競争的行為の疑いについても調査しており、興味深い。これは、日本の競争法の文脈において望ましい、容認できるビジネス慣行と容認できないビジネス慣行との間の線引きに資するものである。

この点に関しては、最近出された、前述の（脚注(4)参照）MCデータプラスにかかる公取委の排除措置命令が注目される。この事件では、下記1から4の行為が独占禁止法上問題となった⁵¹。

第一に、MCデータプラスは、労務安全サービス（グリーンサイトと称される）においてユーザーが帳票として出力する場合を除き、ユーザーが登録した作業員情報等を電磁的記録として直接出力できないようにしたことが問題となった。ユーザーの中には、MCデータプラスに対し、当該ユーザーが求める他社の労務安全サービスに移行可能な形式で作業員情報の提供を要請する者がいた。しかし、MCデータプラスは、遅くとも2020年頃以降、当該要請があった場合に、グリーンサイトのユーザーに対し、当該ユーザー自らが登録した作業員情報であるにもかかわらず個人情報の保護を理由にするなどして、合理的な理由なく当該作業員情報の提供を拒んでいた。

第二に、MCデータプラスは、サービス利用約款の規定を改定し、グリーンサイトから出力した帳票等を他社に提供する行為等を一律に禁止した。

第三に、サービス利用約款の改定から約1ヶ月の周知期間を経て、2019（R1）年10月21日、

⁴⁷ CMA, Public cloud infrastructure services market investigation: Issues statement (Oct. 17, 2023), https://assets.publishing.service.gov.uk/media/652e958b6972600014ccf9f6/Issues_statement_updated.pdf; CMA, Public cloud infrastructure services market investigation: Updated issues statement (Jun. 6, 2024), https://assets.publishing.service.gov.uk/media/66618c622605fac482e67be5/Updated_issues_statement.pdf.

⁴⁸ 公取委・前掲注(20)を参照。

⁴⁹ 公取委・前掲注(20)53-54頁。

⁵⁰ 公取委・前掲注(20)86-90頁。

⁵¹ 公取委「株式会社MCデータプラスに対する排除措置命令について（概要）」（2024年12月24日）を参照。

https://www.jftc.go.jp/houdou/pressrelease/2024/dec/241224_nijo_2.pdf

MCデータプラスは、競合他社（シェルフイー）に対し、シェルフイーが公開した移行記事（グリーンサイトから出力した帳票をシェルフイーに提供することで作業員情報をシェルフイーが提供する労務安全サービスに移行する方法等を記載したシェルフイーのWebサイト上に公開された記事のこと）が、サービス利用約款に違反する行為をグリーンサイトのユーザーに促すものであり、当該ユーザーにとってグリーンサイトの利用停止等の不利益を招きかねない内容であるとして、移行記事の削除等を求める旨を同日付けの配達証明郵便により通知した。

第四に、MCデータプラスは、グリーンサイトのユーザーが、2020年4月頃以降、競合他社（リバスタ）の提供する労務安全サービスへの切替えに当たり、グリーンサイトから出力した帳票等をそのまま他社に提供している事例を把握したことから、グリーンサイトのユーザーに対し、当該行為と同様の行為を行わないように注意喚起することを目的として、同年10月、当該事例はサービス利用約款の禁止事項に該当する旨の周知文を建設サイト・シリーズのポータル画面に掲載するとともに、前記周知文と同様の内容を記載した電子メールを送信した。

公取委は、MCデータプラスの上記行為に対して、同社が、労務安全サービスの取引において、グリーンサイトのユーザーに他社の労務安全サービスへの切替えをしないようにさせていることによって、自己と競争関係にある事業者とその取引の相手方との取引を不当に妨害しているものであるとして、不公正な取引方法（一般指定第14項（競争者に対する取引妨害））に該当し、独占禁止法19条に違反するとして、同社に対して同法20条1項に基づく排除措置命令を下した。本件は、公取委が、クラウド関連の取引で行政処分を行った初めての事例である。なお、本排除措置命令は2024年（令和6年）12月24日に発出されたものであるが、MCデータプラスは同日、「事実認定及び法令の解釈に関し見解の相違が生じている」として、東京地方裁判所に排除措置命令の取消訴訟を提起するとともに、執行停止の申立てを行っており、現在係争中である。

また、これらの規制当局ないし競争当局の報告書・規制事例に加えて、もう2つの調査報告書が注目を集めている。1つはフランスの競争法の大家であるFrédéric Jennyがクラウド・インフラサービスの潜在的な競争制限効果についての分析したレポートである⁵²。このレポートでは、バンドリング、抱き合わせ、ライバル費用引上げ、自己優遇、イノベーションへの影響など、クラウドサービス市場で発生する可能性のあるCSPの潜在的な反競争的慣行がいくつか挙げられ、理論的な評価が提示されている。もう1つは、Centre on Regulation in

⁵² Frédéric Jenny, Cloud infrastructure services: an analysis of potentially anti-competitive practices, CISPE (Oct. 2021).

Europe (CERRE) の報告書⁵³で、2024年に発表され、最近採用された政策や規制の経済的・法的評価と、経済的観点からの正当性をタイムリーに提供している。EUデータ法(DA)とEUデジタル市場法(DMA)の関連条項の解釈に焦点を当てた法的評価の部分は有益であり、「ブリュッセル効果」⁵⁴として知られるDA規制とDMA規制の世界的影響力は継続的かつ広範囲に及んでいるため、一読の価値がある。

要するに、クラウドサービス分野で高度に集中した市場構造がどのように形成されたかは、CSPの反競争的行為を検討する際に考慮すべき重要な問題である。ほとんどの競争当局はこの問題の重要性を認識しており、その市場分析にかかる諸文書の中で懸念を表明している。次節で紹介するDAとDMAは、市場構造の問題に対処するためにEUが行った野心的な試みである。

V クラウドサービスに関するEU法の展開

他の法域と比較して、EUはクラウドサービスに関する分野別規則を率先して採用している。欧州連合機能条約(TFEU)の101条と102条に加え、EUはデジタル市場法とデータ法をそれぞれ2022年と2023年に導入している。競争法および競争政策の観点から⁵⁵、DAとDMAは、予見可能な将来においてCSPの競争に実質的な影響を及ぼすことからクラウドサービスにとって重要な位置を占めている。上記で説明したように、クラウドサービスの経済的特性、特に規模の経済と高いスイッチングコストが、クラウドサービス市場における高い市場集中度をもたらしている。このような慣行を支える構造的問題に対処することなく、クラウドサービス市場における反競争的慣行にのみ着目することは、対症療法に陥るおそれがある。一方、DAとDMAは、前者はスイッチングと相互運用性の問題を、後者はクラウドサービスを含む特定のコア・プラットフォーム・サービスに関する公正性と競争性の問題を扱っている。これらの問題が解決されることで、市場の集中度は低下し、顧客がより少ない障害でCSP間を切り替えることができるようになるため、クラウドサービス市場の競争はより激しくなると予想される。

本節では、クラウドサービス市場に対する事前規制やセクタースペシフィック規制の今次の流れに焦点を合わせるべく、クラウドサービス市場における伝統的な競争法の適用の可能

⁵³ Antonio Manganelli and Daniel Schnurr, Competition and Regulation of Cloud Computing Services : Economic Analysis and Review of EU Policies, CERRE (Feb. 2024).

⁵⁴ 「ブリュッセル効果」とは、アヌ・ブラッドフォード(Anu Bradford)教授の造語で、EUがその法制度や基準を通じてグローバルな問題を一方的に規制する力を持つことを表す。See Anu Bradford, The Brussels Effect, Northwestern University Law Review, Vol.107, No.1 (2012).

⁵⁵ なお、デジタルサービス法(DSA)は、クラウドサービスがホスティングサービスとして利用される場合にも適用されるが、競争法の観点からは、DSAの適用がクラウドサービス市場に与える影響は限定的である。

性⁵⁶ を分析するというよりはむしろDAとDMAに焦点を当て、それぞれの目的とそのクラウドサービスへの影響を説明した上で、かかる規制の導入後に生じる可能性のある潜在的な論点を指摘する。

1. データ法(DA)⁵⁷

DAは欧州データ戦略⁵⁸の重要な柱であり、その中でEU委員会はデータの単一市場である欧州共通データ空間の創設を発表した。このデータ市場を確立するため、DAはデータ処理サービス(DPS)間の顧客の切り替えを促進し、データへのアクセス、転送、利用のための相互運用性基準を策定することを目的としている⁵⁹。この規則は2024年1月11日に発効し、2025年9月12日から適用されている。DAに先立ち、EUはDPSの切り替えとデータのポータビリティを奨励するために自主規制的アプローチを採用していたが、自主規制的アプローチには効果がないことが判明した⁶⁰。DAが採択されたのは、欧州共通データ空間の創設に向けた進展を加速させるためである。

Data Act (DA) が対象とするのは、「コネクテッド製品 (connected products)」およびそれに付随する「関連サービス (related services)」によって収集・生成されるデータである。そのうち、特に以下のものを規律の対象としている。一つは、「生データ (raw data)」でセンサー等によって機械的に収集された未加工のデータ、もう一つは「加工前データ (pre-processed data)」でアルゴリズム処理が行われる前の段階にある技術的データである。利用者には、以下のようなデータアクセスと共有に関する権利が保障される。

① 自己の使用に基づき生成されたデータへのアクセス権、②当該データを第三者に提供・共有する権利、③リアルタイムでのアクセスやポータビリティ（技術的に可能な限り、利用者はデータを容易に取得できるよう配慮されねばならない）。ただし、第三者への提供のうち、ゲートキーパー (Big Tech) 企業への提供は原則として制限される（6条）。これはデジタル市場法 (DMA) との連携的措置であり、GAFA等によるデータ寡占の拡大を抑止する狙いがある。またDA8条は、B2B関係におけるデータ共有の義務を定めている。すなわち、データ保有者 (data holders) は、利用者が選定した第三者 (data recipients) に対して、要請があれば、対象データへのアクセスをFRAND条件 (Fair, Reasonable and Non-Discriminatory : 公正・合理的・非差別的) で提供しなければならない。DAがこのような規制を伴っているの

⁵⁶ クラウドサービスに対する EU 競争法の適用の概要については、see, Niamh Gleeson and Ian Walden, 14 Facilitating Competition in the Cloud, Christopher Millard ed., Cloud Computing Law, 2nd edn, Oxford University Press, 2021, pp 484-492.

⁵⁷ Regulation (EU) 2023/2854.

⁵⁸ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A European strategy for data, COM/2020/66 final.

⁵⁹ DA, Article 1(1)(d), and (f).

⁶⁰ DA, Recital (79).

は、現代のIoT製品は、製造後も膨大な利用データを生み出すが、上述のようにCSP等の「囲い込み」が常態化している。特に中小企業や利用者は、自分が使っている製品から出ているデータであってもアクセスできない状態に置かれている。DAは、これを是正し、データの民主化とクラウド依存からの脱却、競争促進とイノベーションの拡大を図る包括的なデータ法制として制定された。

DAとクラウドサービスの関係について、一般的に、DAは、CSPのクラウドサービスがDPSの定義を満たす場合に適用される。IaaS, PaaS, SaaSのクラウドサービスは、ほとんどの場合、DPSの定義の範囲に含まれる⁶¹。したがって、DAはクラウドサービスに関するセクタースペシフィック規制とみなすことができる⁶²。この点で、クラウドサービス市場における競争を促進するという目的に関して、DAのもとで注目すべき義務は主に2つに分類される。ひとつは、効果的なスイッチングの障害を取り除く義務（主に6章に規定）であり、もうひとつは、DPSプロバイダー間の相互運用性を促進する義務（6章および8章に規定）である。

DAの6章は、23条のタイトルに示されているように、DPS間の効果的なスイッチング⁶³に対する商業的、商業的、技術的、契約的、組織的な障害⁶⁴を除去することを目的としている。具体的には、6章では、DPSの契約条件（25条）、情報提供義務（26条）、誠実協力義務（27条）、契約の透明性（28条）、スイッチング・チャージの段階的撤廃（29条）⁶⁵、IaaSサービスの機能的同等性（30条）、PaaSとSaaSサービスの相互運用性（30条）の観点から消費者保護を強調している。ただし、DPSプロバイダーに課されるスイッチング義務は、顧客が「同じサービスタイプ」をカバーする別のDPSに切り替える場合に限定されるものではないこと

⁶¹ DPSの定義についてはDAの2条8項参照。それによると、DPSの定義とは、顧客に提供されるデジタルサービスであり、集中型、分散型、または高度に分散型の構成を持つ共有可能なコンピューティング・リソースに対し、ユビキタスかつオンデマンドでのネットワークアクセスを可能にするサービスを指す。これらのリソースは、設定可能でスケラブルかつ弾力的であり、最小限の管理労力やサービス提供者とのやり取りで迅速にプロビジョニングおよび解放ができる。この定義は、多様な目的、機能、技術的構成を持つ多数のサービスを包含する。

⁶² Manganelli and Schnurr, *supra* note 53, p 29.

⁶³ DA6章は、DPSプロバイダーが処理するあらゆるデータ（個人および非個人を含む）に適用されることに留意すべきである。See, DA, Article1(2)(e).

⁶⁴ もっとも、DAでは、障害は例示されているが、明確には定義されていない。DA23条によれば、顧客によるDPS契約の解約、同一サービス類型の新たなDPS契約の締結、顧客データやデジタル資産の移転（ポーティング）、顧客が同一サービス類型の新たなDPSを利用する際の機能的同等性の実現、IaaSサービスの他のDPSからのアンバンドリング等、DPS事業者が妨げる場合、それらの行為は、効果的なスイッチングの障害となり、DAに違反する可能性がある。従って、DA23条以下の規定をどのように解釈するかは、適用範囲を決定する上で極めて重要な問題である。

⁶⁵ DA2条36項によれば、「スイッチング・チャージ」とは、「標準サービスフィーまたは途中解約に伴う違約金以外で、データ処理サービスの顧客が、当該サービスのプロバイダー以外のシステムまたはオンプレミスのICTインフラへのスイッチングする場合、当該プロバイダーが当該顧客に課す料金」と定義されている。スイッチング・チャージには、前述のとおり、金銭的なスイッチング障壁となるデータ消去料（2条35項）が含まれるが、標準サービス料や途中解約違約金は含まれない。したがって、クラウドサービスが一定期間提供される場合、CSPは顧客に相応の打ち合わせ解約違約金を課すことができる。See, Manganelli and Schnurr, *supra* note 53, pp 32-33.

に留意すべきである。顧客のオンプレミスICTインフラへの切り替えやマルチクラウド戦略の採用など、その他の状況も含まれる⁶⁶。ただ、DAの「同一サービスタイプ」の定義は曖昧である。DPSの「同一サービスタイプ」とは、主要目的、データ処理サービスモデル、主要機能を共有する一連のDPSを意味する⁶⁷。しかし、これらの要素はDPSの運用特性とは関係ない⁶⁸。別の言い方をすれば、「同じサービスタイプ」をカバーするDPSのプロバイダーは、競争法上の意味において必ずしもライバルではない。この理解に基づけば、DAに基づくスイッチング義務は、代替可能なDPSだけでなく、補完的なDPSの場合にも適用される。したがって、これらのスイッチング義務が市場競争に与える全体的な影響をどのように評価するかは、今後の重要な検討課題である。

他方、相互運用性がデータの単一市場の出現に不可欠であることから、DA8章は30条とともに、相互運用性の義務を規定している⁶⁹。具体的には、8章では、データ共有メカニズムやサービスのデータの相互運用性、欧州共通のデータスペースに関する必須要件（33条）、マルチクラウドの場合の相互運用義務（34条）、DPSの相互運用性のためのオープンな相互運用性仕様と調和基準（35条）、データ共有のためのスマートコントラクトに関する必須要件（36条）が規定されている。

すべての義務の中で、29条と30条は、クラウドサービス市場における競争に関して特に重要である。次項で概略的に説明する。

(1) スイッチング・チャージ

まず、29条はスイッチング・チャージに関するEUの考え方を反映したものであり、DPSのプロバイダーは、スイッチングのプロセスにおいて、顧客にいかなるスイッチング・チャージも課すべきではないというものである。しかし、スイッチング・チャージが広く行われている現状を踏まえ、DPSプロバイダーに時間を与えるため、3年間の移行期間が導入された。移行期間中、DPSプロバイダーは、当該スイッチング・プロセスに直接関連するコストを超えないスイッチング・チャージのみを課することができる（29条3項）。この新たに導入された29条により、特にエグレスフィーのような高額なスイッチングコストは、実質的に大幅に引き下げられると推定される。スイッチング・チャージがなければ、顧客は現在の料金プランを他のDPSプロバイダーのプランと比較することが容易になり、予測しやすくなるため、スイッチングが効果的に促進されることをDAは期待している。なお、DAが2025年9月12日に適用開始されたことに伴い、上記3年間の移行期間が開始している。すなわち、2025年9月12

⁶⁶ DA, Article 23.

⁶⁷ DA, Article 2(9).

⁶⁸ DA, Recital (81).

⁶⁹ DA2 条 40 項は、相互運用性を「2 つ以上のデータ空間または通信ネットワーク、システム、接続された製品、アプリケーション、データ処理サービスまたはコンポーネントが、その機能を果たすためにデータを交換し使用する能力」と定義している。

日から2027年1月12日までの間、DPSプロバイダーはスイッチング・プロセスに直接関連するコストを超えないスイッチング・チャージのみを課することができるが、2027年1月12日以降は、スイッチング・チャージは完全に撤廃される（29条2項）。ただし、29条の義務には例外がある。マルチクラウドの場合、マルチクラウドの目的のために発生したエグレスコストの範囲内に限り、エグレスフィーを徴収する慣行を認めることができる（34条2項）⁷⁰。

（2）機能的同等性と相互運用性

第二に、DAの30条は、IaaSサービスの機能的同等性（パラ1）とPaaSおよびSaaSサービスの相互運用性（パラ2～4）を強調している。IaaSサービスの機能的同等性については、30条1項において、DPSプロバイダーは、顧客が同じサービスタイプをカバーする他のDPSに乗り換えた後、機能的同等性⁷¹を促進するために、あらゆる合理的な措置を講じなければならないと規定されている。30条1項に基づき、IaaS CSPは、新たなカテゴリーのDPSを開発したり、移行先のDPSプロバイダーのインフラ内でサービスを再構築したりするのではなく、能力、適切な情報、文書、技術サポート、必要なツールの提供を通じて、その能力の範囲内で顧客に支援とサポートを提供することが求められる⁷²。他方、PaaSおよびSaaSサービスの相互運用性に関しては、30条2項において、PaaSおよびSaaSサービスプロバイダーは、「切り替えプロセスを容易にするために、すべての顧客および関係するデータ処理サービスの提供先プロバイダーが、等しくオープンなインタフェースを無償で利用できるようにする」べきであると規定されており、30条3項において、これらのプロバイダーは、オープンな相互運用性仕様または相互運用性のための整合化された標準に基づく仕様との互換性を確保することを求めている⁷³。さらに、オープンな相互運用性の仕様または規格がまだ特定されていない場合、30条4項に基づき、顧客から要求があれば、構造化され、一般的に使用され、機械が読み取り可能な形式で、すべてのエクスポート可能なデータをエクスポートする義務がある。相互運用性を促進することで、DAは「競争と新サービスの発展を損なうベンダーロックインを克服する」ことを目的としている⁷⁴。これらの義務（30条2項、30条3項、30条4項）は、マルチクラウドの場合のDPSプロバイダーにも準用される（34条）。

DAを紹介・検討する文献のなかには、DAが意図的に水平的相互運用性（同じサービスタイプをカバーするDPS間でデータ交換を行う場合の相互運用性）と垂直的相互運用性（同じサービスタイプでないDPS間でデータ交換を行う場合の相互運用性⁷⁵）を区別しており、前

⁷⁰ この例外の正当化については、See, DA, Recital (99).

⁷¹ 機能的同等性の定義については、DA2 条 37 項を参照。

⁷² DA, Recital (92).

⁷³ DPS の相互運用性に関するオープンの仕様の詳細な規格要件については、DA35 条を参照のこと。

⁷⁴ DA, Recital (90).

⁷⁵ Ibid, n 75, p 30.

者は30条で保証され、後者は34条で保証されていると指摘しているものもある⁷⁶。しかし、34条の正確な文言は、DAのリサイクル(99)で用いられている「補完的な機能を有する複数のデータ処理サービスの並行利用」ではなく、「データ処理サービスの並行利用」であるため、34条がマルチクラウドの文脈における垂直的相互運用性にのみ焦点を当てているという理解を前提としたこのような解釈は、34条の文言と矛盾するように思われる。したがって、DA30条と34条の関係をどのように正確に理解するかは、さらに明確にされる必要がある。

以上、概略的に説明したように、新たに導入されたDAによって、クラウドサービスの提供方法は大きく変わりうる可能性があるものの、その解釈には解決すべきさまざまな課題が残されている。

2. デジタル市場法(DMA)⁷⁷

DMAは、デジタル分野における市場の競争性と公平性を確保することを目的としている。DMAは、EU委員会に対し、事業者が提供するコア・プラットフォーム・サービス(CPS)がビジネスユーザーと消費者の間の重要なゲートウェイを構成する場合、事業者をゲートキーパーとして指定する権限を与えている。というのも、クラウドサービス⁷⁸も、DMA2条2項1号に規定されるCPSの一種であるため、DMAの適用範囲に含まれる。

EUの立法者は、EU競争法がデジタル市場における競争問題に取り組むには十分でないと観察している。その理由は、第一に、EU機能条約(TFEU)101条と102条の適用範囲が市場支配力のある特定の事例に限定されていること、第二に、EU競争法のエンフォースメントが基本的に事後規制として行われ、ケースバイケースで広範かつ時間のかかる調査が必要であること、第三に、ゲートキーパーが競争法の意味において必ずしも支配的ではなく、その行為がEU競争法⁷⁹の下で効果的に規制されない可能性があること、などである。したがって、DMAはEU競争法を補完する役割を果たす。

規模や市場支配力に関係なく、すべてのCSPプロバイダーに対称的に適用されるDAと比較すると、DMAは非対称的な規制であり、特定のCPSに関してゲートキーパーとして量的・質的に適格な指定事業者にのみ義務を課している⁸⁰。CSPが欧州委員会からゲートキーパーに指定されると、DMA5条および6条に基づく事前義務が課される。5条には9つの義務からな

⁷⁶ Manganelli and Schnurr, *supra* note 53, p 37. ただし、DA2条9項の「同一サービスタイプ“same service type”」の定義が曖昧で不明確であるため、この区別も疑わしいと思われる。

⁷⁷ Regulation (EU) 2022/1925.

⁷⁸ DMAにおける「クラウド・コンピューティング・サービス」の定義は、指令(EU)2016/1148の4条19項に定義されているように、「共有可能なコンピューティング・リソースのスケラブルで弾力的なプールへのアクセスを可能にするデジタルサービス (a digital service that enables access to a scalable and elastic pool of shareable computing resources)」を意味する。

⁷⁹ DMA, Recital (5).

⁸⁰ DMA, Article 3.

る「ブラックリスト」が含まれており、そのほとんどはself-executingな禁止事項である。一方、6条には12の義務からなる「グレーリスト」が含まれており、その措置はDMA8条2項⁸¹に従い、EU委員会がさらに指定する必要がある。どちらのリストも一般的には、ビジネスモデルや市場の特徴に関係なく、すべての指定ゲートキーパーに適用されるが、これらの義務の一部は特定のCPSや、クラウド・コンピューティングの文脈では適用されないように思われる⁸²。したがって、クラウドサービスに関連するDMAの義務は限定的であるように思われる⁸³。

3. DMAによるクラウドサービス規制への批判

実際、他の多くのCPSとは異なり、クラウドサービスは一般的にマルチサイド型のプラットフォームではなく、ワンサイド型のそれであると指摘する者もいる⁸⁴。クラウドサービスは、ビジネスユーザーと消費者の間を仲介するものではなく、SaaS, PaaS, IaaS, またはこれらの組み合わせのサービスを、仲介者として機能することなく顧客に提供するものである。DMA3条1項(b)のゲートキーパーの定義によれば、CPSは「ビジネスユーザーがエンドユーザーに到達するための重要なゲートウェイ」でなければならない。しかし、クラウドサービスは、ほとんどの場合、そのような特徴を含んでいない⁸⁵。したがって、欧州委員会が影響力のあるCSPをゲートキーパーに指定するかどうかについて、重要な進展があった。2025年11月、欧州委員会は、DMAに基づき、クラウド・コンピューティング・サービスに関する3件の市場調査を開始した。そのうち2件は、Amazon Web Services (AWS) およびMicrosoft Azureが、DMAの標準的な量的閾値を満たさないにもかかわらず、事業者と消費者の間の重要なゲートウェイとしての機能を果たしているかどうかを評価するものであり、3件目は、DMAの現行の枠組みがクラウド・コンピューティング・サービスにおける競争性と公正性を制限する慣行に効果的に対処し得るかどうかを評価するものである。なお、欧州委員会は2026年4月のDMA

⁸¹ 「ブラックリスト」と「グレーリスト」という用語は、DMAの下でのゲートキーパーの義務や禁止事項に関する議論においてよく使われる。例えば、Alexandre de Streel, *The European Proposal for a Digital Markets Act: A First Assessment*, CERRE (Jan. 2021) pp 16-18 参照。

⁸² 例えば、6条11項の義務は、オンライン検索エンジンのゲートキーパーにのみ適用される。同様に、6条12項に基づく義務は、オンライン仲介サービス（ソフトウェア・アプリケーション・ストア）、オンライン検索エンジン、オンライン・ソーシャル・ネットワーキング・サービスのゲートキーパーに適用される。さらに、広告ベースのビジネスモデルがCSPによってほとんど採用されていないことを考慮すると、5条2項(a)、5条9項、5条10項および6条8項に基づく義務は、クラウドサービスの文脈では重要ではないように思われる。

⁸³ クラウドサービスの文脈におけるDMA義務の適用可能性の分析については、See, Manganelli and Schnurr, *supra* note 53, pp 47-50.

⁸⁴ Bania and Geradin, *supra* note 38, pp 104-105; Manganelli and Schnurr, *supra* note 53, p 44.

⁸⁵ 多くのクラウド・コンピューティング・サービスを提供しているMicrosoftは、当該サービスについて、ビジネスユーザーとエンドユーザーを仲介し、商業的な意味で需要と供給を結びつけるものではないことから、ビジネスユーザーとエンドユーザーを繋ぐゲートキーパーとしての役割は果たしておらず、DMAの規制対象からは除外されるべきである、と主張している。

レビュー報告書において、DMAは現行の形で目的に適合しており改正は不要であるとの評価を示す一方、AIおよびクラウド・コンピューティング・サービスへの適用が今後の重点課題であることを明示している⁸⁶。仮に欧州委員会がクラウドサービスに関して何らかのCSPを指定し、その指定が裁判所によって支持されたとしても、DMA5条および6条に基づく上記の義務をどのように適用するかは、また別の論点となる。

一方、CSPが提供するマーケットプレイスの場合、確かに独立系ソフトウェアベンダーとエンドユーザーをマーケットプレイスを介して結びつけ、間接的なネットワーク効果を発揮している。しかし、その事業特性からすると、このようなマーケットプレイスは、2条14項にいう「ソフトウェア・アプリケーション・ストア」の定義を満たし、「クラウド・コンピューティング・サービス」(2条2項1号)ではなく、「オンライン仲介サービス」(2条2項1号)とみなされる可能性が高いと思われる。

4. クラウドサービスに関するDAとDMAの相互作用に関する潜在的問題点

上記の通り、DAはクラウドサービスに関するセクタースペシフィック規制と考えられるが、DMAは競争規則を補完するための事前規制を規定しており、主に個別案件における事後的な執行に重点を置いている。現在までのところ、DMAのもとではクラウドサービスのゲートキーパーが指定されていないが（なお前述のとおり、2025年11月にAWSおよびAzureに対する市場調査が開始されている）、これらの法律が共存しているため、その実施に関する問題が生じている⁸⁷。これらの問題は、実質的な懸念と制度的な懸念の2つの側面に大別される。

実質的な問題については、まず、DMAより後に採択されたDAには明確なセーフガードが規定されていないため、DMAとDAの関係をどのように解釈するかが不明確である。これに対し、例えばDA1条5項は、規則(EU)2016/679(GDPR)の適用を保障している。このため、DMAとDAで適用範囲が重複する場合、どちらの規制を優先すべきか、言い換えれば、2つの規制の一貫性と整合性を確保するために関連規定をどのように解釈すべきかが不明確である。例えば、クラウドサービスにおけるデータポータビリティ義務に関して、DA25条と26条、DMA6条9項をどのように調和的に解釈するかは難しい問題である。

この点で、規範の重複やアンチノミーを避けるためには、2つの規制の中核的な目的が部分的に重複していることを考慮する必要がある⁸⁸。クラウドサービスの文脈に限らないが、

⁸⁶ 現在までに欧州委員会は、DMAの下で8種類のCPSに関して7つのゲートキーパーを指定しているが、クラウドサービスとバーチャル・アシスタントに関してはゲートキーパーを指定していない。See, EU Commission, https://digital-markets-act.ec.europa.eu/gatekeepers_en (last visited Sep. 2024).

⁸⁷ DAとDMAの関係についての予備的分析については、see, Manganelli and Schnurr, *supra* note 53, pp 53-58.

⁸⁸ Manganelli and Schnurr, *supra* note 53, pp 53-54.

DA5条3項は、関連する規定を首尾一貫して解釈する方法について良い指針を与えてくれる。DA5条3項は、DMAに基づくゲートキーパーが、接続されたスマート製品または関連サービスの使用によって生成されたユーザーデータへのアクセスを要求または取得することを禁止している。ゲートキーパーをデータアクセス権の受益者に含めない理由は、「(EU)規則(EU)2022/1925に従い、これらの事業者がデータを取得する比類のない能力を有していることを考慮すると、本規則の目的を達成するためにゲートキーパーを含める必要はない」⁸⁹というものである。したがって、DMAに定義された競争目的は、DAの解釈と執行において考慮されうると言える。他方、DAの目的を念頭に置いてDMAを実施することは可能であろうか。非対称的なDMAと対称的なDAという両者の規制上の特徴に鑑みれば、DAがDMAの解釈と執行のベースラインを提供するというもっともな議論が成り立つ。いずれにせよ、不確実性を最小化するためには、関係するすべての法令や規制の一貫性と相互整合性に寄与する広範な明確化を提供するガイドラインの制定が望ましい。

さらに、制度的な懸念として、複数の適用規制が存在することは、クラウドサービスを管理する複数の執行機関が存在することを意味する。欧州委員会はDMAの唯一の執行機関であり、ハイレベル・グループはDMA⁹⁰の実施または執行に関する一般的な問題について助言と専門知識を提供するのみである。これとは対照的に、DAは分権的なレベルで施行され、複数の管轄当局が指定された場合には、国レベルで断片化される可能性がある⁹¹。このため、両者の並行適用は、それぞれの規制の適用における協調の欠如につながり、法的矛盾を含むさまざまな種類の紛争を引き起こすおそれがある。この潜在的なリスクに対処するためには、規制当局間のコミュニケーションと協力を促進することが必要であることは間違いない。最終的には、このリスクを回避するために制度の再設計が必要になるかもしれない。

VI 課題と展望

本章では、まずクラウドサービスの基本概念とそのサービスモデルであるIaaS, PaaS, SaaSサービスについて説明し、次にクラウドサービスの主な経済的特徴について議論した。これには、規模の経済（これには、コンピュータ資源と研究開発の2つの側面を含む）、ネットワーク効果（主にCSPが提供するマーケットプレイスに関連するネットワーク効果）、垂直統合の傾向（ワンストップショッピングに対する顧客の強いニーズとCSPのクラウドエコシステムの競争力追求の結果として生じるもの）、高い参入障壁（特にPaaSとIaaSのレイヤーにおけるそれ）、高いスイッチングコスト（技術的および財政的なスイッチング障壁を含む）が含まれ、これらがあいまってロックイン効果を引き起こす。これらの経済的特徴は、

⁸⁹ DA, Recital (40).

⁹⁰ DMA, Article 40(5), 40(6) and 40(7).

⁹¹ DA, Article 37.

クラウドサービス市場における高い集中の主な決定要因であり、多くの競争当局は、クラウドサービス市場の寡占構造やそこでの反競争的慣行について懸念を表明している。これらの当局の市場調査において、本稿では、クラウドサービス市場における高度に集中した市場構造がほとんどの先進国で観察されていること、また、ほとんどの競争当局が、例えば、クラウドサービス利用者に不利益をもたらす競争を阻害するために支配的なCSPによって実施される可能性のあるエグレスフィーのような潜在的な反競争的慣行を調査していることを確認した。この点で、EUは、クラウドサービス市場で生じる競争問題にハードローアプローチで取り組む決意を示している。EUが採用した新たな規制アプローチであるDAとDMAは、それに対して否定的であれ肯定的であれ、クラウドサービス市場の競争に大きな影響を与える。とはいえ、DAは、制定後まもない法制であり、依然として検討すべき多くの疑問点があるように思われる。一方、DMAは、その規制の枠組みが、ほとんどの場合、ビジネスユーザーとエンドユーザーの間を仲介しないクラウドサービスには直接の関係をもたないことから、クラウドサービス規律の観点から批判の対象ともなっている。さらに、DMAとDAの目的は実質的に重複しており、これら2つの法律はともに競争促進を目的とした一定の措置を導入しているため、DMAとDAの一般的な適用関係に関する問題も残されている。これらの問題は、規制アプローチに由来するもの（例えば、相互運用性の問題）と、複数の規制当局の関与に起因するものとに分類することができるが、EUに特有の問題ではなく、複数の競争関連法がクラウドサービスに適用される他の法域でも生じ得るものであることを念頭に置くべきである。

クラウドサービスを、事後的な競争法のエンフォースメントに加え、事前的な競争政策的規制（DMA等）の下で規制するかどうかは、特に注目すべき重要な課題である。クラウドサービスの経済的・産業的特性を周到に考慮することなくクラウドサービスを規制することは、クラウドサービス分野における技術革新の発展を阻害し、最終的には消費者の利益を損なうことになる。しかし、DAとDMAのいわゆる「ブリュッセル効果」⁹²を考慮すると、他の法域でも同様の規制イニシアチブが導入される可能性が広く想定されている。タイムリーな例として、日本では2024年6月、日本のスマートフォン市場における新たな競争問題に取り組むため、日本版DMAに相当する「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律（スマホソフトウェア競争促進法）」⁹³が制定された。スマホソフトウェア競争促進法は、次の3つから構成される法律である。①OS事業者は、他の事業者がアプリストアを提供することを妨げてはならない。②ただし、（i）「セキュリテ

⁹² 部分的・断片的な蓄積を頼りに、米コロンビア大 Anu Bradford 教授の著書（前掲注(53)）で指摘されている「ブリュッセル効果」によりEUのデジタル法制を強く参照した立法を余儀なくされているのが、我が国のデジタル法制の一つの側面であると言わざるを得ない。

⁹³ 令和六年法律第五十八号。同法は2025年12月19日から施行される。

ィ」，(ii)「プライバシー」，(iii)「青少年保護」，(iv)「その他政令で定める目的」のために必要な措置を行う場合であって，他の行為によってその目的を達成することが困難であるときは，当該措置を行うことができる（正当化事由）。③なお，この規律は，上記①のとおり，OS事業者以外の事業者が運営するアプリストア（新規参入アプリストア）を経由してアプリを提供することを可能にする規律である一方，いかなるアプリストアも経由せずにウェブサイトからアプリを直接提供することを可能にする規律ではない。またCSPはこの法律の対象外であり，モバイルオペレーティングシステム，アプリケーションストア，ブラウザー，検索エンジンのプロバイダーのみに適用されるが，上述の問題（複数の規制当局の所掌に関わる問題）と類似した状況が観察される。つまりそれはこういうことである。

公取委という，公正競争の専門家ではあるがセキュリティやプライバシーの専門家ではない，あるいは（仮に詳しい職員を中途採用等したとしても）公正競争確保については行政責任を負っているがセキュリティ，プライバシーの確保については国民に対し行政責任を負っていない官庁に法執行の運用を任せきりにしていると，公正競争と安心安全という2つの保護法益を中立的に判断できず，どうしても公正競争を過度に重視した判断がなされるおそれがないか，という懸念の声が，法案の検討過程において度々提起された。他方，独立規制機関である公正取引委員会が個別事案の法執行をしようとするたびに事業所管官庁等にいちいち「お伺い」を立てなければならなくなってしまうと公取委の執行の「独立性」や「迅速性」が確保されないのではないか，という懸念も提起されていた⁹⁴。

このような点を踏まえ，スマホソフトウェア競争促進法では，セキュリティ，プライバシー，青少年保護等の観点から，①公取委が関係行政機関に対し意見を求めることができるとともに，②関係行政機関が公正取引委員会に対し意見を述べるができるとする，関係行政機関との連携に係る規定が明文で設けられている（同法43条⁹⁵）。これを受け，新法の施行に伴うセキュリティ，プライバシー，青少年保護等に関し，公取委と関係行政機関が連携して円滑に対応するため，関係省庁連絡会議が開催されている。また，前述の正当化事由に関

⁹⁴ この点，欧州のDMA40条では，「電気通信規制当局」，「データ保護当局」，「競争当局」，「消費者保護当局」，「視聴覚通信規制当局」の5分野の当局からなる「ハイレベル・グループ」が，DMAの法執行に関し勧告や助言を与えることができる，という枠組みが明文で法定されている。

⁹⁵ 43条（関係行政機関の意見の聴取）

公正取引委員会は，第七条ただし書又は第八条ただし書の規定の適用に関し必要があると認めるときは，内閣総理大臣，総務大臣，文部科学大臣，経済産業大臣又はこども家庭庁長官その他の関係行政機関の長に対し，意見を求めることができる。

2 前項に定めるもののほか，公正取引委員会は，この法律の施行に関し必要があると認めるときは，関係行政機関の長に対し，意見を求めることができる。

3 内閣総理大臣，総務大臣，文部科学大臣，経済産業大臣及びこども家庭庁長官その他の関係行政機関の長は，第七条ただし書及び第八条ただし書の規定の適用について，公正取引委員会に対して意見を述べるができる。

4 前項に定めるもののほか，関係行政機関の長は，この法律の施行に関し，公共の利益を保護するため，公正取引委員会に対して意見を述べるができる。

する考え方の明確化を図るため、公正取引委員会とこれらの関係行政機関が連携して、ガイドラインが策定されている。なお、同法は2025年12月18日に施行されている。いずれにせよ、複数の規制当局が関与することによって生じるある種のジレンマは、規制当局間のコミュニケーションと協力によってのみ解決できるものである⁹⁶。

VII 結語

わが国においても、データ駆動社会の実現に向け、データの信頼性を担保しつつ、データ利活用の幅を広げる枠組みを構築するため、ハードロー（規制法）のみならず、技術標準やガイドライン（ソフトロー）を織り交ぜたアプローチを推進する必要がある。具体的には官民データ活用推進基本法の改正を行うとともに、独占禁止法の厳正な執行とともに、データポータビリティ及び相互運用性に関する法制度（日本版データ法）を整備することにより、公平で公正なクラウド利用環境を構築することが求められる。その際、本章で検討したDAとDMAの相互作用に関する諸問題、及びスマホソフトウェア競争促進法の執行において顕在化した複数の規制当局間の連携の課題は、わが国の制度設計においても十分に参照されるべきであろう。さらに、2025年以降、クラウドサービスと生成AI（Generative AI）との結合が急速に進展していることに鑑みれば、クラウドサービス市場の競争分析は、生成AI市場の構造分析と不可分の関係にある。CSPとAI開発企業との間の大規模投資・提携関係がもたらす競争上の含意については、今後さらに研究を深める必要がある。

* 本稿は、名古屋大学外国人資料調査員・巫昆霖氏（肩書は執筆当時）との共同研究に基づく研究成果の一部である。

⁹⁶ この点で、考慮すべき要素に関する公取委の方針や原則をまとめたガイドラインは、政府の透明性を高めるツールとして参考になるだろう。

第 6 章

サイバー攻撃に対する国際法の適用

東京大学大学院教授
西 村 弓

I はじめに

情報通信技術(Information and Communications Technologies : ICT)の発達と当該技術に対する社会規模での依存度が高まることに応じて、サイバー攻撃（何らかの意図や悪意を持った者が、特定の国家や企業、団体、個人に対して、コンピュータ・ネットワーク上で行うクラッキング行為）が社会基盤を脅かし得る重大な脅威となりつつある。こうした事態に対応して、国内外でサイバーセキュリティの強化が急務となっている。エネルギー産業分野においても、G7エネルギー大臣ハンブルク会合（2015年）が「持続可能なエネルギー安全保障のためのG7ハンブルク・イニシアティブ」を公表して、「エネルギー輸送システムへのサイバー上の脅威はますます複合的で巧妙になってきている。我々の経済は、インフラやサービスをモニターし管理する相互に接続されたICT設備を通じて、エネルギーの産出、輸送および分配を確保するデジタルネットワーク上のシステムを基盤として成り立っている。エネルギーのバリューチェーン全体を通じてこれらのシステムが運用され相互接続される必要性は日々増大しており、そのためにデジタル上のフレームワークおよびインフラを維持する必要性も増している」という当時の現状認識を示すとともに¹、「我々は、エネルギー分野におけるサイバーセキュリティの改善に向けて取り組むことを約束する。そうした取り組みには、異なるアプローチの分析、サイバー上の脅威の識別、脆弱性およびベストプラクティスの定義や方法に関する情報交換、サイバーセキュリティ能力向上への投資や能力構築が含まれる」としてエネルギー分野におけるサイバーセキュリティ向上の必要性を謳っている²。とりわけエネルギー産業分野におけるサイバーセキュリティが取り上げて論じられるのは、同分野を対象とするサイバー攻撃が一企業にとどまらない社会全体への影響をもたらし得る重大性を帯びる可能性を孕み、それだけに攻撃側から見れば魅力的な対象だからである。

実際、エネルギー関連分野におけるサイバー攻撃には下記のような事例がある³。

表：エネルギー分野におけるサイバー攻撃事例

	年	発生国	攻撃内容	もたらされた影響
1	2003	米国・カナダ	米国東海岸、カナダ・オンタリオ州の送電システムに対するハッカーによる攻撃	数時間にわたる送電障害
2	2003	米国	オハイオ州デービス・ベッセ原子力発電所でサーバを狙ったSlammerワームが、契約ベ	5-6時間にわたる安全管理システムの停

¹ G7 Energy Ministerial in Hamburg, Communiqué, G7 Hamburg Initiative for Sustainable Energy Security (2015), para. 9.

² *Ibid.*, para. 16.

³ データについては、Kon Briefing, *Cyber Attacks News Today 2024/2023*, at (<https://konbriefing.com/en-topics/cyber-attacks.html>)や日本電気株式会社 Web サイト「重要インフラに対するサイバー攻撃の実態と分析」at (<https://jpn.nec.com/techrep/journal/g17/n02/170204.html>)等を参照。

			ンダーが使用するVPN接続を介して侵入・感染	止
3	2005	日本	従業員の自宅PCがマルウェアに感染し、機密情報がファイル共有ソフト経由で流出	原子力発電所の機密情報流出
4	2007～	米国・英国	英米エネルギー企業5社が数年にわたり中国を発信源とする組織的ハッカーからマルウェアNight Dragonによる攻撃を受ける。	ガス田や入札に関する機密情報の窃取
5	2008	シリア	レーダー網をハッキングした上でイスラエル戦闘機が侵入し核施設を空爆	核施設の破壊
6	2008	トルコ	制御システムに対するサイバー攻撃により石油パイプライン内の圧力上昇	パイプラインの爆発
7	2010	イラン	Natanzウラン濃縮施設におけるSiemens製制御系システムがUSBを介してコンピュータワームStuxnetに感染。米国およびイスラエルによる作戦とされる。	約1,000台の遠心分離機が破壊される。
8	2011	カナダ	複数のエネルギー企業にリモート管理ツールを提供するカナダ企業のネットワークがマルウェアに感染	リモート管理ツールの脆弱性に関する情報が漏洩
9	2012	サウジアラビア	国営石油会社Aramcoのワークステーション3万台がShamoonウィルスに感染	データ消去。内部ネットワークの1週間以上にわたる遮断
10	2012	英国	ロンドン五輪会場の電力システムに対して40分間にわたり1000万回以上の攻撃	実害なし
11	2012	米国	2つの発電所で制御システムがマルウェアに感染	片方は再稼働が3週間遅延，もう一方も運用制限
12	2013	米国	ニューヨーク州ダム管理システムに対する攻撃	一定時間水門を制御される。
13	2014	米国・欧州	Dragonflyハッカーグループによる発電所，電力系統，石油パイプライン等を標的としたマルウェアHavexに数百社が感染	多数の情報の窃取
14	2015	ウクライナ	発電所がマルウェアBlack Energy 3に感染	同国西部で数時間にわたる大規模停電

15	2015	トルコ	イランによるサイバー攻撃	各地における12時間 にわたる大規模停電
16	2016	ドイツ	原子力発電所の燃料棒監視システムがマル ウェアに感染	実害なし
17	2016	イスラ エル	電力公社のシステムがフィッシング攻撃に よりマルウェアに感染	一部システムが2日 間停止
18	2016	ウクラ イナ	マルウェア Industroyer/Crash Overrideを用い たサイバー攻撃	キエフ市内1/5が約1 時間停電
19	2017	ウクラ イナ	チェルノブイリ原子力発電所の放射線モニ タリングシステムがランサムウェアNot Petya に感染	手動制御を余儀無く される。
20	2017	サウジ アラビ ア	発電所の安全システムがマルウェア Triton に感染	実害なし
21	2019	インド	Kudankulam 原発管理システムに対する Dtrack系マルウェアによる攻撃	データ盗取
22	2020	イラン	Natanz 原発に対するサイバー攻撃（＋爆発 物の設置）。イスラエルによるとされる。	施設の爆発。核開発 計画を1-2年遅らせ たと指摘される。
23	2021	イラン	Natanz 原発に対するサイバー攻撃。イスラ エルによるとされる。	停電。遠心分離機数 千台の破壊
24	2021	米国	フロリダ州水道システムに対するサイバー 攻撃	水酸化ナトリウム濃 度設定が通常の100 倍に変更される。
25	2021	米国	従業員のVPN接続用パスワード盗取により Colonial Pipelineがランサムウェアに感染	製油所から東海岸地 域への石油パイプラ インの数日間の操業 停止。75ビットコイ ン（500万ドル相 当）の支払いにより ネットワークへのア クセスを回復
26	2022	ウクラ	ロシアと関係があるとされるサイバー集団	ロシア軍の軍事行動

		イナ	Sandwormによる電力監視制御システムおよび送電網に対するサイバー攻撃	に合わせた停電惹起
--	--	----	---------------------------------------	-----------

上記諸事例の中には、攻撃の発信源が国家によるとされるものと非国家主体によるものがある。また、被害法益に着目しても、企業の機密情報の窃取、停電等による社会経済への影響、さらにはより深刻な大規模損害が発生する恐れがあった例が含まれており、その性質は多様である。これらの多様なサイバー攻撃に対して、国際法はどのように適用されるだろうか。本稿は、主としてエネルギー分野におけるサイバー攻撃を想定してサイバー空間における国際法の適用に関する議論状況や課題について概観する。

Ⅱ サイバー攻撃の法的評価と対応措置

1. 既存の国際法の適用の適否

サイバー攻撃に対して国際法をいかに適用して対処すべきかを巡っては、2000年代に入って議論が本格化した。国連は、2004年に、サイバー空間での責任ある国家の行動に関する政府専門家による議論の場として「サイバーセキュリティに関する国連政府専門家会合（国連サイバーGGE）」を総会第1委員会の下に設置した。同会合は、後述のように、2021年の最終報告書に至るまで数次にわたり報告書を作成している。

他方、NATOサイバー防衛協力センター(CCDCOE: Cooperative Cyber Defence Centre of Excellence)は、2017年に「タリン・マニュアル2.0」を公表した。同マニュアルは、個人資格で議論に参加した研究者・実務家によって作成されておりNATOの公式見解を示したものではないが、非公式に多数の国および国際組織から見解を聴取しつつ作成された経緯もあって、この分野における標準的な文書として広く参照されている。

また、上記国連サイバーGGEにはすべての加盟国が参加していたわけではないこともあって⁴、国連においては、全加盟国および国際組織やNGO等の関係ステークホルダーが広く参加可能な議論の場として、国連オープン・エンド作業部会(Open-ended Working Group(OEWG))が2019年に別途召集され、2021年には国連総会に最終報告書を提出している。

本稿では、サイバー攻撃に関する国際法の規律の現状と課題について、これら諸文書を参照しつつ整理するが、その前提として、国連における当初の議論においては、サイバー攻撃という新たな事象に対してそもそも既存の国際法枠組みを適用して対処すべきか自体が問われたため、この点について確認する。

当初、米国やヨーロッパ諸国、オーストラリアおよび日本は、サイバー攻撃に関して新たな条約の締結や法の「再発明」は不要であり、既存の国際法を適用すれば足りるとし、これ

⁴ 国連サイバーGGE 第6会期の委員は25カ国出身の政府専門家で構成された。

に対して中国・ロシア等は新たな規範が必要であると主張していた。両陣営の対立の焦点は、米欧日豪が既存のインターネット利用の自由やプライバシーの保護、民間ガバナンスの原則を重視するのに対して、中ロが国家によるインターネットの管理強化（いわばガバメント）を正当化する新たな規範の創出を目的とした点にあったとされる。ロシアが国連サイバーGGEというフォーラムがすでに存在した中でOEWGの開催を主導したのも、GGEでは新たな規範の作成について否定的な見解が多数を占めたため、新規範作成のための議論を改めて惹起する意図があったという⁵。

この対立については、国連サイバーGGE第3会期報告書（2013年）が、「平和・安全を維持し、開放的・安全・平和でアクセス可能なICT環境を推進するために、国際法、とりわけ国連憲章は〔ICT活動に〕適用されるし、その重要性は否定できない(is applicable and is essential)」⁶との参加国のコンセンサスを示したことで一応の決着をみた。国連サイバーGGE第4会期報告書（2015年）および第6会期報告書（2021年）も、この点を再確認している⁷。その上で、第4会期および第6会期報告書では、「責任ある国家行動に関する規範、規則および原則(norms, rules and principles)」と「国際法(international law)」について章を分けて取り上げ、後者においてより具体的に国際法がどのようにサイバー活動に適用されるかに関して一步踏み込んだ規定を設けた。第6会期報告書は概要以下の点をGGEのコンセンサスとして掲げている⁸。

- (a) ICTの利用をめぐる国際紛争の当事国は、国連憲章2条3項および第6章に従い、憲章33条に定める諸手段を通して平和的に当該紛争の解決を図らなければならない。
- (b) 国家主権および主権に由来する国際規範および原則は、国家によるICT関連活動および国家領域内のICTインフラに対する管轄権行使に関して適用される。既存の国際法上の義務が国家のICT関連活動に適用される。国家は、自国領域内のICTインフラに対して、とりわけ、政策と法令を整備し、ICT上の脅威からこれらインフラを保護するために必要なメカニズムを構築することを通して管轄権を行使する。
- (c) 不干涉原則に従って、国家はICT技術を用いて他国の国内管轄事項に対して直接的にあるいは間接的に干渉してはならない。

⁵ 赤堀毅『サイバーセキュリティと国際法の基本—国連における議論を中心に—』（東信堂、2023年）11-12頁。

⁶ Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, para. 19.

⁷ Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, para. 24; Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, para. 69. なお、第5会期は報告書の採択に至らなかった。

⁸ *Ibid.*, para. 71.

- (d) ICTの利用においては、国連憲章に従って、武力の行使または武力による威嚇を控えねばならない。
- (e) 国家は国際法に従い国連憲章で認められた措置をとる固有の権利を有する。この点についてはさらなる研究を要する。
- (f) 国際人道法は、武力紛争時においてのみ適用される。人道、必要性、比例性、区別原則等が、ICT利用に関してどのように適用されるかについてはさらなる研究を要する。
- (g) 国家は国際法上自国に帰属される国際違法行為に関して義務を果たさなければならない。国家は、私人に国際違法行為を行わせてはならず、また自国領域が非国家主体によって違法行為に使用されないように努めなければならない。もっとも、ICT上の行為が領域内で行われたことのみでは当該行為は国家に帰属せず、国家が違法行為を組織・実行したという主張は立証されなければならない。

国連OEWG最終報告書（2021年）も、GGE第4会期報告書が国連総会によって確認され、ICT利用の枠組みを確立したことに触れ、OEWGもこの基礎に立脚することを謳った⁹。

このように、国連での議論を経てサイバー活動に対しても既存の国際法規範の適用が肯定されるに至った。他方で、後述するように、より具体的にこれら諸原則をサイバー攻撃にいかに関適用し得るかについてはサイバー活動の特質に応じた種々の争点が存在する。では、具体的にはどのような議論がなされ、どういった課題が存在するのだろうか。以下では、サイバー攻撃を分類しつつ、それぞれの類型に当たる事態を想定して国際法の適用のあり方を検討しよう。

2. 武力攻撃／武力行使に該当するサイバー攻撃への対応

(1) 武力攻撃

国際法上、「武力攻撃(an armed attack)」に対しては、自衛権行使によって武力を用いて対応することが認められる。サイバー攻撃との関係では、まずサイバー上の攻撃が「武力攻撃」に当たるかが問題となるが、対象国においてその「規模と効果」の観点から一定の閾値を超える物理的破壊をもたらすサイバー攻撃は、武力攻撃に該当し、自衛権行使の対象となると一般に解されている¹⁰。日本においても、「どのようなサイバー攻撃であれば武力攻撃に当たるかについては、その時点の国際情勢、相手方の明示された意図、攻撃の手段、態様等を踏

⁹ Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, A/AC.290/2021/CRP.2, paras. 7-8.

¹⁰ Michael N. Schmitt ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (Cambridge University Press, 2017), p. 339; Ise-Shima Summit, Communiqué, G7 Principles and Actions on Cyber (2016), p. 1.

まえ、個別の状況に応じて判断すべきものと考えています。その上で、一般論として申し上げれば、サイバー攻撃のみであっても、例えば、物理的手段による攻撃と同様の極めて深刻な被害が発生し、これが相手方により組織的、計画的に行われている場合には武力攻撃に当たり得ると考えられます」との国会答弁が示されているところである¹¹。

ただし、個別状況を強調する上記答弁も示唆するように、武力攻撃に該当する「規模と効果」の具体的な閾値について国際社会に一致した見解があるわけではない。米国防省が作成した『戦争法マニュアル』では、例えば、原子力発電所のメルトダウンを引き起こす攻撃、人口密集地域の上流に位置するダムを決壊させる攻撃、航空管制システムに不具合を生じさせ航空機を墜落させる攻撃等が武力攻撃に含まれ得るとしており¹²、大規模な物理的損害を引き起こす攻撃を想定しているように思われるが、それ自体で直ちには物理的被害を伴わない軍の命令システムや防空システムの麻痺をもたらすサイバー攻撃がいかに評価されるか等、その外延については明らかではない。また、物理的な攻撃に先んじてサイバー攻撃が実施される場合、いかなる時点で武力攻撃の着手を認めることができるのかも問題となる。例えば、2007年にはシリアに建設中の核関連施設とみられる施設が、イスラエル空軍機の爆撃を受けて破壊されたが（表：事例5）、当該爆撃の際、事前にマルウェアに感染させられていたシリアの防空システムはイスラエル空軍機の飛来を探知できなかったという。そうした事例において、いかなる時点で武力攻撃の着手を認め得るのかは問題となろう。もっとも、武力攻撃の「規模と効果」の閾値や武力攻撃の着手時点をめぐっては、サイバー攻撃に限らず一般的にも議論がなされているところであるから、この点については既存の国際法の解釈問題とも評価できる。

他方で、仮に武力攻撃が発生したと評価し得る場合に、これに対する自衛権の行使としてキネティックな武力行使が可能かについては、米欧はこれを肯定し、ロシアはサイバー上の反撃のみが許容されると主張する。この点の合意が得られなかったことはGGE第5会期（2017年）が報告書の採択に失敗した要因の1つとされており、残された課題の1つである。

（2）武力行使

国際法上、上記の武力攻撃に閾値に達しない「武力行使（use of force）」に対して、被害国が何をなし得るかについても争いがある。タリン・マニュアル2.0は、「規模と効果」においてキネティックな武力行使に匹敵するサイバー攻撃は、国連憲章2条4項で禁止される武力行使に該当するとする¹³。もっともその具体的な閾値について合意はない。例えば、遠心分離機を破壊したStuxnetによるイラン核施設に対するサイバー攻撃事案（表：事例7）は武力の行使に当たると考えられるだろうか。また、ウクライナの原子力発電所の放射線モニタリン

¹¹ 安倍晋三総理大臣答弁、第198回国会衆議院本会議会議録 第24号（令和元年5月16日）13頁。

¹² U.S. Department of Defense, *Law of War Manual* (2015), para. 16.3.1.

¹³ Tallinn Manual 2.0, *supra* note 10, p. 330.

グシステムを機能喪失に至らしめたNotPetyaによるサイバー攻撃事案（表：事例19）のように、直接の物理的被害を発生させるわけではないサイバー攻撃はどうだろうか。同様に、例えば、銀行・証券システム、航空機・鉄道輸送、年金等の社会福祉制度、保健システム、配電網等に対してなされる物理的損害を生じない攻撃が武力行使に当たるかについて、どういった判断基準を設け得るかが問題となる。

また、仮に上記のようなサイバー攻撃を武力行使と評価し得るとして、これに対して、攻撃を受けた国がいかなる措置を講ずることができるかについても多くの整理すべき点がある。第1に、武力攻撃に至らない侵害に対し、自衛権の行使として必要最小限度の範囲内において武力を行使することが認められるかは一般国際法上も争点となっているが¹⁴、これをサイバー分野においてどのように解すべきだろうか。第2に、武力行使に対して比例性のある武力を用いた対抗措置をとることができるのかも、ニカラグア事件に関する国際司法裁判所（ICJ）判決をどう読むかを含めて一般国際法上の議論の延長として問題となる¹⁵。第3に、サイバー攻撃においては攻撃主体が直ちには判明しないことも想定されるが、そうした状況下で攻撃を排除するためにハックバック等を行うことは比例性のある反撃として認められるだろうか。第4に、武力攻撃に至らないサイバー攻撃に対し、反撃措置は、当該サイバー攻撃そのものを排除する限度（on-the-spot-reaction）に限られるか、再発防止を含めたより積極的な措置までとり得るか。第5に、サイバー攻撃に対し、物理的な攻撃で反撃することは可能か。仮に可能であるとして、比例性要件の充足をいかに考えるべきかも問題となる。

3. 国家による武力行使に至らないサイバー攻撃への対応

以上のように、どのようなサイバー攻撃が武力攻撃または武力行使に当たるか、それらに対してどのような対応が可能かについては未だ不明確な点が多く議論は続いている。もっとも、実際のサイバー攻撃は、武力行使に至らないと考えられるものが大半を占める。上記の国連サイバーGGE第6会期報告書における国際法原則(c)および(g)からも見てとれるように、そうしたサイバー行動が国家に帰属し、かつ違法な干渉に当たる等の理由によって国際法違反を構成すれば、攻撃国の国家責任が発生する。干渉とは、国家がその主権に基づいて自由に決定すべき事項に対して、他国が強制的な方法を用いて関与することを指す¹⁶。サイバー

¹⁴ 武力攻撃に至らない武力行使に対する自衛権行使の可能性について、東郷和彦外務省条約局長答弁、第143回国会衆議院外務委員会会議録第4号（平成10年9月18日）14頁。

¹⁵ ニカラグア事件本案判決は、仮にニカラグアがエルサルバドル等に対して武力行使を行なっていたとしても、これに対しては被害国による比例性のある対抗措置のみが正当化されるのであり、第三国である米国による、とりわけ武力行使を含むニカラグアに対する介入は正当化されないとするが（*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, I.C.J. Reports 1986, p. 127, para. 249）、当該判示は被害国による武力を伴う対抗措置を肯定する趣旨かが争われてきた。

¹⁶ *Ibid.*, pp. 107-108, para. 205.

手段を使用した脅迫によって、他国にその意思に反して何らかの行為を行わせる行為等は典型的な干渉に当たろう。もっとも、サイバー行動の国家への帰属を立証することは往々にして困難であり、また、仮に立証できる際にも探知能力・手法を秘匿するために立証過程の詳細を明かすことに躊躇する国も多いとされる¹⁷。

仮に国際法に反するサイバー行動が国家に帰属することを立証し得た場合には、国家責任が生じ、当該国が違法行為を行ったことを認めて違法なサイバー行動を停止し、発生した損害を賠償すれば事態は解決に向かう。しかし、違反の事実や責任を国が認めない場合には、被害国には一定の条件の下で対抗措置に訴えることが認められることになる。対抗措置についてはGGE報告書では明記されなかったが、サイバー空間における責任ある国家の行動に関するG7ルッカ宣言（2017年）は、「国際違法行為の被害者である国家は、一定の場合には、その違法行為について責任を有する国家に国際的な義務を遵守させるために、当該責任を有する国家に対して均衡性のある対抗措置（ICTを介して実施する措置を含む）及びその他の合法的な対応をとることができる」とする¹⁸。タリン・マニュアル2.0規則24も同様に被害国が対抗措置をとることを肯定している¹⁹。

サイバー攻撃に対して被害国がサイバー上の対抗措置をとる場面を想定すると、各国の技術的差異が問題となる可能性がある。一般国際法上、第三国による対抗措置が可能かについては議論があるが、例えば、サイバー攻撃を受けた国が、法的には均衡の取れた対抗措置を講じ得るにもかかわらず、そのためのサイバー関連能力を有しない場合、第三国による技術的援助が可能か否かは問題となろう。

4. 非国家主体によるサイバー攻撃への対応

(1) 相当の注意義務を介した国家責任追及

サイバー攻撃が非国家主体によって行われたとしても、これがいずれかの国家の指示による場合もある。もっとも、侵害行為の国家への帰属を証明することは往々にして困難である。また、そもそも国家の意思とは関係なく私的主体がサイバー攻撃を行うことが実際には多い。これらの場合において、非国家主体の行為自体の国家への帰属を証明できなくとも、「国家は、領域主権の行使により、その国家領域をみずから使用しまたは私人にその使用をゆるすにあたっては、他国の領域その他の国際法上の権利を害する結果にならないよう、一般国際法上、特別の注意義務を課される」²⁰とする「領域使用の管理責任」に基づいて、侵害行為

¹⁷ サイバー行動に関する立証問題については、Sharngan Aravindakshan, “Cyberattacks: A Look at Evidentiary Thresholds in International Law,” *Indian Journal of International Law*, Vol. 59 (2021), pp. 285-299.

¹⁸ G7 Foreign Ministers’ Meeting in Lucca, G7 Declaration on Responsible States Behavior in Cyberspace (2017), p. 2.

¹⁹ Tallinn Manual 2.0, *supra* note 10, p. 130.

²⁰ 山本草二『国際法〔新版〕』（有斐閣、1994年）275頁。

に利用されるサイバーインフラが領域内に所在する領域国に相当の注意義務を負わせることを介して関係国の国家責任を問うことができないかが議論されている。

上記の国連サイバーGGE最終報告書は、国際法原則(g)において領域管理責任に言及するが、「国家は自国領域が非国家実体によって国際違法行為のために使用されないよう確保に努める(should seek to ensure)」として、法的義務性については曖昧な書き振りをとっていた。これは、領域使用の管理責任に基づく「相当の注意義務」が国家に過大な負担を強いることを危惧する国があったためであるが、ジェノサイド防止義務についてさえ、ICJは「自国にとり得る(within its power)すべての措置をとったか」という枠組みで判断をしていることからわかるように²¹、相当の注意義務は、国家に合理的に要求し得ないことまで要求しない。領域国は自国のサイバー能力の範囲内において、自国領域内の非国家主体が他国・他国民に対してサイバー攻撃を行わないように相当の注意を払えば良いことになる²²。

タリン・マニュアル2.0においては、規則6および7に相当の注意が義務として規定されている。規則6は、「国家は自国領域や自国のコントロール下の領域ないしサイバーインフラが他国の権利に影響を与えこれに深刻な結果をもたらすように利用されないように相当の注意を払う義務がある」²³とする。ここでは義務性が確認された上で、領域に加えて管轄下の行動も対象に加えられている。その上で、規則7は、「相当の注意原則は、他国の権利に影響し、深刻な結果をもたらすサイバー活動を停止させるために、状況において可能なあらゆる手段をとることを国家に要求する」²⁴とその内容を具体化し、求められる注意の程度が対象国のサイバー能力によって変わり得ることを確認する。

なお、領域使用管理責任については、サイバー空間の接続性から、サイバー空間を介した侵害行為の経由国がどのような責任を負うかが問題となる。仮に各国がその領域内のサイバーインフラを通過するだけの侵害行為に対して責任を持つとして、その場合の責任は侵害行為の発信源が所在する国と同程度か等については検討が必要であろう。

(2) 非国家主体に対する管轄権行使

非国家主体によるサイバー攻撃に対しては、これを特定の国家と結びつけるのではなく、私人による犯罪行為として捉え刑事処罰を行うという対応も考えられる。この場合、複数国が関係し得るというサイバー犯罪の特徴に応じて、いずれの国が捜査や訴追等の管轄権を行使し得るかが問題となる。

²¹ Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 221, para. 430.

²² サイバー攻撃と相当の注意義務について詳しくは、拙稿「サイバー・セキュリティ事案における『相当の注意』義務」浅田正彦ほか編『現代国際法の潮流 II』（東信堂、2020年）301-316頁参照。

²³ Tallinn Manual 2.0, supra note 10, p. 30.

²⁴ Ibid., p. 43.

このうちサイバー上の捜査活動については、2001年に締結されたサイバー犯罪に関する条約（サイバー犯罪条約：ブタペスト条約）およびその附属議定書（コンピュータ上のヘイトクライムに関する2003年第1追加議定書；協力強化および電子的証拠の開示に関する2021年第2議定書）が一定の規律を定めている。もっとも、同条約は、データにアクセスする権限を持つ者の「合法的なかつ任意の同意」がない場合に、他国領域内のコンピュータに蔵置されているデータに越境アクセスを伴う捜査をなし得るかについて、条約策定時には実行が少なく不明確であるとして規定を置かなかった²⁵。また、「犯罪が自国の領域内で行われる場合」に当該国による裁判権行使を想定するが（22条1(a)）、そもそもサイバー上の行為については、いずれの国の領域で発生したか自体が解釈問題となる。さらに、同条約の当事国は2024年5月末現在で72カ国であるから、非当事国が行う、あるいは非当事国に所在するデータに関する越境捜査やサイバー犯罪の訴追は、いずれにせよ一般国際法に基づいて評価すべき問題となる。

では、一般国際法上、サイバー犯罪に対する管轄権行使はどのように理解すれば良いか。第1に、一般国際法上、犯罪捜査等を含む執行管轄権は、外国領域において行使できないとされる。国連サイバーGGE最終報告書の国際法原則(b)では、「国家領域内のICTインフラに対する管轄権行使」への言及がある。確かにサイバーインフラに着目すれば、それが設置されている領域国を特定することができ、当該国の同意なしにサイバーインフラにアクセスし証拠収集等の執行管轄権を行使することは違法な執行管轄権行使の域外適用と考えることもできるかもしれない。しかし、サイバー犯罪の捜査において主たる搜索対象となるのは物理的な機器自体というよりもデジタルデータであろう。とりわけ、クラウド上のデータについては、いずれの国家内のストレージに所在するかは往々にして不明であるし、複数国に所在する複数のストレージに分有されていることも多く、特定の「領域国」との結びつきは希薄である。外国領域における執行管轄権行使が禁止される理由が、領域国の排他的統治権を害することの禁止にあるとすれば、そもそも特定の領域国の管轄と排他的に結びついていないという側面を持つデジタルデータについては、執行管轄権行使の限界をどのように捉えれば良いのかという問題が浮上するのである²⁶。

第2に、域外で行われたサイバー犯罪の訴追については、立法管轄権およびこれを前提とした司法管轄権行使の射程の問題となる。立法管轄権の行使範囲については、当該国が事案の性質に照らして密接な関連を持ち管轄権を行使することが合理的かという枠組みで捉える

²⁵ Council of Europe, Explanatory Report to the Convention on Cybercrime (2001), para. 293.

²⁶ 詳しくは、拙稿「越境サイバー対処措置の国際法上の位置づけ」国際法研究 14 号（2024 年）62-67 頁。

ことができる²⁷。その際の考慮要因の1つとして、管轄権行使が他国の政策実現を害する程度が検討されるが、この点については国家がそもそもサイバー活動について持つ管轄権の内容が関係する。例えば、関係する国の間でサイバー政策に根本的な差がなく、問題となるサイバー犯罪を訴追することを等しく望むのであれば、訴追の意思と能力を持つ国がこれを行うこともサイバー犯罪の国際的な抑圧という観点からは合理的と考える余地が生じるだろう。

Ⅲ サイバーセキュリティの回復措置

以上に確認したように、サイバー攻撃に対しては、それが武力攻撃に当たれば自衛権行使による対応が認められ、武力攻撃に満たない武力行使に対しては武力によって対抗することの是非およびその根拠について議論が続いている。国家に帰属するサイバー攻撃や国家が領域国としての管理責任を怠った結果発生したサイバー攻撃に対しては、当該国の国家責任を追及し、対抗措置をとることが想定され、サイバー攻撃を行なった私人を犯罪者として処罰することも考えられる。

もっとも、責任追及や関係者の処罰といった後者の措置は事後的な対応にとどまる点で限界を有する。対抗措置も違反国に対して責任を認めて賠償を行うように、あるいは相手国が義務違反や責任を認めないのであれば、適切な紛争解決手続を利用するように圧力をかける間接強制としての性質を持つものである。これに対して、サイバー攻撃が続いている場合には、まずはこれを遮断し、サイバーセキュリティを回復することが現実にはより重要であろう。その一環として、外国に所在する攻撃発信元に対してハックバック措置をとることが、領域国の管轄権を侵害する場合は、国際法上はそうした対応措置が緊急避難として例外的に正当化されるかという問題となる。

国連国際法委員会が作成した国家責任条文25条は、「重大かつ差し迫った危険(a grave and imminent peril)」から「根本的利益(an essential interest)」を守るために、国は緊急避難を援用して行動できることを規定しているが、サイバー空間を通じた侵害のうち、いかなるものが上記に該当すると考えられるだろうか。緊急避難について定めるタリン・マニュアル2.0規則26に付されたコメンタリーは、「根本的利益」について国際法上定まった見解はないとしつつも、防空システム、銀行・証券システム、航空機・鉄道輸送・電力供給等に関するインフラ、社会福祉・保健制度といった、国の安全保障・経済・公衆衛生・治安・環境等を支える重要インフラに深刻な被害が生じた場合をその例として挙げる²⁸。

では、そうした重要インフラへのサイバー攻撃に直面した国は、攻撃元コンピュータ等に

²⁷ 国家管轄権に関する考え方については、拙稿「国家管轄権の『域外適用』再考」日本エネルギー法研究所編『エネルギーに関する国際取決めの法的問題の諸相－2017～2018年度 エネルギーに関する国際取決めの法的問題検討班報告書－(JELI-R-No.154)』（2023年）143-158頁。

²⁸ Tallinn Manual 2.0, *supra* note 10, p. 136.

対してどのような範囲でハックバック措置をとることができるだろうか。国家責任条文26条では、緊急避難の法理によっても、強行規範たる武力不行使原則違反を正当化することはできないとされているが、タリン・マニュアル2.0においては、武力を用いた緊急避難措置が許されるか否かについて、合意に至らなかったとされる。サイバー攻撃を阻止する方法として、発信源のサイバーインフラを破壊することが不可欠であり、当該措置が武力行使と見做される場合、緊急避難によってそうした措置が正当化され得ると解するのかが問題となる。また、第三国に所在するサイバーインフラを経由してサイバー攻撃が行われ、当該攻撃を排除するためには、当該第三国に所在するサイバーインフラを破壊する必要がある場合、サイバー攻撃の被害国は、緊急避難を援用して当該インフラを破壊することができるかも問題となる。

IV むすびに代えて

本稿は、サイバー攻撃が発生した場合を念頭に置いて、国際法上、そうした攻撃がどのように評価され、被害国にはいかなる対応が認められるかについて整理した。その結果、サイバー攻撃とそれへの対応は、概ね既存の国際法の枠組みに照らして位置づけ得ること、しかし、サイバー上の攻撃とこれへの対応であることの特質に起因して解釈・適用上の多くの課題が存在することが確認された。

上記の国際法上の枠組みは、基本的にサイバー攻撃を受けた国家による対応を中心に構築されている。もっとも、エネルギー産業に対するサイバー攻撃は、まず第一に事業者に対して向けられるものである。サイバーセキュリティの維持・回復における事業者の役割はどのように位置づけられるだろうか。むすびに代えて、日本におけるサイバーセキュリティ対策を概観することを通して、この点について最後に確認しよう。

日本においては、2014年にサイバーセキュリティ基本法（平成26年法律第104号）が採択された。同法は、「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者」を「重要社会基盤事業者」と位置づけ（3条1項）、これら事業者に対して、「基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努める」ことを義務づける（6条）。また、政府は、重要社会基盤事業者におけるサイバーセキュリティの確保の推進に関する事項を含むサイバーセキュリティ戦略を定めることとされ（12条）、重要社会基盤事業者におけるサイバーセキュリティに関し、基準の策定、演習および訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずることも国の責務として定められた（14条）。同法に基づき、内閣サイバーセキュリティセンター

(NISC)では、サイバーセキュリティ戦略および重要インフラのサイバーセキュリティに関する行動計画等を作成し、サイバーセキュリティの確保を事業者に促している²⁹。同行動計画では、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油および港湾を重要インフラサービスと位置づけ、これらに関与する事業者をサイバーセキュリティ上の重要社会基盤事業者（重要インフラ事業者）と指定する³⁰。重要インフラ事業者には行動計画に沿った一定のサイバーセキュリティ対策が求められることになる³¹。

電力分野においては、「事業用電気工作物を設置する者は、事業用電気工作物を主務省令で定める技術基準に適合するように維持しなければならない」と定める電気事業法39条1項を受け、電気設備に関する技術基準を定める省令15条の2が、「事業用電気工作物（小規模事業用電気工作物を除く。）の運転を管理する電子計算機は、当該電気工作物が人体に危害を及ぼし、又は物件に損傷を与えるおそれ及び一般送配電事業に係る電気の供給に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成26年法律第104号）第2条に規定するサイバーセキュリティをいう。）を確保しなければならない」とする。

セキュリティ対策としては、日本電気技術規格委員会(JECS)が定めた「電力制御システムセキュリティガイドライン」（2016年）や「スマートメーターシステムセキュリティガイドライン」（2016年）が存在し、また、2017年には電力ISAC(Information Sharing and Analysis Center) (JE-ISAC)が設立された。電力ISACは、電力10社、大規模発電業者等27社、日本卸電力取引所および電力広域的運営推進機関で構成され、セキュリティインシデントやベストプラクティスに関する情報共有を行っている。さらに、2018年には日欧米でMOUを締結し連携して情報収集・分析に当たっている。

上記の電力インフラのサイバーリスク対策は、基本的に平時におけるサイバーセキュリティの維持を念頭に置いて、サイバー攻撃に対する耐性を高める事業者の責任を定めている。もちろん、サイバー攻撃の大部分は、私人によって平時に行われる犯罪行為であり、これに対して備えることは極めて重要である。しかし、表（事例7, 15, 22, 23, 26）でも見たとおり、電力インフラは有事を含め外国からの攻撃対象となることも想定される。そうしたリスクに対して、事業者と国の責任分担をどう考えるのかは今後の課題であろう。仮に事前防護措置をとったにも関わらずサイバー攻撃の被害に遭った際に、国と事業者の間で対応措置や生じた損害に対する費用負担等はどのように分担すべきだろうか。より具体的には、例え

²⁹ 最新の行動計画等については、NISC Web サイト(<https://www.nisc.go.jp/policy/group/infra/index.html>)を参照。

³⁰ サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」（2022年6月17日）別紙1。

³¹ 重要インフラ事業者が取り組むべき事項について詳しくは、同上、36-37頁。

ば、サイバー攻撃を受けた際に、事業者としては、事業内ネットワークを外部から遮断したり、侵入されたウィルスを駆除したりしてさらなる被害を防ぐことは当然として、攻撃元の特定や証拠収集、盗取されたデータの無効化等のためにハックバック措置をとることも認められるべきだろうか³²。また、自前で十分なサイバーセキュリティ対策をとる体力のない事業者や能力があっても十分な対策を取らない事業者が攻撃対象となった場合、これら事業者の責任をどう解するべきか。サイバーセキュリティ対策についての議論が進む米国では、権限を持つ連邦政府とサイバー対応能力を持つ事業者を含む私的セクター間の協働によって攻撃に対処する必要性が強調されているが³³、日本においても国と事業者の責任分担のあり方についてより詳細な検討が望まれる。

（追記）本稿脱稿後に、中村和彦『越境サイバー侵害行動と国際法——国家実行から読み解く規律の行方——』（信山社、2024年）に接した。また、第217国会（2025年）において「重要電子計算機に対する不正な行為による被害の防止に関する法律」が可決・成立し、日本においても官民間の情報共有によるサイバー攻撃事案の未然防止、対処支援強化等が図られるに至った。

³² 米国では、2019年に、民間のサイバー攻撃被害者が自ら自己ネットワーク外でのハックバック措置をとることを正当化する Active Cyber Defense Certainty Act 法案が提出されたが（法案については、<https://www.congress.gov/bill/116th-congress/house-bill/3270> 参照）、正確なトラックバックが行われない可能性や第三者に被害を与えた場合の対処、正当な自衛の範囲の確定等の難点から廃案となっている。Jen Ellis, “Hack Back is Still Wack,” at (<https://www.rapid7.com/blog/post/2021/08/10/hack-back-is-still-wack/>).

³³ The White House, *National Cybersecurity Strategy* (2023), p. 15.

第 7 章

行政法の域外適用と執行管轄権

京都大学大学院教授
原田 大樹

I はじめに

グローバル化の進展とともに、国内法学と国際法学の対話がさまざまな場面で進んできた。その中で、例えば条約の国内実施の議論をめぐっては、問題関心に齟齬があることや、立憲化（憲法）、民主政、国家責任、執行といった両法分野の基本概念に類似性とともな相違点があることが明確化してきた。本稿が取り上げる国家管轄権も、その一例である。国家管轄権とは、「国家がその国内法を一定範囲の人、財産または事実に対して具体的に適用し行使する国際法上の権能」¹とされ、作用面での態様の違いに着目して、立法（規律）管轄権、執行管轄権・司法管轄権（強制管轄権）に区分され、また適用基準の分類として、属地主義（主体的属地主義・客体的属地主義²・効果理論）、属人主義、保護主義、普遍主義などが挙げられることが多い。そして、立法管轄権については、領域主権との緊張関係の弱さ³から、民事法については特に制約はなく、刑法・行政法については正当な根拠・事案との真正の連関がある場合に限り域外適用できるとされてきた。これに対して、執行管轄権については、原則として属地主義であり、他国領域内での執行管轄権は相手国の同意がないと行使できないとされる⁴。

ここで問題は、行政法学の基本的概念である「公権力の行使」と執行管轄権とが、どのような関係に立っているかである。政府見解によれば、公権力の行使とは「法令に基づく権限による職務行為である」⁵とされ、実務上は執行管轄権と公権力の行使概念をほぼ同義に扱っているように見える。もっとも、両者には差異があり、一般性と個別性の側面及び法的行為と事実行為の側面にその特色が見られる。そこで本稿では、この2つの観点から、公権力の行使と執行管轄権の概念を検証し、両者の差異を解明することとしたい。具体的には、まず、国内法学の「公権力の行使」の意味内容を、一般性・個別性の軸と、法的効果の有無の軸から提示する（Ⅱ公権力の行使の外延）。次に、国際法学の「執行管轄権」を、実施・執行の観点と物理的実力行使の要素から整理する（Ⅲ執行管轄権の内包）。そして、国内法学の「公権力の行使」と国際法学の「執行管轄権」の相互関係について、立法・規律・実現の3つの段階に着目して検討する（Ⅳ公権力の行使と執行管轄権）。こうした作業を踏まえて、執行管轄権の内容に関する暫定的な結論を提示することとしたい（Ⅴおわりに）。

¹ 山本草二『国際法【新版】』（有斐閣、1994年）232頁。

² この概念につき参照、岩沢雄司『国際法（第2版）』（東京大学出版会、2023年）172頁（「主観的属地主義」「客観的属地主義」の語を用いる基本書が多い）。「行為地基準」と「効果発生地基準」の語を用いるものとして、高橋宏司「証券関係法規の規律管轄権とICO(Initial Coin Offering)」国際法外交雑誌117巻4号（2019年）693-717(711-712)頁。

³ 柳原正治ほか編『プラクティス国際法講義（第3版）』（信山社、2017年）139頁[兼原敦子]。

⁴ 小寺彰ほか編『講義国際法（第2版）』（有斐閣、2010年）174頁[中川淳司]。

⁵ 第71回国会衆議院外務委員会第35号「会議録」[松永信雄発言]（1973年9月12日）5頁。

Ⅱ 公権力の行使の外延

1. 一般性と個別性

公権力の行使の定義は学説上独自になされているというよりも、東京都ごみ焼却場事件の最高裁判決の定式である「公権力の主体たる国または公共団体が行う行為のうち、その行為によつて、直接国民の権利義務を形成しまたはその範囲を確定することが法律上認められているもの」⁶を用いている。公権力の行使の典型は、申請に対して許認可を与える、あるいは食中毒を出した店に対して営業停止命令や改善命令を出す不利益処分といった行政行為と呼ばれるものである。逆に、公権力の行使ではないものとして行政法学が通常考えているのは、立法や行政基準（政省令等）あるいは条例のような抽象的な内容の規範定立である。その理由は、それらが最終的な決定であるという意味での成熟性を持たないからである。法律や条例等によっても権利義務関係は変動しているものの、それは最終的な確定ではなく、最終的には行政機関がそれらに基づいて一定の判断を下し、それを前提に例えば義務履行強制等がされる過程をたどる。そこで、法的な意味での最終的決定の段階まで待って、それを公権力の行使=処分と捉える理解が一般的である。換言すれば、一般的・抽象的なものは公権力の行使ではなく、個別的・具体的な性格が必要であるとするのが、取消訴訟のような行政訴訟の場面における公権力の行使の意味である。

これに対して、違法な行政活動に対する金銭賠償である国家賠償の方にも同じ公権力の行使という言葉が使われているものの、こちらはより広く「国の私経済作用及び国家賠償法2条の対象となるものを除く全ての活動」⁷の意味で用いられており、一般性・個別性という区別はない。もちろん、国家賠償法の違法性の判断の時に当該行為が一般的かどうかという要素は考慮されており、一般的な活動の場合には違法性を肯定する条件が厳しくなる。しかし、少なくとも国家賠償法における「公権力の行使」という言葉の中には、一般性・個別性の区別がない。なぜこのような違いが生じているかは様々な説明があり得るものの、救済の手段が行政訴訟の場合には違法行為の是正で、その活動自体を取り除くということであるのに対して、国家賠償の場合にはその活動の法的効果はそのまま金銭的に決着を付けるだけというところが異なっており、その結果、救済のタイミングとしても、国家賠償は違法行為が生じてから時間が経った段階で最終的な法的責任を問うという性格を持っているところに理由があると思われる。

2. 法的行為と事実行為

公権力の行使に関するもうひとつの判断要素は、法的行為と事実行為という側面であり、権利義務関係を変動させるのか、それとも物理的な実力の行使なのかという点である。行政

⁶ 最一小判 1964（昭和 39）・10・29 民集 18 卷 8 号 1809 頁。

⁷ 塩野宏『行政法Ⅱ（第 6 版）』（有斐閣、2019 年）324 頁。

法学では、法的な行為でないものを「事実行為」としてきた。その結果、残余概念である事実行為には極めて雑多なものが含まれることになる⁸。事実行為はその定義上、法的な行為ではないのだから、権利義務関係を変動・確定させないことになるので、法学的にアプローチする必要はないようにも思われる。もっとも、少なくとも権力的事実行為と呼ばれるものだけは、公権力の行使に当たるものとこれまで理解されてきた。旧行政不服審査法2条1項では、公権力の行使に当たる事実上の行為の存在が明示されており、人の収容、物の留置その他その内容が継続的性質を有するものも公権力の行使であるとされていた。現在の行政不服審査法にはこの規定はないものの、同法46条1項に「処分（事実上の行為を除く）」という表現が見られることから、処分の中には事実上の行為もあるということは現在も前提となっている。そして、物理的な行為は、受忍義務と結びつかない限りは、原則として処分性を否定するのが国内法上の理解と考えられる。例えば、権力的事実行為の典型である即時執行（即時強制）や武器の使用、行政代執行等はいずれも、相手方に受忍義務を課しているから公権力の行使に当たるとされる。あるいは、厚木基地訴訟最高裁判決⁹は、自衛隊の飛行機の飛行が権力的事実行為であることを根拠に処分性を認めた判決で、これもやはり（ある種の）受忍義務があることを理由にしている。

これに対して、国家賠償法における公権力の行使での事実行為の扱いは、基本的には2条の問題だと理解されている。物理的事実行為のほとんどが公共事業や公共施設の供用の場面で問題となるものであり、これらはいずれも公の営造物の設置・管理の瑕疵として構成できる。そして、そのように構成できないものについては、同法1条1項の公権力の行使に関する広義説に従って、幅広く公権力の行使に含められている。

Ⅲ 執行管轄権の内包

1. 執行概念の複合的性格

執行という言葉は、国内法では大別すると次の2つの意味で使われている。第1は、行政基本決定と行政執行活動という区別を前提とする「執行」である¹⁰。これはアメリカの行政学・行政法で言われている政策決定と政策実施という区別（policy-makingとpolicy-implementationの区別）とも対応している。法律や行政基準のような一般的な形での決定を行政基本決定と呼び、それを特定の名宛人に対して内容を具体化したものを行政執行活動としている。ここでの執行は、個別的・具体的な活動という意味で使われている。これに対して、enforcementの意味で「執行」が語られることがある。ここでの執行は、義務履行確保と

⁸ 高木光「事実行為」同『事実行為と行政訴訟』（有斐閣，1988年）1-32(1)頁[初出1984年]。

⁹ 最一小判1993（平成5）・2・25民集47巻2号643頁（第1次厚木基地訴訟），原田大樹「訴訟類型論の現在—処分なき行政訴訟の理論的課題」同『公共紛争解決の基礎理論』（弘文堂，2021年）155-189（166-168）頁[初出2020年]。

¹⁰ 小早川光郎『行政法（上）』（弘文堂，1999年）50-51頁。

言い換えることができ、行為の性格が個別的かというよりはむしろ、権利義務関係が確定された後にそれを「現実化」するための手段という要素に焦点が当てられている。

そして、この2つの意味の対立が、立法管轄権の理解にも影響を与えているように見える。立法管轄権の代表的な定義では、「国内法令を制定して」という法令の制定という要素と、合法性の有無を認定する権限¹¹という要素—個別的・具体的に合法であることを認定する権限—も含まれているように見える。もともと行政概念は残余概念—全ての国家作用から立法と司法を引いたもの—という控除説的な理解が学説では一般的であることを前提とすると、立法管轄権との関係では執行管轄権が残余概念だと考えるべきかもしれない。つまり、立法管轄権を法規範の定立と理解すると、個別的な執行活動が執行管轄権の内容となる¹²。そうではなく、立法管轄権には合法性に関する認定権限まで入っていると考えれば、その残余概念が現実化、つまり実力による義務履行強制が執行管轄権の問題となる¹³ので、**enforcement**が執行管轄権の内容として理解されることになる¹⁴。もっとも、こうした区別よりも、現実の行政事務を重視していると読むことができる記述もある¹⁵。すなわち、現地の国内法上、国家機関の専属権能である場合について、他国が執行管轄権を行使すると国際法違反になると説明されており、郵便業務もここに含まれている。

2. 観念的な実力行使?

執行に関するもうひとつの問題は、それが法的なものか、あるいは事実に・物理的なものかという点である。執行管轄権に該当するものとしてよく言及されるのは、武力行使・武器使用、犯罪捜査、逮捕、強制力を伴う行政調査であり、これらのように国家がまさにその物理的な実力を行使する作用が執行管轄権に含まれているということは共通の理解と言ってよいだろう。しかし、その実力の行使が本当になされるのか不確定なものを執行管轄権に含めるかは、不透明である。例えば、刑事罰を背景とする行政調査は、調査への不協力に対して刑事罰が科されれば確かに実力行使ではあるものの、刑事罰は心理的な強制のために用いられることがほとんどで、実際に刑事罰が行使されることはあまり想定されない。あるいは、刑事罰をそもそも背景としないような任意の調査であっても、相手国への立入行為を伴う場

¹¹ 山本・前掲注(1)232頁。

¹² 小松一郎『実践国際法(第3版)』(信山社, 2022年)23頁。

¹³ 村瀬信也「国際法における国家管轄権の域外執行——国際テロリズムへの対応——」同『国際法論集』(信山社, 2012年)171-202(172)頁[初出2006年], 柳原正治『国際法(改訂版)』(放送大学教育振興会, 2019年)85頁。白石忠志『独占禁止法(第3版)』(有斐閣, 2016年)178頁注128は、違反要件に関する問題を「規律管轄権」、エンフォースメントに関する議論を「執行管轄権」とする。

¹⁴ 松下満雄「独占禁止法の域外適用」経済法13号(1970年)17-20(17)頁は、立法管轄権を「国家の立法権ないし立法による規制権」とし、法の施行をする権限を手続管轄権と整理する。

¹⁵ 山本草二「国家管轄権の域外適用」ジュリスト781号(1983年)196-202(199)頁は、現地の国内法上国家機関の専属権能である場合について他国が執行管轄権を行使すると国際法違反であるとし、その具体例として徴税・訴訟手続・徴兵・検疫・郵便業務を挙げている。

合には、国際法的には執行管轄権に含まれるとする理解も有力である¹⁶。さらに、サイバー攻撃や民間主体を通じて国が他の国の事業者の情報を収集させる手法¹⁷、あるいは司法取引のようにインフォーマルな解決を図るものについても、執行管轄権の行使に含まれる可能性がある¹⁸。

国際法のこうした議論動向は、国内法学から見ると、実力の行使からその法的な効果に注目する方向に転換しているとも評価できる。刑事罰を背景とする行政調査が執行管轄権に入っているという理解は、出発点としては刑事罰という実力行使の存在を根拠としているものの、実際には刑事罰を他国の公務員がやってきて実際に科すことはあり得ないので、結局その対象となっている行政調査に受忍義務が発生していることを理由に執行管轄権の問題と理解できる。あるいは、訴状の送達についても、裁判所の職員が物理的に訴状を持ってくるという意味で執行管轄権に含まれると解するのではなく、訴訟手続上の一定の法的効果が生じるところを根拠としているように思われる。さらに、サイバー攻撃についても、被害が甚大というところを重視して武力行使に相当するという議論¹⁹もあり得るものの、「相当の注意義務」という国家の注意義務違反に着目する議論²⁰は、その法的効果に注目して執行管轄権を判断しているようにも見える。

IV 公権力の行使と執行管轄権

1. 立法と規律

以上の議論状況を前提に、国内法学における公権力の行使と国際法学における執行管轄権とを比較する。まず、立法と規律の関係である。国際法学では、立法管轄権ではなく規律管轄権という用語も用いられる。立法管轄権という言葉は、国家作用が立法、司法及び行政に分かれていて、それぞれが立法機関、行政機関及び司法機関によって担われているという前提に立つのに対して、誰が担当しているかではなくその作用にのみ注目する見解—行政機関や裁判所も、法がどのようなものであるかを記述することができることを重視する立場から

¹⁶ 竹内真理「国際法における国家管轄権行使に関する基本原則」鶴田順編『海賊対処法の研究』（有信堂高文社、2016年）83-97(86)頁。「任意の事情聴取や訴状の送達等の物理的強制力を伴わない公権力の行使も執行管轄権概念に含まれる」（黒崎将広ほか『防衛実務国際法』（弘文堂、2021年）188頁〔西村弓〕）。

¹⁷ 竹内真理「サイバー捜査と国家管轄権」ジュリスト 1547号（2020年）73-78(76)頁。

¹⁸ 竹内真理「国内法の拡張的適用を制約する判断枠組みについての一考察—米国の外国腐敗行為法（FCPA）の実践を素材として」芹田健太郎ほか編・安藤仁介先生追悼『実証の国際法学の継承』（信山社、2019年）307-322(314)頁。

¹⁹ サイバー攻撃に対する自衛権行使の可能性につき参照、黒崎将広「サイバー空間における主権——その論争が意味するもの」森肇志=岩月直樹編『サブテキスト国際法』（日本評論社、2020年）31-43(37)頁、同ほか『防衛実務国際法』（弘文堂、2021年）240-244頁〔森肇志〕。

²⁰ 西村弓「サイバー・セキュリティ事案における『相当の注意』義務」浅田正彦ほか編・坂元茂樹先生・薬師寺公夫先生古稀記念『現代国際法の潮流Ⅱ』（東信堂、2020年）301-316(304)頁。

は、法がどのようなものであるかを形成し確定することを規律と呼び²¹、国家管轄権の一つとして規律管轄権を挙げている。立法管轄権と規律管轄権を同義に用いる理解²²もあるものの、あえて両者の違いを挙げるならば、立法管轄権は国家「作用」としての立法と立法府という「組織」の両方に注目しているのに対して、規律管轄権はもっぱら規律「作用」のみを考慮し、国家機関のうちそれをどこが担当しているかは重視していない。そうすると、規律管轄権の内容が広がった分だけ執行管轄権が狭くなり、物理的な強制作用だけが執行管轄権に残ることになる²³。

行政法学の側でも、行政行為（処分）について、それが「規律」であると理解をする見解が2000年代以降一般化してきている²⁴。この発想を規律管轄権と直結させると²⁵、行政行為の域外適用に関する法制度設計の議論にも大きな影響を与えることになる²⁶。現在の日本法では、おおむね次の4つの類型が用いられている。

第1の類型は、国内に代表者・代理人を置くという方法である。電気通信事業法が2020年の改正でこのようなしくみを盛り込んでおり、登録制度の中で、外国法人について国内における代表者・代理人を申請書に書くように求める規定が設けられている。また、条文上は明確ではないものの、個人情報保護法の2020年の改正では、個人情報保護委員会の行政指導の中で代理人を置くように指導をすることがある程度予定されているようである²⁷。この場合には、国内に一定の連結ポイントを置いておき、その代表者又は代理人に対して、国内と全く同じように執行活動を行うことができるので、執行管轄権の問題が表面化することはあま

²¹ 酒井啓亘ほか『国際法』（有斐閣、2011年）85頁[寺谷広司]。

²² 松尾直彦『金融商品取引法（第6版）』（商事法務、2021年）93-99頁、田宮寿人「行政法の域外適用に関する立法政策上の諸論点——個人情報保護法・令和2年改正の視点から——」情報法制研究8号（2020年）63-74(65)頁。

²³ 野村美明「域外適用の法と理論——国際法と国内法の交錯」阪大法学（大阪大学）190=191号（1997年）971-1002(974)頁、金井貴嗣「域外適用によって生ずる独禁法上の問題」法学新報（中央大学）105巻6=7号（1999年）207-232(212)頁、中川丈久「行政法の域外適用」神戸法学雑誌（神戸大学）32号（2019年）173-210(181)頁、竹内真理「個人情報保護法改正における域外適用の在り方」法律のひろば73巻10号（2020年）33-41(39)頁。

²⁴ 山本隆司「訴訟類型・行政行為・法関係」民商法雑誌130巻4=5号（2004年）640-675(648)頁、太田匡彦「行政行為——古くからある概念の、今認められるべき意味をめぐって」公法研究67号（2005年）237-251(238)頁。

²⁵ 中川丈久「行政法の体系における行政行為・行政処分の位置付け」高木光ほか編・阿部泰隆先生古稀記念『行政法学の未来に向けて』（有斐閣、2012年）59-87(84-85)頁。もっとも、行政行為の性質決定と履行確保を切り離して行政行為の法的拘束性を把握した上で（齋藤誠「自治体の法政策における実効性確保」同『現代地方自治の法的基層』（有斐閣、2012年）401-417(407)頁[初出2002年]）、権利義務の変動自体に着目して域外効力を制限的に捉える方向性もありうる（この点については、本研究会における齋藤誠先生からのご教示による）。

²⁶ 渡部友一郎「域外適用の4類型とイコールフットイングに関する実務的展望——個人情報保護法、住宅宿泊事業法、デジタルプラットフォーム法、電気通信事業法」NBL1180号（2020年）33-39頁、原田大樹「プラットフォームビジネス規制の制度設計」千葉恵美子編『デジタル・プラットフォームとルール・メイキング』（日本評論社、2023年）180-215頁[初出2021年]。

²⁷ 田宮・前掲注(22)73頁。

りないと思われる。

第2の類型は、命令・請求読替規定であり、消費生活用製品安全法で採用されてから多くの実定法で採用されている。この規定は、行政処分が執行管轄権の行使に含まれるとの前提に立った上で、外国の事業者に対しては命令ではなく請求すると読みかえるものである。このように、行政行為・行政処分ではなく、ある種の行政指導にすることで、刑事罰の制裁の前提となる義務賦課を除去することになるため、執行管轄権との関係では、特に緊張関係は生じない。

第3の類型は、行政行為（処分）の成立のために領事送達をまず試みて、それが不可能ならば公示送達をする規定である。これは独占禁止法で導入され、金融商品取引法や景品表示法などに広がり、個人情報保護法にも含まれている。領事送達においては、相手国の同意を取った上で領事が送達することになるものの、それがどうしてもできない場合には本国内で内容を公示し、それが一定期間経ったことによって、国外にいる相手方に対して送達したとみなされる。処分が執行管轄権の行使と考えているから領事送達という相手国の同意を取ることを原則にしており、それがどうしても無理な場合に公示送達をすると理解する立場に立つと、行政処分の発令は執行管轄権に含まれていると解する可能性がある。他方で、処分をするところまでは規律管轄権の問題と考える可能性もあり、公示送達の規定はこれを実現するための手続に過ぎないとする見方もあり得る。

第4の類型は、刑事罰を代替する公表規定である。外国人に対して罰則を適用するのが実際には難しいため、命令に違反したことが公表できるという規定を置くものが増えつつある²⁸。これは刑罰による担保が実際には難しく、公表で担保するということで、行政行為（処分）が執行管轄権の問題ではなくて、立法管轄権ないしは規律管轄権の問題であることを前提に、その実効性確保のために公表という規定を置いたという説明が可能である。他方で、これまで条例でしばしば利用されてきた公表規定は、それにより関係する法律との抵触関係を避ける目的をもっていた。この場合の公表規定は、公表に先立つ義務賦課の規定が実は義務の賦課ではなく、行政指導であるというある種の言い逃れを可能にするものであり、もしそれがこの法律についても言えるとする、そもそも義務賦課行為自体を否定する余地を残しておいて、執行管轄権の抵触を避けたという説明もできるように思われる。

2. 規律と実現

次に、事実的な物理的な力の行使との関係では、規律と実現の問題が挙げられる。行政法学はドイツにおけるその確立期において、直接的な実力行使を法的に把握して、それに対して適法性のコントロールを行い、手続的な防護策を講じ、それらを通じて予見可能性を高め

²⁸ 村瀬光ほか『『個人情報の保護に関する法律等の一部を改正する法律』（令和2年改正）等について』法律のひろば 73 巻 10 号（2020 年）4-13(12)頁。

ることを目指してきた（行政のJustizförmigkeit）²⁹。この場合に、物理的な権力行使を法的に把握して実力の行使を観念化すれば、国際法における執行管轄権の議論の現在の動向と、行政法学誕生の歴史とが重なり合うということになる。これに対して、執行管轄権を実力の行使、あるいはそれに準ずるものだけと理解すると、即時執行—典型的には武器使用や武力行使のみを素材に執行管轄権を議論していくことになる。

さらに、執行管轄権の範囲を考える上で考慮する必要があると思われるのは、グローバル化と実効性の要請である。経済活動がグローバル化することによって社会問題がグローバル化し、これに対応する形で法技術もグローバル化対応をしてきたことから、最近では特に立法管轄権の拡張傾向が看取される。つまり、国内の問題を解決するためには、国内の措置だけを念頭に置くのではもはや意味がなく、国外での対処も要求されるようになってきている³⁰。そのように考えると、一方では立法管轄権を域外にも幅広く及ぼす理論枠組を構想することは確かに重要である。他方で、問題を実効的に解決するという視点からすると、立法管轄権を仮に広げたとしても、それが執行（＝現実化）できなければ、問題の解決手段の選択という意味では目的を達成できていないとも言える。例えば、執行管轄権行使の前提として対人管轄権を必要とする見方³¹は、国内に何らかの拠点がないとそもそも執行しようがないという点で示唆的である³²。

V おわりに

本稿では、執行管轄権をめぐる議論を国内法・国際法の双方から検討し、その概念の現状を紹介した。本稿の暫定的な結論としては、以下のような理由から、執行管轄権を物理的な実力行使だけではなく、個別的・具体的な権利義務ないしは法的地位の変動をもたらす行為（の少なくとも一部）も含めて考えるべきと思われる。

第1に、国家管轄権という言葉自体に、「国家」がどういう権限を持っているかということが問題として含まれており、その際には作用と組織の両面を考慮する方が自然である。第2に、法を適用する段階で既に相手方には具体的な危険が生じていると評価できる場合には、それが物理的に強制されなくてもその義務の履行を決断する時間的ポイントに至っている。これは、国内法では成熟性として議論されている要素であって、その時点で成熟性が認めら

²⁹ 塩野宏『オットー・マイヤー行政法学の構造』（有斐閣、1962年）179-180頁。規制の仕組みの中で即時強制、下命・禁止、許可制・届出制を連続的に説明する見解として参照、小早川・前掲注（10）192-199頁。

³⁰ 岩沢雄司「現代国際法の変容とその意義」浅田正彦ほか編・坂元茂樹先生・薬師寺公夫先生古稀記念『現代国際法の潮流Ⅰ』（東信堂、2020年）4-21（20）頁のいう「対外適用」（国家機関が国外における外国・外国人の行為に国際法を適用すること）はこれとは区別される法現象と考えられる。

³¹ 松下満雄『独占禁止法と国際取引』（東京大学出版会、1970年）138頁。

³² 国際租税法における恒久的施設(permanent establishment)の議論（増井良啓＝宮崎裕子『国際租税法（第4版）』（東京大学出版会、2019年）15頁）もこれと関連する。

れるならば、もはや「執行」の問題と考えてよいように思われる。物理的な実力行使は国内法では例外的な存在であり、同様の認識は国際法の世界でも広がっている。

このように考えると、執行管轄権の幅が広がり、その管轄権の主体を属地主義とか旗国主義で決めることとなる。確かに、執行管轄権の存否をめぐることは、属地主義や旗国主義を原則にすべきである。もっとも、行為の性格や国家間の利害状況によっては、こうした原則以外の考慮を容れる余地があると思われる。例えば、旗国主義との関係では、実効性という観点を念頭に置くと、誰がそれをエンフォースという意味で執行するのが適当なのかということとを考慮せざるを得ない³³。つまり、どの国が執行することが自国にとって、あるいは他国にとって利益になるのかという観点が出てくる³⁴。このような考え方は、既に海賊に対する普遍主義や、国際租税法におけるBEPS（Base Erosion and Profit Shifting：税源浸食と利益移転）の問題にも見られる。国内公法学がこれまで重視してきた正統性ももちろん重要であるものの、正統性と実効性のバランスの中で執行管轄権の存否・限界を考える必要があるように思われる。

³³ 兼原敦子「現代公海漁業規制における旗国主義の存立根拠」立教法学（立教大学）75巻（2008年）23-66(50)頁は、遠海にある自国船舶の活動をあまねく把握し、公海上で執行措置をかけることで法令遵守・違反取締が実効的に行われるという想定がどこまで現実味をもっていたかは疑問であるとし、公海での旗国主義には、他国による規制を排除する消極的意味はあっても、秩序維持という積極的な機能は空白であると指摘する。

³⁴ 黒崎ほか・前掲注(16)192頁は、執行管轄権の内在的制約として、合理性・必要性・比例性の一般原則を挙げる。今後、その具体的な基準を国際法学・国内法学の対話によって形成していくことが重要であると思われる。

【追記】本稿は2022年2月に執筆され、2023年2月に脱稿したものであり、その後に刊行された関連著作（とりわけ『公共部門法の組織と手続』（東京大学出版会・2024年））との役割分担を想定した記述を行っていた。本稿の刊行が遅れ、関連著作の一部の記述の趣旨が伝わりにくくなってしまったことをお詫び申し上げます。

第 8 章

通商協定における労働条項の法的機能

—資源・エネルギー産業への経済的・政策的示唆—

東京大学大学院教授
伊藤 一頼

I はじめに

近時、国際経済分野の条約において、締約国内の労働問題を扱う条項を設ける例が増加している。労働問題に関する条約としては、国際労働機関(ILO)憲章や、その下で作成された多数の個別条約が存在するが、そうしたILO諸条約とは別に、貿易や投資といった分野を主に対象とする条約において、労働問題にも一定の規律を及ぼそうとするケースが現れているのである。これは、特に発展途上国において適切な労働者保護法制が整備されていないことにより、当該国の企業が支払う労働コストが減り、不当に高い国際競争力を獲得しているという問題に対処し、先進国と途上国との間で公平な競争条件(level playing field)を確保することが目的であるとされる。それゆえ、こうした経済協定の中の「労働条項」が実際に有効に機能し、諸国の労働条件が改善されれば、それらの国から輸出される物品等の価格もそれに応じて増加する可能性がある。発展途上国において労働問題が指摘されるセクターには、鉱物資源等の採掘・精錬といったエネルギー資源に関わる分野も多く、そこでの労働条件について改善圧力がかかるとすれば、それはもちろん労働者保護の面では望ましいものの、国際的には、資源・エネルギーの価格が上昇したり、かかる分野に参入している先進国企業の経営環境が悪化するといった影響が生じることになる。

したがって、こうした労働条項の効果を法的観点から検討し、労働者保護とエネルギー安定供給との両立を可能にするような法政策のあり方を考えていくことは、国際法上の重要な課題であると考えられる。そこで本稿では、主要国が締結した国際協定における労働条項の発展の経緯を概観することを通じて、同条項が有する法的意義を明らかにしていきたい。とりわけ、労働条項が援用された具体的な紛争事例を取り上げ、そこで司法機関によりどのような法的解釈がなされたかを分析することで、同条項が実際にいかなる条件の下で機能しうるのかを探究する。なお、労働条項が含まれる経済協定全てを検討の対象とすることは困難であるため、さしあたり本稿では通商分野の協定における労働条項について取り上げ、投資などその他の分野の協定については他日を期することとしたい。

II 通商協定における労働条項の系譜

1. WTO協定

1980年代以降、先進国の企業が生産拠点を労賃の安い発展途上国へと移す動きが加速し、産業空洞化による雇用の減少や、途上国からの安価な製品の流入といった問題が発生した。上述のように、これを受けて先進国政府は、こうした労働コストの大きな差は、途上国政府が労働者の権利を国内で適切に保護していないために生じているとして、公正競争の観点から諸国間の労働基準の調和を図る必要があると主張した。先進国は当初、WTO協定のなかに労働基準に関する規律を導入しようと試みたが、途上国側の反発は大きく、結局1996年のシンガポール閣僚宣言において、労働基準の問題はILOでの議論に委ね、WTOの枠組みでは

扱わないという方針が決定された。もっとも、この頃から、自由貿易協定(FTA)や経済連携協定(EPA)といった地域的な通商協定を締結する動きが活発になり、そうした少数国間の交渉では先進国と途上国の力の差が反映されやすいため、それらの協定において労働条項を設ける例が増えていくこととなった。

2. 二国間ないし地域的な通商協定

地理的に見ると、米州地域ではほとんどの国が労働条項を含む通商協定を1つ以上締結しているのに対し、アジア太平洋地域ではそうした国は約半数にとどまる¹。以下では、労働条項の発展を主導してきた米国の通商協定を概観したうえで、他の諸国の通商協定についても検討することとしたい。

(1) 米国

米国とカナダ・メキシコは、1992年に北米自由貿易協定(NAFTA)に合意したが、米国内では、労賃の安いメキシコに企業が移転し雇用が悪化するとの批判が噴出した。そこで、大統領選挙に臨んでいたクリントン氏は、労働基準の向上に関してNAFTAを補完する協定の締結を約束し、これが北米労働協力協定(North American Agreement on Labor Cooperation: NAALC)として1994年にNAFTAとともに発効した。もっとも、NAALCは各締約国が共通に遵守すべき国際的な労働基準を明確に定めたわけではなく、あくまでも各国の国内法が「高い労働基準」を達成するよう求めるにとどまる(2条)。ただ、各締約国は、みずから定めた労働法については、その遵守及び実効的な実施を促進する義務があり(3条)、後述のように紛争処理手続においては主にこの義務の違反が問われることになった。

その後、2001年に締結された米ヨルダンFTAでは、「国際的に認められた労働者の権利」の保護を確保する努力義務が規定され(6条)、労働基準の内容について両国間で共通化を図ろうとする姿勢が現れた。さらに2004年の米シンガポールFTAは、ILO総会が1998年に採択した「労働における基本的原則及び権利に関する宣言」の下でのコミットメントを両国が確認するとしている(17.1条)。このILO宣言は、4つの原則(①結社の自由及び団体交渉権の効果的な承認、②あらゆる形態の強制労働の禁止、③児童労働の実効的な廃止、④雇用及び職業における差別の排除)を中核的な労働基準として認定し、これらの原則に関連する最も重要な8つの条約²の早期批准を求めるとともに、たとえ未批准の段階であってもILO加盟国

¹ ILO, *Social Dimensions of Free Trade* (2013), p.21.

² 8つの条約とは、ILOの下で採択された次の諸条約を指す。①結社の自由及び団結権の保護に関する条約(第87号)、②団結権及び団体交渉権についての原則の適用に関する条約(第98号)、③強制労働に関する条約(第29号)、④強制労働の廃止に関する条約(第105号)、⑤同一価値の労働についての男女労働者に対する同一報酬に関する条約(第100号)、⑥雇用及び職業についての差別待遇に関する条約(第111号)、⑦就業の最低年齢に関する条約(第138号)、⑧最悪の形態の児童労働に関する条約(第182号)。

である以上はこれらの原則を尊重・実現する義務があると述べている。この宣言は、形式上は法的拘束力を持たないものであるが、上記のように通商協定のなかに取り込まれた場合には、その締約国は国内法において4つの中核的労働基準を実現するよう法的に拘束されることになる。

さらに2007年5月10日には、ブッシュ政権と連邦議会の民主党との間で、以後米国が締結する通商協定において確保されるべき内容に関する超党派合意が成立した（いわゆるMay 10合意）。労働分野に関しては、ILO宣言に含まれる中核的労働基準を国内法で実施すべきこと、かかる労働規律は通商上の義務に適用されるのと同じの紛争処理制度に服すべきこと、などが求められており、これらの要請は当時交渉中であったペルー・コロンビア・パナマ・韓国とのFTAに取り入れられた。

(2) その他の諸国

上記のような米国の動向に明確に追随しているのはカナダである。カナダがペルー・コロンビア・パナマ・ヨルダンと締結したFTAでは、May 10合意以降の米国のFTAをモデルとした労働条項が規定されている。

EUは、2009年のリスボン条約により、欧州連合条約21条が定めるEUの対外行動の原則の1つとして「人権と基本的自由の普遍性及び不可分性」を掲げた。ここには労働者の権利も含まれると考えられ、例えば2011年に発効した韓国とのFTAは、ILO宣言の国内的な実施、及びすでに批准したILO条約の実効的な履行を義務づけている（13.4条）。また、2016年10月に署名されたカナダとのFTAにおいても同様の規定を設けている（23.3条）。

(3) 環太平洋パートナーシップ(TPP)協定³

TPP協定の第19章（労働章）は、米国流の労働条項を基礎としつつ、それを一部発展させた内容となっている。まず19.3条1項では、従来と同様に、ILO宣言に示された諸原則を自国の法令及び慣行において採用・維持することが義務づけられる。他方、同条2項は、最低賃金、労働時間、職業上の安全・保健に関し、各締約国がみずから決定した受入れ可能な労働条件を自国の法令及び慣行において採用・維持するよう求めており、これは従来の米国のFTAに見られなかった要素である。そして、以上の内容を規定した国内労働法令については、締約国間の貿易又は投資に影響を及ぼすような態様で作為又は不作為を継続・反復することにより、その「効果的な執行」を怠ってはならないと定めている（19.5条）。

また19.6条は、強制労働によって生産された物品を自国企業等が輸入しないよう、各締約国は自国が適当と認める自発的活動を通じて奨励することとしており、これも従来の米国の

³ TPP協定は米国の加入見送りにより発効しなかったが、その内容をほぼ全て取り込んだ形の「環太平洋パートナーシップに関する包括的及び先進的な協定(CPTPP)」が2018年に発効した。ここでは当初のTPP協定で規定された内容に基づき検討を行う。

FTAには見られなかった規定である。実際、米国の国務省は、マレーシア・メキシコ・ペルー・ベトナムの一部の産業において強制労働が存在すると指摘していた⁴。

さらに米国は、TPP協定には加入しなかったものの、ベトナム・マレーシア・ブルネイのそれぞれとの間で、「労働整合性計画」等と題する個別の二国間条約を作成していた。これはTPP協定の労働章を補完する内容ではあるが、TPP協定本体とは区別された別個の条約である。これらの条約の下で、例えばベトナムは、労働者が事前の許可なしに自由に組合を結成し、またその代表の選出や内部規則の作成を自律的に行えるよう法令で保障することをはじめ、極めて多岐にわたる対応が求められていた。またマレーシアの労働整合性計画では、強制労働や人身取引、移住労働者の権利保護の不足といった問題が扱われ、パスポートの取り上げ禁止、反人身取引立法の推進などが規定された。これらの義務の履行状況を評価するため、米国と各々の国の間で、高級実務者による常設委員会を設けるほか、義務の不履行についてはTPP協定の紛争処理制度に付託しうることとされていた。

Ⅲ 通商協定における労働条項の下での紛争処理

以上のように、TPP協定を含む近年の通商協定は、ILO宣言が掲げる中核的労働基準を締約国が国内法において取り込み、かつそれを実効的に執行するよう求めているものが多い。しかし、これらの規定が有効に機能するためには、義務違反に対する紛争処理のメカニズムが適切に設計されていなければならない。特に、政府間の紛争処理手続を設けるだけでは、外交上の配慮や相手国の国内事情に関する情報の不足から、ほとんど発動がなされない恐れがある。この点、米国流の労働条項では、私人が他国政府に対して直接に申立を行うことで紛争処理手続の発動を促す仕組みを導入しており、実際、これにより一定の成果も挙がっている。また後述のように、TPP協定の労働章もこれと同様の仕組みを採用している。そこで以下では、従来の通商協定の下で私人による申立の制度がどのように規定され、どの程度活用されてきたかを簡単に整理しておきたい。

1. 北米労働協力協定 (NAALC)

NAALCが用意する政府間の紛争処理手続では、労働当局間協議（21条）、閣僚間協議（22条）、専門家評価委員会による調査（23条）、仲裁パネルによる審査（29条）、という4つの段階が設けられている⁵。仮に仲裁パネルで義務の不履行が認定された場合には、被提訴国は

⁴ Cf. Cathleen Cimino-Isaacs, “Labor Standards in the TPP,” in Jeffrey J. Schott & Cathleen Cimino-Isaacs (eds), *Assessing the Trans-Pacific Partnership, Volume 2: Innovations in Trading Rules* (Peterson Institute for International Economics, 2016), p.48.

⁵ 閣僚間協議では、NAALCが附表1に掲げる「11の原則」（①結社の自由と団結権の保護、②団体交渉の権利、③ストライキの権利、④強制労働の禁止、⑤児童・年少者労働の禁止、⑥最低雇用基準、⑦労働差別の撤廃、⑧男女の平等賃金、⑨労働災害及び疾病の防止、⑩労働災害及び疾病に対する補

問題解決のための行動計画を策定する必要がある、さらにその行動計画を遵守していないと仲裁パネルが判断した場合には最大2000万ドルの金銭支払いが命じられる（38～39条）⁶。もともと、これまでのところNAALCに基づき仲裁パネルに付託された案件は1つもない。

ところで、NAALCの下で各締約国は国内管理事務所 (National Administrative Office: NAO) を設置している。そして、もしいずれかの締約国が義務の遵守を怠っていると考えられる場合、それに関心を持つ私人（必ずしも当該事案の当事者でなくともよい）は、他の締約国のNAOに対してその問題を申し立てることができる（16条3項）。この際、当該問題が発生している国において予め国内的な救済手段を尽くしておく必要はなく、また複数の国のNAOに申立を行うことも妨げられない。

こうした申立を取り扱うための手続規則は、各締約国が独自に作成する。例えば、米国のNAOである労働省の貿易・労働問題事務所 (Office of Trade and Labor Affairs: OTLA) は、申立に記載されるべき事項をガイドラインにおいて列挙している⁷。OTLAは、申立から原則60日以内に受理の可否を決定するとしており、申立を受理するか否かの判断に際して考慮される要素についてもガイドラインで示している⁸。受理を決定した場合、OTLAは申立人、関連締約国、その他の適当な者に対して書面による通知を迅速に行うとともに、受理の判断に至った理由を官報に公表する。そして、受理の決定から原則180日以内にOTLAは報告書を公表する。報告書には、当該事案の手続の要約、申し立てられた違反に関する判断、勧告の内容などが記載される。

償、⑪移民労働者の保護）の全てを取り上げることができる。一方、専門家評価委員会は、④～⑪の問題のみを扱うことができる。また、仲裁パネルには、⑤⑥⑨の問題のみを付託することができる。⁶ この金銭は、被申立国が労働法令の実施能力を向上させるための基金に払い込まれる。その支払いがなされなかったときはNAFTAの下での恩恵が当該金額の範囲内で停止される。

⁷ これによれば、申立は、次のような事項を可能な限り詳細に説明したものでなければならない。①申立に言及された事項が、FTA 労働章における義務又は約束に反した他国の行為を立証しているか。②申立人あるいはその他の者に被害が生じたか（生じたとすれば、どの程度の被害か）。③申立に言及された事項が、労働法規の不実施に関する他国の継続的・反復的な行為（又は不作為）を立証しているか。④申立に言及された事項が、締約国間の貿易に影響を与えているか。⑤当該国の国内法の下での救済は試みられたか（試みられた場合には、かかる手続はいかなる結果になったか）。⑥申立に言及された事項は、いずれかの国際機関において処理され、又は係属しているか。Cf. OTLA, *Notice of Procedural Guidelines* (Federal Register, vol.71, no.245, pp.76694-76696), Section F, para.2.

⁸ 申立の受理の可否を判断する際には次のような要素を考慮する。①申立が労働章の下で生じる事柄に関連する問題を提起しているか。②申立の審査により労働章の目的が促進されるか。③申立において、申立人が特定され、日付・署名があり、かつ請求の本質を決定して適切な審査を行いうる程度に十分な詳細さを有しているか。④申立に含まれる主張は、もし立証されれば、労働章の義務に関する他国の違反を構成することになるか。⑤相手方締約国の国内法の下で適当な救済が試みられたこと、もしくは当該問題がいずれかの国際機関において係属していることが、申立に含まれる主張あるいは入手可能な情報を通じて明らかになったか。⑥当該申立は最近の申立と実質的に類似していないか（以前になされた申立との差別化を可能にするような新しい重要情報が提示されているか）。Cf.

OTLA, *Notice of Procedural Guidelines*, op.cit., Section G, para.2.

1994年から2011年の間に、NAOへの私人申立は合計41件なされており、年間では概ね0～5件ずつの申立がある。その内訳は、表1のようになる。やはりメキシコの不遵守を対象とした申立が多いが、米国やカナダの不遵守を問う申立も一定程度あることは留意すべきである。なお米国は、クリントン政権時代には、申立の半数以上を閣僚間協議へと付託していたが、ブッシュ政権では反労働的な姿勢が強まったことでその割合が5分の1程度にまで低下し、申立を不受理とするケースも増加した。

表1 NALCの下における私人申立の内訳（1994年～2011年）

締約国	不遵守を問われる対象 となった件数	NAOに申立を受けた件数
米国	13	25
カナダ	2	6
メキシコ	26	10
計	41	41

出典：ILO, *Social Dimensions of Free Trade* (2013), p.45.

では、NAOへの申立は具体的に労働者側にどのような成果をもたらしてきたのだろうか。例えば、1996年に申立がなされたMaxi-Switch事件では、メキシコの労働組合が当局に登録を拒否されていたが、米国NAOに申立がなされ、その公聴会が開かれる4日前になった時点でメキシコ当局は当該組合の登録を許可した。これは申立を契機として政府の行動が改められた初めての例であるとされる⁹。また、1997年のGender Discrimination事件では、メキシコの民間企業や政府機関が、女性の採用に際して妊娠中か否かの検査を行っていたことに関し、米国NAOに申立がなされ、閣僚間協議で話し合われた結果、そうした検査は以後行わないこととなった¹⁰。

他方、1998年のApple Growers事件やDecoster Egg事件では、米国の農業部門で働くメキシコの移民労働者が、人種差別的な扱いを受け、危険かつ不衛生な労働環境に置かれていることにつき、メキシコNAOに申立がなされた。閣僚間協議が行われた結果、米国の政府機関は、移民労働者の権利に関する説明会の開催やガイドの発行による使用者の意識改革を図るとともに、スペイン語による労働問題ホットラインを開設するなどの対策を講じた¹¹。

⁹ Cf. Tamara Kay, *NAFTA and the Politics of Labor Transnationalism* (Cambridge University Press, 2011), p.133.

¹⁰ Cf. ILO, *Social Dimensions of Free Trade*, op.cit., p.59.

¹¹ *Ibid.*; Kay, op.cit., p.149.

なお、多くの申立においては、労働問題により直接に不利益を被っている労働者らに加え、その国の労組の上部団体等が共同の申立人となり、費用やノウハウの支援を行っている。さらに、申立先の国の労組上部団体も共同申立人として現地での各種の便宜を供与することが定着しており、例えば米国NAOへの申立案件ではアメリカ労働総同盟・産業別組合会議(AFL-CIO)も申立人に加わっているケースが多い。このように、通商協定における私人申立の制度は、国境を超えた労働者間の新たな連携関係を生み出す素地ともなっている。

2. 環境分野における私人申立の仕組み（参考）

NAFTAの下では、労働分野と同様の関心から、環境分野においても、締約国の環境問題について私人申立の仕組みが設けられた。すなわち、NAFTA環境協力協定(NAAEC)の下では、ある締約国が自国の環境法令を実効的に実施していない旨の私人からの申立を協定事務局が受理することができるとされ、一定の要件が満たされていれば、事務局は申立をされた国に対し、応答を求めることができる(14条)。こうした申立と応答に基づき、事務局は、「事実報告書(factual report)」の作成に関する勧告を理事会(Council on Environmental Cooperation)に行うことができ、理事会の3か国中2か国が支持すれば、事実報告書を作成して理事会に提出する。事実報告書の目的は、申立がなされた事案に関する公式の記録を提供することであるとされ、理事会の3か国中2か国の賛成により公表される。

米国やカナダは、このNAAECの手法をその後のFTAにも用いている。ただ、カナダの最近のFTAは私人申立の仕組みを取り入れていないのに対し、米国のFTAは、こうした環境法令実施義務を協定本体に規定するとともに、私人申立の仕組みも存続させている(例えば米ペルーFTA18.8, 18.9条)。加えて、米国の最近のFTAでは、国内環境法令の実施義務のみならず、いくつかの環境条約上の義務を遵守するよう求める規定も設けられている(米パナマFTA17.2条, 米韓FTA20.2条, 米豪FTA19.1条, 米チリFTA19.1条, 米シンガポールFTA18.1条)。

こうした条項の違反の疑いに関する私人の申立等を契機として、締約国間において協議等がなされることになるが、そこで問題の解決ができない場合は、仲裁パネルが設置される(NAAEC24-36条, 米豪FTA21章, 米チリ22章, 米シンガポール20章)。仲裁パネルが継続的な法令不実施があると認定すれば、まず締約国間で相互に合意された行動計画を採択するが、それでも問題が解決されなければ、金銭支払いが課される(NAAEC34.4.b条, 米豪FTA21.11条, 米チリ22.15.1条, 米シンガポール20.6.1条)。そして、それが支払われなければ貿易制裁が課されることとなる(NAAEC36条, 米豪FTA21.11.2条, 米チリ22.15.2条, 米シンガポール20.6.2条)。こうした、仲裁から貿易制裁に至る一連の紛争処理プロセスは、労働条項に関しても同様の内容で規定されている場合が多い。

3. TPP協定の労働章における紛争処理手続

TPP協定の労働章は、政府間の紛争処理の手続として、①協力的労働対話（19.11条）、②労働協議（19.15条）、③パネル付託（19.15条12項）の3つの仕組みを設けており、これは米韓FTAや米ペルーFTAを踏襲した形である。③のパネルは、紛争解決章（第28章）に基づいて設置されるものであり、そこで違反が認定された場合は、被申立国が一定の金銭を基金として支払い、それを被申立国における労働法令の実施促進に向けた取組みに活用することが認められる（28.20条8項）。ただし、パネルの設置を要請できるのは、まず労働協議を行い、そこで60日以内に問題が解決されなかった場合に限られる。

これらの政府間手続の発動を促す要素として、TPP協定もやはり私人の申立を重視している。まず各締約国は、自国の公衆が労働章の規定に関連する事項について意見を提供できるよう、国内に協議機関・諮問機関等の仕組みを設けなければならない（19.14条2項）。これに加えて各締約国は、労働章の規定に関連する事項について、全ての締約国の者からの意見書を自国の連絡部局において受領する（19.9条1項）。そして、こうした意見書により提起される事項について検討したうえで、当該意見の提出者に対し、（適当な場合には書面により）適時に回答することが求められる（同条3項）。また、このような個別国家への申立に加えて、政府間で設置する「労働評議会」に対しても、労働章に関連する事項の利害関係者は申立を行うことができる（19.14条1項）。

このように、TPP協定の労働章は私人による申立の制度を取り入れるとともに、さらに一層の拡充を図っており、これまで以上に活発な申立が展開される可能性もある。従来は米州地域に限られていた申立の事例が、アジア太平洋地域にも拡がることになれば、この制度が普遍化・一般化していくうえでの大きな一歩となるであろう。

IV 労働条項に基づく仲裁事例 ―米国対グアテマラ事件―

上述のように、労働条項の下では紛争解決の方式として仲裁が規定されることも多く、これに基づき実際に仲裁が実施された事例も現れてきている。以下では、そうした仲裁事例の最初のものである米国対グアテマラ事件を取り上げ、仲裁パネルが示した判断を検討することで、労働条項が実際にどのような条件の下で機能しうるかを把握するための手掛かりとしたい。

1. 事案の背景

本件は、2008年にAFL-CIOとグアテマラの幾つかの労働団体が、中米自由貿易協定（CAFTA-DR）に基づき共同で米国に付託したものである。申立人は、グアテマラ政府が結社の自由及び団体交渉権を全体的に侵害し、組合活動家に対する殺害・拉致・監禁といった深刻な暴力事件も発生していると訴えた。米当局はこの主張を認め、詳細な分析を含む報告書

を公表した¹²。これに基づき、米国は2010年にグアテマラに協議を要請したが、望ましい結果が得られなかったため、2011年に仲裁パネルの設置を要請した。

両国政府は2013年8月に18項目からなる実施計画に合意したため、仲裁手続は一時中断されたが、グアテマラが同計画の執行を怠ったため米国の要請により手続が再開された。そして、2016年9月17日に仲裁パネルの中間報告書が当事国に配布され、これに対して両国が意見を述べたうえで最終報告書が作成された。この審理の過程では両国が興味深い弁論を行っている。とりわけ、労働条項の違反が成立する要件として、被申立国の行為が「貿易・投資に影響を与え」たことの立証を求める場合が多いが、本件で米国はこれを広く捉え、労働基準違反に関わった企業が、相手国と何らかの形で貿易に関わっていれば、それだけで要件は満たされると主張した¹³。他方グアテマラは、この要件は厳格なハードルを課すものであり、両国間の貿易構造に現実の変化が生じていなければならないと主張した¹⁴。こうした経緯を経て、2017年6月14日に仲裁パネルの判断が示された¹⁵。

2. 仲裁パネルの判断

以下では、本事件で争われた3つの主要な論点につき、仲裁パネルが示した判断を紹介していきたい。

(1) グアテマラは自国の労働法令を効果的に執行しなかったか

米国は、グアテマラ政府が、グアテマラ労働法 (GLC) で保障された団結権や団体交渉権を適切に執行しなかったと主張する。

¹² ここでは次のような点が指摘されている。①労働法 281 条によりグアテマラ労働省は企業への検査を行う権限を有しているが、企業側による検査官の立入拒否や情報不提供のため同権限を実効的に行使できていない。②労働省は労働法違反に対する制裁の権限を欠いている（事案が司法機関に付託されるとそれ以降は関与できない）。③使用者が裁判判決に従わなかったときは、当該使用者の刑事責任を問う手続に直ちに移行しなければならないものの、それが適切になされていない。④本申立の範囲内では 11 の判決の不履行が見られている。⑤組合活動家に対する殺害及び深刻な暴力が発生している。⑥組合活動家が殺害され、しかも処罰がされずに終わったことは、他の人々に対しても脅威を与え、団結権及び団体交渉権を弱体化させている。⑦司法判決の履行や検査官による立入検査の確実な実施を進めるため、組織横断的な連携を強めるべきである。⑧2003 年の大統領令で設立された「労働関係に関する多機関委員会」は、複数の省庁により構成されるが、これがその活動を再開させたことは問題解決に寄与しうる。⑨経済省は、企業に対して課税免除を許可する権限を持つが、その条件として労働法規の遵守や社会保障税の納付を求めることは有効な方策であろう。Cf. *Public Report of Review of OTLA U.S. Submission 2008-01 (Guatemala)*, January 16, 2009, pp.ii-iv.

¹³ *Guatemala – Issues relating to the obligations under Article 16.2.1(a) of CAFTA-DR*, Initial written submission of the United States, 3 November 2014, pp.21-22.

¹⁴ *Guatemala – Issues relating to the obligations under Article 16.2.1(a) of CAFTA-DR*, Initial written submission of Guatemala, 2 February 2015, pp.66-67.

¹⁵ *In the Matter of Guatemala – Issues Relating to the Obligations Under Article 16.2.1(a) of the CAFTA-DR*, Final Report of The Panel, June 14, 2017. なお、本仲裁パネルは、Kevin Banks, Theodore R. Posner, Ricardo Ramírez Hernández の 3 氏で構成された。

CAFTA-DR16.8条によれば、同協定16章における「労働法令(labor laws)」とは、結社の権利、団結権・団体交渉権、強制労働の禁止、最悪の形態の児童労働の禁止、最低賃金・労働時間・職業上の安全と保健に関する受容可能な労働条件、といった国際的に承認された労働者の権利に直接的に関連する法律もしくは規制又はその諸規定を意味する。

そこで、遵守が確保されていないと米国が主張するGLCの各条文を見ていく¹⁶。①10条は、労働者が権利を行使することを妨げるために、あるいは労働者が権利を行使したことを理由として報復を加えることを禁止する。②62条(c)は、労働者が労働組合や法的団体から脱退するよう強制したり、他の団体に加入するよう強制することを禁止する。③209条は、労働者が一般労働監督官(General Labor Inspectorate)に組合結成を通知した時点から、組合活動に参加したことを理由として労働者が解雇されないことを規定する。これに違反した場合、労働者は24時間以内に復職することとされ、雇用者は罰金を伴う罰則を受ける(不遵守が7日以上続けば罰金額が50%増える)。④223条は、労働者が組合執行部の役職に就いている間、及び役職を離れた後12か月間は、十分な理由なく解雇してはならないとする。⑤379条では、労働裁判所に集団的労働紛争が付託された場合、雇用者と労働者は相互に報復的措置をとることが禁止される。⑥380条は、集団的労働紛争において要求項目が提示された後は、雇用の終了は裁判官により承認されなければならない。これに違反したときは、裁判官は罰金の賦課及び当該労働者の復職を命じる。以上の規定は、結社の権利、団結権、団体交渉権に関連することが条文上明らかなので、協定上の「労働法令」に該当する¹⁷。

以下、8つの雇用者につき、法令の遵守に到達するのに十分な仕方で裁判所の命令の執行をグアテマラ政府が追求したかを検討する。

①ITM

米国によれば、2008年に労働裁判所はITMがGLC209条に違反する(組合結成に関わった14名の港湾労働者を解雇した)と判断したが、ITMはこれらの労働者を復職させず、補償や賠償も支払っていない。労働裁判所はこの事案に関し訴追のための認証を行い行政庁に通知したが、刑事的罰則は科されず、労働裁判所も不遵守に対する罰則の加重を行わなかったという。米国はこれらの労働者からの6つの匿名証言を提出した¹⁸。これらの証拠は信頼性・一貫性があり、グアテマラ労働裁判所の命令は遵守を実現するうえで十分に確実に執行されていないと言える¹⁹。

②NEPORA

¹⁶ *Ibid.*, paras.282-283.

¹⁷ *Ibid.*, para.284.

¹⁸ *Ibid.*, paras.287-288.

¹⁹ *Ibid.*, para.294.

①と同様に、解雇された4名の港湾労働者に関して、復職をさせておらず、労働裁判所は命令の遵守を確保できていない²⁰。

③ODIVESA

①と同様に、解雇された2名の港湾労働者に関して、復職をさせておらず、労働裁判所は命令の遵守を確保できていない²¹。

④Fribo

組合結成に関わった15名の労働者を解雇し、3か月後に復職させたものの、7名についてはその間の給与の補償はなされず、また解雇前よりも賃金の低い部署に異動させられた。労働裁判所は、同社に対して罰金を加重したり政府に刑事罰を課すよう通知したりする行動をとらなかった²²。

⑤RTM

①と同様に、解雇された6名の港湾労働者に関して、復職をさせておらず、労働裁判所は命令の遵守を確保できていない²³。

⑥Alianza

①と同様に、解雇された数名の労働者に関して、復職をさせておらず、労働裁判所は命令の遵守を確保できていない²⁴。

⑦Avandia

①と同様に、解雇された9名の労働者に関して、8か月ないし9か月にわたり復職を認めなかったため、労働裁判所は命令の遵守を確保できていない²⁵。

⑧Solesa

①と同様に、解雇された2名の労働者に関して、復職をさせておらず、労働裁判所は命令の遵守を確保できていない²⁶。

以上のように、グアテマラの公的機関は、組合結成に関わって解雇された労働者を復職させることや罰金の支払いを要求した労働裁判所の命令が、雇用者により遵守されるよう確保することができず、不遵守による責任を問われたいとのシグナルを雇用者に与えた²⁷。CAFTA-DR16.2.1(a)条は、労働上の諸原則及び国際的に承認された労働者の権利を確保することに関する締約国の意図を示しているが、これは条約法条約31条3項(c)により、CAFTA-

²⁰ *Ibid.*, para.330.

²¹ *Ibid.*, para.363.

²² *Ibid.*, para.376.

²³ *Ibid.*, para.382.

²⁴ *Ibid.*, para.394.

²⁵ *Ibid.*, para.405.

²⁶ *Ibid.*, para.425.

²⁷ *Ibid.*, para.426.

DR締約国の全てが加盟しているILOを考慮して解釈せねばならない。特に、ILO加盟国は、ILO憲章に基礎づけられ1998年宣言に明示された義務である、結社の自由及び団体交渉権の効果的な承認という基本的権利を尊重し促進し実現する義務を負っている。これに関して、ILOの「結社の自由委員会」は、組合活動に対する報復的解雇は結社の自由及び団体交渉権を損なう深刻な違法行為であり、こうした国際的に承認された権利を保護するためにはかかる解雇を禁止し、迅速かつ効果的な救済を与えることが必要であるとの見解を示している²⁸。これらのことから、グアテマラは8事業所における74名の労働者に関して、CAFTA-DR16.2.1(a)条に言う意味での労働法令の効果的な執行を行わなかったと結論する²⁹。

(2) 「持続的又は反復的な一連の行為又は不作為(sustained or recurring course of action or inaction)」が存在したか

上記で米国が立証した事実は、複数の事業所で同様の行為が持続的又は反復的になされていたことを示している。ただ、それだけでは不十分であり、それが「一連の(course of)」と言える態様を示していなければならない³⁰。つまり、これらの行為が相互に孤立した無関係のものではなく、時間や場所に関する十分な近接性を持っていて関連した行為だとみなしうるようなものでなければならない³¹。ただ、これは法執行の欠如が執行行為全体を代表していることやシステム全体で一般的であることまでは要求せず、相互につながりのある一まとまりの行為を構成していればよい³²。

これを検討する際の指針としては、①執行の欠如の背後に意図的なものがあったり、特定のセクターや事業者、労働権に関する執行のバイアスがあったりする場合は、一連の行為であると認めやすくなる³³。②過去にそうした関連性のある形で執行欠如という出来事が起こったことは、他の要因がない限り、将来も同様の状況で執行欠如が関連性を持って起こりやすいという方向性を合理的に推測させる³⁴。

本件では、そうした意図性やバイアス、方向性などは必ずしも立証されていないが、多くの事例の間には、復職と補償という特定の法令上の義務に関する持続的な執行欠如という類似性がある。こうしたパターンからして、執行欠如はランダムな出来事とはいえず、相互に孤立した行為ではない可能性が高い³⁵。

²⁸ *Ibid.*, para.427.

²⁹ *Ibid.*, para.428.

³⁰ *Ibid.*, para.432.

³¹ *Ibid.*, para.433.

³² *Ibid.*, para.435.

³³ *Ibid.*, para.437.

³⁴ *Ibid.*, para.439.

³⁵ *Ibid.*, para.442.

ただ、本件で認定された、5年間で74名という件数は、将来的な執行欠如の方向性を示すにはやや少ないことは確かである³⁶。しかし、次に扱う論点の結果により、本論点には決定的な結論を出す必要はないので、さしあたり一連の行為に当たるものとしておく³⁷。

(3) 「貿易に影響する態様で(in a manner affecting trade)」の要件は充足されるか

米国は、本件の執行欠如によりグアテマラの雇用者は、解雇した労働者への賃金支払いや罰金の支払いを免れたことに加え、組合との交渉による賃金や労働条件の上昇を抑えることができ、より少ないコストで操業できたと主張する³⁸。そして、これらの港湾業者の顧客であるグアテマラの輸出企業も、これによりコスト削減を享受することができたという。また、ある雇用者による不遵守があると、そのセクターの他の業者もそれに対抗して不遵守の行動をとろうとするため、セクター全体の労働コストが低下し、グアテマラの産業と他国の企業との競争条件を不公正に変更させる、という³⁹。

他方、グアテマラは、米国は貿易への実際の影響、及び執行欠如がいかにかそうした貿易への影響に結び付いているかの因果関係を立証していないと主張する。また、執行欠如によりコスト削減効果が生じたことは証拠により裏付けられておらず、純粹に理論的な主張として述べられているにすぎないという⁴⁰。

以下では、本件におけるグアテマラの雇用者を、セクター別に分けて検討する。

①港湾業者(ITM, NEPORS, ODIVESA, RTM)

米国によれば、これら4社はグアテマラにおける太平洋側最大の港であるQuetzalにおいて、準政府機関と契約を締結したうえで港湾サービスを提供している。グアテマラの輸出企業は、こうした業者の港湾労働サービスを利用することでコストを引き下げることができたと米国は主張する⁴¹。確かに多くのグアテマラの企業が同港から他の締約国に向けて輸出しているが、それらの企業がNEPORS以外の3社の港湾労働サービスを利用した証拠が提出されていない⁴²。同港では15の港湾業者が操業しているが、本件の3業者がそのなかで代表的なシェアを有するとの証拠も提出されていない⁴³。3業者に対する執行欠如が、他の業者にも不遵守は罰せられないとの認識を与えた可能性はあるが、同港における他業者の組合の結成状況に関しては証拠があまりない⁴⁴。

³⁶ *Ibid.*, para.443.

³⁷ *Ibid.*, para.444.

³⁸ *Ibid.*, para.446.

³⁹ *Ibid.*, para.447.

⁴⁰ *Ibid.*, para.448.

⁴¹ *Ibid.*, para.453.

⁴² *Ibid.*, paras.456-457.

⁴³ *Ibid.*, para.458.

⁴⁴ *Ibid.*, para.460.

また、最も重要な点は、グアテマラの輸出企業が港湾業者への労働法令の執行欠如から競争上の優位を得たことを示す証拠が米国から提出されていないことである⁴⁵。第一、港湾業者への執行欠如から得られたコスト削減が、輸出企業に競争上の優位をもたらすうえで十分なものかどうかにつき、かかる港湾作業費用がコスト全体に占める相対的な重要性がどれくらいかも含めて、米国からは何らの説明もなされていない⁴⁶。第二に、同港での港湾業者の役務提供は準政府機関との契約的枠組みの下で行われており、個別の輸出企業に対する役務提供において業者間に価格競争が行われていたのかに関する証拠はない。それゆえ、たとえ執行欠如によりコスト削減が生じたとしても、それが港湾業者の手元に利益として残ることなく輸出企業へと移転したとは言えない⁴⁷。したがって、港湾業者に対する執行欠如が、貿易に影響を与える態様でなされたことは立証されなかった⁴⁸。

②衣類生産者(Avandia, Fribo, Alianza)

まず、これらの企業は他の締約国の企業と、他国の競争市場で、あるいはグアテマラの市場で競争関係にあったことは証拠により示されている⁴⁹。では、執行欠如はこれらの企業の競争力にいかなる効果を及ぼし、それは競争上の優位を与えるに十分なほどの規模(scale)と期間(duration)を伴っていたのか。この点、米国からは、解雇された労働者に支払うべきであった賃金が総額でどれほどなのか、そしてそれがコスト全体のうちどれほどを占めているのか、近似的な証拠すら提出されていない⁵⁰。また、米国は、組合結成に関わった労働者が解雇され復職できなかったことで、雇用者は組合との交渉によるコスト増大を回避できたと主張するが、解雇されなかった他の労働者が組合活動に参加して雇用者との間で団体交渉を行うことが妨げられたとする証拠は提示されていない⁵¹。米国は、労働者の解雇等により組合活動が少しでも制約を受ければ、それは雇用者の限界コストの低下につながり、競争上の優位をもたらすと主張する⁵²。しかし、そうした理解は、「貿易に影響を与える(affecting trade)」という文言の通常の意味を奪い、単に「貿易に関連する(trade-related)」という意味と同じものにしてしまう。この要件を充足するためには、競争条件を変更し、競争上の優位を与えることが不可欠である⁵³。したがって、執行欠如により、貿易に携わる雇用者の労働コストが少しでも低下すれば直ちに「貿易に影響を与え」たことになるという解釈は誤りで

⁴⁵ *Ibid.*, para.462.

⁴⁶ *Ibid.*, para.463.

⁴⁷ *Ibid.*, para.464.

⁴⁸ *Ibid.*, para.465.

⁴⁹ *Ibid.*, para.468.

⁵⁰ *Ibid.*, para.471.

⁵¹ *Ibid.*, para.476.

⁵² *Ibid.*, para.478.

⁵³ *Ibid.*, para.479.

ある。原告は、証拠から合理的に推測される労働コストへの効果が何らかの競争上の優位をもたらすのに十分なものであることを立証せねばならない⁵⁴。

そのためには、組合活動に関与した者が報復的な解雇を受けたことで、当該企業において労働者が組合を結成して団体交渉を行うことが実質的に困難となり、それにより雇用者に競争上の優位がもたらされたことを立証せねばならない⁵⁵。確かに、一般論として、報復的な解雇は、他の労働者が組合活動に関与する能力に対して深刻な脅威を与えることになる⁵⁶。それゆえ、可能性としては、執行欠如が報復的解雇のリスクを減らし、そうした解雇が増えることで組合活動が阻害されて競争条件（ひいては貿易）に影響を与える、という因果関係が生じうることは否定できない⁵⁷。しかし、そうした因果関係が、執行欠如があった全ての事案において必然的に生じるとは言い切れない。解雇された労働者の数、解雇のタイミング、組合のリーダーが解雇されたか、法的救済がなされない期間がどれほど続いたか、といった要因に基づき影響のあり方を検証せねばならない⁵⁸。もちろん、あまりに深刻な法令違反について執行欠如があるため、それ以上の証拠なしに組合活動の阻害が論証されるケースもありうるが、一般には、執行欠如の程度と期間が、労働者の組合活動の能力にどの程度影響したかに関する直接の証拠が必要になる⁵⁹。

Avandiaに関しては、結成が進められていた組合の暫定的な執行委員会を構成する労働者9名が全て解雇され、9か月後にそのうち2名はより低い職位で復職したが、残りの7名は復職できないままになった。裁判所はこの復職命令の執行を確保しようとしなかった。こうした出来事が、他の労働者の組合活動を阻害する影響をどれだけ持ったかを示す直接の証拠はないが、この事案の状況においては、そうした証拠がなくとも執行欠如がAvandiaに競争上の優位を与えたことは十分に推認できる⁶⁰。

他方、Friboに関しては、団体交渉を始めようとした15名の労働者が解雇されたが、これらの労働者が組合の幹部だったことを示す証拠はない。また、この15名は後に復職し、うち8名には解雇期間の給与も支払われた。こうした状況では、Friboに対する執行欠如が、他の労働者の団体交渉能力を実質的に損なうほどの効果を持ったとは結論できない。そのような結論を出すためには、労働者や組合自身から、それがどのような阻害効果を持ったかに関する証拠の提出を受ける必要がある⁶¹。Alianzaに関しても同様の状況である⁶²。

③ ゴム生産者(Solesa)

⁵⁴ *Ibid.*, para.480.

⁵⁵ *Ibid.*, para.481.

⁵⁶ *Ibid.*, para.482.

⁵⁷ *Ibid.*, para.483.

⁵⁸ *Ibid.*, para.484.

⁵⁹ *Ibid.*, para.485.

⁶⁰ *Ibid.*, para.487.

⁶¹ *Ibid.*, para.488.

⁶² *Ibid.*, para.489.

Solesaは、確かにゴム生産者であり、グアテマラから他の締約国にゴムは多く輸出されているが、Solesa自身が輸出に携わっているという証拠は提出されていない⁶³。それゆえ、Solesaに対する執行欠如が、グアテマラのゴム産業全体に影響を及ぼしていることが立証されない限り、「貿易に影響を与える」の要件は満たせない⁶⁴。しかし、他の業者にそうした波及効果があったことを示す証拠を米国は提示していない。また、解雇された証拠があるのは2名だけであり、しかも組合の幹部でもないので、こうした状況では、追加的な証拠がない限り、Solesaへの執行欠如が組合活動を阻害し貿易に影響を与えたとは言えない⁶⁵。

結論として、以上のように、執行欠如が認められた8の雇用者のうち、それが貿易に影響を与えると認められるのは1社のみである。1社だけに対する執行欠如では、「継続的又は反復的な一連の行為」によって「貿易に影響を与えて」いるとは言えない。また、この1社に対する執行欠如が他の企業の行動に対しても広く制度的なインパクトを与えているという証拠もない⁶⁶。したがって、本件の事案では16.2.1(a)条の違反があったとは認定できない⁶⁷。

このように、本件仲裁パネルは、とりわけ労働法令の遵守確保義務の違反が「貿易に影響」を与えるという要件につき厳格な解釈姿勢を示し、グアテマラによる協定違反を認定しなかった。貿易に影響を与えるという要件は、通商協定に労働条項を含めることの正当性を持たせるために設けられたものと推測されるが、実際の紛争においては、この要件の立証が必ずしも容易ではないことが本件により示唆されたと言える。もともと、近時のFTAの労働条項では、かかる要件をもはや設けない例も見られるようになっており、そのような協定に基づき仲裁が提起された場合には違反の成立が認められやすくなると考えられる。

V おわりに

以上のように、通商協定の労働条項は、特に私人による申立の仕組みと結合されることで、労働問題を解決するためのかつてない手立てを創出してきている。もちろんそれは、当局による報告書公表にせよ閣僚間協議にせよ、外交的な圧力を中心とするものにとどまるが、最後には仲裁パネルに付託する余地があることによって、そうした圧力はかなりの効果を持ちうるのである。この点、近時のグアテマラの案件において、最終的に違反が認定されなかったとはいえ、実際に仲裁パネルに付託するケースが現れたことは重要な出来事であった⁶⁸。

⁶³ *Ibid.*, para.493.

⁶⁴ *Ibid.*, para.495.

⁶⁵ *Ibid.*, para.496.

⁶⁶ *Ibid.*, para.504.

⁶⁷ *Ibid.*, para.505.

⁶⁸ その後、EU＝韓国 FTA の労働条項に基づく仲裁において、韓国の協定違反が認定される事例も現れている。*Panel of Experts Proceeding Constituted Under Article 13.15 of the EU-Korea Free Trade Agreement*, Report of the Panel of Experts, January 20, 2021.

他方で、こうした労働条項が法的・政策的にいくつかの課題を生じさせていることも確かである。第一に、達成すべき労働基準としてILO宣言がしばしば参照されることの是非を改めて考える必要がある。これは、各々のFTAにおいてILO宣言の諸原則が解釈適用されていけば、解釈が不統一になる恐れがあるからである。この点、EU-CARIFORUM通商協定195.4条は、協議段階において、ILO諸条約の解釈についてILOに意見を要請する権利を各当事国に与えており、解釈断片化問題への1つの対応策を示している。また、もう1つの問題として、ILO宣言自体の不明瞭さがある。これは、従来のILO諸条約により構築されてきた労働者の具体的な「権利」の概念を、曖昧な「原則」に押し戻してしまう可能性があり、各国が都合よくその内容を定義することにつながりかねない。これは労働者保護の観点から見て、必ずしも労働条項がプラスの効果のみを持つわけではないことを示唆している。

第二に、経済的なインプリケーションとして、労働条項は労働者の搾取を背景とする不当に安価な製品との競争から自国産業を守ることにつながる反面、それは貿易される物品等の価格を増加させ、また海外に進出する企業にとっては労働コストが上昇することになる。冒頭で述べたように、これは特に資源・エネルギー関連の物品・企業にとって大きな影響を及ぼす可能性がある。これは、仮に日本が締結するFTAに労働条項が含まれていなくても、米国等のFTAを通じて途上国の労働条件が向上すれば、その影響は日本企業にも及ぶのであり、特定国とのFTAに含まれる労働条項の内容が世界全体に影響を与えることになる。労働条項がそのような経済効果をもたらすことを念頭に置いて、労働条項の望ましいあり方について諸国間での議論を重ねていくべきであろう。

第三に、私人による申立への対処方針を慎重に検討する必要がある。上述のように、労働条項の下では、労働条件の改善に関し利害関係を同じくする労働団体の間で国境を越えた連携関係が構築され、自国内で解決できない労働問題が他国の労働当局に持ち込まれる現象が生じている。使用者側や政府にとっては、国内の労働問題が他国に持ち込まれるという事態は決して歓迎できるものではない。そこでは、他国の労働当局が、過度に「労働者寄り」の立場から批判や要求をしてくることも考えられる。政府としては、自国の労働問題が他国の労働当局に持ち込まれた場合、及び他国の労働問題が自国に持ち込まれた場合に、どのような態度でそれに対応すべきかについて入念に議論しておく必要があろう。

JELI R-No. 160

エネルギー安全保障に関する国際問題の諸相

—2019～2020年度 エネルギー安全保障に関する国際問題検討班報告書—

2026年 6月

発行 日本エネルギー法研究所

〒141-0031 東京都品川区西五反田七丁目9番2号

KDX五反田ビル8F

T E L 03-6420-0902 (代)

<https://www.jeli.gr.jp/>

E-mail contact-jeli@jeli.gr.jp

本報告書の内容を他誌等に掲載する場合には、日本エネルギー法研究所にご連絡下さい。
