公共政策ワークショップ　Ⅰ
最終報告書

プロジェクトＣ

我が国の経済安全保障の確保に向けた研究

令和４（2022）年度

目次

はじめに

「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（令和 4 年法律第 43 号。以下「経済安全保障推進法」という。）が 2022 年 5 月 11 日に成立し、同月 18 日に公布された。経済安全保障推進法ではその目的を第 1 条において「国際情勢の複雑化、社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み、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基本的な方針を策定するとともに、安全保障の確保に関する経済施策として、特定重要物資の安定的な供給の確保及び特定社会基盤役務の安定的な提供の確保に関する制度並びに特定重要技術の開発支援及び特許出願の非公開に関する制度を創設することにより、安全保障の確保に関する経済施策を総合的かつ効果的に推進すること」と規定したところである。これにより我が国は法律という形で経済安全保障施策を積極的に推進していくことを内外に示すに至った。

また、国家安全保障に関する基本方針である「国家安全保障戦略」（令和 4 年 12 月 16 日国家安全保障会議決定及び閣議決定）が策定された。当戦略では、我が国の国益の一つとして「経済的な繁栄を主体的に達成しつつ、開かれ安定した国際経済秩序を維持・強化し、我が国と他国が共存共栄できる国際的な環境を実現する[1]」が掲げられ、これを達成するための戦略的アプローチの一つとして「自主的な経済的繁栄を実現するための経済安全保障政策の促進」が示され、サプライチェーンの強靭化や重要インフラのサイバーセキュリティ、データ・情報保護、先端重要技術の開発・育成などに取り組むこととされた[2]。これにより、経済安全保障が我が国の安全保障において重要な位置を占めることが改めて示された。

これら我が国における経済安全保障についての取組が急速に進んだ背景には、国際社会の歴史的変化と地政学的競争の激化に伴い、自由で開かれた安定的な国際秩序が重大な挑戦に晒されていること[3]、また、国家安全保障の対象が経済・技術等、これまで非軍事的とされてきた分野にまで拡大し、軍事と非軍事の分野の境目が曖昧になっていること[4]、さらに、感染症危機といった緊急時において各国が必要な物資を自国民に優先的に用いることで、我が国が対外的に依存していた物資が不足する事態が発生し、供給体制の脆弱性が露呈したこと[5]等があげられる。我が国は戦後最も厳しく複雑な安全保障環境のただ中にあると現下の情勢を認識しており、そうした情勢においても我が国の平和と安全、繁栄、国民の安全、国際社会との共存共栄を主な内容とする我が国の国益を守るために必要な施策として、

---

[1] 内閣官房、「国家安全保障戦略」、2022 年 12 月 16 日、5 頁。
［https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf］、（2023 年 1 月 17 日閲覧）。
[2] 同上、26-27 頁。（2023 年 1 月 17 日閲覧）。
[3] 同上、3 頁。（2023 年 1 月 17 日閲覧）。
[4] 同上、4 頁。（2023 年 1 月 17 日閲覧）。
[5] 経済産業省、「通商白書 2020」、2021 年 7 月、220-231 頁。
［https://www.meti.go.jp/report/tsuhaku2020/pdf/02-01-05.pdf］、（2023 年 1 月 26 日閲覧）。

経済安全保障の概念が注目されたと考えられる[6]。

そこで本報告書は、経済安全保障に関する現状と課題を検討するとともに、我が国の経済安全保障の確保に資する政策を検討したものである。本研究は、東北大学公共政策大学院「公共政策ワークショップⅠ」の国際プロジェクトとして行われ、本報告書はその研究結果を取りまとめたものである。「公共政策ワークショップⅠ」は、現実の政策課題について自ら調査し、解決策を立案することを目的として開講されている授業科目であり、学生が主体的にグループワークを行うこととなっている。今年度のプロジェクトCにおいても、8名の学生が現状分析のための調査や政策提言に向けた議論を重ねてきた。

本研究では主に文献調査及びヒアリング調査を実施した。特にヒアリング調査に関しては、①日本政府関係者、②企業関係者、③研究者・有識者、④外国政府関係者の4つの軸で行った。①日本政府関係者に関しては、経済安全保障施策の中心である内閣官房国家安全保障局経済班をはじめ、霞が関での現地調査も実施し、計25か所に対してヒアリング調査を実施した。②企業関係者に関しては、電気通信事業会社やセキュリティ関連会社、独立行政法人エネルギー・金属鉱物資源機構(Japan Organization for Metals and Energy Security。以下「JOGMEC」という。)、日本経済新聞社等の、経済安全保障に深く関係する企業・団体計11か所に対してヒアリング調査を実施した。③研究者・有識者に関しては、衆議院議員の甘利明氏（自由民主党前幹事長）及び大野敬太郎氏（現自由民主党副幹事長）、北村エコノミックセキュリティ合同会社代表の北村滋氏（元国家安全保障局長）、同志社大学法学部教授の兼原信克氏（元国家安全保障局次長）、本学教授の遠藤哲郎氏（現国際集積エレクトロニクス研究開発センター所長）等の、経済安全保障に精通した計13名の方々に対してヒアリング調査を実施した。④については、新型コロナウイルスの影響により中止となっていた海外研修が再開し、豪州へ訪問した。現地において、外務貿易省や内務省、政府系シンクタンクのASPI（Australian Strategic Policy Institute。以下「ASPI」という。）、シドニー大学 United States Studies Centre のCEOであるマイケル・グリーン氏等計11か所にヒアリング調査を行った。経済安全保障はその対象とする施策の幅が広く、結果として私たちは今までに実施されたワークショップの中で最も多い計60か所へのヒアリング調査を実施することができ、これらの方々に報告書の作成に当たっても様々な支援を受け、官民における施策の第一人者の方々の大変に貴重な時間をいただいたこと、心より感謝を申し上げる。本報告書はその時間をいただいたことに見合うものになるよう学生一同で約一年間をかけて作成したものである。

なお、ヒアリング調査で得られた貴重な資料等については、付属資料として本報告書の最後に掲載されており、我々が必ずしも掘り下げられなかった内容も記載されているためご覧いただけると幸いである（もっとも、ヒアリング調査先の名称や調査報告書の非公開が求められている場合もあるため、60 か所全ての報告書が掲載されていないことについてはご理解いただきたい）。

[6] 内閣官房、「国家安全保障戦略」、4頁。（2023年1月17日閲覧）。

本報告書は、「第1部　問題の所在」及び「第2部　政策提言」の2部構成である。第1部では、第 1 章で本研究の背景及び目的を説明し、第 2 章では海外での経済安全保障施策を述べ、第3章では我が国の経済安全保障施策について時系列ごとに概観する。

第 2 部は、第 1 章でサプライチェーン分野における国際連携の強靭化及びジスプロシウム・半導体の安定供給に資する政策提言を行い、第2章でサイバーセキュリティ分野において、サイバー攻撃に対する防御力の向上や中小企業でのセキュリティ強化、人材育成に資する政策提言を行い、第 3 章で経済インテリジェンス分野における産官学の連携強化や情報共有体制の構築、人材育成に資する政策提言を行う。

以上のような観点から、国家安全保障局経済班を中心とした政府機関等への政策提言を行うことが本報告書の目的である。

2023 年 1 月

第１部　問題の所在
第１章　研究の背景・目的
第１節　我が国の安全保障をめぐる背景

我が国は時代を画する変化に直面している。冷戦終結以降、国際社会は共存共栄の国際秩序と自由貿易体制の下、各国の相互依存が進んだ。我が国を含む先進的民主主義国家は、自由、民主主義、基本的人権の尊重、法の支配といった普遍的価値を擁護し、共存共栄の国際社会の形成を主導してきた[7]。これにより、世界は経済成長と社会の発展という利益を享受してきた[8]。

しかし、近年、そのような経済相互依存関係を築いていたにも関わらず、中国、ロシアという普遍的価値を共有しない一部の国家が、独自の歴史観・価値観に基づき、既存の国際秩序の修正を図ろうとする動きを見せている(表 1)。

表 1　近年の既存の国際秩序の修正を図ろうとする動き
出典：筆者作成

2014 年 3 月	ロシアによるクリミア自治共和国及びセヴァストーポリ特別市の「併合」
2016 年 7 月	中国、国連海洋法条約附属書 VII 仲裁裁判所の南シナ海に関する仲裁判断を認めない声明を出す。
2022 年 2 月	ロシアによるウクライナへの軍事行動

特に近年では、経済分野と安全保障が密接に関わるようになった。そのために、世界各国が経済相互依存関係を武器に他国に圧力をかける事態が起きている（表 2）ことは、その証左であり、我が国の健全な経済成長を脅かす要因となっている。

[7] 内閣官房、「国家安全保障戦略」、3 頁。（2023 年 1 月 24 日閲覧）。
[8] この国際秩序と自由貿易体制に、冷戦時代にイデオロギー的に敵対した旧共産圏も加わったことを、民主主義や自由市場経済の勝利と称した有識者が一定数存在した。例えば、国際政治学者のフランシス・フクヤマ氏は著書『歴史の終わり』で、「歴史の根底をなす諸原理や諸制度はもはや進歩も発展もなくなる」と著述し、元米大統領のジョージ・H・W・ブッシュ氏は「ジャングルの掟」から「法の支配」が取って代わると発言した。フランシス・フクヤマ『歴史の終わり』、三笠書房、1992 年、15 頁；北岡伸一・細谷雄一『新しい地政学』、東洋経済新報社、2020 年、46 頁。

表 2　経済分野における他国への圧力行動

出典：筆者作成

2010 年 9 月	尖閣諸島漁船衝突事故を契機に中国による日本へのレアアース輸出制限措置
2012 年 10 月	中国の人権活動家の劉暁波氏に対するノーベル平和賞授与を契機に、中国がノルウェー産サーモンの検疫を強化し、事実上輸入を制限。ノルウェー産サーモンの中国シェアは 92%から 29%に。
2017 年 3 月	中国、韓国での THAAD 配備決定に反発し、韓国企業への一方的な措置
2022 年 11 月	リトアニアに「台湾代表処」が開設される。中国はリトアニア産品やリトアニアと関係のある EU 産品を差別的に取り扱ったため、EU は WTO 紛争解決手続き開始。
2022 年 11 月	モルドバが EU と「深化した包括的自由貿易協定」を締結したことを契機に、ロシアが、輸出する天然ガスを値上げするとともに一部供給を停止。

そして、立案に大きく携わった政治家[9]、有識者[10]の指摘通り、近年の技術覇権をめぐる競争やデジタル化といった将来の社会変革等、経済安全保障分野の課題は山積している。ゆえに、このような社会動向を踏まえた経済安全保障施策がますます必要とされる。

第 2 節　研究の射程・目的

我々は、調査を重ねる中で、以下 3 点の社会動向に注目した。

・地政学的リスクの増大

ロシアによるウクライナ侵略により、権威主義的国家と自由民主主義的国家との間における世界経済の分断やブロック化・多極化の動きがこれまで以上に加速している[11]。

このような地政学的リスクは、マクロ経済学の分野で、不確実性の動向を定量的に把握す

[9] 自由民主党衆議院議員甘利明氏に対するヒアリング調査（2022 年 9 月 26 日実施）；自由民主党衆議院議員大野敬太郎氏に対するヒアリング調査（2022 年 11 月 21 日実施）。

[10]北村滋『経済安全保障　異形の大国、中国を直視せよ』、中央公論新社、2022 年、102-105 頁；同志社大学法学部教授元国家安全保障局次長兼原信克氏に対するヒアリング調査（2022 年 8 月 26 日実施）；慶應義塾大学土屋大洋教授に対するヒアリング調査（2022 年 10 月 4 日実施）；東京大学先端科学技術研究センター特任講師井形彬氏に対するヒアリング調査（2022 年 10 月 13 日実施）。

[11] 経済産業省、「通商白書 2022」、224 頁。（2023 年 1 月 25 日閲覧）。

る代表的な 4 つの不確実指数[12]に反映されている[13]。そのほかにも、下図の地政学リスク指数(geopolitical risk index)は、ウクライナ侵略が始まった 2022 年が米同時多発テロとイラク戦争以来の高い数字を出している。

図 1　地政学リスク指数(geopolitical risk index)
出典：通商白書 2022

この動きと同時に、資源ナショナリズムの高まりと特定国に物資を依存するリスクの顕在化が生じている。資源ナショナリズムとは、自国に存在する資源を自国で管理・開発しようという動きで、近年では、下図のように、発展途上国だけでなく、チリといった先進諸国でも見られる[14]。

12 「マクロ経済不確実性指数」、「エコノミック・サプライズ指数」、「株式ボラティリティ指数」、「経済政策不確実性指数」の 4 つ。篠原武史、奥田達志、中島上智、「マクロ経済に関する不確実性指標の特性について」、2020 年 10 月、1 頁。
[https://www.boj.or.jp/research/wps_rev/wps_2020/data/wp20j07.pdf]、（2023 年 1 月 20 日閲覧）。

13 経済産業省、「通商白書 2022」、224-226 頁。（2023 年 1 月 24 日閲覧）。

14 西山孝『資源論』、丸善出版、2016 年、157 頁。

国・地域	産業政策支援の主な動向
コンゴ民主共和国	・2018 年に改正鉱山法が可決・公布され、戦略的鉱物資源に対するロイヤリティ引上げ等が盛り込まれた（コバルトは 10%）。
ザンビア	・2012 年以降、銅とコバルトに加え、亜鉛等の鉱石にも 10%の輸出税を賦課。2012 年に付加価値税の還付を廃止。 ・2016 年に銅価格に応じた新たなロイヤリティ制度を閣議決定。
マダガスカル	・2019 年に新大統領が就任し、「既存の大規模鉱山法は企業に有利な条件となっており、国が 30%の株式を持つか、ロイヤリティを引き上げるべき」と発言。
南アフリカ	・2017 年黒人企業（BEE）による採掘権 30%保有やローカルコンテンツ要求等が盛り込まれた改正鉱業憲章が発表。 ・18 年パブリックコメントを経て、高付加価値化（Beneficiation）義務や、BEE への 26%の資本譲渡義務を内容とする改正鉱業法案が閣議決定。
フィリピン	・2017 年新規鉱業ライセンスの発給を停止する大統領が発令。 ・2018 年新規露天掘り鉱山の開発を禁止する大統領令が発令。 ・2018 年鉱業法改正案が下院委員会で承認。鉱石輸出に対し 20%以上の高関税を賦課。実質的な輸出禁止に近い内容。現在も審議中。
インドネシア	・09 年に鉱業法を改正。尼企業等への 51%の資本譲渡を義務付け。 ・14 年高付加価値化義務により、事実上の鉱石等の輸出禁止。
メキシコ	・リチウムを国のエネルギー転換のための重要な鉱物資源と特定し、リチウム開発に際し、外国企業排除の姿勢を強め、国が開発を独占するべく、電力国有化と併せて憲法改正に向けた動きが見られる。
チリ	・環境委員会にて、鉱業民間企業の国有化が一般承認され、現在、制憲議会本会議での審議待ち。また、新鉱業ロイヤリティ法案（ハイブリッド方式＜年間売上高に対する課税と収益に基づく限界及び累進か成立＞の採用）について、上院の委員会で修正案を承認。 ・ボリッチ大統領（2022 年 3 月誕生）は、大統領選を通じて、戦略的国家資源であるリチウムにかかる産業を発展させるために、生産に付加価値をつけることができる国家リチウム会社の設立を推進することを発表。

資料：資源エネルギー庁「2050 年カーボンニュートラル社会実現に向けた鉱物資源政策」を基に作成。

図 2　重要鉱物保有国における資源ナショナリズムの高揚

出典：経済産業省

さらに、気候変動・環境問題の意識の高まりで、各国は EV や再生可能エネルギーの導入を目指しているが、これらの部品や原材料の希少金属を我が国は特定国に依存しており[15]、地政学的リスクの増大により、その安定供給が脅かされている。

・社会のデジタル変革

2010 年以降、デジタル技術が急速に進展し、経済・社会システムの再設計や企業経営の DX など、モノのインターネット(IoT) やビッグデータ、人工知能(AI)といったコアとなる技術の革新である第四次産業革命が進展している[16]。この第四次産業革命の進展で、サイバー空間はデジタル産業だけでなく、全ての産業に関係するようになる。そして、第四次産業革命のようなデジタル変革には半導体や先端技術製品が基盤となるため、これら製品の供給問題はデジタル産業を含む全ての産業に影響を及ぼす。

・主要国による先端技術開発競争

1980 年代以降は、米国、欧州など先進国を中心に、政府の役割を最小限に抑え、産業政策を前面に出す動きを控える潮流が続いていたが、近年は米中対立、半導体や重要鉱物の供給問題、カーボンニュートラル等により、各国も技術が国力につながるという認識から、産業政策を積極的に打ち出す動きが進んでいる[17]。

加えて、従来、国民生活や経済活動において重要となる先端技術は、国の機関や一部の大企業等が主体となり開発され、その成果が広く経済・社会に活用されてきたが、近年急速に

[15] 経済産業省、「通商白書 2022」、232 頁。（2023 年 1 月 20 日閲覧）。
[16] 同上、217 頁。（2023 年 1 月 20 日閲覧）。
[17] 同上、237 頁。（2023 年 1 月 20 日閲覧）。

進展しつつある AI、量子等の新興技術の研究開発は、アカデミアやスタートアップ企業を含めた多様な主体がボトムアップで推進しており、先端技術の研究開発を担う主体に変化が生じている[18]。このような新興技術は経済社会活動に大きな影響を与えるのみならず、軍事的に応用されれば、安全保障秩序も変化させうる可能性がある[19]。経済産業委員会調査室の中村直貴氏は、「有力な技術を獲得した国家は、経済と軍事の両面で大きなアドバンテージを得る一方、技術力を失った国家は大幅な後退を余儀なくされることを意味し、それが故に技術覇権を巡る競争を従来に増して熾烈なものとしている[20]」と指摘している。

特に、中国政府は 1990 年代末期に軍民融合政策に舵を切っており、軍需産業への集中投資に加え、民間技術を軍事技術に積極的に導入してきた。また、2008 年ごろには「千人計画」を打ち出し、海外の優秀な研究人材の獲得をおこなっており、我が国の研究者も勧誘された事例がヒアリング調査で聞かれた。さらには、物理的なスパイ行動からサイバー攻撃による日米欧からの先端技術の窃取も発生している[21]。実際に、「APT1」や「APT10」による、米国に対するサイバー攻撃では中国政府が密接に関与しているとされること[22]や、中国共産党員による JAXA 等へのサイバー攻撃[23]が発生しており、米国は、中国が多量かつ効果的なサイバースパイ活動の脅威をもたらし、実質的なサイバー攻撃能力を有し、影響力の脅威を増大させていると評価している[24]。

なお、米中対立で語られる「技術覇権」とは、東京大学公共政策大学院教授の鈴木一人氏が「特定の技術を保有し、他国が長期にわたってその技術を得られない状態を作り、その技術を用いて国際秩序を形成する力」と定義しており、単に科学技術力的なイノベーションや技術開発力だけでなく、大量に生産できる能力を用いて社会実装する観点も含まれている[25]。中国には、新しい技術を開発し、それを大量生産し、社会実装する産業基盤は十分に整っている一方、米国は高い研究開発能力は持つものの、製造業は衰退している[26]。他方、我が国は研究開発能力と生産基盤は持つものの、米中を凌駕するものではない。

上記動向を受けて、我が国がこれからも経済的に成長し、経済分野で国益を確保し続ける

---

[18] 内閣府、「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に関する基本指針」、2022 年 9 月 30 日、3 頁。[https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin3.pdf]、（2023 年 1 月 26 日閲覧）。

[19] 宮本雄二・伊集院敦・日本経済研究センター『米中分断の虚実』、日本経済新聞出版、2021 年、46 頁。

[20] 中村直貴「経済安全保障政策の再構築 -急務となる優位性の獲得と自律性の確保-」『立法と調査』439 号、2021 年 10 月 1 日、68 頁。

[21] 公安調査庁、「経済安全保障の確保に向けて 2022」、2022 年、5-12 頁。
［https://www.moj.go.jp/content/001373771.pdf］、（2023 年 1 月 20 日閲覧）。

[22] 公安調査庁、「サイバー空間における脅威の状況」、2022 年。
［https://www.moj.go.jp/content/001371280.pdf］、（2023 年 1 月 20 日閲覧）。

[23] 同上。（2023 年 1 月 20 日）。

[24] Office of the Director of National Intelligence, *ANNUAL THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY*, April 9, 2021, p.8,
［https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf］, accessed January 26, 2023.

[25] 宮本雄二・伊集院敦・日本経済研究センター、『米中分断の虚実』、41 頁。

[26] 同上、41 頁。

ためには、以下の理由で、①サプライチェーンの強靭化、②サイバーセキュリティの強化、③経済インテリジェンス体制の強化が重要な課題となる。

そのために、我々はこの 3 点について政策提言を行うこととした。

① サプライチェーン分野での政策提言

上述の通り、地政学的リスクの増大により、特定国に依存する物資の安定供給が脅かされている。さらに、技術覇権をめぐる米中間の競争も踏まえ、米国と EU をはじめ、各国はサプライチェーンの強靭化を図っている[27]。なおかつ、デジタル変革に必要な、半導体や先端技術製品の供給問題は全ての産業に影響を及ぼす。

そのためには、同盟国・有志国[28]間の連携を強化し、サプライチェーンの強靭化を行い、加えて新興技術管理を厳格化する必要がある。

② サイバーセキュリティ分野での政策提言

第四次産業革命の舞台となるサイバー空間は、社会横断的に、個々人までピンポイントで攻撃することができる空間であるため、国家・全産業だけでなく個々人までもが外国のサイバー攻撃にさらされるリスクがある[29]。さらに、技術覇権をめぐる争いにおいて、国家の関与が疑われる情報窃取型サイバー攻撃も発生している。そのため、これまで以上にサイバーセキュリティ施策が必要になるものの、我が国のサイバーセキュリティ施策や情報共有体制は各国に比べて進んでいないと評される[30]。ゆえに、我が国のサイバーセキュリティを向上させる施策が必要となる。

③ 経済インテリジェンス分野での政策提言

経済安全保障では、国家だけでなく、企業、大学がプレイヤーとして存在している。経済安全保障の必要性が高まる[31]中で、分野によっては、各ステークホルダーが有している情報を常に新しい状態で、産官学間で共有することが必要である。

また、主要国の技術開発競争を我が国が勝ち抜くためには、国家安全保障の観点から保全と育成をすべき分野を指定し、技術優越の確保・維持を図るべき具体的な重要技術を特定し、

---

[27] 経済産業省、「通商白書 2022」、282-287 頁。（2023 年 1 月 26 日閲覧）；内閣府、「特定重要物資の安定的な供給の確保に関する基本指針」、2022 年 9 月 30 日、3 頁。[https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin1.pdf]、（2023 年 1 月 24 日閲覧）。

[28] 我が国にとっての同盟国とはアメリカである。また、有志国は価値観を共有する国々であり、サプライチェーンの強靭化において、我が国は、有志国との連携が重要としている。例えば、2021 年 4 月に立ち上げられた、インド太平洋地域におけるサプライチェーンの混乱に日豪印三か国で協力して対応する日豪印三か国の貿易大臣による SCRI（サプライチェーン強靭化イニシアティブ）を例に挙げている。経済産業省、「通商白書 2022」、286 頁。（2023 年 1 月 26 日閲覧）。

[29] 船橋洋一『地経学とは何か』、文藝春秋、2020 年、202 頁。

[30] マイケル・グリーン氏に対するヒアリング調査（2022 年 11 月 15 日実施）；ASPI に対するヒアリング調査（2022 年 11 月 10 日実施）。

[31] 経済産業省、「通商白書 2022」、226 頁。（2023 年 1 月 25 日閲覧）。

支援しなければならない。加えて、今後、我が国が留学生の受け入れや海外の研究機関との連携等を推進していく上で、このような重要技術が漏洩しないよう、機微情報の取扱いに係る資格のあり方を設ける必要がある。

そして、これら 3 点の政策提言は下図 3 のように、相互に連関するものである。

「1. サプライチェーン分野での政策提言」により、我が国のサイバー空間を支える半導体の供給確保と、これからの社会で不可欠となる EV や風力発電に必要なネオジム磁石の 2 点について、安定確保・技術育成を目指す。

「2. サイバーセキュリティ分野での政策提言」により、外的脅威等により、我が国のサイバー空間がサイバー攻撃に遭っても被害を最小限化することを目指す。

以上の 2 点の提言では、技術を使用・育成する研究機関や民間企業が大きな役割を果たす。したがって、「3. 経済インテリジェンス分野での政策提言」により、不可欠となる産官学の情報の共有体制を整える必要がある。それと同時に、研究機関・民間企業等から集まった情報を分析する機能の強化、そして情報漏洩を防ぐ体制も必要となる。

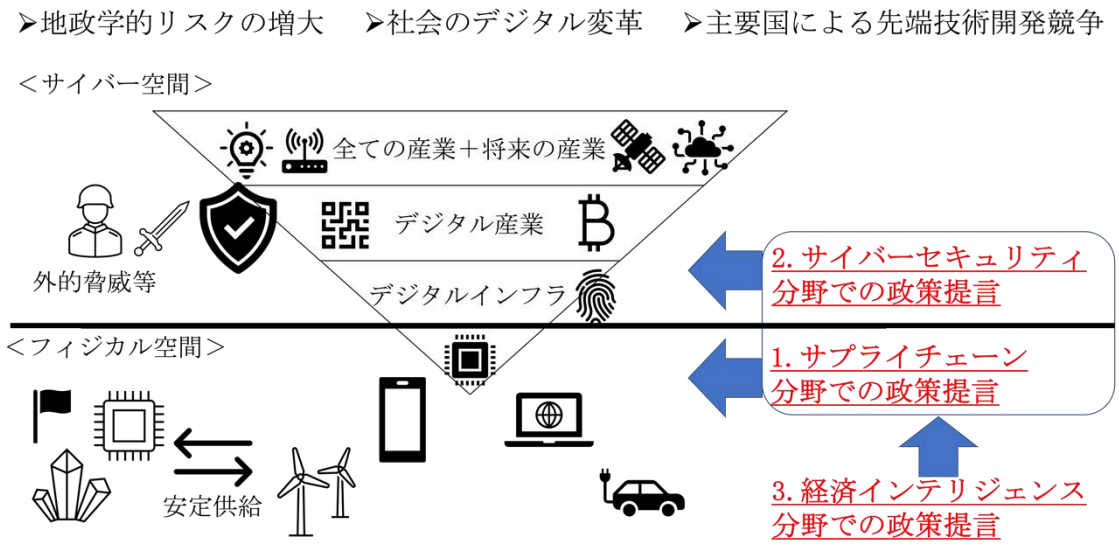


図 3　提言の全体像

出典：筆者作成

第 3 節　研究方法

我々は、先行研究の整理のほか、国家安全保障局経済班をはじめとする中央省庁及び地方自治体、各企業、大学、有識者、豪州政府等、60 か所へヒアリング調査を行い、議論を重ねた。

第一に、経済安全保障全般について、我々は我が国のこれまでの経済安全保障施策や各国の経済安全保障施策を調査した。そして、我が国の経済安全保障施策を主導した衆議院議員

甘利明氏及び大野敬太郎氏、国家安全保障局経済班、各省庁の経済安全保障担当部局等の中央省庁の担当者にヒアリングを行った。また、北村エコノミックセキュリティ合同会社代表の北村滋氏（元国家安全保障局長）、同志社大学法学部教授の兼原信克氏（元国家安全保障局次長）、慶應義塾大学教授の土屋大洋氏、東京大学講師の小泉悠氏、東京大学特任講師の井形彬氏といった有識者にヒアリングを行った。さらに、豪州への現地調査のため、外務省大洋州課及び在日豪州大使館、東京大学特任助教の山口亮氏にヒアリングを行った。豪州では、豪州連邦政府外務貿易省及び内務省、並びに在豪日本国大使館、United States Studies Centre CEO のマイケル・グリーン氏、同国シンクタンクの ASPI、JETRO シドニー事務所、在豪日本企業にヒアリングを行った。

第二に、サプライチェーン分野での政策提言では、輸出管理を管轄する経済産業省安全保障輸出管理課及び半導体産業を所管する同省情報産業課、鉱物資源を担当する同省資源エネルギー庁鉱物資源課、蓄電池を担当する同省電池産業室、東北経済産業局、九州経済産業局、外務省中国・モンゴル課にヒアリングを行った。さらに、鉱物資源に関しては、JOGMEC 及び豪州連邦政府外務貿易省重要資源課にヒアリングを行った。半導体については、東北大学教授の遠藤哲郎氏及び日本経済新聞編集委員の太田泰彦氏、キオクシア株式会社にヒアリングを行った。

第三に、サイバーセキュリティ分野での政策提言では、経済産業省及び警察庁、総務省のサイバーセキュリティ部局、内閣サイバーセキュリティセンター、情報通信研究機構、東北電力、某セキュリティ企業、電気通信事業会社にヒアリングを行った。加えて、国際比較のため、豪州連邦政府外務貿易省サイバーセキュリティ課及び ASPI 課長のファーガス・ハンソン氏、ニューサウスウェールズ大学法学部教授のリリア・ベネット・モーゼス氏にヒアリングを行った。

第四に、経済インテリジェンス分野での政策提言では、警察庁外事課及び文部科学省科学技術・学術政策局、宮城県警察、内閣府、東北大学教授の佐々木孝彦氏、東北大学安全保障輸出管理室、PHP 総研にヒアリングを行った。

これらの文献・ヒアリング調査の下、政策提言を行うこととする。

第 2 章　各国の経済安全保障施策

前章では、我が国の経済安全保障をめぐる背景と我々の研究の射程・目的について言及した。もっとも、経済安全保障に対する機運は我が国だけではなく世界全体で高まり、経済安全保障を推進する取組は他国においても急速に進められている。米中の対立が激化するなか、欧州連合（European Union。以下「EU」という。）は米国との協力体制を強化する方針を示しており、今後の米中及び EU の動向が注目される。また、我が国は今後の安全保障及び経済安全保障においてインド太平洋を重要な地域の一つと考えており、豪州とは QUAD 等の枠組みでも連携を強化している。そこで、以下では、近年の米国、EU、豪州、中国の経済安全保障施策について概観する。

第 1 節　米国における経済安全保障施策

米国ではその年の国防予算の大枠が、「国防権限法」によって決定される。「2019 年国防権限法」では、「外国投資リスク審査現代化法及び輸出管理改革法」の内容が改訂され、当該国防権限法に盛り込まれることとなったほか、米国政府機関に対する中国企業の通信・監視関連機器・サービスの購入、利用の禁止規定が創設された[32]。外国投資リスク審査現代化法においては、従来は通常の買収を指す「支配を及ぼす投資」のみが審査対象であったが、内容の改定に伴い、「支配を及ぼさない投資」も審査対象となり、対米外国投資委員会の権限を強化する内容となった[33]。「支配を及ばさない投資」とは、重要インフラや重要技術等に関連する米国事業者への投資のうち、非公知情報へのアクセスが可能となるものや、役員等の職位につくことが可能となるもの、米国人の機微な個人データへのアクセスが可能となるものなどである[34]。「輸出管理改革法」については、国家安全保障上重要となる「新興・基盤的技術」などが新たな対象分野として追加された[35]。

また、2019 年に制定された「安全で信頼できる通信ネットワーク法」が 2022 年に改正され、中国通信大手 5 社のほか新たに中国企業 2 社とロシア企業 1 社を国家安全保障の脅威として指定し、政府補助金を利用して当該中国企業の通信機器等を購入することを禁止するとともに、撤去・交換のための助成が行われている[36]。2020 年には「国家緊急経済権限法」等に基づく大統領令が公布され、「外国敵対者」によって設計・開発・製造・供給される通

---

[32] the Senate and House of Representatives of the United States of America , *One Hundred Fifteenth Congress of the United States of America*, https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf, accessed January 21, 2023.
[33] 田上靖「米国 FIRRMA（外国投資リスク審査現代化法）及びその改正下位規則の概要」『CISTEC JOURNAL』No186、2020 年 3 月、80 頁。
[34] 同上、80-81 頁。
[35] JETRO、「続・厳格化する米国の輸出管理法令　留意点と対策」、2021 年 8 月、18-24 頁。［https://www.jetro.go.jp/ext_images/_Reports/01/e95620416cd2f8d3/20210031.pdf］、（2023 年 1 月 24 日閲覧）。
[36] JETRO、「米連邦通信委、国家安全保障の脅威の機器・サービスにカスペルスキーや中国電信など 3 社を追加」、2022 年 3 月 29 日。［https://www.jetro.go.jp/biznews/2022/03/9ba15d812e7eb629.html］、（2023 年 1 月 24 日閲覧）。

信機器等が規制されることとなった[37]。

2021 年には、同年 2 月に署名された「サプライチェーンの強靭化に関する大統領令」に基づき、同年 6 月に報告書「強靭なサプライチェーンの構築、米製造業の再活性化、幅広い成長の促進」が公表された。当報告書では、半導体、大容量電池、重要鉱物、医療品等についての短期的取組及びコロナ禍からの経済再開に向けた長期的戦略が示された[38]。2022 年 2 月には 1 年以内のレビューが求められていた特定分野に関する計画も発表され[39]、サプライチェーン強靭化に向けて、現在進行形で数多くの施策が打ち出されている。

第 2 節　EU における経済安全保障施策

EU は 2020 年に「グローバルな変革のための新たな環大西洋協力アジェンダ」を発表し、2019 年～2024 年において取り組むべき優先課題を取り決め、あらゆる分野で米国と協力関係を構築していくことを示した。特に、COVID-19 への対処や環境保護、通商、先端技術、デジタル政策、民主主義の推進など、あらゆる分野において米国と協力して取り組むこととした[40]。その中では、グローバル経済や安全保障の観点から、5G 等の重要技術を保護するための共通施策を打ち出していくことが明記されている[41]。

2020 年には「欧州原材料同盟」が発足した。EU は、経済活動に不可欠でありながらも、EU 域外からの調達に依存している原材料を「重要な原材料」と定義し、そうした原材料のサプライチェーンを強靭化し、域外輸入依存度引き下げることを目標としている[42]。当面の課題は、中国にその調達を依存しているレアアース（希土類）の輸入依存度の引き下げである。

また、軍民両用品目輸出管理に関する欧州議会・理事会規則が改正され、2021 年より適用された。民生及び軍事双方において利用が可能な二重用途物品に対する輸出管理を強化

---

[37] 内閣府、「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 第一回資料」、2021 年 12 月 10 日、5 頁。
［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou4.pdf］、（2023 年 1 月 24 日閲覧）。

[38] 内閣府、「経済安全保障法制に関する有識者会議 サプライチェーン強靭化に関する検討会合 第 1 回資料」、2021 年 12 月 8 日、6 頁。
［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou1.pdf］、（2023 年 1 月 24 日閲覧）。

[39] JETRO、「バイデン米政権、サプライチェーン強化策発表、エネルギーや ICT など 6 分野で」、2022 年 2 月 28 日。［https://www.jetro.go.jp/biznews/2022/02/4b787e74559f4268.html］、（2023 年 1 月 24 日閲覧）。

[40] European Commission, *EU-US: A new transatlantic agenda for global change*, December 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279, accessed January 20, 2023.

[41] European Commission, *A NEW EU-US AGENDA FOR GLOBAL CHANGE*, December 2020, https://ec.europa.eu/commission/presscorner/detail/en/fs_20_2285, accessed January 20, 2023.

[42] 三菱 UFJ リサーチ＆コンサルティング、「原材料の戦略的な確保を図る EU ～欧州原材料同盟（ERMA）構想の特徴と問題点 」、2021 年 8 月 31 日。［https://www.murc.jp/wp-content/uploads/2021/08/report_210831.pdf］、（2023 年 1 月 22 日閲覧）。

し、輸出認可の対象範囲を拡大する内容となった[43]。

2021 年には新たな通商戦略を発表し、経済変革や地政学的変化のなかで、2030 年の世界を見据えた通商政策を打ち出した。「開かれた戦略的自律性」のもと、持続可能なバリューチェーンの推進や、デジタル化への移行とサービス貿易の推進、EU 規制の影響力の強化を含む、今後の通商政策において重要となる分野を指定した[44]。

加えて、第１回米 EU 貿易・技術評議会（TTC）が米国で開催された。科学技術、経済、貿易に関する主要課題や、民主主義的価値に基づき、複雑化する貿易・経済関係に対する解決の方向性を模索することを目的とし、この目的を達成するために、投資審査や輸出管理、AI、半導体、国際通商課題の各分野において協力し、成果を上げることを目指している[45]。

第 3 節　豪州における経済安全保障施策

2018 年、「重要インフラ安全保障法」が成立した。重要インフラに関わる国家安全保障への脅威に対処し、自国における重要インフラの所有・管理の透明性を高め、関係者間で協力・協働を推進していくことを目的としている。

2021 年には「外資による取得・買収に関する法律」が改正され、投資額に関係なく、安全保障上重要な土地や事業に対する外国投資が、政府による審査の対象となった。電気や港等の重要インフラ、通信事業、防衛関連事業の他、高度教育・研究、宇宙技術等の新たな分野にも審査が及ぶこととなり、審査対象範囲が拡大した[46]。

2021 年には、「重要インフラ安全保障法」が改正され、その対象となる産業分野が拡充されるとともに、サイバーインシデントに係る官民の情報共有体制の強化が盛り込まれた。

また、同年には「サイバー・重要技術国際関与戦略」が策定された。サイバー及び重要技術によって、自国やインド太平洋地域、そして世界の安全保障や繁栄を実現することを目的とし、国際関与を高めていくとした。政府は、サイバーや AI、5G など、国益に関わる重要技術の特定などを推進する方針を示している[47]。

---

[43] JETRO、「EU 輸出品目規制：I.二重用途物品に関する規制　詳細」、2022 年 12 月 12 日。［https://www.jetro.go.jp/ext_images/jfile/country/eu/trade_02/pdfs/eu_p11_2F010.pdf］、（2023 年 1 月 21 日閲覧）。

[44] European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Trade Policy Review – An Open, Sustainable and Assertive Trade Policy*, February 18, 2021, https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159438.pdf, accessed January 21, 2023.

[45] Office of the United States Trade Representative, *U.S.-EU Trade and Technology Council Inaugural Joint Statement*, September 29, 2021, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/september/us-eu-trade-and-technology-council-inaugural-joint-statement, accessed January 21, 2023.

[46] JETRO、「重要インフラ安全保障法の改正法が発効、外資審査の対象拡大」、2021 年 12 月 9 日。［https://www.jetro.go.jp/biznews/2021/12/bc10d9712d63af19.html］、（2023 年 1 月 20 日閲覧）。

[47] Department of Foreign Affairs and Trade, *Australia's International Cyber and Critical Tech Engagement Strategy*, April 2021, p.8,

そして、2022 年には、「2022 年重要鉱物戦略」が打ち出され、重要鉱物分野におけるサプライチェーンの確保などについてその重要性が明記されている。重要鉱物のサプライチェーンの強靭化に加え、知見・技術の発展、重要鉱物分野における労働力の向上を目標に、各取組が示されている[48]。

第 4 節　中国における経済安全保障施策

中国は、これまでも緊急事態における民間資源の軍事利用を目的として国防動員体制を敷いてきたが、近年では国家戦略として軍民融合を進めている。軍民融合とは、従前の「国防動員体制の整備に加え、緊急事態に限られない平素からの民間資源の軍事利用や、軍事技術の民間転用などを推進するもの[49]」とされている。特に、海洋、宇宙、サイバー、AI 等の分野は「新興領域」とされ、これらの分野における先端技術の開発・獲得が積極的に行われている[50]。

2015 年、第 13 次 5 か年計画期に「中国製造 2025」が打ち出され、中国を製造大国へと導くための産業政策が示された。その中で特に重要な分野として、ICT 産業、高級 NC 工作機器とロボット、航空・宇宙用機器、海洋土木設備及びハイテク船舶、先進型軌道系交通設備、省エネルギー・新エネルギー車、電力機器、農業設備、新材料、バイオ医薬品並びに高性能医療機器の 10 分野が指定され、これらの重点産業における多くの品目について、2025 年までに 60～80%の国内生産を目指すものとされた[51]。

2020 年には「輸出管理法」が施行された。「輸出管理法」は「国の安全と利益」を目的としているが、他国にとって不利益となりうる条文や再輸出規制、みなし輸出規制に関する条文が存在していることや、制度の全容及び規制対象となる取引範囲が明らかにされていないことが問題視されている。

2021 年には「外商投資安全審査弁法」が施行され、国防やエネルギー、重要インフラといった国家安全に係る重要領域に投資し、かつ、投資先企業の実質支配権を取得する場合に事前申請が義務付けられた。

同じく 2021 年には「反外国制裁法」が施行された。反外国制裁法第 3 条第 2 項によると、「外国国家が国際法および国際関係の基本的な規範に違反し、各種の口実またはその国の

---

https://www.internationalcybertech.gov.au/sites/default/files/2021-04/21045%20DFAT%20Cyber%20Affairs%20Strategy%20Internals_Acc_update_1_0.pdf, accessed January 20, 2023.

[48] Australian Government Department of Industry, Science Energy and Resources, *2022 CRITICAL MINERALS STRATEGY*, March 2022, p3, https://www.industry.gov.au/sites/default/files/2022-09/2022-critical-minerals-strategy_0.pdf, accessed January 22, 2023.

[49] 防衛省、「令和 3 年版防衛白書」、2021 年、18 頁。
［http://www.clearing.mod.go.jp/hakusho_data/2021/pdf/R03010202.pdf］、（2023 年 1 月 25 日閲覧）。

[50] 同上、18 頁。

[51] 株式会社 エイジアム研究所、「平成 29 年度製造基盤技術実態等調査（中国製造業の実態を踏まえた我が国製造業の産業競争力調査)」、2018 年 3 月 30 日、7-11 頁。
［https://www.meti.go.jp/meti_lib/report/H29FY/000403.pdf］、（2023 年 1 月 24 日）。

法律に基づき、中国に対し抑制・抑圧を行い、中国の公民、組織に対し差別的制限措置を講じ、中国の内政に干渉すること[52]」は、自国への「外国制裁」に当たり、対抗措置の対象となるとされている。入国拒否や自国領域内の各種財産の差し押さえ、押収、凍結、自国領域内の組織や個人との関連取引等の禁止、制限などが制裁として行われる。対抗措置の対象となるのは、「外国制裁」を直接的に行った個人、組織に限らず、間接的な関与を持つ個人、組織も該当するが、どの程度の関与が対象となるのかについては明確化されていない。

また、同年、データ及びセキュリティの監督管理等について定めた「データセキュリティ法」も施行された。工業や電気通信、天然資源等の各部門は、業務で収集したデータ及びセキュリティに対して責任を負うとするとともに、国家安全や公共の利益などに与える危害の程度に応じて、データを分類管理する分類・等級区分保護制度を構築し、データを管理するといった内容が定められた。また、データの越境移転や輸出規制に関する規定が含まれている他、データ及びデータの開発・利用技術にかかわる投資、貿易における自国への差別的禁止、制限等の措置に対し、対抗措置を講じることを可能とする条文も盛り込まれている[53]。

以上、米国、EU、豪州、中国の経済安全保障施策を概観した。経済安全保障施策は各国で積極的に進められており、我が国においても施策の策定が急務となっている。次章では、我が国の経済安全保障施策について、その動向と具体的取組について説明する。

[52] JETRO、「反外国制裁法の概要～中国の安全保障貿易管理に関する制度情報専門家による政策解説～」、2021年9月、1頁。
［https://www.jetro.go.jp/ext_images/_Reports/01/2600bae53b7255f4/20210037_02.pdf］、（2023年1月19日閲覧）。
[53] JETRO、「「データセキュリティ法」の概要」、2021年12月。
[https://www.jetro.go.jp/ext_images/_Reports/01/580a6448fa87f0bb/20210056_04.pdf]、（2023年1月25日閲覧）。

第 3 章　我が国の経済安全保障施策

本章では、第 1 部の結びとして、我が国の経済安全保障施策について概観する。第 1 節では国内での経済安全保障の動向について時系列に沿って整理し、第 2 節では我が国の経済安全保障施策について述べていく。最後の第 3 節では、国際社会との連携による経済安全保障施策について概観し、我が国の経済安全保障施策の概要について包括的に理解することを目標とする。

第 1 節　我が国の経済安全保障の動向

1　大平正芳氏による経済的安全保障

我が国において、経済安全保障の考え方は近年になって初めて出てきたものではない。1980 年に、当時の首相である大平正芳氏のもと、『総合安全保障』が出版され、経済的安全保障政策が言及されている[54]。当文書においては、安全保障を「国民生活を様々な脅威から守ること」と定義し、そのための努力を「脅威そのものをなくするための、国際環境を全体的に好ましいものにする努力」、「脅威に対処する自助努力」、「その中間として、理念や利益を同じくする国々と連帯して安全を守り、国際環境を部分的に好ましいものにする努力」の 3 つのレベルから構成した[55]。

これらを経済的安全保障政策に具体的に当てはめ、自由貿易体制の維持や南北問題の解決といった「相互依存の体系の運営、維持」を第一のレベルの努力、その国の経済にとって重要ないくつかの国々との関係を友好的なものとすることといった「中間的方策」を第二のレベルの努力、備蓄やある程度の自給力といった「自助努力」を第三のレベルの努力としている[56]。具体的な経済的安全保障政策としては、エネルギー安全保障と食料安全保障を掲げている[57]。当政策は、1973 年に発生した石油危機や、経済成長を実現し高度産業社会となった我が国の産業構造の変化に起因するものと考えられる[58]。

2　近年における経済安全保障の動向

もっとも、1989 年の冷戦終結以降、国際社会は共存共栄の国際秩序と自由貿易体制のもとに各国の相互依存が進んだ。グローバリゼーションの展開によって、旧共産主義諸国が自由民主主義諸国に類する形で変質することが期待されたために、相互依存による経済的影響力について懸念されることはなくなり[59]、大平氏が掲げた経済的安全保障の観念は具現化

---

[54] 内閣官房内閣審議室分室・内閣総理大臣補佐官室『総合安全保障』、大蔵省印刷局、1980 年、24 頁。
[55] 同上、7 頁。
[56] 同上、24 頁。
[57] 同上、12-13 頁。
[58] 『総合安全保障』の 1 頁には「「近代化」を達成した欧米先進諸国と日本は、高度産業社会として成熟し、多くの困難な問題に直面するに至った」と記され、エネルギー安全保障に言及する 41 頁には「1973 年の石油危機は、エネルギー問題を劇的な形で示し、経済的安全保障を考える必要をわれわれに教えた」と記されていることから、経済的安全保障政策の発端になったと考えられる。
[59] 本報告書第 1 部第 1 章第 1 節を参照。

されなかった。

しかし、そのような期待は幻想となり、旧共産主義諸国の民主化は実現せず、普遍的価値を共有しないまま現代に至る。2010 年には、尖閣沖で海上保安庁の巡視船に体当たりをした中国船の船長の身柄を拘束したことに反発し、中国当局はレアアースの輸出を規制して我が国に圧力を加えるといった、経済的依存を背景とする経済力を武器に安全保障上の国益を追求する事態が発生した[60]。

このような状況の下、日本国内で本格的に経済安全保障の観念が再燃し、2019 年には甘利明氏をはじめとする自由民主党の衆参国会議員によって構成されるルール形成戦略議員連盟が、国家経済会議（日本版 NEC）の創設を提言した。中国の台頭と米中対立を背景に、安全保障の観点から経済政策を立案する米国の国家経済会議をモデルに、日本でも同様の組織を作るべきだとした提言である[61]。

2020 年 4 月には、経済安全保障上の課題について、俯瞰的・戦略的な政策の企画立案・総合調整を迅速かつ必要な取組を推進するため、内閣官房国家安全保障局に経済班が設置された。北村滋氏は、「このような新たなシステムが作られたことで、省庁ごとの垣根無く経済安全保障の政策を作ることができるようになり、また、外国企業からの投資で経済安全保障上懸念のありそうな個別条件についても情報が入ってくるなど、情報共有が可能となった[62]」と経済班について述べている。

同年 12 月には、自由民主党政務調査会・新国際秩序想像戦略本部が「提言『経済安全保障戦略』の策定に向けて」を発表した。当提言は、経済安全保障の定義を「わが国の生存、独立及び繁栄を経済面から確保すること」とし、国際社会のパワーバランスの変化・経済的依存関係の政治目的利用・新型コロナによる脆弱性の露呈・デジタル化の普及といった観点から、国家としての包括的な戦略的取組の必要性を述べている[63]。また、経済安全保障戦略の基本的考え方として戦略的自律性の確保と戦略的不可欠性の強化・獲得を示し、政府に対して「経済安全保障戦略」の早急な策定を求めた[64]。

2021 年に入ると、立て続けに経済安全保障への言及が政府でなされた。6 月に発表された「経済財政運営と改革の基本方針 2021」（令和 3 年 6 月 18 日閣議決定）には、経済安全保障の文言が示され、経済安全保障に係る戦略的な方向性として、「基本的価値やルールに基づく国際秩序の下で、有志国との協力の拡大・深化を図りつつ、我が国の自律性の確保・優位性の獲得を実現することとし、こうした観点から重要技術を特定し、保全・育成する取組を強化するとともに、基幹的な産業を強靭化するため、今後、その具体化と施策の実施を進

---

[60] 同上。
[61] 北村滋、『経済安全保障』、176 頁。
[62] 同上、177 頁。
[63] 自由民主党政務調査会新国際秩序想像戦略本部、「提言『経済安全保障戦略』の策定に向けて」、2020 年 12 月 16 日、2-3 頁。［https://storage.jimin.jp/pdf/news/policy/201021_1.pdf］、（2023 年 1 月 1 日閲覧）。
[64] 同上、3-4 頁。（2023 年 1 月 1 日閲覧）。

めること」が記されている[65]。また、「成長戦略実行計画」（令和3年6月18日閣議決定）においても、経済安全保障の文言が明記され、自律性の確保と優位性の獲得の実現のための施策が言及されている[66]。

10月3日に行われた第205回国会における岸田内閣総理大臣所信表明演説では、成長戦略の第三の柱として経済安全保障を掲げ、新たに設けた担当大臣の下、戦略物資の確保や技術流出の防止に向けた取組を進め、自律的な経済構造の実現及び強靭なサプライチェーンを構築し、我が国の経済安全保障を推進するための法案の策定を行うと述べている[67]。その後、内閣府特命担当大臣経済安全保障担当大臣（経済安全保障担当）のポストを新たに設置し、初代大臣として小林鷹之が任命され、同年11月から経済安全保障推進会議及び経済安全保障法制に関する有識者会議が開催されている。

2022年1月には、第208回国会における岸田内閣総理大臣施政方針演説にて経済安全保障が言及され、新たな法律により、サプライチェーン強靭化への支援、電力、通信、金融などの基幹インフラにおける重要機器・システムの事前安全性審査制度、安全保障上機微な発明の特許非公開制度等を準備し、あわせて、半導体製造工場の設備投資や、AI、量子、バイオ、ライフサイエンス、光通信、宇宙、海洋といった分野に対する官民の研究開発投資を後押ししていくと述べられた[68]。

5月には「経済安全保障推進法」が成立し、後に経済安全保障推進室が内閣府に設置された。「経済財政運営と改革の基本方針 2022」（令和4年6月7日閣議決定）には前年同様に経済安全保障の強化が明記され、「経済安全保障推進法」の着実な施行、サプライチェーン・官民技術協力関連施策の先行的な実施が求められた[69]。さらに、12月に閣議決定した「国家安全保障戦略」には、経済安全保障が明記された。当戦略においては、経済安全保障を「我が国の平和と安全や経済的な繁栄等の国益を経済上の措置を講じ確保すること」と定義し、安全保障上の観点から政府一体となって必要な取組を行うことが示されている[70]。

このように、1980年以降約30年に渡り議論されてこなかった経済安全保障が、今日では政府の安全保障施策の一つとして重要な位置にあることが伺える。

---

[65] 内閣府、「経済財政運営と改革の基本方針 2021」、2021年6月18日、25-26頁。［https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2021/2021_basicpolicies_ja.pdf］、（2022年12月31日閲覧）。

[66] 内閣官房、「成長戦略実行計画」、2021年6月18日、15-19頁。［https://www.cas.go.jp/jp/seisaku/seicho/pdf/ap2021.pdf］、（2022年1月4日閲覧）。

[67] 首相官邸、「第205回国会における岸田内閣総理大臣所信表明演説」、2021年10月8日。［https://www.kantei.go.jp/jp/100_kishida/statement/2021/1008shoshinhyomei.html］、（2023年1月5日閲覧）。

[68] 首相官邸、「第208回国会における岸田内閣総理大臣施政方針演説」、2022年1月17日。［https://www.kantei.go.jp/jp/101_kishida/statement/2022/0117shiseihoshin.html］、（2023年1月5日閲覧）。

[69] 内閣府、「経済財政運営と改革の基本方針 2022」、2022年6月7日、22-23頁。［https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2022/2022_basicpolicies_ja.pdf］、（2023年2月10日閲覧）。

[70] 内閣官房、「国家安全保障戦略」、26-27頁。（2023年1月5日閲覧）。

第 2 節　我が国の経済安全保障施策

本節では、我が国における近年の経済安全保障施策について概観する。

令和 3 年 11 月 19 日に開催された経済安全保障推進会議では、現状認識と経済安全保障の推進に向けた目標・アプローチについての資料が提示された。当資料においては経済安全保障施策の策定が急務となっている現状についての言及がなされるとともに、経済安全保障施策における我が国としての大きな方向性を示した。経済安全保障施策の目標を①基幹インフラやサプライチェーン等の脆弱性解消といった「自律性の向上」、②研究開発強化等による技術・産業競争力の向上や技術流出の防止といった「優位性ひいては不可欠性の確保」、③基本的価値やルールに基づく国際秩序の維持・強化とし、政府のみならず産学官が連携して各種政策手段を講じ、目標にアプローチすることが記されている。

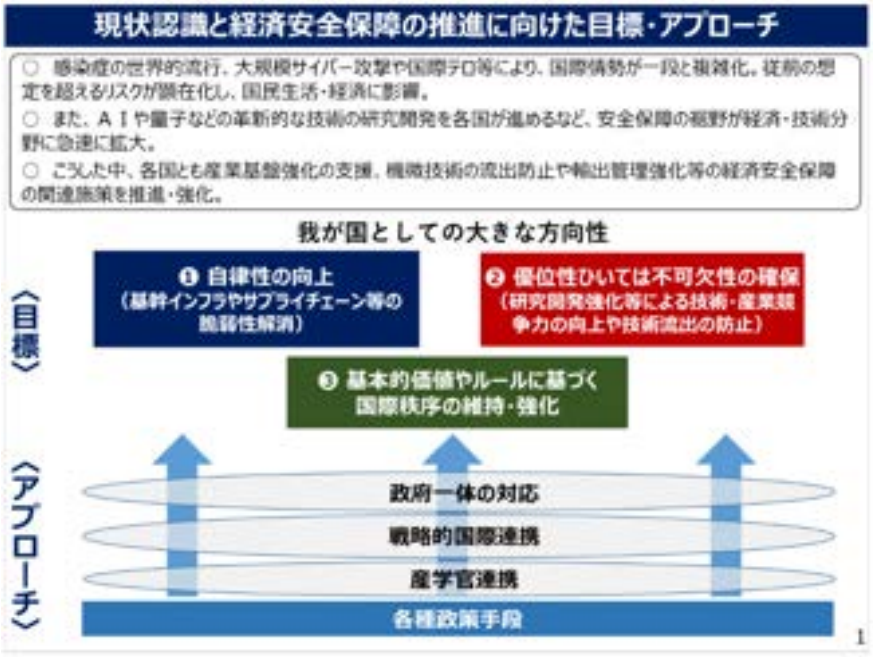


図 4　現状認識と経済安全保障の推進に向けた目標・アプローチ
出典：内閣官房　経済安全保障推進会議第 1 回(令和 3 年 11 月 19 日)

また、同会議では我が国の経済安全保障上の主要課題について下の資料が提示された。

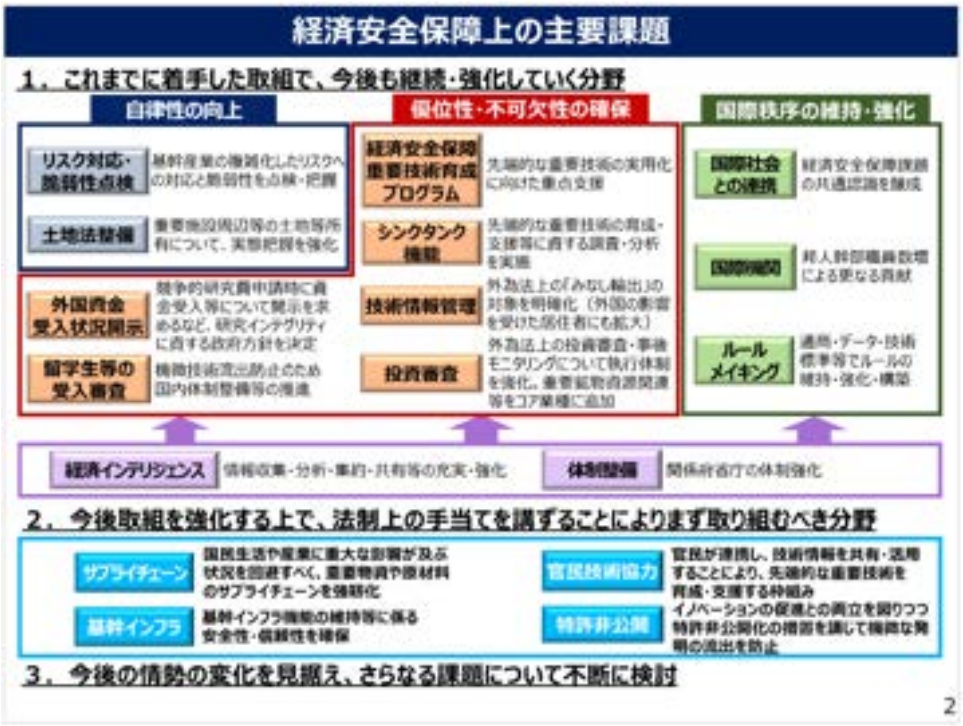


図 5　経済安全保障上の主要課題

出典：内閣官房　経済安全保障推進会議第 1 回(令和 3 年 11 月 19 日)

以下、この資料における整理に基づいて説明する。

1　これまでに着手した取組で、今後も継続・強化していく分野

資料では初めに、前述した目標ごとに分野が振り分けられ、各分野で簡単な説明がなされている。本項では、各分野での取組を具体的に説明する。なお、国際秩序の維持・強化については次節で述べることとする。

(1)　リスク対応・脆弱性点検

2021 年度に、経済産業省等関係省庁が「経済安全保障推進法」のための立法事実調査として半導体・医療品・電気自動車などに使う大容量電池などの原材料や部品を、どの国にどの程度依存しているかを点検した。レアアース（希土類）といった鉱物についても、どの国からどの程度輸入しているのかを調べた[71]。このほか、金融・銀行・鉄道・電力・電気通信といった国民生活の基盤となる業界の企業についても関係省庁が調査を行っている[72]。

[71] 北村滋、『経済安全保障』、179 頁。
[72] 同上、179 頁。

(2)　土地法整備

安全保障上他国に買い占められると不都合な土地の取得を規制する「重要施設周辺及び国境離島等における土地等の利用状況の調査及び利用の規制等に関する法律」（令和3年法律第84号）が2021年6月23日に公布、2022年9月に全面施行された。もっとも、当法律が経済安全保障施策の一部であるとの評価は外部的なものであり、起草者はそのような認識を持っていないとのことだった[73]。

(3)　外国資金受入状況開示

研究インテグリティの確保として政府が方針を示し、研究者、所属機関向けのチェックリスト雛形の作成や競争的研究費の適正な執行に関する指針を改正し、2022年4月以降に公募を行うものから実施されている[74]。

(4)　留学生等の受入審査

「統合イノベーション戦略2020」（2020年7月17日閣議決定）においては、「技術流出防止のより実効的な水際管理を図るため、関係府省庁の連携による出入国管理やビザ発給の在り方の検討を含め、留学生・研究者等の受入れの審査強化に取り組み、そのためのＩＴ環境の整備等を推進」することが明記されている[75]。これは、安全保障に関係する先端技術や情報が留学生らを通じて中国などに流出しているとの懸念に端を発している[76]。

(5)　技術情報管理

従来から「外国為替及び外国貿易法」（昭和24年法律第228号。以下「外為法」という。）に基づき管理が行われていた。具体的には、安全保障の観点から軍事転用可能な機微技術の提供について、①国境を越える技術提供（ボーダー管理）と②国内外における居住者から非居住者に対する提供を管理していた[77]。後者を一般的にみなし輸出管理と呼ぶが、本邦内の事務所に勤務する外国人も「居住者」とされ、また、本邦に入国後6か月以上経過した外国人も「居住者」とされていたため、企業や大学等によるこれらの人への技術提供が、みなし輸出管理の対象外となる場合があった。

---

[73] 内閣府 政策統括官（重要土地担当）に対するヒアリング調査（2022年7月7日実施）。本報告書付属資料のヒアリング報告書に記載はないが、ヒアリングに際しこのような旨意が述べられた。

[74] 内閣府、「研究インテグリティの確保に係る対応方針」、2022年9月。［https://www.mext.go.jp/content/20211220-mxt_kagkoku-000019002_3.pdf］、（2023年1月6日閲覧）。

[75] 内閣府、「統合イノベーション戦略2020」、2020年7月17日、141頁。［https://www8.cao.go.jp/cstp/togo2020_honbun.pdf］、（2023年1月21日閲覧）。

[76] 読売新聞オンライン、「【独自】留学生のビザの審査厳格化へ...中国念頭、安保技術を流出防止」、2020年10月5日。［https://www.yomiuri.co.jp/politics/20201005-OYT1T50013/］、（2023年1月6日閲覧）。

[77] 経済産業省、「『みなし輸出』管理の明確化について」、2021年11月。［https://www.meti.go.jp/policy/anpo/law_document/minashi/jp_kigyou.pdf］、（2023年1月7日閲覧）。

このような状況を踏まえ、2022 年 5 月よりみなし輸出管理が明確化され、たとえ「居住者」への技術提供であっても、「非居住者」の強い影響下にある場合には、みなし輸出管理の対象であることを明確にした[78]。

(6) 経済安全保障重要技術育成プログラム

内閣府主導のもと創設され、我が国が国際社会において中長期的に確固たる地位を確保し続ける上で不可欠な要素となる先端的な重要技術について、研究開発及びその成果の活用を推進するものである[79]。2022 年 12 月 5 日に当プログラムの WEB サイトが公開され、研究開発課題の公募が始まるなど、まさに現在進行中のプログラムとなっている。

(7) シンクタンク機能

2022 年 11 月 29 日に「第 1 回安全・安心に関するシンクタンク設立準備検討会」が開かれ、経済安全保障推進法第 64 条第 2 項の 4 要件を満たす特定重要技術調査研究機関としてのシンクタンク設立の検討がまさになされている[80]。

(8) 投資審査

懸念国の投資家が、我が国の重要技術を有する企業を買収することにより、我が国の技術・データ・製品等が懸念国に流出する懸念があり、我が国の安全を損なう等のおそれがあるため、外為法で対内直接投資制度を管理している。経済安全保障の強化に伴い、2019 年に上場会社の取得時事前届出の閾値を 10%から 1%に引き下げ、また、2021 年には安定供給を確保するためにレアアース等の重要鉱物資源に係る業種をコア業種へ追加した[81]。さらに、関係省庁や外国当局と連携し、対内直接投資審査能力や事後モニタリング能力を強化している[82]。

(9) 経済インテリジェンス及び体制整備

経済安全保障政策の強化に向け、中央省庁の定員を 100 人超の規模で増やすといった報道もあり、着々と整備が進んでいると理解できる[83]。

---

[78] 同上。（2023 年 1 月 7 日閲覧）。
[79] 国立研究開発法人科学技術振興機構、「経済安全保障重要技術育成プログラム WEB サイト」、2022 年 12 月 5 日。［https://www.jst.go.jp/k-program/］、（2023 年 1 月 7 日閲覧）。
[80] 内閣府、「経済安全保障推進法上の特定重要技術調査研究機関としても期待される安全・安心シンクタンクの役割」、2022 年 11 月 29 日。
［https://www8.cao.go.jp/cstp/anzen_anshin/thinktank/1kai/sanko2.pdf］、（2023 年 1 月 7 日閲覧）。
[81] 財務省、「対内直接投資審査制度について」、2021 年 11 月 16 日。
［https://www.mof.go.jp/about_mof/councils/customs_foreign_exchange/sub-foreign_exchange/proceedings/material/gai20211116_5.pdf］、（2023 年 1 月 6 日閲覧）。
[82] 同上。（2023 年 1 月 6 日閲覧）。
[83] 日本経済新聞、「経済安保、省庁 100 人超職員　技術流出防止や外為審査　来年度、別枠で確保」、

2　経済安全保障推進法の成立

前述したような経済安全保障施策が講じられる中、2021 年 11 月 19 日に行われた経済安全保障推進会議では、特に法制上の手当てを講ずることによりまず取り組むべき分野として①重要物資や原材料のサプライチェーンの強靭化、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 つが示された[84]。その後、経済安全保障法制に関する有識者会議が 2021 年 11 月に設置され、以降 4 回の全体会合と 4 つの分野に関する検討会合が計 12 回、あわせて 16 回の会合による議論の下、法案策定の準備が進められた。2022 年 2 月 1 日には、「経済安全保障法制に関する提言」が策定され、政府に対し新規立法措置の速やかな具体化とその成立を強く求めた[85]。

そして、第 208 回国会に「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案」が提出され、2022 年 5 月 11 日に成立、同月 18 日に公布された。

経済安全保障推進法第 2 条第 1 項は、政府が「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基本的な方針」（以下「基本方針」という。）を定めることとし、2022 年 9 月 30 日に、基本方針が閣議決定された[86]。

また、本法第 6 条第 1 項の規定及び基本方針に基づき、「特定重要物資の安定的な供給の確保に関する基本指針」が同年同日に閣議決定された[87]。

さらに、本法第 60 条第 1 項の規定及び基本指針に基づき、「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に関する基本指針」が同年同日に閣議決定された[88]。

2021 年 9 月 12 日。［https://www.nikkei.com/article/DGKKZO75684760S1A910C2EA3000/］、（2023 年 1 月 7 日閲覧）。

[84] 内閣官房、「経済安全保障の推進に向けて」、2021 年 11 月 19 日。［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai1/shiryou3.pdf］、（2023 年 1 月 20 日閲覧）。

[85] 内閣官房、「経済安全保障法制に関する提言の概要」、2022 年 2 月 4 日。［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai2/shiryou1.pdf］、（2023 年 1 月 21 日閲覧）。

[86] 内閣府、「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基本的な方針」、2022 年 9 月 30 日、2 頁。［https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonhoushin.pdf］、（2023 年 1 月 7 日閲覧）。

[87] 内閣府、「特定重要物資の安定的な供給の確保に関する基本指針」、4 頁。（2023 年 1 月 7 日閲覧）。

[88] 内閣府、「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に関する基本指針」、3 頁。（2023 年 1 月 7 日閲覧）。

図 6　経済安全保障推進法の概要

出典：内閣府

第 3 節　国際社会との連携による経済安全保障施策

最後に、図 5 の「国際秩序の維持・強化」に関して、国際社会との連携による経済安全保障施策を概観する。二国間関係については同盟国である米国、有志国であり我々が訪問した豪州、多国間関係については、経済安全保障に向けて既に動き始めている QUAD、IPEF、G7 について言及する。

1　米国

2022 年 5 月 23 日、岸田内閣総理大臣は、訪日中のバイデン米国大統領と日米首脳会談を行い、その成果として共同声明を発出した。この共同声明において、半導体を中心にサプライチェーンの強靭性やサイバーセキュリティに言及しつつ、我が国での「経済安全保障推進法」の成立に留意したうえで、経済安全保障を強化するための更なる協力を追求していくことで両首脳は一致した[89]。同会談で発出した「ファクト・シート：日米競争力・強靭性パートナーシップ」は、2021 年 4 月に発表した「日米競争力・強靭性（コア）パートナーシップ」の下での進展を記すものであり、科学技術協力やサプライチェーン強靭性など、あらゆる分野での経済安全保障施策の進展を示すものだった[90]。

また、2022 年 7 月 29 日には、日米経済政策協議委員会（経済版 2+2）が開催された。外交・安全保障と経済を一体として議論する枠組みとして共同声明を発出し、重要・新興技術及び重要インフラの促進と保護やサプライチェーンの強靭化の強化などの経済安全保障を念頭に置いたルールに基づく国際経済秩序の形成に向けて協力することに合意した[91]。

2　豪州

2022 年 10 月 22 日、岸田内閣総理大臣は豪州のパースでアルバニージー・豪州連邦首相と日豪首脳会談を行い、共同声明を発出した。当声明には、経済安全保障協力が明記され、サプライチェーン強靭化や重要・新興技術政策、サイバーセキュリティについての協力を深化させることを合意した[92]。また、同日に署名された安全保障協力に関する日豪共同宣言においても経済安全保障の促進が明記され[93]、さらに、経済産業省と豪州・産業科学資源省及び外務貿易省により、「重要鉱物に関するパートナーシップ」が署名された[94]。

---

[89] 外務省、「日米首脳共同声明『自由で開かれた国際秩序の強化』」、2022 年 5 月 23 日、4-5 頁。［https://www.mofa.go.jp/mofaj/files/100347254.pdf］、（2023 年 1 月 8 日閲覧）。
[90] 外務省、「ファクト・シート：日米競争力・強靭性パートナーシップ」、2022 年 5 月 23 日。［https://www.mofa.go.jp/mofaj/files/100347258.pdf］、（2023 年 1 月 8 日閲覧）。
[91] 外務省、「日米経済政策協議委員会共同声明　経済安全保障とルールに基づく秩序の強化（仮訳）」、2022 年 7 月 29 日。［https://www.mofa.go.jp/mofaj/files/100376269.pdf］、（2023 年 1 月 8 日閲覧）。
[92] 外務省、「日豪首脳共同声明」、2022 年 10 月 22 日。［https://www.mofa.go.jp/mofaj/files/100410295.pdf］、（2023 年 1 月 8 日閲覧）。
[93] 外務省、「安全保障協力に関する日豪共同宣言」、2022 年 10 月 22 日。［https://www.mofa.go.jp/mofaj/files/100410297.pdf］、（2023 年 1 月 8 日閲覧）。
[94] 経済産業省、「豪州・産業科学資源省及び外務貿易省と重要鉱物に関するパートナーシップを締結しま

3 QUAD

QUAD は、基本的価値を共有し自由で開かれた国際秩序の強化にコミットするべく作られた日米豪印の 4 か国による戦略対話の枠組みである。

2022 年 5 月 24 日、東京で日米豪印首脳会合が行われ、共同声明などが採択された。

とりわけ、サイバーセキュリティに関しては「日米豪印サイバーセキュリティ・パートナーシップ」を立ち上げ、「デジタル化が一層進展し高度なサイバー脅威が存在する世界において、サイバーセキュリティを向上させる必要性を認識する[95]」とし、重要インフラのサイバーセキュリティやサプライチェーンリスクのマネジメント、ソフトウェアセキュリティ及び人材育成の発展に向けた強化について協力することとしている[96]。

また、重要・新興技術に関しては「日米豪印サプライチェーンに関する原則の共同声明」を発表した。当声明では、重要技術による経済的繁栄とリスクをもたらす可能性について言及し、セキュリティ・透明性・自律性と健全性を柱とした安全でかつ持続可能な技術サプライチェーンの構築を追求することとしている[97]。

4 IPEF

2022 年 5 月 23 日、インド太平洋地域の持続可能で包摂的な経済成長を実現する目的の下、日本・米国・韓国・インド・豪州・ニュージーランド・ブルネイ・タイ・マレーシア・インドネシア・フィリピン・シンガポール・ベトナム・フィジーの 14 か国でインド太平洋経済枠組み（IPEF：Indo-Pacific Economic Framework）を立ち上げた。同年 9 月には閣僚声明が採択され、そのなかでもサプライチェーンにおいては重要分野における強靭性の確保等が言及される[98]など、中国を念頭に置いた経済安全保障施策が進んでいる。

5 G7

2022 年 6 月にドイツで開催された G7 エルマウサミットで発表された G7 コミュニケにおいては、「経済安全保障に関する我々の既存の協力を評価しつつ、この問題に関する G7 としての進展中の戦略的協調にコミットする[99]」との記載がある。

2023 年は我が国が議長国であるが、西村経済産業大臣は「今年の G7 は経済安保の強化が

した」、2022 年 10 月 25 日。
［https://www.meti.go.jp/press/2022/10/20221024002/20221024002.html］、（2023 年 1 月 21 日閲覧）。

[95] 外務省、「日米豪印サイバーセキュリティ・パートナーシップ：共同原則」、2022 年 5 月 24 日。
［https://www.mofa.go.jp/mofaj/files/100347891.pdf］、（2023 年 1 月 21 日閲覧）。

[96] 同上。（2023 年 1 月 21 日閲覧）。

[97] 外務省、「重要技術サプライチェーンに関する原則の共同声明」、2022 年 5 月 24 日。
［https://www.mofa.go.jp/mofaj/files/100347970.pdf］、（2023 年 1 月 21 日閲覧）。

[98] 経済産業省、「繁栄のためのインド太平洋経済枠組み　柱２　閣僚声明」、2021 年 9 月 13 日。
［https://www.meti.go.jp/press/2022/09/20220913006/20220913006-14.pdf］、（2023 年 1 月 9 日閲覧）。

[99] 外務省、「G7 首脳コミュニケ」、2022 年 6 月 28 日。
［https://www.mofa.go.jp/mofaj/files/100376624.pdf］、（2023 年 1 月 9 日閲覧）。

最大のテーマとなる。同志国の連携がこれまでになく重要だ[100]」としており、G7 での経済安全保障施策の進展が期待される。

以上、本章では我が国の経済安全保障施策をテーマに、第 1 節では国内での経済安全保障の動向、第 2 節では我が国の経済安全保障施策、第 3 節では国際社会との連携による経済安全保障施策を概観した。経済安全保障の考えは以前からあったものの、具体的施策については近年に集中している。今後、施策を深化させていく局面となるため、政府の動向に注目する必要がある。

[100] JIJI.COM、「日米首脳、経済安保強化で合意へ　G7 主導、中ロ念頭」、2023 年 1 月 11 日。［https://www.jiji.com/jc/article?k=2023011000833&g=pol］、（2023 年 1 月 11 日閲覧）。

第 2 部　我が国の経済安全保障の確保に向けた政策提言

以降、前述したように、第 1 章ではサプライチェーン分野、第 2 章ではサイバーセキュリティ分野、第 3 章では経済インテリジェンス分野において、現状分析・課題抽出・政策提言の流れの下に我々の考えを述べていく。

第 1 章　サプライチェーン分野での政策提言

第 1 節　総論

サプライチェーンは、「ある製品を生産するための各工程のつながり」であり[101]、製品によるものの、一国内で完結するものだけでなく、自動車産業のように複数国間にまたがるものも存在する。現在では、科学技術の進展、グローバル化の深化により、多くの産業で複数国間にわたるサプライチェーンが構築され、多様化していったが、その結果、世界各国・地域で重要な物資を外部に過度に依存することによる供給リスクが顕在化している[102]。

そして近年、各国では、今後需要が大きく見込まれる物資のサプライチェーンについて、その強靭化を図る動きを見せている[103]。

我が国は、経済安全保障推進法第 6 条により、国は特定重要物資を指定し、その安定供給の基本指針を定めるものとした。この特定重要物質については、政令により、特定重要物資には、「半導体」、「工作機械・産業用ロボット」、「クラウドサービス」、「船舶関連部品」、「重要鉱物」、「永久磁石」、「航空機部品」等が指定されている。

しかし、密接な経済相互依存関係が構築されている中で、地政学的リスクが顕在化した場合、どのような形で供給不安が生じてしまうのだろうか。また、現在のところ、各品目の具体的な供給確保計画は立てられていないが、具体的にはどのような方策をとるべきだろうか。我が国が強みを持つ物品と特定国に依存しなければならない物品では、対応策にどのような共通点と相違点があるのだろうか。そこで、本章では、地政学的リスクを念頭に、特に我が国の産業に不可欠で、性質が異なる 2 品目について、そのサプライチェーンの強靭化の施策を提言する。

まず、第 2 節では、これまでの経済相互依存に関して考察しつつ、我が国を取り巻く地政学的リスクに関して現状分析を行い、課題として、供給が特に不安視される 2 品目を特定する。第 3 節、第 4 節では、特定した 2 品目に関し、品目ごとの現状の分析を行いつつ、具体的なサプライチェーンの強靭化について提言する。第 5 節では、総括として 2 品目の比較を行う。

---

[101] 樋口修、「本調査の趣旨と報告書の構成」『変化する国際環境と総合安全保障 総合調査報告書』、［https://dl.ndl.go.jp/view/download/digidepo_12198931_po_2020302.pdf?contentNo=1］、（2023 年 1 月 24 日閲覧）。

[102] 内閣府、「特定重要物資の安定的な供給の確保に関する基本指針」、3 頁。（2023 年 1 月 24 日閲覧）。

[103] 同上、3 頁。（2023 年 1 月 24 日閲覧）。

第2節　サプライチェーンの現状分析と特に課題視される品目

1　地政学的リスクの顕在化

近年、地政学的リスクによる供給問題がサプライチェーンに大きな影響を与える事態が発生している。例えば、2022 年のロシアによるウクライナへの軍事行動により、欧州への天然ガス供給[104]や中東及びアフリカ諸国の食糧供給[105]が一時停止したことは記憶に新しい。一方で、我が国の周辺環境も日々悪化している。

中国・習近平主席は中台統一に関して、武力行使を否定しない旨を表明し[106]、2022 年 8 月には台湾封鎖などを念頭においた大規模演習が行われた[107]。また、中国は一部の国に対し経済制裁を行っている。2020 年には、豪州による、コロナウイルスの流行に対する中国の対応に関する調査と、5G 通信インフラへの HUAWEI の排除を契機に、中国は豪州産の大麦、ワイン、その他の商品に関税を課し、豪州の牛肉と石炭の輸入を停止した[108]。2021 年 3 月には、台湾に対し台湾産パイナップルの輸入通関申告の受け付けを 3 月 1 日から暫時停止した[109]。

さらに米議会の米中経済・安全保障委員会の 2022 年次報告書[110]では、習近平主席の権力集中が強まっており、それをリスクとして認識している。このことから、台湾をめぐり、地政学的対立の可能性が増しているといえる。米国政府も中国を「既存の国際秩序を再構築する意図を持ち、経済・軍事・外交・技術でそれを行う唯一の競争相手」と位置付けている[111]。2022 年 10 月上旬には、中国向けの半導体・スパコン分野では、輸出管理規制を著しく強化し、半導体製造装置等の実質的な禁輸をする等の制裁に近い異例の措置を打ち出した。

我が国も、2022 年 12 月に「国家安全保障戦略」が閣議決定され、中国を「我が国の平和と安全及び国際社会の平和と安定を確保し、法の支配に基づく国際秩序を強化する上で、こ

---

[104] BBC、「ロシア国営ガスプロム、EU への送ガス停止延長」、2022 年 9 月 3 日、[https://www.bbc.com/japanese/62776665]、（2023 年 1 月 24 日）。

[105] 日本経済新聞、「WTO、危機下で分断鮮明　閣僚会議開幕　ウクライナ連帯、加盟国 3 分の 1 どまり　物流や食料など利害対立」、2022 年 6 月 14 日、[https://www.nikkei.com/article/DGKKZO61679070T10C22A6EP0000/]、（2023 年 1 月 24 日）。

[106] 読売新聞オンライン、「中台統一へ習氏「武力行使を決して放棄しない」…共産党大会開幕」、2022 年 10 月 17 日、［https://www.yomiuri.co.jp/world/20221017-OYT1T50007/］、（2023 年 1 月 22 日閲覧）。

[107] 読売新聞オンライン、「中国軍が「台湾封鎖」大規模演習開始…弾道ミサイル 11 発発射、5 発が日本ＥＥＺ内に落下」、2022 年 8 月 4 日、［https://www.yomiuri.co.jp/world/20220804-OYT1T50208/］、（2023 年 1 月 22 日閲覧）。

[108] Gary Clyde Hufbauer (PIIE), Euijin Jung (PIIE), “China plays the sanctions game, anticipating a bad US habit,” December 14, 2020, https://www.piie.com/blogs/china-economic-watch/china-plays-sanctions-game-anticipating-bad-us-habit, accessed January 27, 2023.

[109] JETRO、「税関総署、3 月 1 日から台湾産パイナップル輸入を暫時停止」、2021 年 3 月 3 日。[https://www.jetro.go.jp/biznews/2021/03/9e86e9b7eeb3b346.html]、（2023 年 1 月 27 日閲覧）。

[110] U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, *2022 REPORT TO CONGRESS*, November 2022, https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf, accessed January 25, 2023.

[111] White House, *NATIONAL SECURITY STRATEGY*, October 2022, p.23, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf, accessed January 25, 2023.

れまでにない最大の戦略的な挑戦」と位置付けた[112]。さらに、「国家防衛戦略」では、「国家の意思決定過程が不透明であれば、脅威が顕在化する素地が常に存在する。」と指摘している[113]。

地政学について慶應義塾大学法学部教授の細谷雄一氏は「国際関係を考える際、海洋や、大陸、半島、島嶼というような地理的な条件に注目して、それをグローバルな広域的視野から行う思考であり戦略」と述べている[114]。米中間の貿易摩擦の激化は、米中の戦略によって引き起こされる地政学的対立と評される。このような地政学的対立のリスク（地政学的リスク。以下、「地政学的リスク」という）が我が国の経済に影響を与えた実例として、2010 年の尖閣諸島漁船衝突事故を契機とする「レアアース(Rare Earth Elements。以下、「REE」という)、タングステン及びモリブデンの輸出規制措置」が挙げられる。この措置により、我が国への REE 輸出が停滞した。これにより、REE を原材料・部品等に用いる日本企業は大きな影響を受けた。

中国による「REE、タングステン及びモリブデンの輸出規制措置」は 2014 年 8 月、上級委員会報告書を受けて、WTO の紛争解決機関が、中国の措置を違法と認定し、協定に整合的にするよう中国に勧告した[115]。中国は WTO の勧告に従い、輸出制限措置を 2015 年 5 月 1 日から撤廃した[116]。国は重要資源である REE 等の安定供給の確保のみならず、一部の資源国の保護主義的な動きを牽制する観点からも意義深いとしている[117]。他国に生産を依存する製品の供給問題が我が国の産業や国民生活に大きな影響を及ぼし、他国に行動を変容させられるという問題を提起した。

地政学的リスクが顕在化した前例がある中、我が国周辺では、中国及びロシアといった、意思決定過程が不透明な国々が存在する以上、今後、地政学的リスクはサプライチェーンに大きな影響を及ぼす可能性が高い。

2　経済相互依存とその武器化

冷戦終結以降、自由貿易体制が旧共産主義諸国まで広がり、我が国を含む先進的民主主義国家は、自由、民主主義、基本的人権の尊重、法の支配といった普遍的価値を擁護し、共存共栄の国際社会の形成を主導し、その前提の下で、多くの国が国際社会の平和と安定と経済

---

112 内閣官房、「国家安全保障戦略」、9 頁。（2023 年 1 月 21 日閲覧）。
113 内閣官房、「国家防衛戦略」、2022 年 12 月、5 頁。
［https://www.cas.go.jp/jp/siryou/221216anzenhoshou/boueisenryaki.pdf］、（2023 年 1 月 21 日閲覧）。
114 北岡伸一・細谷雄一、『新しい地政学』、40 頁。
115 外務省、「外交青書 2015」、2015 年 4 月、233 頁。
[https://www.mofa.go.jp/mofaj/gaiko/bluebook/2015/pdf/pdfs/3_3.pdf]、（2023 年 1 月 27 日閲覧）。
116 経済産業省、「通商白書 2015」、2015 年 8 月、311 頁。
[https://www.meti.go.jp/report/tsuhaku2015/2015honbun_p/pdf/2015_03-01-04.pdf］、（2023 年 1 月 21 日閲覧）。
117 同上、311 頁。

発展の果実を享受してきた[118]。このことは、世界の GDP の成長からも窺える。

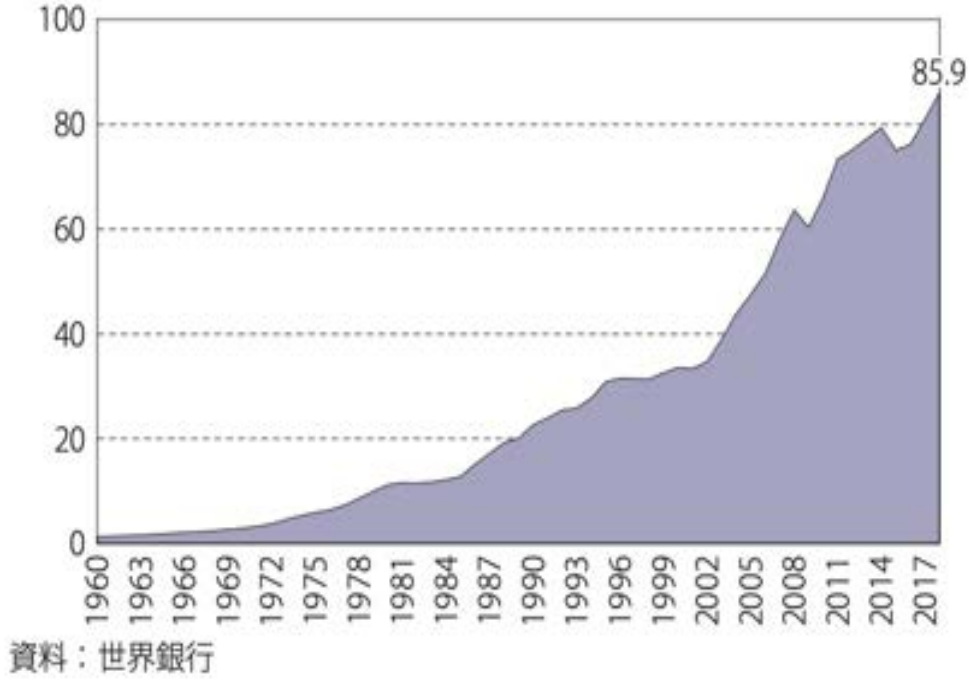


図 7　世界 GDP の推移
出典:通商白書 2020

3　課題抽出

グローバリゼーションと経済相互依存の深化は国際社会の平和と繁栄をもたらした。その結果、世界の隅々にまで経済のグローバリゼーションが完全に浸透し、国民生活は多くを他国経済に依存するようになったため、米中対立が生じている中でも、世界経済、米国経済と中国経済を切り離すことはできない[119]。そのため、かつて相互に密接な経済関係を有していなかった米ソ両国の冷戦と異なり、直接武力衝突に移るとは限らず、経済分野における様々な措置を通じて相手に影響を与え、国家の戦略的目標を達成しようとする手段が用いられるようになった[120]。これを「エコノミック・ステイトクラフト（Economic Statecraft。以下、「ES」という。）」と呼ぶ[121]。事実、豪州や台湾に対する経済制裁のように、中国は経済的手段を用いて、自国の戦略的利益を維持・拡大しようとしている[122]。

---

[118] 内閣官房、「国家安全保障戦略」、3 頁。（2023 年 1 月 10 日閲覧）。
[119] 宮本雄二・伊集院敦・日本経済研究センター、『米中分断の虚実』、20-21 頁。
[120] 鈴木一人「エコノミック・ステイトクラフトと国際社会」村山編著『米中の経済安全保障戦略』、芙蓉書房出版、2021 年、10 頁。
[121] 東京大学公共政策大学院教授の鈴木一人氏は、「エコノミック・ステイトクラフト」とは、経済的手段を用いて自らの政治的意志を強制し、国家戦略上の目標を実現することと定義づけている。同上、11 頁。
[122] 久野新、「中国の経済制裁：その特徴と有効性」、2021 年 4 月 20 日、1 頁。[https://www.jfir.or.jp/wp/wp-content/uploads/2021/04/210420Kunoa.pdf]、（2023 年 1 月 27 日閲覧）。

ES が効果的に発揮されるためには、グローバル・サプライチェーンの中で、特定の国家が生産する品目に対して、ES の対象国が強度に依存している状態にある必要がある[123]。例えば、第四次中東戦争時にアラブ諸国が西側諸国に対して原油禁輸措置を行い、原油価格を高騰させ、各国に経済的混乱が生じたことが実例として挙げられている[124]。

ES に対して、我が国が影響を受けないためには、依存する分野を減らす必要がある。さらに、相手国が我が国に依存させることで、我が国が ES を手段として用いて、戦略的に主導権を握ることができる。

そのため、我々は我が国が依存する分野と強みを有している分野をヒアリング調査・文献調査等を通して分析し、下の評価基準を設けて検討した。なお、特定重要物資には 2022 年 5 月の段階では REE、蓄電池、医薬品、半導体の 4 品目が予想されていた[125]。

① 国民の生存に必要不可欠、または広く国民生活もしくは経済活動が依拠している重要な物質[126]。
② 外部に過度な依存、または依存するおそれがある物質[127]。特に我々が注目した社会動向である「デジタル化」及び「低炭素社会」に必要な物質。
③ 外部から行われる供給途絶等の蓋然性が高い物質[128]で、特に我々が着目している地政学的リスクの影響を受ける物資。
④ 「経済安全保障推進法」の適用を受ける必要のある物質[129]。

我々は以上の 4 点を満たす物品として、ジスプロシウムと半導体に注目した。

第一に、ジスプロシウムである。ジスプロシウムは、自動車産業等様々な業界で使用され、さらに、次世代自動車(EV 等)のモーターに使われるネオジム磁石の製造に欠かせない。そもそも、天然資源は地理的偏在性が高く、容易に多角化をすることはできない。その上、ジスプロシウムを多く含む鉱石の鉱床は中国南部に集中しており、世界の製錬量のほぼ 100%

---

123 鈴木、「エコノミック・ステイトクラフトと国際社会」、18 頁。
124 同上、18 頁。
125 朝日新聞、「（時時刻刻）規制・支援、見えぬ全容　経済安保法」、2022 年 5 月 12 日。[https://www.asahi.com/articles/DA3S15291154.html]、（2023 年 1 月 26 日閲覧）。
126 国民の生存に不可欠、または広く国民生活もしくは経済活動が依拠している重要な物質であるかの判断に当たっては、事象の重大性、影響範囲及び代替が困難であることを考慮する。内閣府、「特定重要物資の安定的な供給の確保に関する基本指針」、10-11 頁。（2023 年 1 月 25 日閲覧）。
127 外部に過度に依存する物資、またはその恐れのある物質とは、供給が特定少数国・地域に偏っており、当該特定少数国・地域からの供給途絶が発生した場合に甚大な影響が生じ得るものを指す。外部に過度に依存するおそれがある物資とは、将来の動向を踏まえ、依存するリスクのあるものを指す。同上、11-13 頁。（2023 年 1 月 25 日閲覧）。
128 物資後との状況や外交・安全保障環境等の様々な要因を踏まえ、地域による輸出の停止・制限、当該供給国・地域内への優先的な供給の実施、 生産抑制につながる制限の導入・強化等、外部から行われる行為により想定される供給途絶等のリスクを想定している。同上、11-13 頁。（2023 年 1 月 25 日閲覧）。
129 他制度による措置が行われていないもの、近年供給途絶が発生した実績があるもの、または将来の社会動向を踏まえ中長期的に戦略的重要性があるものとされる。同上、13-14 頁。（2023 年 1 月 25 日閲覧）。

が中国に集中している[130]。また、ジスプロシウムはREEの一種であり、REEは中国による輸出規制措置で我が国が供給途絶を受けた物質である。

そのほかの重要鉱物であるLi(リチウム)及びNi(ニッケル)、そしてCe(セリウム)等の軽希土類鉱石は、現在米国や豪州で開発・生産のプロジェクトが開始されている[131]、または生産されている[132]ことから除外した。また、Tb（テルビウム）といったそのほかの重希土類鉱石は、我々が注目した「デジタル化」や「低炭素技術」に用途がない[133]ことから除外した。

第二に、半導体である。半導体は「産業のコメ」と呼ばれ、あらゆる身近な電子機器に使用されているだけでなく、5G 等のデジタル社会を支える基幹部品であり、国民生活や産業にとって必要不可欠である。そして、半導体の輸入割合は約 79%と外部に過度に依存しており、かつ、主な輸入先も台湾、中国、米国と限定的である[134]。また、半導体の高性能化は省エネ化に直結し[135]、「低炭素社会」の実現に資すると言える。

また、半導体は実際にコロナ禍で、特定の国での工場の停止、輸出入の制限による供給途絶が起こった。また、最先端半導体を製造する技術を有していることから近年注目されているTSMCは台湾企業であり、中台統一といった地政学的なリスクを抱えている[136]。

本2品目の対照的な供給確保・国際連携のスキームは、今後、その他の品目で安定供給を確保する上で、大きな参考となるだろう。本研究ではこの2品目に着目し、供給確保の方策を提言する。

第3節　ジスプロシウムの供給確保についての提言

1　意義

(1)　ジスプロシウムについて

ジスプロシウム（Dysprosium。以下、「Dy」という。）とは、原子番号 66 番の元素で、REEの一種である。 REEは、低炭素エネルギー技術に必要な鉱石とされる[137]。Dyは、グリ

---

[130] 経済産業省、「半導体に係る安定供給確保を図るための取組方針」、2023年1月19日、7頁。［https://www.meti.go.jp/policy/economy/economic_security/semicon/torikumihousin_semicon.pdf］、（2023年1月26日閲覧）。

[131] LiやNiは我が国の各鉱種クリティカリティ強度を見ると、脅威国からの依存度は25%以下とされる。一方でレアアースは脅威国からの依存度は25%を超える。MUFG、「レアアース(希土類)の需給動向 と今後の展開可能性について」、2021年9月26日、11頁。［https://www.cistec.or.jp/jaist/event/kenkyuutaikai/kenkyu32/02-01-shimizu.pdf］、（2023年1月25日閲覧）。

[132] 軽希土類鉱石は豪・Lynas社がMt. Weldから生産している。

[133] そのほかの重希土類鉱石は主にレーザー関係など多様な用途がある。福田一徳『日本と中国のレアアース政策』、木鐸社、2013年、18頁。

[134] 経済産業省、「半導体に係る安定供給確保を図るための取組方針」、2023年1月19日。［https://www.meti.go.jp/policy/economy/economic_security/semicon/torikumihousin_semicon.pdf］、（2023年1月26日閲覧）。

[135] 同上。（2023年1月26日閲覧）。

[136] 同志社大学教授兼原信克氏に対するヒアリング調査（2022年8月26日実施）。

[137] Benjamin K. Sovacool, et al., “Sustainable minerals and metals for a low-carbon future,” *Science*, January 3, 2020, https://www.science.org/doi/10.1126/science.aaz6003, accessed January 23, 2023.

ーン技術に重要な用途を持つ重希土類元素(Heavy Rare Earth Elements。HREEs という。)で、ネオジム磁石の製造に欠かせない。一般的に Dy の添加によって、ネオジム磁石の高温化での性能を保ち、優れた磁気性能を維持できるようにする。また、ネオジム磁石は永久磁石の中で磁力と保磁力に一番優れている[138]。

ネオジム磁石は永久磁石であるが、その用途は多岐にわたる。最も重要な用途として、次世代自動車のモーターへの使途が挙げられる。そのほかにも PC の HDD 等にも用いられる。

(2)　Dy の供給確保の戦略的意義

Dy を優先的に確保する必要があることは以下 4 点の理由によるものである。

第一に、ネオジム磁石の需要はますます拡大すると予想されるからである。

我が国では電動車の販売を 20 年に目指している。我が国は 2030 年 4t 以下の乗用車の 8 割を電動車に、2035 年には 100%を電動車に、2050 年にはカーボンニュートラルを目指している。なおかつ、世界各国も EV への転換を進めており、導入目標を設定している。

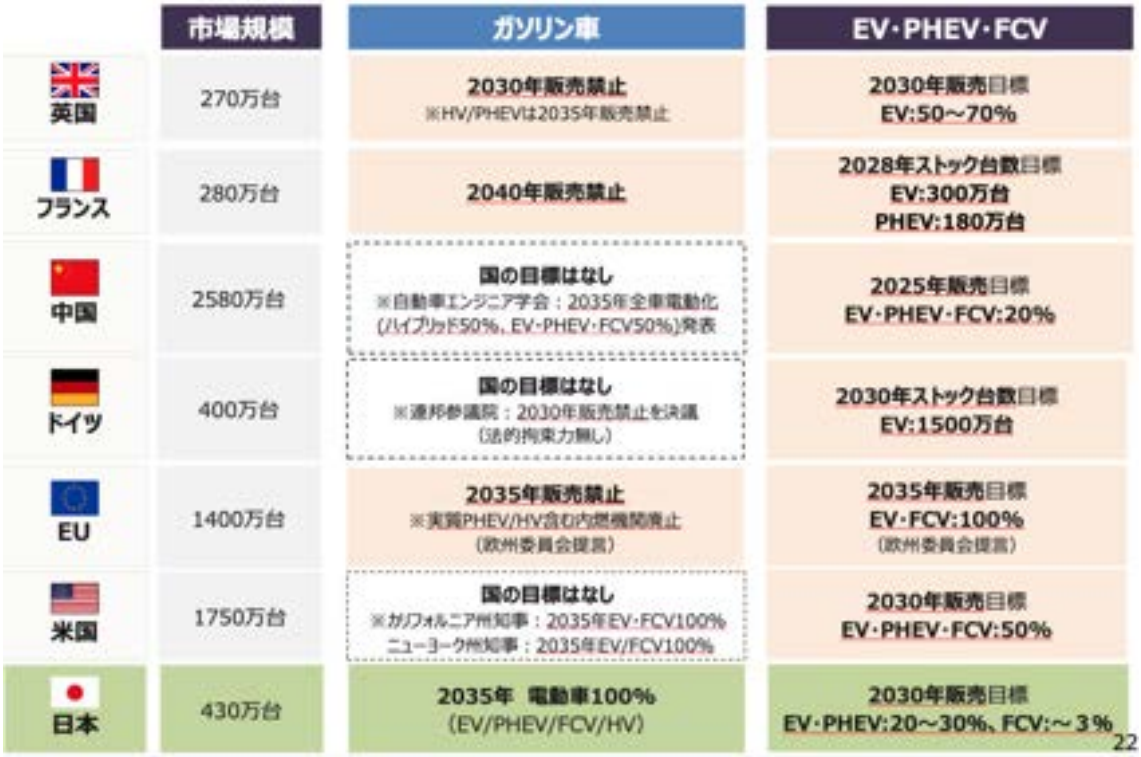


図 8　各国の電動自動車の導入目標

出典：経済産業省

また、BCG の調査[139]によると今後、世界の新車販売台数は 100 万台を超え、その半分以上

[138] 株式会社　相模化学金属、「ネオジム磁石の特徴」。［https://www.sagami-magnet.co.jp/explanation-magnet/feature-neodymium］、（2023 年 1 月 21 日閲覧）。

[139] BCG、「世界の電動車（xEV）シェアは 2030 年に 51%へ。日本では 2030 年に 55%、ハイブリッド車が

が電動自動車にあたると予測している。

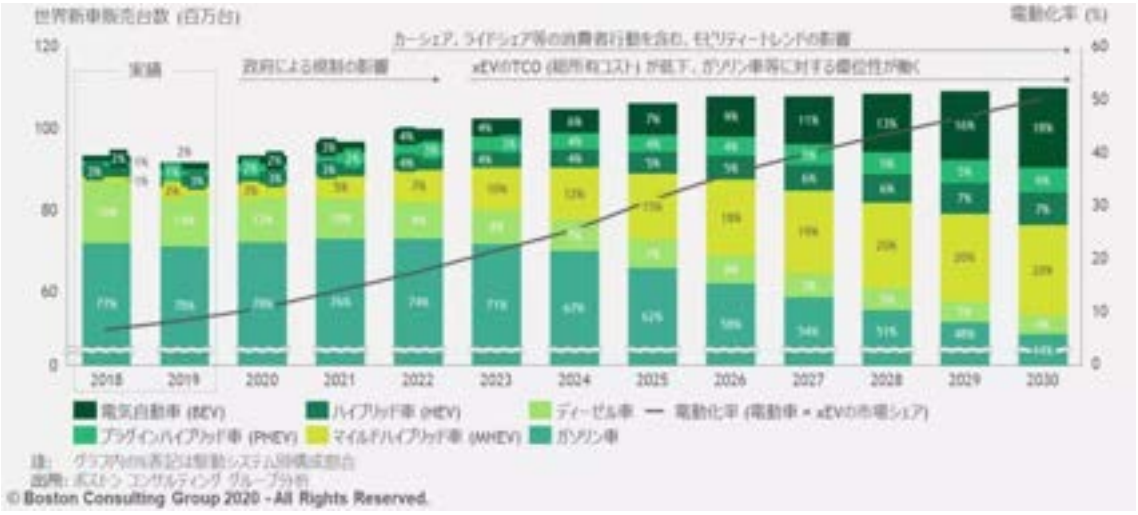


図 9　電動車の新車販売台数の将来予測(BCG 作成)

出典:BCG

ゆえに、EV 等は今後も需要が増え続けることから、Dy の低減・代替技術の進展なしには Dy の需要量も必然的に増加する。

加えて、ネオジム磁石を含む永久磁石は高性能モーターに使われるため、グリーン技術の要ともなる。事実、経済産業省では、半導体を脳、電池を心臓、モーターを筋肉と、重要な要素に位置付けており[140]、重要性が増している。

第二に、我が国は Dy の供給を完全に中国に依存しているからである。Dy はイオン吸着鉱から多量に生産できるが、この鉱石は世界では中国南部の鉱山でしか生産していない[141]。各国でも Dy を含む鉱石は存在するものの、イオン吸着鉱に比べ、その量はわずかである。

さらに、Dy といった REE の分離精製工程では、放射性物質が発生する[142]。そのため、分離精製工程を行う際、除去コストがかかり、製品に価格が転嫁される。また、REE 分離精製工場は中国を除くと、マレーシアに Lynas 社・Kuantan 工場があるが、本工場は建設にあた

引き続きシェアを維持～BCG 調査」、2020 年 1 月 10 日。［https://www.bcg.com/ja-jp/press/10january2020-electric-car］、（2023 年 1 月 21 日閲覧）。

[140] 経済産業省、「特定重要物資の指定について」、2022 年 11 月。［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai4/siryou1.pdf］、（2023 年 1 月 23 日閲覧）。

[141] 中国以外でも南米やマダカスカル等で同様の鉱石は発見されているものの、環境負荷が未知数であること、生産コストの問題から開発まで至っていない。渡辺寧、「レアアースから見た鉱物資源供給の将来像」、2018 年 8 月。［https://www.jstage.jst.go.jp/article/shigenchishitsu/66/1/66_27/_pdf］、（2023 年 1 月 21 日閲覧）。

[142] 加藤泰浩『太平洋のレアアース泥が日本を救う』、PHP 新書、2021 年、64-70 頁。

って、住民運動が起きている[143]。なお、従来、REE は米国・豪州が世界の生産量の大部分を占めていたが､環境問題について規制されていなかった中国が安いコストで REE を生産し、供給したことで、米国・豪州の鉱山は閉山に追い込まれた。

今後地政学的対立に加え、後述の通り、中国の国内需要の増加により、中国が Dy の輸出制限を課す可能性は高い。さらに、中国では環境規制を強化し、HREEs の生産量を減らしているため、分離・精製技術をより強力な武器とする傾向が指摘されている[144]こと、海外の鉱山権益を獲得する行動に出る可能性もあること[145]が挙げられる。

第三に、ネオジム磁石は他の特定重要物資の部品であるからである。「工作機械・産業用ロボット」、「船舶関連部品」、「永久磁石」、「航空機部品」にはネオジム磁石が部品として使われている。

第四に、ジスプロシウムを低減させる技術は開発されている[146]が、実用化まで至っていないからである。長期的にはこれらの技術が実用化される可能性が高いが、短期的には期待できない。

以上の 4 つの理由から、早急に我が国が Dy を安定的に確保できるようにしなければならない。かつ、長期的には Dy 低減・代替技術といった、Dy の使用量を減らしたネオジム磁石の供給を可能とする方策も取らなければならない。

2　現状分析

(1)　Dy のサプライチェーン

我が国は Dy の供給を完全に中国に依存している。以下はそのフローである。

---

[143] マレーシアでの Lynas 社工場の建設反対運動の経緯については以下の論文に詳しい。和田喜彦、「レアアース製錬に伴うトリウム等の放射性廃棄物管理に関する一考察 : エィジアンレアアース(ARE)社事件, ライナス社問題を事例として」、2014 年 3 月 20 日。
［https://doshisha.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=27419&item_no=1&page_id=13&block_id=100］、（2023 年 1 月 22 日閲覧）。
なお、2022 年 9 月 5 日の JOGMEC「ニュース・フラッシュ」によると、同年 8 月に、マレーシア当局は Lynas 社事業に反対する活動家の訴えに基づき、本工場を司法審査の対象とした。JOGMEC、「マレーシア : Lynas 社、Kuantan 選鉱施設における浸出精製残留物の永久処分施設が司法審査の対象に」、2022 年 9 月 5 日、［https://mric.jogmec.go.jp/news_flash/?me=レアアース/希土類］、（2023 年 1 月 22 日閲覧）。

[144] 角田昌太郎、「サプライチェーンの安全保障―米中対立下の懸念と米国が主導する経済的連携―」『変化する国際環境と総合安全保障 総合調査報告書』、2022 年 3 月 25 日、63 頁。（2023 年 1 月 27 日閲覧）。

[145] 下の論文では、3.6.3 において、今後増加する中国の Dy 需要を満たすために、海外鉱山権益の獲得を提案している。Qiao-Chu Wang, et al., ”Illustrating the supply chain of dysprosium in China through material flow analysis,” *Resources, Conservation and Recycling*, September 2022, [https://www.sciencedirect.com/science/article/pii/S0921344922002610#bib0075], accessed January 22, 2023.

[146] NEDO、「高性能磁石向けジスプロシウムの使用量 4 割削減に成功」、2010 年 12 月 27 日。
[https://www.nedo.go.jp/news/press/ZZ_0515A.html]、（2023 年 1 月 22 日閲覧）。

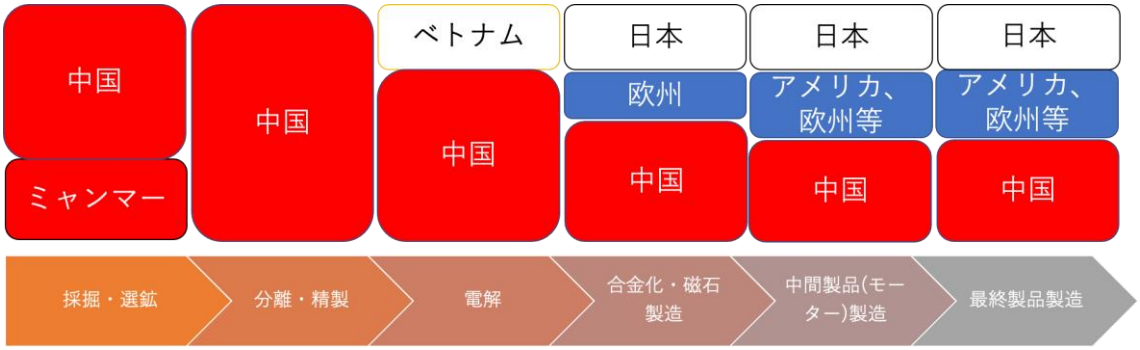


図 10　Dy をめぐるフロー
出典:JOGMEC 公開資料より筆者作成

中国は Dy の生産で支配的地位にある[147]。Dy を多く含む鉱石の鉱床は中国南部の鉱山に集中しており、資源の偏在性や技術力、 コストの問題等から世界の製錬量のほぼ 100%が中国に集中している[148]。また、分離・精製においては、完全に中国に依存しており、合金化も大きなシェアを占めている[149]。なお、合金化以降の工程は我が国や有志国がシェアを有している[150]。

(2)　Dy のリスク

今後の Dy の需要の増加

Dy の将来的な需要量は予測[151]によると、現状の供給量の 7-22 倍程度増加すると予想されている。また、リサイクルや Dy 低減・代替技術が実用化されない場合、各国がグリーン技術の導入目標を履行した場合、Dy の需要が増加することは明白である。

中国に依存していることと近年の中国政府の動向

中国は Dy の最大の輸出国であり、消費国である。中国の国内 Dy 需要は過去 15 年間で 16

[147] Qiao-Chu Wang, et al.,"Illustrating the supply chain of dysprosium in China through material flow analysis,", accessed January 22, 2023.
[148] 経済産業省、「半導体に係る安定供給確保を図るための取組方針」、7 頁。（2023 年 1 月 26 日閲覧）。
[149] デロイト トーマツ コンサルティング合同会社、「北米におけるレアアースのサプライチェーン状況分析業務　最終報告書」、2020 年 2 月 28 日、88 頁。[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjJlrjHydr8AhU3sVYBHX3aAGsQFnoECBoQAQ&url=https%3A%2F%2Fmric.jogmec.go.jp%2Fwp-content%2Fuploads%2F2020%2F05%2Free_supply_northamerica20200228.pdf&usg=AOvVaw1C4uTFPqwocZOsobSualb4]、（2023 年 1 月 22 日閲覧）。
[150] 同上、88 頁。（2023 年 1 月 22 日閲覧）。
[151] Tobias Junne, et al.," Critical materials in global low-carbon energy scenarios: The case for neodymium, dysprosium, lithium, and cobalt," *Energy*, November 15, 2020, https://www.sciencedirect.com/science/article/pii/S0360544220316406?via%3Dihub, accessed January 22, 2023

倍に増加した[152]。主に風力発電での Dy 需要が著しい。さらに中国政府は近年、REE 業界に対し、ますます影響力を強めている。例えば、REE の生産をおこなっていた 6 大企業[153]のうち 3 社が 2021 年 12 月に統合され、4 大企業に集約された。また、中国・国務院は「レアアース管理条例案」と呼ばれる、REE の統一的な法律を制定しようとしている[154]。なお、Dy の採掘による環境汚染も深刻で、中国では環境規制が強化された。結果、以下の図のように需給ギャップが生じている。

[152] Qiao-Chu Wang, et al.,"Illustrating the supply chain of dysprosium in China through material flow analysis,", accessed January 22, 2023.

[153] 中国稀有稀土、五鉱稀土集団、中国北方稀土(集団)高科技、厦門鎢業、中国南方稀土集団、広東省稀土産業集団の 6 社。2021 年１２月には、中国稀有稀土、五鉱稀土集団、中国南方稀土集団の 3 社が「中国稀土集団」と、4 大企業に集約された。JETRO、「中国のレアアース管理に関する政策の概要と動向」、2022 年 1 月、2 頁。
[https://www.jetro.go.jp/ext_images/_Reports/01/6d50807a44f904c1/20210070_05.pdf]、（2023 年 1 月 22 日閲覧）。

[154] その内容は大まかに述べると、国務院によるレアアース共同管理メカニズムを構築し、違法採掘・生産等の罰則を規定。また、レアアース鉱山・製品の戦略備蓄を実施する内容となっている。同上、3-4 頁。

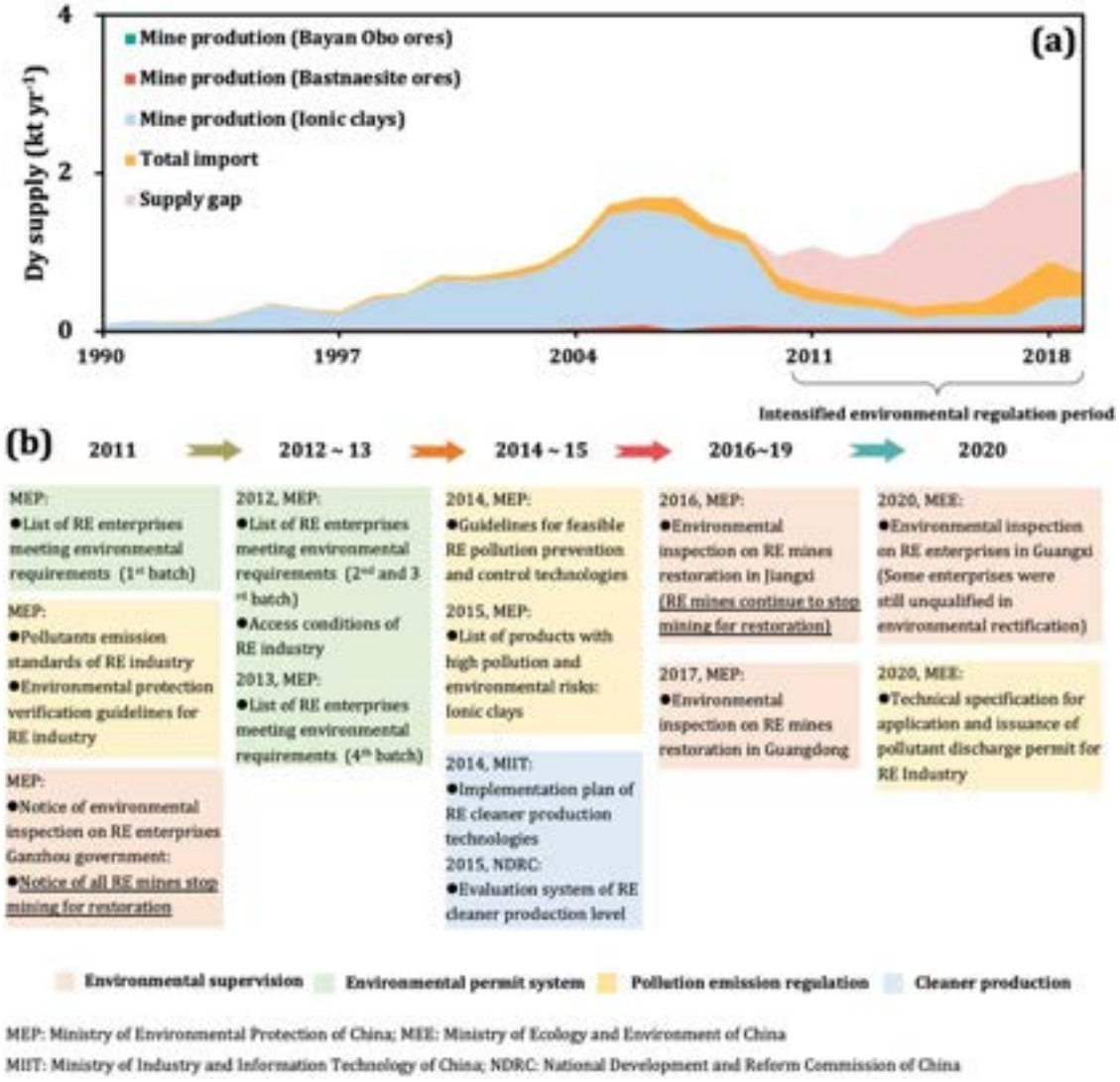


図 11　中国の生産量と規制の推移

出典：Qiao-Chu Wang, et al.

ゆえに、地政学的対立だけでなく、国内需要が増加することにより、中国が REE 輸出制限を課す可能性は高い。

（3）　現状の取り組み

ア　国の取り組み

我が国の鉱物資源政策は以下の図の通り、5 点の方向性で行っている。

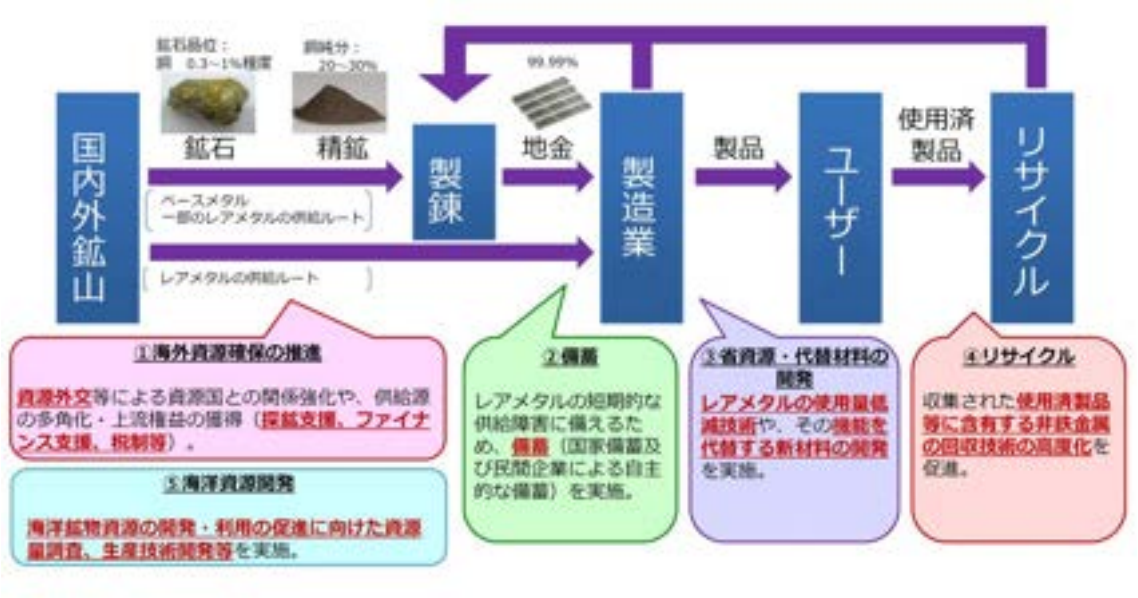


図 12　我が国の鉱物資源政策の全体像

出典：経済産業省

（ア）　海外資源確保の推進

第一に、JOGMEC の権限拡大が挙げられる。JOGMEC は近年、探鉱支援のため、鉱山ジュニア企業への投資や鉱山権益の確保を推進している。令和 2 年 6 月には、設置法令の独立行政法人エネルギー・金属鉱物資源機構法が改正され、金属鉱物の安定供給の確保に向けて、鉱山の開発や製錬事業へのリスクマネー支援(出資・債務保証)を強化した。事実、2010 年の中国による REE 実質禁輸措置においては、JOGMEC が双日と共同で会社を設立し、豪州・Lynas 社への出資を行った結果、Mt. Weld の鉱山開発が成功し、REE の長期供給契約が締結され、我が国の REE の中国依存脱却の一歩となった。また、最近では、合弁会社を設立し、ナミビアでの HREEs に関するプロジェクトを立ち上げている[155]。しかし、鉱山開発は「千三つ」、つまり、鉱山が見つかっても操業までに至るものは、千個のうちの 3 つしかないと一般的に呼ばれる[156]。

また、鉱山開発は 10～30 年と長期間かかり、莫大な資金を必要とする[157]。各国との資源開発競争が激化している中で、我が国単独で有望な鉱山を見つけ出し開発を行っていくこ

[155] Argus, “Japan aims to diversify rare earth supply,” January 3, 2023, https://www.argusmedia.com/en/news/2405752-japan-aims-to-diversify-rare-earth-supply, accessed January 22, 2023.
[156] JOGMEC シドニー事務所に対するヒアリング調査（2022 年 11 月 24 日実施）。
[157] 同上。

とは現実的に厳しい。

その中で有力な方策として期待されているのが、有志国との国際連携である。我が国は2022 年 10 月に米国主導の鉱物資源安全保障パートナーシップ（Minerals Security Partnership。以下、「MSP」という。）に参加し[158]、 2022 年 6 月に豪州と鉱物資源に関するパートナーシップを結んでいる[159]。しかし、資源輸出国内で資源ナショナリズムが高まっており、各国とも自国の権益を獲得するために独自の動きも多い。

（イ） 備蓄

備蓄に関しては、我が国では希少金属の備蓄を昭和 58 年に開始している。2020 年に改正が行われ、以下の図のようになり、以前よりも格段に強化された。

	これまで	見直しのポイント
備蓄の方針	● 国が方針を具体的に示したことはなし（主として、審議会報告書を通じて提示）	➢ 備蓄制度を国の資源確保政策の一環として着実に実施すべく、備蓄目標日数、買入・放出、情報管理等について国の方針を策定
備蓄目標日数	● 国家備蓄と民間備蓄（任意）を合わせ日数を設定 ● 一律60日分（国備42日、民備18日） ● 供給安定性が高まった一部の鉱種はこの半分の日数（30日分）	➢ 供給途絶時の「最後の手段」として、国家備蓄のみで日数を設定 ➢ 特に地政学的リスクや産業上の重要性が高い鉱種をより長くするなど、リスクの定量評価を踏まえ、よりメリハリある目標日数に
備蓄計画（国の同意）	● 買入と放出（売却）で別々に計画策定。 ● 放出については、平時の品質保持等のための入替売却、緊急時の放出とも、その都度JOGMECが計画を国の同意を得た上で策定	➢ 国の方針を踏まえ、買入・放出を統合した備蓄計画を策定 ➢ 期間は、中期計画期間を想定（必要に応じ、柔軟に見直し） ➢ JOGMECが国の同意を得た上で計画を策定
放出の機動性	● 緊急時に放出する場合も、都度、計画を策定し、国の同意を得る必要があり、放出まで時間を要する	➢ あらかじめ、国が買入・放出を含む備蓄計画を同意することで、JOGMEC判断による放出の場合の同意を不要とし、放出までの機動性を大きく向上（国は、独法評価プロセスで事後チェックする）
情報管理	● 備蓄制度に係る各種情報の取扱いが不明確	➢ 経済安全保障の確保等の観点から、具体的な備蓄目標日数、実際の備蓄量等は非公開と明確化

図 13　レアメタル備蓄制度の令和 2 年度改正までの内容と改正後の内容[160]

出典：経済産業省

---

158 外務省、「鉱物安全保障パートナーシップ（MSP）概要」、2022 年。
［https://www.mofa.go.jp/mofaj/files/100431183.pdf］、（2023 年 1 月 20 日閲覧）。

159 Prime Minister's Office of Japan, "Partnership between Japan's Ministry of Economy, Trade and Industry and Australia's Department of Industry, Science and Resources and Department of Foreign Affairs and Trade Concerning Critical Minerals," October 22, 2022, https://japan.kantei.go.jp/101_kishida/documents/2022/_00019.html, accessed January 25, 2023.

160 経済産業省、「レアメタル備蓄制度の見直しについて」、2020 年 7 月。
［https://www.meti.go.jp/shingikai/enecho/shigen_nenryo/pdf/029_05_02.pdf］、（2023 年 1 月 22 日閲覧）。

（ウ）　省資源・代替材料の開発

JST、NEDO を通して、Dy 低減のネオジム磁石[161]や、不使用のネオジム磁石[162]の開発が行われており、実用化・量産化が待たれる。

（エ）　リサイクル

リサイクルに関しては、技術の開発が行われている。

（オ）　海洋資源開発

2011 年 11 月に東京大学教授の加藤泰浩氏がレアアース泥を日本の排他的経済水域内で発見した[163]。しかし、深海にある資源であることから、実用化に向けては、資源量の把握、生産技術の確立、開発コストの削減など、様々な課題が存在し、こうした課題を一つずつ解決していくため、海洋基本計画(平成 30 年 5 月閣議決定)に基づき、関係府省が連携して取り組んでいる。

イ　経済安全保障推進法に基づく金属鉱産物の「特定重要物資」指定

2022 年 12 月、「特定重要物資」（経済安全保障推進法 7 条）として「金属鉱産物」（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施行令 1 条 10 号）が指定された。また、経済産業省は、2023 年 1 月に「安定供給確保を図るための取組方針」（同法 8 条 1 項）を作成しており[164]、当該取組方針に基づき、探鉱[165]・FS[166]支援、鉱山開発支援、製錬等事業支援、技術開発支援といった安定供給確保のための個別施策を推進していくこととなる[167]。

3　課題抽出

Dy は今後世界中で需要が増加する。Dy は資源の偏在性や技術力、 コストの問題等から世界の製錬量のほぼ 100%が中国に集中している[168]。一方で近年中国では Dy の需給ギャップが

---

[161] NEDO、「高性能磁石向けジスプロシウムの使用量 4 割削減に成功」。（2023 年 1 月 22 日閲覧）。
[162] NEDO、「世界初、ジスプロシウム不使用の省ネオジム耐熱磁石を開発」、2018 年 2 月 20 日。[https://www.nedo.go.jp/news/press/AA5_100921.html]、（2023 年 1 月 22 日閲覧）。
[163] 加藤、「太平洋のレアアース泥が日本を救う」、214 頁。
[164] 経済産業省、「重要鉱物に係る安定供給確保を図るための取組方針」、2023 年 1 月 19 日、[https://www.meti.go.jp/policy/economy/economic_security/metal/torikumihoshin.pdf]（2023 年 1 月 26 日閲覧）。
[165] 探鉱とは、リモートセンシング調査、地質調査、物理探査、ボーリング調査、鉱床の評価を経て、鉱床の規模、品位、形状を確定し、開発の可能性を技術的・経済的側面から評価することをいう。同上、13 頁。（2023 年 1 月 27 日閲覧）。
[166] FS(フィージビリティスタディ)とは、探鉱で確認された鉱床について、採掘から生産物(鉱物精鉱)販売までの実現性と採算性を調査し、事業実現性評価をすることをいう。同上、13 頁。（2023 年 1 月 27 日閲覧）。
[167] 同上、13-16 頁。（2023 年 1 月 27 日閲覧）。
[168] 経済産業省、「半導体に係る安定供給確保を図るための取組方針」、7 頁。（2023 年 1 月 26 日閲覧）。

生じていること、各種規制が強化されていることから、今後中国による供給停止の可能性は非常に高い。

我が国も需要が増加されることから、国は 5 つの方向性で対策している。そして、基本方針では、2030 年までに Dy を含む HREEs を 1200t 確保する目標を立てている。

しかし、Dy 低減・代替技術は開発され、海洋資源開発も現在取り組みが進んでいるところではあるものの、長期的に実現可能ではあるが、2030 年までに目標を達成するには、短期的に供給源の多角化が必要である。

4　政策提言

上記の課題を解決し、我が国の産業に欠かせないネオジム磁石を確保するためには、以下の方策が必要である。

(1)　政策目標

ネオジム磁石の確保のために、Dy の安定的に供給できるようにする。しかし、我が国の産業の競争力を保つために、企業には過重なコストを負担させないようにしなければならない。

(2)　提言の全体像

ネオジム磁石の安定供給の確保のためには、Dy を利用する場合と利用しない場合の二つの手段が存在する。Dy を利用する場合、現状では中国からの輸入、海洋資源開発、リサイクルの取り組みが存在する。整理すると、以下の図のような選択肢が存在する。

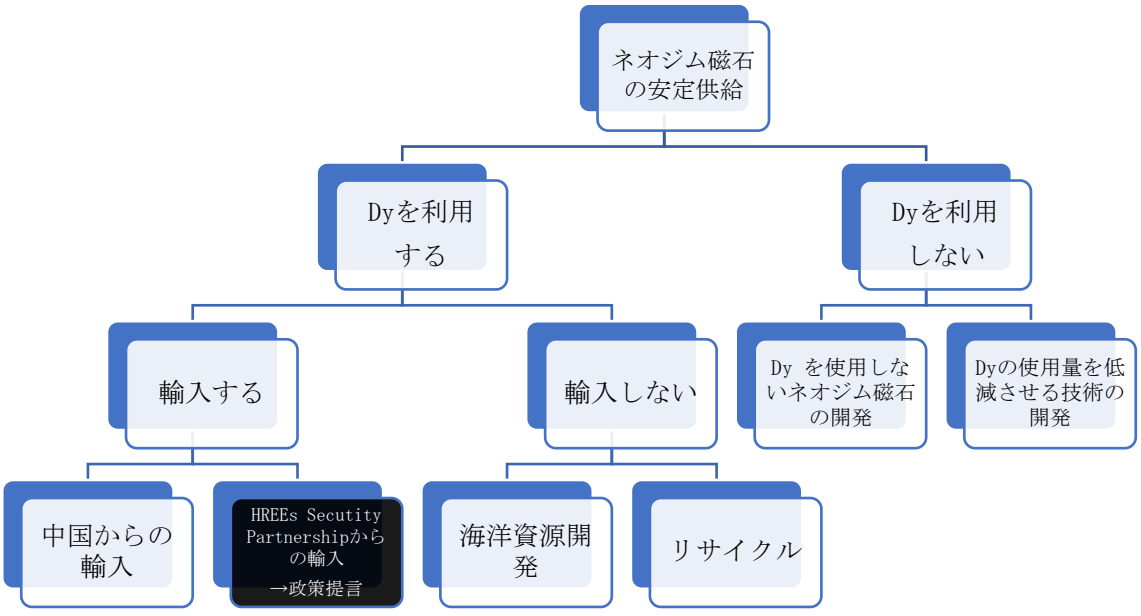


図 14　「日中間レアアース問題の原因分析と日本の対応」を参考に筆者作成

出典：伊藤昭男「日中間レアアース問題の原因分析と日本の対応」[169]より

（３）では、政策提言で中国を介在しないルートの形成について考察し、（４）、（５）では Dy の確保ルートの構築のための具体策について検討する。

(3)　政策提言“HREEs Security Partnership”の構築

ネオジム磁石のサプライチェーンにおいて、現状の中国を介在するルートからの輸入は継続するものの、有志国と協力し、有志国内や東南アジア諸国で各工程を行えるようにして、下の図のような、中国を介在しないルートの構築を目指す。その支援の枠組みとして、“HREEs Security Partnership”の設立を提言する。“HREEs Security Partnership”とは、Dy を主眼として、中国を介在しない重希土類鉱石を確保するための国際枠組みであり、二つのルートの構築を目標とする。「ア　有志国のルート」と「イ　東南アジア諸国のルート」である。なお、Dy のサプライチェーンについては、「北米におけるレアアースのサプライチェーン状況分析業務　最終報告書」[170]で用いられている工程表を用いる。

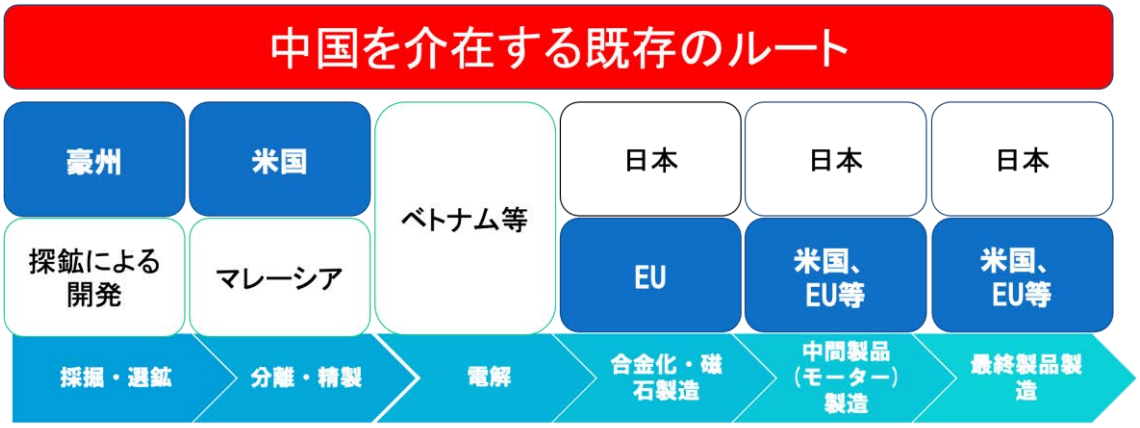


図 15　中国を介在しないルートの提言
出典：筆者作成

ア　有志国のルート

有志国でのルートでは、各工程は以下のようになる。

（ア）採掘・選鉱

豪州・Lynas 社が権益を有している Mt. Weld や海外での探鉱による開発から確保する。

[169] 伊藤昭男「日中間レアアース問題の原因分析と日本の対応」『東アジア評論』第 3 号、2011 年 3 月、172 頁。
[170] デロイト、「北米におけるレアアースのサプライチェーン状況分析業務　最終報告書」、88 頁。（2023 年 1 月 27 日閲覧）。

（イ）　米国での分離・精製過程の実施

米国はすでにDyの分離･精製のための工場建設や投資を行っている[171]。特に､米国はLynas社と契約して、テキサス州でHREEsの分離精製工場を建設している[172]。

イ　東南アジア諸国のルート

東南アジアでは、分離・精製をマレーシアが担う。また、合金化をベトナムが担う。

（ア）　マレーシアでの分離・精製

Lynas社はマレーシアに軽希土類鉱石の分離工場を有している。このLynas社の施設を増設する形でマレーシアが分離・精製を担う。

（イ）　ベトナムでの合金化

JOGMEC の委託を受けたデロイト トーマツ コンサルティング合同会社の調査[173]によると、HREEsの合金化は中国･ベトナムで行われている。事実、ベトナム･Vietnam Rare Earth JSC社が合金化(Refining)したDy製品を販売している[174]。

(4)　政策提言“HREEs Security Partnership”のための国際連携

では、この”HREEs Security Partnership”を実現するためには、どのような課題があり、どのような国際連携が必要となるか。以下、2点の課題がある。

ア　有志国による支援

イ　ASEANへの支援

本連携を推進する上で、米国と豪州との協力は重要である。ゆえに、ウでは、”HREEs Security Partnership”推進の具体策について論ずる。

ア　有志国内での支援

（ア）　では採掘・選鉱から電解工程の支援、（イ）では合金化・磁石製造から最終製品製造の工程の支援を提言する。

---

[171] 笹井秀起、「2021年Biden政権成立後の米国レアアース関連動向」、2022年1月25日。[https://mric.jogmec.go.jp/reports/mr/20220125/165301/]、（2023年1月22日閲覧）。

[172] Argus, “Lynas secures DoD funds for US heavy rare earth plant,” June 14, 2022, https://www.argusmedia.com/en/news/2341111-lynas-secures-dod-funds-for-us-heavy-rare-earth-plant, accessed January 22, 2023.

[173] デロイト、「北米におけるレアアースのサプライチェーン状況分析業務　最終報告書」、88頁。（2023年1月22日閲覧）。

[174] Vietnam Rare Earth JSC, “products details,” http://vtre.vn/products.html, accessed January 22, 2023.

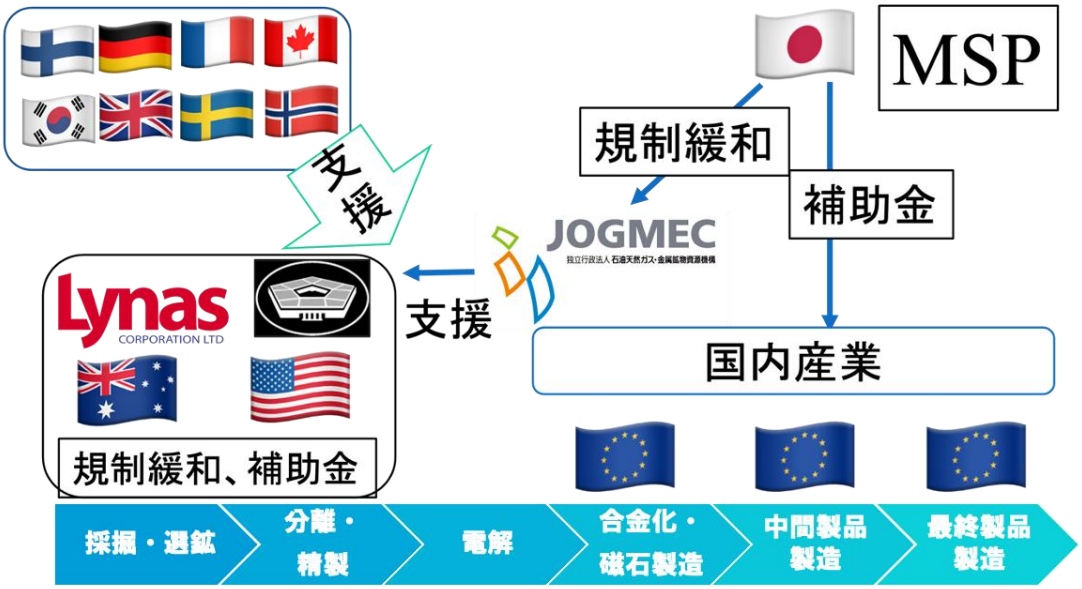


図 16　有志国での支援体制

出典：筆者作成

（ア）　採掘・選鉱から電解工程の支援

豪州の Mt. Weld は米国の Mt. Pass に比べ、Dy 等の重希土類鉱石が含まれている。かつ、Mt. Weld は世界でも有数の REE の生産量を誇る REE の鉱山である[175]。また、豪州は現在、資源ナショナリズムの動きが発生しておらず[176]、資源国家の中では、鉱物の潜在性と政治的安定性を高く評価されており、鉱業投資では世界で最も魅力的な地域とされる[177]。我が国は 2022 年 9 月に JOGMEC と双日を通じて Lynas 社と取引を続けており、最近でも Lynas 社に資金を提供した[178]。

豪州・米国からの確保を行うためには、MSP の活用が求められる。MSP はメンバー国間で情報共有を行い、環境、社会、ガバナンス(ESG)基準 に準拠した戦略的な鉱山開発・精錬・

[175] 中国の鉱山はもちろん、米国の有力な REE 鉱山である Mt. Pass も中国企業と関係があるが、Mt. Weld の権益を所有する Lynas 社は中国との資本関係がないため、中国政府の影響を受けにくいと考えられる。角田昌太郎、「サプライチェーンの安全保障―米中対立下の懸念と米国が主導する経済的連携―」、62-63 頁。（2023 年 1 月 22 日閲覧）。

[176] JOGMEC シドニー事務所に対するヒアリング調査（2022 年 11 月 24 日実施）。

[177] Fraser Institute の”Annual SURVEY OF MINING COMPANIES 2021”では、9 頁で、世界各国・地域の中で Mt. Weld を有する西オーストラリア州が世界トップの評価を受けている。そのほかの州についても、他の諸国に比べ、高いスコアを出している。Fraser Institute, “Annual SURVEY OF MINING COMPANIES 2021,” April 12, 2022, p. 32, [https://www.fraserinstitute.org/sites/default/files/annual-survey-of-mining-companies-2021.pdf], accessed January 22, 2023.

[178] 双日、JOGMEC、「豪州ライナス社への追加出資について」、2022 年 9 月 20 日。[https://www.sojitz.com/jp/news/2022/09/20220920.php]、（2023 年 1 月 22 日閲覧）。

加工、投資の呼び込み、鉱物資源のリサイクル・リユースの実現などを目指すものである[179]。MSP の役割を拡大し、各国が短期的には豪州の Mt. Weld から生産された Dy 等の HREEs を購入すること、豪州や米国、その他地域での探鉱を支援し、各国の最低限量は供給する仕組みを設けることが必要である。

留意点として、以下の論点が存在する。

第一に、Mt. Weld の重希土類鉱石の推定含有量が我が国や有志国の需要を短期的に満たせるだろうが、中長期的に満たせないことが挙げられる。その点につき、各国とも国民生活に必要な最低限量の確保で協調すること、JOGMEC が Mt. Weld に代わる鉱山を見つけるための探鉱支援を行うこと、研究開発やリサイクル施策、既存の政策で解決される。

第二に、豪州は人件費が高い[180]。現在、労働党政権は同一労働同一賃金を制度化しようとしており[181]、今後も人件費は高騰すると予想される。事実、2021 年の本邦法人に対するアンケート調査で、豪州の経営上の問題点として、従業員の賃金上昇を 1 番に挙げている[182]。しかし、下記の下流工程への各国による支援、東南アジアでの生産で解決可能である。

（イ）合金化・磁石製造から最終製品製造の工程の支援

下流工程は我が国の他、米国・欧州・韓国がシェアを有している[183]。しかし、現在磁石製造から最終製品(モーター等)までは中国が価格競争力を有しており、シェアを急速に伸ばしている。さらに上流を有志国内で完結させた場合、生産コストは高騰すると予想される。そのために、各国が本ルートで生産された Dy を購入した自国企業への補助金の提供、税制優遇を行うことが求められる。

留意点として、中国による価格競争の可能性が挙げられる。中国はこれまで、価格競争に勝利し、米国・豪州の REE 鉱山は閉業に追い込まれた[184]。しかし、本上流工程での Dy 製品は Mt. Weld の生産量が需要に対して小規模ゆえ、企業にかける補助金等も少額であると予想されるため、企業に多大な負荷を課すものではない。

---

[179] 外務省、「鉱物安全保障パートナーシップ（MSP）概要」。（2023 年 1 月 20 日閲覧）。

[180] オーストラリアは 2018 年の時点で世界主要国の中で最低賃金が最高額である。また、2022 年 7 月には最低賃金を 2018 年以上の 21.38 豪ドルになった。JETRO、「オーストラリア、最低賃金が世界主要国で最高額」、2019 年 7 月 24 日。[https://www.jetro.go.jp/biznews/2019/07/e7d9171b27ade8fe.html]（2023 年 1 月 26 日閲覧）; JETRO、「最低賃金を 7 月から 5.2%引き上げ」、2022 年 6 月 16 日。[https://www.jetro.go.jp/biznews/2022/06/9f04bf8406970d9c.html]、（2023 年 1 月 26 日閲覧）。

[181] JETRO シドニー事務所に対するヒアリング調査（2022 年 11 月 15 日実施）。

[182] JETRO、「2021 年度 海外進出日系企業実態調査アジア・オセアニア編-感染状況等により、在アジア日系企業の業績に差異も。 インド、中国で業績回復・拡大、ASEAN では回復弱く-」2021 年 12 月 7 日、40 頁。[https://www.jetro.go.jp/ext_images/_Reports/01/6e5157e362606548/20210045.pdf]、（2023 年 1 月 26 日閲覧）。

[183] デロイト、「北米におけるレアアースのサプライチェーン状況分析業務　最終報告書」、88 頁。（2023 年 1 月 22 日閲覧）。

[184] 加藤、「太平洋のレアアース泥が日本を救う」、74-80 頁。

イ　ASEAN への協力

ASEAN は 2019 年 6 月に取りまとめられた ASEAN の方針(ASEAN Outlook on the Indo-Pacific：AOIP)に対する論評[185]によると、米中対立に消極的な立場である。これは、井形彬氏[186]によると、ASEAN 諸国の政府関係者は”Don’t make us choose”と言い、片方の立場に立つことを望んでいない。事実、ASEAN 諸国は大国主導のインド太平洋構想に不安感を持っており、ASEAN 及び ASEAN 諸国の伝統的な外交戦略にそぐわないものである[187]。

しかし、ASEAN 諸国は米中対立による、中国からの資本の移転には歓迎している[188]。ゆえに、政府ではなく企業による投資という形での参加が望ましい。

そのためには、我が国や有志国での環境整備での協力が必要となる。我が国がこれまで行なってきた、ODA 等のインフラ投資に加え、日豪パートナーシップ、MSP、Quad、”HREEs Security Partnership”でのインフラ支援が求められる。また、最終的には、サプライチェーンで一翼を担うベトナム・マレーシアが、自国の担当する工程で優位性、ひいては不可欠性を有するよう、技術の提供等が求められる。そのためにも、各国と技術移転協定を結ぶことが求められる。

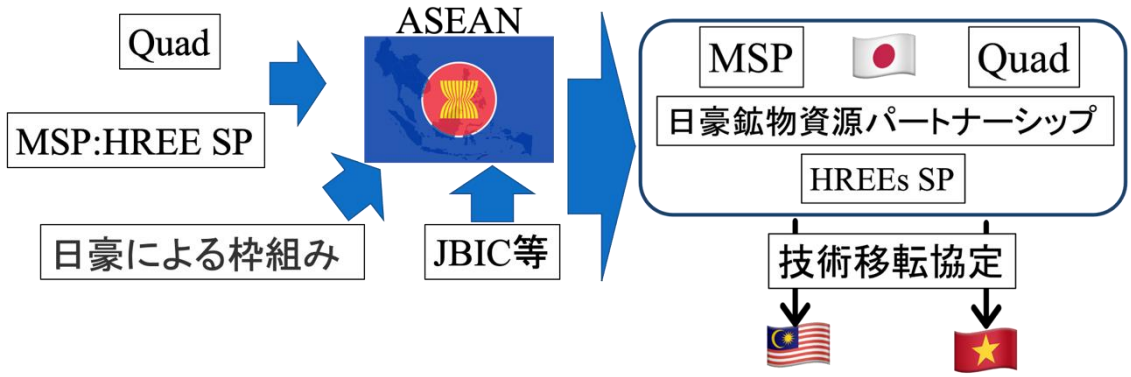


図 17　ASEAN 諸国への支援体制

出典：筆者作成

ウ　“HREEs Security Partnership”推進の具体策

この国際連携を行うために、まず、（ア）米国、（イ）豪州との交渉を行うべきである。

---

[185] 鈴木早苗、「ASEAN のインド太平洋方針と日中の対応」、2021 年 3 月 12 日。[https://www.jiia.or.jp/research-report/post-58.html]、（2023 年 1 月 22 日閲覧）。

[186]東京大学先端科学技術研究センター特任講師　井形彬氏に対するヒアリング調査（2022 年 10 月 13 日実施）。

[187] 大庭三枝「「インド太平洋」の多様性:ASEAN からの視点」『インド太平洋地域の海洋安全保障と『法の支配』の実体化に向けて』、2019 年 3 月、84 頁。

[188] 東京大学先端科学技術研究センター特任講師井形彬氏に対するヒアリング調査（2022 年 10 月 13 日実施）。

（ア）　米国

我が国は日米経済 2+2 でサプライチェーンの強靭化の連携に合意している。特に Dy を含む重要鉱物は米国も課題視しており、日米が協力できる可能性は高い。日米で主導することは HREEs Security Partnership の実現につながる。

（イ）　豪州

現在、日豪間で重要鉱物のパートナーシップが締結されている。これを基に HREEs Security Partnership 実現の協力を提案すべきである。日豪間でのこの協力は国民間の賛意も得られると予想される。事実、シドニー大学の調査では、日豪間の軍事同盟締結のアンケートをとっており、日豪ともに約半分が賛意を示している[189]。ゆえに、安全保障上重要となる Dy の確保において、HREEs Security Partnership の協力は十分に可能性がある。

(5)　“HREEs Security Partnership”のための国内政策

では、国内ではどのような施策が必要になるだろうか。 A では上流工程の支援、B では下流工程の支援を提言する。

ア　採掘・選鉱から電解工程の支援

上流工程では、JOGMEC の業務拡大が求められる。出資の限度額は、原則として、採掘等に必要な資金又は採掘等の権利を取得するために必要な資金に充当される出資の額の 50%以内とされ、さらに、JOGMEC が単独で出資先の最大株主とならない範囲に限られる[190]。
ゆえに Dy に関しては 100%の出資が可能になるよう変更すべきである。これにより、JOGMEC が単独で全てのリスクを負う。これは、以下の理由からそうしたリスクを取ることが正当化される。

第一に Dy は短期的には確保が必要ではあるが、長期的には需要が低下する可能性が高く、暴落する可能性もあるからだ。これは REE が「添加剤」としての用途が主であり、需要量が少なく、価格変動性が大きいため、REE の需要予測は難しいとされる[191]。事実、Dy 低減・代替技術は進んでおり、長期的には需要が激減する可能性が高い。Dy はネオジム磁石への添加の他には使途がないため、ネオジム磁石への使途がなくなれば、価格は暴落する。

第二に Dy の国内需要は小規模であるからだ。Dy は増加すれども、ベースメタルやその他の REE に比べ、小規模であり、大手鉱山企業は参入しづらい[192]。

これら二つの理由から、リスクが大きいものの、ネオジム磁石は国が重視し、確保する必

---

[189] United States Studies Centre, “US MIDTERMS 2022 The stakes for Australia and the alliance” October 2022, p.10.
[190] JOGMEC、「金属採掘等資金及び金属権利譲受け資金出資細則」、2010 年 7 月 1 日、2-3 頁。[https://www.jogmec.go.jp/content/300113923.pdf]、（2023 年 1 月 22 日閲覧）。
[191] 福田、『日本と中国のレアアース政策』、33 頁。
[192] JOGMEC シドニー事務所に対するヒアリング調査（2022 年 11 月 24 日実施）。

要があることから、国の果たすべき役割は大きく、全てのリスクを負うことには公共的に意義がある。

イ　合金化・磁石製造から最終製品製造の工程の支援

“HREEs Security Partnership”を維持する上で、国内産業への補助金が必要となる。具体的には、受給要件として、本邦法人で、ネオジム磁石製造を行う者がこのルートから一定量を購入した場合に、一定額の補助金を支給する。

以上、(4)、(5)の施策により、”HREEs Security Partnership”は実現できる。

第 4 節　半導体の供給確保についての提言

1　意義

半導体は身近な家電製品から社会インフラまであらゆるものに組み込まれている。国民生活や産業に不可欠な存在であることから、「産業のコメ」と呼ばれることも多い。そして、近年デジタル化が進む中で、その重要性は一層増してきた。

また、地政学的にも、半導体は高い価値を持つ。陸、海、空に加えて、新たに生まれたサイバー空間では日々競争が繰り広げられている。デジタル情報が行き交うこの舞台では、半導体が仮想的なデータの受け皿となり、電子的に処理している。その戦略的な価値の高さから、半導体は国際情勢を語るには欠かせない要素となった[193]。もはや半導体は産業そのものであると言える。

さらに、半導体は兵器の開発においても大きな価値がある。例えば、マッハ 5～10 のスピードを誇る極超音速ミサイルには、超高性能な半導体が頭脳として組み込まれる。このようなミサイルが懸念国で開発されれば、国家安全保障上の脅威となりえる。世界の国々にとって半導体を確保することは死活的な利益となっている[194]。

以上のように半導体は重要であるが、近年そのサプライチェーンがリスクに見舞われた。2020 年には、新型コロナウイルスの流行により、特定の国での工場の停止、輸出入の制限がなされた。その結果、一部の高度な技術が必要な半導体の流通が大きく阻害され、世界的に半導体を中心とする電子部品（自動車部品）の供給途絶が起こり、自動車等の生産が阻害される事態が発生した。

このような事情だけを踏まえると、重要な半導体の供給は全て日本国内でまかなうことが理想とも思える。しかし、現実問題として半導体の素材、製造装置、それを生産する技術等は各国に偏在しており、すべてを内製化することは不可能である。そこで、半導体の研究開発、生産においては他国との協力、連携は不可欠であると言える。

---

[193] 太田泰彦、『2030 半導体の地政学 戦略物資を支配するのは誰か』、日本経済新聞出版、2021 年、14 - 15 頁。
[194] 同上、17 - 19 頁。

以上より、本節では、半導体分野における国際連携の在り方やそれに伴い行うべき施策について検討していく。

2　現状分析

(1)　生産における分業化の進展、技術の偏在

ア　経緯

半導体は大きく分けて、開発、設計、製造、組立の 4 つの生産工程がある。すべての生産工程から販売までを一貫して手掛けるメーカーは垂直統合型企業（IDM 型メーカー）と呼ばれ、1970 年代まではこの IDM 型メーカーが主流であった。しかし、技術の進展に伴い生産工程が複雑になったため、一社だけでは製品に仕上げるには時間がかかりすぎるようになり、水平分業化が進んだ。具体的には、製造装置のみを扱うメーカーや、設計ツールのみを扱うメーカーが登場した。また、ロジック半導体の重要性が増すにつれ、製造部門が設計のみを担うファブレス企業と製造のみを担うファウンドリ企業とに分かれる動きも起こった[195]。結果として、半導体サプライチェーンは複雑になり、各々のメーカーが生産技術を独占することとなった。そして、このことは各々のメーカーが所属する一部の国や地域に技術が偏在する状況をもたらした。

イ　日本の状況

このような状況下で、日本が強みを持つようになった分野はメモリ半導体[196]、半導体素材、製造装置である。

メモリ半導体に関しては、NAND メモリ[197]のシェアの約 3 割以上を日本が占めている（ウェスタンデジタルは米国の企業だが、日本の四日市で生産を行っている[198]）。

---

[195] セント・アンド・フォース『図解入門業界研究 最新半導体業界の動向とカラクリがよ～くわかる本[第3版]』、秀和システム、2021 年、28 - 29 頁。

[196] データを保存する半導体のこと。日本経済新聞、「ロジック半導体とは　スマホや自動運転の「頭脳」を担う」、2022 年 12 月 14 日。［https://www.nikkei.com/article/DGXZQOUC1352Y0T11C22A2000000/］、（2023 年 1 月 27 日閲覧）。

[197] 電源がなくても記憶を保持できる不揮発性メモリの一種。佐鳥 SP テクノロジ株式会社、「NAND 型フラッシュメモリとは？特徴や NOR 型フラッシュメモリとの違いについても解説」、2022 年 6 月 16 日。［https://www.satori.co.jp/sptechnology/column/nand.html#:~:text=NAND%E5%9E%8B%E3%83%95%E3%83%A9%E3%83%83%E3%82%B7%E3%83%A5%E3%83%A1%E3%83%A2%E3%83%AA%E3%81%A8%E3%81%AF%E3%80%81%E9%9B%BB%E6%BA%90%E3%81%8C%E3%81%AA%E3%81%8F%E3%81%A6,%E5%BA%83%E3%81%8F%E6%99%AE%E5%8F%8A%E3%81%97%E3%81%A6%E3%81%84%E3%81%BE%E3%81%99%E3%80%82］、（2023 年 1 月 27 日閲覧）。

[198] キオクシア株式会社に対するヒアリング調査（2022 年 11 月 30 日実施）。

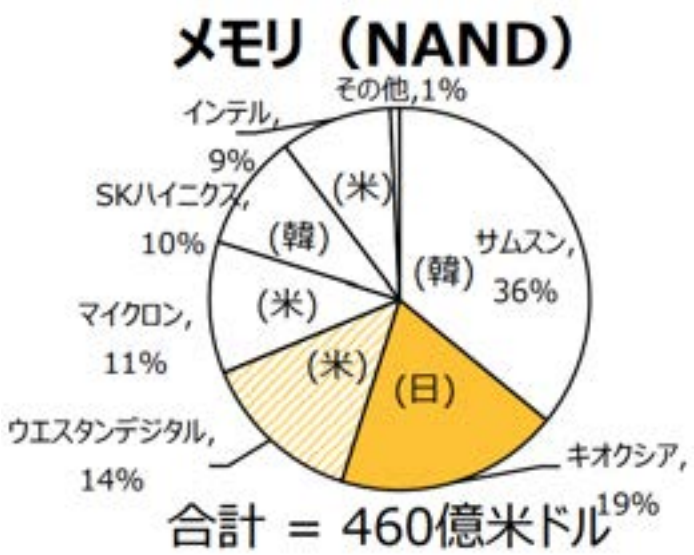


図 18　NAND メモリのシェア

出典：半導体戦略

また、半導体素材に関しては、日本は世界一位と評されている[199]。この理由は長年のノウハウの蓄積があるために、日本にしか作れない技術があるから[200]、そして、他国に比べてエコシステムが出来上がっているからである[201]。特に日本が強みを持つ素材としては、シリコンウエハ[202]が挙げられる。このシリコンウエハにおいては、日本企業である信越化学工業が 3 割以上のシェアを誇り、世界 1 位となっている。また、SUMCO 含む他の日本企業も合わせると、日本全体が占めるシェアは約 6 割にも上る。半導体素材の中でも最重要ともいえるこの分野でリードできている現状は、日本がある程度の不可欠性を有していると評価できる。

[199] 国立研究開発法人 新エネルギー・産業技術総合開発機構 技術戦略研究センター（TSC）「TSC トレンド　グローバルな半導体競争～エコシステム確保をかけて～」、2021 年 4 月。［https://www.nedo.go.jp/content/100931733.pdf］、（2023 年 1 月 18 日閲覧）。

[200] 経済産業省商務情報政策局に対するヒアリング調査（2022 年 9 月 16 日実施）。

[201] キオクシア株式会社に対するヒアリング調査（2022 年 11 月 30 日実施）。

[202] 表面を鏡面に磨き上げ、世界中のあらゆる物質の中で最も高い平坦度を誇り、微細な凹凸や微粒子を限界まで排除した、超平坦・超清浄な円盤のこと。シリコンウエハは半導体の基盤の材料となるため、唯一半導体製造の全工程に関わってくる重要なものである。また、最先端の半導体を作るためには、最高品質なシリコンウエハが必ず必要とされるため、シリコンウエハは半導体素材の中でも一際その重要性が高い。SUMCO、「シリコンウェーハとは」。［https://www.sumcosi.com/ir/glance/wafer.html］、（2023 年 1 月 25 日閲覧）。

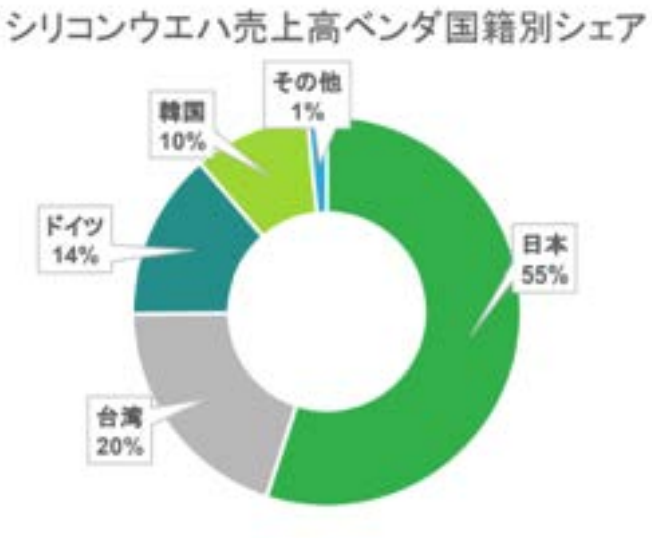


図 19　シリコンウエハ売上高ベンダ国籍別シェア
出典：令和元年度安全保障貿易管理対策事業（電子機器製造の産業基盤実態等調査）

製造装置に関しては、日本は世界 2 位である（1 位は米国）[203][204]。世界の売上高において、装置メーカー15 社中 7 社が日本企業となっており、シェアにして約 3 割を誇っている。しかし、露光装置[205]に関してのみはオランダの ASML が全体の 8 割を占め、EUV 装置[206]に至っては 100%を達成している。この EUV 装置は半導体の微細化には必須の装置であり、先端半導体の生産における日本のチョークポイント[207]となっている。

[203] 国立研究開発法人 新エネルギー・産業技術総合開発機構 技術戦略研究センター（TSC）「TSC トレンド　グローバルな半導体競争～エコシステム確保をかけて～」、2021 年 4 月。［https://www.nedo.go.jp/content/100931733.pdf］、（2023 年 1 月 18 日閲覧）。

[204] 東北大学工学研究科遠藤哲郎教授に対するヒアリング調査（2022 年 10 月 25 日実施）。

[205] 複雑で微細な電子回路のパターンを大きなガラス板に描いたフォトマスクを、極めて高性能なレンズで縮小して、シリコンウエハに焼き付ける装置のこと。Nikon、「半導体露光装置」。［https://www.jp.nikon.com/company/technology/product/semiconductor/］、（2023 年 1 月 25 日閲覧）。

[206] EUV（極端紫外線）を利用した露光装置のこと。コンスタントに 3 ナノメートルで回路を描く性能を有する。太田、『2030 半導体の地政学 戦略物資を支配するのは誰か』、170 頁。自由民主党衆議院議員甘利明様に対するヒアリング調査（2022 年 9 月 26 日実施）。

[207] サプライチェーン上の要所のこと。経済産業省、「経済安全保障に関する国際情勢や日本の対応」、2022 年 9 月。［https://www.kanto.meti.go.jp/seisaku/boeki/data/1-1gijyutu_keizai_2022.pdf］、（2023 年 1 月 26 日閲覧）。

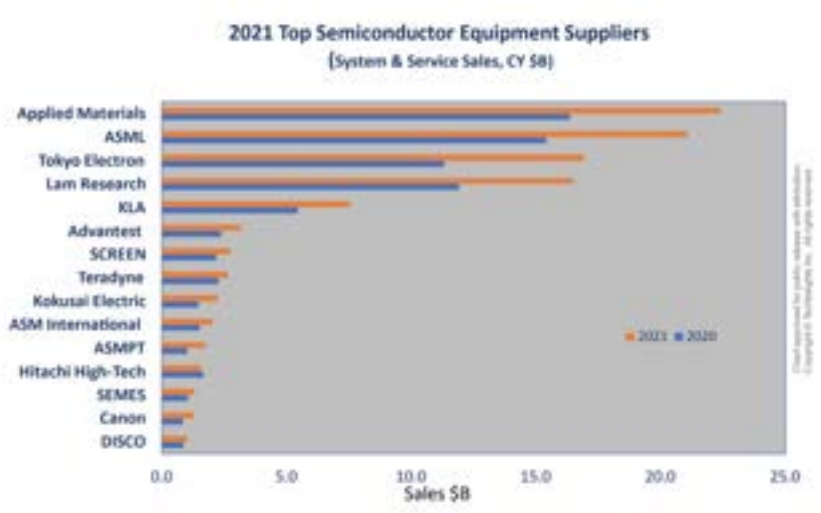


図 20　2021 Top Semiconductor Equipment Suppliers(System & Service Sales, CY $B)
出典：Tech Insights 2021 Top Semiconductor Equipment Suppliers

露光装置のほか、日本の弱点となっている分野としては、先端ロジック半導体[208]も挙げられる。現在、世界で最先端のロジック半導体は、台湾の TSMC 製であり、半導体の回路線幅を 3 ナノメートルに細くするところまでその技術は進んでいる[209]。一方の日本は 40 ナノメートルの製品しか生産できておらず、世界から 10 年も遅れを取っていると言われている。実際、スマートフォンやハイパフォーマンスコンピュータなどに使用されている高性能な先端ロジック半導体（ハイエンド）の製造基盤が日本には存在していない。そのうえ、産業機械や自動車などに使用されるロジック半導体（ミドルレンジ）の需給もひっ迫している状況となっている[210]。

ウ　日本の半導体生産における海外のキープレイヤー

以上を踏まえると、日本の半導体の生産において重要視されている企業は 2 つあることがわかる。

1 つ目は、TSMC である。TSMC はファウンドリ企業で、先端ロジック半導体の生産におい

[208] 制御や加工、演算処理などを行う半導体。パソコンをはじめとしたデジタル機器の中核部品となる半導体。日本経済新聞、「ロジック半導体とは」、2019 年 2 月 16 日。
［https://www.nikkei.com/article/DGKKZO41355730V10C19A2DTA000/］、（2022 年 1 月 27 日閲覧）。
[209] チップの集積度が高いほど微細化できるために、半導体は高性能になる。そのため、回路線幅を細くして狭い面積に多くの回路を詰め込む技術が重要となっている。太田、『2030 半導体の地政学 戦略物資を支配するのは誰か』、79 - 81 頁。
[210] 経済産業省、「半導体・デジタル産業戦略」、2021 年 6 月。
［https://www.meti.go.jp/policy/mono_info_service/joho/conference/semicon_digital/20210603008-1.pdf］、（2022 年 1 月 18 日閲覧）。

て世界一の技術力[211]を持っている。サイズ別の半導体製造能力の国際比較において、10 ナノメートル未満の 92%を台湾が占めている。

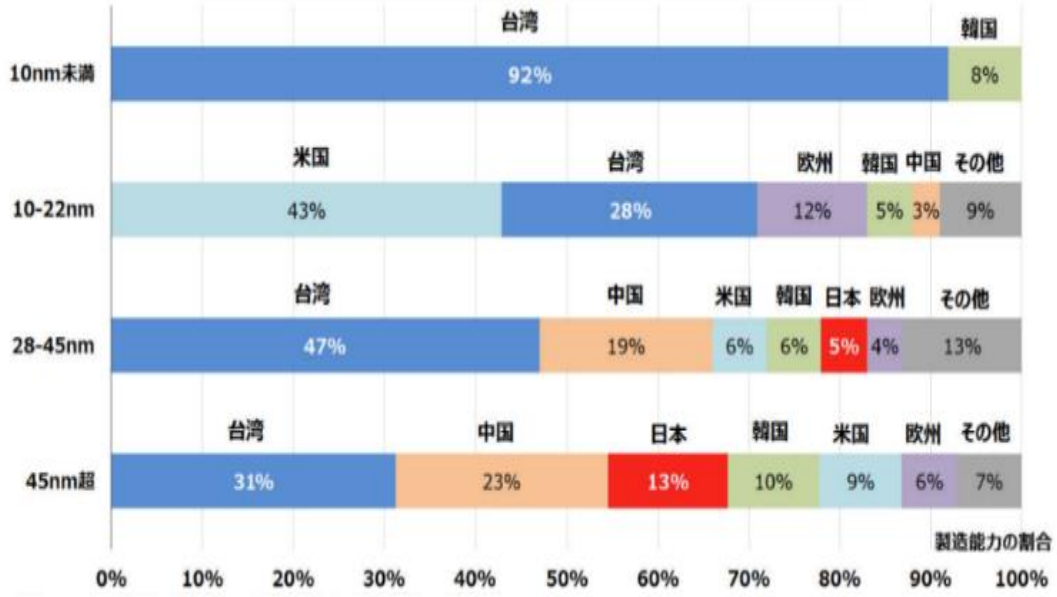


図 21　サイズ別半導体製造能力の国際比較

出典：内閣官房　成長戦略会議（2021 年 4 月 12 日）

現在、その製造能力の高さゆえに、各国は TSMC を誘致している。これは自国の半導体サプライチェーンの不足分を補うことと同時に、自国内で生産体制を整備し台湾有事に備えることも目的として挙げられる。実際、日本も熊本県に TSMC の工場を建設しており、国内での 22～28 ナノメートルのロジック半導体の生産を目指している。これにより、日本はミドルレンジの増産が可能となると見込まれている。

2 つ目は、ASML である。ASML は露光装置で約 8 割のシェアを誇っており、EUV 装置に関しては 100%を達成している。この EUV 装置とは、コンスタントに 3 ナノメートル当たりに回路を描くことができる性能を有しており[212]、半導体の微細化には不可欠な製造装置となっている。すなわち、先端半導体の生産において、ASML の技術は各国のチョークポイントとなっている。また、ASML は電機メーカー大手フィリップスを母体としているオランダ企業である一方で、光学系の装置、レーザー光線の発生器に関してはドイツ製を使っており、かつ、EU の補助金を多く受け取っているため、オランダ企業というより、オールヨーロッパで支えられていると見ることができる[213]。よって、ASML と協力するということは、オランダだけではなく、EU 全体との協力を意味すると言える。

[211] TSMC は世界で唯一電子回路の線幅を 3 ナノで量産できる段階に入っており、世界一の集積度を誇るチップを作ることができる。太田、『2030 半導体の地政学 戦略物資を支配するのは誰か』、79 - 81 頁。
[212] 自由民主党衆議院議員甘利明氏に対するヒアリング調査（2022 年 9 月 26 日実施）。
[213] 太田泰彦、『2030 半導体の地政学』、169 - 178 頁。

以上の事情に沿って、自由民主党衆議院議員甘利明氏も、「オランダとアメリカと日本で同盟国同志国間の連携をとる」ことが重要であるという話を述べていた[214]。

エ　米中対立の深化と、それによる中国とのデカップリングの進行

米中対立が深まる中、米国は中国企業であるファーウェイに対して 2020 年に直接製品規制を制度化した。直接製品規制とは、米国再輸出規制の一種であり、概略としては、米国製機器・技術・ソフト等を使って製造した機器等を米国以外の国から輸出する場合に、米商務省 BIS の許可が必要というものである[215]。この規制により、米国製の半導体製造装置・自動設計ソフトを使って製造した専用・汎用半導体の中国向け輸出は、実質的に封じられた。特に、中国は自社で設計した高性能半導体の製造を TSMC に委託することができなくなった。

また、中国は ASML の EUV 装置や日本の半導体素材等を輸入できなくなり、先端半導体の分野から手を引かざるを得なくなった。その後も米国は、エンドユース規制等を行った結果、中国は世界各国による先端半導体における技術競争に参戦するハードルがかなり高くなった。よって、今後西側諸国にとって強力なライバルにならないと考えられ、デカップリングが果たされたと言える。実際、中国の投資動向を観察すると、先端部分への設備投資は激減している。

しかし、中国は半導体分野を諦めたわけではなく、最近はレガシー半導体[216]の分野への投資を積極的に行い始めている。すなわち、現在世の中に必要とされている半導体を作る能力が 2、3 年後に爆発的に大きくなるということが予想される。結果として、近い将来、中国製の安いレガシー半導体が世界中に供給され、熾烈な価格競争が起きると考えられる[217]。そして、中国は当該競争により半導体の優良企業を淘汰していく過程で、先端分野においても優位性を確保することを企図しているとも考えられる。

(2)　日本政府の動き

以上の情勢を踏まえて、経済産業省は 2021 年 6 月に「半導体戦略」を策定し[218]、国家として必要となる半導体生産・供給能力の確保に取り組むとともに、日米連携をはじめとした有志国等との連携も図りながら、国際共同研究・開発を促進することを方針として示した[219]。

---

[214] 自由民主党衆議院議員甘利明氏に対するヒアリング調査（2022 年 9 月 26 日実施）。
[215] CISTEC 事務局、「米国による対中輸出規制の著しい強化について（改訂 2 版）」、2022 年 12 月 13 日。［https://www.cistec.or.jp/service/uschina/52-20221011.pdf］、（2023 年 1 月 18 日閲覧）。
[216] パワー、マイコン、アナログなどの半導体のこと。技術的には先端ではないが、現在様々な製品に組み込まれているため、一定の需要がある。経済産業省商務情報政策局情報産業課に対するヒアリング調査（2022 年 9 月 16 日実施）。
[217] 日本経済新聞編集委員太田泰彦氏に対するヒアリング調査（2022 年 11 月 22 日実施）。
[218] 経済産業省、「半導体・デジタル産業戦略検討会議」。
［https://www.meti.go.jp/policy/mono_info_service/joho/conference/semicon_digital.html］、（2023 年 1 月 24 日閲覧）。
[219] 経済産業省、「半導体戦略」、2021 年 6 月。
［https://www.meti.go.jp/policy/mono_info_service/joho/conference/semicon_digital/20210603008-4.pdf］、（2023 年 1 月 24 日閲覧）。

以降では、当該戦略等を踏まえ、既存の技術に関する施策（サプライチェーンの強靭化）と、先端技術に関する施策（研究開発）、そして、これらの技術の流出を防止する仕組みについて整理し、分析していく。また、既存の国際連携の枠組みについても分析していく。

ア　既存の技術に関して～サプライチェーンの強靭化に関する施策～

（ア）　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及び国立研究開発法人新エネルギー・産業技術総合開発機構法の一部を改正する法律

「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及び国立研究開発法人新エネルギー・産業技術総合開発機構法の一部を改正する法律」が 2022 年 3 月から施行された[220]。この法改正は、事業者による高性能な半導体の生産施設整備等への投資判断を後押しし、国内における安定的な生産の確保に資することを目的としている。内容は、一定基準以上の性能の半導体を作る事業者が、日本で 10 年以上継続して製造する、需給ひっ迫時に情報産業に協力する、適切な情報管理を行っている等の条件を満たした場合、経済産業省の認定を受けて NEDO から補助金を受け取ることができるという内容である[221]。現在は計 3 件が認定を受けている[222]。TSMC の熊本への誘致もこの制度を利用して行われた[223]。

（イ）　令和 3 年度補正予算「サプライチェーン上不可欠性の高い半導体の生産設備の脱炭素化・刷新事業費補助金」

本補助金は、民間事業者が国民生活への影響や経済的な損失が大きく公益性が高い半導体を安定的に供給するための製造設備を入替、増設する事業に要する経費等を補助することにより、今後到来する自動運転・IoT 時代に備え、半導体サプライチェーンの強靭化を実現し、安定供給に必要な体制を確保することを目的としたものである[224]。経済産業省は応募総数 36 件中 30 件、約 465 億円を採択し、国内に存在するレガシー半導体工場の 81 工場中 27 工場（約 33%）に補助金を支給した[225]。

---

[220] 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律（特定半導体生産施設整備等関係）」、2022 年 3 月 1 日。
［https://www.meti.go.jp/policy/mono_info_service/joho/laws/semiconductor.html］、（2023 年 1 月 18 日閲覧）。

[221] 経済産業省商務情報政策局情報産業課に対するヒアリング調査（2022 年 9 月 16 日実施）。

[222] 経済産業省、「認定特定半導体生産施設整備等計画」。
［https://www.meti.go.jp/policy/mono_info_service/joho/laws/semiconductor/semiconductor_plan.html］、（2023 年 1 月 24 日閲覧）。

[223] 同上。（2023 年 1 月 24 日閲覧）。

[224] 経済産業省、「令和 3 年度補正「産業技術実用化開発事業費補助金（サプライチェーン上不可欠性の高い半導体の生産設備の脱炭素化・刷新事業費補助金）」に係る補助事業者募集要領」、2021 年 12 月 21 日。
［https://www.meti.go.jp/information/publicoffer/kobo/2021/downloadfiles/k211221001_01.pdf］、（2023 年 1 月 18 日閲覧）。

[225] 経済産業省商務情報政策局情報産業課に対するヒアリング調査（2022 年 9 月 16 日実施）。

（ウ）　経済安全保障推進法に基づく半導体の「特定重要物資」指定

2022 年 12 月、「特定重要物資」（経済安全保障推進法第 7 条）として「半導体素子及び集積回路」（同施行令 1 条 6 号）が指定された。また、経済産業省は「安定供給確保を図るための基本方針」（同法第 8 条 1 項）を作成し[226]、レガシー半導体、製造装置、半導体素材、半導体原料を対象として、生産施設・生産設備の導入、リサイクル施設・設備の導入、リサイクル技術開発、備蓄・輸送体制の強化の取組を行うことを公表した。今後は、これらの取組と既存の施策を組み合わせてサプライチェーンの強靭化を図っていくこととなる。

イ　先端技術に関して～研究開発に関する施策

（ア）　ポスト 5G 情報通信システム基盤強化研究開発事業

令和元年度補正予算において、ポスト 5G 情報通信システム基盤強化研究開発事業(以下、「ポスト 5G 基金事業」という。）が開始された。同事業では、5G に更に超低遅延や多数同時接続といった機能が強化された 5G（以下、「ポスト 5G」という。）について、これに対応した情報通信システム（以下、「ポスト 5G 情報通信システム」という。） の中核となる技術開発を基金で支援することとしている。具体的には、ポスト 5G 情報通信システムや当該システムで用いられる半導体を開発するとともに、ポスト 5G で必要となる先端的な半導体を将来的に国内で製造できる技術の開発に取り組むこととしている[227]。令和 4 年度補正予算額としては、4850 億円が予定されている[228]。

（イ）　次世代半導体プロジェクト

日本では次世代半導体プロジェクトが 2022 年から始まっている。具体的には、日米経済政策協議委員会（経済版「2＋2」）での合意を受け、日本は研究開発プラットフォームである LSTC[229]を立ち上げ、そこで開発された技術を量産製造拠点である Rapidus[230]が事業化を図

---

[226] 経済産業省、「半導体に係る安定供給確保を図るための取組方針」。（2023 年 1 月 27 日閲覧）。

[227] 国立研究開発法人 新エネルギー・産業技術総合開発機構、「ポスト 5G 情報通信システム基盤強化研究開発事業」、2019 年。［https://www.nedo.go.jp/activities/ZZJP_100172.html］、（2023 年 1 月 18 日閲覧）。

[228] 経済産業省、「令和 4 年度補正予算の事業概要（PR 資料）」、2022 年 12 月。
［https://www.meti.go.jp/main/yosan/yosan_fy2022/hosei/pdf/pr_hosei_221202.pdf］、（2023 年 1 月 24 日閲覧）。

[229] Leading-edge Semiconductor Technology Center の略称であり、技術研究組合最先端半導体技術センターのこと。次世代半導体研究のための新しい研究開発を行う。経済産業省、「次世代半導体の設計・製造基盤確立に向けた取組について公表します」、2022 年 11 月 11 日。
［https://www.meti.go.jp/press/2022/11/20221111004/20221111004.html］、（2023 年 1 月 25 日閲覧）。

[230] 次世代半導体の量産製造拠点を目指すため、日本国内トップの技術者が集結し、国内主要企業からの賛同を得て設立された事業会社のこと。経済産業省、「次世代半導体の設計・製造基盤確立に向けて」、2022 年 11 月。［https://www.meti.go.jp/press/2022/11/20221111004/20221111004-1.pdf］、（2023 年 1 月 24 日閲覧）。

るというスキームを作った[231]。目標は 2 ナノメートルの半導体を作るための集積化技術と短 TAT 製造技術の研究開発である[232]。そして、日本はこの研究開発等において、米国の NSTC[233]や IBM[234]と協力する方針が決定されており、さらに現在は、IMEC[235]、ASML とも連携をとることも協議されている。この中でも、特に IBM や ASML は、先端ロジック半導体や露光装置といった日本の弱点分野をカバーすることが期待されている。

ウ　技術流出を防止する法律～外国為替及び外国貿易法

（ア）　輸出管理

我が国は、安全保障と国際的な平和及び安全の維持の観点から、外為法により、大量破壊兵器や通常兵器の開発・製造等に関連する資機材並びに関連汎用品の輸出やこれらの関連技術の非居住者への提供について、管理をしている。したがって、外為法で規制している貨物や技術を輸出、提供しようとする場合には、原則として、経済産業大臣の許可を受ける必要がある。具体的には、専ら貨物や技術の機能や性能に着目した規制であるリスト規制と専ら需要者や用途に着目した規制であるキャッチオール規制の 2 種類がある[236]。

半導体関連産業に関しては、「集積回路」「半導体製造装置等」「半導体基板」等がリスト規制の対象となっており、幅広く輸出管理がなされている。

（イ）　対内直接投資規制

外為法では、外国投資家が、一定の事業を営む日本の会社（発行会社）に、直接投資等一定の行為を行う場合、外国投資家に対して事前届出を義務付けている（外為法 27 条）。そして、審査の結果、国の安全を損なう等のおそれがある場合、関係大臣は、中止の勧告等を行うことができる（同法 29 条）。また、無届けや虚偽の届出により、国の安全を損なう等のおそれがある対内直接投資等を行った外国投資家に対し、必要な措置命令を行うこともできる（同条）。2020 年 5 月には、同法が改正され、一定の基準尊守を前提に、事前届出制度（同法第 27 条の 2）が導入された[237]。

原則として、事前届出の対象となるのは、外国投資家による「指定業種」に関する対内直

---

[231] 同上。（2023 年 1 月 24 日閲覧）。
[232] 同上。（2023 年 1 月 24 日閲覧）。
[233] National Semiconductor Technology Center の略称であり、CHIPS 法に基づいて設立された米国の半導体技術センターのこと。経済産業省、「次世代半導体の設計・製造基盤確立に向けて」。（2023 年 1 月 27 日閲覧）。
[234] International Business Machines Corporation の略称であり、米国のロジック半導体のファブレス企業のこと。経済産業省商務情報政策局情報産業課に対するヒアリング調査（2022 年 9 月 16 日実施）。
[235] Interuniversity Microelectronics Centre の略称であり、ベルギーの研究開発機関のこと。太田、『2030 半導体の地政学』、173 頁。
[236] 安全保障貿易情報センター、「輸出管理の基礎」。
［https://www.cistec.or.jp/export/yukan_kiso/anpo_gaiyou/index.html］、（2023 年 1 月 24 日閲覧）。
[237] 経済産業省貿易経済協力局国際投資管理室、「対内直接投資審査制度について」。
［https://www.kanto.meti.go.jp/seisaku/boeki/data/1-2gijyutu_toushi_2022.pdf］、（2023 年 1 月 24 日閲覧）。

接投資である。指定業種は、対内直接投資等に関する命令 3 条 3 項に基づき、告示で指定されている。さらには、指定業種のうち国の安全に係る対内直接投資等に該当するおそれが大きいものに関わる業種を、いわゆるコア業種、として同令第 3 条の 2 第 3 項に基づき告示で指定している。コア業種に関しては、事前届出免除制度において、基準が上乗せされており、より厳しく取り扱われている[238]。

半導体関連産業においては、集積回路に係る業種はすべて指定業種となっており、規制の対象である（光電変換素子製造業、半導体素子製造業等ディスクリート半導体に係る業種は対象外）。しかし、その中でコア業種に指定されているのは集積回路製造業、半導体メモリメディア製造業のみである。

エ　国際連携

（ア）　米国

日米は半導体に関しての協力関係を大きく構築している。2022 年 5 月には、日米商務・産業パートナーシップ（JUCIP）で「日米半導体協力基本原則」が合意された[239]。原則の中では、特に半導体製造能力の強化・多様化、労働力開発の促進、透明性向上、半導体不足に対する緊急時対応の協調及び研究開発協力の強化について、有志国・地域と共に、二国間で協力していくことの重要性が強調された[240]。その後、日米首脳会談では「半導体製造能力、多様化、次世代半導体の研究開発、供給不足への対応」の分野における協力が発表され[241]、次世代半導体の開発を模索する日米の合同タスクフォースの設置が決定した[242]。そして、経済版「2＋2」では、当該タスクフォース実現のため[243]、米国の NSTC に対応する形で日本に LSTC の立ち上げが決められた[244]。

（イ）　EU

日 EU デジタルパートナーシップを締結し[245]、互いのサプライチェーンの強靭化へ向けた

---

238 同上。（2023 年 1 月 24 日閲覧）。
239 経済産業省、「萩生田経済産業大臣が米国に出張しました」、2022 年 5 月 6 日。［https://www.meti.go.jp/press/2022/05/20220506002/20220506002.html］、（2023 年 1 月 24 日閲覧）。
240 経済産業省、「半導体協力基本原則（仮訳）」、2022 年 5 月 4 日。［https://www.meti.go.jp/press/2022/05/20220506002/20220506002-4.pdf］、（2023 年 1 月 18 日閲覧）。
241 外務省、「ファクトシート：日米競争力・強靭化パートナーシップ」、2022 年 5 月 23 日。［https://www.mofa.go.jp/mofaj/files/100347258.pdf］、（2023 年 1 月 24 日閲覧）。
242 外務省、「日米首脳共同声明「自由で開かれた国際秩序の強化」」、2022 年 5 月 23 日。［https://www.mofa.go.jp/mofaj/files/100347254.pdf］、（2023 年 1 月 24 日閲覧）。
243 外務省、「日米経済政策協議委員会 2022 年行動計画」、2022 年 7 月 29 日。［https://www.mofa.go.jp/mofaj/files/100376269.pdf］、（2023 年 1 月 24 日閲覧）。
244 経済産業省、「次世代半導体の設計・製造基盤確立に向けて」。（2023 年 1 月 24 日閲覧）。
245 経済産業省、「日 EU デジタルパートナーシップが立ち上げられました」、2022 年 5 月 12 日。［https://www.meti.go.jp/press/2022/05/20220512005/20220512005.html］、（2023 年 1 月 24 日閲覧）。

施策、長期的投資戦略についての情報交換、関連する当局間での輸出管理の調整の達成、半導体などの技術開発において協力することを取り決めた[246]。

（ウ） IPEF

インド太平洋経済枠組み（IPEF）では、2022 年 9 月に行われた閣僚級会合で、全参加国により、半導体を含む需要物資サプライチェーン強靭化に関する声明をまとめ、交渉を開始することで合意した[247]。この声明では、重要分野及び物品の基準の策定、重要分野と物品における強靭性及び投資の増加、情報共有及び危機対応のメカニズムの構築等を進めることが合意された。また、「公正で開かれた市場及び WTO を中核とするルールに基づく多角的貿易体制の重要性を認識し、これらに対する我々のコミットメントを再確認」した[248]。

（エ） QUAD

2022 年 5 月に、首脳会合が行われた。そして、「グローバルな半導体サプライチェーンにおける日米豪印の能力及び脆弱性をマッピングし、多様で競争力のある半導体市場を実現する」ため、各国の「補完的な強みを一層活用する」ことを決定した[249]。また、本会合で発表された「重要技術サプライチェーンに関する原則の共通声明」は、地域への様々なリスクに対する日米豪印の強靭性を向上させるための協力基盤を提供し、半導体及びその他の重要技術に関する協力を推進するものである[250]。

（オ） CHIP4

日本、米国、韓国、台湾の先端半導体に関する同盟であり、半導体製造におけるサプライチェーンを構築することが目的である。パートナーとして台湾を入れている点、対中色が強い点が特徴として挙げられる[251]。

---

[246] 経済産業省、「付属書：最初の共同行動」『（仮訳）日 EU デジタルパートナーシップ』、2022 年 5 月 12 日。
［https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/b530adc8-3af1-4d9f-af84-6f21af4067af/5c1b4399/20220512_news_digital_group_japanese_03.pdf］、（2023 年 1 月 24 日閲覧）。

[247] 経済産業省、「西村経済産業大臣がインド太平洋経済枠組み（IPEF）閣僚会合に出席しました」、2022 年 9 月 13 日。［https://www.meti.go.jp/press/2022/09/20220913006/20220913006.html］、（2023 年 1 月 24 日閲覧）。

[248] 経済産業省、「繁栄のためのインド太平洋経済枠組み 柱 2 閣僚声明 繁栄のためのインド太平洋経済枠組み（ＩＰＥＦ） 柱２－サプライチェーン」、2022 年 9 月 13 日。
［https://www.meti.go.jp/press/2022/09/20220913006/20220913006-14.pdf］、（2023 年 1 月 24 日閲覧）。

[249] 外務省、「日米豪印首脳会合共同声明」、2022 年 5 月 4 日。
［https://www.mofa.go.jp/mofaj/fp/nsp/page1_001188.html］、（2023 年 1 月 18 日閲覧）。

[250] 外務省、「重要技術サプライチェーンに関する原則の共通声明（仮訳）」、2021 年 3 月 12 日。
［https://www.mofa.go.jp/mofaj/files/100347897.pdf］、（2023 年 1 月 18 日閲覧）。

[251] 日刊工業新聞、「社説/半導体の安定供給 「チップ 4」構想の行方を注視」、2022 年 8 月 1 日。
［https://www.nikkan.co.jp/articles/view/00644117］、（2023 年 1 月 24 日閲覧）。

3　課題抽出

（1）　どのような国際連携の枠組みを構築するべきか

現在、日本は次世代半導体プロジェクト等において、米国、台湾等と協力して研究開発を行っている。一方で、技術の発展のためには競争は不可欠であり、大部分の分野においては、引き続き有志国、地域同士でも競争していくことが重要である。しかし、世界には自国の戦略的利益確保の観点から経済的依存関係を利用し[252]、また、強制的な技術移転、知的財産窃取、国有企業による市場歪曲的な行動、有害な産業補助金といった不公正な慣行を行う[253]国も存在する。そこで、半導体に係る技術競争を正当に行うことができる環境を構築することが課題として挙げられる。具体的には、有志国、地域等の合意のもと、レベルプレイングフィールドを構築するべきである。また、この枠組みを構築する際には、既存のどの国際的枠組みを利用するべきかという課題もある。

（2）　有志国、地域内の技術をどう守るべきか

上記の枠組みが実効性を持つには、この枠組み外の国や地域への技術流出を防ぐことが重要である。そこで、どのような流出防止の仕組みを構築するべきかが課題として挙げられる。

（3）　有志国にすら渡せない日本の強みをどう守るべきか

有志国、地域と連携を進める中では、日本から他国への技術移転もある程度なされることが求められる。しかし、そのような動きの中でも、日本が強みを持つ技術に関しては国外へ流出することは防がなければならない。というのも半導体産業において日本のプレゼンスを維持、向上させるためには、不可欠性を保つことが重要だからである。しかし、現在日本が強みを持っている半導体素材、製造装置に関しては外為法の直接投資規制のコア業種に指定されておらず、事前届出制度が厳しく適応されていない。そこで、これらの業種をより徹底的に技術流出から守っていくことが課題として挙げられる。

（4）　レガシー半導体分野において、中国との競争にどのように備えるべきか

中国は先端半導体の分野において西側諸国にデカップリングをされ、レガシー半導体の生産に力を入れている。そこで、数年後に激化するであろうレガシー半導体の価格競争に日本はどのように備えるべきかが課題として挙げられる。

---

[252] 外務省、「外交青書 2022」、2022 年 4 月、17 頁。
[https://www.mofa.go.jp/mofaj/gaiko/bluebook/2022/pdf/pdfs/1_2.pdf#page=5]、（2023 年 1 月 27 日閲覧）。

[253] 外務省、「外交青書 2022」、2022 年 4 月、161 頁。
[https://www.mofa.go.jp/mofaj/gaiko/bluebook/2022/pdf/pdfs/3_1.pdf]、（2023 年 1 月 27 日閲覧）。

4　政策提言

(1)「先端技術競争協定」の締結

ア　提言

「先端技術競争協定」を有志国、地域等の合意のもと、締結することを提言する。この協定は、先端半導体等の先端技術の開発競争におけるレベルプレイングフィールドを目指すものである。

具体的な目的としては、経済安全保障上重要な物資及び技術を不正な手段を用いて技術を盗む国への移転と蓄積を防止することによって、科学技術の研究開発において正当な競争と共存を行うことである。したがって、不正に技術を盗む国や過去にエコノミックステイトクラフト等政治的な要因で WTO ルールに違反した国はこの協定には一定期間入ることができないように定める必要がある。

この協定の締結国、地域は技術流出を防止する国内法を制定する義務を負う。具体的には、人材流出防止、輸出管理、投資規制に関する法律を制定し、ヒト、カネ、モノの 3 つの面から非締結国から技術を守るようにする。また、締結国同士での情報交換、非締結国へのアウトリーチ活動を行う。

加盟することが予想される国、地域は、日本、米国、韓国、台湾、EU、豪州、ASEAN の一部の国等が挙げられる。また、高度技術を保有する国が一国でも抜けてしまっている状態では、その国から技術が流出してしまう恐れがあるため、すべての国が参画することが重要である。

イ　既存の国際枠組みとの関連性

この協定は、IPEF 加盟国を中心に作っていくべきである。IPEF では、公正で開かれた市場及び WTO を中核とするルールを遵守することを明言しており、本協定に求められる基本的価値観を共有できる国々が集まっているからである。そこで、IPEF をもとに、ASML を有するオランダ、ひいては EU を加えて作り上げていく。

ウ　中国とのデカップリングによる経済損失は許容範囲内か

世界では米国、中国、欧州の 3 つの大きい市場がある[254]。そこで、「先端技術競争協定」が実現した暁には、先端半導体分野において、中国とのデカップリングが完全に果たされるため、大きな市場を損失してしまうのではないかという懸念が浮かぶ。

しかし、元国家安全保障局長北村滋氏は「とりわけ米国においては 2018 年以降の政策転換から既にデカップリングが始まっており、今更ファーウェイを外したことで問題になることもないし、多少のコスト面の問題はあれども技術面での問題はない。高度技術のデカップリングは日本や欧米諸国の高い購買力を持つ国の間で安定した契約関係の下、相当の受

[254] 自由民主党衆議院議員甘利明氏に対するヒアリング調査（2022 年 9 月 26 日実施）。

注が確保できるということでもあり、個々の企業はともかく業界全体としてはメリットが大きいこともある[255]」と述べていた。すなわち、中国以外の市場国からの安定した需要が確保できるため、デカップリングによる経済損失は日本にとって許容範囲内であると言える。

また、この協定は中国との半永久的なデカップリングを目指すものではない。中国が一定期間エコノミックステイトクラフトや技術窃取を行わず、締結国と基本的な価値観が共有できると認めることができれば、加入できるものとする。そのためにも、非締結国へのアウトリーチ活動は重要であり、経済安全保障の概念を積極的に広めている[256]日本の役割は重要となってくると考えられる。

(2) 日本が強みを持つ分野のコア業種への指定

ア　提言

半導体素材、製造装置に関する業種を外為法の直接投資規制のコア業種に指定することを提言する。これにより、事前届出免除制度の基準が上乗せされ、国がより厳しく規制することができる。

イ　提言の妥当性について

最終報告会にて本提言を発表した際に、コメンテーターとしてお呼びした経済産業省貿易経済協力局貿易管理部安全保障貿易管理課の末藤氏に、外為法により半導体産業全体をカバーすることが良いとは断言できず、その必要性については精査する必要があるとのコメントをいただいた。

確かに、日本国内の中小企業が新たな技術を開発するたびに、コア業種に該当するおそれがあることを考えると、特に中小企業の割合が高い半導体素材企業や製造装置企業をコア業種指定することは、それらの企業に大きな負担を負わせかねないという問題点はある。しかし、平時から地方局と中小企業との関係性を深めておき、コア業種の該当性の判断などに際して積極的にサポートする体制を作ることで、その負担を軽くすることはできる。また、企業の負担を考慮しても、安全保障の観点からは日本の強みである半導体素材、製造装置は徹底的に防御を固めるべきである。

(3) レガシー半導体工場への補助金支給と税制優遇

ア　提言

レガシー半導体を生産する工場に補助金を支給すること、税制優遇措置を行うことの２つを提言する。

まず、１つ目の補助金支給に関しては、「特定重要物資」に指定されたレガシー半導体の工場に、同法に基づき補助金を支給する。前述したとおり、令和３年度補正予算にて、国内

[255] 元国家安全保障局長北村滋氏に対するヒアリング調査（2022 年 7 月 12 日実施）。
[256] 外務省総合外交政策局経済安全保障政策室に対するヒアリング調査（2022 年 7 月 6 日実施）。

のレガシー半導体工場に補助金を支給している一方で、いまだ 7 割近くの工場には支給が行き届いていない。そこで、残りのいくつかの工場にも新たに支援をすべきである。この際に注意すべき点は、ただ補助金を工場の頭数で割って支給するのではなく、しっかりとした調査のもと将来性がある工場のみに重点的に支援を行うことである。これにより、予算を効率的に執行できるようになる。また、当該補助金は、令和 4 年度補正予算にて「半導体サプライチェーンの強靭化支援」に 2,163 億円の予算が割り当てられているように、今後も重要物資のサプライチェーンを強靭化することを目的とした予算を継続的に編成することにより捻出するべきである。

次に、2 つ目の税制優遇措置に関しては、生産能力向上のための一定の設備投資について、税額控除を行う。また、取得設備について、新たに固定資産税が課される年度から 3 年程度の軽減措置を受けられるようにする。

以上の措置により、レガシー半導体の向上の生産能力を向上させるべきである。また、これらの措置は、あくまでサプライチェーンが危機に陥ったときの備えでもあり、国内で作ることこそが重要であるため、日本企業であろうと、外国企業であろうと積極的に補助をしていくべきである。

イ　「備蓄」の検討

経済安全保障推進法第 7 条には、サプライチェーンの強靭化のためのオプションとして、「備蓄」が掲げられており、補助金による「生産設備の整備」とともに行うことも当初は考えた。

しかし、東北経済産業局地域経済部製造産業・情報政策課は、「半導体と一口に言っても相当な種類あり、これを一括で備蓄をして、管理をして、必要なところに届けること」は難しいと述べていた[257]。そのため、レガシー半導体の生産能力を向上させるための手段としては、不適であると判断し、提言には至らなかった。しかし、将来的に、AI や IoT 等デジタル技術を利用し維持管理や搬送を効率的に行うことが出来れば、備蓄という選択肢も検討の余地があると思われる。

[257] 東北経済産業局地域経済部製造産業・情報政策課に対するヒアリング調査（2022 年 12 月 16 日実施）。

第 5 節　総括

我々は性質が異なる二品目に着目し、供給確保を図った。性質・取りうる施策の相違点、共通点を以下で総括する。

表 3　2 品目の比較

出典:筆者作成

品目	ジスプロシウム	半導体
性質		
場所	地理的に偏在している。	技術があればどこでも作れる
我が国の依存度	我が国は依存している。	我が国は強みを有し、依存させている。
政策		
施策の違い	国際連携による、代替ルートの構築	技術を漏洩させないように国際連携・国内整備
施策の共通点	現状を変革するための技術を育成	

ジスプロシウム（Dysprosium。以下、「Dy」という。）は、地理的に偏在しており、我が国は依存せざるを得ない。ゆえに、国際連携による代替ルートの構築を主な手段としなければならない。

一方で半導体は技術があればどこでも作れる。さらに我が国は強みを有しており、他国を依存させることが可能である。ゆえに、技術を漏洩させないよう、国際連携・国内整備が必要である。

なお、この施策をより完全なものにするために、第 4 章第 2 節で、我々はセキュリティ・クリアランス制度について論ずる。しかし、どちらの状況でも、現状を変革するための技術を育成することが必要である。そのためには、国が重要技術を選び、育成する機能が第一に必要である。そのために我々は第 4 章第 3 節でシンクタンク機能について提言する。

2022 年 12 月、経済安全保障推進法の特定重要物資の指定が行われた。我が国は国民の生命、財産のため、特に重要な物資は途切れなく供給されることが望ましい。そのための対応策を準備することは重要である。我々の施策はサプライチェーンの強靭化が必要な物質の今後の施策に対して一つの解を示した。

我が国と価値観を共有する有志国は不変ではなく、流動的である。技術革新やルールメイキングでの変革が著しい昨今の情勢では、前提とする状況・ルールが一変することもありうる。本施策を行うためにも、情報を常にキャッチアップし、柔軟で機動的な体制が求められる。変化する状況に臨機応変に対応し、この二品目の安定供給を成し遂げて、我が国は熾烈な競争を勝ち抜くことができると確信している。

第 2 章　サイバーセキュリティ分野での政策提言

第 1 節　総論

情報通信技術の進化とともにサイバー空間の新たな活用シーンが次々と生み出され、人々の暮らしや経済活動に大きな変革をもたらしている。そして、サイバー空間は今日において国民生活に欠かせない公共空間になっている。一方、サイバー空間ではサイバー犯罪が頻発し、個人・企業の権利や国家の主権を脅かす深刻なリスクとなっている。このような状況に対応するため、2022 年 12 月に閣議決定された国家安全保障戦略では「サイバーセキュリティの強化」が明記された。その中で我が国がとるべき戦略的アプローチとして「不正行為からサイバー空間を守り、その自由かつ安全な利用を確保するとともに、国家の関与が疑われる場合を含むサイバー攻撃から我が国の重要な社会システムを防護するため、国全体として防護・対応能力を強化し、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を図る」、「平素から官民の連携を強化するとともに、セキュリティ人材層の強化等についても総合的に検討を行い、必要な措置を講ずる」、「技術・運用両面における国際協力の強化のための施策を講ずるとともに、サイバー防衛協力を推進する」が列記された[258]。

サイバーセキュリティの強化は、安全保障と経済安全保障の両方に関わり、我が国の国益を守る上で極めて重要である。

本章では経済安全保障上のサイバーセキュリティに焦点を当てながら、第 2 節においてサイバーセキュリティの現状と問題点を把握し、第 3 節において課題抽出を行う。そして、第 4 節において、それぞれの課題に対する解決策について政策提言を行う。

第 2 節　現状分析

1　サイバー空間を取り巻く環境の変化

情報通信技術の進歩と相まって、便益を追求する国民と、利潤を追求する企業活動が原動力となり、人々の暮らしのあらゆるところに情報通信技術の活用が浸透した。身近な例を挙げれば、航空券や JR 切符の予約、ETC を使った高速道路利用、オンラインバンキング・オンライントレーディング、オンラインショッピングなど、あらゆる面で情報通信技術が活用されるようになり、これに伴って情報通信を支えるサイバー空間の利用も広がっている。もはやサイバー空間無しには国民生活は成り立たなくなってきている。

2020 年、新型コロナウイルス感染症が世界中に広がり、世界保健機関（WHO）は、世界的な感染拡大の状況、重症度等から 3 月 11 日に新型コロナウイルス感染症をパンデミック（世界的な大流行）とみなせると表明した[259]。我が国でも緊急事態宣言が発出され、首相官

---

[258] 内閣官房、「国家安全保障戦略（概要）、Ⅳ　我が国がとるべき国家安全保障上の戦略的アプローチ」。[https://www.cas.go.jp/jp/siryou/131217anzenhoshou/gaiyou.html]、（2023 年 1 月 19 日閲覧）。

[259] 国立感染症研究所感染症疫学センター、「IDWR2020 年第 21 号〈注目すべき感染所〉新型コロナウイルス感染症（COVID-19）」。[https://www.niid.go.jp/niid/ja/2019-ncov/2487-idsc/idwr-topic/9669-idwrc-2021.html]、（2023 年 1 月 18 日閲覧）。

邸をはじめとする国の機関、ならびに地方公共団体等は、国民に外出の自粛、感染の防止のための３密（密閉、密集、密接）の回避を呼び掛けた[260]。企業においても大企業を中心に、テレワーク導入の動きが一挙に進んだ。また、大学においても、対面授業からオンライン授業に切り替えられた。これらの例で見るように、新型コロナウイルス感染症の流行は人々の暮らしと行動様式を大きく変容させ、リアルな空間の中で行われていた営みの多くがサイバー空間の中で行われるようになった。結果として、新型コロナ感染症の流行は、サイバー空間の重要性を一挙に高めた。

このほかにも、サイバー空間を利用したFacebookやTwitter等のソーシャルメディアの普及、YouTube等の動画、LINE等のメッセージアプリの普及が進んだことで、個人の意見を多くの人に訴えることが可能になった。テレビ、新聞、ラジオがブロードキャストの唯一の手段であった時代とは大きく様変わりした。サイバー空間は、個人の意見の発信のみならず、選挙活動や、世論形成、あるいは敵対する相手を攻撃する道具にも使われるようになっている。また、情報の検索においては、検索エンジンの管理者がアルゴリズムを操作することで、誰かにとって都合が良い情報を検索結果の上位に来るような恣意的な操作も可能である。しかし、それを規制する法律も存在しないなど、我が国の制度はサイバー空間の環境変化に追いついていない。そして、サイバー空間を流通する情報の中には偽情報も混じっており、言論の自由を基本とする民主主義国家においては、サイバー空間を流通する情報の真偽の見極めも重要になっている。

2　サイバー空間のリスクの高まり

サイバー空間を行き交うデータは瞬時に国境を越えて流通する。また情報発信者の匿名性が高く、なりすましも可能である。サイバー空間内の攻撃者は、インターネットさえ繋がっていれば、地球上のどこからでもサイバー攻撃が可能である。そのうえ、インターネットの超高速化が進んだ。例えば、不正アクセスに成功すれば短時間で膨大な量の機密情報の摂取も可能である。

組織犯罪や国家の関与が疑われる攻撃が多く発生しており、海外では選挙に対する攻撃をはじめとする民主プロセスへの干渉や、サプライチェーンの弱点を悪用した大規模な攻撃、制御系システムを対象とした攻撃をはじめ広範な社会経済活動、ひいては国家安全保障に影響を与え得るインフラへの攻撃が猛威を奮っている[261]。

サイバー犯罪の取り締まりを担う警察庁は、「国内においてランサムウェアによる感染被害が多発し、事業活動の停止・遅延等、社会経済活動に多大な影響を及ぼしているほか、サイバー攻撃や不正アクセスによる情報流出の相次ぐ発生など、サイバー空間における脅威

[260] 首相官邸・厚生労働省、「3つの密を避けましょう」。
[https://www.kantei.go.jp/jp/content/000061868.pdf]、（2023年1月18日閲覧）。
[261] NISC、「サイバーセキュリティ戦略」2001年9月28 日、9頁。
[https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf]、（2023年1月26日閲覧）。

は極めて深刻な情勢が続いている」と分析結果を公表している[262]。

また、公安調査庁は、「脅威主体（サイバー攻撃者）には、アクティビスト集団、金銭目的の犯罪者、愉快犯、そして国家が関与・支援するサイバー攻撃集団など、多様な主体が含まれ、特に深刻な脅威として懸念されるのは、国家が関与・支援する高度なサイバー攻撃集団」[263]と分析している。そして同庁は、サイバー攻撃集団の特徴として、「重要インフラの破壊、情報操作、諜報活動など、政治的・軍事的な国家目標を達成するため、軍や情報機関のオペレーションとして攻撃を実行、任務達成のためコスト度外視で執ような攻撃を継続、犯罪者や民間のハッカーを外部の協力者・代理人として使う」[264]などを挙げている。

このような状況を踏まえ、2022 年 6 月の G7 首脳会合[265]ならびに 2022 年 4 月の日米豪印首脳会合[266]においてはサイバーセキュリティの強化に向けた各国の連携強化を確認しており、サイバー空間の脅威に対する各国の認識は共通のものとなっている。

3　サイバー空間の脅威の現状

図　22 は国立研究開発法人情報通信研究機構（以下、「NICT」という）がリアルタイムで観測しているサイバー攻撃の状況を表している。攻撃は世界各地から行われていることが見て取れる。

[262]警察庁、「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」、2022 年 9 月 15 日。
[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf]、（2023 年 1 月 17 日閲覧）。
[263] 公安調査庁、「サイバー空間における脅威の概況 2022」、9 頁。
[https://www.moj.go.jp/content/001371280.pdf]、（2023 年 1 月 17 日閲覧）。
[264] 同上、9 頁。
[265] 外務省、「G７首脳コミュニケ」、2022 年 6 月 28 日、27 頁。
[https://www.mofa.go.jp/mofaj/files/100376624.pdf]、（2023 年 1 月 25 日閲覧）。
[266]外務省、「日米豪印首脳会合共同声明」、2022 年 5 月 24 日。
[https://www.mofa.go.jp/mofaj/fp/nsp/page1_001188.html]、（2022 年 10 月 15 日閲覧）。

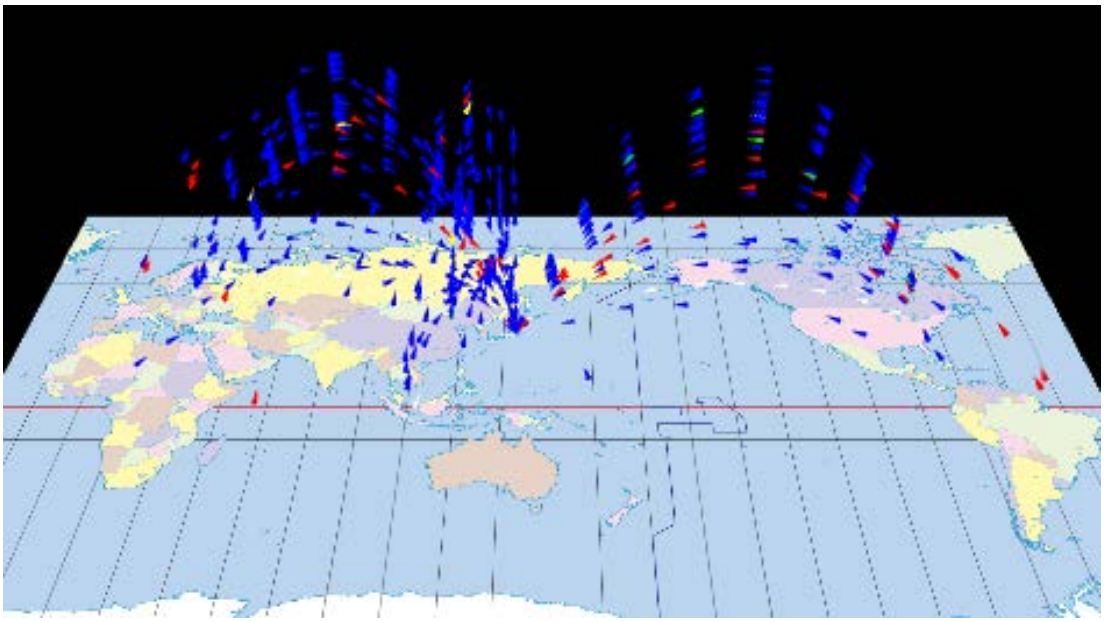


図 22　リアルタイムでのサイバー攻撃状況
出典：国立研究開発法人 情報通信研究機構（NICT）

警察庁においてはインターネット上にセンサーを設置し、サイバー攻撃者が攻撃対象を探索している状況をリアルタイムに把握している。図 23 に示す通り、2022 年上半期には１日・１ＩＰアドレス当たり約 7,700 件と増加傾向にある。検知したアクセスの送信元の国・地域に着目すると、海外を送信元とするアクセス件数が大半を占めている[267]。

[267] 警察庁、「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」、13-14 頁。[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf]、（2023 年 1 月 19 日閲覧）。

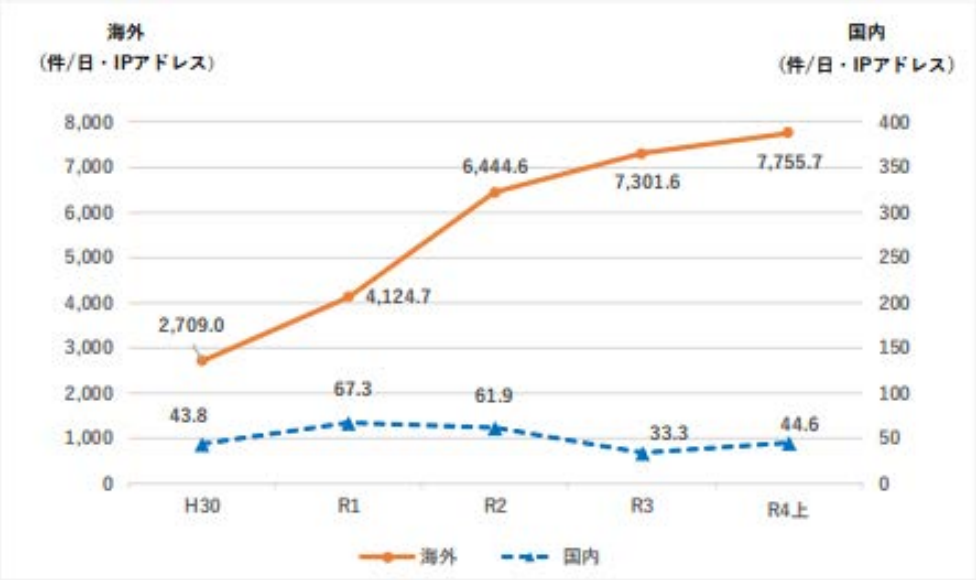


図 23　検知した不正アクセス件数
出典：警察庁

サイバー攻撃は、個人を狙ったフィッシング詐欺から重要インフラへの攻撃、サプライチェーンを狙った攻撃、身代金要求を狙った攻撃、機微技術の窃取を狙った攻撃など、多岐にわたる。個人を狙ったサイバー攻撃はフィッシングが多く、フィッシング対策協議会は、2021 年のフィッシング報告件数は 526,504 件、2020 年と比較して約 2.3 倍、昨今のフィッシングは、基本的にはクレジットカード情報を狙ったものであると公表している[268]。

重要インフラを狙ったサイバー攻撃事案も発生している。日経クロステックは、米国の水道施設（浄水場）がサイバー攻撃を受け、飲用水の水酸化ナトリウム濃度の設定値が 100ppm から 1 万 1100ppm に引き上げられたと報じている[269]。この事案は、幼児や子供も含めた多くの人々を無差別に攻撃する悪質な犯行であると同時に、国民の生命にかかわる重大な事案である。これ以外もパイプラインを狙ったサイバー攻撃[270]、通信事業者を狙ったサイバー攻撃[271]なども確認されている。

サプライチェーンに打撃が及んだサイバー攻撃事案も発生している。日本経済新聞は、「トヨタ自動車に内外装部品を提供する小島プレス工業（愛知県豊田市）がサイバー攻撃を受け、同社のシステムに障害が発生し、この影響により丸 1 日、トヨタが国内に有する全て

[268] フィッシング対策協議会、「フィッシングレポート 2022」、2022 年 6 月、6 頁。
[phishing_report_2022.pdf (antiphishing.jp)]、（2023 年 1 月 20 日閲覧）。
[269] 日経 XTECH、「水道施設に「毒混入」狙ったサイバー攻撃、お粗末すぎるセキュリティーの恐怖」、2021 年 2 月 24 日。
[https://xtech.nikkei.com/atcl/nxt/column/18/00676/021700072/]、（2022 年 10 月 14 日閲覧）。
[270] 2021 年 5 月、米国最大の石油パイプラインであるコロニアル・パイプラインがランサムウェア攻撃を受けた。
[271] 2022 年 9 月、豪州の大手移動体通信事業者であるオプタス社がサイバー攻撃を受けた。

の完成車工場(14工場28ライン、日野自動車の羽村工場とダイハツ工業の京都工場を含む)が稼働を停止し、約1万3000台の生産の遅れが発生した」と報じている[272]。

医療機関を狙ったサイバー攻撃事案も発生している。日本経済新聞は、「徳島県つるぎ町の町立半田病院がランサムウェアによるサイバー攻撃を受け、電子カルテが閲覧できなくなり新規患者の受け入れを停止した」と報じている[273]。地域医療を揺るがす悪質な犯罪である。

機微技術の窃取を狙ったサイバー攻撃事案も発生している。三菱電機は、「サイバー攻撃を受けて防衛関連情報が盗まれた可能性がある」と発表した[274]。発表では、攻撃者はウイルス対策ソフトウェアの脆弱性を突いてシステムへの侵入に成功している。防衛機密に該当する防衛関連情報にまで攻撃者に侵入を許した事実は重い。この手の問題は、安全保障に係る同盟国との連携にも影を落とし、国の信頼を失墜するばかりか、日本とは機微な情報を共有できないという同盟国防衛関係者の認識形成にもつながりかねない。

サイバー攻撃による被害額について日本経済新聞は米IBMの調査を引用し、「サイバー攻撃などによるデータ侵害で企業に発生する損失額は、2022年には1件あたり平均435万ドル（約6億4千万円）と過去最高になった」と報じている[275]。我が国の上場企業の営業利益率は概ね10%程度とすれば、一回のサイバー被害で60億円相当の売り上げを失うことと同じインパクトがあり、企業経営にとって大きな打撃となる。企業の財務体力にもよるが、企業を狙ったサイバー攻撃被害は経営の存続にも影響しかねない。

警察庁は、「宇宙航空研究開発機構（JAXA）をはじめとする国内企業等へのサイバー攻撃を実行した集団の背景に、中国人民解放軍第61419部隊が関与している可能性が高いと結論付けるに至った」と公表している[276]。この事案における攻撃者の真の意図は確認できないが、宇宙技術の窃取を狙った可能性も否定できない。宇宙技術を含め、先端技術の窃取を防ぐには、研究機関や大学のみならず企業のサイバーセキュリティも重要となる。それぞれの組織が日々の対策を確実に実行し、それが漏れなく適切に行われているのかを客観的に評価し、脆弱な状態を放置させない仕組みは現時点では存在しないのが問題である。

---

[272] 日本経済新聞記事、「ハッカーに狙われたトヨタの部品　小島プレスがなぜ」、2022年3月8日。[https://www.nikkei.com/article/DGXZQOUC0319Y0T00C22A3000000/]、（2023年1月19日閲覧）。

[273] 日本掲載新聞、「ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃」、2021年11月12日 。[https://www.nikkei.com/article/DGXZQOUE071OK0X01C21A1000000/]、（2023年1月19日閲覧）。

[274] 三菱電機株式会社、「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」、2020年2月12日。[https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf]、（2023年1月19日閲覧）。

[275] 日本経済新聞記事、「契約書も「サイバー防衛」免責や賠償上限定め紛争予防」、2022年10月15日。[https://www.nikkei.com/article/DGXZQOUC227RQ0S2A920C2000000/]、（2022年10月17日閲覧）。

[276] 警察庁、「令和３年におけるサイバー空間をめぐる脅威の情勢等について（別紙）」、2022年4月7日、1-2頁。[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf]、（2023年1月19日閲覧）。

4　我が国のサイバーセキュリティ政策

（1）基本理念・基本原則

我が国のサイバーセキュリティに関する基本理念は、サイバーセキュリティ基本法（平成26年法律第104号）第3条で6つ示されている。

基本原則はサイバーセキュリティ戦略の中で①情報の自由な流通の確保 、②法の支配、③開放性、④自律性、⑤多様な主体の連携の5つが示されている[277]。

（2）　国の体制

図 24　サイバーセキュリティ政策の推進体制

出典：総務省

我が国のサイバーセキュリティ体制は、サイバーセキュリティ基本法に基づき、内閣にサイバーセキュリティ戦略本部が設置され、内閣官房長官を本部長とし、国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣等を本部員としている。また、同本部は国家安全保障会議（NSC）などとも連携している。

NICT サイバーセキュリティ研究所では、政府の方針を踏まえ、サイバーセキュリティに関する演習、サイバーセキュリティ産学官連携拠点形成、パスワード設定等に不備のあるIoT 機器の調査などの業務（システム名称：NOTICE）を担っている[278]。NOTICE の導入に当たっては、不正アクセス禁止法との関係を整理するために、NICT 法を改正している[279]。

独立行政法人情報処理推進機構（以下「IPA」という。）は、標的型攻撃から組織・企業を

[277] NISC、「サイバーセキュリティ戦略」、2021年9月28日、4-5頁。
[https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf]、（2023年1月22日閲覧）。
[278] NOTICE、「NOTICEについて」。[https://notice.go.jp/] 、（2022年11月30日閲覧）。
[279] NISCに対するヒアリング調査（2022年10月12日実施）。

守るための情報共有体制や、サイバーレスキュー隊による取り組みに加え、攻撃に関する対策情報の発信、各種ガイドブックの公開やセミナー・イベントの開催、一般国民向けの「情報セキュリティ安心相談窓口」など、サイバーセキュリティ対策の向上に向けた、様々な施策を実施している。また、電力・ガス・鉄道などの社会インフラや産業基盤事業者を対象に、自社システムのリスクを認識し、必要なセキュリティ施策の判断ができる人材の育成に取り組んでいる。さらには、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析などを通じて、日本の産業サイバーセキュリティ強化に取り組んでいる[280]。一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」という。）は、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内に関するインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている[281]。

(3)　サイバー攻撃の防御

サイバー攻撃による被害の発生を未然に防ぐには、攻撃者の手口を知り、それに対応した防御が有効である。攻撃者の手口を知るには、攻撃中のパケットストリームの傍受と解析が必要であるが、我が国の現行法制度では防犯を目的とした通信傍受を可能にする法制度が存在していないことが問題である[282]。

経済安全保障上、特に重要な重要インフラにおいては、任務保証[283]の考え方を踏まえ、重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することとしている[284]。

我々が実施した NISC に対するヒアリング調査において、積極防御と攻撃誘因技術の活用

---

[280] IPA、「部門を知る 」。[https://www.ipa.go.jp/shinsotsu/department.html]、（2022 年 11 月 30 日閲覧）。

[281] 一般社団法人 JPCERT コーディネーションセンター、「JPCERT/CC について」。[https://www.jpcert.or.jp/about/]、（2022 年 11 月 30 日閲覧）。

[282] 犯罪が成立した後であれば犯罪捜査のための通信傍受に関する法律（平成十一年法律第百三十七号。以下「通信傍受法」という。）に定める捜査手続きを経て傍受が可能となるが、対象犯罪が限られる上に、ほかに手段がない場合の手段とされている。

[283] 任務保障とは、サイバーセキュリティ戦略(2021 年 9 月 28 日閣議決定)において示す、「企業、重要インフラ事業者や政府機関に代表 されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の 組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方である。

[284] NISC、「重要インフラのサイバーセキュリティに係る行動計画 」、2022 年 6 月 17 日、１頁、脚注。[https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf]、（2023 年 1 月 26 日閲覧）。

については尋ねたところ、「2021 年 9 月に閣議決定された「サイバーセキュリティ戦略」において、「積極的防御」に取り組んでいくということが記載されており、従来、政府機関や金融、電力等の重要インフラといった防御側のセキュリティを高めることが中心であったが、サイバー攻撃の深刻化・巧妙化を踏まえ、脅威に対して、事前に積極的な防御策を講じていくことについて「積極的防御」という言葉を使っている。このほか、2021 年 9 月の戦略には、攻撃誘引技術の活用についても記載されている。今の法律で出来ることについて、工夫して取り組みつつ、今後も発生している又は想定されるリスクに合わせて、国民の権利等との関係を踏まえながら、本当に必要となる制度的手当について慎重に検討する必要がある」とのことであった[285]。

経済安全保障推進法制に関する有識者会議[286]においては、重要インフラにおけるサイバーセキュリティの重要性について議論された。その中では、不正な仕組み（バックドアなど）が重要インフラに組み込まれてしまうサプライチェーンリスク、内部協力者が存在するリスク、ハッキングなどの不正侵入リスクが挙げられている。サイバーセキュリティは事業者の自助努力に任せる仕組みではなく、網羅的・産業横断的に政府として対応する仕組みが必要なことなどが議論された。有識者からは、基幹インフラの安全性・信頼性確保という形で、基幹インフラ設備の導入等の際に事前にリスクを排除することなどが提言された。

2022 年 12 月に閣議決定された国家安全保障戦略においては、サイバー安全保障としてサイバー防御の強化が盛り込まれ、「能動的サイバー防御」の導入及びその実施のために必要な措置の実現に向けた検討が明記された。これらのために、サイバー安全保障の政策を一元的に総合調整する新たな組織の設置、法制度の整備、運用の強化をすることとしている[287]。

5　企業のサイバーセキュリティ

サイバー攻撃が活発化し、被害が増加していく中で、企業においても対策が進められていくと考えられる。しかしながら、企業と一言で言っても大企業、中小企業、重要インフラに関わる企業といった種類に分けられる。それぞれ、取ることのできる対策や求められる対策基準について差が出てくる。これから企業のサイバーセキュリティを高めるためにどうしていくべきかを考えていくにあたり、ここでは、大企業、中小企業、重要インフラについて現状どのような対策が行われ、どういった被害が起きているのかを企業規模別に見ていく。また、企業経営者の意識も重要となってくる。そのため、企業経営者がサイバーセキュリティに対してどのような印象を持っているのかについても見ていく。

---

[285] NISC に対するヒアリング調査（2022 年 10 月 12 日実施）。

[286] 内閣官房、「「経済安全保障法制に関する有識者会議」（第 2 回）議事録要旨」。[https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai2/gijiyousi.pdf]、（2023 年 1 月 25 日閲覧）。

[287] 国家安全保障局、「国家安全保障戦略（概要）」2022 年 12 月。[https://www.cas.go.jp/jp/siryou/221216anzenhoshou/hosyousennryaku_gaiyou.pdf]、（2023 年 01 月 4 日閲覧）。

（1）大企業

大企業のサイバーセキュリティの体制についてはどのようになっているのか。特に大企業は関連子会社や海外支社などの繋がりを持っていることも多く、今後は、そうした関連企業も合わせたサイバーセキュリティの向上が求められる。

大企業であっても、サイバーセキュリティ対策が十分であるとは言えない。日本経済新聞は「日本経済新聞が診断ツールを用いて日経平均を構成する 225 社を独自に調べたところ、サイバー攻撃を受ける危険性がある企業は 4 割弱に上った」と報じている[288]。日経 225 を構成する企業は我が国を代表する企業であり、重要インフラや、自動車、化学、食品、医薬品など、いずれも日本経済を背負う屋台骨である。その屋台骨のサイバーセキュリティが脆弱なことは、我が国にとっても由々しき事態である。

実は問題はこの他にもある。それは、今回は日本経済新聞が調査した結果このような状況にあることが露見したが、このような状態にあることを政府自らが把握できていない点である。

ランサムウェアの被害状況を見ると、企業・団体等におけるランサムウェア被害として、2022 年上半期に都道府県警から警察庁に報告のあった件数は 114 件となっている[289]。これは企業・団体等の全てを合わせた数字である。

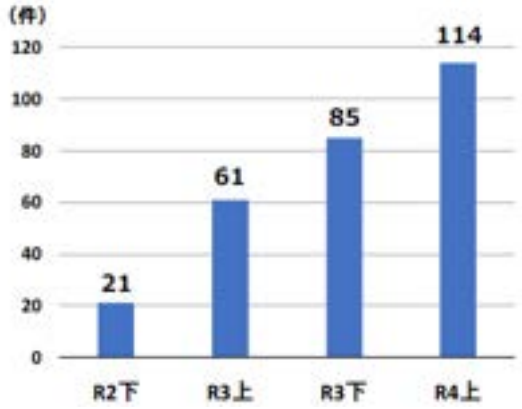


図 25　企業・団体等におけるランサムウェア被害の報告件数の推移
出典：警察庁

この 114 件をさらに細かく見た場合、大企業は 36 件、中小企業は 59 件という結果とな

[288] 日本経済新聞、「大企業のサイバー対策、4 割に危険性、車や機械目立つ」、2022 年 6 月 5 日。[https://www.nikkei.com/article/DGXZQOUC15C8V0V10C22A4000000/?type=my#RQAUAgAAMjAyMTA5MjYyMTExMDg2MzU3NTE2MTQ] 、（2023 年 1 月 21 日閲覧）。

[289] 警察庁、「令和 4 年上半期におけるサイバー空間をめぐる脅威の情勢等について」、2022 年 9 月 15 日、3 頁。[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf] 、（2023 年 1 月 20 日閲覧）。

っている[290]。中小企業の方が件数は多いが、大企業が被害を受けないというわけではない。そして、この被害件数については警察に届け出があったもののみであり、実際にはさらに多くの企業がランサムウェア被害を受けている可能性もある。

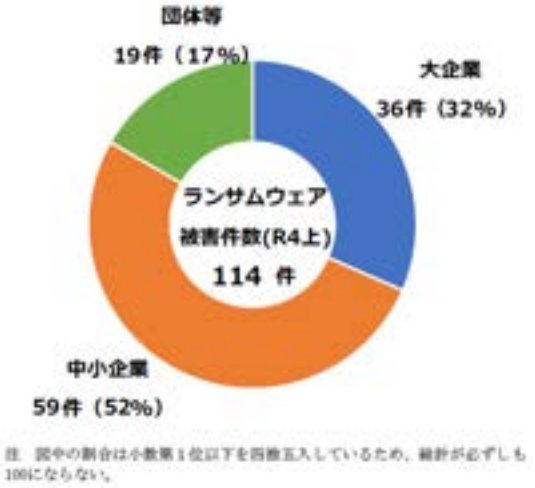


図 26　ランサムウェア被害の企業・団体等の規模別報告件数
出典：警察庁

大企業が国内関連会社、国外関連子会社、国内ビジネスパートナーや委託先についてのセキュリティ対策状況を把握している割合は以下の図の通りである（図 27）。

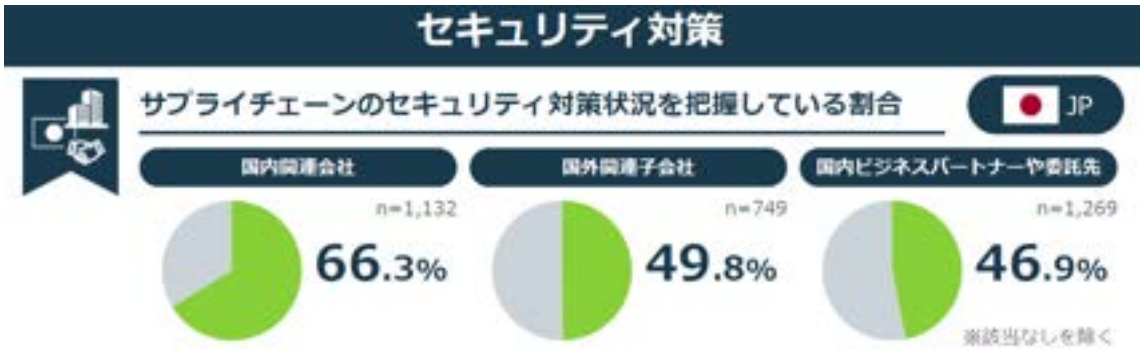


図 27　サプライチェーンのセキュリティ対策状況を把握している割合
出典:野村総合研究所

大企業がサプライチェーンのセキュリティ対策状況を把握している割合は、国内関連会社については 66.3%把握することが出来ている。また、国外関連子会社と国内ビジネスパー

[290]同上、3 頁。（2023 年 1 月 20 日閲覧）。

トナーや委託先については50%以下となっている[291]。

しかし、ここで問題となってくるのが独占禁止法や下請法である。某セキュリティ企業に対するヒアリング調査においても、「中小の取引先があった場合にも、独占禁止法の関係上対策を強要できないようである[292]」とする問題意識があった。

公正取引委員会では、取引先への対策の支援・要請についての考え方の中で、「独占禁止法上問題となるのは、行為者の取引上の地位が相手方に優越していること、また、取引の相手方が今後の取引に与える影響等を懸念して、行為者による要請等を受け入れざるを得ないこと」が前提となるとしている[293]。

(2) 中小企業

中小企業においてもサイバーセキュリティ上の脅威の認識はされている。例として、IPAが調査を行った結果、コンピュータウイルスに対しては約半数以上の割合が非常に大きな脅威として認識しており、不正アクセスについても半数が非常に大きな脅威であるとして認識している[294]。また、被害に遭った場合には、数千万円の損害が発生するおそれがあり、自社のみならず取引先も含めて操業が停止する可能性もある。サプライチェーンを構成する中小企業においてもサイバーセキュリティ対策が求められている[295]。

IPAが中小企業40,000社を対象に実施したアンケート調査結果によれば、情報セキュリティ対策投資を行わなかった理由として、必要性を感じないという割合が40.5%となっており、コストがかかり過ぎるという割合が22.0%となっている[296]。脆弱性診断を行う場合は通常100万円以上の費用が掛かるとされている[297]。

---

[291] NRI SECURE、「NRI Secure Insight 2021 企業における情報セキュリティ実態調査 Since2002」、2頁。[https://www.nri-secure.co.jp/hubfs/NRIS/download/ebook/NRISecure_Insight2021_Report.pdf]、(2023年1月20日閲覧)。

[292] 某セキュリティ企業に対するヒアリング調査(2022年8月3日実施)。

[293] 公正取引委員会、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築に向けて」、2022年10月28日。[https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html#:~:text=%E5%8F%96%E5%BC%95%E4%B8%8A%E3%81%AE%E5%9C%B0%E4%BD%8D%E3%81%8C,%E6%B3%95%E4%B8%8A%E5%95%8F%E9%A1%8C%E3%81%A8%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82]、(2023年1月20日閲覧)。

[294] IPA、「2021年度中小企業における情報セキュリティ対策に関する実態調査―調査報告書―」、42頁。[https://www.ipa.go.jp/files/000097060.pdf]、(2022年12月6日閲覧)。

[295] 経済産業省、「中小企業のサイバーセキュリティ対策」。[https://www.meti.go.jp/policy/netsecurity/sme-guide.html]、(2023年1月20日閲覧)。

[296] IPA、「2021年度中小企業における情報セキュリティ対策に関する実態調査―調査報告書―」、18頁、2022年3月31日。[https://www.ipa.go.jp/files/000097060.pdf] (2022年12月6日閲覧)。

[297] ECサイトの専門家による脆弱性診断の場合の例である。IPA、「中小企業が運営するECサイト向け無償脆弱性診断の募集」、2022年4月12日。[https://www.ipa.go.jp/security/vuln/ec-site/vuln-ec-site2022.html]、(2023年1月20日閲覧)。

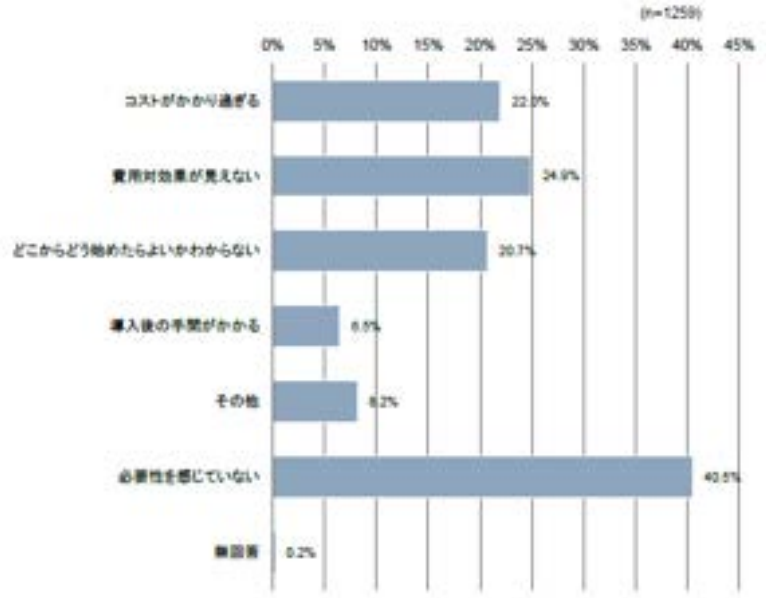


図 28　情報セキュリティ対策投資を行わなかった理由（MA）
出典：IPA

中小企業に向けたサイバーセキュリティ施策として、「SECURITY ACTION」というものがある。これは、中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度である。注意点として、これは情報セキュリティ対策状況について IPA が認定をするわけではなく、あくまで自己宣言を行うものである。取組目標に応じて一つ星と二つ星のロゴマークを使用することが出来る。自己宣言をすることによって情報セキュリティの取組をしていることをアピールすることが出来る[298]。

(3)　重要インフラ企業

重要インフラとは「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生じるもので、重要インフラ分野に属するもの[299]」であるとしている。そして、重要インフラ分野として業種ごとに指定されているのは、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「科学」、「クレジット」及び「石油」の 14 分野である

重要インフラがサイバー攻撃され機能停止に陥った場合、国民生活に大きな影響を及ぼ

[298]IPA 、「SECURITY ACTION とは？」。
[https://www.ipa.go.jp/security/security-action/sa/index.html] 、（2023 年 1 月 22 日閲覧）。
[299] NISC、「重要インフラのサイバーセキュリティに係る行動計画」、2022 年 6 月 17 日。
[https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf] 、（2023 年 1 月 20 日閲覧）。

し、場合によっては国民の生命財産にも影響が及ぶ。 サイバーセキュリティ基本法第１条に基づき設置されているサイバーセキュリティ戦略本部は「重要インフラのサイバーセキュリティに係る行動計画」[300]を 2022 年 6 月に作成した。この中で、重要インフラにおいては、任務保障[301]の考え方を踏まえて、重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制するとしている[302]。

重要インフラを担う通信、電力事業者に対して我々が実施したヒアリング調査では、NTT においては、「調達する通信設備のサプライヤーに対して NTT が納入するハードウェアおよびソフトウェアにおいて悪意をもった改変がされないように要請するとともに、NTT のネットワークと外部のネットワークを接続するポイント等において、UTM （Unified Threat Management）などにより攻撃を防御、24 時間、365 日、ネットワークのセキュリティ情報を常時監視し、インシデントが発生した場合には速やかに回復措置をとるとともに、原因究明のうえ再発防止、セキュリティに関する最新動向の把握、対応する人材の育成などを行っている」とのことである。一方、部品レベルの情報収集の在り方として、「NTT は必要に応じて完成品メーカーに対して情報収集の依頼を出すと想定しているが、完成品メーカーよりも上流（先）にあたる２次以降メーカーの部品に関する情報については、完成品メーカーから回答を得られる保証はない」とのことである[303]。これは、サプライチェーン上のサイバーセキュリティリスクの完全排除の難しさを表している。つまり、製造過程でバックドア[304]等を仕込まれるリスクを排除することはできない。

米国においては「情報通信技術・サービス（ICTS）サプライチェーンの安全確保」に関する大統領令 13873 号により安全を担保している[305]。

KDDI は、「通信インフラの不正使用により障害を引き起こされる、いわゆるサイバーテロから自らの通信インフラを守るため、外部攻撃に対する専門組織による 24 時間 365 日での監視や ICT-ISAC を通じた他事業者との連携など、常に適切な防御措置を講じている」と

---

300 NISC、「重要インフラのサイバーセキュリティに係る行動計画」、2022 年 6 月 12 日、１頁。[https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf]、（2023 年 1 月 25 日閲覧）。

301 サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」

302 NISC、「重要インフラのサイバーセキュリティに係る行動計画」、2022 年 6 月 12 日。[https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf]、（2023 年 1 月 25 日閲覧）。

303 NTT に対するヒアリング調査（2022 年 6 月 17 日実施）。

304 装置製造段階で秘密裏に設置される裏口で、敵対勢力によるシステムの遠隔操作が可能になる。これにより、データの窃取、ルーティング情報の書き換え削除も可能。さらに、重要インフラ機能を麻痺させることも可能。

305 東京海上ディーアール株式会社、「リスクマネージメント最前線、2022、No.8」、6 頁、脚注。[https://www.tokio-dr.jp/publication/report/riskmanagement/pdf/pdf-riskmanagement-367.pdf]、（2023 年 1 月 25 日閲覧）。

述べている[306]。

東北電力は、「発電設備等の制御系システムについては閉域ネットワークで運用しているため外部側からのアクセスは出来ない仕組みになっており、セキュリティに関する危機管理体制として「東北電力ーSIRT」を設置し、24 時間体制でセキュリティを監視し、セキュリティ事故の未然防止と事故発生時の被害最小化に努めている」と述べている。そのうえで、「電力事業者間（電力 ISAC）での情報共有も日頃から行っているが、APT[307]などから執拗に攻撃された場合、一民間だけでは対応は難しい」との見方も示している[308]。

一方、電気通信事業者を所管する総務省によれば、実際に重要インフラが大規模サイバー攻撃を受けた際には、大規模サイバー攻撃事態（「大規模サイバー攻撃事態等への初動対処について」（平成二十二年三月十九日内閣危機管理監決裁）等に基づき、政府一体となった初動対処体制をとるとのことである[309]。

NATO サイバー防衛協力センター（CCDCOE）が主催するサイバー防衛演習「ロックド・シールズ 2022」には重要インフラ事業者も参加し、サイバー攻撃への対処能力向上及びサイバーセキュリティ動向の把握を進めている[310]。

（4） 企業経営者の意識

NRI セキュリティテクノロジー社 の調査結果によれば、セキュリティ対策を実施するきっかけや理由を調査した結果によれば、日本では「他社でのセキュリティインシデント事例」が 1 位であった[311]。このことから、セキュリティに対する意識の向上には他社の被害事例が有効であることが裏付けられる。一方、IPA はサイバーセキュリティ経営ガイドラインの中で、経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えてしまった場合の経営責任や法的責任などを指摘したうえで、経営者はセキュリティ対策を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることの重要性を訴えている [312]。

企業経営者の使命は利益を生み出し経営を存続させることであるが、そのためには、サイバーセキュリティ対策が必要不可欠な投資であることをいかに啓発できるか、企業経営者

---

306 KDDI に対するヒアリング調査（2022 年 8 月 9 日実施）。

307 APT（Advanced Persistent Threats）攻撃とは、主に組織や集団が、特定の組織や企業に対して、様々な手段を用いて持続的に行うサイバー攻撃を指す。

308 東北電力に対するヒアリング調査（2022 年 10 月 4 日実施）。

309 経済産業省サイバーセキュリティ統括官室に対するヒアリング調査(2022 年 9 月 22 日実施)

310 防衛省・自衛隊、「NATO サイバー協力センターによるサイバー防衛演習「ロックド・シールズ 2022」への参加について」、2022 年 4 月 19 日。
[https://www.mod.go.jp/j/press/news/2022/04/19e.html]、（2022 年 11 月 23 日閲覧）。

311 NRI セキュリティテクノロジー社、「NRI Secure Insight 2021」、16 頁。
[https://www.nri-secure.co.jp/hubfs/NRIS/download/ebook/NRISecure_Insight2021_Report.pdf]、（2022 年 12 月 3 日閲覧）。

312経済産業省・IPA、「情報セキュリティ経営ガイドライン Ver2.0」、1 頁。
[https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf]、（2023 年 1 月 24 日閲覧）。

の意識改革が重要な問題である。

6　サイバーセキュリティ人材の確保・育成に向けて

我が国ではサイバーセキュリティ人材が近年急激に増加したが、IT の利活用の場面は一層増え、それに伴いサイバー空間における脅威もこれまで以上に高まっている。現状として、多くの企業でサイバーセキュリティ人材が不足しており、専門人材の配置やセキュリティ対策投資、サプライチェーンへの統制状況も不十分である。

(ISC)²（International Information Systems Security Certification Consortium）は、サイバーセキュリティ人材の規模と人材不足を評価するため、「(ISC)² Cybersecurity Workforce Study」を毎年実施している。2022 年版の「(ISC)² Cybersecurity Workforce Study」によると、世界のサイバーセキュリティ人材は、過去最高水準となる約 470 万人（前年比 5.5%増）であり、日本においても約 39 万人（前年比 40.4%増）と、サイバーセキュリティ人材は大きく増加している。サイバーセキュリティ人材が急速に増加する一方で、サイバーセキュリティ人材の不足はさらに深刻化している。サイバーセキュリティ人材の不足数は世界全体で約 343 万人（前年比 26.2%増）、日本においては約 5 万 6 千人（前年比 37.9%増）不足している[313]。

また、NRI セキュアテクノロジーズ株式会社は企業のサイバーセキュリティに関する実態調査を毎年実施しており、「NRI Secure Insight 2021」[314]では、日本、米国、豪州の 2653 社の企業を対象に調査を行った。セキュリティ対策に従事する人材の充足状況について、米国及び豪州では 8 割以上の企業が「充足している」と回答した一方、日本では約 9 割の企業が「不足している」と回答した。

図 29　セキュリティ対策に従事する人材の充足状況
出典：野村総合研究所

313　(ISC)², “Cybersecurity Workforce Gap & Estimate,” (ISC)² Cybersecurity Workforce Study, 2022, October 2022, pp.5-9.
314 NRI セキュアテクノロジーズ、「NRI Secure Insight 2021」、13 頁。
[https://www.nri-secure.co.jp/insight2021]（2023 年 1 月 14 日閲覧）。

企業のセキュリティ担当者として最も対応に困っている事項については、日本の企業においては「セキュリティ人材の育成」（41.1%）が最も多く、「セキュリティインシデント発生時の緊急対応」（35.1%）、「サイバー攻撃の高度化への対応」（33.8%）と続く。企業のセキュリティ担当者としても、セキュリティ人材の育成が懸念事項となっており、また、自社内でのセキュリティインシデント発生時の緊急対応や、より高度なサイバー攻撃への対応ができる人材の確保・育成も急務と言える。さらに、セキュリティマネジメントの観点からは、CISO(Chief Information Security Officer)の設置率は、米国や豪州では9割を超えるのに対して、日本においてはCISOの設置率は50%以下に留まる。

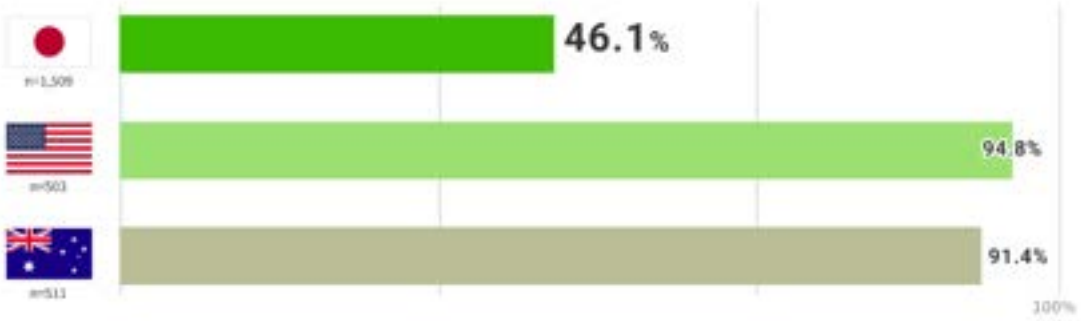


図 30　情報システム及びセキュリティを統括する人材（CISO）の設置状況
出典：野村総合研究所

また、他国が新規セキュリティ対策予算を増額するなか、日本における新規セキュリティ対策への投資額は昨年度からほぼ横ばいとなっている。

図 31　昨年度と比較した新規セキュリティ対策予算（BIT*）の増減
出典：野村総合研究所

加えて、パートナー・委託先や関連子会社といったサプライチェーンへの統制についても、

自社のセキュリティ水準を満たすように改善要求している企業は少なく、セキュリティ対策状況を把握すらしていない企業も多い。

図 32　サプライチェーンへの統制状況
出典：野村総合研究所

サイバーセキュリティを担う人材の数を官民双方で確保することに加え、人材の確保・育成を加速化させるために産官学と連携した若手人材の育成が求められる。また、攻撃者側の視点に立った防御スキルを有する技術者の育成も重要である[315]。

2021 年に策定された「サイバーセキュリティ戦略」では、セキュリティに係る人材育成に関して、「DX with cybersecurity の推進」として「プラス・セキュリティ」知識を補充できる環境整備や、「巧妙化・複雑化する脅威への対処」として人材教育プログラムの強化や人材育成共有基盤の構築が盛り込まれた。情報セキュリティ専門人材の需要は更に伸びるとともに、DX 推進によりセキュリティ関連業務を主とする職種以外においてもセキュリティ能力を持った人材の需要が高まっている[316]。

各国を比較した NRI セキュリティテクノロジー社の調査では、セキュリティに対する人材の充足状況は、日本は７％であるのに対し、米国／豪州では 85%以上であった[317]。日本企業の殆どにおいて人材が不足している結果であった。

人材育成と確保に関する課題について、国際サイバーセキュリティ協会代表理事鶴保征城氏は「サイバー攻撃に対する企業の危機意識が低いことだ。日本ではセキュリティ人材を外部に頼る傾向があった。しかし、攻撃の原因となる抜け穴は各業界で異なる。社内で人セキュリティに適したセキュリティを構築していくのがよい。経営層の意識を変えることも重要だ 」と日本経済新聞で述べている[318]。他方、サイバーセキュリティ技術者の処遇改善・

[315] 某セキュリティ会社に対するヒアリング調査（2022 年 8 月 3 日実施）。
[316] IPA『情報セキュリティ白書 2022』、独立行政法人情報処理推進機構、第 1 版、2022 年、101 頁。
[317] NRI セキュリティテクノロジー社、「NRI Secure Insight 2021」、13 頁。[https://www.nri-secure.co.jp/hubfs/NRIS/download/ebook/NRISecure_Insight2021_Report.pdf]、（2022 年 10 月 14 日閲覧）。
[318] 日本経済新聞、「サイバーセキュリティ人材育成「アジア共通資格めざす」」、国際サイバーセキュ

地位の向上もセキュリティ人材を確保する上での課題となっている[319]。

各省庁で行われている現在の取組として、総務省では、NICT の「ナショナルサイバートレーニングセンター」を通じて、サイバーセキュリティ人材育成の取組（CYDER、SecHack365）を積極的に推進している[320]。CYDER は、国の機関、重要インフラ事業者などの情報システム担当者を対象とした実践的サイバー防御演習であり、受講者は、チーム単位で演習に参加し、組織のネットワーク環境を模した大規模仮想 LAN 環境下で、実機の操作を伴ってサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験する演習である[321]。2017 年度（平成 29 年度）からの合計で 13,867 名が受講しており、2021 年度（令和 3 年度）から、従来の初級・中級の集合演習コースの実施に加え、サイバーコロッセオ[322]の知見を活用した、より高度なセキュリティ技術を習得可能な準上級コースや、地理的・時間的要因などにより CYDER が受講できていない者への最低限の対応をするオンライン演習のコースを追加した[323]。

SecHack365 は、日本国内に居住する 25 歳以下の若手 ICT 人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材（セキュリティイノベーター）を育成するプログラムである。NICT の持つ実際のサイバー攻撃関連データを活用しつつ、第一線で活躍する研究者・技術者が、セキュリティ技術の研究・開発などを 1 年かけて継続的かつ本格的に指導する。2021 年度（令和 3 年度）は 41 名が修了し、2017 年度（平成 29 年度）からの合計で 212 名が修了している[324]。

リティ協会代表理事　鶴保征城氏発言、2021 年 12 月 21 日。
[https://www.nikkei.com/article/DGXZQOUC08ARV0Y1A201C2000000/]、（2022 年 12 月 2 日閲覧）。

[319] 某セキュリティ会社に対するヒアリング調査（2022 年 8 月 3 日）。

[320] 総務省、「令和 4 年版　情報通信白書」、160-161 頁。
[https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/n4500000.pdf]、（2023 年 1 月 15 日閲覧）。

[321] 総務省、「令和 4 年版　情報通信白書」、160 頁。
[https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/n4500000.pdf]、（2023 年 1 月 15 日閲覧）。

[322] NICT、「東京 2020 オリンピック・パラリンピック競技大会に向けた実践的サイバー演習「サイバーコロッセオ」の実施について」、2017 年 12 月 7 日。
[https://www.nict.go.jp/press/2017/12/07-1.html]、（2023 年 1 月 25 日閲覧）

[323] 総務省、「令和 4 年版　情報通信白書」、160-161 頁。
[https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/n4500000.pdf]、（2023 年 1 月 15 日閲覧）。

[324] 総務省、「令和 4 年版　情報通信白書」、161 頁。
[https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/n4500000.pdf]、（2023 年 1 月 15 日閲覧）。

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	47都道府県	68回	7月～翌年2月
B-1		中級	システム管理者・運用者（主体的な事案対応・セキュリティ管理）	地方公共団体	全国11地域	21回	10月～翌年2月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	13回	翌年1月～2月
C		準上級	セキュリティ専門担当者（高度なセキュリティ技術）	全組織共通	東京	3回	翌年1月～2月
オンライン A	オンライン演習	初級	システムに携わり始めた者（事案発生時の対応の流れ）	全組織共通	（受講者職場等）	随時	11月～翌年3月（6～8月に試験提供）

令和3年度から新規開設

図 33　令和 3 年度 CYDER 実施状況
出典：令和 4 年版　情報通信白書

経済産業省では、情報処理安全確保支援士制度を設け、専門人材に求められる能力の「見える化」を図っている。情報処理安全確保支援士は、サイバー攻撃の急激な増加に対し、政府機関や企業等のセキュリティ対策強化に向けて、サイバーセキュリティに関する実践的な知識・技能を有する専門人材の育成と確保を目的とした国家資格であり、その登録事務（受付・実施等）は IPA において実施している[325]。資格取得後も、サイバーセキュリティに関するリスクが日々、高度化・多様化していることを踏まえ、最新の知識・技能を維持、向上するための講習の受講を義務づけている[326]。また、IPA は、標的型攻撃や内部不正などのサイバー空間における脅威を、適切な情報管理や業務フローの見直し、組織内規定順守のための従業員の意識向上といった、人的管理面の対策も重要であるとの背景から、情報セキュリティマネジメントを担う人材の育成を推進するため、情報セキュリティマネジメント試験も実施している[327]。

IPA では若者を対象とした人材育成事業として、セキュリティ・キャンプを開催している。情報セキュリティに関する高い意識と技術力を持った人材の発掘と育成を行うべく、22 歳以下の若者を対象に、合宿形式での講習会を実施している[328]。2004 年に開始され、現在は全国大会を首都圏で毎年 1 回、2013 年に開始された地方大会を毎年各地で 10 回程度開催している[329]。さらに、セキュリティ・キャンプフォーラムというイベントは、過去にセキュリティ・キャンプに参加した修了生どうしや講師等との年度を超えた交流の場の提供、および修了後の活動成果発表を通じた修了生の認知度向上と産業界での活躍に向けたきっかけの提供、という 2 点を目的として毎年実施されている。

[325] 経済産業省、「IT 人材の育成」。[https://www.meti.go.jp/policy/it_policy/jinzai/index.html]、（2023 年 1 月 16 日閲覧）。
[326]同上。（2023 年 1 月 25 日閲覧）。
[327]IPA、「情報セキュリティマネジメント試験とは」。[https://www.jitec.ipa.go.jp/sg/about.html]、（2023 年 1 月 22 日閲覧）。
[328] 情報処理推進機構、「セキュリティ・キャンプ」。
[https://www.ipa.go.jp/jinzai/camp/index.html]、（2023 年 1 月 16 日閲覧）。
[329] 同上。

7　サイバー被害への対応

（1）犯罪捜査

警察機関はサイバー犯罪成立後に捜査を開始するが、先に述べたように海外からの攻撃が大部分を占める中で、他国には我が国の管轄権が及ばないため、最も疑わしいと推定される非友好国への捜査については、当該国からの協力は得られず追跡が及ばないなど、捜査には限界がある。

警察庁長官官房長の小島裕史氏は政府参考人として第 208 回国会 参議院内閣委員会のなかで次のように発言している。「ランサムウェアを用いた事案を始めとする重大サイバー犯罪には、捜査等を通じて攻撃者を特定し責任を負わせることにより、犯罪者らに警告を与え抑止を進めることが重要である。他方、この種の事案は、攻撃者が海外にいるなどの理由から一つの国単独で捜査することは困難であるため、各国との国際連携を進め、共同で捜査し、その抑止に取り組むことが不可欠である。しかし、これまでの外国捜査機関との連携においては、捜査機関を持たない警察庁は都道府県警察との窓口にすぎず、案件ごとに捜査を担当する都道府県警察が入れ替わっていくために、国際連携の前提となる外国捜査機関との継続的な信頼関係の構築を進めることが困難な状況にある」[330]。このような状況に対応するため、国の捜査機関として直接に捜査を行う関東管区警察局サイバー特別捜査隊を設置し、日本警察として外国捜査機関との円滑な国際連携を進め、重大サイバー事案の捜査を通じた抑止に取り組むために、2022 年 3 月、警察法の一部の改正案が可決成立した。

サイバー攻撃の殆どは海外からの犯行であり、国際捜査機関との連携が欠かせないことは前述のとおりであるが、そのためには相互信頼が重要なことは言うまでもない。

日本経済新聞は、「データを暗号化して金銭を要求するランサムウエア（身代金要求型ウイルス）の一種に対し、警察庁がウイルスの暗号を強制解除し、国内企業 3 社でデータの復元に成功」と報じている[331]。このような実績捜査当局からの頼られるような存在になることが、犯罪捜査に不可欠な国際連携の基礎を築くと考える。

（2）　被害情報の共有

サイバー攻撃被害によって企業が保有する顧客の個人情報が漏えいした場合は、「個人データの漏えい等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第 1 号）[332]の中で「漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発

---

[330] 参議院、「第 208 回国会 参議院内閣委員会 第 5 号」、政府参考人 小島裕史氏の答弁、2022 年 3 月 29 日。
[https://kokkai.ndl.go.jp/simple/detail?minId=120814889X00520220329&spkNum=0#s0]、（2022 年 11 月 23 日閲覧）。

[331] 日本経済新聞、「身代金ウイルス、警察庁が暗号解除成功　支払い未然防止」、2022 年 12 月 28 日。
[https://www.nikkei.com/article/DGXZQOUE062930W2A201C2000000/?type=my#RQAUAgAAMjAyMTA5MjYyMTExMDg2MzU3NTE2MTQ]、（2022 年 12 月 31 日閲覧）。

[332]内閣府 個人情報保護委員会、「個人データの漏えい等の事案が発生した場合等の対応について」。
[https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf]、（2023 年 1 月 20 日閲覧）。

生防止等の観点から、事実関係及び再発防止策等について、速やかに公表する」と規定されているため、被害情報は公表されることにより間接的ではあるが共有される。しかし、我が国の現行の法制度では、個人情報保護法第２６条（漏えい等の報告等）が義務付けられているものの、個人情報の漏洩を伴わない事案についての報告義務はない。

我々が某サイバーセキュリティ企業に行ったヒアリング調査[333]では、現在の情報共有枠組みとしては法的根拠のあるサイバーセキュリティ協議会や IPA が主導する J-CSIP が存在するものの、サイバーセキュリティ企業にとって被害情報の共有は、手間が掛かる割には、得られるメリットが少なく、モチベーションに繋がらないことが分かった。被害情報を共有するにしても、被害解析で得たデータと、お客様から預かった情報を含むデータに大別すると、後者に関しては一般的にはそのまま提供することができないため、提供の可否について個々の判断も必要となり、手間と時間を要することが問題であることが分かった。

我々が国立研究開発法人情報通信研究機構に行ったヒアリング調査[334]では、被害情報が集まらなければ、データ負けによる「負のスパイラル」が生じ、これが大きな問題と認識されていることが分かった。負のスパイラルとは、①データが集まらない → ②研究開発/人材育成できない → ③国産技術を作れない →③国産技術が世界に普及しない → ④海外製品が跋扈→⑥データは海外へ→⑦データが集まらないことを指す。今のままでは大量のデータを集めることが出来ている海外企業にはかなわないこと、また、国内にある貴重なデータを可能なかぎり共有しそれを活かしていけるような環境が必要であること、そしてサイバー攻撃被害を受けたシステムの痕跡を調べ攻撃の手口を知ることはサイバー攻撃からシステムを守るための手掛かりとなることが分かった。

我々が NISC に行ったヒアリング調査[335]では、情報共有する場合には、お互いに信頼出来る関係性も重要であり、さらに情報の取り扱いにも注意が必要であることが分かった。例として、脆弱性に関する情報を共有するときに、その脆弱性の対策が講じられる前に、悪意のある者に伝わると、その脆弱性を悪用した攻撃に繋がってしまうおそれも考えられるほか、会社の場合は、顧客や取引先等との関係もあることから、顧客等に連絡して対策を取ってもらった後で情報共有するなどの注意が必要である。

我々が経済産業省商務情報政策局サイバーセキュリティ課に行ったヒアリング調査[336]では被害の拡大を防ぐには攻撃技術情報が重要であり、いかに素早く攻撃技術情報の共有を進めることができるか問題であることが分かった。

8　パブリック・アトリビューション

パブリック・アトリビューションは、国家による不正なサイバー活動を抑止するため、攻

[333] 某セキュリティ会社に対するヒアリング調査（2022 年 8 月 3 日実施）。
[334] 国立研究開発法人情報通信研究機構に対するヒアリング調査（2022 年 9 月 22 日実施）。
[335] NISC に対するヒアリング調査（2022 年 10 月 12 日実施）。
[336] 経済産業省商務情報政策局サイバーセキュリティ課に対するヒアリング調査（2022 年 8 月 31 日実施）。

撃実行者と背後にいる国家機関を特定・公表する取り組みを指す[337]。

我々が実施した警察庁へのヒアリング調査[338]では数多くの知見が得られた。その要点は次のとおりである。一、国家を名指しで批判すれば、当該国家は関与を否定するとしても、国際社会から国際法違反を非難されることとなり、非難を払拭するにも相応のコストがかかることから、行動変容は期待されること。二、日本の警察にはテクニカルスタッフが多くおり、その人たちの緻密な解析技術があれば他国にも貢献できること。三、サイバー攻撃の過程も含めた日本国内の痕跡を調べ、証拠を集め、パズルのピースを少しでも多く集めることができれば、サイバー攻撃の攻撃者の特定に役立ち、他国と協働で攻撃者の全体像を描くことに貢献することとなり、日本の警察のプレゼンスも向上すること。四、サイバー攻撃の捜査は国境を越えた国際捜査とならざるを得ず、捜査に時間を要する上、 様々なサーバーを経由している場合には実行者の特定が困難となること。五、国家が関与しているものもあるため、仮に攻撃者を特定したとしても、相手国が引き渡すかどうかといった問題があること。

アトリビューションを効果的に行うには、通常の捜査では被害を受けたサーバーなどの情報機器に残された通信記録を解析することで攻撃者の IP アドレス、MAC アドレスなどを特定するが、残された通信記録が消去されているなど、攻撃者の特定に十分な証拠が得られない場合がある。より多くの証拠を取集するには、攻撃者側のシステムに侵入し通信記録などの情報の収集・分析が有効である。しかし、我が国においては不正アクセス禁止法により他人の情報システムへの侵入は禁じられている。また、相手国の同意なしに行えば違法となる[339]。

9　能動的サイバー防御

サイバー空間を監視し、疑わしい挙動をする相手のシステムに潜入し、機能を麻痺させる行為、あるいは攻撃者の無力化や追跡プログラム等を埋め込む行為、いわゆる「能動的サイバー防御」を我が国が備えることは、サイバー攻撃側にとっては脅威となり攻撃を思いとどまらせる一定の効果が期待できる。しかし、我が国は技術的な面ではこのような能力はあっても、現行の法制度下においては、不正アクセス禁止法および刑法[340]に抵触するため、今すぐにはこの手法は使えない。

2022 年 12 月に閣議決定された国家安全保障戦略において、「能動的サイバー防御」が明記されたことを受けて、今後、国のどの組織がこの任務にあたり、どのような行為まで許容するのかなどの詳細について議論され、不正アクセス禁止法、刑法との関係性を考慮した新たな立法措置あるいは既存の法改正等の検討も並行して進められると考えられる。

---

[337] 公安調査庁、「サーバー空間における脅威の概況　2021）、7 頁。
[https://www.moj.go.jp/content/001343410.pdf]、（2023 年 1 月 26 日閲覧）。
[338] 警察庁サイバー情報参事官室に対するヒアリング調査（2022 年 7 月 7 日実施）。
[339] 中谷和弘、河野桂子、黒﨑将広 、『サイバー攻撃の国際法（タリンマニュアル 2.0 の解説）』、新山社、2018 年、14 頁。
[340] 刑法 168 条の 2 および 168 条の 3 で規定する不正指令電磁的記録に関する罪に該当する。

諸外国では既に能動的サイバー防御を実施しているとの情報は存在するが、活動自体も秘密裏に行われる性質のものであるため、我々の調査では証拠として裏付けられる情報には辿り着けなかった。

サイバーセキュリティ技術に詳しいNTTの秋山満昭氏は、NTTが公式に配信している動画の中で「サイバー攻撃からの防御には早期探知や攻撃元の特定や攻撃の未然防止のための相手方システムへの侵入など「能動的サイバー防御」が欠かせない。また、攻撃者の視点に立ち、システムやサービスの潜在的なプライバシー・セキュリティ脅威を発見して対処することで攻撃を未然に防ぐこと、そして攻撃者の先回りをして問題を発見することも重要である」と述べている[341]。

また、サイバーセキュリティに詳しい某セキュリティ企業の専門家は我々のヒアリング調査において「攻撃者の視点に立ってシステムやサービスの潜在的な欠陥を攻撃者に先んじて発見し、悪用される前に対策を講じることで被害を防ぐことが出来る。しかし、攻撃者側の視点に立った攻撃スキルを有する技術者が殆どいないなど、能動的サイバー防御を進めるにも様々な問題ある」と述べている[342]。

日本経済新聞編集委員の小柳建彦氏は、「ワイパーのようなデータ破壊型のサイバー攻撃は、攻撃を実行されてから対処する「受動的防御」では手遅れになりがちだ。このため、本格攻撃を受ける前に攻撃者の正体とマルウェアなどの「武器」を特定して破壊する、積極的防御を有効にできるかどうかがサイバー防衛のカギだ」と述べている[343]。

サイバー空間の脅威が高まっている状況においては、能動的サイバー防御を可能にする法整備が急がれる。

10　サイバーセキュリティとインテリジェンスの関係性

NTT チーフ・サイバーセキュリティ・ストラテジストの松原実穂子氏は「能動的なサイバー防御と懲罰的抑止のいずれの実行においても不可欠なのが、様々な情報源から収集した情報を精査・分析して現状を把握し、次にどのような行動を取るかの判断材料にするインテジェンス」であると述べている[344]。

サイバー攻撃者が誰であるか、何を意図しているのかを把握することは重要であり、そのためにはインテリジェンスは不可欠である。また、パブリック・アトリビューションをより

---

[341] NTTプラットフォーム研究所、「オフェンシブ セキュリティへのアプローチ」、上席特別研究員　秋山満昭氏。
[https://www.bing.com/videos/search?q=%e3%82%aa%e3%83%95%e3%82%a7%e3%83%b3%e3%82%b7%e3%83%96%e3%82%bb%e3%82%ad%e3%83%a5%e3%83%aa%e3%83%86%e3%82%a3&&view=detail&mid=30F182455A79893ACDEF30F182455A79893ACDEF&&FORM=VDRVSR]、（2022年10月17日閲覧）。

[342] 某セキュリティ会社に対するヒアリング調査（2022年8月3日実施）。

[343] 日本経済新聞、「ウクライナが問うサイバー防衛（下）」、2022年9月8日。
[https://www.nikkei.com/article/DGXZQODK2282N0S2A820C2000000/?type=my]、（2022年11月18日閲覧）。

[344] 新潮社Foresight、「波紋を広げる「アクティブ・ディフェンス」解釈論争とサイバー攻撃者の暗殺 」、2021年10月8日。 [https://www.fsight.jp/articles/-/48319]、（2022年11月23日閲覧）。

効果的に実施可能にするためにもインテリジェンスは必須と考える。

11　セキュリティ技術者の視点

我々が某セキュリティ企業へ行ったヒアリング調査[345]では多くの知見を得ることが出来た。一、現行法制では、企業はサイバーセキュリティの脆弱性を放置しても罰せられず、誰も改善を強制することは出来ないこと。二、NISC や JPCERT/CC が深刻で影響範囲の広い情報セキュリティ上の脅威脆弱性、およびソフトウェアなどの脆弱性と対策情報を公開し注意喚起をしているが、企業はそれを無視できること。三、脆弱性の存在を知らない、脆弱性への知識がない、使っているソフトウェアの情報を知らないことが、脆弱性が放置される背景にあること。四、公的機関が企業のソフトウェア使用状況の情報を定期的に収集し、脆弱点を有するソフトウェアを使用する企業に適時通知し、ソフトウェアのアップデートをフォローする仕組みがあれば脆弱性解消に役立つこと。

某セキュリティ企業は、セキュリティインシデントが発生したときに被害報告義務がないことも問題視し、「必ずしも一般公表する必要はないが、被害の情報を公的機関等に報告し、その内容をセキュリティ事業者や捜査機関が把握・共有することは、同様の手口による被害を未然に食い止めるのに役立」つと見ている。

某セキュリティ企業によれば、「公開サーバーなどのセキュリティ診断が不完全な例も散見され、新しい Web サービス開始時等のセキュリティ診断のみでは不十分であり、定期的なセキュリティ診断は必要であるとしたうえで、セキュリティ診断実施のお墨付きだけを求める企業も存在し、脆弱点が見つかっても黙認したり、それを隠したり、改善しないまま放置しているケースも散見される」とのことであった。また、クレジットカード決済基盤を提供するメタップスペイメント社のデータベースから顧客情報などが流出したケースを例に挙げ、「メタップスペイメント社 は脆弱点を認識していたにもかかわらず、それを隠し続けていたことが問題であり、先ずはそうした部分を改善することが必要である」との見方を示している。

12　海外のサイバーセキュリティ政策

サイバー攻撃の脅威にさらされている国は日本だけではない。海外においてもサイバーセキュリティの脅威にさらされている国は存在している。2021 年は、世界的にランサムウェア攻撃による被害が拡大した[346]。

サイバーセキュリティ対策等について、イギリスのシンクタンクである国際戦略研究所（IISS）が各国のサイバー能力を発表しており、日本は 3 段階中最も低いグループとなっていた[347]。

---

[345] 某セキュリティ会社に対するヒアリング調査（2022 年 8 月 3 日実施）。
[346] 公安調査庁、「サイバー空間における脅威の概況 2022」、4 頁。
[https://www.moj.go.jp/content/001371280.pdf]、（2023 年 1 月 5 日閲覧）
[347] 兼原信克、『現実主義のためのリアル』、ビジネス社、2021 年、48 頁。

IISS では、サイバー能力を評価するための新たな方法論として、各国のサイバーエコシステムを分析し、国家安全保障、経済競争、軍事問題がどのように交錯しているかを分析する方法を提示している。これは、7つの項目で評価され、Tier1、Tier2、Tier3に分類される[348]。 Tier1はIISSの評価手法の全項目で世界トップレベルの強さを持つとされており、米国のみとなっている[349]。Tier2はIISSの評価手法のいくつかのカテゴリーで世界トップクラスの強さを持っているとされており、豪州、カナダ、中国、フランス、イスラエル、ロシア、イギリスとなっている[350]。Tier3は重大な弱点があるとされており、インド、インドネシア、イラン、日本、マレーシア、北朝鮮、ベトナムとなっている[351]。

日本は一番レベルの低い Tier3 に分類されている。理由は「日本は1980年代初頭から情報通信技術の商業的応用において世界をリードしてきたが、特に民間部門による情報共有の点で、米国や英国などの国よりも緩い。そして日本のサイバー防御力は強固ではなく、多くの企業はセキュリティ投資に積極的でない」と評価しているためだ[352]。

本報告書では米国、豪州に着目し比較を行う。なぜならば、QUAD でサイバーセキュリティに関し、「日米豪印サイバーセキュリティ・パートナーシップ」を立ち上げ具体的な取り組みを進めていくこととしているからだ[353]。米国、豪州についてはサイバー能力がトップレベルであり、両国と比較をすることによって我が国の弱点及び課題を明らかにする。

(1) サイバーセキュリティに係る重要インフラについて

表 4 重要インフラ分野の国際比較

出典：筆者作成

	日本	米国	豪州
重要インフラ分野	情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、	化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急対応サービス、エネルギー、金融、食料・農業、政府施設、ヘルスケ	1、通信部門 2、データ保存・処理部門 3、金融サービス・市場部門 4、水・上下水道部門 5、エネルギー部門

[348] IISS, “Cyber Capabilities and National Power: A Net Assessment” [https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power], accessed January 15, 2023.
[349] IISS, “Cyber Power - Tier One”. [https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one], accessed January 15, 2023.
[350] IISS, “Cyber Power - Tier Two”. [https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two], accessed January 15, 2023.
[351] IISS, “Cyber Power - Tier Three”. [https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three], accessed January 15, 2023.
[352] IISS, “Cyber Power - Tier Three”. [https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three], accessed January 15, 2023.
[353] 外務省、「日米豪印首脳会合」、2022年5月24日。 [https://www.mofa.go.jp/mofaj/fp/nsp/page1_001186.html]、（2023年1月15日閲覧）。

	医療、水道、物流、科学、クレジット、石油（計 14 分野）[354]	ア・公衆衛生、情報技術、原子炉・核物質・核廃棄物、輸送システム、水・排水システム（計 16 分野）[355]	6、ヘルスケア・医療部門 7、高等教育研究部門 8、食品食料品部門 9、輸送部門 10、宇宙産業部門 11、防衛産業部門 （計 11 部門）

重要インフラとしているものについて各国で違いがある。日本ではサイバーセキュリティ戦略において重要インフラを定義している[356]。

次に、米国で重要インフラと定義されているのは 16 分野となっている[357]。

豪州においては、重要インフラ防護強化の取組を積極的に進めている。具体的には、「2021 年セキュリティ法改正」が 2021 年 12 月に成立した。重要インフラの定義の拡大（４部門から 11 部門への拡大）、拡大された部門における重要インフラ資産の登録、当該資産に対するサイバーセキュリティインシデントの報告義務及び政府支援（介入）措置について定めている。この法改正は、多くの産業界に対して横串で規制をかけることにより、豪州の重要インフラに対するサイバーセキュリティインシデントへの強靭化を図るもので、主にインシデント発生時の対応が主となっている。その後、2022 年３月に、この法案に次いで、インシデント発生前の対策となるリスク管理プログラム（重要インフラの所有者及び運用者に、重要サービスの提供に影響を与える脅威に対するリスク管理を義務付ける）等を内容とする法案が成立し、これにより、豪州の重要インフラ防護対策が一層強化されることとなった[358]。

[354]サイバーセキュリティ戦略本部、「重要インフラのサイバーセキュリティに係る行動計画」、2022 年 6 月 17 日、58 頁。[https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf]、（2023 年 1 月 24 日閲覧）。

[355] 総務省、「諸外国のサイバーセキュリティ政策について」。
[https://www.google.com/url?client=internal-element-cse&cx=017998645568075274792:lrqatnruwxq&q=https://www.soumu.go.jp/main_content/000488150.pdf&sa=U&ved=2ahUKEwjJ-rbWsrr8AhVKmFYBHa07CTgQFnoECAMQAQ&usg=AOvVaw11AI1X9n-fYxc92Rwnz16p]
（2023 年 1 月 9 日閲覧）。

[356]NISC、「重要インフラとは」。
[https://www.nisc.go.jp/policy/group/infra/index.html]、（2023 年 1 月 21 日閲覧）。

[357] 総務省、「諸外国のサイバーセキュリティ政策について」。
[https://www.google.com/url?client=internal-element-cse&cx=017998645568075274792:lrqatnruwxq&q=https://www.soumu.go.jp/main_content/000488150.pdf&sa=U&ved=2ahUKEwjJ-rbWsrr8AhVKmFYBHa07CTgQFnoECAMQAQ&usg=AOvVaw11AI1X9n-fYxc92Rwnz16p]
（2023 年 1 月 9 日閲覧）。

[358] サイバーセキュリティ戦略本部、「サイバーセキュリティ 2022（2021 年度年次報告・2022 年度年次計画）」、2022 年 6 月 17 日、35 頁。[https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf]、（2023 年 1 月 16 日閲覧）。

(2)　サイバーインシデント報告義務について

表 5　報告義務に関する国際比較

出典：筆者作成

	日本	米国	豪州
サイバーインシデント報告義務	なし	あり	あり
根拠	―	Executive Order on Improving the Nation's Cybersecurity	Security Legislation Amendment (Critical Infrastructure) Act 2021

米国では 2021 年 5 月 12 日にサイバーセキュリティ強化のための大統領令に署名をしている。これは政府と契約する情報通信サービス企業との間で、サイバーセキュリティ分野での官民連携を深め、同分野の発展を目指すとしたものだ[359]。Executive Order on Improving the Nation's Cybersecurity において、サービス・プロバイダーはサイバー脅威情報とインシデント情報について政府機関と共有することとされている。

豪州では Security of Critical Infrastructure Act 2018 の改正が行われ、インシデント報告の義務化スキームが含まれた[360]。30BC　Notification of Critical Cyber Incident の中で、重大なサイバーセキュリティインシデントの場合には 12 時間以内に報告を行う必要があるとされている。そして、30BD　Notification of other cyber security incidents の中で、その他の場合には 72 時間以内に報告を行うこととされている。

このサイバーセキュリティインシデント報告は、The Australian Cyber Security Centre（以下「ACSC」という。）に対して行うことが規定されている。上記の法令に基づく報告義務が課されていない場合であっても、ACSC は、全ての個人、中小企業、重要インフラ関係者及び政府機関に対し、サイバーセキュリティインシデント又はサイバー犯罪が発生した場合には、ACSC のウェブページを通じて報告することを強く推奨している[361]。

[359] JETRO、「バイデン米大統領、サイバーセキュリティを強化する大統領令に署名」、2021 年 5 月 14 日。[https://www.jetro.go.jp/biznews/2021/05/35e8aca1614f6fe5.html]、（2023 年 1 月 21 日閲覧）。

[360] Department of Home Affairs に対するヒアリング調査(2022 年 11 月 10 日実施)。

[361] 在豪州大使館に対するヒアリング調査（2022 年 11 月 11 日実施）。

（3）人材育成体制について

米国では Federal Cybersecurity Workforce Strategy（2016,Executive Office of the President）において人材のニーズの特定、教育・訓練による人材補強、多様な人材採用の促進、キャリアパスを構築し、高度なスキルを有する人材の維持・促進が掲げられている[362]。

豪州では、産業界と協力する重要な方法として、能力開発プログラムがある。このプログラムは産業界のパートナーに助成金を提供し、インド太平洋地域で能力開発を実施し、サイバーセキュリティの技術的なスキルを身に着けることを目指している。また、産業界のパートナーやその専門知識に基づき、パートナーのスキル向上も目指している。さらに、豪州国立大学（Australian National University）のサイバー・ブートキャンプ（Cyber Boot Camp）を通じて、5 日間のコースも存在する[363]。

（4）通信傍受について

表 6　通信傍受に関する国際比較

出典：筆者作成

	日本	米国	豪州
通信の秘密	あり	あり	あり
通信傍受（犯罪予防）	不可	可	可
通信傍受（犯罪捜査）	可（限定的）	可	可

合衆国憲法第 4 修正は、不当な捜索等に対する国民の権利保護を定めている。捜査には令状が必要であり、令状を取得するにも相当の理由が必要とされている。このような憲法の下で、連邦政府が通信傍受を可能にする根拠法として、1978 年に FISA 法が制定された[364]。

この FISA 法は、その目的が外国諜報情報の入手であること、米国国内で実施されること、監視対象が外国勢力のエージェントであると信じるに足る「相当な理由」があることなどの条件の下で、Foreign Intelligence Surveillance Court が通信傍受の請求を許可すると定めている[365]。

---

[362] 総務省、「諸外国のサイバーセキュリティ政策について」。[https://www.soumu.go.jp/main_content/000488150.pdf]、（2023 年 1 月 13 日閲覧）。

[363] Australian Government Department of Foreign Affairs and Trade に対するヒアリング調査（2022 年 11 月 10 日実施）。

[364] 鈴木滋 、「米国自由法―米国における通信監視活動と人権への配慮―」、7 頁。[https://dl.ndl.go.jp/view/download/digidepo_9914660_po_02670003.pdf?contentNo=1]、（2023 年 1 月 24 日閲覧）。

[365] 国立国会図書館　調査及び立法考査局、「米国自由法―米国における通信監視活動と人権への配慮―」、7 頁。[https://dl.ndl.go.jp/view/download/digidepo_9914660_po_02670003.pdf?contentNo=1]、（2023 年 1 月 24 日閲覧）。

通信傍受活動実施請求の実績については、1978 年外国情報監視法(改正法、合衆国法律集第 50 編第 1801 条他)の第 107 条および第 502 条に基づき、毎年、U.S. Department of Justice が連邦議会に報告している[366]。

豪州においても通信の秘密は保護されているが、通信傍受を許可する法律も存在する。主なものは以下の２つである[367]。電気通信（傍受およびアクセス）法 - TELECOMMUNICATIONS（INTERCEPTION AND ACCESS）ACT 1979[368]。監視法改正（特定と破壊）法 2021 年 - Surveillance Legislation Amendment（Identify and Disrupt）Act 2021[369]。また、Foreign Intelligence Legislation Amendment Bill 2021 が 2021 年 9 月に成立し、通信の傍受に関して、情報機関に大きな権限が与えられている。具体的には、上記の 1979 年電気通信（傍受およびアクセス）法を改正し、安全保障局長が外国通信から外国情報を入手する目的で通信傍受を許可する令状を申請できるものとしている。また、一定の状況下で提供された外国情報を司法長官が承認した目的に使用できることを規定している。さらには、1979 年豪州治安情報組織法および 1979 年電気通信（傍受およびアクセス）法を改正し、司法長官が外国情報の令状を発行し、外国のために活動している豪州人について外国情報を収集できるようにしている[370]。この 1979 年電気通信（傍受及びアクセス）法は、2015 年改正にて、電気通信事業者に対し、通信によって生じた情報から内容を除いたデータ、例えば、ユーザー名、アドレス、位置情報等の保全義務を 2 年間課すとしている[371]。

13　ウクライナにおけるサイバー戦

2022 年 2 月に始まったロシアによるウクライナ侵略戦争においては、リアルな空間では火力戦と経済制裁の応酬が続いている。サイバー戦も繰り広げられているとの報道もあるが、それを裏付ける証拠の入手は現時点では難しい。しかし、報道内容は蓋然性が高く考えさせられることが多い。

日本経済新聞記事[372]によれば、ウクライナは、2014 年のロシアによるクリミア半島侵攻

---

366 U.S. Department of Justice、
Apri29,2022,[https://www.justice.gov/nsd/page/file/1498046/download],accessed January 21,2023.
367 UNSW Sydney Professor Lyria Bennett Moses に対するヒアリング調査（2022 年 11 月 26 日実施）。
368 豪州政府、「TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979」。
[http://classic.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/]、（2023 年 1 月 9 日閲覧）。
369 豪州政府、「 Surveillance Legislation Amendment (Identify and Disrupt) Act 2021」。
[https://www.legislation.gov.au/Details/C2021A00098]、（2023 年 1 月 9 日閲覧）。
370PARIAMENT of AUSTRALIA, “Foreign Intelligence Legislation Amendment Bill 2021”.
[https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6748],accessed January 9,2023.
371 国会図書館、立法と情報、「【オーストラリア】1979 年電気通信（傍受及びアクセス）法の改正」、30 頁。
[https://dl.ndl.go.jp/view/download/digidepo_11976514_po_02900113.pdf?contentNo=1]、（2023 年 1 月 9 日閲覧）。
372 日本経済新聞記事、「ウクライナが問うサイバー防衛（上） 」、2022 年 9 月 8 日。
[https://www.nikkei.com/article/DGXZQODK2282N0S2A820C2000000] 、（2022 年 11 月 23 日閲覧）。

に際してサイバー攻撃により国家が機能麻痺に陥った反省から、ウクライナはサイバー防衛力を強化し、情報システム等の脆弱性を減らすとともに、監視や敵方システムへの侵入などのスキルを磨いてきたとのことである。さらに、同紙記事[373]によれば、ウクライナ国内に仕掛けられたマルウェアを米欧の専門家の協力により探知・発見して無力化したとのことである。これらの記事を通じて、日本が学ぶことは、サイバー空間は有事の際にも利用され国家機能を麻痺させることも可能なこと。そして、予めサイバー攻撃に備えることで致命傷は防ぐことができるということである。

地政学的に我が国が置かれている状況は厳しさを増しており、国益を守るためにも、新たな立法措置により、違法性を阻却しつつ、能動的サイバー防御を可能にする必要がある。

第 3 節　課題抽出

現状把握を通して見えて来た問題点を踏まえ浮き彫りになった主な課題は、防御面、対処面に大別することが出来る。それぞれの主な課題は次のとおりである。

1　防御面での課題

防御面での主な課題は、①脆弱な状態を放置させない仕組みづくり、②サイバー攻撃に関する知見の蓄積、③サイバー攻撃に対する能動的防御、④中小企業におけるセキュリティ診断の普及、⑤中小企業のサイバーインシデント対応支援、⑥サイバーセキュリティへの企業経営者の意識向上、⑦専門人材の育成対象の拡大、⑧中小企業のセキュリティ対策負担の軽減、⑨バックドア埋込などサプライチェーンリスク排除のためのルール作りなどである。

[373] 日本経済新聞記事、ウクライナが問うサイバー防衛（下） 、2022 年 9 月 9 日。
[https://www.nikkei.com/article/DGXZQODK025WC0S2A900C2000000/] 、（2022 年 11 月 23 日閲覧）。

図 34　浮き彫りになった主な課題（防御面）

出典：筆者作成

2　対処面での課題

サイバー攻撃被害発生後の対処面での主な課題は、①身代金支払い拒否を社会全体に浸透、②サイバー被害情報共有、③企業が被害情報の公表を嫌い情報が集まらないため、処方箋が作れず対処が遅れるといった負のスパイラルの克服、④復旧時間短縮による国民生活への影響縮小、⑤重要インフラ等が烈度の高い攻撃に晒された場合における自衛隊による民間支援、⑥行政令状のみで疑わしい相手システムへの潜入を可能にする法整備、⑦サイバー捜査体制の強化、⑧国際連携の前提となる外国捜査機関との継続的な信頼関係の構築、⑨アトリビューションに不可欠なインテリジェンス機能の充実である。

図 35　浮き彫りになった主な課題（対処面）

出典：筆者作成

3　課題解決の方向性

浮き彫りになった主な課題のうち、本研究では防御面の課題に焦点を当て解決の方向性を探ることとしたい。

防御面の課題のうち、特に注目した課題は、①脆弱な状態を放置させない仕組みづくり、②サイバー攻撃に関する知見の蓄積、③サイバー攻撃に対する能動的防御、④サイバーセキュリティへの企業経営者の関心度向上、⑤サイバーセキュリティ人材育成、⑥中小企業におけるセキュリティ診断の普及、⑦中小企業のサイバーインシデント対応支援の７つである。

これら７つの課題は、3 つのグループに大別できる。１つ目のグループは「サイバー攻撃に対する防御力向上」、2 つ目は「中小企業のサイバーセキュリティの強化」、3 つ目は「産官学連携教育・演習・職業斡旋プラットフォームの創設 」である。それぞれのグループについての課題解決の方向性は次に示す通りである。

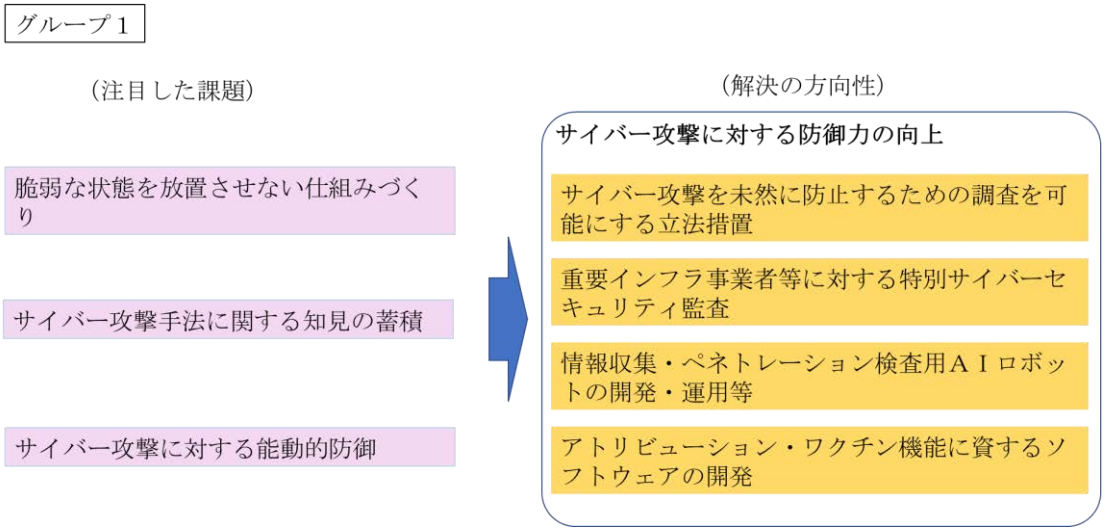


図 36　注目した課題と解決の方向性（グループ 1）

出典：筆者作成

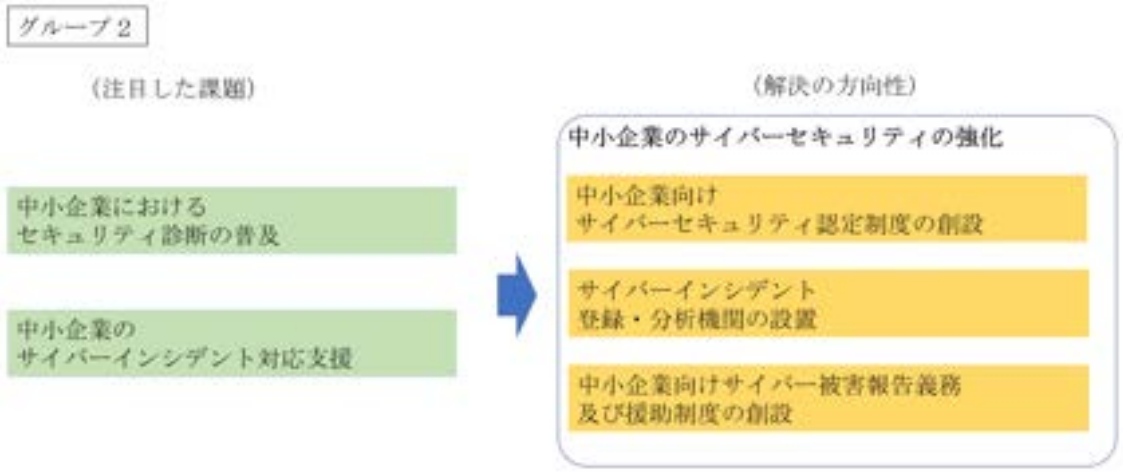


図 37　注目した課題と解決の方向性（グループ 2）

出典：筆者作成

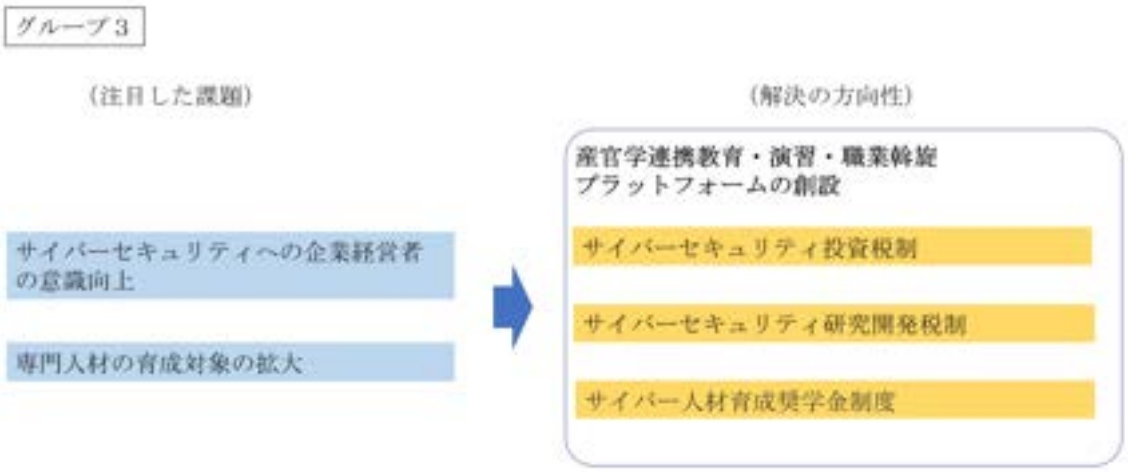


図 38　注目した課題と解決の方向性（グループ 3）

出典：筆者作成

第 4 節　政策提言

1　サイバー攻撃に対する防御力を高める政策提言

サイバー攻撃に対する防御力を高めるための政策を４つ提言する。

（1）　政策提言　サイバー攻撃を未然に防止するための調査を可能にする立法措置

ア　概要

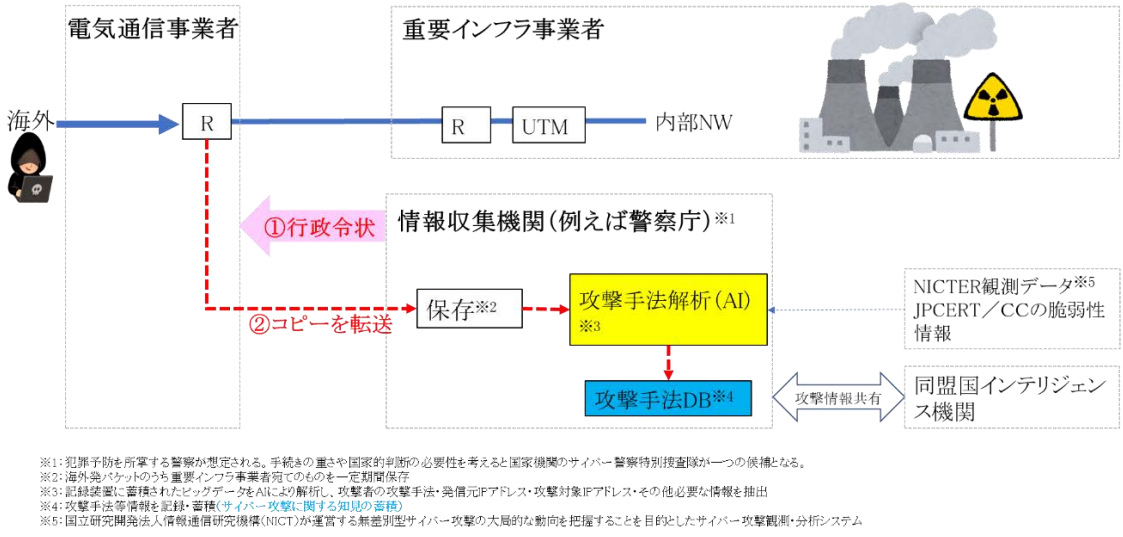


図 39　行政令状による通信傍受のイメージ

出典：筆者作成

経済安全保障上、特にサイバー攻撃から防御する必要があると認められる重要なインフラに関係する通信については、国際情勢・ＡＰＴ・組織犯罪集団の動向等により攻撃を受ける高度の蓋然性が認められる状況下（G7 等の大規模イベントの開催中、重要インフラへの具体的な攻撃予告がなされている場合等）において、サイバー攻撃の未然防止を所掌する実施機関[374]がＡＰＴの攻撃手法・攻撃対象その他サイバー攻撃からの防御に必要な通信内容を含む情報のうち、他国からの通信又は自国内から他国への通信であって自国民の通信が含まれるおそれのあるものにつき、サイバー攻撃の予防に必要と認められる通信内容に関する情報を、内閣府に設置した独立行政委員会（仮称「サイバー攻撃防御特別管理委員会」）が発行する許可状により収集することを可能にする。当該委員会は個別の許可状の妥当性のみならず、大規模監視や恣意的な利用がなされていないかを事前及び事後にチェックする体制を確保するとともに、審査を担当する委員については高度の秘密を取り扱う必要があることから外国政府の影響力の有無を含む基準を踏まえた厳格なセキュリティクリアランスを実施し、これを合格した者について、内閣が国会に任命の承認を求めることとする。

また、本情報収集により得られた情報については当該委員会に報告され、利用方法に必要な限定を付した上で関係省庁と共有され、サイバー攻撃の予防に活用されるものとする。

イ　憲法２１条第２項「通信の秘密」との関係性

この政策は通信傍受に係る内容である。通信傍受についてはこれまでも通信傍受法[375]が制定される過程において議論され、国民の権利の侵害度合いと公共の福祉のバランスについての考え方が整理されてきた。その考え方について国民の理解を深める目的で、法務省は「犯罪捜査のための通信傍受に関する法律案Ｑ＆Ａ」を作成しホームページにより情報を発信している[376]。そのなかで「通信の傍受を認めることは、通信の秘密を保障する憲法に違反しないのですか」という問いに対して「憲法第２１条第２項は、通信の秘密を保障しており、これについて最大限尊重すべきことは言うまでもありません。他方，憲法第１２条及び第１３条は，公共の福祉による制約を規定しており，通信の秘密の保障も，絶対無制限のものではなく，公共の福祉の要請に基づく場合には，必要最小限の範囲でその制約が許されるということは，憲法解釈の常識です。通信傍受法案は，犯罪捜査という公共の福祉の要請に基づき，通信傍受の要件を厳格に定めるなど，必要最小限の範囲に限定して傍受を行うものであり，決して憲法に違反するものではありません」との答えを示している。

本政策提言においても、通信傍受法制定において整理された考え方を踏襲したうえで、通信の秘密の侵害の程度を最小限にとどめるために傍受できる通信の範囲を限定するととも

---

374 犯罪予防を所掌する警察、自衛隊施設の防御を担当する自衛隊、不正通信に係る業の監視を行う総務省が想定される。手続きの重さや国家的判断の必要性を考えると具体的な例としては、警察庁関東管区警察局サイバー警察特別捜査隊が一つの候補となる。

375 犯罪捜査のための通信傍受に関する法律。

376 法務省、「犯罪捜査のための通信傍受に関する法律案Ｑ＆Ａ法務省：犯罪捜査のための通信傍受に関する法律案Ｑ＆Ａ」 。
[https://www.moj.go.jp/houan1/houan_soshikiho_qanda_qanda.html] 、（2022 年 12 月 16 日閲覧）。

に、その手続きも厳格なものとしている。実施を監督する機関としては、行政プロセスの詳細の監督を行う必要があることや国民の個人情報を厳格に守る観点から高度の独立性を保持した上で一定の体制を持つサイバー防御特別管理委員会を設立し、高度なセキュリティクリアランスを受けた委員・職員で構成するものとする。

他国（米国・豪州等）のいわゆる「行政傍受」と比べると傍受を行うことができる範囲が狭いことが課題であるが、後述のAIの開発等によりサイバー防御特別管理委員会が適切な監督を行うことができるようであれば、より広範な情報収集を行うことができる。

なお、裁判所の許可状によることも考えられるが通常の裁判所にこれを担わせた場合、行政プロセスに知悉している必要性や高度なインテリジェンスを扱う技能が求められるため、一般の裁判所にこれを担わせることは必ずしも適当ではなく独立性の高い行政委員会に相当の体制を整備することが実効性のある監督をするために必要であると考える。本傍受に関連して権利侵害が疑われる場合、最終的に国家賠償訴訟により争うことを妨げるものではない。

ウ　解析を行うためのAI開発

AI セキュリティの研究は近年最も注目度の高い分野の一つであり、我が国としても、サイバーセキュリティ戦略（令和3年9月28日閣議決定）やAI戦略 2022（令和4年4月22日統合イノベーション戦略推進会議決定）において、AI セキュリティの必要性が述べられており、国として独自の技術力を確保することが重要である。

「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セキュリティ技術の確立」に関する研究開発構想は、個別研究型として、こうした背景の下、自由、公正かつ安全なサイバー空間の確保に資する支援対象とする技術として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）において定められた「AI セキュリティに係る知識・技術体系」の整理・獲得を目指すものである。実際に高度なサイバー攻撃を受けた事例を募り、当該システムを対象にセキュリティシステムについて要件定義を行うことによる、必要となる防御の核となる要素技術の特定し、先端的な攻撃技術の知識・技術を取り込みながら、攻撃者の視点から知見を得るとともに、これらを活かした革新的な AI 活用によるセキュリティ技術を確立する[377]。AI 開発財源としては経済安全保障重要技術育成プログラム（K-Program）の活用を想定している[378]。

エ　本施策の費用対効果

AI 開発費用は相当程度かかるとみられるが、サイバー攻撃に対する抗堪性が高まり、我

[377] 内閣府、「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セ キュリティ技術の確立」に関する研究開発構想（個別研究型） 。
[https://www8.cao.go.jp/cstp/anzen_anshin/20221021_mext_3.pdf]、（2022年12月29日閲覧）。
[378] JST、「K Programとは」。
[https://www.jst.go.jp/k-program/]、(2023年1月16日閲覧)。

が国の経済安全保障に寄与することが期待できるため、費用対効果は十分期待できると考える。

（2） 政策提言 重要インフラ事業者等に対する特別サイバーセキュリティ監査

ア 概要

経済安全保障上、特にサイバー攻撃から防御する必要があると認められる重要なインフラへの攻撃に備えるため、前述の政策提言「サイバー攻撃を未然に防止するための調査を可能にする立法措置」で蓄積した知見を踏まえた攻撃パターンを用いたペネトレーションテスト[379]を定期的に実施する。そして、情報を収集・分析した機関から情報共有等を受けた地方機関・都道府県単位機関[380]は、セキュリティクリアランスを経たセキュリティ企業等と連携し、当該事業者に対して、ペネトレーションテストの結果を通知するとともに、注意喚起・指導・勧告ができるものとする。特別な事情がないにもかかわらず勧告に従わない企業は業務改善命令および刑罰の対象とする。重要インフラ事業者は、ペネトレーションテストの受任義務を負い、当該ペネトレーションテストについては、不正アクセス禁止法等の適用を除外する。なお、経済安全保障推進法又はその他の法律により、脆弱性解消に必要な費用の一部を国が補助することとする。

イ 必要となる法整備

本政策実施に当たっては、「不正アクセス行為の禁止等に関する法律」の適用を除外する法整備が必要である。

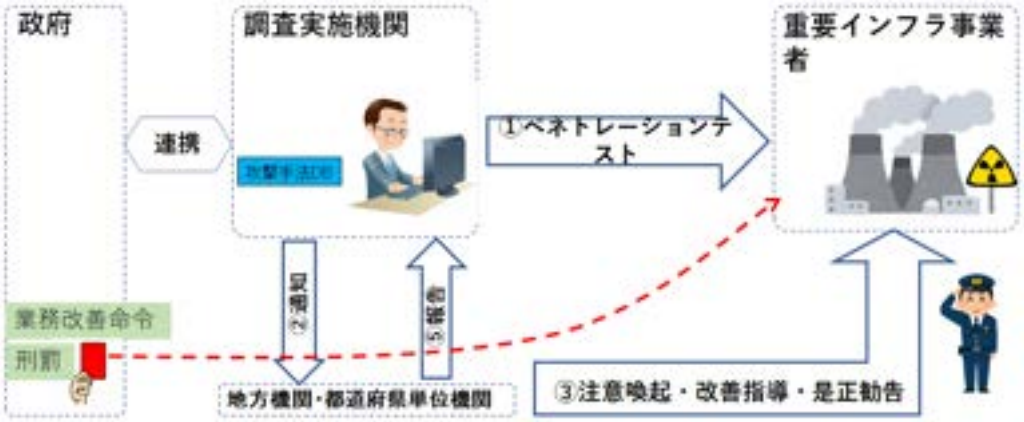


図 40 特別サイバーセキュリティ監査のイメージ

出典：筆者作成

[379] 既知の攻撃手法を用いてシステムに侵入を試み脆弱性を評価する手法。

[380] 都道府県警察・管区警察局・総務省通信部門地方局等のサイバー担当部署を想定。

ウ　都道府県警等における注意喚起・指導体制づくり

宮城県警へのヒアリング結果では、現状においてもWEBサーバに穴があったという書き込みがあった場合には県警のサイバー部隊が企業に対して改善指導を行っており、これに準ずる形で現行体制での対応が可能と見られるが、こうした検査に必要な知識は犯罪予防に関するものだけではなく事業者に関する知識、通信行政に関する知識が必要であることに鑑み、関係省庁が合同で対応するプロジェクトチームを作り、これに従事することも考えられる。

(3)　政策提言　情報収集・ペネトレーション検査用ＡＩロボットの開発・運用等

ア　概要

この政策提言は、前述の政策提言「重要インフラ事業者等に対する特別サイバーセキュリティ監査」を効率的に実施するために、AI ロボットを開発・運用し、それを用いた情報収集やペネトレーションテストを可能にする。

イ　必要となる法整備

AIの開発・運用に当たり、国・自治体・企業・大学研究室等の不正アクセス禁止法、ウイルス作成・提供・保管等の刑法等の適用を一部[381]除外すること、ならびにAIロボットでペネトレーションテストできる範囲を重要インフラ事業者に限定し、その線を超えたとき、例えばAIが暴走してしまった場合には刑事罰は問わずに、不正アクセス禁止法以外の法律を新たに作って線を引きなおすことが重要と考える。また、AIロボットによるペネトレーションテストで実現しようしている法益と、不正アクセス禁止法で一般的に守ろうとしている法益とが、どういう関係にあるか整理することがポイントとなる。また、その過程で損害を与えた場合に被害者を救済するための損害賠償保険制度を構築することも必要であると考える。

[381] AIロボット開発時におけるシステム動作確認試験時、およびAIロボット運用・保守・点検時には除外する。

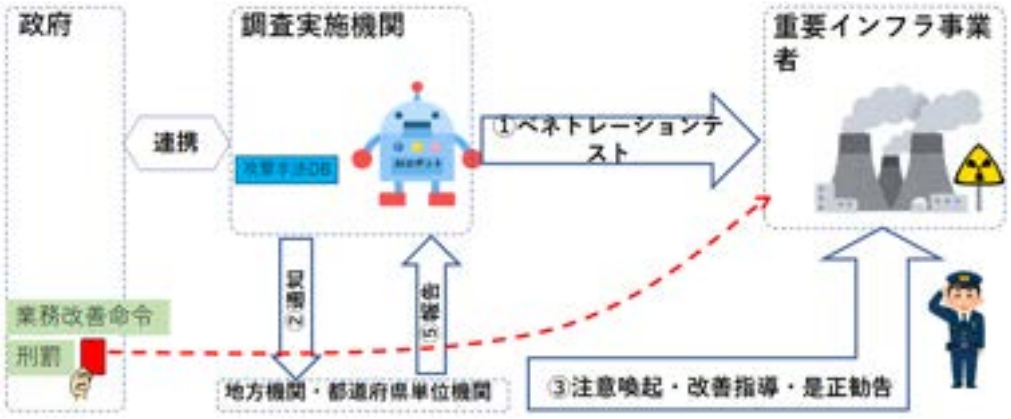


図 41　ＡＩロボットによるペネトレーション検査のイメージ
出典：筆者作成

ウ　ペネトレーションテスト用 AI ロボット開発

経済安全保障重要技術育成プログラム（K-Program）の活用を想定。

エ　本施策の費用対効果

重要インフラ事業者は国内の数千社存在する。人手によるペネトレーションテストは時間などのコストがかかり、リソースも限られるため現実的とは言えない。AI ロボットを用いれば、効率性は飛躍的に向上する。AI ロボット開発にはある程度のコストを伴うが、それでも我が国の経済安全保障がより確かなものになるのであれば、費用対効果は十分期待できると考える。

（4）　政策提言　アトリビューションやワクチン機能に資するソフトウェアの開発

ア　概要

この政策提言は、前述の政策提言「情報収集・ペネトレーション検査用ＡＩロボットの開発・運用等」の AI ロボットに利用した技術を活用し、攻撃に利用されたマルウェア等について、犯人のＰＣ内の情報や接続機器のＭＡＣアドレス等の情報を送信する機能（ビーコン機能）やサーバーからのマルウェアの除去・機能停止を可能にする機能（ワクチン機能）を持つよう改変し、その改変したマルウェアを攻撃者のＰＣに送り込む機能を AI ロボットに実装する。

サイバー攻撃のアトリビューションを実施する捜査機関は、マルウェアによる被害が確認され、今後被害が拡大する蓋然性が認められる場合、裁判所の許可状を得て、当該ソフトウェアを当該事件の捜査のために運用することができることとする。

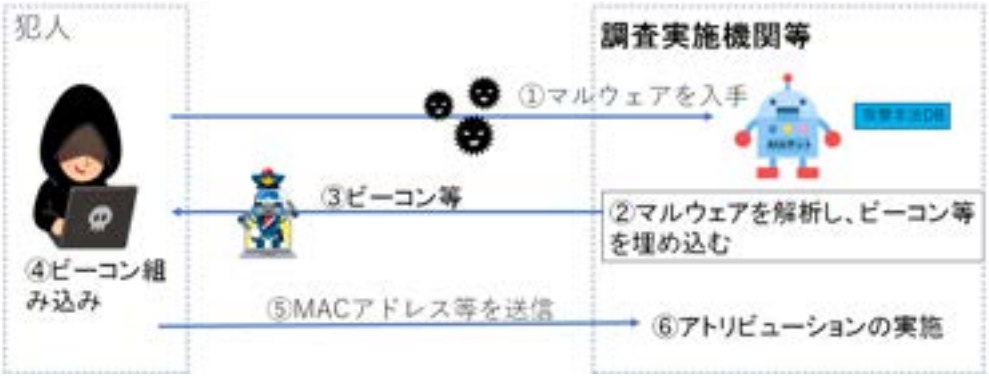


図 42　アトリビューション・ワクチン機能に資するソフトウェアのイメージ
出典：筆者作成

イ　必要となる法整備

本政策実施に当たっては、不正アクセス禁止法や刑法等の適用を除外する法整備が必要である。

ウ　本施策の費用対効果

AI ロボットへの機能実装開発にはある程度のコストを伴うが、それでも我が国の経済安全保障がより確かなものになるのであれば、費用対効果は十分期待できると考える。

2　中小企業のサイバーセキュリティ強化について

（1）　政策提言　経済安全保障に関係する中小企業向けサイバーセキュリティ認定制度の創設

ア　概要

経済安全保障に関係する重要インフラ・サプライチェーン関連の中小企業のサイバーセキュリティ向上を目的として、一定のセキュリティレベルを確保している企業を「経済安全保障サイバーセキュリティ優良企業」として認定を行い、中小企業のサイバーセキュリティを更にレベルアップすることを目指すものである。

「経済安全保障サイバーセキュリティ優良企業」として認定されるまでの流れは、①WEB を通して経済産業省へ申込み、その申込みを受けて、②経済産業省は情報セキュリティサービス基準[382]を満たしたセキュリティ企業に対してセキュリティ診断の発注を行う。そして、③発注を受けたセキュリティ企業が申込を行った中小企業のセキュリティ診断を行う。④セキュリティ診断を行った後に、セキュリティ企業から診断を行った中小企業のセキュリティ対策が基準に満たしているかどうかについての調査完了報告を経済産業省に対して行

[382] 経済産業省、「情報セキュリティサービス基準 第 2 版 」、2022 年 1 月 31 日。[https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun2.pdf]、（2023 年 1 月 14 日閲覧）。

う。⑤一定の基準を満たしている場合には経済産業省が「経済安全保障サイバーセキュリティ優良企業」としてデジタル認定証を発行する。このデジタル認定証の有効期間は 1 年間とする。なぜならば、サイバー空間は変化が激しく、新たな技術が台頭してくることから、一度の対策で過信することなく常にアップデートをしていく必要があるからである[383]。この経済安全保障サイバーセキュリティ優良企業として認定された場合のメリットとしては、経済安全保障に関連する政府調達等の総合評価方式での入札に参加できる等の優遇措置が考えられる。

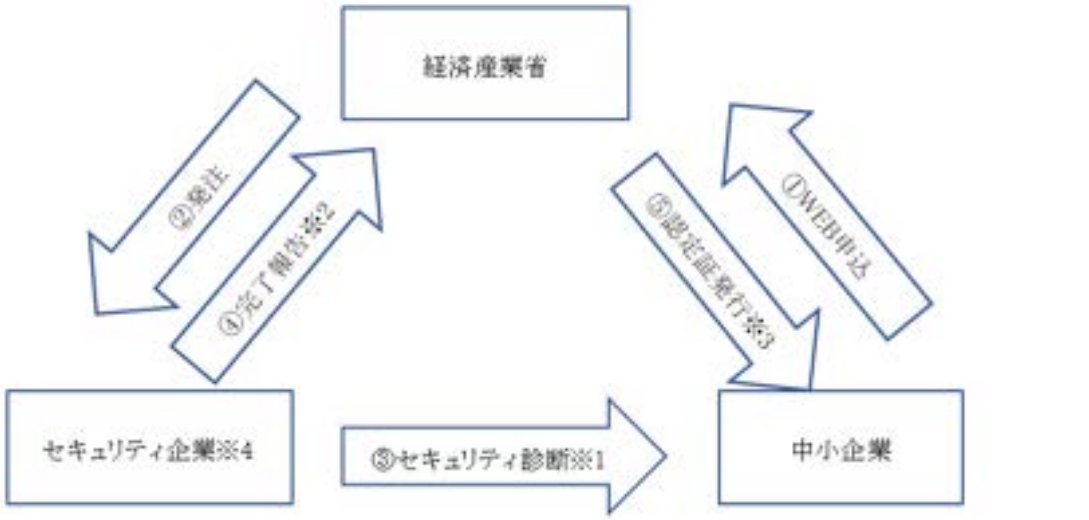


図 43　サイバーセキュリティ制度のイメージ
出典：筆者作成

イ　期待される効果

先にも述べた通り、情報セキュリティ対策投資が行われない理由としてコストがかかりすぎるということがある。そのため、セキュリティ診断について 1 社のみで行うのではなく、複数社がまとめて申込むことによって、診断費用の削減を図る。費用を抑えることにより、中小企業が、セキュリティ診断を受ける機会を増やすことを可能にすると考える。

公的機関による認定制度ではないが、中小企業に特化したものとして SECURITY ACTION がある。しかし、SECURITY ACTION の一つ星及び二つ星を宣言している企業はどちらも 5%に満たない[384]。これは、公的な認定ではなく、あくまでも自己宣言であるということも影響して

[383] 警察庁サイバー情報参事官室に対するヒアリング調査(2022 年 7 月 7 日実施)。
[384]IPA、「2021 年度中小企業における情報セキュリティ対策に関する実態調査―調査報告書―」、2022 年 3 月 31 日、41 頁。[https://www.ipa.go.jp/files/000097060.pdf]、(2022 年 12 月 3 日閲覧)。

いると考えられる。自己宣言は主観的であることから、経済産業省の認定とすることによって、客観性を得られることもメリットになると考える。

(2)　政策提言　中小企業サイバー攻撃被害報告義務と援助制度の創設

ア　概要

経済安全保障に関係する中小企業がサイバー攻撃被害に遭った場合に、被害報告を義務付けるものである。経済産業省の中にポータルサイトを立ち上げる。そして、このポータルサイトに被害情報を登録することにより被害情報の共有をするとともにサイバーセキュリティお助け隊による回復支援を受けることが出来る制度とする。

共有された情報は一般に非公開とし、セキュリティ・クリアランスの資格を有する者のみを閲覧可能とする。そして、回復支援では、サイバーセキュリティお助け隊がサイバー攻撃被害に遭った現場へと向かう。この際に報告までの時間によって回復支援にかかる費用の補助率に差を設ける。被害発生から 24 時間以内の報告であれば、100%の補助率とし、48 時間以内の報告であれば 50%の補助率とする。そして、「経済安全保障サイバーセキュリティ優良企業」であれば報告時間に関わらず無料とする。

イ　期待される効果

サイバー攻撃被害情報というのは、サイバー攻撃被害を防ぐためにも重要な情報である。ここで得られた被害情報を活用し今後のサイバー攻撃対策に役立てることが可能となる。これまで被害情報についての報告は一部を除いて義務化されていない[385]。そのため、義務化をするにあたって被害情報を出すことによってメリットを受けることが出来る形とした。このことによって、更なる被害情報の収集と支援をすることが可能となると考える。

(3)　政策提言　経済安全保障に関係する中小企業向けサイバーインシデント登録・分析機関の設置

ア　概要

サイバーインシデントが発生した場合、または情報システムの動作に異変や不安を感じた場合、その事象をポータルサイトへ登録をすることで、サイバーセキュリティお助け隊が相談に応じる体制を整える。これにより、サイバー犯罪被害の未然防止や、被害の深刻化を防ぐ。また、サイバー犯罪の可能性がある場合には、速やかな捜査着手が犯人逮捕へと繋がるとされ、迅速な通報を支援する[386]。

ポータルサイトへのサイバーインシデントの登録方法については、ACSC が用いている Report Cyber の手法が参考になる。このサイトでは、発生事象を簡潔に登録できるよう工

---

[385] 個人情報保護委員会、「漏えい等報告・本人への通知の義務化について」。[https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/]、（2022 年 1 月 22 日閲覧）。

[386] 宮城県警警察本部生活安全部犯罪対策課に対するヒアリング調査（2022 年 11 月 1 日実施）。

夫されており、登録する側の負担が少ないように作られている。まず、登録する人が個人であるのか、会社であるのか、政府機関であるのかという選択肢が表示される。登録する際に、差し迫った危険がある場合には豪州の緊急連絡先である 000 へ連絡をすることを伝えている（図 44）。個人を選択した場合には、レポートを送信しない場合についての注意書きが表示され、当てはまらない場合にはサイバー犯罪を警察に通報するという選択をすることが出来る。企業を選択した場合には、大規模組織や重要インフラに影響を与えているかどうかが表示され、重要インフラについては報告の義務が課されることについても示される。政府機関を選択した場合には、警察にサイバー犯罪を報告する、サイバーセキュリティインシデントを ACSC に報告する、サイバーセキュリティの脆弱性を ACSC に報告するという内容が表示される[387]。

日本でも、IPA が国内のコンピュータウイルスの感染被害や不正アクセス被害の届け出を受け付けている。また、ウイルスの発生状況や不正アクセスに繋がる攻撃の発生状況についても情報を収集し、被害の拡大や再発の防止に活用するため、攻撃が未遂で実被害が生じなかった場合についても届出の協力を求めている。届出の方法はメールとなっており、届出内容によってはメールアドレスが異なっている[388]。

中小企業は人数も限られてくることから、登録する際の手間がかからない方法が求められる。ポータルサイトに登録された内容を分析することで、中小企業が抱えているサイバーセキュリティ上の悩み事や問題点の把握も可能となる。

[387] ACSC, “ReportCyber Report a cybercrime , incident or vulnerability”.[https://www.cyber.gov.au/acsc/report] ,accessed January 17,2023.
[388] IPA「コンピュータウイルス・不正アクセスに関する届出」、2022 年 10 月 27 日、[https://www.ipa.go.jp/security/outline/todokede-j.html#ransom] 、（2023 年 1 月 17 日閲覧）。

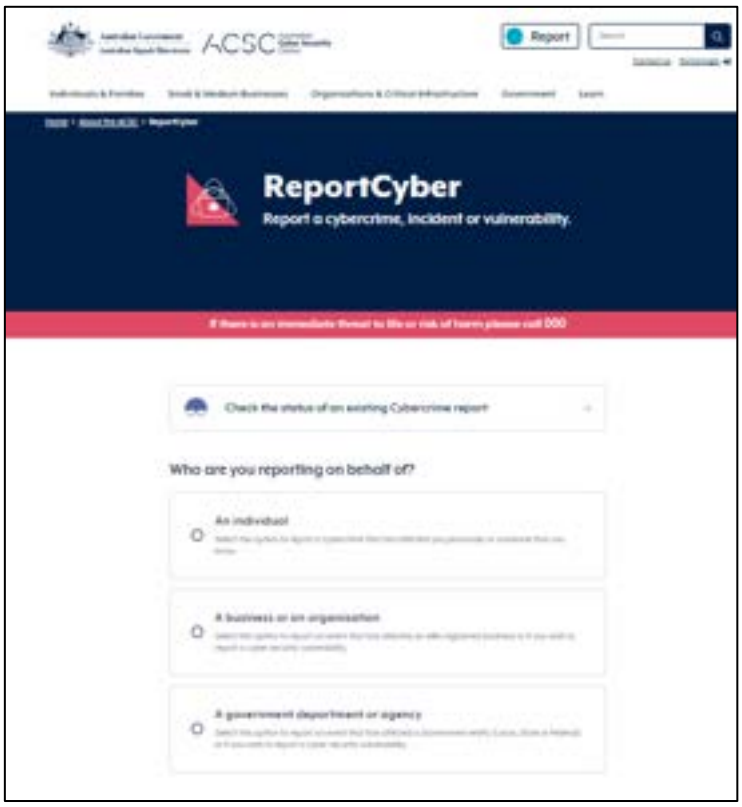


図 44　ReportCyber の概要

出典：ACSC

イ　期待される効果

この施策を実行することによって期待される効果として、深刻な被害となる前に情報を共有することが可能になることが考えられる。現在、会員登録をした場合や情報共有の枠組みに入っている場合について、その組織内において情報を共有するという仕組みは存在している。情報を見る側についてはセキュリティ・クリアランスの問題があることから、会員であることが求められるだろう。しかし、インシデント情報については広く情報を集めることが求められる。

NICT に対するヒアリング調査において、国内にある貴重なデータを可能な限り共有し、活用していくことが重要であるとのことだった[389]。そのため、会員以外でも簡単にインシデント情報の登録が可能なポータルサイトを設置することによってこれまでよりも広く情報を集めることが可能になると考える。

3　産官学連携教育・演習・職業斡旋プラットフォームの創設

産官学連携教育・演習・職業斡旋プラットフォームの創設に関する提言を行う。当該プラットフォームではサイバーセキュリティに関する教育・啓発活動やサイバー演習、サイバー

[389] 国立研究開発法人 情報通信研究機構（NICT）に対するヒアリング調査（2022 年 9 月 2 日実施）。

セキュリティ関連の職業の斡旋を行う。運営方法は、国が一定額の予算を拠出した上で、参画する企業から資金を募ることとする。以下では、当該プラットフォームの運営に必要な 3 つの政策を提言する。

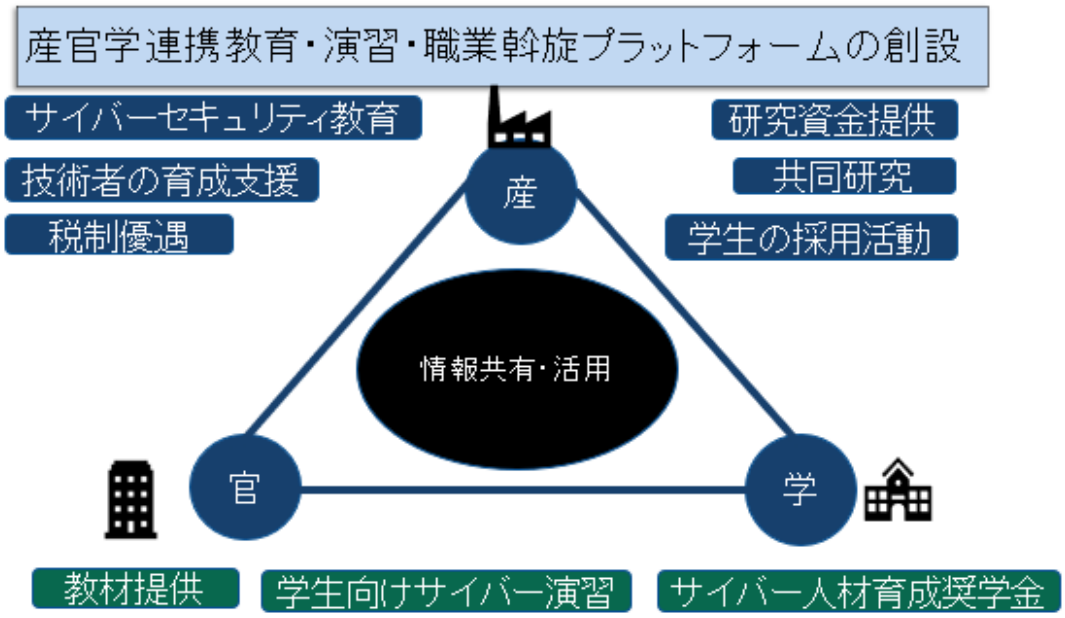


図 45　産官学連携教育・演習・職業斡旋プラットフォーム
出典：筆者作成

(1)　政策提言　サイバーセキュリティ投資税制

企業に対する税制優遇として、サイバーセキュリティ投資税制の導入を提言する。

サイバーセキュリティ投資税制は、現在、防衛関連企業を対象に検討が進められている。これを経済安全保障に関わる重要インフラ事業者やサプライチェーン事業者にも適用範囲を拡大する。当該制度では、ウイルス対策ソフトの導入、2 段階認証システム導入など、サイバーセキュリティを強化した企業が国にその認定申請をし、安全性が認められた企業に対して、事業年度の法人税額からの設備投資の特別控除または資産に係る特別償却を認める制度である。

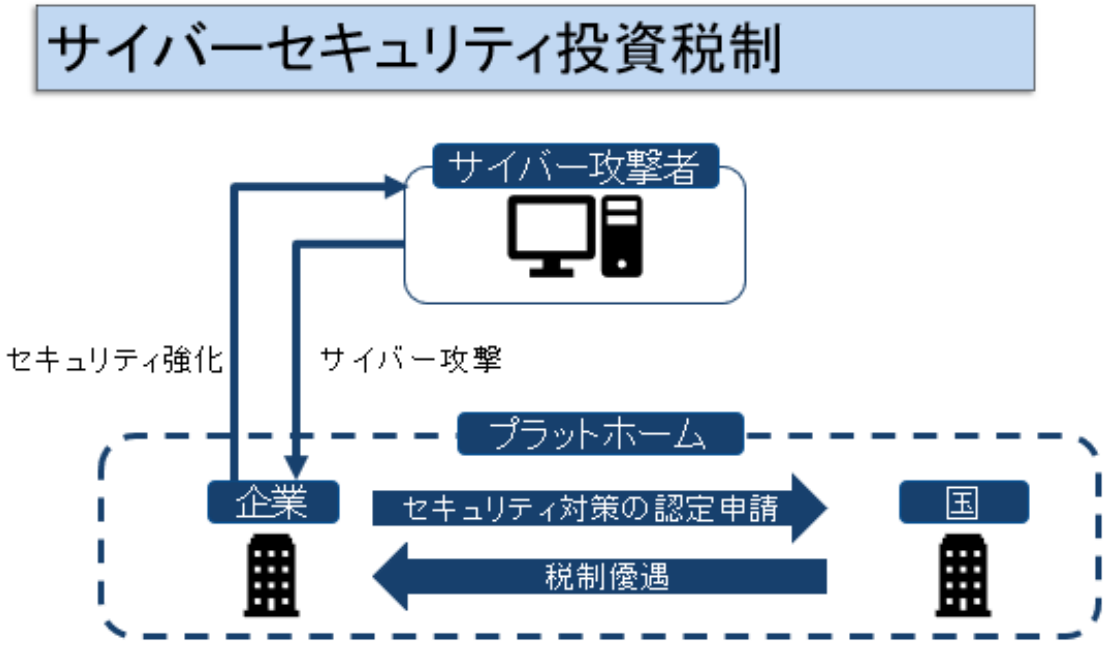


図 46　サイバーセキュリティ投資税制

出典：筆者作成

(2)　政策提言　サイバーセキュリティ研究開発税制

サイバーセキュリティ研究開発税制を政策提言する。この制度はサイバーセキュリティに関連する研究開発に対して税制優遇を行うものである。研究開発税制とは、経済産業省が所管し、研究開発を行う企業が、試験研究費の一定割合を法人税額から控除できる制度である[390]。企業の研究開発を、国がそのコストの一部を負担し支援することで、イノベーションの創出に繋がる中長期的な産業競争力を高め、我が国の発展と国際競争力の強化に資することを目的に創設された。

当該税制は、これをサイバーセキュリティの分野にも適用範囲を拡大したものである。

[390] 経済産業省、「研究開発税制の概要と令和 3 年度税制改正について」。
https://www.meti.go.jp/policy/tech_promotion/tax/R4gaiyov2.pdf]、（2023 年 2 月 17 日閲覧）。

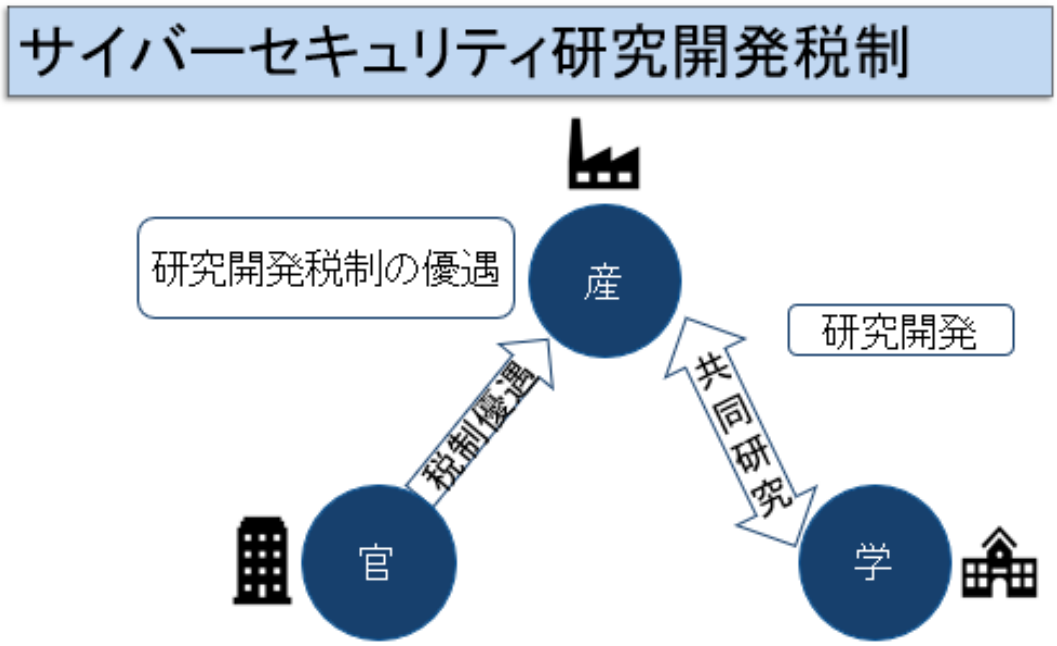


図 47　サイバーセキュリティ研究開発税制

出典：筆者作成

(3)　政策提言　サイバー人材育成奨学金制度

サイバー人材育成奨学金制度を政策提言する。これは若手人材の育成に焦点を当てた政策である。

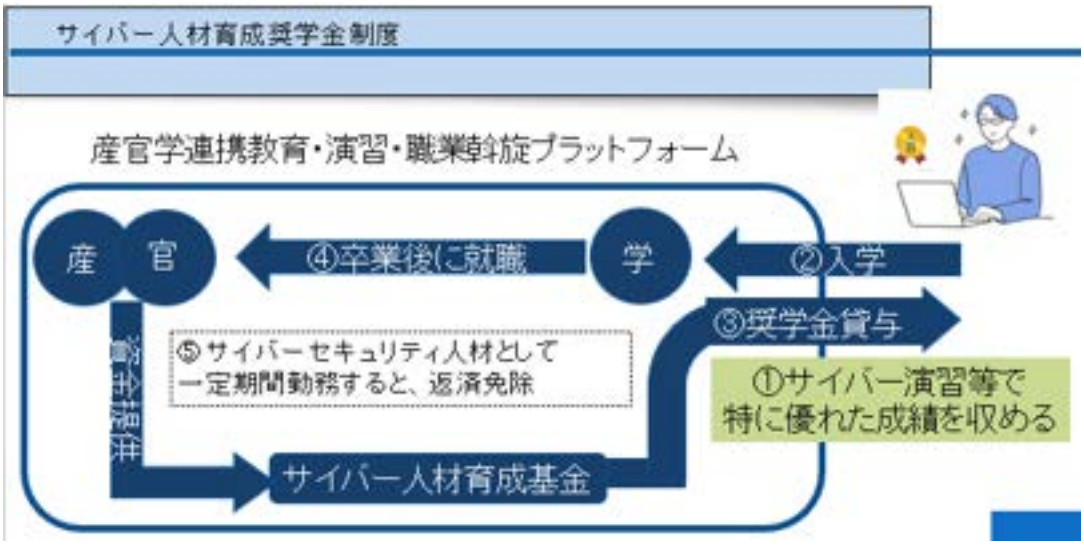


図 48　サイバー人材育成奨学金制度

出典：筆者作成

このサイバー人材育成奨学金制度は、サイバーセキュリティ関連業界・職種に就く若者を増やし、将来のサイバーセキュリティ人材を確保・育成するための制度である。まず、制度の流れとしては、学生向けのサイバー演習等で特に優れた成績を収めた学生に、高専や大学、大学院での就学に必要な費用を、国と企業が共同出資するサイバー人材育成基金を通じ、卒業時まで奨学金を貸与する。そして、学生が卒業後、当該プラットフォームに参加する企業のサイバーセキュリティ人材として一定期間勤務した後に、返済が免除となる仕組みである。この制度は、高等教育機関への就学を資金面で支援し、将来的に我が国の経済安全保障に必要な高度なサイバーセキュリティスキルを有する人材として育成するとともに、就職活動においてもこのプラットフォームに加盟する企業等がその人材を有利に獲得できる環境を整えることが目的だ。

企業と教育・研究機関の間では、当該プラットフォームを人材交流の場として活用し、研究者への研究資金の提供や共同研究、加えて、参加企業が将来のサイバーセキュリティ人材として自社で活躍してほしい学生を有利に獲得できるような場になるような仕組みにする。

そして産官学の間で、国に対するインシデント報告を義務付け、また、サイバー攻撃の被害情報等を研究にも活かせるよう、守秘義務を課した上で情報共有・活用が可能となる体制を整備する。

第 3 章　経済インテリジェンス分野での政策提言

第 1 節　総論

本章において経済インテリジェンス分野での政策提言を行う。「経済インテリジェンス」という文言は政府資料において散見されるが[391]、法令等で明確に定義された概念ではない。論者によってインテリジェンスの定義は様々であることから、まず議論の対象を明らかにするために本章で取り扱うインテリジェンスの概念を整理する必要がある[392]。そこで本節でははじめに、インテリジェンスの定義を整理し、これを基に経済インテリジェンスを定義することとしたい。

川上高司監修の『インテリジェンス用語辞典』は、様々な論者が使う用例を参照し、インテリジェンスの定義に共通する要素として「インフォメーション[393]を処理・分析して得られた決心・行動するために必要な「知識」」を挙げている[394]。また、「必要な知識を獲得するための人間集団ないし組織そのもの」を指す意味でも使われることがあると指摘している[395]。さらに、インテリジェンスを適切に機能させるそもそもの前提として各種情報漏洩を防ぐ必要があり、そのために必要な措置を指す用語としてカウンター・インテリジェンスがある。これは前掲資料において「国外からのインテリジェンス活動による自国に対する脅威を把握して対策をとること」と定義されている[396]。

この両者の定義を総合し、経済安全保障において必要なインテリジェンス活動の対象を明らかにするため、本章で扱う経済インテリジェンスの定義については「経済安全保障施策を実行するために必要な知識及びその知識を獲得するための人間集団ないし組織そのもの。また、経済安全保障に関する国外からのインテリジェンス活動による自国に対する脅威を把握して対策をとること」と広く捉えることとしたい。

インテリジェンスの定義については狭義のものとして政府首脳が意思決定を行うために必要な情報収集・分析を経た生成物を指す用例もあるが、第 1 部第 1 章第 2 節でも述べたように、経済安全保障は国家だけでなく企業・大学がプレイヤーとして存在しており、経済インテリジェンスはこれらのプレイヤーとの情報共有等が課題となっていることからも、本章では前述の定義を採用することで検討対象を広く捉え、幅広い主体の情報共有のあり方についての提言を行うこととしたい。

そして、主要国の技術開発競争で我が国が勝ち抜くためには、国家安全保障の観点から経済インテリジェンス活動を適切に行い、それにより得られたインテリジェンスを踏まえ、技術を保全・育成すべき分野を指定し、技術優越の確保・維持を図るべき具体的な重要技術を特定・支援する必要があるが、その活動の基盤となる人間集団ないし組織そのもの、すなわ

---

391 本報告書第 1 部第 3 章第 2 節を参照。
392 小林良樹『なぜ、インテリジェンスは必要なのか』、慶應義塾大学出版会、2021 年、17 頁。
393 インフォメーションはインテリジェンスと区別され、「各種情報源から得られた知りうることのすべて」と定義される。川上高司監修『インテリジェンス用語事典』、並木書房、2022 年、94 頁。
394 同上、91 頁。
395 同上、同頁。
396 同上、127 頁。

ち人材育成が不可欠であるため本章ではこの点の提言も行うこととしたい。

加えて、経済インテリジェンス活動を適切に行うそもそもの前提としてのカウンター・インテリジェンスについては、我が国が機微技術や経済インテリジェンスに関する国際連携、情報共有を適切に推進していくためにもより一層の高度なものとしていく必要があり、こうした情報漏洩対策の強化についても提言を行うこととしたい。

以上、本章では経済インテリジェンス分野での必要な対策を講じるため、第 2 節では情報漏洩対策に資する政策提言、第 3 節では人材育成に資する政策提言、第 4 節では情報共有に資する政策提言を行うこととする。

第 2 節　産官学連携のインテリジェンス活動についての提言

1　現状分析

（1）　経済安全保障におけるインテリジェンスの意義

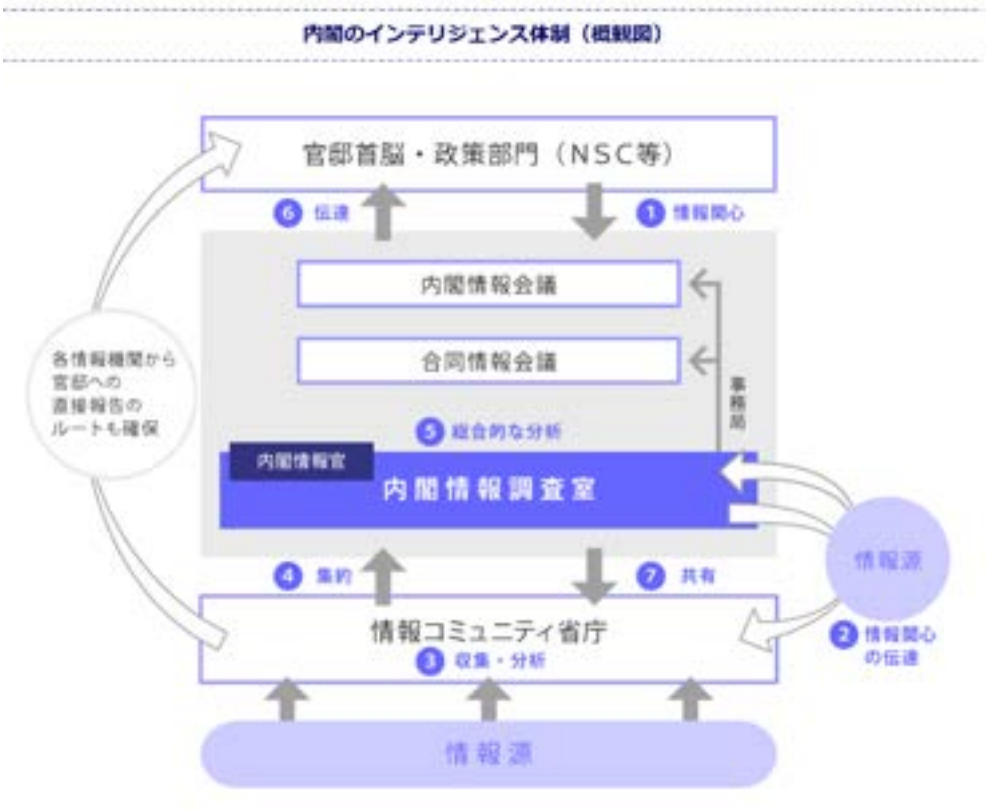


図 49　内閣のインテリジェンス体制（概略図）

出典：内閣情報調査室

日本には政策決定を行う政府首脳に対して機能するインテリジェンス・コミュニティがあり、図 49 のように関連省庁から情報を収集、集積し、分析したうえで内閣の政策の企画立案等に必要な情報を官邸首脳・政策部門に伝達し、国際情勢の移り変わりや日本国内の事情等を鑑みながら様々な政策決定のための情報の収集や分析を担ってきた。

しかし、経済安全保障はこれまで以上に広範な分野に関係しており、政府以外にも企業や大学が重要な主体として存在するため、現状のインテリジェンス・コミュニティよりも広範な情報の要求、収集、分析が求められる。この課題は、政府における経済安全保障上の主要課題として認識されている。第 1 回経済安全保障推進会議で用いられた検討資料では、「経済インテリジェンス」がこれまでに着手した取り組みで、今後も継続・強化していく分野の 1 つに挙げられており、「情報収集・分析・集約・共有等の充実・強化」と記

載されている[397]。経済インテリジェンスの必要性を認識しているのは、経済界も同じである。日本経済団体連合会が経済安全保障法正についての 2022 年に行った提言でも経済インテリジェンス機能の強化が提言されている。

その具体的な方策としては、サプライチェーンの強靭化、重要インフラの確保、官民技術協力、特許非公開化に加え、並行して検討すべき課題として経済インテリジェンス機能強化や情報保全制度の検討が挙げられている[398]。

また、現状では海外との国際的な技術協力や共同研究によって相互に交流をはかることでより技術的な発展を目指す場合、協力は難しい状況にある。技術流出を防止する制度がなければ日本から懸念国への情報流出が危惧されるからだ。我々が行ったヒアリング調査でもシドニー大学のマイケル・グリーン氏から「日本はサイバー分野と情報セキュリティ分野の整備が遅れているため、情報セキュリティ体制が向上しない限り米英豪との高度な技術協力は成立しないだろう。」という趣旨の回答があった[399]。

(2)　情報管理の必要性

現在、政府は機微技術の開発、研究に力をいれている。たとえば内閣府の経済安全保障重要技術育成プログラムという、関係府省が一体となって推進するプログラムが始まりつつある。この会議が、支援すべき重要技術を含めた「研究開発ビジョン」を決定し、当該ビジョンに沿って、関係府省が一体となって研究開発を推進していくものである。また、「研究開発ビジョン」の決定に際しては、国家安全保障会議での経済安全保障に係る審議を経るものとする、というのがこのプログラムの概要である[400]。

まだこのプログラムは募集の段階ではあるが、政府としては特に重要な分野を絞り込んだうえで技術育成を進めていくつもりだが、懸念点が存在する。

他国に対して相対的優位な技術を手に入れたとしても、その技術情報が流出してしまえば我が国の相対的優位は崩れることになるうえに、先端技術は軍事転用可能なものが多々あるために経済上のみならず安全保障上の問題にもなりえる。

情報流出の経路は警察庁の分析によれば企業やアカデミアが狙われるパターンは 3 パターンあり、サイバー攻撃、スパイ工作、そして合法的な経済活動、合弁や買収などや共同研究といった学術活動を隠れ蓑にするパターンがある[401]。

情報流出はサイバー空間という物質的なつながりを攻撃された場合にのみならず人的要

---

397 内閣官房、「経済安全保障推進会議（第 1 回）関連資料 3」、［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai1/shiryou3.pdf］　、（2023 年 1 月 25 日閲覧）。

398 日本経済団体連合会、「経済安全保障法制に関する意見－有識者会議提言を踏まえて－」、2022 年 2 月 9 日。［https://www.keidanren.or.jp/policy/2022/015_honbun.html］、（2023 年 1 月 15 日閲覧）。

399 マイケル・グリーン氏に対するヒアリング調査（2022 年 11 月 15 日実施）。

400 内閣府、「経済安全保障重要技術育成プログラム」。（2023 年 1 月 3 日閲覧）。

401 警察庁、「技術流出の防止にむけて」。［https://www.npa.go.jp/bureau/security/economic-security/index.html］、（2023 年 01 月 15 日閲覧）。

因、人の脆弱性を介しても起こりえるものである。

実際に不審なメールに添付されていたファイルを不用意に開いてパソコンをハッキングされ、情報を抜かれるといった事例から、直接的なものであれば、タッチセンサーのシェアトップを誇る「NISSHA」の元社員が機密情報をもって海外の会社に移籍し、その情報を漏らしたことにより不正競争防止法違反で逮捕された事件[402]、また、軍人が身分を隠して他国の大学で研究し、その成果を帰国後に軍事研究に利用する[403]など枚挙にいとまがない。

現状では企業などの社員から情報が流出した場合に不正競争防止法では 21 条 1 項 1 号乃至 9 号などで刑事的責任を追及することが可能であり、また民事的責任追及も債務不履行といったところで問うことができるが、その情報を漏洩させないためのアクセスできる人間を絞り、その人間の背景調査などを行う、公務員の特定秘密の保護に関する法律第 11 条にある特定秘密の取扱者の制限などに類似する官民両用の公的認証制度がない。

今後ますます経済安全保障、なかでも技術振興に力を入れていくうえでこういった情報の管理への政策強化が急がれる。

(3)　産学の経済安全保障体制の現状

産学の安全保障体制の現状に関して以下の図から大学、研究機関の脆弱性が読み取れる。

[402] サイバーセキュリティ総研、「NISSHA 元社員情報持ち出し　中国競合他社に機密情報リーク」、2019 年 6 月 7 日。［https://cybersecurity-info.com/news/nissha-information-leak/］、（2023 年 1 月 15 日閲覧）。

[403] 警察庁、「技術流出の防止にむけて」。

脆弱な大学・研究機関の管理体制

経済安全保障の整備率（大学等791校）

体制整備の項目	整備済みと回答	割合
安全保障貿易の管理体制	178	22.5%
営業秘密保護の管理体制	72	9.1%
利益相反防止のポリシー・規程類	302	38.1%
上記のすべて	28	3.5%

図 50 平成 30 年大学等における産学連携等実施状況について
出典：文部科学省

大学・研究機関では論文の公表が研究者のキャリアや評価につながることや、そもそも研究は成果の公表を通じて行われることがある。研究上・教育上の必要から機微な研究成果であっても公開する場合があり、その際に公開してはならない相手方に公開しないようにチェックする体制が必要である。管理体制の不備によって情報が流出してしまえば取り返しのつかないことになったり、他国に対する優位性を喪失したりするおそれがあるためだ。

実際に警察庁の経済安全保障関連の技術流出防止の啓蒙パンフレットで取り上げられている実例として国内のとある大学が情報の流出防止に関する“輸出管理条項”を盛り込んだ上で、 外国の大学と人材交流プログラムを締結したところ、その後、先方から既存の合意書を再作成したいとの要望があり、内容を確認すると新しい案文では”輸出管理条項”が何の説明もなく削除されていたという事例が掲載されている[404]。

[404] 警察庁、「技術流出の防止に向けて事例詳細」。［https://www.npa.go.jp/bureau/security/economic-security/assets/pdf/jirei.pdf］、(2023 年 1 月 16 日閲覧)。

（１）民間企業との共同研究の実施件数及び研究費受入額の推移

図 51 平成 30 年大学等における産学連携等実施状況について

出典：文部科学省

また、図 51 のようにますます民間と大学の技術協力が増えている中、このような管理体制の未整備は大学の研究振興上の課題となってくる。前述のとおり国際協力を視野に入れた場合に海外の企業、大学、研究機関からすると日本から第三国に情報が流出することのリスクを高く評価すれば日本とは技術協力をしないという選択もとりかねない。

営業秘密の保護に関する整備ができている大学は図 50 の通り 9.1%にとどまる。企業は営利目的で運営されることがおおいため、研究の内容あるいは営業に関する秘密を保護したいと考えた場合、大学側の体制未整備はこれからすすむであろう研究費の受け入れや民間との共同研究において障害となる可能性がある。

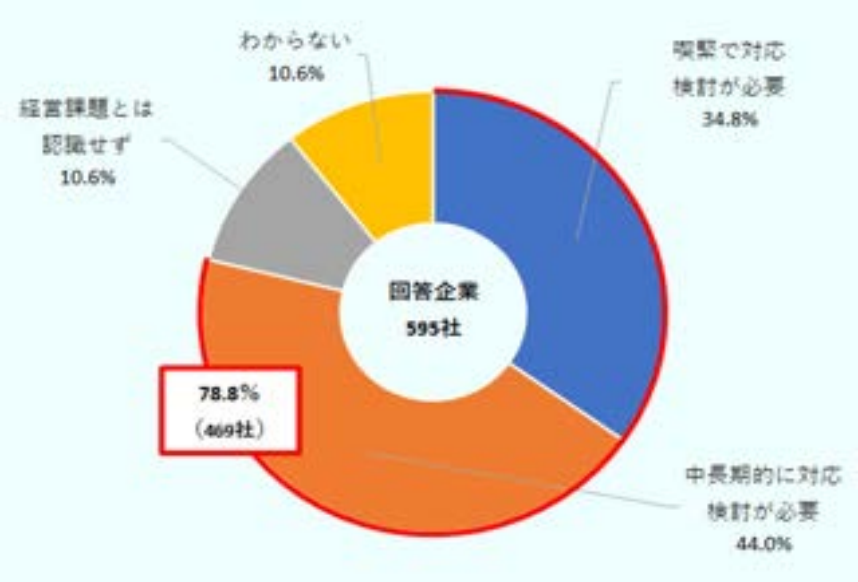


図 52 経済安全保障を経営課題として認識しているか

出典:JETRO

図 52 は JETRO によるアンケート調査のグラフであるが、民間企業では 8 割が経済安全保障を経営上の課題であると認識している。

図 53 経済安全保障に関わる体制や取り組み（複数回答）

出典：JETRO

図 53 は企業が今後とっていく対策のアンケートである。経済安全保障の対策として一番

多く挙げられているのが情報収集の機能強化であり、これは現状で企業が情報を欲している、つまり経営判断に足る十分な情報を得られていないと認識している。日本を取り巻く国際情勢やサプライチェーン上の問題、さらには情報の秘密を守るためにも企業には情報が必要であるが、現状、企業の経済安全保障にかかる情報が不足している理由として経済安全保障という分野が最近始まったばかりの取り組みであることや、そもそも対策や体制作りがわからない[405]といった意見も WS で行ったヒアリング調査でてきた。つまり、経済安全保障対策がすべての企業で十分に行われているわけではなく、また情報収集が課題として挙げられている。

(4)　関連省庁の取り組み

産学の現状に対する既存の取り組みとしては大きく分けて 2 点ある。

外為法改正と研究インテグリティに関する取り組みだ。

まず、外為法の改正とは具体的に輸出規制の強化である。外為法の輸出管理体制に関しては前述のとおりキャッチオール規制やリスト規制などで規制している貨物や技術を輸出、提供しようとする場合には、原則として、経済産業大臣の許可を受ける必要があり、これらの関連技術の非居住者への提供についても外為法 25 条 1 項に基づいて管理している。ここでいう非居住者とは入国後 6 か月以内または国内の事務所などに勤務するわけではない外国人を指す。これをみなし輸出管理といい、国境を超える技術提供や国内における技術提供についても非居住者は最終的に出国する蓋然性が高いことから、居住者からの非居住者に対する提供を管理していた。ただ、この制度では入国後 6 か月経過または国内の事務所に勤務する外国人は居住者としてあつかわれ、管理の対象外となるために外国の影響下にある居住者からの機微技術流出懸念に対応できていないと懸念されてきた。

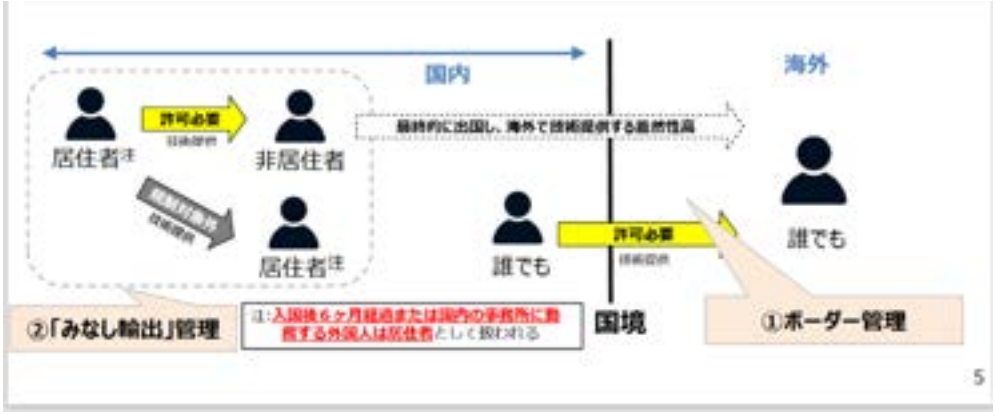


図 54　従来のみなし輸出管理制度の概要

出典：経済産業省

[405] 東北大学安全保障輸出管理室に対するヒアリング調査（2022 年 6 月 14 日実施）。

これが 2022 年 5 月より特定国の非居住者に提供することを目的とした取引について居住者への機微技術提供であっても、当該居住者が、非居住者へ技術情報を提供する取引と事実上同一と考えられるほどに当該非居住者から強い影響を受けている状態に該当する場合はみなし輸出管理の対象となった[406]。

図 55　見直し後のみなし輸出管理制度の概要
出典：経済産業省

次に研究インテグリティに関する取り組みとは関連省庁全体で取り組まれている、機微技術に対して一定の保護をかける取り組みである。

具体的には、文部科学省の研究インテグリティに関する取り組み、警察庁によるアウトリーチ活動、公安調査庁による講演やシンポジウムの開催・パンフレットの公開などが行われている。文部科学省の研究インテグリティに関してはまだ動き始めたばかりのプロジェクトではあるが、①研究者自身による適切な情報開示、②大学・研究機関等のマネジメント強化、 ③公的資金配分機関による申請時の確認の 3 点を軸に大学・研究機関の研究体制を変えていくというのが文部科学省の取り組む研究インテグリティである[407]。

また警察庁によるアウトリーチ活動は 2020 年ごろから開始された活動で、企業を個別訪問し、手口の共有や注意喚起を行っている。

公安調査庁の経済安全保障にかかわる取り組みとして公式ホームページからアクセスできる講演会の依頼受付、シンポジウムの開催、そしてインターネット上でのパンフレットの公開などを行っている[408]。

---

406 経済産業省、「みなし輸出管理」。［https://www.meti.go.jp/policy/anpo/anpo07.html］、（2023 年 1 月 16 日閲覧）。
407 内閣府科学技術・イノベーション推進事務局、「研究インテグリティの確保に係る対応方針（概要）」、2021 年 12 月、2 頁。［https://www.mext.go.jp/content/20211220-mxt_kagkoku-000019002_3.pdf］、（2023 年 1 月 16 日閲覧）。
408 公安調査庁、「経済安全保障特集ページ」。
［https://www.moj.go.jp/psia/keizaianpo.top.html］、（2023 年 1 月 16 日閲覧）。

2　課題抽出

（1）　産官学にまたがる情報保護制度の強化

ア　情報保護の必要性

情報の保護に関する必要性は現状にある通りであるが、特に現状分析の（2）で情報流出の経路に関して述べているとおり、情報はスパイ工作や合法的な経済活動の中で流出の可能性があるが、これに対して日本の民間企業および大学の研究室では企業や大学が独自に情報を保護するために機微情報にアクセスする人間を限定したとしても、欧米のように民間でも政府でも通用する公認の情報取扱資格認定制度が存在しない。

公務員に関しては 2014 年に施行された特定秘密の保護に関する法律があり、これは第 3 条から第 17 条までで、安全保障に関する情報を、一定の条件のもとで特定秘密として指定し、秘密とする期間、秘密の取扱い、秘密を取扱う者の評価、情報漏えい等への罰則を定めているものである。

公務員に対しては一定程度の情報を秘密指定すれば、アクセスできる人間を限定し、さらにアクセス可能な人間に秘密情報の取り扱いの適格があるかという審査をすることができている一方で、民間企業であれば不正競争防止法で責任追及する場合は有用性、非公知性、秘密管理性の三要件を満たしている必要性がある[409]うえに、前述のとおり政府の公的認定制度が日本の企業にはないため、海外との共同研究を視野に入れた場合に、足かせになる。

総論で述べたようにインテリジェンス・プロセスは収集・加工・分析・報告という過程を経て活用される。競合相手に高度分野の技術が漏洩した場合、相手はその情報を収集し、活用するために、相対的な劣位に立つことになる。

たとえば我が国の大学、研究機関に所属したのちに外国において軍事研究に従事する研究者の存在は複数確認されている[410]。また、通信大手のソフトバンクの元社員がロシアの元外交官に情報を売った事例[411]などもあり、人からの情報流出全般に関して対応する政策が早急に必要である。

イ　他国の類似制度との比較

一方、英米などの諸国ではセキュリティ・クリアランスという制度がある。
この制度は情報を何段階かに分けて、その情報にアクセスできる身分資格を持った人間の中で秘密が扱われる。この身分資格は数年に一回監査がはいり、思想、家庭背景、家族構成、といった個人的なことまで調べられたうえで与えられる資格である。そのため、まず情報流

---

[409] 経済産業省、「営業秘密-営業秘密を守り活用する-」、2021 年 2 月 15 日。［https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html#handbook］、（2023 年 1 月 16 日閲覧）。

[410] 公安調査庁、「経済安全保障の確保に向けて 2020 - 技術・データ・製品等の流出防止に向けて－」。［https://www.moj.go.jp/content/001373771.pdf］、（2023 年 1 月 16 日閲覧）。

[411] 朝日新聞デジタル、「ソフトバンク元社員に有罪判決　ロシアへの機密漏洩事件」、2020 年 7 月 9 日。［https://www.asahi.com/articles/ASN795VMLN79UTIL016.html］、（2023 年 1 月 16 日閲覧）。

出の可能性を減らすことができる。

日本においてこのような制度に類似するものとして前述の特定秘密の保護に関する法律の他、公務員全体に守秘義務として職務上知りえた情報を退職後も公開しない義務が課せられている。

しかし民間においてはこのような制度がない。もちろん民間企業内で情報にアクセスできる社員をチェックしているところもあるが、社員のプライバシーにかかわる身辺調査は行われていない。また、公認の制度ではないので、仮に身辺調査を行ったうえで秘密情報取扱資格を付与したとしてもそれは世界的に通用する資格ではないため、国際的な協力ができる水準ではないと判断される可能性がある。官民連携の技術開発を今後進めていくにあたって先端技術が経済安全保障においては重要であることは前述のとおりである。

	日本	米国	英国
秘密の区分と対象範囲	①防衛②外交③特定有害活動の防止④テロリズムの防止に関するものなどを特定秘密として指定	①軍事計画、②インテリジェンスの情報源、③政府の外交活動、④国家安全保障に関する経済的事項等に該当する情報を ①機密 ②極秘 ③秘 に区分して指定	政府の有する情報その他の資産を ①機密 ②極秘 ③秘 に区分して指定
	日本	米国	英国
指定権者	行政機関の長	大統領、副大統領、大統領が指定した行政機関の長と上級幹部職員	秘密の作成者又は指名された所有者
対象者	行政機関の職員、契約業者の従業者、都道府県警察の職員 ※ 行政機関の長、大臣、内閣官房副長官、内閣総理大臣補佐官、副大臣、政務官等は対象外	連邦政府又は契約業者の従業者で、秘密を取り扱う者 ※ 大統領、副大統領は対象外	国、警察機関又は契約業者の従業者で、秘密を取り扱う者 ※ 首相、大臣は対象外
統一的な実施機関	・情報法保全諮問会議を通じて有識	・ホワイトハウスが策定した評価基準に従い、各	・内閣官房がセキュリティ・ポリシーの枠組み

	者からの御意見を聴いた上で、内閣官房が運用基準を作成。 ・これに基づき、各行政機関の長が適性評価を実施。	行政機関が評価を実施。 ・連邦人事管理局に調査を委託可能。	を策定。 ・国防省及び外務・英連邦省の調査部局に調査を委託可能。
秘密指定の有効期間	初期　上限5年 延長　原則30年	初期　原則上限10年 延長　原則上限25年	秘指定の期限なし （国家安全保障等に関する情報は情報自由法上の20年公開原則の例外）

罰則	日本	米国	英国
漏えい	10年以下の懲役・罰金 または ５年以下の懲役・罰金	死刑、無期・有期刑 または 10年以下の自由刑、罰金	３年以上 14 年以下の自由刑 または ２年以下の自由刑、罰金
過失犯	２年以下の禁錮・罰金 または １年以下の禁錮・罰金	10年以下の自由刑、罰金	３月以下の自由刑、罰金
取得	10年以下の懲役・罰金	10年以下の自由刑、罰金	３年以上 14 年以下の自由刑

上記表は内閣府の資料[412]を参考に筆者が作成したものであるが、米英ともに罰則が厳しいことがわかる。また、対象者にも米英ともに民間人が含まれるので、このような官民両方で通用する秘密情報の取扱い資格制度を成立させることで現状の課題となっている海外との技術協力に足る情報保護制度とすることが可能である。

(2)　産官学の連携強化の必要性

前述のとおり、企業側はまずなにをしたらよいか、どのような体制を築くべきかという情報の取得事態が困難であるうえ、体制を管理したところでチェック機能が現状では警察

[412] 内閣府、「特定秘密保護法と諸外国の秘密保全制度の比較」、2014年7月22日。
［https://www.cas.go.jp/jp/tokuteihimitsu/ikenkekka/3_4.pdf］、（2023年1月26日閲覧）。

にたいする相談程度であることから、経済安全保障体制強化に際し、もっと支援を受けられる体制作りが早急に必要である。

また、大学からも、技術や情報を保護するための制度設計がわからない[413]といった声が上がっていることから、東北大学のように安全保障輸出管理室を備え、対策を進めている大学であってもはっきりとした指針やアドバイスが必要であることがわかる。

さらに、日本の情報保護体制が甘いことが国際協力を阻害する可能性がある[414]ことが有識者から指摘されており、日本のさらなる技術振興のためにも、早急に制度整備を行わなければならない。

人を介した情報流出は手口が様々にあるにも関わらず、その調査自体の機密性が高く、また機密情報に関しても何の情報を守るのか、どうやって企業、もしくは大学の運営に支障が出ない形でやっていくのか、といった点があるため、企業や大学にも参加してもらいながら任意のうえで体制整備をすすめていく必要がある。

3　政策提言

(1)　セキュリティ・クリアランス制度の導入

以前からセキュリティ・クリアランス制度の導入は議論されており、プライバシーの問題、守秘義務に関する問題、罰則規定に関して議論されることがおおい。まず、プライバシーに関する問題であるが、秘密情報取扱資格を与えるうえで個人の情報を詳しく審査する際、海外の質問事項を鑑みても日本の特定秘密保護法を鑑みても踏み込んだ質問はプライバシーの侵害に当たるのではないか、という論点がある。これに対して現行の英国や豪州で運用されている制度では機密情報取扱資格の取得を個人の意思にゆだねている。英国で運用されている Security Policy Framework などでは、基本的に機密情報の取り扱い資格を仕事上得たい人が自ら申告して資格を得る制度であるため、本人の同意がある以上プライバシーの侵害にはあたらない。

守秘義務にかんする問題として民間でも国家公務員に求められるものと同等の守秘義務をかけることについて、守秘義務を負うのは誰か、守秘義務については、守秘義務の対象が何であるか、また、機密の保持が求められる範囲はどこまでか、さらに、いつまでの期間で守秘義務を負うことになるのかという論点がでている[415]。有識者会議においてサイバーセキュリティ基本法に基づくサイバーセキュリティ協議会の構成員に対しては国家公務員並びの守秘義務がかかっていることを念頭に置くと、会議体において安心して情報共有を行うためには、基本的に会議体の参加者について一定の枠をかけた上で、情報を共有し、そして

---

413 東北大学安全保障輸出管理室に対するヒアリング調査（2022 年 6 月 14 日実施）。
414 マイケル・グリーン氏に対するヒアリング調査（2022 年 11 月 15 日実施）。
415 内閣官房、「経済安全保障法制に関する有識者会議（第２回）議事要旨」、2021 年 12 月 28 日。［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/gijiyousi.pdf］、（2023 年 1 月 15 日閲覧）。

交換できる仕組みを確立していくことが法制度上、必要ではないか。[416]という議論があり、情報を共有し、交換していく仕組みの上ではやはり情報をランク分けしたうえでランクに応じてアクセスできる人間を限定した制度導入を考えるべきである。守秘義務の責任にかかわる前述の論点においても、秘密の保持においても、まず情報のランク分けとそれにおうじた罰則などの立法が求められている。期間に関しては日本の公務員法では守秘義務は退職しても続くものであり、また、公務員以外の職業にかかる守秘義務も同様である。ただし、国民の知る権利との兼ね合いもあるため、現行の秘密指定の有効期間と同じ期間設定で制度を導入すべきだ。

罰則規定や民間人のプライバシーに関わる情報を国が収集することの是非に関して米国等では民間人にも罰則が適用されており、「国際的な潮流からいえば、罰則適用は致し方ない」とする一方、「共同研究を促進する法律に罰則はそぐわない」とする指摘もある。また、研究者本人の申請を前提とするとされているものの、身上調査において民間事業者の従業員も含む研究者のプライバシーに関わる情報を国の機関が収集するべきなのか、検討が必要とする指摘がある[417]。

しかし、プライバシーに関しては情報に対して保護をかけたり、また、個人の申告によって資格をあたえたりするために問題にはならない。罰則規定も海外に比べて日本の現行制度は重いとはいえず、むしろ現行制度では英米と比較すると秘密指定のランクわけがなされないことや罰則が軽微であること[418]から海外との機微な情報の共有の足かせになってしまう。そのため、先端技術の育成のためにセキュリティ・クリアランス制度の導入は急がれるべきである。

(2)　先端技術 CI ネットワークの設立

CI とは counter　intelligence の略である。このネットワークでは、経済安全保障上、特に脅威から防御する必要があると認められる重要な先端技術を保全するための情報を定期的に発信する。どこがその情報を発信していくのか、というのは実は産業スパイは検挙した時にかかわる警察しか詳細をしることができない。そして捜査情報にかかわる以上、一般の組織などに分析を頼むことも難しいことから情報の分析と発信は主に各都道府県警察から行われることになる。

具体的な CI 情報を保有する警察と企業・大学を所管する関係省庁が協力して、情報盗取等の脅威に関する手口や対策を組織内に素早く周知する。

従来のアウトリーチ活動は個別訪問での注意喚起であるため、従来の活動と比べて一度の声掛けで届く範囲が広くなること、また、各都道府県警察の 2020 年からの努力により、アウトリーチ訪問を受けた企業であれば、ある程度経済安全保障体制に関して把握し

[416] 同上。（2023 年 1 月 15 日閲覧）。
[417] 小谷賢、「対中防諜と秘密保全体制の強化を」、『Voice』518 号、 2021 年 2 月、58 頁。
[418] 内閣府、「特定秘密保護法と諸外国の秘密保全制度の比較」、2014 年 7 月 22 日。
［https://www.cas.go.jp/jp/tokuteihimitsu/ikenkekka/3_4.pdf］、（2023 年 1 月 17 日閲覧）。

ていることから、たとえばヒヤリ・ハット事例や、こういった接近がありました、という企業側、大学側からの情報提供を警察がネットワークを通じて個別に受理することができる。情報の発信や共有が素早く行われることで、よりカウンターインテリジェンスを強化することが可能になる。

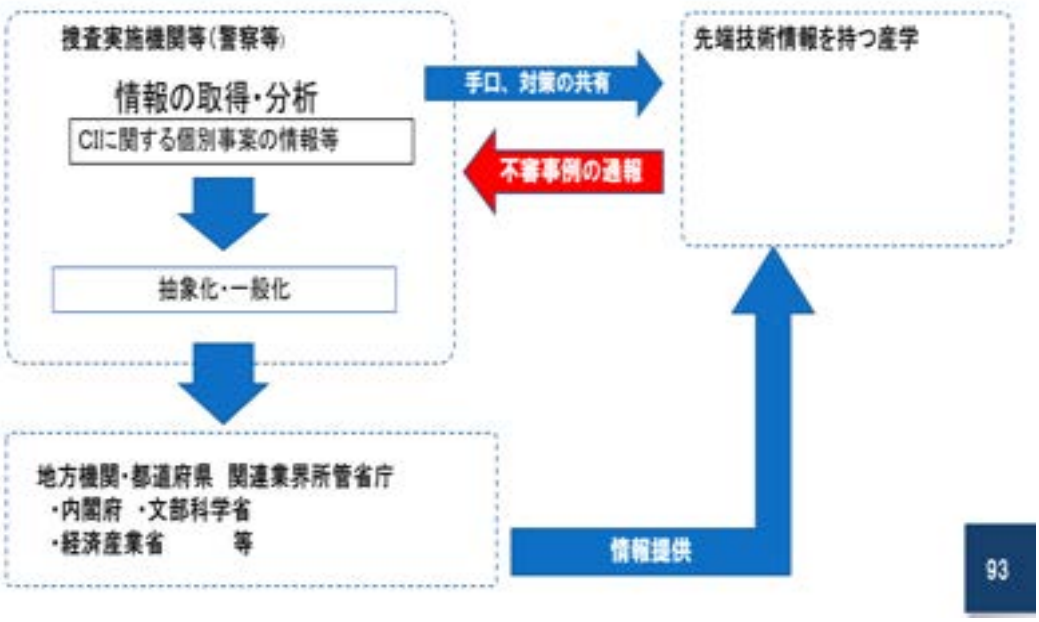


図 56　CI ネットワークの作用図
出典：筆者作成

また、企業や産業にかかわる省庁として経済産業省や文部科学省といった警察以外の関連省庁も省庁横断的に対策せざるを得ない課題であるため、このネットワークにも参加すべきである。なぜならば、経済安全保障は幅広い経済の分野に安全保障を絡め、国家の安定と繁栄に向けた手段であるためにかかわる範囲が多岐にわたり、対策が進められはじめたのが近年である点から専門家も少ない。そのため、関連する省庁、企業、大学といった様々な組織が一体となって対策を行う必要がある。

(3)　セキュリティ支援強化

経済安全保障上、特に防御する必要があると認められる先端技術研究や先端技術産業への攻撃に備えるため、提言１で蓄積した知見を踏まえた攻撃パターンを用いた警察によるチェックを定期的に実施する。

このチェックは抜き打ち的なものか、WS 的な実践的な演習を交えたものにすべきである。実際に企業や大学の管理者が体験することで、どういった点に気を付けるべきかといった視点や、警察の方もセキュリティをどういった用件で満たしていないかの事例が加わ

れば、また提言１のネットワークで注意情報を喚起する際に一般化した注意点としてより効果的に対策をしていくことができるようになるからである。

セキュリティの基準を満たさない企業は早急にセキュリティ対策をとるよう勧告と一定程度の補助金をもってセキュリティレベルを引き上げる。

しかし、警察は企業や大学の経営体制までは把握してないので、その点に関する勧告や、経営体制に即した対策は所管省庁と協力して行うべきである。

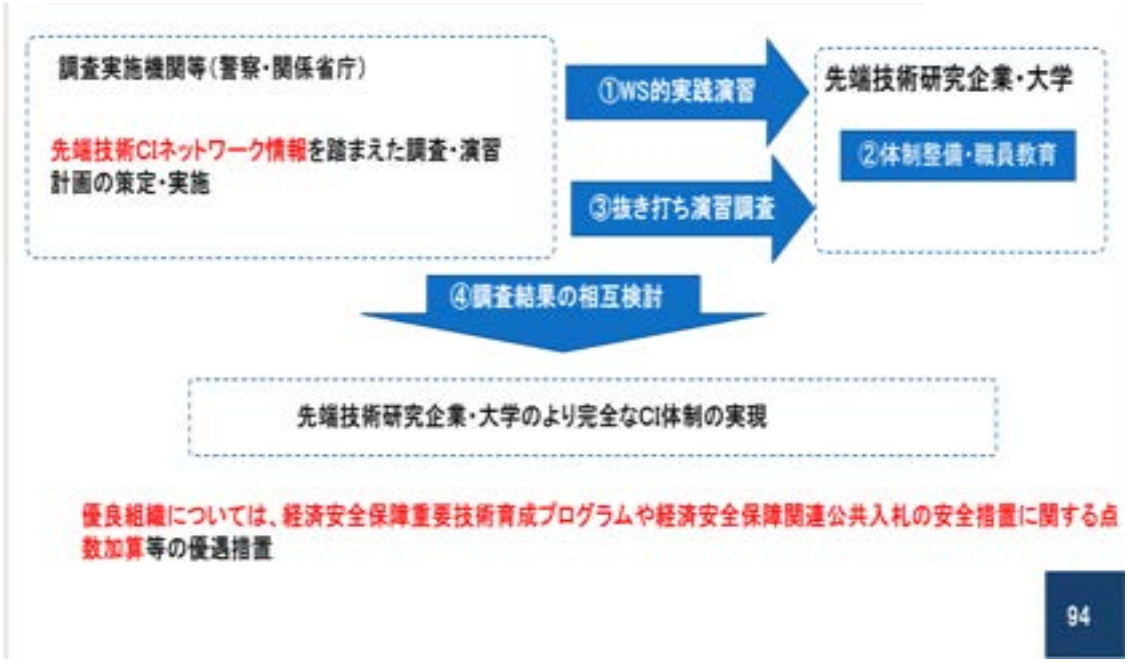


図 57　セキュリティ支援強化の作用図

出典：筆者作成

また、それらの勧告などによって改善された結果も警察や関係省庁に報告することで知見がたまり、正のインテリジェンススパイラルをつくれることでさらに効果的な対策につながる。

第 3 節　経済安全保障シンクタンクの制度設計についての提言

1　現状分析

(1) 意義

本節では経済安全保障シンクタンクの人材育成の観点から提言を行う。経済安全保障上、重要な技術を守り育てるためには政府だけでなく、企業やアカデミアの知見を統合して重要技術の開発に向かう必要がある。実際主要国においては、市場経済のメカニズムのみに委ねていては投資が不十分となりがちな先端技術について、国としての優位性を維持・確保するために大型プロジェクトが順次立ち上げられている[419]。そこで必要となるのが後述する協議会や経済安全保障シンクタンクである。経済安全保障シンクタンクとは内閣総理大臣が一定の力を有し、守秘義務が課される。特定重要技術の見極めや、その開発について調査研究する[420]機関である。経済安全保障シンクタンクに関しては令和 5 年度を目処に新設が予定されているが、政府公開の文書において、シンクタンク参加者のキャリアパスの構築や情報共有ネットワーク構築の必要性に関する記述があるもののその詳細に関しては現時点では確認が取れなかった。また 2022 年 5 月 18 日に成立した経済安全保障推進法案ではシンクタンクに参加するものの守秘義務については定められていたが具体的な制度面の内容を示唆する記述がなかった。これらの点に鑑み本節では 2023 年度に新設される新経済安全保障シンクタンクにおいて求められる人材の輩出機能や具体的な制度、キャリアパスに関して提言を行うこととする。

(2) 重要技術を育てることの重要性

経済安全保障上重要な概念である、他国に対する優位性を持つ上で重要技術の育成は急務となっている。他国にはない技術を日本が保有し、その技術により、他国が日本に依存する仕組みを作ることが将来の日本の経済安全保障を構成する一要素となる。

日本の経済安全保障上の重要技術を守り育てる上で、重要となることは 2 点ある。1 点目が、国家が主導となって技術開発を行うことである。経済安全保障上重要な技術の中にはビジネス的な観点から見ると必ずしも結果に結びつかないような技術も多く、そのような技術に対しては国が主導となり開発を推し進めていく必要がある。産官学の持つ知見を集約し、技術を開発していくことである。それを行う上で、経済安全保障政策においては協議会の元で、資金配分機関からの資金を得て研究開発を行い、国家の経済安全保障政策上、重要となる技術の育成を図っていくことが求められる。

2 点目は産官学の多様な主体が参画して知見を共有し合うことがある。従来、国民生活や経済活動において重要となる先端技術は、国の機関や一部の大企業等が主体となり開発さ

---

[419] 内閣官房、「経済安全保障法制に関する提言」、31 頁。2022 年 2 月 1 日。［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai4/teigen.pdf］、（2023 年 1 月 17 日閲覧）。

[420] ニュースイッチ、「科学技術の経済安保、“攻め”と“守り”の体制構築へ急務なこと」、2022 年 9 月 2 日。［https://newswitch.jp/p/33587］、（2023 年 1 月 26 日閲覧）。

れてきた。例えば、コンピューティング・インターネット・GPS などがその例として挙げられ、成果が広く社会・経済に活用されてきた。一方、近年急速に進展しつつある AI、量子等の新興技術の研究開発は、アカデミアやスタートアップ企業を含めた多様な主体がボトムアップで推進しており、先端技術の研究開発を担う主体に変化が生じている。[421]そのため、産官学の知見及び、多様な主体の参画は必要である。

(3) シンクタンク設立の目的

まず経済安全保障政策の中でシンクタンクがどのように位置付けられているのかについて整理しておきたい。経済安全保障シンクタンクを設立する目的の大きなものとして、協議会及び指定基金協議会に対して知見を提供する特定重要技術調査研究機関としての一端を担うことや産官学の連携のハブとなることがある。これまでも政府が主体となり産官学の連携を促すような取り組みは存在した。「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に関する基本指針」によると、特定重要技術を開発する目的は「経済安全保障政策上、重要な特定重要技術の研究開発に知ることで、日本が国際社会において確固たる地位を確保すること」である。また同条文には「シンクタンクは、単に情報提供の機関ではなく、先端技術の専門性を有する産業界・学術界の人材を確保するとともに、機関やその活動を目に見える形として拠点化した上で、産業界・学術界への必要な情報の提供や、政府の政策の意思決定への貢献・寄与をしていく機関となっていくことが期待される。このため、シンクタンクには、必要な機関との連携体制や、情報共有のネットワークの構築に努めることが求められており、関係行政機関はこれらの実現に必要な支援を行う必要がある。」[422]との記述がある。

これらの記述を踏まえると特定重要技術の調査研究を行うシンクタンクは経済安全保障政策の中で中心的な役割を担っていくものである上このようなシンクタンクを運用するには、“シンクタンクの運用に、科学者・研究者自らが様々な形で関わることができる生態系や仕組みを中長期的に形成していくこと[423]”が肝要である。

---

421 内閣府、「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に関する基本指針」、3 頁。2022 年 9 月 30 日、［https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin3.pdf］、（2023 年 1 月 19 日閲覧）。

422 内閣府、「特定重要技術の研究の開発の促進及びその成果の適切な活用に関する基本指針」、24 頁。［https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin3.pdf］、（2023 年 1 月 21 日閲覧）

423 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、「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）（案）」、2 頁。
［https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai3/shiryou1.pdf］、（2023 年 1 月 17 日閲覧）。

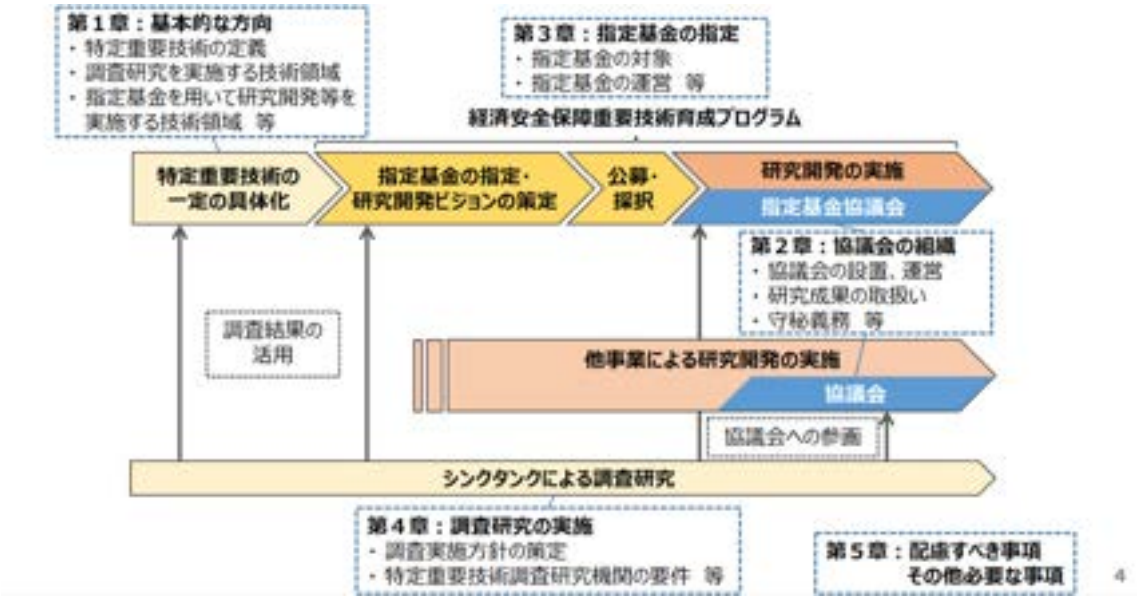


図 58　求められるシンクタンクの機能

出典：内閣府

（4）シンクタンクに求められる能力について

政府の基本方針によると新たに創設されるシンクタンクに求められる 4 要件として以下の 4 つが挙げられている。1 点目が専門的な調査能力に関する能力、2 点目が情報収集・整理・保管に関する能力、3 点目が内外の関係機関との連携に関する能力、4 点目が情報管理体制である。

経済安全保障シンクタンクは特定重要技術調査研究機関の一端を担うことが期待されており、また必要な機関との連携体制や、情報共有のネットワークの構築に努めることが求められており、関係行政機関は、これらの実現に必要な支援を行う必要がある[424]。内閣府が発表した「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に関する基本指針」は、特定重要技術調査研究機関に求められる要件として大きく 4 点を挙げている。

1 点目が専門的な調査研究に関する能力である。具体的には、将来の国民生活及び経済活動の維持にとって重要なものとなり得る先端的な技術に関して、技術面のみならず社会制度や社会システムまでを含めた国内外の情勢や研究開発動向等を適切に調査・分析できる能力とある。日本の経済安全保障政策においては幅広く、関係行政機関、関係機関、先端的技術の研究開発を担う第一線の研究者、社会実装を担う民間企業の知見を糾合すること[425]が求められており、国として守り育てていく機微技術に対して産官学が連携して取り組むことが必要である。

[424] 内閣府、「特定重要技術の研究の開発の促進及びその成果の適切な活用に関する基本指針」、24 頁。（2023 年 1 月 21 日閲覧）。

[425] 同上、21 頁。（2023 年 1 月 21 日閲覧）。

2点目が情報収集・整理・保管に関する能力である。具体的には「国の政策に調査研究を活かしていくためには最新のトレンドを追うのみならず、過去の実績や知見の蓄積を踏まえた継続的な調査・分析が不可欠であり、自ら関連の情報を収集・整理し、それを補完することにより調査研究に役立てていくことが求められる」とある。また、基本的な方針には「施策の立案・実施の過程においては平時から現場の情報を収集・分析しておくことが重要であり、そうした観点からも政府は、事業者等との間でコミュニケーション・連携を図っていく必要がある[426]」との記述があり、これは経済安全保障シンクタンクにおいても同様に当てはまるだろう。特に公的利用だけでなく民生利用での社会実装も想定されているため、迅速な情報共有は必要不可欠である。

3点目が内外の関係機関との連携に関する能力である。具体的には、「調査・分析機能を担保するためには、自ら保有すべき情報と国内外の様々な機関がそれぞれの特徴に応じて有する情報を集約し、連携することが重要である。このため、特定重要技術調査研究機関には、自らが情報集約のハブとなり、内外の様々な機関と連携し、ネットワークを構築する能力が求められる」とあり、これに関しては前述したとおり、産官学が分野の垣根なく一体となって経済安全保障に資するような研究を行っていく必要があるということであろう。

4点目が情報管理体制である。具体的には「関係行政機関や海外の研究機関等との緊密なコミュニケーションを確保し、情報管理を図る必要がある情報を取り扱えるようにするため、適切な情報管理 体制を確保することが求められる。特に、委託事業の調査・分析において様々な主体から提供される情報の中には、守秘義務の対象になり得る情報など、公表に馴染まないものも含まれ得ることから、その取扱いについては、十分な配慮が必要」であるとの記述がある[427]。

1点目の要件からわかることとして、日本の経済安全保障政策上、国が求めている人材は分野横断型の知見を持った人材の育成である。国としてはそれらの人材にシンクタンクでの研究に従事してもらい、特定重要技術に代表される経済安全保障上の重要技術の育成を行なってもらう方針である。

(5) 協議会について

特定重要技術の研究開発に当たっては、潜在的な社会実装の担い手として想定される関係行政機関や民間企業等による、各組織や産学官の枠を超えた伴走支援が有効であり、技術力あるスタートアップ企業や中小企業等も含め、参加者間で機微な情報も含む有用な情報の交換や協議を安心して円滑に行うことのできるパートナーシップの確立が必要である[428]。協議会に期待される事としては、特定重要技術の研究開発等に関する情報管理の枠組みを設けることにより、関係行政機関が保有するニーズ情報や民間企業等の情報セキュリティ

[426] 同上、5頁。（2023年1月21日閲覧）。
[427] 同上、25頁。（2023年1月21日閲覧）。
[428] 同上、9頁。（2023年1月26日閲覧）。

のインシデント情報など、研究開発等には有用であるが、通常であれば、国家公務員法（昭和 22 年法律第 120 号）第 100 条第 1 項に基づく守秘義務等により、研究者には共有されることがなかった機微な情報の共有を可能とすることで、研究開発等のより効果的な実施[429]を行う事や、また機微な情報の共有にとどまらず、社会実装のイメージや研究開発の進め方を議論・共有するほか、必要に応じ、規制緩和の検討や国際標準化の支援など、組織の枠を超えた協議が行われることが期待される。さらに、協議会参加者が納得する形で、技術流出対策を講じるべき対象範囲やオープン・クローズ戦略を決めていくことも期待される[430]。協議会を用いて産官学で一体となって技術開発を行う設計となっている。

（6）協議会の詳細について（経済安全保障推進法の概要より抜粋）

国の資金により行われる特定重要技術の研究開発等について、その資金を交付する大臣（研究開発大臣）が、基本指針に基づき、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を設置する。必要と認める者を、その同意を得て構成員として追加することができる[431]。協議会の構成員としては大きく 4 つの主体が考えられ、研究開発大臣、国の関係行政機関の長、研究代表者/従事者、シンクタンク等などが考えられる[432]。協議会の機能としては、研究開発の推進に有用なシーズ・ニーズ情報の共有や社会実装に向けた制度面での協力など、 政府が積極的な伴走支援を実施し[433]、お互いの了解の下で共有される機微な情報について、協議会構成員に対し、適切な情報管理と国家公務員と同等の守秘義務を求める[434]との記述もある。

協議会設置の大きな目的として、特定重要技術調査研究機関開発基本指針の策定がある[435]。政府は、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に関する基本指針を策定し、本指針に基づき、特定重要技術の研究開発等に対し、必要な情報提供・資金支援等を実施（特定重要技術とは、先端的な技術のうち研究開発情報の外部からの不当な理由や、当該技術により外部から行われる妨害等により、国家及び国民の安全を損なう事態を生ずるおそれがあるものであり、具体的には、宇宙・海洋・量子ＡＩ等の分野における先端的な重要技術を想定している）。研究開発の推進に有用なシーズ・ニーズ情報の共有や社会実装に向けた制度面での協力など政府が積極的な伴走支援を実施し[436]、お互いの了解の下で共有される機微な情報について、協議会構成員に対し、適切な情報管理と国家公務員と同等の守

---

429 同上、9 頁。（2023 年 1 月 26 日閲覧）
430 同上、9 頁。（2023 年 1 月 26 日閲覧）
431 内閣府、「経済安全保障推進法の概要」、4 頁。
［https://www.cao.go.jp/keizai_anzen_hosho/doc/gaiyo.pdf］、（2022 年 1 月 24 日閲覧）。
432 同上、
4 頁。（2023 年 1 月 26 日閲覧）。
433 同上、4 頁。（2023 年 1 月 26 日閲覧）。
434 同上、4 頁。（2023 年 1 月 26 日閲覧）。
435 内閣府、「経済安全保障推進法の概要」、4 頁。
［https://www.cao.go.jp/keizai_anzen_hosho/doc/gaiyo.pdf］、（2022 年 1 月 24 日閲覧）。
436 同上、4 頁。（2023 年 1 月 26 日閲覧）

秘義務を求める[437]）守秘義務の対象となる情報は政府のこれまでの研究成果、サイバーセキュリティの脆弱性情報等を想定している[438]。また、研究成果は公開が基本[439]とし公的分野での活用が一定程度見込まれる段階に至った時点で、当該技術の詳細が公開されることにより公的利用に支障が生じる場合には、 例外的ではあるが、協議会で合意された対応方針を踏まえ、一定の情報をノウハウとして管理するなどの適切な対応が求められる[440]。

2　課題抽出

経済安全保障シンクタンクに関しては令和５年度の創設が目指されており、まだ本格的な運用がなされている状況ではない。本節ではシンクタンクにおいて求められる能力を持った人材をいかにして輩出していくのかという人材育成の観点から課題抽出を行う。本節では現状分析を踏まえた上で以下の 3 つの課題を抽出した。

（1）シンクタンク研究の活動に従事できる人材の育成

経済安全保障シンクタンクにおける調査研究には、分野横断的に知見を持ち、研究活動に従事できる人材の育成が求められている。高度な技術の中から経済安全保障上、必要とされる技術について見極める力が必要となる。本節ではシンクタンクにおいて求められる要件を満たすような機関の設置に関して提言していきたいと考えている。

（2）文理融合で在学中から産官学での就業経験を持つ人材育成を行う必要性

経済安全保障上、重要となる技術を選定することはシンクタンクが果たすべき役割の一つとなる。調査研究を高い水準で実施していくためには、先端的な重要技術を巡る国内外の情勢や研究開発動向等に関して高度な知見を有する人材を中・長期的に養成・確保していくことも必要[441]であることから、その選定に際して、文理融合型の知見が必要である。また産官学での就業経験を持つことがより幅広い視野から物事を捉える能力の醸成につながり、産官学の多様な主体による有機的な連携が求められている経済安全保障政策においては、その能力は効果的に作用する。

経済安全保障シンクタンクに求められる要件を満たす人材を育成するためには大学や大学院終了後の研修及び経験により、育成を図るという方策も考えうる。しかし、それらの人材を育てることには相当程度の時間がかかる。政府発表の経済安全保障推進法案をめぐる国会論議においても「シンクタンクは一朝一夕に育成できるものでもないと考えている[442]」

---

[437] 同上、4 頁。（2023 年 1 月 26 日閲覧）
[438] 同上、4 頁。（2023 年 1 月 26 日閲覧）
[439] 同上、4 頁。（2023 年 1 月 26 日閲覧）
[440] 内閣府、「特定重要技術の研究の開発の促進及びその成果の適切な活用に関する基本指針」、14 頁。
[441] 同上、26 頁。
[442]参議院事務局企画調整室、「経済安全保障推進法案をめぐる国会論議」、2022 年 7 月 8 日、53 頁。

との記述があり、これはシンクタンクの人材育成も包含している。そのため人材の育成に関しても長期的なスパンでの検討が求められるため、その大きな目的が人材の育成にある大学及び大学院の過程から実施することが求められると考えた。

(3)　終了後、退職後の多様なキャリアパスを用意する必要性

経済安全保障シンクタンクがより充実したものとなるためには経済安全保障関連の仕事を離れた後でも多様な選択肢が残されていることや、経済安全保障シンクタンクの要件を満たす人材の養成に関して何らかの機関やカリキュラムが発足した場合にそれらを修了したのちの柔軟なキャリアパスを用意する必要がある。それにより多くの人材がシンクタンクでの研究に関心を持つ雰囲気の醸成につながる。

実際、「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に関する基本指針」の中にもシンクタンクの人材の募集という観点から「シンクタンクが優秀な科学者・企業関係者のキャリアパスの一つとしての立場を確立していくことが重要である」との記述や「人材の確保にあたっては、例えば、所属する大学に籍を置いたままクロスアポイントメント制度を活用して調査・分析に従事するなど個々の事情に応じて柔軟な対応を行うことが期待される[443]」との記述があることから政府としてもシンクタンク研究従事者のキャリアパスに関しては柔軟な制度の構築を目指していると考えられる。そのため、修了後、退職後のキャリアパスを多様にする制度の構築に関しても本節で検討していく。

［https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2022pdf/20220708043.pdf］、（2023 年 1 月 19 日閲覧）。

[443] 内閣府、「特定重要技術の研究の開発の促進及びその成果の適切な活用に関する基本指針」、27 頁。

3　政策提言

上記に述べた課題のもと、本節では三つの提言を行うこととする。

（1）大学における領域横断部門の経済安全保障プログラムの創設

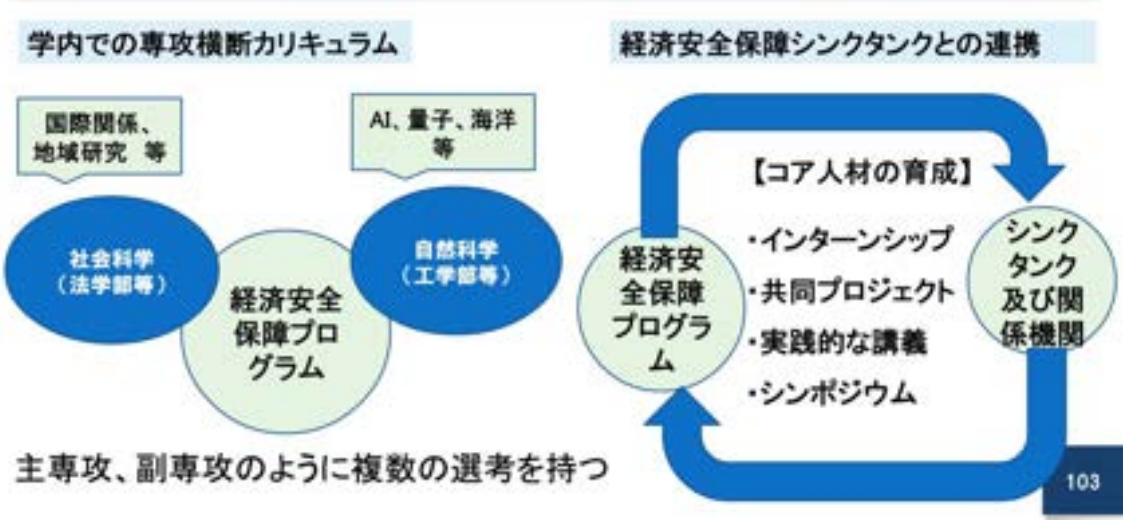


図 59　経済安全保障プログラムの概要

出典：筆者作成

調査研究においては、将来の国民生活及び経済活動の維持にとって重要なものとなり得る先端的な技術に関して、技術面のみならず社会制度や社会システムまでを含めた国内外の情勢や研究開発動向等を適切に調査・分析できる能力を有することが求められる[444]。との記述より、経済安全保障シンクタンクにおいて働く人材には領域横断な知見が求められていると言える。技術が高度化している現代社会及び、最先端の技術に関する知見が求められる経済安全保障政策においては、そのような高度な技術の中から特定重要技術について見極める力が必要となる。

本提言における経済安全保障プログラムは大きく学内での専攻横断カリキュラムと経済安全保障シンクタンクの連携から構成されている（図参照）。学内での専攻カリキュラムに関しては国際関係、地域研究等の社会科学の知見と AI、量子、海洋等の自然科学に関する知見、文理に関して知見を深めることができるプログラムとなっている。

続いて経済安全保障シンクタンクとの連携に関してである。こちらは経済安全保障プログラムと経済安全保障シンクタンク及び関係機関との連携により、企業でのインターンシップ、共同プロジェクト、実践的な講義、シンポジウムなどを通して経済安全保障上のコア人材の育成を目指すものである。以下、構成員及びそのメリットを述べていく。

---

444 内閣府、「特定重要技術の研究の開発の促進及びその成果の適切な活用に関する基本指針」、24 頁。

ア　大学等の研究機関

参加機関は経済安全保障重要技術の育成に関して重要な技術開発に従事する研究所及び人文社会学系の政治学・経済学・法学・社会学等の関連分野で構成される。メリットとして、既存の大学予算とは別に経済安全保障施策に関連する予算措置により、教職員給与・研究費・施設維持費等を負担する（参照：ＯＩＳＴ）。これにより重要技術育成に対して価値貢献できる人材の招聘及び確保について柔軟な対応が可能になる。

イ　民間企業

参加機関は経済安全保障協議会に参加する企業等で構成される。メリットとして、企業の経済安全保障戦略上、求められる人材の確保・育成を行うことが挙げられる。

ウ　行政機関

参加機関は経済安全保障シンクタンク及び関係省庁で構成される。メリットとして、シンクタンクの研究により必要な要件を満たすコア人材の獲得につながる。

エ　学生

学生にとってのメリットとしては、①出身学部・専攻は問わない、②プログラムが修士課程と博士課程からなる、③修士で修了することも可能、博士課程進学者には授業料を免除し、優秀者には学振に相当する生活費（月20万円）及び研究費（しかるべき金額）を支給、④文系出身者には最初の修士課程で、理系分野に関する素養を習得してもらう⑤１学年につき、複数回関係機関での３週間程度のインターンシップ期間を設け、それに対して単位を付与し、それらの授業は必修科目とする、⑥多様なキャリア選択を想定する、⑦元の学部の修士を取ることも可能とする（工学部であれば工学修士、法学部であれば法学修士など）。

オ　教員

教員に対してのメリットは①業務に従事する教員には賞与を与える、②定員を超える新規教員の採用を可能とする、③既存の研究費にプラスアルファで使える、である。

海外からの高度人材に関しては家族の帯同を含めて処遇するとともに、懸念国から自由な研究環境を求めてきた者についてはその家族を含めた安全の確保を含めた処遇を充実させる事で人材を世界中から集めることとする。

なお、財源については経済安全保障重要技術育成プログラムや経済安全保障シンクタンク設置のために内閣府に割り当てられる費用からの捻出を想定している。

(2) 国家公務員試験に経済安全保障専門職試験の導入

この制度は国家公務員試験において経済安全保障専門職試験の導入を企図している。経

済安全保障上重要と考えられる科目に関する試験を課し、経済安全保障シンクタンク及び、経済安全保障上重要な役割を担う機関へ配属することで、経済安全保障上の重要人材の育成を目的とするものである。

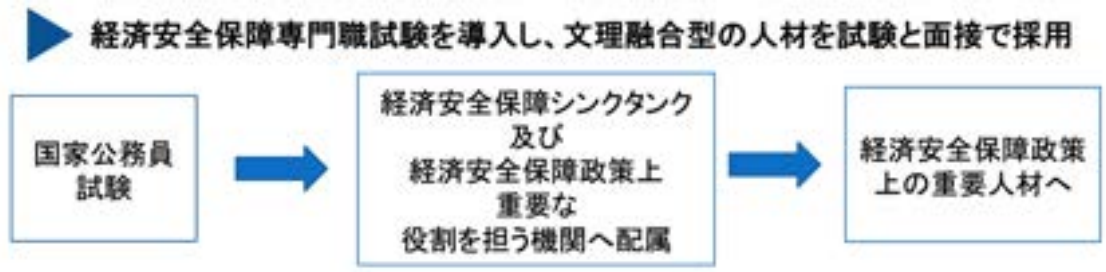


図 60　経済安全保障専門職試験導入の概要

出典：筆者作成

(3) 経済安全保障専門人材育成制度の導入

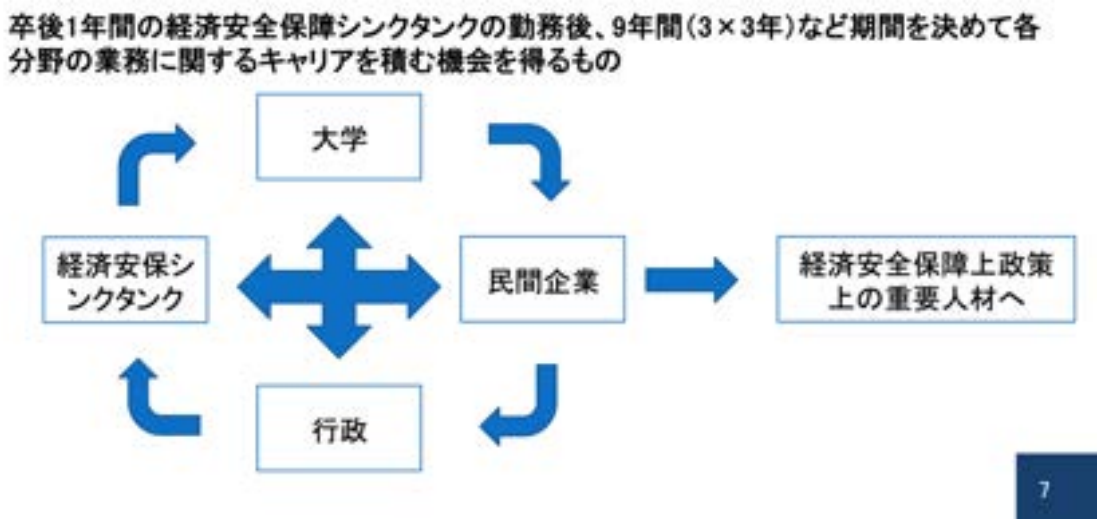


図 61　経済安全保障専門人材育成制度の導入の概要

出典：筆者作成

経済安全保障専門人材育成制度創設の目的としては既に専門領域を持つ人材を雇用し、制度の中で産官学の機関での就労を経験することにより、充実した人脈の形成を行うのと同時にシンクタンク研究員として求められる要件をバランスよく満たす人材の育成を目的とする。経済安全保障シンクタンクに関係する各機関が有機的に連携し、本人の専攻や希望を聞いた上で受け入れ先を総合的に判断し、人材を 3 年間受け入れることで重要人材を育成する。その他に関しては①3 年間の任期を決め自身の所属以外の産官学機関で就労経験を積む、②給与等の人件費、研究費等は経済安全保障シンクタンクが負担する、③経済安全保

障シンクタンクの初期雇用研究員の 2 割程度の人材に適用する、④育成期間は研究成果の発表などは自由に出来る、⑤就業先は本人のこれまでの経験や希望を聞いた上で総合的に判断する、⑥人事機関が定期的に人材に対し、適切な人材へ育つための支援を行う、⑦育成期間には国家公務員と同等の守秘義務を与えることで機微な情報の共有を可能とする。

第 4 節　産官学を交えた情報共有体制の構築についての提言

繰り返しになるが、経済安全保障の確保に資する施策を総合的かつ効果的に推進していくためには、政府がその役割を果たすことはもとより、実際に経済活動を行っている事業者等を含む国民全体の理解と協力が不可欠である[445]。もっとも、政府の介入を要しない自由な経済活動が従前においては重要視されていたため、経済安全保障という考えが広まったのはここ最近であり、その考えを理解していない企業や大学も多いだろう。また、経済安全保障上の相談・被害報告をすることが可能な体制が整っていなければ、企業や大学が効果的な施策を講じることは難しい。経済安全保障の主体は、政府機関以外の多岐に渡るため、より実効的な施策を講じるためには、企業や大学が持つ経済安全保障上の脅威や被害といった情報を政府機関が収集・分析し、実効的な施策を講じることが必要である。

このような考えの下、本節では、経済安全保障における政策提言の一つとして、「産官学を交えた情報共有体制の構築」について論じていくものとする。「1」にて、本研究において産官学が連携した情報共有体制の構築という分野を扱うことについての意義を示し、次いで政府における現行の体制について分析する。「2」では現状における政府の情報収集・分析の両者における課題の抽出を行う。最後に「3」にて、前節の課題を踏まえた上で国家安全保障局経済班へ向けた政策提言を行う。

1　現状分析

(1)　意義

経済安全保障の確保のための産官学を交えた情報共有体制の構築について、産官学はそれぞれどのように考えているのだろうか。

政府の考えから見ていこう。経済安全保障推進法第 2 条第 1 項を根拠に、令和 4 年 9 月 30 日に閣議決定された「経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本的な方針」（以下「基本方針」という。）においては、第 1 章第 2 節「安全保障の確保に関する経済施策の実施に当たって配慮すべき事項」の (3) に「事業者との連携」が記されており、「事業者等による自発的な行動を促進するため、第 4 章でも触れるように、本法や本基本方針等の趣旨や政策内容について周知・広報及び情報共有を行うこと等に努める」という記述がある[446]。また、第 4 章「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し必要なその他の事項」の (3) には、「本法等に関する国民に対する周知・広報及び情報提供」が記されており、「政府は、本法、本基本方針、基本指針及び下位法令の趣旨や政策内容並びに 4 施策に係る具体的な手続等について、事業者等を含む国民に対して、十分な周知・広報及び情報提供を行うとともに、施策によっては、その措置の対象者からの相談にきめ細かく対応する相談窓口を設置することや、施策の実施に係る Q&A

[445] 内閣府、「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基本的な方針」、2022 年 9 月 30 日、5 頁。［https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonhoushin.pdf］、（2023 年 1 月 16 日閲覧）。

[446] 同上、5 頁。（2023 年 1 月 16 日閲覧）。

を公表すること等を通じて積極的に双方向のコミュニケーションを図る必要がある」という記述がある[447]。

警察庁警備局外事情報部外事課経済安全保障推進室によると、経済安全保障施策を実施するためには、企業及び大学の自衛意識を高める必要があり、警察としてのアウトリーチ活動の重要性を強調していた[448]。

このように、政府の経済安全保障施策の軸となる基本方針には、事業者等に対して情報提供を行うこと、相談窓口を通して双方向のコミュニケーションを図ることが必要と記されている。そのために、産官学の情報共有体制の構築は不可欠である。

次に、企業の考えについて見ていく。JETRO が 2022 年 9 月に実施した日本企業への経済安全保障についてのアンケートによると、経済安全保障を経営課題として認識する割合は 78.8%と高い値であった[449]。また、経済安全保障に関わる体制や取組について、「情報収集の機能強化」（64.2%）が最も多くの回答を集めた[450]。取り組む上での課題としては、「取り組むための社内リソース不足」（48.4%）に次いで、「関連する情報を集めることが難しい」（39.5%）、「経営層における理解や課題認識の浸透が不十分である」（26.0%）、「サプライヤーの協力や理解を得ることが難しい」（16.0%）が並んだ[451]。

これらのアンケート結果より、企業は経済安全保障を経営課題として認識しており、情報収集の機能強化に焦点を当てた取組をしているものの、関連する情報を集めることが難しいという問題を抱えていることが理解できる。さらに、経営層やサプライヤーの理解を得ることができないという回答も、経済安全保障の情報が上手く行き届いていないことが露呈した結果である。某セキュリティ企業へヒアリングを行った際には、国だけが保有している情報もあるため、可能であれば共有してもらいたいといった回答もあった[452]。以上より、政府から企業への情報提供の重要性が理解できる。

また、課題として「取り組むための社内リソースが不足している」と回答した企業の一つが「懸念のある取引の是非を判断する部署や方針がなく、対応に苦慮している」とコメントしていることから[453]、企業が実効的に経済安全保障施策を講じるうえで、その判断を仰ぐ相談体制などが求められていることが伺える。

---

447 同上、11 頁。（2023 年 1 月 16 日閲覧）。
448 警察庁警備局外事情報部外事課経済安全保障推進室に対するヒアリング調査（2022 年 7 月 7 日実施）。
449 JETRO、「経済安全保障、8 割の日本企業が経営課題と認識」、2022 年 11 月 24 日。［https://www.jetro.go.jp/biz/areareports/special/2022/1002/2c2eecd972c6c47e.html］、（2022 年 12 月 2 日閲覧）。
450 同上。（2023 年 1 月 22 日閲覧）。
451 同上。（2023 年 1 月 22 日閲覧）。
452 某セキュリティ企業に対するヒアリング調査（2022 年 8 月 3 日実施）。
453 JETRO、「経済安全保障、8 割の日本企業が経営課題と認識」。（2023 年 1 月 22 日閲覧）。

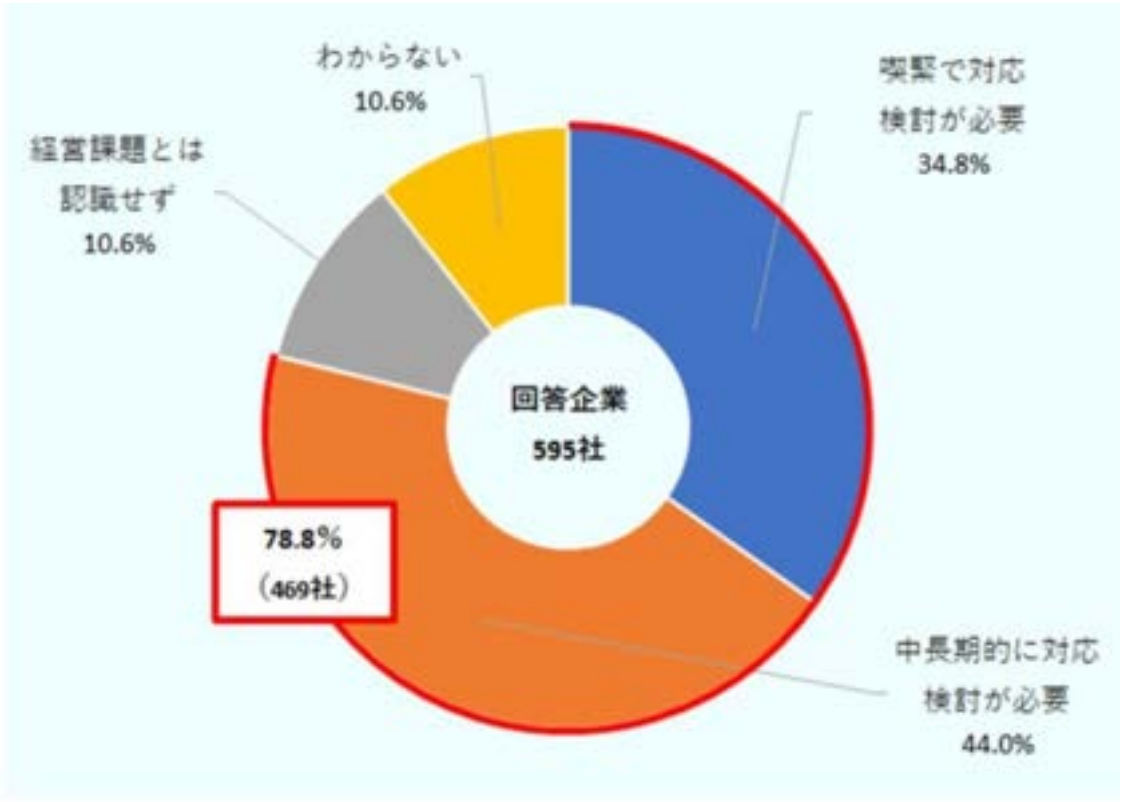


図 62　経済安全保障を経営課題として認識しているか

出典：JETRO

図 63　経済安全保障に関わる体制や取組（複数回答）

出典：JETRO

図 64　経済安全保障に取り組む上での課題（複数回答）

出典：JETRO

最後に、大学等について見ていく。東北大学金属材料研究所副所長の佐々木孝彦教授によると、東北大学は多くの留学生を受け入れており、研究インテグリティを確保する動きはあるものの、経済安全保障といった言葉が話題になることは少なく、政府への相談体制についても形式上は存在するものの、実質的には相談体制があるとはいえず、これから政府と調整をすることが実情であるとのことだった[454]。つまり、大学・政府間の相談体制は、これから本格的に構築せねばならないといえる。

また、経済安全保障に精通している東京大学先端科学技術研究センター特任講師である井形彬氏へのヒアリングでは、政府から事業者等へオープンソースとして定期的に情報を提供していかなければならないことはもちろんのこと、政府も事業者等からの情報を必要としており、事業者等から恒常的に情報を収集できる枠組みの形成が求められるという回答を頂いた[455]。さらに、自由民主党の甘利明氏へのヒアリングでは、特にサイバーセキュリティの世界において、事業者等が自発的に行動するのはもとより、事業者等の想定していなかった事件等の情報を政府に渡すことによって、常に新しい情報を産官学で共有する体制整備が必要であると回答を頂いた[456]。

[454] 東北大学副理事（研究公正担当）兼金属材料研究所副所長　佐々木孝彦教授に対するヒアリング調査（2022 年 10 月 11 日実施）。

[455] 東京大学先端科学技術研究センター特任講師　井形彬氏に対するヒアリング調査（2022 年 10 月 13 日実施）。

[456] 自由民主党元幹事長　甘利明氏に対するヒアリング調査（2022 年 9 月 26 日実施）。

以上より、産官学及び政治家や研究者等が、政府と事業者等との双方向の情報共有体制を必要としていることが明らかとなった。従って、本節では、経済安全保障に関する産官学を交えた情報共有体制について現状分析及び課題を抽出した後、より一層の共有体制を構築するべく提言を行いたい。

(2)　現状分析

では、現状において経済安全保障に関する産官学を交えた情報共有体制は構築されているのだろうか。経済安全保障に関する分野と言っても多岐に渡るため、ここでは特に3つの分野、サイバーセキュリティ、サプライチェーン、技術流出等防止について情報共有体制が構築されているのか見ていく。

ア　サイバーセキュリティ分野における情報共有体制

まず初めに、サイバーセキュリティにおける情報共有体制について概観する。サイバーセキュリティ分野においては、既に国・各地域・各都道府県で情報共有体制が構築されつつある。これについて、制度等の分析を行っていく。

（ア）　サイバーセキュリティ協議会について

最初に、国が運営する情報共有体制について説明する。

〇名称：サイバーセキュリティ協議会

〇設立年月日：平成31年4月1日

〇設立根拠：

サイバーセキュリティ基本法（以下「法」という。）第17条第1項に基づき組織[457]。

〇活動目的：

協議会は、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、大学その他の教育研究機関等のうち、我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行うこと（サイバーセキュリティ協議会規約（以下「規約」という。）第3条）。

〇構成：

協議会は事務局、運営委員、構成員からなる。事務局はNISC及び政令指定法人JPCERT/CCが務める。運営委員はNISCのサイバーセキュリティ戦略本部長等からなる。構成員については次に記す。

〇構成員の詳細：

[457] NISC、「サイバーセキュリティ協議会について（詳細版）」、2022年4月、3頁。［https://www.nisc.go.jp/pdf/council/cs/kyogikai/kyogikai_gaiyou.pdf］、（2023年1月15日閲覧）。

協議会は構成員をもって構成される。構成員になることができる事業者等は、国の関係行政機関、地方公共団体、重要インフラ事業者、サイバー関連事業者、大学・教育研究機関等である[458]。加入は任意であり、協議会に加入したい事業者等は入会申し込みを行い、運営委員会の判断を仰ぐこととなる。令和 4 年 4 月 1 日現在において、構成員の数は 303 者である。なお、構成員は一般には非公開となっている。

〇タスクフォース：

当協議会には、タスクフォースと呼ばれる一般の構成員とは異なる構成員が中心となり、サイバーセキュリティに関する脅威情報等の積極的な共有及び分析を行い、我が国のサイバーセキュリティを確保するために必要な情報の作出及び共有を積極的に行う（24 条タスクフォース規則（以下「規則」という。）第 2 条）。タスクフォースは第一類構成員と第二類構成員に分けられる。

・第一類構成員は、構成員のうち、他の情報共有体制に参加又は運営する主体であって、活動に積極的に貢献する能力と意欲を有し、サイバーセキュリティの確保に資する情報を積極的に提供できる者（規則第 1 条 1 号より抜粋）が申し込みを行い任命された者及び JPCERT/CC から成る。

・第二類構成員は、構成員のうち、第一類構成員等から提供される情報に対し一定の応答を行うことができる能力と意欲を有する者が申し込みを行い任命された者からなる。

〇活動内容：

以下、箇条書きに活動内容を整理していく。

・総会：毎年の定時総会及び運営委員会が必要と認める場合は、臨時総会を開催している（規約第 10 条より抜粋）。総会では、規約の改正等を行っている。

・情報分析活動：情報分析活動は、第一類構成員等及び第二類構成員が行う。第一類構成員等は、自組織単独ではまだ確証を得るに至っていない専門的な分析内容等を積極的に提供し合い、具体的な対策情報等を作出していく[459]。第二類構成員は、第一類構成員等から共有された対策情報に対してフィードバックを行い、第一類構成員等による対策情報等の精度向上等に積極的に協力する[460]。

・情報共有活動（協議会→構成員）：事務局は、構成員に対し、サイバーセキュリティの確保に資する情報を随時提供する（規約第 16 条第 3 項）。事務局は、構成員に対して情報を提供するに際し、TLP（Traffic Light Protocol）という、情報共有範囲を示すことができる（規約第 17 条第 4 項）。

・情報共有活動（構成員→協議会）：構成員は、事務局に対し、サイバーセキュリティの確保に資する情報を任意に提供することができる（規約第 16 条第 3 項）。これは、直感的な違和感といった早期の段階であっても、希望すれば、守秘義務の下、安心して情報提供や相

[458] 同上、1 頁。（2023 年 1 月 15 日閲覧）。
[459] 同上、16 頁。（2023 年 1 月 15 日閲覧）。
[460] 同上、16 頁。（2023 年 1 月 15 日閲覧）。

談を行うことが可能であり、対策手法の助言や周辺状況のフィードバックを得ることができるというものである[461]。共有された情報は、第一類構成員等や第二類構成員が分析し、フィードバックを得ることができる。

・情報提供義務：協議会は、構成員に対して、法第 17 条第 3 項に基づく情報提供等の協力の求めを行うものとする（規約第 23 条）。また、協議会は、規約第 23 条第 1 項の規定にかかわらず、第一類構成員又は第二類構成員に対して情報提供の協力を求める必要があると認められる場合には、法第 17 条第 3 項に基づく情報提供等の協力の求めを行うものとする（規則第 4 条）。

〇罰則の有無等：

規約第 18 条には秘密の管理について記載があり、構成員は、事務局に対し任意に情報を提供するに際し、法第 17 条第 4 項に規定する秘密の有無を明示すること（規則第 18 条第 1 項）、また、事務局は、構成員に対し情報を提供するに際し、法第 17 条第 4 項に規定する秘密の範囲を明示することができる（規則第 18 条第 2 項）。

法第 17 条第 4 項には、「協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事務に関して知りえた秘密を漏らし、又は盗用してはならない」との記載があり、法第 38 条において、「第 17 条第 4 項（中略）の規定に違反した者は、1 年以下の懲役又は五十万円以下の罰金に処する」と記載がある。

つまり、協議会及び構成員は、情報を共有する際に秘匿の有無及び共有範囲を指定することができ、それに反した協議会及び構成員は、行政罰を科されることとなる。

[461] 同上、16 頁。（2023 年 1 月 15 日閲覧）。

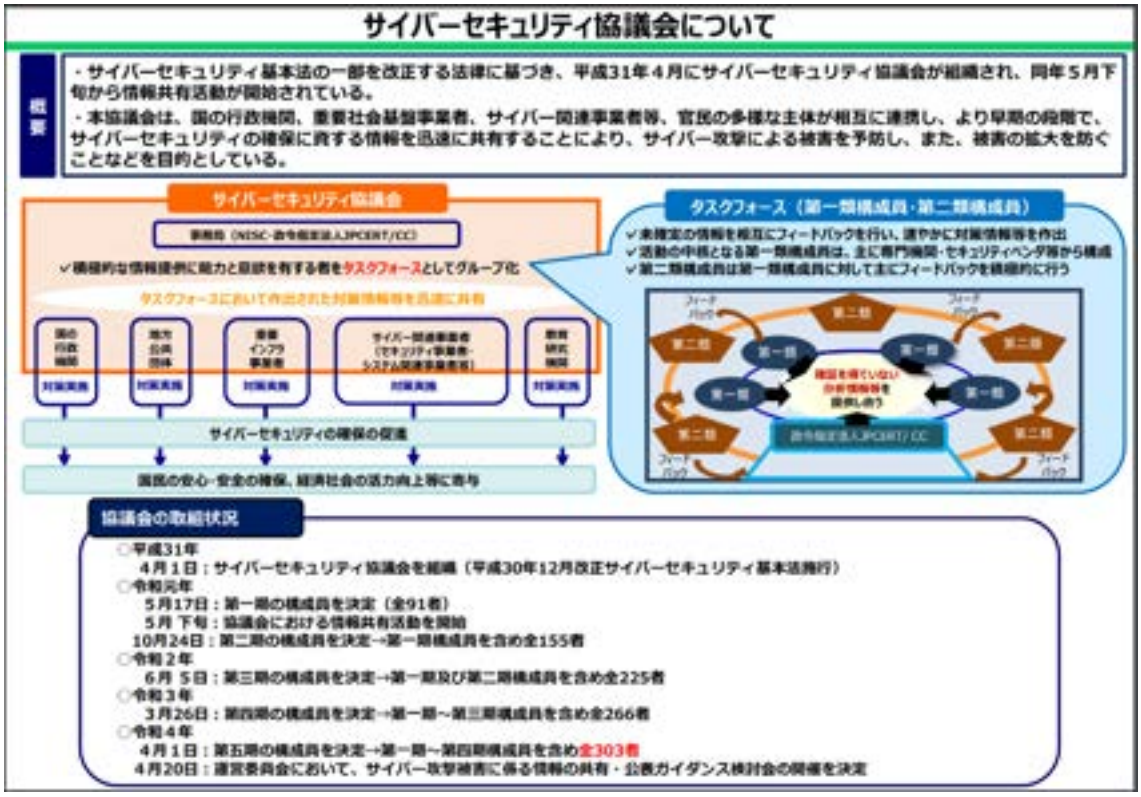


図 65　サイバーセキュリティ協議会について

出典　NISC

（イ）　東北地域サイバーセキュリティ連絡会について

続いて、各地域が運営する情報共有体制として、東北地域で運営されているものについて説明する。

〇名称：東北地域サイバーセキュリティ連絡会

〇設立年月：令和 4 年 11 月

〇活動目的：

東北地域におけるサイバーセキュリティに対する意識向上・人材育成等に向けた取組を、産官学が連携して行うこと[462]。

〇構成：

東北経済産業局及び東北総合通信局が連携して事務局を運営し、国の機関・地方公共団体・業界団体・事業者・研究機関・教育機関・連携団体等で構成される。令和 3 年 11 月 8 日現在において、構成員は計 43 団体。

〇活動内容[463]：

[462] 東北経済産業局、「東北地域サイバーセキュリティ連絡会の概要」、2021 年 11 月 8 日。［https://www.tohoku.meti.go.jp/s_joho/topics/pdf/cyber_security_gaiyo.pdf］、（2023 年 1 月 15 日閲覧）。

[463] 同上。（2023 年 1 月 15 日閲覧）。

・NISC からのサイバーセキュリティに関する最新情報等の提供
・サイバーセキュリティ対策をテーマとした中小企業のサイバー対応事例等を含むセミナー開催、インシデント演習の実施
・構成員相互間の情報共有
・その他会員に有益となる活動
〇罰則の有無：無し。

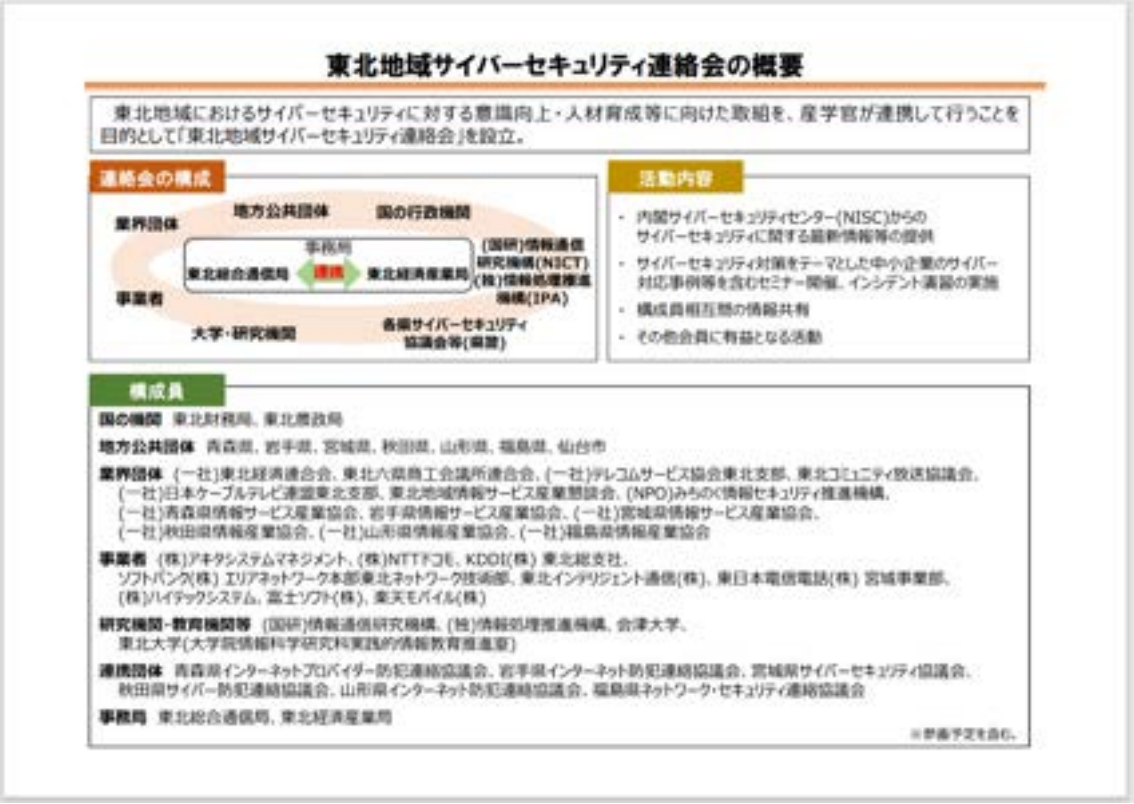


図 66　東北地域サイバーセキュリティ連絡会の概要
出典：東北経済産業局

また、政府が主導する同様の協議会として、北海道地域情報セキュリティ連絡会、関東サイバーセキュリティ連絡会、東海サイバーセキュリティ連絡会、北陸サイバーセキュリティ連絡会、関西サイバーセキュリティ・ネットワーク、中国サイバーセキュリティ連絡会、四国 IT 協同組合がある[464]。

（ウ）　宮城県サイバーセキュリティ協議会について

最後に、都道府県が運営する情報共有体制として、宮城県で運営されているものについて

[464] 経済産業省、「地域 SECUNITY リスト」、2022 年 5 月。
［https://www.meti.go.jp/policy/netsecurity/comunitylist.pdf］、（2023 年 1 月 15 日閲覧）。

説明する。

〇名称：宮城県サイバーセキュリティ協議会

〇設立年月日：令和元年 5 月 8 日

〇設立契機：

2019 年はサイバー犯罪の件数が最も増加していた時期であり、2020 東京オリパラ競技大会の開催に万全を期すため国にサイバーセキュリティ協議会が設立されたことに鑑み、県においてもサイバーセキュリティ対策が急務であることより、宮城県と宮城県警察が一体となり、発足するに至った[465]。

〇活動目的：

会員相互及び関係機関が緊密に連携し、サイバーセキュリティ等に関する各種情報交換及び情報共有を行い、サイバーセキュリティに関する施策の推進に努め、県民生活の安心・安全の確保及び経済社会の活力向上等に寄与すること[466]。

〇構成：

当協議会の構成員は、役員・特別支援構成員・参加団体に区別される。

・役員：会長を東北大学データエナジー創生機構特任教授の曽根秀昭氏が務め、事務局は宮城県企画部デジタル宮城推進課及び宮城県警察本部生活安全部サイバー犯罪対策課が務めている。また、顧問は宮城県知事が務めている[467]。

・特別支援構成員：一般財団法人日本サイバー犯罪対策センター、東北工業大学、経済産業省東北経済産業局といった産官学を代表する計 7 団体が構成している。特別支援構成員は、国のサイバーセキュリティ協議会におけるタスクフォースと類似しており、積極的に情報発信を行う役割を担っている[468]。

・参加団体：民間事業者・国・地方公共団体・医療機関から構成され、その数は民間事業者が 83、国・地方公共団体・教育機関・医療機関が 46 となっている[469]。原則加入は任意となっている。

〇活動内容

・情報共有活動（協議会→構成員）：メーリングリストを用いて、脅威事案等の情報共有や広報啓発等を行っている。また、各種セミナーを開催し、情報セキュリティ対策・サイバーセキュリティ対策を推進している[470]。

・情報共有活動（構成員→協議会）：構成員から、事業等へ被害があった場合の相談体制を設けている[471]。

---

[465] 宮城県庁及び宮城県警察に対するヒアリング調査（2022 年 11 月 1 日実施）。

[466] 宮城県警察、「宮城県サイバーセキュリティ協議会」、2019 年 5 月。［https://www.police.pref.miyagi.jp/cyber/kyougikai.html］、（2023 年 1 月 15 日閲覧）。

[467] 同上。（2023 年 1 月 15 日閲覧）。

[468] 宮城県庁及び宮城県警察に対するヒアリング調査。

[469] 宮城県警察、「宮城県サイバーセキュリティ協議会」（2023 年 1 月 15 日閲覧）。

[470] 宮城県庁及び宮城県警察に対するヒアリング調査。

[471] 同上。

〇罰則の有無：守秘義務はあるものの罰則は設けていない[472]。

また、政府が主導する同様の協議会として、北海道中小企業サイバーセキュリティ支援ネットワーク、福島県ネットワーク・セキュリティ連絡協議会、地域中小企業における情報セキュリティの普及促進に関する検討会 （茨城）、埼玉サイバーセキュリティ推進会議、地域中小企業における情報セキュリティの普及促進に関する検討会 （千葉）、サイバーセキュリティパートナーシップ、サイバー空間の脅威に対する新潟県産学官民合同対策プロジェクト推進協議会、地域中小企業における情報セキュリティの普及促進に関する検討会 （長野）、鳥取県サイバーセキュリティ対策ネットワーク、山口県サイバーセキュリティパートナーシップ、愛媛県ネットワーク防犯連絡協議会、一般社団法人 熊本県サイバーセキュリティ推進協議会、一般社団法人 鹿児島県サイバーセキュリティ協議会、沖縄サイバーセキュリティ・ネットワークがある[473]。

イ　サプライチェーン分野における情報共有体制

次に、サプライチェーンにおける情報共有体制について概観する。

サプライチェーンにおける情報共有体制としてまず挙げられるものは、「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」である。このコンソーシアムの活動内容は、サプライチェーンを共有する企業間における高密度な情報共有・機微技術情報の流出懸念がある場合の報告・多数の関係者に影響するおそれがある場合の公表である[474]。当コンソーシアムの事務局は独立行政法人情報処理推進機構が担っている。もっとも、当コンソーシアムは国・地方・都道府県との連携がないことより、現状分析からは外すこととする。

最近の出来事として、令和4年10月14日に「第1回サプライチェーンデータ共有・連携ワーキンググループ」が行われた。事務局は経済産業省通商政策局である。このワーキンググループでは、自然リスク、地政学リスク、経済リスクといったサプライチェーン上のリスクを念頭に、有識者が今後のサプライチェーンの在り方について議論している[475]。

以上より、産官学を交えた情報共有体制は存在するものの、国から都道府県をつなぐような情報共有体制の構築には至っていないことが理解できる。

ウ　技術流出等防止分野における情報共有体制

最後に、技術流出等防止における情報共有体制について概観する。

第一に、公安調査庁では、経済安全保障特集ページを設けて、重要情報の流出防止のための発信を行っている[476]。また、「経済安全保障に関するご相談・講演依頼等窓口」を設け、

---

472 同上。
473 経済産業省、「地域SECUNITYリスト」（2023年1月15日閲覧）。
474 SC3、「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とは」、2020年11月1日。［https://www.ipa.go.jp/security/sc3/about/］、（2023年1月15日閲覧）。
475 経済産業省、「サプライチェーンデータ共有・連携WG第1回　事務局資料」、2022年10月14日。［https://www.meti.go.jp/shingikai/external_economy/global_supply_chain/supply_chain_data/pdf/001_05_00.pdf］、（2023年1月15日閲覧）。
476 公安調査庁、「経済安全保障特集ページ」、2022年6月10日。［https://www.moj.go.jp/psia/keizaianpo.top.html］、（2023年1月15日閲覧）。

政府からの情報共有及び政府への情報共有体制を構築している。もっとも、前述した佐々木孝彦教授へのヒアリングからもわかるように、相談をしたい側から見ると体制面での整備にとどまり、実質的には機能していない可能性もあることが理解できる。　第二に、警察庁では、警備局外事情報部外事課経済安全保障室を中心に、「技術流出の防止に向けて」という特設サイトを設け、技術流出を防止する上で理解すべき「情勢」「事例」「対策」などを動画やパンフレットを通し、一種のアウトリーチ活動として企業やアカデミアに情報発信をしている[477]。

第三に、経済産業省では、各地域の経済産業局を中心に、「技術流出防止管理説明会・安全保障貿易管理説明会」を開催し、経済安全保障を念頭に置いたアウトリーチ活動を行うことで、情報共有を行っている[478]。

第四に、内閣府及び文部科学省では、主に企業やアカデミアの研究機関に対して、研究インテグリティ[479]の確保を求めるための情報発信を行っている[480]。

以上より、政府からの情報発信は複数の省庁から行われているものの、事業者等からの相談体制を含む情報共有体制は構築されていないと理解できる。

2　課題抽出

ここでは、前節で行った現状分析から課題を抽出する。ここでの課題抽出を基に、「3」の政策提言へつなげていく。

(1)　サイバーセキュリティ分野における情報共有体制に係る課題

まずは、サイバーセキュリティ協議会に係る課題を抽出していく。サイバーセキュリティ協議会は、産官学が連携した情報共有体制であり、国・各地域・各都道府県のつながりもあることから、情報共有体制として機能していると思われる。現状分析を基に課題抽出を行い、当協議会を基にした情報共有体制の構築を政策提言では行いたい。

第一に、国のサイバーセキュリティ協議会の活動内容について、タスクフォースを設け実

---

477 警察庁、「技術流出の防止に向けて」、2022 年 8 月。
［https://www.npa.go.jp/bureau/security/economic-security/index.html］、（2023 年 1 月 15 日閲覧）。

478 関東経済産業局、技術流出防止管理説明会、2022 年 9 月 22 日。
［https://www.kanto.meti.go.jp/seisaku/boeki/keizaianpo_seminar.html］、（2023 年 1 月 15 日閲覧）。

479 研究インテグリティとは、研究の国際化やオープン化に伴う新たなリスクに対して新たに確保が求められる、研究の健全性・公平性を意味する。この新たなリスクにより、開放性、透明性といった研究環境の基盤となる価値が損なわれる懸念や、研究者が意図せず利益相反・責務相反に陥る危険性が指摘されている。こうした中、我が国として国際的に信頼性のある研究環境を構築することが、研究環境の基盤となる価値を守りつつ、必要な国際協力及び国際交流を進めていくために不可欠となっている。
文部科学省、「研究インテグリティ」、2021 年。
［https://www.mext.go.jp/a_menu/kagaku/integrity/index.html］、（2023 年 1 月 15 日閲覧）。

480 内閣府、「研究インテグリティの確保に係る対応方針（概要）」、2022 年 9 月。
［https://www8.cao.go.jp/cstp/kokusaiteki/integrity/gaiyo_202209.pdf］、（2023 年 1 月 15 日閲覧）。

効的な情報分析を行い、分析した情報を構成員に対し、時には守秘義務を課して共有するといった体制は評価できる。もっとも、定例的な活動が総会のみであり、全構成員が参画する機会が少ないことが課題として挙げられる。事務局であるNISC自身も、全構成員を巻き込んだ情報共有活動の活性化について更にできることはないかと考えている[481]ことより、月1回程度オンライン等で定例会を設けることで、政府からの情報を定期的に発信することが可能となり、メーリングリスト等で定期的に行っている脅威情報等についての疑問点等を発言する場を設けることで、全構成員が参画できる機会を設けることができるだろう。

第二に、事業者等からの相談体制について、国のサイバーセキュリティ協議会においては相談体制を設け脅威情報や被害情報の報告や懸念等の相談ができることにはなっている。しかし、特に中小企業にとって協議会が過度に大きな枠組みであることより、相談を躊躇するようなことがないだろうか。令和3年度における相談窓口活用件数について、協議会において取り扱った情報の件数は60件となっている[482]。サイバー攻撃はほぼ毎日行われおり、被害も多数発生している状況に鑑みると、この件数はかなり少ないように思われる。国という大きな枠組みのみならず、各地域・各都道府県に協議会を設置することで、事業者等が身の丈に合う相談窓口を見つけ、躊躇なく相談できる体制を構築することが必要だろう。

第三に、各都道府県にこのような協議会が設置されていないことが挙げられる。前述した課題にもあるように、大企業だけではなく中小企業までをキャッチアップするためには、各都道府県に協議会を設置し、政府からの情報共有及び相談体制の整備といった政府への情報共有をしていかなければならない。情報共有体制そのものが存在しない都道府県や、同じような情報共有体制を置いているものの、事務局が政府主導ではないものや構成員の募集等といった統一が図られていない都道府県がある。政府を軸とした全国画一的な情報共有体制を構築することで、より実効的に情報共有を図ることができるだろう。

第四に、罰則の有無についてである。国のサイバーセキュリティ協議会には罰則があるが、東北地域サイバーセキュリティ連絡会及び宮城県サイバーセキュリティ協議会には罰則がない。企業やアカデミアの慣習からすると罰則があるだけで厳しいという印象を持つためそもそも参加する団体がいなくなってしまう可能性があるという声が聞かれる[483]。

一方、罰則がないために情報の漏洩を恐れ、実効的な情報共有体制を構築できない懸念もある。宮城県サイバーセキュリティ協議会における課題について、情報のギブアンドテイクの一層の活発化が挙げられていることからも[484]、国のサイバーセキュリティ協議会同様最低限の罰則（1年以下の懲役又は五十万円以下の罰金）を各地域及び各都道府県の協議会へ科すことが妥当であると考える。

---

[481] NISCに対するヒアリング調査（2022年10月12日実施）。
[482] NISC、「サイバーセキュリティ協議会について（詳細版）」、4頁。（2023年1月22日閲覧）。
[483] 文部科学省　科学技術・学術政策局に対するヒアリング調査（2022年8月25日実施）。
[484] 宮城県庁及び宮城県警察に対するヒアリング調査。

(2)　サプライチェーン分野における情報共有体制に係る課題

サプライチェーンの情報共有体制において、1 の（2）のイで言及したワーキンググループが、サプライチェーン上の様々なリスクを検討している協議会として機能している。もっとも、当ワーキンググループは限られた有識者間の議論であり、ここでの議論がサプライチェーン関連事業者にどのような形で共有されるのかは定かではない。また、事業者等から政府への情報共有体制を見つけることができなかった。従って、サプライチェーンの情報共有体制において、政府からの情報共有体制及び政府への情報共有体制の構築が未だなされていないこと自体が課題であると言うことができる。

(3)　技術流出等防止分野における情報共有体制に係る課題

技術流出等防止の情報共有体制について、政府から情報を共有する体制は複数の省庁で散見された。これに対して、たしかに、想定される技術流出経路は投資買収・不正調達・留学生研究者の送り込み・共同研究や共同事業・人材リクルート・諜報活動・サイバー攻撃等であり[485]、省庁ごとに情報を共有することに疑問は抱かないものの、事業者等にとっては技術流出防止という一つの目的であるため、現存の体制では情報を収集することに時間を要する。また、政府への情報共有体制として、公安調査庁が相談体制窓口[486]をホームページに設けているものの、国の機関に直接相談できる事業者等がいるのかは甚だ疑問である。経済安全保障の分野における企業への情報提供について、「規模の大小ではなく技術の中身についての企業を優先する」といった声もあるため、このような相談体制を国だけではなく各都道府県に置くことで、中小企業をフォローすることができるのではないか。

3　政策提言

ここまで経済安全保障における産官学を交えた情報共有体制の現状分析及び課題抽出を行った。サイバーセキュリティ分野では課題はあるものの、産官学を交え、国・地域・都道府県が連携した情報共有体制が構築されており、このような情報共有体制をサプライチェーン分野及び技術流出等の分野でも構築すべきであると考える。

以上を受け、ここからは、産官学を交えた情報共有体制として、サイバーセキュリティ・サプライチェーン・技術流出等防止の 3 分野の分科会、そしてそれらを統括する経済安全保障協議会の構築等について提言を行う。

(1)　国・地域・各都道府県に「分科会」の設置

既に設置済みのサイバーセキュリティ協議会をみると、国にサイバーセキュリティ協議会、地域にサイバーセキュリティ連絡会、県にサイバーセキュリティ協議会が置かれてお

---

[485] 公安調査庁、「経済安全保障の確保に向けて 2022」、4 頁（2023 年 1 月 22 日閲覧）。
[486] 公安調査庁、「経済安全保障に関するご相談・講演依頼等窓口」、2021 年 4 月 14 日。［https://www.moj.go.jp/psia/kouan_mail_keizaianpo.html］、（2023 年 1 月 15 日閲覧）。

り、政府と事業者等との連携にとどまらず、国・地域・県が連携できる情報共有体制が構築されており、些細な相談から重大事件までの幅広い情報共有が可能となっている。そこで本研究では、政府と事業者等及び国と地域と各都道府県とが連携可能な情報共有体制を構築するべく、サイバーセキュリティ分野・サプライチェーン分野・技術流出等防止分野において、国・各地域・各都道府県へ分科会を設置することを提言する。

以下、共通する概要について記す。

〇構成員：

原則として任意加入とする。各分科会の構成員はタスクフォースである第一類構成員及び第二類構成員、そして一般の構成員とし、国・地域・都道府県で一貫した体制を組織する。

〇活動内容

・総会及び定例会の開催：年一回の総会において協議会規約等についての改定等を行う。また、月一回の定例会において、主に政府からの情報を共有し、全構成員の情報をアップデートする。

・情報共有活動（構成員→事務局）：各都道府県の協議会において、全構成員は懸念事項等が発生した際に事務局へ情報を共有する。事務局は共有情報を第一類構成員及び第二類構成員に共有することで、懸念事項の分析等を行う。懸念事項の原因等が明らかになった場合には、共有した構成員のみならず全構成員に情報を共有することで、協議会として来る脅威に備える。この際、構成員等のなかに競争企業等がおり、共有したくない情報がある場合には、あらかじめ共有範囲を指定することができる。

・情報分析活動：第一類構成員は、構成員から共有された情報及び第一類構成員内で持ち寄られた情報について、分析する責務を負う。第一類構成員が分析した情報の正確性を向上させるため、第二類構成員に分析した情報を共有し補正した後、その後全構成員に共有する。

・情報共有活動（事務局→構成員）：国内及び国外の経済安全保障施策等の情報及び構成員から共有され分析したことで明らかとなった情報を、メーリングリストを用いて共有する。機密な情報については、罰則を付した守秘義務を設け、共有することができる。

〇罰則の有無：

国・各地域・各都道府県の分科会について、「協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事務に関して知りえた秘密を漏らし、又は盗用してはならず、違反した者は、1 年以下の懲役又は五十万円以下の罰金に処する」こととする。この罰則の程度は、国家公務員法第 100 条第 1 項で定められた守秘義務に反した場合の罰則と同等であり、国のサイバーセキュリティ協議会も構成員が守秘義務に反した場合に同等の罰則を処しているため、妥当であると考える。

また、一般の構成員で守秘義務が課された情報を得たくない場合には情報を受け取ることを拒否する権利を設け、無理に罰則を処される危険にさらされないようにする。

以下、各分科会の概要を記す。

ア　「サイバーセキュリティ分科会」の設置

〇概要：

各都道府県に「〇〇県（または都、道、府）サイバーセキュリティ分科会」を設置する。事務局は各都道府県庁及び各都道府県警察とする。各地域に「〇〇地域サイバーセキュリティ分科会」を設置する。事務局は各地域の経済産業省経済産業局及び総務省通信局とする。国に「サイバーセキュリティ分科会」を設置する。事務局はNISC及び政令指定法人JPCERT/CCとする。

〇活動目的：

国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、大学その他の研究機関等のうち、我が国の経済安全保障の確保に資する一環として、サイバーセキュリティに対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行うこと。そのために主として、サイバーセキュリティの脅威情報等の共有・分析、対策情報等の作出・共有等を行う。

イ　「サプライチェーン分科会」の設置

〇概要：

各都道府県に「〇〇県（または都、道、府）サプライチェーン分科会」を設置する。事務局は各都道府県庁とする。各地域に「〇〇地域サプライチェーン分科会」を設置する。事務局は各地域の経済産業省経済産業局及び農林水産省農政局並びに国土交通省運輸局とする。国に「サプライチェーン分科会」を設置する。事務局は経済産業省及び農林水産省並びに国土交通省とする。

〇活動目的：

国、地方公共団体、サプライチェーン関連事業者、大学その他の研究機関のうち、我が国の経済安全保障の確保に資する一環として、サプライチェーンの多様化等に対応する意思を有する多様な主体が相互に連携して、サプライチェーンに関する施策の推進に関し必要な協議を行うこと。そのために主として、サプライチェーンの脅威情報等の共有・分析、対策情報等の作出・共有等を行う。

ウ　「技術流出等防止分科会」の設置

〇概要：

各都道府県に「技術流出等防止分科会」を設置する。事務局は各都道府県庁及び各都道府県警察とする。各地域に「〇〇地域技術流出等防止分科会」を設置する。事務局は各地域の経済産業省経済産業局及び公安調査庁公安調査局とする。国に「技術流出等防止分科会」を設置する。事務局は公安調査庁及び警察庁並びに経済産業省、文部科学省とする。

〇活動目的：

国、地方公共団体、企業や大学その他の研究機関のうち、我が国の経済安全保障の確保に資

する一環として、技術流出防止及び研究インテグリティの確保等に対応する意思を有する多様な主体が相互に連携して、研究インテグリティの確保及び技術流出防止に関する施策の推進に関し必要な協議を行うこと。そのために主として、技術流出及び研究インテグリティ等の脅威情報等の共有・分析、対策情報等の作出・共有等を行う。

図 67　分科会の例（サプライチェーン分科会）
出典：筆者作成

(2)　国に「経済安全保障協議会」の設置

前述した分科会の統括機関、そして経済安全保障に資する情報共有体制の横串的な機関として、国家安全保障局経済班を中心に経済安全保障協議会を設置する。経済安全保障施策は様々な省庁が跨るものであり、仮に一省庁に事務局を任せると、縦割り的な施策になる懸念がある。経済安全保障施策の統括部局として設置された国家安全保障局経済班を事務局として経済安全保障協議会を設置することで、縦割りを排した経済安全保障に資する情報共有体制を構築することが可能となる。

以下、概要について記す。

〇構成員：

事務局を国家安全保障局経済班とする。 構成員は、省庁等国家機関及び各分科会の第一

類構成員のなかで、特に情報共有や情報分析に資すると認められた事業者等から成る。

〇活動内容

・総会及び定例会の開催：年一回の総会において協議会規約等についての改定等を行う。また、月一回の定例会において、主に政府からの情報を共有し、全構成員の情報をアップデートする。

・情報共有活動（各分科会→事務局）：各分科会の事務局は、日々情報共有を行うなかで特に安全保障上重大だと思われることを経済班へ共有する。

・情報分析活動：協議会構成員は、経済班から共有された情報を分析する責務を負う。

・情報共有活動（事務局→構成員）：経済安全保障上特に重大な国内及び国外の情報を、構成員に共有する。共有された情報の共有可能範囲に応じて、構成員は各分科会の構成員に当該情報を共有する。

〇罰則の有無：各分科会と同等とする。

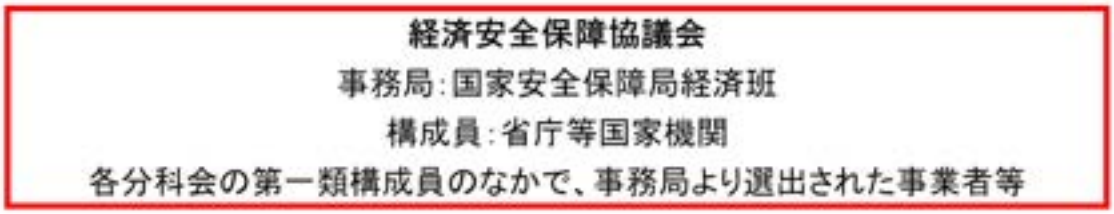


図 68　経済安全保障協議会の概要

出典：筆者作成

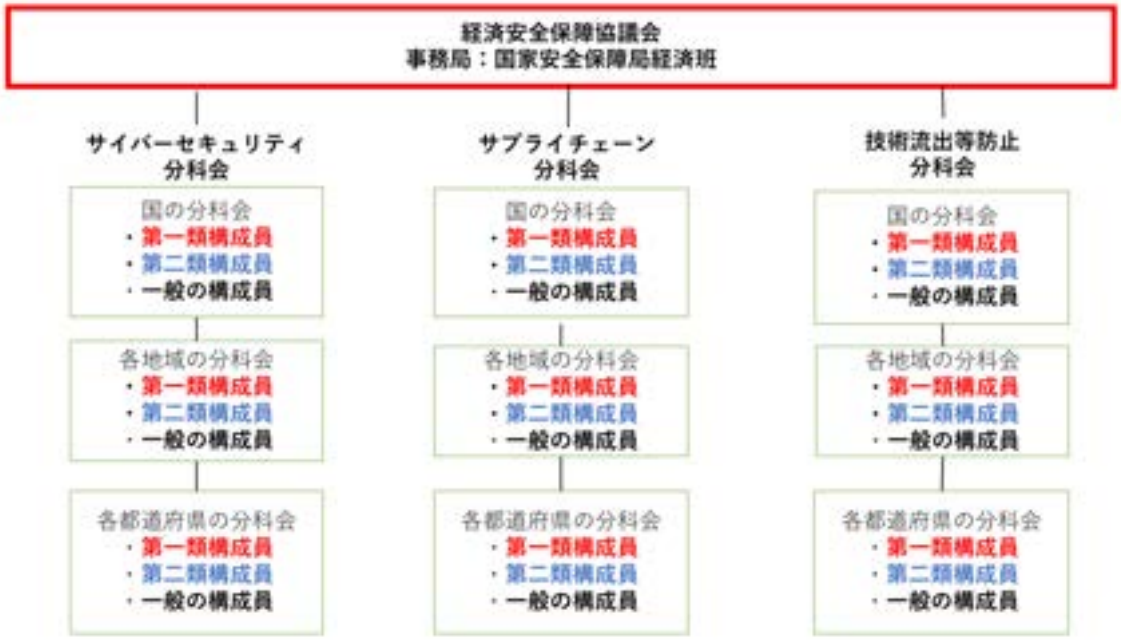


図 69　経済安全保障協議会及び分科会の概略図

出典：筆者作成

(3)　経済安全保障協議会を国家安全保障会議の諮問機関とする

国家安全保障会議の諮問機関として経済安全保障協議会を置くことを提言する。当協議会を諮問機関とすることで、協議会及び分科会で共有された情報が国家の意思決定機関まで共有されることとなり、その情報を基により実効的な経済安全保障施策を講じることが可能になると考える。

図 70　国家安全保障会議と諮問機関としての経済安全保障協議会の概略図
出典：筆者作成

(4)　経済安全保障推進法に「経済安全保障協議会及び分科会設置」を明記

最後に、経済安全保障推進法に「経済安全保障協議会及び分科会の設置」を明記することを提言する。法律に明記することで罰則を処すことが可能となる。また、政府が主導となって経済安全保障の情報共有体制を構築していくことを内外に示すことで、当協議会及び分科会を経済安全保障における重要施策として認識させ、事業者等の積極的な協力を得ることが期待できる。

以上、提言した経済安全保障協議会および分科会での情報共有活動を軸として、第 2 部の第 1 章、第 2 章、第 3 章で言及したサプライチェーンやサイバーセキュリティ、技術流出等防止のための政策を行っていく。すなわち、我が国全体の経済安全保障の確保に向けた素地が当協議会及び分科会を基に作られていくと考える。

おわりに

本研究においては、「我が国の経済安全保障の確保に向けた研究」というテーマの下、現在進行形の施策である経済安全保障について、サプライチェーン、サイバーセキュリティ、経済インテリジェンスの観点から政策提言を行った。

経済安全保障が政府やメディア等で取り上げられ始めた時期はつい最近のことであり、政策分野が多岐にわたるため、経済安全保障とは何かについて理解を深め、政策提言の方向性を定めることに苦労した。研究を進めるにあたっては、経済安全保障施策に精通している日本政府関係者や企業関係者、政治家や研究者、さらに外国政府関係者等に対するヒアリング調査を実施し、経済安全保障に対する理解を深め、問題の把握と課題の抽出に努めた。その中でも我々が問題意識を持ち、現行の経済安全保障施策と方向性が合致した 3 つの分野において政策提言を行った次第である。

本報告書では以上の分野から政策提言を行ってきたが、現段階において検討が及ばなかった課題が存在する。我々の研究を今後より発展させるための課題として、大きく以下の 2 点が挙げられると考える。

第一に、各国の政治的動向の検討である。経済安全保障施策は政治的動向と表裏一体であり、政治的動向の理解なしに経済安全保障の理解はできない。また、我が国が経済安全保障において国際連携を強化する際には、各国の政治的動向を把握し、価値観を共有する国々と協働していかなければならない。本ワークショップでは豪州研修を行ったものの、その他の国の政治的動向を検討し、政策提言に十分に反映することはできなかった。経済安全保障施策を実効的に講じるためにも、不断の検討が必要となるだろう。

第二に、国民の危機意識の醸成に関する検討である。経済安全保障と従来の安全保障との大きな差異は、政府だけではなく企業や大学といった我々の身近な機関がその主体となることだ。従って、国民全員が経済安全保障に対する理解を深め、国家全体として施策を講じていかなければならないだろう。最終報告会において、どのように国民の危機意識を醸成するべきかという質問があったことからも、当課題は経済安全保障施策の一つとして早急に検討する必要があるだろう。

本研究には、以上のような課題は残るものの、我々の提言が我が国の経済安全保障の確保に資することにつながればこれに勝る喜びはない。

謝辞

本報告書を作成するにあたって、我々の研究に他大なるご助力、ご指導をしていただいたすべての方々に、この場を借りて厚く御礼申し上げます。

主担当教員である坪原和洋教授には、実務家教員としての立場から、経済安全保障の基本的な考え方から政策立案における具体的な実務に至るまで、約 1 年間にわたって大変寛大なご指導をしていただきました。ここに深謝の意を表します。

副担当教員である阿南友亮教授及び西本健太郎教授には、我々の議論を温かく見守っていただき、研究の方向性やプレゼンテーションの構成など多くの点で、鋭いご指摘を賜りました。今西淳教授には、本学をお離れになった後もヒアリング調査先のご紹介等ご支援いただきました。石山英顕教授には、我々の豪州研修にご同行していただき、お力添えいただきました。深謝申し上げます。

本学修士 2 年の鈴木七夏海様、コーエンズ英理様には、先輩としての立場から、4 月初めのワークショップのご説明から豪州研修のサポートに至るまで、幅広くご助力をいただきました。深謝申し上げます。

鎌田様、後藤様をはじめとする専門職大学院係の皆様、そして斉藤様、白幡様をはじめとする総務企画係の皆様には、豪州研修含め 1 年間我々の研究活動に多大なるご支援をいただきました。深謝申し上げます。

さらに、ご多忙の中、貴重なお時間を割いて我々のヒアリング調査にご協力いただいた数多くの政府・研究機関・企業といった関係各位に感謝申し上げます。ヒアリング調査では、実務に携わる立場としての見地から、大学院での調査・議論だけでは得ることの叶わない非常に貴重かつ意義深いお話を伺うことができました。

また、ヒアリング調査時にご同席賜りました方々及び調査時に我々との窓口となってくださったご担当者の方々にも併せて深謝申し上げます。

最後に、我々の研究は、東北大学法学部教育研究基金による教育研究助成を受けて実施されました。加えて、豪州研修にあたっては、JR 東日本グローバル人材育成プログラム基金による旅費の支援を受けました。ここに記して深甚なる感謝の意を表します。

2023 年 1 月

参考文献

〈書籍〉

・IPA『情報セキュリティ白書 2022』（IPA、2022 年）

・Jared Mondschein, Victoria Cooper“ US MIDTERMS 2022 The stakes for Australia and the alliance”（ United States Studies Centre, 2022 年）

・セント・アンド・フォース『図解入門業界研究 最新半導体業界の動向とカラクリがよ～くわかる本[第 3 版]』（秀和システム、2021 年）

・フランシス・フクヤマ『歴史の終わり』（三笠書房、1992 年）

・加藤泰浩『太平洋のレアアース泥が日本を救う』(PHP 新書、2021 年)

・宮本雄二・伊集院敦・日本経済研究センター『米中分断の虚実』(日本経済新聞出版、2021 年)

・兼原信克『安全保障戦略』（日本経済新聞出版、2021 年）

・兼原信克『現実主義者のための安全保障のリアル』（ビジネス社、2021 年）

・高坂正堯『国際政治』（中央公論新社、2018 年）

・小林良樹『なぜ、インテリジェンスは必要なのか』（慶應義塾大学出版会、2021 年）

・西山孝『資源論』(丸善出版、2016 年)

・川上高司・監、樋口敬祐他・著『インテリジェンス用語辞典』（並木書房、2022 年）

・船橋洋一『地経学とは何か』(文藝春秋、2020 年)

・総務省『令和 4 年情報通信白書』（総務省、2022 年）

・太田泰彦『2030 半導体の地政学 戦略物資を支配するのは誰か』（日本経済新聞出版、2021 年)

・中谷和弘、河野桂子、黒﨑将広『サイバー攻撃の国際法（タリンマニュアル 2.0 の解説）』（信山社、2018 年）

・内閣官房内閣審議室分室・内閣総理大臣補佐官室『総合安全保障』（大蔵省印刷局、1980 年)

・福田一徳『日本と中国のレアアース政策』(木鐸社、2013 年)

・防衛大学校安全保障学研究会編・著、武田康裕、神谷万丈責任・編集『安全保障学入門（新訂第 5 版）』（亜紀書房、2018 年）

・北岡伸一・細谷雄一『新しい地政学』（東洋経済新報社、2020 年）

・北村滋『経済安全保障-異形の大国、中国を直視せよ』（中央公論新社、2022 年）

・北村滋『情報と国家』（中央公論新社、2021 年）

・村山編著『米中の経済安全保障戦略』（芙蓉書房出版、2021 年）

〈論文〉

・伊藤昭男「日中間レアアース問題の原因分析と日本の対応」『東アジア評論』第 3 号，2011 年 3 月

・角田昌太郎「サプライチェーンの安全保障―米中対立下の懸念と米国が主導する経済的連携

―」『変化する国際環境と総合安全保障 総合調査報告書』、2022 年 3 月
・向和歌奈「日本における経済安全保障への着目：安全保障分野としての台頭と課題」『アジア研究シリーズ』109, 2021 年
・神谷万丈「経済安全保障をめぐる諸論点」『安全保障研究』1 巻 1 号, 2019 年 1 月
・大庭三枝「「インド太平洋」の多様性:ASEAN からの視点」『インド太平洋地域の海洋安全保障と『法の支配』の実体化に向けて』, 2019 年 3 月
・中村直貴「経済安全保障－概念の再定義と一貫した政策体系の構築に向けて―」『立法と調査』428 巻, 2020 年 10 月
・田上靖「米国 FIRRMA（外国投資リスク審査現代化法）及びその改正下位規則の概要」『CISTEC JOURNAL』No186、2020 年 3 月
・樋口修「本調査の趣旨と報告書の構成」『変化する国際環境と総合安全保障 総合調査報告書』、2022 年 3 月
・鈴木一人「現代的経済安全保障の論点」『外交』88 巻, 2021 年 7 月

〈ウェブサイト〉
・(ISC)² “Cybersecurity Workforce Gap & Estimate” (2022 年 10 月)
〈https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx〉
・ACSC “Report Cyber、Report a cybercrime, incident or vulnerability.”
〈https://www.cyber.gov.au/acsc/report〉
・Argus “Japan aims to diversify rare earth supply,” (2023 年 1 月 3 日)
〈https://www.argusmedia.com/en/news/2405752-japan-aims-to-diversify-rare-earth-supply〉
・Argus “Lynas secures DoD funds for US heavy rare earth plant,” (2022 年 6 月 14 日)
〈https://www.argusmedia.com/en/news/2341111-lynas-secures-dod-funds-for-us-heavy-rare-earth-plant〉
・Australian Government Department of Industry, Science Energy and Resources, “2022 CRITICAL MINERALS STRATEGY” (2022 年 3 月)
〈https://www.industry.gov.au/sites/default/files/2022-09/2022-critical-minerals-strategy_0.pdf〉
・BBC「ロシア国営ガスプロム、EU への送ガス停止延長」(2022 年 9 月 3 日)
〈https://www.bbc.com/japanese/62776665〉
・BCG「世界の電動車（xEV)シェアは 2030 年に 51%へ。日本では 2030 年に 55%、ハイブリッド車が引き続きシェアを維持～BCG 調査」（2020 年 10 月）〈https://www.bcg.com/ja-jp/press/10january2020-electric-car〉
・CISTEC 事務局「米国による対中輸出規制の著しい強化について（改訂 2 版）」（2022 年 12 月 13 日）〈https://www.cistec.or.jp/service/uschina/52-20221011.pdf〉

・CISTEC 事務局「米国による対中輸出規制の著しい強化について（改訂 2 版）」（2022 年 12 月 13 日）〈https://www.cistec.or.jp/service/uschina/52-20221011.pdf〉
・Department of Foreign Affairs and Trade, “Australia’s International Cyber and Critical Tech Engagement Strategy”（2021 年 4 月）
〈https://www.internationalcybertech.gov.au/sites/default/files/2021-04/21045%20DFAT%20Cyber%20Affairs%20Strategy%20Internals_Acc_update_1_0.pdf〉
・European Commission, “A NEW EU-US AGENDA FOR GLOBAL CHANGE”（2020 年 12 月）
〈https://ec.europa.eu/commission/presscorner/detail/en/fs_20_2285〉
・European Commission, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Trade Policy Review - An Open, Sustainable and Assertive Trade Policy”（2021 年 2 月）
〈https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159438.pdf〉
・European Commission, “EU-US: A new transatlantic agenda for global change”（2020 年 12 月）〈https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2279〉
・Fraser Institute “Annual SURVEY OF MINING COMPANIES 2021,”（2022 年 4 月 12 日）
〈https://www.fraserinstitute.org/sites/default/files/annual-survey-of-mining-companies-2021.pdf〉
・Gary Clyde Hufbauer (PIIE), Euijin Jung (PIIE), “China plays the sanctions game, anticipating a bad US habit,”（2020 年 12 月 14 日）
〈https://www.piie.com/blogs/china-economic-watch/china-plays-sanctions-game-anticipating-bad-us-habit〉
・IISS “Cyber Capabilities and National Power: A Net Assessment”（2021 年 6 月 28 日）
〈https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power〉
・IISS “Cyber Power - Tier One”（2021 年 6 月 28 日）
〈https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one〉
・IISS “IISS, Cyber Power - Tier Three”（2021 年 6 月 28 日）
〈https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three〉
・IISS “IISS, Cyber Power - Tier Two”（2021 年 6 月 28 日）
〈https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two〉
・IPA「2021 年度中小企業における情報セキュリティ対策に関する実態調査－調査報告書－」（2022 年 3 月 31 日）〈https://www.ipa.go.jp/files/000097060.pdf〉
・IPA「SECURITY ACTION とは？」〈https://www.ipa.go.jp/security/security-action/sa/index.html〉
・IPA「コンピュータウイルス・不正アクセスに関する届出」（2022 年 10 月 27 日）

〈https://www.ipa.go.jp/security/outline/todokede-j.html#ransom〉
・IPA「中小企業が運営するECサイト向け無償脆弱性診断の募集」（2022年4月12日）
〈https://www.ipa.go.jp/security/vuln/ec-site/vuln-ec-site2022.html〉
・IPA「部門を知る」〈https://www.ipa.go.jp/shinsotsu/department.html〉
・JETRO「2021年度 海外進出日系企業実態調査アジア・オセアニア編-感染状況等により、在アジア日系企業の業績に差異も。 インド、中国で業績回復・拡大、ASEANでは回復弱く-」（2021年12月7日）
〈https://www.jetro.go.jp/ext_images/_Reports/01/6e5157e362606548/20210045.pdf〉
・JETRO「EU輸出品目規制：I.二重用途物品に関する規制　詳細」（2022年12月12日）
〈https://www.jetro.go.jp/ext_images/jfile/country/eu/trade_02/pdfs/eu_p11_2F010.pdf〉
・JETRO「「データセキュリティ法」の概要」（2021年12月）
〈https://www.jetro.go.jp/ext_images/_Reports/01/580a6448fa87f0bb/20210056_04.pdf〉
・JETRO「オーストラリア、最低賃金が世界主要国で最高額」（2019年7月24日）
〈https://www.jetro.go.jp/biznews/2019/07/e7d9171b27ade8fe.html〉
・JETRO「バイデン米政権、サプライチェーン強化策発表、エネルギーやICTなど6分野で」（2022年2月28日）〈https://www.jetro.go.jp/biznews/2022/02/4b787e74559f4268.html〉
・JETRO「バイデン米大統領、サイバーセキュリティを強化する大統領令に署名」（2021年05月14日）〈https://www.jetro.go.jp/biznews/2021/05/35e8aca1614f6fe5.html〉
・JETRO「経済安全保障、8割の日本企業が経営課題と認識」（2022年11月24日）
〈https://www.jetro.go.jp/biz/areareports/special/2022/1002/2c2eecd972c6c47e.html〉
・JETRO「最低賃金を7月から5.2%引き上げ」（2022年6月16日）
〈https://www.jetro.go.jp/biznews/2022/06/9f04bf8406970d9c.html〉
・JETRO「重要インフラ安全保障法の改正法が発効、外資審査の対象拡大」（2021年12月9日）〈https://www.jetro.go.jp/biznews/2021/12/bc10d9712d63af19.html〉
・JETRO「税関総署、3月1日から台湾産パイナップル輸入を暫時停止」（2021年3月3日）
〈https://www.jetro.go.jp/biznews/2021/03/9e86e9b7eeb3b346.html〉
・JETRO「続・厳格化する米国の輸出管理法令　留意点と対策」（2021年8月）
〈https://www.jetro.go.jp/ext_images/_Reports/01/e95620416cd2f8d3/20210031.pdf〉
・JETRO「中国のレアアース管理に関する政策の概要と動向」（2022年1月）
〈https://www.jetro.go.jp/ext_images/_Reports/01/6d50807a44f904c1/20210070_05.pdf〉
・JETRO「反外国制裁法の概要～中国の安全保障貿易管理に関する制度情報専門家による政策解説～」（2021年9月）
〈https://www.jetro.go.jp/ext_images/_Reports/01/2600bae53b7255f4/20210037_02.pdf〉
・JETRO「米連邦通信委、国家安全保障の脅威の機器・サービスにカスペルスキーや中国電信など3社を追加」（2022年3月29日）

〈https://www.jetro.go.jp/biznews/2022/03/9ba15d812e7eb629.html〉
・JIJI.COM「日米首脳、経済安保強化で合意へ G7 主導、中ロ念頭」（2023 年 1 月 11 日）
〈https://www.jiji.com/jc/article?k=2023011000833&g=pol〉
・JOGMEC「マレーシア：Lynas 社、Kuantan 選鉱施設における浸出精製残留物の永久処分施設が司法審査の対象に」（2022 年 9 月 5 日）
〈https://mric.jogmec.go.jp/news_flash/20220905/169663/〉
・JOGMEC「金属採掘等資金及び金属権利譲受け資金出資細則」（2010 年 7 月 1 日）
〈https://www.jogmec.go.jp/content/300113923.pdf〉
・JPCERT/CC「JPCERT/CC について」（2019 年 12 月 1 日）
〈https://www.jpcert.or.jp/about/〉
・JPCERT/CC「サイバー攻撃被害情報の共有と公表のあり方について（公開版）」（2021 年 3 月）〈https://www.soumu.go.jp/main_content/000762951.pdf〉
・JPCERT/CC「サイバー攻撃被害情報の共有と公表のあり方について（公開版）＜概要＞」（2021 年 3 月）〈https://www.soumu.go.jp/main_content/000762950.pdf〉
・JST「K Program とは」〈https://www.jst.go.jp/k-program/〉
・KDDI「2022 年 7 月 2 日に発生した通信障害について」（2022 年 7 月 29 日）
〈https://news.kddi.com/kddi/corporate/newsrelease/2022/07/29/6183.html〉
・MUFG「レアアース(希土類)の需給動向 と今後の展開可能性について」（2021 年 9 月 26 日）
〈https://www.cistec.or.jp/jaist/event/kenkyuutaikai/kenkyu32/02-01-shimizu.pdf〉
・NATIONAL ARCHIVES“Information Security Oversight Office (ISOO)”（2009 年 12 月 29 日）〈https://www.archives.gov/isoo/policy-documents/cnsi-eo.html〉
・NEDO「高性能磁石向けジスプロシウムの使用量 4 割削減に成功」（2010 年 12 月 27 日）
〈https://www.nedo.go.jp/news/press/ZZ_0515A.html〉
・NEDO「世界初、ジスプロシウム不使用の省ネオジム耐熱磁石を開発」（2018 年 2 月 20 日）
〈https://www.nedo.go.jp/news/press/AA5_100921.html〉
・NICT「サイバーセキュリティ研究会」〈https://www.nict.go.jp/csri/index.html〉
・NISC「サイバーセキュリティ協議会について（詳細版）」（2022 年 4 月 1 日）
〈https://www.nisc.go.jp/pdf/council/cs/kyogikai/kyogikai_gaiyou.pdf〉
・NISC「サイバーセキュリティ戦略」〈https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf〉
・NISC「重要インフラとは」〈https://www.nisc.go.jp/policy/group/infra/index.html〉
・NISC「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月 17 日）
〈https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf〉
・NRISECURE「NRI Secure Insight 2021」〈https://www.nri-secure.co.jp/hubfs/NRIS/download/ebook/NRISecure_Insight2021_Report.pdf〉
・NRI セキュアテクノロジーズ「NRI Secure Insight 2021」〈https://www.nri-

secure.co.jp/insight2021〉
・NTT「オフェンシブセキュリティへのアプローチ」（2021年1月12日）
〈https://www.bing.com/videos/search?q=%e3%82%aa%e3%83%95%e3%82%a7%e3%83%b3%e3%82%b7%e3%83%96%e3%82%bb%e3%82%ad%e3%83%a5%e3%83%aa%e3%83%86%e3%82%a3&&view=detail&mid=30F182455A79893ACDEF30F182455A79893ACDEF&&FORM=VDRVSR〉
・NTT技術ジャーナル〈https://journal.ntt.co.jp/article/1844〉
・Nikon「半導体露光装置」
〈https://www.jp.nikon.com/company/technology/product/semiconductor/〉
・Office of the United States Trade Representative, “U.S.-EU Trade and Technology Council Inaugural Joint Statement”（2021年9月）〈https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/september/us-eu-trade-and-technology-council-inaugural-joint-statement〉
・Parliament of Australia“Foreign Intelligence Legislation Amendment Bill 2021”
〈https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6748〉
・Proofpoint「身代金を支払うのは正解か？」（2021年07月05日）
〈https://www.proofpoint.com/jp/blog/threat-insight/is-it-right-to-pay-the-ransom〉
・Qiao-Chu Wang, et al., ““Illustrating the supply chain of dysprosium in China through material flow analysis,” *Resources, Conservation and Recycling*,”（2022年9月）〈https://www.sciencedirect.com/science/article/pii/S0921344922002610#bib0075,〉
・SC3「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とは」（2020年11月1日）〈https://www.ipa.go.jp/security/sc3/about/〉
・SUMCO「シリコンウェーハとは」〈https://www.sumcosi.com/ir/glance/wafer.html〉・Tech Insights“Tech Insights 2021 Top Semiconductor Equipment Suppliers”
〈https://www.techinsights.com/blog/2021-top-semiconductor-equipment-suppliers#:~:text=The%20top%20five%20suppliers%20accounted,the%20Top%2015%20last%20year〉
・The American Presidency Project“Executive Order 12968-Access to Classified Information”（1995年8月2日）
〈https://www.presidency.ucsb.edu/documents/executive-order-12968-access-classified-information〉
・The Senate and House of Representatives of the United States of America , “One Hundred Fifteenth Congress of the United States of America”, (2019年)
〈https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf〉
・The White House、Executive Order on Improving the Nation’s Cybersecurity〈Executive Order on Improving the Nation’s Cybersecurity | The White House〉

・Tobias Junne, et al.,“ Critical materials in global low-carbon energy scenarios: The case for neodymium, dysprosium, lithium, and cobalt,” *Energy*,” (2020 年 11 月 15 日)
〈https://www.sciencedirect.com/science/article/pii/S0360544220316406?via%3Dihub〉
・U.S. Department of Justice“This report is submitted in accordance with sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the Act)” (2022 年 4 月 29 日) 〈https://www.justice.gov/nsd/page/file/1498046/download〉
・U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, *2022 REPORT TO CONGRESS*, November 2022, 〈https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf〉
・US Department of Defense“*Department of Defense Cyber Strategy 2018 Summary*” (2018 年 9 月) 〈https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF〉
・White House“*NATIONAL SECURITY STRATEGY*” (2022 年 10 月)
〈https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf〉
・informa tech「令和元年度安全保障貿易管理対策事業（電子機器製造の産業基盤実態等調査）」 (2020 年 3 月) 〈https://www.meti.go.jp/meti_lib/report/2019FY/000182.pdf〉
・オーストラリア連邦議会 “Foreign Intelligence Legislation Amendment Bill 2021”
〈https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6748〉
・サイバーセキュリティ戦略本部「サイバーセキュリティ 2022」 (2022 年 6 月 17 日)
〈https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf〉
・デロイト トーマツ コンサルティング合同会社「北米におけるレアアースのサプライチェーン状況分析業務　最終報告書」 (2020 年 2 月 28 日)
〈https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjJlrjHydr8AhU3sVYBHX3aAGsQFnoECBoQAQ&url=https%3A%2F%2Fmric.jogmec.go.jp%2Fwp-content%2Fuploads%2F2020%2F05%2Free_supply_northamerica20200228.pdf&usg=AOvVaw1C4uTFPqwocZOsobSualb4〉
・フィッシング対策協議会「フィッシングレポート 2022」
〈https://www.antiphishing.jp/report/phishing_report_2022.pdf〉
・安全保障貿易情報センター「輸出管理の基礎」
〈https://www.cistec.or.jp/export/yukan_kiso/anpo_gaiyou/index.html〉
・外務省「2021 年開かれた社会声明」 〈https://www.mofa.go.jp/files/100200087.pdf〉
・外務省「G7 首脳コミュニケ」 (2022 年 6 月 28 日)
〈https://www.mofa.go.jp/mofaj/files/100376624.pdf〉

・外務省「Ｇ７カービスベイ首脳コミュニケ　より良い回復のためのグローバルな行動に向けた我々の共通のアジェンダ」〈https://www.mofa.go.jp/mofaj/files/100200083.pdf〉
・外務省「サイバー・イニシアチブ東京 2022 山田外務副大臣スピーチ原稿」（2022 年 12 月 7 日）〈https://www.mofa.go.jp/mofaj/files/100431283.pdf〉
・外務省「サイバーセキュリティ」（2022 年 12 月 7 日）
〈https://www.mofa.go.jp/mofaj/annai/page5_000250.html〉
・外務省「ファクト・シート：日米競争力・強靭性パートナーシップ」（2022 年 5 月 23 日）
〈https://www.mofa.go.jp/mofaj/files/100347258.pdf〉
・外務省「安全保障協力に関する日豪共同宣言」（2022 年 10 月 22 日）
〈https://www.mofa.go.jp/mofaj/files/100410297.pdf〉
・外務省「鉱物安全保障パートナーシップ（MSP）概要」（2022 年）
〈https://www.mofa.go.jp/mofaj/files/100431183.pdf〉
・外務省「重要技術サプライチェーンに関する原則の共通声明（仮訳）」（2021 年 3 月 12 日）〈https://www.mofa.go.jp/mofaj/files/100347897.pdf〉
・外務省「日豪首脳共同声明」（2022 年 10 月 22 日）
〈https://www.mofa.go.jp/mofaj/files/100410295.pdf〉
・外務省「日米経済政策協議委員会 2022 年行動計画」（2022 年 7 月 29 日）
〈https://www.mofa.go.jp/mofaj/files/100376269.pdf〉
・外務省「日米経済政策協議委員会共同声明 経済安全保障とルールに基づく秩序の強化（仮訳）」（2022 年 7 月 29 日）〈https://www.mofa.go.jp/mofaj/files/100376269.pdf〉
・外務省「日米豪印首脳会合」（2022 年 5 月 24 日）
〈https://www.mofa.go.jp/mofaj/fp/nsp/page1_001186.html〉
・外務省「日米豪印首脳会合共同声明」（2022 年 5 月 24 日）
〈https://www.mofa.go.jp/mofaj/fp/nsp/page1_001188.html〉
・外務省「日米首脳共同声明『自由で開かれた国際秩序の強化』」（2022 年 5 月 23 日）
〈https://www.mofa.go.jp/mofaj/files/100347254.pdf〉
・株式会社　相模化学金属「ネオジム磁石の特徴」〈https://www.sagami-magnet.co.jp/explanation-magnet/feature-neodymium〉
・株式会社エイジアム研究所「平成 29 年度製造基盤技術実態等調査（中国製造業の実態を踏まえた我が国製造業の産業競争力調査)」（2018 年 3 月 30 日）
〈https://www.meti.go.jp/meti_lib/report/H29FY/000403.pdf〉
・関東経済産業局「技術流出防止管理説明会」（2022 年 9 月 22 日）
〈https://www.kanto.meti.go.jp/seisaku/boeki/keizaianpo_seminar.html〉
・久野新「中国の経済制裁：その特徴と有効性」（2021 年 4 月 20 日）
〈https://www.jfir.or.jp/wp/wp-content/uploads/2021/04/210420Kunoa.pdf〉
・宮城県警察「宮城県サイバーセキュリティ協議会」（2019 年 5 月 1 日）

〈https://www.police.pref.miyagi.jp/cyber/kyougikai.html〉
・経済産業省「認定特定半導体生産施設整備等計画」
〈https://www.meti.go.jp/policy/mono_info_service/joho/laws/semiconductor/semiconductor_plan.html〉
・経済産業省・IPA「情報セキュリティ経営ガイドライン Ver2.0」
〈https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf〉
・経済産業省「IT 人材の育成」
〈https://www.meti.go.jp/policy/it_policy/jinzai/index.html〉
・経済産業省「『みなし輸出』管理の明確化について」（2021 年 11 月）
〈https://www.meti.go.jp/policy/anpo/law_document/minashi/jp_kigyou.pdf〉
・経済産業省「オーストラリア、インド、日本の貿易大臣によるサプライチェーン強靭化イニシアティブに関する共同声明（仮訳）」（2021 年 4 月）
〈https://www.meti.go.jp/press/2021/04/20210427004/20210427004-2.pdf〉
・経済産業省「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性」（2022 年 7 月）
〈https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/007_03_00.pdf〉
・経済産業省「サプライチェーンデータ共有・連携 WG 第 1 回 事務局資料」（2022 年 10 月）
〈https://www.meti.go.jp/shingikai/external_economy/global_supply_chain/supply_chain_data/pdf/001_05_00.pdf〉
・経済産業省「レアメタル備蓄制度の見直しについて」（2020 年 7 月）
〈https://www.meti.go.jp/shingikai/enecho/shigen_nenryo/pdf/029_05_02.pdf〉
・経済産業省「経済安全保障に関する国際情勢や日本の対応」（2022 年 9 月）
〈https://www.kanto.meti.go.jp/seisaku/boeki/data/1-1gijyutu_keizai_2022.pdf〉
・経済産業省「参考資料　各国の電動化目標」
〈https://www.meti.go.jp/shingikai/mono_info_service/mobility_kozo_henka/pdf/004_03_00.pdf〉
・経済産業省「次世代半導体の設計・製造基盤確立に向けて」（2022 年 11 月）
〈https://www.meti.go.jp/press/2022/11/20221111004/20221111004-1.pdf〉
・経済産業省「情報セキュリティサービス基準 第 2 版」（2022 年 1 月 31 日）
〈https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun2.pdf〉
・経済産業省「新型コロナウイルスの感染拡大を踏まえた資源・燃料政策の今後の方向性」（2020 年 7 月 1 日）
〈https://www.meti.go.jp/shingikai/enecho/shigen_nenryo/pdf/029_03_00.pdf〉
・経済産業省「西村経済産業大臣がインド太平洋経済枠組み（IPEF）閣僚会合に出席しました」（2022 年 9 月 13 日）

〈https://www.meti.go.jp/press/2022/09/20220913006/20220913006.html〉
・経済産業省「地域 SECUNITY リスト」（2022 年 5 月）
〈https://www.meti.go.jp/policy/netsecurity/comunitylist.pdf〉
・経済産業省「通商白書 2020」（2020 年 7 月）
〈https://www.meti.go.jp/report/tsuhaku2020/pdf/02-02-02.pdf〉
・経済産業省「通商白書 2022」（2022 年 6 月）
〈https://www.meti.go.jp/report/tsuhaku2022/pdf/2022_zentai.pdf〉
・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律（特定半導体生産施設整備等関係）」（2022 年 3 月 1 日）
〈https://www.meti.go.jp/policy/mono_info_service/joho/laws/semiconductor.html〉
・経済産業省「日 EU デジタルパートナーシップが立ち上げられました」（2022 年 5 月 12 日）
〈https://www.meti.go.jp/press/2022/05/20220512005/20220512005.html〉
・経済産業省「萩生田経済産業大臣が米国に出張しました」（2022 年 5 月 6 日）
〈https://www.meti.go.jp/press/2022/05/20220506002/20220506002.html〉
・経済産業省「半導体・デジタル産業戦略」（2021 年 6 月）
〈https://www.meti.go.jp/policy/mono_info_service/joho/conference/semicon_digital/20210603008-1.pdf〉
・経済産業省「半導体協力基本原則（仮訳）」（2022 年 5 月 4 日）
〈https://www.meti.go.jp/press/2022/05/20220506002/20220506002-4.pdf〉
・経済産業省「半導体戦略（概略）」（2021 年 6 月）
〈https://www.meti.go.jp/press/2021/06/20210604008/20210603008-4.pdf〉
・経済産業省「繁栄のためのインド太平洋経済枠組み 柱２ 閣僚声明」（2021 年 9 月）
〈https://www.meti.go.jp/press/2022/09/20220913006/20220913006-14.pdf〉
・経済産業省「付属書：最初の共同行動」『（仮訳）日 EU デジタルパートナーシップ』（2022 年 5 月 12 日）
〈https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/b530adc8-3af1-4d9f-af84-6f21af4067af/5c1b4399/20220512_news_digital_group_japanese_03.pdf〉
・経済産業省「令和 3 年度補正「産業技術実用化開発事業費補助金（サプライチェーン上不可欠性の高い半導体の生産設備の脱炭素化・刷新事業費補助金）」に係る補助事業者募集要領」（2021 年 12 月 21 日）
〈https://www.meti.go.jp/information/publicoffer/kobo/2021/downloadfiles/k211221001_01.pdf〉
・経済産業省「令和 4 年度補正予算の事業概要（PR 資料）」（2022 年 12 月）
〈https://www.meti.go.jp/main/yosan/yosan_fy2022/hosei/pdf/pr_hosei_221202.pdf〉
・経済産業省資源エネルギー庁「世界の産業を支える鉱物資源について知ろう」（2018 年 3 月

22 日）
〈https://www.enecho.meti.go.jp/about/special/tokushu/anzenhosho/koubutsusigen.html〉
・経済産業省貿易経済協力局国際投資管理室「対内直接投資審査制度について」
〈https://www.kanto.meti.go.jp/seisaku/boeki/data/1-2gijyutu_toushi_2022.pdf〉
・警察庁「技術流出の防止に向けて」（2022 年 8 月 1 日）
〈https://www.npa.go.jp/bureau/security/economic-security/index.html〉
・警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について」
〈https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf〉
・警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2022 年 9 月 15 日）
〈https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf〉
・個人情報保護委員会「漏えい等報告・本人への通知の義務化について」
〈https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/〉
・公安調査庁「サイバー空間における脅威の概要 2022」
〈https://www.moj.go.jp/content/001371280.pdf〉
・公安調査庁「サイバー空間における脅威の状況」（2022 年）
〈https://www.moj.go.jp/content/001371280.pdf〉
・公安調査庁「経済安全保障に関するご相談・講演依頼等窓口」（2021 年 4 月）
〈https://www.moj.go.jp/psia/kouan_mail_keizaianpo.html〉
・公安調査庁「経済安全保障の確保に向けて 2022」（2022 年 5 月）
〈https://www.moj.go.jp/content/001373771.pdf〉
・公安調査庁「経済安全保障特集ページ」（2022 年 6 月）
〈https://www.moj.go.jp/psia/keizaianpo.top.html〉
・公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」（2022 年 10 月 28 日）
〈https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html#:~:text=%E5%8F%96%E5%BC%95%E4%B8%8A%E3%81%AE%E5%9C%B0%E4%BD%8D%E3%81%8C,%E6%B3%95%E4%B8%8A%E5%95%8F%E9%A1%8C%E3%81%A8%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82〉
・豪州政府“Surveillance Legislation Amendment (Identify and Disrupt) Act 2021”
〈https://www.legislation.gov.au/Details/C2021A00098〉
・豪州政府“TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979”
〈http://classic.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/〉
・国立感染症研究所「IDWR 2020 年第 21 号＜注目すべき感染症＞ 新型コロナウイルス感染症（COVID-19）」〈https://www.niid.go.jp/niid/ja/2019-ncov/2487-idsc/idwr-topic/9669-

idwrc-2021.html〉
・国立研究開発法人 新エネルギー・産業技術総合開発機構 技術戦略研究センター（TSC）「TSC トレンド　グローバルな半導体競争～エコシステム確保をかけて～」（2021 年 4 月）〈https://www.nedo.go.jp/content/100931733.pdf〉
・国立研究開発法人 新エネルギー・産業技術総合開発機構「ポスト 5G 情報通信システム基盤強化研究開発事業」（2019 年）〈https://www.nedo.go.jp/activities/ZZJP_100172.html〉
・国立研究開発法人　科学技術振興機構「経済安全保障重要技術育成プログラム WEB サイト」（2022 年 12 月 5 日）〈https://www.jst.go.jp/k-program/〉
・国立国会図書館「【オーストラリア】1979 年電気通信（傍受及びアクセス）法の改正」（2022 年 1 月）
〈https://dl.ndl.go.jp/view/download/digidepo_11976514_po_02900113.pdf?contentNo=1〉
・国立国会図書館「米国自由法―米国における通信監視活動と人権への配慮― 」（2016 年 03 月 01 日）
〈https://dl.ndl.go.jp/view/download/digidepo_9914660_po_02670003.pdf?contentNo=1〉
・財務省「対内直接投資審査制度について」（2021 年 11 月）
〈https://www.mof.go.jp/about_mof/councils/customs_foreign_exchange/sub-foreign_exchange/proceedings/material/gai20211116_5.pdf〉
・笹井秀起「2021 年 Biden 政権成立後の米国レアアース関連動向」（2022 年 1 月 25 日）
〈https://mric.jogmec.go.jp/reports/mr/20220125/165301/〉
・三浦惇平、近藤郷平「トヨタ、全工場停止へ 取引先にサイバー攻撃か」『朝日新聞』（2022 年 3 月 1 日）
〈https://digital.asahi.com/articles/DA3S15218897.html?iref=pc_ss_date_article〉
・三菱 UFJ リサーチ&コンサルティング「原材料の戦略的な確保を図る EU ～欧州原材料同盟（ERMA）構想の特徴と問題点 」（2021 年 8 月 31 日）〈https://www.murc.jp/wp-content/uploads/2021/08/report_210831.pdf〉
・三菱電機株式会社「不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）」（2020 年 2 月 12 月）〈https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf〉
・参議院「第 193 回国会（常会）　答弁書　答弁書第 47 号」
〈https://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/193/touh/t193047.htm〉
・参議院「第 208 回国会　参議院　内閣委員会　第 5 号　令和 4 年 3 月 29 日、政府参考人 股野元貞氏の答弁」（2022 年 3 月 29 日）
〈https://kokkai.ndl.go.jp/simple/detail?minId=120814889X00520220329&spkNum=0#s0〉
・参議院「第 208 回国会　参議院　内閣委員会　第 5 号　令和 4 年 3 月 29 日、政府参考人 小島裕史氏の答弁」
〈https://kokkai.ndl.go.jp/simple/detail?minId=120814889X00520220329&spkNum=0#s0〉

・自由民主党政務調査会新国際秩序戦略本部「提言「経済安全保障戦略の策定に向けて」」（2020 年 12 月 16 日）〈https://storage.jimin.jp/pdf/news/policy/201021_1.pdf〉
・篠原武史、奥田達志、中島上智「マクロ経済に関する不確実性指標の特性について」（2020 年 10 月）〈https://www.boj.or.jp/research/wps_rev/wps_2020/data/wp20j07.pdf〉
・首相官邸 “Partnership between Japan’s Ministry of Economy, Trade and Industry and Australia’s Department of Industry, Science and Resources and Department of Foreign Affairs and Trade Concerning Critical Minerals”（2022 年 10 月 22 日）〈https://japan.kantei.go.jp/101_kishida/documents/2022/_00019.html〉
・首相官邸「３つの密を避けましょう」〈https://www.kantei.go.jp/jp/content/000061868.pdf〉
・首相官邸「第 205 回国会における岸田内閣総理大臣所信表明演説」（2021 年 10 月 8 日）〈https://www.kantei.go.jp/jp/100_kishida/statement/2021/1008shoshinhyomei.html〉
・首相官邸「第 208 回国会における岸田内閣総理大臣施政方針演説」（2022 年 1 月 17 日）〈https://www.kantei.go.jp/jp/101_kishida/statement/2022/0117shiseihoshin.html〉
・松原実穂子「新潮社フォーサイト、波紋を広げる「アクティブ・ディフェンス」解釈論争とサイバー攻撃者の暗殺」（2021 年 10 月 8 日）〈https://www.fsight.jp/articles/-/48319〉
・情報処理推進機構「セキュリティ・キャンプ」〈https://www.ipa.go.jp/jinzai/camp/index.html〉
・双日、JOGMEC「豪州ライナス社への追加出資について」（2022 年 9 月 20 日）〈https://www.sojitz.com/jp/news/2022/09/20220920.php〉
・総務省「諸外国のサイバーセキュリティ政策について」〈https://www.google.com/url?client=internal-element-cse&cx=017998645568075274792:lrqatnruwxq&q=https://www.soumu.go.jp/main_content/000488150.pdf&sa=U&ved=2ahUKEwjJ-rbWsrr8AhVKmFYBHa07CTgQFnoECAMQAQ&usg=AOvVaw11AI1X9n-fYxc92Rwnz16p〉
・朝日新聞「（時時刻刻）規制・支援、見えぬ全容　経済安保法」（2022 年 5 月 12 日）〈https://www.asahi.com/articles/DA3S15291154.html〉
・渡辺寧「レアアースから見た鉱物資源供給の将来像」（2018 年 8 月）〈https://www.jstage.jst.go.jp/article/shigenchishitsu/66/1/66_27/_pdf〉
・東北経済産業局「東北地域サイバーセキュリティ連絡会の概要」（2021 年 11 月 8 日）〈https://www.tohoku.meti.go.jp/s_joho/topics/pdf/cyber_security_gaiyo.pdf〉
・藤谷昌敏「なぜ我が国に本格的な情報機関が生まれなかったのか」『日本戦略研究フォーラム』〈https://www.jfss.gr.jp/article/1532〉
・読売新聞オンライン「【独自】留学生のビザの審査厳格化へ...中国念頭、安保技術を流出防止」（2020 円 10 月 5 日）〈https://www.yomiuri.co.jp/politics/20201005-OYT1T50013/〉
・読売新聞オンライン「中国軍が「台湾封鎖」大規模演習開始…弾道ミサイル１１発発射、５

発が日本ＥＥＺ内に落下」（2022 年 8 月 4 日）
〈https://www.yomiuri.co.jp/world/20220804-OYT1T50208/〉
・読売新聞オンライン「中台統一へ習氏「武力行使を決して放棄しない」…共産党大会開幕」（2022 年 10 月 17 日）〈https://www.yomiuri.co.jp/world/20221017-OYT1T50007/〉
・内閣官房「経済安全保障法制に関する有識者会議」
〈https://www.cas.go.jp/jp/siryou/131217anzenhoshou/gaiyou.html〉
・内閣官房「経済安全保障法制に関する有識者会議」
〈https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/4index.html〉
・内閣官房「経済安全保障の推進に向けて」（2021 年 11 月 19 日）
〈https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai1/shiryou3.pdf〉
・内閣官房「経済安全保障法制に関する有識者会議」（2021 年 11 月 26 日）
〈https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai1/siryou3.pdf〉
・内閣官房「国家安全保障戦略（概要）」（2022 年 12 月 16 日）
〈https://www.cas.go.jp/jp/siryou/131217anzenhoshou/gaiyou.html〉
・内閣官房「国家安全保障戦略」（2022 年 12 月 16 日）
〈https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf〉
・内閣官房「国家防衛戦略」（2022 年 12 月）
〈https://www.cas.go.jp/jp/siryou/221216anzenhoshou/boueisenryaki.pdf〉
・内閣官房「成長戦略実行計画」（2021 年 6 月 18 日）
〈https://www.cas.go.jp/jp/seisaku/seicho/pdf/ap2021.pdf〉
・内閣官房「特定重要物資の指定について」（2022 年 11 月）
〈https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai4/siryou1.pdf〉
・内閣官房「平和安全法制等の整備について」
〈https://www.cas.go.jp/jp/gaiyou/jimu/housei_seibi.html〉
・内閣府「経済安全保障法制に関する有識者会議 サプライチェーン強靭化に関する検討会合第 1 回資料」（2021 年 12 月 8 日）
〈https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou1.pdf〉
・内閣府「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 第一回資料」（2021 年 12 月 10 日）
〈https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/dai2/siryou4.pdf〉
・内閣府「統合イノベーション戦略 2020」（2020 年 1 月 21 日）
〈https://www8.cao.go.jp/cstp/togo2020_honbun.pdf〉
・内閣府「「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セキュリティ技術の確立」に関する研究開発構想（個別研究型）」（2022 年 10 月）
〈https://www8.cao.go.jp/cstp/anzen_anshin/20221021_mext_3.pdf〉
・内閣府「経済安全保障重要技術育成プログラム」（2022 年 12 月 5 日）

〈https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html〉
・内閣府「経済安全保障推進法の概要」（2022 年 5 月）
〈https://www.cao.go.jp/keizai_anzen_hosho/doc/gaiyo.pdf〉
・内閣府「経済安全保障推進法上の特定重要技術調査研究機関としても期待される安全・安心シンクタンクの役割」（2022 年 11 月 29 日）
〈https://www8.cao.go.jp/cstp/anzen_anshin/thinktank/1kai/sanko2.pdf〉
・内閣府「経済財政運営と改革の基本方針 2021」（2021 年 6 月 18 日）
〈https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2021/2021_basicpolicies_ja.pdf〉
・内閣府「経済財政運営と改革の基本方針 2022」（2022 年 6 月 7 日）
〈https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2022/2022_basicpolicies_ja.pdf〉
・内閣府「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基本的な方針」（2022 年 9 月 30 日）
〈https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonhoushin.pdf〉
・内閣府「研究インテグリティの確保に係る対応方針（概要）」（2022 年 9 月 1 日）
〈https://www8.cao.go.jp/cstp/kokusaiteki/integrity/gaiyo_202209.pdf〉
・内閣府「個人データの漏えい等の事案が発生した場合等の対応について」
〈https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf〉
・内閣府「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に関する基本指針」（2022 年 9 月 30 日）
〈https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin3.pdf〉
・内閣府「特定重要物資の安定的な供給の確保に関する基本指針」（2022 年 9 月 30 日）
〈https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin1.pdf〉
・内閣府「特定重要物資の指定について」（2022 年 11 月）
〈https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai4/siryou1.pdf〉
・日刊工業新聞「社説/半導体の安定供給　「チップ 4」構想の行方を注視」（2022 年 8 月 1 日）〈https://www.nikkan.co.jp/articles/view/00644117〉
・日経 XTECH「三菱電機にサイバー攻撃、防衛情報が流出」（2020 年 2 月 28 日）
〈https://xtech.nikkei.com/atcl/nxt/mag/nmc/18/00016/00020/〉
・日経 XTECH「水道施設に「毒混入」狙ったサイバー攻撃、お粗末すぎるセキュリティーの恐怖」（2021 年 2 月 24 日）
〈https://xtech.nikkei.com/atcl/nxt/column/18/00676/021700072/〉
・日本経済新聞「WTO、危機下で分断鮮明　閣僚会議開幕　ウクライナ連帯、加盟国 3 分の 1 どまり　物流や食料など利害対立」（2022 年 6 月 14 日）
〈https://www.nikkei.com/article/DGKKZO61679070T10C22A6EP0000/〉
・日本経済新聞「イージス艦情報漏洩、元自衛官の有罪確定へ」（2011 年 3 月 3 日）
〈https://www.nikkei.com/article/DGXNASDG03017_T00C11A3CR0000/〉

・日本経済新聞「ウクライナが問うサイバー防衛（下）」（2022 年 9 月 9 日）
〈https://www.nikkei.com/article/DGXZQODK2282N0S2A820C2000000/?type=my〉
・日本経済新聞「ウクライナが問うサイバー防衛（上）」（2022 年 9 月 8 日）
〈https://www.nikkei.com/article/DGXZQODK2282N0S2A820C2000000/〉
・日本経済新聞「サイバーセキュリティ人材育成「アジア共通資格めざす」」（2021 年 12 月 21 日）〈https://www.nikkei.com/article/DGXZQOUC08ARV0Y1A201C2000000/〉
・日本経済新聞「ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃」（2021 年 11 月 12 日）〈https://www.nikkei.com/article/DGXZQOUE071OK0X01C21A1000000/〉
・日本経済新聞「契約書も「サイバー防衛」　免責や賠償上限定め紛争予防」（2022 年 10 月 15 日）〈https://www.nikkei.com/article/DGXZQOUC227RQ0S2A920C2000000/〉
・日本経済新聞「経済安保、省庁 100 人超職員 技術流出防止や外為審査 来年度、別枠で確保」（2021 年 9 月 12 日）
〈https://www.nikkei.com/article/DGKKZO75684760S1A910C2EA3000/〉
・日本経済新聞「身代金ウイルス、警察庁が暗号解除成功　支払い未然防止」（2022 年 12 月 28 日）
〈https://www.nikkei.com/article/DGXZQOUE062930W2A201C2000000/?type=my#RQAUAgAAMjAyMTA5MjYyMTExMDg2MzU3NTE2MTQ〉
・日本経済新聞「大企業のサイバー対策、4 割に危険性、車や機械目立つ」（2022 年 6 月 5 日）
〈https://www.nikkei.com/article/DGXZQOUC15C8V0V10C22A4000000/?type=my#RQAUAgAAMjAyMTA5MjYyMTExMDg2MzU3NTE2MTQ〉
・文部科学省「研究インテグリティ」（2021 年）
〈https://www.mext.go.jp/a_menu/kagaku/integrity/index.html〉
・法務省「犯罪捜査のための通信傍受に関する法律案Ｑ＆Ａ」
〈https://www.moj.go.jp/houan1/houan_soshikiho_qanda_qanda.html〉
・防衛省・自衛隊〈https://www.mod.go.jp/j/press/news/2022/04/19e.html〉
・防衛省「令和 3 年版防衛白書」（2021 年）
〈http://www.clearing.mod.go.jp/hakusho_data/2021/pdf/R03010202.pdf〉
・鈴木早苗「ASEAN のインド太平洋方針と日中の対応」（2021 年 3 月 12 日）
〈https://www.jiia.or.jp/research-report/post-58.html〉
・和田喜彦「レアアース製錬に伴うトリウム等の放射性廃棄物管理に関する一考察 : エィジアンレアアース(ARE)社事件，ライナス社問題を事例として」（2014 年 3 月 20 日）
〈https://doshisha.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=27419&item_no=1&page_id=13&block_id=100〉

提言一覧

1.サプライチェーン分野での政策提言
提言 1:　HREEs Security Partnership の創設
提言 2:　HREEs Security Partnership のための国際連携
提言 3:　HREEs Security Partnership のための国内政策
提言 4:　「先端技術競争協定」の締結
提言 5:　日本が強みを持つ分野のコア業種への指定
提言 6:　レガシー半導体の生産能力の向上
2.サイバーセキュリティ分野での政策提言
提言 7:　サイバー攻撃を未然に防止するための調査を可能にする立法措置
提言 8:　重要インフラ事業者等に対する特別サイバーセキュリティ監査
提言 9:　情報収集・ペネトレーション検査用ＡＩロボットの開発・運用等
提言 10:　アトリビューション・ワクチン機能に資するソフトウェアの開発
提言 11:　経済安全保障に関係する中小企業向けサイバーセキュリティ認定制度の創設
提言 12:　中小企業サイバー攻撃被害報告義務と援助制度の創設
提言 13:　経済安全保障に関係する中小企業向けサイバーインシデント登録・分析機関の設置
提言 14:　サイバーセキュリティ投資税制
提言 15:　サイバーセキュリティ研究開発税制
提言 16:　サイバー人材育成奨学金制度
3.経済インテリジェンス分野での政策提言
提言 17:　セキュリティ・クリアランス制度の導入
提言 18:　先端技術ＣＩ（Counter Intelligence）ネットワークの設立
提言 19:　情報セキュリティ強化支援の設立
提言 20:　大学における領域横断部門の経済安全保障プログラムの創設
提言 21:　国家公務員試験に経済安全保障専門試験の導入
提言 22:　経済安全保障専門人材育成制度の試験的導入
提言 23:　国・地域・各都道府県に「分科会」の設置
提言 24:　国に「経済安全保障協議会」の設置
提言 25:　経済安全保障協議会を国家安全保障会議の諮問機関とする
提言 26:　経済安全保障推進法に「経済安全保障協議会及び分科会設置」を明記

年表

西暦	経済安全保障に係る主な出来事
1973.12	第一次オイルショック、第四次中東戦争を機に原油価格が高騰
1978.10	第二次オイルショック、イラン革命を機に原油価格が高騰
1982.12	東芝機械ココム違反事件、ココム違反を知りながら工作機械をソ連に輸出
1985.9	プラザ合意、急速な円高の進行
1986.2	日米半導体協定、日本の半導体産業が衰退へ
1989.11	ベルリンの壁崩壊、東西冷戦終結
1995.1	WTO 設立
2001.9	アメリカ同時多発テロ事件、アフガニスタンにおける軍事行動
2001.12	中国が WTO 加盟
2010.9	尖閣諸島沖で中国漁船が海上保安庁巡視船に体当たり、船長を逮捕
2010.11	マルウェア「Stuxnet」によるイラン核関連施設攻撃、 遠心分離機が稼働不能に
2011.1	タイ大洪水、日系企業の工場も水没しサプライチェーンが混乱
2014.2	ロシアがウクライナ領クリミア半島へ軍事介入、 ロシアはクリミア半島を併合
2015.5	日本年金機構、不正アクセスによる個人情報流出
2016.2	日本、米国を含む１２か国がＴＰＰ協定に署名
2016.11	ロシアによる米国大統領選挙の干渉
2017.1	トランプ大統領就任、自国優先主義を表明
2017.1	米国トランプ大統領、TPP 離脱を決定
2017.5	ランサムウェア「WannaCry」事案、身代金要求により世界中で大きな被害
2020.1	中国を起源とする COVID-19 が流行
2020.4	国家安全保障局内（NSS）内に「経済班」設置
2020.6	改正外為法施行、国の安全等を損なうおそれがある投資の制限
2020.9	米国は華為技術（ファーウェイ）に対する輸出規制を発効
2021.5	アメリカ最大手のパイプライン社がランサムウェア被害
2021.1	徳島県のつるぎ町立半田病院のランサムウェア被害
2021.4	宇宙航空研究開発機構（JAXA）へのサイバー攻撃
2021.6	重要土地利用規制法成立
2021.10	岸田内閣が経済安全保障担当閣僚を新設
2021.11	政府が経済安全保障有識者会議を設置
2022.2	ロシアによるウクライナ侵略戦争

2022.3	トヨタ自動車の取引先企業がランサムウェア被害、トヨタの全工場が稼働停止
2022.3	ロシアの特定の銀行を「SWIFT」から締め出し
2022.5	外為法の「みなし輸出」管理の明確化
2022.5	経済安全保障推進法が可決、成立
2022.5	日米豪印(QUAD)首脳会合を東京で開催
2022	ロシアからのLNG途絶リスク、電力不足の懸念

参考法令

刑法（明治四十年法律第四十五号）

（支払用カード電磁的記録不正作出等）

第百六十三条の二　人の財産上の事務処理を誤らせる目的で、その事務処理の用に供する電磁的記録であって、クレジットカードその他の代金又は料金の支払用のカードを構成するものを不正に作った者は、十年以下の懲役又は百万円以下の罰金に処する。預貯金の引出用のカードを構成する電磁的記録を不正に作った者も、同様とする。

２　不正に作られた前項の電磁的記録を、同項の目的で、人の財産上の事務処理の用に供した者も、同項と同様とする。

３　不正に作られた第一項の電磁的記録をその構成部分とするカードを、同項の目的で、譲り渡し、貸し渡し、又は輸入した者も、同項と同様とする。

（不正電磁的記録カード所持）

第百六十三条の三　前条第一項の目的で、同条第三項のカードを所持した者は、五年以下の懲役又は五十万円以下の罰金に処する。

（支払用カード電磁的記録不正作出準備）

第百六十三条の四　第百六十三条の二第一項の犯罪行為の用に供する目的で、同項の電磁的記録の情報を取得した者は、三年以下の懲役又は五十万円以下の罰金に処する。情を知って、その情報を提供した者も、同様とする。

２　不正に取得された第百六十三条の二第一項の電磁的記録の情報を、前項の目的で保管した者も、同項と同様とする。

３　第一項の目的で、器械又は原料を準備した者も、同項と同様とする。

（電子計算機損壊等業務妨害）

第二百三十四条の二　人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。

２　前項の罪の未遂は、罰する。

日本国憲法（昭和二十一年憲法）

第十二条　この憲法が国民に保障する自由及び権利は、国民の不断の努力によつて、これを保持しなければならない。又、国民は、これを濫用してはならないのであつて、常に公共の福祉のためにこれを利用する責任を負ふ。

第十三条　すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。

第二十一条　集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。

②　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

国家公務員法（昭和二十二年法律第百二十号）

（秘密を守る義務）

第百条　職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。

②　法令による証人、鑑定人等となり、職務上の秘密に属する事項を発表するには、所轄庁の長（退職者については、その退職した官職又はこれに相当する官職の所轄庁の長）の許可を要する。

③　前項の許可は、法律又は政令の定める条件及び手続に係る場合を除いては、これを拒むことができない。

④　前三項の規定は、人事院で扱われる調査又は審理の際人事院から求められる情報に関しては、これを適用しない。何人も、人事院の権限によつて行われる調査又は審理に際して、秘密の又は公表を制限された情報を陳述し又は証言することを人事院から求められた場合には、何人からも許可を受ける必要がない。人事院が正式に要求した情報について、人事院に対して、陳述及び証言を行わなかつた者は、この法律の罰則の適用を受けなければならない。

⑤　前項の規定は、第十八条の四の規定により権限の委任を受けた再就職等監視委員会が行う調査について準用する。この場合において、同項中「人事院」とあるのは「再就職等監視委員会」と、「調査又は審理」とあるのは「調査」と読み替えるものとする。

外国為替及び外国貿易法（昭和二十四年法律第二百二十八号）

（対内直接投資等の届出及び変更勧告等）

第二十七条　外国投資家（前条第一項に規定する外国投資家をいう。以下この条、第二十八条、第二十九条第一項から第四項まで、第五十五条の五及び第九章において同じ。）は、

対内直接投資等（前条第二項に規定する対内直接投資等をいい、相続、遺贈、法人の合併その他の事情を勘案して政令で定めるものを除く。以下この条、第二十九条第一項から第四項まで、第五十五条の五、第六十九条の二第二項及び第七十条第一項において同じ。）のうち第三項の規定による審査が必要となる対内直接投資等に該当するおそれがあるものとして政令で定めるものを行おうとするときは、政令で定めるところにより、あらかじめ、当該対内直接投資等について、事業目的、金額、実行の時期その他の政令で定める事項を財務大臣及び事業所管大臣に届け出なければならない。

２　対内直接投資等について前項の規定による届出をした外国投資家は、財務大臣及び事業所管大臣が当該届出を受理した日から起算して三十日を経過する日までは、当該届出に係る対内直接投資等を行つてはならない。ただし、財務大臣及び事業所管大臣は、その期間の満了前に当該届出に係る対内直接投資等がその事業目的その他からみて次項の規定による審査が必要となる対内直接投資等に該当しないと認めるときは、当該期間を短縮することができる。

３　財務大臣及び事業所管大臣は、第一項の規定による届出があつた場合において、当該届出に係る対内直接投資等が次に掲げるいずれかの対内直接投資等（以下「国の安全等に係る対内直接投資等」という。）に該当しないかどうかを審査する必要があると認めるときは、当該届出に係る対内直接投資等を行つてはならない期間を、当該届出を受理した日から起算して四月間に限り、延長することができる。

一　イ又はロに掲げるいずれかの事態を生ずるおそれがある対内直接投資等（我が国が加盟する対内直接投資等に関する多数国間の条約その他の国際約束で政令で定めるもの（以下この号において「条約等」という。）の加盟国の外国投資家が行う対内直接投資等で対内直接投資等に関する制限の除去について当該条約等に基づく義務がないもの及び当該条約等の加盟国以外の国の外国投資家が行う対内直接投資等でその国が当該条約等の加盟国であるものとした場合に当該義務がないこととなるものに限る。）

イ　国の安全を損ない、公の秩序の維持を妨げ、又は公衆の安全の保護に支障を来すことになること。

ロ　我が国経済の円滑な運営に著しい悪影響を及ぼすことになること。

二　当該対内直接投資等が我が国との間に対内直接投資等に関し条約その他の国際約束がない国の外国投資家により行われるものであることにより、これに対する取扱いを我が国の投資家が当該国において行う直接投資等（前条第二項各号に掲げる対内直接投資等に相当するものをいう。）に対する取扱いと実質的に同等なものとするため、その内容の変更又は中止をさせる必要があると認められる対内直接投資等

三　資金の使途その他からみて、当該対内直接投資等の全部又は一部が第二十一条第一項又は第二項の規定により許可を受ける義務を課されている資本取引に当たるものとしてその内容の変更又は中止をさせる必要があると認められる対内直接投資等

4　財務大臣及び事業所管大臣は、前項の規定により対内直接投資等を行つてはならない期間を延長した場合において、同項の規定による審査をした結果、当該延長された期間の満了前に第一項の規定による届出に係る対内直接投資等が国の安全等に係る対内直接投資等に該当しないと認めるときは、当該延長された期間を短縮することができる。

5　財務大臣及び事業所管大臣は、第三項の規定により対内直接投資等を行つてはならない期間を延長した場合において、同項の規定による審査をした結果、第一項の規定による届出に係る対内直接投資等が国の安全等に係る対内直接投資等に該当すると認めるときは、関税・外国為替等審議会の意見を聴いて、当該対内直接投資等の届出をしたものに対し、政令で定めるところにより、当該対内直接投資等に係る内容の変更又は中止を勧告することができる。ただし、当該変更又は中止を勧告することができる期間は、当該届出を受理した日から起算して第三項又は次項の規定により延長された期間の満了する日までとする。

6　前項の規定により関税・外国為替等審議会の意見を聴く場合において、関税・外国為替等審議会が当該事案の性質に鑑み、第三項に規定する四月の期間内に意見を述べることが困難である旨を申し出た場合には、同項に規定する対内直接投資等を行つてはならない期間は、同項の規定にかかわらず、五月とする。

7　第五項の規定による勧告を受けたものは、当該勧告を受けた日から起算して十日以内に、財務大臣及び事業所管大臣に対し、当該勧告を応諾するかしないかを通知しなければならない。

8　前項の規定により勧告を応諾する旨の通知をしたものは、当該勧告をされたところに従い、当該勧告に係る対内直接投資等を行わなければならない。

9　第七項の規定により勧告を応諾する旨の通知をしたものは、第三項又は第六項の規定にかかわらず、当該対内直接投資等に係る届出を行つた日から起算して四月（同項の規定により延長された場合にあつては、五月）を経過しなくても、当該勧告に係る対内直接投資等を行うことができる。

１０　第五項の規定による勧告を受けたものが、第七項の規定による通知をしなかつた場合又は当該勧告を応諾しない旨の通知をした場合には、財務大臣及び事業所管大臣は、当該勧告を受けたものに対し、当該対内直接投資等に係る内容の変更又は中止を命ずることができる。ただし、当該変更又は中止を命ずることができる期間は、当該届出を受理した日から起算して第三項又は第六項の規定により延長された期間の満了する日までとする。

１１　財務大臣及び事業所管大臣は、経済事情の変化その他の事由により、第一項の規定による届出に係る対内直接投資等が国の安全等に係る対内直接投資等に該当しなくなつたと認めるときは、第七項の規定による対内直接投資等に係る内容の変更の勧告を応諾する旨の通知をしたもの又は前項の規定により対内直接投資等に係る内容の変更を命じられたものに対し、当該勧告又は命令の全部又は一部を取り消すことができる。

１２　第五項から前項までに定めるもののほか、対内直接投資等に係る内容の変更又は中止の勧告の手続その他これらの勧告に関し必要な事項は、政令で定める。

１３　特定組合等が行う対内直接投資等に相当するものにより当該特定組合等の組合員（特定組合類似団体にあつてはその構成員。以下同じ。）が取得する財産又は権利については、当該特定組合等が取得し、又は所有し、若しくは保有するものとみなして、前各項及び第二十九条第一項から第四項までの規定を適用する。

１４　外国投資家以外の者（法人その他の団体を含む。）が外国投資家のために当該外国投資家の名義によらないで行う対内直接投資等に相当するものについては、当該外国投資家以外の者を外国投資家とみなして、第一項から第十二項まで及び第二十九条第一項から第四項までの規定を適用する。

（対内直接投資等の届出の特例）

第二十七条の二　外国投資家（第二十六条第一項に規定する外国投資家をいい、この法律、この法律に基づく命令又はこれらに基づく処分に違反したものその他の前条第三項の規定による審査を行う必要性が高いものとして政令で定めるものを除く。以下この条において同じ。）は、対内直接投資等（第二十六条第二項に規定する対内直接投資等をいい、同項第一号から第四号まで及び第九号（第一号から第四号までに掲げる行為に準ずるものに限る。）に掲げる行為に限る。以下この条及び第二十九条第五項において同じ。）のうち、国の安全等に係る対内直接投資等に該当するおそれが大きいものとして政令で定めるもの以外のものを行おうとする場合には、前条第一項の規定にかかわらず、同項の規定による届出をすることを要しない。この場合において、当該外国投資家は、財務大臣及び事業所管大臣が定める対内直接投資等が国の安全等に係る対内直接投資等に該当しないための基準を遵守しなければならない。

２　財務大臣及び事業所管大臣は、前項に規定する基準の制定又は改廃の立案をしようとするときは、関税・外国為替等審議会の意見を聴かなければならない。

３　財務大臣及び事業所管大臣は、第一項の規定により前条第一項の規定による届出をせずに対内直接投資等を行つた外国投資家が、第一項に規定する基準に違反していると認めるときは、当該外国投資家に対し、当該基準を遵守するために必要な措置をとるべきことを勧告することができる。

４　財務大臣及び事業所管大臣は、前項の規定による勧告を受けた外国投資家がその勧告に従わなかつたときは、当該勧告を受けた外国投資家に対し、その勧告に係る措置をとるべきことを命ずることができる。

５　前二項に定めるもののほか、第三項の規定による勧告の手続その他当該勧告に関し必要な事項は、政令で定める。

6　特定組合等が行う対内直接投資等に相当するものにより当該特定組合等の組合員が取得する財産又は権利については、当該特定組合等が取得し、又は所有し、若しくは保有するものとみなして、前各項及び第二十九条第五項の規定を適用する。

7　外国投資家以外の者（法人その他の団体を含む。）が外国投資家のために当該外国投資家の名義によらないで行う対内直接投資等に相当するものについては、当該外国投資家以外の者を外国投資家とみなして、第一項から第五項まで及び第二十九条第五項の規定を適用する。

（措置命令）

第二十九条　財務大臣及び事業所管大臣は、次に掲げる場合において、対内直接投資等又は特定取得が国の安全等に係る対内直接投資等又は国の安全に係る特定取得に該当すると認めるときは、関税・外国為替等審議会の意見を聴いて、当該対内直接投資等又は特定取得を行つた外国投資家に対し、政令で定めるところにより、当該対内直接投資等又は特定取得により取得した株式又は持分の全部又は一部の処分その他必要な措置を命ずることができる。

一　第二十七条第一項又は第二十八条第一項の規定による届出をしなければならない外国投資家が、当該届出をせずに対内直接投資等又は特定取得を行つた場合

二　第二十七条第一項又は第二十八条第一項の規定による届出をした外国投資家が、禁止期間の満了前に、当該届出に係る対内直接投資等又は特定取得を行つた場合

2　財務大臣及び事業所管大臣は、第二十七条第一項又は第二十八条第一項の規定による届出をした外国投資家が、当該届出に関し虚偽の届出をした場合において、当該届出に係る対内直接投資等又は特定取得が国の安全等に係る対内直接投資等又は国の安全に係る特定取得に該当すると認めるときは、関税・外国為替等審議会の意見を聴いて、当該対内直接投資等又は特定取得を行つた外国投資家に対し、政令で定めるところにより、必要な措置を命ずることができる。

3　財務大臣及び事業所管大臣は、第二十七条第一項又は第二十八条第一項の規定による届出をした外国投資家が、第二十七条第七項（第二十八条第七項において準用する場合を含む。）の規定により応諾する旨の通知をした対内直接投資等若しくは特定取得に係る内容の変更の勧告に従わず、又は第二十七条第十項（第二十八条第七項において準用する場合を含む。）の規定による対内直接投資等若しくは特定取得に係る内容の変更の命令に違反した場合には、当該対内直接投資等又は特定取得を行つた外国投資家に対し、政令で定めるところにより、当該対内直接投資等又は特定取得により取得した株式又は持分（第二十七条第五項若しくは第二十八条第五項の規定により当該対内直接投資等若しくは特定取得に係る株式の数若しくは金額若しくは持分の口数若しくは金額の変更を勧告した場合における当該変更に係る部分又は第二十七条第十項（第二十八条第七項において準用する場合を含む。）の規定により当該対内直接投資等若しくは特定取得に係る株式の数若しくは金

額若しくは持分の口数若しくは金額の変更を命じた場合における当該変更に係る部分に限る。）の全部又は一部の処分その他必要な措置を命ずることができる。

4　財務大臣及び事業所管大臣は、第二十七条第一項又は第二十八条第一項の規定による届出をした外国投資家が、第二十七条第七項（第二十八条第七項において準用する場合を含む。）の規定により応諾する旨の通知をした対内直接投資等若しくは特定取得の中止の勧告に従わず、又は第二十七条第十項（第二十八条第七項において準用する場合を含む。）の規定による対内直接投資等若しくは特定取得の中止の命令に違反した場合には、当該対内直接投資等又は特定取得を行つた外国投資家に対し、政令で定めるところにより、当該対内直接投資等又は特定取得により取得した株式又は持分の全部又は一部の処分その他必要な措置を命ずることができる。

5　財務大臣及び事業所管大臣は、第二十七条の二第一項又は前条第一項の規定により第二十七条第一項又は第二十八条第一項の規定による届出をせずに対内直接投資等又は特定取得を行つた第二十七条の二第一項又は前条第一項に規定する外国投資家が、第二十七条の二第四項又は前条第四項の規定による命令に違反した場合であつて、当該対内直接投資等又は特定取得が国の安全等に係る対内直接投資等又は国の安全に係る特定取得に該当すると認めるときは、関税・外国為替等審議会の意見を聴いて、当該対内直接投資等又は特定取得を行つた外国投資家に対し、政令で定めるところにより、当該対内直接投資等又は特定取得により取得した株式又は持分の全部又は一部の処分その他必要な措置を命ずることができる。

6　第一項第二号の「禁止期間」とは、第二十七条第二項本文に規定する期間（同条第三項若しくは第六項の規定により延長され、又は同条第二項ただし書若しくは第四項の規定により短縮された場合には、当該延長され、又は短縮された期間）又は第二十八条第二項本文に規定する期間（同条第三項若しくは第六項の規定により延長され、又は同条第二項ただし書若しくは第四項の規定により短縮された場合には、当該延長され、又は短縮された期間）をいう。

昭和二十二年法律第五十四号（私的独占の禁止及び公正取引の確保に関する法律）（昭和二十二年法律第五十四号）

第九条　他の国内の会社の株式（社員の持分を含む。以下同じ。）を所有することにより事業支配力が過度に集中することとなる会社は、これを設立してはならない。

②　会社（外国会社を含む。以下同じ。）は、他の国内の会社の株式を取得し、又は所有することにより国内において事業支配力が過度に集中することとなる会社となつてはならない。

③　前二項において「事業支配力が過度に集中すること」とは、会社及び子会社その他当該会社が株式の所有により事業活動を支配している他の国内の会社の総合的事業規模が相当

数の事業分野にわたつて著しく大きいこと、これらの会社の資金に係る取引に起因する他の事業者に対する影響力が著しく大きいこと又はこれらの会社が相互に関連性のある相当数の事業分野においてそれぞれ有力な地位を占めていることにより、国民経済に大きな影響を及ぼし、公正かつ自由な競争の促進の妨げとなることをいう。

④　次に掲げる会社は、当該会社及びその子会社の総資産の額（公正取引委員会規則で定める方法による資産の合計金額をいう。以下この項において同じ。）で国内の会社に係るものを公正取引委員会規則で定める方法により合計した額が、それぞれ当該各号に掲げる金額を下回らない範囲内において政令で定める金額を超える場合には、毎事業年度終了の日から三月以内に、公正取引委員会規則で定めるところにより、当該会社及びその子会社の事業に関する報告書を公正取引委員会に提出しなければならない。ただし、当該会社が他の会社の子会社である場合は、この限りでない。

一　子会社の株式の取得価額（最終の貸借対照表において別に付した価額があるときは、その価額）の合計額の当該会社の総資産の額に対する割合が百分の五十を超える会社（次号において「持株会社」という。）　六千億円

二　銀行業、保険業又は第一種金融商品取引業（金融商品取引法（昭和二十三年法律第二十五号）第二十八条第一項に規定する第一種金融商品取引業をいう。次条第三項及び第四項において同じ。）を営む会社（持株会社を除く。）　八兆円

三　前二号に掲げる会社以外の会社　二兆円

⑤　前二項において「子会社」とは、会社がその総株主の議決権（株主総会において決議をすることができる事項の全部につき議決権を行使することができない株式についての議決権を除き、会社法第八百七十九条第三項の規定により議決権を有するものとみなされる株式についての議決権を含む。以下この条から第十一条まで、第二十二条第三号及び第七十条の四第一項において同じ。）の過半数を有する他の国内の会社をいう。この場合において、会社及びその一若しくは二以上の子会社又は会社の一若しくは二以上の子会社がその総株主の議決権の過半数を有する他の国内の会社は、当該会社の子会社とみなす。

⑥　前項の場合において、会社が有する議決権並びに会社及びその一若しくは二以上の子会社又は会社の一若しくは二以上の子会社が有する議決権には、社債、株式等の振替に関する法律第百四十七条第一項又は第百四十八条第一項の規定により発行者に対抗することができない株式に係る議決権を含むものとする。

⑦　新たに設立された会社は、当該会社がその設立時において第四項に規定する場合に該当するときは、公正取引委員会規則で定めるところにより、その設立の日から三十日以内に、その旨を公正取引委員会に届け出なければならない。

自衛隊法（昭和二十九年法律第百六十五号）

（命令による治安出動）

第七十八条　内閣総理大臣は、間接侵略その他の緊急事態に際して、一般の警察力をもつては、治安を維持することができないと認められる場合には、自衛隊の全部又は一部の出動を命ずることができる。

２　内閣総理大臣は、前項の規定による出動を命じた場合には、出動を命じた日から二十日以内に国会に付議して、その承認を求めなければならない。ただし、国会が閉会中の場合又は衆議院が解散されている場合には、その後最初に召集される国会において、すみやかに、その承認を求めなければならない。

３　内閣総理大臣は、前項の場合において不承認の議決があつたとき、又は出動の必要がなくなつたときは、すみやかに、自衛隊の撤収を命じなければならない。

（治安出動待機命令）

第七十九条　防衛大臣は、事態が緊迫し、前条第一項の規定による治安出動命令が発せられることが予測される場合において、これに対処するため必要があると認めるときは、内閣総理大臣の承認を得て、自衛隊の全部又は一部に対し出動待機命令を発することができる。

２　前項の場合においては、防衛大臣は、国家公安委員会と緊密な連絡を保つものとする。

不正競争防止法（平成五年法律第四十七号）

（罰則）

第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは二千万円以下の罰金に処し、又はこれを併科する。

一　不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。次号において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）その他の営業秘密保有者の管理を害する行為をいう。次号において同じ。）により、営業秘密を取得した者

二　詐欺等行為又は管理侵害行為により取得した営業秘密を、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、使用し、又は開示した者

三　営業秘密を営業秘密保有者から示された者であって、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、次のいずれかに掲げる方法でその営業秘密を領得した者

イ　営業秘密記録媒体等（営業秘密が記載され、又は記録された文書、図画又は記録媒体をいう。以下この号において同じ。）又は営業秘密が化体された物件を横領すること。

ロ　営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その複製を作成すること。

ハ　営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装すること。

四　営業秘密を営業秘密保有者から示された者であって、その営業秘密の管理に係る任務に背いて前号イからハまでに掲げる方法により領得した営業秘密を、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、使用し、又は開示した者

五　営業秘密を営業秘密保有者から示されたその役員（理事、取締役、執行役、業務を執行する社員、監事若しくは監査役又はこれらに準ずる者をいう。次号において同じ。）又は従業者であって、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、その営業秘密を使用し、又は開示した者（前号に掲げる者を除く。）

六　営業秘密を営業秘密保有者から示されたその役員又は従業者であった者であって、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その在職中に、その営業秘密の管理に係る任務に背いてその営業秘密の開示の申込みをし、又はその営業秘密の使用若しくは開示について請託を受けて、その営業秘密をその職を退いた後に使用し、又は開示した者（第四号に掲げる者を除く。）

七　不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、第二号若しくは前三号の罪又は第三項第二号の罪（第二号及び前三号の罪に当たる開示に係る部分に限る。）に当たる開示によって営業秘密を取得して、その営業秘密を使用し、又は開示した者

八　不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、第二号若しくは第四号から前号までの罪又は第三項第二号の罪（第二号及び第四号から前号までの罪に当たる開示に係る部分に限る。）に当たる開示が介在したことを知って営業秘密を取得して、その営業秘密を使用し、又は開示した者

九　不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、自己又は他人の第二号若しくは第四号から前号まで又は第三項第三号の罪に当たる行為（技術上の秘密を使用する行為に限る。以下この号及び次条第一項第二号において「違法使用行為」という。）により生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供した者（当該物が違法使用行為により生じた物であることの情を知らないで譲り受け、当該物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供した者を除く。）

２～１２（略）

国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）

（業務の特例）

第八条　機構は、第十四条に規定する業務のほか、当分の間、難視聴地域（日本放送協会が放送法（昭和二十五年法律第百三十二号）第二十条第五項の規定によりテレビジョン放送（同法第二条第十八号に規定するテレビジョン放送をいう。以下この項において同じ。）があまねく全国において受信できるように措置をするに当たり、地形その他の自然的条件の特殊性に起因して、衛星放送（テレビジョン放送であって、放送衛星（同法第二条第一号に規定する放送を行うための無線設備及びこれに附属する設備のみを搭載する人工衛星をいう。）の無線局を用いて行われるものをいう。以下この項において同じ。）によらなければその地域においてテレビジョン放送を受信できるようにすることが困難と認められる地域をいう。）において日本放送協会の衛星放送を受信することのできる受信設備を設置する者に対し助成金を交付する業務及びこれに附帯する業務を行う。

２　機構は、第十四条及び前項に規定する業務のほか、令和六年三月三十一日までの間、次に掲げる業務を行う。

一　特定アクセス行為を行い、通信履歴等の電磁的記録を作成すること。

二　特定アクセス行為に係る電気通信の送信先の電気通信設備が次のイ又はロに掲げる者の電気通信設備であるときは、当該イ又はロに定める者に対し、通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと。

イ　電気通信事業者　当該電気通信事業者

ロ　電気通信事業者（電気通信事業法（昭和五十九年法律第八十六号）第百十六条の二第二項第一号イに該当するものに限る。第八項において同じ。）の利用者　当該電気通信事業者

三　前二号に掲げる業務に附帯する業務を行うこと。

３　機構は、前項第二号に掲げる業務を認定送信型対電気通信設備サイバー攻撃対処協会に委託することができる。

４　この条（第一項及び次項から第七項までを除く。）において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

一　特定アクセス行為　機構の端末設備又は自営電気通信設備を送信元とし、アクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先とする電気通信の送信を行う行為であって、当該アクセス制御機能を有する特定電子計算機である電気通信設備に電

気通信回線を通じて当該アクセス制御機能に係る他人の識別符号（当該識別符号について電気通信事業法第五十二条第一項又は第七十条第一項第一号の規定により認可を受けた技術的条件において定めている基準を勘案して不正アクセス行為から防御するため必要な基準として総務省令で定める基準を満たさないものに限る。）を入力して当該電気通信設備を作動させ、当該アクセス制御機能により制限されている当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備の特定利用をし得る状態にさせる行為をいう。

二　通信履歴等の電磁的記録　特定アクセス行為に係る電気通信の送信元、送信先、通信日時その他の通信履歴を含む特定アクセス行為についての電磁的記録（電子的方式、磁気的方式その他の人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）であって、当該特定アクセス行為に係る電気通信の送信先のアクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれがあることの証拠となるものをいう。

三　電気通信、電気通信設備若しくは電気通信事業者、利用者、端末設備、自営電気通信設備又は送信型対電気通信設備サイバー攻撃若しくは認定送信型対電気通信設備サイバー攻撃対処協会　それぞれ電気通信事業法第二条第一号、第二号若しくは第五号、第十二条の二第四項第二号ロ、第五十二条第一項、第七十条第一項又は第百十六条の二第一項第一号若しくは第二項に規定する電気通信、電気通信設備若しくは電気通信事業者、利用者、端末設備、自営電気通信設備又は送信型対電気通信設備サイバー攻撃若しくは認定送信型対電気通信設備サイバー攻撃対処協会をいう。

四　特定電子計算機若しくは特定利用、識別符号、アクセス制御機能又は不正アクセス行為　それぞれ不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条に規定する特定電子計算機若しくは特定利用、識別符号、アクセス制御機能又は不正アクセス行為をいう。

5　機構は、第十四条並びに第一項及び第二項に規定する業務のほか、令和四年三月三十一日までの間、通信・放送開発法附則第五条第一項に規定する業務を行う。

6　前各項の規定により機構の業務が行われる場合には、第十五条第一項中「の一部」とあるのは「又は附則第八条第五項に規定する業務（通信・放送開発法附則第五条第一項第一号に掲げる業務に限り、債務の保証の決定を除く。）の一部」と、第十六条第二号中「含む。）」とあるのは「含む。）及び附則第八条第五項に規定する業務」と、第十七条第一項、第二十二条第一項第七号及び第二十六条第一号中「第十四条」とあるのは「第十四条並びに附則第八条第一項、第二項及び第五項」と、第十八条第一項中「同じ。）」とあるのは「同じ。）及び附則第八条第五項に規定する業務（通信・放送開発法附則第五条第一項第一号に掲げる業務に限り、これに附帯する業務を

含む。）」と、同条第三項中「業務」とあるのは「業務及び附則第八条第五項に規定する業務（通信・放送開発法附則第五条第一項第一号に掲げる業務に限り、これに附帯する業務を含む。）」と、第十九条中「障害者利用円滑化法第四条第一号に係る部分に限る。）」とあるのは「障害者利用円滑化法第四条第一号に係る部分に限る。）並びに附則第八条第一項」と、第二十二条第一項第一号及び第六号中「含む。）」とあるのは「含む。）及び附則第八条第五項に規定する業務（通信・放送開発法附則第五条第一項第一号に掲げる業務に限り、これに附帯する業務を含む。）」と、第二十三条中「附帯する業務」とあるのは「附帯する業務並びに附則第八条第二項に規定する業務」とする。

7　第二項から第四項までの規定により機構の業務が行われる場合には、次の表の上欄に掲げる規定中同表の中欄に掲げる字句は、それぞれ同表の下欄に掲げる字句とする。

電気通信事業法第百十六条の二第二項	三　前二号に掲げるもののほか、送信型対電気通信設備サイバー攻撃に対処する電気通信事業者を支援すること。	三　国立研究開発法人情報通信研究機構の委託を受けて、国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）附則第八条第二項第二号イ又はロに定める者に対し、同号の通知を行うこと。 四　前三号に掲げるもののほか、送信型対電気通信設備サイバー攻撃に対処する電気通信事業者を支援すること。
不正アクセス行為の禁止等に関する法律第二条第四項第一号	及び当該	、当該
	を除く	及び国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）附則第九条の認可を受けた同条の計画に基づき同法附則第八条第二項第一号に掲げる業務に従事する者がする同条第四項第一号に規定する特定アクセス行為を除く

8　第二項から第四項までの規定により機構の業務が行われる場合には、電気通信事業法第五十二条第一項又は第七十条第一項第一号の規定により認可を受けた電気通信事業者は、当該認可を受けた技術的条件において、アクセス制御機能（特定電子計算機である電気通信設備が有するものに限る。）に係る識別符号について、第四項第一号の総務省令で定める基準に相当する基準又はこれを上回る基準を定めているときを除き、同号の総務省令で定める基準に相当する基準を定めているものとみなす。

不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）

（不正アクセス行為の禁止）

第三条　何人も、不正アクセス行為をしてはならない。

（他人の識別符号を不正に取得する行為の禁止）

第四条　何人も、不正アクセス行為（第二条第四項第一号に該当するものに限る。第六条及び第十二条第二号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。

（不正アクセス行為を助長する行為の禁止）

第五条　何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。

（他人の識別符号を不正に保管する行為の禁止）

第六条　何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。

（識別符号の入力を不正に要求する行為の禁止）

第七条　何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。

一　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為

二　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為

個人情報の保護に関する法律（平成十五年法律第五十七号）

（漏えい等の報告等）

第二十六条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者又は行政機関等から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

２　（略）

特定秘密の保護に関する法律（平成二十五年法律第百八号）

（特定秘密の指定）

第三条　行政機関の長（当該行政機関が合議制の機関である場合にあっては当該行政機関をいい、前条第四号及び第五号の政令で定める機関（合議制の機関を除く。）にあってはその機関ごとに政令で定める者をいう。第十一条第一号を除き、以下同じ。）は、当該行政機関の所掌事務に係る別表に掲げる事項に関する情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるもの（日米相互防衛援助協定等に伴う秘密保護法（昭和二十九年法律第百六十六号）第一条第三項に規定する特別防衛秘密に該当するものを除く。）を特定秘密として指定するものとする。ただし、内閣総理大臣が第十八条第二項に規定する者の意見を聴いて政令で定める行政機関の長については、この限りでない。

２　行政機関の長は、前項の規定による指定（附則第五条を除き、以下単に「指定」という。）をしたときは、政令で定めるところにより指定に関する記録を作成するとともに、当該指定に係る特定秘密の範囲を明らかにするため、特定秘密である情報について、次の各号のいずれかに掲げる措置を講ずるものとする。

一　政令で定めるところにより、特定秘密である情報を記録する文書、図画、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録をいう。以下この号において同じ。）若しくは物件又は当該情報を化体する物件に特定秘密の表示（電磁的記録にあっては、当該表示の記録を含む。）をすること。

二　特定秘密である情報の性質上前号に掲げる措置によることが困難である場合において、政令で定めるところにより、当該情報が前項の規定の適用を受ける旨を当該情報を取り扱う者に通知すること。

３　行政機関の長は、特定秘密である情報について前項第二号に掲げる措置を講じた場合において、当該情報について同項第一号に掲げる措置を講ずることができることとなったときは、直ちに当該措置を講ずるものとする。

（指定の有効期間及び解除）

第四条　行政機関の長は、指定をするときは、当該指定の日から起算して五年を超えない範囲内においてその有効期間を定めるものとする。

２　行政機関の長は、指定の有効期間（この項の規定により延長した有効期間を含む。）が満了する時において、当該指定をした情報が前条第一項に規定する要件を満たすときは、政令で定めるところにより、五年を超えない範囲内においてその有効期間を延長するものとする。

３　指定の有効期間は、通じて三十年を超えることができない。

４　前項の規定にかかわらず、政府の有するその諸活動を国民に説明する責務を全うする観点に立っても、なお指定に係る情報を公にしないことが現に我が国及び国民の安全を確保するためにやむを得ないものであることについて、その理由を示して、内閣の承認を得た場合（行政機関が会計検査院であるときを除く。）は、行政機関の長は、当該指定の有効期間を、通じて三十年を超えて延長することができる。ただし、次の各号に掲げる事項に関する情報を除き、指定の有効期間は、通じて六十年を超えることができない。

一　武器、弾薬、航空機その他の防衛の用に供する物（船舶を含む。別表第一号において同じ。）

二　現に行われている外国（本邦の域外にある国又は地域をいう。以下同じ。）の政府又は国際機関との交渉に不利益を及ぼすおそれのある情報

三　情報収集活動の手法又は能力

四　人的情報源に関する情報

五　暗号

六　外国の政府又は国際機関から六十年を超えて指定を行うことを条件に提供された情報

七　前各号に掲げる事項に関する情報に準ずるもので政令で定める重要な情報

５　行政機関の長は、前項の内閣の承認を得ようとする場合においては、当該指定に係る特定秘密の保護に関し必要なものとして政令で定める措置を講じた上で、内閣に当該特定秘密を提示することができる。

６　行政機関の長は、第四項の内閣の承認が得られなかったときは、公文書等の管理に関する法律（平成二十一年法律第六十六号）第八条第一項の規定にかかわらず、当該指定に係る情報が記録された行政文書ファイル等（同法第五条第五項に規定する行政文書ファイル等をいう。）の保存期間の満了とともに、これを国立公文書館等（同法第二条第三項に規定する国立公文書館等をいう。）に移管しなければならない。

７　行政機関の長は、指定をした情報が前条第一項に規定する要件を欠くに至ったときは、有効期間内であっても、政令で定めるところにより、速やかにその指定を解除するものとする。

（特定秘密の保護措置）

第五条　行政機関の長は、指定をしたときは、第三条第二項に規定する措置のほか、第十一条の規定により特定秘密の取扱いの業務を行うことができることとされる者のうちから、当該行政機関において当該指定に係る特定秘密の取扱いの業務を行わせる職員の範囲を定めることその他の当該特定秘密の保護に関し必要なものとして政令で定める措置を講ずるものとする。

２　警察庁長官は、指定をした場合において、当該指定に係る特定秘密（第七条第一項の規定により提供するものを除く。）で都道府県警察が保有するものがあるときは、当該都道府県警察に対し当該指定をした旨を通知するものとする。

３　前項の場合において、警察庁長官は、都道府県警察が保有する特定秘密の取扱いの業務を行わせる職員の範囲その他の当該都道府県警察による当該特定秘密の保護に関し必要なものとして政令で定める事項について、当該都道府県警察に指示するものとする。この場合において、当該都道府県警察の警視総監又は道府県警察本部長（以下「警察本部長」という。）は、当該指示に従い、当該特定秘密の適切な保護のために必要な措置を講じ、及びその職員に当該特定秘密の取扱いの業務を行わせるものとする。

４　行政機関の長は、指定をした場合において、その所掌事務のうち別表に掲げる事項に係るものを遂行するために特段の必要があると認めたときは、物件の製造又は役務の提供を業とする者で、特定秘密の保護のために必要な施設設備を設置していることその他政令で定める基準に適合するもの（以下「適合事業者」という。）との契約に基づき、当該適合事業者に対し、当該指定をした旨を通知した上で、当該指定に係る特定秘密（第八条第一項の規定により提供するものを除く。）を保有させることができる。

５　前項の契約には、第十一条の規定により特定秘密の取扱いの業務を行うことができることとされる者のうちから、同項の規定により特定秘密を保有する適合事業者が指名して当該特定秘密の取扱いの業務を行わせる代表者、代理人、使用人その他の従業者（以下単に「従業者」という。）の範囲その他の当該適合事業者による当該特定秘密の保護に関し必要なものとして政令で定める事項について定めるものとする。

６　第四項の規定により特定秘密を保有する適合事業者は、同項の契約に従い、当該特定秘密の適切な保護のために必要な措置を講じ、及びその従業者に当該特定秘密の取扱いの業務を行わせるものとする。

（我が国の安全保障上の必要による特定秘密の提供）

第六条　特定秘密を保有する行政機関の長は、他の行政機関が我が国の安全保障に関する事務のうち別表に掲げる事項に係るものを遂行するために当該特定秘密を利用する必要があると認めたときは、当該他の行政機関に当該特定秘密を提供することができる。ただし、当該特定秘密を保有する行政機関以外の行政機関の長が当該特定秘密について指定をしているとき（当該特定秘密が、この項の規定により当該保有する行政機関の長から提供され

たものである場合を除く。）は、当該指定をしている行政機関の長の同意を得なければならない。

2　前項の規定により他の行政機関に特定秘密を提供する行政機関の長は、当該特定秘密の取扱いの業務を行わせる職員の範囲その他の当該他の行政機関による当該特定秘密の保護に関し必要なものとして政令で定める事項について、あらかじめ、当該他の行政機関の長と協議するものとする。

3　第一項の規定により特定秘密の提供を受ける他の行政機関の長は、前項の規定による協議に従い、当該特定秘密の適切な保護のために必要な措置を講じ、及びその職員に当該特定秘密の取扱いの業務を行わせるものとする。

第七条　警察庁長官は、警察庁が保有する特定秘密について、その所掌事務のうち別表に掲げる事項に係るものを遂行するために都道府県警察にこれを利用させる必要があると認めたときは、当該都道府県警察に当該特定秘密を提供することができる。

2　前項の規定により都道府県警察に特定秘密を提供する場合については、第五条第三項の規定を準用する。

3　警察庁長官は、警察本部長に対し、当該都道府県警察が保有する特定秘密で第五条第二項の規定による通知に係るものの提供を求めることができる。

第八条　特定秘密を保有する行政機関の長は、その所掌事務のうち別表に掲げる事項に係るものを遂行するために、適合事業者に当該特定秘密を利用させる特段の必要があると認めたときは、当該適合事業者との契約に基づき、当該適合事業者に当該特定秘密を提供することができる。ただし、当該特定秘密を保有する行政機関以外の行政機関の長が当該特定秘密について指定をしているとき（当該特定秘密が、第六条第一項の規定により当該保有する行政機関の長から提供されたものである場合を除く。）は、当該指定をしている行政機関の長の同意を得なければならない。

2　前項の契約については第五条第五項の規定を、前項の規定により特定秘密の提供を受ける適合事業者については同条第六項の規定を、それぞれ準用する。この場合において、同条第五項中「前項」とあるのは「第八条第一項」と、「を保有する」とあるのは「の提供を受ける」と読み替えるものとする。

3　第五条第四項の規定により適合事業者に特定秘密を保有させている行政機関の長は、同項の契約に基づき、当該適合事業者に対し、当該特定秘密の提供を求めることができる。

第九条　特定秘密を保有する行政機関の長は、その所掌事務のうち別表に掲げる事項に係るものを遂行するために必要があると認めたときは、外国の政府又は国際機関であって、この法律の規定により行政機関が当該特定秘密を保護するために講ずることとされる措置に相当する措置を講じているものに当該特定秘密を提供することができる。ただし、当該特

定秘密を保有する行政機関以外の行政機関の長が当該特定秘密について指定をしているとき（当該特定秘密が、第六条第一項の規定により当該保有する行政機関の長から提供されたものである場合を除く。）は、当該指定をしている行政機関の長の同意を得なければならない。

（その他公益上の必要による特定秘密の提供）

第十条　第四条第五項、第六条から前条まで及び第十八条第四項後段に規定するもののほか、行政機関の長は、次に掲げる場合に限り、特定秘密を提供するものとする。

一　特定秘密の提供を受ける者が次に掲げる業務又は公益上特に必要があると認められるこれらに準ずる業務において当該特定秘密を利用する場合（次号から第四号までに掲げる場合を除く。）であって、当該特定秘密を利用し、又は知る者の範囲を制限すること、当該業務以外に当該特定秘密が利用されないようにすることその他の当該特定秘密を利用し、又は知る者がこれを保護するために必要なものとして、イに掲げる業務にあっては附則第十条の規定に基づいて国会において定める措置、イに掲げる業務以外の業務にあっては政令で定める措置を講じ、かつ、我が国の安全保障に著しい支障を及ぼすおそれがないと認めたとき。

イ　各議院又は各議院の委員会若しくは参議院の調査会が国会法（昭和二十二年法律第七十九号）第百四条第一項（同法第五十四条の四第一項において準用する場合を含む。）又は議院における証人の宣誓及び証言等に関する法律（昭和二十二年法律第二百二十五号）第一条の規定により行う審査又は調査であって、国会法第五十二条第二項（同法第五十四条の四第一項において準用する場合を含む。）又は第六十二条の規定により公開しないこととされたもの

ロ　刑事事件の捜査又は公訴の維持であって、刑事訴訟法（昭和二十三年法律第百三十一号）第三百十六条の二十七第一項（同条第三項及び同法第三百十六条の二十八第二項において準用する場合を含む。）の規定により裁判所に提示する場合のほか、当該捜査又は公訴の維持に必要な業務に従事する者以外の者に当該特定秘密を提供することがないと認められるもの

二　民事訴訟法（平成八年法律第百九号）第二百二十三条第六項の規定により裁判所に提示する場合

三　情報公開・個人情報保護審査会設置法（平成十五年法律第六十号）第九条第一項の規定により情報公開・個人情報保護審査会に提示する場合

四　会計検査院法（昭和二十二年法律第七十三号）第十九条の四において読み替えて準用する情報公開・個人情報保護審査会設置法第九条第一項の規定により会計検査院情報公開・個人情報保護審査会に提示する場合

２　警察本部長は、第七条第三項の規定による求めに応じて警察庁に提供する場合のほか、前項第一号に掲げる場合（当該警察本部長が提供しようとする特定秘密が同号ロに掲げる

業務において利用するものとして提供を受けたものである場合以外の場合にあっては、同号に規定する我が国の安全保障に著しい支障を及ぼすおそれがないと認めることについて、警察庁長官の同意を得た場合に限る。）、同項第二号に掲げる場合又は都道府県の保有する情報の公開を請求する住民等の権利について定める当該都道府県の条例（当該条例の規定による諮問に応じて審議を行う都道府県の機関の設置について定める都道府県の条例を含む。）の規定で情報公開・個人情報保護審査会設置法第九条第一項の規定に相当するものにより当該機関に提示する場合に限り、特定秘密を提供することができる。

３　適合事業者は、第八条第三項の規定による求めに応じて行政機関に提供する場合のほか、第一項第一号に掲げる場合（同号に規定する我が国の安全保障に著しい支障を及ぼすおそれがないと認めることについて、当該適合事業者が提供しようとする特定秘密について指定をした行政機関の長の同意を得た場合に限る。）又は同項第二号若しくは第三号に掲げる場合に限り、特定秘密を提供することができる。

第十一条　特定秘密の取扱いの業務は、当該業務を行わせる行政機関の長若しくは当該業務を行わせる適合事業者に当該特定秘密を保有させ、若しくは提供する行政機関の長又は当該業務を行わせる警察本部長が直近に実施した次条第一項又は第十五条第一項の適性評価（第十三条第一項（第十五条第二項において準用する場合を含む。）の規定による通知があった日から五年を経過していないものに限る。）において特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがないと認められた者（次条第一項第三号又は第十五条第一項第三号に掲げる者として次条第三項又は第十五条第二項において読み替えて準用する次条第三項の規定による告知があった者を除く。）でなければ、行ってはならない。ただし、次に掲げる者については、次条第一項又は第十五条第一項の適性評価を受けることを要しない。

一　行政機関の長

二　国務大臣（前号に掲げる者を除く。）

三　内閣官房副長官

四　内閣総理大臣補佐官

五　副大臣

六　大臣政務官

七　前各号に掲げるもののほか、職務の特性その他の事情を勘案し、次条第一項又は第十五条第一項の適性評価を受けることなく特定秘密の取扱いの業務を行うことができるものとして政令で定める者

サイバーセキュリティ基本法（平成二十六年法律第百四号）

（基本理念）

第三条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。

２　サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靭（じん）な体制を構築するための取組を積極的に推進することを旨として、行われなければならない。

３　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するための取組を積極的に推進することを旨として、行われなければならない。

４　サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない。

５～６（略）

（サイバーセキュリティ協議会）

第十七条　第二十八条第一項に規定するサイバーセキュリティ戦略本部長及びその委嘱を受けた国務大臣（次項において「本部長等」という。）は、サイバーセキュリティに関する施策の推進に関し必要な協議を行うため、サイバーセキュリティ協議会（以下この条において「協議会」という。）を組織するものとする。

２　（略）

３　協議会は、第一項の協議を行うため必要があると認めるときは、その構成員に対し、サイバーセキュリティに関する施策の推進に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該構成員は、正当な理由がある場合を除き、その求めに応じなければならない。

４　協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事務に関して知り得た秘密を漏らし、又は盗用してはならない。

５～６（略）

第三十八条　第十七条第四項又は第三十一条第二項の規定に違反した者は、一年以下の懲役又は五十万円以下の罰金に処する。

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和四年法律第四十三号）

（目的）

第一条　この法律は、国際情勢の複雑化、社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み、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基本的な方針を策定するとともに、安全保障の確保に関する経済施策として、特定重要物資の安定的な供給の確保及び特定社会基盤役務の安定的な提供の確保に関する制度並びに特定重要技術の開発支援及び特許出願の非公開に関する制度を創設することにより、安全保障の確保に関する経済施策を総合的かつ効果的に推進することを目的とする。

（基本方針）

第二条　政府は、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基本的な方針（以下「基本方針」という。）を定めなければならない。

２～５　（略）

（安定供給確保基本指針）

第六条　政府は、基本方針に基づき、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（以下この章において「安定供給確保」という。）に関する基本指針（以下この章において「安定供給確保基本指針」という。）を定めるものとする。

２～６（略）

（特定重要物資の指定）

第七条　国民の生存に必要不可欠な若しくは広く国民生活若しくは経済活動が依拠している重要な物資（プログラムを含む。以下同じ。）又はその生産に必要な原材料、部品、設備、機器、装置若しくはプログラム（以下この章において「原材料等」という。）について、外部に過度に依存し、又は依存するおそれがある場合において、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、当該物資若しくはその生産に必要な原材料等（以下この条において「物資等」という。）の生産基盤の整備、供給源の多様化、備蓄、生産技術の導入、開発若しくは改良その他の当該物資等の供給網を

強靭化するための取組又は物資等の使用の合理化、代替となる物資の開発その他の当該物資等への依存を低減するための取組により、当該物資等の安定供給確保を図ることが特に必要と認められるときは、政令で、当該物資を特定重要物資として指定するものとする。

（安定供給確保取組方針）

第八条　主務大臣は、安定供給確保基本指針に基づき、前条の規定により指定された特定重要物資のうち、その所管する事業に係るものに関し、特定重要物資ごとに当該特定重要物資又はその生産に必要な原材料等（以下この章及び第八十六条第一項第二号において「特定重要物資等」という。）に係る安定供給確保を図るための取組方針（以下この章において「安定供給確保取組方針」という。）を定めるものとする。

２～６（略）

（特定重要技術研究開発基本指針）

第六十条　政府は、基本方針に基づき、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に関する基本指針（以下この章において「特定重要技術研究開発基本指針」という。）を定めるものとする。

２～６（略）

（調査研究）

第六十四条　内閣総理大臣は、特定重要技術研究開発基本指針に基づき、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に必要な調査及び研究（次項及び第三項において「調査研究」という。）を行うものとする。

２　内閣総理大臣は、調査研究の全部又は一部を、その調査研究を適切に実施することができるものとして次に掲げる基準に適合する者（法人に限る。）に委託することができる。

一　先端的技術に関する内外の社会経済情勢及び研究開発の動向の専門的な調査及び研究を行う能力を有すること。

二　先端的技術に関する内外の情報を収集し、整理し、及び保管する能力を有すること。

三　内外の科学技術に関する調査及び研究を行う機関、科学技術に関する研究開発を行う機関その他の内外の関係機関と連携する能力を有すること。

四　情報の安全管理のための措置を適確に実施するに足りる能力を有すること。

３～４（略）

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施行令（令和四年政令第三百九十四号）

（特定重要物資の指定）

第一条　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（第三条第十三号を除き、以下「法」という。）第七条の規定に基づき、次に掲げる物資を特定重要物資として指定する。

一　抗菌性物質製剤

二　肥料

三　永久磁石

四　工作機械及び産業用ロボット

五　航空機の部品（航空機用原動機及び航空機の機体を構成するものに限る。）

六　半導体素子及び集積回路

七　蓄電池

八　インターネットその他の高度情報通信ネットワークを通じて電子計算機（入出力装置を含む。）を他人の情報処理の用に供するシステムに用いるプログラム

九　可燃性天然ガス

十　金属鉱産物（マンガン、ニッケル、クロム、タングステン、モリブデン、コバルト、ニオブ、タンタル、アンチモン、リチウム、ボロン、チタン、バナジウム、ストロンチウム、希土類金属、白金族、ベリリウム、ガリウム、ゲルマニウム、セレン、ルビジウム、ジルコニウム、インジウム、テルル、セシウム、バリウム、ハフニウム、レニウム、タリウム、ビスマス、グラファイト、フッ素、マグネシウム、シリコン及びリンに限る。）

十一　船舶の部品（船舶用機関、航海用具及び推進器に限る。）

サイバーセキュリティ協議会規約(平成 31 年４月１日制定　令和４年３月 22 日一部改正)

（目的）

第３条 協議会は、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、大学その他の教育研究機関等のうち、我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行うことを目的とする。

（総会）

第10 条 協議会は、原則として毎年、構成員(JISP 参加構成員を除く。以下この条において同じ。)による定時総会を開催するものとする。また、運営委員会が必要と認めるときは、臨時総会を開催することができる（以下、定時総会及び臨時総会をあわせて「総会」という。）。

２～８（略）

（事務局と構成員との情報共有）

第16 条 事務局は、JPCERT/CC から提供される情報、構成員（JISP 参加構成員を除く。以下この章及び第７章において同じ。）から直接提供される情報、非構成員から直接提供される情報を取り扱うこととする。
２ 事務局は、構成員に対し、サイバーセキュリティの確保に資する情報を随時提供するもの
のとする。
３ 構成員は、事務局に対し、サイバーセキュリティの確保に資する情報を任意に提供する
ことができる。構成員は、第４条第３項の規定の趣旨に鑑み、自組織内において収集・分析した情報のみでは情報システムの被害の内容・範囲を検知または認知するに至っておらず、平常時に比して直感的な違和感があるといった程度にとどまる早期・初動の時点においても、国内外における類似関連情報その他の有益な助言や情報を、専門的知見を有する政令指定法人JPCERT/CC や他の構成員から得ることを目的として、事務局に対する相談に伴い、情報を提供することができる。

（情報の共有範囲の指定）
第17 条 構成員は、事務局に対し任意に情報を提供するに際し、当該情報の共有範囲を指定することができる。事務局を含め、何人も、当該構成員の同意を得ることなく、当該共有範囲を超えて情報の共有を行ってはならない。
２ 事務局は、構成員に対し情報を提供するに際し、当該情報の共有範囲を指定することができる。何人も、事務局の同意を得ることなく、当該共有範囲を超えて情報の共有を行ってはならない。
３ 事務局は、前条第２項の規定に基づき提供する情報の中に、同条第３項の規定に基づき任意に提供された情報が含まれるときは、当該情報を提供した構成員の同意を得ることなく、第１項の規定に基づき当該構成員が指定した共有範囲を超えて、前項に規定する情報の共有範囲を指定してはならない。
４ 事務局は、構成員（GSOC 連携構成員を除く。以下この項において同じ。）に対し情報を提供するに際し、第２項に規定する情報の共有範囲の指定の有無及び内容に応じて、当該情報に以下に掲げるTLP（Traffic Light Protocol）のいずれかを付与するものとする。
一 TLP:RED 情報の共有範囲が、構成員に所属する協議会事務従事者（当該構成員に係る登録事務従事者を含む。）に限られる場合
二 TLP:AMBER 情報の共有範囲が、構成員に係る協議会事務従事者及び第19 条第３項第２号又は同項第３号の規定に基づき当該構成員を介して非構成員のサイバーセキュリティを確保する必要がある場合における当該非構成員に係る協議会事務従事者に限られる場合

三 TLP:GREEN 前号に規定する範囲よりも広い範囲での共有が認められるが、一般に公開することは認められない場合
四 TLP:WHITE 一般に公開することが認められる場合

（秘密の管理）
第18 条 構成員は、事務局に対し任意に情報を提供するに際し、法第17 条第４項に規定する秘密の有無を明示することとする。
２ 事務局は、構成員に対し情報を提供するに際し、法第17 条第４項に規定する秘密の範囲を明示することとする。
３～６（略）

（協議会からの協力の求め）
第23 条 協議会は、次の各号に掲げる場合に限り、構成員に対して、法第17 条第３項に基づく情報提供等の協力の求めを行うものとする。
一 大規模なサイバー攻撃が発生するなど、情報提供等の協力を求める特別の必要性が認められる場合又はこれに準ずる状況であると認められる場合
二 構成員にとって協議会による求めがなければ提供することができない情報を提供する場合であって、当該構成員が協議会による協力の求めを受けることについて同意している場合
２ 協議会は、前項の規定に基づき情報提供等の協力の求めを行うにあたっては、必要に応じて、当該協力の求めの目的及び当該求めに基づき取得した情報の共有範囲を明示するものとする。

24 条タスクフォース規則（平成 31 年４月１日 24 条タスクフォース決定　令和４年４月１日 一部改正）

（タスクフォース参加者の区分）
第１条 24 条タスクフォース（以下「タスクフォース」という。）に参加する者は、政令指定法人JPCERT/CC のほか、第一類構成員及び第二類構成員の２つの区分により構成する。
一 第一類構成員 構成員のうち、他の情報共有体制に参加又は運営する主体であって、サイバーセキュリティ協議会規約（以下「規約」という。）第４条第１項第１号及び同項第２号に定める活動に積極的に貢献する能力と意欲を有する者として、サイバーセキュリティの確保に資する情報を積極的に提供することができる者
二 第二類構成員 構成員のうち、第一類構成員等（政令指定法人JPCERT/CC 及び第一類構成員をいう。以下同じ。）から提供される情報に対し一定の応答を行うことができる能力

と意欲を有する者

（タスクフォースの業務）
第２条 タスクフォースは、規約第４条第１項第１号及び同項第２号に掲げる協議会の活動として、サイバーセキュリティに関する脅威情報等の積極的な共有及び分析を行い、我が国のサイバーセキュリティを確保するために必要な情報の作出及び共有を積極的に行うものとする。
２～６（略）

（情報提供等の協力の求め）
第４条 協議会は、規約第23 条第１項の規定にかかわらず、第一類構成員又は第二類構成員に対して情報提供等の協力を求める必要があると認められる場合には、別途タスクフォースが定めるところにより、法第17 条第３項に基づく情報提供等の協力の求めを行うものとする。

米国参考法令

Executive Order on Improving the Nation’s Cybersecurity
MAY 12, 2021

(c) The recommended contract language and requirements described in subsection (b) of this section shall be designed to ensure that:
(i) service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies’ requirements;
(ii) service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;

豪州参考法令

Security Legislation Amendment (Critical Infrastructure) Act 2021
No. 124, 2021

8D Meaning of critical infrastructure sector

Each of the following sectors of the Australian economy is a critical infrastructure sector:

(a) the communications sector;

(b) the data storage or processing sector;

(c) the financial services and markets sector;

(d) the water and sewerage sector;

(e) the energy sector;

(f) the health care and medical sector;

(g) the higher education and research sector;

(h) the food and grocery sector;

(i) the transport sector;

(j) the space technology sector;

(k) the defence industry sector.

30BC Notification of critical cyber security incidents

(1) If:

(a) an entity is the responsible entity for a critical infrastructure asset; and

(b) the entity becomes aware that:

(i) a cyber security incident has occurred or is occurring; and

(ii) the incident has had, or is having, a significant impact (whether direct or indirect) on the availability of the asset;

the entity must:

(c) give the relevant Commonwealth body (see section 30BF) a report that:

(i) is about the incident; and

(ii) includes such information (if any) as is prescribed by the rules; and

(d) do so as soon as practicable, and in any event within 12 hours, after the entity becomes so aware.

Civil penalty: 50 penalty units.

Form of report etc.

30BD Notification of other cyber security incidents

(1) If:

(a) an entity is the responsible entity for a critical infrastructure asset; and

(b) the entity becomes aware that:

(i) a cyber security incident has occurred, is occurring or is imminent; and

(ii) the incident has had, is having, or is likely to have, a relevant impact on the asset;

the entity must:

(c) give the relevant Commonwealth body (see section 30BF) a report that:

(i) is about the incident; and

(ii) includes such information (if any) as is prescribed by the rules; and

(d) do so as soon as practicable, and in any event within 72 hours, after the entity becomes so aware.

Civil penalty: 50 penalty units. Form of report etc.

【付属資料】　ヒアリング報告書

以下に附する「ヒアリング報告書」は、本研究で実施した一連のヒアリング調査において聴取した内容をヒアリング調査報告という形でまとめたものである。

いずれの報告書も、調査先による十分な確認・校閲を得た上で、公開の許可を得た情報に限り掲載している。文中の各種表現については、先方の発言内容を最大限に尊重し、可能な限り忠実に反映している旨ご了承いただきたい。

（ヒアリング日時順）

ヒアリング調査報告 No.1 基本情報

日時	2022 年 5 月 31 日
テーマ	アカデミアにおける技術流出の実態と対策について
ヒアリング先 （担当者）	宮城県警察本部 警備部 外事課 課長 工藤良徳 様
場所	東北大学 片平キャンパス エクステンション教育研究棟 201A 講義室
参加者	（WS-C 教授）坪原和洋 教授、阿南友亮 教授、今西淳 教授 （WS-C 学生）稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香髙優一郎、宮内拓、山田麻友 （計 11 名）
調査目的	アカデミアや産業界での技術流出の実態把握や警察による経済安全保障の取り組みの理解を図ること。

（写真）

【レクチャー】

（アカデミアにおける技術流出の実態と対策について）

1. 経済安全保障の推進

2010 年のレアアース対日輸出制限、2020 年のコロナワクチン不足や 2021 年の通信アプリの個人情報管理より、経済安全保障の問題が顕在化した。自民党提言より経済安全保障の方向性として、我が国の自律性の向上や優位性の確保、基本的価値やルールに基づく国際秩序を示され、2022 年 5 月に経済安全保障推進法が成立した。

2. アカデミアにおける技術流出のリスク・接近事例

大学、研究開発法人などのアカデミアは、オープンな環境で研究を行い、その成果は広く公表されている。もっとも、近年はこうしたオープンな特性が利用され、外国による技術流出のリスクが顕在化している。このようななかで、アメリカにおいては、「外国の敵対者（＝国家の影響が背後に及んでいる人）」がアカデミアにおいて狙う標的や、用いる戦術を具体的に列挙し、そのリスクについて警鐘した大学向けの情報提供を行った。イギ

リスにおいては、中国が海外の大学とコラボレーションして入手した技術が、人民解放軍の拡張に転用されるだけでなく、少数民族の人権侵害に使われることを警告し、リスク管理の必要性を指摘した。国家への技術流出のリスクにおいては、サイバー攻撃による直接窃取のほか、合法性・妥当性の濃淡の異なる様々な手法を用いて、幅広く我が国の技術情報を得ようとする動向が認められる。我が国のアカデミアにおける事例としては、接近工作、共同研究、ヘッドハンティング、大学間協定、人事交流等があげられている。

3.技術流出防止の向けた警察の取組

日本警察による取組として、１点目として、全国の警察組織のネットワークを有効に活用し、取締りなどにより把握した外国の工作手口や対策のノウハウを企画やアカデミアに提供する取組を「アウトリーチ活動」として推進している。2 点目として、産官学が推進する流出防止対策に有益な情報を幅広く提供し、被害の未然防止を図ることが重要との認識の下、経済産業省や自治体、経済団体などとも連携している。工作活動の取締りと阻止として、警察では、経済安全保障の観点から、機微技術の不正輸出事案や、産業スパイ事案、サイバー攻撃事案の取締り（事件化）を実施している。また、取締りだけでなく、アウトリーチ活動を通じ、個別の工作活動が成功することを阻止するための注意喚起も推進している。企業・アカデミアの注意喚起も、主に懸念国を念頭に行っている。ある国は海外逃亡した経済犯・汚職犯を帰国させる「キツネ狩り作戦」を行っていた。現在はターゲットが政敵や反体制派等にも拡大し、本国家族の脅迫、海外工作活動、旅券や犯罪人引渡し等を組み合わせて強力に推進されている。在日の方が標的とされ、本国家族に圧力が掛かり、例えばスパイ行為や技術情報の窃取を強要される可能性もあり、予断を許さない。

【質疑応答】

Q1：　実際に怪しい話に誘われたときはどのように通報すればよろしいでしょうか。

A1：　まずは#9110 でもいいし、警察署に相談をしてもらえれば助かる。そもそも被害者の立場になるので相談の秘密は守るし、安心して欲しい。また、警察庁に相談用のメールアドレスもある。

Q2：　全国の警察組織のネットワークを有効に活用し、取締りなどにより把握した外国の工作手口や対策ノウハウを企業やアカデミアに提供する取組を「アウトリーチ活動」として推進しているということだったが、どのような活動を行っていますか。情報を公開するのみなのでしょうか、それとも企業に訪問して指導しているのでしょうか。

A2：　企業には個別にアプローチしている。県内で 10 万の事業体があり、そのなかからアウトリーチをする企業を絞っている。単なる民間企業の製品でも、デュアルユースが行われる可能性がある。技術を一つ一つ調べて選定している。

Q3：　アウトリーチやその他の施策の今後の方向性について教えていただきたいです。

A3：　アウトリーチ活動、違反行為、情報収集の 3 つを効率的に実施する必要がある。その際、企業や大学が規制強化やその自由を制限されると誤解して及び腰になることが懸念される。あくまでも県警のアウトリーチ活動は情報提供であり、企業・大学ファーストの原則で実施することが大事だと考えている。そもそも被害者又は潜在的な被害者が自主防犯活動を効果的にやるための啓発活動であるため、そのような誤解を招かないように丁寧な説明が必要であると考えている。

以上

記録作成担当者：岡本樹

ヒアリング調査報告 No.2 基本情報

日時	2022 年 6 月 14 日
テーマ	東北大学内の安全保障輸出管理に関して
ヒアリング先 (担当者)	東北大学 安全保障輸出管理 全学管理責任者 兼安全保障輸出管理委員会委員長 足立幸志 様 東北大学 安全保障輸出管理室 小松山勝樹 様
場所	東北大学 片平キャンパス エクステンション教育研究棟 201A 講義室
参加者	(WS-C 教授) 坪原和洋 教授、阿南友亮 教授、今西淳 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 11 名)
調査目的	東北大学の学内における安全保障輸出管理に関してヒアリング調査を行うことで現状の安全保障輸出管理の実態を知ること。

【質疑応答】

Q1： 人の受け入れと輸出に関しては別問題でありますが、受け入れた人の帰国後についての情報を大学として知るのは難しいのではないでしょうか。

A1： 留学生の帰国後を追いかけるのは難しいが貨物や技術の持ち帰りをしていないかのチェックはしている。入学時の誓約書の段階で、母国の軍事研究に使わないという誓約をしている。誓約書に拘束力はないが、大学としてできることはしている。理系の研究室で学生が大学を出た後にどこで何をしているかは研究室にもよるが、半分ぐらいは分かっている教授もいる。学生の卒業後の進路を知ることは難しく、学生間で在席中にどれだけ密な関係を築くことが出来るかにかかっている。

Q2： 誰でも参加可能な会合について手続き不要とのことでしたが、そこから情報が洩れていく可能性は考えられるのでしょうか。

A2： 出席を限定しない講演会等での発表は公知化するためであるため、先生の負担を減らすために手続き不要としている。公知化する情報は、情報が洩れるのではなく、むしろ情報を発信していきたいものである。国際会議で発表していいものであるかは精査をしており、さらに公知になるため外為法の範囲外となる。また、守秘義務があるかどうかについては発表者自身が発表するものについて精査している。

Q3: 物理的な輸出の管理については外為法のみなし輸出管理の明確化等により厳格化されるが、知識等情報の流出に関して外為法では規制が難しいと思われます。大学等の研究でノウハウを身に付け、その知識を軍事転用するといったことが現実的なのかどうか、また、現実的である場合に現行の制度で防止するものがあるのでしょうか。

A3: まず学部生や修士までの大学院生が学んだ知識やノウハウを軍事転用することはほぼ不可能ではないかと考えている。法学部卒の学生がいきなり裁判所に立つようなもの。現行の制度上の手続きをしっかり実施することが大学の責務であるとともに、本学で学んだものは論文等で公知化して帰国等をしてもらうことを心掛けている。また、現行制度において、人物の入国に制限をかけるものはない。仮に大学において人物に制限をかける制度を設けるとしても、大学は国際化を推進しているため、ある国や機関からすべてを拒否することは難しい。いったん受け入れたうえで、特定の技術や情報、研究所等には触れさせないといった制度が有効である。どの技術や情報を守るのかといった制度設計は、国が主導して行ってほしい。

Q4: 外国人教員・留学生が退職・退学後、本学で身に付けた機微な技術知識を帰国後に漏らすことまでは防ぎきれないと考えるが、大学ができる対策があるのでしょうか。

A4:　帰国後の行動管理までは不可能なので、大学としては、誓約書の徴取や終了前確認をしっかり行うとともに、在籍期中の研究成果は極力、論文等で発表してから帰国していただくようにしている。しかし、頭に記憶していることまでは管理できない。もっともコアな技術に触れさせないといった対応を取っている以上、それを母国で軍事転用される懸念するはほとんどないのではないか。公知の技術をすぐに軍事転用できるのであれば、既にその国が軍事技術として展開しているだろう。

Q5:　みなし輸出対策としてチェックフロー図や輸出管理シートを確認しているとのことだが、確認の際に教員・学生が情報を隠蔽して回答することも考えられますが、そこで、大学側が正確に情報を把握するための方策等はあるのでしょうか。
A5:　輸出管理の手続きに関しては自由な教育環境を確保することが前提である。情報の隠蔽が全くないとは言い切れないが、輸出管理はあくまでも研究者である教員を守るという趣旨であり、情報の虚偽があるとは考えていない。そもそも研究者にとって自らの研究が不正輸出の対象になったり、学生にスパイのような人間が入ったりといったことは不利益こそあれ、得になることは何もない。そのことを教員によく理解してもらった上で一番の利害関係者として輸出管理の手続きをしっかりとしてもらうために講習会を行っており、大学としては情報を隠蔽されないように手を尽くしている。研究開発にブレーキをかけることがあってはならず、海外の人材を受け入れることは不可欠である。

Q6:　悪意を持った人物が貨物又は技術の提供の目的・用途等を巧みに偽り「輸出管理シート」記載した場合、取引を承認されてしまう可能性もあるのではないでしょうか。
A6:　外国人の受け入れに際しては先ずは水際対策を担っている入国管理局が審査している。疑わしい人物については、経産省から調査依頼が来るので誠実に対応している。巧みな虚偽の申請であれば見抜けないことも有るかもしれない。一方、研究者・学生は2〜3年滞在するため、担当教員はその人物の人となりを見抜けるチャンスは多い。その人物の日ごろの振る舞いを観察することで悪意の有無を判別できると考えている。しかし、本当のスパイであれば担当教員も偽りを見抜けず、取引を承認してしまうかもしれない。

Q7:　技術・データ流出を未然に防ぐためのルールに基づく管理の中で、日ごろ感じておられる課題があれば教えていただけますでしょうか。
A7:　安全保障輸出管理に関する先生方の理解と意識が重要であり大前提となる。年に数回教員への講習を開催し啓発に努めている。全教員に輸出管理の重要性を認識していただくことが課題である。毎年調査票を配布し、それぞれの研究室で取り扱う技術についてリストを作成していただき、リスト規制に該当するか否かを確認している。特に、理系の先生にはご注意いただくよう注意喚起している。

Q8:　教員・学生の情報収集等、実際に輸出管理を行う際に難しい点はありますか。
A8:　受け入れ予定の教員や学生の履歴書と輸出管理シートから、軍事機関への就職経験や軍事研究への関与がないか、場合によっては教員、学生の出身機関や他機関に問い合わせて確認しており、情報収集はできている。しかし、輸出管理にかかわる技術は幅広く、東北大学には様々な研究室があるため、輸出管理担当の職員だけでは判断が難しい。そのため、研究室の教員と何度もやり取りをする。また、受け入れ予定の教員や学生を審査する際は、提出された書類が本当に正しいのか、実際のところは分からない。過去には偽の卒業証書が提出された事例もあるが、さらに難しいのは経歴に空白の期間がある場合である。単なるケアレスミスで書かないこともあるが、空白の期間中に何をしていたのかを確認する必要があり、難しい。

Q9： 輸出管理アドバイザーがいらっしゃるとのことでしたが、輸出管理アドバイザーとする基準などはあるのでしょうか？また、アドバイザーに対する教育などはされているのでしょうか。
A9： 部局の方に選考はお任せしているが、一般的に過去に輸出管理に携わったことのある方が行っていることが多いようだ。アドバイザー向けの研修会もやっており、今年度はどこかのタイミングでやりたいと考えている。アドバイザーの方についてもみなし輸出について理解してもらう必要がある。

Q10： みなし輸出に関して、その人が外国から影響を受けているか判断するのは難しいと思います。もっとこうしてもらった方が判断をしやすいなどはありますでしょうか。
A10： 特定類型②について外国政府等に日本の独立行政法人等に相当する公的機関が該当する可能性がある。該当するかどうかについては、経産省の Q&A があるが、その他にはネットで調べるしかない。正直判断が難しいので、こういった機関が該当するということをリストアップして欲しい。あとは大学の判断と言われるのかもしれないが、やはり明確に判断できる方がよい。

Q11： 軍事転用可能かを判断するのは、専門家でないと難しいのではないかと思います。現在のリストで十分だと思いますでしょうか、不足している部分が多いでしょうか。
A11： 十分かどうかは専門家ではないので、判断が難しいが、国において必要に応じた改正が行われていると理解しています。また、審査では単なるリスト該当性のみならず、軍事転用の可能性についても確認が必要と認識しています。軍事転用の可能性については、専門家である先生方に確認することになるが、輸出管理業務を行う事務方が理解しやすい内容にして欲しい。

Q12： 外国ユーザーリスト掲載機関出身者については特に厳しい審査がなされると思いますが、他にどのような点を考慮して審査しているのか教えていただきたいです。
A12： 外国ユーザーリスト掲載機関出身者の審査は厳しく、委員会審査まで行う。本人の経歴に加え、指導教員の経歴も確認する。軍事研究に関わった経験や、指導教員の研究内容、帰国後に外国ユーザーリスト掲載機関に戻るか否か等を調べる。また、大学が提供する技術が懸念事項に合致しないかを確認することも重要である。

Q13： 仮に手続き上の抜け穴を見つけて潜り抜けるとすれば、どの部分が脆弱点となり得るでしょうか。
A13： 大学のオープン性が脆弱点となる。企業においては情報セキュリティ管理が厳しく行われ、入退出も厳しく管理されている。しかし、大学の場合、隣の研究室にも気軽に出入りでき、企業と比べればセキュリティは甘い。

Q14： 学内講習会の資料にヒヤリハット事例の中で実は軍事関係者であったことが後から分かったとの事例があったかと思います。どうすればこういったヒヤリハットを防ぐことが出来たでしょうか。
A14： このヒヤリハットは履歴の確認を徹底するようになったきっかけである。現在は、履歴書等による経歴（空白期間も含めて）の確認を必ず実施するようにしている。

以上

記録作成担当者：稲田凜香

ヒアリング調査報告No.3 基本情報

日時	2022年6月17日
テーマ	経済安全保障
ヒアリング先 (担当者)	日本電信電話株式会社　経営企画部門 荒巻様
場所	質問表を送付の上、メールでのご回答を得た
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 織田秀夫 (計2名)
調査目的	経済安全保障推進法案の可決成立を踏まえた施策の取り組み状況及び今後の見通しについてお聴きすること。

【質疑応答】

1.基幹インフラ役務の安定的な提供の確保に関する制度について

Q1-1：　御社の通信ネットワークへのサイバー攻撃に対する取り組みの現状、および本法律が施行されることにより必要となる追加的措置についてお聞かせください。

A1-1：　サイバー攻撃に対する主な取り組みは次のとおり。

・調達する通信設備のサプライヤーに対して、弊社が納入するハードウェアおよびソフトウェアにおいて悪意をもった改変がされないように要請。

・弊社のネットワークと外部のネットワークを接続するポイント等において、UTM(Unified Threat Management)などにより攻撃を防御。

・24時間、365日、ネットワークのセキュリティ情報を常時監視し、インシデントが発生した場合には速やかに回復措置をとるとともに、原因究明のうえ再発防止を図る。

・セキュリティに関する最新動向の把握、対応する人材の育成。

なお、本法律が施行されることにより必要となる追加的措置については、具体的な法律の運用条件が明確となっていないため、現時点では特に無い。

Q1-2：　本法律が施行されることで、御社が懸念している課題についてお聞かせください。

A1-2：　政府による審査手続きが加わることにより、タイムリーなお客様への通信サービス提供に影響を与えないようにしたいと考えている。

Q1-3：　今後、政令・省令等で具体的な内容が規定されますが、制度設計において配慮が必要な事項について、ご意見をお聞かせください。

A1-3：　重要な設備の定義・範囲については、通信事業者に過度な負担がかからないよう配慮いただきたい。部品レベルの情報収集の在り方については、通信事業者は必要に応じて完成品メーカーに対して情報収集の依頼を出すと想定しているが、完成品メーカーよりも上流（先）にあたる２次以降メーカーの部品に関する情報については、完成品メーカーから回答を得られる保証は無い。

Q1-4：　現行の電気通信事業法では一定の条件を満たせば、外国企業であっても日本国内での電気通信事業への参入が可能です。仮に諜報活動やサイバー攻撃の使命を負った者が電気通信事業に参入した場合、その事業者が保有する通信設備と御社の通信設備を相互に接続することにより生じるリスクついてご意見をお聞かせください。

A1-4：　ネットワークは従来からグローバルで様々な事業者の設備が相互接続されている。仮に悪意をもった事業者が存在し、彼らの通信設備が新たにネットワークに接

続されたとしても、これまでと同様なサイバー攻撃を受けるリスクがあると考えている。（直接接続する場合と間接的に接続する場合でリスクに特段の差分は無い）

Q1-5：　本法律では国が重要設備の審査を行うこととしています。審査する側にも電気通信技術に関する相当の知見が必要と考えますが、御社としてはどのような審査体制が望ましいと考えるか、ご意見をお聞かせください。
A1-5：　ご指摘のとおり電気通信技術に関する相当の知見が必要と考えますが、審査体制については政府にて検討、整備いただく事項であり、意見等は無い。

2.重要物資の安定的な供給の確保に関する制度について
Q2-1：　2010 年の尖閣諸島事件を契機に中国がレアアースの対日輸出を事実上停止した時のように、他国が経済力を用いて我が国に要求をのませるような手段を取った場合、サプライチェーンは混乱し通信サービス等役務に必要な資材の調達にも影響が生じることが想定されます。そのような事態を回避するために、サプライチェーンにおいて御社はどのような対策を取られているかお聞かせください。
A2-1：　他国が経済力を用いて日本に要求をのませるような手段をとった場合に限らず、サプライチェーンにおけるサステナビリティを実現していくために、「弊社グループサプライチェーンサステナビリティ推進ガイドライン」を制定・公表し、サプライヤーの皆様に以下を要請している。
『Ⅶ　事業継続計画の策定
・大規模自然災害（地震、津波、洪水、豪雨、豪雪、竜巻）及びそれに伴う停電・断水・交通障害など、事故（火災、爆発）、広域伝染病・感染症などの疫病蔓延、テロ・暴動、サイバー攻撃、原材料や部品等の著しい需給バランス変化といった事業継続に大きな影響を及ぼす事態に備え、適切な準備を行い、いち早く生産活動を再開し、サプライチェーンへの影響を最小限に留めるように努めること。』
　また、サプライヤーへの要請だけでなく、弊社が調達するサプライヤーを複数に分散する対策についても一部の設備等で実施している。

Q2-2：　価値観を共有する国から調達している資材であっても、周辺有事等の際は物流が停止する可能性は否めません。そのような場合における御社としての資材調達の考え方についてお聞かせください。
A2-2：　上記と同じ。

Q2-3：　安全保障上の理由から、米国は同盟国である日本に対して、同等の対中輸出入管理を求めてくることは容易に想定されます。我が国がそのような要求を受けた場合の御社としての資材調達の考え方についてお聞かせください。
A2-3：　米国政府が直接弊社の資材調達に何らかの対応を求めてくることはないと考えています。弊社としては、米国（に限らず、日本も含めて世界各国ですが）の安全保障に関する法律の動向や運用を常に注視し、適宜、法律を遵守していく考え。

Q2-4：　制度設計において配慮が必要な事項について、ご意見をお聞かせください。
A2-4：　特に無い。

3.先端的な重要技術の開発支援に関する制度について
Q3-1：　具体的にどのような支援が望ましいかご意見をお聞かせください。
A3-1：　開発分野や内容にもよるため、現段階ではお答えできない。

Q3-2：　懸念される事項について、ご意見をお聞かせください。

A3-2：　同上。

4.特許出願非公開に関する制度について

Q4-1：　本制度は御社にとっては不利益になるとお考えですか？また、それはどんな場合が想定されるかご意見をお聞かせください。

A4-1：　本制度における保全対象となる技術は、核技術や先進武器技術等、国家や国民の安全を損なう事態を生じる恐れが大きい発明が含まれ得る分野の技術とされている。弊社では、これらを目的とした研究開発を行っておらず、現時点においては本制度が弊社の不利益になるかどうかは不明である。

Q4-2：　企業に不利益を生じさせないためには出願技術等の価値に見合う十分な補償が必要となりますが、その価値を計るにはどのような手法が望ましいかご意見をお聞かせください。

A4-2：　A4-1 での回答のとおり、弊社と本制度の関係性が不透明であるので、現時点で補償の考え方に言及することは難しい。しかしながら、一般論で考えると、権利消滅までの遺失利益や技術（特許）の貢献度が客観的かつ公正に評価/算定されるしくみづくりが肝要となるのではないかと考える。

Q4-3：　この制度が導入されることによる新たな技術開発モチベーションへの影響についてご意見をお聞かせください。

A4-3：　現時点では本制度におけるデュアルユース技術の扱い/考え方がクリアになっていないと認識している。今後、デュアルユース技術への適用も増大するとなった場合、本来の研究開発目的からは推測もできない用途において企業が意図せず保全されるケースも想定されるのではないかとの懸念はある。このような場合、当該技術の活用による弊社のビジネス戦略等に大きな影響を及ぼすことも考えられることから、関連技術に対する新たな技術開発モチベーションへの影響が多少なりとも生じるのではないかと考える。

Q4-4：　新たな技術開発モチベーションを低下させないためには、どのような制度設計上の配慮が望ましいと考えるかご意見をお聞かせください。

A4-4：　企業が意図せず保全された場合においても、当初目的での実施を認めるもしくは、補償の範囲を拡大する等の配慮が必要になってくるのではないか。

以上

記録作成担当者：織田秀夫

ヒアリング調査報告 No.4 基本情報

日時	2022 年 7 月 6 日
テーマ	経済安全保障における経済産業省の役割、現行制度について
ヒアリング先 (担当者)	経済産業省 貿易経済協力局 貿易管理部 安全保障貿易管理課 課長補佐 末藤尚希 様 課長補佐 坪井祐子 様
場所	経済産業省総合庁舎別館会議室
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凛香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 9 名)
調査目的	経済産業省における我が国の経済安全保障について、専門知識を有する職員にヒアリングをすることで理解を深めること。

【質疑応答】

Q1： 相手国のエコノミックステイトクラフトにより、特定業種の企業業績が悪化し、経営が立ち行なくなるケースもあると思います。このような場合にはどのような救済策が存在するのでしょうか。

A1： 何をもってエコノミックステイトクラフトと定義するのかは難しい課題。例えば、伝統的には市場歪曲的な産業補助金を以てダンピングされ、日本の産業基盤が損なわれる場合には、アンチダンピング、関税措置で対抗手段打つということも１つの手段。近年、様々な国際フォーラムでも情報共有の在り方や同志国による連携について議論がなされている。対抗策と救済策を整理して考える必要がある。

Q2：　今後リスクヘッジのためにも天然資源の調達先を友好国・有志国といったグループに限定するといったことも考えられるでしょうか。

A2：　サプライチェーンをレジリエントなものとするために、調達先を多元化し、同志国の中で確保していく発想自体はその通りだと思うが、天然資源については、地理的に偏在していることも多く、必ずしも同志国のみで必要な資源をまかなうことが困難な面があるという現実に、しっかり目を向け、そうした中で有効な対策を講じないといけない。

Q3：　WTOなどの国際的枠組みが重要であるものの、国際基準を守らない国への制裁等に関して、既存の枠組みの弱さが露呈しているように感じています。このような状況の中、新たに機関を作るべきなのか、それとも今ある機関を強めていくべきなのか。どのように国際協調を進めていけばよいか、教えていただければ幸いです。

A3：　マルチの枠組みには限界があるにしろ、既存の枠組みを直ちに放棄して新たなものを作ることが、真に合理的なアプローチかどうか、よく考える必要がある。既存の枠組みを機能不全と断じることによって、むしろ相手方から、その枠組みを壊したのはこちらだとの非難を受けるような事態は避けないといけない。どの枠組みについて論じるのかにもよるが、価値観を共有する国かどうかも、必ずしも固定されているわけではなく、流動的に変化する。それぞれの問題に応じて、実効的・機動的な補完的な取り組みを行うことが大事だ。

以上

記録作成担当者：岡本 樹

ヒアリング調査報告 No.5 基本情報

日時	2022 年 7 月 6 日
テーマ	経済安全保障における外務省の役割、中国・台湾の現状について
ヒアリング先 (担当者)	外務省 アジア大洋州局 中国・モンゴル第一課兼中国モンゴル第二課 台湾政策総括官 柿澤未知 様
場所	外務省会議室
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 9 名)
調査目的	台湾の経済安全保障体制がどのように行われているのかを理解すること。

(写真)

【レクチャー】

日台関係を中心に脆弱性がどこにあるかについて。日本の経済安全保障の考え方である戦略的自律性と戦略的不可欠性に台湾をあてはめた場合を考察する。戦略的自律性の部分につき、台湾は唯一の仮想敵国である中国に大きく依存している現状があり、そこでいかに中国への依存を減らして行くのかが重要であると考えられている。その意味で台湾にとって中国は極めて特殊な存在であり、経済安全保障の体制構築にかなり力を入れている。特に台湾はサプライチェーンの強靭化に注力しており、中国に対する累積投資額は中国以外の国への投資金額と比較して多いが、東南アジアへの投資により多元化を図ろうとしている。

戦略的不可欠性の部分については、科学技術分野において、戦略的技術を外に出してしまわないということを重要視している。

なお、輸出分野では、大陸への輸入を止められるという事例が起きており、これが中国の経済的威圧の典型的パターンである。さらにエネルギー分野については外国からの輸入に頼ってしまっているという現状もある。台湾の株式市場は政治にかなり影響を受けるため、台湾有事は台湾経済にまさに致命的な影響を与える可能性がある。

1980 年代から半導体分野に力を入れた点はよかった。しかしながら、今後新たな分野が必要になってくると考えられる。そして、台湾にとって重要なのは人材育成の分野であり、これは戦略的不可欠性に関わってくる部分である。

【質疑応答】

Q1： 台湾の経済安全保障を知るためにはどのようなところにお話を聞くとよいでしょうか。

A1： 大陸委員会は比較的オープンである。また、行政院情報セキュリティ弁公室という NISC のような組織がある。研究機関では、中華経済研究院と台湾経済研究院（シンクタンク）が比較的アクセスしやすくヒアリング先の候補となるのではないか。

Q2： 台湾と我が国が経済安全保障面で連携するとすれば半導体サプライチェーン以外にはどのような場面が可能だと考えられるでしょうか。

A2： 台湾は半導体だけでなく、人材が豊富であり、理系の人材も多く日本へと来てもらうのもいいのではないか。そして高度人材として育成をし、さらに活躍してもらうのもいいと考える。日本人が台湾へ留学し、能力を吸収するといったことも考えられる。

Q3： 台湾の経済安全保障施策の特徴はどのようなものがあるのでしょうか。

A3： 中国という単一の仮想敵国があることや仮想敵国であることを名指ししているということがまず特徴である。中国と台湾の間では 90 年代まで公式な経済往来はなかったが、徐々に制限の緩和を行った。特にその傾向が進んだのが、2016 年から 2018 年の頃だった。これに対して、蔡英文政権は中国による不当な技術窃取・人材引き抜き防止策を強化し、台湾や東南アジアへの投資の多元化を図っている。

Q4： 台湾統一は中国にとって「核心的利益」と位置づけられているとのことですが、中国はウクライナの戦況を自分事に置き換えて分析していると言われています。中国はロシアのウクライナ侵略をどのように分析し、武力による現状変更が困難と判断した場合には、エコノミック・ステイトクラフトとしてどのような方策を台湾に行う可能性があると考えられますか、外務省の見解をお聞かせいただければと思います。

A4： 台湾とウクライナの問題は本質的に違う。中国は台湾に対して、まず、エコノミック・ステイトクラフトを用いることが想定される。それがうまくいかない場合に、最終手段として武力行使が行われるのではないかと考える。武力を行使した後にエコノミック・ステイトクラフトを行うわけではない。また、エコノミック・ステイトクラフトの可能性として、金門島への水の供給停止等も考えられる。

Q5： 台湾は中国のエコノミック・ステイトクラフトに対してどのような方針で対応することとしていますか。

A5： 蔡英文政権は、投資や貿易の対中依存を減らしていこうとしている。中国に投資してきた企業の資本を台湾に回帰投資させるかが重要であり、東南アジア、南アジアへの投資を促進することによって中国依存を相対的に低下させていこうとしている。

Q6： 台湾の経済構造から対中国で脆弱性を持っている分野はどこでしょうか。それに対して台湾はどのような対策を講じようとしていますか。
A6： 台湾にとっての仮想敵国は中国であるが、台湾は中国からの巨額な貿易黒字で成り立っており、切っても切れない関係となってしまっている。中国への投資を減らす等を行うことによって中国への相対的依存を低下させていると考えられる。

Q7： 過去に台湾に対して中国がエコノミック・ステイトクラフトを行ったもので、台湾に最も大きな影響を与えたものはどのような事案でしょうか。また、それを法制度の創設や既存制度の運用改善等はありましたでしょうか。さらに、そのことについて賛成派・反対派で激しい議論が行われたといったことはありましたでしょうか。
A7： 馬英九政権では観光が活発化していたが、2016 年の蔡英文政権になってから、中国は台湾への観光渡航に一定の制限をかけるようになった。このことから、民進党政権の発足によって観光の流れが止まってしまったとのイメージが台湾で広がり、これも 2018 年統一選挙で民進党が惨敗する要因の一つとなった。台湾は新型コロナの影響を受けて、観光目的の入境に厳しい制限を加えており、今後はゼロコロナ政策を行う中でいかに門戸の解放をするかが重要となる。

Q8： 経済安全保障という観点から台湾と協調関係を築く場合、我が国から見たメリット、台湾からメリットはどのようなものがありますでしょうか。また、逆にデメリットはありますでしょうか。
A8： メリットについては、個別分野によって状況は全く異なる。デメリットとして言えるのは、台湾のおかれている不安定さ、民間企業がリスクを考えた際に投資することを躊躇する可能性がある。

Q9： 半導体での協業が契機となり、今後日本と台湾で先端技術の共同開発や人材交流を他の分野でも実施・拡大していくことは考えうるでしょうか。
A9： 現在は半導体に集中している。九州では、九州経済局、九州大学、熊本大学等がコンソーシアムを組んで半導体人材の育成に取り組んでいる。資源を持っている国ではないので強みをどう作っていくかが重要であり、AI や EV といった分野を強みとしていくことが考えられる。

Q10： 台湾が日本以外の国で経済安全保障の観点から重要視している国はどこになりますか。そうした国はどのような特徴がある国ですか。
A10： 一般的にはアメリカは台湾にとって大きな存在感がある。安全保障全般におけるアメリカの影響力は大きく、台湾としても地域的経済連携の枠組みへの参加を強く希求しているが、インド太平洋経済枠組み（IPEF）にはアメリカから声がかからなかった。そのことから、台湾はアメリカとのバイの包括的経済・貿易協定の提携を追求している。また、GCTF という日台米の枠組みがあるが、この枠組みで行われるワークショップ、セミナー等には、経済安全保障分野のものも多く含まれている。

Q11： 中国の企業が台湾から半導体の技術を違法な形で獲得する動きについては投資を禁じるなどの施策を講じているようですが、他に講じている施策はありますでしょうか。また、台湾が先端技術を防衛するために検討している施策などはありますでしょうか。
A11： 大陸地区人民来台投資許可弁法の第 8 条において、中国からの投資を禁じることが出来るようになっている。

Q12： 台湾は経済インテリジェンスをどのような法制度・体制で実施しているのでしょ

うか。また、その特徴はどのようなものでしょうか。
A12： 国家安全法や経済安全保障を脅かす行為を刑法典に規定している。そして、両岸人民関係条例等基本法の下に細かい法律が多くある。

（追加質問）
Q13： 日本はサイバーセキュリティの部分が脆弱であるとかんじていますが、ビジネスと融合することによって改善を図ることが出来るのではないかと考えています。そこで、台湾ではそういったことが行われているのか、そして日本が取り入れることが出来ることはあるのでしょうか。
A13： トレンドマイクロという会社があり、これは台湾で作られた会社である。スタートアップ事業という形でこういった会社と組んで行っているという事例はあるが、ビジネスとして成功しているかを判断するにはまだ年月が必要だろう。

Q14： 台湾では若者が多く活気がある印象を受けています。日本は台湾ほど若者に活気がない印象を受けていますが、台湾は若者が引っ張っているのでしょうか。
A14： 台湾は日本に次いで、少子高齢化が進んでいる。しかし、社会の中核を 30 代から 40 代が担っているのが特徴である。しかし、半導体や IT といった分野でワンマン経営が多いことから次の経営へどうつなげていくのかという課題がある。また、台湾の若者に活気がある理由としては政治的エンゲージメントと危機感があることがあげられる。しかし、政治的な自信を失った時は弱りやすく、その際に大陸へと流れてしまうことがある。

Q15： TSMC やジェラの他に民間企業の動向が関係するもので、有名なものや今後調べておくべきものはあるのでしょうか。
A15： シャープの買収やパナソニックの買収等、日本の企業を買収し再生するということを行っている。台湾が日本企業を買収する事例だけでなく、日本が台湾の重要インフラ建設に投資を行っている事業もある。台湾の洋上風力発電事業に投資を行っており、これは日立が関係しており、政府もサポートをしている。過去には台湾新幹線の例がある。これは日本の技術が活かされた事例でありこうした事例を増やしていくのがいいのではないかと考える。

Q16： テレビ等のエンタメ業界がチャイナマネーに依存をしているように感じられます。日本のテレビの場合、株式の外国保有率に制限があるが台湾ではそのような制限はないのでしょうか。
A16： 多くの規制がある。中国人がコントロールしている場合には規制がかかる等、日本と比較してもより厳しい規制がかけられている。しかしながら、ショービジネスの全てが中国から抜け出すのは難しい。

Q17： 台湾は戦略的不可欠性をどのように見つけて注視していくことになったのでしょうか。
A17： 李登輝の時代に次の成長産業を何にするかが検討され、成長させる産業が絞られた。一番力をつけていきたい分野については、まず政府が会社を作り、政府が投資し成長させた上でスピンアウトをした。TSMC などの EMC、OEM のリーディングカンパニーが生まれるなど、柔軟性とスピード感を持ってビジネスモデルを作ることに成功している。これは自社ブランドを持たないことで、顧客のニーズにスピーディかつ柔軟に対応できるようにしたからこそうまくいったビジネスモデルである。

Q18： 台湾と日本が関係してくるのは人材交流の部分であると考えています。そうした

部分を進めていく上で、課題はどんなことがあげられるでしょうか。また、日本人研究者が出て行ってしまうことや機微技術等の流出をどのように保護していくべきでしょうか。

A18：　日本の教育機関でどれだけ魅力的な環境を作ることが出来るかが大切である。１点目として金銭面があげられる。しっかりした研究を行うことが出来るだけのお金があるかが重要である。２点目として言語があげられる。英語を共通言語として研究を進められるかが重要である。また、台湾の人材だからセキュリティの面で必ずしも安心できるというわけではない。しかし、外国人にはある程度の規則や覚書等の対応をしており一定の担保は出来ているはずである。そのため、日本の技術が流出するというよりは日台の交流を進める形になるのではないかと考えている。

Q19：　法律の改正や修正については誰が主導していたのでしょうか。

A19：　法律によって異なり、議会での議員による質疑が発端となる場合もあれば、世論の流れによって法令改正等へと繋がったという事例もある。

Q20：　中国の人材が台湾へ渡り、その後中国へと戻るという可能性もあるがそれについてはどう考えられるでしょうか。

A20：　リスクについてはどこにでもあり、中国が得ようとしているものは多くある。日本と比較すると台湾の方が必要な対策は行われている。むしろ、日本の対策の方が不足していると台湾側から不安視されている。したがって、台湾企業・台湾人と協業することのリスクを過度に強調する必要はないが、台湾の労働賃金が伸び悩む一方、中国企業から圧倒的に優れた待遇が示される等、台湾企業にも中国の引き抜きに弱い部分が存在しているのは確かである。

Q21：　反浸透法とは何でしょうか。

A21：　与党・民進党が提案して立法した法律であり、中国からの政治的な浸透の防止策である。海外の敵対団体等を列挙しており、何らかの指示委託を行うことによって選挙等に影響が与えられることを防ぐことを目的としている。

Q22：　台湾は外交関係を有している所が少ないが、どのようにして情報を集めているのか。

A22：　サイバーセキュリティの国際枠組み等、台湾が参加出来ていないものは存在する。また、そうした場に入りたいと思っていたとしても、入ることは難しい。しかしながら、アメリカとの関係はかなり緊密であり、サイバー演習についても米台が一緒に行うなどしている。

以上

記録作成担当者：山田麻友

ヒアリング調査報告 No.6 基本情報

日時	2022 年 7 月 7 日
テーマ	経済安全保障施策及び経済安全保障推進法の概要について
ヒアリング先 (担当者)	内閣官房 国家安全保障局 経済班 担当職員　2　名
場所	国家安全保障局会議室
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友　(計 9 名)
調査目的	経済安全保障法の立法事実やその施策に関する具体的な方向性について理解を深めること。

【レクチャー】

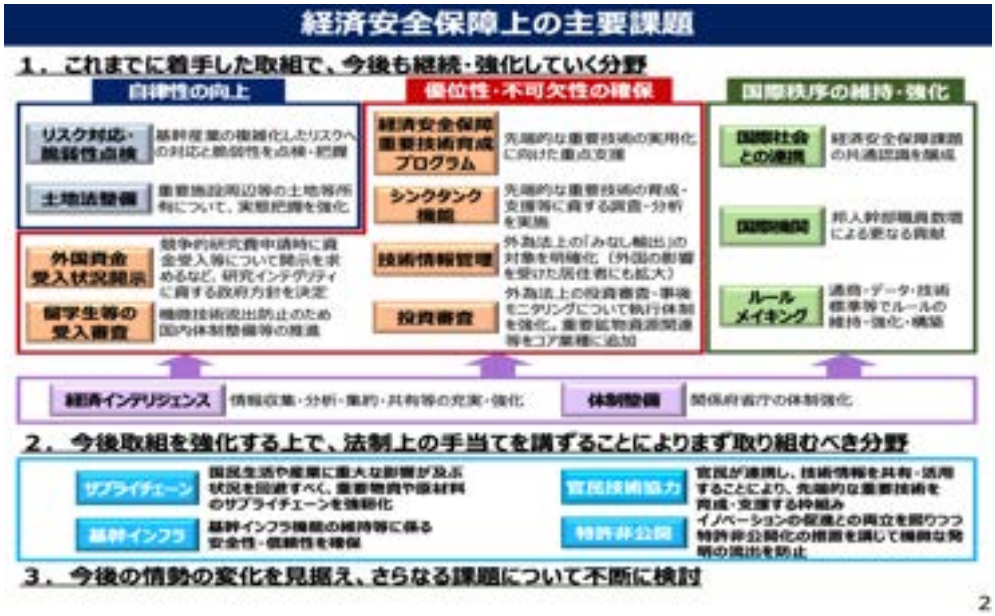
(内閣官房担当者発言)

小林大臣の下、2021 年 11 月経済安全保障推進会議(閣僚級)が行われている。この問題は一つの省庁で進めていくのが難しい。経済安全保障の裾野が広がっている。そのため、大臣がリーダーシップを取る必要がある。岸田総理の指示のもと、取り組むべき課題について、閣僚級の会議で各閣僚が意思疎通を図り、意思統一することとしている。

経済安全保障は岸田政権の最重要課題の一つである。それを受けて経済安全保障推進会議が設置された。下のスライドは経済安全保障の課題についてわかりやすく伝えているので参照して欲しい。

(概要)

資料を踏まえ、それぞれの施策の関係性や体系について国会答弁を踏まえた基礎的な説明を受け、個別施策の担当省庁がどこになるのかなどについてのレクチャーを受けた。



以上

記録作成担当者：香高優一郎

ヒアリング調査報告No.7 基本情報

日時	2022年7月7日
テーマ	重要土地等調査法について
ヒアリング先 (担当者)	内閣府 政策統括官（重要土地担当） 担当者
場所	国家安全保障局会議室
参加者	（WS-C 教授）坪原和洋 教授 （WS-C 学生）稲田凛香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 （計9名）
調査目的	経済安全保障法上重要な位置づけにある重要土地等調査法について理解を深めること。

（担当者発言）

冒頭、担当者から、重要土地等調査法の背景、立法経緯について、大要次のとおり説明を受けた。

近年、我が国の安全保障を取り巻く環境が不確実性を増す中で、外国人や外国法人による土地の取得に対する不安や懸念が広がっている。特に、国境離島や防衛施設周辺等における土地の所有・利用をめぐっては、かねてから、安全保障上の懸念が示されてきた。

こうした状況の中、「国家安全保障戦略」（H25.12.7閣議決定）においては、「国家安全保障の観点から国境離島、防衛施設周辺等における土地所有の状況把握に努め、土地利用等の在り方について検討する」とされ、「海洋基本計画」（H30.5.15閣議決定）においても、国境離島について同様の方針が示された。これらを受け、防衛省は防衛施設に隣接する土地について、内閣府は国境離島の領海基線の近傍の土地について、それぞれ所有状況等の調査を行ったが、これらの調査は登記記録をベースとしており、利用実態等の詳細までは十分に把握できないといった課題があった。

これらの課題に対応するため、「経済財政運営と改革の基本方針2020」（R2.7.17閣議決定）において、「安全保障等の観点から、関係府省による情報収集など土地所有の状況把握に努め、土地利用・管理等の在り方について検討し、所要の措置を講ずる」こととされ、これを受け、内閣官房は令和２年10月に「国土利用の実態把握等に関する有識者会議」を設置し、同会議において、同年12月に「国土利用の実態把握等のための新たな法制度の在り方について　提言」（以下「有識者会議提言」という。）が取りまとめられた。有識者会議提言を踏まえ、内閣から重要施設周辺及び国境離島等における土地等の利用状況の調査及び利用の規制等に関する法律案が第204回国会に提出され、同年６月16日に成立、同月23日に令和３年法律第84号として公布された。

（質疑応答）

引き続き、提供を受けた資料や国会答弁等に基づき、基礎的な説明を受け、法の目的、規制の内容や実効性、地方公共団体との関係、立法作業時の苦労等について質疑応答を行った。

以上

記録作成担当者：宮内拓

ヒアリング調査報告No.8 基本情報

日時	2022年7月7日
テーマ	警察庁における経済安全保障推進法について
ヒアリング先 (担当者)	警察庁 サイバー情報参事官室 奥寺 様
場所	中央合同庁舎2号館B1会議室
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計9名)
調査目的	経済安全保障法の立法事実やその施策に関する具体的な方向性について理解を深めること。

【質疑応答】

Q1： サイバー情報参事官室では経済安全保障に関連してどのような施策を講じておられるかの概要を教えてください。

A1： サイバー攻撃対策の一つとして、情報窃取の標的となるおそれの高い先端技術を有する事業者等との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う「サイバーインテリジェンス情報共有ネットワーク」を従来から構築しており、経済安全保障との関係ではこの枠組みを更に活性化させることが重要となっている。

Q2： 政府・企業に対する近年の情報窃取・システム破壊目的のサイバー攻撃について、警察としてはどのような脅威があると考えていますでしょうか。

A2： サイバー空間の公共空間化が進展することで、サイバー空間上の情報窃取、システムの妨害・破壊は社会的な混乱をもたらすものとなっている。特に、代替することが困難であり、国民の生活及び社会経済活動の基盤となっている重要インフラへのシステム破壊を目的とするサイバーテロや、我が国の国際競争力を担保する先端技術情報の窃取等を目的とするサイバーインテリジェンス等の脅威があるものと考えている。

Q3： 現在のトレンドとなっている攻撃手法についてご教示ください。これに対して政府・企業はどのように対処するべきでしょうか。

A3： 警察庁のHP等で公表されているもののほか、セキュリティ対策をとっている事業者等への直接の攻撃を避け、国外関連会社や子会社、サプライチェーンの一角を担っている中小企業等の比較的セキュリティが弱い対象を攻撃するものもある。また、ランサムウェアの様な挙動を装うことで、金銭目的の攻撃と誤認させ、実際の目的はシステムの破壊、情報の窃取であるようなケースも増えているとの分析もある。政府・企業は本社や基幹システムだけでなく、海外支社、子会社、関連会社、事務系システム等、正常な業務を遂行するのに必要なシステム全体のセキュリティ対策が必要である。加えて職員のリテラシーの向上を図るなどの施策が求められる。

Q4： 国が能動的に企業等のサイバーセキュリティの状態を監視し、欠陥等がある場合には改善指導や、改善勧告などを行う仕組みはありますでしょうか。

A4： 内閣サイバーセキュリティセンターにおいて、「重要インフラのサイバーセキュリティに係る行動計画」を策定し、重要インフラ事業者の必要な取組を後押ししているが、国が主体的・能動的に監視・是正指導を行うものではない。KDDIのインシデントに見られるように、各業界の業務を遂行する上での必要な対策はその業界を所管する

省庁が所管する法律に基づいて指導していくこととなる。

Q5：　日本を代表する大企業の多くが、サイバーセキュリティ対策が不十分であるいうことが、日本経済新聞　電子版「大企業のサイバー対策、4割に危険性　車や機械目立つ」（2022年6月5日）で報じられていました。日経２２５のうち４割は落第点とのことです。企業のサイバーセキュリティは企業側の努力に委ねられていますが、国が国内企業のサイバーセキュリティが確保されているかどうかについて、インターネット上をAIプログラムによりパトロールし、改善指導を行うことができるような仕組みを作りについて研究したいと思っております。パトカーによる警察の巡視・防犯指導と同じように、公的機関がAIロボット等を使ってサイバー空間を巡視し必要に応じて企業を指導するような仕組みを考えているのですが、警察において実際に訪問指導をすることなどを含めて既に類似の仕組みなどはありますでしょうか。

A5：　今のところそういう仕組みは存在していない。警察における類似の取り組みとして、都道府県警察と管内の重要インフラ事業者等で構成する「サイバーテロ対策協議会」が挙げられる。この枠組みを通じて、警察は事業者等に対して訪問指導やセキュリティ脅威の情勢、セキュリティに関する指導、共同対処訓練等を実施している。

Q6：　こうした取組を警察庁や都道府県警察が行うと仮定した場合、どのような点が問題になる可能性がありますでしょうか。

A6：　第一に、パトロールの態様にもよるが、こうした取組は外形的には不正アクセスに該当しうるため、不正アクセス禁止法の処罰対象とならないような制度作りが必要である。また、企業等のシステムから送受信される通信をチェックするのであれば、憲法上の通信の秘密を侵すものと考えられるため、それを回避するような制度設計をしなければならない。第二に、インターネットは国境のない空間であるため、どこまでを活動の対象とするかが問題となる。国外にある国内企業も対象とするのか、拠点が国内にあるが外国にサーバーがある場合にはどうするのか、相手国との関係も考慮していかなければならなくなる。第三に、このような取り組みを行って企業等に改善指導を行ったとしても企業等がその指導に従ってセキュリティ対策を強化するとは限らず、また、企業の運用するシステムの機能上、対策がとれないケース等も考えられる。

Q7：　国が能動的に企業等のセキュリティの状態について、監査・改善指導などを行う制度は存在するのでしょうか。そうした制度に警察がかかわることはあり得るのでしょうか。

A7：　各業界の業務を遂行する上での必要な対策はその業界を所管する省庁が所管する法律に基づいて指導していくこととなるが、サイバーセキュリティの観点から横断的にそのような指導を行う仕組みは現時点でない。なお、原子力発電所への指導に関しては、サイバーセキュリティも含めて警察庁も関与しており、必要な助言を行っている。

Q8：　警察においては、サイバー人材の育成や人材確保がより重要になってくると考えられますがどのような対策をとられていますでしょうか。

A8：　サイバー事案への対処においては、人材の育成は極めて重要である。職員の技能レベルに応じた学校教養、能力検定、民間企業への派遣研修等を実施しながら、人材の育成に努めている。民間の知見の活用について言えば、都道府県警察でＩＴ企業経験者の登用を行っているほか、民間企業や大学等の研究機関と解析技術の共同研究を行うことなどにより、民間の知見、技術を取り入れながら、捜査に必要な技術力の強化を行っている。捜査の保秘という観点から、広く外部人材を登用することが難しい業

務もあるが、今後もこうした取組を進めるとともに、必要な検討を行っていきたい。

Q9： 各国の基幹インフラ等に関するサイバーセキュリティの確保のあり方やサイバー攻撃対策について、調査・研究等は行っていますでしょうか。行っているとすれば、その内容について情報共有していただくことは可能でしょうか。

A9： 海外では、例えば、米国における「The Cyber Incident Reporting for Critical Infrastructure Act of 2022（CIRCIA2022）」のように、重要インフラ事業者等にサイバー攻撃被害の報告の義務付けが制度化されているものもあると承知している。また、サイバー空間における捜査権限も各国において異なっているところ、こうした諸外国の制度を研究することは有益であり、業務で必要な範囲で行っている。内閣サイバーセキュリティセンターのHPには調査研究がアップされていることから参照されたい。

Q10： 現在、民間企業もサイバーセキュリティ強化に向けて動いているのではないかと思います。民間企業が今後対策をしていく上で特に気を付けるべきところは何かありますでしょうか。

A10： あくまで私見であるが、サイバー空間は変化が激しく、新たな技術が台頭してくるため、一度の対策で過信せずに常に対策をアップデートし続けていくことに加え、組織としての対策の持続性を確保するために、人員や予算の配分に関する理解が不可欠となると考えられる。

Q11： サイバー攻撃に関する予防策や対処、その後の対応を含めて会社の経営者層の姿勢が大きな影響を与えるものと考えられます。経営者層に適切に響くような広報・指導を行うためにはどのような工夫が必要と考えられますか。

A11： サイバー空間をめぐる脅威は深刻であり、サイバー攻撃の被害に遭う可能性があることを組織のトップ自らが十分に認識する必要がある。また、一度被害に遭えば、事業の停止のみならず広報や原因究明、ひいてはレピュテーションリスクいった対応に組織としての体力が奪われることになることを、過去に被害に遭っている企業の例を踏まえて十分に認識する必要がある。

Q12： サイバーパトロールのような警察やボランティアによる情報収集は、プライバシー権や電気通信事業法等との関連に配慮して行われているものと承知していますが、現状の課題や限界について教えてください。

A12： サイバー攻撃を警察が認知・把握するのは、①被害企業等からの通報・相談、②リアルタイム検知ネットワークシステムによるパケットの検知、③リークサイト等の情報であるが、いずれも攻撃発生後の時点に限られており、攻撃を行おうとしている事前準備の段階での把握は困難。この点、その予兆も含めて広く情報収集を行おうとすると、不正アクセスや通信の秘密との関係が課題となってくる。

Q13： 警察がサイバー攻撃のアトリビューションとそれを公表することにより、それが行われた国家の行動変容は期待できるのでしょうか。我が国でもJAXAへのサイバー攻撃に関してパブリック・アトリビューションを行ったと承知しており、米・英等の賛同も得られたものと承知していますが、これにより名指しされた国・集団の行動変容は見られたのでしょうか。また、本件についてお話しするのが困難な場合には、他国の例でそのような例をご教示いただけませんでしょうか。

A13： 国家を名指しする行為であるところ、当該国家は関与を否定するとしても、国際社会から非難されることとなり、行動変容は期待される。

Q14：　警察がアトリビューションやサイバー攻撃の関与者を検挙しようと考えた場合、どのような課題がありますでしょうか。他国の例と比較して、法制度や運用における我が国の課題があればご教示いただければ幸いです。
A14：　サイバー攻撃は国境を越えて行われるものであり、捜査も国境を越えた国際捜査とならざるを得ず、捜査に時間を要する上、様々なサーバーを経由している場合には実行者の特定が困難となる。また、国家が関与しているものもあるため、仮に攻撃者を特定したとしても、相手国が引き渡すかどうかといった問題がある。

Q15：　経済安全保障法の施行により警察のサイバー攻撃対策に期待されるものや業務に違いは出てきますでしょうか。
A15：　経済安全保障との関係では、サイバーインテリジェンス情報共有ネットワークを更に活性化させることが重要となっている。

Q16：　警察が民間企業のサイバーセキュリティを向上させるための様々な取組を行っているものと承知していますが、経済安全保障の観点から更に高度な取組が求められると考えられます。今後の施策の方向性についてご教示いただければ幸いです。
A16：　経済安全保障との関係では、サイバーインテリジェンス情報共有ネットワークを更に活性化させることが重要となっている。

Q17：　ダークウェブにおけるランサムウェア等の販売を抑止する方法はあるのでしょうか。
A17：　残念ながら取り締まる法律が存在しない。一般論として、ダークウェブ自体を取り締まる法律はないものと承知している。有害・違法なダークウェブ上のサイトが稼働しているサーバーが特定でき、国内に所在するものであるということが明らかになれば、ISP との協力の下、サーバーをテイクダウンすることも考えられる。

Q18：　サプライチェーン経由でシステムの弱点を探してサイバー攻撃を行ってくるケースに対応することも求められていますが、今後、企業が経済安全保障の観点からサプライチェーンをチェックしていく際にどんな点に気をつけたらよいかについて、警察としてアドバイスできることはありますでしょうか。
A18：　セキュリティ対策をとっている事業者等への直接の攻撃を避け、国外関連会社や子会社、サプライチェーンの一角を担っている中小企業等の比較的セキュリティが弱い対象を攻撃するものもある。政府・企業は本社や基幹システムだけでなく、海外支社、子会社、関連会社、事務系システム等、正常な業務を遂行するのに必要なシステム全体のセキュリティ対策が必要である。加えて全ての職員のリテラシーの向上を図るなどの施策が求められる。

Q19：　企業に限らず大学の研究室もサイバー攻撃への対策を求められると思いますが、大学に対するサイバー攻撃対策の取り組みはどのようなものが行われているのでしょうか。また、今後の課題にはどのようなものがありますでしょうか。
A19：　高度な研究開発等を実施する大学においてサイバー攻撃による被害が現に発生するなど、大学に対するサイバー攻撃の脅威が高まっているものと認識している。警察が運営する協議会やネットワークを通じた情報共有の推進や情報窃取を企図したサイバー攻撃事案等の発生を想定した共同対処訓練を実施するなど、対処能力の向上を図っている。こうした取組を推進し、被害の未然防止・拡大防止につなげられるよう協力関係を深化させていく必要がある。

（追加質問）

Q20：　Q5 で記述したような、AI プログラムによりパトロールし改善指導・勧告、そして勧告を受けた企業は有価証券報告書に記載義務を課す仕組み作りについて研究したいと思っております。パトカーによる警察の巡視・防犯指導と同じように、公的機関が AI ロボット等を使ってサイバー空間を巡視し必要に応じて企業を指導するような仕組みです。このような仕組みは必要でしょうか。また、実現に向けたご意見を頂くことは可能でしょうか。

A20：　様々なメリットがあると思うが、公的機関によるサイバー空間の巡視は監視社会につながるといった意見も考えられるため、行政の様々な面から慎重な検討が必要である。様々な知見が求められると思うが、警察としても必要に応じて関与していく。

追加補足：　技術的な事項については、サイバーセキュリティの研究センターがあるため、そちらからご意見をもらうことも可能（坪原）

Q21：　サイバーセキュリティにおいて国際連携等で日本が他国に貢献できる部分は何処ですか。また、日本のプレゼンス向上には何が必要でしょうか。

A21：　日本の警察にはテクニカルスタッフが多くおり、その人たちの緻密な解析技術があれば他国にも貢献できる。サイバー攻撃は国境を容易に越えるものであるところ、攻撃の過程も含めた日本国内の痕跡を調べ、証拠を集め、パズルのピースを少しでも多く集めることができれば、サイバー攻撃の攻撃者の特定に役立ち、他国と協働で攻撃者の全体像を描くことに貢献することとなり、日本の警察のプレゼンスも向上する。

Q22：　技術支援とそれを取りまとめる部門があると思うのですが実際に運用されていく中でどのような効果があるのかと改善点についてお聞かせください。

A22：　色々な事案でサイバー攻撃の攻撃者（グループ）を特定しその情報を公表してきた。まずは自分たちの持っている手がかりを調べて他の機関と情報共有しながら当たりを付けていく。課題としては、技術的な解析ができる人員を増強し捜査の手掛かりとなるピースを増やすことだと思っている。

Q23：　重要インフラの情報セキュリティ対策に係る第 4 次行動計画」について重要インフラ 14 分野について、数は同じだが業種は異なっているのはなぜか。

A23：　サイバーセキュリティにおける国民の生活に重大な影響が出るという観点と、経済安保の視点から対象とすべきという観点の違いから生じているものだと認識している。

Q24：　外国捜査機関との連携する際の窓口は都道府県単位で一本化されるのでしょうか。

A24：　外国捜査機関との窓口は警察庁に一本化されている。サイバー警察局を設置した大きな狙いの一つが他国との共同オペレーションへの国としての参画である。

以上

記録作成担当者：織田秀夫

ヒアリング調査報告 No.9 基本情報

日時	2022 年 7 月 12 日
テーマ	経済安全保障について
ヒアリング先 (担当者)	元国家安全保障局長　現北村エコノミックセキュリティ合同会社代表 北村滋 様
場所	オンライン
参加者	(WS-C 教授)坪原和洋 教授、阿南友亮 教授 (WS-C 学生)稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 10 名)
調査目的	日本の経済安全保障の管理体制に関して調査すること。

(ヒアリング内容)

【レクチャー】

1.2.24 ロシアのウクライナ侵攻を契機に、グローバル経済に大きな影響が出ている。株安をはじめ世界経済は調整局面に入った。また、ロシアへの経済制裁が結果として資源価格の上昇につながり、ロシアの輸出額は侵攻前と比較して 10%増と皮肉な結果となっている。EU 各国が輸入を減らした分、インド、トルコなどがロシア資源の受け皿となっていることもあり、ロシア資源の禁輸による経済制裁は結果として効果的には働いていない。逆に、西側諸国はエネルギー価格の上昇に苦しむなど、ロシアによるエコノミックステイトクラフトの効果が出ているようにも見える。

また、黒海航路封鎖によりウクライナの小麦輸出が滞り、世界的な食糧価格の上昇を招いている。そして、エネルギー、食糧価格の上昇が世界経済のインフレを惹起している。バイデン政権のウクライナ問題に対する安全保障政策は必ずしも失敗ではないと考えているが、バイデン政権については、ロシアへの経済制裁によるインフレの進展、銃乱射事件などに見られるように治安の悪化、メキシコからの移民増加などの問題を背景として支持率が低迷しており、国内的基盤は必ずしも盤石ではないように思える。

2.2017 年に始まった米国の対中政策変更が米中対立の大きな節目になった。そして COVID19 を契機として対立がより一層明確となり、先鋭化したように見える。特に先端技術関連製品の内製化、デカップリング化が進んでいる。先般行われた G7 の共同コミュニケ、日米首脳会談の共同声明では同志国の協調を表明している。QUAD において最も重要なのは同志国の連携強化である。共同声明をよく読んでみるとよい。どういう観点で技術や産業を守ろうとしているかが分かる。グローバリゼーションというのは今まさに転機にある。

3.近年、権威主義国からのサイバー攻撃の頻度が増している。ハイブリッド戦という考え方があるが、サイバー空間では平時と戦時の境目が曖昧であり、平時においても実際の空間でやれば武力行使になりかねないことをサイバー領域でやってくるようになっている。当面は、この状態が好転することは考えられないため、重要インフラの基幹システム、ネットワークをサイバー攻撃から十全に防御することが重要である。

また、企業の事業計画も地政学的なリスクを十分に考慮して決定していく必要があるし、国民もそうしたことに関心を持ってもらう必要がある。

4.文芸春秋 5 月号に国家安全保障戦略「三本の矢」の話を書いた。

一つ目は反撃能力についてである。特に、我が国を巡るミサイルギャップは深刻な問題で早急に是正が必要な問題である。北朝鮮、中国のミサイル攻撃に対し日米のミサイル防

衛は必ずしも十分であるとは言えない。そもそもアメリカはロシアと中距離核戦力全廃条約（INF）を締結していたため、中距離ミサイルについて攻撃・防衛ともに十分とは言えない。その間隙を縫うように中国は中距離ミサイル（核戦力）を増強してきた。中国のA2/AD（接近阻止・領域拒否)戦略を採用し、米国の空母打撃群に対応するためにDF21D（対艦弾道ミサイル）の改良を進めるほか、DF26等の核弾頭搭載可能な中距離弾道ミサイルを配備することで我が国やグアム等の米軍基地を射程に入れて、日米の軍事力を抑止しようとしている。当然のことながら、日本は中距離ミサイルの保有はゼロであるのに対し、中国は少なくとも数百発持っている。また、最近開発された北朝鮮の弾道ミサイルは迎撃を困難にするために変則軌道により飛ぶように改良が進められている。こうした状況を踏まえると、我が国は敵基地を攻撃できるミサイルを配備して、こうしたギャップを埋める必要があり、それこそが軍事衝突の抑止力となり得ると考えている。我が国の戦略において、ミサイルの不均衡是正は喫緊の課題である。

二つ目は尖閣諸島問題である。尖閣諸島には連日中国の海警船が進出し日本の海上保安庁の巡視船とにらみ合っている。皆さんは変な意味で慣れてしまっているのかもしれないが、まさに中国の脅威が日常的に顕在化しているわけで、危機的な状況であると認識すべきである。しかも、防衛白書によると、中国の海警船は海軍の軍艦を転用したもので76㎜砲を備え、装甲板も軍艦と同じ構造であるのに対し、日本の海上保安庁の巡視船は35㎜砲しか装備しておらず船体の構造は商船と同じ構造である。万が一、海警船が発砲してきた場合には、海上保安庁の船で対抗することは不可能である。したがって、海上保安庁が自衛隊と事態対処や装備面においてどのように連携していくかを真剣に考えていく必要がある。

三つ目はハイブリッド戦への備えである。プーチン大統領は、本年2月のウクライナ侵略においていわゆる電撃戦（Blitzkrieg）によりウクライナ全土を短期で攻略できると考えていたが失敗した。2014年のウクライナ侵攻・クリミア併合の過程で、ロシアは予めサイバー攻撃を仕掛け、ウクライナ軍に偽の情報を流しておびき寄せ、集中攻撃した。これにより、ロシア軍は1.5万人の兵力で5万人のウクライナ軍に勝利した。このサイバー攻撃そのものは戦争の相当前から準備されており、ハイブリッド戦が、実際の戦争の勝利に繋がった事例である。この成功体験がプーチンの判断を誤らせた可能性がある。今回、2014年のような展開にならなかった理由として、その教訓を活かしてウクライナ側がきちんと防御を固めたということがある。ウクライナのゼレンスキー大統領は、将来のロシアの全面侵攻は不可避と考え、デジタル変革省を設置し、サイバー攻撃に備えていた。アメリカをはじめとする西側諸国は、サイバー防衛の面でウクライナを全面支援した。例えば、米国のサイバーコマンドやEUのサイバー即応部隊がウクライナの基幹インフラを総点検し、ロシアが仕組んだ多数のマルウェアを発見し、それを一掃することで、ウクライナの基幹インフラシステムの脆弱性を排除した。米マイクロソフト等の民間企業も支援を行った。今回のウクライナ戦争では、ウクライナ軍は米国のインテリジェンスの協力を得たが、それによる電子戦によってロシア軍の無線通信システムを無力化させたものと見られる。ロシア軍は商用通信の利用を迫られたことから、ウクライナ軍はロシア軍の指揮中枢の位置同定が容易になり、10名を超すロシア軍の将官を殺害するなどの戦果を挙げている。

5.我が国を取り巻く安全保障環境は大きく変化している。現在の世界最強の海軍はアメリカであるが、艦艇数で言えば中国海軍が世界最大とも言える。中国は３隻（福建、遼寧、山東）の空母を保有するに至っている。そのうち福建は最新技術である電磁カタパルトを装備している。遼寧・山東については、スキージャンプ方式のものしか装備していないため、重い固定翼哨戒機の離着艦が困難であり、搭載機数の関係もあって回転翼機による哨戒によらざるを得ない。そのため蒸気カタパルトによりE-2Dのような重量のある固定翼哨戒を多数運用できる米国の空母打撃群が優位であったが、福建については蒸気カタパル

トよりさらに高度な技術を用いる電磁カタパルトを装備（米軍もジェラルド・フォード級で採用。）することにより多数の固定翼機の運用が可能となり、哨戒範囲が広がる。これにより、中国軍はA2/ADをより効果的に実施できるようになり、我が国の安全保障上の脅威が更に増すことになる。我が国の安全保障の観点からは、日米同盟を通じて、中国軍の第二列島線（日本から小笠原諸島、グアムを結んだ線）への進出を押しとどめることが重要となる。

なお、南シナ海の状況は、東シナ海より深刻である。中国は一方的に設定した九段線を根拠にして南沙諸島の7つの地形に3000m級の軍用滑走路を備えた３つの基地を建設し、他の4礁を軍事化した。これを阻止できなかったことは、米国の戦略上の大きなミスである。

6.台湾海峡については、2019年1月に習近平は、北京で台湾問題について演説した。平和統一を目指すのが基本だとしたうえで「外部の干渉や台湾独立勢力に対して武力行使を放棄することはしない。必要な選択肢は留保する」と強調し、米国を念頭に台湾問題への介入を強くけん制した。また、2021年の7月中国共産党建設100年の記念式典の演説では一つの中国を受け入れない台湾を強くけん制した。

そもそも、ウクライナと台湾は国際法上の地位が全く異なる。ウクライナは多くの国から国家承認を受けているが、台湾を国家承認している国はわずかである。また、中国はグローバルサウスを中心に影響力を強めている。仮に台湾が中国軍に侵略されたとしても、今回のウクライナのような各国の反応は期待できない。

一方、ウクライナでは、ロシア軍が35万人規模の兵力を投入しても戦況は今もなお膠着状態にある。中国軍と台湾軍とでは戦力には大きな差があるが、中国が台湾に攻め入るとなると、台湾の東側に連なる山脈が上陸を阻むこととなるし、西側の上陸可能地点も限られる。そして中国軍は台湾の陸軍を上回る大規模な兵員を台湾海峡を越えて輸送する必要がある。しかしながら、現状の海軍力では難しい。さらに、台湾関係法により米軍が介入すると見られ、そのうえ米軍の潜水艦の存在もあるので、台湾攻略は簡単にはいかないのではないかと考えている。

7.中国の一帯一路は、マラッカ海峡からカンボジア、ミャンマー、スリランカ、パキスタンを経て東アフリカ、ペルシャ湾に通じるシーレーン確保と海洋国家覇権から内陸国家覇権への転換というグローバルリバランスを狙ったものである。中国のインド洋覇権を窺う動きはインドにとって深刻な安全保障上の懸念である。そもそもインドはQUAD参加には消極的だったが、こうした深刻な安全保障上の懸念がその姿勢を転換させた。QUADは経済連携に止まるものではない。インフラ分野も盛り込まれているし、サイバーなど安全保障に関連した分野での連携も盛り込まれている。

8.2020年に反政府的言論を取り締まる香港国家安全維持法（国安法）が施行されたことも米国の対中政策に大きく影響した。トランプ政権では米国ファーストを前面に掲げたが、バイデン政権では同盟国重視に変化した。

9.憲法9条のような国内の議論の有無と国外の軍事緊張には全く関係がない。スクランブル回数を見ても日本は年間700回から1000回、NATOは500回、アラスカは50回程度である。これを見ても、日本周辺は世界で極めて軍事的な緊張度が高い状況にあり、我が国の安全保障は岐路に立っていることは間違いない。我が国は、ミサイルの阻止=反撃能力の保持、海上保安庁の増強、経済安全保障、ハイブリッド戦＝中国の考えるいわゆる「超限戦」への対抗のあり方を考えていく必要がある。火力による戦争の前に、経済的手段、技術的手段（サイバー等）、政治的手段（テロ、第五列（内通者）等）こういうものを組み合わせ自国の意思を相手国に押し付ける手法を中国は採用しており、それぞれにきちんと

対応していく必要がある。また、国家に対する敵対勢力は、国家以外にも企業、テロ集団、宗教団体などが存在する。

10.　2010年に尖閣諸島周辺における海上保安庁の船に中国漁船が衝突してきた事案で船長を逮捕勾留したことに対し、中国はそれに対抗し反日キャンペーンを展開し、レアアースの禁輸にも踏み切った。このエコノミックステイトクラフトに日本は屈し、船長を釈放した歴史がある。これはエコノミックステイトクラフトの成功例であり、中国は戦わずして勝利を手にした。こうしたことを繰り返さないよう、民間も含め、サイバー対策、サプライチェーン強靭化、サイバーセキュリティの強化が重要である。

【質疑応答】

Q1：　日本を代表する大企業の多くが、サイバーセキュリティー対策が不十分であるいうことが、日本経済新聞電子版「大企業のサイバー対策、4割に危険性車や機械目立つ」（2022年6月5日）
［https://www.nikkei.com/article/DGXZQOUC15C8V0V10C22A4000000/］で報じられていました。
　日経225のうち4割は落第点とのことです。我が国では、企業の情報セキュリティは企業側の努力に委ねられていますが、国が国内企業のサイバーセキュリティ状態をインターネット側からパトロールするような仕組みを作りについて研究したいと思っております。パトカーによる警察の巡視活動と同じように、公的機関がAIロボット等を使ってサイバー空間を巡視し必要に応じて企業を指導するような仕組みそれなりの効果は期待できると思いますが、そもそも、このような取り組みは我が国の経済安全保障制度設計の考え方等に馴染むものなのでしょうか。また、このような取り組みを研究する場合の相談先はNISCになるのでしょうか。

A1：　AIロボットによるサイバーパトロールは良いかもしれない。IDS（侵入検知システム）との組み合わせも効果的と考えられるが、どこまでできるのか、また、どこまで政府が介入するのか検討の余地がある。AIロボットのパトロールは政府の考え方に反するわけではない。政府自身がやるのか、他の組織がやるのか色々考えていけば、良いやり方はいろいろある。

Q2：　台湾統一は中国にとって「核心的利益」と位置づけていると言われていますが、中国は今のウクライナの戦況を自分事に置き換えて分析していると思われます。武力による一方的な現状変更は高い代償を支払うことになり割に合わないことを悟ってくれればいいのですが、中国はロシアのウクライナ侵略をどのように分析しているか、これは行けると見ているのか、そうでないのか、北村様のお見立てお聞かせいただければと思います。また、このような情勢を踏まえて、経済安全保障の観点から、インテリジェンスの長であられた北村様として、日本にできることをお聞かせいただければ幸いです。

A2：　中国がウクライナ情勢を注視しているのは間違いない。ただロシアは35万投入しても上手く行ってない。台湾有事の際に本当に米国が動くかは分からないが、その時に日本がどうするのか、同盟国として何ができるかを考え、備えることは重要である。

Q3：　韓国に関してはQUADへの参加が未だ不透明な状況であると思いますが、もし参加することになった場合、地政学的、軍事的に、安全保障の面から考えて、日本と韓国の間にはどのような関係が求められるとお考えでしょうか。

A3：　インド洋地域におけるインドの覇権が中国によって脅かされている。ソロモン諸島、キリバスも中国と協力関係を築いており、豪州も警戒している。QUADは軍事同盟

ではないが中国を意識したものであることは間違いないことから、対中国という観点ではQUADと韓国の立ち位置は異なっている。そうした立ち位置が異なる場合、統一的な意思決定等が行えない可能性も高く、韓国のQUAD加入はむしろ安全保障上のリスクを高めることが懸念される。

Q4： 中国が太平洋島嶼国に対して外交攻勢を仕掛けていますが、これらの地域で仮に中国が軍事的拠点を置いた場合、オーストラリア、ニュージーランド、フィジーなどの大洋州諸国に危険が及ぶことが考えられますが、日本としては外交面でアメリカやオーストラリアとこの動きを阻止する必要があると思いますが、経済安全保障の観点から考えて他に日本が取るべき行動としてはどのようなものが考えられますでしょうか。

A4： まず2013年の習近平とオバマ会談において習近平は「太平洋は米中が行動するのに十分な大きさがある」と発言。太平洋を米中で分けようという意図での発言と考えられる。中国は大国思考により、そもそも日豪等の諸国を勢力圏としたいと考えて行動している。

太平洋戦争の激戦地であったガダルカナルがあるソロモン諸島と、同じくタラワのあるキリバスは戦略的な要衝であり、これらの国々と国交を樹立し、軍事面での連携を強めようとしている中国は太平洋の覇権を狙っていることは間違いない。最近のニュースではソロモン諸島と協定を結んだところであり、基地の建設を含めて着々と軍事拠点の設置を進めるものと見られる。

これに対抗する観点から、日米両国は、インド太平洋の平和と安定の維持のために南太平洋諸国との連携強化にも力を入れていくべきである。インド太平洋地域の平和と安定を維持するため何が必要かをしっかりと考えていく必要がある。かつて覇権を争った日米が手を取り合うことで、太平洋には平和と安定がもたらされた。この状態を維持する必要がある。

中国のソロモン、キリバスとの連携は、中国にとって第二列島線を越えて西太平洋に進出するためには重要な足場となる。これらの国の国家財政は、脆弱であり、援助の名を借りてこれらの諸国にエコノミックステイトクラフトを仕掛けている。所謂、債務トラップである。現状、米軍は南太平洋地域には軍事的拠点をおいていないが、ソロモン、キリバスとも極めて重要な地域であることは歴史的観点からも当然であるため、日豪は中国のこうした行動を妨げるために共同して行動する必要がある。

Q5： アメリカが中国の一帯一路に対抗して、G7各国と共同で世界各国へのインフラ投資を行う予定があるとのことですが、これらは現状中国の支援を受けている国々も想定されているものなのでしょうか。その場合、米中の対立はより深まるとお考えでしょうか、また日本にも影響は及びますでしょうか。

A5： 援助を受ける側はどの国からもらってもいいため、それによりなびくかはわからない。中国の援助の仕方は透明性も低く、当該国の財政上、圧迫をかけ、最終的には前述の債務トラップのような形となっている。本来、援助というものは相手国を味方に付けるために行うものではなく、それにより援助国が発展し、世界の経済発展に貢献するためのものである。したがって、中国のような援助の仕方ではなく、透明性が高く本質的に経済発展に繋がるような効果的な支援をするというのが日本の考え方であり、G7共同のインフラ投資もそのようなものであるべきだろう。

Q6： ファーウェイへの米国製品の輸出禁止措置について、最終的には情報技術のやり取りを容認していました。経済制裁を行った場合には、今後の技術開発の情報を得ることが難しくなるということも思います。その際に、どこまで日本がデメリットを受けるのか、デメリット以上を得ることが大切であるといった意見がありました。経済制

裁を行う際に何か注意すべきことはあるのでしょうか。

A6： 日本は2019年頃から企業も含めて脱ファーウェイに舵を切った。実際の現場においてもファーウェイ抜きで技術開発の情報を得ることが難しいという話は聞かないし、同等の技術そのものは日米ともに保有しているため、問題は少ない。もっとも、ファーウェイはこれにより世界市場から退場するというものではなく、仮に欧米市場から締め出されたとしても、アフリカや中国と関係が深い国々のシェアを確保することで生き残ると思われる。結果としては、西側諸国のサプライチェーンとは別のサプライチェーンが構築され、相互の技術進展（5G等）のデカップリングが既に進行しつつある。

とりわけ、米国においては2017年以降の政策転換から既にデカップリングが始まっており、今更ファーウェイを外したことで問題になることもないし、多少のコスト面の問題はあるけれども技術面での問題はない。高度技術のデカップリングは日本や欧米諸国の高い工業力を持つ国の間で安定した契約関係の下、相当の受注が確保できるということでもあり、個々の企業はともかく業界全体としてはメリットが大きいこともある。

もう一方のファーウェイは通信設備、通信機器を東南アジア市場やアフリカ諸国に広げたいと考えているようであり、欧米諸国のそれと比べれば技術水準は高くないが低コストであるため、それらの国々に一定の需要はあると考えられる。もっとも、それらの国々が安全保障上の懸念をどのように重視するかは国により異なるだろう。

Q7： 中国は国内半導体産業を強化するために人材開発をしているということでした。人材開発について、海外プログラムを促進し、優秀な留学人材の登用を強化することと、成果に対する報酬制度を整備するとありました。それは、優秀な留学人材に対しても報酬を出すということでしょうか。また、そうした場合に日本から人材が流出してしまうという可能性もあると思います。そうした事例についてはどのように防いで行くべきでしょう

A7： 米国、中国、欧州のいずれの国もそもそも国の科学技術研究費の大きな塊は、「安全保障」関連のものである。他国と同様に安全保障にかかわる研究にきちんと資金を提供し、人材を育成することが解決策である。そもそも「安全保障」にかかわらない技術・研究というものがあまりなく、デュアルユース技術でもあるのが現在はほとんどであり、人文系学問であったとしても間接的に「安全保障」にかかわらない分野というのは少なくなってきていると考えている。

ただ、大きな問題として学術会議の「軍事研究」の禁止の方針により、大型の資金は活用できなくなってしまっている。すなわち、文科省の科研費で「軍事研究」ができないこととなっている。そもそも学術会議をアカデミアの代表と言って良いのかに疑義はあるものの、形としてはアカデミアが自分で自分の首を絞めているように見える。また、我が国の国民を守るための技術の開発を「軍事研究」と呼んで、国際秩序を侵害して他国を害する意図を持つロシアや中国、北朝鮮の軍事研究への協力を防ぐための安全保障輸出管理に疑義を呈しているような一部のアカデミアの知的怠惰・倒錯は目に余る。そもそも学問の自由の観点からも法定された国の機関である学術会議が具体的な危険性の程度を問わずに一律に国内研究に対して軍事研究を禁止するような結果を招くよう通達を出しているのは、極めて問題である。個々の学者の研究内容への重大な介入であり、学問の自由の甚大な侵害と言え、日本国憲法上極めて問題であると考えている。しかも、そのことが研究者の処遇の低さや少なすぎる研究開発費、頭脳流出をうながしているのであるから、もはや論外と言っていい。若い人たちはぜひ学術会議の通達を読んで真剣に考えて欲しい。私のことを右翼的だという人たちもいるようだが、印象論で語るのではなく人権保障という観点から考えたときにどちらが全体主義的な考え方なのかアカデミアの方々を含めてきちんと考えるべきであ

る。

Q8： 経済産業省から伺った話では迅速に対応し、現場の声を聞きながら反映させていきたいとのことでした。改正外為法の施行により、一定程度効果があったようにおもえます。しかし、海外諸国と比較して、日本の投資規制で課題となっている点はどういったことでしょうか。

A8： 現行法では事後の規制にとどまり、遡及できないことが問題である。米国は遡及できるはずである。取引そのものを無効にすることができないのも欠陥である。事後的規制の権限が現状はなく、これは米国と比較して大きな問題であると考えている。テンセントと楽天は例外規定を利用して投資規制をクリアしているようだが、例外規定などを利用する例も多い。また、投資時点での判断でよしとするのではなく、継続的にモニタリングをすることや監視機能の執行体制の強化も必要。とりわけコア産業は一般の投資規制以上にモニタリングの強化、監視機能の執行体制を一層強化することが必要であろう。経産省以外の省庁からのインテリジェンスを活用した情報の提供が的確に行われる枠組みが構築されることも重要である。

Q9： 国内の生産基盤を強化するためには先端技術への投資が不可欠ですが、日本は研究費取得などの兼ね合いで千人計画に協力した学者も 40 人前後います。研究費を潤沢に投資しているとはいえない日本において、先端技術の投資を高めるために海外から参考にできる方策としてどのようなものがあるのでしょうか。

A9： そもそも中国に限らず安全保障等の名目が立たないものに潤沢に税金を投入するわけがない。特に中国の学術研究があからさまにその軍事研究の支援になっていることを研究者が理解せず、アカデミアも危機感を持っていないことがそもそも問題である。

彼らの研究費に潤沢に投資するために「安全保障」に対して科研費を出せるのであれば、ご指摘の問題は解消するのが道理である。政府は他国と比べてお金を研究者に出していないわけでもないし、その枠もあるのだが単にアカデミアが自分で自分の首を絞めているだけ。A7 と言っていることは同じとなるが、学術会議によって大学の自治や学問の自由が侵害されている状況を改善しなければいけないと考えている。

Q10： 戦略的不可欠性を確保する上でも欠かせない優秀な人材の確保についてですが、他国と比べ日本の研究者の所得が低いことが優秀な人材の海外流出の原因と言われております。また、大学や研究機関の研究開発費が少なすぎることも優秀な人材の海外流出を助長していると言われています。これらの点については、有識者の間では、どのような議論が進められているのでしょうか。

A10： 経済安全保障推進法の枠組みの中で安全保障に関する技術を適切に研究してもらう必要がある。協議会ではどういうことに興味をもってどう研究していくのか方向性をリードしながら随伴的な補佐を行う。この仕組みが育つことにより、現在の硬直したアカデミアの流れが変われば良いと思っている。

（追加質問）

Q11： 外為法のみなし輸出管理を明確化し、外国籍の方々への技術提供等が厳格化されたように思います。経済産業省へのヒアリングにて、職員のお話では、まずはこの制度が上手く執行できるか、そのうえで今後の修正が必要なところを模索していくとのことでした。北村様のご見解として、現行の制度が上手く機能するのか、また、今後改正が必要であるとしたらどのようなものが必要か、教えていただければ幸いです。

A11： うまくいくのかと言われても役所としては建前上は「うまくいく」と答えざるを

得ない。そもそも法律の改正なり制度の改正はうまくいくように制度を設計していくものであり、そうならない改正はしない。つまらない回答と思われるかもしれないが、まずは改正された制度をしっかりと運用し、将来的に上手く行かないところが出てくればまた制度改正するというものの繰り返しである。

Q12： 2017 年に米国は中国のエンゲージメントを見直したが、我が国の対中戦略における戦略的互恵関係は維持すべきでしょうか。

A12： 戦略的互恵関係は都合の良いところは協力しましょうという考えに立っており、その折り合いが付くのであれば両者の「都合の良いところ」で関係構築することはあり得る。もちろんその際に過剰に譲歩する必要はない。あくまでも条件が合致すればだが、習近平を国賓として招くことさえあり得るだろう。こうした考え方は外交関係の基本であると考えている。

我が国は米国とほとんど共通の利害を有しているが、究極的なところで言えば、中国との戦争では米国本土より先に我が国が攻撃されるといった相違もある。そのため米国と完全に一致した外交戦略になり得るかと言えばそうならないケースもあり得る。米国はその軍事的手段を含めて中国と対決するという決断までできるが、我が国はそう勇ましいことばっかりは言ってられないということもあり得る。

したがって、そもそも戦争にならないための安全保障面の抑止力の構築も含めていかに攻撃を受けないようにするか、近隣諸国と安定的な関係を作っていくことも必要である。その上で、お互いに最終的に折り合いを付けるための対話のチャネルを常に維持し続けることも重要である。我が国が戦わず平和を維持していくことこそが大事と考えており、内閣情報官・国家安全保障局長時代からこれを私の行動指針としている。

以上

記録作成担当者：稲田凜香

ヒアリング調査報告No.10 基本情報

日時	2022年8月3日
テーマ	我が国の経済安全保障を推進する上でのサイバーセキュリティ確保に向けた諸課題について
ヒアリング先 (担当者)	某セキュリティ企業
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 岡本樹、織田秀夫、梶山敬生、木戸友香子、山田麻友 (計6名)
調査目的	我が国の経済安全保障を推進する上でのサイバーセキュリティ確保に向けた諸課題の把握すること。

【質疑応答】

サイバーセキュリティにおいて、貴社の持つ情報（どういった人物・機関から攻撃があるのか、何を標的に攻撃をしているのか等）は非常に貴重であり、国もこのような情報を欲していると考えています。

Q1-1： 現在、貴社と国とが互いの持つ情報を共有する機会はありますでしょうか。

A1-1： 複数あるが、一例として日本サイバー犯罪対策センター（JC3）がある。産学、そして警察が連携し、サイバー空間に関する情報を共有している。

Q1-2： また、今日において経済安全保障という考えが注目され、現在のESGやSDGsというように、経済安全保障を踏まえたビジネスを行っている企業が、今後投資家等から注目を浴びると考えています。そのうえで、貴社がビジネス戦略を考える上で、経済安全保障への考えなど、国が持つ情報をご所望するようなことはあるのでしょうか。

A1-2： まず、経済安全保障を踏まえたビジネスを行っている企業が、今後投資家等から注目を浴びるのかは分からない。現状において経済安全保障は企業にとって常識とは言えないが、エコマークが付いている製品を購入しようといった考えが長い期間をかけて根付いたように、長い期間をかけて経済安全保障が投資や消費者にとって重要な要素の一つとなってほしい。マルウェアの情報やIPアドレスなどのなかには、国しか持っていない情報があると考えるため欲しいと思う。もっとも、こういった情報は諜報によるものなど秘匿性が高く、政府機関のみで共有され、一般企業への共有が望ましくないものがあることも承知している。情報の棲み分けが必要なため、情報の共有については解決しない問題だと考える。

追加補足： セキュリティクリアランスが担保され、かつ、それが国の利益にとって必要な場合は提供できるかもしれない。今も守秘義務や罰則がなくても国が任意に情報提供することはある。法的に担保できる場合と出来ない場合とでは提供できる情報の範囲に差が出る。警察の捜査情報が必要なら、おそらく官公庁と同程度のセキュリティクリアランスが企業側にも求められる。制度を担保する必要があるため国としては心苦しいが機微になればなるほど体制整備をしっかりやる必要がある。法制度が整っている国（米・英）は、義務を課したうえで機微な情報を共有している。米英を念頭に置きながら考えてみる必要がある。法制度だけでなく、契約というアプローチもある。（坪原）

Q1-3： 最後に、経済安全保障においては、国だけでなく、経済主体の企業も中心となり、互いに持つ情報を共有することで、より実効的な施策を講じることが必要だと考えています。特に貴社はセキュリティに精通した企業であり、国または他の企業が情報共有等の協力を求めてくるのではないかと考えております。そのうえで、今後、経済安全保障の推進に向けて、国と企業の情報共有枠組みが作られ、貴社にその枠組みへの参加が求められた際に、進んで参加しますでしょうか。参加へのネック等があるようでしたら教えていただければ幸いです。

A1-3： 現在の情報共有枠組みとして、法的根拠のあるサイバーセキュリティ協議会や、IPA が主導する J-CSIP がある。そこでの大きな問題としては、企業にとって情報を提供するメリットが少ないこと。セキュリティ企業においては、主体的に行った調査におけるデータと、お客様から預かったデータがあり、後者に関しては匿名だと可能となる部分はあるものの、一般的にはそのまま提供することができない。また、提供すべきデータか否かといった判断も必要となり、時間がかかる。サイバーセキュリティ協議会においては、共有された情報を自らの顧客等のサイバーセキュリティ確保のために活用することができるなどのインセンティブが存在する。情報を提供しなければ国や他の企業からの信用が失われる可能性はあるものの、直接的な利益がないと現場は動きづらい。やはり、インセンティブの必要性があると考える。

Q2： 国内企業におけるサイバーセキュリティの現状と問題点について、日頃お感じになられていることをお聞かせいただければ幸いです。

A2： セキュリティインシデントが発生したときに被害報告義務がないことが問題であると考える。必ずしも一般公表する必要はないが、被害の情報を公的機関等に報告し、その内容をセキュリティ事業者や捜査機関が把握することは、同様の手口による被害を未然に食い止めるのに役立つ。公開サーバーなどのセキュリティ診断が不完全な例も見受けられる。不十分なツールでセキュリティ診断をしても、脆弱点の炙り出しができない。新しい Web サービス開始時等のセキュリティ診断のみではサイバーセキュリティ対策が十分とは言えない。運用開始後であっても OS やソフトウェアに新たなセキュリティホールが日々発見されている。このためサービス開始後も定期的なセキュリティ診断は必要である。しかし、セキュリティ診断実施のお墨付きだけを求める企業は、脆弱点が見つかっても黙認したり、それを隠したり、改善しないまま放置しているケースも散見される。また、セキュリティ診断で脆弱点が見つかった場合、スコープ外などと理由をつけて結果報告書には記載しないでほしいと頼まれるケースもあるようだ。クレジットカード決済基盤を提供するメタップスペイメント社のデータベースから顧客情報などが流出したケースでも、同社は脆弱点を認識していたことを隠し続けていたということが問題視されている。そうした部分を改善することも必要である。

Q3： また、もしご存じであれば他国との比較での現状と問題点について、日頃お感じになられていることがあればお聞かせいただければ幸いです。

A3： Java ベースのオープンソースのロギングライブラリの Apache Log4j に関して複数の脆弱性が報告された。このケースにおいては、世界中の多くのシステムに甚大な被害が発生した。Apache Log4j に関してアメリカの場合は、企業がサイバーセキュリティ上の脆弱性を放置した場合には、サイバーセキュリティ・インフラセキュリティ庁（CISA）や連邦取引委員会（FTC）が強制力のある措置を講じることができた。日本の現行法制ではサイバーセキュリティの脆弱性を放置しても罰せられず、改善を強制することは出来ないのではないか。NISC や JPCERT/CC でも本件について注意喚起をしているが無視することはできる。この点については法制度上での改善の余地があるの

ではないかと思う。

Q4： 現行の法制度ではサイバーセキュリティについては企業側の努力義務[1)]となっておりますが、企業経営者の意識レベルの差によって、対策にも差が生じてくるものと考えられます。重要インフラなどへのサイバー攻撃は、経済活動への影響のみならず、国民生活や我が国の安全保障にも広く影響することを鑑みると、企業の努力義務だけでは不十分と考えますが、サイバーセキュリティ事業者様としてのご意見をお聞かせいただければ幸いです。

A4： 努力義務ではなく義務化はした方が良い。しかし現状では、Offensive Security の観点で対策をとれる人と評価する人材が確保できない。このため義務化してもその制度がうまく機能する見通しは立ちにくい。だから義務化よりも先に、不足している攻撃側のスキルを有した人材育成が急がれると思う。

Q5： 車社会を支える道路交通法や車検などの様なルールをサイバー空間でも設けることで、サイバー被害リスクは減らせる可能性があるのではと思います。ルールを設けるとすれば、現時点ではどのようなルールが適当でしょうか。例えば、営業用車両の車検と同じように、認定事業者による年一回のセキュリティ診断の受検など。

A5： サイバー攻撃から守るべき情報資産で、たとえ話として一番わかりやすいのは WEB サーバーである。これについてはセキュリティ診断を受けてくださいということはできると思う。イントラネット側（オフィスエリア）にも守るべきもの（従業員個人が利用する PC に保有されている情報）があるが、システムは百社百様であるため、そこに対する診断は決まりきったサービスとしての提供は課題が多いのではないか。IT エンジニアにとってのインターネットは自由で開かれた空間であるため、ルールを設ける際は、上手くやらないと反発を招く恐れがある。ロシアや中国は自由で開かれたインターネットにただ乗りし攻撃しているという現実があることを踏まえて、理解のあるエンジニアを仲間にすればと円滑に進んでいくと思われる。

Q6： 政府機関が基幹インフラ企業ネットワークに対してインターネット側からセキュリティ診断を行い、必要に応じて当該企業に対し指導・改善勧告することは技術的に可能でしょうか。また、これを任意のものではなく義務化をする制度を導入することには意義はありますでしょうか。ご意見をお聞かせいただければ幸いです。ＮＩＣＴが時限的な業務として IoT 機器の調査を行う「NOTICE」[2)]において既に機能実装済みかもしれませんが、今のところ確認は取れていません。

A6： インターネット側からの公開サーバー等へのセキュリティ診断は技術的には可能。しかし、現行法制度では不正アクセス禁止法に抵触する場合があると思われる。また、脆弱性を調べる目的の行為がシステム自体を破壊することもある。このため、できるものだけをやることが一つの選択肢。脆弱性が放置される理由には、脆弱性の存在をしらない、そもそも脆弱性への知識がない、使っているソフトウェアの情報を知らないといったことがある。このような場合には、セキュリティ診断に際してソフトウェア使用状況の情報を収集し、脆弱点を有するソフトウェアを使用する企業に適時通知し、ソフトウェアのアップデートをフォローするようなことは有効かと思う。ただし、有価証券報告書への記載については相当強いので、勧告に至る手前でどのように改善させられるかも課題と思われる。また、間違いなく脆弱性を有することを証明することにも難がある。本当に脆弱性があるか否かは実際に攻撃してみないと分からない場合が多い。

Q7： 現行法では、不正アクセス等のサイバー攻撃を受けた企業から個人情報が流出した場合の報告は法令で義務化[3)]されていますが、個人情報流出を伴わない場合の報告義

務はありません。サイバー攻撃被害を受けた企業等が、その被害に係る情報をサイバーセキュリティ関係組織等と共有することは、発生したサイバー攻撃の全容を解明し、更なる対策の強化を可能とせしめるものであり、サイバー攻撃被害組織等自身にとっても、社会全体にとっても非常に有益です。しかし、現状、サイバー攻撃被害組織等の現場にとって、自組織のレピュテーションに影響しかねない情報共有には慎重であるケースも多く、被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すればよいかの検討にあたり、実務上の参考とすべきものがないため、適切に判断することが難しいとの声も聞かれます[4)]。企業がサイバー攻撃を受けた場合にその情報を共有し易くするために、実務上参考になりえる行動指針はガイドライン（どのような情報を、どのタイミングで、どのような主体と共有すればよいか等）を国が示しておくことは、被害情報の共有の促進に役立つものなのでしょうか。また、これ以外の策は考えられるでしょうか。

A7： 情報を共有するパターンはサイバー被害当事者が報告する場合と、セキュリティ会社が共有する 2 つの事例に分けることが出来る。セキュリティ会社はインセンティブがないことから実施されないことがある。サイバー被害当事者の場合はその情報を隠したいと思う場合がある。また、情報共有を義務化したとしても一般に公開させるというのは問題がある可能性がある。IPA が行っている J-CSIP は重要インフラごとにグループを作っており、そのグループ内で情報共有をする仕組みがある。このような議論の中では、被害を受けたから公表しなければならないということと、被害を受けた際の痕跡情報などを公表すること自体に意味があるという 2 つの意味が混じってしまっている。しかし、これは分けて考えるべきである。国側としては、情報を公開して欲しいという意図があるが、企業としては被害情報を出すことはしたくない。そのことから、身元を隠した情報提供の場があると企業としてもやりやすくなる可能性がある。

Q8： サイバー空間における脅威としてサイバーセキュリティを強化するため、企業だけでは対応が困難であるため国が対応すべきと考えることは何でしょうか。

A8： オフェンシブセキュリティを国内でできる人が少ない。攻撃者側からの視点でセキュリティ対策を実施出来る人が少なく、そのような観点での国内の資格も存在していない。情報処理安全確保支援士という資格はあるが、これは守る側の資格である。攻める側からの視点でセキュリティ対策を実施出来る人材を増やしてほしい。日本だと攻撃などけしからんといった抵抗感がある。そのため、国内にオフェンシブセキュリティの資料が大変少なく、学ぶ場合は英語の文献にあたる必要がある。なかには自腹で高いトレーニングを受講する人もいる。トップダウンの視点としては、国内でオフェンシブセキュリティの資格を作って欲しいと思っている。また、世間に認められる政府の方針を作って欲しい。ボトムアップの視点としては、情報処理安全確保支援士の資格保持者が伸び悩んでいるという状況がある。名称独占資格ではあるが、業務独占資格ではないことなどから、個人が資格を取得する強い動機がない。民間企業目線としては人材を増やして欲しいと思っている。そのためには、セキュリティに対して若者に夢を持たせるような環境として欲しい。セキュリティは楽しく、そうしたことが社会的に認められるようにして欲しい。

（追加質問）

Q9： 攻撃者側の視点を知っていることが重要だと思っています。こうした取り組みで知見の蓄積はどこまで可能になるのか、そして現実環境で攻撃のシミュレーションを行うことは難しいと思います。システムへの侵入を競い合う大会もありますが技術者向けで学生向けや教育用のものはあまり多くないように感じています。現実環境で攻撃のシミュレーションはできないので学校での訓練を期待しますか。また、サイバーセ

キュリティ事業者様から大学に期待することはありますか。

A9： 一例だが、CTF 関連で優秀な人材を集めたいと思っている。練習環境については教育事業で実際にハンズオンによる脆弱環境を構築して攻撃の体験をするコースがある。学生向けにも演習環境を設置して学生が触れる機会を作ることは意義あると思う。その上で、倫理観が必要となってくる。サイバー攻撃で企業等を乗っ取ることで全能感が芽生えるが、その感情を促さないように教育をしていくことが必要。エシカルハッカーという資格もある。人材を増やすことと倫理観の育成の両立が必要。支配的になる感情を作らせるのは良くない。研修でやったあと家に帰って実際に攻撃を仕掛けてしまう人もたまにいる。倫理教育がしっかりできていないから少年の犯罪につながる。

Q10： 現在倫理観を教える場はありますか。

A10： フレームワークはあまり心当たりがない。資格という点では CISSP(Certified Information Systems Security Professional)資格が海外にある。一方で、日本語で日本の法体系に基づいた資格があれば心強い。情報処理安全確保支援士には倫理綱領というものもあるが、資格自体が攻撃側のものではない。

Q11： 現在、多くの日本企業でサイバーセキュリティ対策が不十分な状況です。海外ではサイバーセキュリティサービスを経済政策として国主導で普及させているところもあり、経済安全保障を強化している日本においてもサイバーセキュリティサービスの拡充は不可欠だと考えております。これは、御社のようなサイバーセキュリティサービスを提供する企業にとってもビジネスの拡大という観点から悪い話ではないと思われますが、今後より多くの企業にサイバーセキュリティサービスを利用してもらうために制度面等で国に求めることはございますか。

A11： 現在、国がセキュリティ監視事業者のリストを公開している。この先、当制度をどう運用していくのかを考える必要がある。しかし、官民ともにサイバーセキュリティを評価できる人材が十分にはいないため、民間企業のサイバーセキュリティの不備等を認識できないという課題がある。そのため、国にも技術的な観点から IT を評価し、サイバーセキュリティを推進できるような人材を増やすべきだと考える。

Q12： 今年の 2 月にトヨタ自動車の取引先企業・小島プレス工業がランサムウェアによるサイバー攻撃を受け、トヨタの 14 工場の 28 ラインが止まりました。大手企業よりもセキュリティが脆弱な中小の取引先企業が狙われ易いと言われますが、サプライチェーンを構成する企業が被害に遭えば、その企業の大小に関わらず、結果としてサプライチェーン全体が機能停止し、我が国の経済に大きな損失をもたらします。経験豊富なサイバーセキュリティ事業者目線で見た場合、サイバーセキュリティ対策強化のための中小企業の課題、ならびに国が中小企業を支援するとすれば、どのような観点からの支援が望ましいでしょうか。

A12： 中小の取引先に問題があった場合にも、独占禁止法の関係上対策を強要できないようである。カプコン、ソニーでは海外拠点がサイバー攻撃を受け被害がでた。海外法人の場合、日本の国内法の力が及ばない。日本企業が現地法人にガバナンスを効かせられていなかったようだ。日本の本社が強いガバナンス、指導力を持って行わないといけない。

Q13： APT（Advanced Persistent Threat：国家の関与・支援が想定されるような、洗練された攻撃を特定の標的に対して執ように行うサイバー脅威主体）による重要インフラ（電力、交通、情報通信、金融システムなど）へのサイバー攻撃に備えるためには、より高度な対策が必要になると思いますが、国がサイバーセキュリティ強化

に向けてさらに踏み込んだ対策を取るとすれば、技術面、体制面、制度面、人材育成面、従業員のリテラシー面などにおいて、どのような施策が有効と考えられるか、ご意見をお聞かせ下さい。

A13：　サイバーセキュリティ事業者をもう少し優遇してほしいということに尽きる（APTに立ち向かうモチベーションもさらに高まる）。より高品質で堅牢なサイバーセキュリティシステムの構築・維持・運用に求められる最高レベルの技術スキルを証明するような、より高難度の資格制度が創設されることを望む。攻める側のスキルを有する人材が不足している。サイバーセキュリティ技術に関して日本語での情報量が少ない。

以上

記録作成担当者：織田秀夫

ヒアリング調査報告 No.11 基本情報

日時	2022 年 8 月 9 日
テーマ	経済安全保障推進法への対応について
ヒアリング先 (担当者)	株式会社 KDDI 総合研究所 村上 様
場所	質問表を送付の上、メールでのご回答を得た
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 織田秀夫 (計 2 名)
調査目的	経済安全保障推進法が可決成立したことを踏まえた、電気通信事業者の対応について聞き取りを行うこと。

【質疑応答】

1.基幹インフラ役務の安定的な提供の確保に関する制度について

Q1-1： 御社の通信ネットワークへのサイバー攻撃に対する取り組みの現状、および本法律が施行されることにより必要となる追加的措置についてお聞かせください。

A1-1： 通信インフラの不正使用により障害を引き起こされる、いわゆるサイバーテロから自らの通信インフラを守るため、弊社は、外部攻撃に対する専門組織による 24 時間 365 日での監視や ICT-ISAC を通じた他事業者との連携など、常に適切な防御措置を講じております。本法律が施行されることにより、重要設備の導入・保守業務等の委託に対して事前審査が行われることになることから、通信事業者としては適切な供給者・委託先を選定することで安心・安全な通信サービスを継続的に提供することに努めて行く。

Q1-2： 本法律が施行されることで、御社が懸念している課題についてお聞かせください。

A1-2： 事前審査の結果として導入・委託ができることとなった後にも、国際情勢の変化等々によって事後的に変更を求められることがありえる制度となっており、不測のコスト負担の発生リスクがあることから、経営の予見性に一定程度の影響を及ぼすと考えている。また、重要設備の導入や業務委託の計画の政府による事前審査が行われることになり、設備等の選定・発注に要する準備期間が若干長期化する可能性などが想定されるため、お客さまへのサービス提供への影響と経済安全保障の確保のバランスを取る必要があると考えている。

Q1-3： 今後、政令・省令等で具体的な内容が規定されますが、制度設計において配慮が必要な事項について、ご意見をお聞かせください。

A1-3： 特定社会基盤役務基本指針において定められる予定の「特定社会基盤事業者に対する勧告及び命令に関する基本的な事項」について詳細まで定めることなど、事業者の経営にとって十分な予見性を確保するための配慮が必要であると考えている。

Q1-4： 現行の電気通信事業法では一定の条件を満たせば、外国企業であっても日本国内での電気通信事業への参入が可能です。仮に諜報活動やサイバー攻撃の使命を負った者が電気通信事業に参入した場合、その事業者が保有する通信設備と御社の通信設備を相互に接続することにより生じるリスクついてご意見をお聞かせください。

A1-4： 電気通信事業法において、電気通信事業者は他の電気通信事業者からの接続の請求に応じる接続応諾義務（第 32 条）が課されており、ご指摘のリスクを完全に排除することはできないと考えている。

Q1-5： 本法律では国が重要設備の審査を行うこととしています。審査する側にも電気通信技術に関する相当の知見が必要と考えますが、御社としてはどのような審査体制が望ましいと考えるか、ご意見をお聞かせください。
A1-5： 通信法制・通信技術についての知見をお持ちの総務省で審査いただくのが良いと思う。

2.重要物資の安定的な供給の確保に関する制度について
Q2-1： 2010 年の尖閣諸島事件を契機に中国がレアアースの対日輸出を事実上停止した時のように、他国が経済力を用いて我が国に要求をのませるような手段を取った場合、サプライチェーンは混乱し通信サービス等役務に必要な資材の調達にも影響が生じることが想定されます。そのような事態を回避するために、サプライチェーンにおいて御社はどのような対策を取られているかお聞かせください。
A2-1： 完成品の購入者としては必要数量の長期間の提示や、正式発注タイミングの早期化で、メーカー側が部材確保を進めるタイミングを早めるよう促している。また昨今の半導体不足を受け、製品によっては在庫を厚めにする対応もとっている。

Q2-2： 価値観を共有する国から調達している資材であっても、周辺有事等の際は物流が停止する可能性は否め無い。そのような場合における御社としての資材調達の考え方についてお聞かせください。
A2-2： Q2-1 に回答した通り。

Q2-3： 安全保障上の理由から、米国は同盟国である日本に対して、同等の対中輸出入管理を求めてくることは容易に想定されます。我が国がそのような要求を受けた場合の御社としての資材調達の考え方についてお聞かせください。
A2-3： 調達元を慎重に選定するとともに、その原材料の供給状況について調達元から密に情報を提供いただき、必要に応じて調達元の変更等の措置も実施することになろうかと思う。

Q2-4： 制度設計において配慮が必要な事項について、ご意見をお聞かせください。
A2-4： 実効性のある制度になることを期待している。

3.先端的な重要技術の開発支援に関する制度について
Q3-1： 具体的にどのような支援が望ましいかご意見をお聞かせください。
A3-1： 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」にて議論が行われている「経済安全保障推進法案の概要」に記載されている開発支援の対象となる分野の技術（特定重要技術）は、いずれも直ぐに研究成果が出るものではないため、同会議で議論されている通り、複数年に渡り柔軟かつ機動的な運用が可能な枠組みとなることが望ましいと考える。

Q3-2： 懸念される事項について、ご意見をお聞かせください。
A3-2： まずは同プログラムの詳細が決定されるのを待ちたいと思うが、研究者をはじめ関係者それぞれの意向や自主性を尊重した運営となるようにしていただきたいと考える。

4.特許出願非公開に関する制度について
Q4-1： 制度は御社にとっては不利益になるとお考えですか？また、それはどんな場合が想定されるかご意見をお聞かせください。

A4-1：　政府方針によれば、非公開化の対象となる特定技術分野は核技術や先進武器技術に関わる分野であることが示されており、その詳細は定かではないものの、弊社では当該技術分野の特許出願を取り扱うケースが少ないと考えられ、他社と比べても弊社に特別不利益が生じるとは想定しておりません。

Q4-2：　企業に不利益を生じさせないためには出願技術等の価値に見合う十分な補償が必要となりますが、その価値を計るにはどのような手法が望ましいかご意見をお聞かせください。

A4-2：　非公開化の対象とされた特許発明の実施や開示が制限されることによる損害や逸失利益を補償価値として正確に算定することは現実的に困難と思われます。これを踏まえた補償手法として、例えばですが、非公開と認定された場合は出願人に一律の補償金が付与されるとともに、当該発明に至る研究開発への投資規模や実施準備に費やしたコスト、非公開化に基づく事業計画の変更による利益の減少額など、出願人が個別事情を申請することにより、一定の条件のもと追加の補償金が付与されるような段階的な補償の仕組みが考えられます。

Q4-3：　この制度が導入されることによる新たな技術開発モチベーションへの影響についてご意見をお聞かせください。

A4-3：　Q4-1 で回答しました通り、弊社の技術開発分野は非公開化の対象となる分野と異なる可能性が高いため、モチベーションへの影響は小さいと考えております。

Q4-4：　新たな技術開発モチベーションを低下させないためには、どのような制度設計上の配慮が望ましいと考えるかご意見をお聞かせください。

A4-4：　補償制度の充実（特に、実施制限により企業体力が大きく損なわれる中小・スタートアップ企業向け）、非公開化認定の公平性、諸外国の非公開制度との整合性、について十分に配慮した制度設計を期待しております。

以上

記録作成担当者：織田秀夫

ヒアリング調査報告No.12 基本情報

日時	2022年8月9日
テーマ	経済安全保障推進法への対応について
ヒアリング先 (担当者)	ソフトバンク株式会社 赤澤 様
場所	質問表を送付の上、メールでのご回答を得た
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 織田秀夫 (計2名)
調査目的	経済安全保障推進法が可決成立したことを踏まえた、電気通信事業者の対応について聞き取りを行うこと。

【質疑応答】

1.基幹インフラ役務の安定的な提供の確保に関する制度について

Q1-1： 御社の通信ネットワークへのサイバー攻撃に対する取り組みの現状、および本法律が施行されることにより必要となる追加的措置についてお聞かせください。

A1-1： 弊社ではCISO (Chief Information Security Officer：最高情報セキュリティ責任者) を設置の上、情報セキュリティの確保に努めています。詳細は下記URLをご覧ください。本法律の施行による追加的措置の要否は今後の詳細な制度設計次第と考えております。
https://www.softbank.jp/corp/aboutus/governance/security/

Q1-2： 本法律が施行されることで、御社が懸念している課題についてお聞かせください。

Q1-3： 今後、政令・省令等で具体的な内容が規定されますが、制度設計において配慮が必要な事項について、ご意見をお聞かせください。

A1-2,3：経済安全保障推進法案の意義・必要性については理解している。その上で、経済合理性とのバランスを考慮した規制・規定が望ましいと考える。

Q1-4： 現行の電気通信事業法では一定の条件を満たせば、外国企業であっても日本国内での電気通信事業への参入が可能です。仮に諜報活動やサイバー攻撃の使命を負った者が電気通信事業に参入した場合、その事業者が保有する通信設備と御社の通信設備を相互に接続することにより生じるリスクついてご意見をお聞かせください。

A1-4： 悪意を持った電気通信事業者の参入といった仮定の話であり、ご回答が難しいところだが、弊社では相互接続の開始前に、接続試験の実施や有事の際のトラフィック規制等が行えるよう事前協議を行っている。

Q1-5： 本法律では国が重要設備の審査を行うこととしています。審査する側にも電気通信技術に関する相当の知見が必要と考えますが、御社としてはどのような審査体制が望ましいと考えるか、ご意見をお聞かせください。

A1-5： 必要な審査体制（求められるべき知見の程度）は、今後の詳細な制度設計次第と考える。

2.重要物資の安定的な供給の確保に関する制度について

Q2-1： 2010年の尖閣諸島事件を契機に中国がレアアースの対日輸出を事実上停止した時のように、他国が経済力を用いて我が国に要求をのませるような手段を取った場合、サプライチェーンは混乱し通信サービス等役務に必要な資材の調達にも影響が

生じることが想定されます。そのような事態を回避するために、サプライチェーンにおいて御社はどのような対策を取られているかお聞かせください。

Q2-2：　価値観を共有する国から調達している資材であっても、周辺有事等の際は物流が停止する可能性は否めません。そのような場合における御社としての資材調達の考え方についてお聞かせください。

Q2-3：　安全保障上の理由から、米国は同盟国である日本に対して、同等の対中輸出入管理を求めてくることは容易に想定されます。我が国がそのような要求を受けた場合の御社としての資材調達の考え方についてお聞かせください。

Q2-4：　制度設計において配慮が必要な事項について、ご意見をお聞かせください。

A2-1~4：　上記 Q2-1～Q2-4 をまとめて回答する。サプライチェーンの確保にあたっては、調達先を問わず様々なリスクを踏まえて対策を講じている。基本的には備蓄の他、安定供給確保のため日頃から取引先の拡大を図り、調達先が特定の国・取引先に限定されないように努めている。

3.先端的な重要技術の開発支援に関する制度について

Q3-1：　具体的にどのような支援が望ましいかご意見をお聞かせください。

Q3-2：　懸念される事項について、ご意見をお聞かせください。

A3-1,2：　現時点で特段の意見は無い。

4.特許出願非公開に関する制度について

Q4-1：　制度は御社にとっては不利益になるとお考えですか？また、それはどんな場合が想定されるかご意見をお聞かせください。

Q4-2：　企業に不利益を生じさせないためには出願技術等の価値に見合う十分な補償が必要となりますが、その価値を計るにはどのような手法が望ましいかご意見をお聞かせください。

Q4-3：　この制度が導入されることによる新たな技術開発モチベーションへの影響についてご意見をお聞かせください。

Q4-4：　新たな技術開発モチベーションを低下させないためには、どのような制度設計上の配慮が望ましいと考えるかご意見をお聞かせください。

A4-1~4：　現時点で特段の意見は無い。

以上

記録作成担当者：織田秀夫

ヒアリング調査報告 No.13 基本情報

日時	2022 年 8 月 25 日
テーマ	経済安全保障に係る文部科学省の取り組みについて
ヒアリング先 (担当者)	文部科学省 科学技術・学術政策局 国際戦略担当-参事官付課長補佐 遠藤正紀 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凛香、岡本樹、香高優一郎 (計 4 名)
調査目的	研究インテグリティ等の文部科学省の経済安全保障施策を学び、今後の研究に活かすこと。

(写真)

【レクチャー】

文部科学省は科学技術の観点から経済安全保障関連政策を進めている。特に、日本の優位性、不可欠性の確保に関わっている。日本が世界で不可欠な存在となるためには、技術が重要となっていく。

経済安全保障上の主要課題の中で、文科省が主に進めているのは以下 3 点である。

・外国資金受け入れ状況開示
・技術情報管理
・経済安全保障重要技術育成プログラム

このうち外国資金受け入れ状況開示・技術情報管理が技術を守る施策で、経済安全保障重要技術育成プログラムは技術を育てる施策である。優位性・不可欠性の観点では科学技術は欠かせない。先端的な重要技術を継続的に育て、それを守っていく必要がある。そのため、大学・研究機関等における研究インテグリティの確保や安全保障貿易管理の徹底を進めている。その上で、守るべき技術を生み出せる国であることがまずもって必要であ

り、経済安全保障重要技術育成プログラム等で我が国の研究力の向上にも取り組んでいる。

1.研究インテグリティ

研究インテグリティとは、研究の国際化やオープン化に伴う新たなリスクに対して新たに確保が求められる、研究の健全性・公正性を意味する。この新たなリスクにより、開放性、透明性といった研究環境の基盤となる価値が損なわれる懸念や、研究者が意図せず利益相反・責務相反に陥る危険性が指摘されている。こうした中、我が国として国際的に信頼性のある研究環境を構築することが、研究環境の基盤となる価値を守りつつ、必要な国際協力及び国際交流を進めていくために不可欠となっている。

特に安全保障貿易管理に関しては、機微技術が懸念国に流出するのを防ぐことを中心に、経産省と共同して、外為法の順守をお願いしている。また、みなし輸出の改正など様々な取り組みを行っており、大学や研究機関も対応に尽力している。特に注意すべき対象をどう同定するかという点に関して、大変頑張っていただいている。

外為法によって強制的に規制するような施策は遵守すべきボトムラインであり、研究インテグリティとして求められているものは、研究を自主自立的に行っていく中で、アカデミア内で研究の公正性を確保するために自浄作用を果たすことを目指している。あくまでも研究におけるマネジメントの話であり、外国の不当な影響等は学問的な真実の追究を歪めそもそも研究の公正を損ねるものであるということを理解し、大学組織としてもきちんとリスクマネジメントをしていくことで、日本の研究環境を守るようにしている。あくまでも自律的なマネジメントが求められるものであり、いきなり法規制をするといった性質のものではないと認識している。

2.経済安全保障重要育成プログラム

内閣府科学技術・イノベーション推進事務局とも協働して、合計して補正予算で、2500億円の基金を作った。プログラムの特徴として、以下3点ある。

- 我が国として確保すべき先端的な重要技術にかかる研究開発を推進。基礎研究から一歩進んだ応用以降のレベルを主要ターゲット。
- 国がニーズを踏まえてシーズを育成するための研究開発のビジョンを設定。資金配分機関を通じ個別技術・システムを公募。国がニーズを踏まえてシーズを育成する。
- 研究成果は、民生利用のみならず、成果の活用が見込まれる関係府省において公的利用につなげていくことを指向。国主導による研究成果の社会実装や市場の誘導につなげていく視点を重視。また、技術成熟度や技術分野に応じた適切な技術流出対策を導入。

国がニーズを踏まえてシーズを育成する。研究開発はNEDOやJSTが担当し、国がどの技術が必要か示していく。とりわけ安全保障に関しては市場がニッチなものや、国として必要だが、民間による技術開発が期待できないものもあり得るため、必要な支援等を行いながら公的使用ができるようにしていく。

3.経済安全保障推進法について

官民パートナーシップ協議会が法的に設けられることが特徴である。経済安全保障重要技術育成プログラムは公的利用の技術を念頭に置いているが、公的ニーズ、スペック等を研究者側が知らないと研究ができない。しかし、そのような国の情報は守秘義務なしに渡すことが難しいものもある。そこで本法により、協議会を通じて提供される機微情報に罰則付きの守秘義務を設け、情報共有ができることとした。

もちろん、研究は論文や学会発表による公開が原則である一方、守秘義務対象情報をそのまま載せることとせず、当該情報を開示しないようにするように工夫していただくことになる。これは別に新しい話ではなく、民間企業との共同研究や個人情報保護の観点から

もとから公開できないものがあるというのと同じ話である。

【質疑応答】
1.経済安全保障重要技術育成プログラムに関して
Q1： 経済安全保障推進法における官民技術協力と経済安全保障重要技術育成プログラムの差異について、教えていただければ幸いです。
A1： 経済安全保障重要技術育成プログラム（以下、「経プロ」という。）は、研究開発事業の一つである。予算をつけて、実際に研究者を公募して研究開発を進めていくという、国の政策ということになる。一方で、推進法における官民技術協力というのは、経済安全保障推進法でエンカレッジする対象となる、経済安全保障上の重要技術を育成する取り組み全般を官民技術協力と呼んでいる。この推進法における官民技術協力の具体的手段が官民協議会であり、官民協議会が置かれる対象が経プロということになる。逆に言えば、経プロ以外の様々な研究開発事業にこの官民協議会を置くことによって、法律における官民技術協力となっていくことになる。部分集合関係のようなもの。

Q2： 市場経済のメカニズムのみに委ねていては投資が不十分となりがちな先端技術とは具体的にどういった分野の技術になるとお考えでしょうか。
A2： 公的利用に活かしたい場合でも、どうしても民生市場が必ずしも大きくない、非常にニッチなものであっても、国として必要な技術があるということ。
具体例として、経プロが対象とする技術の中で、例えば領域横断・サイバー空間、バイオ領域という、この縦の枠の中に「支援対象とする技術」というものがある。その上から２番目に、「不正機能検証技術（ファームウェア・ソフトウェア/ハードウェア）」というのがある。将来的には、セキュリティソフトの会社といった民生市場が商売としてやっていくことはあると思う。ただ、喫緊の課題としては、国の重要施設、空港や鉄道、水道といった社会インフラの基幹システムをチェックすること。民生市場が大きくないなかで、国として持っておかなければならない技術ということでこういうものを対象とした研究活動を支援することとしている。

Q3： シンクタンクに蓄積されるデータを活用するといったお話がありましたが、このシンクタンクはどの程度の規模と権限を想定しておられるのでしょうか。
A3： シンクタンクの部分は、まだ検討中ということと、少し文科省の権限を超えるところがあり、お話できることは少ない。言えることとして、昨年度と今年度で、政策研究大学院大学（GRIPS）へ内閣府が委託をして、主に経済安全保障に強いシンクタンクを作るためにはどのようなあり方が望ましいかといったことを調査研究してもらっている。具体的な立ち上げは令和５年度を目指している。海外の例では、米国の RAND 研究所が有名。日本の国情に合った形でシンクタンクを創設するにはどうすればよいのかの研究をしているところ。

Q4： 応用段階の技術であっても研究である以上、論文公表といった情報の公開もまた避けては通れないものだと理解しておりますが、ここで想定されている研究は特許の非公開化と絡めて、公表しない技術研究を想定されているのでしょうか。
A4： 大学の先生方には誤解をされている方が多いため丁寧な説明が必要になるところである。結論から申し上げると、経プロと特許非公開制度は別物であり、この経プロで得た成果が全て特許非公開の対象になるということではない。先ほど申し上げた通り、経プロは、原則として研究成果は公開であり、日本版バイ・ドール規定である産業技術力強化法第１７条により特許も研究を実施された先生や研究機関に帰属する。一方、守秘義務がかかっている情報に係る部分はクローズにしていただく。

特許非公開制度については、制度設計中のため確たることは申し上げられないが、特に防衛装備品や核兵器に直結するような技術の特許が出てきた場合には特許非公開制度の対象になりうるが、実際のところそういったものはほとんどないのではないかと個人的には考えている。

Q5： 当プログラムと先端技術における国際連携について、教えていただければ幸いです。

A5： 非常に重要な論点だと思う。現時点で経プロに関しては、海外連携をどのように行うかというのは、通常の民生プログラムのようにどんどんやりましょうということでもないというのが現状。ただ、いわゆる同志国（like Minded Country）といった法の支配や自由経済といった基本的価値観を共有する国々との間では、国際連携を進めていく価値があるだろうというのは一般論としてはある。今後は国際連携も念頭にしながら制度設計を進めていくと考えているが、最初からできるかどうかはわからない。

2.科学技術振興機構、その他競争的研究費に関するご質問

Q6： 科学技術振興機構（JST）などは産官学が一体となって国の政策に合わせた調査研究を行う場となっており、これらは人材の育成や研究開発の強化、ファンドなどの役割は果たしていると思われますが、情報の共有といった観点から今後さらなる発展を図るために、企業や学術機関に対してどのような働きかけが有効であるとお考えでしょうか。

A6： 産学官が連携してやっていこうというのは、２，30 年前から文科省も経産省もやっている施策ではある。しかし、機微情報を扱う分野では、産学連携や産学官連携が進みにくかった。そういう中で、経済安保推進法に基づいて官民協議会が作られることによって、産学官連携を行いたかったが制度が整っていないため重要な情報を得られなかった研究者が、そうした情報を踏まえて自分の研究の新たな発展の場を得られるようになったのではないかと考えている。

Q7： 半導体の研究、レアアースの確保と NEDO や科研費等の関係性について、教えていただければ幸いです。

A7： JST と NEDO と科研費の関係について。科研費はボトムアップ研究と呼んでいて、研究者の先生が自らの科学的興味に基づいて自由に研究をしていただくというもので、国の目的に合致するからやるというものではない。

一方で、JST や NEDO について、元々JST は文科省所管で NEDO は経産省所管という所管省庁の色の違いがあるが、一定の目的を持った研究開発資金となる。JST はどちらかというと科学技術の振興ということで、０から１を生み出すような、あるいは１を 100 にするような、基礎研究のフェーズを、国として、こういう領域や技術を発展させたいというターゲッティングをした上で研究開発を進めていくというのが JST になる。NEDO は、基礎的なところから出てきた成果を、いかに製品にするためにチューニングしていくか、あるいはプロトタイプは作れたものの製品とするためにはこれを量産していかなければならないときに、量産していくためにはどういうふうにすればいいか等、より産業側に近い研究開発をしている。大学というよりは企業を相手に研究活動を進めているという役割分担である。

半導体やレアアースの事例で JST と NEDO で具体的にどんなことを行っているかについて。半導体であれば、企業が作っている半導体が今足りなくなっているため、日本としても自ら半導体を作れるようにすること、また、今の半導体に変わる、数年先には社会実装できるような効率の良い半導体を作ろうとか、このようなことを行うの

はNEDOになる。一方でJSTは、半導体の概念を変えるような次世代の半導体を作って、10年先ぐらいに社会実装を目指していこうというようなものを研究開発する。

レアアースで言うと、日本にあるがかなりコストをかけなければ採掘できないというようなものを、日本でも安く採掘できるようにしようと、安価で手に入れられるようにしようというような研究開発はNEDOの領域になる。一方でJSTは、レアアースを使わなくても何かできるようにするためにはどうするかとか、ある種概念を変えるような研究開発をしている。両者が連携をしながら、基礎研究の成果をいかに社会に出していくかというようなことで日々精進している。

Q8： 大学や研究機関・民間企業は、我が国の経済安全保障を確保するために必要不可欠な存在であり、経済安全保障重要技術育成プログラム等で、研究資金や競争的研究費を配分していることと思われます。そして、これらの資金提供先のほとんどは、理系分野に限られていると理解しています（人文学、社会科学系等の競争的研究費は「課題設定による先導的人文学・社会科学研究推進事業」のみであったと理解しています）。もっとも、経済安全保障は国際ルールを守らない国家の脅威等の背景があり、今後どのような国家が経済安全保障上脅威となってくるのか、といった判断を基に、重要技術やサプライチェーンについて政策判断を行っていく必要があると感じます。その意味で、今後は、人文社会科学系等についての大学や研究機関、民間企業へ競争的研究費を配分し、経済安全保障の政策判断に協力してもらうことが必要となってくると考えています。将来的に、競争的研究費を拡張し、人文社会科学系等へ資金配分をすることは考えられるのか、教えていただければ幸いです。

A8： これも非常に深遠な課題。特に人文系の先生方からはよく言われることもあるが、競争的資金全体でいうと、理系はお金がかかる。例えば課題数が３つの場合、理系の課題３つと文系の課題３つで全然単価が違うという現状がある。したがって、資金が理系に偏っているという見方になってしまうこともある。その上で、競争的研究費の中でも、科研費に関してはかなり人文系の研究者の先生方の研究を支援しているとは思う。もっとも、こと経済安全保障ということになると、文科省に関しては技術というところに寄るので、経済安全保障の文脈で人文系の研究というのは、ストレートには結びつきにくいと思う。

しかし、人文系の研究については、経済安保だけではない。ライフサイエンスの研究等、先端技術は使い方を間違えると悪いことにも使えてしまう。よくELSIとか言ったりするが、単に新技術を作って喜んで終わるのではなくて、それをいかに社会でよりよく使っていくかということも同時に必要となる。研究開発プログラムの中で予算額的にはそんなに大きくないが、ELSI課題みたいなのも進めていくというものがあるので、経済安全保障においてもこのようなことをしっかりやっていかないと、国民の理解はなかなか得られないところもあると個人的には思う。

もう１点、国際秩序の維持強化について。ここは多分に外交の世界であるが、日本は技術で勝ってビジネスとかルールメイキングで負けると言われることもある。技術だけではない勝負の場があると思うので、経済安保の世界の中で、人文系の方のお力を借りるところは十分にあると思っている。

（追加質問）

Q9： オーストラリアに関して、文科省としては先端技術等の観点に関して、どのような見方をしているのか、また、これからどのように関わっていきたいのか、教えていただければ幸い　です。

A9： 技術を育てるという観点でいうと、オーストラリアは、アメリカ等に比べると、そこまで日本の先を行っているということでは必ずしもないと考えている。逆に言うと、日本と同等のレベルなのでうまくやれることがあれば一緒に高みを目指していき

たいということはある。一方で、技術を守るという観点で言うと、課題意識を持って取り組んでいる国であると認識している。意見交換を行いながら、我々も参考にするべき国と考える。文科省の立場として、技術を守るということは、とにかくガチガチに規制して全てクローズにすればいいということでは決してないが、危ないことにしっかりリスクマネジメントをする必要もあるため、そのうまい塩梅については、オーストラリアは先進的な国と考えている。

Q10： 仮にシンクタンクを設立することになった場合、アカデミアとの連携については、国立のアカデミアと連携していくのか、それとも私立のアカデミアとも連携していくのでしょうか。また、他に文科省以外で、省庁として連携していく、その省庁がどこになるのかについて教えてください。

A10： 政府側としては、国立だから私立だからとかは関係ない。ただ、私立はそれぞれの建学の精神に基づいて設立・運営されているため、あえて国からの委託などを受けるのではなく、むしろ自分たちで独自にシンクタンクのようなものを作り、独自の立場から政策提言をするのが私立としてのあり方ではないか、みたいなことをおっしゃる先生もいるようだ。

どういうところをステークホルダーにするかという話について。欧米の例を考えると、アカデミアやシンクタンクといっても技術関係だけではなく、完全に外交に特化したシンクタンクはあるが、ここでいうシンクタンクは主に技術を対象としたシンクタンクを指す。そういう意味で国際的な先端技術の動向などを、単に公開されている書誌情報とかだけではなく、人的ネットワークでいろいろ収集してもらえるような人材はまさにアカデミアの先生であり、必ず参画していただきたいと考えている。もっとも本件は純粋にアカデミアだけの問題だけではなく、やはり技術をどのように使っていくかという使う側の意見も当然重要になってくるので、使う側・ニーズ側の人たちにも参画してもらうことが必要。ニーズ側というのは、企業やビジネスセクター、パブリックセクターといったところだろう。まさに産学官が結集するようなシンクタンクが必要だという概念的なところはあるが、実際どこがというのはまだまだこれからということになる。

Q11： 経済安保推進法が可決され、法的な整備がなされ研究者の方々も情報提供等を受け入れることができる、提供できるという観点についてのご質問です。これら提供された情報流出の罰則等をみると、国家公務員法や地方公務員法の守秘義務と同等の罰則であり、素人目から見ると罰則的には軽いものであると感じます。特定秘密保護法の中では、安全保障上重要な情報に関してはかなり重い制約がかかっている一方で、経済安全保障に関する情報には現状軽いものになっていると感じます。今後重要技術等の情報はかなり機微な、安全保障に深く関わっていくとなった際に、特定秘密保護法の中でも経済安保上機微な情報を法的に追加部分として、安全保障上の特定秘密ということで重い罰則をかけていく必要があると個人的には思います。このようなことが考えられるのか、教えていただければ幸いです。

A11： 特定秘密保護法があるのはその通り。もっとも、今回の経済安全保障推進法でこのような協議会を作りそこで共有することを想定している機微な情報は、そもそも特定秘密レベルのものではない。役所の中でいくつか機密のレベルがあるが、その中で飛びぬけて一番上が特定秘密になる。そこまでいかないけれど、全く何の手当もなしに外部に出すことは禁じられているというような、守秘義務がかかっているレベルの情報を出すことでもかなり新しい取り組みになる。国家公務員法において国家公務員が規制されている罰則と同等でないと、民間の人になった瞬間に罰則が重くなるということは、公平性の観点でおかしいということで、国家公務員と同じ懲役1年以下また50万円以下の罰金ということで罰則を科している。

文科省的な立場で申し上げると、法制的な平等性ということで国家公務員法と同等の罰則を科しているが、アカデミアの慣習からすると、これでもなかなかという感じ。そこから罰則を上げていくと、そもそも参加する人がいなくなってしまうという懸念がある。機密性を軽んじるわけではないが、ここら辺から始めることが妥当であると考えている。

Q12：　以前は、官公庁は有識者の方々と共同して研究する際に、相互に秘密保持契約を結ぶ形で、それなりの責任を負ってもらうよということを書いた上で、情報共有を行っていたところですが、それに比べると経済安全保障推進法においてはさらに刑事罰でも担保されることになったところかと思います。実際この話が出たときに、アカデミアの方々のご反応でありますとか、今現在、現場からいろんな形で寄せられている声のようなものはありますでしょうか。

A12：　大学の先生方とこの制度について意見交換している中で、ファーストインプレッションとしては、研究に罰則付きの守秘義務をかけるなんてとんでもないというものである。アカデミア・学問というのは自由でオープンであるべきものであって、人類の知的資産にすべきものという原則論から言うと、ファーストインプレッションは忌避感があったのではないかなと思う。

もっとも、この法律が成立したから、文科省の科研費等を含めて、あるいは運営費交付金も含めて、全ての研究開発がこの法律に基づいて罰則付きで云々やらなきゃいけないのかという制度ではない。経プロは法律上、必置になっているので置かれるが、他のものについては、このような座組を作った方がいいと思うのであれば置いていいよという、＋α の任意のものであり、既存の研究に影響を与えるものではない。経プロについても、フィロソフィーとしては、再三申し上げている通り、研究成果は原則として公開であり、特許もどんどん取得して、それを実施してくださいということになる。

ただ、守秘義務の情報が必要なところだけはクローズにしてくださいねということである。これは企業と研究をする時に営業秘密等を秘密にする必要があるというのと同じである。むしろ研究者の先生が、このような制約はあれども、自分として今までアクセスできなかった行政機関が持っている情報を使って研究を進めたいのだという思いがある人はやってもらえばいい。これにより今までは官公庁が情報を提供できないため全くできなかった研究が＋α でできるようになるといったものであり、アカデミアの研究の範囲を広げるものである。もともとはそうした研究には官公庁は原則として情報を提供できず、アカデミアも研究ができなかったところであるが、それを可能にする仕組みである。

また、この制度は任意であって、国から押しつけられるものでもない。こうした説明をすることで、むしろ研究の範囲が広がることについてわかっていただきつつあるのが現状だと思う。今後、実際の運用が始まる中でも、丁寧な説明を続け、丁寧に伴走して理解を得ていくこととしたい。

Q13：　先ほど豪州の情報を守るという点で豪州の制度等が参考になるとおっしゃっていましたが、情報を守る、研究開発を守る、制度を改善していくという点において、各国制度等の中で念頭に置こうと考えているものはございますか。

A13：　研究インテグリティの方の話になるが、これは日本で緒についたばかりということもあって、ある程度最初の制度設計の段階でアメリカ、あるいは欧州、それから豪州、いわゆる同志国の取り組みを参考にしている。特にアメリカについて、ＪＡＳＯＮ　Ｒｅｐｏｒｔがかなり参考になる。ただ、繰り返しにはなるが、これは緒に着いたとこである。

大学の事務の執行部の先生方と話していてよく言われることは、実際研究してい

る研究者の先生方は、研究を進めるためなら多少は危ない橋を渡ってもという人がいないわけではない。そうした中で執行部から、マネジメントサイドからそのリスクマネジメントをすることの難しさがある。

また、アカデミアにおける外国影響というシチュエーションで技術スパイの活動について、一体どのようなことが実際行われており、どのように対策をすればいいのかが大学・文科省にはわからないところもある。この部分については、他国も実際の実例は機微なものとして教えてもらえず、一般論のみが語られるという場合も多い。

そのため日本における研究インテグリティをより実効的なものとしていくためには、我が国自身による経験の積み上げが必要になる。実際にどのような危ないことがあり、それをどのように防いだのか、ここら辺のプラクティス作りみたいなところをどのようにやっていくのかということが、今の課題であり、難しいことであると考えている。

Q14： 経済スパイへの対策は重要である反面、それが安全保障に関係なく特定の国の研究者や留学生を排除する過剰反応につながることも懸念されます。こうした点について、文部科学省として気をつけている点をご教示ください。

A14： 日本の科学や大学の状況を踏まえると、特定国と完全にデカップリングすればよいという単純な話ではない。アメリカも同様で、論文の共著や共同研究、人の行き来を全体として統計的に見ると、各国の関係は量的にはむしろ太くなっている部分もあるようだ。政治経済では確かにデカップリングをある程度進めているものの、科学の世界では安全保障のコアになる部分はデカップリングを進めても、その他の部分とは切り分けるような対応もあり得るようである。

その意味では研究に関して、国籍で判断するというよりは中身で判断していくべきだ。そのため、研究インテグリティに関しては、本来は国による規制的手段ではなく、マネジメントが適切であり、大学側が一つ一つ良し悪しを判断していく形が望ましい。国が前面に出る規制と違い、国はあくまでもサポートにとどまり、アカデミアの自主自律的な取り組みに任せていくべきである。

Q15： JASON Report では、学術機関の幹部に対しては、インテリジェンス機関と執行当局が連携して、エビデンスを持った上で、様々な形で研究成果を窃取されるリスクを説明する必要があるとされています。我が国では公式な仕組みとして、大学と司法関係者が対話を行い、連携するというのはあまり聞いたことはない。他国なども含めて、実際に我が国でこうした仕組みを構想する場合に、文部科学省の範囲内ではどのような仕組みというものが現実的なものとして考えられるのでしょうか。

A15： 突然大学にインテリジェンス機関が来訪して説明を行うとしても、動揺することもあるだろう。国立大学であれば、国立大学協会のように、大学の連合体に説明を行い、その後、個別の大学ごとにアプローチするという方法もあるだろう。最初は国と大学の連合体で繋がり、その後、現場レベルで繋がっていくことが望ましいと思う。

Q16： 経済安全保障の観点から、他国が官民一体となって協力を進めている状況が見られるところ、我が国も企業・大学との連携の枠組みを作っていくべきと考えますが、大学の情報を霞ヶ関の中で一番有している文部科学省だと思いますが、大学からの情報を首相や内閣官房の方に伝える機会というのがそもそもあるのか、大学や企業も国に情報提供する必要があるという要望がもしあるのであれば、教えていただきたいです。

A16： 大学や企業では情報が分散していて、フォーマットも違うことも多く、集約する

のが難しいという背景がある。政府はある意味一体なので、省庁間の連携は日常的にある。アカデミアに関して言えば、アカデミアから、守秘義務のある情報を提供されることもあるが、運用が明確でない。アカデミアから国に対して情報提供された時、機微な情報であった場合は経済安全保障推進法の枠組みを活用していくのではないかと思う。

Q17： 経済安全保障という文脈では、技術流出や科学者の流出が話題に上がることが多いというふうな印象を受けます。とは言いつつも、科学の振興を考えると、その研究者にとって魅力的な研究環境づくりという観点では、自由社会として大学の自由な環境というのは日本の魅力ある資源と考えています。中国や米国などと先端技術の競争が起きていますが、我が国として研究者が魅力を感じて研究できる環境や処遇に関して、具体的にはどういう点を改善していけば、我が国に技術者が定着し、技術開発が頻繁に行われるようになる状況を作れるかという点について、ご見解をいただけないでしょうか。

A17： アメリカに行った日本人研究者に話を聞くと、個人的な意見ではあるものの、日本人ゆえ、最終的には日本で研究したい、日本のために研究したいという人はかなり多いのが確かである。魅力的な研究環境を日本に構築できれば、一度海外に行った人でも、日本に戻ってきてくれるのではと考えている。

実現に関しては研究費と雇用の問題がある。研究費の絶対的なボリュームに関しては見劣りしており、アメリカのようにとなると 10 倍くらいになりいきなりは難しいが、少なくとも今よりは増やしていく。

また、雇用の問題、特に若手の雇用環境が非常に厳しい状況になっている。任期付きの研究者の正規雇用という問題は非常に複合的な問題で、単純に一部の問題だけを手当すればいいものでない。しかし、あえて言えば、安定したポストを増やす、または研究費とポストを増やす、研究施設内の機械を壊れたまま放置するのではなく、十分使えるようにすることで研究者が研究に専念できるような環境を作っていく必要がある。

一方で、自己修養のため海外に行くことや、ポストを変えて自分の研究したい分野のため、研究しやすいところにステップアップするための支援も必要なことである。

Q18： 我が国に海外のスター研究者を招聘するという考え方もあるが、一方でそのような研究者を我が国呼ぶために改善すべき点は何があるでしょうか。

A18： よく言われている話だと、給料の問題がある。海外では、トップ研究者は数億円規模で雇われたり、ベンチャー企業で成功してビリオネアになったりするが、学長以上の給料を外国人研究者に渡すというのは難しい。しかし、国立研究所の一部ではそのような動きはある。

また、帯同する家族の問題もある。お子さんに英語を学ばせられる環境や配偶者が日常生活で溶け込める状況が東京であればまだしも地方ではなかなかない。そのため、定着しづらい。

Q19： 外国人研究者が安心して研究できる環境づくりということで、外国人研究者の福利厚生のあり方や家族の生活環境づくりを大学と自治体が協力して包括的に支援することを考えられるのでしょうか。

A19： トップ大学であれば WPI という政策をやっているところがある。また、大学といえども事務員まで英語が流暢であるわけではないが、国際化が進められているので、少なくとも世間一般よりは英語が通じるため、外国人研究者を家族も含めて受け入れやすく、実際に受け入れているところもある。 OIST は典型例で、沖縄は米軍

基地があることもあり、他地域に比べ、国際的で受け入れられやすい。
　余談だが、かつて核融合の仕事をやっていた際、六ヶ所村で国際研究拠点を作ったが、青森県等が国際学校を作ったり、交流行事として盆踊りを行ったりしていて、町ぐるみで溶け込みやすい環境を作っていた。町ぐるみでやっていただければ、地方大学でも外国人研究者とその家族を受け入れられる環境を作れるのではないかと思う。

Q20：　台湾の TSMC と九州の九州大や高専が連携して、人材育成について様々な施策を行っていますが、TSMC 側としては、日本には人材が豊富にあるから、その人材をどんどん育成していこうという考え方があったというのをお聞きしました。今後、経済安全保障に関して、国際連携が進んでいく中で、日本の強みは人材にあるのではないでしょうか。

A20：　TSMC の誘致に当たって、九州の大学、高専を巻き込んで取り組んでいるのはおっしゃる通りである。最近研究力の低下や博士課程に進む人数の減少という状況に直面しているものの、日本の研究のポテンシャルは未だ高い。
　全分野で人材育成に支援していくのは資源の分配としては難しいが半導体に集中的に政策資源を投下してかつ人材育成も含めてやっていくと、かなり日本は強くなっていくのではないか。

Q21：　現在、TSMC と九大や九州の高専の連携などが行われているという状況の中で、文科省としてはどういった協力を行っているのでしょうか。実際に台湾からどのようなことを求められているのでしょうか。

A21：　直接担当してないので申し上げられること限られるが、文科省としては、TSMC の工場の支援を行うのは、日本の半導体産業の復権のため、ここを起点に日本の半導体産業を復活させていくというその将来的な意味での人材育成である。政府の役割として人材育成や産業振興のため、高専とか九大と熊本県が連携する。一つの政策パッケージで、企業立地と周辺の大学、高専が大規模に連携するのは今までなかった。文科省としては、そこで育成した人材が TSMC の工場だけでなく、日本全体の半導体産業の復権のための人材になっていくということを期待して施策を行っている。

以上

記録作成担当者：岡本樹、香高優一郎

ヒアリング調査報告 No.14　基本情報

日時	2022 年 8 月 26 日
テーマ	安全保障の歴史的経緯及び経済安全保障の各論について
ヒアリング先 (担当者)	元国家安全保障局次長 現同志社大学法学部教授 兼原信克 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凛香、岡本樹、織田秀夫、香高優一郎、宮内拓、山田麻友 (計 7 名)
調査目的	元国家安全保障局副局長を務めた兼原先生の知見や経験を聞いた上で経済安全保障の考え方を学び、今後の研究に活かすこと。

(写真)

【質疑応答】

1.安全保障全般について

Q1：　2010 年に尖閣諸島漁船衝突事故が起こって以来、我が国でも安全保障について議論が活発な傾向にあると思います。しかし、2014 年に NSC や NSS の開設、2020 年に経済班の設置と、若干タイムラグがあると感じました。これは我が国の政治の現場における軍事への忌避が原因で遅くなったのでしょうか。ご意見を伺いたいです。

A1：　内閣制度の強化や NSC の設置と個別の事件はあまり関係がない。尖閣諸島の漁船衝突事件大きな問題だが、日本の安全保障の全体像の中では、あまり大きな問題ではない。

　NSC は、安倍晋三元首相がいたからできた。安倍さん個人の発想で出てきた話で、官界は外務省、警察庁、自衛隊、防衛省、内閣法制局が全員反対した。第一次安倍政権で出た話だが、辞任で宙に浮き、第二次安倍政権で復活したため、尖閣事案とは全く関係がない。

NSC が生まれた背景は、日本の統治体制の歪みにある。

・NSC が強い権力を持つ背景

日本は、長い間、政権交代がなかったため、立法府と行政府が癒着していた。立法府と行政府を含めて、利益集団が縦割りになっており、色々な縦割り集団が互いにぶつかり合って自然調和を現出し、その上に、総理官邸が乗っかっていた。象徴天皇ならぬ象徴総理と呼ばれててもおかしくないほどその権力基盤は弱かった。自民党は、冷戦下の 1955 年の社会党統一により、社会党に政権を渡さないために保守政治家が集まってできた政党だ。そして、政府・自民党がアメリカの声を、社会党・共産党がソ連の声を代弁した。国会の議論はほとんどがイデオロギーがかった安全保障論議で、しかもその議論の中身は双方とも真逆の議論をするので国民的コンセンサスを作るうえでは意味がなかった。個別の政策は全て役人に丸投げであった。当時、高度経済成長で、お金（税収）もどんどん入ってくるため、役所もやりたいことがたくさんあり、そこに国会議員が縦割りでくっついてくる、これが「昭和の政治」だった。この体制が終わったのが平成である。冷戦が終わり、社会党が崩壊し、自民党の役割が終わったとき、現状に危機感を覚えた小沢一派など自民党から飛び出た議員が、自民党と共産党以外の全員で組閣した。これが「八党連立政権」だ。左右双方が連立したため、政権内に不和が生じやすく、社会党がすぐに離脱した。

そして自民党とくっついてできたのが「自社さ連立政権」だ。これもうまくいかなかったが、その後、小渕政権から公明党と連立した自民党が与党の座に居すわる時代が続いた。リーマンショックの後、自民党が下野し、民主党政権となったものの、再び安倍政権で自民党が返り咲いた。この間、三回も政権与党が変わった。そのため政治が圧倒的に官僚より強くなった。国民が主権を行使したといえる。その過程で、総理官邸が力をつけた。象徴天皇の総理大臣から、将軍型の総理大臣にかわっていった。これは以下の理由による。

まず、小選挙区の廃止だ。中選挙区のように、自民党同士が戦うこともなくなり、派閥が必要なくなった。そのため、派閥が力を落とした。

また、総理官邸機能が強化されたことも挙げられる。阪神大震災前、総理官邸に防災機能がなかったが、当時の国土庁では対応できなかった。その反省から森政権のときに総理官邸機能強化が法律化された。その内閣法の改正法案に際し、総理大臣発議権が生まれた。その関係で、総理の秘書室たる内閣官房が、内閣重要施策に対する総合調整権限を与えられた。それ以前は大臣の決裁が降りた後に各省庁から上げられてくる文書を内閣官房は拒否できなかったが、森内閣以降、大臣の決裁書だろうが、「それは総理の考えとは違う」と言って突き返せるようになった。こうした総理官邸権限の強化の過程で NSC が生まれた。だから NSC ははじめから非常に強い権力を持つ組織となった。

・NSC の生まれた背景

中曽根政権まで遡る。中曽根総理は戦後初めて、象徴天皇ではない、大統領的な総理を志向した。そして、内閣官房を拡充強化した。彼は総理官邸の業務を外政、内政、それから安全保障の三つの分野に分けた。中曽根官邸の失敗は、外政と安全保障を官邸内で切り離したことだ。世界中どこでも大統領府や首相官邸では外交と安全保障を結びつける。それが総理の仕事だからだ。しかし中曽根総理は、そうはせず、安全保障と防災支援を結びつけ、外交を切り離した。しかし、外交と軍事を総合調整するのは総理官邸のはずなのだ。

また、小渕・橋本政権下で、防災機能が膨れ上がり、安全保障が若干疎かになった。しかし、突然、第一次安倍政権で安倍首相が、NSC がないのはおかしいと言い始めた。おそらく、総理からすると、外務省や防衛省と個別に話すより、自分のために話をまとめる存在を欲したのかもしれない。また、米国のホワイトハウスから見ても、安全保障に関し、日本のどの省庁に話せばいいかわからなかった。そのため、総

理官邸内に、統一的に安全保障を担当する部局として、NSC が生まれた。対外的な色々な危機があるから創設したのではない。中国も NSC を作った頃にはまだ日本と大差ないほどで、真の脅威たり得なかった。対中関係が厳しいから NSC を創設したわけではない。北朝鮮も脅威ではあったが、NSC を創設した理由ではない。

Q2： NSC や NSS が設置され、数年が経ちましたが、運用上のさらなる課題点や今後期待する方向性などがありましたらお考えをお聞かせください。

A2： 冷戦後期は、西側プラス中国でロシアを抑えてきた。その反動で、本来非同盟のインドは、ロシアに近づかざるを得なかった。今、インドと中国は立場を入れかえつつある。中国が米国と対立関係に入り、インドがロシアから米国に軸足を移しつつある。そのタイミングをうまく捕まえて打ち出したのが安倍総理の「自由で開かれたインド太平洋」構想だ。世界中の国々の外交に影響を与えた。

中国は独裁国家だったが、インドは民主主義国家だ。西側とインドの連携は、太平洋とインド洋を自由主義国家の連携で結ぶことになる。大西洋と合わせて地球的規模で自由主義的国際秩序が立ち上がる。但し、インドは、対中牽制上、ロシアとの関係は引き続き重視せざるを得ないし、また、非同盟主義なので、クアッドに加盟してはいるが、軍事的なことにはつきあわないだろう。日本も様々な国内事情等から軍事的な協力には制約がある。だからアメリカは英豪と AUKUS を作ったのだろう。

ロシアの凋落はあるが、中国の台頭は著しい。NSC は防衛力整備に力をいれるべきである。日本は 76 年の第一次防衛計画大綱以、防衛費 GNP１％の制約があり、また、島国の特性を生かしてソ連軍の侵攻に対して限定小規模対処という戦術をとることになっていた。すなわち、日本の防衛体制は米軍が来援に来るまで北海道を持たせるというのが冷戦期のドクトリンであった。日本に来援する米軍部隊はシアトルとハワイにいるが、10,000 キロを船で渡るには数か月かかる。それまで北海道で持ちこたえるという計画でかつて自衛隊は動いていた。70 年代は日本でも左派が強かったので、冷戦がデタントに切り替わった頃に、三木内閣で「現状凍結」路線を打ち出した。それが防衛費 GNP１％のシーリングである。

台湾有事には、米軍は日本に来援するわけではない。台湾有事の際には米軍は台湾に行くことになる。今のままの自衛隊では中国軍の本格的な攻撃があれば到底持ちこたえられない。台湾有事の可能性は現実にあり、中国との紛争になる可能性はみえてきたのに、予算が全く足りない現状がある。中国軍と向き合うには GNP２％の防衛費でも全然足りない。防衛省には真面目にどうにかしないといけないという危機感がある。

有事には、これまで机上の空論でしかなかった安全保障関連の法律を改正しなければいけない。例えば、国民保護法は日本有事専用であり、台湾有事の際は使えないため、台湾在住邦人や、先島の住民、ひいては中国在留邦人を避難させなければいけないが、日本が攻撃されない限り始国民保護法を用いて自国民を避難させられない。

さらに有事の際の閣僚レベルの訓練も足りていない。政治サイドの問題として、国会論戦は政局の色が濃すぎ、政策の話をあまりしないため、議員の中でも特定の人しか安全保障の勉強していない。しかも、日本の総理は平均で 1 年 10 か月の寿命であり、短期政権が多いうえに、内閣改造も多い。与党議員 400 人の中から閣僚を選ぶのだが、これをコロコロ替えている。なかなか腰が据わらない。だから演習が重要なのだが、有事の勉強や訓練はほとんどやっていない。日本の行政は地震に関しては強い。関東大震災の日に災害訓練を総理以下全大臣で行う。だから大地震の際に自分自身のやることが分かる。ところが、有事の訓練は大きな批判が予想されるために実施していない。しかし、日ごろの訓練がないといざというときに動けない。未だに指揮系統等、政府全体を有事に指揮する体制がかちゃんとできていないので、これをやらないといけないと考えている。戦争になれば、軍事と外交だけではない。それにプラ

スして安全保障面から内政を仕切らないといけなくなるので、全閣僚訓練をやっていくべきである。

2.経済安全保障における科学技術について

Q3： 従来、日本では安全保障に関する研究になかなか進展が見られない状況にあると言われています。その要因として、CSTI（総合科学技術・イノベーション会議）に防衛大臣や外務大臣が参加できないこと、安全保障に関する研究開発に予算がつきにくいこと等が挙げられますが、これを解消するため、産官学が連携して経済安全保障に関する研究開発を推進するための制度上の解決策・改善策としてはどのようなものが考えられるでしょうか。

A3： 学術会議は象徴的な問題で基本的には戦後の学術界のあり方の問題。戦勝国においては、軍事研究と科学技術研究開発は表裏一体である。世界中どこでも、軍事があるからこそ科学が進歩する。なぜかというと、マーケットとは関係なく、国家安全保障のために際限なく資金を使えるからだ。目的はお金儲けじゃなくて戦争に勝つことだから、一番ハイリスクな研究は軍事で行う。

日本も戦前はそうだったが、敗戦後、占領軍に軍事関連の研究開発をすべて停止させられた。50年代はマルクス主義が全盛期で、急進的な社会改造を議論する雰囲気が強く、大学は非常に左傾化していた。教員たちは理系も含めて、ほとんど皆、マルクス主義者だった。ソ連のマルクス主義が正しいという雰囲気だった。冷戦が始まって、米国の要請で日本が再軍備した一方、学会では非武装中立を標榜する人が多く、米軍や防衛省と協力する研究は絶対不可能な状況になった。

つまり、学術界は防衛省とアメリカのペンダゴンとは絶対付き合わないということだ。しかし、軍事研究と民間研究の境は、実はよくわからない。実際に起きていることは、もっと単純に防衛省関連の予算の研究や、米国防省関連の研究はしないということだ。

ところが技術的な進歩が最近凄まじい。特に情報技術、宇宙技術が素晴らしい進歩を遂げている。日本は何とかしなくてはいけないのに、学術界は腰が重い。戦後一貫して、文科省、学術会議、国立研究所、国立大学には、それなりの資金が提供されており、今でも100兆円予算のうち、予算4兆円が文科省、経産省などを通じて学術界に回されているが、絶対に防衛省のために使わせないようにしている。そのために、学術界と防衛省との間に断絶が起きている。これが敗戦国の十字架を背負った日本の最大の問題だ。防衛省には1600億円しかまわらない。一民間企業以下の技術開発予算だ。

外国では、科学技術と軍事の関係は、非常に密接な関係だ。科学者とは基本的にオリンピックに出るアスリートのようなもので、世界最先端の研究や技術開発を行いたいから、お金や家庭生活など関係なく研究に没頭する人が多い。もっとも、画期的な研究は何万人に一人しか成功しないという、厳しい世界だ。このようにして、基礎研究や応用研究が行われている。しかし、発見や技術開発があっても、利益を上げるためには製品化が重要で、企業は将来儲かる研究や技術より、今稼げる研究や技術を重要視する。そのため、研究や技術がマーケットに出ずに死んでいく。これを「死の谷」の問題と言い、世界共通の課題となっている。

しかし、経産省等が補助金を出すと市場原理を守るWTOの規定に抵触してしまう。したがって、アメリカでは、安全保障例外を用いて、マーケットがなく死んでしまう研究や技術に、委託研究という形で資金を提供する。根本的に最先端分野を切り開いていかない国が負けると考えているからだ。軍事技術ではなく、科学そのものが安全保障という考え方である。そこから、素晴らしい研究や技術が生まれてくる。これは軍事技術だけの問題ではなく、科学技術全般の話である。ここから生まれてくる新興大企業を、マーケットでは「ユニコーン」と呼ぶ。好例として、モデルナが挙げられ

る。モデルナ社は、アメリカで発生した炭疽菌テロ事件の際、炭疽菌を至急中和するものを作るためにFBIから資金提供されて大きく成長した。そして現在では、コロナワクチンの開発で大儲けしている。

このように、安全保障例外を用いて、アメリカ政府は企業を支援している。もちろん、このような企業のほとんどが潰れるものの、僅かに生き残った企業が大きく変貌する。そして、そのような企業は自分自身で莫大なお金を使って技術を高度化していき、その民間技術を用いてアメリカでは軍事技術等に応用している。市場の中でごく一部の企業が成功してユニコーンになり、自分の力で技術をどんどん発展させていって、それが政府に還元されていく。これを「ダーウィンの海」と呼ぶ。このようなアメリカの手法は、イギリスはじめヨーロッパでも多かれ少なかれ同じである。中国はもっと露骨で、軍民融合政策の下で産官学と軍隊が合体して研究開発を行っている。日本はまず死の谷は超えられない。学術界が開発した技術を市場に出すため政府から支援を得ようとするとき、成果が出ないという理由で、大した補助金が取れない。諸外国は安全保障の理由で資金提供しているため長期的な視点でこれを行うことができ、国民の納得も得やすい。単に学術は大事だと言っても、数兆円の予算である。国民にとっての利益が見えないなら理解が得られるわけがない。長期的な視点として国民に納得してもらえる具体的な利益としては国際的には安全保障ぐらいしかない。アメリカは国防総省の研究開発に10兆円をかけており、しかも成果を求めない。ハイリスク上等という考え方である。我が国にはこの仕組みがない。

実際、防衛省が100億円を積んで安全保障関連技術推進制度を作ったが、学術界は強硬に反対し、内閣府の日本学術会議が国立大学や国立研究所の研究者たちに資金の受け取りを拒否するよう通達を出した。そのため、予算が学術界には全く行き渡らなかった。逆に、年間4兆円の科学技術予算を払っても、学術界からは全く安全保障に関係するものが出てこない。

これは「おかしい」となり、岸田政権による、経済安全保障法の官民技術協力関連法で、官と学会と企業の技術者たちと交流させ、技術全般を支援し、安全保障に貢献する技術を育てようとしたのだ。この予算は2年間で5000億円だが、うまくいかないのではと恐れる。内閣府が舵を切っても、永年の学術界の考え方や体質は急には変わらないのではないか。

科学技術関連の資金は、科学技術振興機構(JST)と経産省NEDOに配分される。さらにJSTから国立研究開発法人と国立大学に、NEDOから産業技術総合研究所に資金が配分される。ただ、この研究所の研究者の人々は、従来の考え方の範囲内でしか科学技術を考えられず、あまりうまくいかないのではないかと恐れている。

成功する技術開発主体を作るためには、軍事技術や民生技術の区別や技術者の出身官庁が関係ない、全く新しい研究開発拠点の整備がいいと思う。防衛省や経産省や総務省が主管する全く新しい仕組みを作って、お金の流れを変えないといけない。

Q4： 現状、科学技術振興機構（JST）においては研究機関や企業と協力して研究開発や人材の育成について取り組んでいると認識しておりますが、情報の共有という点に関しては事業内容の柱の中に含まれておりませんでした。こちらで経済安全保障に関する重要情報を共有する機会は現在のところあるのでしょうか。また、ないとすればどのような点が問題となっているのかについてお聞かせ願いたいです。

A4： 経済安全保障といっても、科学技術全般の進歩が安全保障になる。そういう哲学が重要である。軍事技術のみを進歩させようという話は誰もいっていない。軍事技術は三菱重工のような民間防衛産業が研究開発するのであって、例えばJSTにはそのような役割を期待してはいない。最先端の技術が人間社会全般をどう変えるのかというのが根幹である。現在では、優れた民間技術が軍事技術に変わっていく。軍事が変わるから社会の技術が変わるわけではない。昔はスピンオフと言って、核兵器を作ったら

原子力発電所ができていましたというみたいに、軍事が先に引っ張ってスピンオフしていた。しかし、最近はありとあらゆる分野で最先端の科学がどんどん前に出ていき、それに応じて軍事技術が影響を受けている。スピンオンと言われる。したがって、軍事機密が降りてきて、それが共有できないといったような話はそもそも逆である。因果が逆の話となっている。

3.経済安全保障におけるサイバーセキュリティについて

Q5： 現行の法制度ではサイバーセキュリティは企業側の努力義務[1)]となっておりますが、企業経営者の意識レベルの差によって、対策にも差が生じてくるものと考えられます。重要インフラなどへのサイバー攻撃は、経済活動への影響のみならず、国民生活や我が国の安全保障にも広く影響することを鑑みれば、もはや企業の努力義務だけでは不十分と考えます。努力義務から一歩踏み込んで、例えば車の車検のようにセキュリティ診断を年一回実施するなど最低限必要と考えられる事項について義務を科すようなサイバーセキュリティ基本法改正にチャレンジすることは、最近の霞が関の空気感からすれば許容されるものなのでしょうか。先生のお見立てをお聞かせください。

A5： 私も全く同じ意見。早く法定義務にすべきと考えている。経産省を退官された元幹部と話をしていると、もう法定義務にしないと駄目だと言っている。今度できた経済安全保障推進法の中の4本柱の1本が重要インフラ法案。これは一言で言うと、西側の信頼できる国から以外から重要インフラのパーツは買うなと言うこと。だけど、経済安保の一つの巨大な柱サイバーセキュリティである。これが今回は外れてしまっている。サイバー基本法を作ったときには、まだよちよち歩きだったので、とりあえず民間頑張ってくださいという法律にした。

サイバー空間のゼロリスクを目指し、国がスタンダードを作って、このレベルのサイバーセキュリティにしてくださいと企業に示して、そして年に1回、国が検査するやる方が良いと思う。

アメリカとかは本当に重要な重要インフラは、政府クラウドに入っている。アメリカは日本と違って官民が合体しているので、Appleとか Google とかの最高水準の技術がそのファイアウォールを作っている。これにより、アメリカはこの政府クラウドさえ守れば良いことになっている。しかし、いくら技術を固めても、人間が破ると意味がないので、人間も奇麗にすることがクリアランスである。そして、軍のハッカー軍団による防護する。これが普通のサイバーセキュリティの形である。

日本の何が問題かというと、まず自衛隊が不正アクセス禁止法の対象になっていること。このため今の自衛隊は案山子のサイバー軍。この辺りを改善し自衛隊が使えるようになると、自衛隊の任務を拡大して政府クラウドを守らせることができる。ここまで来ないと駄目。

去年か一昨年にイギリスの IISS という国際戦略研究所という有名なシンクタンクがあって、彼らが世界のサイバーセキュリティのレベルを3分類した。「優秀」、「並み」、「下」で一応わかれていて、日本は「下」に入って、日本と一緒に「下」レベルに入ったのは北朝鮮だけという惨めなことになった。また、そこに解説が付いていて、日本には技術者がいる、技術もある、お金もある、スーパーコンピュータもある。しかし政策が無いと書いてあった。これは非常に正しい。

Q6： 上記についての更問ですが、国内では有力なセキュリティ事業者様に実施したインタビューにおいて「Offensive Security 対策をとれる人と評価する人材が確保できない。このため企業に対してサイバーセキュリティを義務化してもその制度がうまく機能する見通しは立ちにくい。だから義務化よりも先に、不足している攻撃側のスキルを有した人材育成が急がれると思う」というご意見を拝聴しました。有能な若い人材

を発掘し攻撃スキルを身に付けさせるには、処遇や社会的なステータスにおいても魅力ある職業にしていくことが重要かと思います。この部分については、国ではどのような戦略をもって取り組んでいるのでしょうか。

A6： サイバー防衛の世界では攻勢と防御は裏腹の関係にある。ウィルスを送り付けてくるハッカーを特定し（アトリビューション）、そこに逆侵入して警告などをするからである。この積極防御をやれるのは軍だけである。普通、敵のハッカーのコンピューターに暗号を解いて逆侵入するのは、軍の仕事である。敵軍の調査、偵察、暗号解読は、平時から軍の正統な業務である。民間人にその権限はない。このため、軍に政府全体及び民間の重要インフラの防御もカバーさせるのが普通の国のやり方である。アメリカは政府全体、重要インフラ全体も米軍がカバーしている。彼らはまさに攻撃防御、つまり極防衛の権限を持たされている。

だから彼らは敵の中に入っていく。日本は5年前の防衛大綱を書くときにもサイバー防衛を強化すると書いていて、あまり進んでいない。アトリビューションから積極防衛までやれる一万人規模の体制を一刻も早く立ち上げる必要がある。

おっしゃる通り、正に人材をどうするかという問題がある。全員がウルトラハッカーである必要はなく、大半は普通のハッカーで良い。最上級のウルトラハッカーは、アメリカの場合は一応、形の上は軍人にする。ただ、軍人なのに体力検査がない。学歴不問、学歴不問。小学校でドロップアウトしていていもOKであり、ハッキングの試験だけが課される。

日本政府の場合は数千人をどうやって集めるかから始まる。普通に公務員で雇用すると、まず給料が非常に安い。初任給で年間300万円、残業もやったら多い。しかも一遍入れてしまうと、公務員の立場は安定しており守られているので、60歳まで在職できる。しかし、ハッカーは、特殊な能力を使う頭脳労働なので、若いうちが勝負である。だから給与など新しい採用の仕組みが要ると思う。また、入ってくるハッカーたちは社会的には弱者であることがあるので、彼らのメンタル的なケアも含めた仕組みが必要であろう。

給与については真剣に考えて行く必要がある。霞が関が出せる最高金額は年俸2000万円。次官の年俸が2000万円だからである。民間企業に比べるとかなり低い。それが最高額である。しかし、2000万円では良いハッカーは誰も来ない。皆Googleなどに行ってしまう。外国企業は4000～5000万円くらいすぐに出すと思う、私は、政府も5000万円くらい出したらいんじゃないかと言っているが、役所は固いので、最高額の次官給与以上は出せないと言っている。何とかしないといけない。

Q7： ソフトウエア等の脆弱性に関する情報はNISCやJPCERT/CCでも公表し注意喚起をしていますが、日本の現行法制ではサイバーセキュリティ上の問題となるソフトウエア等の脆弱性を放置しても罰せられません。放置された脆弱点を狙ってAPT等により重要インフラ等がサイバー攻撃を受けた場合の国民生活への影響への影響の大きさを考えれば、サイバー攻撃を受けた企業は被害者でもあり加害者にもなると思います。この点については、法制度上ある程度の強制力を持たせるなどの改善の余地があるのではないかと思います。脆弱点を放置した場合の罰則を規定するような法改正は現実的でしょうか。あるいは、企業側の善良な管理を促すような観点から、サイバーセキュリティに言及した事項を会社法に追記するのであれば世の中からの抵抗は少ないかと思いますがいかがでしょうか。

A7： 重要インフラとそれ以外は分けた方がいいと思う。重要インフラはできれば政府クラウドに取り込むとか、重要インフラ関連の民間企業にはサイバーセキュリティの法的義務をかけて、一定のサイバーセキュリティ基準を満たしているか、政府が毎年1回2回審査に入るということをしなくてはいけないと思う。

重要インフラではない普通の企業、または中小企業、こうした人たちにはサイバー

セキュリティはコストになるわけだが、自前での対応が難しいのであればサイバーセキュリティ会社に委託すればいいと思う。

また、これがスタンダードですよという標準を政府が作った方がいいと思う。罰則をかけるかというと、普通の中小企業を相手に罰則までかける必要があるかはよくわからないが、重要インフラの建設・管理を担当している企業であれば、行政罰ぐらいはつけてもいいかもしれない。

こういうことを検討するための統括部局が必要となる。今は日本のサイバーセキュリティの全体像を見ている人が誰もいない今の NISC を拡大してサイバーセキュリティ局にして、民間に関してどうやって義務を課すかとか、重要インフラ企業と中小企業をどう分けるとか、サイバー基本法をどう改正するかとか、新法を立法するかとか、その審査部局はどこにつくるとか、このようなことを早急に作業する必要がある。

Q8： マルウエアの侵入について積極的に防護する必要があり、やられた場合には即座にやり返す必要があるとのことでした。そのためにはそういったことが出来る人材が多く必要となると思います。しかしながら、現在そうした人材が不足しているという状況であることから人材を育成していく必要があるといわれています。人材育成について、攻撃者の視点に立って防御を行うことが出来る人材が日本にはほとんどおらず育成していく必要があると聞いたことがあります。そうした人材を増やしていくべきでしょうか。また、攻撃側の視点を持った人材を増やしていくにあたって注意をするべきこと等はありますでしょうか。

A8： 基本的に、ホワイトハッカーの人たちはお金に関心のない人が多い。グーグルやアップルに行けば数億円稼げる人たちであるが、そこでアプリを作ることよりも、国家安全保障に携わりたいと言って米国防省に来る人が多いと聞いている。やりがいを求めてきている人たちであり、正義の味方であるという意識を持って入ってきている人々である。基本的に政府に入り協力しようという人たちはホワイトハッカー系である。途中から、悪いほうに流れていくというのはあまりない。先に述べたように、サイバーセキュリティでは攻勢と防御が表裏一体である。アトリビューション、ハックバックの攻撃能力を持っていない人は防御能力もない。もちろんそうした技術を悪用することはあってはならない。退職後のフォローもしっかりとしていかなければならない。

4.経済安全保障におけるインテリジェンスについて

Q9： 兼原先生が書かれた「安全保障戦略」の第 6 講を拝読いたしました。日本のインテリジェンス体制について、国家安全保障局と内閣情報調査室の連携がうまくいっていることや特定秘密保護法ができたことで、以前より機能し始めてきているとのことだったと理解しております。もっとも、安全保障が経済にまで裾野が広がっている現在、収集・分析する情報の多角化、また、インテリジェンス機能は国だけではなく関係する企業や大学にも必要となってきており、国全体として、国家機関・企業・大学が連携したオールソースアナリシスが今後必要となってくると私自身考えています。そのうえで、①安全保障と経済安全保障を比較した場合、インテリジェンスという観点でどのような差異があるでしょうか。②経済安全保障を推進していくうえで、インテリジェンス機能及び体制をどのように強化していく必要があるのでしょうか。教えていただければ幸いです。

A9： 安全保障において、最高価値のインテリジェンスというのは、最高指導者が一番価値を置く情報である。最高指導者が一番気を遣うものが国家安全保障、要するに、国民の命である。それは犯罪・戦争・災害といったもの全部であり、国民の命を守ることは国が立っている最大の理由である。民主主義国家では、この危機管理に失敗した

指導者はすぐ倒れてしまう。だから、政権を取った人は、これだけは失敗できないと考える。したがって、インテリジェンス収集の関心を、まずそこに集中させていく。必然的に軍事・外交・治安に関連するものになっていく。

経済安全保障はここから少し離れる。国の技術覇権という話であり、国民の血が流れるという話から、もう1周遅れる。

科学技術イコール安全保障というのが世界の常識である。これからどういう技術が戦場を激変させるかとか、この技術で先んじられたら負けてしまうとか、特定の技術や、その技術の基盤になっている研究のどこが一番重要か、などというような情報が必要となる。また、逆にこのような情報を取りに来る、あるいは、盗みに来る外国勢力がいる。それがいったい誰であるかとか、どのような技術を出してはいけないのか、守らなくてはいけないのかとか、公開できない技術情報だから秘密特許にしようとか、いろいろ考えなければならない。

また、技術情報を窃取するだけではなくて、開放経済の開放性を利用して、悪さをしようとする外国勢力もある。例えば、自衛隊の基地の横に、中国企業の、非常に大きい太陽パネルやその工場が直ちに作られている。その中国企業は経産省から補助金をもらってさえいる、といったことが起きる。これは一言で言うと、政府の縦割りがおかしいということだ。だから、自衛隊の基地や米軍基地周辺の経済活動の調和をどうするか。これも経済安保の話になってくる。このようなことを調べるのが重要土地等調査法である。

また、普通の経済活動が安全保障に影響を及ぼさないかと言う問題もある。日本は、90年代に新自由主義を大きく取り入れたので、基本的には全部マーケットに任せる発想の法律が多い。他国の法律には、1行、必ず「安全保障に関する措置を例外とする」という文言が入っているが、日本にはそれが入ってないものが多い。だから、様々な事業法において、日本で事業を行うことは自由である。例えば、国家システムの根幹の電気通信事業はフルオープンで、誰で事業を開始もできる。明日、北朝鮮の通信社が入ってきて平壌国営放送と称して通信会社を作ることもできる。本当にこれで大丈夫なのか、という話である。

技術の盗み方には、いろいろある。例えば、株式を買うこと。全体の株式の五割を超えれば支配権が生まれる。そうすると、本当に機微な会社の株をそんな簡単に買わせていいのかという話になる。これに対しては、外為法を改正して縛りをきつくしてある。

経済絡みの安全保障の内容は、基本的には重要な情報を抜かれないであるとか、自由な経済活動を通じて軍事情報はとられない、といった「守り」の活動が大きな部分を占めている。

Q10：　日本のインテリジェンス能力を向上させるうえで各省庁の協力が重要であると認識しています。今後、インテリジェンス機能強化を行う上で各省庁に期待する動きの方向性などありましたら教えていただけますと幸いです。

A10：　各省庁が協力する最大の条件は総理が関心を持つこと。インテリジェンスは、普通の仕事ではなく、最高指導者の政策決定に資するために最高機密の供与することである。だから、誰にでも広く情報を配るという話ではない。最高級の機密の情報を総理だけに渡すこと、これが本当のインテリジェンスである。

ところが、この国の総理大臣は、インテリジェンスを使うという発想があまりない人が多い。日本の総理大臣には、特に昭和後期から平成にかけて、天皇陛下みたいな短命総理が多く、「良きに計らえ」という感じの人が多かった。本当に最高権力使者として自分自身で政策判断をしようと思うと、人間はどんどん孤独になり、不安になる。そうすると、「情報を持ってこい」と言うようになる。そうすると政府の色んな部署から公開情報がどんどん入る。外務省は外交交渉の情報を持ってく

る。それでも、最高権力者なら、裏の裏まで確認するのが本当である。これらの情報は本当なのか、という話になる。そうすると、裏付情報をとりにいく。これがインテリジェンスである。いわゆる「草のもの」、「御庭番」なのである。だから総理がぼうっとしていたらインテリジェンスは機能しない。したがって、各省庁が協力をしていく最大の条件は、政策判断者の総理大臣や官房長官がインテリジェンスの意識を持つことがまず重要である。

次の段階としては、縦割りの排除である。NSC と内閣情報調査室（以下、内調）の連携はうまく行き始めているが、内調の権限がまだまだ弱い。内調はもう少し強くなる必要がある。

このような裏仕事というか、インテリジェンス業務は、戦後はカウンターインテリジェンス業務（防諜、スパイ摘発）に限られてきたので、警察と公安調査庁しか行っていない。しかし、本当にインテリジェンス業務を行うのであれば、外交、軍事を含めて機能を抜本的に強化しなければ駄目だと思う。情報組織と総理がしっかりと繋がり、政府の中で情報をきちんと回すことが必要だと思う。

戦後日本のインテリジェンスには、ヒューミントと言われるスパイ組織が存在しない。これがないと世界中から相手にされない。これはしっかりやらなくてはいけない。日本がやらなかったら、他国もやらないというわけではない。多くの国々は日本でスパイ活動を行っている。日本だけがやっていないのである。

Q11： 企業が持っている重要情報と国家が持っている重要情報を互いに共有する際に障壁となるものはどんなものが考えられますか。

A11： 情報というのはものすごく幅の広い言葉であり、毎日新聞に掲載されているものも情報である。また、プーチンがクレムリンの奥の院で昨日こう言った、という超極秘的なものも情報である。

超極秘情報は極少人数にしか回らない。民間には絶対に出ない。大事なことは、情報はなんのために使うかということである。一般的な情勢の分析、明日どうなるんだ、明後日どうなんだみたいな話や、ウクライナ戦争がどうなっているのか、このような大きく広い文脈での分析というのは、ある程度シェアできる。このような分析の 8 割は公開情報が元になる。これらの情報は、官民で共有して差し支えない。

但し、日本企業の方々は、マーケットの外側の地政学などにあまり関心がないようにみえる。民間企業はお金を儲けなければいけないため、そこに関心が集中する。ウクライナの軍事情勢などにはあまり直接の関心はない。このような情報に関心があれば、政府から説明すればいいと思う。反対に、政府について、個別の業界の細かい話は経産省以外にわからない。これらは、差し支えない範囲で企業から教えてもらえばいいと思う。

まとめると。一般的な情報の共有や総合流通などは行えばよいと思う。しかし、狭い意味でのインテリジェンスと言われている情報は、前述したように最高機密情報なので政府から出ることはない。民間だって、漏れたら損をするため最高企業秘密は絶対に出さない。最高機密情報の共有は、官民ではあまり考えられないことだと思う。

5.その他安全保障について

Q12： 総合安全保障を推進した大平内閣や中曽根内閣以降、第 1 次安倍内閣ができるまでの約二十年間、我が国では安全保障に関する議論が下火になっていました。「歴史の終わり」に代表される楽観的な雰囲気が広がった時期と重なりますが、それが原因で我が国の安全保障施策全体の必要性が揺らいだのでしょうか。

A12： ソ連は崩壊し、中国もまだ弱く、北朝鮮は核を持っていなかった。日本では政局

が大混乱であったが、総じて、90年代は幸せな時代であった。そのため、軍備増強という話にはならなかった。日本の戦後平和主義は300万人もの大きな犠牲と壊滅的な被害によって生まれた。日清・日露戦争の戦場は日本国内にはなく、太平洋戦争で初めて国内が大規模な被害を受けた。そして、二度と馬鹿な戦争をしないということが戦後日本人の平和主義の原点であった。

その後、冷戦が始まったが、日本は特殊な状況になった。敗戦すると、権力の真空地帯が生まれ、そこに冷戦の磁場がかかると、普通国が分裂する。事実、東西ドイツ、大小中国、南北朝鮮とわかれた。日本は国家が分裂することはなかったものの、国論がぱっくりと割れることとなった。1955年で社会党が統一した。当時は労働組合が強く、学生も左傾化が著しかった。当時、ソ連はまだ日本をアメリカ側から引き離せると考えており、社会党や共産党などが暗躍していた。「非武装中立論」はその典型である。そのため、社会党に政権を渡さない目的で自民党が生まれ、国内が二つに割れた。そのため安全保障政策に関する限り、ソ連側の社会党とアメリカ側の自民党がイデオロギー的に全面衝突して、国民的コンセンサスは生まれようがなかった。これが日本に安全保障戦略がない本当の理由だ。

一方、東西ドイツ、大小中国、南北朝鮮のように、分裂した国家ははっきり片方につき、しっかりした安全保障施策がある。

日本政府は一応、自民党政権が長く続いたゆえに、アメリカについているが、社会党などの左派を含んで安全保障上の国民的コンセンサスを生むことは不可能であった。そういう意味では、日本の平和主義にはリアリズムに立脚した中身が全くなかった。そして、国家安保戦略も書かれなかった。誰からどうやって国を守るかという議論ができなかった。ソ連侵攻から日本を守るとすら言えなかった。冷戦初期には、ソ連こそ味方であると考える国民がまだ大勢いた。

このように国論がぱっくり割れたまま冷戦が終結し、世界そのものが平和になった。90年代、国民全体に危機意識がなかったが、政府から見ると大きな事態があった。それは９０年の湾岸戦争だ。世界中から多くの国が参加するものの、日本は憲法9条により参戦せず、代わりに2兆円の支援をおこなった。しかし、なぜ参戦しないのか、と非難を浴びた。この時、国会は大いに荒れたが結局自衛隊は参戦できず、戦後に機雷掃海の任務をおこなったのみであった。

これではいけないということになり、自衛隊を活用した国際貢献として、PKOが開始された。その後に北朝鮮核危機があり、小渕政権下で朝鮮戦争有事の可能性が高まり、日本は後方支援をすべきか問題となった。総じて、90年代は国民の危機意識は低いものの、日本の安全保障政策は大きく転換した。冷戦が終結し、社会党が消滅したことが大きな理由だ。

2001年に9.11事件が起きた。この事件は、テロリスト行為とは違い、国連安保理で憲章7章下の「平和に対する脅威」と認定された。これにより、2001年にはNATOがアフガニスタンに集団的自衛権を行使した。この時、日本は小泉首相という傑出した総理が即断で決断し、自衛隊を後方支援に出した。その後、ブッシュ大統領はイラク戦争を開始し、国際世論が割れ、独仏が離れ、日英がアメリカについた。そして、日本は戦争が終わった後のイラクの復興支援に入った。これが冷戦終結後の日本の安全保障政策の顛末だ。残った懸案が集団的自衛権であった。

国民世論は90年代や00年代では、あまり危機意識がなかったが2012年から中国の国力が急に上がり、2012年から始まった中国の尖閣での実力行使によって国民の意識が変わりはじめた。今年のウクライナ戦争で国民意識がさらにだいぶ変わった。残る懸案が集団的自衛権であった。これを第二次安倍政権で解決した。しかし、2015年に集団的自衛権について解釈の変更をした際、中国は念頭にあったものの、まだ中国が今ほど大きくなく、現在のような危機意識はなかった。この10年で中国の経済力が日本の3倍になった。今が、国民の危機意識は一番強いと思う。

（追加質問）

Q13：　今後、日本は一方の側に立って行動することになると思います。サプライチェーンの強靭化をしていく上で、今後どのような国際連携のあり方が望ましいか、先生のご見解を教えていただきたいです。

A13：　半導体において、半導体を作る技術があることと、半導体を作る技術を使って半導体を製造することは全然違う。半導体を製造する機械を作る技術を持っている国はアメリカ、イギリス、オランダ、日本だ。その機械を使って本当に半導体を製造するのは、中国、台湾、韓国だ。ファウンドリー（受託生産）と呼ばれる。彼らは世界の半導体のほとんどを作っている。

現在問題となっているのは、第一に半導体の途絶だ。パンデミックで工場が製造を停止し、世界的に供給が足りなくなった。日本でもその反動で内製化の動きがあり、最低限のものを作ろうとしている。中台戦争になれば、中国製と台湾製の半導体が途絶するかもしれない。だから内製化を急いでいる。

第二に、最先端の半導体も開発する必要がある。これは日米英蘭の西側諸国が行う。

今、日本が連携するのは台湾に決まっている。韓国と比較しても、やはり台湾だ。なぜかというと台湾が一番進んでいるから。台湾でトップを走るTSMCは、蒋介石が台湾統治を開始した際、差別されて苦難を味わった台湾人（本省人）がアメリカで勉強し、その後、台湾で起業した会社だ。1ナノになろうと言われている最先端半導体は日本ではもう作れないし、それを使う製品さえを作ってない。作るのはもっぱらTSMCしかない。そのため、組むとなると、台湾・TSMCということになる5Gの次の規格・6GをNTTが開発しているが、やはり組むのは米国と台湾だ。

台湾にはときおり旱魃がある。水不足だと半導体の生産が止まる。1番のリスクは中台戦争だ。中台戦争が勃発すると中国と台湾の半導体の輸出が止まる。世界的に半導体が決定的に逼迫する。そうならないよう、アメリカは台湾の工場をアメリカに移転するよう求めている。実際にそうなった。日本も同様に求めている。熊本にTSMCが進出してきた。中台戦争時、日本が中国と組むという選択肢は戦略的にない。半導体の最先端技術を持っているのは、アメリカ、イギリス、オランダといった西側諸国である。西側と連携することになる。

以上

記録作成担当者：岡本樹

ヒアリング調査報告 No.15　基本情報

日時	2022 年 8 月 29 日
テーマ	オーストラリアの経済安全保障について
ヒアリング先 (担当者)	外務省 大洋州課 大洋州課 小林 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凛香、香高優一郎、山田麻友 (計 4 名)
調査目的	オーストラリアの経済安全保障について理解を深めること。

(写真)

【ヒアリング内容】
オーストラリアの経済安全保障政策等についてご教示いただいた。

以上

記録作成担当者:岡本樹

ヒアリング調査報告 No.16 基本情報

日時	2022 年 8 月 29 日
テーマ	経済安全保障に関する取組について
ヒアリング先 (担当者)	アイリスオーヤマ株式会社
場所	質問表を送付の上、メールでのご回答を得た
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 宮内拓　(計２名)
調査目的	アイリスオーヤマが行っている取組について理解を深めること。

【質疑応答】

Q1：　御社は経済安全保障推進法(重要物資の安定的な供給の確保、基幹インフラ役務の安定的な提供の確保、先端的な重要技術の開発支援、特許出願の非公開)を認識していましたでしょうか。
　また、評価する点、懸念点がございましたら、ご教示いただけると幸いです。

A1：　認識していた。
評価できる点：米国など他の先進国と連携して中国やロシアなど権威主義的な国々に経済面からの対応を進める枠組みの一翼を担う点。
懸念点：企業として、経済活動の効率性が損なわれる、自由競争が歪められるなどの弊害も生じ得る点。

Q2：　国が経済安全保障に関して、企業への規制を強めた場合、どのような規制が御社にとって厳しいものとお考えでしょうか。我々としては一定以上の情報流出防止策を取ること(設備投資など)の義務化や、現状以上に自社の技術や製品の輸出入に届出が必要になること、などが厳しいのではないかと考えております。

A2：　届け出の負担やリスクが大きくなる。

Q3：　経済安全保障(情報流出やサプライチェーンなど)の分野で、国の機関(警察や公安調査庁などの防諜機関や、経済安全保障を主務とする国家安全保障局推進班、経済産業省など)に望むものは何でしょうか。

A3：　サプライチェーンは企業が事業戦略に基づいて経済合理性の観点から構築している。そのため、規制的な手法ではなく、企業の主体的な取り組みを後押しする内容を望む。

Q4：　2010 年の尖閣諸島事件を契機に中国がレアアースの対日輸出を事実上停止した時のように、他国が経済力を用いて我が国に要求をのませるような手段を取った場合、サプライチェーンは混乱し通信サービス等役務に必要な資材の調達にも影響が生じることが想定されます。そのような事態を回避するために、サプライチェーンにおいて御社はどのような対策を取られているでしょうか。

A4：　生産拠点の分散化。例えば、中国１か国で生産していたものを日本だけではなく、アメリカ、フランス、韓国でも生産を開始した。

Q5：　価値観を共有する国から調達している資材であっても、周辺有事等の際は物流が停止する可能性は否めません。そのような場合における御社としての資材調達の考え方についてお聞かせください。

A5：　複数社（複数国）調達を実施。アイテムにもよるが、中国 1 か国に頼るのではなく、韓国やベトナムでの調達も実施している。

Q6：　安全保障上の理由から、米国は同盟国である日本に対して、同等の対中輸出入管理を求めてくることは容易に想定されます。我が国がそのような要求を受けた場合の御社としての資材調達の考え方についてお聞かせください。
A6：　米国同等の対中輸出入管理は現実的ではないと考えている。

Q7：　制度設計において配慮が必要な事項について、ご意見をお聞かせください。
A7：　特にない。

Q8：　新型コロナ感染拡大初期の頃は、深刻なマスク不足に陥った中、御社はマスク製造ラインをいち早く作り上げ、マスク供給に寄与されました。
　仮に、あの時のような緊急事態が別な形で発生した場合、国の支援策としてはどのような内容が適切かご意見をお聞かせください。
A8：　設備投資等に関する補助金の明確化。

Q9：　例えば国がマスク製造ラインを戦略的に維持するために内外価格差分を国家予算から補填する制度を作成した場合、企業経営として受け入れることは可能でしょうか。
A9：　受け入れることは不可能ではない。

Q10：　御社は国内外に複数の工場をお持ちですが、こちらの製品はこちらの工場で生産するといった分類はございますでしょうか。もしありましたら、そちらの理由についても差し障りのない範囲でご教示いただけますと幸いです。
A10：　生産拠点による資材調達などの環境が違うため、生産場所によって生産する製品は違う。

Q11：　海外工場の展開について、今後はどのような地域を想定しているのか、差し障りのない範囲でご教示いただけますと幸いです。
A11：　東南アジア。

Q12：　御社の海外工場からの流通が止まってしまった場合の代替手段などは検討されているのでしょうか?また、代替手段がある場合は可能範囲でご教示いただきたく存じます。
A12：　状況によって生産場所を適正化する。状況によってはOSも検討。

Q13：　御社のような大手企業ともなると、サプライチェーン全体におけるデータ等による可視化に基づき、最適な経営判断を下すことが重要であると思います。生産から販売までに発生する各種データは社員全員が閲覧可能なものなのでしょうか。もしもデータを閲覧できる社員に制約等があれば、ご教示いただけますと幸いです。
A13：　閲覧社員に制限はある。主はSCM課とマーケティング部。

Q14：　御社へのサイバー攻撃に対する取り組みの現状、および本法律が施行されることにより必要となる追加的措置についてお聞かせください。
A14：　サイバー攻撃に対しては次世代FW、WAFやウイルス対策ソフトによって防御を行っている。また、ファイルやデータベースのバックアップを定期的に行っているほか、BCP対策として西日本の拠点にサーバーのレプリカを同期させている。

Q15：　懸念される事項について、ご意見をお聞かせください。
A15：　特にない。

Q16：　具体的にどのような支援が望ましいかご意見をお聞かせください。
A16：　特にない。

Q17：　懸念される事項について、ご意見をお聞かせください。
A17：　どのレベルの秘密情報をどの程度の厳格さで守るかといった制度設計。

Q18：　特許出願の非公開制度は御社にとっては不利益になるとお考えですか。また、それはどのような場合でしょうか。
A18：　国の安全保障上極めて機微な発明が生まれるような開発を行う予定はなく、不利益はない。

Q19：　企業に不利益を生じさせないためには出願技術等の価値に見合う十分な補償が必要となりますが、その価値を計るにはどのような手法が望ましいかご意見をお聞かせください。
A19：　上記の通り、国の安全保障上極めて機微な発明が生まれるような開発を行う予定がないため、コメントは控える。

Q20：　この制度が導入されることによる新たな技術開発モチベーションへの影響についてご意見をお聞かせください。
A20：　新たな技術開発モチベーションへの影響はない。

Q21：　新たな技術開発モチベーションを低下させないためには、どのような制度設計上の配慮が望ましいと考えるかご意見をお聞かせください。
A21：　上記の通り、国の安全保障上極めて機微な発明が生まれるような開発を行う予定がないため、コメントは控える。

Q22：　御社では商品開発のための応用研究はどのような人材が担っていますか。
A22：　理系専攻者や素材開発を行ってきたキャリア人材。

Q23：　御社の情報流出防止策について、その内容をお聞きしたいです。具体的には、外部からのサイバーセキュリティだけでなく、技術者のヘッドハンティングや、勧誘などの接近工作といったリスクをどの程度認識していて、各種リスク(サイバー、接近工作、ヘッドハンティング、企業間や外部との協定や人材交流、共同研究など)にどの程度の対策を行っているのでしょうか。
A23：　PC 情報機器のログ管理を行っているが、ヘッドハンティングの対策はできていない。外部連携については産官学連携の実績あり。

Q24：　宮城県警など日本の警察では、技術や情報の流出の防止策として、外国の工作手口や対策のノウハウを企業に提供する「アウトリーチ活動」を推進しております。御社ではそれを認識していらっしゃったか、どの程度参加されているのか、ご教示いただきたく存じます。
A24：　認識していない。

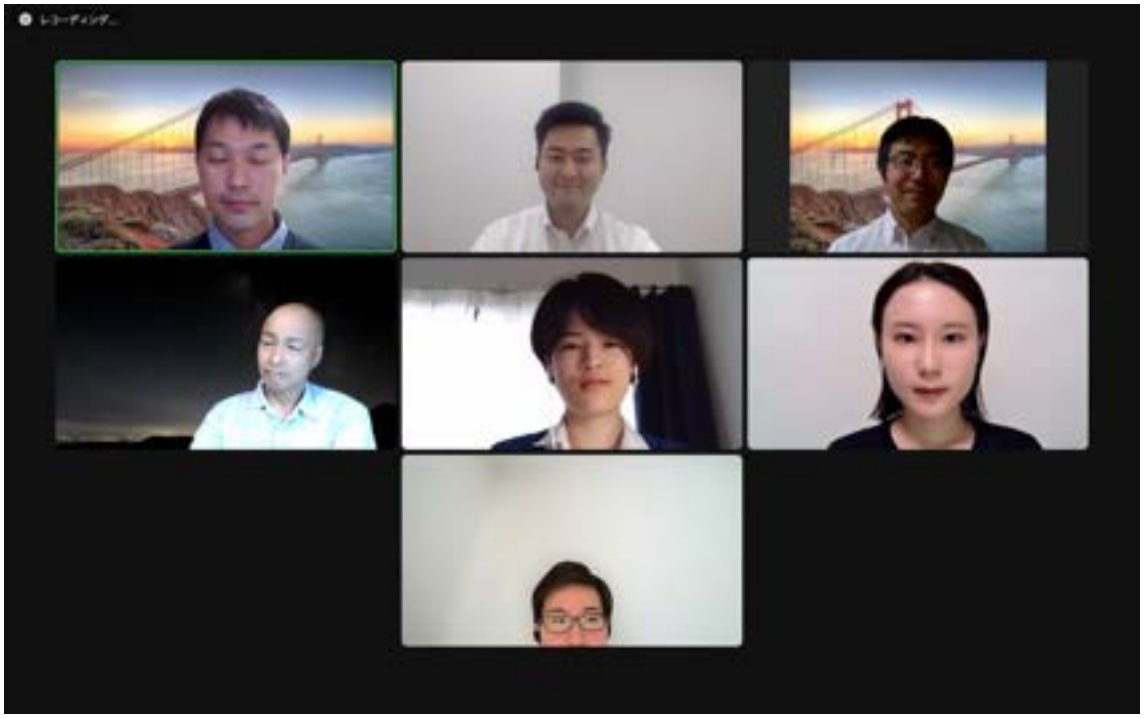
以上

記録作成担当者：宮内拓

ヒアリング調査報告 No.17 基本情報

日時	2022 年 8 月 31 日
テーマ	経済安全保障に係る経済産業省サイバーセキュリティ課の取り組みについて
ヒアリング先 (担当者)	経済産業省 商務情報政策局 サイバーセキュリティ課 総括課長補佐 渡邊貴史 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 織田秀夫、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 5 名)
調査目的	経済産業省サイバーセキュリティ課が執り行っている施策とその課題、諸外国や企業の動向等を、今後の研究に活かすこと。

(写真)



【レクチャー】

1. 高度化巧妙化するサイバー攻撃の現状について

昨今、サイバー攻撃はそのランサムウェア攻撃と呼ばれる、企業の情報を暗号化してしまい、解除のために脅迫金を要求するといったような攻撃や、中・露・北朝鮮といった国家が背景にある攻撃集団が特定の企業を執拗に狙う標的型攻撃など、多種多様になっている。

また、サイバー攻撃が高度化・巧妙化するだけでなく、攻撃の起点が DX で増加していることに伴い、サイバー攻撃が社会や産業に広く深く影響を及ぼしている。特に海外の 2021 年の例ではアメリカのコロニアル・パイプライン社がランサムウェア攻撃を受けて、石油の精製等、燃料輸送のパイプライン自体には影響がなかったようであるが、どこまで影響があるかわからないため、パイプラインでの輸送を止めた。また、徳島の半田病院がランサムウェア攻撃を受け、電子カルテが全部暗号化されてしまったという事例がある。

様々なファクターがあり、さらに誰がやったかわからないというのがサイバー攻撃の特徴になる。

さらに中身の話をすると、水平的脅威と垂直的脅威がある。水平的脅威とは、対象が広くなる傾向である。2017 年 WannaCry というランサムウェアが、ゴールデンウィーク明けにパソコンを開いただけで急激に広がった。Windows の脆弱性を悪用したランサムウェア攻撃で、世界約 150 ヵ国で被害が生じた。具体的には、パソコンを立ち上げると画面がロックされる、データが転送される、等である。また、垂直的脅威としては、サプライチェーンを通じた攻撃がある。IT 企業の正規のアップデートサーバー自体が攻撃を受けて、ユーザーが通常のアップデートを実施したらウイルスに感染してしまい、影響が広がってしまった。コロニアル社は制御系システムまで影響はなかったが、制御系であっても、ネットワークで管理しているがゆえに、攻撃の影響を受けるおそれもある。2016 年には、ウクライナでロシアのサイバー攻撃により、電力プラントが停められた事案も発生した。

サイバー攻撃は直感的にも最近増加している印象がある。経産省の委託先である JPCERT という、国内企業のサイバーインシデントの調整や企業の初動支援、早期復旧、各国機関とに国際窓口業務を行う機関がある。この機関によるインシデント相談報告件数・調整件数の統計は前年比で見ても、増加傾向にある。

また、企業・団体等におけるランサムウェア被害の報告件数は令和 3 年 7 月から 12 月だけで前年比較しても、4 倍に増えている。令和 3 年度のランサムウェア被害の被害企業・団体等の規模別報告件数は、大企業が 49 件に対して中小企業が 79 件と過半超となっている。

サプライチェーンを中小企業も構成しているが、ある企業の例では、EMOTET という水平的脅威に分類される、流行したウイルスに感染してしまい、セキュリティポリシーの未整備で業務停止の判断等が困難な状況であった。結果的に製造ラインの業務停止はなかったものの、製造ラインが健全であると取引先に証明しないといけなかったため、デジタルフォレンジック(ログの確認作業等を指す)を行った。それには 500 万円もかかった。中小企業としては痛い出費だと思う。かなり中小企業も被害を受けている。

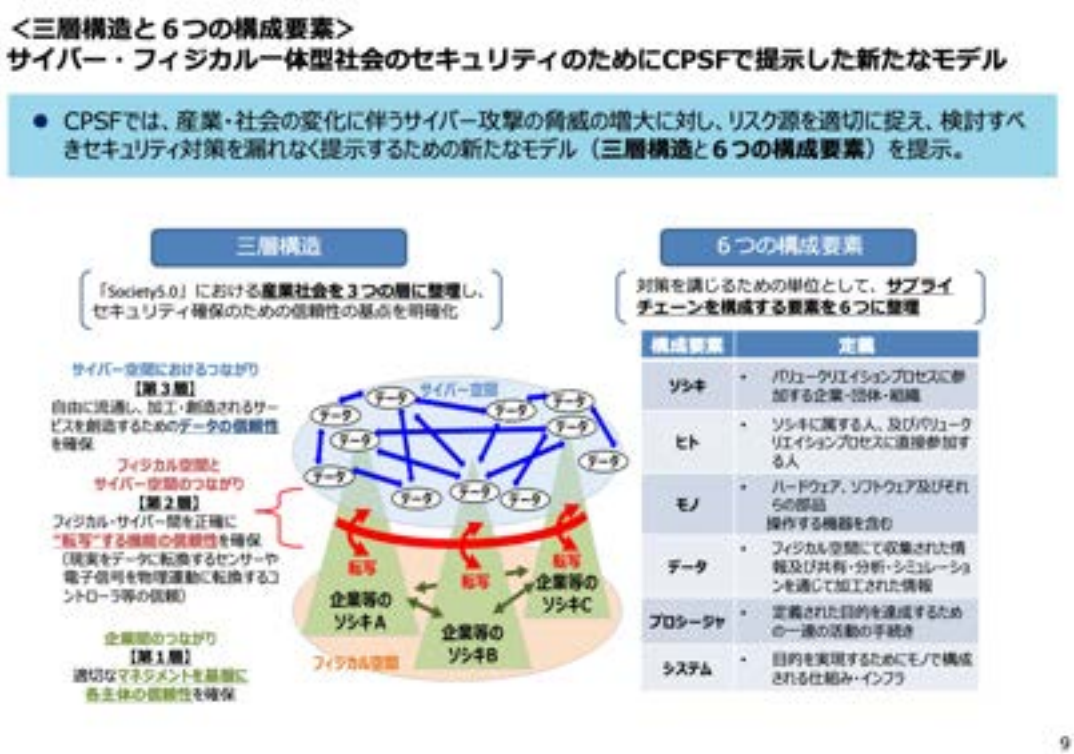
2.サイバーセキュリティに関する各国の動向

バイデン大統領が着任した 2021 年に、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令署名をした。その内容はインシデント情報の共有を義務付けや SBOM(Software Bill of Material)という、政府機関が調達するソフトウェアの構成要素に関する詳細の開示の方法を確立した。

一方で中国は中国サイバーセキュリティ法があり、関連法がいろいろ整理されている。また、新しい法律も多く整備されてきている。

3.「Society5.0」の社会を見据えた対策の検討

経産省では、サイバーとフィジカルが融合し、データの流通・活用を含む、より柔軟で動的なサプライチェーンが可能になる「Society5.0」に対応できるよう、サイバーフィジカルセキュリティ対策フレームワークを策定して、必要な対策を検討している。



(図１)サイバー・フィジカル一体型社会のセキュリティのために CPSF で提示した新たなモデル

フィジカル空間とサイバー空間では、フィジカル空間からサイバー空間に移す機能(例えば IoT 製品)や、サイバー空間のデータを使ってフィジカル空間に戻したり、フィジカル空間のデータをセンサーで拾ってサイバー空間に戻したり、というのが行われている。これが進んだ社会が Society5.0 であるが、3 つの層に整理し(図 1)、その構成要素として組織や人、データ、システム等がある。こういった層や構成要素に分けることで必要な対策をもれなく検討ができるというフレームワークになっている。

平時にどのような対応体制をとっているか、例えば CISO を置いているか、組織内ポリシーをしっかり作っているか、インシデント時にどのサーバーは止めてはいけないか等の持っている情報資産の洗い出しや起きうるインシデントを想定した上で、リスク源を一つずつ整理し、対策要件の整理や検討ができるフレームワークであるが、これに沿って、業種別のガイドラインや分野別の横断的なガイドラインを作っている。

また、システム監査というのは、システム監査人が一定の基準に基づいて、外部監査をするということである。情報システムのガバナンスやマネジメント、コントロールの適切性について保証を与える行為。第三者が点検評価、検証してシステムの信頼性を確保することと、その結果を対外的に示すことで、機能を高めるために運用されている。2018 年の調査では大企業で約 6 割がやっているとのことである。その中の基準として、監査基準と管理基準というものがあり、監査基準というのはこの監査する人の行為規範を定め、管理基準とは、その具体的な行為規範に基づいてどう判断すればいいか、判断尺度を定めたものである。

情報セキュリティサービス審査登録制度とは、良質なサービスセキュリティ製品や、検証サービスの登録を受け付けているというもの。監査制度との違いは、監査制度自体は、企業に入れているシステムが大丈夫かというのを第三者が評価する制度だが、情報セキュリティサービス審査登録制度は情報セキュリティ監査、脆弱性診断サービス、デジタル・フォレンジック、セキュリティ監視運用の観点から、この製品が基準を満たせているか、

審査を行い、リストとして公開をしている。6 月現在で 247 サービスが入っている。
それから、2 層のフィジカル空間とサイバー空間の繋がりについては、確保すべき信頼性というのは、正確に転写されるかということだと考えている。そのように定義すると、物理情報をきちんとデジタル情報に変換できるか、あるいはサイバー空間のデータに基づいて、きちんと制御がされているかという点がフィジカル空間とサイバー空間の繋がりで確保すべき信頼性で、サイバー空間にとどまらず、その安全面で支障をきたす可能性があるから、求められる要件を検討する必要がある。

4. IoT 機器に対するセキュリティ対策の必要性
IoT 機器に対するセキュリティ対策の必要性は増している。一部の調査ではセキュリティ事件／事故による IoT 機器や OT システムの一時停止を約 25%の企業が経験している。これは、必ずしもサイバー攻撃に起因しているわけではないと思われるが、4 分の 1 の企業が経験しているということで、大きな課題と認識している。ソフトウェアはどんどんアップデートされていくし、脆弱性が発見されたら修正パッチが出て、それを当てなければ、脆弱性が残り、不正操作や誤作動が実行されて機器の利用者に影響を及ぼしてしまう。例えば、アメリカの事例では、140 万台のリコール、さらにペースメーカーの 46.5 万台のリコール、家庭用ネットワークカメラの不正アクセスに対する訴訟があった。最後の事例では、500 万ドルを求める集団訴訟が起こされた。
元来自社の中で開発環境が閉じていたため、開発者が、何が起きているかコントロールできたが、今の開発環境はオープンソースソフトウェアで、全体を俯瞰しても、開発者自身が全て把握するのが困難になっている。したがって、第三者が検証していくということが IoT 機器においても重要になってきている。こういった産業の育成を図っていかなければならない。
最近、米欧では IoT 機器のラベリング制度を作ろうという議論がなされている。アメリカはラベリング自体を作ろうとしているが、事業者に義務を負わせるところまでは今は議論されてない。一方、EU は何らかのセキュリティ基準を担保させた上でそれを義務化させる話がある。日本は必ずしも対策が義務化されていないという状況である。他の諸国では、シンガポール、フィンランドが既に制度化しており、イギリスでも議論が始まっている

5. 第 3 層におけるデータマネジメントの新たな捉え方
サイバー空間の第 3 層、サイバー空間のことにおけるデータの流通の信頼性の確保についてどうするかというところについても議論をしている。具体的には、データマネジメントについてのフレームワークを作っている。データマネジメントとは、「データの属性が場におけるイベントにより変化する過程を、ライフスタイルを踏まえて管理する」ということで、この定義を設定することで、容易に流通するデータに関するリスクポイントがどこにあるかということと、その時にどういうことを考えないといけないかということを可視化している。この共通の定規を使用すると、各国とのデータのプロトコルの問題を可視化できて、囲い込みを回避できるという議論がある。

（図２）サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定

したがって、第３層におけるデータマネジメントの新たな捉え方（図 2）を用いると、たとえば、POS データであれば、使う「場」として販売店と EC サイトがあり、個人情報保護法や割賦販売法等により規制されているという前提のもとで流通している。まずイベントとしてデータが生成されて取得され、販売店・EC サイトでまとめて加工(統合)して、統合販売データになったとき、ネットワーク上の通信の盗聴の危険性やデータ統合の際に名寄せ誤りがあるといったことを可視化することでリスクポイントをしっかり認識した上で必要な対策を取ることができる。

また、諸外国ではデータの取扱いにおけるそのギャップがある。GDPR に関する Schrems II 判決では、欧州から米国への個人データ移転が問題となった。アメリカが設けている Privacy Shield という特別な枠組みを無効にしたため、データ移転ができなくなったというのが大きなポイントである。一方、日本では、アメリカとは制度が違うこと、つまり上図のフレームワークに従って分析をすると、十分性認定を受けているので、問題にならないことが分かる。こうした考え方を用いて、DFFT(Data Free Flow with Trust)を実現するべく OECD 等と議論している。

6.SBOM に係る取組の進展

SBOM(Software bill of Material)とは、最終製品を構成するソフトウェアの成分表である。SBOM がなければ、あるパーツで脆弱性が見つかってそれを直したとしても、当該パーツを利用していたコンポーネントでも修正が必要となることが後から分かって、対応が遅れるが、あらかじめ全部が分かっていると、その対応から完了までの時間を短縮することができる。アメリカもヘルスケア、自動車、電力分野でやっていて、我々も自動車、医療、ソフトウェア分野で実証を行っている。QUAD でもソフトウェア分野でしっかりやろうとしている。

7.諸外国のインシデント報告

米国のサイバーインシデントの報告義務については、民間企業、特に重要インフラである、大規模電力システムや防衛等については一定時間以内の報告義務がある。また、その対象を重要インフラ、証券について広げようとしている。

諸外国でも類似の報告義務がある。日本の場合は、各業法で当該サービス停止との関係で、報告が義務付けられているものがある。

NISC が作成している「重要インフラのサイバーセキュリティに係る行動計画」や各省と協力しながら情報が集まる仕組みも設けている。

もっと強化すべきという議論もあるが、中小企業まで報告を義務化すべきかといった点や、重要インフラといっても、それを担う企業の範囲、サプライチェーンまで考慮すべきかといって点など、なかなか難しい側面がある。

8.サイバーセキュリティと企業経営

企業経営との関係では、サイバーセキュリティ対策はコストではなく投資であると位置づけ、経営者がリーダーシップを取らないと対策が進まないということで 2017 年に「サイバーセキュリティ経営ガイドライン」を出した。

サイバーセキュリティ経営はコーポレートガバナンスの一環であるということで、「コーポレートガバナンスコード」の実務指針を経産省が出しており、その中でも触れられている。たとえば、親会社の取締役会レベルだけでなく子会社を含めたグループ全体の話を取締役会できちんと議論すべきということなどを明記している。

中小企業向けにも対策を整備している。そのうち、「Security Action」とは中小企業のセキュリティ対策の取組を宣言してもらい、セキュリティに取り組んでいる企業を可視化するという制度で、IT 導入補助金等の申請要件にしている。

「サイバーセキュリティお助け隊サービス」は、中小企業のリソース・人・金が不足している中では大企業のようにセキュリティオペレーションセンターを設置できない状況で、相談窓口、システムの常時監視、緊急時の対応や保険をワンパッケージにしたサービスを提供している。また、SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)という団体を組織しており、ここで利用推奨を行いながら、より多くの中小企業の方がこのサービスを活用して万が一の際に、早急に正しい対処が行えるようにしたいと考えている。

サプライチェーンでのセキュリティをどう確保するかということが、産業界の最大のポイントだ。自動車会社の工場停止も、自動車会社本体が被害を受けたわけでなく、部品を作っている取引先が攻撃を受けたことで、供給不足になり、稼働停止してしまった。大企業を守るためにも、サプライチェーンを構成する中小企業までどう守るかが問題となっている。

したがって、中小企業の身近な相談相手であるような地域金融機関や地域のコミュニティ活動を、セキュニティ(セキュリティ+コミュニティ)と称して、その活動支援を通じて、底上げを図っている。ただ、2021 年 IPA が中小企業に対して実態把握をしたが、サイバーセキュリティ対策の必要性は感じないとした企業が 2 割いて、我々としては強い問題意識を持って、サプライチェーン対策を検討している。現在 SC3 には 96 団体ぐらい入っている。

9.人材育成の観点からの取組

IPA に産業サイバーセキュリティーセンター(ICSCoE)を設けていて、制御系セキュリティについて、実際のプラントのセキュリティに精通する講師を招いて 1 年間の国内留学を実施している。300 名超が修了しており、アメリカのサイバーセキュリティトレーニングに参加する者もいるなど、海外とも協調したトレーニングを実施している。

このトレーニングでは、実機を使った模擬プラントを攻撃して脆弱性を発見して検討するということもやっている。

東工大とも連携して「サイバーセキュリティ経営戦略コース」を共に開催している。また、産業サイバーセキュリティセンターでは、1年間のプログラムが難しい場合に対して、対象を経営者に引き上げた上で、10時間ぐらいの講義を行う「戦略マネジメント系セミナー」を開いている

サイバーインシデントに係る事故調査の体制整備について、国内でも整備を進めている。事故が発生したときに、まずは当該業法で規定されるようなサービス供給の停止について各業界所管庁に連絡があるが、サイバーインシデントに関してはIPAに原因究明の調査を要請することができるという規定を設けている(cf.高圧ガス保安法改正法第60条の2)。

電気、ガス、高圧ガスについては法改正を実施しており、他分野にも広げていきたい。

10.インシデント情報の収集・共有によるサイバーセキュリティ対策の強化

IPAは、重要インフラ事業者に対するサイバー攻撃情報共有体制（J-CSIP(ジェイシップ):Initiative for Cyber Security Information sharing Partnership of Japan、15業種、262組織が参加)を構築している。
J-CSIPには電気通信放送郵便が入ってないが、情報通信分野はICT-ISACという組織との連携を図っている。

J-CSIPでは、公的機関としての信頼性をもとにIPAと参加組織との間で秘密保持契約を結んで、匿名性を排除している。企業としてではなく、業界としての情報共有活動することで、改めてそのセキュリティ対策を見直していく活動に繋げている。

サイバーセキュリティ協議会にIPAは入っているが、情報共有活動は一元化すべきだという指摘は、その方が効率的であると思っている。(一元化すると)どのような問題があるかと言われると、結局は信頼関係でやっているので、秘密保持契約を結び、「あなたなら渡してもいいですよ」という活動が基本となっている。一足飛びに法律を作って、秘密を漏らした場合に罰金をかけるような法律で縛ったからといって活動が促進されるわけではない。情報共有をどう活性化させていくかということが重要な論点だと思う。枠組みを根っこから変えるとなると、それだけでもかなりのコストがかかるので、既にある枠組みからどううまくここに繋げていくか、あるいは有機的な連携の方法を考えるのが、まずやるべきことだと思う。

11.サイバー攻撃にかかる情報の共有・公表のあり方について

サイバー攻撃被害の情報共有のあり方として、おそらく、JPCERTの資料をご覧になってだと思うが、まさにその通りで、NISC、総務省、警察庁、JPCERTを交えて、ガイダンスを作っている。

被害の拡大を防ぐには攻撃技術情報が重要であり、被害先企業名や事業への影響は重要ではない。いかに素早く攻撃技術情報の共有を進めることができるかという観点からガイダンスを策定するのが、「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」の趣旨である。どんな情報を出すべきか、どんな出し方をするべきか、送られた情報をどのように扱うか、公表のあり方といった点について、ガイダンスで示したいと思っている。

12.より高難度の国家資格制度創設

特に攻撃スキルを証明するような、より高難度な国家資格制度の創設については、産業サイバーセキュリティセンターで1年間手法を学んで、それを修了すると、メリットが二つあり、一つは産業サイバーセキュリティエキスパート（Industrial Cyber Security Expert）の独占名称使用権をIPAから付与している。この有資格者の引き抜きが起き始めており、評価されている。

もう1つは情報処理安全確保支援士という制度で、これは1年間の受講を終えると、有

資格者であるということで、試験受けずとも、申請すれば登録できる。

13.高度な標的型サイバー攻撃への対応

高度な標的型サイバー攻撃を受けた被害組織をどう初動支援するかはかなり重要な問題で、例えば公的機関、一般社団法人、公益財団等にもサイバー攻撃された時、こうした組織はセキュリティ専用の人材を設置することが難しく、被害の連鎖を断ち切ることができないという問題があった。そのため、「サイバーレスキュー隊(J-CRAT)」を IPA に作っていて、事案対処で得られた知見を基に情報分析しながら、緊急時の初動対応支援をしている。

14.経済産業省による国際連携について

国際連携について、産業サイバーセキュリティセンターで、日米 EU でインド太平洋地域向けの演習をやっている。これを通じて、インド太平洋地域のそのキャパビルを図っている。1 年に 1 回だが、かなり大変なので、1 年間かけて先方と調整する過程で、日本とアメリカと EU の情報交換を促進することをやっている。

日米 EU のサイバーセキュリティの演習のほかに、JICA の研修、海外施策や国際標準等の動向を調査している。また、国際会議もたくさんあり、二国間(日米、日独、日英、日 ASEAN)のサイバー協議や QUAD でも議論が加速している。また、アメリカの DHS とか、CISA、DOS、DOE、EU の DG CONNECT、英国だと DCMS、イスラエルも INCD と呼ばれる国家の官邸直結のサイバーセキュリティ組織と密接にやりとりを続けている。

15.総務省との役割分担について

インターネットの提供は総務省だが、サイバー空間のインフラとしてのコンピュータ、サーバー、ソフトウェア、企業そのものについては経産省が所管している。

【質疑応答】

Q1： 経済産業省が所掌する J-CSIP は、IPA が情報のハブとなり、電力業界、ガス業界、化学業界、航空業界、鉄道業界など国土交通省の所掌する業界を含めた各業界間でのサイバー攻撃に関する手口や被害情報等に関する情報共有の枠組みと理解しており。しかし、経済安全保障推進法の基幹インフラ役務の安定的な提供の確保に関する制度（第３章）の対処となる１４分野のうち、総務省が所掌する電気通信、放送、郵便については、現時点では J-CSIP の枠組みの中に含まれていません。また、サイバーセキュリティ基本法に基づき組織された「サイバーセキュリティ協議会」においてもサイバーセキュリティに資する情報を迅速に共有することになっています。攻撃方法を解析し適切な処方箋を速やかに作り出すには手口や被害情報等に関する情報の一元化は不可欠と思いますが、色々な枠組みが存在する中で情報の一元化を目指す場合、どのような問題があるのでしょうか。

A1： 一元化した方が効率的なのはその通りだと思う。しかし、J-CSIP の枠組みはこれまで長い時間を掛けて培ってきた信頼関係で成り立っている。通信・放送、金融については含まれていないが、通信については ICT-ISAC、金融については金融 ISAC がそれぞれ独立して存在し、J-CSIP とも連携している。一元化する方法もなくはないが、既に存在するそれぞれの枠組みを今後どのように発展させるかが当面の課題と考える。

Q2： サイバー攻撃被害については原因特定や被害特定を行わなければ公表やノウハウ共有は難しいと思われますが、攻撃手法とマルウエアの通信先については攻撃活動全体が継続されている最中に情報が共有されることで被害拡大防止の効果が見込めると言われております[1)]。被害企業のイメージ毀損を避ける観点から一定の配慮は必要になるかとは思いますが、攻撃手法とマルウエアの通信先など特定情報に限って、速やか

な情報共有を義務付ける制度の導入を目指すとしたら何か問題はありますでしょうか。また、セキュリティ事業者側からは、情報提供をするにも不必要な情報を仕分けする手間がかかりインセンティブが無いためメリットが少ないとの声も聴かれます。情報提供に関するインセンティブ制度の導入は現実的なものなのでしょうか。

A2： サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会においてガイダンスを作成しているところである。民間での情報共有を促進するのがガイダンスの趣旨である。その際には特定の企業名は伏せる形で、どのようなサイバー攻撃を受けたという事実を、速やかに情報共有することを促すようなガイダンスの内容を目指している。被害報告を法律で義務付けるのは、対象範囲をどうするのかといった点などから、現段階ではなかなか難しいのではないかと思う。

Q3： APT による重要インフラへのサイバー攻撃に備えるためには、より高度な対策が必要になると思いますが、サイバーセキュリティ事業者の体制強化やモチベーション向上には、サイバーセキュリティ事業者をもう少し優遇してほしいという声も聴かれます。例えば、より高品質で堅牢なサイバーセキュリティシステムの構築・維持・運用に求められる最高レベルの技術スキル、特に攻撃スキル（オフェンシブスキル）を証明するような、より高難度の国家資格制度創設は可能でしょうか。

A3： 既存する最高レベルのサイバーセキュリティエキスパート養成プログラムとしては、産業セキュリティセンターが重要インフラのセキュリティの中核を担う人材を 1 年かけて養成する「中核人材育成プログラム」を実施している。本プログラムを修了した者には「産業サイバーエキスパート」という名称使用権が与えられる。また、本プログラムを修了した者には、「情報処理促進に関する法律」に基づき、申請のみで国家資格「情報処理安全確保支援士」（通称：登録セキスペ）が与えられる。

Q4： 現在、DX 化が課題となっているとのことですが、この課題を克服できない場合に、DX 化が実現しないだけでなく、2025 年の崖ということで経済損失が生じる可能性があるとの資料を拝見しました。経済安全保障の観点から、社会経済活動の維持に不可欠な基盤として戦略的自律性の部分に関わるのではないかと思っています。今後、経済活動を行っていく場所がサイバー空間へ移っていくことが予想されますが、情報を守るためのサイバーセキュリティや情報流出防止以外にも経済活動を行っていく中で気をつけるべきことなどはありますでしょうか。

A4： 有形資産に対して、無形資産の価値が高まっている。そのため、サイバーセキュリティが重要となる。しかし、無形資産については価値を評価することが難しく、その点をどのように解決するのかが重要となる。関連する事例として、人への投資というものがある。人への投資は可視化をすることが難しい。有価証券報告書の中に人への投資についての報告の義務付けを行うといった取組が進められている。

Q5： 貴省の「情報セキュリティサービス審査登録制度」と「システム監査制度」の違いについてご教示いただきたいです。前者の制度にもシステム監査が含まれていると理解しておりますが、前者の制度は情報セキュリティサービスの利用に係るもの、後者は企業内の情報セキュリティにおけるガバナンスに係るものなのでしょうか。

A5： 上記レクチャーを参照。

Q6： 国として情報セキュリティを推進していくためには、Q5 で挙げたような制度を企業の任意ではなく、ある程度強制力をもって利用してもらうことも一つの策かと思いますが、この点について貴省はどのようにお考えでしょうか。　また、これらの制度の現在の利用状況についても教えていただけますと幸いです。

A6： 例えば、ある製品を入れなさい、このレベルまで対策を引き上げろというのはかな

り難しいが、まずそれぞれの業法においてサイバーセキュリティ対策について、電気事業法やガス事業法、高圧ガス保安法に書かれている。
　対策はどんどんアップデートするため、更新しなければ陳腐化してしまうことが起きるので、個々の守るべき要素を示した上で、それぞれの業界の中で対策をやっていただくことが大事だと思う。

Q7：　サイバーセキュリティに関する経済産業省と総務省の役割分担は、経済産業省はサーバー空間の安全利用に関すること、総務省はサイバー空間の安定提供に関すること、概ねこの2つに大別した理解でよろしいのでしょうか。
A7：　上記回答を参照。

Q8：　各府省庁が所掌する業法でサーバーセキュリティについてまで縛るのは実効性に欠けるのではと思います。例えば通信の場合の業法は電気通信事業法になるのですが、サイバーに言及した法律にはなっておりません。サイバーセキュリティ基本法などで広く網を掛け罰則も設ける必要性を感じます。仮に罰則が馴染まないものであれば、有価証券報告書への記載義務を課すなどの工夫も有効と思いますがいかがでしょうか。
A8：　電気通信事業法はサービスを止めるな、そして止めてしまった場合の報告義務が書かれている。サービスが止まる原因には、災害、人為的ミス、故障、サイバー攻撃などがあるが、原因別にはなっていない。罰則は現時点ではそれぞれの業法に従うこととなりますが、有価証券報告書への記載についてはBCP項目の中に追加するのが良いと思う（※「リスク管理」が必須記載事項になったようです）。

Q9：　各業法、何かあればガイドラインが作られつつあるという状況はおそらく黎明期の犯罪収益対策にかなり似たような状況があると思います。現状では、事故を起こしたこと、一定のセキュリティレベルに達しないことについて罰するというより、疑われる情報を報告しなかったということについて罰することが若干多いと感じます。このような義務づけの国際的潮流はどんな方向性が見えているでしょうか。
A9：　間違いなく各国とも強化の方向に向いている。 日本の取組では中小企業対策が注目されている。各国とも規制すべき範囲について苦悩している中で、日本の取組は業界団体を組織化して、取組を進めていることはかなり関心を持たれている。また、サイバーセキュリティお助け隊サービスのような誰でも使えるサービスを作ったことは海外から質問をよく受けるところである。
　我々も今後IoTのラベリング制度、あるいは安全性を担保した制度を立てていきたいと考えている。

Q10：　PAが情報のハブ・高度な分析をやっていますが、公的機関だからこそ、信頼性があり、情報を出していると思いますが、実際どれほどの情報を集められているのでしょうか。
A10：　集められている。J-CSIPの活動で言うと、昨年は少なかったが一昨年前は情報提供件数が約6000件であった。また、(ソフトウェアの脆弱性を発見した場合に届出をIPAが受け付けて公表する業務は年間大体1000件行っている。これほどの実績をあげているのは長年活動を行ってきているからで、知見もかなり蓄積されている。

Q11：　企業にとって情報を提供することに何のメリットもない、付き合いでやっている何とかならないかみたいな愚痴をよく聞くものですね。
A11：　企業としては、特段のメリットがないし、報告による信用度の毀損につながることに危機感を持っているのではないかと受け止めている。IPAに届け出るよう経産省

が告示を出しているが企業内部でも、制度で届け出ることが決まっていると担当者が言える方が説明しやすいとの指摘もある。届け出てもらうことで、攻撃の手口が分かり、対策につなげることができ、必要な注意喚起を起こせるので、促していきたい。

Q12：　日本のサイバー人材のその特徴として、およそ7割近くのそのサイバー人材がサイバー関連企業に集中しているという業種間の偏在があります。インシデントへの早急な対応のためにも、企業内で早急な対応を取るべきだと思います。しかし専門のサイバー人材に高額な報酬を提示している企業もごく一部ありますが、人材確保は難しいというのが実情です。人材を確保する中でその難しい点として企業からはどのような声が上がっているのかというのについてお聞きしたいです。

　また、その業種間の偏在に関して貴省ではどのような議論が行われているのか、お話を伺えればと思います。

A12：　前者の質問について、企業は大企業になればなるほど、自社でSOC(セキュリティオペレーションセンター)を持つ傾向にある。そのため、経産省の産業サイバーセキュリティセンターの人材育成プログラムに人を派遣している。毎期、１人ずつでも派遣した企業は、高度なサイバーセキュリティ人材を6人ほど揃えられるので、ある程度のサイバーセキュリティができる。このほかは、OJTで人材確保をしているのが実情だと思う。

　後者の質問について、確かにITベンダー企業(ITツールをユーザーに販売する企業)に偏在しているが、ITユーザー企業も人材が足りていない。これはサイバーセキュリティ人材も同様だ。対策としては、IT人材をベンダー企業からユーザー企業に移るようにするのではなく、IT人材そのものを増やすという方向で議論するべきと考えている。そのため、経産省では、「デジタル人材育成プラットフォーム」を立ち上げ、必要な講座を分かりやすくしたり、地方でも取組を行ったりしている。また、厚労省が企業のOJTでデジタル人材を育成する場合、高額助成する施策をやっている。

以上

記録作成担当者：香高優一郎

ヒアリング調査報告 No.18 基本情報

日時	2022 年 9 月 15 日
テーマ	鉱物資源の確保に関する施策について
ヒアリング先 (担当者)	経済産業省 資源エネルギー庁 鉱物資源課 総括補佐 野崎開太 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 宮内拓 (計 2 名)
調査目的	レアアースの確保に関する知見を深めること。

【質疑応答】

Q1： 我が国のレアアースの確保において、どの物質を重要視しているのか、採掘国だけでなく、レアアースの加工・精製を担当する国としてどのような国と関係を持っているか、現状をお教えいただきたいです。

A1： 加工・精製はマレーシアで行っている。

Q2： 希土類金属、酸化セリウム、セリウム化合物の面では、ベトナムやマレーシアなど、東南アジア諸国からの輸入が増加している傾向にあります。現在と今後のベトナムやマレーシアといった東南アジア諸国との関係についてお聞きしたいです。

A2： 日本、オーストラリアよりもベトナム、マレーシアは電気代、人件費が安い。よって、加工・精製をする地域として適しているため、東南アジア諸国からの輸入が増加している。今後は日本国内でリサイクルをするなど、国内である程度確保する取組も重要である。

Q3： IPEF や日豪首脳会談、日豪印 SCMI など、クアッド諸国とのサプライチェーンの強靭化での連携が行われています。アメリカ、豪州、インドとの国際連携の現状と今後についてお聞きしたいです。

Q4： 特に豪州に関しては、日豪首脳会談で、鉱物資源のサプライチェーンの強靭化で協力していくとお聞きしました。具体的にどのような解決を図っていくのでしょうか。

A3,4： アメリカ主導の MSP、クリティカルミネラル会合など同志国による様々な枠組みが存在している。これらの枠組みを利用して、各国との間で個別案件を交渉していくことが重要である。

Q6： 中国は鉱物資源の採掘だけでなく、加工(分離・精製)の分野まで一貫して行う技術と設備を持った唯一の国で、大部分のレアアースの加工を中国が行っているとお聞きします。貴所では、中国がレアアースの加工の大部分を担っていることを課題視しているのでしょうか。

A6： 課題視している。
中国は価格競争力があり、安く買える。日本国内におけるリサイクルの取り組みが重要であると思われる。

Q7： 日本が中国による一方的なレアメタル禁輸に対し、対処できたのは、どのような要因があったとお考えでしょうか。

A7： Q8 に挙げられている 4 つの手段を尽くした結果であると思う。

Q8： 平成 22 年、総合レアアース対策として、1 代替材料・使用量低減技術開発、2 レア

アース・リサイクル、3 レアアース等利用産業の高度化、4 鉱山開発・権益確保/供給確保が行われたとお聞きします。それぞれについて、どのような課題があり、どのように解決を図って行ったのでしょうか。

A8： 1 に関しては、半導体デバイスは軍事にも関係してくるため、代替先をよく考える必要がある。解決の方向性に関しては万全の回答ができないのが、課題の大きさを表している。

2 に関しては、リサイクルの仕組みをどのように維持、拡大していくかが課題である。リサイクルは磁石を作る過程で発生するクズを再利用する形式と電化製品のゴミなどから取り出して再利用する形式があり、今後は後者も重要となってくる。

4 に関しては、今後は鉱物資源を経済安全保障法の特定重要物資に位置付けて、補助金を与えることで鉱山開発を進めることで解決を図っていく。

（追加質問）

Q9： 今後、日本はどのようにリチウムを確保していけばいいのでしょうか。

A9： レアアースと対策は同じである。鉱山をなるべく買うことなどが挙げられる。

Q10： 経済産業省の組織として何か強化すべき力点がありましたら、教えていただけませんか。

A10： 2 年ごとに人事異動があるので、個人としての専門家はいない。そのため、特に重要な力点としては実際に事業に取り組んでいる企業との関係作りが挙げられる。特に情報収集の分野においては、どこを調べるべきかといった相場観が重要であるため、何年もやっている専門家である人材が重要である。

Q11： JETRO はどのような活動をしているのでしょうか。

A11： 南アフリカの大使館にいたときに一緒に仕事をしていた。新聞や政府資料を読むほか、多くの人と関わりコネクションを作っていたのを目にした。

Q12： 経済産業省は JOGMEC とライナス社を繋ぐ役割を担ったと思うのですが、どのような働きかけをしたのでしょうか。

A12： 制度的に特殊なことをすることを理解してもらうように働きかけた。

以上

記録作成担当者：宮内拓

ヒアリング調査報告 No.19 基本情報

日時	2022 年 9 月 16 日
テーマ	半導体に関する施策について
ヒアリング先 （担当者）	経済産業省 商務情報政策局 情報産業課 係長 藤原ゆか 様
場所	オンライン
参加者	（WS-C 教授）坪原和洋 （WS-C 学生）梶山敬生、宮内拓 （計 3 名）
調査目的	半導体政策について学ぶこと。

（写真）

（ヒアリング内容）

【レクチャー】
○半導体の市場規模は 2030 年度には 100 兆円規模になると予想されている。半導体は大きくロジック、メモリ、その他の 3 つに分類され、日本はメモリ、その他には強みがあるものの、先端ロジックを製造する企業は少ない。だからこそ、熊本に TSMC を誘致して、確保に努めた。

○1980 年代に日本の半導体シェアは 50%近くあったが、2019 年度には 10%と落ちてしまった。原因は、日米貿易摩擦や、設計と製造の水平分離の失敗などが挙げられる。

○2050 年のカーボンニュートラルの実現には、デジタル化が必要不可欠であり、デジタル化には半導体が大切である。

○日本の半導体施策は、①IoT 用半導体の生産基盤を確保→②米国と連携し次世代半導体

技術基盤を確保→③光電融合技術など将来技術の実現の順に実行していく。

〇5G 促進法が 2021 年に改正された。一定基準以上の高性能な半導体を作る事業者の中で、日本で 10 年以上継続して製造する、需給がひっ迫した場合に増産に関する取組を行う等の条件を満たすものに対して、経済産業省が認定して、認定を受けた事業者は NEDO から補助金を支給されるという内容である。
　その最初の動きが TSMC であり、政府は最大 4760 億円の支援の決定をした。28 ナノプロセス以下のロジック半導体を作る。
　また、キオクシアのメモリ半導体には、最大約 929 億円の支援決定をした。

〇日本は、ロジックの次世代半導体（2 ナノ）の開発に乗り出しており、国際連携を図っている。この新しい半導体は構造が現在の Fin-FET 型とは異なり、GAA 型となる。日本は Fin-FET 型では後れを取っていたため、GAA 型では追いつきたいと考えている。

〇日米連携による半導体産業政策を現在行っている。研究開発組織（日本版 NSTC）の立ち上げを目指している。

〇また、半導体業界は人材育成にも力を入れている。九州、東北を中心に取組が行われている。

以上

記録作成担当者：宮内

ヒアリング調査報告No.20 基本情報

日時	2022年9月22日
テーマ	経済安全保障とサイバーセキュリティについて
ヒアリング先 (担当者)	国立研究開発法人 情報通信研究機構 サイバーセキュリティ研究所 主管エキスパート 田沼知行 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 岡本樹、織田秀夫、木戸友香子、山田麻友 (計5名)
調査目的	NICT が運用する NOTICE 等に関する法制上の裏付けの経緯などを確認し、政策提言に向けた課題の把握および研究を模索すること。

(写真)

【レクチャー】

(概略について)

NOTICE導入を検討した背景には、IoT機器を踏み台にしたボットネットによるサイバー攻撃が盛んになってきたことがある。総務省では関係省庁等と対応策を議論し、2017.1にはサイバーセキュリティタスクフォースで専門家の意見を踏まえ、パブリックコメントを聞いたうえで、2017.8には翌年度の調査費用の概算要求を行った。その後、調査を経て、NICT法改正案を国会に提出し可決成立した。詳しくは2017年度のタスクフォースの議事録
を見ると良い。
(https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/index.html
)

NOTICE運用に当たって問題となったのは、一つは国民が保有する任意のインターネット上のIoT機器に容易に推測されるパスワードを入力することなどによりサイバー攻撃に悪用されるおそれのある機器を特定する行為が不正アクセス禁止法に抵触することをいかに回避するかであった。もう一つはNICTの業務範囲を定めているNICT法の改正であった。

前者については警察庁をはじめとする関係省庁と調整し、NICTという法律に基づいた組織がその法律で当該行為については不正アクセス禁止法違反にはならないと明記することで対応することとした。

後者については、NICT法において、付則第８条等を追加して、NOTICEに関する調査業務を2023年度中まではNICTの業務の一部として規定する改正を行った。

NOTICEは2023年度いっぱいで終了するため、現在はその後の運用をどうするかについ

て、再来年度の概算要求も意識しながら検討を始めている。

【質疑応答】

Q1： 我が国のサイバーセキュリティについての課題を挙げるとすれば、NICT 様の目線からは何が一番重要でしょうか。

A1： 負のスパイラルが一番の問題である。負のスパイラルとは、①データが集まらない → ②研究開発/人材育成できない → ③国産技術を作れない →④国産技術が世界に普及しない → ⑤海外製品が跋扈→⑥データは海外へ→⑦データが集まらない 。これは NICT が感じる問題というよりは総務省や政府全体の問題意識でもある。どの組織も自分のデータは囲い込みがちだが、それではより大量のデータを活用している海外企業にはかなわない。国内にある貴重なデータを可能なかぎり共有してそれを活かしていけるような環境が必要。

Q2： NOTICE についてですが、パスワードアタックなどを行う上で、不正アクセス禁止法に関する違法性阻却事由について、どのようなプロセスを踏んで、どのような議論がなされ、どの様に整理したのでしょうか。

A2： 概略で説明したとおり、NICT 法を改正して NOTICE に関する調査業務を不正アクセス禁止法の適用外と位置付けている。国会での議論については 2018 年の通常国会の議事録を見るとよい。総務委員会で審議されている。

Q3： NOTICE についてですが、現在の取り組みに加えて、希望する企業に対するインターネット側からのセキュリティースキャン（サイバーパトロール）を組み入れることは可能でしょうか。また、NICT 法などの制度面で支障があるとすればどのようなことがあるのでしょうか。

A3： NICT の役割は NICT 法で定められているとおり技術の研究及び開発、高度通信・放送研究開発を行う者に対する支援であるため、現状の NICT が実施することは難しい。NICT 法を改正してそうした役割を担わせる可能性は否定しないが、特定の企業のためにサービスを提供する、ということはなかなか認められないのではないかと思う。

Q4： NICTER で観測したサイバー攻撃観測・分析結果を国内電気通信事業者へ提供し利用者への注意喚起以外の用途、例えば電気通信事業者の（国際関門局）においてサイバー攻撃の遮断に活かすことは現実的でしょうか。また、このようなことを実現する場合、現行の国立研究開発法人情報通信研究機構法 第 4 条（機構の目的）には合致するものの、同 第 14 条（業務の範囲）を越えてしまうと考えますが、このような解釈でよろしいでしょうか。

A4： 前項 3 と同様、NICT が電気通信事業者に指示をすることは難しい。NICTER での観測情報は一般にも公開している。これを専門家が見ればサイバー攻撃の予兆等いろいろなことがわかるので、その情報をネットワークの運用に活用することは出来ると思う。

Q5： APT によるサイバー攻撃については、軍と文民の区別が難しく、むしろ一体として捉えて対策を取ることが国益にかなうと思います。このような観点においては NICT と防衛省との連携体制はあるのでしょうか。また、もし連携がなければですが、サイバー攻撃に対する抗堪性を高めるためには防衛省との連携は必要とお感じでしょうか。

A5： NICT は 2014 年に防衛装備庁との間で覚書を結んでいるが、今のところそれ以上の具体的な進展はない。大学と比べると NICT の方が相対的には協力は行いやすいよう

に感じる。一方で、サイバーセキュリティの世界では、どこも人材不足。このため、人材育成プログラムでの連携は行いやすい。

Q6： サイバーセキュリティの分野では、サイバー攻撃に関連したデータを大量に集めることと、データを分析して正しく対処できるヒトを育てることが重要とのことですが、データを集める際に課題となることはあるのでしょうか。

A6： サイバーセキュリティの分野に限らず、世の中を良くしていくという事を考えた際にデータが重要となってくる。日本ではデータを取っていくということに対しての意識が非常に低いという現状があり、こうした状況について分かっている人もいる。データについては色々な所から集めて、塊としていくことが求められる。しかし、自分のデータを出すことについては拒否反応をしめしつつ、人のデータについては欲しいということや、自分のデータを出すことについて拒否をしている中で、実は海外の企業には大したチェックもせずにデータを出してしまっているという状況が起きている。もっと大局的な観点から行動していくことが必要である。サイバーセキュリティ分野を例としても、対策を立てるためのデータがうまく取れていない。そしてデータを取れているのは、海外のサイバーセキュリティサービスを提供している業者であるということがある。日本国内で IoT 機器が様々な場所で使われているにも関わらず、情報が全部海外に流れていってしまっている。その結果として、海外から提供されるサービスに対して高いお金を払うということになってしまう。こうした部分について変えていかないといけないというのが一番大きい。そして、データを集める際の課題としては、データを提供している人の理解が得られないという難しさが最大の問題としてある。またセキュリティ以外の分野であっても同じような状況であると考えられる。経済安全保障の観点から見た場合でも、セキュリティ対策を立てるときに自分たちのデータを持っていない状態で、自前でそうした体制が立てられないというのはかなり問題となる。

Q7： NICT 様の中期目標（第 5 期）の中で、若手サイバーセキュリティ人材についての記載がありますが、サイバーセキュリティ人材が不足すると考えられている中で、特に若手に着目する理由は何かあるのでしょうか。

A7： 若手だけでなく、地方公共団体や重要インフラを担っている企業のなかでも人材不足が起きている。セキュリティ上の警告を伝えたとしても、警告を踏まえて何をすればいいのかが分からないということが起きるために、対策が進まないということが現実に起きている。どこを強化していくのかということについては、全部が重要ではある。その中でも若手については、将来という面がある。特にサイバーセキュリティでは日本人として活躍できる場があるのも関わらず、そこに気づかずそうした業界に入ってくれる人がいないという現状がある。若い時からこうした分野について関心を持ってもらうことが長い目で見ても非常に重要になる。NICT でも特別なプログラムを作っており、特に優秀な人については国としても、優れた人材であるということを世の中に示すことで動機付けを行っている。そして少しでも活躍出来る場を広げることや、そうした人材が増えて欲しいということから、若手を強調している。しかし、若手だけについて言っているわけではなく、インフラを今支えている人たちのセキュリティに対するリテラシーについてもあげていかなければいけないということも喫緊の課題である。自治体については研修機会の提供などを行っているが全ての自治体まで行き渡らせることは難しい。機会の提供を行っているものの、日々の業務があることから対応が出来ないという場合がある。その場合については、地方の主要都市で演習開催をするだけでなく、実際に NICT の職員が現地に行って自治体の職員の演習の機会を提供するということを行っている。

Q8： 日本ではサイバーセキュリティ人材の不足が官民ともに課題となっています。今後サイバーセキュリティ人材を発掘、育成・支援していく上で、最も障壁だと考えられることはどのようなことでしょうか。

A8： 一番重要なのはこういうことに気をつけないといけないということを知らない人が多い。最初の説明では触れていないが、NOTICE の調査を開始する際は世の中からの反発の声も多かった。政府機関が我々の IoT 機器にアクセスをして情報を取ってしまうのではないか、それは国がやりすぎではないか、という声も上がっていた。サイバーセキュリティは現実世界と比べるとイメージが描きにくいのが悩ましいところ。物理的な世界では、例えば自分の部屋に他人に入られたくなければドアに鍵をかければよいし、そもそも部屋に入ろうとするならそこまで行かなければいけない。ところが、ネットワークにつながっているカメラやパソコン等はアクセスをしようと思えば世界中から簡単にアクセス出来てしまう。このような環境でそのカメラやパソコンに対して物理的に言えば鍵もかけていない、だれでもわかりそうなパスワードを使っているということがいかに危険かということは認識があまりされていない。まずはこういったことに少しでも多くの人に気づいてほしい。

〔追加質問〕

Q9： サイバーセキュリティ基本法を根拠に作られているサイバーセキュリティ協議会について、加入が任意なのにもかかわらず 303 団体入っている理由、加入することへのメリット及びデメリット、また、今後、サイバーセキュリティ協議会へ求めるものについて教えていただけますと幸いです。

A9： 罰則的なものは協議会のルールの一つに定められていて、それも理解した上でメンバーになってもらっている、ということだと思うが、それはサイバーセキュリティの分野においてはある程度の強制的な力もあった方が、最終的にはメンバーにも役に立つだろうという判断があってのことだろう。入会することが義務ではないにもかかわらずそのような強い条件もある中、多くの団体が協議会に入られている理由は、漠然とサイバーセキュリティについて何かやらないといけないと皆さんが思っているからなのではないか。ただ、何をやらなければいけないのかと、一段ブレークダウンして物事を考えていこうと思ったときに、なかなか手がかりとなるものがないというのが実態だと思う。したがって、そういったところにさらに踏み込んでもらうために、協議会という場が活かされていけばいい。メンバーが集まっているということは、皆が問題意識を漠然と持っているが、何をすればいいかわからないという実態が反映されていると思う。したがって、問題点としては、協議会に参加している団体に対し、何をするべきなのか、というところまで踏み込んだ活動ができるかということだと思う。

Q10： Q2, Q3 に関連しますが、インターネット側からセキュリティ診断をしたところ約 6 割の企業が落第点となっているという日本経済新聞記事を目にしました。サイバーセキュリティは企業の努力義務となっていますが、重要インフラや自動車工場等が止まった場合の日本経済や国民生活への影響の大きさを考えれば、サイバーセキュリティ対策が杜撰な企業に対しては、強制力を持った改善指導が必要と考えます。事前に同意した企業のネットワークをインターネット側からセキュリティ診断を自動で行うような仕組みを実装するとした場合、NICT 様が運用している NOTICE への機能追加が近道かと思うのですが、そのようなことは可能でしょうか。

A10： NICT が実施しているのは、NOTICE 業務全体のうちの調査業務であり、実際にその調査結果を活用して利用者指導を行っているのは通信事業者である。NICT 法を改正さえすればいろいろと行える可能性はあるが、基本的には研究機関である NICT が行

える業務については、おのずと限界がある。強制力を持った指導改善となると、その役割は例えば警察のような機関が担うことになるのではないだろうか。

Q11： 会社の経営層や従業員から出てくる声としてサイバーセキュリティ資格は負担となるだけで、メリットが少ないという声が聞かれます。サイバーセキュリティが産業化しにくいことの背景になっていると考えられます。なぜそのようなことになってしまうのか、どのようにすべきかNICT様のお考えをお聞かせください。

A11： セキュリティに係る費用がコストとみなされがちなことはそのとおり。大きな問題が起こらないとセキュリティの重要性がなかなか理解されない。ただ、あまり喜ばしいことではないが最近のようにランサムウェアで引っかかりお金がかかる事例が頻繁に耳にするようになると、被害に遭った場合の備えとして、世の中に説明できる人材が会社の中にも必要だということが分かってくるのではないかと思う。そういった意味では、被害事例により学習する場面が顕在化しているので、更に被害を広げないためにもうまく事例を活用してセキュリティの必要性に共感いただけるような取り組みが必要と感じている。

Q12： 人材育成、共同研究について、CYNEXのプログラムの枠組みの中で、大学に対して求めることはありますでしょうか。

A12： 個別の技術で共同研究を行っている大学はすでにいくつかある。また、セキュリティに関する教材を自校だけではなかなかアップデートできないと悩んでいる大学、高専も多く、NICTで保有する教材を共同で活用してもらう等、いろいろな連携の可能性があると考えている。

Q13： 大学の教育過程での協力では、enPiT-Securityにおいては東北大学がサイバーセキュリティに関する講座を提供するなどの取組があります。こうした講座の中で学生をNICTの活動に体験参加させることで理解を深めさせるような取組はいかがでしょうか。また、大学としてNICTにご協力を出来ることはありますでしょうか。

A13： 将来的には出来ることもあるのではないかと思う。NICTでは、リサーチアシスタントとして学生を受け入れている実績もある。また、多くのNICTの研究者が大学の講義に出向いており、今後ともそうした取組も進めていく必要があるのだろう。サイバーセキュリティの分野の先生は人材不足でNICTの研究者もかなり多忙。

以上

記録作成担当者：織田秀夫

ヒアリング調査報告 No.21 基本情報

日時	2022 年 9 月 22 日
テーマ	経済安全保障とサイバーセキュリティについて
ヒアリング先 (担当者)	総務省 サイバーセキュリティ統括官室 参事官 酒井雅之 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 岡本樹、織田秀夫、木戸友香子、山田麻友 (計 5 名)
調査目的	サイバーセキュリティに関する総務省の政策を確認し、政策提言に向けた課題の把握および研究を模索すること。

(写真)

【質疑応答】

1.法律との関係性について

Q1： 現行の法制度ではサイバーセキュリティは企業側の努力義務となっておりますが、企業経営者の意識レベルの差によって、対策にも差が生じてくるものと考えられます。重要インフラなどへのサイバー攻撃は、経済活動への影響のみならず、国民生活や我が国の安全保障にも広く影響することを鑑みれば、もはや企業の努力義務だけでは不十分と考えます。努力義務から一歩踏み込んで、例えば重要インフラについては車の車検のようにセキュリティ診断を定期的に実施するなど最低限必要と考えられる事項について義務を科す必要があるのではと考えますが、電気通信事業者・放送事業者・郵便事業者を所掌する総務省内ではこのような議論はなされていますでしょうか。また、サイバーセキュリティ統括官室様としては、義務化の必要性についてはどのようにお考えでしょうか。そして、義務を課す場合は、各業法改正での個別対応、サイバーセキュリティ基本法改正で一元的対応、どちらでの対応が現実的でしょうか。

A1： 企業が負う責任は、サイバーセキュリティ基本法だけではなく、事態対処法や各業法などにも定められている。重要インフラ事業者が目標とすべきサービスレベルは各業法等に定められているが、これらを NISC が安全基準等としてとりまとめて公表している。NISC は重要インフラ業界毎に、業法等に定められた安全基準等をどこまで満たしているのかについて毎年調査しており、その結果は NISC の HP で公表されている。小規模な事業者まで一律の対策を義務化出来るのかとなると難しい面もあるだろ

う。

Q2-1： サイバー攻撃の被害を抑制するために、国際関門局（外国と日本の境界にあるゲートウェイ）にファイアーウォール機能と IDS（侵入検知）機能を持たせ、危険な通信を遮断するとこが出来れば我が国の安全保障・経済安全保障において有益と考えます。サイバーセキュリティ統括官室様としてはどのような見解をお持ちでしょうか。

A2-1： セキュリティ一般にいえることだが、先に何をどのレベルで守るのかを決めないとコストが無限にかかってしまう。通常、ファイアーウォールは企業が自身のネットワークシステムを守るために設置をするものである。これを国の規模に拡大して、国際関門局にファイアーウォールを設置して日本全体を守るということになると、相当なスケールになるので、技術的にそれが出来るのか疑わしい。安全な通信と危険な通信の識別ができなければ、安全な通信もろとも止めることとなってしまいかねず、正常な通信にも影響が及ぶ。現在、総務省施策はこうしたアプローチをとっていない。

Q2-2： DDoS 攻撃については止めやすいと思います。電気通信事業法上も、通信の妨害をする物は止めていいことになっています。DDoS 攻撃パケットを止めるだけでも相当の効果が期待できると思います。NICT が運用する NICTER の観測点情報を AI で処理し、怪しい発信源の IP アドレスのテーブルを作成し、AI で大まかなフィルタリングを掛けるのであれば、演算処理の負荷はそれほど大きくないと思います。NICT で研究・調査したうえで社会実装を検討すると良いのではないかと思います。

A2-2： DDoS は頭の痛い問題である。現状では、通信事業者が自らが管理するネットワーク上の DDoS 攻撃の全てを遮断するのは困難だろう。攻撃側は、膨大な数の IoT 機器をウイルス感染等で乗っ取り、C2 サーバーから指示を出し、特定の標的に一斉に攻撃を仕掛けてくる。攻撃を受けるサーバー側の自衛的な対策として、DDoS 攻撃を遮断する民間のソリューションサービスを利用することは可能である。攻撃指令を出す C2 サーバーを特定出来れば、別のアプローチによる対策を検討できるが、敵も巧妙で、C2 サーバーは 1 個止めただけでは対処をすることが難しいのが現状。

2.NICT に関する事項

Q3： NICT が運用している NOTICE についてですが、脆弱なパスワードによるログインなどを行う上で、不正アクセス禁止法に関する違法性阻却理由について、どのようなプロセスを踏んで、どのような議論がなされ、どの様に整理されたのでしょうか。

A3： IoT ボットネットという DoS の攻撃インフラが社会問題になっていた。NOTICE では日本のインターネットに脆弱な IoT 機器がどれだけ接続されているのかを調べている。工場出荷時の設定で用いられているような、一般的に知られている ID とパスワードの組み合わせで管理されている IoT 機器は脆弱だと言える。こうした ID とパスワードでログインを試みる行為は不正アクセス禁止法に抵触することから、NICT が調査目的で実施する IoT 機器へのログインの試行を、不正アクセス禁止法の例外とするため、NICT 法改正を行った。現行法では NICT による調査が許されるのは、2023 年度までの 5 年間に限定されている。その間に脆弱な IoT 機器を探して対処いくという取り組みとなっている。

Q4： NICT が運用している NOTICE についてですが、現在の取り組みに加えて、希望する企業に対するインターネット側からのセキュリティースキャン（サイバーパトロール）を組み入れることは可能でしょうか。また、NICT 法などの制度面で支障があるとすればどのようなことがあるのでしょうか。

A4： そのような取り組みは研究領域ではなく事業領域になる。研究機関である NICT が

これを行うのは現実的ではない。

Q5： NICT が運用する NICTER で観測したサイバー攻撃観測・分析結果を国内電気通信事業者へ提供し利用者への注意喚起以外の用途、例えば電気通信事業者の国際関門局においてサイバー攻撃の遮断に活かすことは現実的でしょうか。また、このようなことを実現する場合、現行の国立研究開発法人情報通信研究機構法第 4 条（機構の目的）には合致するものの、同第 14 条（業務の範囲）を越えてしまうと考えますが、このような理解でよろしいでしょうか。さらには、電気通信事業法の改正も必要となるのでしょうか。

A5： C2 サーバーの IP アドレスを検知して ISP にその情報を共有し、全ての ISP が一斉に C2 サーバー発の通信を遮断することが出来れば一定の効果が期待できると思う。しかし、C2 サーバーの IP アドレスを検知して追跡するのは簡単ではなく、また情報の信頼性をどのように担保するのかが課題になる。

3.その他

Q6： 電気通信設備に用いる装置類のサイバーセキュリティについてですが、サプライチェーンの段階で、バックドアなどが埋め込まれないよう相当注意を払っていることは大手各社へのヒアリングで確認できております。より安全性を追求するのであれば、部品レベルでも全て日本製にするか、同盟国内製に限定するといった対応が必要と考えますが、サイバーセキュリティ統括官室様としてはどのような見解をお持ちでしょうか。

A6： サプライチェーンについては高い関心がある。全てを社内で開発していれば最後までトレース出来るが、今は海外製品を使うのも当たり前になっている。総務省では来年度の概算要求の中で、SBOM（Software Bill of Material：ソフトウェア部品表のことで、ソフトウェアサプライチェーンのなかで利用されているソフトウェア部品を正確に把握するための手法）で主要な装置の構成部品の一つ一つの出所を調べる取組み試行的に取り組む予定である。

（追加質問）

Q7： サイバーセキュリティ基本法を根拠に作られているサイバーセキュリティ協議会について、加入が任意なのにもかかわらず 303 団体入っている理由、加入することへのメリット及びデメリット、また、今後、サイバーセキュリティ協議会へ求めるものについて教えていただけますと幸いです。

A7： 日本国内には、JPCERT や IPA のような、セキュリティ注意喚起情報を集めて、評価、公表している機関がいくつかある。こうした情報があるにもかかわらず、セキュリティ協議会が必要になったのは、APT 攻撃のような一般に知られていない攻撃が存在するからである。攻撃された企業が、観測した攻撃手法や対策方法を、他の企業に情報共有していくことが理想型だと思う。

以上

報告書作成担当者：織田秀夫

ヒアリング調査報告 No.22 基本情報

日時	2022 年 9 月 26 日
テーマ	我が国の経済安全保障について～端緒と現施策、及び今後の展望～
ヒアリング先 (担当者)	衆議院議員 自由民主党 元幹事長 甘利明 様
場所	議員会館及びオンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凛香、岡本樹、織田秀夫、梶山敬生、香高優一郎、山田麻友 (計 7 名)
調査目的	経済安全保障施策の中心に立つ甘利明議員からその概要をご教示いただくとともに、メンバーが抱く疑問についてお答えいただくこと。

(写真)

＜現地での撮影＞

＜オンライン上での撮影＞

【レクチャー】
（経済安全保障の端緒について）
私は、戦車やミサイルが大変だ、といった従来の伝統的な安全保障から、新たな安全保障の概念がだんだん出てきたと感じていた。それは、データ駆動型社会に端を発している。20 世紀は石油を制す者が世界を制したが、21 世紀はデータを制する者が世界を制する。そのデータをどのように構築していくか、どのように守っていくのか。これによって国の栄枯盛衰が変わってくると非常に感じた。特許の世界では、模造品やコピー品、あるいはそっくり特許を盗んで同じものを作りコストを安くというのはあったが、国家や企業の運営に関わる重要なデータが窃取されると、それまでに投じた年月や資金が水の泡になってしまうと思った。このようなことから、新しい安全保障の分野、あるいは従来の安全保障とシームレスに繋がっていく部分について、問題提起をしたいと思った。

【質疑応答】
1.経済安全保障一般に関するご質問
Q1： 経済安全保障に関しては国会においても幅広い理解を得て法案策定がなされたものと承知していますが、そうした幅広い理解を得るために苦労されたことや留意されたことなどがございましたらご教示いただければ幸いです。
A1： 理解を得るというのは多数を得るということ。何に苦労したかというと、最初の枠組みを作る際の匙加減。80 点は取らない方がいいかな、というか取れないな、難しい課題は次のバージョンアップをするときに組み入れようかな、というようなこと。コロナ禍において、日本は、ミサイルや爆弾ではなく、簡単な物品でチョークポイントを押さえきることで崩壊すると分かった。医療現場の 3 品、医療の手袋、マスク、ガウンがないと、診療行為が止まる。医療体制が崩壊するということは日本が崩壊することなので、文明国家は簡単に侵攻することができる。このような背景の下、重要物資のサプライチェーンを洗い出すことで、リスクがある国、緊張感で対峙している国に多くを依存すると日本のチョークポイントは握られるな、と皆さん感じたと思う。
これがまさに経済安全保障であるが、最初から満点を取らない方がいい、65 点でいいと思った。80 点や満点にしたいがために法案全体が成立しないことは一番まずいと思った。そこで、セキュリティクリアランスを、経済安全保障に関して最も重要な一つの要素でありながらあえて外した。例えば、国同士・企業同士が機微な研究を共同で行う際に、相手の国からその機密が漏れないような人員で研究しないといけない。セキュリティクリアランス制度がないため、日本だけ先進国の中で研究者の裏取りができない。つまり、機微な情報に参加している人が、スパイかどうか裏取りをできないのは日本だけである。
類似した法律として特定秘密保護法がある。これは、公務員を中心に、国家の特定秘密に関わる人がバックグラウンドチェックをするもの。もっとも、これは申告制度であり、調査機関が全部裏取りしたわけではない、ものすごく簡便な調査方法である。ただ、この法律ですら、デモ隊が国会を取り巻いた。セキュリティクリアランスは民間に対してまで同様なことを広めていくという話なので、この項目が経済安保推進法にあるだけでもデモ隊が国会を取り巻くと思った。したがって、これはどうしても施行したいが、最初から満点や 80 点以上を目指すと全体が崩れると思ったため、あえて外した。
そうしたら、野党が賛成をする際、付帯決議をつけてセキュリティクリアランス制度を早く施行しましょうと言ってきた。これはとてもありがたい話である。最初から我々が持ち出したら多分反対されたと思うが、国会で議論をしていく中で、機微技術を守る、データを守るという仕組みの中に、あるべきものが日本にはなかったということで野党が注文を付けたと思う。
最初から 100 点とか、80 点とかを欲張らず、ギリギリ合格点を狙っていこうとか、

このようなところが、少し苦労をした点である。

Q2： 我が国の経済安全保障を守る上でデュアルユース技術をどのように取り扱うべきとお考えでしょうか。また、昨今の台湾海峡の情勢やウクライナ侵略等を受け、こうした考え方に対する議員の先生方の考え方が変化しているような状況は見られますか。

A2： 世界は民生も軍事も区別はない。全てデュアルユースである。アカデミアの研究成果を軍事流用してはならないというようなことを言っている国は日本以外には世界中どこにもないと思う。

2.サイバーセキュリティに関するご質問

Q3： サイバー攻撃の被害を抑制するために、国際関門局（外国と日本の境界にあるゲートウエイ）に IDS（侵入検知）機能を持たせ、危険な通信を遮断するとこが出来れば我が国の安全保障・経済安全保障において有益と考えます。

一方、これを実現するためには、「通信の秘密」を定めている憲法第２１条 第２項とこの趣旨を踏まえて策定された電気通信事業法第４条（及び第 179 条の罰則）の改正等について検討し、侵入検知によって得られる公益と通信の秘密の保持の利益衡量を適切に行い、国民の理解を得る必要があるかと思います。

A3： サイバーの世界には有事と平時の区別はない。中国やロシアからはサイバー攻撃が今この瞬間にも山のように来ている。サイバー空間は常に有事の状態にある。このためサイバー攻撃には専守防衛は成立しない。攻撃元を特定するアトリビューションが重要である。攻撃元を突き止めてそこから攻撃できなくする。また、サイバーの世界とリアルの世界は全く違う。常時、国民の通信を傍受しているわけではない。色々なところからくるサイバーアタックをふるいにかけて残った怪しいものを調べるという考えに立てば、通信の秘密とは棲み分けが出来ると考えることが出来る。

Q4： サイバーセキュリティ対策を進めていくには、高度なセキュリティ人材が増やしていくことが必要であると考えており、そうした人材は日本の優位性へとつながる人材となるのではないかと思います。こうした人材が海外へ流出してしまうことを防止するためには、日本に残ることが魅力的と考えてもらう必要があると思いますが、どのような取組が重要と考えられますか。

A4： 人材の問題は極めて重要な課題の一つである。日本ではサイバーセキュリティの人材及び IT 人材が圧倒的に少ない。これに対して、政府は今取組を強化している。また、政府と大学、企業コラボレーションをして人材を育成し、キャリアパスまでしっかりと繋げていくという取組を始めているところである。サイバーセキュリティの人材は半導体に係る人材とも一部重複している。同盟国・同志国間でどのように人材を育成していくかについての情報交換を行うことや、サイバーセキュリティや半導体に関する仕組みについての学習を取り入れていけたらいいのではないかと考えている。また、IT やサイバーセキュリティについてブラッシュアップする機会についても設けたい。

3.サプライチェーンに関するご質問

Q5： 我が国の持つ半導体技術は、製造機械やシリコンウエハー等の分野で非常に優れているという評価を得ています。しかし、その様な技術を持つ企業に対して、CHIPS 法でアメリカ自身も自国内で技術を保持する方向に進んでいる状況の中、半導体分野において我が国が優位性・不可欠性を確保するためには、有志国間での調整をどのようにすべきとお考えでしょうか。

A5： 半導体は実際に日本にとってハードの部分を全面的に支えている部署だから、非常に重要なところである。日本は半導体に関して、例えばシリコンウエハーのような材

料の分野は、日本が信越化学はじめ、三井三菱化学系の会社が担っている。
製造装置は感光剤を塗布する技術から出来上がりを検査する技術、あるいはシリコンウエハーを極小の幅で焼き付けていく露光装置等、いろいろな分野があるが、総合して、日本の製造装置産業は世界の35%を占めている。日本に何が欠けているかというと、半導体の中で頭脳の部分で該当するロジック半導体、CPUである。
ロジック半導体の生産基盤をどう作っていくかというと、材料や製造装置の優位性をどう生かしていくかということになる。材料でいうと、日本の製造技術のすごさは、シリコンウエハーの平坦度、3,000 万分の1 以内にフラットに作れる技術、そして、シリコンウエハーを世界最高のイレブンナインという純度で仕上げる技術があることだ。
それから製造装置でも東京エレクトロンを初め製造装置部門全体の世界シェアが35%にのぼっている。ただ、露光装置という、フィルムを写真に焼き付けるような作業をしていく装置が現在、線幅が極小化していて、今や5nm から3nm の世界になっている。3nm 当たりに刻んでいく装置は、オランダが独占している。だから、日本の強みは、この露光装置以外の製造部分に関する力が強いこと、材料は日本が世界一ということ。そして、足らない部分と連携をとっていく。
世界最高の露光装置製造企業はオランダのASMLだから、オランダとアメリカと日本で同盟国同志国間の連携をとる。この強みの連携で日本に拠点をつくるということは大事だ。例えば、熊本のTSMC 工場では12nm から28nm までのラインができる。これからの自動運転や工場現場のさらなるスマート化にとってですね、大事になっていく。シングルナノレベル(10nm 未満)の半導体が自動運転や工場現場のスマート化等で需要が拡大しているため、日米間で、アメリカの設計技術を使って日本の製造技術をコラボし、作っていこうというようなプランやTSMCとソニーの合弁、それからウエスタンデジタルとKIOXIAの共同投資の国による補助などの協力が行われている。
日本が半導体戦略を打ち出した時点で色々な国から提案が来ている。同盟国同志国連合の拠点を日本とアメリカあるいは欧州に一つずつ作っていくということは大事で、それに向かって今、全力でプランが進んでいるところだ。これから10年計画ぐらいで、相当な金額をアメリカにならって、日本も負けないくらいの支援の仕組みを作っていかなければならないと考えている。

Q6： サプライチェーンの問題を考えるときに権威主義国家によるエコノミック・ステイトクラフトは無視できないと考えています。これに対抗するためには経済安全保障推進法による国内業界との調整も必要になると承知していますが、それ以外にも有志国との協調が必要不可欠であると考えています。もっとも有志国といってもどのような枠組みでどのような国と関係を構築するべきかについては様々な意見があると承知しています。我が国はCPTTP、RCEP、IPEF等の多様な枠組みを有していますが、さらに国際協力を強化するためにはどのようなことが必要でしょうか。また、有事には完全デカップリングとなっても支障がないように代替手段を考えなければならないと考えられますが、平時にはある程度のリスクを織り込みつつ最先端技術以外は権威主義国家ともある程度の経済関係を維持せざるを得ないとの意見もありますが、その際に留意すべきことなどについてご教示いただけますと幸いです。
A6： 経済安全保障の推進法の4本の柱の1本目の柱が重要物資のサプライチェーンを洗い出して、リスクを克服するために、(サプライチェーン上に)どういうリスクが存在するか、当事者の民間企業、あるいは国と連携して対応していくかというものだ。重要物資を指定して、それがどういう供給網で日本の市場にもたらされているかということ洗い出す必要がある。そして洗い出した先にどういうリスクがあるか、つまり、この権威主義国家がそのサプライチェーンの一翼を担っており、そこの国と外交関係がおかしくなったときに、それを止められてしまうと、全部の生産が止まってしまう

というようなことになるとしたら、リスク分散を図る、同盟国、あるいは同志国の間でサプライチェーンが完結するようにする、あるいはサプライチェーンをいくつかに分散する、あるいは、この体制の違う国に多くを依存してきたものに関して、その代替品を開発するということが1本目の柱だ。

2本目の柱というのが、インフラ、電気、ガス、水道をあるいは物流、あるいは金融等のインフラのリスクを洗い出す。例えば、金融システムのインフラを更新するときに、導入する仕組みはどの国のものかと、非常にリスクがある国からその機器や部品が納入されてないか、あるいはその更新作業をするような企業が、日本と緊張関係にある国からの出資がその企業になされてないか等、そのようなリスクを洗い出して、是正していくということがインフラの強靭化となる。

そして、エコノミック・ステイトクラフトというのはかなり幅広い概念だ。例えば、市場国に対して日本経済が輸出をして、そこへの依存度が高いと、向こうから見たら輸入を完全に止めた場合、日本経済に大きなダメージを与えることが可能である。そうした自由貿易の考え方とは違う考え方をするような市場国に、一般のものでも過度に依存していると、輸入を止められたり、増やしたりすることによって、日本の産業界が翻弄されてしまう。だから、貿易による内政干渉のことをエコノミック・ステイトクラフトと呼んでいる。世界で市場国というのは、アメリカとEUと中国しかない。つまり市場が大きいから、世界の経済がそこの市場に依存していく。そうすると依存度が高くなると、相手の国に生殺与奪権を与えてしまうということになるから向こうが急に輸入をやめるといった場合に、日本経済が立ち行かなくなるようなこともないように、何がどこに依存しているか、相手の国は政治的リスクがどのぐらいかといったことを洗い出し、もし外交関係が緊張したときに、向こうが難癖をつけて、例えば農産物であれば、問題が生じてからは一品ごとに検査をするといって、上陸をさせないような嫌がらせを受けたときに、日本経済が深刻ダメージを受けないかということをきちんと精査していく。これがエコミック・ステイトクラフトに対する対抗策だ。つまり、リスクがある国にいろんなものを過度に依存しすぎないということが「経済安全保障」だ。特に「重要物資」については、サプライチェーンの中にそのような国を入れない、政治・外交的に安心できる国でサプライチェーンを組む、あるいはものすごく大事なものについては、日本で代替品を開発する、あるいは一定の供給が止まったときにシステムが止まってしまわないよう重要物資の備蓄をどう図るか等、通常の供給システムに支障がないようにするために、いろいろ弱点を洗い出して、対策を打っていくということになる。

4.経済安全保障推進法における官民協議会に関するご質問

Q7： 先端技術を育成するための官民協議会においては研究開発等に従事する人からの同意が協議会の設置のためには必要であると認識していますが、できる限り広範な同意を得るためにはどのようなことが必要でしょうか。

A7： 経済安全保障推進法の4つの柱の中で、3点目は世界中が日本に依存するような技術を開発していくという三本目の柱。官民協議会で色々なチームを組んで、AIや量子といった、世界がしのぎを削っていく分野の専門家を集めて、官民で協議会を作る。安全保障基金2500億が確保されている。そのうち1250を文科省所管のJST、残りの1250を経産省所管のNEDOにわりあてられている。これを早急に5000億に積み上げる。最終的に1兆円にしたい。豊富な資金をAIとか量子、バイオなどに関し、これからを担う先端研究のチームを作って、経済安全保障のための資金を投入してその研究を完成させていく。具体的な設計は現在行っている。具体的には政令に落とし込んで行っていく。

Q8： 協議会により開発された技術の社会実装は、実装の段階であっても協議会の中だけ

で行われるのか、それとも新たに民間企業などと協力してオープンに行っていくのとどちらが望ましいと考えられますか。技術の種類によっても異なるかもしれませんが、ご教示をいただければ幸いです。

A8： 特定の重要技術を研究開発していく際には、もちろん秘密保持について制約をかけていかなければならない。研究成果を都合の悪い国に窃取されたら意味がない。その中で研究を進めていく。知財をどう守るか、公開しないかについては４本目の柱に非公開特許という仕組みを作る。世界の先進国にあって日本にないもの。セキュリティクリアランスがないのと同様に、日本にはないものである。秘密特許という言葉に昔の戦時中のイメージがあるのかもしれない。特許の非公開制度、特許は公開が原則であり、製品を開発して、作っていくノウハウをみんなが持つという事だが、これを緊張関係にある国に持たれてしまっては、日本の技術から日本を脅かす技術を作られてしまう。日本の技術が日本のリスクとなる。日本が非常に困るような武器になるものについては公開をしない。色々なやり方がある。普通のものは作れるが、一番いい部分についてはブラックボックスとする。そこから出てきた技術について世界中に実装されれば役に立つというものについてはオープンにしていく。オープン・クローズ戦略については研究していくテーマが具体的になっていく中で考えていくことがいい。モノによってはビジネスで成功する可能性もある。世界中はほぼ同じであるが、最高性能のものは日本だけが持つなどというビジネス戦略もある。オープングローズ戦略は会社の技術によって様々なやり方があり、一律ではない。一つの会社、一つの技術ごとに戦略的に考えていくのがいい。その過程で民間企業に参画してもらわないと実装できない。研究を開発していくのと実装していくのにはいろいろなやり方がある。

Q9： 研究チームには所属しているが協議会の参画には同意しない場合や、協議会から離脱した研究者などが協議会に参加せずとも、研究は継続して行うことが可能であると理解しています。このような場合、協議会には参加していないため機微な情報の提供は受けないが研究チームの一員として共同研究を行うという状態が続くと考えられますが、機微な情報を持っている研究者と持っていない研究者が共に研究を行うことは、機密保持や研究協力の観点からも問題が出てくることが予想されます。そのためにも後述のセキュリティクリアランスやカウンターインテリジェンス等がより重要になると考えられますが、どのように取組を強化するべきでしょうか。

A9： 国家のお金を使い、国家の経済安全保障や伝統的な安全保障に資するような技術を開発していく。世界のチョークポイントを握り、日本が開発していく。日本の国益がかかっている。そのためには趣旨を理解し、参加してもらうと言う意思表示をしてもらう必要がある。セキュリティクリアランスについても参加する人に関してはバックグラウンドのチェックも行い、国の重要技術研究に参加している人が政治的に対立している国の関係者ではないという証明をすることが必要になってくる。機密を保持しながら研究を進める体制を作るために、セキュリティクリアランス制度がない状況でどのようにしていくのか。みなし公務員であるなら、重要秘密に関わる人間として秘密を漏らさないという誓約をしてもらう必要がある。国のお金を使い、日本の国益に資するような研究をしていくための今の法制の中での秘密保持の仕組みや、SC の仕組みができた時にどうしていくか考える必要がある。今ある仕組みや将来できる仕組みについては、効果的に使って研究が日本に資するようなものになるようにする必要がある。研究した物が対峙している国からの攻撃に、資することとならないように取り組んでいく必要がある。やってみないと分からないということもある。研究に参加する人の意思を縛りすぎないことも重要だが、国のお金を投じることから、研究成果がよその国に摂取されると言うことがないようにすることが重要である。

5.経済インテリジェンスに関するご質問

自民党においては、「提言『経済安全保障戦略』の策定に向けて」や「『経済財政運営と改革の基本方針 2022』に向けた提言」において経済インテリジェンス体制・機能の強化について言及されています。もっとも、経済安全保障推進法においては経済インテリジェンスの文言について記載はなく、経済財政運営と改革の基本方針 2022 においてはインテリジェンス能力の強化について言及があるものの、具体的内容は未だ決定していないものと理解しております。
これらを踏まえ、

Q10： 現状における経済インテリジェンス体制・機能をどのように強化するべきかについて先生の考え方をお聞かせいただければ幸いです。

A10： まず、民間企業において、経営指標の中に今までなかった手法、経済インテリジェンスに対してどういう体制をその企業が取れているかということが、企業を経営していく重要な要素になりますよ、ということは申し上げてきた。重要技術をもとに製品やサービスを提供している企業が、サイバーアタックに対してどういう防御を全体としてとっているか。従来の財務諸表での投資対象適格不適格かに加えて、経済インテリジェンス上の措置がなされているかということが投資対象企業として重要な要素になりますよと、いうことを何年も前から申し上げてきた。つまり、BS や PL は非常に良い数字、経営内容も財務状況も満点で投資対象としては A ランクの企業という評価があっても、経済インテリジェンス上の認識がない場合には、突然倒産しますよ、というようなこと。例えば、そこの会社の製品は非常に優れていて、競争力もあって使い勝手も良くみんな使うけども、それにバックドアが仕掛けられていたり、マルウェアが混入していたり、そのようなことがないという保証がないようなサイバーセキュリティシステムしか取ってない企業からは、サイバーセキュリティ上の対応が甘いということで製品の納入を切られることがある。つまり、BS も PL も絶好調だが明日倒産ということがありますよということ。
事実、アメリカの国防総省に納入していた企業が、突然契約を打ち切られた例が発生した。その会社はサイバーセキュリティを国防総省が要求する基準を満たしておらず、そこの製品はサイバーアタックを受けやすいから、どういう仕掛けがなされてしまっているかわからない、そういうものを導入するとこちらが危ないということで、打ち切られた。経営指標の中に、財務上の指標及び経営がうまくいっているかどうかの指標以外に、経済インテリジェンスに対してきちんと意識を持って備えているかということが、その企業の投資対象の新しい基準として入ってきますよ、ということを申し上げてきた。例えば、アメリカの NIST（National Institute of Standards and Technology）（国立標準技術研究所）の SP800-171 と枠組みがあります。国防総省は、国防総省に製品やサービスを納入している企業に対して、SP800-171 を基にきちんとサイバーセキュリティが図られているか要求してくると思う。つまり、サイバーアタックに対して甘い企業は、どんなにいいものを作っていようとも納入しないという新しい経営指標が加わってきますよ、ということを申し上げている。民間経済が健全に運営していくための指標として、経済安全保障の指標が加わったことが、現社会だと思っている。

Q11： 経済インテリジェンス体制・機能を強化する際に、参考とすべきと考える国等がございましたら、教えていただきたいです。

A11： もちろんアメリカであり、オーストラリアだと思う。そういう基準から言えば、イギリスを含め、ファイブアイズの国々は、それぞれ従来の安全保障のチーム情報を共有しているため、サイバーセキュリティ標準というのは、基本参考になると思う。あるいは、エストニアやリトアニアといった IT 先進国。IT の先進国は、サイバーセキュリティに関しても、かなり水準が高いと思う。こういった IT 先進国、あるいはサイバーセキュリティに対してきちんと意識のある国のシステムは学ぶべきだ

と思う。

Q12： 経済インテリジェンスの強化に当たっては、企業のみで実施することは困難であると考えられます。今回のウクライナ侵略においては大学や民間シンクタンクの専門家が積極的に情報収集・分析・広報を行っていたようにも見受けられます。とりわけ地域研究という観点からは大学の力は不可欠なようにも見受けられますし、海外ではベリングキャットのような民間における OSINT を専門とする企業が活躍しているようです。インテリジェンスにおいて大学や研究者がどのような役割を果たすべきかについてお考えがありましたら教えていただきたいです。

A12： インテリジェンスは、経済の側のインテリジェンスと、いわゆる従来の安全保障から伸びてくるインテリジェンスと、両方あると思う。民間の活力以前に、政府としてのインテリジェンスの仕組みが全くできてない。アメリカの元情報長官デニス・ブレアさんが日本に来て、日本のサイバーインテリジェンスはマイナーリーグだと。アメリカの同盟国・同志国の間で一番水準が低いと言われて帰ったが、まさにその通りである。日本は、インテリジェンスコミュニティの指揮命令系統が確立されていない。それぞれに防衛省が担い、外務省が担い、経産省が担い、総務省が担い、あるいは内閣官房が、あるいは公安が担ったりしている。これらが合同して行う会議はあるが、指揮命令系統がきっちりしていないのと、やはり人員が全然いない。政府の仕組みからまずしっかり作っていくことが大事だと思う。

民間については、先ほどから申し上げているように、企業経営に新しい視点、経済安全保障という視点を企業経営に１本加えてもらいたい。製品の優秀性に加えて、企業として、経済インテリジェンスにしっかり関心を深めて、サイバーアタックを跳ね返すような仕組みが、体制が取れていることを納入先の機関に認識してもらわないと、あそこの製品サービス危ないよねという評価が生じた際に、どんなにいいものを作っていても倒産する危険があることを経営者に理解してもらいたい。

Q13： 米国には RAND,CSIS、豪州には ASPI、英国には RUSI、IISS 等の有力なシンクタンクが政策提言やインテリジェンスにおいて大きな力を発揮しているように見えます。議員の先生から見て日本のシンクタンクとこうした他国のシンクタンクとの違いや、我が国のシンクタンクはこうあって欲しいというお考えはありますでしょうか。

A13： 日本にはインテリジェンスに関して忌避する雰囲気がある。一番大事な部分であるが、民間企業もシンクタンクも、インテリジェンスの提言が出来るようなところは聞いたことがない。学術界において全体的に安全保障研究を避ける雰囲気は各自にあり、外交においてインテリジェンスを研究の中心に据えて提言をするシンクタンクは見当たらない。我が国の安全保障の確保のためにはインテリジェンスは必要不可欠である。日本の憲法には、日本国の存続と日本国民の安全は各国の良識にゆだねると書いてある。しかしながら、ロシアの良心に期待していたが、ウクライナは現在のような状態になった。安全保障に関わるインテリジェンスに忌避感を持つような状況はおかしく、それを専門に研究し、提言をするところがもっとなければならないし、それが求められているのではないか

6.セキュリティクリアランスに関するご質問

Q14： 令和４年の経済安全保障対策本部中間とりまとめではセキュリティクリアランスへの言及などもなされておりますが、このセキュリティクリアランス制度はどのようなものであるべきでしょうか。現状では特定秘密保護法における適格性審査が似たような制度であると考えられますが、同じように考えるべきでしょうか。それとも違うものとして考える必要がありますか。

A14：　特定秘密保護法のセキュリティクリアランスというのはファイブアイズ標準には全く足りない。アメリカやイギリスや豪州が合格点をくれるとは思えない制度である。国家同士が機密情報をやり取りするというのは、共有する国から漏れないことが前提である。今ある特定秘密保護法では海外の基準を満たしていない。とはいえ、以前よりは日本にリスクがかかるような国際的な情報が入るようになった。だとしてもファイブアイズで共有している情報は日本の秘密保持能力が懸念されている現状では日本に入ってこない。民間機関同士が海外の民間機関と共同研究を行う場合には共有する機密データが日本側から出るというようなことが一つでも起きてしまうと日本の大学や企業とは研究出来ないという事態にもなる。そうなると日本の大学や民間企業はデカップリングされてしまうため、それを阻止していかなければならない。色々な国同士で共同研究をするが、日本からは情報が漏れるという指摘があると国際競争力などの観点からはギリギリの状況で、これ以上先延ばしに出来ない。ということで経済安全保障の骨子を出した。セキュリティクリアランスを本格的に導入しようとするとかなり大変である。秘密の度合いが高くなる機密情報を取り扱うことになっていく。関係者は身辺を洗われて面倒なことになる。それをクリアしないと機微技術を共同研究するというコアなところに日本は入れてもらえない。早くから国際標準に見合う仕組みを作って行かないといけないと考えている。

7.その他

Q15：　本ワークショップは、11 月上旬に豪州を訪問し、調査研究活動を行うほか、米国・台湾等との制度比較を実施したいと考えております。先生は経済安全保障を研究される際に他国を様々に参考にされたと承知していますが、これらの国においてどのような方・機関にどのようなお話を聞いてくるべきと考えますでしょうか。アドバイスをいただければ幸いでございます。

A15：　アメリカにもオーストラリアにも様々なシンクタンクがある。オーストラリアには、インテリジェンスにかなりフォーカスを絞ったシンクタンクもある。そういう機関についてはご紹介できる。私は、CSIS 含めアメリカの様々なシンクタンクと協議しているし、キーノートスピーチをしたこともある。

（追加質問）

Q16：　鉱物資源は現在各国が確保に鎬を削っている状況ですが、どのように確保していくべきでしょうか。

A16：　重要物資を極力政治外交上のリスクがある国に依存しないっていうのは基本的な考え方だ。ただし、ある程度依存しなければ成り立たない、つまり、特定の国に特定の資源が偏在をしているということがあるから、極力多国間で調達できるようにするということが基本だがどうしてもリスクのある国に依存するという可能性も排除できない。そのときは何をするかというと、その国にとって、致命的に大事なものを日本は持っているということが必要だ。これは技術でもいい。日本の技術がないと立ち行かなくなる等、相手のチョークポイントをこちらが握る、日本のチョークポイントを特定の国に握らせないということとだ。そしてリスクのある国とどうしても交渉することが、(可能性として)ゼロにはならない。その時にはその国が日本に依存している依存していくという物を日本が持つ。これは技術でもいいが、日本の技術が供与されないと立ち行かなくなるというような、相手のチョークポイントを日本がもつ。そのために戦略的重要な技術を開発していく。日本しか持ってない技術というのは、リスクのある国に対する抑止力になるから、向こうがそうならこっちも対抗できるという材料を持っているということが必要だ。

Q17： 日本の大きな強みとしての技術について、特にどの部分が権威主義体制の国に有効であるとお考えでしょうか。

A17： アメリカが、半導体で日本と組みたい、というのは、アメリカには優れた設計能力があるが、製造能力というのは日本がいろいろな分野で世界トップに立っている。半導体材料を 99.9^{-11} にできること、半導体基盤をフラットに、高低差を 3,000 万分の 1 以内に収めることなど、驚異的な物作りの技術があるからそれをしっかり生かして新たなものを作っていくっていうことが一つあると思う。そして、日本は世界を変えるような発明を結構している。

3D プリンターは世界のもの作りでなくてはならない存在になっているが、これは日本が発明して現物を作った。けれども、幅広い事業化になる目がいかなくて、特許を放棄してしまった。それを拾い上げて、ビジネスとして成功させたのが海外の企業だ。

日本が生み出して世界のものになったものはたくさんある。日本は技術で勝ってビジネスで負けるということよく言われるが、強みはしっかりブラッシュアップして、それから、産業化していくためにどこにネックがあったかということを洗い出す。これは主に資金的なものだが、研究を実装していくために、資金が必要だ。「死の谷」や「ダーウィンの海」と言われるように、できたものを製品化していく、量産化していくのに、資金が足りない。資金供給的なもので技術が製品化されない、技術で勝ってビジネスで負ける、ということを克服していくための資金供給の仕組みもしっかり作っていく。なければ、海外のベンチャーキャピタルを呼び込むような仕組みが必要だ。今我々は国立大学の改革をやった。10 兆円の大学改革の資金というのを作った。特に国公立大学は自分のアセットを使って大学自身の基本財産、予算を増やしていくという感覚はほぼゼロだ。

海外の大学は、私学以外でも、例えばアメリカで言えば、州立大学、UC バークレーみたいなところでも、公的な補助金はどんどん減っているが、予算は 7%以上毎年増やしている。それは自分の研究シーズや大学が持っているアセットをマネタイズして、あるいは商業化していく仕組みを持っている。ということは、大学というのは研究をし、人材を育てる上に、その研究成果をビジネスに繋げていくという、経営を考える人が世界中のトップ大学に必ずいる。

日本には、運営を考える人ばっかりいるけど、経営を考える人はいない。自らのアセットをどうやったら有効活用できるかということを考えて、基本財産を増やして年度予算を増やしていくというように切り替えていかないと、国家予算だけで、年率で大学の予算を 7-8%のレベルで拡大していくということはできない。だから、大学改革とは、経営を考える人を置いて、大学の運営を、使命に従って人を育てる、研究をする、加えて学術の中心的存在としての従来の使命以外にも、研究成果をビジネスに繋げていくという視点がないと(海外との競争に)負けてしまう。そのために大学を改革して、研究のデータベースを作ってそれをシーズとして、どうマネタイズして行くかという仕組みを今作りつつある。世界中の大学就中、アメリカの私学は数兆円の endowment、基本財産、基本基金を持っている。

私学だからと言う人がいるが、UC バークレーは州立大学であり、オックスフォード、ケンブリッジはいわば国立大学である。国立大学でも endowment を 1 兆円持っている。東大は 180 億円と(海外に比べ、)桁が 2 桁違う。だから今からではもう間に合わないので、国が 10 兆円規模のファンドを作った。これを運用して、3000 億を意識の高いところに投入していく。その対象から外れたところにはまた別な総合パッケージというのを作って、私学も含めて、しっかり応援していく。また、既に、博士課程の大学生で、一定水準以上のレベルであれば、生活費を支給するというのも始めた。

年間 200 億の予算を、既に取って、毎年、博士課程に進む人にも負担を減らして

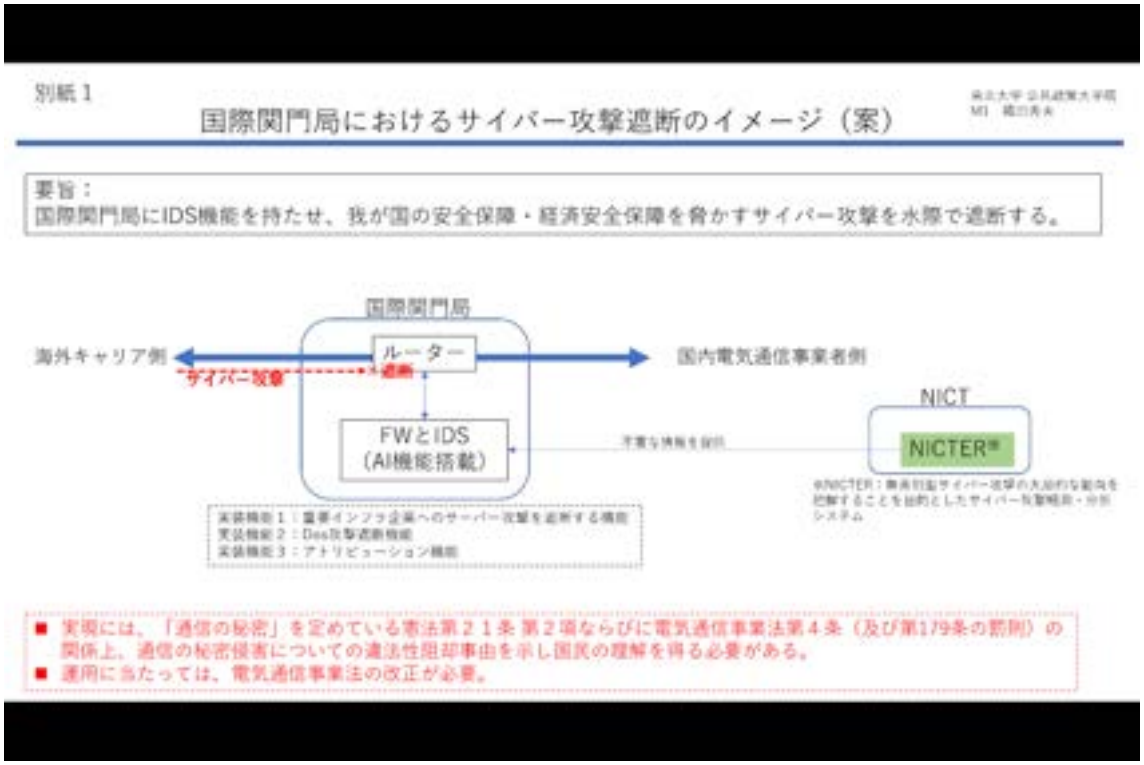
いっている。これを一連の大学改革で我々が取り組んできた。その大学のシーズをスタートアップに繋げていくような、いわば、グローバルキャンパスみたいなものも作ろうというプランが今、実行に移りつつある。3年以内にはグローバルスタートアップキャンパスができる。そこには世界中の優秀な大学がサテライトキャンパスを設置する。そういう日本にアジア最大のシリコンバレーのように、研究成果がよくてシーズがあるのに、それがビジネス化できず、ビジネスで負けるということがないように、研究から実用化、実用化から製品化していく際に、資金力ができるような仕組みを作っていこうと考えている。それが日本もう一度世界に冠たる技術立国に復活させるという道筋だと思っている。

Q18：　先日9月16日、自民党において経済安全保障推進法の基本方針を了承したという報道がなされたと理解しております。その基本方針の中の第１章の第２節「安全保障の確保に関する経済策の実施にあたって配慮すべき事項」の一つとして、「事業者等との連携」が記されておりました。先ほどのインテリジェンスにも関わってくると思いますが、経済安全保障は国家だけではなく、むしろ企業や大学が自発的に行動することが求められると思っております。ただ、企業や大学が自発的に行動しない要因として、経済安全保障に対する危機感や、情報共有がなされてないことが挙げられると思います。従いまして、基本方針にも記されている通り、いかに国家と企業、大学それぞれが情報共有をするかが重要なことと理解しております。このような状況のもと、先生が考える経済安全保障に関しての、国・企業・大学の情報共有体制を今後どのように構築していくべきか、教えていただければ幸いです。

A18：　サイバーセキュリティの世界は、常に新しい脅威が出現する世界である。だから、国から注意してくださいと言われたところから外れた場所でも様々問題が発生する。民間は国から言われていることをしたけどひどい目に遭った、ではなくて、サイバーセキュリティのリスクに常にさらされているという自覚のもとに自身でいろいろ対処する姿勢が必要である。

　また、想定していなかった事件等の情報を官に上げていただいて、官のなかで共有して、それをそれぞれ所管官庁から降ろして、常に民間が得た新しいサイバーセキュリティの情報を得ることができる体制の整備を構築していくことが必要である。

Q19：　ご覧いただいている別紙「国際関門局におけるサイバー攻撃遮断のイメージ（案）」のように、怪しい通信については日本の入り口で遮断するという考え方についてのご質問です。中国のグレートファイヤーウォールとまではいかないまでも、我が国においても懸念国等からの怪しい通信パケットを海底ケーブルの陸揚げ局で遮断すれば、サイバーセキュリティには有益だと思います。技術的にはある程度のことは出来るとしたうえで、このような取り組みをしようとした場合、憲法で定める通信の秘密にも抵触する恐れが出てきます。このため違法性阻却事由を整理し、国民の理解を得る必要があるかと思いますが、この種の議論について国会の空気間というかハードルの高さとしてはどの程度のものでしょうか。



A19：　憲法で保障されている通信の秘密のコアの部分である通信の内容に立ち入るようなことはしない。つまり、怪しい通信の外形的な部分をフィルターにかけてフィルターにひっかかった通信のみを調査をしていくというように説明する。フィルターを掛けること自体は通信の秘密を侵害するものではないということを理解していただくことが大切。

Q20：　追加 A1 のような議論は政府内では始まっていますでしょうか。
A20：　まだ本格的議論は始まっていない。フィルターにひっかけて落とした通信のアトリビューションを行い、反撃するということが重要である。アトリビューションは 1 丁目一番地、攻撃元を特定しそこに適切な反撃をすることということが必要である。またサイバー攻撃は宣戦布告なしで行われている。サイバーの世界は常に有事状態にある。フィルターで濾して危ない情報の発信元を突き止める。その仕組みについて理解を深めることが重要。

Q21：　被害を受けた企業自らが反撃は違法行為になりかねないと考えています。反撃するとすれば国家になると思いますがいかがでしょうか。
A21：　日本政府としてサイバー部隊が反撃をする。ある企業のユーザーに対してだけでも 1 日 30 万回ものサイバーアタックを受ける。一箇所当たり 100 回の攻撃があり、3000 箇所ぐらいから毎日攻撃を受けている。95%は簡単に跳ね返せるが、1%は高度な技術が要る。攻撃元を突き止め、攻撃できないようにすることは国が考えないといけないと思っている。

Q22：　アトリビューションを行うための手法として他国がやっているビーコンプログラムを打ち込んで相手のサーバーを突き止めるような追跡手法を日本ではないものかを考えた場合、NISC と司法機関の連携体制においては、どちらが司令塔になってアトリビューションを進めるべきか先生のお考えをお聞かせいただければ幸いです。

A22：　人材が集まっているのはNISCだが、NISCはサイバー実動部隊ではない。実働部隊をどうするか、そしてNISCを司令塔とした指揮命令下に実動部隊をどのように繋げて行くかを考えなければならない。
　サイバーについては従来の安全保障と同じ定義を当てはめて対応判断すべきではない。サイバー攻撃は宣戦布告もなしに行われ、しかも常時有事の状態にある。反撃力が非常に重要であり、アトリビューションをして攻撃元を叩く。憲法解釈についてもサイバー戦と物理戦は別物という理解の元で議論すべきである。サイバーは新しいカテゴリーとして（法制度）を組み立てた方が良いと考える。

Q23：　他国、例えば米国においては、FBIは国内捜査以外の広範な権限を持っています。今後はこのような点についても研究を進めていきたいと考えておりますが、アドバイス等いただけますと幸いです。
A23：　サイバーについて、特に防御について何処までやるかは、新しいカテゴリーとして組み立てたほうが良いと個人的には思っている。

以上

記録作成担当者：岡本樹

ヒアリング調査報告 No.23 基本情報

日時	2022 年 10 月 4 日
テーマ	経済安全保障に係るサイバー空間とインテリジェンスの関係について
ヒアリング先 (担当者)	慶應義塾大学大学院 政策・メディア研究科 教授 土屋大洋 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、梶山敬生、香高優一郎、宮内拓、山田麻友 (計 7 名)
調査目的	経済安全保障についてサイバー空間やインテリジェンスを中心に、学生の疑問についてお答え頂き理解を深めること。

(写真)

【質疑応答】

Q1： 海底ケーブルは有事になれば切断されるため、ある程度我が国自身で制御しなければならないと考えております。オーストラリアなどの近隣諸国とは安定しているものの、その他諸国とどのように関係性を安定させればいいでしょうか 。

A1： Submarine Cable Map という海底ケーブルを示した地図がある。日本近海には多くの海底ケーブルが通っている。その反面ウクライナが面している黒海にはケーブルがあまり通っていない。2014 年のロシアによるクリミア併合の後、ケルチ海峡ケーブルが併合 2 か月後の 2014 年 4 月に作られた。それ以後、クリミア半島の情報はロシアとつながる 1 本の海底ケーブルのみでコントロールされている。情報源のすべてである。オーナーはロシア企業であり、その企業が握ってしまっている。一見すると単なる民間のインフラ事業であるが、全ての生活に影響を与えており、政治経済文化に大きく影響している。ミランダというのはロシアのメーカーである。

一方で台湾には海底ケーブルが多く存在している。しかし、1996 年に台湾の南部で地震が発生し、海底ケーブルが切れてしまうということがあった。そのため、東京の投資家が香港の金融市場にアクセスすることが出来ないという事態が発生した。海底

ケーブルの切断や海底ケーブルの陸揚げ局を襲撃するような物理的な破壊が行われる可能性もあるが、物理的な方法以外にもサプライチェーンを利用した形で、不正な部品が仕込まれるという可能性も考えられる。

最後にオーストラリアについてであるが、オーストラリアは巨大であるが島国である。オーストラリアの海底ケーブルはハワイやシンガポールを経由している。特にシンガポールとのケーブルが自分たちの生命線だと理解していることから、こうしたケーブルがどこに陸揚げされているのかについては情報を出さないようにしている。他の国の場合はこういった情報は漏れていることがあるが、オーストラリアではシドニーに沢山入っている海底ケーブルの詳細な住所については法律によって隠されている。しかしながら、情報について暴露する人もいるため問題となっている。

オーストラリアと中国との関係については、新型コロナウイルス流行までは良好な関係だった。オーストラリアの大学についても中国の資金が入り込んでいた。しかし、新型コロナウイルス発生源の調査についての話題がでてから対立するようになり、豪中関係は非常に劣悪となったことからクアッドへとも繋がったと考えられる。

Q2: ウクライナが、スペースX（SpaceX）の衛星インターネットサービス、スターリンク（Starlink）を使用しています。技術的に、将来的にはスターリンクが海底ケーブルを代替するのでしょうか。

A2: 19世紀の半ばに海底ケーブが創設された。現在と比べると細い銅線だった。マルコーニの無線通信は第一次世界大戦から第二次世界大戦まで使われたが、海底ケーブルは第二次世界大戦の際に切断されてしまった。その復興をしていく中で人工衛星を経由した通信という発展があった。その後、人工衛星を介した通信は2秒程のラグがあったが、ラグのない光ファイバーの海底ケーブルを使用する時代へと移行した。スターリンクについては静止軌道衛星よりも低い軌道に人工衛星を飛ばしている。しかし、高度が低い所では重力に引かれてしまうことから、燃料を使い周回させる必要がある。そのため同じ場所にい続けるということが難しい。海底ケーブルは有線であることから、ケーブルを引きにくいところについては、スターリンクを介すことによってネットワークを利用することが出来る。ウクライナにおいても、地上の光ファイバーが切断された事例があった。そうした場合はスターリンクは使っていくべきである。これらがどこまで使えるのかは通信容量の問題であるが5Gについてはウクライナではどこにもない。スターリンクのネットワークは速いことから、戦況について伝えやすくなる。置き換わるとは思えないが、非常時の代替手段としては有効である。電波は各国の主権が強く、ウクライナでは政府がスターリンク用の周波数を許可するから使える。ロシアはスターリンクの周波数を許可していない。許可されていなくても使おうと思えば使えるが、スターリンクをロシアに合法的に持ち込めないようになっている。電波は非常に主権が及ぶ領域である。

Q3： 土屋様が考える経済安全保障の定義について、ご教示いただけますと幸いです。

A3： 経済安全保障は政府の法案の中でも定義されていない。法律を作成する際は、使用される言葉について定義をするのが当たり前であるが、あえて定義をしていない。この理由としては、多元的な意味があるからだと思っている。

私が（経済安全保障について）聞かれたときにはいつも、ロバート・ブラックウィル（RobertD. Blackwill）というアメリカの元外交官が著している『War by Other Means：Geoeconomics and Statecraft』という本を紹介している。タイトルの意味は、経済に限らずいろいろな手段を使い、実質的な戦争を行うということ。彼が書いた論文や講演録によると、彼は「地経学」という言葉を使っている。地経学という言葉について、彼は「国益を促進あるいは擁護するため、また地政学上有利な成果を生み出すために、経済的な手段を用いること。また、他国の経済活動が自国の地政学的

目標に及ぼす諸効果。」と定義をしている。私はこの定義がフィットすると思う。経済安全保障という曖昧な言葉を使うよりは、地経学や、需要エコノミクス、エコノミックステイトクラフト等を用いた方がいいと思う。

元々、日本では1970年代の末に、元朝日新聞記者の船橋洋一さんが『経済安全保障論-地球経済時代のパワー・エコノミックス』という著書を出版している。こちらが、（経済安全保障のような議論についての著書として）日本では早い段階で出版され、このような書籍が出版されたことによって、通産省が通商白書の中で取り上げている。それから3年ぐらい経つと、政権が変わり、大平政権のもと総合安全保障という言葉に変わる。経済だけに限らず、様々なことを踏まえて安全保障考えなければならないという議論に変化した。このような議論がいつの間にか忘れられたものの、2020年代になってまた復活してきたというのが今の状況だと思う。そういう面では、「経済安全保障」は元々古い言葉であり、様々なところで意識的に使われていた。私として「経済安全保障」の定義は、ブラックウィルの地経学の定義がよいと思う。

Q4： 経済安全保障が生まれた原因として、米中対立が大きな要因と私どもは考えています。米中対立等、国際関係が厳しくなった原因についてご教示をお願いします。

A4： 2016年のアメリカ大統領選挙中、トランプ候補が大きな貿易赤字を問題視した。その原因は、中国が不正な貿易をしているからだとしていた。政治経済学的に考えると、覇権国と言われるグローバル化の中心となる国は赤字体質となるということが学問的に分かっている。しかし、政治の世界では赤字になると困るという意識がある。それは、会社が赤字になって困ってしまうことと同じイメージである。そしてトランプ候補は赤字の原因は中国にあるということを一種の政治的なステートメントとして言っていた。カリフォルニア大学バークレー校の教授だった、ピーター・ナヴァロがトランプのアドバイザーになった際に『米中もし戦わば』という本を出しているが、米中対立についてトランプ候補に吹き込んだ人がいる。その過程で色々な物資を中国に依存していることが分かってきた。結果としてそれが政治的に取り上げられたという事である。もちろんグローバル化の中では、そういう一部の物資を原材料や製品を海外に依存するというのは当たり前である。しかし、トランプの場合はアメリカファーストやメイクアメリカグレートアゲインという言葉を繰り返し使っていく中で、そういったことが攻撃対象となった。そして中国の不公正貿易が明らかになったことが、経済安全保障という言葉が日本で生まれた理由である。しかしながら、経済安全保障という言葉はアメリカではあまり使われていない。英語のエコノミックセキュリティの本来の意味は、家計を維持するということである。エコノミックセキュリティをいわゆる国家安全保障という使い方で使っているのは日本人だけである。アメリカ人はエコノミックステイトクラフトやジオエコノミクスという言葉を使っている。そしてそうした考え方はトランプの指摘から始まったのではないかと思っている。

Q5： 米国はじめ諸外国は「国防は経済に優先する」という考えで、企業に対し、安全保障の観点から保護や排除をしていると考えております。一方で日本がこの考えで政策を進める場合、どのような課題があるとお考えでしょうか。

A5： 日本は貿易国家であると自分たちを定義してきた。特に資源については輸入せざるを得ないため、貿易を止めるわけにはいかない。江戸時代は非常に自立した経済であり、ほとんど長崎を通じて中国、朝鮮半島、オランダとしか貿易をしていなかった。物資がなくても成り立ってはいた。理由としては人口が少なかったことや、人口抑制策が取られていたためである。産児制限や生まれた子供を育てないということが日本社会の中で行われている時代だったからこそ、ある程度自立的な経済が江戸時代では維持されていたと思う。しかし、現代で同様の事を行うことは出来ないため、海外から物資や食料を輸入し、それを何らかの形で埋め合わせるような製品を輸出するとい

うことが必要となる。第二次世界大戦の際に日本は大東亜共栄圏としてアジアの国々との連携を強めて、欧米との関係を断つことによってブロック経済を実行しようとした。結果的に大きな戦争を生み出し、日本敗戦に繋がっていることから、そういった選択はしないということが第二次世界大戦後の日本の政策である。中国との関係は厳しくなっているが、それ以外の国々との関係について断つことは出来ない。中国との政治的な関係性がよくなれば関係を復活させていくということになるだろう。今は注意しておく必要があることとして、不公正な形で日本の技術が中国に渡ってしまうということについては止める必要はあるが、全面的な排除は政策として考えられない。

Q6： サイバーセキュリティを目的として、世界標準となるような指標を作ることについてどのような意義はあるでしょうか。標準となるものが明らかになることで、企業間の取引の際の安全性の参考になるのではないかと思っていますが、攻撃をする側からも基準が分かってしまうことになるので問題があるのではないかと考えています。

A6： サイバーセキュリティに関する色々な指標が作られている。例として、ロンドンにはIISS（国際戦略研究所）というシンクタンクがあるが、そこで世界各国のサイバー能力についてレベルわけをしている。具体的にはティア１、ティア２、ティア３という風にレベルが分かれている。そしてティア１に入っているのはアメリカだけであり、その他の国々はだいたいティア２に含まれている。日本についてはティア３であるとされている。サイバー攻撃は標的の裏をかいていく世界であり、標準となるものが決まったとしても、それを守ればなんとかなるという世界ではない。標準については最低限守らなければいけないというミニマムなものとしては意味がある。しかし、その最低限の基準を守り、さらに超えていれば満足という事ではない。100%のセキュリティはないということが常識であり、信頼をしてはいけないということがサイバーセキュリティ上の世界のルールとなっている。標準を基準として自分たちは大丈夫であるということにはならない。それだけを守っているだけでは攻撃側に隙を与えることとなり、効果が薄くなると考えられる。

Q7： オーストラリアでは、民間主導サイバーセキュリティセンター(Industry-led Cyber Security Growth Center）に出資をすることによって国内のサイバーセキュリティ市場の活性化を図っているとのことでした。国全体としてサイバーセキュリティを強化していくためには、市場を活性化させることによって、意識を向けさせることが重要でしょうか。また、国としての組織だけでなく、民間としてもサイバーセキュリティに関する組織があることの利点とは何でしょうか。

A7： 民間と政府との間で協力することは当然であり、サイバーセキュリティはチームスポーツであると言われている。1人エースがいればいいわけではなく、色々なアクターが協力していく必要がある。アメリカや韓国では政府で働いている若い人材を大学院に行かせ、修士号や博士号を取得させることによって、最新のサイバーセキュリティを学ばせている。また、政府の費用を奨学金として使うことから、政府に戻って来ることを求めるが、3〜7年などの期間を経た後に民間へ出ていくというケースもある。そうした人は最新の知見を持った人であり、かつ政府の中でサイバーセキュリティを担当した人が、民間に出ていき起業をして民間のサイバーセキュリティビジネスを始めることによって、民間企業を守っていくということをしている。政府の中から知見を持った人が順に民間へ出ていくという構図が出来る。このことによってサイバーセキュリティ市場が活性化するだけでなく、国全体のサイバーセキュリティの活性化へとつながる。この２つの前提があることから、有能な若手政府職員を大学院に活かせるための奨学金を用意することが出来る。そして、そういった人たちが起業した時に、そういうサイバーセキュリティ起業を他の民間企業がどう使っていくかにかかっている。例をあげるとすれば、銀行や鉄道会社といった企業がサイバーセキュリテ

ィ企業を使うかどうかである。そういった企業について信頼をすることが出来なければお金を払うということに繋がらず、ビジネスとして成り立たなくなってしまう可能性がある。このビジネスとして成り立つかについてうまくいっている国とうまくいっていない国がある。そして日本はうまくいっていない国である。警察庁でもサイバー局を作ったことから、能力構築を更に進んでいくと考えられる。それに加えて、能力を身に着けた人が外に出ていく事を止めない方がいいのではないかと思っている。そういった人材に民間を守るということをやってもらっていく。そのためには、今政府が検討しているセキュリティクリアランスについてうまく運用していく必要があり、これがうまく行けばサイバー局でセキュリティクリアランスを取った人が民間に出ていき、政府の情報もある程度共有を受けた上で民間を守っていくことが出来るのではないかと思う。

Q8：　オーストラリアは抑止を目的としたサイバー攻撃を保持しており、攻撃をされた場合に反撃が可能であると印象づけることから、抑止力が働くと考えています。抑止を目的としたサイバー攻撃能力の威力としては、実際にサイバー攻撃をされた際に同程度のサイバー攻撃能力を持って反撃することが出来る能力と同等のイメージでしょうか。また、攻撃との表現はついていますが自衛力ととらえていいものでしょうか。

A8：　一般的な核ミサイルの時代に知られていた方法としては、懲罰的抑止と拒否的抑止という物がある。懲罰的抑止というのは攻撃に対して徹底的にやり返すというイメージである。そして拒否的抑止というのは攻撃をしても意味がないという認識をさせる抑止である。拒否的抑止についてはレジリエンスと言い換えることも出来る。どんなサイバー攻撃を受けても、オーストラリアの企業や政府がそれに意に介さずにいる状態である。しかし、そこまで言い切ることはかなり大変である。懲罰的抑止を考える際に、どうやって懲罰を加えるかについて、国際法の世界ではプロポーショナリティという言葉がある。それは、被害を受けたら、それに見合うだけの反撃しかしてはいけないということになっている。しかしサイバー攻撃を受けたらサイバー攻撃でしか反撃が出来ないかというとそんなことはないというのが今の解釈となっている。つまり、サイバー攻撃を受けた後ミサイルで反撃をしてもいいことになっている。このことからサイバー攻撃に対してサイバー攻撃だけでの防衛や反撃に限定してしまうと防御が出来なくなってしまう。今はクロスドメインというが陸海空宇宙サイバーのあらゆる所を使って防衛・攻撃が行われるという風に考えられるため、あまりサイバーという所に限定をしない方がいい。日本の場合には 2018 年の防衛大綱に緊急時、非常時においてサイバー攻撃を日本が受けたら、相手のサイバー攻撃能力を妨げることが出来るという風になった。しかし、これについてはあまり意味がない。なぜなら、仮に日本の原発に対するサイバー攻撃が行われて放射能漏れや爆発が起きたという状況下でサイバー攻撃の発信元にウイルスを送り込むというのは意味がない。原発が爆発してしまった時点で自衛権の行使が可能となるため戦闘機やミサイルでの反撃が可能となる。サイバー攻撃に対してサイバー攻撃で反応するということはあまり考える必要はなく、それにとらわれていると抑止をすることが出来ないと思う。どんな攻撃でも自分たちに対して攻撃をしたならば、それに対して何らかの方法で反撃するということが重要なのではないか。

Q9：　オーストラリアでは、中国を念頭に外国からの影響を受けないための立法措置を取ったとのことでしたが、こうした法律が作られた理由として国内でどのようなことが問題として感じられていたのでしょうか。

A9：　『目に見えぬ侵略　中国のオーストラリア支配計画』という有名な本が出ている。クライブ・ハミルトンという作家が書いた本であり、最初は相手にされていなかった。その本の中では、オーストラリアが中国のお金に影響を受けているということに

オーストラリアの人が気づかず、気づいていたとしても問題視はしなかったために、これからの未来についても中国と共にあるとオーストラリアは思っていたとされている。中国との協力を進めるということが政府・大学・企業レベルで行われていた。新型コロナウイルスが流行したことから、モリソン首相が新型コロナウイルスの発生源について確認すべきだと主張したところ、中国が豹変した。中国人の観光客を送らない、オーストラリアのワインを輸入しないという色々な経済制裁を始めた。これにより、オーストラリアは中国について信頼出来る国ではないと感じるようになった。そして中国を排除するという方向に方向転換をした。アメリカについても同様であり、中国のことを信じていた。『China 2049』という本が出ており、これは元 CIA の分析官が書いた本である。中国は 2049 年までの 100 年戦争を戦っているという趣旨の本である。これも最初に出た時には全く相手にされておらず、中国を研究している人についても読んではいなかった。しかし、トランプ政権が出来て中国との問題が次々と明らかになるにつれて、中国に対する意識が変わって行った。オーストラリアもアメリカも途中から中国に対する意見がガラッと変わり、中国の実態について我々よりも後になって感じ始めた。ここ４、５年で大きく変わってきた。オーストラリアについては新型コロナが流行した後であり、アメリカはそれより少し前ぐらいからである。中国が様々な形で社会の中に浸透して影響力を及ぼそうとしているということに対する危機感というのがようやく共有されたということではないか。

Q10： オーストラリアでは懸念国に対して様々な立法措置をとられていますが、民間企業やアカデミアにおいて、脅威情報の共有枠組はどのようなものがございますか。

A10： オーストラリアの専門家ではないため詳細について詳細はわからないが、例を挙げるとすれば ASPI と言うシンクタンクがある。ASPI が出したデータベースにおいて、中国の留学生の出身大学についてリスクがあるかどうかっていうデータベースを出している。慶応義塾大学でも留学生が来たい、大学院に行きたいというときや、あるいは向こうの研究者が客員研究員として来たいという時には、まずそのデータベースをチェックする。そのデータベースでリスクが高い大学を教えてくれる。それを見てみると、大学によっては人民解放軍との関係が深いということが分かる。そういう人には来ることについてご遠慮願うこともある。色々な層の脅威情報や、リスクがある組織みたいなものがオーストラリアでは色々研究されてデータベースになっていると考えられる。

Q11： 日本でも今後は官民技術協力による先端技術の保護開発、特にサイバー分野や宇宙開発、半導体といった分野が注力されていくことと思います。そういったなかで、産業スパイも含む情報漏洩に対する保護制度として、特に日本が今後参考にするべき制度などはどういったものがございますか。

A11： 既に高市大臣が言及しているが、セキュリティクリアランスの制度が一番重要であり、この制度については長い間日本では必要だと言われている。それに変わる制度としてかつては公務員倫理法があり、公務員についてはある程度の守秘義務があるため、そういったものを活用していたが、2013 年に特定秘密保護法が作られて防衛に関する情報については、一層厳しくしていくという、法制度化が図られた。しかし、欧米で言われているようなセキュリティクリアランスが、全面的にはまだ採用されていない。一部防衛省自衛隊外務省の人は認識しており、特に日米安保に関わるような人についてはバックグラウンドチェックが行われている。ただ日本においては全面的に採用されているわけではない。アメリカの人口は約３億２千万人いるがそのうちセキュリティクリアランスを何らかの形で持っている人は 500 万人いると言われている。500 万人というのは、東京都の 3 分の 1 ぐらいであり仙台市より遥かに多い。それぐらいの人たちが政府の秘密を保護しながら情報を共有するとい

う枠組みの中に参加している。セキュリティクリアランスについては色々なレベルがあるうえ、一旦セキュリティクリアランスを取ると一生涯使えるというものではない。てある程度年限が来たら、それを一度取り直さなければいけない。民間にいる人たちにもセキュリティクリアランスはかかっている。例えば政府で働いていた人が政府をやめたとしても、その有効期間の間は民間企業にいながらクリアランスを維持することも認められている。そういった制度を維持することについて、私が10年ぐらい前に調べたときは年間円で1兆円ぐらいの、経費がかかっていた。特にバックグラウンドチェックが大変で、例えば本格的にセキュリティクリアランスが実施されると、私が政府の中で働いて防衛関係の仕事をするときには、私のバックグラウンドをチェックが行われる。私は最初に124ページぐらいの文書に全部いろいろ記入し、生まれてこの方、行ったことがある全ての国について書きなさい、借金があります、何か不倫関係がありますかということについて全部書かないといけない。不倫をしているから、借金があるからといって弾かれるというわけではなく、嘘をつくかどうか確認をされる。そこで私は不倫なんかしていませんと言いながら、実際にチェックをする人たちが確認をした時に浮気をしていたという事実がわかるとその人を弾くということが行われる。例えば昔だったら同姓愛者であるということもネガティブな要因だったが、今はそれを公言しているかどうかが問われる。つまり外国政府に弱みを握られるかどうかを確認しなければいけない。そうしたことを500万人分チェックするとものすごいお金がかかる。それを民間企業に委託するため、もっとお金がかかる。そういった制度を日本はどれくらいのスケールでやるのかが今問われている。もう一つ日本の場合には政治的な問題、歴史的な問題がある。元々中国系の人や朝鮮半島系の人がいて、そういう人たちがずっと差別されてきた。あるいはいわゆる部落差別というものも残っていて、特定の部落出身の人々は自分の出自を知られるということが嫌だということがある。そうしたことがあり日本はそのセキュリティクリアランスの制度を入れられなかった。そこを乗り越えてこの制度を作って、諸外国とサイバー、宇宙などの様々な分野で、情報漏洩がしないように情報を守っていくことをやるというのはすごく大変だと思う。しかし、私はこういう制度をつくるべきだと思っており、そういうバックグラウンドチェックされるのが嫌であれば、私はクリアランスが必要な仕事はしませんと言えばいいだけの話だと思うので、セキュリティクリアランスが一番やらなくてはいけないことではないだろうか。

Q12：　我が国は経済安保推進法のサプライチェーン強靭化において、半導体等の物資が特定重要物資に指定されると予想されています。今後サイバー空間がますます重要になるにつれ、必要となる物資は半導体や大容量電池の他にありますでしょうか。

A12：　どこにでも必要となるものとして、半導体や電池というものはあげられるかもしれない。しかし、意外なものがどうしても足りなくなる可能性はある。レアアースについては電子製品を作るときには必要となってくる。政府の法案の中で議論をしたときにマスクもサプライチェーン上重要な物資であると言われていた。可能性としては、別のパンデミックといった大きなことが起きた時に、意外な物が足りなかったとなるのかもしれない。政府においても何がサプライチェーンなのかを特定するという作業が始まっており、その中で出てくる可能性はあるが、現状で他に何かあるかという所については特には思いつかない。

以上

記録作成担当者：山田麻友

ヒアリング調査報告 No.24　基本情報

日時	2022 年 10 月 4 日
テーマ	重要インフラに関連する経済安全保障について
ヒアリング先 (担当者)	東北電力株式会社 阿部克之 様、齋藤靖浩 様、竹内直人 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 9 名)
調査目的	重要インフラでは経済安全保障についてどのような点が重要視されているのかについて調査を行うこと。

(写真)

【レクチャー】

電力における経済安全保障というのは電力供給の安定のことである。そしてそれには 2 つの観点がある。1 つ目としてはリスク管理、2 つ目としてエネルギー安全保障の観点である。

まず 1 つ目のリスク管理について、統合報告書というものが東北電力のホームページに掲載されており、詳細が記載されている。具体的なリスク管理としては、管理方針を定めており、リスクの分析・調査を行っている。災害や市場、オペーレーションリスクに分散して対応している。特に重要な案件やリスクについては統合リスクマネジメント管路を行っている。

そして 2 つ目のエネルギー安全保障については S+3E ということを意識している。これは S が安全性、そして 3E が安定共有、経済性、環境性を表している。東日本大震災以降、原子力発電の稼働が止まっている。このことから、化石燃料が 7 割を占めている。化石燃料については石炭とガスが燃料となっており、使用する燃料を分けることでリスク分散をしている。また、原子力発電の再稼働や再生可能エネルギーについても現在取り組んでいる。ウクライナ侵攻によって燃料の高騰や途絶リスクが発生している。さらに 2022

年3月の福島県沖地震の影響で火力発電が停止していることから、これに代わる供給力確保が課題となっている。

【質疑応答】

Q1： 御社の発電設備、送電設備の制御系システムのサイバーセキュリティ対策については全て御社独自で実施しているのでしょうか。それともサイバーセキュリティ業務を担う会社に一部の業務を委託しているのでしょうか。

A1： 発電設備等の制御系システムは電力保安通信網という独自の（ほぼ閉域の）ネットワーク上で運用している。日常的な点検と併せて、異変検知もできる仕組みが整っている。ファイアウォールなどで通信を一方向（内側から外側へ）に制限しており、外部側からのアクセスは出来ない仕組みになっている。このネットワーク監視はグループ会社に委託している。高度な解析が必要な部分は専門スキルを備えたベンダーに委託している。また、セキュリティに関する危機管理体制として「東北電力－CSIRT]、24時間体制セキュリティ監視を行う「東北電力－SOC」を整備し、グループ会社と連携してセキュリティ事故の未然防止と事故発生時の被害最小化に取り組んでいる。

Q2： 女川原子力発電所および東通原子力発電所においてはAPT等の高度な技能を有する集団によるサイバー攻撃を想定していますでしょうか。また、APTからサイバー攻撃を受けた場合の被害を最小限に食い止めるためにどのような備えをしてますでしょうか。

A2： ATPからの攻撃となれば一民間だけでは対応できない。日頃からアンテナを高くして、電力事業者間（電力ISAC）での情報共有を行っている。このことは原子力発電所に限ったことではない。原子力発電所については、核物質の管理も重要である。セキュリティクリアランスを経た人のみの間で情報共有している。一般企業がどの程度できているかは把握していないが、東北電力は事業を行う上で必要な対策を行っているものの、APTからの攻撃への備えとしては十分とは言い切れない。

Q3： サイバーセキュリティ技術者の育成については、どのような育成プログラムで取り組んでいますでしょうか。

A3： サイバーセキュリティ専門人材を確保するのは難しい。サーバーやネットワーク技術者の中からセキュリティ人材を育成している。より高度な技術者育成に向けて、IPAの「中核人材育成プログラム[487]」に1年間参加させている。現在参加している社員を含めこれまで3名参加させた。このプログラムでは制御系システムのセキュリティ対策の他、セキュリティ対策の重要性を経営層に理解させるための伝え方なども学んでいる。また、平時における訓練も重要である。そして、机上で訓練プランを作成することも重要である。電力中央研究所とも連携している。

Q4： サイバーセキュリティを高めていくためには、どのような被害があるのかについて知り対策を立てていくことが重要であると考えています。実際に攻撃された被害について共有する仕組みがあった場合に、どのような課題があるでしょうか。

---

[487] IPAが実施しているサイバーセキュリティ人材育成プログラム。産業サイバーセキュリティセンターでは、セキュリティの観点から企業などの経営層と現場担当者を繋ぐ人材（中核人材）を対象とした「中核人材育成プログラム」を実施しています。 社会インフラ・産業基盤のサイバーセキュリティ対策の強化をテーマに、テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ1年程度（7月～翌年6月）のトレーニングで、初歩的なレベル合わせの期間を経てから、実践的で高度な実習プログラムを行っていきます。 本プログラムでは、受講者が自社に近い環境での演習を体験できるよう、各業界のシステムを想定した模擬システムを使用します。また、海外のトップレベルのセキュリティ対策のノウハウの獲得等を目的に、海外関連機関との連携トレーニングを実施します。

A4： 情報共有については非常に重要であると考えている。電気事業者の間で電力 ISAC という組織がある。具体的には電気設備に特化したような攻撃や有効な対策について情報共有をするという活動を行っている。電力 ISAC においても情報共有を行っているが、基本的に電気事業者であるが政府や、NISC、IPA の間でも情報共有は行っている。特に制御システムに対してのセキュリティ対策が難しい。海外で同じような組織があることから、そういったところと情報共有をしている。そこでは、海外のサイバー攻撃の情報や対策について情報共有を行っている。情報共有をするうえで、守る対策を共有することは非常に有効である。しかし攻撃者にとっては、新しい攻撃を考えるネタになることから、扱うことが難しい内容については共有する際にどういったレベルで情報共有をするか、相手が信頼出来るか、オンラインではなくリアル空間でコミュニケーションを取れる勉強会、会合を行うことによって信頼関係を作っていく。ISAC では TLP というルールを定めている。それは、どの人まで機密情報について共有する際にどこまで情報共有をするのかということを分けている。ホワイトは一般にも公開するといった形式で情報を発信する側が整理をしていく。情報を受け取った人が次にどこまで共有出来るか、情報を受け取った人が困らないようにしている。

Q5： 貴社は、宮城県警が主導する宮城県サイバーセキュリティ協議会に所属していると理解しております。当協議会への加入は任意であるものの、加入した理由を教えていただければ幸いです。また、協議会に加入したことのメリット及びデメリットを教えていただければ幸いです。

A5： 東北電力は地域の繁栄といった経営理念があるため、サイバーセキュリティ協議会の、地域の防犯体制にサイバー領域を加えていくという考えは、全く賛同する部分であった。加入は任意であるが、我々も協議会から何かを得ることが多々ある。我々の取り組み等が多くの方の何かしらのヒントになればいいというような気持ちも持ちつつ、入会している。

背景として、日本でオリパラが開催されるにあたりサイバー対策は重要なので、しっかり備えをしなければいけないということで、国にサイバーセキュリティ協議会なるものが設立される動きがあった。従って、地方の団体とかも含め、各県でも同様の体制を作るという動きがあったと思う。その中で、自治体はもちろんのこと、重要インフラということで電力、通信、金融を含め、地域の大企業というか、一生懸命に活動している企業が参画する必要性はあったと認識している。国だけではなく、地域の特性に特化したような企業も含めて活動できればという気持ちもあったと思う。オリパラでも、電力の供給は非常に大事なミッションであり、その際にも県警にサイバーの専門部隊・部署が設置され、そちらの方々と連携して訓練も実施した。実際、宮城県内ではサッカーが行われ、福島県ではソフトボールが行われたので、各県のサイバー関係を管轄する警察関係の組織の方々とも連携して備えをして対応を行ってきた。こういった協議会のおかげで、警察等の方々と連携しやすくなった。オリパラは終わったが、毎年の訓練ではサイバーの部署の方々に参加あるいは見学などをしていただいており、有事の際の確認を適切にできていると感じる。情報共有については、毎月何かを行っているわけではないが、定例の総会で大きな活動の紹介等をしている。このような活動を通して、お互いに相談しやすい窓口や、勉強しやすいような環境になると感じている。協議会に加入することへのデメリットはないと思う。

Q6： 貴社では、電力供給体制におけるサプライチェーン上のリスクを把握していますでしょうか。また、どのような点にリスクを感じていますでしょうか。

A6： サプライチェーンで当社に一番影響のあるものは燃料だ。燃料が途絶されると、電力の安定供給ができなくなる。そのため、燃料のサプライチェーンに対しての備えが一番大きなテーマとなる。

燃料の種類ごとにリスクの大小は異なるが大きく分けると以下の 3 点だ。
⑴　カントリーリスク　⑵　生産設備　⑶　輸送
これらに対し、分散の考え方で対応している。

Q7：　サプライチェーン上のリスクに対してどのような取組をしていますでしょうか。
A7：　あくまで東北電力は受け手側であるため、カントリーリスク、設備リスク、輸送リスクのそれぞれに対策を行うわけではなく、それらを一体のものとして捉えてできる限り分散して調達することが中心となる。
　具体的には、まず燃料種を 1 つに絞らず、油、石炭、LNG に分散する。次にそれぞれの燃料種ごとに調達する国を変える。さらに同じ国の中であっても、積み出し港を複数要しておくことなどが主な取り組みになってくる。
　例えば、LNG に関しては、マレーシア、インドネシア、オーストラリア、アメリカ、カタール、ロシアなどから調達している。しかし、今回のロシアの動きによって、分散させたがゆえにリスクになってしまった。実際の数値的には、LNG の約 10%をロシアから輸入しているため、1/3×1/10=1/30=約 3%のリスクが顕在化していると評価できる。また、石炭に関しては、オーストラリア、インドネシア、アメリカ、カナダ等から調達している。

（追加質問）
Q8：　貴社では SDGs 経営で、再生可能エネルギーの推進を掲げています。今後私どもとしては、東北という地方が半導体の製造拠点となりうると考えていて、半導体製造には非常に多くの電力を必要とする中で、東北地方の安定供給について、どのぐらいのレジリエンスについて備えているのでしょうか。
A8：　リスクの評価を定量的に行うのは難しい。全体のパーセンテージの比率を考えながら対応している。例えばある 1 か所から多くの数量を買うとディスカウントになるというようなことも供給が余っているときにはあるが、そこにあまりに過度に依存しないというところが大きな考え方だ。
　再生可能エネルギーについては、リスク分散の観点から一定程度調達を増やしたいと考えている。
　ただし再生可能エネルギーは、供給が不安定で、特に太陽光は昼間大量に電気が入ってきて余ってしまうが、夜や夕方は足りないということになっている。それを補うために火力発電所が逆の動きの発電をしている。この逆の動きをする発電設備をどれだけ持っているかが、再生可能エネルギーをどれだけ導入できるかが変わってくる。

Q9-1：　カントリーリスクを判断する際国家が絡んでくることもあり、一企業での判断は難しいと理解しております。そのような中でカントリーリスクを判断する際に、貴社が何を根拠に判断をされているのか、可能な範囲でご教示いただければ幸いです。
A9-1：　カントリーリスクを定量的に判断することは非常に難しく、それを定めていることはない。重要なことは、情報を多岐にわたって収集すること。情報収集の手法として、商社を介した手法やエネルギー関係の国際的な機関等様々な関係機関からの収集、国からの情報収集もある。これら収集した情報を総合的に勘案する。また、直接その国に出向き、サプライヤーとディスカッションをしながら情報を得ることもある。これまでに長期間調達している企業があるため、長期間調達を安定的にできるということは、国としても安定しているという考え方もできるし、一方で長く調達していると、国としては一定程度安定しているが、その地方や地方政府が安定しない、暮らしている企業が非常に不安定だとかいう点もある。様々な点を勘案しながら調達している。

Q9-2：　商社や関係機関等で情報収集をされているということですが、それらはサイト等からのオープンソースではなく、密な関係を築いた上でオープンソースではない情報等をいただいているという形なのでしょうか。

A9-2：　こちらについては、一般的な情報というより、対面の中で得られる情報とがメインになる。商社等については、手数料といったそれなりの対価を支払いながら情報を得ている。関係機関についても同じようなところがあり、また、人を派遣していることもある。派遣されたメンバーが、ある国、特定の国に実際赴任し、そこから得た情報を総合的に判断する。

Q10-1：　東北は半導体の生産拠点があり、今後製造拠点として重要であると思う。今後国内電力の安定供給に関して、災害やカントリーリスクに関してどのくらいのレジリエンスを備えているか。

A10-1：　レジリエンスがどれほどか、定量的なところは難しい。安定供給という意味合いではどれくらいの系統が大きいかが一つの指標になる。大きな牌になっていれば安定しているということだ。

日本全体で 50hz,60hz に分かれているが、東北地方は 50hz で、関東地方の東京電力と同じだ。電気的な安定性という意味で、東北地方は東京の非常に大きな系統と一体になっているので、系統的には比較的安定していると捉えていいと思う。東北系統と東京系統を繋ぐ「連系線」が、約 500 万 kW ぐらいあるが、東北系統の規模は 1500 万 kW ぐらいなので、その 3 分の 1 ぐらいが東京系と繋がっている。そのため電気的には非常に安定性が高い。

災害に対するリスクに対しては、当社では発電所を配置する際に分散している。太平洋側と日本海側でほぼ同量で、太平洋側は福島、仙台、八戸などにある。これによって、地震等の災害リスクを一定程度分散できる。実際、震災で被害は受けたが一定期間で復旧が早急であったのは、このように分散された背景があったからだ。このような考え方で今後も安定供給を図っていきたい。

Q10-2：　他の地方に比べてレジリエンスが高いのでしょうか。

A10-2：　特別に東北が高いというわけではない。一定程度安定性が保たれているという位置づけだ。数年前に北海道で地震があったときにブラックアウトが発生した。北海道は単独系統で、本州と 90 万 kw の連系線でつながっているが、災害が起きた時に他から融通を受ける際、線が細いというところがある。安定性はこのような観点で評価すると、東北は大きく系統的に劣っているところはないと理解している。

Q11：　使用可能な原資に限りがあるなかで、電気料金に転嫁できない場合は会社の負担が大きい場合もあると思われます。現状は経産省による補助がありますが、貴社がその他に国の制度として必要なものはありますでしょうか。

A11：　電気料金がある地方のみ高くなることは公共性の面から問題がある。そのため、総括原価方式であったころから各料金が逸脱しないように維持されている。

しかし、電力自由化に伴い規制料金と自由料金とに分かれたにもかかわらず、現在は自由料金にもいまだ規制の考えが残っている。この自由と規制が混在している状態はわかりづらく、東北電力としても動きづらい。そこで、国には、自由度をどちらかに割り切ってもらうことで、この状態を解消してもらいたい。

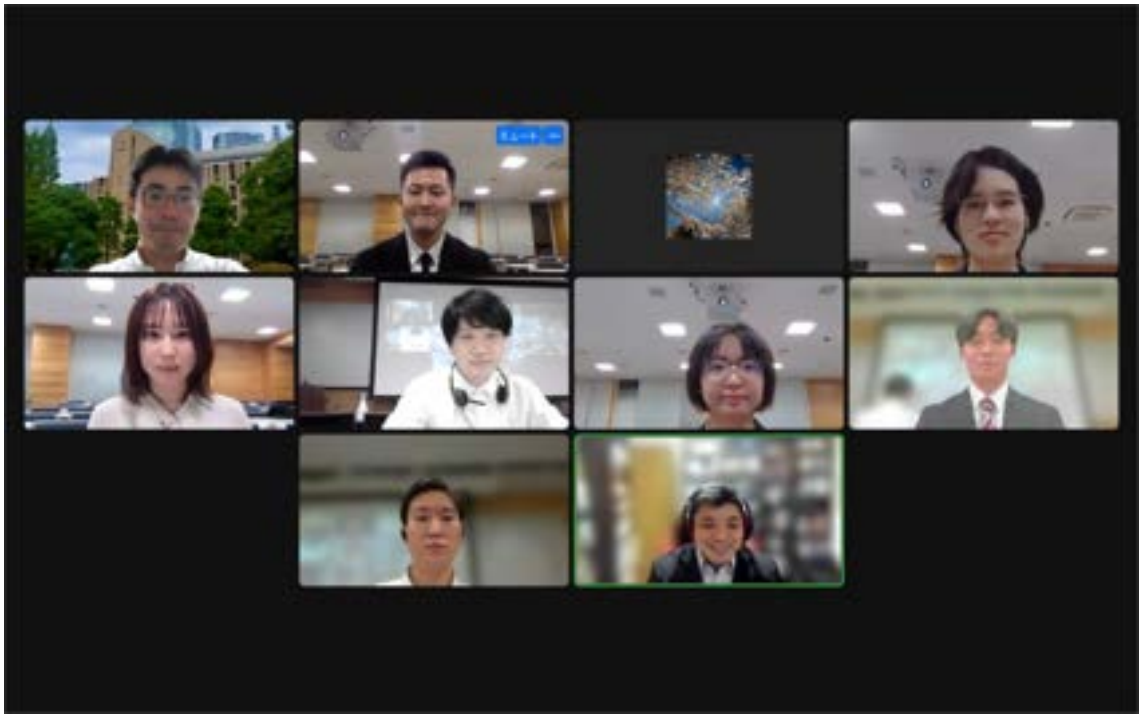
以上

記録作成担当者：宮内拓

ヒアリング調査報告 No.25 基本情報

日時	2022 年 10 月 4 日
テーマ	豪州の経済安全保障について
ヒアリング先 (担当者)	東京大学 先端科学技術研究センター 特任教授 山口亮 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 9 名)
調査目的	豪州ヒアリングをより効果的なものとするため、豪州の制度等について学ぶこと。

(写真)



【レクチャー】

1. オーストラリアの安全保障観

3 つある。

①犯罪・テロ

豪州は多民族国家であるがゆえに、民族間での紛争が多かった。マジョリティである白人 vs 原住民だけではなく、移民系のギャングなど多岐にわたる国内犯罪やテロが起こっていた。

②地政学

マクロな地政学的な敵はいない。しかし、東南アジア情勢にはかなりの注意を払っている。特に隣国であるインドネシアは 90 年代までは独裁政権であり、過激派組織の存在や、東チモールの件もあったため、準仮想敵国であった。ここ数年では、中国が経済成長するとともに南シナ海に進出してきたために、警戒し始めた。同盟国である米国と連携して、中国による工作や諜報を対処しようとしているが、一方で豪州は中国との経済的な結

びつきが強いから、両者のバランスが大事になる。
③環境問題
豪州は気候問題に非常に敏感な国である。特にトーレス諸島は海面上昇により消えてしまう恐れがあり、住民保護と領土維持の双方の観点から対処が急がれている。また、豪州は密輸された外来種により生態系が破壊されることも恐れている。そのため、空港での取り締まりが厳しく、山口先生も過去にイナゴの佃煮で取り調べを受けたことがあった。この豪州の危機意識は昔外国人が外界から様々なものを持ち込んで環境問題が起こったことがきっかけだと思われる。

2.安全保障上の取り組み
豪州は世界の安全が豪州の安全であると考えており、安全保障に対する意識が高く積極的である。特に豪州は同盟国としての責務・責任感が非常に強いため、ことさら米国と英国が参加する戦争にはほとんど加勢している。
様々な国際的な枠組みの中で、豪州は最も重要視しているのはFiveEyesとANZUSである。その次は防衛技術に基づくAUKUSである。QUADに関しては、同盟というよりは共通意識の表明という側面が強く、どちらかというと非伝統的な安全保障を重視してきている。
国内においては、厳格な法の整備と執行を行って、治安を維持している。安全保障、貿易、諜報には特に注意を払っている。そして、日本と比べて水不足に陥りやすいため、過度な使用は取り締まりの対象となる。また、外来種の持ち込み、児童ポルノも強く取り締まられている。

3.国家安全保障会議について
豪州における有事の際に国家安全保障会議が招集され、重要な決定がなされる。

4.軍について
国防軍は“Australian Defence Force”だが、英国系であるため、Defenceの綴りはcである。また、海軍、空軍ともに“Royal”が付く。
永住権があると入隊の対象とはなるが、国籍がないと正式に入隊できない。山口先生自身も入隊の一歩手前まで行ったことがある。

5.法執行機関について
法執行機関は日本とは大きく異なる。特に特徴的なものとして“Australian Federal Police”（「連邦警察」）が挙げられる。この組織は警察庁と警視庁と公安調査庁を足したようなものであり、ここから民間人に連絡が来ることは相当まずいことが起きた時だと考えられる。
また、“Australian Border Force”（国境警備隊）という国境警備、税関、入国管理等を前線で行っている組織もある。

6.情報・諜報について
豪州の諜報機関は省庁ごとに分かれている。入るためには厳しい審査があり、試験だけでなくバックグラウンドチェックもある。また、応募するときには口外してはならない。

【質疑応答】
Q1： 豪州は多様な国際関係を構築しており、日米豪、日豪印、QUAD、AUKUS、FiveEyesなど、さまざまあります。豪州はそれぞれ、安全保障上どのような戦略の下で各国との関係を構築しているのか、それぞれにどのような目的を持っているのか、ご教示願いたいです。
A1： 2000年代までは豪州は西側諸国の一員として、主に米国、英国と協力して戦おうと

いう考えであった。しかし、ここ 2～30 年で地理的（地政学的）な要素が以前より増してきたため、よりマクロに新たに日本、印度と協力する QUAD や ASEAN 諸国との協力のような構想が生まれた。

Q2： 中国はどういった思惑で南半球にある豪州に対して直接投資や内政干渉が懸念される事態を引き起こす政策をとっているのか、それが豪州の安全保障関係にどのような影響を及ぼしているのかを教えていただけますと幸いです。

A2： 経済安全保障に関してはわからないが、90 年代の半ばから中国と豪州は深い経済関係を持ち始めた。中国の豪州への干渉のベースは資源。資源、土地、不動産を狙っていて、投資先が豪州だと考えられる。様々な建物にはチャイナマネーが関わっている。豪州から資源を買うことと、経済的影響力をたかめることが狙いだ。他にも南太平洋、マクロ的に見ると、ソロモン諸島にも投資先として選択している。軍事的なものもからんでおり、港を押さえておきたい狙いがあるとみている。

内政干渉に関しては、中国に有利な政権になるような思惑がある。工作意識は強まってきており、また、オーストラリアには華僑も多い。90 年代ごろまでは香港系や東南アジアの華僑が殆どだったが、90 年代終わりごろから中国から人が入ってくるようになった。少数派ではあるが、今まで聞いたことない中国寄りの声も聞こえてきた。チャイナマネーの影響もある。

Q3： 豪州の周辺諸国（インドネシア、ニュージーランド等）はそれぞれその安全保障についてどのような位置付けなのでしょうか。豪州は近隣諸国と協調的な関係を築くことができるようなが安全保障上の利害が共通しているような状況なのでしょうか。

A3： ニュージーランドは同盟国であり、オーストラリアと似ている点が多く、敵対関係なるのはラグビーの時くらい。運命共同体と言える。

ニュージーランドは豪州に頼っていて、たとえば、ニュージーランドは空軍に戦闘機がない。仮想敵国との中間地点であるオーストラリアが守ってくれるだろう、そして、相手も豪州の上空を通過してニュージーランドを攻めてこないだろうという読みからニュージーランドに戦闘機はない。オーストラリアとニュージーランドの軍事協力体制は非常に強力である。

インドネシアは、00 年代まではある意味仮想敵国だった。直接的に攻めてくるとすればここだろうと思われていた。長らく独裁政権が続いており、過激派組織の存在もあり、人口も二億を超えているのでオーストラリアも警戒はしていた。インドネシアは近いし、人口も多い。人種的宗教的にも異なる、白豪主義的な側面からの考えも、イスラム教徒への不信感、インドネシアに対する嫌悪感は以前からあった。東ティモールの件で、オーストラリアとインドネシアの戦いがありえるという考えが浮上し、またオーストラリア人が被害となったバリでのテロ事件もあった。

最近では交流があるが、インドネシアとは未だに緊張関係が続いている面もある。

Q4： ローウィー研究所の調査結果において豪州国民が対内投資や 2020 年の貿易制裁などに強い懸念を抱いているという話がありましたが、これは安全保障上の観点からというものでしょうか。今後の環太平洋地域において豪州はどういった働きを期待されているのでしょうか。ご教示いただけますと幸いです。

A4： 経済安全保障の観点もあるが、環境的な問題もある。豪州の自然が破壊されてしまうという懸念と、豪州は非常に愛国心が強いため、いまだに外国に対する警戒感はある。

経済制裁はする側としてもされる側としても色々あるが、する側としては当然だという感性が強いが、された側は敵対行為と感じる。豪州の高い安全保障意識を反映しているのではないだろうか。

Q5： オーストラリア国内では台湾問題や米中対立に対する人々の意識は高いものがあるのでしょうか。

A5： ロシア、ウクライナに対して関心はあるが、オーストラリアの安全保障を脅かすほどとは考えていない。しかし、中国に対する関心は相当強い。位置的に離れていたとしても米中対立には関心があり、懸念している。また中国の高圧的な動きに関しては、オーストラリアにも関係してくるものである。ソロモン諸島が最近中国から影響を受けているという状況がある。ソロモン諸島はオーストラリアに近いため、中国の影響が強まると非常に厄介である。オーストラリアとして怖いのはオセアニアの国々が中国から影響を受けること。それは中国に周りを囲まれるということを意味するためである。台湾に関しては、もし中国が台湾進攻を行うのであれば、オーストラリアが参戦してもおかしくはない。そのため、オーストラリアとしては中国の高圧的な現状変更を抑止したいという考えが強い。国の名前で最もよく聞くのが中国。次に東南アジアのあたりで何か起きれば、という話もある。インドネシアに話は戻るが、いまでは昔ほど言われなくなったが昔はかなり脅威であった。軍もそこそこ強く、特殊部隊ランキングでいうと世界トップ５に入るくらい強いのではないかと感じている。特にゲリラ戦等、インドネシアによる脅威はそこそこ大きいものがある。

Q6： ご専門ではないかもしれませんが、山口様が考える経済安全保障の意義について、ご教示いただけますと幸いです。また、軍事的な先端技術の保全という観点では豪州は何か取り組まれているのでしょうか。

A6： 経済安全保障は非常に重要な問題である。国民の生活に直接影響する問題であり、特にサプライチェーンに問題があれば生きていくことはできない。日本は以前から経済安全保障について考えるべきであった。もっとも、経済安全保障を強化することで、それが逆に仇となり脆弱性が生じる部分も出てくる。サプライチェーンをどのように強化するのか、どのように脅威から守るかについて、真剣に考えていく必要がある。

豪州の取組について、先端技術の情報保全に関する体制が非常に厳しい。これは、従来豪州が諸外国の技術に頼っていることが要因として挙げられる。同様の情報保全体制を持つ国々と協力し、軍の近代化を図ろうとしている。その一つが Five Eyes や AUKUS である。日本はこういった厳しい情報保全体制が整っていないため、信頼度において依然として問題がある。

Q7： 今年７月に日米経済政策協議委員会（経済版「2＋2」）が開かれ、経済安全保障の議論が進展したと理解しております。日豪間では、日豪外務・防衛閣僚会合（2＋2）が存在し、将来的に経済版 2+2 が開かれる可能性もあると考えています。日米経済版 2+2 に対する国際的な評価及び日豪間で経済版 2+2 が開かれる可能性について、ご教示いただけますと幸いです。また、こうした路線は軍事技術面での豪州への我が国からの技術移転も想定されているものと考えられますが、我が国や豪州の技術面の安全保障協力の展望についてご教示いただければ幸いです。

A7： 前半部分に関しては、日米豪の三角形のフレーム、枠組みが必要になると思う。

日本からの技術移転に関しては、前々から様々な話が出ている。豪州は積極的に取り組んでいるが、時々ふらふらしていることがある。2016 年には、潜水艦を日本から受注しようという動きがあったが、結局フランスから受注することとなり、それも一方的に破棄して AUKUS に移った。

豪州の意思にも左右されるが、日本にも課題がまだ残っている。第一に、日本の製品は高価すぎる。第二に、防衛技術の輸出体制が整っていない。第三に、情報保全体制が甘すぎる。これら３つの問題を解決しないと、防衛技術の共同開発や輸出は難し

いと思う。

Q8： 豪州における海外との通信に関する安全保障面でのサイバーセキュリティについてですが、海外サイバー空間との国内サイバー空間との接続点（海底光ファイバーケーブルの陸揚げ局）にサイバー攻撃をモニターする仕組みもしくは検知・遮断する仕組みは存在するのでしょうか。もしそれが存在するとすれば、その運用管理は誰が行っているのでしょうか。また、このことについて更に詳しく調べるにはどのような文献を当たれば参考になるでしょうか。また、安全保障面ではその位置を明らかにしないことや物理的・軍事的な防御が必要と考えられますが、そうした点についての法令の担保はされておりますでしょうか。

A8： インターネットとかサイバー関係の専門家ではないが、サイバーについては国防省、内務省、情報諜報機関等が取り組んでいる。国土が広すぎるため光海底ケーブルを豪州国内でどのように繋ぐのか等、通信インフラの問題がある。豪州では要注意人物、または繋がりがあると判断された場合、通信内容が検閲されることがある。また、情報保全・漏洩に関する法律はかなり厳しい。省庁、警察、軍だけに限らず企業においても情報を一寸漏らしただけでも解雇される。機密情報が入っているUSBや文書をプロトコール外に扱った場合、または紛失した場合は解雇され、処罰を受けることもある。大学の近くに諜報機関の本部があったが何も書いておらず、公然の秘密だった。写真を撮っていた観光客が取り調べを受ける事例も起きていた。有事の際はいろんなスイッチがある。どの国でもそうだが、大規模なハッキングDOS等については通信省、もっと大きいものについては防衛省等が担当する可能性がある。質問の趣旨であるサイバー攻撃をモニターする仕組みもしくは検知・遮断する仕組みは存在するかについてはＹＥＳだが、内容については不明である。罰則も存在する。サイバーに限らず、国が安全保障上に係ると判断する事象に対しては厳しい措置が取られる。豪州の選挙は特徴的であり、投票は国民の義務であり投票棄権は罰金の対象となっている。

Q9： 豪州国内のサイバーセキュリティについて、安全保障の観点から戦時または関係緊張時に需要インフラ企業のシステム脆弱点を国が能動的に発見し改善指導するような仕組みは存在するのでしょうか。仮に、このような仕組みが存在する場合についてですが、改善指導に従わない場合の法令による罰則規定も存在するのでしょうか。

A9： 有事の際は色々なスイッチは入ると思うが状況にもよる。大規模なハッキングがあれば通信省、内務省や諜報機関、紛争につながる行為は国防省が対応する。企業が国の改善指導に従わない場合は、サイバーに関わらず罰則がある。国の安全保障に係る事項であれば、厳しいペナルティが予想される。

Q10： 豪州・英国・米国の間ではすでにファイブ・アイズの枠組みがあり、データの収集等の活動をしているのかと思います。さらにAUKUSにおいてもサイバー等の技術についても協力するとされています。安全保障の観点からは両者が重複するようにも見えますが、ファイブ・アイズだけでなくAUKUSも結んだことに何か理由があるのでしょうか。

A10： 米英豪でまとめればいいとではないかと感じるのも不思議ではない。しかし、安全保障の協定というのは特定の問題や目的意識に沿って決めていく物である。マクロ的な物については10年以上前からあるが、特定の細かい所まで決めた物についても必要性が出てくる。具体的にどのように共有・保全していくのかについての合意が別途必要であるということから、Five Eyesが出てきた。加盟国は若干異なっており、豪州、イギリスについては名前を連ねているが、AUKUSについては、潜水艦の購入が主な目的であったとも言える。日本も入るべきであるとの意見もあるがそれは

違う。枠組みについて色々なものが出てくるのは意外な事ではない。但し、将来的にはマクロ的な物については日本が含まれる可能性がある。QUAD や日米豪はここ 15 年ぐらいの関係である。また、在豪州日本国大使館の防衛に関する職員は 1 名程であったが、2015 年からは 3 名に増加している。安全保障協力関係が強くなったことが伺える。

（追加質問）

Q11： サプライチェーンに関して、日本は経済産業省が中心となりリスクの洗い出しやインテリジェンス・企業への情報収集を行っています。豪州では、サプライチェーン上のリスクや企業への安全保障関連の情報収集はどこの機関が担っているのでしょうか。

A11： 情報機関、財務省、内務省、資源科学産業省が中心となってしていると思われる。経済産業関係省庁が複雑に絡んでいる。

Q12： シンクタンクには影響力をもつものがありますが、実際には政策提言系、研究系のどちらが多いのでしょうか。

A12： シンクタンクの仕組みにおいて豪州は米国と似ており、ある程度信頼を寄せられているシンクタンクは政策に影響を与える。代表的なものには ASPI がある。しかし、米国ほど政策系のシンクタンクの数は多くない。

いくつかのシンクタンクでは元政府の人も働いている一方で、これから政府の一員となる人もいる。政策に深く関わる職務のため、基本的に豪州国籍を持っている人しか働けない。

Q13： コロナのタイミングで中国が豪州ワインを禁輸したが、困窮した産業にたいしての補助や安全意識の変化などはあったのでしょうか。

A13: 豪州政府は対応に窮していて、他の国に輸出できないかなどを検討していた。

Q14： 豪州のシンクタンクと政府機関との間で人材の流動性はあるのでしょうか。

A14： 流動性は高い。新卒採用の仕組み自体はあるが、人材が回っているところが多い。

Q15： Q14 に関連して、日本における人材の流動性の状況はいかがなものでしょうか。

A15： 他国に比べるとあまりない。

Q16： 産官学でのリボルビングドアを日本ではできないのでしょうか。

A16： 日本の組織は対応が固い。クロス、連携ができる組織に変わっていけばできるのではないかと思う。

豪州ではむしろ、様々な部署を経験して昇進していくケースが多い。これは安全保障の意識が大きいからこそ柔軟な体制であると思われる。

Q17： 豪州では、大学等の外部と交流人事を行う場合、政府部内でライン職、スタッフ職のいずれになることが多いのでしょうか。

A17： 両者ともある。特に区別されているわけでもない。

以上

記録作成担当者：宮内拓

ヒアリング調査報告 No.26 基本情報

日時	2022 年 10 月 6 日
テーマ	経済安全保障に係る経済産業省電池産業室の取り組みについて
ヒアリング先 (担当者)	経済産業省 商務情報政策局 電池産業室 加藤周 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 香高優一郎、宮内拓 (計 3 名)
調査目的	「蓄電池産業戦略」や経済産業省電池産業室が執り行っている施策とその課題、諸外国や企業の動向等を、今後の研究に活かすこと。

(写真)

【レクチャー】
「蓄電池産業戦略」を参照。

【質疑応答】
1.我が国の蓄電池産業について
Q1： 我が国の蓄電池の世界シェアが落ちている要因は何でしょうか。
A1： 製造設備の増強を諸外国と比べると大規模に進めることができず、コスト競争で遅れを取っていることが要因と考えている。

Q2： 蓄電池のリサイクル・リユースは現在どのくらい進んでいるのでしょうか。
A2： リユースは、実態把握が足元の課題である。
リサイクルについては、足元では使用済みの蓄電池の回収量が少ない状況であり、今後、事業的に成立させていくことが課題だと思う。

Q3： 蓄電池サプライチェーン(蓄電池産業戦略 p.7)において、特に日本が強みを持つもの、今後注力していくべき部品について、詳細にお話をお聞きしたいです。

A3： 電池の材料となる鉱物資源の部分は、日本に資源がないため、日本がシェアを大幅に上げていくことは難しい。
サプライチェーン全体として、コスト面での競争力を持たせていくことが一番重要で、製造設備の増強の支援をして行くことが特に重要だと考えている。

2.蓄電池の国際連携について
Q4： 各原材料(ニッケル・コバルト・リチウム・黒鉛)の人権リスク・環境リスク等について現在どのような状況が起こっているのでしょうか。
A4： 具体的な指標として、企業として人権面にどのように配慮するべきかを定めた「責任あるサプライチェーン等における人権尊重のためのガイドライン」があり、かなり重要視されている。事業者の中でどの程度、人権や環境に係るリスクへの対応状況について把握がなされていて、実際どれほど遵守されているのか、今年度試行事業で調査をする。調査結果を踏まえて今後の対応を考えていく予定だ。

Q5： 電池の原材料の製錬工程の代替先となりえる日本の有志国として挙げられるのはどのような国なのでしょうか。
A5： 原料が埋蔵している国はかなり偏りがあり、政府として、ファイナンスの面での支援により、供給源の多角化を進め、供給途絶リスクを低減・分散させることが重要である。
JOGMEC が重要な役割を果たしており、出資割合を高めることで事業者のリスクを低減させるなど、資源開発プロジェクトへの民間企業の投資を促進するための措置を行っている。

Q6： 蓄電池の安全性、機能性に関する国際的な指標の確立に関して、どの程度日本は影響力を持っているのでしょうか。また、国際的な影響力を高めるために貴省が特に行っている取り組みはあるのでしょうか。
A6： 日本の強みは技術面で、特に安全性の高さだと思う。BAJ が安全基準を考案して IEC に具体的に提案をし、国際的に議論を進めているので、日本は影響力が結構あるのではないかと思う。
政府としても、特にリユースの分野は国際基準を定めるべく、リユースの細かい部分について IEC に提案をしていて、来年以降発効させて、実行に移していく予定だ。

（追加質問）
Q7： 日本でも経済産業省が 9 月に「責任あるサプライチェーン等における人権尊重のためのガイドライン」を作成しておりましたが、蓄電池産業戦略と関係ありますか。
A7： 関係は全体論としてはある。また、蓄電池のデュー・ディリジェンス試行事業は欧州バッテリー規則を念頭に置いて進めているもので、上記ガイドラインと方向性は同じだ。

Q8： NEDO への資金投入の現状と、今の取組み、経産省として、NEDO にはどの様な課題があると考えているか。また、官民協議会等を通じた技術開発への期待はどれほどでしょうか。
A8： NEDO は経済産業省と違い、研究分野の方も在籍しており、ただ単純にお金を配るということだけではなく、実際に技術開発でどのような支援が必要か、どのようなことを一緒にすべきか、技術的なサポートの取組をやっている。官民協議会を通じた技術開発においては全固体電池などの次世代電池の分野に期待している。

Q9：　経済安全保障推進法により、蓄電池が特定重要物資に指定された場合、今後資金提供のスキームが変わるのでしょうか。

A9：　現時点で、資金提供機関を新設しようという話もないので、補助金の執行のスキームが大きく変わることは想定していない。

以上

記録作成担当者：香高優一郎

ヒアリング調査報告 No.27 基本情報

Date	6, October 2022
Topic	Economic security in Australia
Interviewee (Person in Charge)	Australian Embassy in Japan Ms. Jessica ROBINSON, First Secretary (Economics) Ms. Ichiko FUYUNO, Senior Research Officer (Economics)
Location	Online
Participants	(WS-C Professor) TSUBOHARA Kazuhiro (WS-C Students) INADA Rinka, OKAMOTO Itsuki, KAJIYAMA Kei, KOTAKA Yuichiro, YAMADA Mayu (6 people in total)
Purpose of the Interview	To talk about the survey in Australia and to understand economic security policy in Australia.

Q and A Session

We talked about the following issues:

1. National Security of Australian Government.
2. International Relations of Australia, especially, Japan-Australia relations.

Q1: In order to ensure the protection of critical infrastructure and other assets, it is necessary to focus on human resource development in the field of cyber security. We would be grateful if you could tell us about the measures and prospects for cybersecurity human resources development in your country.

A1: In Australia, the Security strategy is shared among several agencies, so there are the operational agencies that look after government and critical infrastructure systems protection. Moreover, we have policy responsibility for cyber security shared amongst our foreign affairs department.

Q2: Your country is promoting international cooperation on security in various frameworks, including AUKUS and our own. We would be grateful if you could explain the environment and concerns surrounding economic security in your country.

A2: This is also very broad. Some areas are responsible for AUKUS. Foreign policy is a central government role.

Q3: Your country and ours have a close relationship about supply chain cooperation, for example, at the Australia-Japan Summit. We would be grateful if you could tell us what kind of cooperation and collaboration your country is seeking from our country.

A3: QUAD is a significant architecture for collaboration with Japan, the US and India, things like supply chain resilience. Such groupings like the Quad are essential because they bring together like-minded countries that can bring technology development, supply chain development, and purchasing power. Thus, Australia and Japan collaborate closely on supply chains. Moreover, the same happened with infrastructure development in the Pacific.

Australia and Japan successfully work closely together to bring other countries into cooperation because we have excellent relationships with other like-minded countries.

Reporting officer: Kotaka Yuichiro

ヒアリング調査報告 No.28 基本情報

日時	2022 年 10 月 11 日
テーマ	研究インテグリティについて
ヒアリング先 (担当者)	東北大学副理事（研究公正担当）、金属材料研究所副所長 佐々木孝彦 様
場所	東北大学 片平キャンパス エクステンション教育研究棟 201A 講義室
参加者	（WS-C 教授）坪原教授 （WS-C 学生）稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 （計 9 名）
調査目的	経済安全保障と研究活動との関係性について調査すること。

(写真)

【レクチャー】

1. 共同研究への風潮について

東北大学は留学生への門戸開放を初めて行った大学である。そして留学生に対して博士号を授与したのも日本で初めてである。魯迅をはじめ中国から多くの留学生をこれまで受け入れている。中国との関係があったことから、江沢民が来日した際に唯一訪問した大学が東北大学だった。海外との交流については波があり、特に東アジアの国々と日本の関係はアップダウンが激しい。アカデミアとしての学術交流や研究倫理をベースとしたものが行われている。

研究活動の基礎科学から応用、社会実装に至るイノベーションの部分で透明性や説明責任を果たすという部分について一般社会や政府から求められている。サイエンスとエンジニアリング、テクノロジーは違う物である。そして、サイエンスでの交流と技術（テクノロジー）移転については，両者を適切に区分して行う必要がある。実の所、日本の研究不正の 3 分の 2 は文系から出ており、社会科学系が最も多い。

研究費の制度について利益相反、安全保障が注目されるようになり、最近の研究インテグリティという言葉で表される研究活動の透明性の確保という物が求められるようになった。政治経済といった安全保障環境の変化によって、大学からの技術流出について懸念す

るという声が多くなった。
　中国の大学にラボを開くということについて、以前までであればポジティブに捉えられていた。しかし、最近は新聞においても頭脳流出などの言葉が使われるなど、あまりいいイメージが持たれなくなった。人の循環によって頭脳循環が行われることは学術の発展には悪いことではない。人が循環するということは学術研究をする上で決してネガティブに捉えられることではなく、むしろサイエンスを発展させるためには必要な事である。国際化、オープンサイエンスとして外国人教員や留学生を増やすということはこれまでも求められており、今でも求められている。しかし、一部世論との整合性の取れない風潮となってしまっている。

2.中国やアメリカの状況について
　中国では千人計画という中国人研究者を中国に呼び戻すというプログラムが行われていた。元々は、中国から海外に渡った中国人研究者を呼び戻すというプログラムだった。著名な外国人もその中に含むとしたのは比較的最近の事である。
　アメリカがどのような状況は、トランプ政権下であり米中の緊張感が高まっていた。米国から中国への技術流出という懸念があった。そして象徴的な事件として、ハーバード大学の化学・化学生物学科長のチャールズ・リーバー教授の問題が起きた。リーバー教授はノーベル賞の前段とも言われるウルフ賞を受賞する著名な教授である。ハーバードの出前ラボを中国に作っていた。このこと自体は問題ではなく、大学としてもプレスリリースを出すなど宣伝も行われていた。問題となったのはリーバー教授の個人給料について大学や政府に申告をしていなかった事である。そのことから、虚偽、詐欺のために逮捕・起訴されるに至った。技術流出の罪に問われたことが問題だったのではなく、詐欺の部分にかんして逮捕されたということがポイントである。しかしながら、非常に影響力のある人が逮捕されたことから、同様に虚偽申告漏れによって起訴される研究者が存在した。起訴はされるが、ほぼ全て起訴猶予や無罪判決となっている。米国の科学界に対する起訴については方向性が変わってきている。

3.国際的な環境について
　いわゆる先進西側諸国では研究の透明性を確保していこうという国際合意がある。G7 サミットの会議と合わせて科学技術会議等色々な会議が行われている。G7 コーンウォール・サミットにおいてリサーチコンパクトという研究に関しての合意文書が採択された。これは、研究の透明性とインテグリティの向上ということを各国政府の間で取り決めて行きましょうという国際合意となっている。この時には、ロシアによるウクライナ侵攻については全く想定されていなかった。しかし、国際的な学術交流やオープンサイエンス、グローバル化については進めていく。そのことから、経済安全保障の考えを入れることによって、研究活動の透明性を確保するという合意が関係国間でなされている。今年の G7 の科学技術大臣会合はドイツのフランクフルトで行われたが、研究インテグリティと研究セキュリティについての文章が出ている。日本の中では研究セキュリティについては研究インテグリティに含むものとしてあまり明確には示されていない。日本の中で言っている研究インテグリティというのは日本で作られた造語であり、もともとの Research Integrity の意味が拡張されて定義されている。各国間での言葉の定義が異なるので，それぞれの相違を明確にする必要がある。
　2023 年 5 月に G7 科学技術大臣会合が仙台で開催される。間違いなく、ロシア情勢も含め、研究インテグリティ、研究セキュリティについてよりセキュリティ側によった話が出てくる。国際合意の中で、日本学術会議や国立大学協会、科学技術振興機構(以下、JST)、ファンディングエージェンシー（以下、FA）についても研究インテグリティについての文章を出している。日本としても研究インテグリティや安全保障、経済安全保障の観点を科学技術政策の中に入れていこうとしている。

4.日本の科学技術政策について

科学技術政策は6年ごとに改定されている。最初に出てくる現状認識として国内外における情勢の変化が入っている。いわゆる科学技術イノベーションの中でも覇権争いが顕在化している。もちろん大学研究機関の研究力をアップするということが1番である。基本計画の中ではレジリエントで安全・安心な社会の構築という形で出てくるが、中身としては安全保障貿易管理や研究セキュリティをより高めていくことによって研究を健全に行っていくということで、健全性が求められている。

この第6期基本計画について、政府としての取り組み強化のポイントとして、アカデミアや民間企業で留学生及び外国人研究者に対する入国審査に関する出入国管理・ビザ発給の審査強化をするということがある。これは法務省，出入国在留管理庁が所管している。そして、政府資金申請時の外国資金受入状況等の情報開示について研究インテグリティとして表記している。この部分については文部科学省と内閣府の所管となっている。大学研究機関に対して、研究データの情報に関するアクセス管理をどうするのかという所が出てきていない。安全保障輸出管理の中では、みなし輸出管理の明確化について経済産業省の中で外為法の改正という形で行われた。

そして、大学にいる研究者に対して求めることとして出された物がある。それは研究費に関して、しっかり管理していくことだ。基本的には研究者個人の研究活動の透明性について、経歴や研究内容を大学に適切な手続きにより開示することを求めている。

そして、開示された情報については大学・研究機関がマネジメントしていくことを求めている。それらの情報を研究者から受けることによって、過度な投資や、同じ研究テーマで研究資金を貰っていないか、違う機関から同じテーマで資金を貰っていないかといったことをFAはしっかり見ていくということが求められている。これについては、過度な研究費の集中を排除するという通知の中に少し出てくる。過度な研究費の集中を排除することによって、偉い先生の所に集中せず、若い研究者にも研究費が回るようにしていく。

5.経済安全保障の重要技術育成プログラムについて

経済安全保障の重要技術育成プログラムというものが、令和3年の補正予算から始まった。基本的には政府からJST経由と国立研究開発法人新エネルギー・産業技術総合開発機構(以下、NEDO)経由で資金が出される。大学についてはJST、民間企業はNEDOからというプログラムが計画されている。予算規模が非常に大きく、JSTとNEDOで1,250億円ずつ、合わせて2,500億円である。日本の科研費は年間約2000億円である。参考として、東北大学の年間運営費は約1500億円である。

この費用については、宇宙、量子、AI、スパコン・半導体、原子力、先端材料、バイオ、海洋等といった経済安全保障の重要であると思われる技術に、集中的に投下していく。こうしたことは今までも色々な所であったが、いくつか特徴がある。一つは技術流出防止対策をするということが書いてある。機微技術といった部分については、その研究にタッチ出来る人については資格が設定されるかもしれない。そして、もう一つのプログラムの特徴として、民生用のみならず、関係府省において公的利用に繋げていくことを試行するという一文が入っている。これまでの研究資金配分の中ではこれまで出てこなかった一文である。大学・研究機関に対して防衛装備庁に係る補助金については議論が色々ある。この議論については、いいところ悪いところの両面あるが、政府主張においての公的利用に繋げて行くというのは、デュアルユースに対しての意図が入っており、経済安全保障という国の施策として行っていくという中にそういった側面があるのではないかと思っている。このプログラムを受ける際には技術流出防止対策することが求められている。これに関係してくるのが、研究インテグリティである。

6.研究インテグリティについて

令和3年4月に文部科学省から大学研究機関向けに研究インテグリティを確保することという通知がなされた。研究インテグリティの定義について、新たなリスクに対して、技術流出が起こらないようにして欲しいということになっている。新たなリスクというのが何であるかということも不明確ではあるが、端的に言えば意図しない技術流出が起こらないようにするということが含まれる。そのために、研究者は職歴や研究経歴、兼業、外部からの支援状況について大学に対して開示をすることということが求められている。通常であればこれまでも研究者、大学に雇用される人については、研究をするのであれば研究用の手続きをし、職歴・研究テーマといった、いわゆる履歴書で嘘は書かないということになっている。また、他から資金を貰っているのであれば、相手方について情報を開示して、民間との間であれば共同研究手続きを取ってもらうということをしていく。当たり前の事ではあるが、改めて大学研究機関はしっかりとマネジメントしていくということが求められている。これまでの、研究不正、利益相反、安全保障貿易管理が土台にあり、基本的には一つの技術流出防止対策と言われている。さらに、大学の中ではそれに対するマネジメント体制を作り、相談窓口を作るといった組織整備をしていくことが求められた。どういった所にFAが出ているのかというと、科研費がある。科研費の公募要領の中に研究インテグリティについて入っており、研究計画書の中に研究費の応募受入予定の状況を記載することが求められている。JSTが出している募集要項の中でも研究インテグリティの確保の部分で研究資金について情報を出すことが求められている。

7.研究インテグリティという言葉について

論文など色々な所でリサーチインテグリティやリサーチセキュリティ、研究インテグリティという言葉が使われている。これらの言葉を使う時には注意する必要がある。漢字で表記する研究インテグリティという日本語は内閣府と文部科学省で作られた。しかし、漢字で書いている研究インテグリティというのはリサーチセキュリティの意味を含んでいる。国際的に使われているリサーチインテグリティというのは、いわゆる研究不正や論文不正、公的研究費不正というコンテンツのことを指している。各国にはリサーチインテグリティに関係する省庁がある。イギリスの場合はUK Research Integrity Office(UKRIO)、アメリカだと、Office of Research Integrity(ORI)という米国研究公正局がある。いずれについても、いわゆる安全保障ということではなく、研究不正防止に関係する役所である。

一方で、日本のリサーチインテグリティについては研究インテグリティと訳すことによって定義が変わってしまっている。これについては、文部科学省が出しているものであり、国際化・オープン化に伴う新たなリスクに対して、研究活動を行う時に、必要な情報について、適切な報告・申告を行うということに定義が変わってしまっている。同じようなものとして日本学術会議から出ている研究インテグリティの定義がある。その中には、研究活動について自主的、自律的な健全性、透明性、説明責任に関するマネジメントについてといったことが含まれている。本来のリサーチインテグリティはいわゆる研究の健全性の話である。日本で漢字を使った場合の研究インテグリティについては国際連携の中では研究活動の健全性、透明性という意味に変わってしまう。このように意味が変わってきてしまうのは、漢字文化が影響してしまっている。

研究倫理について英語ではResearch Ethicsと表されるが、日本は研究倫理と研究公正が混ざってしまった状態になっている。英語でのResearch EthicsとResearch Integrityは別の意味を持っている。日本学術振興会の研究インテグリティについてどのように表記されているかというと、eL Coreという研究者や大学院生向けのeラーニングコースに表記されている。そこではe-Learning Course on Research EthicsとしてResearch Ethicsという言葉が使われている。しかし、ホームページ上ではリサーチインテグリティと表記されており、混ざってしまっている。国際的にはリサーチインテグリティ（Research Integrity）が研究公正を指している。日本の中で、Research Ethicsというのが何を指

しているのかというと人を対象とした生命科学や医学研究に置ける倫理指針といった物について指している。しかし、国際的にはリサーチインテグリティは規範や価値観のことであり、リサーチセキュリティについては規制や基礎に係る部分であるとして概念が分かれている。G7 での議論においても定義されている。

8. 東北大学としての対応

東北大学では 2010 年前後から、公正な研究活動、研究活動不正、安全保障輸出管理、利益相反マネジメントといった活動がスタートしている。文部科学省から研究インテグリティに関する通知が出されたのは去年の 4 月であるが、東北大学内部としては米国の状況や報告書を元として対応を検討していた。文部科学省から通知は出されてはいたが、大学研究機関での運用方法については定まってはいなかった。そのため、研究インテグリティを確保するための方法を受託研究として公募した。東北大学で 2021 年に「研究インテグリティの確保に係る調査分析業務」を業務受託した。この中で、報告書を作成し大学研究機関でセキュリティを確保していくためのモデルシステム、モデル体制というものを示した。それと合わせて、大学の中での研究インテグリティ、マネジメント体制を今年の 4 月から開始している。

東北大学では研究インテグリティについて研究者に対して求める規範型で進めており、ファンクションとして安全保障輸出管理や利益相反、人事、共同研究契約について既存の事務のフローで行うという方法にしている。大学によって方法は異なっている。例として東海国立大学機構を構成する名古屋大学は安全保障輸出管理がメインとして始まっており、規範は後からという建付けとなっている。各大学法人に任せられている部分であり、どちらがいいという問題ではない。

大学の中ではコンプライアンスに関係する部署が色々な所に分かれている。例えば、研究推進部の中に研究公正や人を対象とする医学系研究を担当している。一方で、安全保障輸出管理はハラスメント等を担当している法務・コンプライアンス課が所掌している。そして、産学連携、企業との共同研究、地域間連携については産学連携部が担当している。留学生については教務・学生支援部の留学生課が担当しており、様々な組織に分かれていることから、色々な部署が情報を共有している。ヘッドクオーターとしてマネジメント委員会があり、公正な研究活動の推進委員会が存在している。基本的に大学で行う共同研究については機関承認が必要となる。機関承認をしないということはあまりないが、公式に要請をすることが出来るという仕組みを作った。さらに相談窓口を作り、相談をしてもらう体制を整えた。

9. どのような相談があったのかについて

2022 年 4 月からどのような相談があったかを紹介する。優秀な若手研究者に対して、ある国からの共同研究者から連絡がきたというものだ。共同研究のプロジェクトに応募をしてみないかというものであり、内容としては以下のようなものだった。

「共同研究プログラムの応募について、プログラムに関するお金は研究者のサラリーとすることができる。基本的には COVID の関係もあることから、こちらの国に来ることなく、オンラインの共同研究で大丈夫である。このプロジェクトは 2 年間の物であり、申込の締め切りは 2 週間先となっているため期限が迫っている。申請書はこちらの国の言葉で書く必要があり、代わりにこちらで作成をしておく。もし、興味があれば応募をして欲しい。そして、こちらの大学の所属の承認は必要であるが、東北大学側の承認については必要ない。」

この内容について東北大学側の承認なしに出来るという所について懸念があるということから、最終的には断ることになった。

個々の先生にアプローチがあるということについて知ることが出来たのは、研究インテグリティに関する FD 等を行っており、不安なことについては相談窓口に相談をするとい

うことを伝えていたことから、その先生が相談をしたからである。そして、1 件あるということは、他にも沢山あるのではないかと思っている。
現実問題として、違法性があるかというとそういうことは全くない。グレーな部分であり、インテグリティの範疇である。安全保障や利益相反の良し悪しについては基準を決めることが出来ない。そのため、先生方に規範を求めるという状況がある。

10. 研究セキュリティについて
東京 JST で北欧 4 か国のノルウェー、スウェーデン、デンマーク、フィンランドの間で FA 同士のリサーチインターアナリゼーションという国際化についてのワークショップが開催された。日本側から 10 人、向こう側から 10 人の計 20 人ぐらいで 5 人ずつのグループに分かれて 2 日間ディスカッションをするということが行われた。そこで、グレーゾーンマネジメントという日本の研究現場での研究セキュリティがどのようになっているのかについて話した。
中国の国防科学技術大学でマスターを取った人が、中国政府の留学支援制度を使い、国防科学技術大学の出身ではあるが、民間人として東北大学の研究室にドクターの過程で入った。その研究室では地中の中の埋蔵物を探すようなレーダーの研究をしていた。そして、この人物が国防科学技術大学に戻り、レーダーの妨害をどのように行うのかといった内容の論文を書いた。民生技術だったものをミリタリーユースという使い方をしていた。そして、これについてはデータを持ってきたというわけではなく、そこで教育を受けて頭に入っていたものであるということになる。しかし、ミリタリーユースと民生ユースについて、大学としては民間人としてうけいれていた。
政策と現場の乖離についてという部分であるが国防科学技術大学が当時は安全保障輸出管理のユーザーリストに入っていなかった。この事案が起きた後にすぐにユーザーリストに加えられた。
民生ユース、ミリタリーユースといったかなりグレーに近い部分については、意図した技術流出というよりは、技術移転を狙った入学というものがあるということを実感した。
こうした規制についてはその時の風向きに影響を受ける。インドのモディ首相が来日し日印協力等を結んだ。これまで、インドは核兵器保有国であり、インドの研究機関が核関連施設として安全保障輸出管理のユーザーリストに入っていた。しかし、日・インド原子力協定が結ばれると、ほとんどのインドの原子力機関がユーザーリストから外された。その時の政治状況や風向きによって規制については変わっていく。学術については原理原則を重視する研究者は、基本的には原理原則に基づいた行動をする。そのことから、そうした原則と現実のすり合わせが大学でセキュリティを実施するというオペ―レーションをするときの観点で一番重要な観点である。経済産業省や文部科学省、内閣府に対しては大学という現場はこうなっているという実情を知ってもらった制度設計としてもらうことが重要である。

【質疑応答】
Q1： 研究室内で「経済安全保障」という言葉が話題になることはありますか。
A1： 私の研究室ではない。研究領域によると思う。金属材料研究所は、理学と工学の研究者の合体の組織で、私はどちらかといえばかなり理学側なので、私の研究室自身では経済安全保障に関した話題が出ることはない。ただ、金属材料研究所のなかでも、金属 3D プリンターといった技術や、電池関係の研究室は経済安全保障という言葉を知っていると思う。実際、3D プリンターを扱う研究室は、外為法安全保障輸出管理の中の機微技術であり、中国から留学生がたくさん訪問していたということもあり、そこに関する感度は高いところがある。大学の中では、青葉山の半導体技術を扱う研究室が、一番これに近いに研究室（経済安全保障と言う言葉が話題になる研究室）だと思う。

Q2： 研究資金の獲得が大変とお聞きします。諸外国と比べ、我が国で研究する研究者のメリット・デメリットはなんでしょうか。

A2： 特に国立大学では、大学の法人化以降、いわゆる運営費の減少、教員自身の削減が進まざるを得なかった。現在でも実は、運営費と教員数を毎年1.6%削減するよう求められている。例えば、金属材料研究所の教員の数は大体150名だったが、一年間に1.6%減らすということは、一年間に大体教員を3、4名減らすということだ。それが10年以上続いている。1年に4人減らすということは1年に1つの研究室を潰すということだ。金研に約25～27の研究室があったが、今、実質稼働できるのは20研究室しかない。

日本の科学政策の中でのお金の入り方は、大量にお金が入っている中国や欧米含め、一国だけ蚊帳の外感がある。それが一番端的なのが若手の方の研究ポストが少なくなっていることだ。いい意味ではなく、海外、中国にポストを求めている若手研究者が増えているというよりは、増えざるを得ないという現実がある。最近、新聞で円安の問題があると認識されていると思う。日本の給料だけ、他の国々よりも上がってないと思うが、これは大学の教員の人の給料も同じであり、一昔前までは中国より日本の教授の方が、給料は良かったが、今はほぼ同じか下手すると逆転している。

先ほど紹介したチャールズ・リーバー氏は保釈金を現金で払ったが、その額は100万ドルだった。日本円で言えば、1億3000万円ほどをキャッシュでその場で払っている。中国の先生も、教授であれば円換算すれば同じかそれ以上もらっている。日本の研究者が日本で研究するメリット・デメリットはあるが、海外に比べてそういう環境やモチベーションの点ですごく厳しいところが感覚的に感じる。私の同期ぐらいの人で民間企業に行った修士号取得の技術者は私達の1.5倍ぐらいは普通にもらっている。民間企業のいわゆる大企業の研究職の方々はそれほどの給与水準で働いている。

研究資金という意味だと、日本の場合は非常に短期の申請が多い。例えば、科研費は基本的に全ての研究者の方に研究資金を入れる。いろいろなプロジェクトがあるが、大体3年の補助期間だ。3年やったら、また次に応募して、ということの繰り返しで、申請を書いて、報告書を書くという自転車操業だ。海外でわたしの知る限りだと、10年だ。もちろん一回ごとの申請、報告書は大変だが、自転車操業と、安定した研究環境の中での状況というのはかなり違う。

Q3： 研究内容の流出を防ぐため、研究室内で行っていることはありますでしょうか。

A3： 流出はなかなか難しい定義である。サイエンスの分野では、基本的には研究を公開するのが原則である。従って、論文にするという観点からも、サイエンスの分野で流出という概念は現状としてはないと思う。私も海外の研究者と共同研究をするが、その際は基本的には研究内容をフェアに共有している。これらの内容が外に出るかというと、研究のプライオリティがあり、契約ベースではないが、グループの外には基本的には出さない。一方、テクノロジーやエンジニアリングのところでは、特に研究内容が知財に絡む分野のときは、学生がどのように研究に関与するかについて少し違いがある。職員の場合は、大学の就業規則があり、悪いことをしてはいけないことが就業規則により定められる。学生の場合は大学と雇用関係がないので、知財が絡む研究をするときに学生がどう関与するのかということを、あらかじめ決めてから行うことが多い。特に工学部だと、通常の修論の発表会は公開だが、該当者のセッションのみ非公開という修論の発表会がある。これに入るときには、ここで聞いたことは外に漏らさないという誓約にサインをしてからということが工学系では時々ある。

また、博士論文や修士論文も、知財に関係する流出を抑えるということで、3年までは博士論文を公開しなくてもよかった。概要だけは出すが、本文については決められた年限（最長3年）まで、博士論文を公開しない選択は現在も可能であり、このよ

うな選択をする研究室はあるが、個人個人の学生による。
　また、学生が卒業した際や民間企業に進んだ際に、ある会社と共同研究をしていた内容に守秘義務が発生するかについては、非常に難しい問題が関係する。というのは、学生は大学に雇用されていないため、守秘義務が発生しない。教員であれば守秘義務が存在するが、学生は雇用関係がないためそこの部分が曖昧になっている。従って、仮に学生の研究テーマが機微なものになった際には、その学生との間で個別の契約書を取り交わす。ただそれがどこまで有効かというのはかなり怪しく、法的には様々議論があると思う。

Q4：　経済安全保障施策の主体は国家だけではなく企業や大学も含まれますが、研究内容や情報流出の防御などで、大学や研究室が政府機関等に相談できる体制は現状あるのでしょうか。
A4：　形式上はあることになっている。HP には所掌している室や課があることになっているが、ほぼないと思っていい。経済安全保障を担当するのは、JST と NEDO である。NEDO は経産省所管で、JST は文科省が所管しており、担当室の参事官と課長補佐が担当をしている。しかし、基本的に課長補佐と２人程度で会議をするに留まるため、体制は整っていないと思う。まして、システマティックに技術流出に対応できる水準までにはいっていない。実際の研究現場や大学でどうしたらいいかというのは、これから話をするというのが実情である。

Q5：　共同研究を行う際に特に気を付けていること等はあるのでしょうか。
A5：　共同研究については大学間では難しいが、企業と共同研究を行う場合には共同研究契約書がある。研究者同士の共同研究については共同研究契約を結ぶことはない。海外との共同研究をしている割合は 98%以上であり、研究者間の信頼関係で行っている。相手がどういう人間であるかについては、信頼関係に頼ってしまっている。例えば、海外の国際会議の際に討議をする中で、テーマについて一緒にやらないかという話になる。そういった感覚で共同研究は行われている。サイエンスや工学、エンジニアリングについても同じことが言える。世界的に見ても研究者同士の共同研究の始め方は共通である。一方で企業とのやりとりの場合は、研究費が入っていないようなものについても成果の取り扱いをどうするかという書類を作成する。基本的には研究者と企業ではなく、東北大学と企業として契約を結んでいる。研究者の先生はその間に入っている。海外の企業とは年に 10 件あるかないかである。契約の内容として秘密保持契約がある。研究の内容について合意があったら発表をしようというものである。また、研究者同士ではないが、会社が入った場合の秘密保持契約もあり、これは研究者個人で結ぶことができ、東北大学に届ける必要がない。秘密保持を個人で結べるというのは東北大学の特徴である。他の大学は個人で結べず、法人間で結ぶことになっている場合が多い。同じ国立大学だったとしても制度設計が違う。色々な制約があり、実際の研究の現場でどういう活動が行われているのかということが分からないと、秘密保持契約と行った制度等があったとしても実効性がないということになりがちである。制度があったとしても機能しないということがある。

Q6：　あの金属材料研究所ですら、減らせと言う状況とは初耳でした。かなりの実績をあげられていますが、なぜ減らすという現状が起きているのでしょうか。
A6：　大学法人化でも元々あったが、根底には国家公務員数削減というのが根底にある。今でも国立大学法人のいわゆる「座布団上がり」、承継枠という、私たちのような昔からの退職手当がつくようないわゆる公務員型の教員数には公務員数削減の大前提がある。所長も含めみんな削減対象となった。今は年間の定員数として毎年 1.6%の削減となっている。実は金属材料研究所を含め他の研究所は昨年まで 3.2%の削減を求めら

れた。なぜそうなったかというと、世の中的には基本的に大学は高等教育機関で、研究機関ではない。金研や他の研究所は研究科ではないので学生がいない。教員区分の教員はいないという名目で実は研究所分は3.2%、研究科は1.6%の削減が求められた。それはおかしいとして、総長にねじ込んで、なんとか研究所も研究科も同じ削減割合にした。

文科省としてはそういう公務員型の教員を減らして、プロジェクト型の教員を増やそうとしている。なので、一定額、大学に毎年同じ分だけ振り込むということはやっている。ただ、総額ベースにするとほとんど変わらないくらいの増額で、毎年増えているのは競争的研究費があるが、大学に対していろいろなプロジェクトや概算要求事項に応募させて、5〜10年というプロジェクトの中で教員の雇用経費も賄わせようとしている。しかし、そこで雇用される先生はどうしても将来に関しての財政的な担保が取れない。5〜10年任期をつけた特任という形での雇用が今増えている。もちろんそれでも、ちゃんとそういう人材が各大学を回ればいいが、5〜10年で任期が切れ、次のプロジェクトが立つか立たないかわからないという状況だと、なかなか継続的な研究ができない、プロジェクトの継続性がない、ということが起こる。これが今の日本の科学技術が一番うまく回っていない現状だ。当初の目論見では海外への循環を含め、そのような制度設計をすれば、ちゃんと研究者が働くだろうというのがあったが、正ではなく負のスパイラルに陥っている。そこが日本の科学技術が一人負けをしている元凶だ。しかし、政府は決して大学法人化が失敗したとは口が裂けても言えない。大学の人間は皆、日本の科学技術が復活するためにはそこを検証すべきと言っている。

Q7： 国立法人化することで、基金を用意し、大学自身がマネジメントする大学ファンドは機能しますでしょうか。

A7： まだ走り始めたのでなんとも言えないが、大学ファンドという制度が今年度中には選考のプロセスが始まり、東北大も入ろうと努力している。ただ、学術、科学技術は選択と集中が合わない。なぜ中国があれだけ上に行ったかというと、お金を投資している裾野が広い。中国は人とお金の底辺をすごく広げている。研究を正三角形に例えると、上を上げるには、その底辺を広げないといけない。それが日本はうまく行かなかった。底辺は萎めて、トップを上げるという二等辺三角形を目指したが、科学技術の世界だと、底辺を広げなければ、伸びなかった。そのような仕組みじゃないと多分うまくいかない。

大学ファンドも、国立大学数校に重点的に支援しても、それだけでは国として科学技術力は上がらない。何を目標にしていいかわからないが、いわゆる欧米型の仕組みをとる国々も、本当に底辺となる大学の数が多い。日本は負けているのは留学生が魅力を感じないので、増やそうと思ってもなかなか数が増えず、トップの人も来ない。

大学ファンドで数校に集中的に、というのは予算の面もあるだろうが、うまく行かないだろう。その理由は、お金より人だと思う。科学技術はお金がいくらあっても人なのだ。それ以外ではお金の投資が必要だ。また、人の循環が絶対に必要だ。日本の学生が、日本だけでなく、海外からの留学生と交流したり、日本の外の方にも行って帰ったりして、そのような循環でしか再生はできないと思う。

東北大の運営費は約1500億円だが、大学ファンドによる交付で1000億くらい追加されるだろう。

1億で賄える研究者は7〜8人だ。100人の研究所を作ろうと思ったら、人件費だけで20〜30億円かかる。運営費を含めたら100億かかる。しかし100人の研究所はそこまで大きくない。金属材料研究所は130人ほどだが、大きな研究所かというとそうでもない。根本から国の研究へのお金のかけ方はもっと考えなければならない。

Q8：　大学から見て文部科学省というのはどのような存在なのでしょうか。
A8：　文部科学省は大学を所管してはいるが、一番のボリュームゾーンは初等・中等・高等教育までが一番大きい。大学は教育機関であり研究機関ではないことから、教育機能が重視されていると感じる。

Q9：　沖縄科学技術大学院大学(OIST)や北陸先端科学技術大学院大学(JAIST)といった資金提供は他大学と異なっているのでしょうか。
A9：　OIST は内閣府が主導した大学院大学であり、一般の大学院大学と比較することは難しい。研究主導でありパイロット的な要素もある。また、沖縄振興という部分も入っていることから、教員の選考方法についても違っている。さらに教授会がなく、トップダウンで物事が決まっている。OIST の総長については世界公募で決めており、在任期間はかなり短く、すぐに違うところへと移っていく。大学の成果の出し方としていい正のスパイラルとなっている。しかし他の場所で同じようにやろうとするのは難しい。ミッションや創設者がそうした形で作らないと国立大学では難しい。そもそも、日本の入学制度がよくない。偏差値が基準となっているという所がうまく行かなくなっている。例えばドイツの場合は中小都市にも大学があり数も多いが、粒が揃っている。そしてヨーロッパの人は地元志向が強いことから、ドイツからフランスの大学に行くということはそこまで多くなく、地元の大学に行く人が多い。そして、地元の優秀な人が集まり、最後には地元に帰る先生が多い。いわゆる愛校心というものが欧米にはあり、これが寄付へとも繋がっていると考えられる。

以上

記録作成担当者：山田麻友

ヒアリング調査報告 No.29 基本情報

日時	2022 年 10 月 12 日
テーマ	経済安全保障とサイバーセキュリティについて
ヒアリング先 (担当者)	内閣官房 内閣サイバーセキュリティセンター 企画官 山田隆裕 様
場所	Webex によるオンライン
参加者	(WS-C 学生) 岡本樹、織田秀夫、木戸友香子、山田麻友 (計 4 名)
調査目的	我が国のサイバーセキュリティ政策についてお聞きし、政策提言に向けた課題および研究の出口を模索すること。

(写真)

【質疑応答】

Q1： デジタル庁と NISC の責任分担はどのようになっているのでしょうか。また、業法を所掌している、経産省、総務省、国交省、厚労省、金融庁との責任分担お聞かせいただければ幸いです。

A1： デジタル庁はデジタル改革の司令塔として、デジタル社会形成に関する施策の策定に当たって必要なサイバーセキュリティの確保に関する施策に取り組んでいる。NISC は、行政機関のサイバーセキュリティに関する監視・監査・助言を行うほか、サイバーセキュリティ戦略本部の事務局として、サイバーセキュリティ戦略 (案) の作成など、各省庁によるサイバーセキュリティに係る政策等の総合調整機能を担っている。

各省庁は、所管分野におけるサービス提供等の機能保証の観点から、それぞれの業法に則り企業を監督しているほか、経済産業省や総務省は、情報政策や通信・ネットワーク政策の観点から、サイバーセキュリティの確保に取り組んでいる。
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf

Q2： 我が国のサイバーセキュリティ対策については各業法を所掌している各省庁も独自の取り組みをしておりますが、とりわけ APT からのサイバー攻撃へのレジリエンスを高めるには、内閣官房に所属する NISC の役割は極めて重要と考えます。そのうえで、各省庁の力を最大化するために NISC が感じておられる課題を挙げるとすればどのようなものがありますでしょうか。

A2： 特定の分野に限らず、分野横断的にサイバー攻撃は発生していることから、NISC がハブ機能としての役割を担いつつ、各省庁が連携して対応に当たることが重要。サイバーセキュリティ戦略において、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能としてのナショナルサート（CSIRT/CERT）の枠組みを強化することとしている。
https://www.nisc.go.jp/about/organize/kinokyoka.html
インシデント等発生時に各省庁で得た情報を迅速かつ的確に集約し、得た情報を分析して各省庁等への的確なアドバイスや社会全体への注意喚起を実施する機能を強化していくことが重要。

（追加質問）

Q3： 積極防衛まで踏み込んでいるのでしょうか。また、防衛省との連携はあるのでしょうか。

A3： サイバーセキュリティ戦略にも、国民・社会を守るための取組施策の例として、脅威に対する事前の防御（積極的サイバー防御）策の構築を明記している。例えば、NICT の NOTICE の取組も攻撃に対する事前の備えの一つとして考えることが出来る。この取組に当たっては、不正アクセス禁止法の関係を NICT 法において整理することで可能としている。・サイバー空間における脅威に対して、何をしても良いというわけではなく、関係する法令の解釈と運用については NISC が「サイバーセキュリティ関係法令 Q&A ハンドブック」を作成している。
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018-zentaigaiyou.pdf
https://notice.go.jp/
https://security-portal.nisc.go.jp/law_handbook/index.html

Q4： サイバーセキュリティ協議会について、その概要ならびに課題点を教えていただければ幸いです。また、宮城県サイバーセキュリティ協議会と連携しているというお話を宮城県警様よりお伺いました。どのような連携を行っているのかについて、その概要と課題を教えていただければ幸いです。
kyogikai_gaiyou_kanryaku.pdf (nisc.go.jp)

A4： サイバーセキュリティ協議会は、情報共有を始めとした官民連携を進めるために組織された。全省庁の大臣が構成員となっているほか、民間企業や研究機関など、多様な方々に構成員になっていただいている。様々な組織に協議会の構成員になっていただくためには、ギブアンドテイクの関係が一つの重要な要素になると考えている。そのため、サイバーセキュリティ協議会の中に、タスクフォースを設けて、様々な情報を収集・分析して、対策情報を協議会全体のメンバーに広げていくという活動があり、その点を評価していただいて、たくさんの方々が共有活動に参加されている面があると思われる。一方で、タスクフォース以外の構成員を含む、全構成員を巻き込ん

だ、情報共有活動の活性化については、更にできることがあるのではないかと考えており、その点について、サイバー攻撃被害に係る情報共有のガイダンスに関する検討会を協議会のもとに立ち上げて検討している。最近では、クラウド事業者やシステムベンダー等のサイバー空間を作り、提供する方々が、サイバー空間の様々な情報を保有しているので、そういった主体との連携を進めて対策に繋げていくことも重要と考えている。宮城県のサイバーセキュリティ協議会には、本サイバーセキュリティ協議会の構成員となっていただいている。自治体自身ではない地域の団体が加入している例は珍しいかと思われる。宮城県サイバーセキュリティ協議会はタスクフォースメンバーではなく、今後、構成員の方々との情報共有活動の活性化の中で、連携の強化を進めていく必要があると思う。

Q5： サイバーセキュリティ協議会への加入が任意のため、加入してほしい事業者等を全て加入させることは難しいと思います。加入してほしい事業者等は既に当協議会に加入しているのでしょうか。または加入していないという状態なのでしょうか。

A5： 法律において加入が想定されている団体としては、国の行政機関、地方公共団体、重要インフラ事業者、サイバー関連事業者、教育研究機関となっている。そのため、このような団体には特に積極的にご参加いただければと思っている。なお、重要インフラ事業者については、重要インフラ 14 分野全てからから加入いただいている。自身が被害に遭ったまたは遭いそうになったときに、被害の事実というよりも、どのような攻撃を受けたかといった攻撃側の情報を共有してもらえると、現に起きている攻撃への対策や同じようなことが起きた際の対策につなげることが可能となるため、加入していただいた上で、こういった情報を積極的に共有していただけるとありがたい。

Q6： 現行の法制度ではサイバーセキュリティについては企業側の努力義務となっておりますが、企業経営者の意識レベルの差によって、対策にも差が生じてくるものと考えられます。そもそも企業の努力義務だけで良いものなのかご意見をお聞かせいただければ幸いです。

A6： 重要インフラ事業者とそれ以外と 2 つに分けて考える必要がある。前者については、緊密な官民連携が取れるよう、官民共通の行動計画である「重要インフラのサイバーセキュリティに係る行動計画」を作成して、それに基づき取り組んでいる。これらによる取組も努力義務であることには変わりはないが、今年の 6 月に行動計画を改定し、経営層の重要インフラサービス障害等に対する責任等を明記することで経営層の関与を促し、さらに踏み込んで、組織統治の一部としてサイバーセキュリティを組み入れ、組織全体での対応することを求めている。後者については、企業経営においては様々な観点が求められ、経営リソースも限られる中で、サイバーセキュリティ対策に経営資源を投入していただくべく、サイバーセキュリティの重要性について経営者の理解を深める啓発活動が重要と考えている。
cip_policy_2022.pdf (nisc.go.jp)

Q7： 政府機関が基幹インフラ企業ネットワークに対してインターネット側からサイバーパトロールを行い、必要に応じて当該企業に対し指導・改善勧告する制度を導入することには意義はありますでしょうか。ご意見をお聞かせいただければ幸いです。

A7： インターネット側から調査を行う場合は、その行為自体がサイバー攻撃と類似する行為となる可能性があるため、慎重に行う必要があり、社会に生じているリスク等との関係で考えるべきものと思われる。例えば、NICT が行っている NOTICE の導入に当たっては、不正アクセス禁止法との関係を整理するために、NICT 法を改正している。なお、企業のサイバーセキュリティへの取り組みの有価証券報告書等への記載につい

ては、総務省で過去に検討していたと記憶している。（追記：総務省のサイバーセキュリティタスクフォースにおいて議論され、「サイバーセキュリティ対策情報開示の手引き」が公表されている。）

Q8： APT による重要インフラへのサイバー攻撃に備えるためには、より高度な対策が必要になると思いますが、サイバーセキュリティ事業者の体制強化やモチベーション向上には、サイバーセキュリティ事業者をもう少し優遇してほしいという声も聞かれます。例えば、より高品質で堅牢なサイバーセキュリティシステムの構築・維持・運用に求められる最高レベルの技術スキル、特に攻撃スキル（オフェンシブスキル）を証明するような、より高難度の国家資格制度創設は可能でしょうか。また、文科省の所掌範囲にはなりますが、「技術士」資格の中に「サイバーセキュリティ」を創設することで、サイバーセキュリティ技術者にとってはステータスになると思います。

A8： 情報処理安全確保支援士の資格は存在するが、新たに「技術士」の中にサイバーセキュリティを加えることについては、技術士資格を所掌する文部科学省の判断になると思われる。なお、「より高品質で堅牢なサイバーセキュリティシステム」があったとしても、そういった技術や技術者に対して企業が投資していくことが重要であり、各企業においては、保有する情報の重要性やリスク等に合わせて必要な対策を判断できるような人材が重要になっているのではないかと思われる。

Q9： サイバーセキュリティ基本法は強制力を伴わない努力義務を基本に作られているものと解しているところです。昨今の世界情勢からすると、国家機能麻痺を狙ったサイバー攻撃も想定しておかねばならないと思います。そのうえで、重要インフラを担う企業については、業法での縛りはあるものの、影響が国家の存亡にも影響しかねないことを鑑みると、サイバーセキュリティ基本法の適用をより厳しくする必要があると考えます。NISC としてのお考えをお聞かせ頂ければ幸いです。

A9： 「重要インフラのサイバーセキュリティに係る行動計画」に基づく取組により、官民連携が機能していると理解しており、単に強制力を持たせることで、より効果的に対策できるようなものでもないと考えている。ただし、今後の状況や、国際情勢の変化も注視しながら考えていくことは重要である。なお、重要インフラの各分野において、IT への依存度や事業者の規模等の事情が異なることから、サイバーセキュリティ基本法に係る基本的な取組に加え、各分野の特性を踏まえ、必要に応じ、個別法令（業法）において重要インフラ事業者に対する義務が課されている。

Q10： サイバー攻撃については事前に情報を得ることによって、防御の可能性を上げる場合があるとされています。しかし、そうした情報を得ようとすること自体が不正アクセスに当たってしまう場合があります。サイバー攻撃の事前情報を得るために活動をする人はある程度限定されるとは思いますが、このような活動を行う人が活動しやすくするためにはどのような方法が適切でしょうか。

A10： 2018 年及び昨年閣議決定された「サイバーセキュリティ戦略」において、「積極的防御」に取り組んでいくということが記載されている。従来、政府機関や金融、電力等の重要インフラといった防御側のセキュリティを高めることが中心であったが、最近のサイバー攻撃の深刻化・巧妙化を踏まえ、脅威に対して、事前に積極的な防御策を講じていくことについて「積極的防御」という言葉を使っている。分かりやすい例として、脆弱性情報を共有することによって積極的に対策を講じていくことが積極的防御といえる。このほか、2018 年の戦略には、攻撃誘引技術の活用についても記載されている。今の法律で出来ることについて、工夫して取り組みつつ、今後も発生している又は想定されるリスクに合わせて、国民の権利等との関係を踏まえながら、本当に必要となる制度的手当について慎重に検討する必要があ

る。

Q11：　サイバー空間の利用については安全保障と経済安全保障の線引きは難しいと思います。昨今の国際情勢を鑑みれば、サイバー攻撃への防御については文民の区別なく、防衛相と民間企業そしてアカデミアとが連携することでさらに高度な対応が可能になると思いますが、この点について御意見をお聞かせいただければ幸いです。

A11：　サイバー攻撃への対応として、事前の対応としては、守るべきもの・機能に応じて対策を講じていくこと、攻撃発生時には、攻撃に合わせた対策を行うため、攻撃に関する情報共有を強化し、対策を講じていくことが重要である。その点、サイバーセキュリティ協議会には、防衛省を含めた各省庁や民間企業、教育研究機関等が入っているため、このような枠組みを通じて連携することで、防御力の強化につなげていければと考えている。

Q12：　サイバーセキュリティについて大学等で研究が進められていくと思います。サイバー攻撃被害の情報は研究を進める際の貴重なデータとなると考えられます。しかし、サイバー攻撃被害については公表がされない場合もあるとされています。大学が研究のために情報を集めることは難しいと考えられます。このことから、サイバー攻撃の研究を行う際には官民連携等が行われるのではないかと思っています。情報共有をする機関・組織が多くなる際に注意するべきことは何かありますか。

A12：　情報共有の組織の数が増えることは良いことかと思うが、情報共有活動そのものが活性化するということも重要である。被害組織からすると、自分の被害情報が含まれると情報共有しにくいということも考えられるため、情報共有の方法として、例えば、お互いの顔が見える形で行う方法のほかに、ハブ組織を通じて情報提供することにより、匿名で行う方法が考えられる。その際、攻撃側についての情報についてのみを共有して、誰が攻撃されたのか分からないようにすることなども考えられる。情報共有する場合には、信頼出来る関係性も重要であり、さらに情報の取り扱い方法も重要となる。例として、脆弱性に関する情報を共有するときに、その脆弱性の対策が講じられる前に、悪意のある者に伝わると、その脆弱性を悪用した攻撃に繋がってしまうおそれも考えられるほか、会社の場合は、顧客や取引先等との関係もあることから、顧客等に連絡して対策を取ってもらった後で情報共有するなど、取り扱われる情報の種類によって、様々な留意点が存在する。サイバー攻撃の研究に関する官民連携については、アメリカで進んでいるという話を聞いたことがあり、今後、産学連携や官民連携はより重要になっていくのではないかと考えられる。

Q13：　国際社会で日本のプレゼンスを向上させることがサイバーセキュリティにおいても重要ですが、今後の国際協力・連携に日本が活かせる強みと課題についてご教示ください。

A13：　例えば、各種施策を講じたことにより、東京オリンピック・パラリンピックにおいては、大会運営に影響を与えるサイバー攻撃がなかったことが、海外からも高く評価されていると承知しており、こういった実績もアピールしながら連携を強化していくことが考えられる。また、ASEAN 地域については、人材育成に取り組んでいる等、強みを生かした国際協力を行っている。

以上

記録作成担当者　岡本樹

ヒアリング調査報告No.30 基本情報

日時	2022年10月13日
テーマ	国際的な面から見た経済安全保障について
ヒアリング先 (担当者)	東京大学先 端科学技術研究センター 特任講師 井形彬 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 岡本樹、梶山敬生、香高優一郎、山田麻友 (計5名)
調査目的	豪州でのヒアリングに向けて、国際関係を中心とする経済安全保障について学生の疑問についてお答えいただき理解を深めること。

(写真)

【質疑応答】

Q1-1： IPEF や日豪首脳会談、日豪印、SCRI など、クアッド諸国とのサプライチェーンの強靭化での連携が行われています。アメリカ、豪州、インドとの国際連携の現状と今後についてお聞きしたいです。

A1-1： サプライチェーンの協力を国際的に進めていくことについてコンセンサスがある一方で、色々なものが乱立してしまっている。時系列的に見て一番早かったのは日米の2ヵ国間で、半導体についてサプライチェーンの協力や5Gの話、テレコミュニケーション技術について一緒に色々やっていこうという話があった。そのすぐ後に日豪でもサプライチェーンをやりましょうという話が出てきた。SCRIでも、IPEFでも、さらにいうとG7においてもサプライチェーンの協力ということが、どんどん出てきている。現状としては、コンセンサスはあるが乱立している状態であり、役割分担が明確に決まっていない。まさに、今後どの枠組みが何の役割を果たすのかについてはしっかり考えて行かないといけない。

SCRIとQUAD(クアッド)に関しては、アメリカがいるかどうかという所が大きい。アメリカを入れずに日豪印の三か国でサプライチェーンの協力をした方がアメリカを入れない場合と比べてよくなる部分というのは何なのかが見えてこない。役割分担を明確化していくことに尽きるのかと思う。アメリカでは、ワシントンD.Cやセントルイス、シアトル、カリフォルニアで意見交換をしたが、大体みんな同じでサプライチェーンが大事だという事だった。脱ロシア、中国ということが部分的に重要になって

きているが、どこが何の役割を果たすのかという所が明確にはなっていない。これから外交の力でそういった部分が決まって行くのだろうと思っている。

Q1-2： 政策提言という形で考えている案としてオーストラリアやアメリカといった一番信頼出来る国、また、マレーシアといった友好国といったグループで、サプライチェーンについて役割分担をしていこうかと考えており、本当に信頼出来る国については半導体といった重要物資について連携をしていき、それ以外の物資についてはマレーシア等の友好国間での枠組みを作っていくという形を構想しているのですが、それについてご意見を頂ければと思います。

A1-2： 日本の都合を考えるのであればその通りである。ただ、「言うは易く行うは難し」で、何が難しいのかというと、マレーシアに限らず、東南アジアの国々はどこもそうだと思うが、基本的にこういう枠組みに入りたくないと思っている。その理由として、“Don’t make us choose.”と言われる。つまり、アメリカと中国のどっちかということを我々に選ばせないで欲しいという事である。例えば脱中国と見られた場合、中国とビジネスをしにくくなってしまう。ただ、実質的に今まで中国やその他のところにあった生産拠点をベトナムやマレーシア、インドネシアに移して貰うということについてはメリットがあると感じている。実質的にそういう協力関係を進めて行くっていうことに関しては、おそらく大丈夫である。ただし、その時に新しい枠組みの名前を作って、東アジアの枠組みを作りましょうというのは、嫌がられる可能性が高い。どういうパッケージングをするのかについて東南アジアを巻き込んでいく場合は少し考えた方がいい。

Q1-3： 東南アジアというのはどちらかというと日和見的であり、枠組み等について、中国についていたいが、もし、利益があるのであれば日本にも付きたいという雰囲気を持っているのでしょうか。

A1-3： とにかくビジネスを続けたいと思っている。よく言われているのは、日本が様々な枠組みに入っていくことについても、枠組みに入って欲しくないと思っているというアジアの国は多い。その理由として、日本が日和見的な態度を取っている以上は、東南アジアでもどちらか選べと言われたとしても、日本だって日和見しているのに我々に対して選択する事を求めるというのは違うという人も多くなっているからだ。

ただ、その一方で若干トーンが変わってきたと感じており、今までは最初から”Don’t make us choose”だったが、そう言っていられないという認識を持っている外交官が増えてきている。東南アジアとして”Beyond don’t make us choose strategy”が必要であるという事を言っている人もいた。

ロシアのウクライナ侵攻や中国と台湾の関係などの中で、今までの完全日和見状態では東南アジアも今後は駄目だと思っているようである。そこに対して、完全に中国に敵対するような形ではないが、経済的なビジネスの枠組みとして一緒に儲けていくというのはいいのではないかと思っている、それをパッケージとして、例えば中国は入っていない枠組みだったとしても、そっちの方が協力関係を円滑に進めていく上で良いと感じるのであれば、入ってもいいのではないかと思う可能性はある。説得力や外交の力でそういう所に引っ張っていくということは出来るのではないかと思う。

Q2-1： 最近、グローバルサウスということで色々な先生が言及されるようになりましたが、必ずしも二軸の中に入りたくないというような形で出てくる場合に、米国の場合であれば分かりやすく民主主義というのを前に出すというケースもありますが、実際にグローバルサウスをひきつけるという意味ではどのような要素が我が国の外交に求められるのでしょうか。

A2-1： グローバルサウスという単語をアメリカの研究者が使った際に、インドの研究者

が反発していた。最近、アメリカにも中国にも付かないグローバルサウスという第三極について話す人が多いが、グローバルサウスとは何なのかということをインドがいっている。彼らとしては全然一枚岩ではなく。インドもいれば、東南アジア、アフリカもいる。全て一緒にしないで欲しいということをいっており、そうしたことについてパッケージングという意味でも気をつけていかないといけない。彼らが一緒くたにされたくないということについては、各国の特色をしっかり見て、例えばインドであれば対インド政策、対インド外交といった形で引っ張って欲しい、ピンポイントでやって欲しいということになってくるのではないか。対グローバルサウス戦略を考えると、共通項としてもちろん何個かはあると思うが、決定打となりそうなものは、各国や地域的な特徴にうまく答えられるような物を探していくことが大事である。

Q2-2：　昔のような非同盟諸国といった形で集団的に何かを得るというよりは一国一国の力が、各国で上がってきているということ思っています。また、大国が小国を掌握するということが現実的には難しくなってきていることから、第三諸国としてまとめてしまうことに反感を覚えるのかと思います。自分の力というものについて相当自信を持っている時代になりつつあるのでしょうか。

A2-2：　インドや東南アジアもそうだが、将来について見ると、人口は更に増えていくと考えられる。そして、現状では経済の中心とはなっていないが、将来的には自分たちが経済の中心になるという自信についても持っていると思う。

Q3：　サプライチェーンにおいて日本は同志国との連携を高めている状況ですが、その信頼の度合いはどのように判断すべきなのでしょうか。

A3：　信頼の度合いについて細かく数値化するというのは難しい。それこそデモクラシー・インテックスのように細かく点数をつけていくというよりは、ざっくりと過去5年となどの期間を決めてしまい、その期間の中で意図的に、明らかに外交的政治的理由でサプライチェーンを止めたという実績のある国と、止めたことがない国を分けることによって、信頼出来ない国というのが出てくる。信頼出来ない国というのは少ないが、それ以外は信頼できるという形でブラックリストを作るという形式でいいのではないかと思っている。物資が寸断する可能性がある中で、例えば豪州が日本に対して物資を輸出してくれるかということの信頼性については、日本としても確実性を上げていくことが出来るのではないかと思っている。例えば、日本が持っていて、オーストラリアが持っていないものについては何があっても安定的に供給をするからその代わりオーストラリアも、これに関しては日本に安定的に供給をしてくださいというアグリーメントを作っておけばいい。そして、これについてアメリカやカナダ、イギリス、ドイツ等ともやっていくということをやっておけば信頼性や安定供給の確実性は上がっていくと思う。一概にこの国だから信頼出来る、信頼出来ないという分け方とは別に外交の力で、その部分についての確定度を変えていくという努力は日本側からも出来ることだと思っている。

Q4：　レアアースの採掘、加工のフローにおいては環境的、人権的な制約があると思われます。今後、国際的にどのようなルールメイキングがなされていくべきだとお考えでしょうか。

A4：　安定的な供給という経済を取るために環境や人権を犠牲にするようなルールメイキングが必要であるとは思っていない。重要鉱物の採掘については物資が埋まっていなければ仕方がないが、加工の部分では、資金をかければ出来ないことはない。新しいルールメイキングで対応するのではなく、各国の政策レベルで対応出来るのではないかと感じている。新しいルールを作ればいいというわけではないので、そこについてはよく検討する必要がある。

Q5：　レアアースの製造行程において、放射性物質が大量に出てしまうという所で、強制労働ありきでコストダウンを中国が行っているのではないかということが疑われています。最近、マレーシアは中国よりは日本に近づいてきているのではないかと思っていますが、マレーシアに工場と作るという場合を考えたときに、人権を無視してしまう国に対抗するために、その基準を価値観として、その部分について目をつぶるというようなルールメイキングが許されるのか、それとも我が国として、我が国の高い環境基準を用いても更にプラスとなるようなメリットがあるという希望を持たせるような使い方は出来るのでしょうか。

A5：　国際的なルールメイキングというよりは、日本国内でのルールメイキングが必要な部分が出てくると思う。どういうことかというと、国連に日本政府が持って行った、人権 DD というものがある。日本企業が物を買ったり、作ったりする時に、自社のサプライチェーンにおいて、強制労働や人権侵害が起きていないかどうかをしっかり観察するような仕組みのことであり、これを作るべきであるという動きは出てきている。ただ、日本政府はこれについて法制化という形でするのではなく、まずは完全にボランタリーなガイドラインを作り、それで日本企業の行動が変わるのかどうかを見た上でそれでも変わらなければ数年後にもしかしたら法制化もありかもしれないという緩い立場となっている。海外を見るとアメリカや EU では人権 DD はしっかりやるべきであるとして、法律として通し始めている。その意味だと、日本国内的なルールメイキングとして人権 DD の法制化を早く進めると、日本企業にとって、日本が間接的にサプライチェーン上の強制労働や児童労働について間接的に加担しているという批判がされなくなることからビジネス上のメリットはある。人権侵害を抑えるという意味において、価値観的なプラスの面もある一方で、中国からのデカップリングのような、中国で作られたレアアースやレアメタルというのは強制労働を使っているものだから買っては駄目であるという国際世論作りにも貢献するという意味だと経済安全保障的な効果もあるのかと思う。

　もう 1 個似ているものとして、強制労働で作られたものをマーケットから排除するという動きも進んでいる。アメリカの「ウイグル強制労働防止法(UFLPA)」がある。アメリカ国内では、基本的にウイグルで作られたものは強制労働で作られたものだとみなし、強制労働で作られたものについてはもう輸入をしないというはじき方をしている。

　EU でもフォンデアライエン欧州委員長が似たようなことをウイグルに限定するのではなく、強制労働で作られている疑惑のあるものについては EU 市場に入れさせないという法律を通す方向で動いている。日本でそういった議論については全くない。国際的ではなく、国内的なルールメイキングにはなるが、人権 DD の法制化と日本市場からの強制労働で作られた製品の排除の二つというのは考えられる。

Q6-1：　蓄電池産業戦略の p.17 においては、バッテリーの国際ルールの構築推進が謳われています。今後我が国がこのようなルール形成を推進するにあたり、現状とその課題についてご見解をいただきたいです。

A6-1：　どのコンテンツでどのようなルールを作っていくかを考える前に、まず、どの国際枠組みでそのルールを作っていくかについて考えるべきである。参加する国が多ければ多いほど、物事を決めるのには時間がかかるので、できればフォーカスした方がいいけれども、重要なステークホルダーがいないと不完全なものになってしまう。そのため、ルール構築を行う場の確定というのが難しい。また、確定後、実際にどのようなルールを盛り込むかも重要となっていく。原材料生産国と製造国の二つのグループがあるが、どちらも思惑は異なると思う。日本一国が有利になりそうなルールを作るのではなく、日本と同じようなマーケットポジションにある国と一緒にスクラムを

組んで原材料生産国に圧力をかけていければ外交政策として上々だと思う。

Q6-2： 日本は、EU のような連合体でもなく、そうは言って米国とも経済関係では対立することもあります。このような連携をするのは日本にとって難しいと思いますがいかがでしょうか。

A6-2： 難しいと思うが、まず、EU は常に一枚岩ではない。内部でゴタゴタすることがある。EU を過大評価するのは良くないし、EU は連合体として統一したポジションを取るために、ものすごく資源を使っている。EU もできるなら日本にもできるはずだと思う。逆に今まで日本はなんでも日米基軸にしていて、他が若干弱かったところがあるので、特に蓄電池についてはイギリスと色々連携できるのではないか。素材の部分であったら、豪州、カナダ等、色々できると思う。

一概には言えないが、なんとなく日本の外務省のエリートコースは北米一、二課に行き、カナダ、豪州担当は若干下に見られがちなところがどうしてもあるとは思う。だが、そうではなくて、これからの日本は日米同盟だけでなく、より第三国のパートナーを重視していかないとダメだから、例えば、エース級の人材を日豪関係の担当者に送ることが挙げられる。イギリスも Brexit した後に新しいパートナーを探しているという。数ヶ月前ロンドンに行った時にグローバル・ブリテン構想として日本と色々連携したいということを言っていたので、向こうがその気ならこっちもそれなりのリソースを投じて、別に第二次日英同盟まで行かなくとも、もっともっと頑張れば何かできるはずなのではないかと思う。

Q6-3： 英国以外でも日本と組みたいという話は聞かれるものなのでしょうか。

A6-3： 聞かれる。英国ではトラス政権になったが、トラス氏自身、すごい日本好きだ。しかも、Brexit 後、イギリスが初めて結んだ FTA が日本であった。その時の国際貿易大臣がトラス氏だったし、経済安保が大好きで、トラス政権が続くのであれば、このバッテリーの協力は絶対できると思う。3 ヶ月前に経済版 2 プラス 2 において、日米バッテリー協力があり、英国はバッテリー戦略を既に出している。日本が提案すれば英国は多分好意的に見てくれる。あとはオーストラリアに関しては、今の日本の政権も日豪関係を準同盟化するとまでは踏み込まないが、そのようなナラティブが出ているくらい協力関係は活発化してきている。イギリス、オーストラリア、無理ではあるが韓国、ドイツ、資源関係はカナダになっていくと思う。

Q7： ドイツなどの国と日本と組むというような話を続ける時に、日本は市場力として期待をされているというよりかは、技術協力や製品供給元として何らかの協力が出来ないかときたいされていると思っています。それらを考えたときに、中国に対してのドイツ、イギリスの視点がおそらく市場として、何かを買って欲しいというものである場合、そして日本が供給側としてきたいされているとする場合に、連携をする際には、ある程度中国を意識することになり悩んでいるのではないかという気がしています。現在のヨーロッパでそういった雰囲気はあるのでしょうか。

A7： ここ 5 年ぐらいで対中脅威認識が上がってきている。数字で分かりやすいのは一般世論である。例えばピュー・リサーチセンターが 20 か国ぐらいに対して、主要国に対しての好感度について、同じ質問で各国に聞いてパーセンテージを出している。ここ 5 年ぐらいで好感度は軒並み下がっている。中国について嫌いである、危ない、脅威がと思っている人が増えており、最近では 7～8 割ぐらいは中国に対するケイパビリティについて低い数字が出ている。一般世論についても変化し始めている。

政府レベルで言うとイギリスである。トラス首相がイギリス政府として初めて中国を”threat”である、脅威国であるということを言った。国のリーダーが完全に脅威だ、脅威の対象としての国だというのは、今の所はただのレトリックではあるが、実

際に政策にどれだけ反映されるかについては見ていく必要はあるが、それぐらいまで認識は悪化しているということだと思っている。

ヨーロッパで重要なのは、EU を動かしているドイツである。そして、ドイツを動かしているのはドイツの産業団体である。ドイツの経団連のような所が報告書を出しているが、中国のことをシステミックコンペティターというような言い方をしている。そこが、完全にただのマーケットとしての中国というものから脅威ではないにせよ、もっと警戒しなければならない相手という風に変わってきている。さらにロシアのウクライナ侵攻があり、中国がこれを支持してしまった。あんな酷いことをしているプーチンを支持する習近平はやっぱり駄目だということで、一気に対中認識がまた悪くなったという所がある。じわじわと中国が脅威だという方向性になっており、最近起こっている状況についてもこのトレンドが続く要素しか出てきていない。このまま対中脅威認識は高まっていくし、実際に中国のパワーも上がってきていることから、ある程度経済を犠牲にしたとしても、安全保障を取るというような方向性でヨーロッパも動くのではないかと思っている。

Q8： クリアランス制度に関して、セキュリティ向上の鍵はクリアランスにあるとおっしゃっていたと思いますが、現状、国内に制度を導入するにあたって障壁であると考えられることなどがあれば教えていただきたいです。

A8： クリアランスの導入への障壁はたくさんあるが、一番大きいのは、やっぱり国民世論、国民感情かと考えている。詳しいことをしっかりと説明すればわかっていただける方は多いとは思うが、いかんせんこのクリアランスは非常に複雑な側面もあり、ちょっとでも誤解があるとものすごい批判をされる可能性がある問題である。例の特定秘密保護法を通そうと思ったときですらあれほどの反発があったのに、似たようなものを民間にも拡大すべきだっていう議論がどれだけ今の一般国民に理解できるのかを考えると、頑張って説明を続ければわかってくれるとは思うが、やはりその世論の反応が一つの障壁で、もう一つはそれをその世論を説得してでもこれが必要だということを訴えかける。政治家でパワフルな人が今いるかって言われると、多分今の岸田政権に、この政治リスクを取ってまでこのクリアランス残しても通すのだという気概は多分ないと思っている。ポリティカルキャピタルがちょっと足りてないと、今の政権というのも障壁になると思っています。あとは実際にクリアランス制度って作るためには法律を通せばいいというだけではなくて、実際にそれをインプリメンテーション、インプレしてかないと駄目だと考えている。クリアランス制度はインプレするのにコストがかかるものである。

例えば、井形がセキュリティクリアランスをするということになったときに本当にこの井形という人が信頼できるのかというのをチェックするために、まず過去 20 年分の渡航歴全部洗ってそのような外国人と仲が良くて実際にどういう会議に今まで参加して、どういうところでどんなことを言っているのかというのを洗いざらい調べることから始まって、例えば僕の住んでいる隣の近所の人のところに実際に行って「井形さんってどんな方ですか」ということを聞く、あとは大学のときの先生、中学校高校の頃の同級生の所も回り、昔の思想など、そういうことまで全部聞いて言っている。それを全部やった上でこれもそのクリアランスで、どこのどれだけの機密の情報にアクセスできるかって、そのバックグラウンドチェックの度合いっていうものの厳しさが変わってくる。

例えばアメリカとかだと、これもポリグラフを繋げて嘘発見器みたいに、一つ一つ質問をする。内容についても結構センシティブなことを聞いていく。例えば浮気とか不倫とかしてしたことないですかだったり、酒癖悪かったりしませんでしたかといったことや、あとはカナダに居たときに、何か違法物質を吸ったりしていないかといったこと、借金があるかということについて等の要はブラックメールに使われてしまう

ようなことをこの人が隠してないかということを全部調べていく。それを1人だけにするのではなく、クリアランスを取る人数っていうのを考えると、ものすごい数になる。最新の状況を見るとアメリカではクリアランス保持している人は400万人以上いる。

アメリカでは人口の一割以上がクリアランスを持っている。日本で人口の一割、同じくらいもしクリアランスを取るという前提でやるのだとすると、およそ1000万人となる。1000万人分このバックグラウンドチェックをするために一体何年、どれだけのお金がかかるのかを考えるとここのインプレへの障壁はすごく大きなものであるだろうと思う。

やるべきだと言いながら障壁ばっかりって言っていると悲観的にはなってしまうが、現状としてはこのような状況である。

Q9： 重要物資を入手するにあたって、サプライチェーンの強化はもちろん、事前に取引相手のリスク評価といったことも重要ではないかと感じます。しかし、大企業でも物流の末端まで把握することが難しい中、どのように日本の企業に対してアプローチしていくことが重要だとお考えでしょうか。

A9： 重要なことはいくつかあるが、一つは取引相手のリスク評価っていうのは経済安保関係なく普段からやっているべきことではある。なので、引き続きちゃんとやる必要はおそらくあると思う。あとは末端まで把握することは難しいというふうに企業側は言うが、できないことはない。できないことはないっていうことについて、どういう根拠で言っているかというと、例えばEUにおける環境規制の法律、あるいは電子部品とかに関する環境計画環境系の規制とかっていうのを見ると、このパソコンのネジ1本に至るまで、ちゃんとそれを製造するときに変なケミカルが漏れてないかといったことや、環境アセスメントがちゃんとしているのかについてチェックしないといけない。物を売ろうと思っている限りは、それしか使わないと駄目なので、それをやっている。日本企業もEUと関係があるところは、コストがかかるだけで、出来ない訳じゃないということと、あとはさらに最近ブロックチェーンの技術など、色々このトレーサビリティを容易にするような技術というのがどんどん出てきていて、効率も精度も上がり、コストも少しずつ下がってきている。そういう新しいツール、新しいサービスもしっかりと利用して末端までしっかり把握する。逆に把握できないところっていうのは、やっぱりなにか理由があるところで、それはどういう所かというと、また中国の話になってしまうが、例えば監査しに行ったら、公安に捕まってしまったということが起こる。そういうところにサプライチェーンは依存したら駄目だろうということに段々なりつつあると思う。なので、アプローチの仕方としてはやっぱり企業ブランドをしっかりと守っていきたいと思うのであれば、物を買ったり売ったりしている相手が信頼できるかどうか、今までもちゃんとチェックしなければ駄目であったが、さらにこれからちはちゃんとチェックしていこうというマインドセットを広げていくと共に、それが出来ない国、出来ない相手方に関しては、取引をやめるっていうところが重要なのかなとは思う。

Q10-1： 経済安全保障推進法の下、基本方針等が作成されております。基本方針案の第1章第2節

(3)に「事業者等との連携」が記されています。従来念頭に置かずに経済活動を行ってきた事業者が多数いるために、本法の施策やそれ以外の経済安全保障施策を実効的に行うためには、事業者へ情報を提供する必要性があり、このような記載をしたと私自身は考えております。どのような事業者との連携が望ましいか、ご教示いただけますと幸いです。

A10-1： 様々な側面で連携を進めていくことが望ましいというのが一番ジェネラルなア

ンサー。もう少し個別に落としていくと、政府から事業者へ情報提供をする枠組みももちろん必要になる。本来であれば、国家安全保障局の経済班や経済安保推進法を実際に運用していくためにできた内閣府の経済安全保障推進室など、ある機関が情報収集のハブになりオープンソースとして情報を提供していけばいい。リスクアラートのような形で定期的に発信していく方法や、海外での動向を噛み砕いて提供する方法もある。実際に公安調査庁が経済安保特設 Web サイトというものを作っている。このような情報発信をより定期的に、パワフルに行う機関があればいいと思う。

政府から事業者への情報の流れも重要ではあるが、政府としては事業者からの情報が欲しい。例えば、サプライチェーン上の脆弱性を改善すると政府が思っても、何が脆弱かを理解しなければいけない。考えればわかるところはあるものの、考えてもわからないところが意外とある。それが一番顕著だったのが、新型コロナウイルス下でのマスク不足。経産省でマスクのサプライチェーンを見ている部署はない。そうなると、どの企業がマスクを作り、どこがマスクを輸入しているのか、どこから輸入しているのか、等の情報を急いで集めなければならなった。事業者からの情報をより恒常的にしっかりと吸収できる枠組みが必要になると思う。

これらが情報の柱とすると、もう一つの協力関係として、どれだけ特定の国からデカップリングを進めるかということ。多くの企業は、経済のロジックを優先して一番安いところから買い続けたい側面がある一方、政府としては安全保障を優先し多少経済の論理が破綻してでも自国で生産したり、あるいは信頼できる国々で生産したり購入するスキームにしたいと考える際に、ここの綱引きをどうするのか考えることが重要。この一つのアンサーが今回の推進法である。民間企業側から、このような形でサプライチェーンをシフトしたいと計画が出てきたら、それを政府がチェックし、重要だと思えば補助金をつけるということは、この協力関係の一つだと思う。どのくらい当法が機能するか、今後の動向に注目したい。

Q10-2： ESG 投資のように、企業が経済安全保障を念頭に経営活動を行っているか否かによって投資家が投資先を決めるといったことは、今後起こりうるのでしょうか。

A10-2： 去年から、スチュワードシップコードの中に経済安保の重要性をしっかりと民間が意識しているかといった要素が少しずつ入り始めているので、投資家の中で経済安保を意識し始めている人たちもいるとは思う。一方で、その要素をどれだけ考慮して実際に投資を決めている投資家はまだそこまで多くないと思う。ただ、少しずつ経済安保方向には動いてはいる。中国やロシアを念頭に、経済安保や外交、政治的リスクを考え、ピュアな経済ロジック以外の部分で判断する企業は増えている。ただ、環境や人権を念頭においた考え方があるために、そういったロジックで考えることは新しいことではない。経済安保の考えが広まってきているため、あとは投資家サイドでいかに素早く対応できるかが問題になると思う。

Q11： 今年 7 月に日米経済版 2+2 が開催されました。この委員会の開催に対する評価、及び、米国以外でこのような委員会を開くべき国がありましたらご教示いただけますと幸いです。

A11： この委員会の開催に対する評価というと、何か似たようなことをすべきだと言っていた人は以前からいた。こういった会合は、本来であれば行うのは目的ではなく、その問題に対する中身の詰まった議論がハイレベルな環境でできるところまで、日米の間で議論が進んでいることが重要である。従って、その一つのモデルとして日米経済版 2 プラス 2 が開催されたことは非常にいいことだと思う。一方で、もう少しいろいろなことができたと思う。Q1 に戻るが、例えば、現状様々な国際枠組みがある中で、全てに加入しているのは日本とアメリカである。経済版２＋２に

おいて、日米の間で、この枠組みではこれを話そう、これを決めようといった役割分担の話をするのかなと思っていたが、あまり話さなかった。この点が少し残念である。

アメリカ以外にこういった委員会を開くべき国があるかについては、今後の意気込みを世界に示すために、日豪経済安保 2+2 や、日英経済安保 2+2 という形でどんどん開いていってもよい。ただ、経済版 2+2 を開くことが重要ではなく、アメリカ以外の国々と一緒に経済安保の協力を進めていくことが大事であり、その目的に資する上で経済版 2+2 を開くことがプラスになるのであれば、開くべきだと思う。開くべき国としては、再度となるが、オーストラリアやイギリス、さらにドイツ、韓国がいいのではないか。

Q12： サイバーセキュリティを強化していくにあたって、どういった部品が使われているかについても重要になってくると考えています。自国製の部品のみを使うことや、特定の国ついては使わないというのは制約が多いと思います。そのことから、どの国の部品を使っているのかについてはある程度把握しておくことで、セキュリティの安全性を担保することが出来るのではないかと思い考えています。しかし、大企業であったとしてもそうしたことを行うことは難しいという現状がある中で、こうした部品の把握についてのどこ由来の物であるかを把握することを義務付けることはハードルが高いでしょうか。

A12： 製品に使われている部品について把握出来るかについて話をしたことがあるが、どのような製品が使われているのかについて把握することは出来た。しかし、使われているものが大体中国製だったことから困ってしまったということがある。政府が民間に対してちゃんとトレーサビリティを行うようにということを一般的に行うことは難しい。しかし、限定的に実施することは出来ると思う。今回の経済安全保障推進法の中の基幹インフラの大柱の中に入っていて、これは日本国民にとって重要なインフラを経営している会社に関してだけは、甘いサイバーセキュリティのシステムを使っているとまずいという認識があることから、政府としても危ないソフトウェアやハードウェア、プログラムを　使っているというのは論外であるとなっている。把握すること自体が重要なわけではなく、危ないと思われる国の部品についてハードウェアであればメモリーなど、情報をキープすることの出来るようなアクティブパーツと呼ばれる物については、信頼出来ない国で作られたような物や特定の国家情報法のような物がある国に関してはそこから情報が漏れる可能性があることから使用をしない。反対に、電源コードのようなものであればアクティブパーツではないことからサイバーセキュリティ上は特定の国に依存しても一応問題はないということにはなる。しかし経済外交で止められるリスクというのはあるが、サイバーセキュリティの面であればアクティブパーツであるかが一つの鍵となる。

Q13： 日本の民間企業等が優れた技術をもっていたとしても、サイバー攻撃等によってそうした情報を入手されてしますという可能性が考えられます。サイバー攻撃については企業の中で対策を進めることが出来ているところと出来ていない所で差が出ています。対策がまだ進んでいない企業ではどういった技術を守るべきかについて判断に迷っている場合もあるのではないかと思います。しかし、今後、経済安全保障を進めていく上で、どういった技術を大切としていくかを知ることは重要であると考えおり、企業がどういった情報を守っていきたいかを知ることによってサイバー攻撃対策を進めることにも繋がるのではないかと思っています。 企業等がどういった技術を重要視し守っていこうとしているのかという情報を集めていくことに意義はありますでしょうか。また、技術情報については民間で行う場合に同業他社といった競合がいることから、情報を収集することは難しいと思います。このことか

ら、国として情報を集めることがいいのではないかと思っていますが、こうしたことは可能でしょうか。

A13：　国として情報を求めたとしても、そこまで情報を出してくれない可能性が高い。特に日本で技術開発をしている会社となると更に情報は出てこないと考えられる。また、中小企業については報告をするという余力がないことから、大企業の一部のみの情報が集まり、外資系企業からは無視されて、中小企業についても無視されて終わる可能性が高い。輸出管理や投資規制、外部から日本にきて勉強や研究をする科学者に対する査証という形で、少なくとも政府がどういう技術を重要だと考えているのかは民間に対してそういった法律規制を通じて一応は周知されているはずである。

政府が今まで特定してきた重要技術とは違い、そこから漏れている技術について民間が持っているかもしれないという考えについては、経済産業省で中小企業リストアップなどをおこなっており、経産省としてもやっていこうとはしているが、さすがに数が多いことから、上場企業だけで精一杯となってしまう。どういうインセンティブストラクチャーを作って企業に報告させるのかが問題となる。

こうした情報については地方自治体や地方議員が情報をよく知っているはずである。特に地方議員であれば、基本的には中小企業の人がどういう仕事をしているのかということを知っているはずである。地方議員のネットワークを活かし、情報収集をするということを神奈川県の相模原市など3か所ぐらいで行われており、地方議員が集まって提言書についても出されていたと思う。

以上

記録作成担当者：山田 麻友

ヒアリング調査報告 No.31 基本情報

日時	2022 年 11 月 1 日
テーマ	宮城県・宮城県警察によるサイバーセキュリティ・情報共有体制等について
ヒアリング先 (担当者)	宮城県警察本部生活安全部サイバー犯罪対策課サイバーセキュリティ推進係長 宮城県警部補 佐藤智彦 様 宮城県企画部 デジタルみやぎ推進課 ネットワーク最適化班主任主査 池田篤志 様
場所	東北大学 片平キャンパス エクステンション教育研究棟　201A 講義室
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、香高優一郎、宮内拓、山田麻友 (計 8 名)
調査目的	宮城県・宮城県警によるサイバーセキュリティ協議会等の取り組みについて調査すること。

(写真)

【質疑応答】

Q1-1：　協議会の設立経緯を教えていただけますと幸いです。

A1-1：　2019 年に遡るが、この時はサイバー犯罪の件数等が最も増加していた時期であった。サイバーセキュリティに対する脅威がまさに深刻化していた時期となる。その中で、2020 東京オリンピックパラリンピック競技大会の開催を控えており、その開催に万全を期すためということで、官民の多様な主体が相互に連携してサイバーセキュリ

ティ施策推進を図るための協議の場として、国においてサイバーセキュリティ協議会が平成31年の4月1日に設立された。このようにサイバーセキュリティ対策が急務であるというところで、本県において宮城県と県警が一体となり、会員相互および関係機関が緻密に連携してサイバー空間の脅威情報を情報共有という形で円滑に共有して、サイバーセキュリティ対策の向上の目的のもと、宮城県サイバーセキュリティ協議会が発足するに至った。（池田様）

Q1-2：　他の都道府県にもない先進的な取り組みということで、協議会を設立する以前から、宮城県はサイバーセキュリティに対して敏感であったのでしょうか。
A1-2：　そうだ。事件捜査においても、東北で一番という自負を持ち、サイバー犯罪についての事件捜査に力を入れている。（佐藤様）

Q2：　協議会を設立するにあたって、どのような点に注意をしておりましたか。また、参考とした協議会などがございましたら教えていただけますと幸いです。
A2：　国のサイバーセキュリティ協議会を参考としている。こちらの協議会は、国の関係行政機関、地方公共団体、重要インフラ事業者、サイバー関係事業者、大学・教育研究機関という五つの機関で構成されている。これらを参考にして、対象団体へ働きかけを行った。設立にあたり、会員相互の連携強化や情報交換・情報共有の推進を図るという点で、県と県警が一体となって、関係機関がまとまった体制となるよう意識して設立した。（池田様）

Q3-1：　協議会の具体的な活動内容について、教えていただけますと幸いです。
A3-1：　メーリングリストを用いて、脅威事案等の情報共有を行っている。また、サイバー犯罪被害の防止の観点から、広報啓発等についてメーリングリスト等を利用して行っている。さらに、各種セミナーを開催し情報セキュリティ対策・サイバーセキュリティ対策を推進している。（池田様）

Q3-2：　国のサイバーセキュリティ協議会では、官から民への情報のみではなく、民がどのような被害が起きたということをすぐ分析等するタスクフォースを設けて、分析情報をまた民の方に発信するという相互的な仕組みがあります。このような仕組みは宮城県サイバーセキュリティ協議会にはあるのでしょうか。
A3-2：　ある。協議会の会員から、例えば自分の事業者に対して何か被害があった場合に、警察にも相談と通報をしてもらい、それらを警察の方で広報資料として新たに作成し、会員の皆様に注意を呼びかけるような形で行っている。（佐藤様）

Q4-1：　協議会の運用にあたって、良かった点及び課題点、改善点を教えてください。
A4-1：　良かった点としては、早期の段階で迅速な情報共有が図れること。それにより、より早期に対策を行うことができる。協議会という大規模ネットワークでこういったものを構築できた点は非常に良い点として挙げられると思う。一方、課題というほどではないが、ギブアンドテイクといった、情報を出し合うことが大事であり、その情報共有をより一層活発化することが必要だと感じる。協議会の中に特別支援構成員という会員を設けており、この会員に積極的に情報発信を行ってもらうことで、会員全体を引っ張る役目を引き受けていただいている。（池田様）

Q4-2：　ギブアンドテイクが課題点であるということで、どのようなことがギブアンドテイクの障壁になっているのか教えていただけますと幸いです。
A4-2：　企業が、情報提供するに当たり、例えば自分の会社にサイバー攻撃があったという場合に、自分の会社が被害に遭ったことが公表されるのではないかという心配があ

る。このような点で、会員の皆様に情報提供をしてもよいのかと躊躇することがあり、障壁となっているのではないかと思う。（佐藤様）

Q5：　加入団体が非常に多い（民間事業者：83、国・地方公共団体・教育機関・医療機関：46）ですが、これら団体の加入は強制でしょうか、それとも任意でしょうか。もし任意であるとしたら、なぜこんなにも多くの団体が加入しているのでしょうか。また、加入団体の制限等がございましたら、教えていただけますと幸いです。
A5：　加入については任意である。加入団体について制限等はない。なぜこのように多くの団体が入っているのかについては、元々県警で取り組んでいた協議会が三つあり、それらを一つにまとめたということが一つ理由として挙げられる。この三つの協議会は、宮城県ネットワーク防犯連絡協議会、宮城県複合カフェ防犯連絡協議会、宮城中小企業情報セキュリティ支援ネットワーク会議である。また、宮城県サイバーセキュリティ協議会を設立するに当たり、そのタイミングで各業界の企業や団体に働きかけを行った。さらに、宮城県が県警の取り組みと一体になることで、市町村なども参加し、より多くの団体の加入に繋がっていると思う。（池田様）

Q6-1：　加入団体が、共有された情報を漏洩した場合、罰則等はございますか。
A6-1：　罰則はないが、守秘義務はある。（池田様）

Q6-2：　守秘義務を守らなかった場合、制裁等はございますか。
A6-2：　制裁等はない。あくまで団体との信頼関係を重視し、仮に情報漏洩等が発生した場合には、内容により不正競争防止法等の関係法令に違反するのであれば捜査することとなる。（佐藤様）

Q7：　NISC を中心とした「サイバーセキュリティ協議会」とも連携されていると伺いました。どのような連携がなされているのか、教えていただけますと幸いです。
A7：　そもそも宮城県のサイバーセキュリティ協議会は、国のサイバーセキュリティ協議会の会員でもある。具体的な取り組みとしては、国のサイバーセキュリティ協議会から提供された脆弱性等の共有情報をすぐに会員間で共有することが一つ挙げられる。また、本県の協議会のセミナーの講師として国のサイバーセキュリティ協議会の方に参加していただくこともある。（池田様）

Q8-1：　APT 等による宮城県内企業へのサイバー攻撃が発生し被害企業から宮城県警に訴えがあった場合アトリビューションはどの組織がどのような役割分担で実施するのでしょうか。また、アトリビューションを進める上での難しさはどのような点ですか。
A8-1：　まずは宮城県警公安課を中心に他課とも協力し、どのような攻撃が行われたのか情報収集しつつ、被害を最小限にとどめ、NISC にも一報を入れる。また、警察庁にもエスカレーションし、必要に応じて支援を要請する。（佐藤様）

Q8-2：　アトリビューションにおいては不正アクセス禁止法への抵触も気になると思いますが、被疑者を追跡捜査する上でやりづらさもあるのではないでしょうか
A8-2：　当然法律にのっとった方法しかできない。不正アクセス禁止法への抵触が懸念される場合は相手側の承諾を得るようにしているが、相手国側が非友好国の場合は承諾を得るのは難しい。（佐藤様）

Q8-3：　発電設備など重要インフラが攻撃された場合の対応について、自衛隊や防衛省との連携がとれる体制は整っているのでしょうか。
A8-3：　防衛省と警察庁との連携になると思うが、お答えできる立場にない。（佐藤様）

Q9：　協議会に限らず、サイバー攻撃についての情報共有を行う際に困難に感じることはありますでしょうか。
A9：　企業がサイバー攻撃を受けた場合に、警察以外に公表するということについては企業のイメージに影響する可能性がある。被害にあった人から出来る限りシナリオを貰ってはいるが、それを公表することについては企業イメージが関わって来ることから、そういったやり取りについて慎重に行っている。（佐藤様）

Q10：　サイバーに関する被害通報のうち個人からの被害通報はどれくらいの割合を占めるものなのでしょうか。
A10：　一般の方からの通報は県警全体、各警察署の方で受け付けている。（佐藤様）

Q11：　サイバー犯罪の被害者に対してはどのような取組や支援が行われていますか。
A11：　サイバー犯罪被害者に限らず、サイバー犯罪被害者の被害申告に基づいて、警察が捜査・予防策を講じ、被害者の方がそれ以上の被害にあわないようにしている。あわせて、可能な範囲で情報発信をしているという形になっている。（佐藤様）

Q12：　サイバー犯罪に関して今後、もっと民間の理解や協力を得られれば犯罪の予防や犯人のスムーズな検挙につながるなどのお考えはございますか。もしあれば可能な範囲でおしえていただけますと幸いです。
A12：　サイバー犯罪は、匿名性もあるし、地域的な制限もないので、できる限り速やかな事件捜査というのが、犯人逮捕に繋がるということもあり、被害に遭われた方からは、迅速な通報をお願いしている。しかし、被害に遭われた方が被害を警察に届けていいものかと通報を躊躇する場合もある。もしくは被害に遭ったことがわからず、被害通報が遅れるということもある。例えば、フィッシング被害に遭った方はそれが本物だと思って情報を入力し、後になって身に覚えのない請求が来た時に被害に気付き、結果として時間がかかってしまって、犯人がわからなくなるということもある。被害に遭ったことが判明した場合は速やかに警察の方に相談をお願いするよう呼びかけている。（佐藤様）

Q13：　人材育成の観点からはどのような取り組みが行われているのか、可能な範囲で教えていただけますと幸いです。
A13：　協議会のことに関しては、各会員からのセミナー、NISC 等サイバー関係の方からの知見を集め、会員のスキルアップを図っている。（佐藤様）

Q14-1：　Q13 と関連して、県内でサイバー人材を確保、育成する上での課題についてご教示ください。
A14-1：　人材は県警に限らずどこの企業でも分野でも必要とされている。特に県警では、サイバー犯罪の事件捜査でそのような IT 人材を必要している。
　今ある人材もサイバー捜査に卓越して対応できるよう、教育をおこなっている。例えば、民間の IT 企業主催の交流会に参加することや JC3 や Yahoo といった民間企業へ半年間出向させて、業務を通じて育成をおこなっている。（佐藤様）

Q14-2：　警察庁でもサイバーの取り組みがございますが、県警としてはそしてどのような役割分担をして行くのでしょうか。
A14-2：　警察庁や管区警察局とは情報収集・情報共有で連携している。また、県警で扱うのが難しい高度な事件は管区警察局、警察庁に速報して、事件の内容、今後の進め方などを共有する。（佐藤様）

Q14-3：　宮城県警としては、初動捜査といったところで、一般的なサイバー犯罪について対処できる人材を求めているのでしょうか。
A14-3：　いわゆる初歩的な捜査やそのほかのサイバー犯罪の事件捜査ができるほどの知識を持ったものとして、サイバー捜査官というものがいる。サイバー捜査官に関しては、国家資格のサイバー基本情報処理の資格を持ったものが活躍している。（佐藤様）

Q15-1：　サイバー犯罪・攻撃の捜査や抑止のためには、多国間の連携が不可欠です。最近、警察庁にサイバー警察局が新設されたこともあり、サイバー空間の安全の確保のための体制が刷新・強化されました。こうした体制の変化を受けて、その効果をどのように感じていらっしゃいますか。また、体制の変化以前の、宮城県の国際連携についてもご教示ください。
A15-1：　サイバー犯罪は、国境を越えておこなわれるものもあり、国際連携が不可欠となる。2022 年の 4 月に警察庁のサイバー警察局が発足し、国際連携も含め、事件調査について各都道府県警察と連携して行うという形になっている。このような体制も整ったことで、これまで以上に国際連携と国際事件捜査についてやりやすくなると思う。
　改正前の国際捜査に関しては、通信記録の提供や事件捜査の協力を依頼されたら実施していた。（佐藤様）

Q15-2：　具体的にやりやすくなったのはどのようなところでしょうか。
A15-2：　部署が一本化されたため、報告する場所が明確になった。それはメリットだと思う。（佐藤様）

Q15-3：　以前は分散化されていたのでしょうか？
A15-3：　事件の性質によって、報告先が変わるということがあった。（佐藤様）

（追加質問）
Q16：　私が所属する NTT でもセキュリティ技術者の流出が激しい。社内で育成した人材が、GAFA 等に年間数十名流れており、社内で問題視されている。実際に私の周りでも起きている。優秀なセキュリティ技術者を確保するとなると年収数千万円の処遇が必要であるが、公務員の場合、次官級が年収 2300 万円の上限と言われ、優秀なセキュリティ技術者の確保も、流出の食い止めにも苦労されていると思いますがどのような状況にあるのでしょうか。
A16：　一般の警察官とサイバー捜査官では採用が違う。犯人よりも上のスキルが必要だが探すのは難しい。（佐藤様）

Q17：　2018 年に日本にも合意制度が導入されましたが、ここの罪状が組織的な経済犯罪がはいっていたと記憶しています。サイバー犯罪の中でも一部の犯罪はこの合意制度の対象になりうるのでしょうか。
A17：　フィッシング詐欺等について、合意制度の対象となり得るかについてはお答えを差し控える。（佐藤様）

Q18-1：　加入が任意ということでしたが、加入企業の中に敵国等の人材がいた場合には、協議会への加入が逆に仇となり、情報漏洩との危険性が高まるのではないかと感じます。任意ではあるものの、県庁様や県警様から加入する前に企業に対して調査等はあるのでしょうか。

A18-1：　原則加入は任意であり、企業から入りたいと言われれば断る理由はないため入っていただくことがほとんどである。企業の加入に対しては、警察の方から勧誘という形で、「こういう協議会がありますが入会しませんか」という形で勧誘活動を行っている。関連する企業については警察署内で、県全体のサイバーセキュリティを向上させるためにはこの事業者にも入ってもらった方がいいのでは、ということで事前に調べた上で勧誘活動を行っている。（佐藤様）

Q18-2：　断ることもあるのでしょうか。
A18-2：　断ることはほぼないと思うが相手方による可能性はある。（佐藤様）

Q19-1：　現在、宮城県、宮城県警が入っている枠組みは他にはあるのでしょうか？
A19-1：　国以外だと、SC３に加入している。また、東北地域サイバーセキュリティ連絡会に加入している。（佐藤様）

Q19-2：　SC3 や宮城のセキュリティ協議会についてどのような役割分担、意義づけがされているのでしょうか
A19-2：　SC３については中小企業、サプライチェーンリスクの軽減・企業の情報セキュリティリスクの低減、サイバーセキュリティ対策の促進が主たる目的である。その点が宮城県サイバーセキュリティ協議会と違う点だ。また、地域について限定されていることから、地域の特色を活かした、情報共有を図ることが出来るということが違うと思う。（池田様）
　宮城県サイバーセキュリティ協議会が県内企業で構成されているため、情報提供する内容は県が関係するものが多い。東北地域サイバーセキュリティ連絡会は、東北 6 県の情報や取り組みの共有やセミナーを実施している。SC3 はサプライチェーンに関して全国規模で情報共有を行っている。（佐藤様）

Q20：　協議会を都道府県につくるに当たり、現状気になっている点、課題点、仮に設立するとしたら注意した方がいい点等を、お二人からお伺いできれば幸いです。
A20：　県と県警が主体となりサイバーセキュリティ協議会というものを持っていることはほぼないので、協議会という形ではないかもしれないが、お互いに連携を取った共同体のような枠組みを確立してほしい。おこがましくはあるが、その際に注意すべき点として、可能な限り業界内すべからく情報が伝わるような体制を構築してほしい。（佐藤様）
　繰り返しになり恐縮だが、最初に課題として挙げた点として、情報共有がもう少し活発になった方がよいという点がある。本県では特別支援構成員を設置して会員を引っ張る形で情報発信をお願いしているが、そういったギブアンドテイクで情報を出し合う仕組み作りが仕掛けとしてあればいいと思う。（池田様）

Q21-1：　サイバーの世界で、どちらかというと警察本部の話が出ていきますが、企業周りを担当するのは警察署の役割が大きいと思います。警察署が出来ること、経済安全保障についての警察署の役割について教えて欲しいです。
A21-1：　サイバーに特化した職員は少ない。企業とつながる点では苦労しているものの、県警で作成したサイバーに関する資料等を活用して色々な講話・集会等で注意喚起を含めた情報共有を行っている。（佐藤様）

Q21-2：　このような取り組みで県庁が前向きにやってもらえるというのは全国的に多くないですが、宮城県がやっているのは、何かきっかけがあったか、またはやる気がある人がいたというのが大きいのでしょうか。

A21-2：　当時、東京五輪で会場等の関係で力を入れていた背景があり、サイバーセキュリティ対策に力を入れなければいけないという流れがあった。その中で一緒にやっていこうという話が県警からあった。それで、当時の担当が頑張って作り上げたと聞いている。（池田様）

Q22：　本研究において私は警察機関がロボットを使ってサイバー空間をパトロールし、企業のウェブサーバー等の脆弱性を拾い出し、必要に応じて、県警のサイバー部隊の方から注意喚起と改善指導するような仕組み作りについての政策提言を考えています。その場合、宮城県警様においては、企業のサイバーセキュリティの脆弱性を改善指導することは可能でしょうか。
A22：　実際の問題としてWEBサーバーにセキュリティホールがあったという書き込みがあった場合に、県警のサイバー課等が注意喚起を行っている。これに準ずる形において現行体制で対応可能である。（佐藤様）

Q23-1：　以前経産省のサイバーセキュリティ課に話をうかがった際、地方の中小企業の意識が低くて課題だと感じていると聞きました。県ではそういった問題意識を感じることはあるのでしょうか。
A23-1：　企業と話す上では意識が低いとは感じない。ただ、セミナーに参加する企業は意識が高い。参加しない企業をどのように促すかが問題だ。（佐藤様）

Q23-2：　どのような取り組みをすればいいでしょうか。
A23-2：　検討中である。（佐藤様）

Q23-3：　口コミで広がればいいと思うが、一筋縄ではいかないのではないでしょうか。
A23-3：　口コミで拡散されるといいと思うが、なかなか難しいと感じる。もちろん、企業はサイバーセキュリティ対策をすべきだと考えているものの、人材面や費用面で難しいと考える企業もいる。そこをいかにして盛り上げていくかが課題と感じる。（佐藤様）

Q24-1：　サイバーセキュリティ課では、サイバーセキュリティお助け隊サービスやサイバー保険等で中小企業の意識を高めたいと言っていたが、実際このような、経産省の出しているサービスの普及状況はどのようなものでしょうか。
A24-1：　県警の方でもどこまで普及しているかは把握していないが、サイバーセキュリティお助け隊サービスやサイバー保険といったサービスについては承知している。それらサービスの仕組みについては協議会の中で周知している。今月もセミナーで周知しようと考えている。（佐藤様）

Q24-2：　宮城県サイバーセキュリティ協議会には中小企業の連合会や業界団体が構成員として名を連ねています。経産省でもこのような横串の団体がいることでサイバーセキュリティ協議会が活性化しているということを聞きましたが、宮城県サイバーセキュリティ協議会でも意識の広がりや構成員の拡大が見られたのでしょうか。
A24-2：　設立当時から業界団体に声かけをしており、そのような効果を期待している。（佐藤様）

Q25：　個人情報については情報漏洩した場合に報告を行う義務があったかと思います。企業のサイバー攻撃被害についても義務化をしていければいいのではないかと思っていますが、何か意見があれば教えてください。

A25：　防犯情報とはいっても個人情報である。宮城県警の方でも、被害についての注意の呼びかけ等を行っている。特定の企業が被害にあっているということもある。そういった場合にはそうした情報について資料を出す場合には、その事業者の了承を取った上で、さらにどういった資料を作るのかについても了承をとるようにしている。今後、この枠組みがもう少し簡素化されていけばいいのではないかと思っている。（佐藤様）

Q26-1：　協議会のメンバーには大学なども入っているが、例えば大学の研究室などと連携やセミナー等アウトリーチ活動はやっているか。

Q26-1：　大学の研究室では専門的に研究をしているので、協議会でも情報を提供していただくことがある。実際、協議会に大学は参加しており、事務局レベルで大学の教授に成果や拡散したい情報を会員に共有していただいている。（佐藤様）

Q26-2：　研究室でなくてもセミナーという形で中高生に対してもイベントがあるのでしょうか。何か取組が活発に行われているのでしょうか。

A26-2：　協議会の方でも委託をしており、サイバーセキュリティの講話をしている。オンラインで講話をするといったこともやっている。

　大学での講義についても県警の方では職員を派遣してやっている。問い合わせが在れば調整して行っていきたい。（佐藤様）

Q27：　宮城県サイバーセキュリティ協議会と東北地域サイバーセキュリティ連絡会の中で情報共有等の繋がりがありましたら教えていただければ幸いです。２点目として、東北地域ではおそらく宮城県のみが宮城県サイバーセキュリティ協議会のような枠組みを構築しているが、東北地域サイバーセキュリティ連絡会に参加された際に、宮城県サイバーセキュリティ協議会を構築していてよかった点等がもしありましたら教えていただければ幸いです。最後３点目として、池田様にご質問なのですが、県警様においては経済安全保障というワードはおそらく日々出ていると思うのですが、県庁等行政機関の中で経済安全保障というワードを聞かれることがあるのか、また県庁様が発信することがあるのか教えていただければ幸いです。

A27：　東北地域連絡会に入った経緯については、当連絡会が設立するにあたり、宮城県ではサイバーセキュリティ協議会を開催しているということで、先方から会員になりませんかという話があった。互いの情報共有にも有効だということで、会員として加入させてもらった。これまでにも何回かセミナーの開催があり、オンラインではあるもののその席上で各地域の担当者の方と様々な情報を共有できている。例えばその地域によって特色のある対応や、その地域の事務所・事務局ではこういった対策をとっているとか、こういうセミナーを開催したという話が出れば、宮城県でも参考にして今後開催しようかな、といった形で情報共有だけではなく様々な面でも協働している。（佐藤様）

　県庁全体としてこういったキーワードを幹部等の間で挙げられていることは聞いているが、経済商工観光部が担当となるため、大変恐縮ではあるが、私の方で詳細は存じ上げていない。（池田様）

以上

記録作成担当者：香高優一郎

ヒアリング調査報告 No. 32 基本情報

Date	10, November 2022
Theme	Australian national security and cybersecurity
Interviewee (Person in Charge)	ASPI (Australian Strategic Policy Institute) Mr. Fergus Hanson Ms. Vahri Fotheringham
Location	ASPI's office building in Canberra
participant	（WS-C Professor）ISHIYMA Hideaki （WS-C Members）OKAMOTO Itsuki, YAMADA Mayu, MIYAUCHI Taku, KOUTAKA Yuichiro, INADA Rinka , ODA Hideo, KIDO Yukako (8 people in total)
Purpose of the Hearing	To Hear from think tanks about Australian security and cybersecurity.

(Picture)

Q and A session

Q1: In ASPI, is there a frequent flow of personnel with experience in government agencies, private companies, etc., and in their respective time periods?

A1: The Australian Public Service still tend to have a mentality that once you leave government, you're out and don't really see value in gaining expertise and other industry. There's a little bit of an exception in ASPI because it is located in Canberra, and also a Commonwealth company. We have folks who are from the government. However, there's less flow of personnel from the private sector.

Q2: What do you think is the biggest difference between a think tank like ASPI and a university or other institution?

A2: From the view of time-oriented comparison, there are differences between three organizations, government, think tanks and universities; They all deal with different issues at a different point in time. As an example, compare in the Ukraine war, at the government level it is an immediate issue that must be handle, whereas think tank gets ahead of the government by six to 12 months. In

academics, they analyze in a long-term period:10 or 20 years.

Think tank roles are to think ahead of where there might be risks or opportunities for policymakers that the government isn't yet aware of or thinking of, or not focused on. Therefore, based on the horizon analogy, implementation and practical application of the knowledge is different between academia, think tanks and government.

Q3: Are there frequent opportunities for Australian think tanks to exchange personnel between think tanks?

A3: The greatest interaction is the Think Tank to the government. Think Tank to Think Tank happens, particularly on public panels, because it is a small community. We do have that exchange, but it's more informal, and more argumentative.

Q4: As for counterattacks in the event of cyberattacks, the interpretation of international law allows only counterattacks by states. However, under the current system, Japan's Self-Defense Forces cannot protect the cyber security of private companies except in wartime.

In the case of Australia, does the legal system allow the military to protect the cyber security of private companies at all times?

Q5: In Australia, is there a system in place whereby a national agency patrols cyberspace to find cybersecurity vulnerabilities in the private sector and instructs private companies to make improvements?

No such mechanism exists in Japan. In Japan, even if the cyber security of private companies is weak, the government does not provide guidance and leaves them alone. Therefore, this study aims to make a policy recommendation to the government to introduce a cyber patrol system.

A4 and A5: During peacetime, especially in Australia, the independence of private companies is well respected. It is not the government's prerogative to mandate or enforce particular cyber practices during times of peace during times of war. The Australian Cyber Security Centre provides the private sector with the opportunity to report a cyber crime and ask for assistance but the government does not actively monitor private business online presence and vulnerabilities.

As an exception, the Defense Department might have policies in place for things to do with critical infrastructure: Water, electricity, telecommunications, banking. The legislation to support this is the Security of Critical Infrastructure Act 2018.

To sum up, Private companies are encouraged by the government to have high levels of cybersecurity, although it is not enforced.

Additional Question

Q: If a private company is attacked, will it be identified from which country it was attacked?

A: It depends on the company and what they are willing to hand over information. However, with the critical infrastructure act, some information is compulsory if it is considered to be critical infrastructure. And that's so that the ACSC can assess the vulnerability and the damage that can be done.

Additional Question

Q: Does the ACSC perform attribution?

A: Attribution normally is a political act. It would have ACSC and ASD providing technical advice and Information on where they think the attack might have come from. Then it's up to the politicians to make the determination on whether they're going to make the attribution or not.

Q6: Does Australia monitor packet streams sent to and received from outside the country?

A6: There is a legislation called the telecommunications interception and Access Act of 1979. That basically says, you cannot intercept information and communications on an Australian network that extends to 12 nautical miles outside of Australia and extends to any communication that

touches a network, which is all communications. So the answer is no. However, internet service providers, large ones of telecommunication companies like Telstra and Optus, they may be able to look at packets coming through their cables if they want to.

Q7: Is the term "economic security" used in Australia? If so, I would like to know both the general view and your view on the definition of the term.

A7: It doesn't have precise meaning in terms of how it's used in the common usage. But the strands to it, particularly in the pandemic, where there was supply chain disruption, from everything from PPE, face masks and medical equipment. So there's a spectrum of, of materials that we need to function as an economy. So I think economic security is tied up with this notion of what do we need to have access to in Australia, because we may not be able to access it for reasons of global pandemics.

The other element of this is China, is using economic coercion against a whole range of democratic states, so there's an issue there around where could China coerce us in a way that actually hurt us.

I think there's a meaning of withhold to "Economic Security."

Additional Question

Q: Is Japan a trustworthy country for Australia?

A: China is both a partner and competitor whereas Japan represents joint values and interests in trade and cultural exchange. China has proven it is willing to withhold trade and supply which can be a challenge for Australia A:

Additional Question

Q: Is Japan more reliable than South Korea and South-East Asia?

A: There's a really good empirical data on this question the LOWE poll. So they have a poll they do every year where they ask Australians, which country do you trust the most, and Japan is always at the top. So ahead of America, Japan is heavily trusted. So it's, I think the only country that is trusted more than Japan is New Zealand. But it's Japan is like very, very high in terms of public trust, and you prefer very close ties between Australia and Japan.

Additional Question

Q: Why is Japan the best country?

A: There is a lot of reasons.

When we had the war in Iraq, and Australia was being pressured by the Americans to commit forces in a more strategic and more frontline ways. It was publicly difficult because the war in Iraq was not popular in Australia. And the way they chose the government chose to intervene was partnering with Japan. Because the government thought Japan was so liked by Australia, and so trusted by Australians.

Also, there's alignment of values and principles. There's demonstrated alignment in terms of we see the world in a very similar way. If you take China as the latest example, both countries see China's big problem, and don't like being pushed around by China and the aggressiveness that China is demonstrating, we don't like it, and we're on the same page.

And trade is obviously there's been a long time. We've been trading with each other for a very long time. Japan is our largest trading partner.

Q8: Japan has a government-led information sharing framework called the Cyber Security Council, where industry, government, and academia share information on cyber security threats in an interactive manner. Does Australia have such a framework for information sharing among industry, government, and academia?

A8: The Joint Cyber Security Centers is a direct connection for industry to engage with the ACSC. The ACSC website is cyber.gov.au. It categorizes the resources for individual, small business, large business, and they give different education material for different categories. For example, for large business, they have the essential eight, which is the eight things to do to make sure your business

is secure.

Additional Question
Q: Is there a system of information sharing between academia, the private sector and government on cyber chains and supply security in Australia?
A: There is not a set Framework about sharing threat information however, all with academia, business government, that is fed into by lots of different people.
There are different networks of threat sharing. For, example the banks, our banks have a network where they each share information about the threats they're seeing amongst themselves. Telstra our largest telecommunications provider and Optus, they have an informal threat sharing arrangement. There are informal networks between industry bodies.
It would be powerful if there was because for people who, or businesses who were newer, or had expanded from small business to medium or medium business to large business, it would help them prepare or be aware of current threats, instead of being caught out before they were ready.

Additional Question
Q: Is there a feasibility of an information sharing system?
A: It is feasible, it's usually political, because it may be sensitive. The level of detail that you have available about a threat indicates your capability as a business or an organization, but as a collective, it would be powerful in a positive way.
One of the big arguments in Australia in this space is that government does not share enough with industry. Therefore, industry offered to provide all of our threat information to government, however Industry gets very little back from government. Part of that is a classification issue. There is also a cultural issue that government is not used to sharing public.

Q9: In Australia, I believe there is an obligation to notify in the event of a cyber-attack that has a significant impact on critical infrastructure. Is there a possibility of requiring notification of cyber-attack damage outside of critical infrastructure? Is there an obligation to notify if a critical infrastructure asset is attacked?
A9: Yes, there is. Under the legislation. We talked about the security of critical infrastructure act.
There's no obligation except in some areas. So for example, we have a data breach notification. Law. So if you lose personal information, you're under an obligation to notify. And it's called the Information Commissioner. It doesn't have to even be a cyber-attack, it can be if an employee accidentally shares a spreadsheet with client names on it. That's a data breach. It can be both a malicious attack and a human error situation and there's obligations to report that. However, that's the only obligations we have regarding these the private sector.

Q10: Is the private sector in Australia more aware of cyber security measures?
A10: In the past month, as you would know Australia has suffered multiple data breaches.
There was no news channel that wasn't talking about this. So I would say with a confidence that every business has seen what can happen and that we need to have more Cybersecurity Awareness. But it is impossible to say because the government has no mandate to make questions toward industries. I would say that given the level of media around the recent instances Australian private sector would be more aware than ever of the risk severity compose.

Q11: Are there any countries that you use as references when promoting cyber security measures?
A11: The United States on standards, therefore very commonly referenced. Also, Japan is another one that’s seen as technologically advanced attempting to try some different things such as IOT.

Additional Question
Q: What do you find wrong with Australia's cybersecurity? What policies would you recommend to the Government?
A: Any policy or any improvement that the government should release, I would like to see being trifold. So three elements, individuals, business for economic prosperity and Defense. As individuals, make

them increase their cybersecurity awareness and practices. With regards to economic prosperity, we want to make sure that businesses small, medium and large uplift their cybersecurity measures. And finally, with regards to defense, our larger critical infrastructure needs to be prepared for increased aggression, definitely by China, and other states, such as North Korea, which can conduct ransomware attacks ransoms in order for to supplement revenue. We need to work with like-minded countries like Japan, United States, India. Others to call out China more often.

Additional Question

Q: What are the good points of Japanese cyber security?

A: One advantage is Japan speaks a language that no other isn't spoken by a lot of other countries, which makes it a bit harder to become an English speaker can't break into a Japanese company system.

Japan was looking at create an integrated secure network layer for IoT devices that was going to be sort of separated off. It is a highly secure approach to IoT development.Telecommunications industry is still largely owned by Japanese companies. Japan has a close relationship between the companies and the government, which provides a nice opportunity to provide directions.

Reporting Officer: Kajiyama Kei

ヒアリング調査報告 No. 33 基本情報

Date	10, November 2022
Topic	Interview on Cyber Security
Interviewee (Person in Charge)	（Australian Government Department of Foreign Affairs and Trade） Mr. CRAIG GILLIES, Director of Cyber Cooperation Ms. Michelle Hughes, Assistant Director – Southeast Asia, Cyber Cooperation （Australian Government Department of Home Affairs） Ms. Izzy Cox, Assistant Director, North Asia
Location	RG Casey Building, John McEwen Crescent, Barton ACT 0221 Australia
Participants	（WS-C Professors）ISHIYAMA Hideaki, TUBOHARA Kazuhiro, （WS-C Members） ODA Hideo, KOTAKA Yuichiro, YAMADA Mayu, OKAMOTO Itsuki, INADA Rinka, KIDO Yukako, MIYAUCHI Taku、KAJIYAMA Kei (10 people in total)
Purpose of the Interview	To hear about Australia's server security law policy and compare it with Japan's cyber security law system.

(picture)

Q1: In promoting international cooperation, what are your concerns about Japan in terms of cyber security?

A1:

<DFAT>

Speaking from the DFAT, we do not have any concerns. We work with Japan through the QUAD and the partners of the blue pacific initiative to coordinate on capacity building in cybersecurity skills for the Indo-Pacific. Therefore, we would like to continuously build a long-term relationship.

<Department of Home Affairs>

From the Department of Home Affairs, we've seen Japan take several extensive programs and policies to uplift its cybersecurity and critical infrastructure security. The Department of Home

Affairs collaborates closely with the Government of Japan particularly the National center for Incident readiness and Strategy for Cybersecurity. We believe both of our countries take these issues seriously.

Q2: What are your expectations for Japan in terms of cyber security when promoting international cooperation?
A2:
<DFAT>
Australia's priority is to make sure we coordinate and that we don't have conflicting activities where we're trying to do the same thing in the same place or give opposite messages to each other. Australia funds capacity building in southeast Asia and the pacific. Also, Japan has goals and programs for capacity building in the same region. Japan is a trusted partner and a like minded country toward capacity building in South-Asia and the Pacific, so we look forward to continuing that type of cooperation.
<Department of Home Affairs>
QUAD Senior Cyber Officials' Group is a key mechanism where we can work multilaterally with Japan, India and the United States to uplift cyber security within the Indo-Pacific. We would like to work closely together, to enhance the development of supply chain risk management, software security and a cyber workforce.

Q3: Please tell us about any cyber security measures that Australia is working on that you would like to recommend to Japan.
A3:
<Department of Home Affairs>
Australian Government has taken two significant actions recently. First is, establishment of dedicated Minister for Cyber Security. It was announced that the Minister for Cyber Security, the Hon Clare O'Neil MP is leading the development of Australia's new cyber strategy. This strategy includes building cyber resilience through industry partnerships and engagement. It will be developed in consultation with industry and the international community. Also, the cyber strategy is looking at international norms and standards and the role of critical technologies and economic opportunities within the cyber ecosystem.
We've also undertaken several reforms to the Security of Critical Infrastructure Act 2018. Reforms include a mandatory incident reporting scheme. It means the entities of critical infrastructure assets must report certain types of cyber security incidents. Significant incident must be report mandatory within 12 hours and if it's a relevant incident within 72 hours. That's something which has been an international exemplar for the rest of cybersecurity throughout the world.

Additional question related to Q3: Which authority is attributed the decision to be released in public?
<DFAT>
Our attribution is a collaborative effort. In every case we consider whether it is in Australia's national interest to make an attribution. There is collaboration between the Department of Foreign Affairs and Trade, Department of Home Affairs, the Australian Cyber Security Centre, and others. Therefore, we share information amongst each other and decide based on advice including legal advice, and then we have approval from the Minister for Foreign Affairs and Minister for Cyber Security, so it's signed off at that higher level before we make in public.

Q4: Are there any legal regulations regarding the elimination of cybersecurity risks on the supply chain, for example, the elimination of the risk of a back door in the manufacturing process of telecommunications equipment for telecommunications carriers? Moreover, how do you make the second and third subcontractors deal with the cyber security.
A4:
<Department of Home Affairs>
In terms of supply chain management, there's a number of pieces of guidance that the government

provides to businesses who procuring critical technologies or cyber security equipment or software. Australian Cyber Security Centre has cyber supply chain guidance which is publicly available on their website, and that assists businesses to consider what they're using within their supply chains.
Secondly, the Department of Home Affairs in 2021 released the Critical Technology Supply Chain Principles. It helps governments and businesses to decide about the suppliers of their critical technology products. These principles were co designed with industry.
These principles and the guidance are voluntary for industry, but they do assist industry when making their decisions.
<DFAT>
It is difficult for business to grasp 2nd and 3rd layer supply chain, therefore it's so important to educate industry about what their supply chain looks like and where vulnerabilities are, and what are the alternatives.

Q5: In Australia, is there a system in place whereby a national agency patrols cyberspace to find cybersecurity vulnerabilities in the private sector and instructs private companies to make improvements?
A5:
<Department of Home Affairs>
There's quite a few obligations. Firstly, there's a register of critical infrastructure assets, which the government keeps. Then there's the mandatory cyber incident reporting. We have a reporting portal which is cyber.gov.au, so that's a website where people can go and report an incident.
Other parts of the reforms, industry must put in place a risk management program. Company or an entity must look at the risks to cyber incidents within their company and then come up with a program to deal with them.
Also, the most important assets are what we call systems of national significance.
These are the systems of national significance which are the most essential to Australia's social and economic security: Electricity grids, telecommunications network and things like defense and national security. They have additional obligations and that means that they must undertake some additional cyber activities which includes cybersecurity exercises and having response plans and undertaking vulnerability assessments. Therefore, depending on how important these entities are to Australia, they then must do more things because the impact would be potentially catastrophic to our society if that piece of infrastructure goes down.

Q6: What initiatives are in place for cooperation between the State and the private sector with regard to cyber security? We would also like to ask about how such initiatives have been promoted and what problems they are currently facing.
A6:
<Department of Home Affairs>
We need to have strong collaboration between the public and the private spheres.
The Cyber and Infrastructure Security Centre (CISC) engages with critical infrastructure providers with what's called the Trusted Information Sharing Network (TISN). The TISN is for industry and government to come together and to engage with each other and to enhance the security and resilience of critical infrastructure.
In terms of the private sector, with the development of Australia's cybersecurity strategy and so many others.
The Australian Government have a very open and transparent consultation system where people can submit, their views to help inform our policies.
Australia's cyber security strategies undertake formal submission opportunities, and we meet with industry hold workshops and seek views of people throughout the community as well.
<DFAT>
Also, an important way that our department and our branch work with industry is in our capacity building programs. With our grant funding we give grant money to industry partners, and they carry out capacity building in the Indo-pacific on behalf of Australia so they might engage in technical cybersecurity skills. We rely on them and their expertise to then help build the skills and resilience

of our partners as well.
We also talked to other countries in the region, for example through a program with the Australian National University called the cyber boot camp.
We run a five-day course where we talk about matters including our relationships with industry.Through those kinds of training programs for policymakers and cyber security office from our partner governments, we can explain how we have had success not just through these technical opportunities but also through the development of our strategies.

Q7: In Japan, under the Cyber Security Basic Act, there is a government-led cyber security information sharing framework called the Cyber Security Council, which is a collaboration between industry, government, and academia. Does Australia also have such a framework for information sharing on cyber security through cooperation among industry, government, and academia? In addition to cyber security, if there is any other information sharing between industry, government and academia in the area of security, we would appreciate it if you could let us know.

A7:

<DFAT>

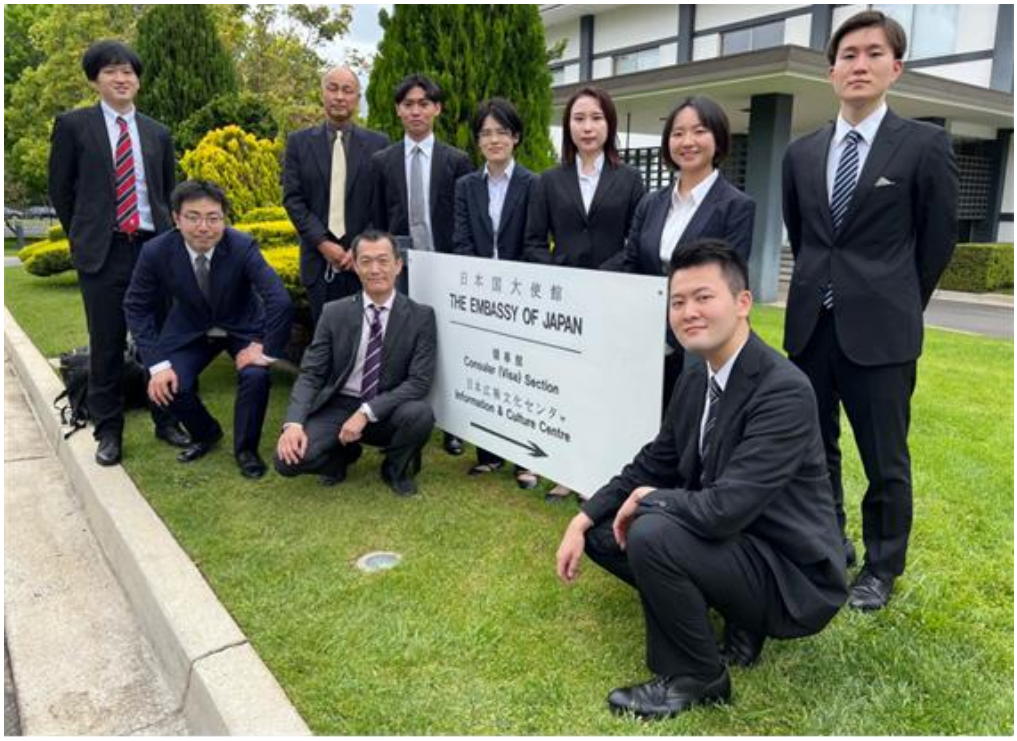
Australia doesn't have a cyber-Security council like Japan as a standing counsel, it's generally formulated based on continuous consultation. Through the ACSC Partnership program where entities, whether they are government industry academia, not for profit partner with the ACSC, they can receive information at different layers.
One of the big issues associated with sharing information is about regulatory or legislative or litigation, litigation threats. ACSC is not a regulating authority, there's one of the big concerns is that the ACSC Provides threat information and then a company takes that information on purpose. That doesn't happen because they know as soon as that happens the information flow stops.
We've got really large companies that may have a lot of cyber security capabilities or ability to protect their critical infrastructure, but then we've got small to medium organizations that maybe don't have as much information or understanding of this steps that they need to take. So that's why it's so important that entities or the Australian Cyber Security Center releases guidance for industries and business so that they can be educated about what they must do to uplift their cyber security capabilities. It's good that we have a regime within Australia, within the Australia government that's focused not only on implementing laws and powers, we also seek to work with industry and also educate them on the risks and how to mitigate those risks as well.

Reporting Officer: Oda Hideo

ヒアリング調査報告 No.34 基本情報

日時	2022 年 11 月 11 日
テーマ	オーストラリアのサイバーセキュリティ政策について
ヒアリング先 (担当者)	在オーストラリア日本国大使館 一等書記官 佐竹紘彰 様
場所	在オーストラリア日本国大使館
参加者	(WS-C 教授) 坪原和洋 教授、石山英顕 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 (計 10 名)
調査目的	オーストラリアのサイバーセキュリティ体制と各種施策、最近のトピックについてお聞きすること。

(写真)



【レクチャー】

1. 重要インフラ保安法(2018 年制定、2021 年改正)について

a. 2018 年重要インフラ保安法の概要

日本でも、基幹インフラの事前審査登録制度が設立されたものと承知しているが、オーストラリアにおいては、安全保障上の観点から重要インフラの保安を確保するための法律として、2018 年に"Security of Critical Infrastructure Act 2018"(SOCI 法、以下「重要インフラ保安法」)が成立している。

同法は 2021 年と 2022 年に 2 回改正が行われており、これらの改正によりサイバーセキュリティに対する重要インフラ防護の向上等が図られている。

b. 2018 年の重要インフラ保安法の経緯

この法律の目的は、豪州の重要インフラについて、悪意ある行為者や他国の関与により引き起こされる妨害といった安全保障上のリスクの管理を目指すものだ。

2018 年に同法が制定された時点では、対象範囲となる重要インフラは限定されており、電気・ガス・水道・港湾を対象とする法律としてスタートした。

重要インフラ保安法では、国家安全保障の観点からこれらの対象となる重要なインフラ資産を登録させ、安全保障上のリスクを伴う事案が発生した場合には政府支援として内務大臣に必要な指示を行う権限を与えた。

c. 2021 年改正法の概要

2021 年末、重要インフラ保安法について、サイバーセキュリティ・インシデントへの対応を強化するための法改正を行った。これは、近年のサイバーセキュリティに関する事案の発生状況等を踏まえ、重要インフラにサイバー攻撃が加えられた際に重要インフラの所有者・運用者がかかるインシデントに対して確実な対応がとれるようにするため法制化に踏み切ったものである。

d. 2021 年改正法の経緯

豪州では、 近年、 重要インフラに対して以下のような事象が発生している。

ⅰ. この数年間、 豪州連邦議会ネットワークを狙ったサイバー攻撃が何度か発生している。

ⅱ. COVID-19 が 医療分野に与えた圧力を悪意ある者が利用し、医療機関や医学研究施設がサイバー攻撃の標的になった。

ⅲ. 食料品や医薬品を輸送する主要なサプライチェーン企業も標的になった。

このような民主主義の根幹を揺るがし、人命にも関わり得る事態が発生したことに伴い、政府は、 「2021 年セキュリティ法改正（重要インフラ）」により既存の重要インフラ保安法を改正し、 重要インフラの定義を大幅に拡大するとともに、関連するサイバーセキュリティ・インシデントへの対応の強化を図るための規制の枠組みを導入した。

e. 2021 年改正法の内容（要旨）

2021 年改正法の主な内容は、 i. 定義の拡大、ii. 積極的なセキュリティ義務、iii. 政府支援（介入）の３項目で構成されており、それぞれの要旨は次のとおり。実際の法適用の詳細な条件は法律及び下位法令（規則）に規定されている。

ⅰ. 定義の拡大

従前の重要インフラ保安法に規定された重要インフラ保安法の対象となる 4 部門（電気、ガス、水道、港湾）を以下の 11 の部門、 22 の重要インフラ資産のクラスに拡大。

⑴通信部門（電気通信資産、 放送資産、 ドメインネームシステム）
⑵データ保存 処理部門（データ保存又は処理資産）
⑶金融サービス・市場部門（銀行資産、 年金資産、 保険資産、 金融市場インフラ資産）
⑷水・下水道部門（水資産）
⑸エネルギー部門（ガス資産、 電気資産、 エネルギー市場運営者資産、 液体燃料資産）
⑹ヘルスケア・医療部門（病院）
⑺高等教育研究部門（教育資産）
⑻食品 食料品部門（食品・食料品資産）

⑼輸送部門（貨物インフラ資産、 貨物サービス資産、 港湾資産、 公共交通機 関資産、 航空資産）
⑽宇宙産業部門（防衛産業資産）
⑾防衛産業部門（防衛産業資産）

現在多くの重要インフラがネットワークに繋がり、相互に依存していることを踏まえ、サイバー攻撃が加えられることで国民生活に大きな影響を及ぼすリスクのある重要インフラの部門を広く同法の対象として定義に加えている。

実際に、対象となる範囲は従前の重要インフラ保安法と比較すると非常に広く規定されており、例えば、エネルギー部門は 2018 年重要インフラ保安法で定義された 4 部門のうち 2 部門を占めていた電気資産とガス資産に、エネルギー市場運営者資産、 液体燃料資産を加えて 4 資産をまとめて 1 つの部門として新たに定義し直されている。また、広い意味で社会生活のインフラとなる食品・食料品のような部門までが、実態を踏まえて重要インフラとして規定されている。

ⅱ. 積極的なセキュリティ義務

⑴重要インフラ資産の登録

重要インフラ資産のうち、連邦政府が法令で規定する条件を満たすものについて、連邦政府に対する登録を義務付ける。（注：従前の法律でも規定されていた項目であるが、対象が拡大された重要インフラ資産に対しても、下位法令で規定される資産について同様の登録義務が課せられたもの。）

⑵サイバーセキュリティ・インシデントの報告

重大な又は当該資産の可用性に影響を及ぼし得るサイバーセキュリティ・インシデントが発生した際には速やかに（注：インシデントの程度に応じて、発生認知から報告までの期限が具体的に規定されている。）報告を行う義務を課す。

ⅲ. 政府支援(介入)

法令で規定される条件を満たす社会的・経済的安定、防衛又は国家安全保障に重大な影響を及ぼし得るサイバーセキュリティ・インシデントが発生して、かつ当該インシデントへの対処について、連邦政府や州・準州の既存の制度による適切な対応が見込まれない等の状況が発生した場合には、連邦政府が介入し、内務大臣がその対応を指示する権限を与える。

f. 執行

本改正法は 2021 年 12 月に公布されており、重要インフラ資産の登録には 6 ヶ月間、サイバーセキュリティ・インシデントへの報告義務には 3 ヶ月間の執行猶予が設けられた。現在、猶予期間が終わり、重要インフラ資産のうち下位法令（規則）で規定されたものに対して、本法改正に基づく義務が課されている状況である。

2.「2022 年セキュリティ改正(重要インフラ防護)」(2022 年 4 月 2 日公布)

a. 2022 年改正法の概要・経緯

2021 年 11 月の重要インフラ保安法改正に続き、 翌年 2022 年に同法の更なる改正を行っている。2021 年改正ではサイバーセキュリティ・インシデントが発生した後の報告義務や政府支援について規定がなされたが、2022 年セキュリティ改正では、インシデントが発生する前に対応策を講じてインシデント発生リスクを低減し、その防護能力を高める趣旨の規定がなされている。

なお、本改正で想定されているリスクについては、サイバーセキュリティに起因するリスクのみならず、サプライチェーンや災害等に基づくリスクも広く重要インフラに対する脅威として捉えられ、これらの脅威に対抗するための制度として設計されている。

法改正が二段階に分けられたのは直接的には議会審議が理由である。元々は一つの法改正としてパッケージされて議会に提出されていたが、議会での委員会審議において利害関係者への聴講会や意見募集を行ったところ、規制が厳重であることや、その立法プロセスの不透明性等について業界等から意見が提示され、これを受けて委員会から分割が提言されたもの。

このため、サイバーセキュリティ・インシデント報告義務等の緊急で処置すべき内容については2021年改正で法制化し、事前の対策に関する改正事項については改めて業界と相談しながら時間をかけて改正が行われたもの。

b.2022年改正法の内容（要旨）

2022年改正法の内容は、 i. リスク管理プログラム、ii. 国家的重要性を持つシステムの宣言、iii. 強化されたサイバーセキュリティ義務、iv 情報共有規定の改善の4項目で構成されており、それぞれの要旨は次のとおり。実際の法適用の条件の詳細は法律及び下位法令（規則）に規定されている。

ⅰ.リスク管理プログラム

重要インフラの所有者及び運用者に、重要なサービスの提供に影響を与える 脅威に対するリスク管理プログラムの策定を義務付ける。 当該プログラムは、既存の規制の枠組みを基礎として可能な限り業界と協力して設計される。

ⅱ.国家的重要性を持つシステムの宣言

重要インフラ資産のうち、最も相互接続性及び相互依存性が高いシステムを「国家的重要性を持つシステム」として宣言する権限を政府に付与。

ⅲ.強化されたサイバーセキュリティ義務

宣言された国家的重要性を持つシステムの所有者及び運用者に対し、政府との関係性強化を中心としたサイバーセキュリティ義務を強化。

ⅳ.情報共有規定の改善

規制対象事業者と政府が義務を遵守するために必要な情報共有を容易にする ための情報共有規定の改正。

3.法適用の流れ(通知義務及び情報活用)

2021年改正法後の 「2018年重要インフラ保安法」 等における サイバーセキュリティ・インシデント報告義務については、 一元的に豪州サイバーセキュリティ・センター(ACSC) に対して報告を行うことが規定されている。

上記の法令に基づく通知義務が課されていない場合であっても、 ACSC は、全ての個人、 中小企業、重要インフラ関係者及び政府機関に対し、 サイバーセキュリティ・インシデント又はサイバー犯罪が発生した場合に、 ACSC の ウェブページ(Report Cyber) を通じて報告することを強く推奨している。

実際に、2021年法改正に基づく報告義務が施行される前の2020年7月～2021年6月（2020年度）の期間において、 ACSC は67,500件以上のサイバー犯罪に関する報告を受けている。

ACSC は、 当該報告を統計的に取りまとめ、 分析を加えた 「年次サイバー脅威レポート」 を毎年公開している。 2021年度のレポートは2022年11月初旬に公表されており、サイバー犯罪については全体で前年度比13%ほどの増加率となっている。これは、2020年度は8分に1回のペースでサイバー犯罪が起きていたが、2021年度は7分に1回のペース

に上昇したことを意味し、このようなサイバー脅威の情勢を受けて、同レポートでは国民や企業等に警戒を促す記述が散見される。
国民や企業等が ACSC に報告することで得られたサイバーセキュリティ・インシデント及びサイバー犯罪に関する情報は、このような「年次サイバー脅威レポート」の形で取りまとめられ公表されている他、国民や企業等向けに、サイバー脅威情報やツールの脆弱性等に関する警告をウェブページ上で公表するなどして活用されている。

4.オプタス(OPTUS)社による個人情報流出事案
a.概要
2022 年 9 月 21 日に発覚した史上最大規模のデータ漏洩事件。豪州第 2 位の移動体通信事業者であるオプタス社が サイバー攻撃により、豪州の全人口が 2500 万人の中、顧客約 1,000 万人の個人情報が流出したことが判明した。
事案発覚以降、 複数のメディアにより多くの関連する報道がなされているところであり、同年 9 月 30 日までに次のような報道がなされた。

ⅰ.オプタス社と豪州政府は、今回の事案を引き起こしたハッカーとされる者の手口の巧妙さについて、 意見が一致していない。 同社は高度なサイバー攻撃の犠牲 になったと主張するが、 オニール内務大臣 (兼サイバーセキュリティ担当大 臣)は、この攻撃は 「基本的 (basic) なもの」と表現し、 同社のセキュリティの 低さを批判した。
ⅱ.また、同大臣は、インタビューに対し、「オプタス社は、個人情報に関するデータを盗めるように、ドアを開けたままにした。」と批判した。

b.2022 年プライバシー法改正 (法執行及びその他の手段) 法案の提出
上記への制度的対応のひとつとして、豪州政府では、個人情報を取り扱う企業等の責任を強化することが必要であるとして、1998 年プライバシー法の改正の議論が起こった。その結果、同法に基づき適用される、 重大又は複数次にわたるプライバシー侵害に対する最高罰金を現行の 222 万豪ドルから、以下のいずれか大きい額に大幅に引き上げられた。
ⅰ.5,000 万豪ドル
ⅱ.侵害行為により得られた利益の 3 倍の額、
ⅲ.関連期間における企業の調整後の売上高の 30%
この対応は、同年 9 月 21 日に事案が発生してから、わずか 1 ヶ月後の 10 月 20 日に同法改正が法務省からアナウンスされており、連邦政府内の関係省庁が相互に連携し、かなり迅速に対応がとられている。

5.メディバンク (Medibank) 社による個人情報流出事案
a.概要
2022 年 10 月 20 日、 国内最大の民間医療保険会社であるメディバンク社が、 同社が保有するデータを盗んだと主張する犯罪者から身代金の脅迫を受ける事案が発生した。事案発覚以降、 オプタス社事案と同様に、本事案も複数のメディアにより多くの関連する報道がなされているところであり、同年 11 月 10 日までに次のような報道がなされた。

(10 月 21 日の報道)
ⅰ.最初期、この攻撃の犯人は、盗んだ顧客 100 名の記録のコピーをメディバンク社に送り、 同社への圧力を強めた
ⅱ.盗まれた 「非常に具体的な」 データには、顧客が診断された病名や処方された治療法などのコードが含まれている。これには、 性的健康、 癌などの深刻な診断、

女性が人工妊娠中絶を行ったかどうか、 精神疾患や薬物乱用の治療を受けたかどうかなどに関する深い個人情報が含まれる可能性がある。

ⅲ. この 100 件の記録は氷山の一角と考えられており、盗まれた 200 ギガバイト のデータは現代ではそれほど大きいものではないが、記録の特殊性から極めて重大なプライバシー侵害であると言える。

（11 月 10 日の報道）

ⅳ. 11 月 2 日、身代金交渉は決裂し、ハッカーは行き詰まりと表現した。11 月 5 日、メディバンク社の代表は、 要求に応じないこと、身代金を支払ってはいけないという豪州政府の方針に従い、 このことがもたらす影響を理解する旨を送った。

ⅴ. 11 月 9 日、犯人がメディバンク社のシステムから盗んだと思われる顧客データを含むファイルをダークウェブ上で公開した。

b. 事案への対処

11 月 7 日、メディバンク社は、犯人に対して身代金を支払わないと通知し、豪州政府はこの判断は政府の助言と一致するものとして支持。（注：その後、11 月 9 日に顧客データ等がダークウェブ上で公開されたものの、12 月 8 日、オニール内務大臣兼サイバーセキュリティ大臣は、「ハッカーは身代金の支払いを受けることができないと判断し、残りのデータを破棄して立ち去ったという状況にある。流出されたデータはセンシティブな内容であったが、これが広く出回ったことを我々は確認していない。我々はいじめっ子に立ち向かい勝利したのだと捉えている。」旨をメディアで発言。）

【質疑応答】

Q1： 厳しい内容の法律を導入する際には世論を味方につけることは大切なポイントと考えます。そういった点において、サイバー攻撃被害のニュースを大々的に取り上げているオーストラリアは、メディアが上手く反応してくれているように伺えます。日本とオーストラリアの違いはありますか。

A1： サイバー攻撃によるオプタス及びメディバンクの個人情報漏洩事案は、人口約 2500 万人の豪州で潜在的に 1000 万人分の個人情報が漏洩した事件であるため、自分の情報がどこかで悪用されてしまうかもしれないという危機意識もあり、国民の大きな関心を集めたのではないか。また、大手携帯キャリアや保険会社のような身近な大企業からこのような大規模な個人情報漏洩事案が発生したことも、この関心の高さを後押ししているものと思う。

放送局や主要紙などがこぞって本事件を連日報道しているが、この状況については、国民の関心を反映したものなのではないか。さらに、今回の両事案の発生をきっかけとして、サイバーセキュリティに対する国民の関心が一層高まったようにも思える。日本では、現時点でここまで大きなインシデントが発生していないだけという見方もできるかもしれない。

Q2： 通信の秘密に対する考え方が日本と異なると思いますが、通信傍受による情報収集について通信の秘密に関わる部分の法的な環境は日本と比較してどのような違いがありますか。

A2： 豪州では、1979 年の電気通信傍受法（TIA 法）や豪州保安情報機構法（ASIO 法）など、過去から法執行又は国家安全保障上の目的で、通常では認められない手法にて通信コンテンツにアクセスする際の根拠となる法整備がなされており、多くの種類の令状や認可規定を有していると言われている。他方、多くの権限（法適用の例外）が規定されている一方で、これらの活動がその目的に沿った形で健全に行われるよう、通信の傍受・アクセスを行う際には令状取得などの手続きが存在し、また、本権限の行

使状況については年次報告を行いその透明性を高めているほか、これらの権限に基づく活動を含むインテリジェンス機関の活動を監視する独立監視機関が設置されているなど、幾重にもセーフガードが設けられている。

Q3： ACSC にサイバー攻撃に関する事例紹介や注意喚起を行うような枠組みは存在するのでしょうか。

A3： 法律に基づく枠組みではないが、ACSC のウェブページ上にはセキュリティ脅威情報（アラート、アドバイザリ等）を掲載するページが存在しており、事例紹介や注意喚起も行っている。また、ACSC の会員登録を行うと、脅威情報をタイムリーに通知するメールを受領できるようになるサービスも存在する。

Q4： 日本で産業スパイが確認された場合は、警察から個別に注意喚起を受ける等あるが、豪州には情報保全に関する制度があるのでしょうか。

A4： 豪州は、情報保全の制度として、セキュリティ・クリアランスの制度が整備されており、豪州政府安全保証審査局（AGSVA）がその運用を行っている。当該制度では、資格のレベルが 4 段階定められており、それぞれの資格のレベルに応じてアクセスできる機密情報のレベルが異なっている。また、政府以外の民間企業の職員においても、資格のレベルによってはセキュリティ・クリアランスの資格を取得しているケースもあると承知している。

Q5： セキュリティ・クリアランスを破った場合の罰則はどのようになっているのでしょうか。

A5： セキュリティ・クリアランスの資格を取得する際には、申請者は事前に誓約書を記載する必要がある。ここで、公務上の情報保全に関して法律の適用がなされること、及びこれに違反した場合には刑事訴追の責任を負う可能性があることが明確にされている。罰則の程度については、扱う情報のビジネス影響レベル（BILS）によって異なり、その詳細は AGSVA が所管する保護セキュリティ方針フレームワーク（PSPF）に規定されている。

以上

記録作成担当者：木戸友香子

ヒアリング調査報告 No. 35 基本情報

Date	11, November 2022
Topic	Interview on Critical Minerals
Interviewee (Persons in Charge)	Australian Government Department of Foreign Affairs and Trade Ms. Medina HAJDAREVIC, Director of Critical Minerals Mr. Brett ELMER, Assistant Director of Critical Minerals
Location	RG Casey Building, Department of Foreign Affairs and Trade, John McEwen Crescent, Barton ACT 2600, Australia
Participants	(WS-C Professors) ISHIYAMA Hideaki, TUBOHARA Kazuhiro (WS-C Members) INADA Rinka, OKAMOTO Itsuki, ODA Hideo, KAJIYAMA Kei, KIDO Yukako, KOTAKA Yuichiro, MIYAUCHI Taku, YAMADA Mayu (10 people in total)
Purpose of the Interview	To talk about Australia's strategy of critical mineral resources and cooperation with Japan.

(picture)

Q and A session

Q1: I think Japanese companies perceive risks in Australian environmental regulations. What do you think about something like this?

A1: The Australian Government is continuing to promote Australia’s world-class environmental, social and governance (ESG) standards. It has provided more resources to Standards Australia, linking dedicated government support with industry experts to set standards. The Federal Government is also working with states and territories to develop a critical minerals ethical certification scheme, further improving the quality of Australia’s critical minerals to the global

market.

Please refer to the following links.

https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook47p/ReformAustraliasEnvironmentalLaw
https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook47p/ClimateChangeEmissionsReduction
https://www.dcceew.gov.au/climate-change/emissions-reporting
https://minister.dcceew.gov.au/plibersek/speeches/national-press-club-address-minister-environment-and-water-tanya-plibersek
https://www.csiro.au/en/work-with-us/industries/mining-resources/Resourceful-magazine/Issue-22/CO2-technologies-set-to-deliver-low-emissions-for-mining-operations

Q2: Australia and your states enforce laws such as Mining Act, Environmental Protection Act, Foreign Acquisitions and Takeovers Act 1975, but what do you see as their challenges?

A2: Please refer to the following links.

https://www.industry.gov.au/mining-oil-and-gas/minerals/regulating-offshore-mineral-exploration-and-mining
https://www.austrade.gov.au/land-tenure/land-tenure/mining-and-mineral-exploration-leases
https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook46p/EnvironmentalLaw
https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/Vis/Seminars_and_Lectures_2022-23/SamuelReview
https://firb.gov.au/sites/firb.gov.au/files/2015/11/FIRB-Annual-Report-2009-10_Chapter_3.pdf
https://firb.gov.au/general-guidance/fact-sheets
https://firb.gov.au/general-guidance/australias-foreign-investment-policy
https://firb.gov.au/keynote-address-afr-infrastructure-summit-21-november-2022
https://firb.gov.au/about-firb/news/legislation-updates

Q3: What countries process and refine REEs in Australia?

A3: Currently, no countries (including Australia) process and refine REEs in Australia. However, Australia is investing in this capacity. In April 2022, the Government approved a $1.25 billion loan through the Critical Minerals Facility to Australian company Iluka Resources, to develop Australia's first integrated rare earths refinery in Western Australia.

Please refer to the following links.

https://www.minister.industry.gov.au/ministers/king/speeches/speech-australianpwc-critical-minerals-summit
https://www.wa.gov.au/government/announcements/australias-first-integrated-rare-earths-refinery#:~:text=Perth%2Dbased%20company%20Iluka%20Resources,investment%20decision%20earlier%20this%20week.
https://lynasrareearths.com/projects/
https://iluka.com/operations-resource-development/resource-development/eneabba
https://www.iluka.com/engage/eneabba
https://hastingstechmetals.com/projects/yangibana/
https://asm-au.com/dubbo-project/dubbo-project-overview/

Q4: We would like to know about the current and future state of relations with countries that refine REE.

A4: Australia and Japan have both provided strong support to Lynas Rare Earths, the last rare earths producer outside China.

Please refer to the following links.

JARE Supports Lynas' Development with Additional Equity Investment | 双日株式会社 (sojitz.com)
https://ministers.treasury.gov.au/ministers/jim-chalmers-2022/speeches/address-australian-critical-minerals-summit-sydney

https://www.foreignminister.gov.au/minister/penny-wong/speech/speech-nfacr-dinner-commemorating-50th-anniversary-australia-china-diplomatic-relations

Q5: What is the current situation regarding the securing of REE in Australia? In particular, please tell us about technological improvements and expansion outside of your State.

A5: In September 2022, State-owned Japan Oil, Gas and Metals National Corp (JOGMEC) and Japanese trading house Sojitz Corp have invested $9 million to buy an additional stake in Lynas Rare Earths to help the Australian miner's expansion project.

Please refer to the following links.

Japan's JOGMEC, Sojitz invest $9m in Lynas - MINING.COM

https://www.minister.industry.gov.au/ministers/king/media-releases/new-laboratory-support-new-era-earth-sciences

https://ecat.ga.gov.au/geonetwork/srv/eng/catalog.search#/metadata/146354

https://www.austrade.gov.au/international/invest/opportunities/resources-and-energy

Q6: What is Australia's perception of Southeast Asian countries?

A6: Deepening Australia's engagement with Southeast Asia is a priority. We are linked by choice. We seek to listen and understand your perspectives on the shared challenges we face and how we can meet them together. ASEAN and ASEAN-led institutions hold the centre of the region and Australia supports the ASEAN Outlook on the Indo Pacific. We want the countries of Southeast Asia to exercise their agency in how the region is reshaped. We seek a strategic equilibrium in which countries are not forced to choose sides and can make their own sovereign choices.

Please refer to the following links.

https://www.dfat.gov.au/geo/countries-economies-and-regions

https://www.foreignminister.gov.au/minister/penny-wong/speech/statement-asean-australia-ministerial-meeting

https://www.foreignminister.gov.au/minister/penny-wong/speech/special-lecture-international-institute-strategic-studies-shared-future-australia-asean-and-southeast-asia

https://www.foreignminister.gov.au/minister/penny-wong/speech/keynote-address-kuala-lumpur-malaysia

Q7: I would like to ask about Australia's current and future mining operations in Southeast Asian countries.

A7: Lynas Rare Earths is the key Australian critical minerals company operating in Malaysia.

Please refer to the following links.

https://www.austrade.gov.au/australian/export/export-markets/industries/mining-equipment-technology-services

https://lynasrareearths.com/lynas-malaysias-economic-impact-report-2021/

Q8: What support do you provide to mining companies and others?

A8: As announced on 21 October, the Australian Government Federal Budget will commit new funds to accelerate growth of Australia's critical minerals resources and industries to support new clean-energy technologies as part of the Government's commitment to achieving net-zero emissions.

The Albanese Government is investing in critical minerals, such as lithium, cobalt, manganese, titanium and rare earths, to make sure Australia can build on its world-class resources sector, diversify global supply chains, and meet growing demand for batteries, electric vehicles and clean energy technology.

Please refer to the following links.

Budget boost for Northern Australia and critical minerals | Ministers for the Department of Industry, Science and Resources

https://www.industry.gov.au/mining-oil-and-gas/minerals/critical-minerals/supporting-critical-minerals-projects-australia

https://www.ga.gov.au/scientific-topics/minerals/investing-in-australian-mineral-exploration/publications-and-portals

https://www.industry.gov.au/publications/critical-minerals-strategy-2022
https://ecat.ga.gov.au/geonetwork/srv/eng/catalog.search#/metadata/133857
(Japanese) Australian Energy and Minerals Resources Investor Guide 2020:
https://d28rz98at9flks.cloudfront.net/133857/133857_02_0.pdf
https://www.exportfinance.gov.au/how-we-can-help/our-solutions/critical-minerals/
https://naif.gov.au/about-naif-finance/
https://www.csiro.au/en/work-with-us/industries/mining-resources/resourceful-magazine/issue-22/rare-earths-and-critical-minerals-provide-significant-opportunities-for-australia
https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/CSIRO-futures/Energy-and-Resources/Critical-energy-minerals-roadmap

Q9: I heard that Japan is competing with China and South Korea in securing mineral resources. What kind of competition do you face with other countries in the field of securing resources?

A9: Critical minerals, including rare earths, are crucial components of low-emissions technologies, such as batteries, electric vehicles and solar panels.

Australia has some of the world's largest reserves of critical minerals. Building on the sector by generating new downstream industries and diversifying global supply chains will help Australia and its partners to meet net zero commitments.

Australia is the world's largest lithium producer, and latest figures forecast the value of lithium exports are due to increase more than 10-fold over two years, from $1.1 billion in 2020-21 to almost $14 billion in 2022-23, with export volumes expected to grow steadily in future years.

As well as lithium, we are the world's top producer of rutile (titanium) and the second largest producer of zircon and rare earth elements. Australia also has the world's largest reserves of rutile (titanium), zircon (zirconium) and tantalum. Our reserves of critical minerals like antimony, cobalt, lithium, manganese ore, niobium, tungsten and vanadium, rank in the top five globally.

Please refer to the following links.

https://ministers.treasury.gov.au/ministers/jim-chalmers-2022/speeches/address-australian-critical-minerals-summit-sydney
https://www.minister.industry.gov.au/ministers/king/speeches/speech-australianpwc-critical-minerals-summit
https://www.theaustralian.com.au/commentary/critical-minerals-a-chance-to-secure-future-lead-world/news-story/b347bde8ff1d06e8739978c5e64603fc

Q10: Collaboration with Quad countries on supply chain resilience is underway, including the IPEF, the Japan-Australia Summit, and the Japan-Australia-India SCMI. How do you plan to collaborate with Japan in the future? What are your expectations for Japan?

A10: Japan is a key collaboration partner for Australia. In October 2022, our Trade Ministers committed to working together and with other partners to address regional economic challenges, including the rise of protectionism, non-market practices and economic coercion. Ministers confirmed the importance of strengthened cooperation on economic security and enhanced resilience, including through robust economic architecture, trade diversification and supply chain security. Japan-Australia Ministerial Economic Dialogue | Minister for Trade and Tourism (trademinister.gov.au)

In October 2022, Australia and Japan signed a new partnership on critical minerals to help build secure supply chains for critical minerals, which are crucial elements of clean energy technologies needed to help both countries meet net-zero commitments.

The new Critical Minerals Partnership was signed by Minister for Resources and Minister for Northern Australia Madeleine King and Japan's Vice Minister for International Affairs, Ministry of Economy, Trade and Industry Hirohide Hirai during the Australian visit of Japan's Prime Minister Kishida.

The partnership will establish a framework for building secure critical minerals supply chains between Australia and Japan, and promote opportunities for information sharing and collaboration, including research, investment and commercial arrangements between Japan and Australian projects.

The partnership will support the further development of Australia's critical minerals sector, to ensure Japan has the supply of critical minerals required for its advanced manufacturing sector. Please refer to the following links.

Australia-Japan strengthen critical minerals cooperation | Ministers for the Department of Industry, Science and Resources
https://www.pm.gov.au/media/media-statement-perth
https://www.pm.gov.au/media/opening-remarks-australia-japan-business-leaders-lunch
https://www.pm.gov.au/media/australia-japan-strengthen-critical-minerals-cooperation
https://www.pm.gov.au/media/australia-japan-leaders-meeting-joint-statement
https://www.pm.gov.au/media/opening-remarks-australia-japan-leaders-meeting
https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook47p/AustraliaJapanRelations

Q11: What is the impact of those international collaboration on the field of actual securing?
A11: Please see above answer and below links.
https://www.minister.industry.gov.au/ministers/king/media-releases/australia-joins-global-minerals-security-partnership
https://www.dfat.gov.au/trade/agreements/negotiations/aifta/australia-india-ecta-outcomes/australia-india-ecta-benefits-australian-critical-minerals-and-resources-sectors
https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/outcomes-resources-and-energy
https://www.dfat.gov.au/about-us/publications/trade-investment/business-envoy/business-envoy-february-2022/clean-hydrogen-collaboration-japan
https://www.dfat.gov.au/about-us/publications/trade-investment/business-envoy/business-envoy-february-2022/australia-and-singapore-propelling-our-sustainable-green-economy-future

Q12: I understand that China is the only country with the technology and facilities to not only mine mineral resources but also to process (such as refine) them, and that China processes the majority of REE. Did you consider the fact that China is responsible for most of the processing of rare earths as a challenge? Is this an issue for your office?
A12: See links provided for Q9.

Q13: I would like to ask about the current status and future prospects for REE recycling.
A13: In the rare earths sector, Australia is currently only involved in mining and beneficiation stages of the lengthy and complex rare earths supply chain.

Reporting officer: Kotaka Yuichiro

ヒアリング調査報告 No. 36 基本情報

Date and Time	15, November 2022
Topic	Outline of Security among US, Australia and Japan
Interviewee (Person in Charge)	Chief Executive Officer, United Stares Studies Centre Dr Michael J. Green
Location	Institute Building (H03), City Rd, University of Sydney NSW
Participants	(WS-C Professors) ISHIYAMA Hideaki, TSUBOHARA Kazuhiro (WS-C Students) INADA Rinka, OKAMOTO Itsuki, ODA Hideo, KAJIYAMA Kei, KOTAKA Yuichiro, KIDO Yukako, MIYAUCHI Taku, YAMDA Mayu (10 people in total)
Purpose of the Interview	Understand what the problems about national security among US, Australia and Japan are.

（Picture）

Lecture

Some have argued that Japan is behind Australia in economic security, but in fact Australia is behind Japan in many respects, and so is the United States. For Japan, after World War II, its economy was its security. The Yoshida Doctrine basically saw economic security as the source of Japan's economic recovery: in the late 1980s, people were talking about economic security, and at the time, US academics and officials thought Japan had the most sophisticated economic security strategy in the world. Because, as the term 'total security' suggests, in the 1980s and 1990s, the Japanese Government was very focused on how to use its economic power for national security, and the US side was a bit

afraid of Japan: according to a 1988 national opinion poll, Americans were more afraid of Japan than of the Soviet Union's nuclear weapons. They feared the Japanese economy. In other words, Japan has long implemented economic security measures.

In fact, Japan's economic security dates back to the Meiji era. Wealth and strength are economic security. In other words, Japan has a long history and economic security has been highly developed over more than 150 years.

In recent years, the Abe Government has become increasingly concerned that China may use economic means of coercion, pressure the country with boycotts, steal technology or attempt to control emerging technologies, as confidence in Japan's economic strength has declined. As a result, the Japanese Government began to focus more on economic security: in 2013, when the Abe Government formed a National Security Council structure and national security personnel, and also announced its first National Security Strategy, economic security became very strong After China embargoed rare earths, Huawei's investment and Japan lobbied the US Congress and administration to co-operate, for example, in coordinating semi-conductor manufacturing, and the concept of economic security was promoted. The Ministry of Economy, Trade and Industry (METI) played a particularly important role. Measures such as investment reviews, the CHIPS and Science Act (commonly known as the CHIPS Act), semiconductor export controls and, especially during the Abe administration, the Free and Open Indo-Pacific. These are economic security measures, investing in infrastructure in Southeast and South Asia to ensure that China's One Belt One Road initiative does not dominate and create neo-imperialist states, for example. Almost all of these ideas originate from Japan, including METI and the Abe administration.

The US has traditionally had a very liberal market view, which has met with resistance. The Treasury Department is strongly opposed to industrial policy and when the US does regulate exports, it is usually not for economic security, but for defense and national security. Investment reviews, or so-called CIFIUS, are narrowly aimed at preventing the domination of military technology by China and other countries. This is because traditionally the US has had a belief in free markets and most of the US economic security strategy has been free trade agreements and market opening. Of course, there was some US-Japan friction, but the bulk of the US strategy over the past 70 years has been to open markets and reduce barriers. This is because, in the 1930s, the closure of markets led to war. For the Americans, economic security meant opening markets and reducing barriers. Ideas such as investment screening, strict export controls on commercial technologies such as semiconductors and infrastructure financing were new to the US authorities, and from the US perspective, Japan has an intellectual contribution and leadership role to play with regard to economic security.

The same applies to Australia. Australia is a central founder of the Cairns Group and the WTO, and as an exporter of agriculture and natural resources, it is very opposed to trade barriers. And Australia's economic security depends on open markets. So it could be argued that both the US and Australia have moved in Japan's direction. But there is not much about that in the Japanese media. This is because economic security is perceived as external pressure. This is the first point.

In contrast, there are two areas where Japan lags behind the US and Australia: first, cyber security. Japan is a decade behind the US and Australia in cyber security, and the second is information security. Fujitsu and other Japanese companies do a very good job of protecting information. However, in the dual-use sector - the defense industry - the Japanese Government and Japanese companies lag far behind the US and Australia in protecting and securing information. This is undoubtedly an obstacle to cooperation on AI and hypersonic dual-use technologies. In short, Japan certainly lags behind in cybersecurity and information. However, in the free and open Indo-Pacific region, Japan was ahead of the US and Australia in infrastructure financing, investment screening, regulating semiconductor exports and blocking Huawei. However, these were underwater actions. METI was very clever, and while the US and Australia blocked Huawei with laws, official documents, etc., Japan seems to have made use of administrative guidance as well as legal reform.

On economic security, the first point I have made is that cyber is a separate part of the economic security policy I have described. Because much of it is new. And much of it is dependent on administrative guidance. In the US, the Biden administration announced on 6 October that it would

impose strict export controls on semiconductors destined for China, but a year before that, the White House had called Tokyo Electron, ASML and Western Digital and given them administrative guidance. This was due to the Trump administration's lack of a legal framework.

The second point is that the legal basis for overall economic security is taking shape in the US and Australia, albeit half-heartedly. In the US, the CHIPS and Science Act (commonly known as the CHIPS Act), the Inflation Control Act for investment in wind and solar power, China's very active strategy of intellectual property theft, the 6 October US executive order restricting semiconductor exports, Australia's ban on Huawei use, etc. Various bills have been passed. Some legislation has been passed in Japan, but not much.

In addition, both the US, Australia, Japan and the EU have inconsistent and mish-mash institutional designs. Very difficult for companies. Private companies need clear laws and regulations. Companies like Fujitsu and Tokyo Electron need a consistent legal and regulatory framework because they do a lot of business in the US. The lack of one puts them in a difficult position. However, when talking to managers from Japanese companies like Tokyo Electron, Fujitsu and Hitachi, they understand that decoupling is taking place. This is common in manufacturing and technology companies.

The public in Australia, the US and Japan were surveyed about decoupling from China: in all three countries, less than 20% were in favor of full decoupling, but a majority were in favor of technical decoupling. The main reason for this is that under Xi Jinping's government, China has placed more emphasis on security than on the economy, and the separation of politics and economics has collapsed. The 20th Party Congress and Chinese regulations mean that free markets do not work in China. The government will impose strict regulations to control data and damage technology companies in Japan, South Korea and the US, partly due to the majority's poor economic policies for the lockdown at COVID19. A further factor is that the US, Australia, Japan, South Korea and now Taiwan and Germany also regulate investment and exports.

Another challenge associated with China is supply chain security. The Chinese market is very important, with approximately 26% of Japan's exports going to China and 40% of Australia's exports going to China. It is therefore very difficult to completely decouple them. The US also exports about 15% of its total to China, making complete decoupling almost impossible. The Americans want to export soybeans, import toys and access China's middle-class consumer market. However, it is clear that decoupling is the trend for anything related to AI and semiconductors. In other words, economic security is happening faster than governments are prepared for. And the framework, legal and regulatory framework in the three countries - the US, Australia and Japan - is incomplete.

Finally, there is no doubt that the three countries with the most influence in defining this framework are the USA, Japan and Australia. The survey shows that these three countries are very closely aligned and that intergovernmental agreement is very high. South Korea is also important, and Taiwan is very important. Germany, France and the UK are also important, but there is no clearer agreement than between the US, Australia and Japan.

Q and A session

Q1: Is the term 'economic security' often used in Australia, or is the same thing expressed in different terms? Moreover, when have these sets of measures been adopted in Australian policy?

A1: The word 'economic security' is used more often in Japan because Japan has a sense of economic security crisis and a Minister for Economic Security, but it is not generally different from the Australian view. When the Australian Strategic Policy Institute (ASPI) talks about economic issues, it considers economics as a tool for security. I think ASPI is the first think tank to actually think about economics for economic security.

Q2: What is the significance of the concept of 'economic security' in your opinion? We would be particularly interested to know from the respective perspectives of the US and Australia.

A2: I will tell you two things that economic security should not be: one, economic security should not

just be the Ministry of Defense or the Ministry of National Security. That is too narrow. In other words, it is too narrow to just protect technology needed for military purposes. More than the MoD, MoD leaders know that to compete militarily to win on the battlefield, they must take a much broader view and think for themselves about technology, including information technology. In the Pentagon's view, the most important technology on the battlefield in the next 50 years will be AI - AI is not a technology developed by weapons manufacturers such as Lockheed Martin or Boeing, but by Silicon Valley and others. It is therefore too narrow to define economic security only in the traditional military sphere.

On the other hand, economic security that is too broad is dangerous and can lead to protectionist rent-seeking and interest groups. That was the problem when Japan announced comprehensive security in 1980. In the US, economic security means everything. Educating children is economic security, so budgets for education must be increased; growing crops to feed people is economic security, so government support for soya beans and carrots is necessary. If everything is economic security, then in the end it is the same as nothing.

In other words, the correct definition of economic security is right in the middle between a definition that is too narrow militarily and a definition that is too broad in everything. I think the Biden Government, and the White House, have done a pretty good job of defining it.

The Democrats and the Australian Labor Party tend to think that economic security extends to everything. However, Biden and the White House issued a statement on economic security in June that clarified the definition. Essentially it is technology policy, but in reality it is economic security, with a focus on AI, IoT, semiconductor manufacturing, materials, hypersonics and biotechnology. These are all important areas. We feel that these are areas where the Government should focus its economic security efforts. Japan's definition is very similar to this. These areas are important in future economic and military competition. The US, Japan, South Korea and Taiwan have a 10-15 year advantage over China in semiconductors. It is therefore important to defend it and maintain the lead.

When I was a student, there were those who perceived Japan as a major challenger to the US in economic security. They were worried that Japan would dominate the US. People in the State Department and the Pentagon said: 'Japan is an ally. Japan is an ally and we share common democratic values." they said. But those on the other side said: 'Japan's METI is trying to dominate the US'.

A new economy emerged in the late 1980s. This new economy was based on semiconductors: in 1986-87, DRAMs were very high-tech. However, DRAMs were perceived as commodities and were not considered important in the 1990s. When governments try to identify important technologies, they sometimes look backwards rather than forwards; DRAM became a problem because it became commoditised. There was a need to innovate in newer areas.

Another point on economic security is that governments may be making the wrong measures and choices: the Biden White House statement on technology security in June 2021 was very much a US protectionist policy. If the US, Australia, Japan and South Korea had an economic security strategy, it could reduce the influence of protectionism. Cooperation with developed countries would also give them a better chance to identify what will be important technologies in the future. In short, economic security requires a definition that is neither too narrow nor too broad, and the identification of key technological areas for innovation, such as AI, that will dominate economic security. And it needs allies. Without allies, protectionism will increase, leading to a narrower rather than comprehensive view of what economic security is all about.

On cyber security, Japan still needs to catch up on the cyber security sector. When Prime Minister Abe came to power, there were probably some 20,000 to 30,000 US government officials, CIOs and industry representatives working on cyber security in the US. The Japanese Government, on the other hand, had only 60.

Q3: What are your views on human resources in economic security measures?

A3: Human resources are a major issue. However, our think tanks are staffed by leading experts in defense technology and economic security. They not only analyze problems, but also have a new approach to proposing solutions. In addition, we are basically trying to find a drop-off point

between industry, government and academia for economic and security measures. So it attracts excellent people.

However, Australia has a problem. The Australian Department of Defense needs 1,000 more people than it has budgeted for. The Australian Defense Force needs 3 000 people. This is a big challenge for Australia, and the same for Japan. Perhaps the biggest obstacle to building advanced technology etc. is human resources. As Australia is an immigrant society, it can attract Indians and Koreans. However, it is difficult for them to have the high-tech expertise to be useful in the civilian and military spheres, and Australia would be reluctant to teach the latest submarine, nuclear propulsion or hypersonic technology to an engineer who only arrived from China two months ago.

This is therefore a major problem for Australia. Thanks to AUKUS, Australia is rapidly moving into technology areas such as nuclear power, guided weapons, missiles, engineering, aerospace, and wind, solar and zero-emission energy strategies. However, in the US, the Inflation-Reduction Act (IRA) has been passed, with huge budgets for wind, solar and batteries. Thus, the best talent is going to the US for higher remuneration. How to recruit talent in Australia is a constant topic of discussion.

Around 1990, Japan also had this problem. There were not enough software engineers in Japan. Most of the best software engineers employed by Japanese companies were from South Korea. The Japanese Government did not want to accept a large number of Koreans, so it prepared a special visa for software engineers to come from a country with a large number of software engineers but not a large number of companies. That country was Ireland, where hundreds of Irish software engineers came to Japan between 1987-91. Such a strategy may be required in Japan today.

Q4: What could you tell us about think tanks in the US and Australia?

A4: There are 1,000 think tanks in Washington DC. Sydney has seven or eight, and Canberra has ten, which is a completely different size. The US administrative system is one of checks and balances. There are Congress, the courts and the executive, and Congress in particular needs a lot of expertise. And when the administration changes, they want to bring in political appointees. It is thanks to the federal system, a system of checks and balances, that thousands of Americans, like myself, move from Congress to think tanks and government companies. However, in a unitary parliamentary system such as Japan or Australia, there are not many personnel changes. The courts also do not challenge the government very often. Parliament also does not often investigate or pass legislation separately from the government. So there are fewer jobs for people moving from think tanks to government, and they are smaller in size.

Nevertheless, the Australian government wants more expertise from think tanks. They are very interested in what we do because Australia does not have enough human capital. The US Government provides considerable funding for think tanks. We also receive a lot of funding from the Australian and NSW governments.

But I don't think the Japanese Government gives much money to think tanks. They give money to the Defense Research Institute and the Institute of International Affairs of the Ministry of Foreign Affairs, but they don't give much money to independent think tanks like the Yoichi Funabashi Think Tank. Such think tanks will have to raise funds from companies. In addition, tax laws are very strict in Australia and Japan. Think tanks in the US can get a lot of funding from foundations created by wealthy people, and the scale is totally different because universities and think tanks get a lot of money.

In my view, think tanks in Japan and Australia will become increasingly important. This is because global issues like economic security are horizontal, but governments are designed vertically, and think tanks can cover different areas across government and industry.

Q5: What could you tell us about cyber security?

A5: With regard to the US and the EU, one of the main factors that enabled them to take China to the WTO for cyber IPR damages was that US and EU companies shared such information with their respective governments.

When the US and EU subsequently visited Japan, Japanese companies did not share information

on cyber attacks. METI and the police cooperated in sharing information, but the Keidanren did not want to share information. The reason for this is essentially a matter of reputation. This involves the dilemma that Japanese companies have to share information with the government to protect themselves, but fear losing face if it is disclosed or being criticized by shareholders. This is the problem of cybersecurity.

Q6: What could you tell us about US and Australian anti-spying laws and other legislation?

A6: The USA and Australia are known as 'immigrant societies', attracting the best engineers from all over the world, especially from Asia. As a result, the US and Australia remain highly competitive. However, in the US and Australia, immigrants from China and Russia, or those with family members in mainland China or Russia, are sometimes targeted and espionage cases occur. However, such cases are rare in practice. The US and Australia have been very careful: the FBI, the Department of Justice and the Australian Federal Police have begun to investigate Chinese-Americans and others in earnest.

Japan is not an immigrant society and does not have such problems. However, looking to the future, Japan will need to invite more engineers from Asia to improve its technological capabilities. The security systems that the US and Australia are building have become very sophisticated since World War II, such as the so-called 'Five Eyes'. I believe that Japan cannot develop advanced technology in cooperation with the US, Australia and the UK without improving its information security. The US cooperates to a large extent with Australia, but would not do so with Japan. Even if Japan had more advanced technology, this is because Japan's information security is too weak.

In other words, security-related information needs to be developed and the penalties for non-compliance strengthened. Failure to do so will limit Japan's economic security. The US and Australia cannot share Chinese intelligence, cybercrime, and advanced military technology in hyper-sonics and AI with Japan. Nor will they be able to develop new systems involving Japan. This is a major obstacle.

My own feeling is that the Japanese public would support the establishment of an information security regime on security. We are going to conduct a survey in Japan as part of our research, and the Japanese public would support enhanced information security if there is a functional surveillance regime.

Q7: It has been several years since the NSC and NSS were established in Japan. Do you have any future directions or issues you would like to see regarding the operation of these organizations and the Japanese Government's economic and security policy?

A7: Your question about the NSC is interesting. I worked for five years in the US NSC as a senior director and special assistant. Then, when the Abe Cabinet was formed in July 2006 and the NSC was about to be created, Prime Minister Abe appointed Yuriko Koike as National Security Adviser. I had a number of meetings with her to share my experience with the NSC in the US. She had a project team in the Prime Minister's Office with the Ministry of Economy, Trade and Industry, the Ministry of Defense and the Ministry of Foreign Affairs. When we came out of the PM residence, the Japanese Undersecretary-General of the Ministry of Finance had also left the PM residence and was at the entrance. And he said to Ms. Yuriko: 'Sir, please talk about the NSC. Would you please allow the Ministry of Finance to be part of it?" I said. Then she said, "No". I asked her why she refused the Minister of Finance, she said because they are too powerful.

In 2013, I had lunch with Prime Minister Abe at the Prime Minister's Office. He had just started Japan's National Security Council in July. I asked him if he was going to include economic security in the NSC. And he said, "That's what we want." I said. I said, "Are you going to include either METI or MOF?" He then turned to METI secretary Imai, who was at the luncheon, and said, "Is METI going to be part of the NSC?" Imai said, "I hope so, Prime Minister." I said. Neither METI nor the Ministry of Finance participated in the NSC because Shotaro Yachi, who designed the Ministry of Foreign Affairs, also designed the NSC. I told Prime Minister Abe that economic security would eventually be necessary. In the US, the NSC works with officials from the Ministry of Finance on economic security policy. This is because the Treasury Department knows a lot about export controls, exchange rates, etc. Anyway, the Ministry of Foreign Affairs did not invite

either the Ministry of Economy, Trade and Industry or the Ministry of Finance to the NSC. So what happened.

METI controlled economic security from outside the Ministry of Foreign Affairs. So when Prime Minister Abe met with Putin, METI was there. When Prime Minister Abe responded to the One Belt One Road initiative, METI was initially in charge. When Mr. Suga became Prime Minister and expanded the NSC, he included METI as part of the security policy process. So now economic security is being implemented.

Also, by and large, Japan's NSCs are functioning very well. However, the NSC always depends on the leader. Prime Minister Abe had strong leadership and therefore the NSC was very strong. Prime Ministers Suga and Kishida are not so strong politically and therefore the NSC is not very strong. This is the same in the US, where the strength of the NSC varies from president to president and prime minister to prime minister. If the Prime Minister or President has a very clear strategic vision and political support from his or her party, the NSC is very strong. However, if they do not have a clear vision, like Jimmy Carter or Obama, the NSC does not work well. Prime Minister Suga had a fairly clear vision, especially in the areas of economic security and democracy, but he did not have as much power as Prime Minister Abe. So the Ministry of Finance and the Ministry of Economy, Trade and Industry have been revived and the Ministry of Foreign Affairs has become stronger. I feel that Prime Minister Kishida has a very clear strategic vision, although it is not original and is more like an addition to Prime Minister Abe's vision. However, this does not mean that the NSC works well on its own.

These are the same in Australia. The Australian Prime Minister's Department was very strong under Scott Morrison, but now that Labor is in power, the Department of Foreign Affairs and Trade is regaining power. This is not because Prime Minister Albanese or the Labor Party do not have a strong vision, but because the Minister for Foreign Affairs, Penny Wong, has a strong vision and is becoming by far the most powerful foreign policy officer. In the previous government, the Ministry of Defense and the police had influence. Therefore, which department has power depends on the leader, his approval ratings, etc.

Q8: What are Australia's demands of Japan and the US in the area of security?

A8: We asked the Australian public, "Would Australia be safer if Australia signed a security treaty with Japan?" We conducted a survey asking people 'Would Australia be safer if Australia had a security treaty with Japan? Seventy-five per cent of people said that Australia would be safer if there was an Australia-Japan Security Treaty. Two weeks ago, Prime Minister Albanese and Prime Minister Kishida met in Perth to announce the Australia-Japan Joint Declaration on Security Cooperation. This is the most significant security declaration that Australia and Japan have signed with non-US allies. The Mutual Access Agreement is the most advanced security agreement that Australia and Japan have with a country other than the US.

This means that Japan has high expectations. These trends are also good for the US-Japan alliance. We don't know if China will become more powerful, but it already has enormous power, especially military power, and it is very aggressive. US allies Japan, Australia and South Korea are increasingly dependent on the US. The same thing is happening in Europe and Ukraine; NATO is quite dependent on the US. Thus, in Japan, Australia and South Korea, opposition to the Security Treaty is declining.

At the same time, however, Japan, Australia, South Korea and European countries are calling for independent diplomacy. In Australia, about 75% of the population support the US-Australia Security Treaty, and another 75% want independent diplomacy. Similarly in Japan, 70% of the population support the US-Japan Security Treaty and 70% want independent diplomacy. This is basically about sovereignty.

Last night, the Defense minister gave a speech in which he said of sovereignty: 'We must increase Australia's defense spending. We must build more capability. We need more advanced weapons and technology. We have to protect our sovereignty". He did not say from where he would defend it, but obviously from China. The reason he did not say China was because Prime Minister Albanese had met with Xi Jinping. In other words, Australia needs the US to gain sovereignty. The same applies to Japan. Our allies' dependence on the US is increasing day by day.

The questionnaire also asked whether Americans attach great importance to the US-Japan alliance. It also asked whether Australia and Japan make the US safer. To date, Americans have supported the US-Japan Security Treaty to protect Japan and the US-Australia Security Treaty to protect Australia. Indeed, in response to a similar question two years ago, 48% of Americans said the US-Japan Security Treaty and the US-Australia Security Treaty would make the US safer. This year, however, that percentage was 60%. They believe that Japan, as an ally, makes the US safer. In addition, the US relies heavily on Japan and Australia for force deployment, the cost of troops in the US and the defense of the First Island Line. In this context, the US is also seeking independent diplomacy. The interdependence of these countries has deepened considerably, thanks to China and, to a lesser extent, technological advances.

Therefore, if Japan and Australia gain strength and strengthen their defense and technical cooperation, they will have more influence over Washington. This is good for the US. Because thanks to China, bilateral alliances are moving step by step towards a form of collective security, such as QUAD and Orcas. At the moment there is nothing like NATO in Asia, but if China becomes militarily aggressive, we may need something like NATO in Asia. In this sense, cooperation between Japan and Australia would be desirable not only for themselves but also for the US. Step by step progress towards collective security for economic security and military security may be necessary.

Reporting officer: Okamoto Itsuki

ヒアリング調査報告 No.37 基本情報

日時	2022 年 11 月 15 日
テーマ	経済安全保障の観点から、豪州のビジネス、貿易投資環境の現状について
ヒアリング先 （担当者）	日本貿易振興機構（JETRO）シドニー事務所 宮本敬子様、青島様
場所	日本貿易振興機構（JETRO）シドニー事務所
参加者	（WS-C 教授）坪原和洋 教授、石山英顕 教授 （WS-C 学生）稲田凜香、岡本樹、織田秀夫、梶山敬生、木戸友香子、香高優一郎、宮内拓、山田麻友 （計 10 名）
調査目的	豪州のビジネス、貿易投資環境の現状や施策から、我が国が参考にできることを模索し、政策立案に反映させること。

（写真）

【レクチャー】

（オーストラリアの最新経済動向）

1. 概況

オーストラリア居住者の出生地は、約 7 割がオーストラリアで約 3 割が海外となっている。在留邦人数は約 9,3000 人で、米国、中国に次ぎ 3 位の多さである。

2022 年 5 月 23 日に労働党のアンソニー・アルバニージー氏が首相に就任し、その後、日豪首脳は日米豪印（QUAD）やシャトル外交等で連携強化を図り、両国の関係を深めている。

また、日豪関係については、令和元年度にオーストラリアにおける対日世論調査において、オーストラリアの人々が日本に対して全般的に良いイメージを持っていることが示された。2019 年の訪日旅行者数も前年比 4.4%増の 62 万人で過去最高を更新した。

2.経済動向

オーストラリアの国内 GDP 構成の特徴は、まず、金融、保険、不動産サービスなどのサービス産業を中心とした第三次産業の割合が高い。さらに、広い国土を活かし、小麦、牛肉などの農業・牧畜業も盛んである。また、オーストラリアは鉄鉱石や石炭、天然ガスの豊富な資源国である。人件費の高騰や、広大な国土や少ない人口といった物流面でのネックもあり、製造業はあまり発展していない。近年は高賃金、手厚い労働者保護によるコスト高により、すべての自動車メーカーが生産から撤退した。

貿易統計では、一次産品を輸出し、加工製品を輸入する構造となっている。輸出では石炭、天然ガスなどの鉱物性燃料、鉄鉱石などの原材料が中心となっている。一方、輸入ではコンピュータ・通信機器、乗用車などの機械・機器類、輸送用機器が 4 割を占め、また、国内生産の少ない燃料（石油）の割合が大きい。主な貿易相手国は、輸出では鉄鉱石や石炭等で、中国、日本、韓国の上位 3 か国で全体の 6 割近くを占める。輸入では機械類で、中国、米国が 1/3 以上を占める。また、対日貿易統計を見ると、輸出では天然ガスや石炭といった鉱物性燃料が 5 割以上を占め、輸入では輸送機器や貨物車が中心であり、機械・機器類といった工業製品が大半を占める。

オーストラリア経済は長期にわたって経済成長を遂げており、実質 GDP 成長率は 1991 年 7-9 月から 2019 年 10-12 月期まで 114 四半期連続で景気後退(2 四半期連続のマイナス成長)なく、世界最長を記録した。2018 年後半以降は減速傾向となっており、2020 年は新型コロナウイルス感染症の影響で 29 年ぶりの景気後退入りとなったが、足元の 2021 年は景気回復となっている。

3.トピックス

アルバニージー政権においては、まず、エネルギー政策では、国家送電網再整備計画（Rewiring the Nation）として、再生可能エネルギーの活用や、送電網の安全性の改善、電力料金の引下げを目的として国内送電網の更新や拡大を緊急で実施する。また、新エネルギー産業での投資拡大や雇用の創出を目的として、クイーンズランド州のタウンズビルでのグリーン水素拠点の設立を支援する。さらに、全国規模の電気自動車充電ネットワークの設置や、排出ゼロ車のためのインフラ整備のために追加資金を拠出する。

産業支援では、資源、農業・林業・漁業、メディカル・サイエンス、再生可能エネルギー・低排出技術などの優先分野のプロジェクト投資を行う。また、鉄道産業支援やオーストラリアでの鉄道製造を進めるための技術職の雇用支援や、各州の鉄道や道路関連プロジェクトへの投資を行う。中小企業支援として、中小企業の省エネルギー支援のための助成も行う。

4.日本企業の進出動向

日本の対豪直接投資については、鉱業部門が引き続き大きな割合を占めるも、近年は食料品、金融・保険、卸・小売等が増加している。日本の対世界直接投資先として豪州は第６位だが、豪州から見た場合には日本は第２位の投資国となっている。

現地進出企業からの回答では、投資環境上のメリットとしては「安定した政治・社会情勢」が最も多かった。その一方で、投資環境上のリスクとしては「人件費の高騰」が最も多かった。

【質疑応答】

Q1：　豪州の投資環境についてお教えください。

A1： レクチャーを参照。

Q2： 豪州はサイバーセキュリティに注力しているとの事でした。サイバー攻撃の被害にあった場合に情報を共有して欲しいといったことについての指示が出されたりするのでしょうか。

A2： 特定の法対象となる事業者については、政府への報告が義務付けられており、それを怠った場合には罰金が課される場合もある。

関連する法規制の例としては、以下が挙げられる。

・Security of Critical Infrastructure Act 2018

重要インフラ（港、ガス、電気等）のセキュリティに関する法律。対象となる事業者について、報告義務を課す。

・Telecommunications Act 1997（Telecommunications（Carrier License Conditions-Security Information）Declaration 2022、Telecommunications（Carriage Service Provider-Security Information）Determination 2022）

通信事業者に関する法律。事業者がとるべきライセンスの取得者要件の中で、報告義務を課す。報告はオンラインにて可能。

・The Privacy Act 1988

個人情報保護に関する法律で、対象企業（一定の規模以上の企業）は個人情報漏洩が発生した際には、政府への報告義務がある。なお、昨今大規模な情報流出事件が続いていることから、Privacy Act の改正が予定されている。” serious or repeated breaches of privacy” の場合の罰金増額。報告はオンラインにて可能。

Q3： 豪州に拠点を置く日本企業は、豪州の法律の支配下にあると思います。豪州に拠点を置く日本企業が、サイバーセキュリティの脆弱点を豪州政府から指摘され、改善を求められた事例はありますでしょうか。また、関連子会社がサイバー攻撃対象になり易いといわれておりますが、そのようなリスクについては、豪州に拠点を置く企業は一般的にどのような対応を取られているのでしょうか。知りうる範囲で結構ですので教えていただければ幸いです。

A3： JETRO で行っている調査を探してみたが、個別企業の情報は見つけられなかった。

Q4： 豪州における貿易関連のニュースなどを日本の JETRO と共有する体制の他に、日本の企業やシンクタンク、政府などとの情報共有の体制や連携などはあるのでしょうか。

A4： 政府との連携は随時行われている。

政府と JETRO の連携の具体例として、JETRO は経産省から毎年度運営費交付金が交付されている。そのほか JETRO の予算は、国、および自治体からの予算で成り立っており、それぞれ予算元の方針に沿った事業を運営している。政府の政策にもとづき、JETRO が、イノベーション創出・対日投資の推進、中堅・中小企業等の海外展開支援、農林水産物・食品輸出の促進、通商政策への貢献といった諸事業を行うための予算となっているが、海外事務所もこの事業予算を本部から配賦されて事業を行っている。

オーストラリア国内では在キャンベラ日本大使館や在シドニー総領事館とも連携している。例としてセミナーを共同で行うなどがあげられる。また、要人往来の際にも JETRO 事務所と大使館等が協力して対応する。シンクタンクについては委託調査などを通じて連携することもある。

オーストラリア側の政府機関との連携もしている（JETRO のカウンターパートである Austrade（連邦政府機関）や、連邦政府、各州政府等）。

Q5： 海外のビジネス情報に関するレポートがHP上で公開されているのを拝見しましたが、これらは、主に一般の方に向けて作られているのでしょうか。
A5： 海外進出日系企業や日本の政府機関などビジネス向けや一般の方向け。

Q6： オーストラリアの鉱物資源の環境規制ではどのような規制が課題になっているのでしょうか。また、現地の日本法人や鉱山会社等はそういった規制や住民問題にどのように対応しているのでしょうか。
A6： 日本が輸入する石炭の6割、LNGの4割、鉄鉱石の6割はオーストラリア産であるため、オーストラリアの資源エネルギーへの規制は日本に大きく影響する。
LNG輸出規制については、2022年6月以降、アルバニージー政権が、国内でのガス供給不足を解消するため、オーストラリア国内LNG業者に対して国内でガスが不足した際に、未契約のガスを輸出よりも国内市場へ優先して供給する「オーストラリア国内ガス安全メカニズム（ADGSM）」の発動を検討。（連邦政府がADGSMの発動権限を保有。）今年11月までに導入するか連邦政府が判断する予定だったところ、結局、9月29日にキング資源大臣が記者会見でLNG輸出規制の検討は必要がなくなったと発表し、日本に影響ない方向で解決した。理由として、予測していた不足分の3倍のガスを国内LNG事業者により供給できることになったため、としている。
また、クイーンズランド州の石炭ロイヤリティ料率の引き上げについては、クイーンズランド州政府が高価格帯の石炭に対し、石炭ロイヤリティ料率を事前に事業者への協議なく、7月1日から引き上げ。（例えば、1トン当たり150ドル以上の販売価格の石炭には15%だったところ、7月1日～20%に。）クイーンズランド州で石炭事業を行う日本企業に大きな影響、日本政府から働き掛けを行ったものの、未解決。オーストラリアの資源大手のBHPは、8月石炭ロイヤリティの引き上げを非難し、投資を止めると表明した。

Q7： オーストラリアでは半導体の不足による影響はございますか。また、なぜ豪州政府は半導体産業に15億豪ドルも投入しているのでしょうか。
A7： 半導体不足に影響は表れている。2021年JETRO日系企業調査において、オーストラリアの日系企業（製造業）が経営上の問題点として、第2位に「調達コストの上昇」という回答があげられた。この要因として、半導体不足による原材料価格の高騰の影響があると分析している。他には、コンテナ不足による海外輸送コストの増加などがあげられる。
オーストラリアの主力産業は第3次産業で、製造業が主力産業ではないため、新型コロナウイルス感染症や中国による半導体を始めとする重要品のサプライチェーン供給の途絶問題を経験し、何か問題が発生した場合でも海外に頼らず国内産業で対応する能力を保有しておくこと望ましいと考えているようだ。

Q8： 豪州は多様な国際関係を構築しており、日米豪、日豪印、QUAD、AUKUS、Five Eyesなど、様々あります。ビジネスの現場において、この国際関係により、進出する日本企業や相手先の豪州企業はどの様な恩恵を受けているのでしょうか。
A8： 各同盟国との関係が強固になることによって、同盟国においてのビジネスがしやすくなりますし、同盟国と共同して第三国市場に進出するというケースも増えてくることが想定されている。特に資源についても日本はオーストラリアに多くを依存しているため、サプライチェーンを構築する上でも関係を良好に保つことが重要だ。

Q9： 中国の、南半球にある豪州に対して直接投資や内政干渉が懸念される事態を引き起こす政策によってどの様な被害や報道が出ているのでしょうか。また、それに対する政府の規制や日本との連携の動き等を教えていただけますと幸いです。

A9： 2015年、北部準州が中国企業と、米軍駐留拠点に近い安全保障上重要な港湾であるダーウィン港の商業用港湾施設についての賃貸契約を締結した。これを契機に、連邦政府は、2015年に「外資による取得および買収に関する法律（略して、外資買収法）（Foreign Acquisitions and Takeovers Act 1975）」を改正し、外国投資に関する審査制度を整備した。2017年、中国による連邦議員への献金など内政干渉により、オーストラリア政府の対中姿勢が硬化した。2018年8月、中国企業（ファーウェイ、ZTE）の5G参入を排除、また2020年4月コロナの国際的な独立調査を要求した。また、同年、重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）を成立させ、電力、港湾、水力、ガスの4部門の重要インフラに関する外国投資に対する審査を強化した。中国は2020年以降、石炭、大麦、ワイン、牛肉、ロブスターなどオーストラリア輸出製品へ貿易制限を開始。2021年、2018年重要インフラ安全保障法の改正し、従来の4部門（電力、港湾、水力、ガス）から、通信、金融サービス、ヘルスケア、教育、宇宙産業、防衛産業等を含む11部門に拡大し、これら部門における外国投資に対する審査を強化した。

貿易・投資への影響について、中国との貿易が減少した分については、輸出先の多様化が起きており、石炭はインド、マレーシア、大麦はサウジアラビアなど新しい輸出先との貿易が代わりに増加した。なお、オーストラリアのワインメーカー・トレジャリーエステート社は、「ペンフォールズ」ワインを9月から中国内で生産開始した。シドニー大学・KPMGによる調査によると、2021年の中国の対オーストラリア投資額は、対前年比69.8%マイナスとなった。

日本と豪州の連携については、最近のトピックとして、10月に岸田首相がパースに訪問し、日豪首脳会談を実施した。その際には、中国の大洋州における動きを意識して、日豪の安全保障協力分野で新たな安全保障協力に関する日豪共同宣言を締結した。

Q10： ローウィー研究所の調査結果において豪州国民が対内投資や2020年の貿易制裁などに強い懸念を抱いているという話がありましたが、今後の環太平洋地域において豪州はどういった働きを期待されているのでしょうか。

A10： 労働党新政権は同盟国/同志国との連携を重視し、アルバニージー首相は就任直後の日米豪印（QUAD）首脳会合に出席した際、「政権は変わったが、豪州のQUADへのコミットメントは変わらない」と述べた。また、米国ペロシ下院議員訪問後の台湾周辺での中国軍事行動に対しては、G7と同様懸念を表明。

Q11： オーストラリア国内では台湾問題や米中対立に対する人々の意識は高いものがあるのでしょうか。

A11： この5年間でオーストラリアの対中認識は大きく変化した。ローウィー研究所の世論調査によると、「中国は経済パートナーか、安全保障上の脅威か」について、2015年は77%が経済パートナー、15%が安全保障上の脅威と回答したが、2022年、2022年の調査ではその割合が逆転し、2022年現在は33%が経済パートナー、63%が安全保障上の脅威と回答した。

Q12： オーストラリアでは脅威情報、たとえば警察などからアウトリーチ活動など、民間への産業スパイ等への警戒情報の共有などはなされているのでしょうか。

A12： サイバーセキュリティに関する脅威についてはACSC（Australian Cyber Security Centre）が提供する、アラートサービス（個人向け）、パートナーサービス（ビジネス向け）がある。アラートの内容は、ACSCのサイトを参照。
　警察（州）からのアラートも存在するが（例えばGeo Targeting SMS System）、行方不明者の捜索などのケースが多い。
　その他、災害情報等をふくめ、ツイッター等のSNS媒体を活用し情報拡散をしているケースも見受けられる。

Q13： 豪州における輸出入管理のHPを拝見したのですが、この輸出入管理は日本における外為法と同じような運用なのでしょうか。
A13： 日本の外為法は、各国際輸出管理レジームでの合意にもとづき規制の運用が行われている。オーストラリアも日本と同様に各国際輸出管理レジームに参加し、輸出管理を厳格に実施している国である。

（追加質問）
Q14： 外資買収法と重要インフラ保安法は重複する部分があるのですが、違いはあるのでしょうか。
A14： 外資買収法は、重要インフラ安全保障法の「国家安全保障に関する事業（National security business）」の定義を引用している。国家安全保障に関する事業に分類される事業への投資ついては、一定の条件に該当する場合、投資金額に関係なく、申請の審査を行うよう求めている。

Q15： DFATにヒアリングを行った際、向こうでも外資の対内直接投資に関してはFARBを参照するよう言われました。現地日本法人でも対内直接投資で影響が起きていることはあるのでしょうか。
A15： 日本は優良案件であり、許可が下りなかったことがないとオーストラリア貿易投資促進庁から伺った。

Q16： Q2で日本の不採択がない理由はなぜでしょうか。
A16： 日本との信頼関係によるものでもあるが、米国、韓国、欧州については却下されたとは聞かない。中国に対する投資案件では却下されるものもあると聞く。

Q17： 現代的奴隷法について、日系企業への影響はございますか？
A17： 問い合わせはあり、豪州にいる企業については意識をしているということをジェトロの日系企業調査結果から現れている。
　サプライチェーンの明示化についてはJETROで出している和訳は出しているので参照してほしい。それに対する支援として、JETROが一緒になってシンポジウム等をやっているとのことだが、現代奴隷法のウェビナーはしていない。もしかしたら、やっているかもしれないが、SCR(サプライチェーン強靭化)フォーラムやビジネスマッチングのイベントの方が多く、法律の説明については特異なものが起きたときに限られると思う。

Q18： 豪州のビジネスで人件費の高騰が起きていますが、今後このリスクが悪化するのでしょうか。
A18： なると企業は考えている。また、オーストラリア政府は、同一労働同一賃金を制度化しようとしている。日系企業は注視していると聞く。

Q19： リサーチの成果物やブリーフィングを発表していると思うがリサーチを専門にやっている研究員がいるのでしょうか。
A19： 海外事務所の調査担当がリサーチを実施。ブリーフィング資料を作ったりしている。更新調査などもしている。東京本部が指示をするときもあれば自分たちで企画レポートをすることもある。JETRO の人間がやることもあれば外部に委託することもある。JETRO 職員のほか、省庁、自治体、企業から出向している様々なメンバーがいる。

Q20： 企業と関わることでビジネス的な観点もあると思うが、民間の側面と行政の側面があるという理解が良いか
A20： JETRO は独立行政法人であり、半官半民と言われるが、省庁ではないが民間企業でもない。政策に沿って事業や調査を実施する。事業例としては、セミナーやシンポジウムの開催、ビジネスマッチングイベントの開催、個別企業支援等。政策が変われば JETRO がやることも変わる。例えば過去日米貿易摩擦の時には輸入促進を行っていたこともある。現在注力しているのは、は農林水産・食品やスタートアップ技術、伝統産品等、日本製品・技術の海外展開支援促進、対日投資誘致等。対日投資誘致事業については、日本の生産性向上に資するような技術を持った企業等、日本経済にプラスとなるような企業を誘致ターゲットとしている。そのほか、海外企業との協業連携促進事業や、これら事業すべてのベースとなるような情報収集を行っている。

Q21： サイバーセキュリティに関して、豪州のサイバーセキュリティ方に暗号化の禁止があった。民間企業が暗号をかける場合についても法執行機関等が開けられる鍵を出さないといけない。日本から関係企業がこちらに来ているか分からないが、軋轢のようなものがないかということと、警察のアウトリーチについて、ＡＳＩＯがアウトリーチ活動等の企業に対する周知活動を行っている。これらの団体が JETRO に話に来ることはあるのか。
A21： その法律についての問い合わせをもらったことは今の所ない。ビジネスに影響が出るなら可能性はあるが、今の所ない。この食品はなぜ輸出できないのかなどのミクロなトラブルの方が日頃の対応としては多い。特に事業セクションだとそう。

Q22： 政府と企業との間に JETRO が入ることで、どのような長所が、またはどのような作用があるのか？
A22： 国内の窓口では各県に事務所があり、中小企業支援をメインとしている。大企業であれば、自力でできることでも輸出が初めてでノウハウのない中小企業にはサポートが必要なことも多い。直接現地政府に質問したり交渉したり、ビジネス相手を見つけることは中小企業にとっては困難であるが、JETRO による情報提供やビジネスマッチングを役立てていただいている。JETRO の役割はいったん相談事を全部引き受けつつ、しかるべきところにつないでいく役割がある。

Q23： JETRO 様はどのような情報提供を行っていますか。
A23： 法改正があった場合や問い合わせが多い事項等、情報提供のニーズがある場合には、調査を行い、ウェブサイトでのレポート公開や短信の執筆、セミナーの開催等という形で情報提供を行っている。ただし、あくまで情報提供にとどまり、JETRO として法の解釈を行うものではない。各企業には、各分野の専門家（弁護士等）への相談を勧めている。

Q24：　豪州では外資は申請が必要とのことでしたが、日系企業にとってこれらの法律は不利益に働くと考えられますか。

A24：　日豪貿易の文脈では問題になっていない。

ただ、先般実行されたクイーンズランド州の石炭ロイヤリティの話は受け入れがたい。日本政府も申し入れ等を行っているが解決していない。日本の豪州への関心はここ数年で高まっている。

政治的にも制度的にも安定していて、同盟国でもある。連邦と州政府との間で方針の一致が取れていない場合はあるが、日本にも州政府や連邦政府の出先機関があるのである程度解決が図れるのでは。石炭ロイヤリティのように州政府が事業者に事前の協議なく突然実施することもあるものの、少なくとも外資の申請は日本にとって不利ではない。たとえば豪州飲料市場は寡占市場ともいわれるほど大手メーカーが市場のほとんどを占める状態だが、それら大手メーカーについても日系企業による買収が行われている。

以上

記録作成担当者：木戸友香子

ヒアリング調査報告No.38 基本情報

日時	2022年11月18日
テーマ	経済安全保障シンクタンクについて
ヒアリング先 (担当者)	内閣府 科学技術・イノベーション推進事務局 参事官（重要課題担当）付参事官補佐 丸林夏彦 様
場所	オンライン
参加者	（WS-C 教授）坪原和洋 教授 （WS-C 学生）梶山敬生 （計2名）
調査目的	経済安全保障シンクタンクについて理解を深めること。

【レクチャー】

1.経済安保の資料

・自律性の向上

・優位性不可欠性の確保

・国際秩序の維持・強化

協議会を中心とする経済安全保障重要技術育成プログラムやシンクタンク機能が経済安全保障推進法で規定された。

2.内閣府、内閣官房、総務省のHP

政府の資料を踏まえて内閣府担当からレクチャーが行われた後、以下の質疑応答が行われた。

【質疑応答】

Q1： この資料に書かれてある特定重要技術調査研究機関とシンクタンクは同義と考えてよろしいでしょうか。

A1： 安全・安心シンクタンクは、経済安全保障推進法に基づき内閣総理大臣からの委託を受け、特定重要技術調査研究機関としての一端を担うことが期待されている。令和3年3月に安全・安心シンクタンク機能の立上げが第6期科学技術・イノベーション基本計画により閣議決定された後に、特定重要技術調査研究機関等を盛り込んだ経済安全保障推進法が成立した。安全・安心シンクタンクの方が、特定重要技術調査研究機関よりも先に議論されていた。

Q2： 特定重要技術の研究開発の促進と成果の活用に関してはそれに参画する研究機関や研究者等に対して、安全保障貿易管理、営業秘密保護の実施、研究インテグリティなどの情報漏洩に関わる部分に対して、関係行政機関からの助言等必要な支援を行うことが求められるとのことですが、それはどのぐらいの頻度で開かれるものを想定しておられるのでしょうか。

A2： 具体的な頻度だけを検討するのではなく、協議会を活用した伴走支援や人材育成などの枠組みのほか、関係省庁が独自に行う支援を想定している。協議会には大臣も参加する。実務的な話でもあり、具体的な回数は現時点では決まっていない。回数ありきではなく、どのような形で実施すれば実効性があるのかを考える必要がある。例えば、安全保障貿易管理に関して毎週、誓約書を出してもらっても意味がない。研究者の負担と実際の実効性を考えて、アプローチの仕方を今後詰めていく。やり方に関しては協議会の中で規約などの形で詳細を決めていく。

Q3： 経済安全保障上のリスクから国民を守るための特定重要技術の絞り込みやその育

成、活用方針を検討というのが特定重要技術調査研究機関（シンクタンク）の役割であるというふうに認識しています。その際、参考にすべき技術領域として20分野が挙げられておりますがそれを参考にしつつ、最新の国内外の研究開発及び政策の動向、経済社会情勢等を踏まえ、調査研究を実施するものと規定されております。ここで言われる参考にされる政策や経済社会情勢というものはサプライチェーンやサイバー攻撃のようなものが考えられるでしょうか。

A3：　基本指針が参考として示す20分野に限られるものではなく、サイバーセキュリティやサイバー攻撃も当然に参考にしていく。海外を後追いする趣旨だけではなく、日本としての強み弱みを探していく。

Q4：　特定重要技術の研究開発のために情報共有枠組みを作り、関係行政機関が保有する機微情報を共有すると公務員と同等の守秘義務を科すことが決められていると認識していますが懸念点などはありますでしょうか。

A4：　個人的な見解だが、一番大きいと考えられるのは制度の趣旨に関して、国民への説明不足による誤解が生じている点である。守秘義務に違反すると法律による罰則の対象となるため、経済安全保障に関する協議会やシンクタンクに関与するととんでもないことになるのではないかと思ってしまう人もいるかもしれない。経済安全保障推進法に基づく守秘義務の罰則規定は公務員と同等であり、国立大学法人や国立研究開発法人の職員にもすでに同程度のものがかかっている。また、守秘義務の対象となる情報の範囲は「協議会の事務に関して知り得た」秘密に限定される。このため、研究者自らが生み出した研究成果は、例えば元の守秘義務対象とされた情報が直接的ないし実質的に了知されない限り、守秘義務の対象外となる。本制度において、研究成果は公開を基本としているものである。どのような形で研究者に説明して理解を得るのかは今後よく検討する必要があると考えており、制度の趣旨を正しく理解していただくのかが課題。制度の運用面においては、迅速な対応が可能かどうかという点である。特定重要技術の研究開発に従事した研究者が、その成果を論文や学会発表としてまとめる際に、それらの中に守秘義務対象となる情報が含まれているのかいないのか、直ちに判別が付かない場合もあると思う。そのような場合、具体的にどの機関・部署が担当するのかは検討中であるが、守秘義務対象となる情報の有無について、研究者からの求めに応じて事前の相談や確認がなされる方向で調整中である。それらの相談や確認に対してどれだけ迅速に回答できるのかと言う運用面の懸念があると考えている。

Q5：　研究開発大臣による同意の取得に関して協議会の組織にかかる同意を採択の条件にしてはいけないとありますが、これは協議会の設置なしに、重要技術の研究開発が行われることもあると認識して相違ないでしょうか。

A5：　そのとおり。経済安全保障推進法第62条に基づく協議会は置いても置かなくても良い。第63条に基づく、指定基金を用いて研究を行う指定基金協議会であれば必置。指定基金を使うか使わないかで場合分けが発生。

A6：　https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin3.pdf
　ここのp.11におけるシンクタンクに関してここで言及されているものは民間のシンクタンクや非営利のシンクタンクなども全て含めたものと解釈してよろしいでしょうか。

A6：　特定重要技術調査研究機関の具体例としてシンクタンクが挙げられている。民間企業や非営利組織であっても、内閣総理大臣から委託を受ければ、特定重要技術調査研究機関となり得る。また、p.11の同じパラグラフには「その他民間企業含む社会実装に関係するもの等」という記述もあり、民間企業や非営利シンクタンクはこの条件に

該当する可能性もある。

Q7： 研究者側において講じられる安全管理措置とは具体的にどのようなものが考えられるでしょうか。（資料 p.13）
A7： 現在検討中。全くの個人的な私案であり組織としての見解ではないが、大きく 3 つのカテゴリーに分けられると考えている。
【物理的な対策】
入退出管理システム、建物に入る際の IC カード、生体認証システム、鍵のかかる保管庫、シュレッダー
【技術的な対策】
機密性の高いデータに対するアクセス制御、データの暗号化措置、OS やウイルス対策ソフトの定期的な更新
【制度的な対策】
情報取扱ルールの作成、当該ルールを理解してもらうためのマニュアル整備、情報の取扱いに関する研修制度

Q8： 協議会による研究開発については経済安全保障重要技術育成プログラムを用いたＪＳＴ、ＮＥＤＯなどからの資金提供があると認識しております。一方、シンクタンク創設にかかる財源などは現状、どのようにして確保するとのお考えでしょうか。
A8： 指定基金を財源とするのではなく、予算要求を行う。

Q9： p.20 協議会が技術の開発段階に入っても特定重要技術調査研究機関（シンクタンク）と技術育成と積極的な活用の促進を図るために連携を図り、シンクタンクの行う調査研究に協力するということが明記されていましたが、具体的なシンクタンクの役割としてはどのようなものが想定されていますでしょうか
A9： 調査分析により特定した特定重要技術の候補を提示したり、協議会における研究開発の議論に参画したり、政策提言をしたりすることを想定している。

Q10： p.23 において調査研究機関の継続性の観点からの人材の養成を図る旨が記載されておりますが、これは具体的にどのような取り組みが想定されておりますでしょうか。例えば新卒の人材を採用して育てていくなどといったことは想定されておりますでしょうか。
A10： 新卒の方の育成は想定。どのように育てていくか。求められるシンクタンクの人材象を検討して研修教育プログラムを立ち上げることを想定している。座学だけで調査研究を行うスキルを身に付けるのは難しいため、OJT も実施する考えである。また、クロスアポイントメント制度も活用しながら、大学の学位プログラムへの参画なども考えている。経験者人材だけでなく、新卒の人材も入れてコア人材を強化していくことを検討している。

Q11： 『シンクタンクの育成は一朝一夕にできるものではなく、まずは経済 安全保障重要技術育成プログラムの実施に資する調査・分析を中心に機能を発揮することが想定される。その上で、日進月歩で進展・変化の早い先端技術分野に おいて、最新の知見を取り込みつつ継続的に一定以上の水準の調査・分析を行うため、新たな調査・分析手法の確立や関係機関とのネットワークの拡大など、シンクタンク機能の発展が求められる。』内閣府の資料 p.24 にこのような記述があります。経済安全保障シンクタンクがより立場を拡充したものとして認識を受けるためにどのような機能の拡充が望ましいと考えられるでしょうか。お見立てを伺いたいです。
A11： 全くの個人的な私案であり組織としての見解ではないが、誰（国民、アカデミ

ア、産業界など）に立場を拡充したと認識してもらうのかによって、重点を置くべき取組がそれぞれ変わると思う。
【国民に対して】
日本の政策決定に効果的に関与することが必要。そのため、例えば政府の要職にシンクタンク関係者が就任して、政府のニーズを把握する能力の拡充を図るとともに、政策提言能力や発信力を強化することなどが考えられる。
【アカデミアに対して】
シンクタンクによる研究開発プロジェクトが活発に動き、研究者自身や知り合いが当該プロジェクトに参画したり、論文や学会発表などがなされたりすることが必要。そのため、例えば最新の研究動向を踏まえた調査分析手法の開発・実践を進めるとともに、科学的根拠（エビデンス）に基づく論理的思考を追求するような組織文化を醸成することなどが考えられる。
【産業界に対して】
社会実装された技術が、日本の国際競争力や地位の向上につながることが必要。そのため、例えば科学技術だけでなく、国内外の社会情勢・経済情勢・安全保障などの幅広い視点を持つとともに、領域横断的なコミュニケーションを促進することなどが考えられる。

Q12：　「調査研究においては、将来の国民生活及び経済活動の維持にとって重要なものとなり得る先端的な技術に関して、技術面のみならず社会制度や社会システムまでを含めた国内外の情勢や研究開発動向等を適切に調査・分析できる能力を有することが求められる。」内閣府の資料 p.24 にこのように記されています。これに関して、技術面以外で経済安全保障に資するようなシンクタンクのためにはどの分野での調査能力が必要でしょうか。地政学的リスク、サプライチェーン、サイバー攻撃に関する研究などが入ってくるのではないかと考えておりますがどのようにお考えでしょうか。

A12：　そのとおりであり、地政学的リスクなども含めたあらゆる分野が必要。あわせて、状況の変化を見る柔軟な対応力も不可欠。また、例えばAI、量子技術などの重要性は万人の理解を得られていると思うが、研究開発に投入できる資源には限界があるため、状況の変化を想定した上で、分野や技術に対して総合的に優劣をつけた提言をできることが重要。

Q13：　「シンクタンクが優秀な科学者・企業関係者のキャリアパスの一つとしての立場を確立していくことが重要である」というふうに内閣府の資料 p.27 に記載がありますが、これはシンクタンクで経験を積んだ民間企業の方などが、その後、行政に携わっていくなどといったことも考えられますか。

A13：　そのとおり。全くの個人的な意見だが、シンクタンクで経験したことは、行政組織での業務との親和性も一定程度あると考えている。民間企業と行政組織では文化が異なるところもあるため、間を取り持つ人材が必要。現時点においてシンクタンクは行政機関ではない位置付けだが、シンクタンクでの経験を活用して、行政へのキャリアパスを開いていくこともあり得ると思う。

Q14：　経済安保シンクタンクに関してはキャリアパスや中長期的な視点での人材育成が重要であるという認識をしております。そのような場合、シンクタンクで調査をする研究員は基本的には普通の会社または公務員のように経済安保シンクタンクに職員として席を置き、研究を行っていくという認識でよろしいでしょうか。それとも、いずれ離れることが前提でプロジェクトごとの募集をかけていくといった形でしょうか。

A14：　両方考えている。シンクタンクに関してはコア人材を内部に抱えていないと機能しない。現在考えているシンクタンクはネットワーク型であり、国内外のシンクタンクのネットワークのハブとなる。また、優秀な人材は既に他の組織に所属している可能性が高いため、プロジェクトごとに募集をかけてエフォートを割いてもらうなど、柔軟な対応が必要と考えている。

Q15：　先端的な科学技術の見極めに際してはプログラム会議への参加やシンクタンクへの参画などがありますが、シンクタンクなどへの参画により、科学者の政策への関わり方や役割が形作られ、科学者、研究者の新たなキャリアパスの構築につながることを期待されているものと認識しております。政策への関わり方をそこで身につけた科学者や民間の方が政府に入り込み、政策の実行まで、担うという考えに関してどのようにお考えか聞かせていただきたいです。先生の本においても明治大学の田中教授が政治任用制度や幹部公務員の公募制導入の紹介がされていますが、民間出身社が閣僚の政治的意向に影響を及ぼすというための、知見を積み、政策に対する意識を根付かせる役割（官庁で働くというキャリアパスの構築）を付与できるものと考えていますがその点についてはいかがお考えでしょうか。
A15：　個人的な意見だが、科学者や民間出身者が、シンクタンクへの参画を通じて、政策に対する意識を根付かせ、政策に参画していくのは十分考えられると思う。

Q16：　特定重要技術調査研究機関においては多様な人材の知の集約点となることが求められていると認識しております。このシンクタンクには例えば非営利独立型の、そしてシンクタンク 部門を有する企業、大学発シンクタンクなどからも人材を募ることを想定されていますでしょうか。
A16：　想定している。経済安全保障推進法では、特定重要技術調査研究機関として委託を受ける際の 4 要件が定められており、1. 専門的な調査研究を行う能力,2. 情報収集・整理・保管を行う能力、3. 内外の関係機関との連携能力、4. 情報管理体制である。この 4 要件を満たす法人であれば、受託することが可能となる。また、特定重要技術調査研究機関において調査研究を進める際に、当該機関の判断により、様々なシンクタンク等から人材を雇用したり委嘱したりすることは一般的にあり得ると考えている。

Q18：　経済安全保障重要技術育成プログラムにおける規制緩和や国際標準化というのは具体的にはどのようなものを想定されていますでしょうか
A18：　内閣府 HP に掲載中の研究開発構想から例を挙げると、例えば、ドローン飛行は航空法により規制されているが、都道府県警察、国・地方公共団体又はこれらから依頼を受けた者が、事故・災害に際し、捜索、救助のために無人航空機を飛行させる場合には、無人航空機に関する規制の多くが適用されない（航空法第 139 条の 92）。その場合であっても、例えば「衝突予防の遵守」は適用除外とならないことから、被災地において有人機が低高度に下りてきて人命救助等を行う場合には、有人機と無人機の衝突を避けるため、無人機の利用は禁止され、無人機による救助活動や捜索活動が停止される状況にある。このため、衝突予防に関する画期的な技術が開発され、有人機と無人機の衝突を回避できることが技術的に実証されれば、航空法による規制の緩和に向けた議論が進められていくのではないかと考えている。また、国際標準化に関しては、衛星のコンステレーション基盤技術に関して具体的な技術を確立し世界市場で優位性を持ってルール形成等を行うことも念頭に研究開発構想が作られている。

Q19：　特定重要技術調査研究機関＝令和 5 年度に創設が目指されているシンクタンクと

いうわけではなく特定重要技術調査研究機関として委託先が様々にある中でのシンクタンクという位置づけなのでしょうか

A19： 委託先は複数あり得る。令和３年３月に閣議決定した第６期科学技術・イノベーション基本計画において、安全安心に関するシンクタンク機能の立上げが盛り込まれた。その後、令和４年５月に成立した経済安全保障推進法により、特定重要技術調査研究機関が法定化された。安全・安心シンクタンクは、特定重要技術調査研究機関の一端を担うことが期待されている。

Q20： 特定重要技術調査研究機関においては、海外の同志国の機関との協力して行っていく際には、どの情報を共有してどの情報を共有しないかの判断は必要になってくるのでしょうか。それとも全ての情報を提供するのでしょうか。しかしそれであれば日本の不可欠性が確立されないのではないかと感じています。

A20： 一般論だが、そもそも経済安全保障の取組みは、他国との関係で日本の技術の不可欠性やひいては優位性を確保するために行うもの。全ての情報を提供すると不可欠性も優位性もなくなる。どの技術を共有してどの技術を共有しないのかというのは、判断する必要がある。他国が望む何かを提供することによって、我が国が望む何かを共有してもらい、win-win の関係を築くという選択肢もあり得ると思う。

Q21： 特に、新しい才能を新しい分野で養成していくという観点から、シンクタンクが優秀な科学者・企業関係者のキャリアパスの一つとしての立場を確立していくことが重要である」ということが書かれていますがこれを実現するために必要であると考えるものにはどのようなものがありますでしょうか

A21： 個人的な意見であり、実現可能性をあまり考慮せずに述べると、3つあると考えている。

【魅力のある処遇】給与・報酬体系、複数年雇用、勤務地、社会的信用、シンクタンクのブランド・ネームバリュー

【キャリアアップ・スキルアップ】教授等のアカデミックポスト、研究予算や研究内容における裁量、研究分野をリードする優秀な研究者

【独自性】人脈、国内外の政府機関とのコネクション、海外のシンクタンクとの共同研究、政府関係が保有するデータの利活用、政策立案への参画

Q22： 今回のシンクタンクにおいては議論の場を提供する力という機能も果たせるのではないかと考えていますがその点についていかがお考えでしょうか。

A22： シンクタンクは、内外の社会経済情勢や最新の科学技術に関する知見を糾合するものであり、そのために議論をする場を提供する必要があると考えている。また、将来的には、学会や学術雑誌の創設なども求められてくるのではないかと考えている。

Q23： シンクタンクで経験を積んだ人物の幹部人材としての登用はどれくらい現実性がありそうでしょうか。

A23： 我が国には既に科学技術顧問のポストもあり、個人の頑張りによると思うが、ある程度は現実性のある話だと思う。

以上

記録作成担当者：梶山敬生

ヒアリング調査報告 No.39 基本情報

日時	2022 年 11 月 21 日
テーマ	経済安全保障の概要について。
ヒアリング先 (担当者)	衆議院議員 自由民主党 副幹事長 大野敬太郎 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 梶山敬生、香高優一郎、山田麻友 (計 4 名)
調査目的	経済安全保障に精通されている大野先生にお話を伺うことで、経済安全保障に対する政治的観点からの理解を深めること。

(写真)

【質疑応答】

1.経済安全保障についてのご質問

Q1： 大野様が考える「経済安全保障」の定義について、教えていただけますと幸いです。

A1： 2020 年末に党として初めて、包括的な提言書（「『経済安全保障戦略策定』に向けて」）をまとめた。そこでは、経済安全保障を「国益を経済面から確保すること」と定義をしている。国益とは、現行の国家安保戦略に掲げられているように、1 つ目は国民の生命財産を守っていくこと、2 つ目は経済の繁栄、3 つ目が国際ルールの形成により秩序を守っていくこと。これらの国益を経済面から守ると定義している。一方で、経済安全保障推進法は外部からの脅威という絞られた領域になっているが、私自身は、広く概念をとるべきだという観点から、国益を経済面から確保する、といった定義として経済安全保障を認識している。

2.サプライチェーンについてのご質問

Q2-1： サプライチェーンの脆弱性を克服することは企業にとってコストを伴うことであると思います。今後、経済安全保障の実行部隊となる企業との連携についてどのようにお考えでしょうか。

A2-1： 企業の観点から、経済安全保障は経済合理性を無視しても確保しなければならないことなので、一見コストに見えることは確かである。ところが、それをコストとして見るのではなく、むしろビジネスベースとして考えたときに、どうマネタイズ・キャピタライズするのかに視点をシフトしていくような社会になるべきだと思う。防災の概念で言えば、昔は、災害が来たときにどうするか会社で考えることは無理だという話になり、基本的には外部不経済として放置をしていた事例があったが、最近ではBCP という概念で整理をするようになっている。つまり、外部不経済を内部化し、長期の ROE の積分値の最適化を図った方が持続可能性は高い。そのような場合、長期的に見て経済の合理性は確保できるはずだ。

Q2-2： つまり、防災のようなリスクヘッジ、外部不経済にお金をかけるべきだと、企業に伝えていく形でしょうか。

A2-2： 国家的リスクでもあるので官民が協調する形が望ましい。例えば、ソーシャルインパクトボンドがある。ある会社がその国家にとって経済安保上の重要物資をサプライしている会社だったとして、その会社が対策をしないと困るのであれば、国としては補助金を出すことになる。しかし将来的にはその発想から脱却して、単に補助金を出すのではなく、例えば経営戦略としてその企業がサプライチェーン強靭化と供給目標をしっかりと示したとする。こういった社会へのコミットに対し、ESG ファイナンスのような考えの基に投資家が投資をする。そして、コミットした目標を実現したと認めれば、初めてそこで税金を用いて補助金を投資家に還元する。目標達成の判断は、第三者機関が行う。こうすることで予算の効率的執行も可能となる。あくまでアイディアであって馴染まない領域もあるが。

Q2-3： このようなアイディアを具現化するためにはどのようなことが課題となるか、ご教示をいただけますと幸いです。

A2-3： 新しい資本主義の概念でいうと、民間企業が外部不経済を内部化していく取り組み、つまり社会課題という外部不経済を民間が解決していく、その領域を市場化してキャピタライズ・マネタイズをしていく。社会全体で見れば、新しい投資先が生まれる上、社会の課題が解決される。先ほどのソーシャルインパクトボンドは一つの肝になる。政治としては、国民に対して、企業に対して、マーケットに対して、そういう社会にしたいというディレクションができるかどうかが課題だと思う。具体例に挙げれば、コーポレートガバナンスコードに経済安保を取り込む、つまり例えば重要物資の安定供給を一定の期間保証するといった会社があったら、それを社会が評価できる基準を設けるなどだろう。こうすることで、投資が得られる環境を作ることができる。このような取組を行っていきたい。

Q3： 日本の半導体産業の今後と育成の方向性について教えていただきたいです。

A3： 日の丸半導体の復活を目指している。半導体には、最先端なのかレガシーなのか、あるいはロジックなのかパワー半導体なのか、という種類の他、市場規模の大小、製造工程や研究開発、素材なのか製造装置なのかパッケージなのか等、様々な軸があるが、それぞれに日本には強い部分、弱い部分が存在している。その中で我々が目指しているのが以下 3 点だ。

1. レガシー半導体への注力

国内で安定供給ができる体制を作ること。これはまさに経済安保のサプライチェーン強化の文脈である。また将来はレガシー半導体と呼ばれる可能性はあるものの、し

ばらくは高性能半導体であり続けるものについては、TSMC が大分・熊本に製造工場を建設した。

2.2nm 領域の製造を目指すこと

2nm 領域の製造といっても、ボリュームゾーンじゃない 2nm 領域の次世代ロジック半導体の製造を目指している。つまり、ロングテールや多品種専用という領域で、収益が確保できるようなマーケットが対象になる。このような分野は米・IBM 社が研究で最先端を走っている。たとえば、GAA(次世代半導体の構造技術)が挙げられる。GAA は米・Intel や韓 Samsung、台湾・TSMC も研究に強みがあるが、IBM とは協力できる余地がある。また蘭・ASML も露光装置に強みを持つので、オランダとも協力していきたい。そして、次世代ロジック半導体の分野で再び最先端に躍り出ることを目指したものだ。

3.将来を見据えた研究開発

2.が実現しても、それだけで満足するわけにはいかない。さらにその先を見据えた研究開発が必要だ。オランダ・ASML は、真偽は定かではないが、1Å(1 オングストローム=0.1nm)級の露光装置を作れると言っている。原子と同じサイズであるのでできるか分からないが、それを目指すほど彼らは野心に燃えている。おそらくこの領域になると、既存のやり方では限界が出てくるだろう。どうなるかわからないが、このような動きと協調し、最先端技術の土俵に乗り続けることが重要だ。一方、素材といった、現時点で日本が強い領域はしっかりと維持して伸ばしていく。同時に、マーケット動向の将来を予測して研究開発することも重要だ。例えば素材ではシリコンだけではなく、シリコンカーバイドの時代になろうとしている。さらにその次にも新たな素材の時代になるだろう。将来のボリュームゾーンまたはロングテールの品目で使われる素材をしっかりと研究開発する努力をしていく。

Q4： 現在地政学リスクが高まる中、諸外国(特に西側諸国)が我が国の半導体産業(材料や製造装置)に期待していると思いますが、具体的にどの様な要望がなされているのでしょうか。

A4： 要望というか、マーケットや技術といった様々な軸のそれぞれの強みで連携していきたいということで、お互いにそのすり合わせをしている。例えば、Rapidus（ラピダス）という会社に対して政府は支援をすることにしたが、それと同時に研究と人材のための LSTC(技術研究組合最先端半導体技術センター)という団体を作った。なぜ作ったかというと、米国にも半導体の研究者や実業家が集うコンソーシアム、ナショナルセミコンダクターテクノロジーセンターがある。このカウンターパートとなるような枠組みを作ったらどうか、ということで作った。

具体的な要望があるというよりは、常に話し合いをしながら競争領域と協調領域の調整をしている。この世界の秩序に対してチャレンジをしてくる勢力とどう対峙するか、あるいはどのように安定的な国際秩序を構築していけばよいか。こういった文脈でお互いに何をすべきか、ということを話し合っている。

Q5-1： 諸外国でも半導体や重要鉱物を巡り、様々な連携が行われていると承知しております。どのような国際連携を志向するべきか、大野様のご見解を教えていただきたいです。

A5-1： 我々は自由貿易に最大の価値を置いており、自由な経済取引はその土台であり、この部分は決して間違ってはいけない。ところが自由だけだと、実は経済合理性が失われる。先ほどソーシャルインパクトボンドや外部不経済の内部化に触れたが、持続可能性という意味では自由を制限しなければいけない領域がある。これが経済安全保障だ。そう考えたときに、今の WTO は果たして合理的なのかを考えなければならない。本質的にどの領域でどのような制限を国際ルールとしてかけていくべきなのか。

ルールが定まっているっていうことは実態的に制限であるから、ルールの作り方をしっかりと再設計をしていくことが重要だと思う。既存の秩序への挑戦者が反発する可能性もあり難しいところではあると思うが、やはりWTOの大改革、国際的な秩序形成のためのルール作り、というのは必要だ。その中で、有志国同士で、何を誰がどこにどういうふうに作るのか、ということをある程度すり合わせるべきである。これが個別の国対国の2国間ルールになり、ひいては国際ルールになる可能性もあると思っている。

Q5-2： 現在WTO改革を米国・欧州・日本が中心となって行っていると耳にするが、今後はこのような動きを加速させるべきでしょうか。そして、そこでは日本はどのようにコミットしていくべきなのでしょうか。

A5-2： 現在、日本は極めて重要な役割を担っていると思う。昔は、正しいかは別にして米国が世界の警察官であり正義の絶対軸、絶対座標だと自認をしていた。秩序はある程度守られていた。今は少し違う。例えば米国がトランプ政権であった時代は、米中間で関税対決があり、普遍的価値の絶対座標が両国とも揺らいでいた。今は米国は少しは戻ってきているが、世界の正義の絶対座標を考えたときに、既に無秩序な領域に差し掛かっているのかもしれない。だから、日本は現在、自由を掲げながら各国の橋渡し機能、国際連携に取り組んでいる。5月に東京で開催されたIPEFにおいて、ASEANをIPEFに取り込むように米国に代わり交渉を行っていた。最終的には交渉がまとまり、ASEANが賛同してくれた。

要するに、世界の潮流においては十数年前と全く違う状況が生まれており、その中で日本が活躍してかなくてはならないと思う。

Q5-3： 豪州の政府関係者の方々や日系の企業の方々から、安倍外交のようなソフトな外交が非常に重要視されていて実施されているとお聞きしました。今後このようなASEAN諸国と付き合っていくために、どのような活動をするべきでしょうか。

A5-3： ASEAN諸国には、世界的な秩序を作るにあたりこちらサイドに来てもらわなければならない。なので、IPEFに一生懸命誘った。IPEFには関税ルール等がないため、何かメリットを出すしかない。具体的な例を挙げれば、インドネシアは防災に注力しているが、日本は協力を模索している。防災用のツールセットを同志国とともに展開する。そこでは政府と民間が一緒になってASEANに出資するような形にすることが重要だと感じる。

Q6： 我が国の半導体戦略の目標として、「国家事業としての産業基盤の確保」があり、そのため、TSMCの誘致があったものと承知しております。今後、TSMCのほか、海外の有力企業を日本に進出させるためにはどのようなことが必要になると考えていらっしゃるでしょうか。

A6： 民間事業であるので、税金を使用した誘致合戦だけというのは基本的に望ましいとは考えていない。ビジネスベースで戦略を描いた上で、マッチする領域をしっかり環境整備することが必要である。誘致補助だけではなく、民間に来てもらった際に、出口をどうしようとしているのか、例えばEV自動車の場合、どの国がターゲットだという戦略を共有し、政府が交渉に乗り出す。こういったことが重要だと思う。

一方で、初期投資、固定資産を持つことは会社にとって厳しいものである。例えば、工場を持つこと。費用がかさむ工場は国で持ち、様々な会社に来てもらい工場を国から借りる形で経営をしてもらうことで、日本への進出を促すことも考えられる。

Q7： 半導体の工場を作る際には、そこで働く従業員を中心とする街づくりが必要となるという話を以前伺いました。このような政策の副作用について、国としてどのように支援していくか教えてください。

A7： 新しい資本主義の文脈にもあるように、コストと考えられていることが本当にコストなのか、社会全体がもう一度考え直さなければいけないと思う。コストをむしろベネフィットに変えていくような取り組みはまさに必要である。例えばスーパーを誘致した際に、道路が渋滞して困ることもあったりする。何がベネフィットでなにがコストなのか。ここはある種政治の領域なので、それをコストだと思う方がいるのであれば、政治として何ができるのか考え、可能な限りベネフィットにしていくことが必要である。これからの時代の基本コンセプトであると感じる。

Q8： 半導体育成において、国家の研究費の助成だけでは研究設備を整えることができないとお聞きしました。我が国の半導体産業の育成において、国家による、技術育成や製造の主導はどのような役割を担うとお考えでしょうか。また、国家主導の効果をどのように期待しているでしょうか。

A8： 半導体だけではなく科学技術イノベーション全般に関わってくる。その中でも特に半導体には予算をかなり投じている。問題点としては、予算を投じた技術をしっかりと実装できるエコシステムが成り立っているのか。研究者は、研究を行い、成果を上げて、論文を書くことがある種一つのゴールになっている。しかし、実装をしていって価値を生み、その価値の例えば数%が研究にフィードバックされる、という構図じゃないと社会は当然成り立たない。日本では、技術を実装する人と研究する人とのエコシステムが成り立っていないと言われている。ここを事業化するにあたり、知財戦略を考える人、マーケットを考える人、競合他社を考える人、VC（ベンチャーキャピタル）といったお金を引っ張ってくる人、その環境を提供するような人といったように、様々な人材、事業が必要である。一番の課題はこういったところ。

科学技術イノベーションが政府の主要な政策となったのはここ最近である。安倍元総理が5年ぐらい前に初めて、科学技術イノベーションを政府の骨太方針のトップ課題に持ってきた。以来、大抵トップの方にある。それまでは科学技術に注力している政治家は端牌のような存在だったが、現在はかなり重要視されるようになった。その中で、今年からスタートアップ支援というのを正面でやり始め、実装と研究のエコシステムを作っていこうとしている。

大学の場合、10兆円ファンドという事業を始めた。自己資金で大学が研究に投じていける環境を作らなければならない。米国のスタンフォード大学は自己資金だけで4兆円程度ある。日本は多くて4桁億。この差異が国家の研究力の衰退に繋がっていると思うので、税金も利用するが、エコシステムを回していくことも考えなければならない。

Q9： 半導体産業戦略では、様々な対応策を打っていますが、このほかに大野様は今後にどのような政策が必要になるとお考えでしょうか。

A9： 基本的には人材育成だと思う。どんなことをやるにしてもやはり人である。何かチャレンジングなテーマを見つけて自分でやることが絶対的に必要だと思う。’The Man in the Arena’、アリーナに立つ男、というルーズベルトのスピーチがある。称賛されるべき人はアリーナに立っている人であり、その人はどんな批判があっても、失敗を重ね、批判を受け、トライアンドエラーを繰り返している。そういう人こそが成功を収める。称賛されるべき人はこのような人だということ。このような世界観を私は大切にしており、このような人材が育ってほしい。

Q10： 豪州では、重要鉱物に関して日本の投資に期待しているとの声を政府関係者、有識者から多数お聞きしました。一方で、現地の日系法人から、豪州の投資について、人件費の高騰、規制の多さなど、企業としては無視できないリスクも多数あるともお聞きしました。今後、安全保障として豪州との連携・投資は避けられないとしても、国として、重要鉱物の確保等でどのように支援すべきか、ご見解を教えてください。

A10： 豪州という限定ではなく、重要鉱物の安定調達をしっかりと確保することはまさに経済安全保障である。支援のあり方はいろいろあり、重要鉱物調達自体の支援や代替物資の支援、生産の合理化の支援等がある。国内に限らず、海外で資源を採掘する工場を作りたい、あるいは精錬する工場を作りたいといった声に対し、一定の合理性があるなら支援するというのもある。支援というのは基本的には全部税金である。経済安保上重要な物資ならば、まずは税金で支援することが前提ではあるが、それだけでは物足りない。経済安全保障上課題があることに対して社会自体がどう見るのか。他人の会社の負担であるため関係ない、自身が豪州で展開していくのはコストが発生するため望まない、と考える企業もある。もちろん、政府はコストが発生する部分を支援するが、ある種社会全体の合理性とその持続可能性を企業がどのように位置づけるかを考えるような方向に私はリードしたい。経済安全保障上重要であるため政府が税金をかけ続けると、社会は究極的に言えば共産主義になる。極めて重要な領域には税金を使うが、自由で安定した持続可能な社会を実現するためには、社会全体の構成員が社会の持続可能性を自ら考えられる環境を作る必要がある。

Q11： 今後、大学や産業界における機微技術の育成や保全のためにどういった政策をとるべきでしょうか。セキュリティクリアランスやスパイ対策の強化等についての大野先生のご見解を教えていただければ幸いです。

A11： 今まさに自民党の経済安全保障推進本部で議論をしている。前から話題になっている。年末に改定される国家安全保障戦略には、経済安保、サイバー、クリアランスが明記されるよう、しっかりと提言していく。クリアランスをどこまでやるかは、正直にいってフルスペックでやるべきである。

Q12： 経済安全保障重要技術育成プログラム等の応募に際して、大学や産業界が技術保全や技術開発体制において留意すべきことは何でしょうか。

A12： 協議会に入る時の注意という意味だと理解した。このプログラムは、研究成果の実装の一歩手前くらいを目指している。したがって、 本当にやろうと思っている人に入って欲しい。制限という意味では必要最低限である。例えば罰則付きの保秘義務。協議会のメンバー同士で秘密にしようという合意がなされる場合はそうした制限がかかる。秘密指定しないと、参加する会社や政府が情報を出せないという場合があるからだが、いずれにせよ合議制だ。基本的にはそうしたルールに従ってもらうだけだ。参加者が注意するのは実装に向けた取組に注力出来る人というのが一番重要。研究成果が出ました、論文の扱いをどうすればいいのか、という主張ばかりでは困る。論文は重要だし、政府は何も強制しない。扱いは合議で決めてもらうだけだが、本当に社会に役立つものにしたいという方向の意識が重要だ。

Q13： 経済安全保障においてシンクタンクや大学の文系学部が果たすべき役割について大野先生のご見解をいただければ幸いです。

A13： シンクタンクが一番重要であると思っている。経済安全保障推進法では一番注力をしている。どの領域にどれだけ予算を投じればいいのかを判断するため、日本の英知を結集して分析をしないといけない。出口がどういう会社と繋がっているの

か、マーケットは、ニーズは、リスクは、連携すべき国は、といった分析をしないといけない。今はそこまで深く分析が出来ていない。シンクタンクで答えを出してもらう必要がある。しかもインテリジェンス情報、すなわち各国の情報、同志国の事情等をマッシュアップしていくことが必要な領域となる。シンクタンクの役割は、具体的な政策を提言することだ。シンクタンクの中で担う文系の役割は大きい。文理融合と言われている。そういう時代になったのは、理系の論理だけでは乗り越えられず、デザイン思考で決めないといけない領域があるからだ。たとえばコロナ。理系はモデル分析は出来ても人の感情や倫理感まで組み込んで政策決定することは難しい。アート思考とまでは言わないが、デザイン思考までは持っていく必要がある。シンクタンクに文系的な人が必要になる。文理融合は、法律改正までして、その重要を示した。

Q14： データ破壊型のサイバー攻撃に対しては、攻撃を実行されてから対処する「受動的防御」では手遅れになるかと思います。本格的な攻撃を受ける前に積極的防御を有効にできるかどうかが重要かと思います。しかし、憲法 21 条による通信の秘密や、不正アクセス禁止法、刑法上のサイバー犯罪規定などが存在し、なかなか思うように行動できない状況にあると思いますが、これらの法の解釈や運用についてどのような議論が進められているのでしょうか。

A14： まだ実態的に公式に議論をしている訳ではないが、経済安全保障のフレームワークで水面下で議論は進んでいる。通信の秘密については本質的には狭く解釈されるべきだと思うが、実態的にはかなり広く解釈をされており、そうした政府答弁もされていることから難しい。違法性の阻却事由からくる例外の整理が一番のポイントになってくる。電気通信事業や個人情報保護法などの整合性の問題だ。ただ、ウクライナの事例もあるが日に日にサイバー攻撃のレベルが上がってきている。パッシブでは限界がある。また、ディスインフォメーションのような情報戦、特に選挙に介入してくるのが問題だ。そうなる前にアクティブをやれるようにしないといけない。少なくとも自民党はこうした認識を持っており、他の政党も持っていると思う。年末には少なくとも政府の中で検討を始めることになりそうではある。

Q15： 豪州では、重要インフラに対するサイバー攻撃があった場合に、関連当局へ通告することが義務付けられています。日本の政府機関等についても全てのサイバー攻撃の発生状況について把握することは困難であることが考えられます。そのため、個人情報漏洩以外についても通告の義務化をするべきではないかと考えているのですが、そのためにはどういった点に気を付ければいいでしょうか。

A15： インシデント共有と言われているが、サイバーについては非対称性や越境性、匿名性など普通の犯罪と違いかなり特殊な状況で発生する。あらゆる多様な主体と協力して対処していくというのはすごく重要であり、その主体同士でインシデントを共有していかないといけない。ただ義務化や罰則が唯一のツールという訳ではなく、インセンティブづけのようなことでもいいと思っている。例えば、コーポレートガバナンス上のインシデント共有をしたら点数を与えるといったようなことも考えられる。実際にワークさせることが重要である。努力義務については今も課されているが、全然うまくいっていない。ワークをするためにもう少し知恵を絞っていく必要がある。

Q16： 豪州にヒアリングを行った際に、「サイバーセキュリティや情報共有体制は例外として、日本の経済安全保障政策は米国や豪州よりも進んでいる」といった意見もございました。これについて、大野先生のお考えをご教示いただけますと幸いです。

A16：　包括的に経済安全保障を取り扱った法律を作ったのは、おそらく日本が最初である。経済安全保障に関する党の会議で相当議論を重ねた。党の新国際秩序形成戦略本部が 2019 年に立ち上がる前から、小林鷹之元経済安全保障担当大臣を含めた数名で知的財産の話からはいっていった。守るべきは守らないといけないということから始まり、それが形になってきた。ただ、我々がやりたかった世界観の一部しか実現していない。そして、この世界観については全てが法律で担保しないといけないものというわけではない。なんでも安全保障ということではなく、これからの社会の形、経済の形というのも考え、その形を実現出来る政策ツールを出していきたいと思っている。

以上

記録作成担当者：岡本樹

ヒアリング調査報告 No. 40 基本情報

Date and Time	26, November 2022
Topic	Interview on Cyber Security
Interviewee (Person in Charge)	（Law and Justice at UNSW Sydney） Director of the UNSW Allens Hub for Technology, Law and Innovation and a Professor and Associate Dean (Research) in the Faculty of Law and Justice at UNSW Sydney Professor Lyria Bennett Moses
Location	E-mail
Participants	（WS-C Member）ODA Hideo
Purpose of the Interview	To hear about Australia's server security law policy and compare it with Japan's cyber security law system.

当初対面でのインタビューを予定していたが、開催直前に諸般の事情からオンラインによる対応をリクエストされた。しかし、当方のモバイルルーターの調子が悪く帰国後の開催なった。一方、当初予定していた質問事項に関しては政府機関などへのインタビューで解決したため、疑問点として残っていた通信の秘密に関する事項についてメールで質問し回答を頂いた次第である。メールでの質問及び回答は以下の通り。

Dear Professor Lyria Bennett Moses
Good afternoon
I returned home last week after completing my research in Australia.
Thank you very much for arranging the meeting at TEAMS the other day. However, we regret that it could not be realized due to the malfunction of the mobile wi-fi router we brought from Japan.
Through the interviews with Australian government agencies and the Japanese Embassy, we were able to gain an overview of Australia's cybersecurity system. However, I feel that more research is needed on the interpretation of the law regarding the secrecy of communications.
In Japan's legal policy, the secrecy of communications is stipulated in the Constitution and interpreted and enforced very strictly, which is rather convenient for cyber attackers. Specifically, it is not allowed to intercept communications sent from countries where cyber-attacks are a strong concern, and it has to be a remedial measure after a cyber-attack has caused damage.
Of course, after concrete damage has occurred, it is possible to intercept communications by obtaining judicial approval with evidence of the damage, but this does not help to prevent damage before it occurs.
I believe that the secrecy of communications is guaranteed by law in Australia, but I would appreciate it if you could tell me by e-mail if there are any laws or legal interpretations that allow the interception of communications in order to enable effective cyber defense in Australia.
Sincerely yours
ODA Hideo

Dear Professor Oda,
There are laws in Australia that allow the interception of communications.
The main ones to be aware of are:
Telecommunications (Interception and Access) Act -
see http://classic.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/
Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 – which amended the Surveillance Devices Act. - https://www.legislation.gov.au/Details/C2021A00098
Kind regards
Lyria

Reporting officer: Oda Hideo

ヒアリング調査報告 No.41 基本情報

日時	2022 年 11 月 30 日
テーマ	キオクシア様が行っている半導体事業について
ヒアリング先 （担当者）	キオクシア株式会社 経営企画部 提携・渉外担当 グループ長 泊一修 様 参事 服部智之 様
場所	オンライン
参加者	（WS-C 学生）香髙優一郎、宮内拓 （計 2 名）
調査目的	我が国が誇るメモリ半導体の事業について学ぶこと。

（写真）

【質疑応答】

Q1： サプライチェーンの脆弱性を克服することは企業にとってコストを伴うことであると思いますが、これをマネタイズする方法はどのようなものが考えられるのでしょうか。

A1： 半導体の製造では、多くのものを複数の国から調達しており、その一部に関しては特定の国からしか手に入らないものもある。そこで、コストはかかるが、調達先を増やしていくことが長期的には求められる。

Q2： 現在、私たちは、企業がサプライチェーンの脆弱性を克服する際に必要になる資金を民間からの投資で確保できる仕組み（ソーシャルインパクトボンドのようなもの）を構想しております。このような仕組みの実現可能性についてご意見を伺いたいです。

A2：　企業や扱う物品の種類によって性質に大きな差がある。半導体に関しても数百の取引先があり、どこまで把握すればよいのか判断することが難しい。また、調達先が分散できるかはものによって異なり、企業が脆弱性克服に取り組んでいるかを評価することは難しい。

Q3：　貴社から見て、半導体素材や製造装置等のサプライチェーンにおける我が国の強みとは何でしょうか。
A3：　日本はデバイス以外に装置と材料が強いのはおっしゃる通りだ。世界的に見ても日本ほどエコシステムが整っている国はない。
　そのノウハウや蓄積自体が日本の強みだと思う。

Q4-1：　貴社は政府に対してどのような支援を求めているのでしょうか。
A4-1：　半導体に関して国は重要性を再認識している。今年度も先端半導体に対する補助金として支援がなされている。今後も、税制優遇や海外に比べて高い電力料金の改善など、海外企業とのイコールフッティング(対等な競争環境)になるよう、継続的な支援を求めていきたい。

Q4-2：　海外では米国の CHIPS 法等による巨額な支援がなされています。日本の半導体支援は金額的に不足しているものだと思いますでしょうか。
A4-2：　過去の経緯からすると現在の我が国の半導体予算は増えているが、海外と比べた場合に金額を増やしてほしいという声もあり、引き続き支援のレベルを上げてもらえればいいと思う。

Q5：　日本は中国、韓国に比べて人材のコストが高いと思われます。貴社がお考えになっているコスト削減に繋がる取組とは何でしょうか。また、Q4 とも重複しますが、政府にはやはりイコールフッティングになるような支援を望んでいるのでしょうか。
A5：　かつて日本はアジアの中でも人材コストが高かったが、今は以前ほど大きな違いはないのではないか。現在、技術者に関しては優秀な人が世界中で取り合いになっており、中国ではかなり高い報酬が払われていると聞いている。キオクシアとしては、人材への投資をしっかり行い、優秀な人を採用・育成する一方で、半導体製造過程においてはあらゆるコストを削減したい。そして、政府にもその支援をしてもらいたい。

Q6-1：　現在貴社のグループ企業であるキオクシア岩手様が東北大学等と連携して、東北半導体・エレクトロニクスデザイン研究会という形で、東北地方での人材育成に取り組んでいるとお聞きしたのですが、具体的にどのようなことをなさっているのでしょうか。
A6-1：　キオクシアとしては北上に工場がある岩手県、そして東北の中心である宮城県の 2 つをメインに、人材育成の取組を行っている。
　具体的には若年層への半導体産業の PR などを行っている。大学の中では、特に東北大と連携を行い、技術開発を行っている。高専では、JEITA の人材育成活動の一環としてキャリア講演会を開催しており、仙台では、広瀬、名取で行った。また、全国の公立小学校や図書館にフラッシュメモリに関する漫画を寄贈し、啓蒙活動をしている。
　また、北上の方では、市立図書館と連携して、半導体に関する企画展も開催した。

Q6-2：　教育活動とは具体的にどのようなことを行っているのでしょうか。また、TSMC は九州でどのような活動を行っているかご存じでしょうか。
A6-2：　将来を担う若者が科学技術やものづくりに興味を持ち、優秀な技術者を志すこと

を支援するべく、上述のキャリア講演会や、中学校での出前授業、ワークショップなど、様々な体験の場を提供している。

Q6-3： これらの啓蒙、教育活動の予算は貴社自身の負担なのでしょうか。
A6-3： そうである。人材育成の予算を組んで出費している。

Q6-4： 実際、このような取り組みは人材の質、応募される数といった点で効果があったのでしょうか。
A6-4： 効果が表れるのはまだ先になるかもしれないが、活動を通して、弊社の名前が浸透している実感はある。実際に入社希望者は増えている。
講義で半導体が身近なものに使われている事実を伝えると、面白いと感じてくれる学生も多い。また、日本の半導体が凋落したとメディアでは流れることも多いが、フラッシュメモリやセンサー、パワー半導体、車載向け半導体など分野によっては競争力があることなども伝えることを心掛けている。すると、新たに興味を持ってくれる人も多い。
これらの活動が実を結んで、社会に出る時に半導体業界を選んでくれる人が増えることを望んでいる。

Q7-1： Q6 に関連して、人材育成の枠組みにおいて、官、研究機関、半導体ユーザーメーカーに期待する役割とは何でしょうか。
A7-1： 国には、日本は海外に比べて理系に進む人が少ないため、理系に進む人を増やすような啓蒙活動を進めてほしい。
研究機関には、半導体について研究している大学が全国的に減っているため、より人を呼び込んで盛り立ててほしい。そのためにも、半導体の人材の育成・教育を行ってほしい。

Q7-2： 半導体を研究している大学が減っていることについて具体的に教えていただきたいです。
A7-2： 半導体の研究・開発にはクリーンルームが必要であるが、クリーンルームの建設、維持には莫大なお金がかかるため、予算の制約が大きく、1 つの大学では支えるのが難しい研究分野となっている。

Q7-3： 海外との大学との連携はどのようなことを行っているのでしょうか。
A7-3： 弊社はアメリカの大学と連携している。昔と比べて、より多様なパートナーが増えた。

Q8： 半導体は社会のインフラであると思いますが、一方で、シリコンサイクルの様に、半導体産業では、設備投資や在庫管理のタイミングの調整が難しいとお聞きします。設備投資や在庫管理で失敗しないように、貴社としてはどの様な取組をおこなっているのでしょうか。また、今後の見通しも教えていただきたいです。
A8： 在庫管理、設備投資ともに市況を見ながら調整している。
市況のアップダウンはあるが、中長期的には、NAND 型フラッシュメモリ市場は伸長していくと思われる。

Q9-1： 貴社はメモリ半導体の分野で世界第２位のシェアを占めておられますが、この要因とは何でしょうか。
A9-1： 弊社は東芝時代に NAND 型フラッシュメモリを開発しており、Inventor としての自負を持っている。世界第 2 位であるのはその結果である。

Q9-2：　米国の輸出規制による中国とのデカップリングにはどのように対応していくのでしょうか。
A9-2：　アメリカの輸出規制はこれからも守っていく。一方で、中国は魅力的な市場であるため、アメリカのルールに抵触しない限り、サポートしていきたい。

Q10-1：　また、Q9 に関連して、現在、半導体のマーケットの動向を把握するうえで、どのようにおこなっていますでしょうか。もし、指標等ございましたら、理由についてもご教示いただけると幸いです。
A10-1：　色々な関係者から情報を収集し、かつ、調査会社等も活用している。

Q10-2：　いろいろな関係者からはどのような形式でヒアリングを行っているのか。情報交換の場を設けているのか。
A10-2：　関係者との日々のやり取りから収集することが中心である。

Q10-3：　国が情報をまとめて、シリコンサイクルを可視化することは貴社にとって役立つのでしょうか。
A10-3：　大いに役立つ。現在、電子部品はまとまっているが、メモリなど細かい分野ごとのデータはない。具体的な分野ごとに情報がまとまっているとありがたい。

Q11：　貴社は国際的な連携としてどのようなことを行っているのでしょうか。
A11：　色々な取り組みを行っている。特に挙げるとすれば、ウェスタンデジタルとのジョイントベンチャー事業である。まさに日米連携の象徴と言えると思う。

Q12-1：　現在地政学リスクが高まる中、諸外国(特に西側諸国)は貴社に大きく期待していると思いますが、具体的にどの様な要望がなされているのでしょうか。
A12-1：　具体的な要望を直接言われたことはない。
　しかし、NAND 型フラッシュメモリを製造している国は日本も含めて世界に数か国しかない。よって、同盟国である日本で NAND フラッシュメモリを作っている状況はアメリカにとっては意味が大きく、政府関係者と話し合う中でも、この信頼感は感じ取れている。

Q12-2：　貴社が置かれている状況は今後どのように変化していくのでしょうか。
A12-2：　将来どうなるかはわからないが、現時点での弊社の方針としては国内で製造していくことである。

Q13：　現在の貴社の半導体の研究について、どのような問題について過大視しているのでしょうか。
A13：　色々な取組がある。例えば、次世代不揮発性メモリのデバイス、回路の技術開発や、新規プロセス、次世代リソグラフィ技術の開発を行っている。また、新しい動作原理や構造などにも踏み込みながら、各種新規メモリや、新製品を実現し新市場を開拓するシステム技術開発、ソフトウェア技術の開発にも取り組んでいる。

以上

記録作成担当者：宮内拓

ヒアリング調査報告 No.42 基本情報

日時	2022 年 12 月 6 日
テーマ	サイバーセキュリティの安全保障について。
ヒアリング先 (担当者)	東京大学 先端科学技術研究センター 講師 小泉悠 様
場所	オンライン
参加者	(WS-C 教授) 坪原和洋 教授 (WS-C 学生) 稲田凜香、岡本樹、織田秀夫、梶山敬生、香高優一郎、宮内拓、山田麻友 (計 8 名)
調査目的	ロシアを中心としたサイバーセキュリティの安全保障について理解を深めること。

(写真)

【レクチャー】

1. ロシアの安全保障におけるサイバー空間について

安全保障におけるサイバー空間について、ロシアを中心に説明する。

ロシアでは、対外情報庁 (SVR) が中心となってサイバー戦とそれによる情報窃取を行っている。サイバー理論の教科書等では、CIA モデルというものが言及され、C は機密性 (Confidentiality) 、I は完全性 (Integrity) 、A は可用性 (Availability) を意味する。これら CIA の 3 つのうちどれか一つ以上が損なわれる事態をサイバーインシデントと呼んでいる。

ロシアの情報機関は、まず盗む、すなわち秘匿性を損なわせる。それから情報を破損したり改ざんしたり、あるいは本来使えるべきもののアクセス数を毀損するということを全て行っている。おそらく、我々がサイバー安全保障と言った場合にすぐに考えることは秘匿性を破ることや可用性を破壊することだと思うが、ロシアの場合は改ざんまでする。これを情報機関のミッションとしてずっと行っている。

さらに、秘匿性を破ったらどうするか。伝統的なスパイの世界では、情報を取り敵の意図を知ることだが、ロシアの場合は伝統的に「コンプロマート」という考え方がある。コンプロマートとは、要するに名誉棄損作戦だ。相手にとって、不都合な真実や全くの嘘などを暴露することで相手の信用を落とすというのがロシアの情報機関が昔から行う手段である。突然ホテルに金髪の女性が入ってきて写真を撮られるといった話は昔からあった。つまり、元々ロシアの情報機関はサイバーに限らずに名誉棄損を手段とする情報工作を従前から行ってきた。

それが 2010 年代に入ってから、サイバー戦による情報窃取と情報の暴露によるコンプロマートを組み合わせた手法が非常に活発化してきた。この大規模な組み合わせが初めてロシアで行われたのは、2011 年 12 月である。当時はロシアで下院選挙があったが、これはあからさまに不正であった。90 年代・2000 年代も大規模な選挙不正が行われており、しかも当時のロシアは今よりかなり自由だったため、選挙不正を監視する市民団体が活動をしていた。彼らは選挙不正の事例等を国民にサイトへ投稿してもらい、インタラクティブマップに反映するといった抗議の方法を考えていたが、プーチン政権はこれをターゲットにして、選挙不正を報告するサイトに大量の偽情報を投稿したり、DDoS 攻撃によりサイトに過負荷を与えることで使えないようにするといった手段を用いた。また、それと同時に、知識人たちの発言にも圧力をかけた。ロシアにはライブジャーナルという有名なブログプラットフォームがある。これに対して政府系のサイバー部隊が大規模なサイバー攻撃をして、知識人たちが選挙不正の結果に対し声を上げられないようにすることを行った。

このような国内向けのサイバー戦をロシアは行ってきた。2007 年のエストニアに対する大規模サイバー攻撃の事例や、2008 年のジョージアとの戦争の際にロシアは国外に対するサイバー攻撃を行っていたが、どちらかというと国内向けサイバー攻撃の方が大規模であり洗練されているように見える。

また、2011 年 12 月の際にはコンプロマートも大々的に行っている。特に標的になったのがボリス・ネムツォフという野党の指導者だ。「選挙は不正だからみんな街に出てデモに行こうぜ」という話をしていたが、彼の電話はロシア情報機関に盗聴されており、ネムツォフはその電話の中で「今デモに来ている若者は本物の機動隊を見たことがないような怯えたペンギンやアザラシとかマウスみたいだ」と動物に例えて初めてデモに来た若い子たちを馬鹿にしていたことが暴露された。政治に関心のない若者も彼の呼びかけに応えてデモに来ていたのに、指導者自身が馬鹿にしていることがばらされたということである。

こうした名誉棄損作戦を含めた非常に複合的なやり方、どこからがサイバー戦でどこからが情報戦、あるいはインテリジェンス機関が行う諜報活動だということがきちんと区別ができないような形で、渾然一体になって行われていることが大きな特徴である。2011 年のロシアの国内向けサイバーインテリジェンス戦は、2016 年の米国に対する大統領選挙介入の原型だと考えられる。米国に対する大統領選挙介入では民主党の全国大会の事務所に対してサイバー攻撃を行い、クリントンやポデスタのメールを盗んで来て、特に選挙人の受けが悪そうな話を暴露したところである。これはサイバー戦とコンプロマートとの混合になるかと考えている。また、DDoS 攻撃により一時的に民主党のサーバーを麻痺させている。こうした混合攻撃の原型は国内での 2011 年のやり方であろう。つまり、2011 年から 2016 年の 5 年間で方法を洗練化させ、米国に対して攻撃をしたということである。

それではプーチンはどのような意図でこれを行っているかということであるが、自らが積極的に攻撃をしているというものではなく、西側への復讐であると考えている節が見られる。プーチンは、1999 年に一回首相になり、その後に大統領を 2 期 8 年務めた後に、憲法上続けられないため一度首相に退いている。これが 2008 年から 2012 年の 4 月であり、2011 年 12 月の下院選挙はプーチンの大統領復帰に向けた前哨戦といった非常に重要な下院選挙だったのだが、不正なんかせずに正々堂々と選挙をしても勝てたと思うのだが、プーチンはそれでも心配であるため票を操作しようと考え、大規模な不正を行った。それに対して国民が抗議の声を自発的に上げるとは考えていない。誰かに操作されないと一般大

衆は大規模な行動にでない。あるいはどこかからか大規模な金とか物資が供給されているから大規模な反対運動が起こるのだとプーチンは陰謀論的な考えで物事を理解している。そのため彼の頭の中では自身が首相から大統領に復帰してくることを米国が阻止しようと内政干渉するために反対運動を起こさせているのだから、ロシアの主権を守るためにサイバー戦やコンプロマートを行っているというので自衛であるとなっている。

その後、2014 年に最初のロシアとウクライナの戦争が起きたが、これもプーチンは米国が介入してきたと思ったところであり、クリミア半島を占領し、ドンバス地方に民兵を送り込んだのもそれに対する防衛だと思っていた。そして 2016 年に米国の大統領選があり、そこにドナルド・トランプという非常に付け込みやすい米国の憲政史上非常に稀な人物が立候補してきたため、その選挙戦においてプーチンは米国へのリベンジの格好の機会だと捉えてサイバー戦やコンプロマートを仕掛けたということになる。

つまり我々西側世界から見ると、中国やロシアがサイバー攻撃といった積極工作を用いて我々の社会に介入してくるように見えるが、彼らからは陰謀論的な考え方であるが全く逆に見えているということである。年ぐらいまでは、世界は最終的にグローバルスタンダード、要するに自由民主主義や市場経済であり、そこに収斂していってしまうと考えられ、米国の進歩主義的な人から見ると、それは要するに人類が正しい方向に向かっていくと考えてきた。

しかし、中国やイラン、ロシア等から見ると、その政治体制と今ある権力基盤そのものが米国によって掘り崩されて破壊されていくプロセスに見える。しかも、今のこの権威主義的な政権が破壊されて別の体制になることは、つまりは今の指導者の死を意味することとなる。例えば、プーチンが次の 2024 年の選挙には出ないと言ったら、彼は平穏な老後を送れるかというと、プーチンが好きな人も嫌いな人も彼は死ぬと言う。捕まって死刑になるか、誰かに殺される。それはプーチン自身も理解しているから政権を降りられないし、おそらく習近平もそうだろう。

私は、デカップリングにより世界がブロック化を指向していくのではないかと予想している。例えば、中国は経済的な側面でもテクノロジーの域内確保の側面から見ても明らかに自前で 1 個のブロックが作れる国である。また、ロシアは中国に比べると弱いものとなるが、少なくとも資源についてはその多くを自給できるため、中国と緩い関係を維持し、中央アジアへの影響力を中国と分け合いながら一ブロックとして存在し続けると考えられる。あとはインドや欧州といったブロックが存在し、これはロシアが 90 年代からずっと言っていた多極世界という議論に近い世界が誕生することを予感させる。

多極世界とは、米国が最強の覇権国家であることは当面ひっくり返し難いが、その中で米国が手出しできない領域が存在する、あるいは、その各地域に存在する強力な覇権国、地域覇権国家の周辺に何らかのブロックみたいなものができ、そのブロック同士が共存するといったビジョンのことである。その当時は、ロシアのこうした議論は相手にされなかったが、時代が四半世紀ぐらい経ち、それに近い秩序が生まれつつあるように見える。

このような世界は、単にそのブロックの中心にいる大国が違うというだけではなく、ブロックごとにかなり違った秩序になると思っている。端的に言えば、情報の取り扱い方である。現状我々はテレビで何を言っても、インターネットに何を書いても基本的に怒られることはない。しかし、ロシアはそういう世界ではなくなっている。中国もそうではないし、イスラム圏はより厳しく、北朝鮮はほとんどネットを使ってはいけないみたいな世界になっていくというふうに、まずは情報の取り扱い自体が、どの圏域に属するのかにより大きく異なってくると思う。

もう 1 つ違いが出てくるのが、サイバーである。サイバー空間は人工空間であり、インターネットの根幹であるルート DNS サーバーをたどると世界に 13 台しかないが、うち 10 台は米国で残りの 3 台がドイツと日本とスウェーデンにあり、基本的に西側のインフラということになる。インターネットという技術自体はアメリカで考えられ、根幹が西側で作られて、いまだに西側によって管理されている。インターネットは便利であり、どこの国

でもそれなしにはやっていけないが、ロシアを含めそうした西側に支配されているといった状況を是としている国ばかりではない。

ロシアの場合、2014 年の最初のウクライナ侵略後に米国との関係が決定的に悪化しているため、インターネットは危ないと思い始めており、米国がインターネットからロシアを排除するかもしれないと考えていた。加えて、SWIFT から排除されるかもしれないとも考えていたところであり、実際に今回のウクライナ侵略ではロシアは SWIFT から排除された。今回の紛争において、それと同じようにロシアがインターネットから排除される最悪の想定もしていただろうし、逆に有事において、西側の情報がインターネット経由でどっと流れ込んできてしまうということも懸念していたと見られる。これに備えるため 2015 年ぐらいから、インターネットサービスプロバイダーと通信省等を中心として、ロシアの巨大イントラネット、ロシア国内だけで機能するインターネットの実験を繰り返している。海外とのアクセスノードはオープンだが、そこを完全に国家管理下に置けば有事にシャットダウンするなり入ってくる情報をコントロールできるという思惑だったようだ。今回の戦争ではまだ間に合っていないようだが、一部のサイトに関しては、外国の IP アドレスからは見られないといった処置をとっており、例えばロシア国防省のサイトが見られなくなっている。一方、ロシア国内からはツイッターやフェイスブックといった西側の SNS がシャットダウンされて見えなくなっているため、ロシアのインターネットそのものを独立させるというところまでは至っていないが、ロシア政府にとって特に望ましくない特定のサイトを外から見せない、内から見せないという措置を講じることができるようになっているようだ。この先 10 年 20 年すると、こうしたロシアと同様に地域によって全く異なるインターネットが併存をしていくことはありうると思う。

つまり、ロシアの場合、RU のドメインが通用している空間を「ルーネット」と言い習わしているが、中国やベラルーシ、イラン、潜在的には北朝鮮といった権威主義国家らで何か都合のいい別企画のインターネットを作り運営しようといった話になるということである。こうした状況では、現在のインターネットで全世界が繋がっているという我々の世界理解の前提がだいぶ崩れてくる可能性はある。一方において、それはお互いのサイバー空間に侵入しないということであればサイバー防衛という観点からはメリットはあるのかもしれないが、根本的に世界観が、話がかみ合わないという状況がもっともっと広がっていき、インターネット自体がスプリンター化して全然繋がらないであるとか、あるいは覇権国家ごとのイントラネットが併存するといった状況になった場合、果たして我々の話のかみ合わなさはどこまで行くのか、私はかなりの恐れを抱いている。

現在のロシアにおいては知識人層はインターネットを活用することで世界がどのような状況であるかを理解しているようだが、一般市民のレベルではかなり疑わしい状況に見える。

2.ロシアのサプライチェーン上の問題について

最後にサプライチェーンの話をすると、まず、ロシアは 2014 年の最初の戦争によりサプライチェーンにかなり打撃を受けている。ロシアはソ連時代から工作機械が弱いといった特徴がある。特に半導体といった電子部品やその工作機械、産業用ソフトウェアが弱い。そこで工作機械を回すためのソフトウェアを何とか国産化しようとこの 8 年間目指してきたようだがうまくいっていない。ロシアの普通の会社や役所では Windows のパソコンで Office を使用し、ロシアの工作機械に対する輸入依存度は依然として 8 割、そして、半導体は自分たちのファブを持てない状況である。TSMC 等に匹敵するファブはロシアになく、依存の脱却はできていないということである。

今回の戦争に関するイギリスの防衛研究所の RUSI；Royal United Service Institute の報告書によると、ロシアが戦場で使用している比較的新しい兵器 27 種類の残骸を拾い分解したところ、中から 450 品目ぐらい外国製の電子部品が出てきたとのことである。そこで、最も多いのは米国製だが、日本製、台湾製、韓国製、イギリス製もあり、ロシアは

外国のサプライチェーンにかなり依存しながら軍事大国として生きているということが明らかになったとのことである。したがって、ロシアが次の侵略ができないよう抑止をするという観点からは、サプライチェーンから締め出すことが非常に重要になると考えている。

少し具体的な話をすると、ロシア軍がここ 10 年ぐらい使用しているオルラン 10 というドローンのエンジンは日本製である。千葉の市川にあるラジコン用のエンジンを作っている会社のエンジンを入手してきて使っているらしい。オルラン 10 は第一次紛争やシリアでも使用されており、その腹部についている偵察用のカメラも実はキャノンとニコンのカメラであったり、コントロール装置はアメリカ製であったりする。民生品をそのまま持ちこみ組み込んで、国産ドローンとして使用していることとなる。ラジコン用の小さいエンジンはロシア自身でも作れるとは思うが、安く大量に買うことができるため、国際的なサプライチェーンから調達しているのだろう。今回の戦争をきっかけとして、ロシアを国際的なサプライチェーンからより切り離していくというのはその継戦能力を削ぐ上で大きな意味があるのではないか。

もう 1 つは、中国がアメリカ等の技術を吸収して先行してしまわないようにする必要がある。アメリカのトランプ政権及びバイデン政権はかなり熱心に中国をサプライチェーンから締め出そうとしている。これにより中国もロシアも一時的にダメージを受けることになると考えている。ただ、その後に展開されるのは、先ほどの情報空間のスプリンターネットの話みたいに、中国を中心とする技術圏、伝統的に西側先進工業国を中心とする技術圏、その他もう一つぐらいの技術圏という三つぐらいの技術圏に分断された世界が出現する可能性がある。

今までの話をまとめると技術とサイバー空間の分断化はこれからのトレンドになると考えている。これに備える観点から中国への依存度を減らさなければならないが、完全なデカップリングをするというのは自由貿易の価値そのものを毀損するため目指すべきではないだろう。そもそも複数のサプライヤーがいて、その中から一番安くて品質が良い商品を選べることが自由貿易の価値であるが、現在は安全保障上の理由が商売の論理を阻むという事態だ。これはどちらかがどの場面でも絶対に優先されるというような考え方をするべきではなく、両立できるように工夫をしていく必要がある。

90 年代から 2000 年代ぐらいに私が学生だったときの雰囲気は、中国もロシアも真正面からアメリカと戦える国ではなく、イランと北朝鮮はコピー品のミサイルを作っているというものであり、アメリカの圧倒的な技術的・軍事的・経済規模の優位の恩恵であらゆるものが世界の市場で調達できる自由貿易時代だという感覚があり、これが揺らぐことなど想像もできなかったが、現に揺らぎを見せつつある。何が起きたのかというと、アメリカが圧倒的に強いと思い何でもかんでも自由に売り買いをしていたら、その環境を悪用してロシアや中国といったとんでもない敵を育ててしまい、それがアメリカの優位を揺るがしてしまったということである。そして、イランや北朝鮮のミサイルやドローンを分解すると、相当程度我々の作ったコモディティ品が出てくることは間違いない。事実、以前北朝鮮が撃った宇宙打ち上げロケット SLV の中からかなり日本製の部品が出てきた。

したがっていわゆる米国優位を前提にしたグローバル自由主義経済のシステムを維持することは適当ではないことは明らかであるが、だからと言って何もかも囲い込んでしまうという発想では、19 世紀や 20 世紀前半のような資源や市場や技術は戦争して相手から奪わないと入手できないものであるため、軍隊を作り囲い込んでおこうという発想になってしまう。最近は地政学という言葉が流行ってきているのだが、基本的に地政学者が考えることは資源の囲い込みと分捕りであり、第二次世界大戦の直前や冷戦期の 20 世紀後半といった囲い込みの時代は地政学的なものの考え方が機能してしまったと考えている。

だからこそ 90 年代になり、何でも買ってくればよいから、資源地帯を囲い込む必要がない、地政学は時代遅れであると言われていたのが、現在はその考え方が復権せざるを得ない状況に追い込まれている。このまま地政学の時代に入っていくのか、もう 1 回そのト

レンドを逆転させて、そこまではいかないようにできるのかというところが我々の大きな課題かなと思っている。

【質疑応答】

Q1： 経済安全保障は安全保障の概念の中においてどのように位置付けられるべきかについて、先生のご見解をお聞きしたいです。

A1： 経済安全保障というテーマについてはあまり知見がないため、定義をいうことはできないと思うが、おそらくカウンターインテリジェンスに限定される話ではない。現在の一番狭い理解でいうと、機微技術を流さないとか、あるいは外国からの直接投資で重要地域に外国人に土地を買われてはならないといった話がとても注目されているが、それは経済安全保障という概念のごく一部に過ぎないと思う。

仮に経済の安全保障と素直に解釈した場合、安全保障の定義はいろいろあるが、一般的によく使われるのはアーノルド・ウォルファーズ（Arnold Wolfers）の「獲得した価値に対する脅威の不在」という定義がポピュラーだと思う[488]。経済的に我々が今持っている価値、例えば日本の豊かさであるとか、技術的な比較優位であるとか、そういうものが損なわれないようにする措置の全般がおそらく経済安全保障である。その中にカウンターインテリジェンスや直接投資規制が含まれるのかもしれない。加えて、我が国の経済的な体力そのものを保ち、この先の国際的競争力を持ち続ける、回復させるといったマクロな経済政策全般の話も含まれる。さらに、これまで我が国は経済的に侵襲されているという話だったが、逆に我が国が経済のここを閉めたら世界経済のこの辺が麻痺するといった話を広く含んで、経済安全保障だと考えている。

経済安全保障は明らかに戦略論である。従来の国際政治経済学のような話と一部かぶるのかもしれないが、これは先程の地政学と国際関係論に近いと思う。国際関係論者は客観性がないと考えているため地政学が大嫌いである。ナチスや大日本帝国はそれを利用して領土を拡張しており、ソ連崩壊後のロシアもジオポリティカルと唱えてウクライナ等を侵略している。このように、国家のご都合主義的な行動を正当化するロジックに地政学はなりがちな側面があるのも事実だが、これを「学」と思わずに、そのような戦略論だと捉えるのであれば、私はそれなりに見るべきところはあると思う。経済安全保障は、経済領域における国家の戦い方全般の広い概念を指すと思う。

Q2： 経済安全保障又はそれに近い概念はロシアの安全保障戦略に見られますか。

A2： あるといえばある。法的な国家安全保障戦略（現状 2021 年バージョン）やその他各種政策文書を見ると、現在ロシアが受けている各種経済制裁や技術制裁はアメリカによる戦争行為だ、というような認識が非常に強い。また、2021 年版国家安全保障戦略では初めて、ロシアのスポーツ選手たちが謂れのない迫害を受けているという一文が入った。つまり、ドーピング問題等もアメリカによるロシア締め付けの道具であるというふうにロシアは認識している。要するに、戦争以外のあらゆる手段を使ってアメリカはロシアの弱体化を目論んでいる、あるいは中国やイランといったアメリカにとって都合の悪い国を押さえつけようとしているという考え方は非常に強い。経済領域に限らないが、経済や情報を含む安全保障が非常に重要であることは、ロシアがずっと言い続けている話である。

もう少し狭い話をすると、アメリカに対する経済依存や技術依存が問題であるという考え方は、2000 年代からずっと言ってきている。Microsoft の Word を役所で利用

[488] アーノルド・ウォルファーズ（ Arnold Wolfers）(1962)は、安全保障を「客観的には獲得した価値に対する脅威がないこと」であり、「主観的には、獲得した価値への脅威があるとの恐れが存在しないこと」と指摘している(向、2021)。

する際のバックドアに対する懸念は長期間言及されている。ロシアで新しく交付される法令の最後にはプーチンがサインをするため、サインをした文書がPDF掲載されている。アメリカのホワイトハウスであればPDFで読み取れる形で掲載されているが、ロシアはそうではない。よく見てみると、明らかにタイプライターで打たれている。つまり、ロシアでは重要文書をワードではなく、最後はタイプライターに頼るというぐらいに、自分たちの技術や情報空間がアメリカに握られているということに対して警戒感を強くしていると思う。

他方で、いわゆるエコノミックステイトクラフトといった、経済を通じて他国にいかに意思を強制していくのかという検討もロシアの中でなされていると考えられる。実際に経済開発貿易省といったエコノミックステイトクラフトを担当する役所もあり、それとは別に産業貿易省があり、財務省があり、ロシア中央銀行があるため、そういった観念はある。エコノミックステイトクラフト的な議論をしているとは思うが、安全保障の中にがっちりと組み込まれているのか、あるいは国防当局者や情報機関の人々と財政経済当局者が一緒になりロシアの安全保障について議論ができているかというと、そうではないと感じるところでもあり、ロシアの視点からはこうした議論をしっかり行っていくというのが課題になるのだろう。

Q3： 2014年のウクライナ侵攻以降の日米欧による制裁によりロシアにおいて、軍事戦略上必要な経済安全保障という観点から施策の変更がありましたでしょうか。

A3： 施策の変更というよりは強制的に変えさせられたといった感じだ。ロシアの兵器に用いられているパワー系半導体は主に英国産だった。しかし、イギリスはロシアに対する運輸の半導体のライセンスを停止した。また、ロシアの戦車についている赤外線カメラもフランスのサフランとベラルーシの企業が合同で作ったもので、これも停止された。このように、西側の技術が物理的に入ってこなくなったということである。

こうした状況を踏まえ、ロシアは今現在、経済のあり方を戦時経済に変えている最中である。戦争が予想以上に長期化したため、そうせざるを得なかった。6月の段階で軍需産業が戦時操業体制に入り、二交代や三交代制で24時間ずっと砲弾を作る工場が稼働しているという状態になった。砲弾等は国防省と契約している以上の数を生産するが、追加分については国防省が価格を決めているため、ほとんど儲けが出ていない。その後10月から、今のミシュスキン首相を中心として戦時経済調整委員会のような、戦時下に政府が経済や生産を統制するという体制が始まっていている。

したがって、ロシアのエコノミックステイトクラフト全体が戦争による大きな影響を受けている。問題はその先で、エコノミックステイトクラフトを、西側から金も技術も入ってこないため、どのように立て直していくのかとかというビジョンは見られない。また、これを経済安全保障というのかは分からないが、明らかにロシアはエネルギーを武器化している。ヨーロッパでエネルギーが足りないと言っているなか、わざとパイプラインの流量を下げたりしている。さらに、去年の冬から、スポットでエネルギーを売らなくなった。したがって、パイプラインの流量以上のエネルギーをヨーロッパは入手することができず余計苦しくなっている、といったようにエネルギーを武器に使うということを戦争前からロシアは行っている。ロシアのエネルギーを扱っている専門家や企業の人々は、エネルギーサプライヤーとしての信用が地に落ちるため、ロシアはこういったことを絶対しないと言ってきていたが、ついに武器化した。これが現実になったというのが開戦前後の動きとしては一番大きい。

Q4： ロシアは、中国やインド等との連携により日米欧による制裁の影響を兵器販売・開発等の面で十分に回避できているのでしょうか。

A4： 結論から言うと、できていない。先程の工作機械や半導体の話のように、そもそもその機械を作るマザーマシーン自体が入ってきておらず、兵器を組み立てて作るとい

うところからしてできていない。

もう1つ大きなこととして、2017年にアメリカがCAATSA（Countering America's Adversaries Through Sanctions Act）（対敵対者制裁措置法）を打ち出している。これは、アメリカの国務省のリストに掲載されている要注意企業と取引した国は、そのこと自体を要件として、つまり何か違法な取引をしなくても、制裁対象とするもの。ここにロシアの軍需産業の大部分が入っている。したがって、世界の国々がロシアから武器を買うという行為自体が極めてリスキーであり、これはかなり踏み込んだ制裁措置だったと思う。実際これによってまずは中国が制裁を受け、次にトルコが制裁を受けた。この状況に鑑み、インドネシアはロシアから戦闘機を購入する契約までしていたが、結局買わなかった。一方、インドはアメリカに対して干渉するなというためだけに、ロシアからS400というミサイルを買うという行為を貫徹している。ロシアの武器を買う買わないことは、大きな政治的マターとなっている。

また、最近アメリカの商務省の制裁措置が厳しくなっている。アメリカからロシアに対して直接に機微技術が渡らないようにすることは以前から行われているが、最近になって、アメリカの知的財産権のもとで作られたあらゆる製品がロシアに渡るかどうかをアメリカが審査することとしている。例えば、アメリカの知的財産権のもとにヨーロッパやアジアで作られた製品について、そのグレードの製品はロシアに売ってはいけないみたいにアメリカは口を出してきている。このようになっているため、ロシアはますますやりにくくなっている。中国に支援をしてもらえばいいという話になるが、中国は商売上の損得を越えてロシアを支援すること、あるいはアメリカに睨まれてまで機微技術をロシアに渡すことはしていない。したがって、最終的にロシアがある程度自身で克服しないと、この状況はなかなか変わらないと思う。

Q5：　ロシアの安全保障戦略上、サイバー攻撃はどのように位置付けられていますか。

Q6：　ロシアのインテリジェンス機関は軍事に関わる最先端技術を入手するためにサイバー・人的手段を問わずに活動をしているように見えます。そもそもロシアの安全保障戦略の中にそのような技術入手を前提とした方針があるのでしょうか。

Q7：　こうした軍事に関わる最先端技術の入手についてサイバー分野の登場によりロシアの安全保障における考え方が変化したところはありますでしょうか。

A5~7：　ロシアは当然のことながら、自分たちでサイバー攻撃をしますとは言わない。アメリカがしてくるという言い方をしている。ロシアの政策文書やドクトリン文書を読む際には、敵が行ったという記述をロシアが行ったと読みかえろと必ず習う。

ロシアの政策文書や参謀本部が書いている雑誌、軍事科学アカデミー雑誌を見ると、サイバー戦は戦争の一部であり国家間関係において不可欠な要素ということをロシアは認めていることが読み取れる。日本もサイバー安全保障抜きで自国の安全保障を語れるとは到底思えないし、どこの国でも同じである。サイバー戦の大きな特徴は、平時から有事まで常に継続して行われるということである。

情報戦も同じで、平時から有事へと継続的に行われる。それが平時においては単独で（ピンで）活動し、有事になると緊張をエスカレートさせたりする。有事となり武力闘争が始まったら、暴力とサイバーを組み合わせ、さらにそこに偽情報や経済制裁等の様々なものを組み合わせれば、3発、4発殴ったのと同じぐらいまで効果を高めることができる。

このようなことはロシア軍の中でも2010年頃から活発に言われるようになり、2011年にはロシアの参謀本部がサイバー安全保障に関する基本的な考え方を示した文書を公表している。これは参謀本部の考え方であり、政府の公式文書ではないが、概ねタリンマニュアルに書いてあることとほぼ同じと考えて良い。タリンマニュアルには、サイバー攻撃は武力攻撃とみなされる場合があるということが書かれている。

サイバー戦争に関する考え方は、西側諸国とロシアは大きくは変わらない。ロシアはサイバー空間を流通する情報は国家が管理すべきという考え方に立っている。
日本では、余程悪意ある情報を流さなければ何を流して良く、勝手に人の情報を覗いたりパスワードを盗んだりしなければ何をしてもよいことになっている。
ロシアが考える安全保障は、政権にとって都合の悪い情報は流してはいけないとか、政権にとって都合の良い情報を流すところまでを含めたサイバー空間の管理を前提にしており、これが達成できて初めてサイバー安全保障が確保できると彼らは考えている。ロシアのサイバー安全保障機関は、攻守ともに極めて規模が大きい。ロシア連邦通信監督庁ではサイバー空間の情報を事実上検閲している。マスコミやインターネット空間上にこういった情報が流れているのは駄目と言い回るような役所が存在している。また、ロシアには通信傍受専門の機関があり、相当強力な通信監視機能を備えているところが、ロシアのサイバー安全保障の特徴であろう。技術窃取の話や窃取した技術によってこうなったみたいな話は以前からあった。そもそもプーチンが KGB のスパイだった頃に行った業務の中の留置作戦は、東ドイツを窓口にして西ドイツの技術をかき集めてくることがプーチンの任務の一つだったようである。ソ連時代から外国技術の入手は情報機関の仕事だった。ロシアは日本でも技術入手活動を当然に行っていると思う。外国から盗んできた技術をロシアが何に利用しているかはあまり分からない。中国はかなりあからさまであり、明らかに盗んできた F35B の技術を何処に利用したかが分かる。ロシアは集めるだけ技術を集めてきて、何かの参考にはしているのであろうが、直接に反映をしていない感じがする。

Q8： ロシアのサイバー攻撃は 2014 年のウクライナ侵攻においてどのような役割を果たしていたのでしょうか。また、ロシアの従前の安全保障戦略の中で平時のマルウェアの利用も含めてこうした手法は体系的に整理されているものなのでしょうか。

A8： ロシアは自分たちでこういうことをするとは絶対に言わないが、ロシアの参謀本部の雑誌などを見ていると、こういう議論は非常に盛んに行われてきている。要するに、マルウェアを使って平時に外国を混乱に陥れることとその他の様々な情報戦とを組み合わせることで戦争をしなくても勝てる、相手国の政権を崩壊させられるという議論は以前からある。それと同時に大量の難民を送り込むといった、様々な邪悪なことを考えている。

2014 年のクリミア侵攻に関して、このサイバー戦は結構うまくいった。ここで注意すべきは、クリミア半島をロシアはほぼ数日で掌握し、その際インターネットを同時に遮断したが、そのときのインターネット遮断作戦では、サイバー攻撃ではなく特殊部隊がインターネットサービスプロバイダーを物理的に占拠した。結果的にインターネットを遮断するという目的が達成されている。サイバー戦でもハッカーによらず、破壊工作員がラジオペンチ持って攻撃した方が早いのであれば、そちらの方が良い。

これは宇宙空間でも同じであり、宇宙戦では人工衛星を破壊しなければならない場合もあるが、地上局を破壊しても、妨害電波を流しても良い。目的が達成できているかどうかが重要である。クリミア侵攻の場合はインターネットを遮断し、普通のメディアも遮断し、議会を占拠することで、何が起きているかが分からない、どこに意思決定中枢があるのかが分からないといった状態を作ることで住民を不安に陥れ、住民投票を行うことでロシアに併合してもらった方が安心だという話にした。

その後もロシアは度々ウクライナにサイバー攻撃を仕掛け、2 度電力を落としており、また、会計システムに幅広くウイルスを感染させ、ウクライナの金融決済を混乱させたこともあった。

つまり、攻撃手法が整理されていると言うよりは、これは非常に使えると思った手段を、ロシアの FSB、SVR、GRU が中心になってそれぞれ行っている。彼らが使っているマルウェアを分析したレポートによれば、使われているコードには共通性が全くな

い。ごく一部は共通するが、それはダークウェブで転がっているものであり、基本的にはバラバラである。ということは、各機関がソフトウェア部隊を抱えていることになる。マルウェアも別々に作り運用していると関挙げられる。このような状況のなかで、プーチンが、アメリカの大統領選潰したい、と言うと、SVR・GRU・FSB が、俺たちが一番に攻撃しようと頑張って成果を上げようとする、というようなシステムだと思う。これをロシアの政治評論家がシステマと呼んだ。はっきりした制度は存在しないが、プーチンに対する忖度の中で、なんとなく力関係が決まっている、そういうシステムがあると思う。

Q9： ウクライナは、2014 年のロシア軍によるクリミア半島侵攻の際にサイバー攻撃で手痛くやられました。しかし、今年 3 月から始まったロシアのウクライナ侵略戦争においては、ロシア軍のサイバー攻撃に目立った戦果はなく、ウクライナの事前の準備が功を奏しているよう窺えます。NTT チーフ・サイバーセキュリティ・ストラテジストの松原実穂子さんがフィナンシャル・タイムズ紙の報道を引用して、米軍・米企業のチームによるウクライナ支援の話をしています。ロシアはサイバー攻撃のあり方について何か新しい施策を講じるような動向はありますでしょうか。

A9： これは情報機関の中のことであり、今動いている状態なので、直ぐには分からない。次に大規模なサイバー攻撃が発生したときに見えてくると思う。

Q10： 日本周辺においては台湾有事の現実味を帯びており、有事における重要インフラへのサイバー攻撃の備えとして、平時から安全保障の観点から一定のセキュリティを確保する必要があると考えられます。サイバーと実際の軍事との接続も視野に入れ、ロシアに対抗したウクライナから我が国が学べることはどのようなものがありますでしょうか。

A10： サイバー安全保障に関しては結局のところ、どれだけゼロデイ攻撃に対抗できるのかとか、DDoS 攻撃に対してどれだけ太い回線を用意しておけるのかとか、深いサイバーの話はサイバー専門家に聞いた方が良いと思う。

今回は、ロシアの偽情報戦は余り行われていない。前回のときはかなり行われており、紛争地域に限らずウクライナ全体に偽情報が流布された。当時はまだ偽情報が一つの競争領域になるという考え方すらなかった。当時、ウクライナの国民の半分ぐらいがロシアの大手 SNS のアカウントを持っていた。しかもウクライナ国民のほぼ 100%がロシア語を話すことができるため、言語的にあるいは情報チャンネル的に完全にロシアと繋がったままロシアの侵略を受けたことが痛かったと思う。それ以降、ウクライナはロシアの SNS を禁止し、去年の春頃には親ロシア的な TV 局 3 局を停波処分にした。これによりでロシアからの偽情報には惑わされなかった。

日本がウクライナから学ぶことは、例えば、インターネット上でこういう言説を誰が流していて、インフルエンサーになっているのかを把握しておくことである。今の技術で十分できるし、我々が今ロールスで行っている研究プロジェクトでもそういうことを可視化しようとしている。東大・東工大・筑波大の各先生方でもこういうことを行っている方々がいる。現状では学者が研究をしているが、NISC の中にシチュエーションセンター作り、Information Awareness みたいなものをすることは良いと思う。

例えば、宇宙安全保障に関してまず何から始めるかというと、Space Situation Awareness からである。まずアンテナを作りレーダーで衛星を見ることで、この衛星が毎日この時間にこの軌道を通ることを理解し、今日は何か変な軌道に変わったとかいうことを把握できるようにしておく。それができていればいざというときに、追跡するのか、撃墜するのか、妨害するのかを選択できる。これと同じように、日本は民主国家のため普段から言論統制は出来ないが、変な情報を広めている者やか

なり怪しい者を平時から追跡して、有事の際にその者をダウンができるようにしておくことがいいと思う。イギリスではBBCが外国の情報のトラッキングしている。外国がイギリスをどのように言っているのか、何か変な情報を流しているメディアはないか、といったことをBBCが見ている。

ロシアのイノスミという政府系メディアがあり、ロシアについて外国の誰が何と言っているか把握している。僕とかもしょっちゅう、書いた記事がつるし上げられ、コメント欄で「またこの小泉ってやつがロシアの悪口を言っている」といった感じで書かれる。つまり、ターゲットリストができているわけだ。

まず日本はターゲットを作ることから始めたら良いと思う。

Q11： ROLESの提言でクリアランスがなくても情報共有枠組にいれてもらえるよう働きかけるとありましたが、そもそもそういう交渉は可能なのでしょうか。また、クリアランス制度を採用するならば日本はどのような体制をとるべきなのか、先生のお考えを詳しくお伺いしたいです。

Q13： ROLESの提言でSTRATCOM　COEなどとの連携に関して国際的な研究拠点との連携とのお話がありましたが、現状の大学などに所属している有識者と政府との連携の状況と比較して、もし提携がなされたとすればどのように変化していくのかお考えを伺いたいです。

Q16： 日本のシンクタンクに今後求められる役割として安全保障面でどのようなものがあるとお考えでしょうか。

Q17： ROLESは大学発のシンクタンクですが、他のシンクタンクとの違いや今後求められるROLESのような大学発シンクタンクだからこそ果たせるものとしてどのようなものが考えられるとお考えでしょうか。

Q18： アメリカなどではシンクタンクを経験した方が政府に入り、政策において重要な役割を担うことも頻繁にあると認識しておりますが日本ではそのような動きはあまりないと思われます。今後日本でもシンクタンクと政府の間で人材の高い流動性が実現する可能性はあるとお考えでしょうか。それとも難しいと思われますか。

A11, 13, 16, 17, 18：

ROLESで実現したいことの一つは、研究をするシンクタンクの創設である。日本のシンクタンクは研究をしていない。お金はあるが研究員を雇わずに事務の人ばかり雇っている。会議のためのロジが多いという状況である。ROLESでは、ロジに関しては外部に任せ、中の研究員は研究してレポートを書くことに集中する必要がある。単に研究をするのであれば、大学の研究室でもできるが、ROLESでは現実の政策に反映させたいという思いがあるため、シンクタンクから官庁、官庁からシンクタンクという流れを作りたい。クリアランスなしでの情報共有は難しいため、現時点で官庁から一年ほど来てもらうことなどを考えている。給料は役所に払ってもらう。こちらは研究室などを用意する。その中から大学の教授になるような人が出たりすれば良いと思う。また、政治家等に来ていただいても良いのではないかと考えている。現時点で、NECの方に春から来てもらっている。

Q12： ロシアのウクライナ侵攻により経済的結びつきが武力衝突に発展することを抑止することに繋がるという考え方が大きく後退したように思えます。そもそもロシアは欧州のガス等に見られるような安全保障に資源外交を活用することをもともと考えていたのでしょうか。また、現在のロシアの行動はこうした資源欠乏による経済不安を各国の世論を動揺させ、軍事面での優位性に繋げようといった動きに見えますが、これは露国版の経済安全保障戦略として従前から考えられていたものでしょうか、それとも今回において機会主義的に行われたものなのでしょうか。

A12： 従来からこれを武器にするということをロシアのエネルギー当局や、ガスプロム

などのバティックとか考えていたとはあまり考えられない。なぜならそれは彼らの破滅に繋がりかねず、本来はしたくないことだったのではないかと考えている。一方でプーチンがまだ若い頃に、サンクトペテルブルグ鉱山大学という大学でチーム博士論文を出している。その博士論文は実質の彼の部下が書いたものではあるが、その中身は資源を国家管理下において国家の対外政策のツールとして活用するべきだというものだ。プーチンには資源の国家管理という発想が若いときからあったと思う。また、把握している限りではロシア軍もこういうことは考えており、だから機会主義的なのかどうかという問いに対して、機会主義的というよりは、普通だったら絶対に、ガスを安全保障上の武器として使うという話になれば輸出ができなくなり、外貨を獲得できなくなるエネルギー企業は断るような状況ではあるが、今回の場合は国家存亡の危機なので、国家が業界に圧力をかけてガスを武器として使わざるを得なくなったのではないかというふうに見ている。それに関連してよくわからないのは、この戦争が始まる前後から、天然ガス企業ガスプロムの役員が何人も死んでいるということだ。今年の夏にはルクオイルという石油大手の社長も死んでいる、会長も死んでいる。たぶん天然資源を武器として使われるのは絶対嫌だというエネルギー企業業界、言うことを聞かせたい政権という構図があって、言うことを聞かない者を見せしめにしたということではないかと考えている。ただこれは機会主義的かどうかという話になると、異なる世界観を持つ人がどこの国にもおり、また今は戦争中であることから、圧倒的に諜報機関の人々の発言権が大きくなっている状況なのではないか。

Q14：　今後、サイバーセキュリティを高めていくためには、修正されていない脆弱性を見つけてアップデートする必要があり、その情報が流出してしまわないようにすることが重要であるとの記事を読みました。そして、セキュリティ対策が進められている大企業や役所ではなく個人のセキュリティ対策が重要であるという印象を受けました。個人が出来ることとしてはセキュリティ対策ソフトを使用することだと思います。サイバー安全保障の最大の弱点は人間であるとの事でしたが、この弱点をどのように改善していくべきか、小泉先生のご見解をお聞きしたいです。

A14：　サイバー安全保障の最大の脅威は人間である。サイバー安全保障のプロではないが、ロシアのサイバー戦を見ていると結局は人間であると感じている。人間である以上はなかなか弱点というのはカバーしきれない。組織工学的にカバーできる部分はある。日本のサイバー防御を考えるときに、人間はどういう動機で落ちているUSBをパソコンにさしてしまうことや、開いてはいけないファイルを開くということをしてしまうのか。東大でもサイバーインシデント対策チームがあり、怪しいメールについては開かないように気を付けるということを言っている。つまり怪しいファイルについては開かないようにしましょうということを言っている。しかし、気を付けることが出来ていないところでサイバーインシデントが起こっている要因がある。意外と人文学的なアプローチの領域であると思っている。

参考文献

向和歌奈（2021），「日本における経済安全保障への着目：安全保障分野としての台頭と課題」　『アジア研究シリーズ』 2021年度発行 109
＜https://www.asia-u.ac.jp/uploads/files/20220420165020.pdf＞。

以上

記録作成担当者：岡本樹

ヒアリング調査報告 No.43 基本情報

日時	2022 年 12 月 12 日
テーマ	九州経産局様が行っている半導体施策について
ヒアリング先 (担当者)	経済産業省 九州経済産業局 地域経済部 情報政策課 情報政策係長 岡田宏一 様
場所	オンライン
参加者	(WS-C 学生) 岡本樹、梶山敬生、香高優一郎、宮内拓 (計 4 名)
調査目的	九州における半導体施策について学ぶこと。

(写真)

【質疑応答】

Q1： TSMC を誘致する際に苦労した点は何でしょうか。

A1： 誘致に関しては、本省が中心に動いていたため、弊局はあまり携わっていない。しかし、誘致後には人材育成等の取組に注力している。

Q2-1： TSMC ひいては台湾の方々との協力、連携において特に心掛けていることがございましたら教えていただきたいです。

A2-1： 熊本の工場で働く人材の育成・確保をすること、工場で生産した半導体の取引先を増やすことの２つを課題として台湾と連携しながら取り組んでいる。その際に、台湾側にもメリットを示すことを心掛けている。

Q2-2：　日本と台湾はお互いにどのようなメリットを提示し、協力しているのでしょうか。
A2-2：　日本は素材と製造装置において、台湾は半導体デバイスの生産においてそれぞれ強みを持っており、これらの分野における技術協力という面でメリットを提示しあっている。特に、現在は台湾南部に素材企業が集積させる動きがある。

Q2-3：　台湾南部に素材メーカーが集積しているということでしたが、このような動きは加速しているのでしょうか。
A2-3：　している。日本だけでなく、米国もファウンドリを積極的に誘致することで、サプライチェーンを域内で完結させようと動いている。世界情勢も悪化しているため、加速していると言える。

Q3-1：　TSMC から求められている事項は何でしょうか。
A3-1：　基本的には資金面に関しては本省が対応している。九州経産局は主に人材の面で協力している。特に、熊本工場で働く 1700 人の従業員の確保といった課題を抱えている。
　また、域内のサプライチェーンの強靭化も行う必要があり、JASM も国内から 50%以上の調達を目指している。

Q3-2：　JASM が国内調達率５０％以上を目標にするということでしたが、現在はどの程度なのでしょうか。また、今後調達率を上げるためにはどのような取り組みをする予定なのでしょうか。
A3-2：　現在はまだ工場が稼働していないため、0%である。調達率を上げるには商社の動きも重要になってくると思われる。

Q3-3：　熊本の工場で 1700 人の従業員が必要であるということですが、従業員の生活に関連して街づくり政策も重要になってくると思われます。他省庁と連携はなさっているのでしょうか。
A3-3：　連携はしている。主に、国土交通省、農林水産省、厚生労働省、文部科学省と調整を行っている。

Q4：　日本は台湾や中国に比べて半導体の製造コストが高いとお聞きします。イコールフッティングとなる支援としてどのようなものが考えられるのでしょうか。
A4：　生産している製品が異なるため、コストを比較したことがない。イコールフッティングというよりは、日本の半導体製造能力を高めていくことを目的に、企業には補助金の支給により生産設備を整えてもらっている。

Q5：　日本のハイレベル人材、ワーカー人材の特徴や強みとはそれぞれ何でしょうか。
A5：　ハイレベル人材に関しては、半導体が斜陽産業になっている影響で、全体的には劣ってしまっているうえに、ボリューム的にも少なくなっている。しかし、素材や製造装置などスポットでは育成ができている。台湾の様に半導体の製造工程に沿って満遍なく学べる環境づくりが重要であると思う。
　ワーカー人材に関しても、全体を理解したうえで、専門分野の深堀を行える人材を育成することが重要である。

Q6：　今後日本が最先端技術を研究開発していくうえでは、人材育成・確保がとても重要であると思います。産学官のそれぞれに求められる役割や連携の在り方とはどのようなものなのでしょうか。

A6：　産側には、企業が生産するうえでどのようなニーズがあるのかを明確にしてもらう必要がある。最先端技術であるため長期的なスパンになるかもしれないが、どのような技術を開発したいのか、そのためにどのようなことを学んだ人材が必要なのか等を具体的に示してほしい。そして、学側にはこのようなニーズを受けて人材育成を行ってほしい。さらに、官側はこれらを踏まえて長期的な視点のもと青写真を描くことが求められると思う。

Q7-1：　台湾の大学などの教育機関との協力、連携等で特に心掛けていることがございましたら教えていただきたいです。
A7-1：　台湾側にとってもメリットがあることを伝えることを心掛けている。日本には、素材と製造装置の工場が集積しているので、お互いに留学生を派遣するなどして交流ができればと考えている。

Q7-2：　実際に九州にはどのくらいの台湾からの留学生がいるのでしょうか。
A7-2：　2021 年度は台湾からの留学生は 5000 人程度であった（半導体分野に限らない）。

Q8：　台湾や米国等海外の先進地域との教育交流について具体的にどのようなことをなさっているのでしょうか。
A8：　弊局では台湾以外には特に交流していない。しかし、九州大学は個別に米国とかかわりを持っており、今後このような動きは重要になってくると思われる。

Q9：　セキュリティクリアランスなどが求められているなかでの、半導体産業における海外からの人材の在り方についてのご意見を伺いたいです。
A9：　人材とともに情報も移動することを考えると、セキュリティクリアランスは重要であると思う。しかし、経済安保関連は本省がオールジャパンに取り組んでいるマターのため、弊局独自で取り組んでいることはほぼない。

Q10：　日本国内で半導体の需給のエコシステムを構築することは可能なのでしょうか。また、海外の需要家に向けてどのような半導体製造、販売の在り方が望ましいのでしょうか。
A10：　半導体の生産においてはすでに水平分業化が進んでおり、日本はガス、レアメタル等を海外に頼っている状態である。このことを踏まえると自国のみで完結させることは難しい。今後も有志国、地域と連携して調達、供給を行っていくことが重要である。
　海外の需要家に向けては、サプライチェーンを可視化することが重要になってくると思う。しかし、企業はあまり明かしたがらないと思う。

Q11：　東北地方や関東地方においては、東北経産局や関東経産局を中心にサイバーセキュリティ連絡会を設立し、サイバーセキュリティにおける産学官が連携した情報共有体制を構築していると理解しております。九州地方においては、サイバーセキュリティ推進 WG があるものの、官が主導した情報共有体制は構築されていないと思われます。御局では、今後こういった官主導の連絡会を構築するといった方針はございますか[489]。

---

[489] 経済産業省「地域 SECUNITY リスト（令和 4 年 5 月現在）」
＜https://www.meti.go.jp/policy/netsecurity/comunitylist.pdf＞（2022 年 12 月 9 日閲覧）。

A11：　担当していないから、わからない。

（追加質問）

Q12：　経済安全保障においては民間出身者の知見であったり、大学の研究者の知見も取り入れて、重要な技術の開発を推し進めていく必要があるという風に認識しております。現場でも経済産業省の方に民間の方が出向したり、経済産業省から民間の方へ派遣などはあると思いますがそのような制度を行う上で、短期の出向であれば問題とならないと思いますが長期で行政機関が民間の方を受け入れる際には例えば年金の問題なども出てくると考えています。そこに対してどのような対策が考えられるでしょうか。外部の知見を取り入れる上でどのような課題があるとお考えでしょうか。

A12：　現状弊局では、本省と異なり民間企業との積極的な交流はないので、分からない。

Q13：　民間の人材が行政であったり大学の研究機関と行った産官学の間で人材を流動的に回していくといったことがアメリカなどでは頻繁に行われていると認識していますが日本でそのような動きを活発化させることの現実性はあるとお考えでしょうか。

A13：　日本でも似た動きを取り入れることは重要である。役人だけでは産業界の動きを捉えきれないことがよくあるため、トレンドをヒアリングし政策に反映させることが求められる。産業界の人が政策を作る側に回り、施策を打ち出していく必要がある。

Q14：　経済安全保障においてはその政策の中で、重要な技術を育てていく必要があると考えていますが、その中で理系の知見と文系の知見を融合させて、技術開発にあたっていく必要があると考えていますが、文系の方が果たせる役割に関してはどのようなものがあるとお考えでしょうか

A14：　文系は技術開発に携わることはできないため、資金面からのバックアップをする役割を担う必要がある。具体的には、文系が理系から技術に関する専門的な話を聞いたうえで、それに合う政策を作っていく動きが求められる。

以上

記録作成担当者：宮内拓

ヒアリング調査報告 No.44 基本情報

日時	2022 年 12 月 16 日
テーマ	東北地域の半導体戦略及び人材育成等について
ヒアリング先 （担当者）	経済産業省 東北経済産業局　地域経済部　製造産業・情報政策課 石川俊介 様 平野景之 様
場所	仙台合同庁舎Ｂ棟（県庁前）3 階
参加者	（WS-C 教授）坪原和洋 教授 （WS-C 学生）稲田凜香、岡本樹、梶山敬生、香高優一郎、宮内拓、山田麻友 （計 7 名）
調査目的	東北地域の半導体戦略やそれに伴う人材育成についてご教示いただき、政策提言に向けた知識のブラッシュアップを行うこと。

（写真）

【レクチャー】

（東北地域における半導体等関連産業基盤の強化に向けて）

経緯として、皆さんも体感していると思うが、ここ数年で我々の生活のデジタル化がかなり進んでいる。コロナ禍がデジタル化を加速させ、デジタル化のための技術も追いついてきた。デジタル社会には半導体が不可欠であり、我々のデジタル社会を支える基盤的な技術・物資である。

このような状況であるため、半導体市場も右肩上がりで成長していくと言われており、約 10 年後には現状の倍である 100 兆円の市場規模になると言われている。半導体は、ロ

ジック（制御用）とメモリ（データ記憶用）とその他に分けられているが、先端のロジック半導体を製造している拠点が日本にはない。他方で、メモリ半導体は、Micron や KIOXIA といった、日本で生産する企業があり、東北では、KIOXIA が岩手の北上にある。また、例えば、イメージセンサーでいうと SONY は鶴岡にあり、アナログ半導体を製造している ON semiconductor は会津若松にある。このように、東北地域にも半導体企業が集積をしているが、先端のロジック半導体については、東北はもとより日本にはないということになる。

これについて、経済安全保障上、日本に生産拠点がなくていいのかという議論があり、先端分野については日本に立地をして根付かせていこうという政府の方針が示され、それに伴い支援策が出てきている。

海外では、例えばアメリカで言うと、CHIPS 法が成立して、この法律に基づいて設備投資や技術開発研究活動のための補助金、減税措置が講じられている。こういった支援措置が 5 年で約 7 兆円規模と、非常に大規模な施策展開がなされておりアメリカをはじめとする各国で大規模な施策が打たれている状況になっている。

このような中、日本でも、まずはハード面で支援措置等を大規模に展開していくという手を打っている。その一つが半導体である。日本にない先端分野について国内回帰をしなければならず、設備投資に対して支援措置を講じていく制度を現在立ち上げている。先端半導体について支援措置を講じるということだ。具体的には、5G 促進法という法律が従来あったが、それを改正し、先端半導体の設備投資を日本で行うために支援措置を講じる法律をここで立ち上げている。当法律は今年の 3 月に施行しており、具体的には、特定半導体生産設備等事業者といった事業者が、設備投資をするための事業計画を策定し、国の認定を受けると支援措置が講じられる、というようなスキームになっている。活用事例として、熊本の TSMC の関係での立地が公表されている。

東北関連では、KIOXIA が岩手にも設備投資を行うが、今回は、四日市の設備にのみ当該措置が講じられる。広い目で見れば KIOXIA に支援措置が講じられることになる。

この支援措置は、令和 3 年度の補正予算において 6,170 億円計上されており、その予算を使って支援措置が打たれ、先端半導体分野を支援するということになる。

もちろん、先端半導体だけで世の中が支えられているわけではなく、パワー半導体等といった従来型半導体も経済安全保障上重要な物資であるため、先端分野以外の半導体にも支援措置が講じられる制度を立ち上げたということになる。これが経済安全保障推進法であり、半導体をはじめとして蓄電池などの指定された物資について、設備投資をするといった事業計画を策定し申請して認定を受けると、支援措置が講じられるというような先程同様のスキームになっている。

ハード設備については、このような制度を活用して今後立地が進むであろう一方で、人材育成も重要。それが「半導体人材の育成・確保に向けた取り組みの強化」だ。これについても、九州地域に一定の集積があるため、まずは九州地域で産学官一体になり人材育成のあり方を検討するコンソーシアムが立ち上がり、人材育成のスキームを立ち上げていく取り組みが進んでいる。東北ではキオクシア岩手や東北大を中心に行っている。九州で 3 月下旬ぐらいに立ち上がり、続いて東北・中国で随時立ち上がっている状況である。東北だけで言うと、次世代の X-nics 半導体創生拠点形成事業という、半導体関連の研究開発を行いながら合わせて OJT で人材育成を進めていくというような文科省の予算があるが、その採択を東北大学は受けている。遠藤哲郎先生にはこちらの半導体人材育成等の検討組織（「東北半導体・エレクトロニクスデザイン研究会」）にも入っていただいており、情報共有を逐次しながら連携をしている。

さらに他の動きとしては、高専の一部カリキュラムの新設が挙げられる。現在、九州地域では佐世保高専や熊本の高専で実証事業を行っている。そこでモデルカリキュラムを策定し、さらにそれを全国の高専に横展開しようという動きになっている。横展開するに当たっては、各地域に特徴・特色があるため、それらを踏まえた上でカリキュラムを一部ロ

ーカライズして構成していく。例えば、九州の高専では半導体の実習を行うのに九州地域の大学の施設を活用できるが、東北では人材育成を行うために九州のそのような施設を活用するわけにはいかないので、東北地域では東北大学の試作コインランドリという施設を活用して実習をやっていこうというような調整を進めている。

【質疑応答】
1.半導体についてのご質問
Q1：　東北半導体キックオフ会合はどのような目的で開設されたのでしょうか。
A1：　レクチャーの続きとなるが、このような状況より、人材育成等のあり方を考えていく組織として、東北半導体・エレクトロニクスデザイン研究会を 2022 年 6 月 10 日に立ち上げて、1 回目のキックオフ会合を 7 月 4 日に行った。参画メンバーとして産学官に入っていただき、現在 67 者の企業等に参画いただいている。
　この研究会では、「人材育成・確保」、「サプライチェーン強靭化」、「半導体等関連技術研究の推進」について、検討をしていくこととなっている。今年度及び来年度で検討していこうということになっており、鋭意進めているところである。我々の事務局で推進策のイメージを提示し、これに対する意見をいただきながら、検討を重ねている。
　人材育成・確保という面で特に言及されるのが、特に地域の若年層が半導体や企業についてわからないということである。東北の主要な半導体企業であっても、若年層の間では企業名があまり知られていないことがある。企業の知名度不足や半導体への理解不足があり、就職の際に半導体企業に着目して就職活動をしない、というようなお話もある。したがって、まずは半導体そのものを知っていただく、企業の魅力そのものを知っていただくということをやるべきではないかと考えている。例えば、魅力を発信する動画を作ることや、工場見学を行うことで、少しでも知名度をアップできないか、魅力を発信できないか考えている。
　また、人材育成のプログラム構築として座学と実習を考えている。実習については、東北大学の試作コインランドリを活用した実習を考えている。当施設には、半導体の各工程の製造装置が 100 台以上あり、こういった実機で、実際に半導体のプロセスを体感しながら知っていただく実習を行いたいと考えている。
　さらに、インターンシップについて、企業の魅力を発信しながら人材育成も行えるという意味で、非常に重要だというようなお声も多くあったため、先行してインターンシップの調整を始めている。さらに、高専機構のカリキュラムの横展開をしていき、また、共同研究の推進を行う予定で、具体的には、企業との共同研究を通して、OJT で学生のレベルアップに直結し、また、企業のスキルアップに繋がるようなイメージである。
　サプライチェーンの強靭化という面では、先ほど先端ロジック半導体の製造能力が日本にはないという話だったが、先端半導体という意味では、東北では KIOXIA が北上にあり、SONY 鶴岡で先端的なイメージセンサーを作っており、ウエハーサイズでいうと 300 ミリに対応している。それ以外の企業は 200 ミリや 120 ミリの小さいサイズのウエハーを使った製造装置で半導体を作っている。これらの企業では 20～30 年前の設備を使って半導体を製造しているところもあり、製造装置の老朽化が著しく進んでいる。既に生産が中止された装置部品もある一方、老朽化した設備を上手に延命化しながら使用している企業があることが実情だ。このように設備を延命化させながらうまく使っていくためには、一社単独では難しいため、ネットワークを組みながら知恵を出し合い効率的・効果的な延命策を検討していく必要がある。
　その他、交流不足や物価高騰といった課題はあるが、それぞれ必要に応じて研究会で課題解決方策を検討していくこととなっている。また、東北地域の集積状況についてはまだまだ整理しきれていない。集積状況をマップ等に整理することによって、サ

プライチェーンを地域内に持っていきたい企業が、この企業と組めば地域内でうまくサプライチェーンを作れるということもあるので、企業同士のネットワーク強化及び基礎データとして、現在集積状況をまとめているところである。

半導体等関連技術研究の推進という面では、東北地域でどのような技術開発を行いたいかというニーズを企業にとりながら、大学等の研究シーズの整理をしてうまくマッチングできるような方策を検討するということで進めている。そこで、先程の共同研究及びハイレベルな人材育成に繋がるような仕組みができないか検討している。

Q2： 日本の半導体産業におけるハイレベル人材、ワーカー人材の特徴や強みとはそれぞれ何でしょうか。

A2： ハイレベル人材について、教育制度の観点から、各国を比較して、日本がどのような特徴を持っているかお話する。

現在半導体のトップを走っている国のひとつであるアメリカについて、先日行われたSEMICON Japan2022でのIBM Darío Gil氏の講演によると、大学の研究室に企業から多額の融資が入っており、研究室ごとベンチャー企業になる流れになっている。一方で大学から人材がたくさん出てしまうといった課題もあり、大学の空洞化が進んでいる。このような教育制度がアメリカの特徴だ。

続いて、近年の世界の半導体産業を牽引している台湾について、TSMCが国立台湾大学大学院に半導体専攻科というのも昨年設立した。集積回路学部という、日本では作ることが難しいロジック系の回路を専門に学ぶことができる。このように、有力企業が大胆に大学の教育に入り込んでいることが台湾の特徴の一つとなっている。

韓国も似たような傾向になっており、大学入学とともに企業への内定が決まる「契約学科」の設立を検討している。韓国の有名企業であるサムスンや、メモリにおいて韓国で2番目にシェアを持つSKハイニックスが、韓国の有力大学に学科を設立して人材確保を進めるという動きになっている。これについても、有力企業及び有名大学が都市部に多いため、契約学科を作ることで都市部により人が集中するといった課題はあるが、現政府は進めていく方針になっている。

一方日本については、アカデミカルな教育を行っている。これは、半導体等を学ぶ際に、出口の製品から学ぶのではなく、半導体の材料や仕組み、電圧をかけた際のコンデンサの動きなど、基礎からコツコツと教えていくような教育環境である。実際の製品に応用できるような専門性や出口の製品に関しては、企業に入ってから習得する流れになっている。

この教育方針は大学の教員や共同研究を行う研究者とのOJT教育のような形になっており、大学の先生からしっかりと教わることができる環境がある。

ワーカー人材について、一般的に言われている現場の強みとして、日本は伝統的に「摺り合わせ」が得意とされている。摺り合わせは産業界でよく使われる言葉で、一つの部品の要素が他方に波及するような場合の塩梅の取り方であったり、それぞれの特徴の強みを最大化するような部品の組み合わせを導き出したりすることを指す。今までは自動車業界での強みとされていたが、近年、半導体分野でも言及されている。特に先端半導体の分野で、チップ同士を直接組み合わせるチップレット構造が進んでおり、この構造は各部品の構造が別の部品に直接的に影響しやすい構造であり、日本が得意としている摺り合わせが発揮される期待ができる。このチップ構造の変革によって日本は優位性を得られる可能性がある。

Q3： 日本では、実際に開発研究をしていたとしても製品化に至るまでにかなり困難があるという話をお聞きします。企業からの融資をもとに研究室で行った内容を、ベンチャーを起業して活かすといったアメリカのような動きは、日本において今後起きうるのでしょうか。

A3：　産学官連携のため、東北大学のなかで「半導体テクノロジー共創体」を設立した。これは、大学と企業が協力してオープンイノベーションを目指し研究することを目的とした組織であり、大学の研究室の技術が社会実装されていくという動きは少しずつ起きていると思う。

Q4：　企業と大学の繋がりを作っていく際に重要なこと、また、その際の貴局や貴省の役割・果たすべきことについて教えてください。
A4：　研究会活動の中で、各企業からのニーズ及び各大学からのシーズを聞き出すといったことをしており、今後は当局でシーズとニーズのマッチングをしていきたいと考えている。

Q5：　日本は台湾や中国に比べて半導体の製造コストが高いとお聞きします。イコールフッティングとなる支援としてどのようなものが考えられるのでしょうか。
A5：　経済産業省の最近の傾向として、製造コストよりもむしろ経済安全保障を重要視している。国際情勢の中で、日本にとって必要な物資が国外から入って来なくなると困るため、重要物資の生産拠点を国内に回帰させるような、予算配分がなされているところである。令和4年度の補正予算においては、重要物資を国内で生産するための予算として「経済環境変化に応じた重要物資サプライチェーン強靭化支援事業」が策定されており、重要物資として指定されている半導体やデータセンター等のクラウド、蓄電池等の産業を日本に回帰させることを目的に計上されている。「ポスト5G通信システム基盤強化研究開発事業」といった予算は、研究開発という名前がついている通り、先端半導体の研究開発を推進するための予算になっている。「先端半導体の国内生産拠点」といった予算も、半導体の国内生産拠点の確保を推進するものである。
　このように、かなりの予算額をつけて先端半導体をはじめとする重要指定物資を国内に回帰させる動きが進んでいる。生産コストを低下させることよりも経済安全保障に資する予算組みがされている状況である。

Q6-1：　政策提言の一つとして、補正予算の一つである「半導体サプライチェーンの強靭化支援」の2,163億円を利用し、非常時における半導体を備蓄することを考えている。備蓄に関しまして、その方式や備蓄の場所等、備蓄をするにあたって注意する点がございましたら教えてください。
A6-1：　国として半導体を備蓄することは現状考えられてはいない。各企業それぞれで必要に応じて備蓄はしていくことはある。気をつける点として、あまり多く持ちすぎると、不良在庫、資産だけを持つことになるため、企業の判断にはよるが、貯め過ぎず、持たなすぎずというバランスに気をつけなければいけないと思う。備蓄しなくて済むように国内回帰を進めている点もある。

Q6-2：　もし施行するとしましたら、技術の進歩等を踏まえると、どの程度貯められるものなのでしょうか。
A6-2：　従来型半導体に限ると、半導体を使う家電（エアコンや冷蔵庫）は10年程度までは修理しながら使っている方も多く、修理するためにその半導体が必要なため、その期間は貯める必要があるのではないかと思う。

Q7：　半導体について大企業・中小企業問わずサプライチェーンを止めないためにはセキュリティ対策が必要になってくると思います。セキュリティ対策を進めていく上で問題となっていることはあるのでしょうか。
A7：　半導体を始め、日本のサプライチェーンにおいて、セキュリティ対策を進めることは極めて重要である。昨今、技術の高度化に伴い、技術資産の価格が高騰している。

例えば半導体は技術の高度化が進んだことによって、一つの企業で単独で作ることが難しくなっており、それぞれの工程を分業しなければいけないことから、セキュリティ対策の範囲が拡大している。工場のネットワーク環境についても、IoT が進んでいる中で不適切な取り扱いや不適切なネットワーク構築からウイルスが侵入してしまう場合がある。製造装置間のちょっとしたネットワーク環境についてもセキュリティが大切になってくる。そして、サプライチェーンへの攻撃においては、情報セキュリティ対策が強固とは言えない中小企業を対象としたサイバー攻撃も顕在化していることから、強化することが求められる。IPA では「中小企業の情報セキュリティ対策ガイドライン」を策定している。セキュリティ対策を進めていくためには、社員教育といった理解促進や対策のための投資が必要となる。費用面の問題については IT 導入補助金において IT 導入補助金セキュリティ対策推進枠が創設された。

Q8： 今後日本が最先端技術を研究開発していくうえでは、人材育成・確保がとても重要であると思います。産学官のそれぞれに求められる役割や連携の在り方とはどのようなものなのでしょうか。

A8： 先程の話にもあったように、東北経産局は半導体研究会を立ち上げ、産学官連携して東北ないし日本の導体関連産業を盛り上げていこう・推進させていこうという取り組みを行っている。東北管内においては、最先端技術にこだわることなく裾野を広げていこうという取り組みを進めている。

人材確保については、半導体業界の魅力発信手法を検討している。どのような魅力発信の仕方をしたら効果的なのか学校側の意見を聞くことや、企業がどのようなことをアピールすればよいのか聞き出すことといった、より効果的な PR 方法等を産学官連携しながら考えている。

人材育成については、企業と学校を連携して、学校で行われる教育に企業の出前講座等を設けることで、企業が本当に欲している人材を育成する方針を考えている。実際に手を動かす実習については、東北大学の力を借りて、半導体のプロセスを学生に理解してもらうことや、企業の若手社員等に参加してもらい共に半導体について学んでもらえたらなと思っている。インターンシップについても、インターンシップは企業にとっては大事な PR の場面になり、学生にとっても貴重な学習の場になるため、東北経産局側で取りまとめながら産学官連携していければと思いこのような取り組みをしている。こういう取り組みに産官学それぞれが積極的に参加していただくことが求められており、私達が期待しているところでもある。

Q9： 大学などの教育機関との協力、連携で特に心掛けていることがございましたらご教示いただけますと幸いです。

A9： 我々官の側が研究会を取り持っているが、そこには大学の先生といったスペシャリストの力が必要であり、一緒にやっていきましょうという姿勢を心がけている。

2.産官学連携における情報共有体制等についてのご質問

Q10-1： 東北地域サイバーセキュリティ連絡会について、地域経済部 製造産業・情報政策課が主導をされていると理解しております。その概要について、特に・構成員の受入・事務局の役割・活動内容の具体的事項・国のサイバーセキュリティ協議会及び宮城県サイバーセキュリティ協議会との連携等について、教えていただけますと幸いです。

A10-1： サイバーセキュリティは一社で行っていくものではなく、周知等も含めてなるべくたくさんの方と情報共有をしながら行っていくことが重要になっており、県の取り組みだけではなくそれを連結して東北の取り組みさらには国の取り組みと連結していくことが重要である。それがまさに東北地域サイバーセキュリティ連絡会で

ある。
　活動内容について、例えばサイバーセキュリティに関する最新情報の提供を、先日 11 月 4 日にあったようなセミナーを通して東北局で開催している。また、基本的に情報共有がメインであり、構成員等からの情報共有をメールベースで行っている。

Q10-2：構成員につきまして、官側から決められたのでしょうか、それとも募集等をかけて決められたのでしょうか。また、心掛けた点等はございますか。
A10-2：官側で決めた。当連絡会を立ち上げた際に、東北総合通信局と当局で連携をして現構成員の団体、東北経済連合会や東北商工会議所等、我々と関係の深い業界団体に参画をお願いした。
　政策を企業に届けることは非常に難しく、課題ではあり、情報が行き届くように、という理由でこういった業界団体を入れている。当局は数多くの業界団体を持っているので、我々が入る連絡会に入ることで様々な企業に情報が届くスキームにはなっている。

Q10-3：　活動内容の 3 つ目につきまして、メールベースで構成員相互の情報共有を行うとのことでしたが、官からのみならず、官への情報共有等もあるということでしょうか。
A10-3：　スキーム的にはそうであるが、一企業の情報は機密情報になるため、そのような情報は匿名であってもメールで構成員に共有するということはしない。個別の企業でお困り事があれば、東北経連の会員企業であれば東北経連へ相談をして、東北経連が我々や総通局・宮城県へ個別に相談するかたちになると思う。

Q10-4：　国の機関で財務局と農政局は入っていますが、なぜこの 2 つだけが入っているのでしょうか。
A10-4：　財務局は銀行、農政局は食品加工業を所管しており、情報を少しでも企業にいきわたらせるように、民間企業を所管している局に入ってもらっている。もっとも、連絡会は発足したばかりであり、今後は他局の入会も考えられる。

Q10-5：　東北の広域に活動している団体が含まれていますが、企業の方から東北地域と宮城県のどちらの協議会に入るべきか問われることはありますか。
A10-5：　ない。基本的に、個別企業は東北地域サイバーセキュリティ連絡会には入っていない。事業者についてもセキュリティサービスを提供する側に入ってもらっている。一方、宮城県サイバーセキュリティ協議会にはセキュリティを強化しなければいけない企業も入っており、両協議会でたてつけが異なっている。

Q11：　産官学の連携強化として取り組んでおられる政策について、産学連携オープンイノベーション拠点の整備、東北産学官連携協議会・リエゾンネットワーク会議の大学の活用に関してご教示いただけますと幸いです。
A11：　東北管内には、土地柄を活かして、オープンイノベーションを進めていくようなイノベーションアセットが様々ある。そのような中で、東北地域リエゾンネットワーク会議を開いている。これは、東北産官学連携協議会が置き換わったものであり、開催意義として、各大学等の横の繋がり、ネットワーク構成を進めることが挙げられ、国が主導して進めている。その中では初めの一歩的な取り組みとして、顔合わせや名刺交換を実施し、情報交換等を行うための会議として運営している。参加校は大学や高専などの計 26 機関であり、基本的にメルマガという形で様々な情報を共有している。

産学連携オープンイノベーション拠点整備の取り組みとして、「地域オープンイノベーション拠点選抜制度（J-Innovation HUB）」が、東京で進められている。大学等の企業とのイノベーション拠点を選抜して、経済産業省で伴走支援等を行っていくという施策である。伴走支援の中では、国から施策の紹介や連携強化を行う。東北管内からは、国際展開型として遠藤先生がいらっしゃる「東北大学国際集積エレクトロニクス研究開発センター（CIES）、「山形大学有機エレクトロニクスイノベーションセンター（INOEL）、地域貢献型として「岩手県のものづくり技術研究センター」、「会津大学産学イノベーションセンター（UBIC）・復興支援センター（ARC）」の4拠点が選出されている。

（追加質問）

Q12：　半導体の人材育成やこういったオープンイノベーティブ構想につきまして、福島イノベーションコースト構想や浪江町にできる高等教育機関の構想が今後動き出し、東北大も参加するといった話をお聞きしたが、そのような動きとの連携や関係はあるのでしょうか。

A12：　連携や関係は今のところない。

Q13：　レガシー半導体の備蓄に関して、現在レガシー半導体の生産能力増強が求められており、他国から我が国に対し強い期待が寄せられているということですが、今後補助金を与えて生産能力を増強したとして、需要がそれに追いつくような形になると思っています。現在、中国が半導体の装置を規制されているためレガシー半導体に注力するという話を聞き、日本と中国がレガシー半導体を巡り価格競争といったことを引き起こすのではないかと思っており、一定程度日本政府レガシー半導体を買い取り備蓄することの正当性はあるかと考えています。このような動きがあったとして、備蓄は行っていくべきなのでしょうか。

A13：　需要という観点から言うと、今後日本はEV車をたくさん生産していくことも想定され、従来型半導体の必要性が高まるため、半導体の需要という面では今後さらに拡大していくと考えている。

もっとも、備蓄に関して、政府の備蓄は想定されていないものと考える。半導体と一口に言っても相当な種類あり、これを一括で備蓄をして、管理をして、必要なところに届けることは個人的には難しいのではないかと思う。

Q14：　先端分野の半導体について、国際情勢が変化する中、日本への供給が滞る場合、東北地域で大きな影響を受ける企業等はあるのでしょうか。

A14：　先端分野の半導体を使う東北企業について、例えば、パソコンの製造工場が米沢等にあるが、そういったところは在庫不足になるという影響はあると思う。また、従来型半導体の不足という話を耳にする。

Q15：　東北地域において、経済安全保障という考え方が企業や大学にはどの程度浸透しているのでしょうか。

A15：　企業や大学で経済安全保障についての議論はあまりしていないため、お答えすることが難しい。

以上

記録作成担当者：岡本樹

東北大学公共政策大学院
令和 4(2022)年度　公共政策ワークショップⅠ　プロジェクトC

「我が国の経済安全保障の確保に向けた研究」

学生　稲田凜香　岡本樹　織田秀夫　梶山敬生
　　木戸友香子　香髙優一郎　宮内拓　山田麻友

主担当教員　坪原和洋教授
副担当教員　阿南友亮教授　西本健太郎教授、今西淳教授