「我が国が戦略的に育てるべき
安全・安心の確保に係る重要技術等の検討業務」
報告書

令和 5 年 3 月

国立大学法人 政策研究大学院大学
政策研究院

報告書目録

報告書　上巻

報告書　下巻

はじめに

感染症の拡大、サイバー攻撃やテロ、新興技術やイノベーションを巡る競争、ロシアのウクライナ侵略など、近年、我が国を取り巻く国際情勢は大きく変化、複雑化し、地政学的な緊張が高まるとともに、関連する科学技術を巡る動向は国際経済秩序へも影響を与えている。国民生活や経済活動に対するリスクが一層顕在化している中、様々な脅威に対して国家・国民の安全・安心を確保する上で、関連する重要な技術分野に予算、人材等を重点的に配分し、関係省庁、研究機関等が更に連携を強化し、必要な研究開発を効果的に推進する必要性が高まっている。

上記の問題意識から、「国及び国民の安全・安心の確保に向けた科学技術の活用に必要なシンクタンク機能に関する検討結果報告書」（令和 3 年 4 月内閣府）に基づき、シンクタンク機能を立ち上げ、実際に運用することにより、我が国が戦略的に育てるべき安全・安心の確保に係る重要技術や国内外の戦略等の検討を進め、政府の重要技術等に係る課題の政策決定等に資することを目的として調査研究を行った。

「知る」、「育てる」、「生かす」、「守る」の観点から重要な技術分野について関連情報を収集、分析、調査、研究し、対応策を提示した。科学技術・イノベーションに関する高度な知見を持ち、安全保障の観点も備えた専門家人材の確保、プロジェクトを通じた高度専門人材の育成、専門家ネットワークの構築を行った。また、国内外関係機関との連携ハブ機能と技術シーズ及び政策ニーズの関係情報の集約ハブ機能を提供した。

広範囲調査分析では、政府が提示した 20 の技術調査分野を対象に、安全・安心に関する脅威の動向、諸外国の政策・戦略、脅威に対する重要技術に係る国内外の研究開発動向を調査し、日本の強み、弱みなど課題を分析、整理した。個別調査分析では、特に海洋・宇宙、サイバー、健康・医療の個別分野について、具体的な技術のニーズ、シーズの深掘り調査、分析を行い、ニーズとシーズのマッチングや関連する世界の技術研究開発動向を勘案して安全・安心の観点から育て守るべき重要技術等について示し、社会実装の方策も併せて検討した。

チーム全体として、内外の関係機関・シンクタンクと連携しネットワークを構築しながら、情報収集や調査分析手法の検討、人材育成の実施・検討も含めて推進した。関係省庁との意見交換会や周知広報活動も可能な範囲で積極的に行った。特定された技術の用途、特に公的利用と民生利用の「マルチユース・多義性」の側面についても検討を行った。シンクタンク機能を発揮する事業活動に重要な情報セキュリティ体制構築についての基本的な概念整理も提供した。

本調査研究を実施する間、経済安全保障推進法（「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））が令和 4 年 5 月 11 日に国会で成立し、同月 18 日に公布された。同法では、第四章に「特定重要技術の開発支援」が規定され、その中には調査研究や特定重要技術調査研究機関についても規定された。令和 4 年 9 月 30 日には「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」も閣議決定された。また、「経済安全保障重要技術育成プログラムの第 1 次研究開発ビジョン（令和 4 年 9 月 16 日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）」に基づき「経済安全保障重要技術育成プログラム」（いわゆる K Program）がスタートして

いる。さらに、内閣府において「安全・安心に関するシンクタンク設立準備検討会」が令和 4 年 11 月 29 日から検討を開始し、法人立ち上げに向けた本格的な検討に入るに至った。

本調査研究では、特に令和 4 年夏以降はこうした新たな動向も踏まえながら内外関係者と意思疎通や連携を行いながら調査研究を進めたところである。本事業及び調査報告の内容が今後のシンクタンク機能事業の発展に向けた一助になることをプロジェクト参加者一同切に希望する。

令和 5 年 3 月

プロジェクト参加者一同

報告書総論

Ⅰ．実施体制について

令和 4 年度「我が国が戦略的に育てるべき安全・安心の確保に係る重要技術等の検討業務」については、令和 4 年 4 月 1 日から令和 5 年 3 月末にかけて、以下の体制で実施した。令和 3 年度事業の成果も融合・活用し、令和 4 年度の新たな調査研究を一層発展させ、事業全体として成果をまとめた。

１．実施体制全体

本事業の業務統括者、各分野にプロジェクト・マネージャー（PM）等を置き、併せて広範囲 20 分野の調査の実施を進めた。内閣府が特に政策ニーズが重要であると判断した分野として、健康・医療、サイバーセキュリティ、海洋・宇宙の 3 分野について重点的に検討を進めた。

業務統括責任者は、白石隆政策研究大学院大学名誉教授、政策研究大学院大学政策研究院チーフ・エグゼクティブ・ディレクターが務め、業務総括責任者は、風木淳政策研究大学院大学政策研究院参与が務めた。本受託事業の業務実施計画の運営事項に関しては大学全体として政策研究大学院大学の大田弘子政策研究大学院大学学長が受託責任者である。

業務を統括するボードとして、令和 3 年度に引き続き、運営ボードを設置し毎月 1 回、定期的に会合を開催し、重要事項について討議を行った。また、国内の関係機関との連携、関係省庁との意見交換、海外シンクタンクとの連携を行った。

就任メンバー（五十音順）

- 浦島充佳　　東京慈恵会医科大学教授（健康・医療分野 PM）
- 齊藤孝祐　　上智大学総合グローバル学部准教授（20 分野プロジェクト・リーダー）
- 阪口　秀　　笹川平和財団常任理事・（兼）海洋政策研究所長（海洋分野 PM）
- 佐藤丙午　　拓殖大学国際学部教授
- 白石　隆　　政策研究大学院大学名誉教授・同政策研究院チーフ・エグゼクティブ・ディレクター（業務統括責任者）
- 鈴木一人　　東京大学公共政策大学院教授（宇宙分野 PM）
- 角南　篤　　笹川平和財団理事長・政策研究大学院大学学長特別補佐
- 手塚　悟　　慶應義塾大学環境情報学部教授　（サイバーセキュリティ分野 PM）
- 粗　信仁　　政策研究大学院大学特任教授・同政策研究院参与
- 風木　淳　　政策研究大学院大学政策研究院参与（業務総括責任者）
- 加用利彦　　政策研究大学院大学政策研究院参与
- 石井康彦　　政策研究大学院大学政策研究院参与
- 笠谷圭吾　　政策研究大学院大学政策研究院参与補

２．調査・分析チーム

調査・分析チームについては、①内閣府が提示する個別課題（内閣府が特に政策ニーズが明確であり、重要であると判断する 3 分野（(i)健康・医療、(ii)サイバーセキュリティ、(iii)海洋・宇宙）に対する調査分析（個別調査分析）毎に編成し、プロジェクト・マネージャー（PM）を置き（(iii) 海洋・宇宙については、海洋、宇宙それぞれに PM を置いた)、②内閣府から提示する調査分野に対する国内外の情勢や研究開発動向についての調査分析（広範囲調査分析）についても 1 チーム編成し、プロジェクト・リーダーを置いた。各調査・分析チームについては、プロジェクト・マネージャー／リーダーを責任者に、以下の体制で実施した。

（１） 健康・医療

プロジェクト・マネージャーには、浦島充佳東京慈恵会医科大学教授が就任した。

プロジェクト・メンバーとしては、

- 相良祥之　　アジア・パシフィック・イニシアティブ（API）主任研究員
- 中村勝美　　日興技化株式会社技術部担当部長（化学）
- 梅山吾郎　　福祉防災コミュニティ協会理事・会計
- 阿部圭史　　政策研究大学院大学政策研究院シニア・フェロー
- 坂元晴香　　政策研究大学院大学政策研究院シニア・フェロー
- 小笠原律子　　政策研究大学院大学政策研究院リサーチ・フェロー
- 大谷カタリーナ　　政策研究大学院大学政策研究院リサーチ・フェロー
- 星本峻一郎　　政策研究大学院大学政策研究院リサーチ・フェロー　等が参加した。

（２） サイバーセキュリティ

プロジェクト・マネージャーには、手塚悟慶應義塾大学環境情報学部教授が就任した。

プロジェクト・メンバーとしては、

- 野口和男　　慶應義塾大学 SFC 研究所上席所員
- 甲斐　賢　　政策研究大学院大学政策研究院リサーチ・フェロー
- 近藤賢郎　　政策研究大学院大学政策研究院リサーチ・フェロー
- 原澤克嘉　　政策研究大学院大学政策研究院リサーチ・フェロー　等が参加した。

（３） 海洋

プロジェクト・マネージャーには、阪口秀笹川平和財団常任理事・（兼）海洋政策研究所長が就任した。

プロジェクト・メンバーとしては、

- 赤松友成　　笹川平和財団海洋政策研究部長
- 池田徳宏　　富士通システム統合研究所安全保障研究所長
- 石原靖久　　海洋研究開発機構グループリーダー
- 谷　伸　　科学技術・学術審議会海洋開発分科会委員

・　中島　敏　　元海上保安庁長官
・　古庄幸一　　第 26 代海上幕僚長
・　吉武宣之　　笹川平和財団海洋政策研究所　特別研究員
・　川井大介　　政策研究大学院大学政策研究院リサーチ・フェロー
・　上砂考廣　　政策研究大学院大学政策研究院リサーチ・フェロー
・　中山衣美子　　政策研究大学院大学政策研究院リサーチ・フェロー
・　大村　崇　　政策研究大学院大学政策研究院リサーチ・フェロー　等が参加した。

（４） 宇宙

プロジェクト・マネージャーには、鈴木一人東京大学公共政策大学院教授が就任した。
プロジェクト・メンバーとしては、

・　石澤淳一郎　　宇宙航空研究開発機構技術領域主幹
・　木村俊義　　宇宙航空研究開発機構グループ長
・　小林啓二　　宇宙航空研究開発機構ハブマネージャ
・　川井大介　　政策研究大学院大学政策研究院リサーチ・フェロー
・　上砂考廣　　政策研究大学院大学政策研究院リサーチ・フェロー
・　中山衣美子　　政策研究大学院大学政策研究院リサーチ・フェロー
・　大村　崇　　政策研究大学院大学政策研究院リサーチ・フェロー　等が参加した。

（５） 広範囲調査

プロジェクト・リーダーには、齊藤孝祐上智大学総合グローバル学部准教授が就任した。
プロジェクト・メンバーとしては、

・　奥田将洋　　科学技術振興機構研究開発戦略センターフェロー
・　土屋貴裕　　京都先端科学大学経済経営学部准教授
・　部谷直亮　　慶應義塾大学 SFC 研究所上席所員
・　村野　将　　ハドソン研究所研究員
・　岩城洋子　　政策研究大学院大学政策研究院リサーチ・フェロー
・　大村　崇　　政策研究大学院大学政策研究院リサーチ・フェロー
・　上砂考廣　　政策研究大学院大学政策研究院リサーチ・フェロー
・　川井大介　　政策研究大学院大学政策研究院リサーチ・フェロー
・　近藤賢郎　　政策研究大学院大学政策研究院リサーチ・フェロー
・　佐藤真央　　政策研究大学院大学政策研究院リサーチ・フェロー
・　滋野井宏記　　政策研究大学院大学政策研究院リサーチ・フェロー
・　中山衣美子　　政策研究大学院大学政策研究院リサーチ・フェロー　等が参加した。

プロジェクト・メンバーのうち、土屋貴裕京都先端科学大学経済経営学部准教授、川井大介政策研究大学院大学政策研究院リサーチ・フェローは、プロジェクト・リーダーとともに広範囲調査

の関係会議に出席して全体調整に参画した。
その他、古谷知之慶應義塾大学総合政策学部教授は、重要・新興技術全般についての開発動向と安全保障上の含意に関連して参画した。広範囲調査の分析には、事務局より笠谷圭吾政策研究大学院大学政策研究院参与補が「マルチユース・多義性」調査を含め横断分析に参画し、青木崇政策研究大学院大学政策研究院シニア・フェローが3年度調査を俯瞰した補論や横断分析に参画した。

（参考）分野と責任者

分野	責任者（プロジェクト・マネージャー／リーダー）
個別調査：健康・医療	浦島充佳　東京慈恵会医科大学教授
：サイバーセキュリティ	手塚　悟　慶應義塾大学環境情報学部教授
：海洋	阪口　秀　笹川平和財団常務理事・（兼）海洋政策研究所長
：宇宙	鈴木一人　東京大学公共政策大学院教授
広範囲調査：	齊藤孝祐　上智大学総合グローバル学部准教授

３．事務局機能（総括・企画部門等）

政策研究大学院大学政策研究院に総括・企画チームを置き、運営ボードの運営、各調査チームの進捗管理、関連会議の事務処理、内外委託調査事務処理、総論関係の関連調査研究などを行った。

Ⅱ．調査分析の成果

１．広範囲調査分析

（１） 調査研究の範囲

政府が提示する調査分野について、安全・安心に関する脅威の動向、諸外国の政策・戦略、脅威に対する重要技術に係る国内外の研究開発動向を調査し、日本の強み、弱みなど課題を分析、整理した。

調査研究 20 分野：

- ○バイオ技術
- ○医療・公衆衛生技術（ゲノム学含む）
- ○人工知能・機械学習技術
- ○先端コンピューティング技術
- ○マイクロプロセッサ・半導体技術
- ○データ科学・分析・蓄積・運用技術
- ○先端エンジニアリング・製造技術
- ○ロボット工学
- ○量子情報科学
- ○先端監視・測位・センサー技術
- ○脳コンピュータ・インターフェース技術
- ○先端エネルギー・蓄エネルギー技術
- ○高度情報通信・ネットワーク技術
- ○サイバーセキュリティ技術
- ○宇宙関連技術
- ○海洋関連技術
- ○輸送技術
- ○極超音速
- ○化学・生物・放射性物質及び核（CBRN）
- ○先端材料科学

注：調査研究 20 分野は「経済安全保障法制に関する有識者会議資料（令和 4 年 7 月 25 日）」で調査対象領域として公表された。さらに経済安全保障推進法上の「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」（令和 4 年 9 月 30 日閣議決定）に「令和 3・4 年度内閣府委託事業「安全・安心に関するシンクタンク機能の構築」における広範囲調査の対象領域」として記載されている。

（２）調査研究の概要

安全・安心、経済安全保障の文脈を踏まえ、調査研究 20 分野について、全体を俯瞰して注目される諸技術の動向を捉えつつ、技術領域間の相互関係や課題も含め、「脅威」、「ニーズとシーズ」、「デュアルユース」、「マルチユース・多義性」、「社会実装」などの重要な要素を念頭に調査を行った。

オープンソース調査とインタビュー・意見交換、調査委託を組み合わせ網羅的に実施した。情報収集・データ分析の意見交換や連携を行い、また、特定の科学技術に関する知の生産能力や対外依存の状況、及び喪失リスクを検討するために、国内外における知的生産能力の分布を、学術論文データベース、研究機関・研究者の所在や連携に関する各種情報なども活用しながら調査を行った。

広範囲調査を通じて、健康・医療、サイバーセキュリティ、海洋・宇宙との関連、あるいはその他に深掘りすべき分野なども模索した。

（３）技術の特定

調査研究 20 分野の内外の技術動向につき脅威シナリオを踏まえつつ俯瞰した。AI や量子などの注目分野では同世代技術の競争における総合的な優位の確保が大変な中で、量子・高度情報通信の次世代技術への先行投資の可能性や領域横断的な技術開発の重要性を指摘した。特に日本が伝統的・相対的優位のある技術分野の、先端材料、ロボット工学、先進計算等について、他の技術分野への応用の重要性を指摘した。

「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）（令和 4 年 9 月 16 日決定）」の中で相当程度の分野が取り上げられた一方、更なる分野の深掘り（先端材料など）やバイオ、サイバー分野での更なる調査分析は課題であった。分析手法・指標の開発等のデータ分析を通じた技術の特定も継続的な課題であった。

（４）「マルチユース・多義性」の分析

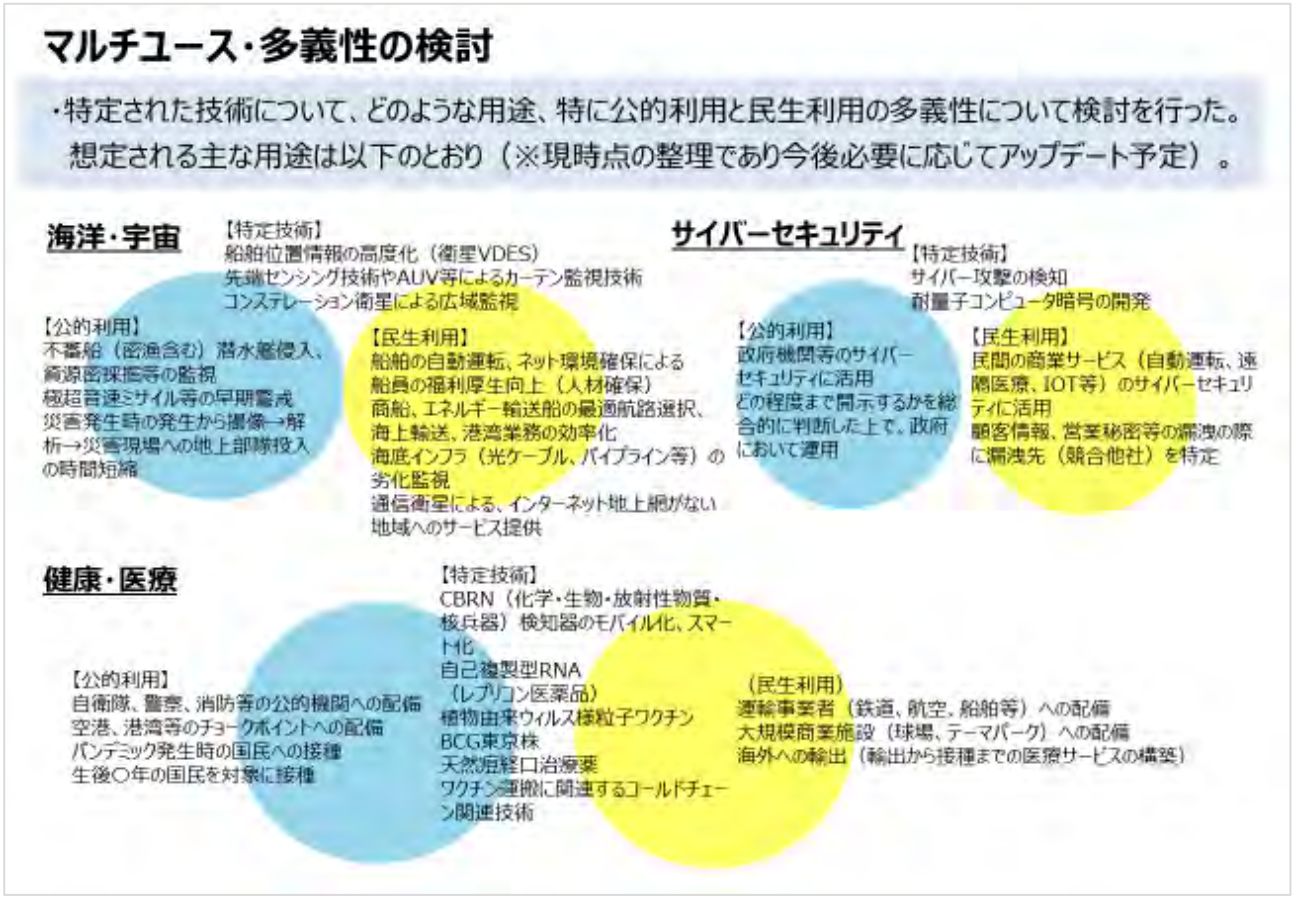
科学技術の研究開発の成果は、研究者の意図を超えて、学術的な成果だけでなく、産業利用、防災利用、社会システム・インフラの維持、安全保障などの多様な用途に使われ得る。特に新興技術においては、予め用途が特定されるものではない。半導体技術は、家電、自動車等で人々の生活を支える一方、将来の空飛ぶクルマの運航やメタバースの構築に資するとともに、既に AI の演算能力向上やドローン、ミサイル等の誘導に使用されている。また、光学センサー技術は、医療、学術研究用途から、防災や安全保障の用途に使われている。ロシアによるウクライナ侵略や、エネルギー問題・脱炭素、高齢化・人口減少などの幅広い社会課題に関連し、技術的成果の実装レベルは国家・国民への影響を増している。こうした状況を踏まえ、本研究調査では、広範囲調査の一環として「マルチユース・多義性」の分析を年度後半に追加的に行った。

「科学技術の多義性」の用語は、第 6 期科学技術・イノベーション基本計画で使用されており、直近では政府文書に「マルチユース」の用語が使用され始めている。具体的には、①技術の用途（公的利用か民生利用か）、②ユーザー（公的機関か民間か）、③技術を獲得するための資金の出し手、などの観点から整

理が必要とされた。特に③については、社会実装との関係で民間企業側の市場への期待や規模がどの程度かによって民間の主体的な商業的取り組みと公的支援の必要性との間に程度の幅がある。戦略的自律性や不可欠性が求められる技術について、官民協議会などの初期の段階から技術の成熟度に応じた対応が必要であり、公的支援（資金提供の他、アンカーテナンシーや試験環境提供等の調達面も含む）の在り方や知的財産権や標準化の扱いなどの課題への対応に向け、今後もシンクタンクでの一層の横断的分析や貢献が期待される。

海洋・宇宙、サイバーセキュリティ、健康・医療分野について「マルチユース・多義性」を例示したものは以下の参考１のとおりである。（令和 5 年 2 月 8 日経済安全保障重要技術育成プログラムに係るプログラム会議（第四回）において政策研究大学院大学政策研究院より資料として説明・提示したもの。）

参考１：マルチユース・多義性の検討



（５）補論（令和 3 年度調査の俯瞰的評価 SWOT 分析）

令和 3 年度に実施した 20 の技術分野（技術的に更に細分整理して 23 分野）の調査について、横断的な整理手法として標準的な SWOT 分析(強み(Strength)、弱み(Weakness)、機会(Opportunity)、脅威(Threat))を更に行った。その際、「脅威」に備えるにあたり重要な共通技術要素の抽出も行い、次のような共通基盤技術が重要であることが改めて認識された。例えば、全分野に共通する基盤技術の一群として、サイバーセキュリティ技術、量子情報科学、データ科学・分析・蓄積・運用技術、先端エンジニアリング・製造技術、先端エネルギー・蓄エネルギー技術、マイクロプロセッサ・半導体技術、先端監視・測位・センサー技術、先端材料科学、人工知能・機械学習技術、高度情報通信・ネットワーク技術、先端コンピューティング技術などが挙げられる。それらを活用する専門・応用技術として、バイオ技術、脳コンピュータ・インターフェース技術、医療・公衆衛生技術（ゲノム学含む）、宇宙関連技術、海洋関連技術、輸送技術、ロボット工学、極超音速技術、化学・生物・放射性物質及び核（CBRN）などが挙げられる。こうした横断的・俯瞰的側面は、令和 4 年度の調査研究において意識して取組み、例えば、先端材料分野についても取り上げたが、将来の調査研究においても共通基盤技術の抽出は重要な視点である。

２．個別調査分析

具体的な個別分野について、政府から提示された課題に応じてニーズの明確化、関連する内外の政策・戦略、脅威に対する情報を調査・分析し、そのニーズの解決につながり得る技術シーズについて、研究開発動向や内外の政策・戦略等について調査・分析を行った。ニーズとシーズをマッチングした結果や関連する技術研究開発動向を勘案して安全・安心の観点から育て守るべき重要技術等について示し、社会実装の方策も併せて検討した。調査研究を進める間に、経済安全保障重要技術育成プログラムの第 1 次研究開発ビジョン（令和 4 年 9 月 16 日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）に基づき「経済安全保障重要技術育成プログラム」（いわゆる K Program）がスタートしたことも踏まえ、研究開発ビジョンへの貢献やそこでも指摘されているマルチユース・多義性の側面の分析も意識しながら進めた。

個別分野の具体的な調査研究の成果は、各レポートに詳細があり、総論では概要を記載するにとどめる。個別分野の以下の記載内容の太宗は令和 5 年 2 月 8 日経済安全保障重要技術育成プログラムに係るプログラム会議（第四回）において政策研究大学院大学政策研究院より資料として提示し政府内での検討に貢献した。

（１） 健康・医療

① 調査研究の概要

危機シナリオの検討により、各フェーズにより必要な対応、対応技術を顕在化する。(検知、診断、対処法策定、治療、隔離、予防)　※この他感染症対策の国の体制づくり、企業育成、社会実装等も提言。

② 技術の特定

- 発生→検知→診断→対処法策定→対処のフローとなるが、特に検知し、診断するまでの時間の縮減と、様々な診断結果に対しての対処法のプールが必要となる。
- CBRN（化学・生物・放射性物質・核兵器）関連：危機に対する検知機能のモバイル化、スマ

ート化による大規模施設等への配備（生物剤検知器、バイオチップ）。

- ✓ 検知した情報をネットワークを介して収集し、早期に診断する体制構築。
- ✓ 案件毎に、対象人数、深刻さ（生命、産業）、時間的余裕、安全性（副反応等）、抗原の持続性（対象者の手間）を考慮し、対処法を決定する。

・ 自己複製型 RNA（レプリコン医薬品）：mRNA ワクチンと異なり、抗原を発現するのみならず、細胞内で RNA を増殖できる。mRNA 型ワクチンと比較し、少量で済むため量産効果が期待。

・ 組み換えタンパクワクチン：副反応が低く、冷蔵保存が可能（途上国等、アクセス向上）。

・ 植物由来ウイルス様粒子ワクチン：VLP （Virus Like Particle）は、ウイルスと同様の外部構造を持ち、ワクチンとしての高い免疫獲得効果（有効性）が期待されることに加え、遺伝子情報を持たないため体内でウイルスの増殖がなく、安全性にも優れる有望なワクチン技術。また、植物を使用した VLP 製造技術により、短期間で大量生産が期待。

・ ユニバーサルワクチンとしての BCG 東京株：科学的エビデンスが必要。信頼性、抗原の持続性が長い。

・ 天然痘経口治療薬：バイオテロの発生の可能性をどの程度見積もり、治療薬を用意するか。

・ ワクチン運搬に関連するコールドチェーン関連技術。

（２） サイバーセキュリティ

① 調査研究の概要

日本のサイバーセキュリティ分野の課題を踏まえ、サイバー攻撃等の脅威の把握・分析に係る要素技術を特定し、マルウェア解析の側面に焦点を当て対応を提言。さらにサイバー攻撃の検知のみならず、属性付けやカウンター技術（アトリビューション技術）に着目。また、サイバーセキュリティの進展と並行して形成されているデジタルトラストの動向と国際相互連携の調査、量子関連技術を中心とした情報通信におけるセキュリティ技術の調査を実施。

② 技術の特定

・ 攻撃観測の強化によるマルウェア捕獲能力の向上、複数組織によるマルウェア解析、統合分析能力、深層的な解析の強化を提言しつつ、脅威把握技術、収集データの分析技術を特定。

- ✓ インターネット環境については、表層 Web の観測・分析（脆弱性を狙うドライブバイ攻撃と人を騙すフィッシング攻撃）、ハニーポット（おとり）を用いた観測・分析、OSINT 情報（ブログ、セキュリティ記事等）から AI を活用して情報を組成し、より高いセキュリティレベルを確保するクラウドシステムを整備し活用する技術。
- ✓ ダークネット環境については、Unused IP アドレスやダーク Web の観測・分析システムの構築、コンテンツ分析、Tor（The Onion Router（玉ねぎのように幾層にも暗号化を重ね接続経路の匿名性を確保。）分析技術。この他、アトリビューション技術については、米国での運用事例なども調査・参照。

・ デジタルトラストは、「人のクリアランス」、「データの分類」、「アクセスコントロール」の制度設計から構成される。国際的な動向、米国での運用状況も調査し、これらを担保するた

めの技術の特定を行う。アクセスコントロールをオンプレミスや分散型で行うか、ゼロトラスト強化によりクラウド型で行うか等、データ格付けと併せ技術的側面を調査。

- 量子関連技術：耐量子コンピュータ暗号の開発、光ファイバ通信を中心とした要素技術や周辺技術の進化に対応するセキュリティ技術の開発、将来ネットワーク構想への対応を考慮した施策の検討を提言。

サイバーセキュリティ分野については、令和 4 年度は、上記の分析もベースにロシアのウクライナ侵略などの国際情勢も踏まえながら海外委託調査なども活用して更なる深堀を進めた。具体的には、サイバー防衛の日米比較を行い、政府、重要インフラ、民間企業、住民に至る国家サイバーインテリジェンスの全体像を提示した。その上でサイバーインテリジェンスシステムが果たす機能としての政策提言、国際連携、安全保障に資する調査分析の重要性を指摘した。システムの全体像としては、米国の例を参考にした 3 レベル（credentialing, suitability, eligibility（need to know））のセキュリティクリアランス付与の仕組みや、扱う機密情報の各段階・区分に応じた管理、そしてデータ管理のためのガバメントクラウドの重要性を指摘した。サイバーインテリジェンスの 2 大分野である CTI（Cyber Threat Intelligence）と CVI（Cyber Vulnerability Intelligence）についてインフラも含めた在り方を、AI、量子技術の活用面も含めて分析した。脅威の評価（アトリビューション）の技術的プロセスや手段、法的・社会的課題についても整理した。全体として体制整備を含めた政府への提言をまとめ、機密情報区分の整理、セキュリティクリアランスの制定、政府クラウド認定（ISMAP 改定）などの具体的課題も示した。

（3） 海洋・宇宙

① 調査研究の概要

- 海洋に関する経済安全保障を脅かす「脅威」の抽出に注力した。守るべき対象として、国民、流通、財産、食糧、環境、健康の 6 領域について整理した。①脅威に対してあるべき姿、理想論の提示、②現状とのギャップの認識、③ギャップを埋めるための技術、情報、体制を提案した。現状レベルでは解決できない課題への技術的解決策を、脅威の深刻度と発生の蓋然性も踏まえて、優先順位付も含めて整理・検討を行った。更に宇宙アセットも利用した「海上状況把握」（Maritime Domain Awareness：MDA）について地上アセットも含めた衛星の技術要求について調査を実施。
- 今般のロシアのウクライナ侵略など安全保障上の新たな脅威を踏まえて、広義の有事における商業衛星も含めた宇宙利用に関する調査を実施。

② 技術の特定

- 船舶の位置情報の高度化：衛星 VDES（VHF Data Exchange System；次世代 AIS（自動船舶認識装置））
- 監視技術の構築：先端センシング技術を用いたケーブルによる海底から海面までの移動体識別技術、風力、太陽光、潮力など再生可能エネルギーを動力源とする無人監視船（AUV）や超長距離潜航が可能な AUV などによるカーテン監視技術の構築。量子センシング技術等を用

いた海中監視技術。海洋データ連携の課題。

・ 宇宙からの広域監視:雲や気象の影響のより少ない衛星を使った電波監視や合成開口レーダを使った情報収集。小型衛星によるコンステレーション体制の構築。
※海洋・宇宙分野については「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）（令和 4 年 9 月 16 日決定）」の中で相当程度取り扱われることとなった。

３．分析手法・指標の開発

（１） 情報収集、データ分析の連携

CRDS,TSC,NISTEP,e-CSTI 他国内機関と連携した。以下が連携した各機関の関連する概要である。

① JST-CRDS（科学技術振興機構ー研究開発戦略センターー） JST のシンクタンクとして国内外の科学技術分野、科学技術政策の動向調査を実施。個別技術分野の調査・開拓だけでなく科学技術・学術・産業政策やイノベーション・エコシステム等の育成をめぐる仕組みについても目配り。詳細な技術カテゴリーに落とし込んだ分析を実施。JST-APRC(アジア太平洋総合研究センターー）は、アジア・太平洋地域における科学技術イノベーション政策、研究開発動向等について調査研究を行っており、最近では、CRDS・APRC で量子技術の国際動向を共同で発表している（APRC は中国調査を担当）。

② NEDO-TSC（新エネルギー・産業技術総合開発機構ー技術研究戦略センターー） イノベーションの推進を目的として技術戦略の策定、プロジェクトの企画立案を行いプロジェクトマネジメントとして産学官の強みを結集した体制構築や運営、評価、資金配分等を通じて技術開発を推進し、成果の社会実装、重要な技術分野の特定を進めている。TSC の取り組み内容はエネルギーと環境が 6 割を占める。

③ NISTEP（科学技術・学術政策研究所） 科学技術指標として、論文の被引用度や研究者の数等の国際比較を定点的に毎年実施。また、20 年から 30 年先を見据えた科学技術予測調査を行い、重要度、国際競争力、科学技術の実現見通し、政策手段、社会的実現見通し等の質問項目を立て、科学技術と社会の未来像のマッチングを実施。

④ e-CSTI（内閣府科学技術・イノベーション推進事務局 e-CSTI 担当部署） 研究・教育・外部資金獲得状況のエビデンスを収集整理し、インプットとアウトプットの関連を分析することを目的としたデータベースを CSTI で運用。①科学技術予算、②国立大学・研究開発法人の研究力、③外部資金・寄付金の獲得状況、④人材育成に係る産業界ニーズの把握等を分析項目としている。

（２） 今後検討し得る分析手法・指標の開発

各機関が有する手法、定期的な文書、知見・経験、データ、e－CSTI などを通じて既に分析がなされている内容など全体を俯瞰し、安全・安心、経済安全保障の文脈を踏まえ、重複がない形で継続的に分析できる手法が望ましい。

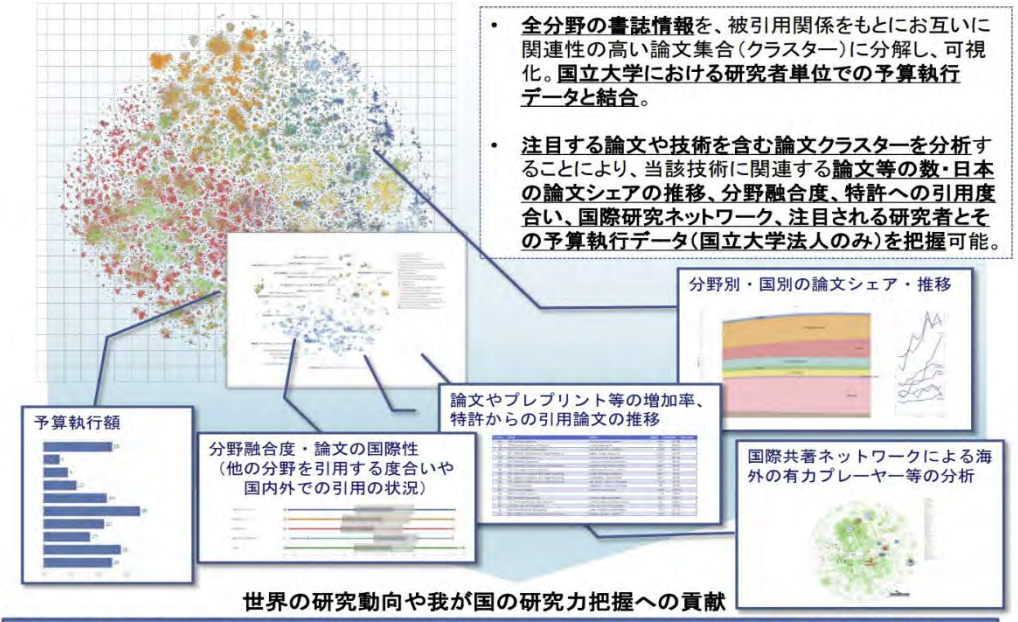
日進月歩の領域であり、直ちに手法の開発を行うことは容易ではないが、まずは、今後の定点観測のためのポイントを整理し、中長期的な視点で一貫した作業を実施するためのベースや整理・ひ

な型を提示することも検討し得る。

今後、経済安全保障環境や技術開発動向の変化を踏まえて、現在調査研究 20 分野を対象としてきた範囲を含め、定期的に技術リスト及び用途記述を更新し、さらにそれらの技術に係る知識分布状況の変容を年単位で追うことを想定され得る。そうしたベースを統一することで、情報更新作業のコスト低下と、変化を把握しやすくなる面もある。

例えば、個別の調査対象技術およびその生産に関わっている研究者の国内外における所在・分布について、論文データベース・研究助成データベース・特許データベース等を様々な市場の民間データ（ベンチャー投資、クラウドファンディング等含め）とも組み合わせながら把握することで、各調査対象技術についての日本及び各国の「強み」（＝特定国への技術・研究者の集積度）を測定することも考え得る（これらの強みの程度が低いまたは存在しない技術分野が、相対的に「弱み」のある分野となる）。脅威、ニーズとシーズとの関係、社会実装面の他、経済安全保障上のリスクを高める技術流出及び対外技術依存の問題も併せて検討し得る。e-CSTI の概要は以下の参考 2。

参考 2：e-CSTI の概要



開発に当たっては、NISTEP、JST/CRDS、NEDO/TSC等の府省横断的な専門家が協力

	エビデンスシステムの分析	具体的内容
1.	科学技術関係予算の見える化	行政事業レビューシートや各省の予算PR資料を活用し、関係各省の予算の事業内容、分野等の分類を可能とすることにより、科学技術関係予算を見える化する。
2.	国立大学・研究開発法人等の研究力の見える化	効果的な資金配分の在り方を検討するため、政府研究開発投資がどのように論文・特許等のアウトプットに結びついているかを見える化する。
3.	大学・研究開発法人等の外部資金・寄付金獲得の見える化	大学・国立研究開発法人等への民間研究開発投資３倍増達成を促進するため、①各法人の外部資金獲得実態を見える化するとともに、②各法人が使途の自由度の高い間接経費や寄付金をどのように獲得しているかを見える化する。
4.	人材育成に係る産業界ニーズの見える化	各大学等が社会ニーズを意識しつつ教育改善を図ることを可能とするため、産業界の社会人の学びニーズや産業界からの就活生への採用ニーズを産業分野別、職種別に見える化する。
5.	地域における大学等の目指すべきビジョンの見える化	イノベーション・エコシステムの中核となる全国の大学等が、今後目指すべきビジョンの検討を進めるため、地域毎の大学等の潜在的研究シーズや地域における人材育成需給を見える化する。

CSTI HP 掲載資料等を基に委託事業事務局で作成

Ⅲ．関係機関との連携

１．海外シンクタンク・国内関係機関との連携

海外シンクタンク（ランド・コーポレーション（RAND)、マイター・コーポレーション（MITRE)、オルビス・オペレーションズ（Orbis））と意見交換、連携、調査委託などを行った。国内機関では、国立研究開発法人科学技術振興機構（JST)・研究開発戦略センター（CRDS)、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO)・技術戦略研究センター（TSC)、文部科学省科学技術・学術政策研究所（NISTEP)、内閣府科学技術・イノベーション推進事務局（e-CSTI 担当部署)、株式会社日本政策投資銀行、民間調査会社（アスタミューゼ株式会社・委託含む)、などと意見交換などを実施した。

RAND 研究所については、令和 3 年度に引き続き調査研究 20 分野に関し、特に先端材料分野、健康・医療分野について深堀調査を行い、関係報告書に反映させた。マイター・コーポレーションについては、サイバーセキュリティ分野における脅威シナリオ、脆弱性の分析について深堀調査を行い、関係報告書に反映させた。オルビス・オペレーションズついては、サイバーセキュリティ分野のデジタルトラストに関連し、米国のセキュリティクリアランスの仕組みについて調査を行い、関係報告書に反映させた。いずれも PM チーム・政策研究大学院大学政策研究院と海外シンクタンクの専門家との WEB 会議等を積み重ね内容の充実を図った。なお、令和 3 年度、委託調査を行った戦略国際問題研究所（CSIS）や国際戦略研究所（IISS)についても令和 4 年度においてもレポートを参照･活用した他､意思疎通を図り関係を維持した。

国内については、前述のとおり JST-CRDS、NEDO-TSC、NISTEP、e-CSTI 担当部署や日本政策投資銀行とは実務レベルの連携会合などの場で連携を深めた。アスタミューゼ株式会社については、広範囲調査チームが調査研究 20 分野についてデータ分析を委託し、公開論文や特許情報等を活用した技術の依存度などを調査し、関係報告書に反映した。

２．参画促進と成果発信（広報）

令和 4 年度後半よりシンクタンク機能事業の周知活動を強化し、令和 4 年 11 月 29 日の内閣府安全・安心シンクタンク設立準備検討会（第一回）の場での説明や令和 5 年 2 月 8 日の「経済安全保障重要技術プログラム会議」の場での説明を行い、概要資料は内閣府 HP にも公表された。

海外の関連シンクタンクへの周知活動を令和 5 年 3 月に重点的に行い、連携関係を確認・強化した。

令和 5 年 3 月には、内閣府が主催する安全・安心シンクタンク準備キックオフの公開会合で各プロジェクト・マネージャー／リーダーから成果を発表。

Ⅳ．人材確保と人材育成

１．人材の確保と育成

（１） 人材確保等

本事業においては、シンクタンク事業実施のための人材確保と人材育成に取り組んできた。人材については、専門家人材と、事務局として組織運営を行う人材の両方がある。前者については、安全保障と科学技術・イノベーションの双方について高度な関心と知見を持ち、インテリジェンス・サイクルを実施できる専門家人材をプロジェクト・マネージャーをはじめとして十分確保し、また事業を推進していく中で、人材育成にも努め、専門家ネットワークを構築することを進めた。

若手人材はリサーチ・フェロー制度を設け、安全保障、国際関係、情報科学、公衆衛生等の多様な専門人材を採用し、研究プロジェクト毎の若手とマネージャーとの議論を重ねることで、シニアから若手への知識の移譲、若手研究者の底上げを図った。

組織運営を行う事務局においては、適切な人材の採用を行うとともに、OJT による能力構築を進めた。シンクタンク機能を発揮するためには、国や国内外の関係機関、研究者等と調整し、企画立案できる人材や、一定規模の予算を国とも調整しながら的確に執行できる人材の確保が必要であり、優秀な人材を雇用していくには、シンクタンク事業は単年度ではなく、一定期間継続していく必要があることが認識された。

なお、本事業が広くネットワーク型でもあることから、学内、学外とのネットワークのセキュリティシステム強化とその具体的な要件整理も併せて取り組んだ。特にゼロトラストセキュリティモデル（※）によるアプローチを検討した。

※従来型の構内と外部の「境界」に着目してセキュリティ対策を行う方式は、一度侵入を許すと脆弱。したがって、ゼロトラスト（誰も信頼しない）との考え方でネットワーク、ID、デバイス、システム、データ単位で各要素のセキュリティ対策を行い、全体としてあらゆる挙動を疑い、適切にリスク評価を行い対処するモデル。

（２） 人材育成

安全・安心に関する重要技術や経済安全保障に関わる人材育成については、大学・大学院教育との関係では、国際政治経済学、国際関係学、比較政治学など主に安全保障や外交面からのアプローチや、科学技術・イノベーション政策における技術評価、政策評価やデータサイエンスの活用などのアプローチなど様々である。具体的な教育プログラムを策定するに当たって育成すべき人材像を検討するに当たっては、現状においては、本分野において政策や分析手法・分析技術が急速に発展する中で、固定的に捉えることは率直に難しい面があり、柔軟な発想が求められる。したがって、当面は、各大学・大学院で行われている様々なプログラムを参考に、調査分析手法として必要なデータサイエンス分野の知見や政策ツール、法制度、国際協力等の施策の実務的知見などを有機的に組み合わせた教育プログラムが考えられる。

シンクタンク機能事業を通じて得られた調査分析手法は教育プログラムに還元することも想定される。特にデータサイエンス分野の分析手法は、先端・重要技術やサプライチェーンの分析はもとより、EBPM（Evidence Based Policy Making）に資するなどあらゆる政策研究分野に活用できるものである。また、政策ツール、法制度などの国内及び国際的動向の把握や分析をケース・スタディを通じて行うことは、アカデミックな知見と実務の知見を融合させ、双方にとって有益な知的基盤を提供すると考えられる。さらに分析手法もケース・スタディも刻々と変化する内外の情勢に応じて不断に更新していくことが望ましい。

（目指すべき人材像の具体策）

目指すべき人材像については、中堅・若手行政官や政府関係機関の職員が、科学技術イノベーションと安全保障の両側面を含む政策の大局的な視点を得つつ、調査分析手法（データサイエンス含む）や経済安

全保障に関連する政策ツールの知見を高めることが期待される。90 分×15 コマ・2 単位相当の研修を第一段階とすることが考え得る。更に意欲や適性のある者は、修士号を目指し所要の科目を履修する。履修者は、各部署で質の高い政策の企画立案や執行に当たるリーダーとして活躍することが期待される。

また、本分野の政策研究に関心の高い学生やミッドキャリアの社会人が修士コースに参加し、産官学の融合による切磋琢磨が期待される。更に高いレベルの専門家を目指す者は、博士号取得コースも用意することが考えられる。人材育成の取り組みを通じて、産官学の間での人材の行き来、人材交流のエコシステムの構築も期待される。

さらに、本件シンクタンク機能の立ち上げが我が国喫緊の課題であることを踏まえれば、即戦力も確保しなければならない。そのため、すでに公的調査研究機関や民間シンクタンクにおいて調査研究に従事している若手研究者を集め、シンクタンクにおける調査研究に参画させ、OJT により能力開発をしていくとの視点も重要である。

教育プログラムとそのプログラムに還元する可能性のある調査研究に関連して、国の所有するデータの使用範囲や安全保障貿易管理の扱い、留学生の扱いについては、あらゆる大学法人において同様であり、研究に関する利害相反や不正防止に関するコンプライアンス・ルール、研究インテグリティに関するルールや「安全保障貿易に係る機微技術管理ガイダンス（大学・研究機関用）」などを通じて適切な対応がなされると考えられる。

（シンクタンクを支えるコア人材と人材流動性確保による新陳代謝）

我が国を代表するシンクタンクを本格的に構築していくに当たっては、過去から続く調査研究の中で得られた知見やノウハウをレガシーとしてシンクタンクに蓄積していくことが不可欠であるが、それを支えるのはデータベース等の情報やシステムだけではなく、最後は人材である。すなわち、コアとなる人材を確保し、中長期にわたってシンクタンク機能の維持・向上を担ってもらうことが必要となる。

一方で、技術は日進月歩であり、調査・分析手法も進化していくことを踏まえれば、最先端の技術領域や政策動向に通じた人材を常時内在化させるべく、人材の流動性を確保することもまた重要である。

この観点から、シンクタンクがこうした調査研究に従事する研究者のキャリアパス上で重要な位置を占め、人材のインキュベーション機能をも担うことが期待される。

海外のシンクタンクの例を見ても、同一機関・組織に長期わたり在籍してシンクタンクの根幹を支えている層がある一方で、社会・経済状況の変化に臨機応変に対応し、その時々のトピックに適確・適時に対応できるような人材流動性を確保している。また、個々の研究者のキャリアパスの中でシンクタンクとアカデミア・民間企業を相互に移動出来るよう、キャリアアップの道が見通せることが、人材確保に取って重要である。

我が国シンクタンクにおいても、こうした海外事例を参考に、日本版のキャリアパスの在り方、人材育成の在り方を検討していくことが求められる。

Ⅴ．セキュリティの確保について

１．情報セキュリティの確保について

（１） 検討の前提

本事業における情報セキュリティ確保の重要性に鑑み、検討の前提として、①機微なデータを含む情報を扱うため、通信経路・データの保存方法、アクセス管理等について可能な限り高いセキュリティを担保したものとすること、②本事業が内外の多くの研究者等の参画によるネットワーク型で展開されることが予想されることから、内外の許可された者のみにアクセス可能なものとすること、③利用者の端末やアクセス環境の多様性に可能な限り配慮すること、④将来の拡張性の確保を前提に費用対効率の高い方法を段階的に実装可能なものとすることを念頭に成案を得ることとした。

上記を踏まえ令和 4 年度においては、令和 3 年度に引き続き NTT コミュニケーションズ株式会社と共に検討を行った。

令和 3 年度の調査検討においては、一般的にインターネット利用の際に広く使われているネットワーク重視型のセキュリティ対策方法である「境界型セキュリティモデル」（構内ネットワークと外部ネットワークとの「境界」にてファイアウォールなどのセキュリティ対策を行う方法）は、「一度侵入を許すと無力」、「内部犯行リスクに脆弱」、「クラウド利用により境界自体があいまいに」等の課題があり、新たなセキュリティモデルを採用する必要があると結論付けられ、高度なセキュリティ対策と、所属・端末・回線に依存しない接続方法を両立させるため、「ゼロトラストセキュリティモデル」を採用することが妥当との結論を得た。

参考：ゼロトラストセキュリティモデルとは
「何も信頼しない（＝Zero Trust）」という考え方に基づいたセキュリティ対策であり、ネットワーク、ID、デバイス、システム、データ単位で、各要素のセキュリティ対策を行う方法。セキュリティ対策について、あらゆる挙動を疑い、適切にリスク評価して対処する事が可能とされている。

令和 4 年度の調査検討においてはこれを一歩進め、ゼロトラストセキュリティモデルの利便性を活かしつつ、より機微な情報のやり取りを安全に行うために閉域網の利用を組み合わせたハイブリッド型のモデルの検討を行うことにより、より安全性の高いシステム構成の成案を得ることを目的とした。このため、本件調査検討においては、利用者の端末やアクセス環境の多様性はゼロトラストセキュリティモデルで担保されていることから、そうした利便性を若干制約したとしても、安全性に重きを置いてゼロトラストセキュリティモデルでは扱うことの難しい情報についてもその重要度に応じた複数のアクセス手法を効果的に使い分けることにより、扱い可能とする方法を検討することとした。

さらに、現時点における最新の日本政府のガイドラインに沿う形で、扱う情報の機密性のレベルに応じて情報の配属先としてクラウドを使い分ける構成とした。

（２） セキュリティモデルの選定

① ゼロトラストセキュリティモデルと閉域網の併用型ネットワークの検討

本事業に関わり管理すべき情報を扱う内外の全ての関係者をゼロトラストセキュリティモデルで接続したうえで、より機密性の高い情報にアクセスする権限を有する特定の関係者の情報管理のために、ネットワークの途中経路での通信傍受や情報摂取を脅威と位置付けて閉域網によるネットワークを提供し、ゼロトラストセキュリティモデルと閉域網の間に管理された情報のアクセスポイントを設け、二つのネットワーク相互の情報のアクセスを可能とする構成とした。

② 閉域網の検討

閉域網には独自に専用線を引くタイプから商用サービスを利用するものまでさまざまなタイプがあるが、シンクタンク事業関係者による利便性、費用対効果（安全性とコスト）、ネットワークの保守管理の容易さ等を総合的に勘案して、本事業関係者の多くが本邦の大学その他の研究機関に所属していることから、大学共同利用機関である国立情報学研究所が大学及び研究機関向けに提供する「学術情報ネットワーク」SINET6（Science Information NETwork）の閉域網サービス（VPN: Virtual Private Network）を採用し、SINET6 利用に制約のある関係者については商用の閉域網サービス利用を併用したネットワーク構成とした。

③ 情報の収納場所

情報は商用のクラウドサービスの利用を前提に、情報管理の安全性の観点から本邦法人が国内に設置するクラウドの利用が望ましいとしつつも、米国等の普遍的価値を共有する同盟国に事業者が提供するサービスが国内事業者より優れた安全性を備える場合その利用が望ましいとした。なお、将来的に日本国政府が機密性の高い情報の管理を行うためのガバメントクラウドを構築する場合には、そこで管理すべきことは言うまでもない。

④ 海外に居住する関係者との情報手段

本事業では海外に居住する研究者の参加も予想されるが、これら海外の関係者の利用環境はインターネットを利用する方式が一般的であることから、ゼロトラストセキュリティモデルでの接続を前提とした。なお、海外の関係者が「機密性高」までの情報を扱う必要が生じた場合は、閉域網での海外との接続等の必要性に関する検討が必要となる。

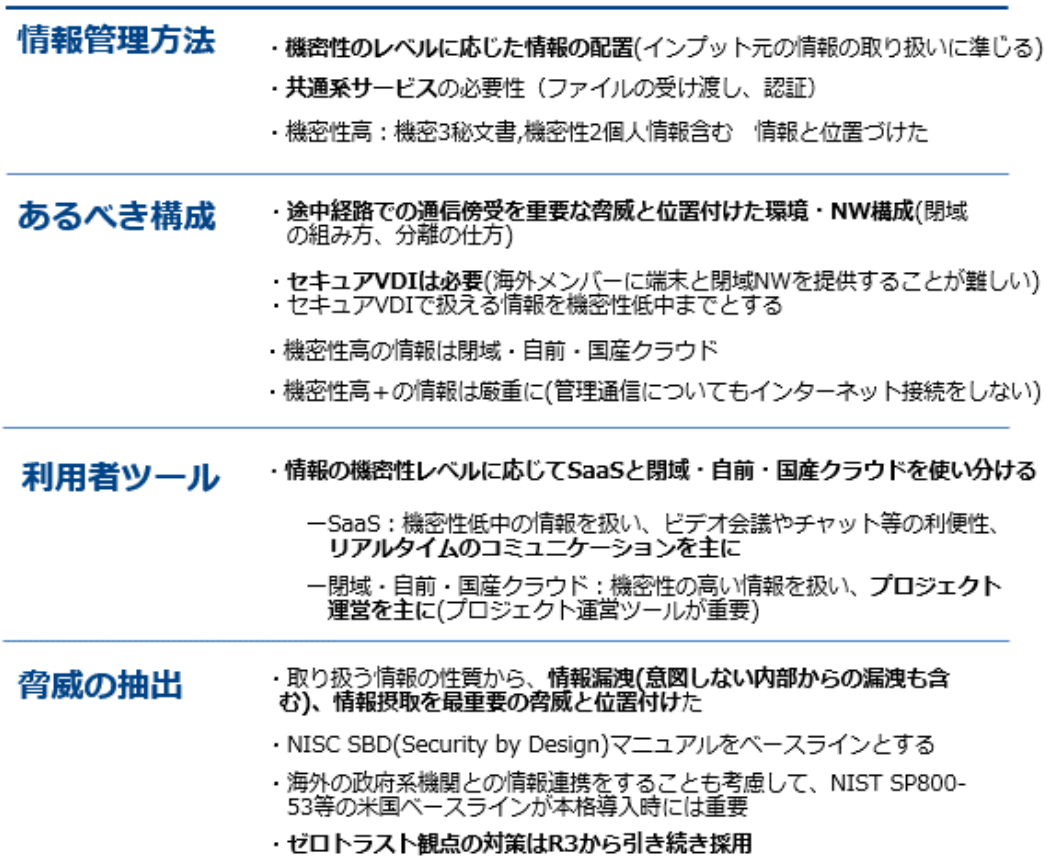
（３） 将来の実施機関への提案

以上の検討を基に、現時点での情報技術や商用サービスの状況を踏まえ、最も効果的かつ効率的なものとして、ゼロトラストセキュリティモデルと SINET6 の利用を中心とした閉域網を組み合わせ、扱う情報の重要度に応じてこれらを使い分けることを提案し、さらに将来の拡張性を踏まえたネットワークの概念を示している。その際、将来のシンクタンク事業において適切な情報管理が行われるためには、日本政府等のガイドラインだけでなく、米国等関係国のガイドライン

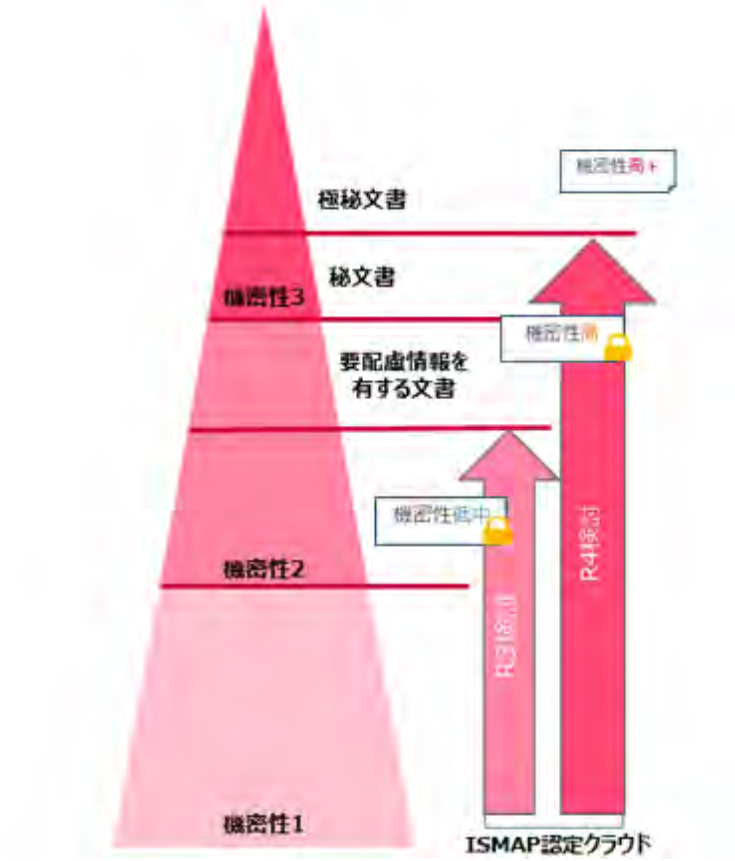
やガバメントクラウドの動向にも留意する必要がある。また、シンクタンクの内外での Input 元からの情報の受け取りや Output 先への提供といった一連の流れは権限と責任を有する者に集約され、情報の管理が可視化されていることも重要である。

本調査検討結果が、将来のシンクタンク事業を構成する関係者の属性、扱う情報の秘匿性のレベル、情報量、日本国政府における政策の方向性、実現時点での情報ネットワーク環境の進化等を踏まえた適切な情報管理体制の在り方を検討するための一助となることを期待したい。以下の参考 3 が令和 4 年度の検討の方向性、参考 4 が取り扱う情報の機密性レベルに応じた使い分けのイメージをまとめたものである。

参考 3：令和 4 年度　検討の方向性



参考 4：取り扱う情報の機密性レベルに応じた使い分けのイメージ



注 1：クラウドサービスの利用に係る政府方針

・ 安全保障等の機微な情報等に係る政府情報システムの取扱い DS-910(R4/12/28 書難:デジタル社会推進会議幹事会決定)要点：

✓ 秘密文書中秘文書に該当する情報及びそれに準ずる情報の取り扱いについて記載したもの

✓ 「安全保障等の機微な情報等を扱う情報システムも含め、クラウド化を検討していくことが求められる」

✓ 高度な自律性の確保が重要としている

✓ デジタル・ガバメント推進標準ガイドライン DS-100 附属文書

注 2：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対策のための統一基準群

・ 政府機関等の情報セキュリティ対策のための統一基準(平成 30 年度版）(H30/7/25:サイバーセキュリティ戦略本部)要点：

✓ 機密性 3 情報を扱う場合は、「インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用すること」

２．その他セキュリティの確保について

本学「政策研究大学院大学政策研究院文書管理規程（安全・安心シンクタンク事業）」に基づき、

本事業において扱う文書・情報の管理（特に電子ファイルの組織的な管理）について関係者に周知徹底するとともに、実務的なガイドライン「法人文書の電子ファイル管理に関するガイドライン（安全・安心シンクタンク事業）」を作成した。

Ⅵ. 課題設定・組織のあり方・シンクタンク発展のイメージ

１．本事業からのこれまでの示唆

経済安全保障と先端・重要技術の課題は、経済、科学技術、安全保障含め多面的で新しく、国内、国外の知見を結集して取り組む必要がある。先端技術の発展、世界情勢に沿ってスピード感を持って取り組むには、国が指針を示しつつ、国内の政府全体・官民アカデミア全体での取組み（whole of government. holistic approach）を進めるなかで、シンクタンクが一翼として役割を果たすことが重要である。

課題に対して、分析手法の確立や内外の連携拡大を不断に進めることが必要であり、データサイエンス分析や、様々なケース・スタディを通じ、調査、分析、課題抽出、実施、検証の方法論を内外連携しつつ、発展させるべきである（例：「脅威シナリオ・政策ニーズ」→「技術シーズ調査」→「ニーズとシーズのマッチング・技術の特定と社会実装を踏まえた提言」のサイクル確立など）。また、発信がなければ情報集約も十分確保できないことを踏まえ、対外発信と交流を通じた内外連携、海外機関・シンクタンク等との協働（alignment, Track 1.5 workshop etc.）による世界情勢の先取りが重要である。

また、中長期的な課題設定が不可欠である。短期的な年度毎の喫緊の対応のみならず、5 年、10 年、15 年以上の期間を見据えた対応を行うマンデート、シンクタンク自身の自律的な活動、知見の蓄積を確保すべきである。同時に中長期的な取り組みの中で本分野における人材育成、人材の行き来、人材エコシステムの確立が望まれる。

なお、本事業は、2 ヵ年にわたり「我が国が育てるべき安全・安心の確保に係る重要技術等の検討業務」として、シンクタンク機能を実際に動かしてきたところであり、その結果、令和 4 年度中の 7 月以降に公表された政府文書（特定重要技術開発基本方針、重要技術開発ビジョン等）には、具体的な技術分野やシンクタンク機能に関する考え方などが示されたところである。

２．今後のシンクタンク機能の在り方

今後のシンクタンク機能の在り方については、当初の機能事業開始時からの大きな局面の展開として、経済安全保障推進法の成立（2022 年 5 月）を踏まえれば、まずその範囲・外縁が議論となる。最も広範な考え方としては、安全・安心の確保に関する重要技術等の検討を幅広く捉えて、災害対策やスタートアップ支援なども含めた範囲を扱う考え方（①いわば安全・安心シンクタンク）、さらに安全・安心の考え方の中で特に外部からの脅威に着目して経済安全保障を中心に捉え、自律性、不可欠性の要素を見据えて、先端的な技術の開発のみならずサプライチェーンの強靭化など経済安全保障推進法に関わる様々な要素を扱う考え方（②いわば経済安全保障推進シンクタンク）、その上で、さらに限定的な範囲としては、経済安全保障推進法の第四章（特定重要技術の開発支援）に示された法定事項を達成するため、「特定重要技術」（外部の不当利用等の問題への対応）の開発に関する委託調査研究を行うものがある（③特定重要技術調査研究機関としてのシンクタンク）。

いずれにせよ、安全・安心から発展し、経済安全保障も含めたシンクタンク機能が法令上の国の基本方

針、基本指針、調査実施方針に沿って実現されていくためには、機能事業からの示唆として、情報収集、情報保全の在り方、人材確保・定着の在り方、内外連携・成果の公表の在り方などの明確化、組織体制整備の方針の明確化、法令の整備（特別法上の法人等の仕組みも含めた組織の検討）が国に一層求められる。

その際、国が前面に立って、国全体の司令塔の役割、関係省庁の役割、実行のためのスケジュールも含め具体的な方向性を明確に示すべきである。現実的には当初は小規模でスタートしつつ、事業環境の変化に応じて大きく育てる余地を柔軟に残すという発想もあろう。

なお、シンクタンク機能の中で期待される調査分析手法は、いずれかの組織で将来実施される可能性がある教育プログラムへの還元も想定され、特にデータサイエンス分野の分析手法は、先端・重要技術やサプライチェーンの分析はもとより、EBPM（Evidence Based Policy Making）に活用できるものである。また、政策ツール、法制度などの国内及び国際的動向の把握や分析をケース・スタディを通じて内外連携しながら実施することは、アカデミックな知見と実務の知見を融合させ、教育にも還元され、双方にとって有益な知的基盤を提供すると考えられる。米欧のシンクタンクではそうした動きが盛んに進められており、我が国のカウンターパートの存在も待望（Track 1.5）されている。

Ⅶ. 政府検討状況（参考）

本事業を進める間、令和 4 年 10 月の段階で上記の課題設定・組織のあり方・シンクタンク発展のイメージについては、内閣府や関係省庁に対して問題提起を行い、令和 4 年 11 月 29 日に内閣府で開催された「安全・安心に関するシンクタンク設立準備検討会（第一回）」において政策研究大学院大学政策研究院より説明を行った。その後、同検討会は検討を継続し、令和 4 年末に以下の中間整理（参考 5）をまとめたところである。令和 4 年度末に報告書がまとめられる方向である。検討会メンバーは参考 6 のとおり。

参考 5：「安全・安心に関するシンクタンク設立準備検討会」での安全・安心シンクタンクの立上げに向けた中間整理状況

【シンクタンクにおける当面の具体的なミッション】

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

【シンクタンクの果たすべき役割・機能】

	立上げ時点で持つべき機能	将来的に拡張されるべき機能	留意点
情報収集	・オープンソース（各種公表資料、データベース、ワークショップ等）からの情報収集 ・人的ネットワークを介した非公開情報の収集	・国内外の政府機関等からの非公表情報の入手 ・在外公館等からの情報収集 ・海外連携機関等とのクローズドの意見交換における情報収集	・機密性の高い情報の取扱いに当たっては適切な情報管理体制を構築する必要あり ・収集した情報の整理・蓄積の在り方は別途検討（特に公開／非公開の考え方）
解析・分析	・研究開発・技術開発動向の分析 ・国際情勢、経済等の社会科学的分析 ・成熟度レベル、依存度等の技術評価 ・シーズ・ニーズの抽出・分析	・データサイエンス、シナリオ分析等の新たな分析手法の開発 ・潜在シーズ・ニーズの見える化の手法の高度化	・解析・分析能力についてはコア・コンピタンスとしてシンクタンクに内在化させることが重要
人材育成	・即戦力人材の確保 ・ＯＪＴによる人材養成・能力開発 ・産学官の関係機関・組織との人事交流	・人材育成プログラムの構築 ・連携大学院制度による学位プログラム	・処遇面も含めて魅力度を高めることが課題 ・国内の人材の層を厚くすることも重要
ネットワーク構築	・大学等を含む国内外の関係機関とのネットワーク構築 ・既存の国内公的シンクタンクとの連携	・海外の公的シンクタンクとの連携強化 ・学会等の関連コミュニティの構築	・シンクタンクがコア機能として持つべきものと外部連携機関に依存するものの峻別が課題

※　ファンディング機能なども含めて調査研究以外の機能を持たせるか否かについては将来課題として別途検討

※　調査・分析の担い手のほか、シンクタンクを組織として機能させるためにはしっかりとした管理部門の存在が不可欠

参考 6：検討会メンバー

上山　隆大　　総合科学技術・イノベーション会議・常勤議員（座長）
青木　節子　　慶應義塾大学大学院法学研究科教授
金子　将史　　政策シンクタンク PHP 総研代表・研究主幹
白石　隆　　政策研究大学院大学名誉教授
角南　篤　　笹川平和財団理事長
西山　淳一　　未来工学研究所研究参与
橋本　和仁　　内閣官房科学技術顧問・科学技術振興機構理事長
松本　洋一郎　外務省科学技術顧問・東京大学名誉教授

＜開催実績＞

第一回　令和 4 年 11 月 29 日
第二回　令和 4 年 12 月 23 日
第三回　令和 5 年 2 月 27 日
第四回　令和 5 年 3 月 14 日
第五回　令和 5 年 3 月 24 日
（※令和 5 年 3 月 28 日に内閣府主催安全・安心シンクタンク準備キックオフの公開会合開催）