

インターネットガバナンス及びデータ流通等に
関する国際的な動向に関する調査研究の請負
成果報告書

2023（令和5）年3月

総務省情報流通行政局情報通信政策課情報通信経済室

（委託先：株式会社エヌ・ティ・ティ・データ経営研究所）

目次

| | |
|--|----|
| 1. 調査研究の概要..... | 1 |
| 1.1. 背景..... | 1 |
| 1.2. 目的..... | 1 |
| 1.3. 実施期間..... | 1 |
| 1.4. 実施体制..... | 1 |
| 2. 調査研究手法..... | 2 |
| 3. 調査研究結果..... | 4 |
| 3.1. 信頼性のある自由なデータ流通（DFFT）に関する調査..... | 4 |
| 3.1.1. DFFT の概観と各国のデータ流通に関する動向 | 4 |
| 3.1.2. これまでの国際的な議論の経緯と今後の見通し | 15 |
| 3.1.3. DFFT の実装に向けて焦点となる 3 つの事項..... | 26 |
| 3.2. 自由で開かれたインターネット空間の維持に関する調査..... | 33 |
| 3.2.1. インターネットの分断における現状と国際的な影響 | 33 |
| 3.2.2. 自由で開かれたインターネット空間の維持に向けた国際団体の動向 | 43 |
| 3.3. 我が国における経済安全保障推進法の意義および ICT インフラの経済安全保障上の課題..... | 46 |
| 3.3.1. 経済安全保障推進法の概要 | 46 |
| 3.3.2. 経済安全保障における ICT インフラの安定的な稼働の重要性 | 64 |
| 4. 参考文献一覧..... | 83 |

図表一覧

| | | |
|---------|---|----|
| 図表 1-1 | 本調査研究の実施体制 | 2 |
| 図表 2-1 | 外部有識者ヒアリング実施対象（実施日順） | 2 |
| 図表 3-1 | 越境データ・フローの上位国・地域 | 5 |
| 図表 3-2 | 欧州のデータスペース構築と GAIA-X の概要 | 7 |
| 図表 3-3 | 米国のデータ関連規制の現状 | 9 |
| 図表 3-4 | 中国データ関連 3 規則 | 10 |
| 図表 3-5 | 中国データ関連 3 規則の比較 | 11 |
| 図表 3-6 | 包括的データ戦略のアーキテクチャ | 13 |
| 図表 3-7 | DFFT の実装 3 つの取り組み | 14 |
| 図表 3-8 | 自由で開かれたインド太平洋（Free and Open Indo-Pacific）の概要 | 15 |
| 図表 3-9 | G7 ROADMAP FOR COOPERATION ON DATA FREE FLOW WITH TRUST | 19 |
| 図表 3-10 | DFFT を実現する仕組みの構築に関するロードマップ | 20 |
| 図表 3-11 | 政府によるデータ収集の 7 原則 | 22 |
| 図表 3-12 | DFFT 具体化に向けて核となる 5 つの領域 | 23 |
| 図表 3-13 | 相互運用のための制度的取り決め（IAP） | 24 |
| 図表 3-14 | G7 デジタル・技術大臣会合にて議論が予定されている DFFT 推進の枠組み | 25 |
| 図表 3-15 | 秘密計算の概要 | 29 |
| 図表 3-16 | 差分プライバシー技術の概要 | 30 |
| 図表 3-17 | 価値創出プロセスとデータ取引プロセスの関係 | 31 |
| 図表 3-18 | インターネットのガバナンスを支える国際組織 | 34 |
| 図表 3-19 | 世界で発生したインターネットの遮断回数 | 36 |
| 図表 3-20 | インターネットの分割における分類 | 41 |
| 図表 3-21 | 情報通信における標準の種類 | 43 |
| 図表 3-22 | 経済安全保障の推進における我が国としての大きな方向性 | 47 |
| 図表 3-23 | 経済安全保障上の主要課題 | 48 |
| 図表 3-24 | 特定重要物資の指定の要件 | 50 |
| 図表 3-25 | 特定重要物資 11 分野と所管省庁および 2022 年度第 2 次補正予算における計上額 | 51 |
| 図表 3-26 | 安定供給確保取組方針の全体像および横断的事項 | 52 |
| 図表 3-27 | 特定重要技術の概念整理 | 56 |
| 図表 3-28 | 特定重要技術研究開発協議会における守秘義務登録情報の取り扱い | 57 |
| 図表 3-29 | 経済安全保障重要技術育成プログラムに係る研究開発ビジョン（第一次） | 59 |
| 図表 3-30 | 経済安全保障重要技術育成プログラムの強化に向けて | 60 |
| 図表 3-31 | K プログラムにおけるシンクタンクのミッションおよび果たすべき役割 | 61 |
| 図表 3-32 | 対象とすべき発明のイメージ | 63 |
| 図表 3-33 | 非公開となる発明（保全対象発明） | 64 |
| 図表 3-34 | デジタル田園都市国家構想実現におけるデジタルインフラの強化 | 65 |

| | | |
|---------|---|----|
| 図表 3-35 | 政府によるデジタルインフラの地方分散支援..... | 70 |
| 図表 3-36 | 5G セキュリティ検証環境の構築 | 72 |
| 図表 3-37 | 脅威シナリオ検討と検証に基づく 5G システムドメインの重要度の整理..... | 73 |
| 図表 3-38 | ガイドライン策定に向けた包括的な脅威分析の実施..... | 73 |
| 図表 3-39 | 「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」の概要 . | 74 |
| 図表 3-40 | 「NOTICE」および「NOTICER」プロジェクトの概要..... | 76 |
| 図表 3-41 | メガクラウドと HSDC の概念図..... | 78 |
| 図表 3-42 | データセンターの地方拠点整備..... | 80 |
| 図表 3-43 | デジタルインフラ整備に当たっての官民等の役割 | 82 |

1. 調査研究の概要

1.1. 背景

インターネットが我々の日常生活に密接不可分となっている現在、インターネットに関して生じる問題は、リテラシーの向上や権利の保護といった個人レベルのものから、通信インフラや事業環境の整備、情報セキュリティの向上といった社会レベルのもの、国家間対立のような国家レベルのものまで多岐にわたっている。また、デジタルデータの経済的価値が高まるにつれ、国境を越えて流通する膨大なデジタルデータの取扱いについて、各国で対応が分かれてきている。

こうしたインターネット及びデータ流通に関する国際的な問題は、これまで、様々な多国間・マルチステークホルダーシステムにより議論がなされてきた。我が国がデジタル分野で世界にプレゼンスを示していくためには、このような国内外のデジタル分野を取り巻く最新動向を踏まえて、必要とされる取組や政策の方向性を検討することが必要である。

1.2. 目的

本調査研究では、このような背景を踏まえ、信頼性のある自由なデータ流通（DFFT）や「自由で開かれたインターネット空間の維持」に向けた国際連携の強化等、デジタル分野における国際的な議論の最新動向、各国政府の取組等を調査・分析することで、今後の情報通信政策の企画・立案等に資することを目的とする

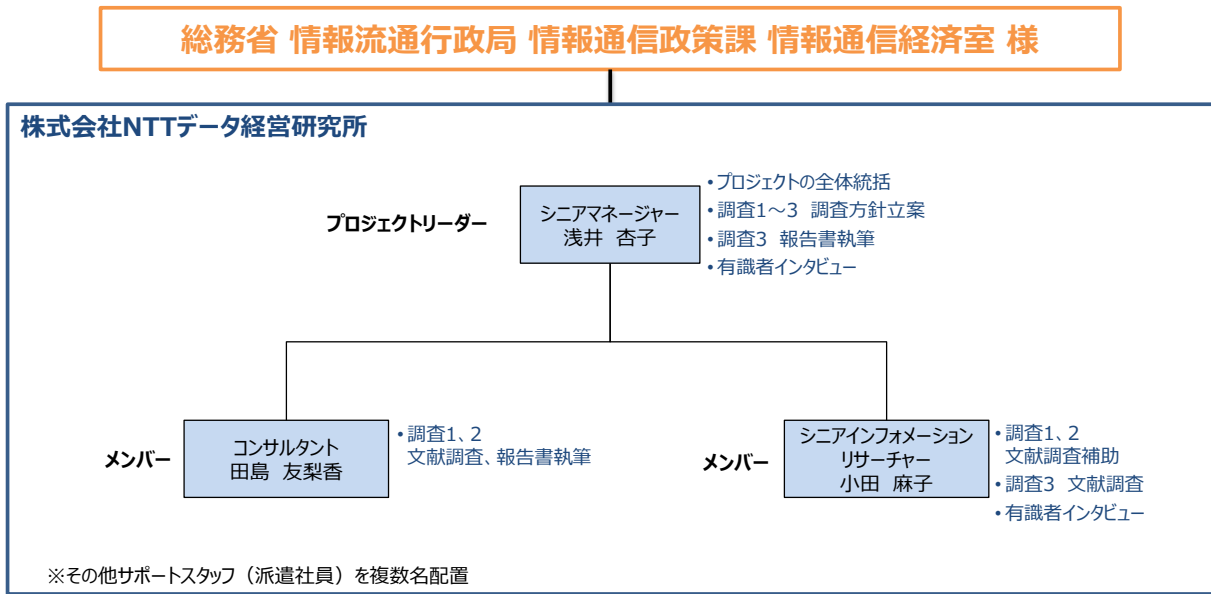
1.3. 実施期間

2023（令和5）年2月14日から、2023（令和5）年3月31日までの期間にて実施した。

1.4. 実施体制

本調査研究は、株式会社NTTデータ経営研究所が実施した。
実施体制を図表 1-1 に示す。

図表 1-1 本調査研究の実施体制



2. 調査研究手法

本調査は仕様書「3. 請負の内容」に記載された調査項目に沿って実施した。

本調査の内容の充実や正確性の向上等を目的として、下記 2 名の外部有識者に対してヒアリングを実施した。

図表 2-1 外部有識者ヒアリング実施対象（実施日順）

| No | 氏名 (敬称略) | 所属・役職等 | ヒアリング 実施日 | ヒアリング項目 (例) |
|----|-------------|-------------------|--------------------|---|
| 1 | 実積 寿也 | 中央大学 総合政策学部 教授 | 2023 年 3 月 23 日 | <ul style="list-style-type: none"> ●インターネット空間の分断（splinternet）に関する動向 <ul style="list-style-type: none"> ✓ Splinternet 1.0 から Splinternet2.0 へと性質が変化しているとされる、昨今のsplinternetの特徴 ●開かれたインターネット空間の維持に向けた国際連携の在り方 <ul style="list-style-type: none"> ➢ 昨今の国際情勢を踏まえたインターネットガバナンスの在り方 <ul style="list-style-type: none"> ✓ マルチステークホルダー主義によるガバナンス体制の課題と展望 ✓ マルチラテラル主義によるガバナンス体制が優勢となった場合のインターネットの姿 ➢ インターネット監視団体などの第三者機関の在り方 <ul style="list-style-type: none"> ✓ 国際NPO団体「Internet Society」をはじめとするインターネットガバナンスを担っている各国際 |

| No | 氏名 (敬称略) | 所属・役職等 | ヒアリング 実施日 | ヒアリング項目 (例) |
|----|-------------|-----------------|--------------------|---|
| | | | | 団体の動向および展望 ✓ Google 傘下のシンクタンク「Jigsaw」をはじめとするインターネットガバナンスを担っている民間企業の動向および展望 |
| 2 | 鈴木 一人 | 東京大学 公共政策大学院 教授 | 2023 年 3 月 28 日 | <ul style="list-style-type: none"> ●我が国における経済安全保障推進法の意義および検討すべき課題 <ul style="list-style-type: none"> ✓ 経済安全保障推進法に関して、評価すべき点と議論が必要とされている課題 ✓ 経済安全保障と自由な貿易のバランスを取るうえで重視すべき課題 ✓ 官民対話をより強化する必要性を踏まえて、具体的に実現すべき制度・対応策 ● 基幹インフラの安定的な稼働の維持に向けた ICT インフラの課題 ● 経済安全保障全体における、データセンター、海底ケーブル、5G 等の ICT インフラの重要性および検討すべき課題 |

3. 調査研究結果

3.1. 信頼性のある自由なデータ流通（DFFT）に関する調査

3.1.1. DFFT の概観と各国のデータ流通に関する動向

(1) 急増する越境データフローと DFFT 推進の意義

インターネットやテクノロジーの発展に伴うデータ利活用の重要性が、様々な産業で認識されるようになって久しい。昨今は自国内でのデータ利用に留まらず、国境を越えたデータ流通が活発化しており、越境データ流通量（以下越境データフロー）が急激に増加している。日本貿易振興機構（JETRO）のレポートによると、2021年の越境データフローは2017年との比較で約2.7倍と拡大傾向にある。また、国、地域別では欧州を中心にドイツ、米国、フランス、英国、オランダが上位5位となっている（図表3-1）。このように急激な増加傾向にある越境データフローについて、各国はそれぞれ独自のルールや規制を発展させてきている一方で、世界共通の方向性は未だ存在していない。気候変動をはじめとする環境問題や新型コロナウイルスで浮き彫りになった感染症対策などの世界共通の社会課題解決のためには、越境データの活用が必要不可欠であり、国や企業が自身の利益追求のためにデータを囲い込むのではなく、課題解決のための重要なリソースとして活用することが求められる時代となっており、これを達成する上では、世界共通のルールが必要であるといえる。

世界共通のルール作りのための国際連携が急務の課題として認識されている中で、「DFFT（Data Free Flow with Trust）：信頼性のある自由なデータ流通」（以下、DFFT）というポリシーがある。2019年1月のダボス会議において安倍元首相が提唱したDFFTは、プライバシーやセキュリティ・知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指すコンセプトである¹。DFFTは和訳で「信頼性のある自由なデータ流通」として認識されているが、「Trust（信頼性のある）」、つまり人権や安全保障を担保し、国や企業によるデータの悪用などのリスクを排除することで信頼を構築しつつ、同時に「Free（自由な）」、ボーダーレスにデータの活発かつ自由な流通を促すことで、ビジネスに限らず様々な場面でのデータ活用を促進することを目指している。

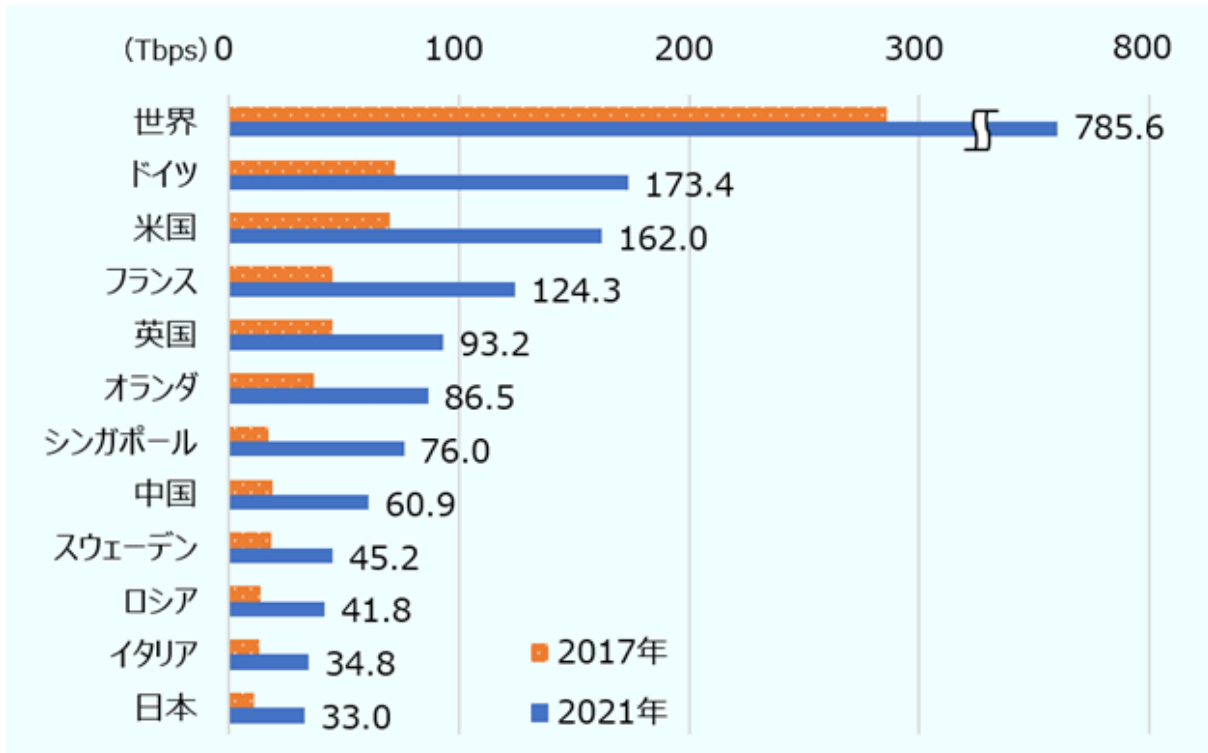
DFFTは、コンセプト自体は明確かつ誰もが理解しやすいものとなっており、その理想については多くの国が賛同する一方で、実現に向けた政策レベルでの議論は様々な問題を包含しており、各国の思惑が異なるなかで「データ保護とデータ移転」の両者をバランスよく盛り込んだ国際ルールの制定に向けた道のりが長いことは想像に難くない。しかしながら、DFFTが実現しなければ、今後世界が別々の方向を向きつつけることとなり、そのような状況においてはデータの価値を最大限に発揮させることはできない上に、データの悪用に対して世界が一枚岩で対抗することができず、大きなリスクとなってしまう。

2023年には、DFFTを提唱した日本が議長国としてG7が開催される。ここでデータの未来に必要な

¹ デジタル庁「DFFT（Data Free Flow with Trust：信頼性のある自由なデータ流通）」
(<https://www.digital.go.jp/policies/dfft/>) (2023.1.16 閲覧時点)

不可欠な DFFT の議論をどれだけ加速させることができるかは大きな正念場と言えるであろう。

図表 3-1 越境データ・フローの上位国・地域



出典：「データ取り巻く環境は今（世界）越境データ・フロー、投資、通商ルールからの考察」（日本貿易振興機構（JETRO），2022.8.2）

(<https://www.jetro.go.jp/biz/areareports/2022/a0f8f01fb2cb87d3.html>)

(2) 国内外におけるデータ流通等に関する姿勢・取り組み等

国際的なデータガバナンス構築において DFFT の実現が急務とされるなか、各国が足並みを揃えた動きを見せているとは言い難い現状がある。以下、データ保護やデータ保護をはじめとする各国の政策動向を整理する。

1) EU

EU はデータ保護およびデータの越境移転について、人権保護を最優先とする一貫した姿勢を見せ続けている。データ保護に関して EU がこのような姿勢を見せる背景には、第二次世界大戦中、ナチスドイツが当時のドイツ IBM 社が開発した「ホレリスシステム（Hollerith machines）」を利用し、個人情報を悪用することにより、ユダヤ人をはじめとするマイノリティを特定し、ホロコーストを効率的に実行する一助となったという負の歴史に対する反省がある。そのため、世界でもデータ保護の議論をリードする責任感と自負があり、他地域と比較しても厳しいルールメイキングを行ってきた²。

² TIME, Olivia B. Waxman (2018.5.24) 「The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History」 (<https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/>)

冷戦終結後の1993年にEUが発足したことを契機として、よりデータ保護を強化する目的で1995年には「個人データ保護指令(Directive 95/46/EC)」が発出され、特に第三国への個人データの移転に関し、第三国が十分なレベルの保護措置を確保していることを条件とする等の「充分性認定 (adequate level of protection)」などが盛り込まれた。「充分性認定」は、国として十分なレベルの保護措置を行っていることとEUが認めた国のみに適用されるが、米国はデータ保護にかかる包括的な法令を国として整備できていなかったため、この状況を補完する目的で、2000年にセーフハーバー協定と呼ばれるEUと米国の二国間協定が締結された³。米国のセーフハーバー協定の有効性をめぐる議論は、その後2013年にエドワード・スノーデン氏が、米国国家安全保障局(NSA)の行っていたネット監視問題をめぐる膨大な機密情報を暴露した「スノーデン事件」を契機に、当時のEUのデータ保護に対してEU市民に大きな疑問を投げかけることとなる。同年、オーストリア市民のMaximilian Schrems氏が起こした、米国へのEUデータ移転の有効性に対する訴えはSchrems判決(シュレムス判決)として世界のデータ流通に大きな衝撃を与えることとなる。Schrems氏の訴えについて、「米国政府による諜報活動はEUの制度に比べて十分な保護を提供していない」等として、2015年に欧州司法裁判所(CJEC)はセーフハーバー協定を無効であるとする判決を下した。

セーフハーバー協定という枠組み自体が否定される結果となったこの判決に、米国企業を中心に世界中のビジネスは大打撃を受けた。これを受けて、2016年にはEU加盟国から米国へのデータ移転に関して新たに「プライバシー・シールド」が採択された。その後、急速な技術発展やデータに関する急速な社会変化に対抗することを目的とし、2016年「GDPR (General Data Protection Regulation) : EU 一般データ保護規則」が発効され、2018年から適用が開始された。EEA内から日本を含むEEA外への個人データの移転は原則として違法とされるが、データ輸出者とデータ輸入者との間で「SCC (Standard Contract Clauses) : 標準契約条項」を締結することが、移転が適法と認められるためのひとつの手段とされている⁴。2020年7月には、プライバシー・シールドについても無効であるとするSchrems II判決(シュレムスII判決)が欧州司法裁判所(CJEU)から出されることとなった。判決理由として、米国政府機関が個人データにアクセスする場合、米国の法に基づく個人データの保護はEUにおける保護と同等のレベルであるとは認められないとのことである。⁵この判決に対応する形で2020年11月には、EUは前述のSCCの内容を厳格化する改定案を発表し、2021年7月に採択された。

このように、プライバシー等の観点から一貫してデータ保護の姿勢を取り、GDPRなどの法整備を進めてきたEUであるが、データのもつ価値を最大限活用し、EUの発展、経済成長、社会課題の解決にかなげるという観点においては、米国や中国などから遅れを取っていると云わざるを得ない。そのような背景において、2020年2月に公表した「欧州データ戦略 (A European strategy for data)」が公表され、「欧州データスペース (European data space)」のビジョンが打ち出された。データスペースとは、「データ主権 (data sovereignty)」と「信頼性 (Trust)」を元にしたデータ流通を基盤とし、民間、公的組織に

³ 総務省 パーソナルデータの利用・流通に関する研究会 (第1回) 配布資料「資料3 EU、米国における個人情報・プライバシー保護等に関する制度の概要」(https://www.soumu.go.jp/main_content/000197631.pdf)

⁴ 「標準的契約条項 (Standard contractual clauses : SCC) (欧州委員会資料の仮訳) (2018年3月)」(日本貿易振興機構 (JETRO), 2018.3.28) (<https://www.jetro.go.jp/world/reports/2018/01/8d894f365ea5c3a7.html>)

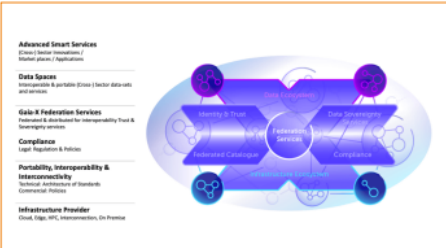
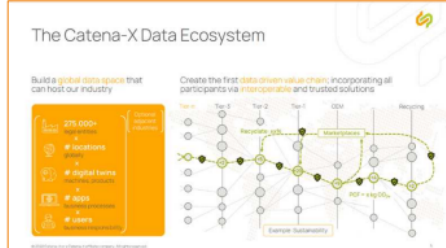
⁵ 「EU司法裁、米国との個人データ移転に関する「プライバシー・シールド」を無効と判断」(日本貿易振興機構 (JETRO), 2020.7.17) (<https://www.jetro.go.jp/biznews/2020/07/d4dfd684421ffb4b.html>)

おけるデータがシームレスに行き来するデジタル領域であると、「欧州データ戦略」にて定義されている。このデータスペースの構築は、2015年ごろから欧州委員会（EC）が戦略として提唱している「デジタル単一市場（a single market for data）」を実現する上で鍵となるとされており、EUにおけるデータ戦略の特徴の1つでもある。データスペースの構築がなされることで、データ共有や流通が促進され、結果としてデータ駆動型のイノベーションがもたらされ、EU デジタル単一市場の実現にもつながるとされている⁶。

さらに、「欧州データスペース」を技術面において支えるインフラストラクチャーを開発する取り組みとして、2020年6月に発足したのがデータ基盤プロジェクトの「GAIA-X（ガイア・エックス）」である（図表 3-2）。従来と異なる点としては、ルール、システム、そしてエコシステムを一体的に整備することで、他国に奪われつつあるデータ主権を取り戻す狙いがある⁷。インフラとしてのエコシステムと、データのエコシステムが一体となることによって、データ流通を効率化し、行政サービスやコンプライアンスの向上を図る仕組みとなっている⁸。

図表 3-2 欧州のデータスペース構築と GAIA-X の概要

- 欧州では、データスペースの確立と、様々な分野のデータが連携されるデータの単一市場（a single market for data）に向け、産業界側で分野横断的に、その哲学や考え方をまとめる**GAIA-Xが各種ドキュメントを積極的に公表**
- ドイツのフ라운ホーファが開発した技術を基礎に、コネクタ技術の実装を自動車分野で目指す**CATENA-Xなどが、政府の支援を受けて、その技術の現場での実証・実装を実施**。CFP規制の動きなどが取組加速に向けた起爆剤に。

| 欧州データ戦略 | |
|---|--|
| <ul style="list-style-type: none"> 産業・商業データはデジタル経済の推進力。利用可能データの拡大や、データ生成者の権利確保を推進。 欧州がデータ分野のリーダーになるため、データスペースやクラウドインフラ・サービスに総額40～60億€投資。 | |
| ①データスペースのコミュニティ構築 | ②データスペースの実装 |
| Gaia-X（2019年10月に独・仏政府が発表） ・ 欧州の価値観に則ったクラウドインフラを定義・構築し、産業・商業データの利活用を促進 | Catena-X（2021年3月設立、2023年稼働予定）の例 ・ 自動車業界のサプライチェーン全体を通じてマテリアルフローを追跡可能とする、データのエコシステムを構築 |
|  <p>欧州以外のプラットフォームへの対抗を意識しつつ、欧州に必要なインフラの考え方を議論。</p> <p>The European Data Strategy https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283 Gaia-X Architecture https://www.gxfs.eu/connection-to-gaia-x/ Catena-X https://catena-x.net/fileadmin/user_upload/Vereinsdokumente/Catena-X_UEbersicht.pdf</p> |  <p>ドイツ連邦政府は中小企業にも積極的に参加を呼びかけ、ドイツの産業戦略を立ち上げ。</p> |

出典：デジタル庁 データ戦略推進ワーキンググループ（第5回）「資料2-1 データ連携により実現可能なサービス」（2022.12.21）

⁶ 「欧州で推進されるデータスペースとは？～データ共有の新しい潮流～」(株式会社 NTT データ, DATA INSIGHT, 2022.11.4) (<https://www.nttdata.com/jp/ja/data-insight/2022/1104/>)

⁷ 「各国が推進する「データ取引市場」関連最新動向」(世界経済フォーラム第四次産業革命日本センター, 2021.7.15) (<https://note.com/c4irj/n/n98547fb73e67>)

⁸ Gaia-X「What is Gaia-X?」(2023.1.30 閲覧時点) (<https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html>)

(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/541c6d41-59b2-4017-8b06-833f7483fdc8/faf967cc/20221221_meeting_data_strategy_outline_02.pdf)

このように、EU は人権やプライバシーを最優先事項としながらも、デジタル単一市場の実現に向けたプロジェクトや戦略を効果的に打ち出すことで、データの価値を活用できる仕組みの構築を進めている実情がある。

2) 米国

米国は、ビジネスの成長やデータの利活用を最重要視しており、データの越境移転を推進することを念頭に置いた国家戦略を取っている。GAFA をはじめとする巨大 IT 企業を多く抱える米国は、民間部門におけるデータ活用促進が活発であり、個人情報保護などプライバシー観点でのデータ保護には強くは介入しない姿勢を見せている。国家主導での戦略としては、2019 年 6 月の連邦データ戦略に基づいて、公的部門におけるデータ価値向上やガバナンス体制の構築を急速に進めている背景がある。また、NSCAI (National Security Commission on Artificial Intelligence) が、国防分野において AI 活用を高度化することなどが盛り込まれた最終報告書が 2021 年 3 月に発表されている⁹。

民間部門に関するデータ活用および保護に関する介入を行わない、自由奔放的な戦略をとってきたアメリカにおいて、現状は個人データの保護に関する包括的な連邦法は存在していない。すなわち、国主導での個人情報保護に関する法整備がなされておらず、これが、前述の欧州司法裁判所が一連の Schrems 判決においてセーフハーバー協定やプライバシー・シールドを無効とする判決を下した理由となっていた。また、図表 3-3 に示す通り、金融や医療など分野別のデータ関連の個別法としては、Electronic Communications Privacy Act of 1986 (ECPA: 電子通信プライバシー法)、Gramm Leach Bliley Act (GLBA: グラム・リーチ・ブライリー法)、そして Health Insurance Portability and Accounting Act (HIPAA) があるが、いずれもデータの越境移転に関する規定は定められていない。

歴史的にデータ保護に関する規制がない状態が続いていた中、2022 年 6 月、「ADPPA (The American Data Privacy and Protection Act: 米国データプライバシー・保護法案)」の草案が公表された。背景としては、GAFAM をはじめとする巨大 IT 企業によるさまざまな個人情報管理が国民の社会生活に与える影響の大きさやリスクを無視できなくなってきたこと、過去にも同様に作られ、廃案となった政策立案とは対照的に、超党派での草案の提出に至った¹⁰。そのため、同法案は超党派での支持を集めており、法案が可決される機運が高まっている。内容は、ユーザー認証や詐欺防止など、法案に明記された 17 の事項に該当する目的以外でのデータ収集および利用を禁止している。

この法案は、個人情報保護他国ほどセンシティブになる必要なくデータ活用を行いながら成長を続けてきた、米国の様々な産業にとって根本的な転換をもたらすこととなる。米国におけるプライバシ

⁹ デジタル庁「包括的データ戦略」(2023.1.30 閲覧時点)

(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/02063701/policies_data_strategy_outline_02.pdf)

¹⁰ 「米国版 GDPR 策定へ 個人情報の扱いに忠実義務求める - Global Economics Trends 編集委員 瀬川奈都子」(日本経済新聞, 2022.8.22)

一保護派としてはより厳格な内容を要求しているが、全体として ADPPA は議会での評判も極めてよく、下院商業委員会では、法案を議会へ提出することに賛成 53、反対 2 という圧倒的に賛成票が多い結果からも推察できる¹¹。

図表 3-3 米国のデータ関連規制の現状

| 制度名 | 対象者 | 対象データ | 制度の目的 | データ越境流通に関する制度の内容 |
|---------------------------|------------------------------------|--|--------|---|
| 電子通信プライバシー法 (ECPA) | 個人データの電子的保存を行う公的部門 (含地方自治体) 及び民間部門 | 電子通信 (有線又は電子システムによって全部又は部分的に送信される、あらゆる性質の記号、信号、文章、画像、音声、データ、又は情報の伝達) | 個人情報保護 | データの越境移転に関する規定は定められていない |
| グラム・リーチ・ブライリー法 (GLBA) | 金融サービス業に「実質的に従事する」民間の金融機関 | 非公開個人情報 (金融サービスの提供を通じて顧客から収集されるあらゆる情報) | 個人情報保護 | データの越境移転に関する規定は定められていない (金融機関が非関連第三者に対して非公開個人情報を開示する場合、顧客にオプトアウトの機会を提供する) |
| 医療保険の携行性と責任に関する法律 (HIPAA) | 公的機関 (含地方自治体) 及び民間機関 | 保護されるべき健康情報 (健康状態、医療の提供、医療費の支払いに関連する情報で、個人に結びつけることが可能なもの) | 個人情報保護 | データの越境移転に関する規定は定められていない |

出典：経済産業省 データの越境移転に関する研究会「データの越境移転に関する研究会報告書」(2022.2.28)

(https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_1.pdf)

3) 中国

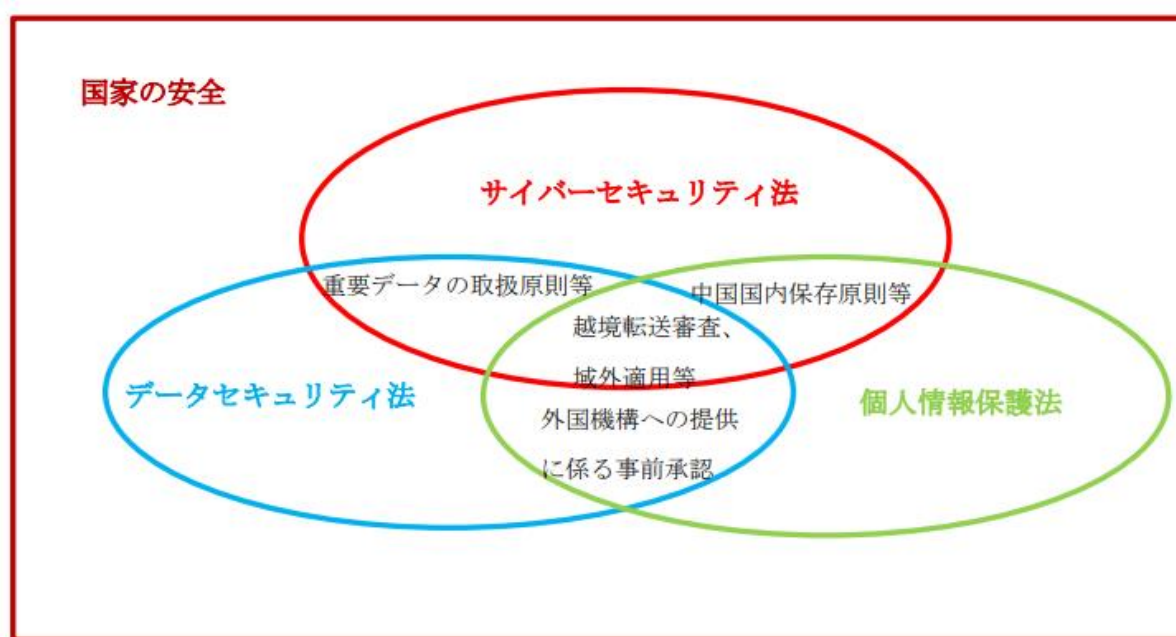
中国共産党主導での中長期的な国家戦略を掲げる中国であるが、本論ではデータに関する政策のうち特に国内におけるデータ保護、データ利活用、そして国外におけるデータ収集の3点について整理する。

中国のデータ保護政策を理解する上では、「安全保障」「国家の関与」の2つのキーワードが広く認識されているであろう。中国共産党政権の安全保障に関する基本方針「総体的国家安全観」では、いわゆるハードパワーである軍事だけでなく、ソフトパワーに分類される文化なども11領域ある安全保障の対象に位置付けられている。また、情報も11領域のうちの1つに該当する。弊社が編集・発行している情報誌である「情報未来」の2022年3月号の「経済安全保障から見た米中関係」によると、総体的国家安全観の背景には、中国の世界経済・産業におけるプレゼンスが高まるにつれてこれを抑え込もうとする動きが強まり、この対外的な圧力が中国国内に存在する発展の不均衡など「矛盾」と結びついて国家の「安全」が脅かされることを警戒しているとされる。従って、国内の脆弱な要素を解決し、国内

¹¹「米国のデータプライバシー保護法が、ついに実現へ？ ここにきて超党派の支持が集まった理由」(WIRED, 2022.7.5) (<https://wired.jp/article/american-data-privacy-protection-act-adppa/>)

と対外関係とを合わせた一体的な国家安全システムを構築する方針を示していると理解できる¹²。これらの背景から国によるデータのコントロールを推し進める中国だが、サイバーセキュリティ法、データセキュリティ法、そして個人情報保護法の3つが、データに関する法規制としては記憶に新しい。それぞれの規制は、図表 3-4 に記載されているイメージのとおり、守備範囲がある程度重なり合っており、データの越境移転、データローカライゼーション、ガバメントアクセス等の政策など、3つの規制で包括的にデータ規制をカバーしあっている。

図表 3-4 中国データ関連3規則



出典：「中国におけるサイバーセキュリティー、データセキュリティーおよび個人情報保護の法規制にかかわる対策マニュアル」（日本貿易振興機構（JETRO），2021.11.18）

https://www.jetro.go.jp/ext_images/_Reports/02/0c080037fe572f0d/202111.pdf

¹² 「経済安全保障から見た米中関係」（株式会社 NTT データ経営研究所, 情報未来 No.69(2022 年 3 月号))
<https://www.nttdata-strategy.com/knowledge/infofuture/69/report11.html>

図表 3-5 中国データ関連3規則の比較

| 制度名 | 対象者 | 対象データ | 制度の目的 | データ越境流通に関する制度の内容 |
|----------------|---|---|---|---|
| 個人情報保護法 (2021) | ①重要情報インフラの運営者 ②取扱いに係る個人情報 が国家ネットワーク情報部門所定の数量に達する個人情報取扱者 ③中国境内に保存された個人情報 を外国の私法又は法律執行機関に対して提供する個人情報取扱者 | ①重要情報インフラの運営者が中国境内で収集した個人情報 ②所定の数量に達する個人情報 ③外国の司法又は法律執行機関に対して提供する個人情報 | | 重要情報インフラの運営者及び取扱いに係る個人情報が国家ネットワーク情報部門所定の数量に達する個人情報取扱者は、中国の国内において収集し、及び発生した個人情報を国内において保存しなければならない。 国外に提供する必要がある場合には、国家ネットワーク情報部門が組織する安全評価に合格しなければならない。法律・行政法規及び国家ネットワーク情報部門が安全評価を行わなくてよい旨を定める場合には、その規定に従う(40条)。 また、主管機関は、関連する法律及び中国が締結し、若しくは参加する国際条約若しくは協定に基づいて、又は平等互恵原則に従い、外国の司法又は法律執行機関による国内に保存された個人情報の提供に関する請求を処理する。主管機関の認可を経ない場合には、個人情報取扱者は外国の司法又は法律執行機関に対して中国境内に保存されている個人情報を提供してはならない(41条)。 |
| 制度名 | 対象者 | 対象データ | 制度の目的 | データ越境流通に関する制度の内容 |
| サイバーセキュリティ法 | 重要情報インフラの運営者(37条) | 中国国内での運営において収集、発生させた個人情報及び重要データ(37条)。外国の事業者からの移転により取得した個人データには適用されない場合があると解される。 | ネットワークの安全保障、ネットワーク空間の主権並びに国の安全及び社会の公共の利益の保持、諸組織の適法な権利利益の保護、経済・社会の情報化の健全な発展の促進 | 域外移転を行うことに業務上の必要性がある場合には、国家ネットワーク情報部門が國務院の関係部門と共同して制定する弁法39に従い安全評価を行わなければならない。かつ、国の関連規定及び関連基準の要求に従わなければならない(サイバーセキュリティ法 37条後段)。 中国国内で業務を展開し、製品又はサービスを提供する活動を通じて収集した個人情報及び重要データについては、中国国内に保存する必要がある(サイバーセキュリティ法37条前段)。外国企業であってもかかる要件を満たす限り規制の適用を受け、収集した個人情報を中国国内のサーバーに保存する必要がある。 |
| データセキュリティ法 | ①重要情報インフラの運営者 ②中国境内の組織又は個人(36条) | ①重要データ ②中国境内に保存されているデータ | 国家主権、安全と利益発展の維持 | ①国の安全と利益の維持、国際的義務の履行の維持に関連する管理品目に該当するデータに対して、法に基づき輸出管理を実施する(データセキュリティ法25条)。 ②中国国内で保存されているデータの取り寄せを外国の司法又は法律執行機関から要求された場合、中国主管部門の認可を経ずに当該データを提供してはならない(データセキュリティ法36条)。 |

出典：経済産業省 データの越境移転に関する研究会「データの越境移転に関する研究会報告書」(2022.2.28)

(https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_1.pdf)

そのほか、関連する規定が存在するものとしては、「サイバーセキュリティ法」(2017年6月1日より施行)、「データセキュリティ法」(2021年9月1日より施行)がある。(図表 3-5) DFFT に関連して、データローカライゼーションに関する内容が含まれる「サイバーセキュリティ法」の 37 条には、データの越境移転の制限に関する安全評価制度が規定されている。この条項は、個人データを取り扱うビジネスを中国において運営する場合、当該データを中国で保管することを義務付ける国内保管義務、いわゆるデータ・ローカライゼーションを一定範囲で求めるものとなっており、データの越境移転の規制を中心に据えている欧州や日本とは大きく違う点となっている。また、例外的なデータの越境移転を行う場合は、安全評価が必要となっている¹³。

また、2021年11月末には、ビッグデータ産業の5か年計画を発表しており、ビッグデータ産業の規模を2020年から2025年までで3倍に相当する3兆元(約53兆円)に引き上げるとしている。他国の

¹³ 松尾 剛行 (2022)「中国の個人情報保護法とデータ運用に関する法制度の論点」(総務省 学術雑誌『情報通信政策研究』第5巻第2号, P39)(https://www.soumu.go.jp/main_content/000800520.pdf)

制裁などの影響を受けない形でのビッグデータ産業体系の構築を目標とし、データを活用して社会管理を進め、通信、金融、医療、公安、交通、電力などの重要インフラをはじめとし、農業・水利、就業などを重点的に利用拡大する分野として挙げている¹⁴。また、前述の EU だけでなく、中国においてもデータ取引市場が定着しつつある。20 年以上前の 2001 年ごろからデータ取引市場が創設され始め、現在 10 以上の取引所で金融、エネルギー、モビリティ、農業、観光、教育、ヘルスケアなどの分野で、データセットや分析結果が売買される状況となっている¹⁵。また、単なるデータ販売だけでなく、データの収集、加工、分析やデータ提供を支援するサービスも有効であるとされており、データ流通のみならず必要なデータを生成、提供することでビジネスチャンスにつなげているとされている¹⁶。

ここまで、中国国内におけるデータ保護およびデータ利活用について述べたが、DFFT に関連してデータの越境移転に関して特に欧米各国が危険視していることとして、中国が国内におけるデータ管理体制構築だけでなく、国外のデータや情報を取り込むための動きを加速化させていることにある。2021 年末に米紙ワシントン・ポストが報じた内容には、中国当局が Twitter や Facebook などの国外のソーシャルメディアを 24 時間態勢で監視し、学術専門家、政治家、ジャーナリストに関する SNS 上の情報をもとに、データベースを構築しているとされている。膨大な数の越境データや情報が中国国内に流れ込んでいるとされ、今までは中国国内を中心に行われてきた言論統制や検閲といった仕組みを海外における情報に対して行うようになってきている現状が見て取れる¹⁷。また、中国共産党は監視だけでなく諜報活動、宣伝工作など複数の目的でデータを収集し、収集したデータをもとに顔認証や音声認識をとった AI (人工知能) を使って宣伝工作を行っているとされている。多言語でのデータ収集が進み、機械翻訳の精度が上がれば、他国における宣伝工作の質は上がるとされ、当局によるデータの関与はさらに強まることが予想される¹⁸。

4) 日本

データが国の豊かさや国際競争力の源となることが認識され始め、各国がデータ戦略を策定し、戦略に基づいた法規制や技術開発を行ってきたなか、日本は長らくデータに関する戦略の不足が指摘され、求められてきた。2021 年 6 月、日本ではじめて「包括的データ戦略」が閣議決定され、理念、ビジョン、行動指針、アーキテクチャとしてのレイヤー構造などが明らかとなった。図表 3-6 に示すように、アーキテクチャ＝日本全体のデータ構造には 7 つの階層と 2 つの横断的な階層が位置付けられ、戦略の基礎として常にこのアーキテクチャを踏まえて実践が行われる。また、デジタル庁が 2021 年 9 月に発足とな

¹⁴ 「中国、25 年にビッグデータ産業規模を 3 倍に 政府計画」(日本経済新聞, 2021.11.30)

¹⁵ 「各国が推進する「データ取引市場」関連最新動向」(世界経済フォーラム第四次産業革命日本センター, 2021.7.15)
(<https://note.com/c4irj/n/n98547fb73e67>)

¹⁶ 「中国・韓国におけるビッグデータ流通プラットフォーム」(株式会社日立コンサルティング, 2020.6.30)
(https://www.hitachiconsulting.co.jp/column/asia_data/03/index.html)

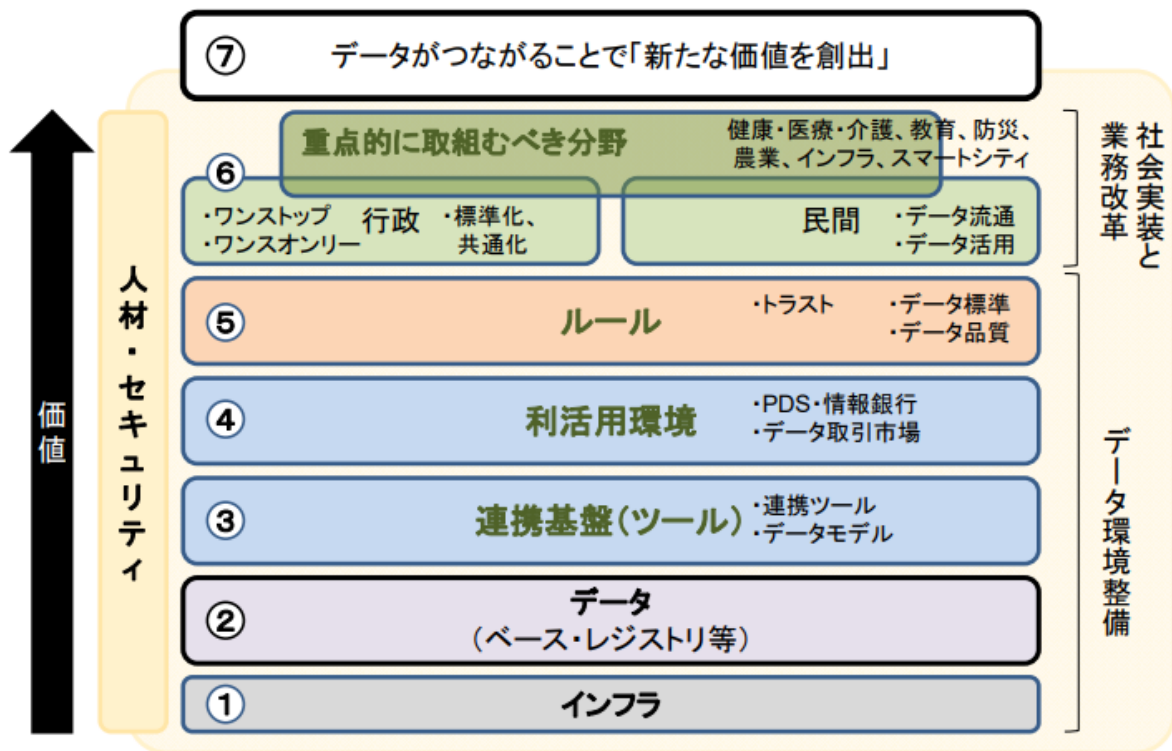
¹⁷ 「China harvests masses of data on Western targets, documents show」(The Washington Post, 2021.12.31)
(https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html)

¹⁸ 「中国が進める世界規模のデータ収集「リスク認識を」」(朝日新聞デジタル, 2021.7.2)
(https://digital.asahi.com/articles/ASP716THGP6WULZU00H.html?_requesturl=articles%2FASP716THGP6WULZU00H.html)

り、行政システムの構築のみならず日本社会全体のデジタル化の司令塔としての役割を果たすこととなっている。また、「包括的データ戦略」には、「IV 国際連携」の章があり、この中では DFFT の意義、これまでの取り組み、今後の方向性について述べられていることから、日本のデータ戦略において DFFT が重要な意味を持つことが改めて理解できる。

包括的データ戦略において、注目すべき事項として「データ取引市場」のコンセプトが打ち出されていることにある。通常、対企業間でのデータの取引が行われるため、それぞれの個別のやりとりにおいては新しい取引相手の発見機会が乏しい状況にある。また、新しい取引相手とデータのやりとりを行うことは、データ提供者、データ利用者はお互いに信用（トラスト）がないため、データの取引には躊躇いが生じてしまう。この状況を打開するうえで、「適切なマッチングの増進」および「取引に関するトラストの担保」が重要となるとされ、そのためにはデータ取引市場の運営事業者が中立公正な立場から取引の安全と信頼を担保するガバナンス体制を構築すること必要であるとされた¹⁹。「データ取引市場」のコンセプトは、前述の EU、中国の項目においても述べた通りであるが、現在世界各国において推進されており、日本政府の方針を打ち出した形となる。

図表 3-6 包括的データ戦略のアーキテクチャ



出典：デジタル庁「包括的データ戦略」(2021.6.18)

(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/02063701/policies_data_strategy_outline_02.pdf)

¹⁹ 「包括的データ戦略とデータ取引市場構想」(世界経済フォーラム第四次産業革命日本センター, 2021.7.12)

(<https://note.com/c4irj/n/n3dd91a335a86>)

また、日本による DFFT の推進に関して、大きな役割を果たしているとされているのが「世界経済フォーラム第四次産業革命日本センター」である。図表 3-7 に示すとおり、3つの注力すべき取り組みを掲げ、2019年のダボス会議以降 DFFT の実装に向けた取り組みを続けている。

図表 3-7 DFFT の実装3つの取り組み

| Data Free Flow with Trust (DFFT) の実現に向けた 世界経済フォーラム第四次産業革命日本センターの取組 | | |
|--|---|---|
| 国境を越えた自由なデータ流通 | 個人・企業・都市間の 自由なデータ取引市場 | 規制・ルールのアップデートによる トラストの再設計 |
| <ul style="list-style-type: none"> ◆ インターオペラビリティ（相互運用性）を確保することで、国家間のルールの壁を打ち破り、国境を越えて自由にデータを流通することを目指す ◆ 各国が異なる法制度をもつなかで、包括的な標準化を行うのではなく、各国家のルールのギャップを補う架け橋の構築に臨んでいる | <ul style="list-style-type: none"> ◆ 世界経済フォーラムにて取り組まれている 「DCPI (Data for Common Purpose Initiative)」に対応 ◆ DCPIは、疫病予防や防災などの「社会全体の共通の目的」において、個人データを第三者が活用する際のルール制定、システム設計、基盤となる市場の整備を行っている ◆ 日本センターは、政府、企業、アカデミアなどを巻き込み、データ取引市場の実証実験を推進している | <ul style="list-style-type: none"> ◆ 国境を越えた自由なデータ流通や、個人・企業・都市間の自由なデータ取引市場を実現するうえでは、各国や地域の法規制を踏まえ、新たなデータガバナンスの仕組みを構築していくことが必要不可欠 ◆ 日本センターは、世界の先進事例に基づく知見を、日本のステークホルダーにつなぐことで議論の場を提供し、アジャイル・ガバナンスの構築を目指している |

出典：「DFFT(Data Free Flow with Trust): 信頼性のある自由なデータ流通」（世界経済フォーラム第四次産業革命日本センター, 2020.11.4）(<https://note.com/c4irj/n/ndca7be20691a>)を元に作成

また、国際外交においても、DFFT は注力すべき項目の1つとして位置づけられている。図表 3-8 に概要を示している FOIP (Free and Open Indo-Pacific: 自由で開かれたインド太平洋) は日本外交の重要な基本方針の1つであり、外務省や経済産業省などが中心となって推進されている枠組みであるが、FOIP における経済産業省の3つの注力分野である「資源・エネルギー」「デジタル」「インフラ」のうちの、「デジタル」において、DFFT に基づいた国際的なデータ流通ルール形成に向けた WTO 電子商取引交渉等での議論の推進が明記されている²⁰。

²⁰ 経済産業省「FOIP (自由で開かれたインド太平洋)」(2021.7.6)
(https://www.meti.go.jp/policy/external_economy/trade/foip/index.html)

図表 3-8 自由で開かれたインド太平洋（Free and Open Indo-Pacific）の概要



出典：外務省「外交政策 自由で開かれたインド太平洋」（2022.5.16）

https://www.mofa.go.jp/mofaj/gaiko/page25_001766.html

3.1.2. これまでの国際的な議論の経緯と今後の見通し

(1) 2019年1月にダボス会議でDFFT提唱に至るまで

DFFTがデータ流通に関するコンセプトとして提唱される以前にも、2010年ごろから地域間、また国際会議にて自由なデータ、情報の流通に関する議論がなされてきている。前述のEUにおけるGDPR策定に向けた動きは、地域間におけるデータ流通の枠組みとして、データ保護をメインテーマとして法整備を中心に取組まれてきた。そのほかの地域間における取組としては、アジア太平洋経済協力会議（APEC）で2011年に策定された域内の越境データ移転ルールであるCBPR（Cross Border Privacy Rules：APEC越境プライバシールール）が挙げられる。CBPRは、企業等の越境個人データの保護に関して、プライバシー原則への適合性を認証するシステムとして、APECの取組みとして運用されていた²¹。しかしながら、APECにおける従来のCBPRの議論では、データ流通を活発化したい米国と、国家主導でデータ管理を行いたい中国が対立したことで議論が難航する局面が多く、このような背景を元に、CBPR

²¹ 経済産業省「グローバル越境プライバシールール（CBPR）フォーラム設立に向けた宣言をすることに合意しました」（2022.4.1）<https://www.meti.go.jp/press/2022/04/20220421001/20220421001.html>

は 2022 年に新たに Global CBPR というかたちで策定された。Global CBPR は、「APEC 以外の南米などの国々を取り込むことで、枠組みの拡大を目指す」としつつ、中国の干渉を受けずに米国主導のルール作りを行う狙いがあり、CBPR および Global CBPR は国や地域の思惑が大きく出ている状態である²²。また、2016 年の環太平洋経済連携協定（TPP 協定）では、第 14 章の電子商取引の章において、国境を超える情報移転の自由の確保等について、「各締約国は、対象者の事業の実施のために行われる場合には、情報（個人情報を含む）の電子的手段による国境を超える移転を許可する。」との記載がある。また、「いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、または設置することを要求してはならない。」という、データローカライゼーション要求禁止などを盛り込んでいる。

地域間でのデータ流通に関する議論が徐々に盛んになってきた中で、国際会議においても 2017 年ごろからデータ流通に関する議論が行われるようになってきている。2017 年の G7 の情報通信・産業相会合における「G7 情報通信・産業大臣宣言（G7 ICT AND INDUSTRY MINISTERS' DECLARATION）の本文には、開かれた、自由なグローバルインターネットを支え、経済成長を促す目的で、「国境を越えた情報の自由な流通の促進」が盛り込まれている²³。同年の G20 サミットにおいても、「我々は、プライバシー、個人情報の保護及び知的財産権に関する適用可能な法的枠組みを尊重しつつ、情報の自由な流通を支持する。」との文言が盛り込まれ²⁴、国境を越えた情報の自由な流通を支持することが各国間で合意されている²⁵。

DFFT 提唱前の状況を概観すると、急増するデータ流通量に対し、各地域において対策が見られるようになった一方で、G7 や G20 における主要なテーマとしての議論はなされておらず、また世界共通のデータガバナンスを支える取り組みも不十分であったといえる。様々な分野において、世界共通のデータ流通における枠組みの必要性が必要とされつつも、それぞれの地域、国における方向性が大きく異なっていた時代においては、国際的な取り組みが策定されるに至らないままであったと推測される。

このような背景において、2017 年 12 月の「第 11 回 WTO 閣僚会議」での電子商取引交渉の議論がなされた。デジタル経済について、有志国による共同声明イニシアティブが発出され、現在は 86 か国が参画する WTO 電子商取引交渉が活発化している²⁶。世界的に個人情報保護によるデータ規制が増加した結果として、電子商取引を含むデジタル貿易に関するルールメイキングが必要とされ、その文脈においてデータ規制に関する議論が活発化した。2018 年 12 月までに 9 回の会合が開催され、2019 年 1 月のダボス会議において、有志国による閣僚共同声明が発出されるに至った²⁷。

WTO における閣僚共同声明と時を同じくして、2019 年 1 月、安倍元首相がダボス会議に出席。演説

²² 「米、データ流通で中国排除狙う APEC ルール見直し提案」（日本経済新聞, 2020.8.21）

²³ 総務省 G7 2017 「G7 ICT AND INDUSTRY MINISTERS' DECLARATION」

https://www.soumu.go.jp/main_content/000509689.pdf

²⁴ 外務省 G20 2017 「G20 ハンブルク首脳宣言」（2017.7.7）<https://www.mofa.go.jp/mofaj/files/000271331.pdf>

²⁵ 「【2023年G7で注目、DFFT徹底解説】国際的なデータ移転ルールどう作るか？「DFFT」を各国がいま議論するワケ」（日経クロステック, 2022.12.19）<https://xtech.nikkei.com/atcl/nxt/column/18/02299/121400001/>

²⁶ 外務省（2021）「令和3年版 外交青書・白書」

²⁷ 「増加するデータ関連規制、世界的な調和は図れるか」（日本貿易振興機構（JETRO）, 2019.5.16）

<https://www.jetro.go.jp/biz/areareports/2019/3b8bf9106614b766.html>

において DFFT というコンセプトを提唱し、同年 6 月に開催される G20 サミットにおいて、「世界的なデータ・ガバナンスが始まった機会として、長く記憶される場と致したく思います。」と述べた。これを受けて、2019 年 6 月に開催された G20 大阪サミットにおいて、デジタル経済、特にデータ流通や電子商取引に関するルール作りを進めるための「大阪トラック」を立ち上げるに至った。「大阪トラック」は、その後、デジタル経済や電子商取引に関する国際的なルール作りを進めていくプロセスとして、2019 年、2020 年 1 月ごろまで様々な会合が開催された²⁸。そのような国際的な討議の場はそれまで存在しなかったことから、この「大阪トラック」は、関連するプライバシー、セキュリティ、データへのアクセスなどの課題にあらゆる側面を討議する最初の国際的なイニシアティブであったとされている²⁹。

(2) DFFT 提唱後の国際会議における議論の展開

2019 年の DFFT 提唱後、先に述べた「大阪トラック」において、デジタル貿易を中心として、データ流通に関する様々な会合が開催された。提唱後から 2021 年ごろまでは、国際会議においてはあまり大きな動きは見られず、電子商取引規定関連の規定や、地域間における協定等で DFFT に関連する内容の一部、データの越境移転に関して議論されることが主であった。

地域間の動きとしては、2020 年 11 月に署名された RCEP (Regional Comprehensive Economic Partnership Agreement : 地域的な包括的経済連携協定) に、越境データ流通に関する規定が盛り込まれている。RCEP は中国が主要国として参加しており、合計 13 개국、世界の GDP、貿易総額、人口の約 3 割にのぼる経済連携協定である³⁰。内容については、2018 年に署名された TPP と同様、データの越境移転に関しては「対象者の事業の実施のために行われる場合には、当該移転を妨げてはならない」と規定されているほか、データローカライゼーションの禁止についても盛り込まれている。TPP と異なる点としては、公共政策におけるデータの越境移転に関して、必要性および正当性については締約国自身が最終判断を行うこととし、安全保障上の重大な利益の保護のために必要である場合には、他の締約国は争わない、すなわち口を出さないという、ことが強調された形となっている。

電子商取引におけるデータの越境移転、という文脈での議論が続いていた中、WTO における検討状況においては、2020 年の 12 月には電子商取引共同声明イニシアティブが出されており、電子商取引においては大きな議論の進展が見られているものの、データ流通を促進する規律については、2021 年に議論を一層深める必要がある、とされているため、議論における対立が続いていたものと推測できる³¹。当時の中国の交渉状況および主張が残されているが、「1) 技術進歩、ビジネスの発展、正当な公共政策目的のバランスを踏まえたリーズナブルな目標設定が重要である、2) 発展段階や政策関心も異なる発展途上国

²⁸ 外務省「国際的なルール作りと政策協調の推進 大阪トラック・プロセス」(2021.12.27)

https://www.mofa.go.jp/mofaj/ecm/it/page25_001989.html

²⁹ 「グローバル・サイバースペースでの信頼を構築するための行動計画」(WORLD ECONOMIC FORUM, 2020.6.5)

(<https://jp.weforum.org/press/2020/06/we-need-data-to-move-seamlessly-more-than-ever-action-plan-launched-to-build-trust-in-global-cyberspace>)

³⁰ 外務省「地域的な包括的経済連携(RCEP)協定」

(https://www.meti.go.jp/policy/trade_policy/epa/epa/rcep/index.html) (2023.1.28 閲覧時点)

³¹ 「国際的なデータガバナンスの課題と対応」(公益財団法人日本国際問題研究所, 2021.3.24)

(<https://www.jiia.or.jp/research-report/post-73.html#sdendnote10sym>)

にも配慮すべきである、3)データ流通、データ保存等の議論を一部の国は主張するが、様々な議論があるのであり、交渉に先立ってより探求的議論が必要である、4)データ流通の基礎にはセキュリティがあるべきだ」というのが原則的な議論であったとされ、交渉が難航する理由の1つであったことがうかがえる³²。

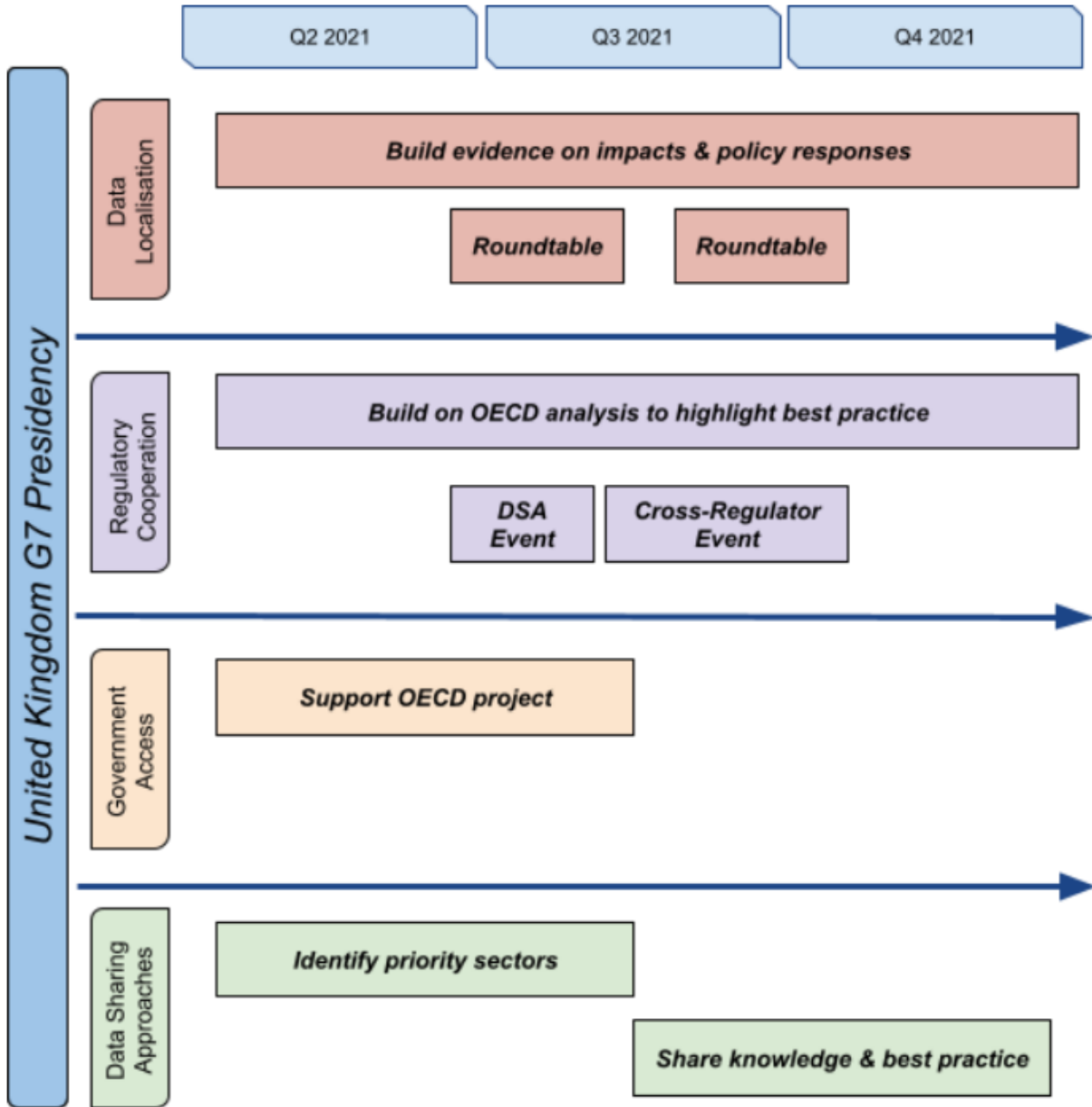
2020年末までは、DFFTというキーワードが国際会議や地域間の会議において用いられる機会は少なかった中大きな進展を見せたのが、DFFTのロードマップが初めて提示された2021年4月28日・29日開催のG7 Digital and Technology Track (G7 デジタル・技術大臣会合)である³³。(図表 3-9) 主な内容としては、データローカライゼーションの影響に関する分析を行うこと、越境データ・フローにおける各国の規制について、共通項をもとに最適解の調整アプローチ方法を検討すること、政府による民間企業へのデータアクセスに対する合理性を検討すること、データ流通アプローチについての優先分野を検討することの4点が挙げられている。

³² WTO, "Joint Statement on Electronic Commerce- communication from China" (INF/ECOM/19, 2019.4.24) (https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=253697,253698,253699,253560,252791&CurrentCatalogueIdIndex=3&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True)

³³ 総務省 「G7 デジタル・技術大臣会合（テレビ会議）の開催結果」（2021.4.30）
(https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000222.html)

図表 3-9 G7 ROADMAP FOR COOPERATION ON DATA FREE FLOW WITH TRUST

Roadmap



出典：「Ministerial Declaration G7 Digital and Technology Ministers' meeting」（2021.4.28）
https://www.soumu.go.jp/main_content/000748187.pdf

G7で示されたロードマップを元に、同年6月に開催されたG7コーンウォール・サミットでのデータ流通に関する議論が行われ、採択された共同宣言の全文にて、「引き続きデータ保護に関する課題に対処しながら価値のあるデータ主導の技術の潜在力をより良く活用するため、信頼性のある自由なデータ流通を擁護すること。そのために我々は、デジタル大臣による「データフリーフローウィズトラストに関する協力のためのG7ロードマップ」を承認する。（仮訳）³⁴」として、一定の進展を見せた。

³⁴ 「G7 サミット 共同宣言の全文」（日本経済新聞, 2021.6.14）
<https://www.nikkei.com/article/DGXZQOUA143KS0U1A610C2000000/>

DFFT の提唱国である日本においては、同年 9 月に就任した岸田首相の所信表明演説で「DFFT の実現」という文言が盛り込まれ、さらには DFFT の具体化に向けた議論において世界をリードすべく、同年 11 月には経済産業省主導により「データの越境移転に関する研究会」が発足された。第 1 回の開催に際して、DFFT の仕組み構築に関してロードマップが作成され、2023 年の G7 を見据えた動きが加速化した。(図表 3-10)

図表 3-10 DFFT を実現する仕組みの構築に関するロードマップ

【第 1 段階】 データの取扱いに関する制度の問題点をお互いに指摘し合う

- 2021年秋に勉強会を立ち上げ、2021年度内に成果を公表。
 - ・ 越境流通のニーズが高いデータ（具体例）
 - ・ 各国のデータ取り扱いに関する制度の概要
 - ・ 比較分析に必要な枠組みの要素

【第 2 段階】 各国間のギャップ分析を国際機関と連携して実施

- データ取扱いに関する各国の制度を同じ尺度で比較分析する調査を2022年度中に実施
- 比較分析の枠組みとして、日本で検討中の「データ・マネジメント・フレームワーク」[※]も 1 つの選択肢

※データを軸に置き、データのライフサイクルを通じて、その置かれている状態を可視化してリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とするフレームワーク。経産省が提案（2021年10月 一次パブコメ終了）。

【第 3 段階】 各国間のギャップの調整措置を行うための体制の構築を決定（2023年G7）

- 各国間のギャップを調整する措置の実行とモニタリングを行う体制を有志国で構築することをG7（2023年日本開催）で宣言。

出典：経済産業省 データの越境移転に関する研究会（第 1 回）配布資料

「資料 3 データの越境移転に関する研究会 事務局説明資料」（2021.11.1）

(https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/001_03_00.pdf)

DFFT における議論が徐々に盛り上がりを見せる中、国際会議において大きな進展を見せたとして特筆すべきは 2022 年 5 月の G7 デジタル大臣宣言である。"Strong together"をテーマに、①デジタル化及び環境、②標準化、③信頼性のある自由なデータ流通（以下、「DFFT」）、④デジタル競争市場、⑤オンラインの安全性（eSafety）、⑥電子的移転可能記録（ETRs）の 6 分野に加え、ロシアのウクライナ侵攻に関連して、サイバー・レジリエンスについての議論が行われた中で、核となる 6 分野のうちの 1 つとして、DFFT が据えられた。

DFFT 促進へのコミットメントとして、DFFT のための証拠基盤の強化、将来の相互運用性促進のための共通性の構築、規制協力の継続、デジタル貿易の文脈における DFFT の促進、国際データスペースの展望に関する知識の共有 5 つの項目がアクションプランとして示されている³⁵。

³⁵ 経済産業省「G7 デジタル大臣会合 附属書 1 信頼性のある自由なデータ流通の促進のための G7 アクションプラン」(<https://www.meti.go.jp/press/2022/05/20220512004/20220512004-2.pdf>) (2023.2.13 閲覧時点)

DFFT 推進の推進の立役者の 1 人である経済産業省 国際室 目黒統括補佐は JIPDEC 主催のインタビューで、2021 年と 2022 年の G7 デジタル大臣宣言の大きな違いの 1 つとして、2021 年 G7 はでトレードトラック、すなわちあくまでも貿易に関連するデジタル原則の採択がメインとなっていたが、2022 年 G7 ではデジタルトラックに議論の中心が移ったことで、電子商取引などの貿易という枠組みに留まらず、データ戦略に関する包括的な議論を可能としたことを挙げた³⁶。

また、2022 年 9 月 1 日には、G20 デジタル経済大臣会合がインドネシアで開催され、DFFT に関する内容が議論された。その後開かれた G20 バリ・サミットで発出された「G20 バリ首脳宣言」には、対処すべき事項として、デジタル・デバインド、プライバシー、データ保護、知的財産権及びオンラインの安全性に関する課題を挙げ、「我々は、信頼性のある自由なデータ流通（DFFT）を更に可能にし、国境を越えたデータ流通を促進することにコミットしている。」との文言が盛り込まれた³⁷。

同年 9 月にドイツで開催された G7 データ保護・プライバシー機関ラウンドテーブル会合でも、越境移転についてプライバシー強化技術（Privacy Enhanced Technologies）が議題の 1 つとされており、越境移転のルール面での整備だけでなく、越境移転の際に用いられるプライバシー強化技術についても議論が行われた³⁸。

さらには 2022 年 12 月にスペインで開催された「OECD デジタル経済に関する閣僚会合」では、2 つの閣僚宣言が採択された。1 つは「信頼性のある、持続可能で、包摂的なデジタルの未来に関する閣僚宣言」、DFFT に関連して課題認識や方向性が取りまとめられた。もう 1 つは「信頼性のあるガバメントアクセスに関する高次原則に係る宣言」として、DFFT の具体化にあたって障壁となっている GA に関連した原則を盛り込んだ閣僚宣言を採択した³⁹。特に重要な点としては、「信頼性のあるガバメントアクセスに関する高次原則に係る宣言」において、GA に関して明確な方針が打ち出されたことにある。安全保障や犯罪捜査など正当な目的で収集する際は、法的根拠のもと監督機関などの事前承認を得ることを項目として閣僚宣言に明記したほか、「民主主義や法の支配に反する、無制限で恣意的な GA はいかなる場合も拒絶する」として中国やロシアをはじめとする権威主義国家をけん制する狙いで下記 7 つの原則が作成された。（図表 3-11）

³⁶ 「DFFT の具体化を加速する経済産業省 商務情報政策局 総務課 国際室の取り組み ～ インタビュー取材 経済産業省 国際室 目黒統括補佐～」(一般財団法人日本情報経済社会推進協会 (JIPDEC), 2022.6.6)

(https://www.jipdec.or.jp/library/report/20220606_01.html)

³⁷ 外務省「G20 バリ首脳宣言」(2022.11.15) (https://www.mofa.go.jp/mofaj/ecm/ec/page3_003519.html)

³⁸ 個人情報保護委員会「令和 4 年 9 月「第 2 回 G7 データ保護・プライバシー機関ラウンドテーブル会合」」(2023.1.31 閲覧) (https://www.ppc.go.jp/enforcement/cooperation/international_conference/g7_roundtable_202209/)

³⁹ 一般財団法人日本情報経済社会推進協 (JIPDEC) 「2022 年秋期 OECD CDEP (デジタル経済政策委員会) 会議レポート」 (2023.1.19) (<https://www.jipdec.or.jp/library/report/20230119.html>)

図表 3-11 政府によるデータ収集の7原則

| | |
|------|-----------------------|
| 法的根拠 | 法的根拠に基づくデータ収集 |
| 正当目的 | 反対意見の弾圧などのためにデータ収集しない |
| 承認 | 事前承認の法的枠組みがある |
| 取り扱い | 権限を持つ人だけがデータを扱う |
| 透明性 | 国民が政府の活動を知ることができる |
| 監督 | 独立委員会などの監督機関をもつ |
| 救済 | 収集停止などの救済措置をもつ |

出典：「政府の民間データ収集に7原則 OECD 合意、中国けん制」（日本経済新聞, 2022.12.16）を元に作成

(3) 今後予定されている国際会議および議論の具現化に向けた動き

今後予定されている議論の具体化に関しては経済産業省主催の「データの越境移転に関する研究会」において、2023年以降の動きについても整理されている。前述のとおり、2022年12月に行われたCDEP（デジタル経済政策委員会）において、2022年にOECDと合同で実施されたギャップ分析をもとに、議論がなされた。具体的には、OECD／科学技術イノベーション（STI）局において、2022年2月に取りまとめられた「データの越境移転に関する研究会」の中間報告書における5つのポイント（図表3-12）を元に、企業およびその他関係機関へのインタビュー調査、関連する規制当局及び政策立案者へのインタビュー調査等をギャップ分析がすでに実施された。関連してギャップ分析としてさらに今後、各ステークホルダーが参加するラウンドテーブルの開催が、時期は未定であるが予想されている⁴⁰。

⁴⁰ 経済産業省 データの越境移転に関する研究会（第4回）「資料3 データの越境移転に関する研究会 事務局説明資料」（2022.6.27）（https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/004_03_00.pdf）

図表 3-12 DFFT 具体化に向けて核となる 5 つの領域



出典：経済産業省 「データの越境移転に関する研究会 報告書（概要説明資料）」（2022.2.28）
https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_1.pdf

また、2023 年は G7 の開催国が日本となっており、DFFT の具体化に向けて、現在経済産業省が取り組んでいるのが、図表 3-13 の「Institutional Arrangement for Partnership (IAP=相互運用のための制度的取り決め)」の設立に向けた動きである。現在は主に政府中心で行われている会合（パネル）を、民間企業、大学などデータに関するステークホルダーの参加も促すこと、今までは G7 や G20 など単発的な場での議論がメインであった DFFT に向けた取り組みを、恒久的な事務局を構えることで各ステークホルダーによる会合の実施やプロジェクトの工程管理について、継続的に課題解決が行える場を作っていくことを目的としている。基本的な IAP のスタンスとして、「各国の規制のあり方には口を挟まない」ことである。これは各国それぞれの政策や規制があるなかで、DFFT の実現に向けてはとても重要なポイントであるといえるであろう。また、前述の「データの越境移転に係る研究会」のなかでの OECD との分析結果や議論から、IAP にて想定される政策課題として、データ流通に関する規制の透明性の確保やデータの品質、プライバシー保護の技術などが明確化されてきており、G7 における議論にて重要な役割を果たしていくこととなる⁴¹。

2023 年の 1 月には、世界経済フォーラム年次総会（通称「ダボス会議」）に河野太郎デジタル大臣が登場し、DFFT の実装化に向けた取り組みとして IAP を提唱。具体的な IAP の内容については、前述のとおり、マルチステークホルダーでの参画の呼びかけ、そして「各国の規制のあり方には口を挟まない」というスタンスの中で、別々の規制を断片的に運用するのではなく、「相互運用性 (interoperability)」、「相互的合成 (compatibility)」の 2 つの向上を目指すことがある。それらに加えて、技術対応についても言

⁴¹ 「政策特集 2023 年日本開催 G7 3 つの経済テーマで先読み vol.3 G7 の論点②「デジタル化」データの自由な流通と信頼を確保」(METI JOURNAL, 2022.12.21) (<https://journal.meti.go.jp/p/24752/>)

及がなされた。これは 2022 年の G7 においても「Privacy Enhancing Technology(PETs：プライバシー強化技術)」として示されていたものであるが、制度構築だけでなく技術対応や標準化も IAP の運用に取り込むことで、各国の規制の断片化に対抗する狙いである。さらには、事務局を設置し、プロジェクトベースで実装に向けた取り組みを行うとし、今回のダボス会議にて河野氏が言及したものが、データの越境移転や国内保存に関する規制の国際的なベースレジストリの開発である。これは、ビジネスの観点で非常に重要な施策の 1 つとなるとされる。理由としては、各国が断片的に行っているデータの越境移転に関するルールメイキングである。現状、各国それぞれが異なる規制を打ち出しているがゆえに重複し、複雑化してしまっている。また、経済安全保障上の理由から頻繁にルール改正、変更が行われてしまっている傾向もあり、これは法律事務所などへのアクセスが難しい中小企業やスタートアップ企業などにとっては、アップデートに追いつくことが難しく、それがゆえにビジネスの障壁となっている。事実、このプロジェクトに先立って行われた世界経済フォーラム第四次産業革命日本センターとスイスのザンクトガレン大学の共同提案において、規制情報を一覧化してほしいとの声が企業、業界団体、法律事務所からのヒアリングの結果として判明している⁴²。

図表 3-13 相互運用のための制度的取り決め (IAP)

経済産業省が設置を目指すDFFT具体化のための国際枠組み (IAP)

DFFT (信頼性のあるデータの自由な流通)の実現に向け、産官学が連携して、障壁が何かを抽出し、優先順位をつけて議論。成果をG7などで示す



出典：「政策特集 2023 年日本開催 G7 3つの経済テーマで先読み vol.3 G7の論点②「デジタル化」データの自由な流通と信頼を確保」(METI JOURNAL, 2022.12.21) (<https://journal.meti.go.jp/p/24752/>)

⁴² 「河野デジタル相が G7 に向けて提案、DFFT を実装する官民新枠組みとは」 (日経クロステック, 2023.1.30) (<https://xtech.nikkei.com/atcl/nxt/column/18/02299/012500003/?P=2>)

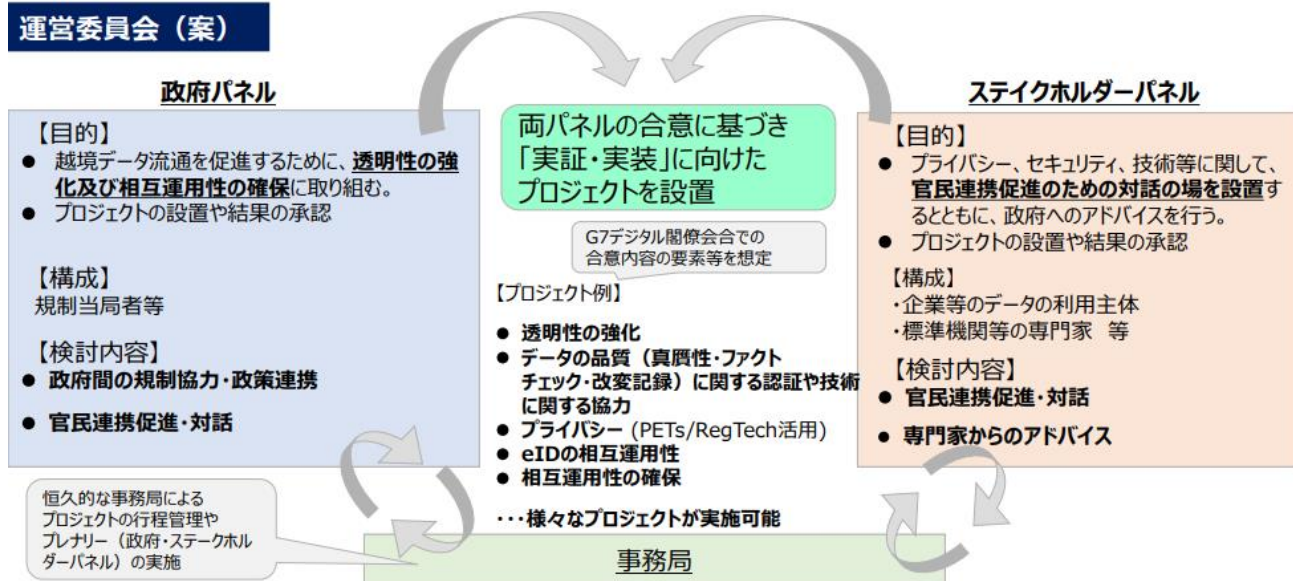
また、G7 における DFDT の議論の場として、2023 年 4 月 29 日と 30 日に、群馬県高崎市において「G7 デジタル・技術大臣会合」が開催される予定となっている。デジタル庁、総務省、経済産業省が主導し、G7 各国に加え、EU や国際機関、その他招待国などの参加が予定されている。会合に先立ち、デジタル庁の「データ戦略推進ワーキンググループ」において、図表 3-14 に示す通り、DFDT のパートナーシップの詳細が記されている。データの越境流通における阻害要因（障壁）を明らかにすることと、越境データ流通に関する各国の規制状況の一覧を提供することなどが盛り込まれている⁴³。各国が異なるデータ規制を運用していることによるデータ規制の複雑性が、ビジネスにおける成長阻害要因となっていることは先に述べた通りであるが、今回の G7 の会議においてこの枠組みの実装について、議論の進展がなされることが期待されている。また、ダボス会議においても話題となった恒常的な事務局の設置についてもこの枠組みに組み込まれており、この枠組みが今後の DFDT の議論を進展させるうえで重要となることが予想される。

図表 3-14 G7 デジタル・技術大臣会合にて議論が予定されている DFDT 推進の枠組み

G7 デジタル・技術大臣会合 DFDT 推進の枠組み（パートナーシップ）の立ち上げ

目的 データ流通を促進し、越境データ流通に係る「障壁」を取り除く。政府と民間（企業、大学など）が協働し、デジタル経済のエコシステムを踏まえた国際制度を実装する。

運営委員会（案）



出典：デジタル庁 データ戦略推進ワーキンググループ（第6回）配布資料「資料2 DFDT の具体化に向けた取組」（2023.2.28）

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/62ec4ac2-783b-4461-8559-df2c5b3e5592/18a6dcccb/20230228_meeting_data_strategy_outline_02.pdf

⁴³ 「令和5年度 経済産業省デジタル関連施策について」（一般財団法人日本情報経済社会推進協会, 2023.2.27）

<https://www.jipdec.or.jp/library/report/20230126.html>

3.1.3. DFFT の実装に向けて焦点となる 3つの事項

ここまで、DFFT の意義、データ流通に関して異なる姿勢を見せる各国の動向、そして国際会議において DFFT に関する議論がどのように推進されてきているのかについて整理した。本項目においては、今後 DFFT を実装させるにあたって重要な観点であるとされる、制度面、技術面、そしてデータ流通環境の整備の 3 つについてまとめる。

(1) 制度面

1) ガバメントアクセス

DFFT の議論におけるポイントの 1 つに、ガバメントアクセス（以下、GA）がある。渡辺（2019）によると、ガバメントアクセス（GA）とは、政府機関等の公的機関による、民間部門が保有する情報への強制力を持ったアクセスを意味する。ガバメントアクセスはデータが個人のものか非個人のものに関わらず、国がデータに関与することが可能となっており、国主導での経済成長に寄与するだけでなく、安全保障においても重要なデータの流出を防ぎ、政府にとって都合の悪い情報をコントロールする上で有効な手段となるなど、特に権威主義国家にとってはなくてはならないデータ戦略の一つといえる⁴⁴。

ガバメントアクセスがどのように行われているかについては OECD が調査を行っている。1 つには、民間企業から政府が直接データを購入する、もしくは企業側が自発的に政府や安全保障機関へとデータを提供するパターンであり、これは犯罪者である可能性があるなど、疑わしいケースにおいてその情報を受け渡すといったケースにも行われる。民主主義国家においては、司法当局などがフォーマルな法的アプローチに則って行われるのに対し、民主主義国家ではない国々においては強制力が用いられると分析されている⁴⁵。

ガバメントアクセスについては、個人データ・非個人データに関わらず、国家の安全保障などを名目にして国が関与、閲覧できる状態を支持する中国を筆頭にした権威主義国家にとっては、データの越境移転に際しても重要な政策の 1 つである。それに対して、欧米各国は、ガバメントアクセスは個人情報保護の観点から人権侵害であるとして非難する論調が強く、国家によってどのようにデータが利用されるかが不透明であり、それ自体がリスクであるとする見方も多いため、ガバメントアクセスを禁止するよう求めている背景がある。

DFFT が直面する課題において、最も困難であると指摘されているのは、データ保護やデータの信頼性の確立について、各国が異なる姿勢やイデオロギーを元にして臨んでいることである。それゆえに、データガバナンスの国際的な調和を困難なものとしているが、大きな問題の一つとしてあげられているのが GA である。2022 年 12 月にスペインで開催された「OECD デジタル経済に関する閣僚会合」において採択された「信頼性のあるガバメントアクセスに関する高次原則に係る宣言」において、無制限で恣意

⁴⁴ 渡辺翔太（2019）野村総合研究所「ガバメントアクセス（GA）を理由とするデータの越境移転制限—その現状と国際通商法による規律、そして DFFT に対する含意—」

<https://www.rieti.go.jp/jp/publications/dp/19j067.pdf>

⁴⁵ 「Towards OECD Principles for Government Access to Data」(LAWFARE, 2021.12.20)

<https://www.lawfareblog.com/towards-oecd-principles-government-access-data>

的な GA はいかなる場合も拒絶するとして GA に断固反対の姿勢を見せている。しかしながら、中国やロシアといった GA を取り入れたい権威主義国家は OECD に未加盟であるため、将来的にはそれらの国々が参加したうえでの議論がなされる必要がある。この状況を打破する上では、各国が様々な形で対応しているガバメントアクセスを分類し、類型化することにより、各国政策担当者やステークホルダー間での認識合わせを行うという地道な対話の積み重ねが非常に重要であるとされている⁴⁶。国際的合意に至るまでには時間を要することが予想されているが、2023 年の G7 において、事務局の設置などの恒常的な議論の場の設置が合意されることで、各国が議論を重ねる必要がある。

2) データローカライゼーション

データローカライゼーションとは、『平成 30 年版情報通信白書』⁴⁷によると、EU などが行う個人情報保護を観点とするデータの越境移転規制と異なり、ある国において特定の事業活動を営む場合、当該事業活動に必要なサーバーやデータ自体の国内設置・管理・保存を求める規制である。個人データに限ったデータの越境移転規制であれば、個人が同意を行うことで移転が許可されることがあるが、データローカライゼーションにおいては、データは個人データに限らないため、データの主権が個人にはなく、国政府主体がデータの越境移転における決定権を持つこととなる。データローカライゼーション規制に関しては、2017 年に中国で施行されたサイバーセキュリティ法をきっかけに広く世界の注目を集めることとなったが、現在はロシア、インドネシア、ベトナム、インド、ナイジェリアと多くの国々で導入の動きが進められている⁴⁸。データローカライゼーションは、自国への経済的価値の集中、国内産業の保護、安全保障の確保、犯罪捜査対策等が様々な目的において行われているが、国際展開する企業にとっては、ビジネスの障壁となるものである⁴⁹。

データローカライゼーションが注目されるきっかけとなった中国においては、近年データローカライゼーションは強化される傾向にある。中国がデータローカライゼーション規制を強化している背景には、米中対立の激化で安全保障上データの重要性が高まるなか、ビッグデータを今まで以上に国家で管理したいという思惑や、プラットフォームに対する影響力の強化が目的であるとされている⁵⁰。

昨今のウクライナ危機や、米中対立など、緊迫した世界情勢が続くなか、データ流通においては、「データナショナリズム」、すなわち多くの国々がデータローカライゼーションを導入する動きが急速に加速するのではないかとの見方もある。データローカライゼーションは国家安全保障などとも密接に関わり、政治的思惑の影響が大きく出るところになるが⁵¹、このような動向において、2023 年の G7 でデータロ

⁴⁶ 「DFFT が直面する課題と、その解決策」(世界経済フォーラム第四次産業革命日本センター, 2022.6.29)

(<https://note.com/c4irj/n/n7bbd8b73c529>)

⁴⁷ 総務省 「平成 30 年度版 情報通信白書」

(<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd112220.html>)

⁴⁸ 「越境データ流通の拡大と データローカライゼーションの動き」(情報通信総合研究所, 2018.5.29)

(<https://www.icr.co.jp/newsletter/wtr350-20180529-hirata.html>)

⁴⁹ 板津直孝 (2021) 「データローカライゼーション規制とデジタル経済の分断—強化される越境データの流通制限」, 野村資本市場クォーターリー 2021 年秋号 (<http://www.nicmr.com/nicmr/report/repo/2021/2021aut13.pdf>)

⁵⁰ 小野寺良文 (2022) 「中国のデジタル戦略と法 中国情報法の現在地とデジタル社会のゆくえ」 弘文堂 第 6 章 P174

⁵¹ 「データローカライゼーションへの対応が急務となる——特集「THE WORLD IN 2023」」(WIRED, 2022.12.24)

ーカライゼーションの広がりを読み止められるような具体的な内容が議論されることが望ましい。データの信用性を重視し、トラストに基づいたガバナンス体制が築けるかどうかも焦点となるであろう。

(2) 技術面

DFFT の推進に当たっては、法的なアプローチだけではなく技術の導入が必要不可欠である。2022 年の 5 月の G7 において実装に向けた議論が加速化する中で、PETs (Privacy Enhancing Technology : プライバシー強化技術) が議題にのぼり、技術的措置が制度や法規制の補完的な対策として議論が行われた。データの利活用が進む中で、産業や社会生活において多くの利益をもたらしている一方で、個人の情報がどのように取得されているのかが不透明となっている動向を踏まえて、プライバシー強化技術は、世界から注目を集めている。さらに、プライバシーの保護とデータ活用の両立をサポートする技術として、2022 年 9 月の G7 データ保護・プライバシー機関ラウンドテーブルにおいて、イギリスの ICO (Information Commissioner's office) が中心となって議論が行われた⁵²。

プライバシー強化技術は様々な種類のものがあるが、中でも「秘密計算技術」と「差分プライバシー技術」について整理をする。図表 3-15 に示す「秘密計算技術」は、データを断片化して乱数を加えて、一定数以上の断片が揃わないと復号できない状態で演算を行うことにより、特定の計算を安全に行う技術であり⁵³、電子資産の鍵管理の実用化が進んでおり、データ分析において活用される例も見られる。従来のデータ分析が、生データを使って分析処理を行うものであるのに対し、「秘密計算」は複数人によりデータを秘匿化した状態でデータ処理が可能となる技術である。これにより、攻撃者が分析システムに侵入している場合においても、生データ情報を読み取ることが不可能となり、秘密計算技術を使ったデータ活用の促進が期待されている。

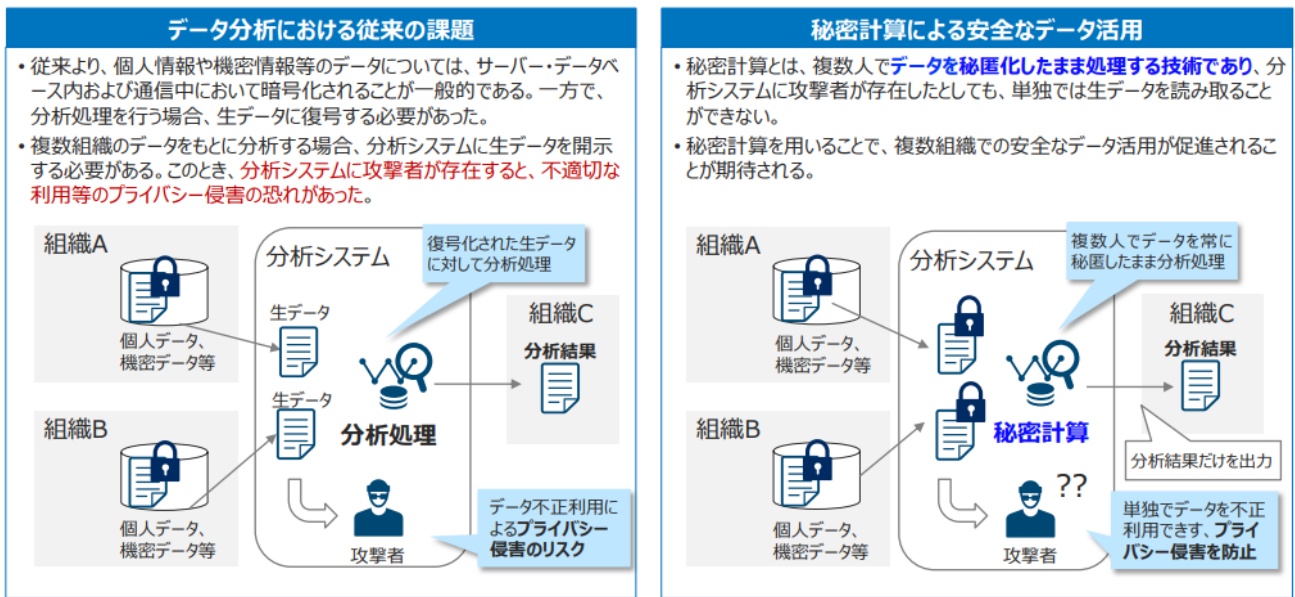
⁵² 「ICO publishes guidance on privacy enhancing technologies」(ICO, 2022.9.7)

(<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies>)

⁵³ デロイトトーマツ「次世代のデータ共有を可能にするプライバシー強化技術」

(<https://www2.deloitte.com/jp/ja/pages/deloitte-analytics/articles/privacy-enhancing-technologies.html>) (2023.3.28 閲覧)

図表 3-15 秘密計算の概要

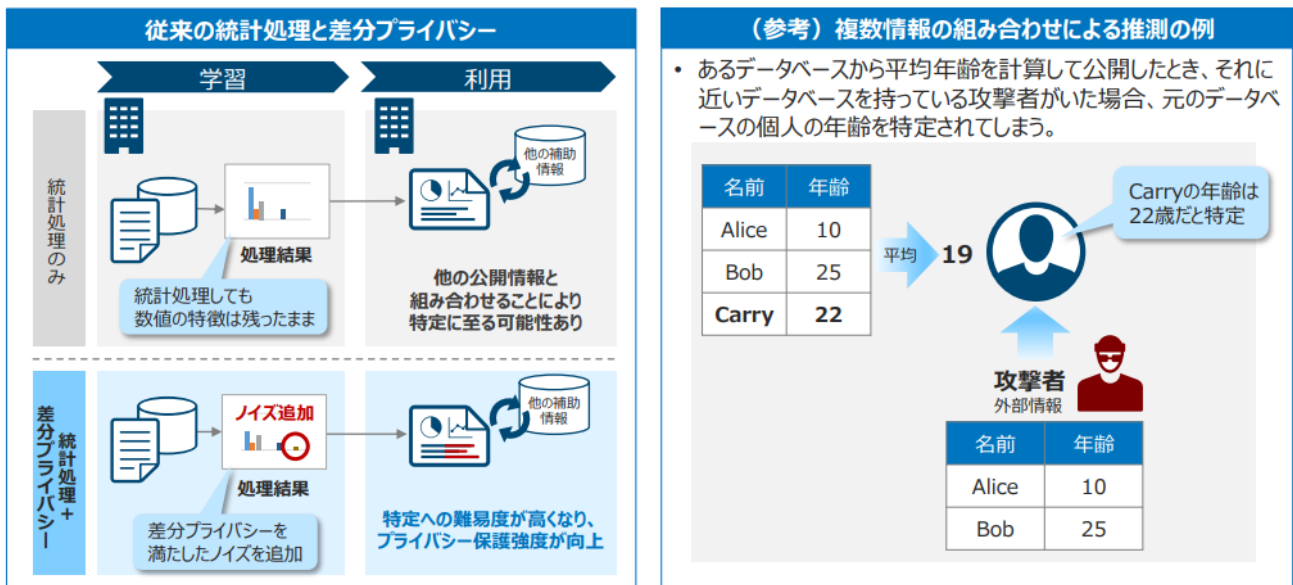


出典：「プライバシー強化技術の概説と動向」(株式会社日本総合研究所 先端技術ラボ, 2021.11.22)

(<https://www.jri.co.jp/MediaLibrary/file/column/opinion/pdf/13005.pdf>)

また、図表 3-16 に示す「差分プライバシー技術」は、ある処理から得られた結果が、どのデータベースから導出されたかの特定を困難にすることによって、プライバシー保護を強化する技術である。従来の統計情報やデータの処理においては、統計処理結果は、それ自体では個人情報の特定には至らなくとも、他の公開リソースに記載されている情報データを組み合わせることで、個人情報特定が可能となるという脆弱性をはらんでいる。これに対し差分プライバシー技術においては、データ分析にはほとんど影響の与えない程度のノイズデータを追加することにより、個人情報特定を難しくことができ、プライバシー保護の強化につながるとされている。

図表 3-16 差分プライバシー技術の概要



出典：「プライバシー強化技術の概説と動向」(株式会社日本総合研究所 先端技術ラボ, 2021.11.22)
<https://www.jri.co.jp/MediaLibrary/file/column/opinion/pdf/13005.pdf>

2022年9月のG7データ保護・プライバシー機関ラウンドテーブルにおいて、ICOが公開した資料においては、プライバシー強化技術を利用することについてのリスクについても述べられている。一つには、標準化やスケーラビリティ、攻撃に対する強靭さにおいて十分に成熟した技術であるとは言えないとされている。また、プライバシー強化技術を扱う際に、高度な専門知識を有していない人間が対応することが大きな問題を生じさせる可能性のある技術であるほか、理論上においては社会実装がうまくいっていても、実行してみた場合に差が生じることもあるとしている。そのため、あくまで、法整備において透明性が担保された状態での補完として、技術が導入されるべきであるとしている⁵⁴。

さらには、法令遵守や規制プロセスを自動化するよう設計された技術として「レグテック (RegTech)」の導入についても議論がなされている。レグテックは、Regulation (規制) と Technology (技術) の造語であり、2015年ごろから規制に対するソリューションとして存在していたが、実社会の変化のスピードがとても速い現代においては、規制のアップデートの迅速な対応には限界もある。そのような状況下においてレグテックは、規制に関わるプロセスをデジタル化することにより、規制する側のアジャイルガバナンスの実装に不可欠な要素として注目がなされている。2022年4月に世界経済フォーラムが公表した白書には、レグテック導入を成功させるにおいて必要な要素が紹介されている。それによると、まずレグテックの導入にあたっては、官民連携のパートナーシップやステークホルダーとの連携の重要性や、ユーザー第一主義のデザインであることなどが盛り込まれている⁵⁵。

⁵⁴ 「Privacy-enhancing technologies (PETs) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance」(ICO, 2022.9.7) (<https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf>)

⁵⁵ 「Regulatory Technology for the 21st Century」(WORLD ECONOMIC FORUM, 2022.4.13) (https://www3.weforum.org/docs/WEF_Regulatory_Tech_for_the_21st_Century_2022.pdf)

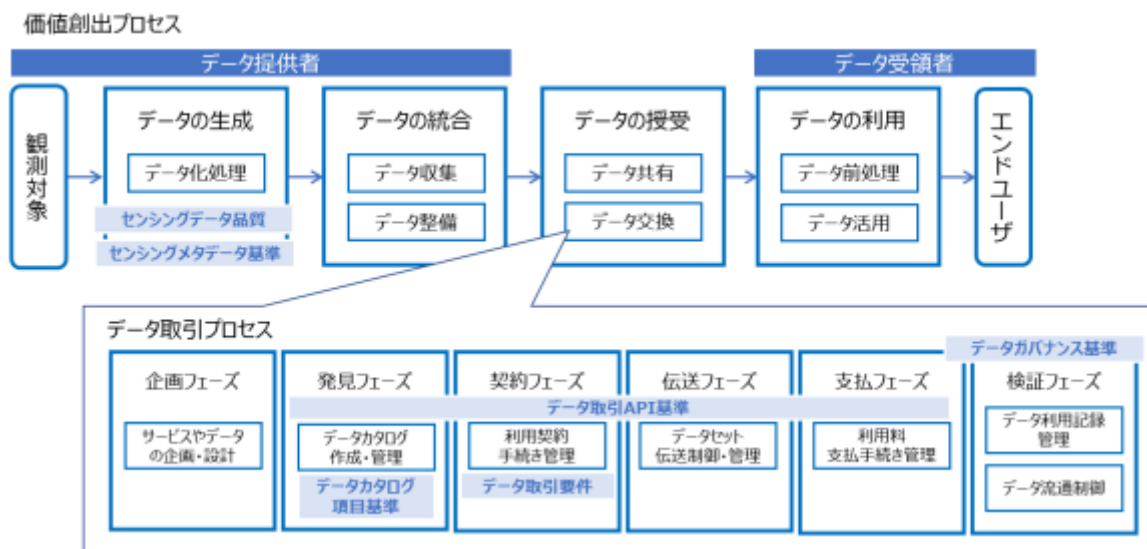
DFFT の議論が徐々に実装化に向けて具体的にになってきた段階において、また、制度面については各国の思惑が強く調整が難航することが予想される現状において、技術認証や標準化を進めることはDFFTの国際的な交渉を前進させることにおいても大きな役割を果たすことが予想される。

(3) 環境整備

データガバナンスにおいては、先に述べた制度面、技術面のみならず、データ流通の社会基盤の整備が必要不可欠である。我が国におけるデータ連携基盤構築における取組としては、「DATA-EX」がある。「DATA-EX」は国内のデータ連携のハブだけでなく、国際的なデータ基盤との連携や、相互運用にも取り組む姿勢を見せており⁵⁶、DFFT 実現に向けたアーキテクチャの設計や国際標準化推進の研究についても、内閣府に成果公表を行っている⁵⁷。

「DATA-EX」を推進する「一般社団法人データ社会推進協議会」は、「データ連携の機能全体像に関する検討」を2022年11月に公表している。異なる分野の組織間でデータの相互利用が進む中で、それぞれの組織が生成、保有しているデータをシステムやアプリケーションをまたいで利用する際に必要な機能の全体像について説明している。データ連携の機能の全体像を示すにあたり、生成・統合されたデータを利用することで価値を創出するプロセス(価値創出プロセス)と、必要データを発見・入手し、その対価を支払うプロセス(データ取引プロセス)の2つの軸に分けて整理が行われている。図表3-17に示す通り、価値創出プロセスは、データ提供者によってデータが生成されてから、データ受領者においてデータが利用されるまでの全体のプロセスを示している。その間、データの収集や統合、加工などが行われる。それに対してデータ取引プロセスは、データの授受におけるプロセスの詳細が示されている。

図表 3-17 価値創出プロセスとデータ取引プロセスの関係



⁵⁶ 「【2023年G7で注目、DFFT徹底解説】国際的なデータ移転ルールどう作るか？「DFFT」を各国がいま議論するワケ」（日経クロステック, 2022.12.19）(<https://xtech.nikkei.com/atcl/nxt/column/18/02299/121400001/>)

⁵⁷ 「SIP サイバー/アーキテクチャ構築及び実証研究の成果公表」（内閣府, 2020.3.18）(<https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html>)

出典：「データ連携の機能全体像に関する検討」（一般社団法人データ社会推進協議会, 2022.11.1）

(<https://data-society-alliance.org/wp-content/uploads/2022/11/20221101-D108-data-exchange-system-overview-wp-tecst.pdf>)

データ連携基盤構築に関する各国の取り組みとしては、前述の、EU のデータ取引市場を推進する「Gaia-X」に加え、中国のデータ取引市場として 2021 年 3 月に設立された「北京国際ビッグデータ取引所（Beijing International Big Data Exchange）」、世界フォーラムが推進する DCPI（Data for Common Purpose Initiative：共通目的データ・イニシアチブ）、が例として挙げられるであろう。

「データスペース」に関しては、先に述べた EU において推進されているコンセプトとして知られるが、デジタル空間の社会基盤として欧州以外でも構築に向けた議論が行われており、2022 年の G7 デジタル大臣会合においては、DFFT アクションプランの採択に伴い国際データスペースの可能性についても議題として挙げられている⁵⁸。データスペースに関して主流となっているのはコネクタ型といわれるものであり、分野間のデータ連携を実現するソフトウェアをもとにした構築が進められている。データスペースの導入は、データドリブンな経済および社会を実現させるうえで重要なデータ連携基盤の 1 つであるといえ、今後 DFFT においてどのように構築に向けた議論がなされるのかについて注目すべきである。

⁵⁸ 総務省「デジタル大臣会合の開催結果」（2022.5.12）(https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000239.html)

3.2. 自由で開かれたインターネット空間の維持に関する調査

3.2.1. インターネットの分断における現状と国際的な影響

(1) インターネットが本来目指していた世界

1) 世界共通プラットフォームとしてのインターネット

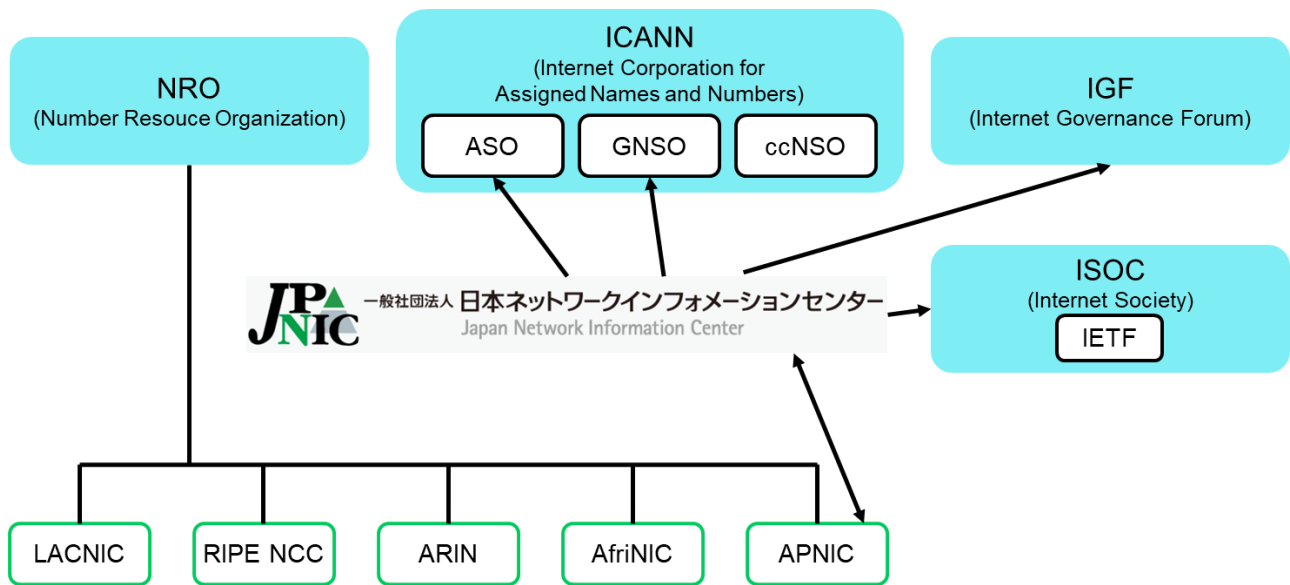
インターネットは 20 世紀に誕生してから今日に至るまで大きな進化を遂げながら、様々な分野で利用され、単なるツールを超え欠かすことのできないものとなっている。1969 年に米国の 4 つの大学と研究所を結んだ通信から始まり、インターネットが「自律・分散・協調」という基本理念に則って、全ての人がアクセスできるという不文律のもとインターネットは世界共通のコミュニケーションの基盤とされてきた。

世界に 5 つある地域レジストリの 1 つとして IP アドレス・AS 番号の管理業務を行っている APNIC (Asia Pacific Network Information Centre) の Paul Wilson は、2022 年の TWIGF (テーマ: The challenge of Internet – and how the future Internet will be) において、「インターネットは複数のネットワークを 1 つのネットワークとするという構想からの産物である。黎明期においては相互に繋がりのない別々のネットワークがいくつもある状態であったが、インターネットはそれらのネットワークに繋がりを生んだのである。それぞれのネットワークを相互に繋がった状態とすることについては自然とスタンダードとして受け入れられていき、また共通の利益としてインターネットを 1 つのネットワークとすることを、技術を運用するオペレーター、ベンダー、ブランド、企業は共通認識としたのである。」と述べている。また、インターネットの設計思想について、Andrew Sullivan (ISOC CEO) は「ローカルインターネットを肯定することは、インターネットの否定であり、インターネットの断絶は偽情報を防げるが、真実も届かないことを意味する。」としている。

2) インターネットの発展を支えてきたガバナンス体制

インターネットは前述のとおり、世界で 1 つの、誰もが利用できるプラットフォームであり続けてきた。図表 3-18 に示す組織によってインターネットガバナンスが支えられてきた中で、資源管理の観点では ICANN (The Internet Corporation for Assigned Names and Numbers)、技術面では IETF (The Internet Engineering Task Force) の 2 つの団体が大きな役割を果たしてきている。

図表 3-18 インターネットのガバナンスを支える国際組織



出典：「国際関係組織一覧」（一般社団法人日本ネットワークインフォメーションセンター（JPNIC），2016.12.21）（<https://www.nic.ad.jp/ja/intl/org/org.html>）を元に作成

インターネット資源の管理に関しては、インターネットが米国連邦予算の資金投入をもとに開発されたという経緯があるため、米国政府主導であった。しかしながら、インターネットの普及に伴い、米国主導の管理に議論が噴出し、1998年にICANNという民間主導に移行したのである。⁵⁹ICANNの前身はIANA（Internet Assigned Numbers Authority）と呼ばれる、インターネット黎明期に南カリフォルニア大学情報科学研究所（ISI）のプロジェクトグループである。IANAはドメイン名、IPアドレス、プロトコル番号など、インターネット資源のグローバルな管理を担ってきており、ICANNはこれを引き継ぎ、現在はドメイン名、IPアドレスなどを世界規模で管理・調整するマルチステークホルダー型の非営利法人である。ICANNの支持組織としては、IPアドレスをいかに運用するか議論し、ICANN理事会に勧告を行うASO（The Address Supporting Organization）、分野別トップレベルドメイン（gTLD）に関するポリシーを策定し、ICANN理事会への勧告を行うGNSO（Generic Names Supporting Organization）、国コードトップレベルドメイン（ccTLD）に関するグローバルポリシーを策定し、ICANN理事会への勧告を行うccNSO（Country Code Names Supporting Organization）の3つがある。

また、IANAが担っていた役割のうち、インターネットリソースの配分と登録の管理については世界に5つあるRIR（Regional Internet Registry：地域レジストリ）が引き継いでいる。RIPE NCC（Réseaux IP Européens Network Coordination Centre）はヨーロッパ、中近東、アジアの一部、LACNIC（Latin American and Caribbean Internet Addresses Registry）はラテンアメリカとカリブ海地域、ARIN（American Registry for Internet Numbers）は北米、カリブ海周辺の一部地域、AfriNIC（African Internet Numbers Registry）はアフリカ地域、そしてAPNIC（Asia Pacific Network Information Centre）はアジア太平洋地域の管理を行っている。また、NRO（The Number Resource Organization）は、RIR全体として外部組織との調整が

⁵⁹ Digital Policy Forum Japan, 谷脇康彦（デジタル政策フォーラム顧問） 「#11 インターネットガバナンスをめぐる国際的議論」（2022.4.15）（<https://www.digitalpolicyforum.jp/column/220415/>）

必要な場合に全 RIR を代表する非営利組織として運営されている。

ICANN およびその支持組織がインターネット資源の管理を行うのに対して、IETF はインターネット技術の標準化を推進するマルチステークホルダー型の任意団体であり、コンピュータシステムを相互接続するため、共通の技術仕様策定を議論するグループから発展した歴史がある。母体である ISOC (Internet Society) はインターネット技術およびシステムに関する標準化、教育、ポリシーに関する課題や問題を解決あるいは議論することを目的とした非営利法人となっている。

ICANN、IETF を中心として、インターネットに関する議論を行っている組織としては、IGF (Internet Governance Forum: インターネットガバナンスフォーラム) がある。IGF は 2003 年および 2005 年に国連で開催された世界情報社会サミット (WSIS) の合意文書において設立が明記されて以降、インターネットガバナンスの問題に関してマルチステークホルダー間で政策対話が行われている⁶⁰。2023 年の 12 月には、日本での開催が決定している。

ICANN、IETF、IGF に共通していることは、マルチステークホルダー主義であるということだ。マルチステークホルダー主義とは、政府のみならず大学等の研究者、企業の技術者などの民間組織を含む、様々なアクターが関わって意思決定を行うことを原則としている。国および政府は意思決定に関わることは可能だが、政府の提案や発言が絶対的な強制力を持つことはなく、したがってマルチステークホルダー主義は多様な参加者を受け入れる民主主義的な運営方法であるといえる。国家主権を 100%認めることは表現の自由や報道の自由に公的権力が介入する根拠を与える恐れがあることや、インターネット関連技術は政府の規制の外にあったからこそ社会基盤になるまでの発展を遂げてきたということが挙げられる⁶¹。

このようにインターネットが国家の方針や対立に制限されることなく発展を遂げてきた中で、近年インターネットのガバナンスへの関与を強めようとする動きが見られるのが ITU (International Telecommunication Union: 国際電気通信連合) である。ITU は主に無線通信と電気通信分野における各国間の標準化と規制の確立を行っており、国連に設置されている専門機関の 1 つであるが、インターネットはその発生からは一貫して ITU の外で発展してきている背景がある。ICANN、IETF、IGF などとの大きな違いとしては、一国一票制のマルチラテラル主義での意思決定および運用がなされているため、民間組織は決定に関与することができない。

2012 年には ITR (International Telecommunication Regulations: 国際電気通信規則) の改定に関する会議が開催されていたが⁶²、政府の関与やインターネットコンテンツの規制、検閲、遮断等の規制強化につながりかねないため、米国、EU、カナダ、日本など 55 か国は署名を見送った。国際条約としての法的拘束力をもつ ITR の改訂版は 2015 年 1 月 1 日から施行され、署名したのはロシアや中国、その他新興国など 89 か国に適用された一方で、署名しなかった国には改正前の ITR (1988 年採択) が適用されて

⁶⁰ 一般社団法人日本ネットワークインフォメーションセンター (JPNIC) 「国際関係組織一覧」(2016.12.21) (<https://www.nic.ad.jp/ja/intl/org/org.html>)

⁶¹ 「#19 インターネットを巡る”国家主権”と”サイバー主権”」(Digital Policy Forum Japan, 2022.9.2) (<https://www.digitalpolicyforum.jp/column/220902/>)

⁶² 「国家によるネット遮断が正当化される——ITR 改正、日本など 55 カ国が署名拒否」(INTERNET Watch, 2012.12.17) (<https://internet.watch.impress.co.jp/docs/news/579155.html>)

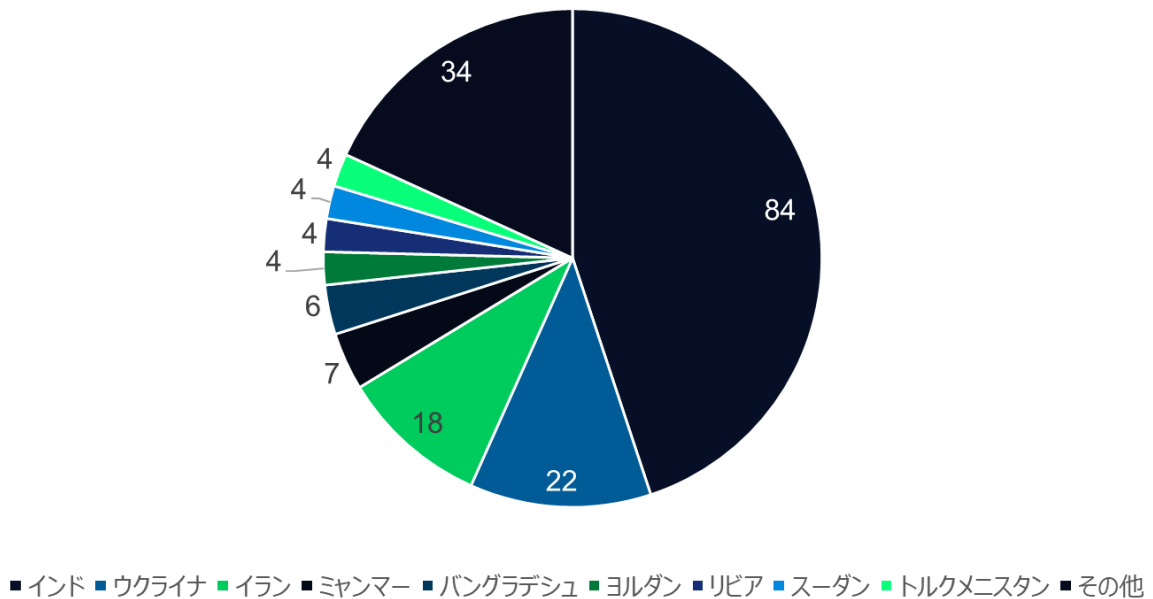
いる⁶³。

(2) インターネットの分断について現状の概観と分断が行われている各国の事例

1つのプラットフォームを世界で共有することで、世界の平和と発展に寄与してきたインターネットであるが、近年分断が行われるようになってきている。特に民主主義の弱い国、権威主義国家と呼ばれる国において、各国の政治情勢や思想に合わせて、国主導で自国のインターネットを他国から切り離し、情報統制に使用することで自国民をうまくコントロールする目的で行われることが多い。国際NPO法人 Access Now が2023年3月に発表したレポートによると、2022年には、世界で少なくとも187回のインターネットの断絶が発生しており、断絶が発生した国は35の国にのぼるといふ。これはいずれも2021年を上回っている。最も遮断が行われていたのはインド、2位はウクライナとなっているが、ウクライナについては外部組織によるものであるとの注意書きがなされている。(図表 3-19)

図表 3-19 世界で発生したインターネットの遮断回数

各国におけるインターネットの遮断回数 (2022年)



出典：「Weapons of control, shields of impunity: Internet shutdowns in 2022」(国際NPO法人 Access Now, 2023.3.22) (<https://www.accessnow.org/wp-content/uploads/2023/03/2022-KIO-Report-final.pdf>) を元に作成

⁶³ 総務省「国際電気通信連合 (ITU) 2012 年世界国際電気通信会議 (WCIT-12) の結果」(2012.12.15) (https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000042.html)

また、Google の親会社である Alphabet 傘下のシンクタンクである Jigsaw と国際 NPO 法人 Access Now が 2021 年に共同で発表したレポートによると、インターネット断絶が過去 10 年間で 850 回近く行われたとされており、抗議運動の抑圧や言論の封殺などを目的としたインターネットの断絶が急増している実態が明らかにされている。このレポートでは、インターネットの断絶が市民生活にどのような影響を及ぼすかについて、アフリカやアジアの小国におけるインターネットの断絶にも焦点を当ててレポートが行われている。発展途上国においてはインターネットの断絶は、医療などの命に係わる現場、WhatsApp や Facebook をコミュニケーションツールとしているビジネスの現場など、教師と生徒のオンラインコミュニケーションなど、様々な場面で悪影響を及ぼしている⁶⁴。

このように、近年様々な国において発生しているインターネットの断絶であるが、特にロシア、ウクライナ、中国、そしてアジア、アフリカ（イラン、ミャンマー、スーダン、インド）についてインターネットの分断を整理する。

1) ロシアおよびウクライナ

インターネットの分断に関して、2022 年のロシアによるウクライナ侵攻、それに伴ってウクライナが戦略的に行った、ICANN へのロシアドメイン失効の要求は、インターネットの歴史においても例を見ない事例であった。ウクライナ侵攻に先立ってロシアで行われてきた「インターネット鎖国」に向けた動きについても、インターネットの分断をより深刻にする可能性があり、ウクライナ危機はインターネットガバナンスを語るうえで非常に重要な局面といえる。

2022 年 2 月 24 日、ロシアがウクライナへと侵攻開始し、2023 年 1 月現在、実際の武力衝突における戦闘行為のみならず、インターネット空間においても激しい攻防が続いている。侵攻開始から 4 日後の 2022 年 2 月 28 日、非営利団体「ICANN」の CEO、ヨーラン・マービー氏の元へ、ウクライナ副首相兼デジタル改革大臣のミハエル・フェドロフ氏より「ロシアのドメインである.ru や.PΦ、.suなどを永久に、または一時的に失効させてほしい。そして上記ドメインの SSL 証明書の無効化、ロシア内の DNS ルートサーバーも停止してほしい」との要望が届いた。同様の文書は、世界に 5 つある地域インターネットレジストリー (RIR) の 1 つである「RIPE NCC」のマネージングディレクター、ハンス・ペッター・ホーレン氏へも送られている。これは過去に例を見ない要請として世界が注目し、動向をうかがった。前述のとおり、インターネットは世界中すべての人がアクセスできるという不文律のもとで利用されているただ一つのグローバルプラットフォームであり、このウクライナ政府からの要請は、インターネットの根幹を揺るがすものである。ウクライナ政府は、「ロシアによる残虐な犯罪行為を可能にしたのは、ロシアのプロバガンダによる偽情報やヘイトスピーチなど、ウクライナの戦争に関する真実を隠す Web サイトがあるからだ」、ロシアの反撃の戦術の 1 つとして、ロシアをインターネットから遮断しようと試みたのである。

⁶⁴ 「The Current – When the Internet is shut down, more than a connection is lost in the dark.」 (JIGSAW, 2021.9.1)
(<https://jigsaw.google.com/the-current/shutdown/>)

この要請に対し、ICANN のマービー氏は、「ICANN は一方的にドメインの接続を解除することはポリシーとして規定されていない」として、ウクライナ政府の要求を突っぱねた。ICANN は、あくまでインターネットを機能させることを目的に設立された調整役であり、インターネットの機能を止める立場にないということだ。そのうえで、「貴殿は、(ロシアによる)プロパガンダや偽情報を防ぐための支援を求めているが、市民が信頼できる情報や多様な視点を受け取ることができるのは、インターネットへの自由で広範なアクセスを通じてのみ可能だ」(同氏)とし、インターネットへつながり続けることへの重要性を強調した。RIPE NCC のホーレン氏も同様の回答を行った。

ウクライナ政府による、ICANN への要請は突っぱねられる結果となったが、ウクライナ危機においては国だけでなく企業側の動きも注目されている。2022 年 3 月初旬、米国の大手通信事業者がロシアとの通信を遮断したとして大きな話題を呼んだ。米国の大手通信事業者コージェント・コミュニケーションズ(コージェント)からロシア最大手の通信事業者トランステレコムへつながる通信が切断され、さらに米国の大手通信事業者であるルーメン・テクノロジーズも「ロシア国内のセキュリティーリスクが高まったため、ネットワークを切断することにした」との声明を出し、ロシア国内のネットワークを停止すると発表。この動きは 2 社に留まったものの、この件を受け、企業がインターネットの断絶を行うという新たな時代の到来として、専門家間で衝撃が走った⁶⁵。

ウクライナ危機をとおして、有事の際にインターネットが繋がり続けることは必ずしも善であると言いきることができないという見方も生まれており、一連の応酬は、インターネット運用の在り方に改めて疑問を投げかける結果となっている。

他方ロシア側も、2019 年ごろから海外のインターネットから同国を遮断する「インターネット鎖国」に向けた動きが、プーチン大統領主導で行われてきた。2019 年 11 月には、有事の際などに外国とのインターネット通信を遮断・制限する連邦法(通称「主権インターネット法」)が発効され、通信事業者はインターネット通信トラフィック(送受信情報)への脅威に対抗したり、禁止されたウェブサイトへのアクセスを制限したりする技術手段をネットワーク上に設置することが義務付けられ、ロシアのインターネットが脅威にさらされた際、通信網の集中管理が連邦通信・IT・マスコミ監督局(ロスコムナドゾル)によって行われることについても規定された⁶⁶。また、2019 年末までで「Runet(ルネット)」(ロシアの国内インターネット)のシステムテストを、サイバーセキュリティ対策の一環で実施したとロシア政府は発表している。しかしこの取り組みに対するロシアの思惑は、国内のデジタル情報へのアクセスをコントロールし、検閲するためであるとして、国内外から指摘されている⁶⁷。またこれに先駆けて 2016 年にはグレートファイアウォールの創設者として知られる Fang Binxing がロシアを訪問し、ロシア版のファイアウォールの作成に力を貸しているとも報道されている⁶⁸。

このように、ウクライナ危機およびロシア国内の動きは、インターネットの分断の大きな影を投げかけ

⁶⁵ 「ロシアへのインターネットを遮断」 専門家に衝撃 決断の理由、通信大手が明かした」(The Asahi Shimbun Globe+, 2022.7.17) (<https://globe.asahi.com/article/14668549>)

⁶⁶ 「外国とのインターネット通信を制限する連邦法が発効(ロシア)」(日本貿易振興機構(JETRO), 2019.11.6) (<https://www.jetro.go.jp/biznews/2019/11/a38ae40b5937dd7c.html>)

⁶⁷ 「ロシアによる「インターネット鎖国」の実験完了は、次なる統制に向けた新たな一歩になる」(WIRED, 2020.1.16) (<https://wired.jp/2020/01/16/russia-internet-control-disconnect-censorship/>)

⁶⁸ 「Russia-Ukraine: Is internet on verge of break-up?」(BBC News, 2022.3.9) (<https://www.bbc.com/news/technology-60661987>)

ている。国のみならず企業もインターネットの分断に関与することができる時代であり、今後動きについても注視する必要がある。

2) 中国

中国におけるインターネットの分断については、国家戦略として Great Firewall を基盤にインターネットの検閲および規制を行うと同時に、近年国際的なインターネットガバナンスへのアンチテーゼとして、ITU における影響力拡大などの動向が見られている。

中国は、世界の中でも先駆けて、国家戦略としてネットの分断を進めてきた。「金字工程」と呼ばれる国家戦略の一部として、1993 年に国家戦略の一部として計画が始まり、1999 年に導入、2003 年の段階で基本的な検閲システムが完成した背景があり、インターネット検閲システムの歴史は非常に長い。インターネットの分断として世界で最も知られている事例の 1 つに、中国共産党が作り上げてきた Great Firewall (グレートファイアーウォール) がある⁶⁹。30 年以上前から構築が進められてきているインターネット検閲システムであるが、Google、Facebook、Youtube、New York Times などといった米国主導のサービスは一切排除され、「サイバー主権」を標榜し、海外の影響を受けずに国家の利益を守ることが習国家主席および中国共産党の狙いである。Freedom House が実施した調査においても、対象の 65 か国のうち最もインターネットにおける自由がない国として報じられている。

2021 年に明らかになったこととしては、グレートファイアーウォールがどのようなドメインをブロックしているのかを測定するシステムを開発することによって、米国のコーネル大学 (Cornell University) の研究者グエン・フォン・ホアン氏が膨大なドメインのテストを実施した。グレートファイアーウォールにおいて最も多くブロックされたウェブサイトのジャンルは「ビジネス」「ポルノ」「IT 技術」となっていた。また、新型コロナウイルス感染症拡大に伴い、新型コロナウイルス感染症に関連する、もしくはパンデミックを批判する内容の投稿を行うウェブサイトに関するドメインがブロックされていたとされる⁷⁰。

自国のインターネット検閲システムを構築することで、世界のインターネットからは切り離された状態にあるといっても過言ではない中国だが、後述する ITU (国際電気通信連合) における影響力強化に乗り出している。中国の動きとして特筆すべきこととして、2019 年 9 月に中国の通信大手華為技術 (ファーウェイ) および国営の通信会社 2 社、そして工業情報化部 (経済産業省に相当) が、ITU に対して新たなインターネットの基本技術となる「新 IP (インターネットプロトコル)」技術を提案したのである。ファーウェイが主張しているのは、現在のインターネットプロトコルのクオリティでは、今後の最先端技術の導入に対応できないとし、デジタル界の発展に純粋に寄与する狙いでの提案であるため、情報統制の機能は一切組み込まれていないとしている。しかしながら、英サイバーセキュリティ企業はそれに

⁶⁹ 「The Great Firewall of China: Background」 (Torfox, A Stanford Project, 2011.6.11) (<https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html>)

⁷⁰ Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, Michalis Polychronakis, Cornell University 「How Great is the Great Firewall? Measuring China's DNS Censorship」 (2021.6.3) (<https://arxiv.org/abs/2106.02167>)

反対し、新 IP がネットワーク基盤への統制機能の埋め込みを可能とされている⁷¹。

このように、情報統制を長らく行ってきた権威主義国家として、中国はインターネットガバナンスにおいても自国の技術、制度を適用できるようにする思惑があるとされ、インターネットの分断におけるプレイヤーとして今後も注視する必要がある。

3) アジアおよびアフリカ

ロシアや中国といった大国だけでなく、アジアやアフリカの国々においても、抗議デモの弾圧や少数民族の排除を目的としたインターネットの断絶を行っている。国家によるインターネットの遮断が広がっている。イランでは、9月にクルド女性のマフサ・アミニさんがスカーフのかぶり方が不適切だとして、風紀警察に拘束され急死した事件が発生しており、反政府勢力鎮圧の目的で当局がインターネットを遮断したとして報じられている⁷²。

また、ミャンマーでは2021年2月1日の軍事クーデターを皮切りに、インターネット上で起こっている反対運動を押さえる目的でインターネット遮断を行っている。国際NPO団体Access Nowのキャンペーン#KeepItOnは、ミャンマー軍によるインターネット断絶は2021年の1年間で少なくとも15回行われたとしている⁷³。人権団体の「フリー・エクスプレッション・ミャンマー (FEM)」は、ミャンマーはインターネット利用者の自由が制限されている国のなかで、最もひどい状態になったと、2022年10月の取材で述べている。また、ミャンマーの軍評議会 (SAC) は2022年9月20日、「フェイスブックなどのSNSに投稿された国民統一政府 (NUG) や市民防衛隊 (PDF) の記事に『いいね!』を押したり、シェアしたりした者は禁錮3年から10年の刑に処し、100チャット (およそ7円) でもPDFに寄付すれば破壊活動防止法に抵触し、死刑もありえる」として国民からインターネットにおける自由を奪っている⁷⁴。

インドでは、2019年以降カシミール地方でのネット遮断を本格化しており、2020年3月には同地方のネット遮断と速度制限は累計9000時間にのぼっている。背景には、モディ首相が率いる与党インド人民党 (BJP) はヒンドゥー至上主義を掲げており、イスラム教徒が多いカシミール地方におけるイスラム教徒排除を目的とした措置であるとの見方が強い⁷⁵。

スーダンでは、2021年、5回にわたってネット遮断を実施。同年10月25日に軍がクーデターを起こし、暫定政府から権力を掌握し、首相や政府関係者を恣意的に拘束し、インターネットの遮断を行った。翌年の10月25日にも軍部クーデターから1年を機に民衆の抗議デモに先立ってインターネット遮断を政権側が実施。

⁷¹ 日本経済新聞「[FT]中国が国連に新IP提案、ネットに国家管理の懸念」(2020.4.6)

(<https://www.nikkei.com/article/DGXMZO57703570W0A400C2I00000/>)

⁷² REUTERS「イランで大規模ネット遮断、クルド勢力弾圧の懸念高まる」(2022.11.22)

(<https://jp.reuters.com/article/iran-women-internet-idJPKBN2SB21T>)

⁷³ 「THE RETURN OF DIGITAL AUTHORITARIANISM Internet shutdowns in 2021」

(<https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>)

⁷⁴ 時事通信社、アジアビジネス情報「ミャンマーのネット遮断は世界最悪＝人権団体」(2022.10.19)

⁷⁵ 日本経済新聞「ネット遮断損失 世界で4000億円－ベラルーシはIT企業が流出」(2021.1.21)

(<https://www.nikkei.com/article/DGXZQOGM196RL0Z10C21A1000000/>)

このように、アジアやアフリカにおいては、とくに紛争当事国、権威主義政権や民主主義の弱い国において、治安部隊による抗議者への弾圧という人権侵害を隠蔽するためのツールとして、ネット遮断を用いているのである⁷⁶。

(3) スプリンターネットとは：Splinter1.0 から 2.0 へ

1 つのグローバルプラットフォームを志向して作られたインターネットが分断していく動きについて、研究者らは「スプリンターネット (Splinternet)」と呼んでいる。英語の「Splinter(分裂、断片)」と「Internet」を結び付けた造語である。スプリンターネットに対する 1 つの統一した定義は存在せず、ステークホルダーや学者ごとに異なった見方がある。2022 年 6 月の GLOCOM 六本木会議オンライン#42 Splinternet スプリンターネット – インターネットと国際政治の関係 (ロシアのウクライナ侵攻によって顕在化する問題シリーズ) のセッション内において、小宮山 功一朗氏が行ったインターネットの分割に関する分類によれば、(図表 3-20)「インターネットは分割しない」とする意見や、米中/伝統的な東西対決などによる 2 分割、米国、中国、欧州による 3 分割、民主主義国家、権威主義国家、ビッグテックによる 3 分割、そしてシリコンバレー、DC、ブリュッセル、北京による 4 分割と、様々な形で意見が分かれている。

図表 3-20 インターネットの分割における分類

| いくつに分割 | 主たるアクター | 主な提唱者、支持者 | 重視される価値 |
|--------|--------------------------|------------------------|---|
| 分割しない | プラットフォームとグローバルな専門家ネットワーク | ICANN、技術者コミュニティ | 「情報の自由な流通」、「言論の自由」。そもそも、データは一箇所に固まる修正をもつ。 |
| 2分割 | 米国と中国 西側と東側。 | 多くの国際政治学者 | 「国家安全保障」伝統的東西対決。台頭する中国への警戒 |
| 2分割 | 国家とビッグテック | イアン・ブレマー | 「伝統」と「新しい秩序」 |
| 3分割 | 米国と中国と欧州 | バラグ・カンナ、横澤、 マクロン大統領 | 欧州はプライバシー保護などの分野で米国とは異なっている 「イノベーションと開放」、「プライバシーと思想の自由」、「統制による成長」 |
| 3分割 | 民主主義国家と権威主義国家 とビッグテック | ダニ・ロドリック、小宮 山 | 「民主主義」、「国家主権」、「グローバリゼーション」 |
| 4分割 | シリコンバレー、DC、ブ リュッセル、北京 | キーロン・オハラ | シリコンバレー「非中央集権」「相互接続性」 ブリュッセル「人権」、「プライバシー」 D.C.「マーケットに委ねる」、「独占を許容」、「契約」 北京型：「社会の安定」、「効率性」 |

出典：「Splinternet スプリンターネット – インターネットと国際政治の関係 (ロシアのウクライナ侵攻によって顕在化する問題シリーズ)」(GLOCOM 六本木会議オンライン#42, 2022.6.7 開催)
(<https://ropongi-kaigi.org/topics/2694/>)

スプリンターネットについて考える際に、インターネットはどのような場合にオープンで 1 つのイン

⁷⁶ 「世界のインターネット遮断 (2021)：デジタル権威主義の再来」(Themeisle P2Ptk.org, 2022.6.20)
(<https://p2ptk.org/freedom-of-speech/3697>)

ターネットであると言えるのかという論点がある。中央大学の實積寿也教授は、オープンなインターネットは技術、制度、ビジネスという3つの局面の協調によって実現されているとし、「インターネットのサービスを使うためにはまず、技術的に可能であるということが大前提にある。そのうえで、政府による規制等で他国のインターネットを見ること自体が制限されることがないといった制度面での条件が満たされ、さらには実際にビジネスとしてそのサービスが提供されるという条件が満たされなければ、インターネットを自由に使うことはできない。」と話している。例えば、2010年から2012年に発生した、「アラブの春」においてもインターネットの断絶が行われたが、このケースは「技術やビジネスの条件はそろっているものの、制度面において国の規制があったがゆえに、3つの条件の1つが満たされておらず、インターネットを使うことができなかつたという意味でスプリンターネットと定義することができる。」と実積教授は話している。また、また、実積教授は、Yahoo! Japanのインターネットサービスが2022年4月以降、欧州およびイギリスから利用できなくなっている事例⁷⁷についても、一種のスプリンターネットであるとし、3つの要素のうちのビジネスの条件が満たされていないものであるとしている⁷⁸。

また、スプリンターネットの潮流や性質自体が時代とともに大きく変化している中で、Splinternet1.0から、Splinternet2.0へと移り変わっているとの指摘もある。Splinternet1.0とは、2022年10月に開催されたの日本インターネットガバナンスフォーラムの「スプリンターネット？」というテーマセッション内で水越一郎氏は、「中国における Great Firewall に代表される、防衛の側面が強く、流入阻止・アクセス制限などのアプローチを取ってきたものである」と個人の見解を述べている。それに対して Splinter2.0 について同氏は、「攻撃、制裁を特徴とし、他者が敵国に提供する権限はく奪およびサービスの停止などを行うものである」とし、前述のウクライナ危機におけるドメイン停止要求もその一例であるとしている⁷⁹。

実積寿也教授は、いわゆる Splinternet 1.0 の段階においてはインターネットの断絶は国主体で行われてきているのに対し、Splinternet2.0 は国の意向とは必ずしも関係なく、民間企業のみ力で実施されていることが特徴であるとしている。ロシアのウクライナ侵攻においては、インターネットサービスを提供している企業が、ロシアでビジネスを続けることによる風評被害を避けるため、あるいは評判を守るために、ロシアでのインターネットサービスを止めてしまうという事象が見られたが、このように企業がある種 CSR の一環としてインターネットの断絶をおこなうことができるという点は、Splinternet2.0 の特徴であると実積教授は述べている⁸⁰。

このように、スプリンターネットは時代と共にメインアクターの変化、性質の変化を伴っており、有識者によっても。インターネット空間の分断に対抗する上では、これらの見解の整理および分類を行いつつ、同時並行でこれに対抗する具体策を講じるが必要不可欠である。

⁷⁷ 「2022年4月6日(水)より Yahoo! JAPAN は欧州経済領域 (EEA) およびイギリスからご利用いただけなくなります」 (<https://privacy.yahoo.co.jp/notice/globalaccess.html>) (2023.3.28 時点閲覧)

⁷⁸ 有識者ヒアリング (中央大学総合政策学部 実積 寿也教授) に基づく。

⁷⁹ JPNIC 一般社団法人日本ネットワークインフォメーション「Day 2 テーマセッション(3)「スプリンターネット？」@日本インターネットガバナンスフォーラム 2022 ~ IGF2023 日本開催を見据えて」 (<https://www.youtube.com/watch?v=Q6y0R1ymbqw>)

⁸⁰ 有識者ヒアリング (中央大学総合政策学部 実積 寿也教授) に基づく。

3.2.2. 自由で開かれたインターネット空間の維持に向けた国際団体の動向

(1) インターネットガバナンスを担う運営団体の動向

インターネットの分断をこれ以上引き起こさないためには、国際連携が必要不可欠である。1)の(ア)iiにおいて、インターネットガバナンスを支えてきた団体の中で、今までインターネットのガバナンスに関与していなかったITUがインターネットのガバナンス体制に影響を及ぼそうと動きを見せていることについて言及した。昨今のITUの動向は、自由で開かれたインターネット空間を今後も維持できるかどうかに関わる事項であり、特に中国とロシアに代表される権威主義国家主導でのITU運営は、監視社会のツールとしてインターネットが使われかねない。

ITUにおいて中国が影響力を強めようとしている背景には、ITUが前述のとおり、マルチラテラル主義を取っていることにある。加えて、情報通信における国際標準には「デジュール標準」「フォーラム標準」「デファクト標準」の3種類があるが、IETFなどが位置付けられる「フォーラム標準」は、民間組織が集まってフォーラムと呼ばれる組織が結成され、公的ではないなかで標準を策定するもの、また、「デファクト基準」は市場で多くの人に受け入れられることで標準になったもののことをいうのに対し、ITUで策定された標準は「デジュール標準」と呼ばれており、ほか2つと違って公的な位置付けの標準化機関において定められた手続きに従い、関係者の合意で制定される標準である⁸¹。(図表 3-21)

図表 3-21 情報通信における標準の種類

| 標準の種類 | 標準の概要 | 代表的な標準化機関 |
|--------------------------------|--|--|
| デジュール標準 (de jure standard) | 公的な位置づけの標準化機関において明確に定められた透明かつ公正な手続きで関係者が合意の上、制定される標準 | <ul style="list-style-type: none"> ● ITU (国際電気通信連合) : 情報通信標準 ● ISO (国際標準化機構) : 情報処理・工業標準 ● IEC (国際電気標準会議) : 電気機器標準 |
| フォーラム標準 (forum standard) | 複数の企業等により結成されるフォーラムと呼ばれる組織が、公的ではないが開かれた標準化手続きにより策定する標準 | <ul style="list-style-type: none"> ● IETF (Internet Engineering Task Force) : インターネット技術の標準 ● IEEE (Institute of Electrical and Electronics Engineers) : 米国電気電子技術者学会の標準 ● W3C (World Wide Web Consortium) : ウェブ技術の標準 |
| デファクト標準 (de facto standard) | デジュール標準のような標準化プロセスを経ず、市場で多くの人に受け入れられることで事実上の標準となったもの | <ul style="list-style-type: none"> ● マイクロソフト社のOS (MS-Windows) ● アップル社のOS (iOS) ● グーグル社のOS (Android) |

出典：一般社団法人情報通信技術委員会 (TTC)「情報通信分野における標準化活動のための標準化教育テキスト」(https://www.ttc.or.jp/application/files/5016/5345/9954/Standard_text_v8.0.pdf) を元に作成

⁸¹ 一般社団法人情報通信技術委員会 (TTC)「情報通信分野における標準化活動のための標準化教育テキスト」(2022.3) https://www.ttc.or.jp/application/files/5016/5345/9954/Standard_text_v8.0.pdf

このような背景のもと中国が影響力を強める中で、2014年から2022年までITUのトップである事務総長に中国の趙厚麟氏が選挙に勝利し、2期連続で務めることとなった。趙厚麟氏をトップとしながら、中国は挙国一致でITUの事業に取り組み、インターネットプロトコルに関する監視社会に向けた中央集権的な提案をはじめとし、5G、サイバーセキュリティに加え、本来ITUが守備範囲としていなかった知的財産権、人工知能などに関する2,000以上の新たな基準を提案し、中国に有利な議会運営がなされていた。また、2022年2月には、ロシアと共同で声明を発表し、声明の中でITUについて明確に触れながら、更なる関与に大きな関心を寄せている⁸²。

この状況を打開すべく、2021年の5月には、ブリンケン國務長官が、米国のドリーン・ボグダン＝マーティン候補を推薦し、さらには米国の戦略国際問題研究所（CSIS）がITUの事務総長選挙にマーティン氏を勝利させるために必要なアクションについて提言するなど⁸³、米国側が取り組みを加速させた。結果として、2022年9月の事務総長選挙ではロシアが擁立した候補を押さえ、米国のドリーン・ボグダン＝マーティン候補が圧勝する結果で終わっている。これと並行し、2021年9月、日本政府はITUの重要ポストである電気通信標準化局長に、尾上誠蔵氏の擁立を発表し、2022年9月に日本人として初めて局長に選ばれる結果となった。中国の華為技術（ファーウェイ）の強力な支援を受けたとされるチュニジアの候補に終盤で追い上げられつつも、総務省など各政府関係者による事前のロビー活動が功を奏した形となり、日米が連携して情報通信分野の経済安全保障を確立する体制を整えた⁸⁴。また、ITU選挙以外の動きでは2022年5月には、米国政府主導で「未来のインターネットに関する宣言」が発表され、日本や欧州各国を含む60か国および地域が名を連ねた。マルチステークホルダーによるインターネットガバナンスを源氏すべき5つの原則のうちの1つにあげている。

(2) インターネットガバナンスを第三者の立場で外から監視する団体の動向

インターネット空間の分断を食い止める動きは、インターネットガバナンスを担ってきたマルチステークホルダーの民間組織のみならず、人権団体なども含む国際NGOの働きが大きい。あくまで国際NGOはインターネットの断絶を直接止める手段にはなり得ないが、特に国家によって自国のインターネットを外から遮断する動きや、自国の国民がインターネットを使用できないようにする動きについて監視を行い、世界に訴えかける役割は重要であるといえる。

インターネットの監視を行う団体のなかでも、前述したIETFの上層団体である国際NPO「インターネットソサイエティ（ISOC）」は、1992年に設立がなされてから30年以上にわたってインターネットの発展を支えてきている。直接的にインターネットガバナンスに関わることはないものの、デジタルデバイドの解消に向け、インターネットに全ての人がアクセスできるよう、各地でインフラ構築や人材育成に携わるほか、さらにはインターネットガバナンスについてのディスカッションの場を提供するにあ

⁸² President of Russia 「Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development」 (2022.2.4)
(<http://www.en.kremlin.ru/supplement/5770>)

⁸³ CSIS(Center For Strategic and International studies),Kristen Cordell 「How to Win at the International Telecommunication Union」 (2021.5.20)(<https://www.csis.org/analysis/how-win-international-telecommunication-union>)

⁸⁴ 「6Gで中国対抗 「LTEの父」尾上氏、国連通信機関局長に」(日本経済新聞, 2023.1.5)

たり、IGF 開催ともかかわりが深い。同団体が発表している「Action Plan 2023 Our Internet, Our Future」には、インターネットの強化、発展、そして人々がアクションを起こすためのエンパワーメント施策などについてそれぞれ対策が述べられている⁸⁵。

また、イギリスに拠点を置く国際 NPO 団体「ネットブロックス (NetBlocks)」は、設立が 2017 年の比較的新しい国際団体である。インターネットにおける自由度を監視する団体として設立され、特徴としては、独自のインターネット監視ツールである「The Internet Observatory (インターネット天文台)」をもとに、重要インフラへのインターネットの断絶、オンラインにおける検閲、サイバー攻撃を検出し、可視化していることである。また、「Cost of Shutdown Tool」というツールもサイト上で公開されており、インターネットの断絶やネットワークの遅延などの妨害行為の経済的コストの概算を算出できるようになっている。実際に誰もが無料で利用できるツールとなっており、サイト上で影響を受けた国やインターネットサービスを選択し、インターネットの断絶が行われた日数および時間を入力することですぐにコスト算出を行うことができる。そのほかにも、インターネットの断絶に関するレポートを多く公表しており、世界に発信を続けている⁸⁶。

最後に、2023 年はインターネットガバナンスについての「対話」の場を提供しているインターネットガバナンスフォーラム (IGF) について、日本での開催が予定されている⁸⁷。インターネットガバナンスに関する課題について、マルチステークホルダー (政府、民間部門、技術・学術コミュニティ、市民社会等) が参加する国連主催のハイレベル会合となっており、インターネットガバナンスについてそれぞれの立場についての相互理解がなされることが期待される。

⁸⁵ Internet Society 「Action Plan 2023 Our Internet, Our Future: Protecting the Internet for Today and Tomorrow」
(<https://www.internetsociety.org/wp-content/uploads/2022/12/Internet-Society-Action-Plan-2023-EN.pdf>)

⁸⁶ NETBLOCKS 公式サイト (<https://netblocks.org/>) (2023.3.30 閲覧時点)

⁸⁷ Japan IGF (<https://japanigf.jp/about/igf-2023igf>) (2023.3.31 閲覧時点)

3.3. 我が国における経済安全保障推進法の意義および ICT インフラの経済安全 全保障上の課題

3.3.1. 経済安全保障推進法の概要

2022年のロシアによるウクライナ侵攻や、近年激しい対立を見せる米中関係などの昨今の国際情勢を踏まえ、我が国においても経済安全保障分野への対応が喫緊の課題となっている。多摩大学大学院教授の國分俊史教授は「経済を使った戦争」であるとし、「いわゆる核抑止力によって軍事衝突の脅威が遠のいた結果、いわば『経済が武器』となり、『経済を使った戦争』になった」としている⁸⁸。

東京大学公共政策大学院の鈴木一人教授によると、経済安全保障という言葉には、グローバルコンセンサスとして固まった定義があるわけではなく、各国がそれぞれに解釈をして定義を行っているとする。例えばアメリカにおいては、「経済安全保障は、意図的・非意図的に関わらず、サプライチェーンが寸断されるような状態は、アメリカの経済安全保障上の問題であるという建て付けになっている」と話している。そのようななかで、2022年5月には、我が国においても経済安全保障へ国を挙げた対策を行うために、経済安全保障推進法が成立し、我が国としての経済安全保障が定義されている。図表 3-22 に示すように、我が国の経済安全保障の大きな方向性として「自律性の向上」と「優位性ひいては不可欠性の確保」をあげている⁸⁹。小林鷹之経済安全保障担当大臣は、「国益を経済面から確保する」と経済安全保障を位置づけたうえで、そのアプローチの1つが「自律性の向上」であり、経済構造の自立性を向上させ、日本の産業の脆弱性を把握し、解消することであるとしている。さらに、「優位性ひいては不可欠性の確保」については、日本が競争力を持つ先端的な技術を見極めて磨きをかけることで、世界において不可欠な存在になることと説明している⁹⁰。

先に述べたとおり、「自律性の向上」と「優位性ひいては不可欠性の確保」を大きな方向性としている経済安全保障推進法において、鈴木教授は、日本の経済安全保障は「安全保障という言葉が付いているだけに、国家の安定、経済、社会の安定ということが目的として設定されているだろう。また経済という言葉が付いているのは、国家の安定や経済社会の安定に対して、何らかの外国からの圧力や影響を受けた場合に、軍事とは異なる経済的な手段によって、国家や、社会、経済を守るという性格を持つものであろう。」と述べている。また、ポイントとしては、日本の経済安全保障は、先に述べたアメリカの経済安全保障とは異なり、意図した攻撃のみを想定していることがある。地震や台風などの自然災害なども国家の安定や経済社会の安定を考えるうえでは重要な要素であるものの、経済安全保障推進法においては、あくまで意図的な攻撃のみを想定したものとなっている。

今後、経済安全保障推進法の範囲内のみならず、より幅広く経済安全保障についての議論がなされるこ

⁸⁸ 「新たな「防衛力」経済安全保障とは何か」(NHK 政治マガジン, 2020.10.21)

(<https://www.nhk.or.jp/politics/articles/feature/46667.html>)

⁸⁹ 内閣官房 経済安全保障推進会議 (第1回) 配布資料「資料3 経済安全保障の推進に向けて」(2021.11.19)

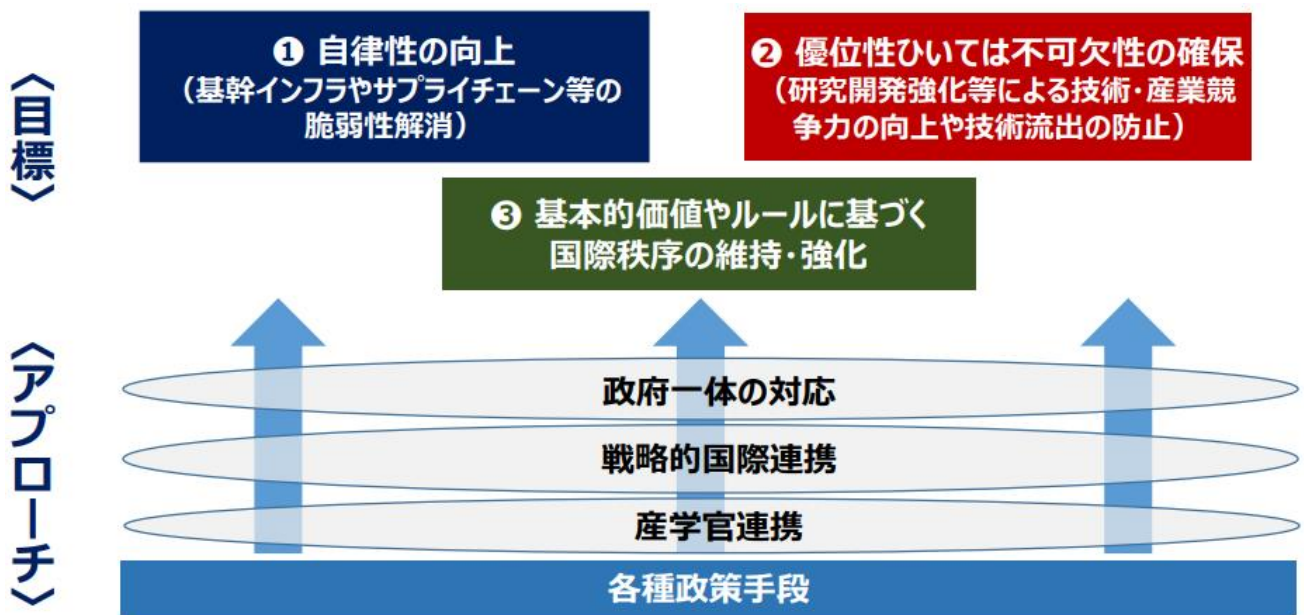
(https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai1/shiryoku3.pdf)

⁹⁰ 「「国内クラウドの能力は重要な国家課題」、小林大臣が語る経済安保の本質」(日経クロステック, 2022.4.8)

(<https://xtech.nikkei.com/atcl/nxt/column/18/02014/040700005/>)

とが予想される。鈴木教授は、経済安全保障は他国の圧力や脅威などその時の外部的な要因によって我が国がどのように対抗するかが左右されるため、プロアクティブに不変的なビジョンをもって進めることが難しく、今後は柔軟性をもった対応が重要となるとしている。また、産業界においては、経済安全保障への対応が迫られることによって損失を被る可能性もあるとしながらも、経済安全保障時代のビジネスチャンスもあるとしている。「信頼感や信用を得るということについて、日本の企業はブランド力やレピュテーションを持っているので、それを武器に、例えばアメリカやヨーロッパで、中国製品を買わなくなったようなお客さんに売っていくといったことができる。さらには日本国内でも、今まで中国製品を買っていた事業者が、やはり国産のものを買おうという風になっていけば、値段が高くても買ってもらえるというメリットがこれから生まれてくる。」と話している⁹¹。

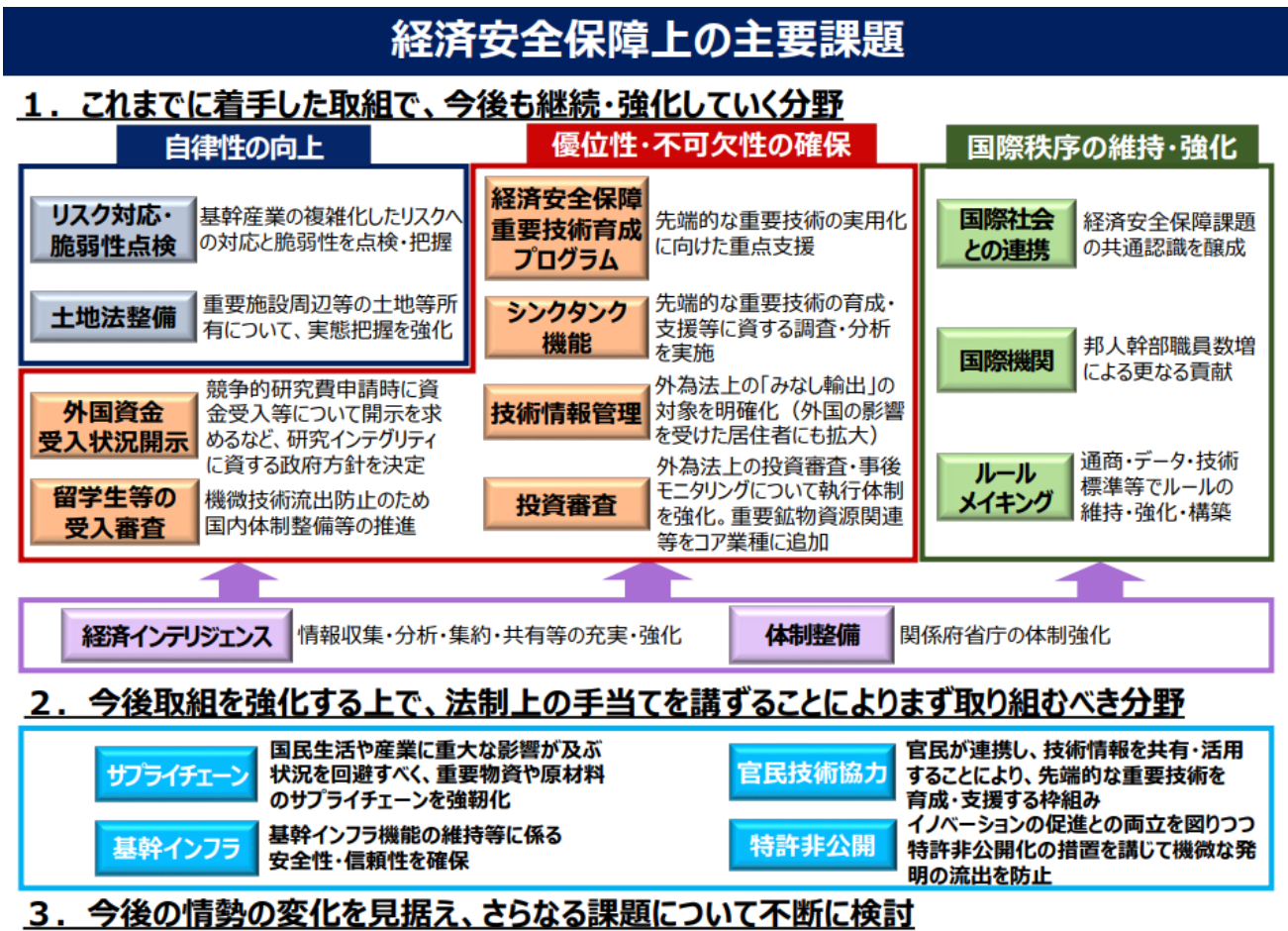
図表 3-22 経済安全保障の推進における我が国としての大きな方向性



出典：内閣官房 経済安全保障推進会議（第1回）配布資料「資料3 経済安全保障の推進に向けて」（2021.11.19） (https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai1/shiryous3.pdf)

⁹¹ 有識者ヒアリング（東京大学公共政策大学院 鈴木 一人教授）に基づく。

図表 3-23 経済安全保障上の主要課題



出典：内閣官房 経済安全保障推進会議（第1回）配布資料「資料3 経済安全保障の推進に向けて」（2021.11.19）（https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai1/shiryous3.pdf）

このような方向性において、図表 3-23 に示す経済安全保障上の主要課題のうち、法整備を最優先で進めるべき分野として、①重要物資や原材料のサプライチェーンの強靱化、②基幹インフラ機能の安全性・信頼性の確保、③官民で重要技術を育成・支援する枠組み、④特許非公開化による機微な発明の流出防止の4つが提示され、経済安全保障担当大臣の下に設置された「経済安全保障法制に関する有識者会議」において、法整備へ向けた検討が開始された⁹²。

2022年3月の衆議院本会議において経済安全保障推進法が審議入りし、2022年5月11日の参議院本会議における賛成多数での可決により法案が成立した。以下、主な法案の内容について、4つの柱を軸として整理をする。

⁹² 内閣官房 経済安全保障推進会議（第2回）配布資料「資料1 経済安全保障法制に関する提言の概要」（2022.2.4）（https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai2/shiryous1.pdf）

(1) 経済安全保障推進法の4つの柱

1) 特定重要物資の安定的な供給の確保

(ア) 概要

この20年、世界は自由貿易によるグローバル化の恩恵を享受してきた。各国が経済的に相互依存を深めることが安全保障となるとされ、サプライチェーンと呼ばれるいわゆる製品供給網は他国において製造された部品などで構成されるようになっていった。しかし、昨今の米中対立などの地政学リスクにより、各国がサプライチェーンの見直しに迫られている。経済安全保障推進法における第2の柱である、基幹インフラの安定稼働に対する対策においても、サプライチェーンリスクは重要な課題となっている⁹³。

経済安全保障推進法の第1の柱として定められている「特定重要物資の安定的な供給の確保」においては、基本方針として「外部から行われる行為により国家及び国民の安全を損なう事態を未然に防止するため、特定重要物資の安定的な供給の確保」⁹⁴を目指すものとして、法案に定められている。制度の枠組みとしては主に、対象となる特定重要物資の指定を行い、指定された特定重要物資を扱う民間事業者に対するサプライチェーン上の脆弱性に対する対策支援を行う。

(イ) 特定重要物資の指定（政令による指定）

2022年5月の法案成立後、特定重要物資の指定に向けて、物資を所管する各省庁によって、公的・業界統計、業界団体および事業者からのヒアリング結果等を基にして、候補となる物資の検討が進められた。さらなる精査として、候補物資について、内閣府と所管省庁によって、図表3-24の4つの要件に該当しているかどうかについて精査が進められた。

⁹³ 平井宏治（2022）「経済安全保障のジレンマ 米中対立で迫られる日本企業の決断」育鵬社

⁹⁴ 内閣官房「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（2022.5.11）
<https://www.cas.go.jp/jp/houan/220225/siryou3.pdf>

図表 3-24 特定重要物資の指定の要件

➤ 以下の4要件を全て満たす、特に安定供給確保を図るべき重要な物資に絞り込んで適切に指定する。

| | | |
|-----|---|---|
| 要件1 | <p>国民の生存に必要不可欠 又は 広く国民生活又は経済活動が依拠</p> | <p>国民の生存に直接的な影響が生じる物資をいう。</p> <p>国民の大多数に普及していたり、様々な産業に組み込まれていたりして、経済合理的な観点からの代替品がない物資をいう。</p> |
| 要件2 | <p>外部に過度に依存 又は 外部に過度に依存するおそれ</p> | <p>供給が特定少数国・地域に偏っており、供給途絶等が発生した場合に甚大な影響が生じ得る物資をいう。</p> <p>社会経済構造の変化や技術革新の動向（メガトレンド）等を踏まえ、我が国が措置を講じなければ将来的な外部依存のリスクの蓋然性が認められる物資をいう。</p> |
| 要件3 | <p>外部から行われる行為による供給途絶等の蓋然性</p> | <p>外部から行われる行為により供給途絶等が発生し、国民の生存や国民生活・経済活動に甚大な影響を及ぼす可能性を評価し、その蓋然性が認められること。</p> |
| 要件4 | <p>本制度による措置の必要性</p> | <p>要件1～3に加え、本制度による施策が特に必要と認められる場合に指定を行う。</p> <p>①他制度による措置が既に講じられている場合には、本制度により措置を講ずる必要性は小さいと判断される。</p> <p>②措置を講ずる優先度が高く、特にその必要性が認められる場合としては、例えば、次に掲げる場合が考えられる。</p> <ul style="list-style-type: none"> ✓ 国民の生存に必要不可欠な物資又は基幹的な役割を果たすインフラ機能の維持に与える影響が顕著と考えられる物資のうち、例えば、近年、供給途絶等が発生した実績がある、供給途絶等のリスクが高まる傾向がみられるなど、早急に措置を講ずる必要がある場合 ✓ 中長期的な社会経済構造の変化や技術革新の動向（メガトレンド）を踏まえ将来にわたって重要性や成長性が見込まれる場合や、我が国及び諸外国・地域における産業戦略や科学技術戦略での位置づけ等を総合的に勘案し、例えば、近年、国際環境の変化等を受け、諸外国・地域で物資の囲い込みが行われるリスクが高まっている、集中的な支援が検討されているなど、早急に措置を講ずる必要がある場合 |

出典：内閣官房 経済安全保障法制に関する有識者会議（令和4年度～）（第3回）配布資料

「資料 サプライチェーン強靱化パートの運用に向けた検討」（2022.10.6）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai3/siryuu.pdf

4つの要件を踏まえて精査が行われた特定重要物資の候補について有識者会議およびパブリックコメントを実施し、2022年12月、特定重要物資として11分野が指定された。（図表3-25）指定された物資には、今後更なる需要が見込まれる半導体、再生可能エネルギー普及におけるEV等の機関製品とされる蓄電池、2022年3月のウクライナ危機により世界的に需給がひっ迫した液化天然ガス（LNG）など含まれた⁹⁵。これらの11分野の特定重要物資については、それぞれに「安定供給確保取組方針」として、サプライチェーン上の課題や動向等を踏まえた取組の方向性や全体像が規定され、効果的な取組の実施がなされる。

⁹⁵ 「経済安全保障「重要物資」半導体など11分野、閣議決定」（日本経済新聞、2022.12.20）

<https://www.nikkei.com/article/DGXZQOUA180QD0Y2A211C2000000/>

図表 3-25 特定重要物資 11 分野と所管省庁および 2022 年度第 2 次補正予算における計上額

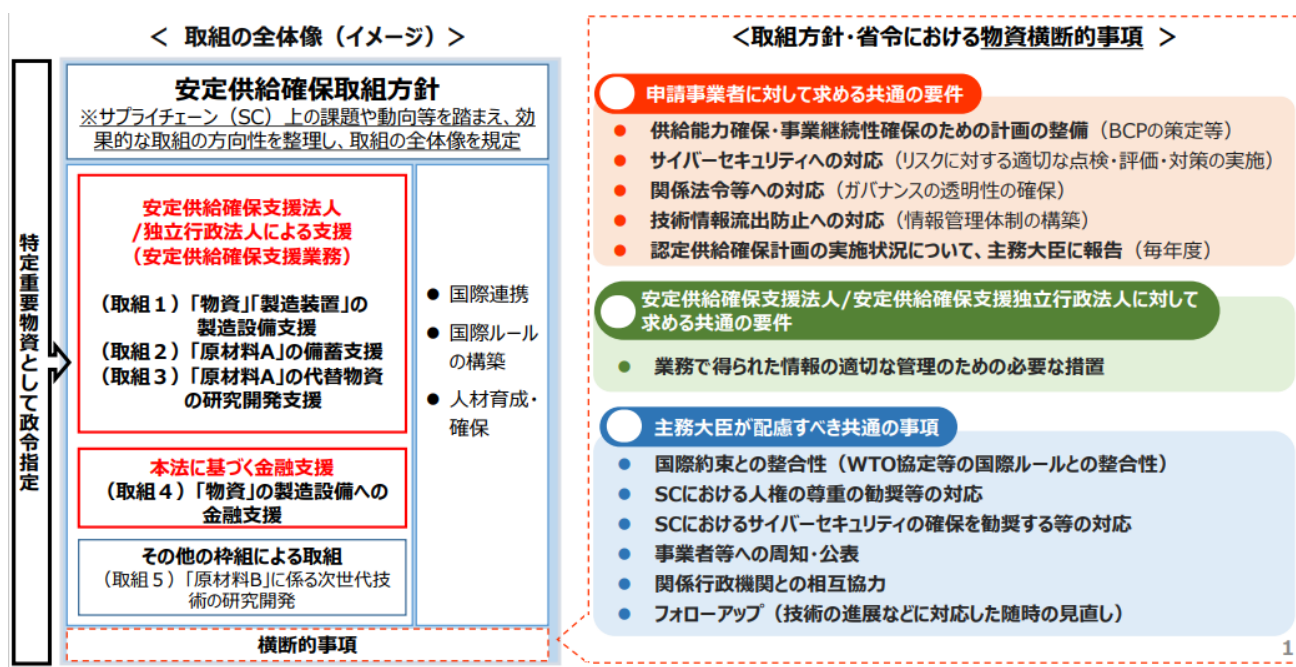
| | | |
|-------|-----------------|--------|
| 経済産業省 | 半導体 | 3686億円 |
| | 蓄電池 | 3316億円 |
| | 重要鉱物 | 1058億円 |
| | 航空機の部品 | 417億円 |
| | 工作機械 産業用ロボット | 416億円 |
| | 永久磁石 | 253億円 |
| | 天然ガス | 236億円 |
| | クラウドプログラム | 200億円 |
| 国土交通省 | 船舶の部品 | 63億円 |
| 厚生労働省 | 抗菌性物質製剤 | 553億円 |
| 農林水産省 | 肥料 | 160億円 |

出典：「経済安全保障「重要物資」半導体など 11 分野、閣議決定」（日本経済新聞,2022.12.20）
<https://www.nikkei.com/article/DGXZQOUA180QD0Y2A211C2000000/> を元に作成

(ウ) 民間事業者による供給計画の策定と支援措置

先に述べたとおり、特定重要物資に指定された物資については、「安定供給確保取組方針」として、サプライチェーン上の対策が行われる。図表 3-26 の取り組みの全体像（イメージ）に記載されているとおり、特定重要物資として政令に指定された物資については、製造設備の支援や、原材料の備蓄支援、代替物資の研究開発支援、そして製造設備への金銭的な支援が行われる。

図表 3-26 安定供給確保取組方針の全体像および横断的事項



出典：内閣官房 経済安全保障法制に関する有識者会議（令和4年～）（第4回）配布資料
 「資料1 特定重要物資の指定について【安定供給確保取組方針（概要案）】」（2022.11.16）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai4/siryou1.pdf

取組においては、申請事業者、安定供給確保支援法人、および主務大臣の3つの関係セクターに対して物資横断的事項として要件が課されている。（図表 3-26）本取組の主体となる特定重要物資の申請事業者に対しては、事業継続性確保のための計画、サイバーセキュリティへの対応、ガバナンスの透明性等の計画、実施が求められている一方で、安定供給確保支援法人や主務大臣はそれらの取組をサポートし運用する事項が定められている。

各省庁の職員が省庁横断的に問題の調整を行うことを目的として2022年8月1日には内閣府に「経済安全保障推進室」が設置された⁹⁶。また、同日には法案の一部の施行が開始され、特定重要物資の安定確保に向けた、経済安全保障推進法第48条第1項に基づくサプライチェーン調査が可能となった。サプライチェーン調査の留意点として、民間事業者の理解を得るため、適切な調査内容の絞り込み、調査の目的、主旨、位置づけ等について丁寧な説明の実施が必要である旨が、2022年9月30日に閣議決定がなされた「特定重要物資の安定的な供給の確保に関する基本指針」にも明記されている⁹⁷。

⁹⁶ 「「重要物資」を指定へ 経済安保推進室が発足」（日本経済新聞,2022.8.1）
<https://www.nikkei.com/article/DGXZQOUA013VM0R00C22A800000/>

⁹⁷ 「特定重要物資の安定的な供給の確保に関する基本指針」
https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin1.pdf

2) 特定社会基盤役務の安定的な提供の確保

(ア) 概要

特定社会基盤役務の安定的な提供の確保については、「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保」を基本方針としている⁹⁸。特定妨害行為とは、「サイバー攻撃などの電磁的な方法によるものだけでなく、物理的な方法によるものも想定される」のことであり、具体的には、特定重要設備の脆弱性に関する情報を用いて感染するウイルス、埋め込まれた不正プログラム等によって、特定重要設備の機能を停止・低下させる行為が例示されている。同法では、特定妨害行為を未然に防ぐ目的で、重要設備の導入・維持管理等の委託について、事前に審査を行うことを規定している。

2022年1月に行われた「第3回 経済安全保障法制に関する有識者会議 基幹インフラに関する検討会合」の提言骨子において、基幹インフラを含むあらゆる領域におけるサイバー攻撃に関して、「一度システムを導入した後にリスクを排除することは困難」であるとし、被害の防止には「設備の導入等の際に事前にリスクを排除することが必要である」としており、基幹インフラの安全性確保には、事業者への事前の規制が不可欠であることが述べられている。一方で、規制によって経済活動が過度に制限されることのないよう、制度設計全体、および規制の対象とする事業、事業者、設備それぞれについても「国家及び国民の安全」に与える影響に鑑み真に必要なものに限定するべきである」としている⁹⁹。

現在、特定社会基盤役務の安定的な提供の確保に関する制度は2024年春ごろからの運用開始を目指して検討が進められている。2023年2月に経済安全保障法制に関する有識者会議において公表された「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（案）」に基づき、パブリックコメントの募集が行われ、それに基づいた審議が同有識者会議においてなされた後、閣議決定がなされる予定である。

閣議決定後は、基本指針に基づいて政令および主務省令の策定、特定社会基盤事業者の指定が行われる予定であり、それに伴い事業者に向けたQ&Aやガイドラインの作成・公表が予定されている¹⁰⁰。

(イ) 審査対象

特定社会基盤事業者の対象分野については、同法第50条において規定されており、14種類の事業（電気事業、ガス事業、石油事業、水道事業、鉄道事業、貨物自動車運送事業、外航貨物事業、航空事業、空港事業、電気通信事業、放送事業、郵便事業、金融事業、クレジットカード事業）のうち、政令で定める

⁹⁸ 内閣官房「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（2022.5.11）

<https://www.cas.go.jp/jp/houan/220225/siryou3.pdf>

⁹⁹ 内閣官房 経済安全保障法制に関する有識者会議（令和3年度）（第2回）基幹インフラに関する検討会合 配布資料「経済安全保障法制に関する提言骨子（基幹インフラの安全性・信頼性の確保）」（2022.1.19）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai3/teigenkossi2.pdf

¹⁰⁰ 内閣官房 経済安全保障法制に関する有識者会議（令和4年度～）（第5回）配布資料「資料6 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針(案)の概要」（2023.2.8）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai5/siryou6.pdf

ものとされている。¹⁰¹ また、2023年2月には、各省において検討中ではあるものの、相当に具体的な事業者の指定基準が示され、規模にかかわらず代替が困難なインフラ役務を提供するような一定の事業を除き、基本的には、中小の事業者は対象とならず、大規模事業者のみが指定対象となる方向性が示された。特に、国民の財産に直結する金融に関しては、銀行、信用金庫、信用組合だけでも500以上に及んでおり、規模は小さくても特定の地域において独占しているケースなどが考慮された場合、規模のみを考慮した線引きとならない可能性についても示唆されていた¹⁰²。結果的には、銀行業を営む者のうち、①預金残高：10兆円以上、②口座数：1,000万口座以上又は③ATM台数：1万台以上、系統中央機関（信金中央金庫、全国信用協同組合連合会、労働金庫連合会及び農林中央金庫）が行う事業は、系統中央機関の業務を行う者、など線引きが明確化されている¹⁰³。

(ウ) 審査および勧告・命令

審査は主に、重要設備を導入する際もしくは維持管理の委託を行う際に、事前に計画書を所管省庁の大臣に届け出るというものである。事前審査にかかる期間は原則30日、最大で4カ月とされているが、場合によっては期間の短縮も可能となっている。虚偽の届け出には2年以下の懲役か100万円の罰金が科される。審査が行われた結果として、国外からの特定妨害行為の手段として使用されるリスクが高い重要設備であると国が認定した場合には、重要設備の導入の変更および中止や、維持管理内容の変更および中止などが必要な措置として勧告される。

2023年2月に公表された「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（案）」¹⁰⁴において、「リスク管理措置」という新たな概念が導入されている。特定社会基盤事業者である企業が自らリスクを評価し、そのリスクの内容や程度に応じて講ずる対策のことが「リスク管理措置」という。事前審査において「リスク管理措置」の実施状況は、特定重要設備が特定妨害行為の手段として使用されるリスクを判断する上で、審査に必要な要素の一つとなる。すなわち企業自ら可能な限りリスクマネジメントを行うことによって、国による勧告・中止命令の対象とならずに、重要設備を導入し、維持・管理の委託を行う余地ができたといえる¹⁰⁵。

¹⁰¹ 内閣官房「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（2022.5.11）

<https://www.cas.go.jp/jp/houan/220225/siryou3.pdf>

¹⁰² 「インフラ安全確保、14業種に事前審査 対象設備は不明確」（日本経済新聞, 2022.11.9）

<https://www.nikkei.com/article/DGXZQOUA2934I0Z20C22A9000000/>

¹⁰³ 内閣官房 経済安全保障法制に関する有識者会議（令和4年度～）（第5回）配布資料「資料8 特定社会基盤役務の安定的な提供の確保に関する制度における特定社会基盤事業・特定社会基盤事業者の指定基準の考え方」（2023.2.8）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai5/siryou8.pdf

¹⁰⁴ 内閣官房 経済安全保障法制に関する有識者会議（令和4年度～）（第5回）配布資料「資料7 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（案）」（2023.2.8）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai5/siryou7.pdf

¹⁰⁵ 「経済安全保障推進法アップデートー基幹インフラ役務の安定的な提供の確保に関する制度（基本指針案等の公表）」（西村あさひ法律事務所, 2023.2.13）

https://www.nishimura.com/sites/default/files/newsletters/file/newsletter_230213_competition_law_international_trade.pdf

3) 特定重要技術の開発支援

(ア) 概要

経済安全保障をめぐる議論において核となる観点の 1 つは技術である。東京大学公共政策大学院の鈴木一人教授は、「技術の優劣が各国の軍事力の優劣を左右するなかで、軍事に関わる技術が漏洩もしくは公開され、それが対立する国の手に渡れば、その技術を使って強化した軍事力によって圧迫されかね」なると述べている。¹⁰⁶また、米中技術覇権とも称される時代において、米国を中心とする同盟国の 1 国として我が国が技術の開発支援を強化する重要性は高いといえる。

特定重要技術の開発支援においては、国の施策として「特定重要技術の研究開発の促進及びその成果の適切な活用を図るため、必要な情報の提供、資金の確保、人材の養成及び資質の向上その他の措置を講ずるよう努める」と法案に記されている。¹⁰⁷ 資金面のみならず、人材育成、官民のコミュニケーションなど、技術開発支援において経済安全保障を推進するために必要とされるすべての措置を体系的に講じることが求められている。

技術開発支援のプロセスにおいては、広範囲にわたって様々な技術の調査研究を新たに設立されるシンクタンク（特定重要技術調査研究機関）が担う。その調査研究内容を元に、「特定重要技術」の定義に該当する技術については、個別プロジェクトごとに、研究代表者の同意を得て協議会の設置がなされる。また、「特定重要技術」に該当する技術のなかでも、特に優先して育成すべき技術については、「経済安全保障重要技術育成プログラム（通称：K Program）」において、指定基金協議会が設置され、全ての関係者が一丸となり研究開発を強力に推進する。

以下、特定重要技術の概念整理（シンクタンクが調査研究を実施する技術領域や特定重要技術の定義など）、2022 年 11 月に公表された協議会の運営に関するモデル案、そして「経済安全保障重要技術育成プログラム（通称：K Program）」の概要について整理する。

(イ) 特定重要技術の概念整理

先に述べたとおり、シンクタンクは「特定重要技術」のみならず、広範囲にわたって様々な技術の調査研究を行うものとされているが、より具体的には、「科学技術・イノベーション基本計画」や「統合イノベーション戦略 2022」等の各技術分野の戦略に基づく施策との整合性を配慮すべきとされている。調査研究を実施する具体的な技術領域としては、図表 3-27 における「調査研究を実施する技術領域」に記載されている技術が対象とされている。

また、それらの調査研究が実施された技術領域のなかでも、図表 3-27 における「特定重要技術」の①②③の定義がなされている技術に関しては、後述する「協議会」の設置が可能となる。「特定重要技術」に該当する技術については、協議会における必要な情報が国から提供されるほか、資金面での援助、人材

¹⁰⁶ 「経済安全保障は日米同盟強化の一環、共に「技術」を高め、守る」（日経ビジネス, 2022.7.13）

[\(https://business.nikkei.com/atcl/gen/19/00478/071100010/\)](https://business.nikkei.com/atcl/gen/19/00478/071100010/)

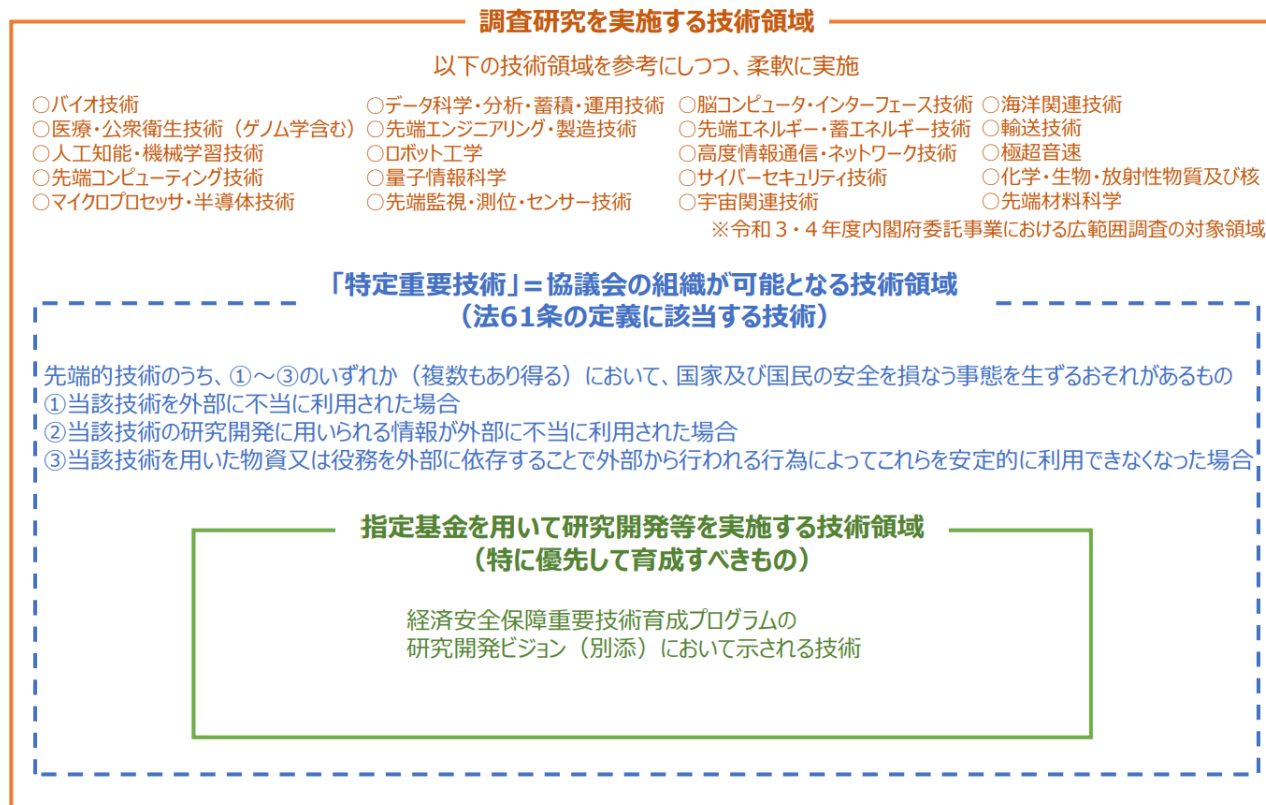
¹⁰⁷ 内閣官房「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（2022.5.11）

<https://www.cas.go.jp/jp/houan/220225/siryous3.pdf>

養成と資質の向上などの措置が講じられる。この「特定重要技術」について、鈴木一人教授は、選定された技術は我が国が他国と比較して劣っている技術であり、キャッチアップの要素が強いため、戦略的不可欠性の観点で不足していると指摘する。「他の国に対して、日本に何か突出して優れたものがある、そのために他国が日本に依存する、ということを目指したものにはなっていない」と話している¹⁰⁸。

「特定重要技術」のうち、後述する「経済安全保障重要技術育成プログラム（通称：K Program）」において、最優先として支援対象とする技術について現在検討が進められている。

図表 3-27 特定重要技術の概念整理



出典：内閣官房 経済安全保障法制に関する有識者会議（令和4年度～）（第1回）配布資料「資料4 各説明資料」（2022.7.25）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai1/siryoku4.pdf

(ウ) 協議会（官民パートナーシップ）

協議会とは、「官民パートナーシップ」という言葉で称されるとおり、技術開発を行う民間事業者とそれを支援し国家戦略として推し進める行政機関の官民連携の枠組みである。官民連携は、経済安全保障分野における技術開発支援において特に重要であるとされている。従来、科学者が戦争に関与した反省から、日本学術会議は大学では軍事目的の科学研究は行わないとする方針を貫いてきており、安全保障にかかわる技術は、防衛装備庁などの国の限られた研究機関のみで行われており、支援も民間の研究

¹⁰⁸ 有識者ヒアリング（東京大学公共政策大学院 鈴木 一人教授）に基づく。

機関を対象とする必要はなく、安全保障分野における技術開発支援において官民連携という概念はなかった。しかしながら、科学技術の急激な進歩により、特に最先端の技術においては軍事と民生の利用をはっきりと区別することは難しくなっており、日本学術会議（梶田隆章会長）は、軍事と民生双方で活用できる「デュアルユース（両用）」の先端科学技術研究について、軍事に無関係な研究と「単純に二分することはもはや困難」とし、事実上容認する見解を示している¹⁰⁹。「特定重要技術」に指定されている技術の多くが大学などの民間の研究機関にて研究が進められている現状においては、研究が行われている民間側の研究と政府の官民連携が必要となっており、協議会の設置はいわば時代の要請ともいえる。

また、研究者が研究を進める上でのプロジェクト運用の自由についても、協議会の設置は制約を課すこととなる。伝統的な科学技術であれば、一部の研究者が代表となり全ての科学技術分野について包括的に政策調整を行うことが一般的である。それに対して、経済安全保障推進法においては、「特定重要技術」それぞれの研究プロジェクトに対して協議会が設置され、研究者の代表だけでなく政府も構成員となる。すなわち、従来の科学技術に対する支援の形としては、あくまで研究計画に基づいた資金提供のみに政府が関わり、運用については研究者に一定の自由度があったといえるが、経済安全保障推進法においては、研究者のみならず研究開発大臣、国の関係行政機関の長、シンクタンク等によって構成される協議会が、研究プロジェクトの運用および管理を行うこととなるため、研究者の自由は一定程度制約される¹¹⁰。また、協議会の構成員は、守秘義務登録情報の取り扱いについても厳格な管理が求められる。図表 3-28 に示す通り、人的措置、物理的措置、技術的措置についての規定について有識者会議において検討が進められている。

図表 3-28 特定重要技術研究開発協議会における守秘義務登録情報の取り扱い

| 守秘義務登録情報の取扱い | | | |
|--------------|------------------------------------|-------|---------------------------------|
| 人的措置 | 守秘義務登録情報の範囲、守秘義務の存続期間、共有する範囲等の明示 | 技術的措置 | 電子情報の暗号化措置（外部電磁記録媒体又はファイルの暗号化等） |
| | 目録の作成・維持 | | 情報端末使用時のアクセス制限及びログの記録 |
| 物理的措置 | ICカード等により制御された入口、受付又は施錠等による取扱区域の管理 | 技術的措置 | 外部ネットワーク接続端末使用時のフルスキャン |
| | 施錠した引き出し又はロッカー等で保管 | | 技術的脆弱性に関する情報の取得と適切な対処 |
| | 持出しに伴うリスクを回避できる場合を除き、持出しを制限 | | 電子的な伝達時の暗号化措置 |
| | 構成員等による四半期毎目途の保管状況の点検 | | 破棄時、復元できないように削除 |
| | 破棄時、復元できないよう裁断 | | |
| | 書留など許可されていないアクセス及び不正使用等から保護する手段で送付 | | |

出典：内閣官房 経済安全保障法制に関する有識者会議（令和4年度～）（第4回）配布資料「資料5 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第62条第1項に規定する協議会に関する協議会モデル規約（案）等」（2022.11.16）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai4/siryous5.pdf

¹⁰⁹ 「学術会議、軍民「両用」技術の研究を容認…「単純に二分するのはもはや困難」（読売新聞、2022.7.27）

<https://www.yomiuri.co.jp/science/20220726-OYT1T50377/>

¹¹⁰ 「経済安全保障推進法は科学技術政策を変えるか？」（東京財団政策研究所、2023.2.15）

https://www.tkfd.or.jp/research/detail.php?id=4186#_ftn1

また、研究成果は公開が基本とされ、研究者を含む協議会が、研究開発の進展や技術の特性、政府インフラ、テロ・サイバー攻撃対策、安全保障等での利用において支障のある技術に関し、研究開発の促進方策や個々の技術の成果の取扱等を決定する。協議会における研究成果は安全保障面のみならず経済活動への応用が期待されており、政府から共有される有用なシーズ（技術の萌芽）とニーズ（その技術を使った製品やサービスの需要）に関する情報も踏まえた活用が見込まれている。東京大学公共政策大学院の鈴木一人教授は、「新興技術」が民間部門で活用され、社会実装が進み経済活動が活性化する一方、そこで開発された技術が安全保障にも資するものとなっていくことが期待されている。つまり、経済活動のための研究開発を支援するという「手段」を通じて、結果的に技術開発が進むことで安全保障に必要な技術も取得するという「目的」という位置づけになっている。」と述べている¹¹¹。

(エ) 経済安全保障重要技術育成プログラム（通称：K Program）

先述のとおり、「特定重要技術」として指定されている技術のうち、特に優先的に技術開発支援を行うべき技術については、「経済安全保障重要技術育成プログラム（通称：K Program）」において技術開発が推進される。プログラム推進にあたっては、経済安全保障上我が国に必要な重要技術を見極め、技術における優位性・不可欠性を確保・維持することが重要視され、市場経済のメカニズムのみに委ねては投資が不十分となりがちな先端技術を育成・支援することが期待されている¹¹²。実証度合が高い技術は経済産業省の所管するNEDO（新エネルギー・産業技術総合開発機構）に、基礎研究に近いものは文科省が所管するJST（科学技術振興機構）にそれぞれ基金を組成するため、令和4年度補正予算においてそれぞれ1250億円、合計2500億円を計上している。

2022年9月、経済安全保障推進会議・統合イノベーション戦略推進会議合同会議が開催され、「経済安全保障重要技術育成プログラム 研究開発ビジョン（第一次）」において支援対象とする全27の技術が決定された。図表3-29に示す通り、「海洋領域」、「宇宙・航空領域」、「領域横断・サイバー空間領域」、「バイオ領域」の領域および、「AI技術」「量子技術」「ロボット工学」「先端センサー技術」、「先端エネルギー技術」の5つの最先端技術をベースとし、それらに基づく27の具体的な支援対象とする技術が定められている。この決定を元に、2022年10月中旬に第一弾の研究開発構想として、図表3-29の青色点線枠の技術、同年12月下旬には第二弾の研究開発構想として図表3-29の赤色実線枠の技術について公表がなされた。第三弾は2023年3月ごろを予定している。さらに、これらの研究開発構想の公表と並行し、2022年12月には公募が開始された。2023年春頃採択を見込んでおり、それぞれの技術の指定基金協議会に参加予定の関係行政機関についても整理が進められている¹¹³。

¹¹¹ 「経済安全保障と経済制裁：新たな国際経済秩序の「表裏一体の盾と矛」（新潮社 Foresight, 2022.5.16）

<https://www.fsight.jp/articles/-/48869>

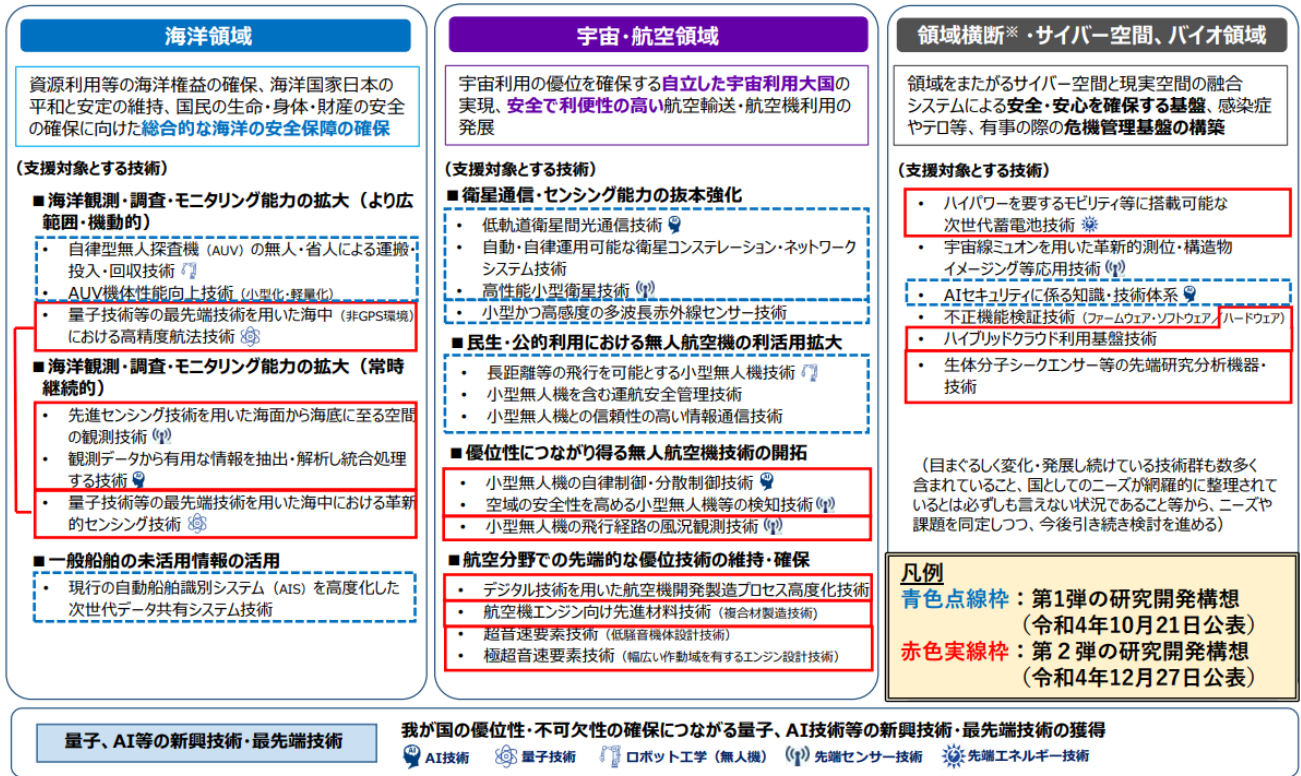
¹¹² 内閣府 経済安全保障重要技術育成プログラムに係るプログラム会議（第3回）「資料2-1 研究開発ビジョン（第一次）（案）概要」（2022.8.29）https://www8.cao.go.jp/cstp/enzen_anshin/program/3kai/siryu2-1.pdf

¹¹³ 内閣府 経済安全保障重要技術育成プログラムに係るプログラム会議（第4回）「別紙4 令和4年12月に公募を開始した研究開発構想に係る指定基金協議会に参加が想定される関係行政機関等について」（2023.2.8）

https://www8.cao.go.jp/cstp/enzen_anshin/program/4kai/bessi4.pdf

図表 3-29 経済安全保障重要技術育成プログラムに係る研究開発ビジョン（第一次）

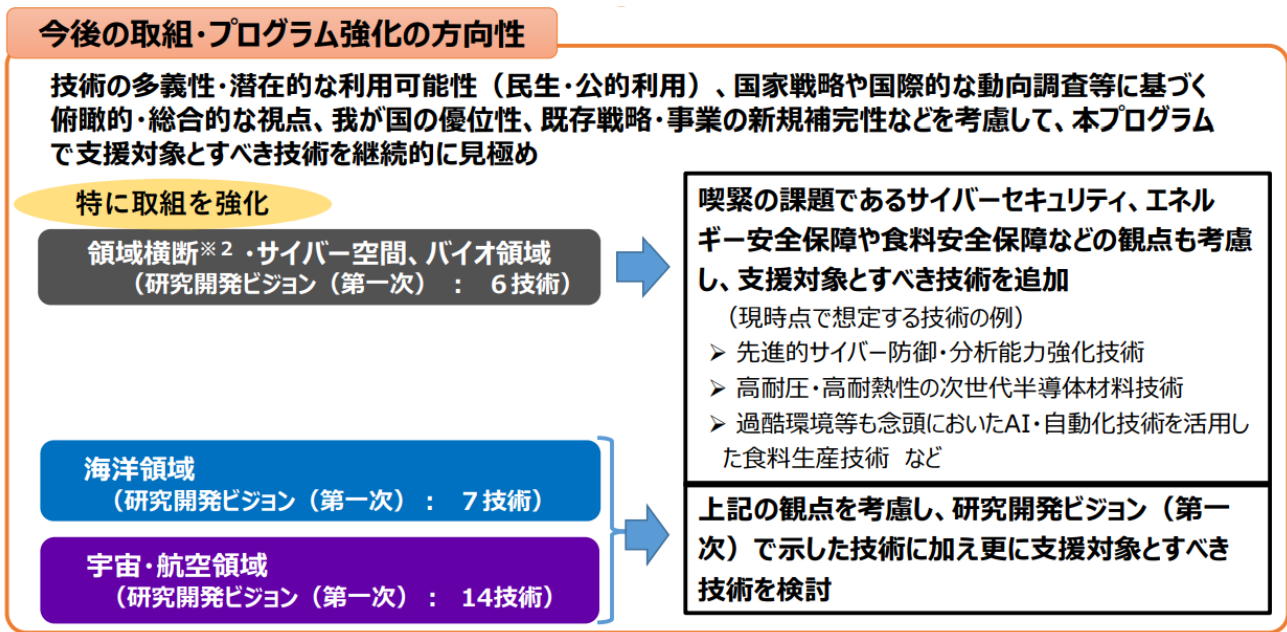
支援対象とする 27 の技術



出典：内閣府 経済安全保障重要技術育成プログラムに係るプログラム会議（第4回）「別紙1 経済安全保障重要技術育成プログラムに係る研究開発ビジョン（第一次）支援対象とする技術」（2023.2.8）
https://www8.cao.go.jp/cstp/anzen_anshin/program/4kai/bessi1.pdf

また、今後のプログラム強化の方向性として、図表 3-30 に示す通り、現在取組が進められている「領域横断・サイバー空間領域」、「バイオ領域」の領域については、サイバーセキュリティやエネルギー安全保障、食料安全保障などの観点も考慮に入れ、支援対象とすべき技術を随時追加していく予定とされている。「海洋領域」、「宇宙・航空領域」についても、支援対象とする技術の検討は継続的に行われるものとしている。

図表 3-30 経済安全保障重要技術育成プログラムの強化に向けて



出典：内閣府 経済安全保障重要技術育成プログラムに係るプログラム会議（第4回）「資料2-1 経済安全保障重要技術育成プログラムの予算措置状況について」（2023.2.8）

https://www8.cao.go.jp/cstp/anzen_anshin/program/4kai/siryoy2-1.pdf

図表 3-31 Kプログラムにおけるシンクタンクのミッションおよび果たすべき役割

安全・安心に関するシンクタンク機能の基本方針（案）

当面の具体的なミッション

- ① 経済安全保障重要技術育成プログラムの運用に当たって必要な情報提供・助言や、経済安全保障推進法に基づく調査研究の受託を可能とする調査・分析基盤の構築
- ② 新たな分析手法の開発とOJTによる人材養成・能力開発
- ③ 国内外の関係機関との間の調査研究ネットワークの構築

シンクタンクの果たすべき機能・役割

○シンクタンクとして果たすべき基本的な機能・役割については以下のように整理される。

| | 立上げ時点で持つべき機能・役割 | 将来的に拡張するべき機能・役割 | 留意点 |
|----------|--|---|--|
| 情報収集 | <ul style="list-style-type: none"> ・オープンソースからの情報収集 ・人的ネットワークを介した非公開情報の収集 | <ul style="list-style-type: none"> ・国内外の政府機関等からの非公開情報の入手 ・在外公館等と連携した情報収集 ・海外とのクローズドな意見交換 | <ul style="list-style-type: none"> ・適切な情報管理体制の構築 ・組織全体に法的な守秘義務をかけることにより保秘を担保 ・情報公開ポリシーの作成 |
| 解析・分析 | <ul style="list-style-type: none"> ・技術動向分析、社会科学的分析 ・成熟度、依存度などの技術評価 ・シーズとニーズのマッチング | <ul style="list-style-type: none"> ・データサイエンス、シナリオ分析等の新たな分析手法の開発 ・マッチングの高度化 | <ul style="list-style-type: none"> ・解析・分析能力はコア能力として内在化 ・政策立案に向けたアウトプット |
| 人材育成 | <ul style="list-style-type: none"> ・即戦力の確保とOJTによる人材養成・能力開発 ・産学官との人材交流 | <ul style="list-style-type: none"> ・人材育成プログラムや学位プログラムの構築 ・海外との人材交流 | <ul style="list-style-type: none"> ・処遇やキャリアパスの面で魅力度を高めることが課題 ・産学官との人事交流に当たっての障壁の排除 |
| ネットワーク構築 | <ul style="list-style-type: none"> ・国内外の関係機関とのネットワーク構築 ・国内公的シンクタンクとの連携 | <ul style="list-style-type: none"> ・海外シンクタンクとの連携強化 ・人材の層を厚くするための関係コミュニティの構築 | <ul style="list-style-type: none"> ・シンクタンクが内在化すべきコア機能と外部機関と連携して対応する機能の峻別が必要 |

- ファンディング等のその他の機能については将来課題とし、まずは喫緊の課題であるシンクタンク機能を立ち上げ
 ○シンクタンク機能を十全に発揮できるような人事・給与システムの構築や事務サポート体制の整備も重要

出典：内閣府 安全・安心に関するシンクタンク設立準備キックオフ会合「資料1 安全・安心に関するシンクタンク機能の基本方針（案）」（2023.3.28）

(<https://www8.cao.go.jp/cstp/stmain/pdf/20230314thinktank/siry01.pdf>)

また、プログラムの運用にあたって必要な情報提供・助言や、経済安全保障推進法に基づく調査を行うとされているシンクタンクの設立に関して、2023年3月に内閣府による「安全・安心に関するシンクタンク設立準備キックオフ会合」において、議論がなされた（図表 3-31）。会議参加者である鈴木教授はこのシンクタンクについて、具体的なシンクタンクの輪郭はまだ今後も議論が必要であるとしつつも、他国の技術動向を踏まえたうえで、日本の技術で劣っているものは何か、あるいはこれから伸ばすべき技術は何かという戦略を考えるという大きな方向性については固まっていると述べている¹¹⁴。シンクタンクの本格的な設立準備は令和5年度において行われることとなっており、今後も検討が行われることとなる。

¹¹⁴ 有識者ヒアリング（東京大学公共政策大学院 鈴木 一人教授）に基づく。

4) 特許出願の非公開

(ア) 概要

特許制度の非公開については、以前から経済安全保障上の課題として議論がなされてきた背景がある。我が国においては、特許出願された発明は、原則として一定期間後に公開がなされるが、世界では、国家の安全、国防上の利害にかかわる機微な発明に関する特許については非公開とする国も多く、特許の非公開に関する制度が整備されていない国は G20 においてはアルゼンチン、メキシコ、そして日本のみとなっている¹¹⁵。

昨今の国際情勢を踏まえ、我が国においても特許の非公開を行うべきであるとの声が高まっている。「統合イノベーション戦略 2020」においては、イノベーションの促進と技術流出防止の観点との両立が図られるよう、特許出願公開や特許公表についての検討の必要性について指摘されており¹¹⁶、翌年 2021 年の「統合イノベーション戦略 2021」においては、レジリエントで安全・安心な社会の構築を推進するうえで、総合的な安全保障の基盤となる科学技術力を強化するための分野横断的な取組として、特許の非公開化を行うための検討を進めるとの内容が盛り込まれている¹¹⁷。

その後、制度の必要性を踏まえた検討が重ねられ、2022 年 5 月には経済安全保障推進法の 4 つの柱の 1 つとして法案が成立。特許の非公開制度の施行は 2024 年 5 月となっており、他の 3 つの柱よりも施行までの期間は長くなっており、法案を元にした具体的な制度設計が進められている。

(イ) 発明の選定プロセスと選定後の情報保全措置

情報保全を行う発明を選定するにあたり、特許の非公開における審査は二段階に分けられることとなった。図表 3-32 に示す通り、まず、特許庁が審査を行う「技術分野等によるスクリーニング(一次審査)」において、可能な限り対象を絞り込んだうえで二次審査を行う内閣府へと送られる。内閣府が審査を行う「保全審査(二次審査)」で、発明の情報を保全することが適切かどうかについての判断がなされることとなる。この際内閣府は、国の機関や外部の専門家の協力を得ながら検討を重ね、「保全対象発明」を指定する。

¹¹⁵ 内閣官房 経済安全保障法制に関する有識者会議(令和 3 年度)(第 2 回)配布資料「資料 10 経済安全保障法制に関する有識者会議 特許非公開に関する検討会合第一回資料」(2021.12.28)

(https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou10.pdf)

¹¹⁶ 内閣府「統合イノベーション戦略 2020」(2020.7.17) (https://www8.cao.go.jp/cstp/togo2020_honbun.pdf)

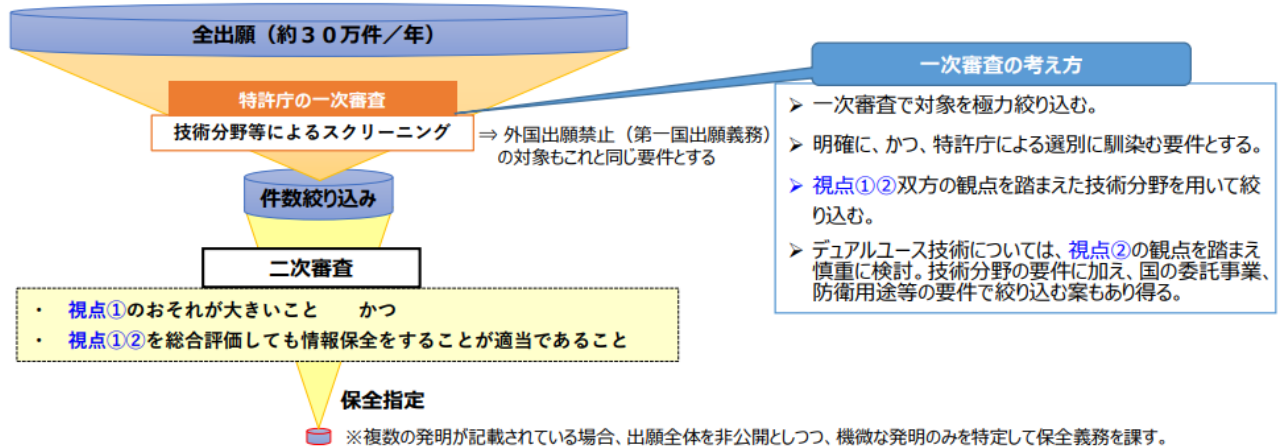
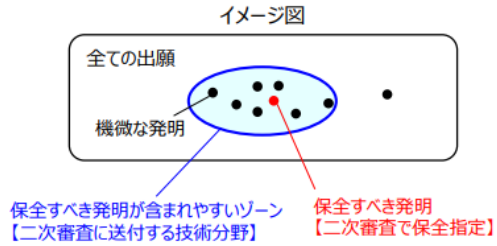
¹¹⁷ 内閣府「統合イノベーション戦略 2021」(2021.6.18)

(https://www8.cao.go.jp/cstp/tougosenryaku/togo2021_honbun.pdf)

図表 3-32 対象とすべき発明のイメージ

対象発明を選定する視点（一次審査・二次審査に共通）

- 視点①：技術の機微性**
- ▶ 我が国の安全保障を損なう事態を生ずるおそれ（例えば、核兵器を含む大量破壊兵器につながる技術など）
- 視点②：経済活動・イノベーションへの影響**
- ▶ 非公開とし、発明の実施や外国出願を制限することで、産業の発達にどの程度の影響（支障）を及ぼすか



出典：内閣官房 経済安全保障法制に関する有識者会議（令和3年度）（第3回）配布資料「資料10 経済安全保障法制に関する有識者会議 特許非公開に関する検討会合 第二回資料」（2022.1.19）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai3/siryou10.pdf

「保全対象発明」を選定する審査においては、2つの視点をもとに非公開とする発明の選定が行われることとなった。1つは「技術の機微性」、すなわち国家及び国民の安全を損なう自体を生ずるリスク、もう1つは「経済活動・イノベーションへの影響」として、発明を非公開とした場合に産業の発達に及ぼす影響度として、2022年5月の法案可決時点では整理がなされていた。これらを踏まえて更なる検討が行われ、2023年2月には非公開となる発明の詳細案について公表された。図表 3-33 に示す通り、前述の「技術の機微性」として、多大な影響や甚大な被害を与えうるものなのかどうか重要視され、宇宙やサイバー領域の先端技術、大量破壊兵器への転用が可能な核技術などが具体例として示されている。「経済活動・イノベーションへの影響」の観点では、当該発明の関係者の経済活動への影響をはじめ、産業の発展を阻害する可能性を十分に留意することが求められている。

図表 3-33 非公開となる発明（保全対象発明）

非公開の対象となる発明（保全対象発明）の考え方

➤ **機微性の要件（公にすることにより外部から行われる行為によって国家及び国民の安全を損なう事態を生ずるおそれが大きいこと）を満たすことを前提としつつ、その機微性の程度と保全指定をすることによる産業の発達への影響等との総合考慮により、情報の保全をすることが適当と認められた場合に保全指定をする。**

| | |
|--|--|
| <p>国家及び国民の安全を損なう事態を生ずるおそれが大きい発明</p> <p>➤ 安全保障上の機微性が極めて高いもの、すなわち、国としての基本的な秩序の平穏あるいは多数の国民の生命や生活を害する手段に用いられるおそれがある技術の発明が該当。</p> <p>➤ 具体的な類型：</p> <ol style="list-style-type: none"> ① 我が国の安全保障の在り方に多大な影響を与え得る先端技術の発明（将来の戦闘様相を一変させかねない武器に用いられ得る先端技術や、宇宙・サイバー等の比較的新しい領域における深刻な加害行為に用いられ得る先端技術等） ② 我が国の国民生活や経済活動に甚大な被害を生じさせる手段となり得る技術の発明（大量破壊兵器への転用が可能な核技術等） | <p>産業の発達に及ぼす影響等の考慮</p> <p>➤ 安全保障上極めて機微な発明であっても一律に非公開とはせず、保全指定をした場合に産業の発達に及ぼす影響等を考慮し、適当と認められる場合に限り保全指定をする。</p> <p>➤ 産業の発達に及ぼす影響の内容：次の観点から総合的に考慮</p> <ol style="list-style-type: none"> ① 特許出願人を含む当該発明の関係者の経済活動に及ぼす影響 ② 非公開の先願に抵触するリスクに関して第三者の経済活動に及ぼす影響 ③ 我が国におけるイノベーションに及ぼす影響 <p>➤ 特に、今後民生分野の産業や市場に幅広く展開され、発展していくような発明については、発明の内容の開示や実施を制限することが我が国の経済活動やイノベーションへ支障を及ぼしかねないことに十分留意。</p> |
|--|--|

出典：内閣官房 経済安全保障法制に関する有識者会議（令和4年度）（第5回）配布資料「資料4 特許出願の非公開に関する基本指針(案)の概要」（2023.2.8）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai5/siryou4.pdf

「保全対象発明」の選定においては、特許出願人との密なコミュニケーションを行うことで、特許出願人にとって過度な負担とならないことを留意することが求められている。また、保全対象発明の特許出願人については、損失の補償を国が行う旨も盛り込まれている。また、選定がなされた後については、情報保全措置として、発明内容の開示の原則禁止や、外国の出願の禁止、他の事業者との発明の共有が承認制となるなどの形で、特許発明の非公開にかかる対策が講じられる。また、保全指定の期間は1年ごとに延長の可否が判断されることとなる。

そのほか、法案に盛り込まれた「外国出願の制限」については、日本国内で行われた発明かつ、先に述べた「保全対象発明」にあてはまる発明の場合には、外国ではなく日本の特許庁に出願を行わなければならないとし、第一国出願義務とされている。外国出願の禁止は、特許出願後最大10カ月で自動解除される仕組みになっており、この期間内に保全審査が行われる必要があるとされている¹¹⁸。

3.3.2. 経済安全保障における ICT インフラの安定的な稼働の重要性

経済安全保障推進法における4つの柱において、以下では「特定社会基盤役務の安定的な提供の確保」について述べる。特定社会基盤事業者として同法案において14の分野が定められていることは先に述べた通りであるが、電気通信事業のなかでも、戦略的自律性および戦略的不可欠性を担保するための基盤となる ICT インフラ（海底ケーブル、5G、データセンター）について、経済安全推進法で検討されてい

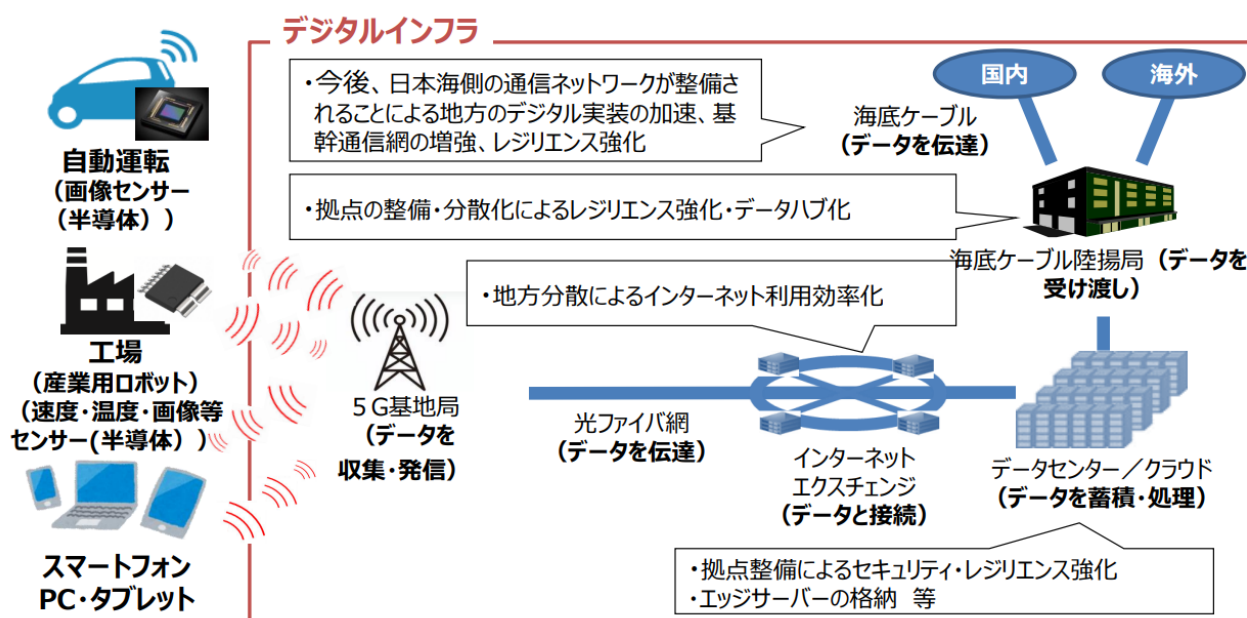
¹¹⁸ 内閣官房 経済安全保障法制に関する有識者会議（令和4年度）（第5回）「資料5 特許法の出願公開の特例に関する措置、同法第三十六条第一項の規定による特許出願に係る明細書、特許請求の範囲又は図面に記載された発明に係る情報の適正管理その他公にすることにより外部から行われる行為によって国家及び国民の安全を損なう事態を生ずるおそれが大きい発明に係る情報の流出を防止するための措置に関する基本指針（案）」（2023.2.8）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai5/siryou5.pdf

ることの範囲外も含めた「経済安全保障」という概念において、重要性および課題を整理する。

経済安全保障における ICT インフラの重要性については、総務省においても整理がなされている。安心性、信頼性の確保が世界的に重要視されていることを踏まえ、サプライチェーンリスク対策を含む経済安全保障対策として同志国との連携を強化しつつ、我が国の 5G や国際的データ流通の増大に対応する海底ケーブル等の海外展開を官民で推進するとしている¹¹⁹。また、我が国が推進している「デジタル田園都市国家構想」が実現された社会においては、あらゆる場所でデータが収集され、データセンター（クラウド上）で処理されたあと、最終的には現場にそれぞれのデータが戻っていくという「データの循環」が実現される必要があるとされている。データセンターを支える 5G ネットワークや海底ケーブルの増設を行うにあたり、単に数を増やすだけではなく、セキュリティやレジリエンスの強化といった経済安全保障の観点でのインフラ強化が必要である。（図表 3-34）

図表 3-34 デジタル田園都市国家構想実現におけるデジタルインフラの強化



出典：総務省 経済産業省 デジタルインフラ（DC等）整備に関する有識者会合（第3回）
「デジタルインフラ（DC等）整備に関する有識者会合中間とりまとめ（概要）」（2021/12/13）
(https://www.soumu.go.jp/main_content/000787667.pdf)

経済安全保障の観点においてこれらのインフラが最重要視されている背景には、他国からの攻撃などによって ICT インフラの戦略的自律性が失われ、インターネット通信が途絶した場合、国の様々な機能が停止すると想定されているためである。特に、図表 3-34 に示す通り、海底ケーブルが途絶した場合には、5G 基地局やデータセンターは基盤のインフラを失い、機能停止が予想されている。後述するとおり我が国の国際通信の 99%を担う海底ケーブルの切断が発生した場合、多くの情報基盤を海底ケーブルで

¹¹⁹ 総務省 情報通信審議会 情報通信政策部会 総合政策委員会（第7回）「資料7-5 国際戦略の取り組み状況について」（2022/3/31） (https://www.soumu.go.jp/main_content/000807266.pdf)

つながる米国に依存しているクラウドサービスが停止してしまう可能性がある。現状、重要情報の取り扱いの多くを海外のクラウドサービスに依存している状況のため、クラウドサービスの停止が社会インフラや企業経営に与える影響は計り知れない。

さらには、米国 SNS サービスの使用についても、海底ケーブルを通して米国のデータセンターと繋がることで日本国内にサービスが提供されているため、海底ケーブルが途絶した場合には使用不可となる。航空券の予約システムや国際電話の使用不可、SWIFT（国際銀行間通信協会）ネットワークの機能停止なども予想され¹²⁰、想定されうる被害事例は枚挙にいとまがない。海底ケーブルをはじめとし、データセンター、5G 通信の経済安全保障における重要性を認識したうえで、リスクマネジメントを官民連携でいかに推進できるかが今後の焦点となる。

以下の章では、それぞれの ICT インフラの経済安全保障上の重要性について整理し、安定的な稼働を維持する上での課題および対策について検討する。

(1) 海底ケーブル

1) 経済安全保障における海底ケーブルの重要性

先に述べた通り、島国であり海に囲まれた我が国の国際通信は、その 99%を海底ケーブルに依存している。近年は、通信手段の一つとしての衛星通信技術の発展も見られ、ウクライナ侵攻においては、イーロンマスク氏が CEO を務める米 Space X 社、自社構築した人工衛星軍による通信網「Starlink（スターリンク）」をウクライナの国民や軍に対して提供し、有事の通信手段としても話題となっている¹²¹。しかしながら、通信速度の観点からは、例えば日米間における海底ケーブルの長さが約 9000 キロであるのに対し、衛星通信は一般的にその 8 倍の長さとなっている。衛星よりも利用者までの距離が近い海底ケーブルの通信速度は圧倒的な速さとなっているため、国際通信において海底ケーブルは必要不可欠なインフラとなっている。

海底ケーブルの安定的な稼働および通信の供給は、図表 3-34 に示す通り、全てのデジタルインフラの基盤となっており、海底ケーブルが途絶は文字通り致命的となり、情報通信インフラサービスにとって、戦略的自律性の要となっている。また、近年、太平洋における海底ケーブルの敷設において米中対立が激化しており、我が国にとっても戦略的不可欠性の観点でも重要さを増している。中国は、巨大経済圏構想「一帯一路」政策の一環で、「デジタルシルクロード」構想を提唱しているが、海底ケーブルにおいてもこの動きが見られるのである。「デジタルシルクロード」構想とは、中国主導のもと、発展途上国などの諸外国においてデジタル化を進める構想であり、デジタル製品・サービスの輸出の促進、5G などの次世代デジタル技術の主導権を確保することを目的としている¹²²。中国は、発展途上国のなかでも特に権威

¹²⁰ 「ヤバすぎる日本の海底ケーブル 台湾有事でネット接続全滅リスク」（週刊エコノミスト Online, 2022.1.31）
(<https://weekly-economist.mainichi.jp/articles/20220208/se1/00m/020/046000c>)

¹²¹ 「ウクライナで証明された衛星インターネットの有効性…アメリカ空軍もスターリンクと契約」（BUSINESS INSIDER, 2022.8.18）(<https://www.businessinsider.jp/post-257742>)

¹²² 「新型コロナで取り組みが加速する中国のデジタルシルクロード」（日本総研, 2020.10.19）
(<https://www.jri.co.jp/page.jsp?id=37464>)

主義体制の国に対して、安価で海底ケーブルの敷設を実施しつつ、中国製の 5G 携帯をはじめ、対話アプリ・微信(ウィーチャット)、キャッシュレス決済・支付宝(アリペイ)をえるようにと、「デジタルシルクロード」構想の推進がなされている。その結果として、アフリカ西海岸のカメルーンから南米のブラジルまでの約 6000 キロメートルの海底ケーブルを中国が敷設している¹²³。

中国は 2020 年、さらなる海底ケーブル敷設を行うべく、チリから中国を繋ぐ長距離の海底ケーブル構想を打ち出した。チリにとって中国は最大の輸出国であり、2019 年にはファーウェイ社がチリにデータセンター投資を行うとする話も出ていたが、この動きに対し、米国のポンペオ元米務長官がチリ側に中国企業の受注を避けるようくぎを刺していた。当時のトランプ政権の働きかけもあり、結果としてチリ政府は 2020 年 7 月下旬、NEC 社などの日本企業が提案したルートを採用した¹²⁴。

米国は、中国の海底ケーブルをめぐる動向を受けた 2020 年 8 月、「Clean Network Project (クリーン・ネットワーク構想)」を発表し、中国共産党などの悪意ある攻撃者による攻撃から市民のプライバシーと企業の機密情報を守るアプローチとして、通信キャリア、クラウドなどと並んで、海底ケーブルがクリーンであるべき対象として掲げられていた¹²⁵。クリーン・ネットワーク構想自体はトランプ政権による政策であったものの、方針としてはバイデン政権においても継承されている。その後、2021 年 3 月には中国が参加していたマイクロネシア連邦、キリバス、ナウルを結ぶ海底ケーブル事業についても入札が無効となった。中国企業の受注を警戒した日米豪の 3 か国が、事業を投げ推進していた世界銀行とマイクロネシア連邦をはじめとする 3 か国に対して、入札の見直しを迫っていた結果とされている¹²⁶。

このような動向において、我が国は同盟国を中心とした国際連携によって、経済と安全保障の両方の利を確保することで、自律性、ひいては戦略的不可欠性・優位性の向上に寄与するような対策を練る必要がある。

2) 海底ケーブルの安定的な稼働を維持するうえでの課題と対策

海底ケーブルにとってのリスクには、海底ケーブル自体が何らかの形で切断されてしまうことで、通信が途絶してしまうケースと、海底ケーブルの陸揚げ局に対するサイバー攻撃等による海底ケーブルの機能停止がある。以下ではそれぞれの課題および対策について、経済安全保障の観点から整理を行う。

(ア) 海底ケーブル自体の切断リスクおよび講じるべき対策

海底ケーブルの切断は、自然災害によって発生するケースも非常に多い。東日本大震災においては、KDDI 社の太平洋側の茨城県沖や千葉の銚子沖などで海底ケーブル 10 か所、10 か国以上に繋がる回線

¹²³ 「海底ケーブルで起きた米中の覇権争い、なぜ? 専門家に聞いた」(朝日新聞 GLOBE+, 2020.11.1)

(<https://globe.asahi.com/article/13885191>)

¹²⁴ 「チリ-豪の光海底ケーブル、日本案採用 脱・中国依存へ」(日本経済新聞, 2020.7.29)

(<https://www.nikkei.com/article/DGXMZO62014440Y0A720C2MM8000/>)

¹²⁵ 「クリーンネットワークとは? 中国をネットから排除する 5 つの取り組み。ポンペオ務長官が挙げる」

(Huffington Post, 2020.8.7) (https://www.huffingtonpost.jp/entry/clean-network_jp_5f2d0e96c5b6b9cff7f021f1)

¹²⁶ 「太平洋の光ケーブル、中国企業の入札無効 日米豪懸念で」(日本経済新聞, 2021.3.18)

(<https://www.nikkei.com/article/DGXZQODF021U30S1A300C2000000/>)

において障害が発生、完全復旧までには半年を要し、大きな被害が伴った。地震で海底の地盤がずれ、ケーブルに過剰な負荷がかかったことで断線してしまったとみられる¹²⁷。また、2022年1月には、トンガ沖の海底火山が噴火し、海底ケーブルの切断が発生。それにより、トンガにおけるインターネットトラフィックは現地時間1月15日午後5時30分ごろ、ほぼゼロになった。トンガは主に一本の海底ケーブルでインターネットに接続していたため、通信の復旧までには5週間を要した¹²⁸。

また、海底ケーブル自体の切断が発生する原因には、故意による人為的な切断がある。有事における海底ケーブルの切断は、歴史をさかのぼれば第一次世界大戦中に行われている。1914年8月、英国によるドイツに対する宣戦布告の発効後に英国側によってドイツー英国間の海底ケーブルが切断された。その後の第二次世界大戦においても多くの海底ケーブルが切断される事態となった¹²⁹。

100年以上前から、戦争における通信途絶の手段として行われてきた海底ケーブルの切断だが、我が国においても他国から海底ケーブルの切断が行われる可能性は高まっている。2023年2月2日には、中国籍の漁船によって台湾本島と中国福建省に近い離島・馬祖列島を結ぶ海底ケーブルが切断された。その6日後、中国籍の貨物船によって別のケーブルが切断されるという報道もなされている¹³⁰。さらには、中国は、台湾進攻の際には、沖縄の米軍基地のインターネット通信を遮断する目的で、沖縄の海底ケーブルを切断する可能性についても指摘されている。海底ケーブル破壊用の自爆ドローン「NH-1」なども中国によって開発されており、海底ケーブルの他国による物理的な切断によって我が国の通信の安定的な稼働が妨害され、最悪の場合には完全に途絶してしまう可能性もゼロとはいえない状態にある。

自然・故意による海底ケーブルの安定的な稼働への被害を最小限とするためには、ルートダイバーシティー（複線化）を確保することが望ましいとされている。2016年には日米間をつなぐ太平洋横断の海底ケーブルとして、「FASTER（ファスター）」の運用が開始され、東日本大震災当時にKDDIが運用していた2本の主要ケーブルに加えて、さらに敷設されるなど、自然災害への対策は我が国においても強化されている。また、ケーブル自体の強度を引き上げることも望ましい。自然災害等による被害を防ぐために、船の行き来や台風などの影響を受けやすい浅いエリアにおいては、ケーブルの周りに鉄線を巻いて強度を高めたり、海底数千メートルといった深海においては、細いケーブルとするなど、地形によって条件を変えることも行われている¹³¹。

海底ケーブルの切断における国際的な規制については、1994年発効の「海洋法に関する国際連合条約（UNCLOS）第113条 海底電線又は海底パイプラインの損壊」によって、公海上にて自国の船が海底ケーブルの切断を行った場合について、各国で犯罪とするよう求められている。しかしながら、他国の船が

¹²⁷ 「海底ケーブル 推進 6000メートルの海底で何が？～災害時の通信を守れ！～」

(NHK WEB 特集, 2021.3.9) (<https://www3.nhk.or.jp/news/html/20210309/k10012904451000.html>)

¹²⁸ 「トンガ噴火で浮き彫りになったネットの脆弱さ、復旧に数週間か」(MIT TECHNOLOGY REVIEW, 2022.1.21)

(<https://www.technologyreview.jp/s/266975/tongas-volcano-blast-cut-it-off-from-the-world-heres-what-it-will-take-to-get-it-reconnected/>)

¹²⁹ 土屋大洋 (2021)「米中分断の虚実 デカップリングとサプライチェーンの政治経済分析」, 日本経済新聞出版

¹³⁰ 「中国の「海底ケーブル切断」で「島国が完全に孤立化」の危機…！中国軍が進める「沖縄封鎖作戦」のヤバすぎる実態」(2023.3.25) (<https://gendai.media/articles/-/107823?imp=0>)

¹³¹ 「災害に強い海底ケーブルを KDDI や NEC、不断の挑戦」(日本経済新聞, 2022.3.11)

(<https://www.nikkei.com/article/DGXZQOUC060ES0W2A300C2000000/>)

公海上で故意に海底ケーブルの切断を行った場合については規定がなく、他国による海底ケーブルの切断に対する抑止力としては不十分な法整備となっている。また、海底ケーブルの運用は従来、民間事業者に委ねられてきており、他国の攻撃を想定した対策は不十分であるのが現状である¹³²。経済安全保障推進法における基幹インフラの一つとして、今後更なる法整備を進めていく必要がある。

(イ) 海底ケーブルの陸揚げ局の機能停止リスクおよび講じるべき対策

海底ケーブルのリスクには、ケーブル本体の切断のみならず陸揚げ局の機能停止の可能性についても考慮する必要がある。海底ケーブルは通常、陸揚げ局から延びているケーブルを沖合でつないだあと、海底ケーブル専用の敷設船によってケーブルを少しずつ海底にたらしつけて敷設していく。この陸揚げ局のシステムが物理的、あるいはサイバーによる攻撃を受けた場合には、海外との通信接続に支障をきたしてしまう。

有事の際には陸揚げ局が物理的な攻撃の対象となる可能性もあるため、多くが純粋な民間施設である陸揚げ局についても、重要インフラとして場所を秘匿する国もある¹³³。我が国においては、現在海底ケーブルは太平洋側に陸揚げ局が多く敷設されており、主な陸揚げ拠点は南房総地域から北茨城地域一帯、そして伊勢志摩エリアに集中しているが、我が国にある10か所の海底ケーブルの陸揚げ局のうち、千葉県と三重県の2か所にあるものが突出して大きく、この2か所が物理的な攻撃を受けて破壊された場合、被害は甚大なものとなることが指摘されている¹³⁴。

これらを踏まえ、海底ケーブルの立地の分散化についても対策が練られている。「デジタル田園都市国家インフラ整備計画」の一環として、海底ケーブルの陸揚げ局を地方分散化することにより、有事の安全保障対策のみならず、自然災害による被害も最小限に留める狙いがある。今後は日本海側にも敷設を進めることで、2025年度末までに日本を周回する海底ケーブルの実現を目指している。(図表 3-35)

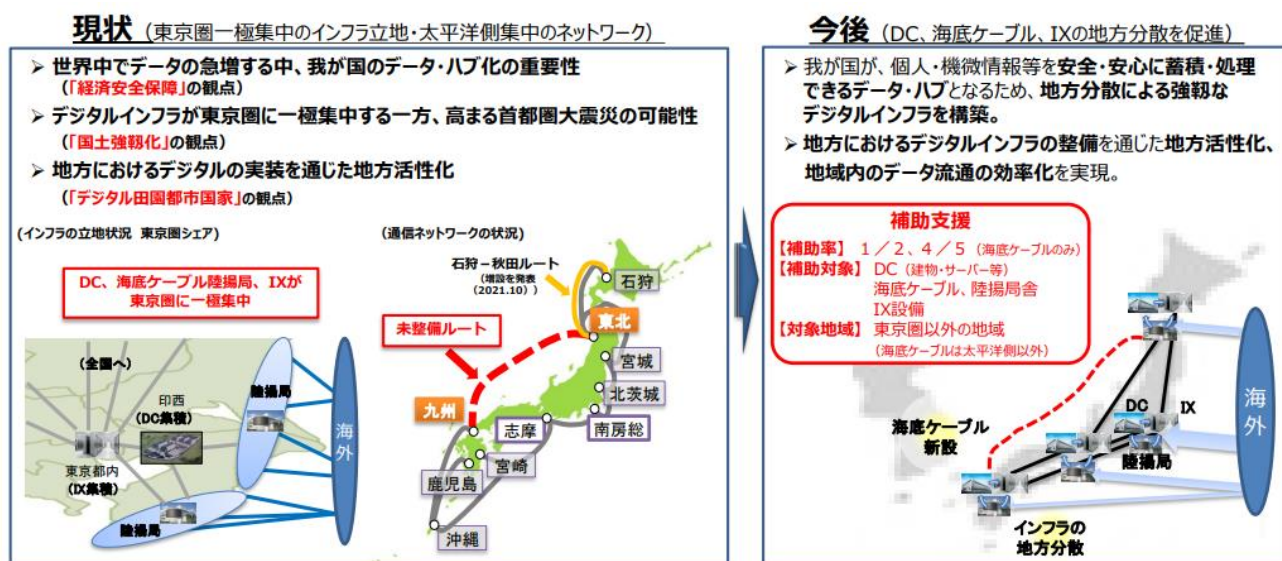
¹³² 「狙われる海底ケーブル 中国サイバー部隊はこう攻撃する」(Wedge ONLINE, 2021.11.22)

(<https://wedge.ismedia.jp/articles/-/24865>)

¹³³ 土屋大洋(2020)「サイバークレートゲーム」,千倉書房

¹³⁴ 「サイバー戦、物理的攻撃の脅威」(Japan In-depth, 2021.7.19) (<https://japan-indepth.jp/?p=60613>)

図表 3-35 政府によるデジタルインフラの地方分散支援



出典：総務省 経済産業省 デジタルインフラ（DC等）整備に関する有識者会合（第3回）
 「デジタルインフラ（DC等）整備に関する有識者会合中間とりまとめ（概要）」（2021/12/13）
https://www.soumu.go.jp/main_content/000787667.pdf

また、陸揚げ局へのサイバー攻撃への対策としては、経済安全保障推進法の基幹インフラ全般に関わることはあるが、サプライチェーンの脆弱性向上による未然防止対策、そして設備導入後のサイバー攻撃対策がある。海底ケーブルの陸揚げ局に入る設備は、世界で中国ファーウェイ社のものが増え始めているという¹³⁵。現在、海底ケーブルは需要が高まるなかで着々と増設が進められているが、陸揚げ局へのサイバー攻撃を想定した、経済安全保障推進法に基づく事前審査は必要不可欠である。

最後に、海底ケーブルの切断および陸揚げ局の機能停止など、海底ケーブルのリスクを踏まえた法整備の不十分さについては指摘されている。1994年発効の「海洋法に関する国際連合条約（UNCLOS）第113条 海底電線又は海底パイプラインの損壊」が、他国からの攻撃を想定しておらず、海底ケーブルの切断に対する抑止力とはなり得ていないことについては先に述べた通りである。加えて、我が国においての海底ケーブルの全般に関する法整備について、矢野（2019）は「始めに海洋基本法（平成19年法律第33号、以下「基本法」という。）に基づき、内閣に設置された総理大臣を本部長とする総合海洋政策本部について見るならば、海底通信ケーブルの防護という問題は検討対象にすら挙げられていない。因みに基本法に基づき2008年から5年ごとに策定されてきた海洋基本計画、海洋の状況及び海洋に関して講じた施策を取りまとめた年次報告を見ても、海底通信ケーブルという用語は見受けられない。また2001年の米中枢同時多発テロを契機に、米国で考え出された海洋状況把握（Maritime Domain Awareness、MDA）という安全保障政策を参考に、2016年7月に総合海洋政策本部が決定した『我が国の海洋状況把握の能力強化に向けた取組』を見ても、領海等における外国漁船の違法操業、近隣諸国による海洋権益をめぐる挑発的行為、地球温暖化による気象災害、海域での地震・津波災害、海洋汚染等が脅威とされ、海底通信ケーブルの防護については全く言及されていない。」とし、日本において海底ケーブルの防護に対

¹³⁵ 「海底ケーブルで起きた米中の覇権争い、なぜ？ 専門家に聞いた」（朝日新聞 GLOBE+, 2020.11.1）
<https://globe.asahi.com/article/13885191>

する取組が不足している現状について述べている¹³⁶。今後は、基幹インフラの 1 つとして、経済安全保障の観点から包括的な対策方針が策定され、法整備が行われることが望ましい。

(2) 5G

1) 経済安全保障における 5G 通信ネットワークの重要性

経済安全保障における 5G の重要性については、社会経済インフラとして安定的な稼働を維持することで国民生活を守るという安全保障上の観点、もしくは、次世代通信手段として社会実装を推進するなかで、各国がしのぎを削っている「技術シェア争い」という文脈において語られることが多い。前者は戦略的自律性を確保することにより、社会インフラとして国民生活を守るという色合いが強く、後者は戦略的不可欠性を獲得する、すなわち 5G 産業において我が国の 5G 製品・部品が世界的なシェアを獲得するという攻めの色合いが強い。

「デジタル田園都市国家構想」の実現に向けて、「デジタル田園都市国家インフラ整備計画」が推進されているなかで、社会活動の維持に欠かすことのできないデジタルインフラとして 5G の重要性が高まっている。特に、サイバー空間と実空間の一体化が一層進むことが予想されているなかで、5G ネットワークの機能停止は、通信手段が途絶えるということとは異なり、社会に甚大な被害をもたらすことが予想される。これらを踏まえ、以下では 5G の戦略的自律性、すなわち安定的な稼働を維持するうえでの課題と対策について整理を行う。

2) 5G 通信ネットワークの安定的な稼働を維持するうえでの課題と講じるべき対策

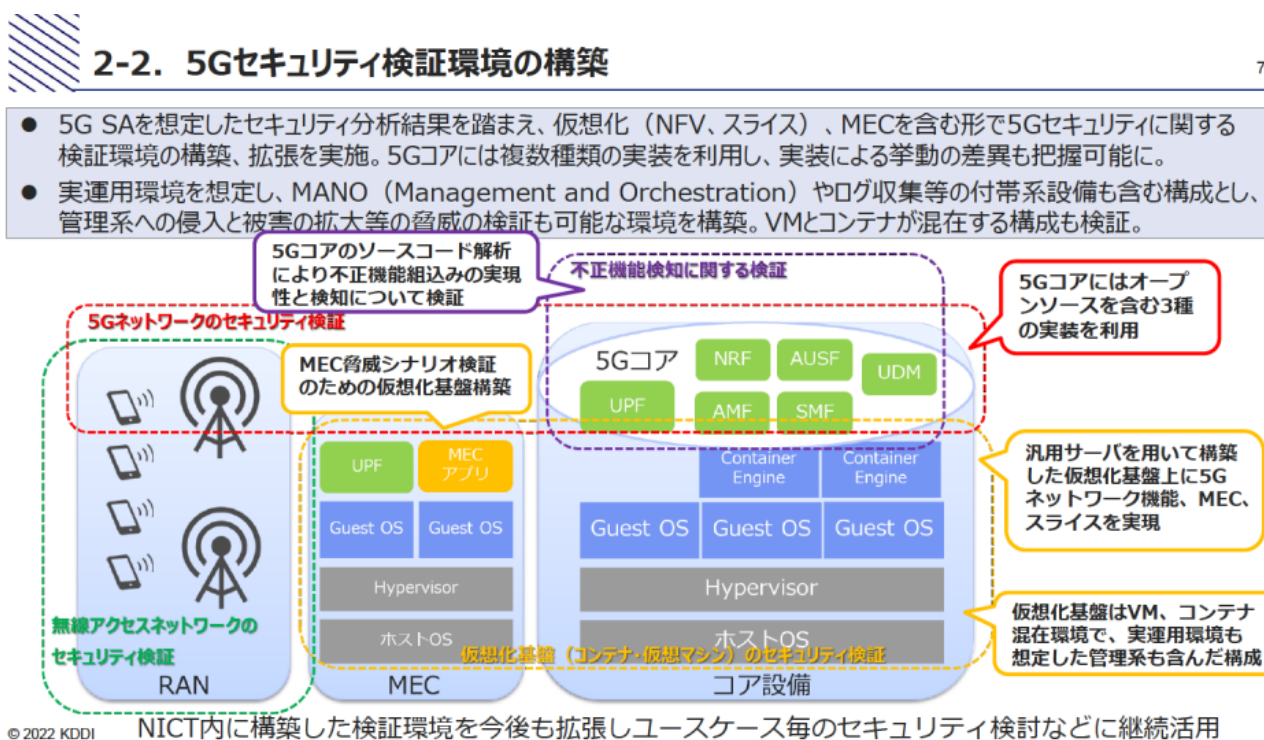
5G のネットワークは 4G 以前のセキュリティ対策と異なる点として、ネットワーク機能が仮想化・ソフトウェア化が技術的に可能となっていることである。それゆえに、5G 通信ネットワークにおいては、サイバーセキュリティの強化が喫緊の課題である。

総務省は 2022 年、「5G セキュリティガイドライン第 1 版」¹³⁷として、KDDI 社に委託してガイドラインを作成している。ガイドライン策定に向けた調査のなかで、5G ネットワークに組み込まれている新技術活用と、社会実装の両方において、それぞれのセキュリティ課題があるとしている。新技術活用においては、汎用ハードウェアやオープンソースソフトウェア (OSS)、ネットワークスライシングといった技術についての脅威について指摘されているほか、ネットワークのエッジ (基地局とコア網の間に設置) で通信処理や高度な演算・データ処理がなされるモバイルエッジコンピューティング (MEC) についてもセキュリティ対策を実施する必要があるとしている。また、社会実装における 5G 活用においては、IoT をはじめとし、自動車、プラント、医療、金融・決済など、それぞれの産業分野において検証が必要であるとされている。

¹³⁶ 矢野 哲也 (2019)「海底通信ケーブル防護のための日本の海洋ストラテジック・コミュニケーション」大阪経済法科大学 21 世紀社会総合研究センター (https://keiho.repo.nii.ac.jp/record/25/files/21c-social_10_2.pdf)

¹³⁷ 総務省「5G セキュリティガイドライン第 1 版」(2022.4.22)
(https://www.soumu.go.jp/main_content/000812253.pdf)

図表 3-36 5Gセキュリティ検証環境の構築

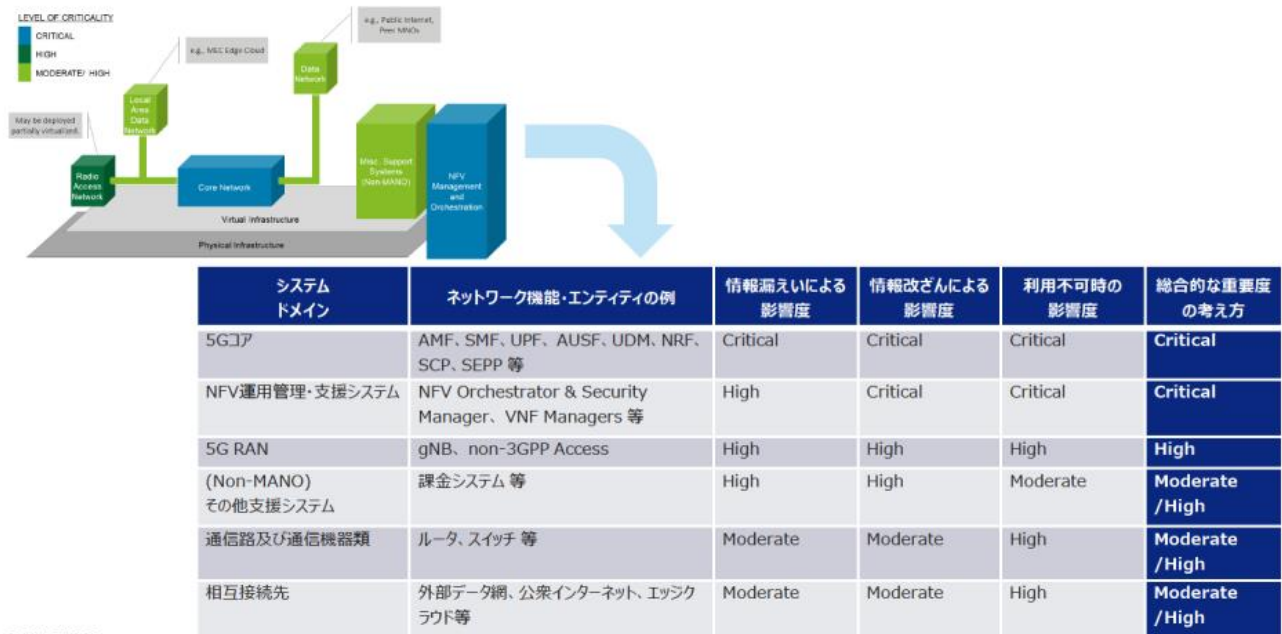


出典：総務省 サイバーセキュリティタスクフォース（第 37 回）配布資料

「資料 37-2-2 5G ネットワークにおけるセキュリティ確保に向けた調査・検討 及び 5G セキュリティガイドライン（第一版）について」 (https://www.soumu.go.jp/main_content/000812245.pdf)

セキュリティ分析結果をもとに、図表 3-36 に示す通り、仮想化技術と MEC を含めた包括的な検証環境の構築が行われ、検証が実施された。検証の結果として洗い出された想定されるセキュリティ課題を元に、ガイドラインの策定がなされた。ガイドライン策定にあたっては、情報漏洩、情報改ざん、利用不可時の3つの脅威シナリオにおける、システムドメインごとの重要度の整理がなされている(図表 3-37)。そのうえで、サイバーセキュリティの脅威分析モデルである「STRIDE-RM モデル」を用いて、図表 3-38 に示す 5G システムのすべての領域においてセキュリティの脅威が整理されている。

図表 3-37 脅威シナリオ検討と検証に基づく 5G システムドメインの重要度の整理



© 2022 KDDI

出典：総務省 サイバーセキュリティタスクフォース（第 37 回）配布資料

「資料 37-2-2 5G ネットワークにおけるセキュリティ確保に向けた調査・検討 及び 5G セキュリティガイドライン（第一版）について」 (https://www.soumu.go.jp/main_content/000812245.pdf)

図表 3-38 ガイドライン策定に向けた包括的な脅威分析の実施

| 脅威 | 脅威に対応したセキュリティ目的 |
|------------|-----------------|
| なりすまし | 認証 |
| 改ざん | 完全性の確保 |
| 否認 | 否認防止 |
| 情報漏えい | 機密性の確保 |
| サービスの拒否 | 可用性の確保 |
| 特権の昇格 | 適切な認可 |
| ラテラルムーブメント | ネットワークの分離 |

STRIDE-LMモデル

脅威分析の対象

- ・5Gシステム全般
- ・NFVインフラストラクチャとMANO
- ・NFVワークロード
- ・RAN
- ・コアネットワーク
- ・ネットワークスライス
- ・MEC

脅威アクターの分類

- 内部アクター：
 - 不注意な者 (Negligent Insiders) (N)
 - 内部犯行者 (Malicious Insiders) (M)
- 外部アクター：
 - サプライヤー・通信事業者 (S)
 - 取引先・契約者 (C)
 - その他の外部の者 (O) (ハッカー、組織的犯罪者等を含む)

出典：総務省 サイバーセキュリティタスクフォース（第 37 回）配布資料

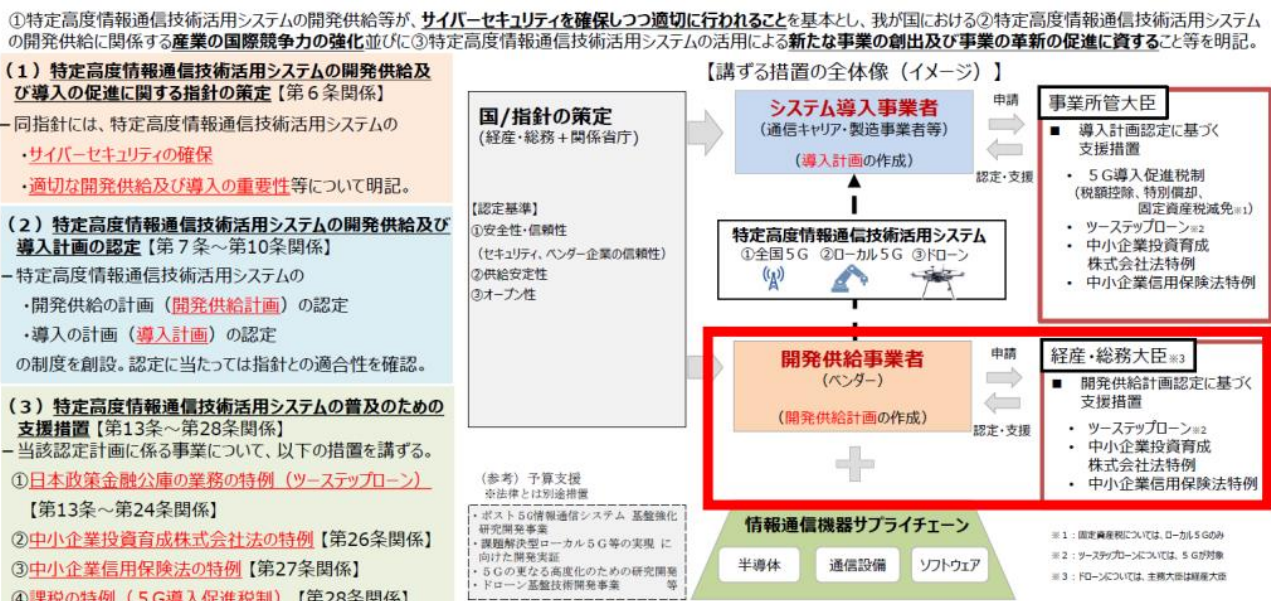
「資料 37-2-2 5G ネットワークにおけるセキュリティ確保に向けた調査・検討 及び 5G セキュリティガイドライン（第一版）について」 (https://www.soumu.go.jp/main_content/000812245.pdf)

また、2022年8月には、総務省のサイバーセキュリティタスクフォースより「ICT サイバーセキュリティ総合対策 2022」¹³⁸が公表されている。「情報通信ネットワークの安全性・信頼性の確保」、「サイバー攻撃への自律的な対処能力の向上」、「国際連携の推進」及び「普及啓発の推進」の4点を柱として、現状取り組んでいる施策と、今後取り組むべき施策について列挙しているが、そのうちの一つに、5Gのサプライチェーンリスク対策がある。サプライチェーンリスクへの対処として現状総務省主導で実施されている政策としては、先に述べた「5Gセキュリティガイドライン第1版」に公表およびそのための5Gネットワークに対する脅威や脆弱性等の技術的検証がある。

さらには、5Gのセキュリティ対策の促進のための政策的措置として、「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」(図表 3-39)に基づいた、サプライチェーン対策も行っている。この法案は、特定高度情報通信技術活用システムとして、主に5Gやドローンのサイバーセキュリティの確保を目的として2020年8月に施行が開始されており、5G等の開発供給計画の認定を受けた事業者やベンダーが、各種支援措置を受けられる制度となっている。開発供給計画の認定基準は、①安全性、信頼性、②供給安定性、③オープン性の3つについてであり、計画認定に基づいた設備の導入がなされた場合には、一定額の税額控除を受けられることができることとなっている¹³⁹。

図表 3-39 「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律」の概要

- 特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律（5G法）に基づき、開発供給計画の認定を受けた開発供給事業者（ベンダー）は、ツーステップローン等の支援を受けられることができる。



出典：総務省 総合通信基盤局 電波部電波政策課「事務局資料」

(https://www.soumu.go.jp/main_content/000857640.pdf)

¹³⁸ 総務省 サイバーセキュリティタスクフォース 「ICT サイバーセキュリティ総合対策 2022」(2022.8.12)

(https://www.soumu.go.jp/main_content/000829941.pdf)

¹³⁹ 経済産業省 「特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法」

(https://www.meti.go.jp/policy/mono_info_service/joho/laws/5g_drone.html) (2023.3.27 閲覧時点)

さらに、今後取り組むべき事項として、先に述べた「5G セキュリティガイドライン第1版」の普及を行うとしている。同ガイドライン策定にあたって情報通信研究機構（NICT）に構築されているセキュリティ検証環境（図表 3-36）について、今後も社会実装などにおいて活用がなされるべきであるとしている。

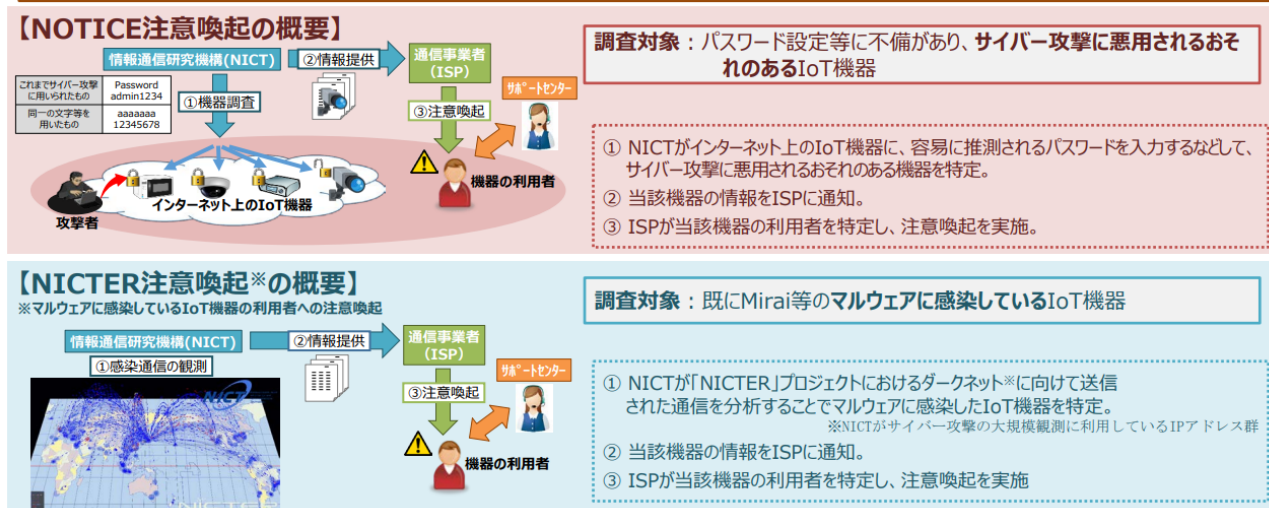
ガイドライン策定やサプライチェーンリスクへの対策に加えて、今後さらなる普及が予想される IoT におけるサイバーセキュリティの確保についても「NOTICE」プロジェクトを中心とした注意喚起が行われている。（図表 3-40）「NOTICE」プロジェクトにおいては、2019 年から NICT 主導で IoT 機器の調査が実施されており、電気通信事業者を通じた利用者への注意喚起が行われている。「NOTICE」の発足により、日本のインターネットに接続されている脆弱 IoT 機器の詳細や程度が明らかとなり、注意喚起のみならず、リスク評価の観点でも成果が見られている¹⁴⁰。また、「NOTICER」プロジェクトにおいては、既にマルウェア感染状態にある IoT 機器の特定を行い、通信事業者を通して注意喚起を行う仕組みとなっている。今後の取り組みについては、先述した「ICT サイバーセキュリティ総合対策 2022」において、「NOTICE」、「NOTICER」プロジェクトの継続のみならず、IoT 機器の設計、製造、販売段階において、製造事業者側がセキュリティ・バイ・デザインのコンセプトを十分に理解したうえで、脆弱性のある IoT 機器自体をそもそも増やさないための根源的な取組が必要であるとされている。また、IoT 機器の利用者側が、利用する機器を自主的に確認できるようなサポート体制についても言及されており、IoT 機器のセキュリティを考えるうえでは、インフラ事業者のみならず、製造者や利用者も含めた包括的なセキュリティ対策を行うべきであるとしている。

¹⁴⁰ 出典：総務省 サイバーセキュリティタスクフォース 情報通信ネットワークにおけるサイバーセキュリティ対策分科会（第1回）配布資料「資料1-4-1 NOTICEの現況」（2023.1.18）
(https://www.soumu.go.jp/main_content/000856811.pdf)

図表 3-40 「NOTICE」および「NOTICER」プロジェクトの概要

④IoT機器調査及び利用者への注意喚起

- ▶ 情報通信研究機構(NICT)がサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「NOTICE」を2019年2月より実施。
- ▶ NOTICEの取組に加え、マルウェアに感染しているIoT機器をNICTの「NOTICER」プロジェクト*で得られた情報を基に特定し、ISPから利用者へ注意喚起を行う取組を2019年6月より開始。



出典：総務省 関東総合通信局 令和3年度 関東サイバーセキュリティセミナー 配布資料「講演2 総務省のサイバーセキュリティ政策の最新動向」(2022.2.18) (https://www.telesa.or.jp/vc-files/kantou/telecomlec20220218_Hirose.pdf)

(3) データセンター

1) 経済安全保障におけるデータセンターの重要性

新型コロナウイルス感染症の世界的流行下で、データ利用量が急激に増加したことにより世界各国でデータセンターの増産が進められている。さらには、3. 1 「信頼性のある自由なデータ流通 (DFFT) に関する調査」においても述べた通りではあるが、国際的なデータガバナンスの不在のなかで、政府や自治体が保有する機密情報や個人情報を適切に管理することは経済安全保障上重要であると言える。過度なデータ保護やデータローカライゼーションといった政策は望ましくないが、機密情報や個人情報データを格納するデータセンターは国内設置が不可欠であるとの認識は、我が国においても高まっている¹⁴¹。

このような昨今の情勢においてデータセンターは経済安全保障の観点において大変重要なデジタルインフラとなっている。データセンターは、図表 3-34 に示す通り、データを蓄積し、処理する機能を果たしており、先に述べた海底ケーブル、5G 同様に、インターネット通信やクラウドサービスなどの様々な産業および社会生活の基盤となっており、我が国の戦略的自律性を保つうえで欠かすことのできない基

¹⁴¹ 総務省 経済産業省 デジタルインフラ (DC等) 整備に関する有識者会合 (第3回) 「デジタルインフラ (DC等) 整備に関する有識者会合中間とりまとめ (概要)」(2021/12/13) (https://www.soumu.go.jp/main_content/000787667.pdf)

幹インフラの一つである。さらには、各国が我が国にデータセンターの設置を行うことにより、データによる相互依存が高まり、我が国がアジアにおけるデータセンターのハブとなるという戦略的不可欠性・優位性の観点での重要性もある。

2) データセンターの安定的な稼働を維持するうえでの課題と講じるべき対策

データセンターが我が国の重要なデジタルインフラとして安定的に稼働供給を続けるうえで考慮すべき課題およびリスクとしては、データセンターの建物自体への物理的損傷・損壊により、データセンターが機能停止してしまうことがある。さらには、データセンターへのサイバー攻撃も新たな脅威として認識されている。以下ではそれぞれの課題および対策について、経済安全保障の観点から整理を行う。

(ア) 物理的な破壊によるデータセンターの機能停止と対策

データセンターの安定稼働に対するリスクの一つには、データセンターの建物自体の物理的な破壊による機能停止が考えられる。物理的な破壊の原因については、大規模災害やテロ等を中心とした議論が進められているが、加えて、他国からの攻撃も考慮すべきリスクとされている。

ロシアによるウクライナ侵攻において、ロシアがウクライナ政府のデータセンターを狙って巡行ミサイル攻撃を行った。この件を受けて、各国はデータセンターへの物理的な破壊工作について改めて危機感を示し、SWIFT（国際銀行間通信協会）が所有するスイスのサーバセンターが、武装した警備隊を配置するなどの対策も見られた¹⁴²。また、ウクライナ侵攻におけるデータセンターへの物理的攻撃が現実のものとなったことを踏まえて、英国サイバーセキュリティセンター（NCSC）による新たなガイダンスには「データセンター事業者は、物理的な通信経路を分離しているか確認するべきだ。また、電力供給や非常用電源を複数用意し、物理的な攻撃や妨害行為から建物が保護されていることを検証してほしい。」との一文も盛り込まれており、特に欧州を中心として各国はデータセンターへの物理的な攻撃への対策を行っている¹⁴³。

我が国においては、データセンターの首都圏一極集中が、データセンターの物理的な破壊を未然に防ぐうえでの大きな障壁となっている。現在、我が国のデータセンターの立地の約 6 割が首都圏に集中しているが、大規模災害が首都圏一体に発生した場合には、全国でネットサービスが利用できなくなる恐れがある¹⁴⁴。また、テロや他国からの攻撃といった恣意的かつ人為的な物理破壊においては、攻撃を行う側にとってはデータセンターが一極集中していることで一箇所を集中的に狙うことが容易となる。

データセンターが首都圏に集中している背景には、少数の独占企業によって通信事業が運営されてい

¹⁴² 「How the war in Ukraine could impact data centers」(S&P Global Market Intelligence, 2022.4.12)

(<https://www.spglobal.com/marketintelligence/en/news-insights/research/how-the-war-in-ukraine-could-impact-data-centers>)

¹⁴³ 「今すぐ見直すべきデータセンターのセキュリティ」(Canon サイバーセキュリティ情報局, 2022.6.8) (https://eset-info.canon-its.jp/malware_info/special/detail/220608.html)

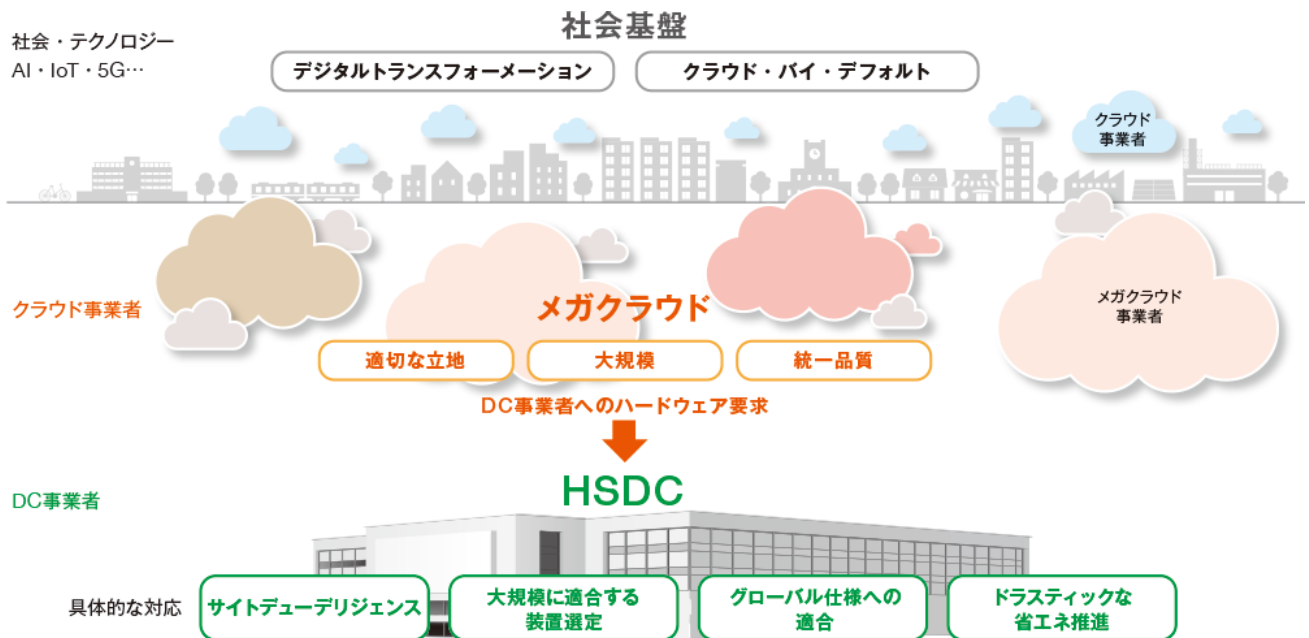
¹⁴⁴ 「本格稼働を始める経済安全保障政策」(野村総合研究所, 2021.12.1)

(<https://www.nri.com/jp/knowledge/blog/lst/2021/fis/kiuchi/1201>)

たという歴史もある¹⁴⁵。さらには、データの最大需要地である東京から近い位置にデータセンターを建設することで、通信の遅延時間が短くなり、サービスの質の向上につながるうえ、運用・保守の観点でも、メンテナンス要員がアクセスしやすい立地が望ましいなど、事業者側としても首都圏という立地は大きなメリットをもたらしてきた。

さらに、データセンターのなかでも昨今需要が高まっているハイパースケールデータセンター（以下、HSDC）も首都圏一極集中の原因であると言える。HSDC は膨大なデータ処理とストレージを必要とする事業者向けに建設する大規模なデータセンターのことをいい、特にメガクラウドとも呼ばれるグローバルにクラウドサービスを提供する事業者が必要としている（図表 3-41）。自社内で IT システムを保有する、いわゆるオンプレミスでの運用を行う企業が減少し、クラウドサービスへの需要が高まっていること、5G、AI、IoT 市場の拡大に対応するための施設であり、今後もさらなる需要が見込まれている¹⁴⁶。

図表 3-41 メガクラウドと HSDC の概念図



出典：「ハイパースケールデータセンターのファシリティトレンド」

(NTT ファシリティーズジャーナル 334 号, 2020.8,21) (<https://www.ntt-f.co.jp/ntt-fjd/feature/0032/>)

HSDC は、用地選定の際に IX（インターネットエクスチェンジ）からの距離が重視されており、首都圏では東京都の大手町、関西圏では大阪府の堂島にある主要 IX から 35km 圏内に設置することを念頭に置いて整備が進められたため、地方は立地としては検討の範囲外とされていた¹⁴⁷。また、クラウドやデー

¹⁴⁵ 「データセンターの地政学 立地はどこに向かうのか」（日本経済新聞, 2021.2.24）

(<https://www.nikkei.com/article/DGXZQOGH204530Q1A220C2000000/>)

¹⁴⁶ 「ハイパースケールデータセンターとは？【特集】」（Data Center Café, 2022.9.23）([https://cafe-](https://cafe-dc.com/special/what-is-a-hyperscale-data-center/)

[dc.com/special/what-is-a-hyperscale-data-center/](https://cafe-dc.com/special/what-is-a-hyperscale-data-center/))

¹⁴⁷ 総務省 デジタルインフラ（DC 等）整備に関する有識者会合（第 4 回）配布資料「資料 3 デジタルインフラ（DC 等）整備に関する有識者会合（第 4 回事務局説明資料）」（2023.3.3）

データセンターを専門的に扱う Structure Research 社のリサーチ責任者を務めるジャベス・タンは、HSDC が日本の首都圏において需要が大きいことについて、「GDP で世界第 3 位の大国である日本の市場規模が大きいこと、国内にハイパースケールクラウドのプラットフォームがなく、米国や中国のハイパースケールクラウドプロバイダーとの間で理想的な競争環境を提供していること、米国西海岸からアジア太平洋地域に向けて敷設されている海底ケーブルの主要な接続拠点であることなど、いくつかの重要な要因が集約されていることによるもの」¹⁴⁸と述べている。

データセンターの首都圏一極集中には様々な背景があるなかで、データセンターが一箇所に集中している現状では共倒れとなってしまうことが予想され、いわゆるデジタル経済安全保障を考えるうえではデータセンターは複数の地域に分散している方がいいとされる。現在、総務省主導でのデータセンターの地方拠点の整備が進められており、10 数か所の地方拠点を 5 年程度で整備するとの整備方針が固められた。令和 3 年度補正予算による「データセンター、海底ケーブル等の地方分散によるデジタルインフラ強靱化事業」によって、データセンターをはじめ、海底ケーブル、インターネットエクスチェンジ (IX) 等のデジタルインフラの地方立地を支援する事業が推進されている。事業の一環として設置された「デジタルインフラ整備基金（特定電気通信施設等整備推進基金）」を財源とし、デジタルインフラ整備を行う民間事業者等への助成に向けた公募および採択が 2022 年 6 月に実施された¹⁴⁹。

また、総務省と経済産業省が共同で行う事業としては、図表 3-42 に示す「データセンターの地方拠点整備」がある。主に、データセンターを運用するうえで必要不可欠な電力供給および通信回線の引き込みを行う「電力・通信インフラ整備支援」と、データセンター建設にあたって必要な土地造成の費用を支援する「地域拠点用地整備」の 2 本の柱をもとに、首都圏一極集中からの脱却が進められている。

(https://www.soumu.go.jp/main_content/000866263.pdf)

¹⁴⁸ 「プリンストン・デジタル・グループ、東京で 100MW のハイパースケールデータセンターキャンパスを建設する計画を発表」(日本経済新聞, 2021.6.29) (https://www.nikkei.com/article/DGXLRSP613438_Z20C21A6000000/)





¹⁴⁹ 総務省 デジタルインフラ (DC 等) 整備に関する有識者会合 (第 4 回) 配布資料「資料 3 デジタルインフラ (DC 等) 整備に関する有識者会合 (第 4 回事務局説明資料)」(2023.3.3)

(https://www.soumu.go.jp/main_content/000866263.pdf)

図表 3-42 データセンターの地方拠点整備

データセンターの地方拠点整備

令和3年度補正予算額 **71.0億円** (+令和4年度以降4年間で総額455億円を国庫債務負担行為により支出)

| 事業の内容 | 事業イメージ |
|--|--|
| <p>事業目的・概要</p> <ul style="list-style-type: none"> ● データセンター（以下、DC）は、様々な社会課題解決に資する新たなデジタルサービスの提供を支えるとともに、企業等の営業秘密や個人情報が集積され、安全保障の観点からも重要なデジタルインフラです。 ● 一方で、国内DCの6割は東京圏に集中しています。レジリエンスの強化や再生可能エネルギー活用といった課題解決に加え、2020年代後半に普及が見込まれるポスト5Gにより展開される自動運転や遠隔医療・遠隔教育などのサービスの実現には、トラフィックの地方分散を通じた低遅延性の確保も不可欠です。 ● このため、DCの民間需要動向を見極めつつ、我が国全体でのDC最適配置（新規拠点整備）を後押しします。 <p>成果目標</p> <ul style="list-style-type: none"> ● 本事業では、特にDC新規拠点の地方設置の際に障害となる電力・通信インフラ整備等を通じ、東京圏以外におけるDC拠点の新規整備（複数件）を目指します。 <p>条件（対象者、対象行為、補助率等）</p> <div style="display: flex; align-items: center; gap: 10px;"> <div style="background-color: #0070C0; color: white; padding: 5px;">国</div> <div style="font-size: 2em;">→</div> <div style="border: 1px solid #0070C0; padding: 5px;">補助 (1/2)</div> <div style="font-size: 2em;">→</div> <div style="background-color: #0070C0; color: white; padding: 5px;">民間企業等</div> </div> | <p>（1）電力・通信インフラ整備支援</p> <ul style="list-style-type: none"> ● 複数のDCが集積する中核DC拠点の設置にあたり、電力供給や通信回線の引込等を行うためのインフラ（共同溝等）の整備費用の一部を支援。 <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p><共同溝イメージ></p>  </div> <div style="text-align: center;"> <p><共同溝例></p>  </div> </div> <p>（2）地域拠点用地整備</p> <ul style="list-style-type: none"> ● 複数のDCが集積する中核DC拠点の設置にあたり、土地造成のための費用を支援。 <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p><中核DC拠点イメージ></p>  </div> <div style="text-align: center;"> <p><DC拠点例（印西大和ハウス）></p>  </div> </div> |

出典：経済産業省・総務省 デジタルインフラ（DC等）整備に関する有識者会合「デジタルインフラ（DC等）整備に関する有識者会合中間とりまとめ（概要）」（2022.1.17）

https://www.soumu.go.jp/main_content/000787667.pdf

（イ）サイバー攻撃によるデータセンターの機能停止と対策

データセンターは、物理的な攻撃に対するセキュリティのみならず、サイバー攻撃への対策も講じる必要がある。ロシアによるウクライナ侵攻においては、マルウェアやDDoS攻撃といったかたちでのサイバー攻撃が国営銀行や政府機関、その他ウクライナの組織を標的にして行われている。重要なファイルを破壊する目的で作成されたマルウェアは、侵入経路は不明であるが、数カ月かけて計画されていたものとみられている。ウクライナ侵攻前の2017年には、同じくウクライナを標的としたサイバー攻撃として、国外のデータセンターにも連鎖的な被害が生じており、ランサムウェアに見せかけて、標的としたコンピューターのマスターブートレコードとよばれる、コンピューターの起動に必要なプログラムや情報を記録したハードディスク内の領域を破壊することで、再起動を不可能とするタイプの攻撃も見られるなど、様々な形態のサイバー攻撃が確認されている¹⁵⁰。

サイバー攻撃を未然に防ごうと、他の基幹インフラと同様、サプライチェーンの脆弱性が課題とな

¹⁵⁰ 「今すぐ見直すべきデータセンターのセキュリティ」（Canon サイバーセキュリティ情報局, 2022.6.8）https://eset-info.canon-its.jp/malware_info/special/detail/220608.html

っている。あらかじめ悪質なマルウェアが組み込まれた設備を調達してしまうことにより、サイバー攻撃に利用されるなどのケースがあり、攻撃者がプロバイダーのセキュリティを侵害し、それを足がかりにして、プロバイダーの顧客のネットワークへのアクセスを獲得しようとする可能性も指摘されている¹⁵¹。

データセンターのサプライチェーン管理については、データセンターを運営する民間事業者においても対策が講じられている。Microsoft 社はサプライチェーンのセキュリティ保護対策として、設備を供給するサプライヤーに対して、変更や改ざんのリスクを軽減するため、輸送時に厳格な保管チェーン手順を設け、監視プロセスに組み込んでいるほか、機器のメンテナンス、インベントリ（在庫管理）、ソフトウェア設備の保有期間などについて対策が講じられている¹⁵²。また、セキュリティの国際的なコンプライアンス標準である「ISO」、「HIPAA」「FedRAMP」、「SOC」や、オーストラリアの IRAP、英国の G-Cloud、シンガポールの MTCS のような各国固有の標準などに適合しているかどうかについて、厳格な第三者監視が行われている¹⁵³。

データセンターのサイバー攻撃対策においては、クラウドサービスへの対策についても考慮する必要がある。2021年9月には、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」が総務省より公表されており、2018年に公表された第2版を比較すると、サプライチェーンの観点盛り込まれている。クラウドサービスは、「IaaS(Infrastructure as a Service)」(インフラ機能を提供するサービス)、「PaaS (Platform as a Service)」(プラットフォームを提供するサービス)、「SaaS (Software as a Service)」(ソフトウェアを提供するサービス)といったかたちで、サプライチェーンの複雑性が特徴となっている。そのため、クラウドサービスの情報セキュリティ対策のレベルを上げるには、サプライチェーンを構成する各事業者の責任範囲を明確にした上で、各事業者それぞれのサービスにおいてセキュリティ対策を講じているかを管理する必要があるとしている¹⁵⁴。

データセンターは、社会インフラとしての重要性を考慮しつつも、基本的には事業者のビジネスとして運営されるべき施設であり、政府はあくまで、民間の経営判断として、採算の見通しが立ちづらい部分に対するサポートを行うべきとの方針が打ち出されている。(図表 3-43) これは、経済安全保障を考えると重要な観点であり、すなわち、経済の自由を最優先としつつ、安全保障を担保する上では、官民連携でのセキュリティ対策を推進することが望ましいとされている。

¹⁵¹ 「データセンターもハッカーの標的となる恐れ--セキュリティを強化するには」(ZDNet, 2022.3.24)

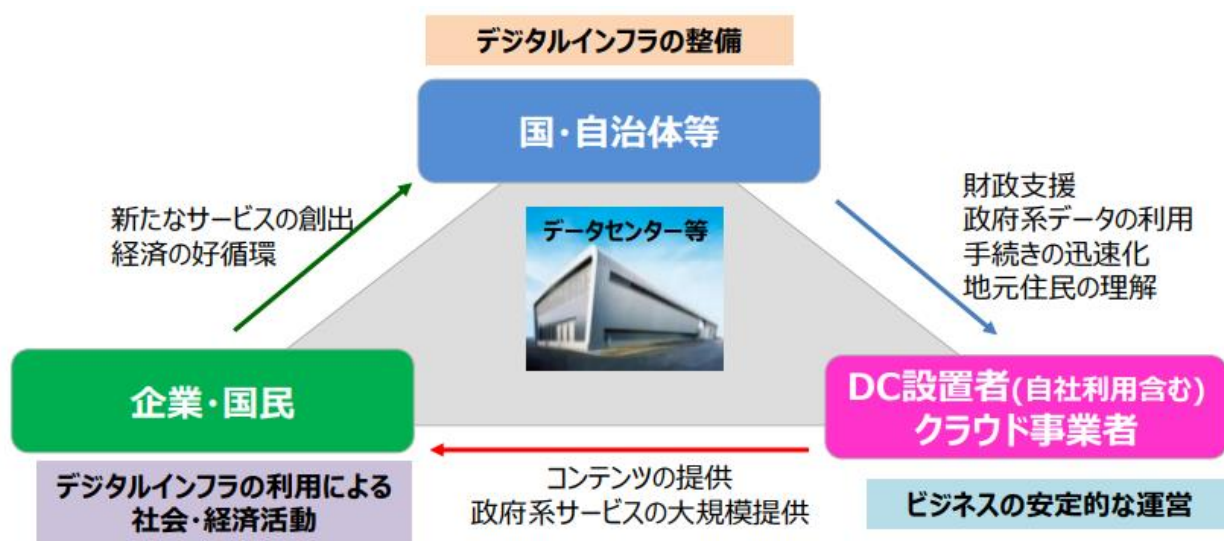
(<https://japan.zdnet.com/article/35185111/p/2/>)

¹⁵² 「データセンターの資産管理」(Microsoft, 2023.3.7) (<https://learn.microsoft.com/ja-jp/compliance/assurance/assurance-datacenter-asset-management>)

¹⁵³ 「データセンターのセキュリティの概要」(2023.3.17) (<https://learn.microsoft.com/ja-jp/compliance/assurance/assurance-datacenter-security>)

¹⁵⁴ 総務省「別紙2 クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」(2021.9.30) (https://www.soumu.go.jp/main_content/000771515.pdf)

図表 3-43 デジタルインフラ整備に当たっての官民等の役割



出典：総務省 経済産業省 デジタルインフラ（DC等）整備に関する有識者会合（第3回）
「デジタルインフラ（DC等）整備に関する有識者会合中間とりまとめ（概要）」（2021/12/13）
(https://www.soumu.go.jp/main_content/000787667.pdf)

4. 参考文献一覧

| 著者等 | 発行/発行年 | タイトル | 出版社/掲載誌 |
|-----------|--------|--|---------|
| デジタル庁 | 2021 | 包括的データ戦略 | |
| 総務省 | 2017 | G7 ICT AND INDUSTRY MINISTERS' DECLARATION | |
| 総務省 | 2018 | 平成 30 年度版 情報通信白書 | |
| 総務省 | 2022 | 5G セキュリティガイドライン第1版 | |
| 総務省 | 2022 | ICT サイバーセキュリティ総合対策 2022 | |
| 総務省 | 2021 | クラウドサービス提供における情報セキュリティ対策ガイドライン (第3版) | |
| 総務省 経済産業省 | 2022 | デジタルインフラ (DC 等) 整備に関する有識者会合中間とりまとめ | |
| 経済産業省 | 2020 | 特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法 | |
| 経済産業省 | 2022 | データの越境移転に関する研究会報告書 | |
| 外務省 | 2021 | 令和3年版 外交青書・白書 | |
| 外務省 | 2020 | 地域的な包括的経済連携(RCEP)協定 | |
| 外務省 | 2017 | G20 ハンブルク首脳宣言 | |
| 内閣官房 | | 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 | |

| 著者等 | 発行/発行年 | タイトル | 出版社/掲載誌 |
|-------------------------------|--------|---|----------|
| 内閣府 | 2020 | 統合イノベーション戦略 2020 | |
| 内閣府 | 2021 | 統合イノベーション戦略 2021 | |
| 一般社団法人情報通信技術委員会 (TTC) | 2022 | 情報通信分野における標準化活動のための標準化教育テキスト | |
| 世界経済フォーラム | 2020 | グローバル・サイバースペースでの信頼を構築するための行動計画 | |
| 石本茂彦、松尾剛行、森脇章、岡野寿彦、小野寺良文、角本和理 | 2022 | 中国のデジタル戦略と法 中国情報法の現在地とデジタル社会のゆくえ | 弘文堂 |
| 平井宏治 | 2022 | 経済安全保障のジレンマ 米中対立で迫られる日本企業の決断 | 育鵬社 |
| 宮本雄二、伊集院敦、他 | 2021 | 米中分断の虚実 デカップリングとサプライチェーンの政治経済分析 | 日本経済新聞出版 |
| 土屋大洋 | 2020 | サイバークレートゲーム | 千倉書房 |
| Access Now | 2023 | Weapons of control, shields of impunity: Internet shutdowns in 2022 | |
| Access Now | 2022 | THE RETURN OF DIGITAL AUTHORITARIANISM Internet shutdowns in 2021 | |
| Internet Society | 2022 | Action Plan 2023 Our Internet, Our Future: Protecting the Internet for Today and Tomorrow | |