内閣府政策統括官（経済安全保障担当）御中

令和５年度国内及び主要国における情報保全を伴う研究開発の推進体制等に関する調査・分析

成果報告書

令和６年３月

株式会社エヌ・ティ・ティ・データ経営研究所

内容

1. エグゼプティブサマリ（要約） 3

2. 調査の背景・目的 5

3. 調査方針 6

3.1 調査の全体像 6

3.2 調査方法 13

3.2.1 国内及び主要国の企業・国立研究所・会議等における秘密情報等の取扱い及びこれに従事する主な機関の調査及び整理 13

3.2.2 指定基金協議会の効果的な運営に資する事例調査 38

3.2.3 意見交換の開催 40

4. 調査結果 42

4.1 国内及び主要国の企業・国立研究所・会議等における秘密情報等の取扱い及びこれに従事する主な機関の調査及び整理 42

4.1.1 国内外の秘密情報の取り扱いに係る法令・ガイドライン等の調査・整理 42

4.1.2 研究開発実施主体、推進会議等事務局における秘密情報等の取扱いに関する実態調査 269

4.2 指定基金協議会の効果的な運営に資する事例調査 413

4.3 意見交換の開催 436

4.3.1 第 1 回意見交換会 436

4.3.2 第 2 回意見交換会 437

4.3.3 第 3 回意見交換会 438

4.3.4 第 4 回意見交換会 439

4.4 比較・分析の対象とする調査結果 440

5. 調査結果の比較整理・分析 446

5.1 研究開発の情報保全措置に関する比較・分析 446

5.2 研究開発の運営要領に関する比較・分析 467

6. 指定基金協議会の設置・運営に係る分析 473

6.1 情報保全措置に関する分析 474

6.2 指定基金協議会の運営要領に関する分析 482

7. Appendix 491

1. エグゼプティブサマリ（要約）

本事業では、経済安全保障推進法に基づく特定重要技術の開発支援等を効果的に推進するための検討を目的として、「日本及び諸外国において政府、企業、国立研究所等の複数機関が連携して行う研究開発における情報保全等の運用の在り方」の調査を実施した。

まず調査対象国の概況、情報保全及び研究開発の動向を把握するためマクロ調査を行い、研究開発に関連する戦略や主要な研究開発機関（資金配分機関、国研、民間企業、大学等の研究開発実施主体）・研究開発プログラム、及び秘密情報やそれに準じる情報（以下「秘密情報等」とする）の取り扱いに係る法体系などを明らかにした。次いでマクロ調査結果を踏まえて研究開発プログラムや法令・ガイドライン等（以下、「法令等」とする）のリストアップによって、調査対象とする法令等を絞り込み、その規定内容を調査した。そして上記で調査した各国の研究開発動向や法体系を踏まえて、資金配分機関や研究開発実施主体における秘密情報等の取り扱いの実態についてヒアリングを含めて調査を実施した。

上記と並行して指定基金協議会による特定重要技術の研究開発とその成果の活用促進を効果的に行うことを念頭に、各国の研究開発推進に係る会議等の運営事例について、上記で絞り込んだ研究開発プログラム及びその所管機関を主な調査単位として調査を実施した。

なお、調査と並行して経済安全保障、研究開発等に係る政府関係者を招聘しての意見交換会を開催し、現状の調査状況や今後の調査予定、ヒアリング先の選定候補、調査結果の取り纏め、示唆の検討の方向性等についてコメントをいただき、逐次調査内容への反映を行った。

その後調査結果を総合して、研究開発実施主体の公募・採択から研究開発の実施、成果の活用に至る一連の流れの中で情報保全上留意すべき観点に沿って、調査対象国のうち日米英韓横並びでの調査結果の比較・整理を行い、その結果を踏まえ指定基金協議会の設置・運営に係る全体像を意識したファクトベースの分析を実施した。

特定重要技術の研究開発を行う「経済安全保障重要技術育成プログラム（以下、「Kプログラム」という。）」を例とした分析を行った結果、各観点から以下のような結果を得た。なお、比較に際しては、各研究開発プログラムで取り扱われる情報の機微度に差異がある点に注意が必要である。

【情報保全措置】

- 米国・英国・韓国ではセキュリティ・クリアランスの取得を要件とした参加制限を設けている。また、研究開発実施主体及びそれに所属する個人に対する背景・身上に係るデューデリジェンス等を実施している。
- 米国・韓国では機密情報の共有にあたり、機密性レベルに応じた情報取扱要領が統一的に規定されているため、当該要領に基づいた共有が成されているものと想定される。また、機密情報を取り扱うための作業区域やネットワークへのアクセス支援やセキュリティ性の高い研究の従事者に対する金銭的支援を規定することによって研究開発実施主体への支援を行っており、機密情報の共有を円滑化していると考えられる。
- 米国・英国・韓国ではプログラムで取り扱う情報の機密性レベルや研究開発課題自体のセキュリティ等級の設定による一律の保全レベルの規定や、安全保障上の必要性において成果の帰属・公表に対する制限が規定されている。
- 米国・英国・韓国では、開発推進会議体やプロジェクトに依らず政府の定めた法令・

ガイドラインに基づき情報の機密性に応じた統一的な情報管理策を定めている。また、技術標準や政府の認定規格等を参照した物理的・技術的な情報の保存・利用、管理、廃棄等に係る具体的手順を規定していることに加え、保全対象情報を口頭情報、ハードコピー情報、電子情報に区分し、区分ごとに管理策を規定している。

【研究開発とその成果の活用促進を効果的にするための開発推進会議体の運営】

- 米国・英国・韓国においては、政府の課題解決に繋がる具体的なアイデアを見つけるために、広範な産官学コミュニティへのヒアリング、市場調査による潜在的な投資価値の把握、専門家である PM（プログラムマネージャー）による自律的な企画立案といったプロセスが規定されている。
- 米国・英国では、意思決定機構/非意思決定機構を分けた評価体制の構築や、最終的な決定権を PM に委ねた公募・採択が実施されている。
- 米国・英国では、PM による研究実施体制の変更も含めた進捗管理や、アドバイザーの設置による産業界からのアドバイスの提供、提案段階から継続した研究開発実施主体の支援、プロジェクトの難易度・リスクに応じた進捗管理責任者の業務範囲の設定等を行っている。
- 米国・英国・韓国においては、商業化戦略策定のためのガイドラインの策定や、アドバイザーによる知的財産権ポートフォリオの形成や輸出規制への対応等についての支援、一定期間以内に成果活用先との技術実施契約の締結を行うことを研究開発実施主体の義務として規定する等実施している。

2. 調査の背景・目的

令和 4 年 5 月 11 日の「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」（以下、経済安全保障推進法）の成立により、安全保障を確保するための経済施策の一つとして、我が国にとって重要な先端的技術を特定重要技術として定義し、指定基金協議会の支援によって研究開発の促進とその成果の活用を図ることとなっている。

政府の推進する研究開発において機密性の高い情報を取り扱う場合は、その情報を関係者間で適切に共有して効果的に研究開発を進めることが重要となる。

そのため本事業では、政府、企業、国立研究所等の複数機関が連携して行う研究開発における情報保全等の運用の在り方を明らかにすることにより、経済安全保障推進法に基づく特定重要技術の開発支援等を効果的に推進するための検討を行うことを目的として、調査を行うこととする。

3. 調査方針

3.1 調査の全体像

2 項に示した目的を達成するために、本事業においては実施計画書をもって契約期間中の実施事項について意識合わせを実施のうえ実施管理を行い（仕様書 6.(1)）、国内及び主要国の企業・国立研究所・会議等における秘密情報等の取扱い及びこれに従事する主な機関の調査及び整理（同 6.(2)）、及び指定基金協議会の効果的な運営に資する事例調査（同 6.(3)）を意見交換会のフィードバックを受けつつ（同 6.(4)）実施し、最終的な検討結果を調査報告書として取り纏め作成する（同 6.(5)）。

それにより、社会実装を成功させるための方法論・課題、指定基金協議会の規約、特定重要技術研究開発協議会情報管理規程等の検討に資する示唆を抽出し、今後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を推進することを本事業のスコープとする（図 3.1-1）。

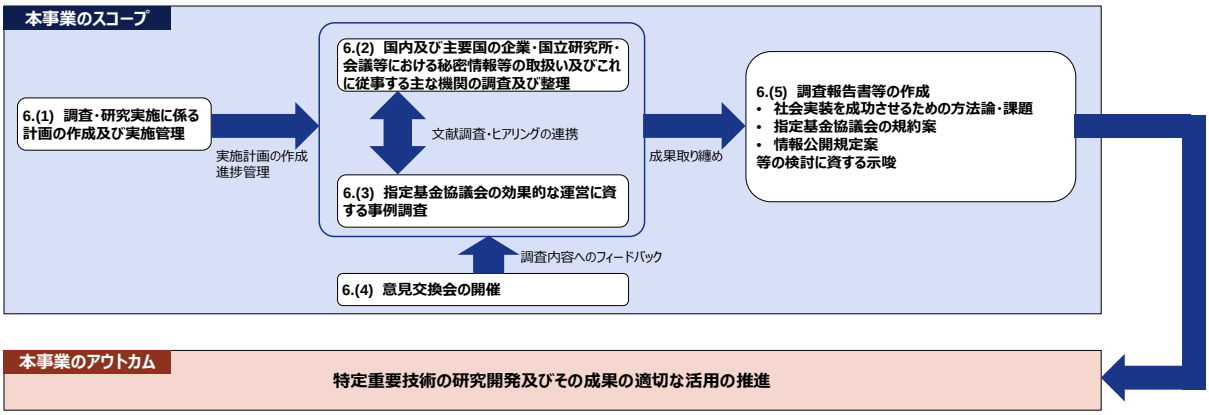


図 3.1-1　本事業実施の全体像

なお、本報告書で頻出する用語について以下のとおり定義する

表 3.1-1　本報告書での頻出用語の定義

区分	用語	定義
共通	法令・ガイドライン等（法令等）	国もしくは地方自治体の制定する法律、命令、規則や、政府機関・民間の業界団体の策定するガイドライン、及び民間企業の内部規則等を含む、文書化されたルール全般を指す
	研究開発プログラム（プログラム）	政策目標の達成に向けた研究開発を民間企業、大学、国立研究所等に委託するための、公募、採択、資金提供、進捗管理・評価といった一連の仕組みを持つ制度を指す
	研究開発プロジェクト（プロジェクト）	研究開発プログラムにおいて採択された、個別の研究テーマに取り組む活動単位を指す
	資金配分機関	競争的資金の制度を運営し、競争的資金を研究機関又は研究者に配分する機関

区分	用語	定義
	研究開発実施主体	研究開発プログラムにおいて採択された個別のプロジェクトで、実際の研究開発活動に従事する民間企業、大学、国立研究所等を指す ※資金配分機関の中でも自ら研究開発を実施する能力を有している場合は、研究開発実施主体として調査する場合がある
	研究開発機関等	資金配分機関と研究開発実施主体を総称する場合に用いる
	研究開発推進会議体	資金配分機関を中心として、外部の有識者や研究開発実施主体の代表者等複数の機関で構成される、研究開発プログラムもしくはプロジェクトを進めていくための議論、事務局機能を担う会議体を指す
日本	AMED	Japan Agency for Medical Research and Development：日本医療研究開発機構
	FRA	Fisheries Research and Education Agency：水産研究・開発機構
	JAMSTEC	Japan Agency for Marine-Earth Science and Technology：海洋研究開発機構
	JAXA	Japan Aerospace Exploration Agency：宇宙航空研究開発機構
	JOGMEC	Japan Organization for Metals and Energy Security：エネルギー・金属鉱物資源機構
	MDA	Maritime Domain Awareness：海上状況把握[1]
	NARO	National Agriculture and Food Research Organization：農業・食品産業技術総合研究機構
	NICT	National Institute of Information and Communications Technology：情報通信研究機構
	NIES	National Institute for Environmental Studies：国立環境研究所
	NIG	National Institute of Genetics：国立遺伝学研究所
	NIID	National Institute of Infectious Diseases：国立感染症研究所
	SDA	Space Domain Awareness：宇宙領域把握[2]
米国	APST	Assistant to the President for Science and Technology：科学技術担当大統領補佐官
	CCL	Commerce Control List：規制品目リスト[3]
	CFIUS	The Committee on Foreign Investments in the United States：対米外国投資委員会

[1] https://www8.cao.go.jp/ocean/policies/mda/pdf/r05_mda_main.pdf

[2] https://www8.cao.go.jp/space/comittee/27-anpo/anpo-dai58/siryou2.pdf

[3] https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

区分	用語	定義
	CSA	Cognizant Security Agency：認知安全保障機関
	CUI	Controlled Unclassified Information：管理対象非機密情報[4]
	DARPA	Defense Advanced Research Projects Agency：国防高等研究計画局
	EAA	Export Administrative Act：輸出管理法
	EAR	Export Administration Regulations：輸出管理規則
	ECRA	Export Control Reform Act：輸出管理改革法
	FIRRMA	Foreign Investment Risk Review Modernization Act：外国投資リスク審査近代化法
	GSA	General Services Administration：米国一般調達局
	ITAR	International Traffic in Arms Regulations：国際武器取引規則
	NASA	National Aeronautics and Space Administration：米国航空宇宙局
	NDAA	National Defense Authorization Act：国防権限法
	NIH	National Institutes of Health：国立衛生研究所
	NIST	National Institute of Standards and Technology：国立標準技術研究所
	NISP	National Industrial Security Program：国家安全保障産業プログラム
	NISPOM	National Industrial Security Program Operating Manual: 国家安全保障産業プログラムオペレーションマニュアル
	NOAA	National Oceanic and Atmospheric Administration：海洋大気庁
	NSTC	National Science and Technology Council ：国家科学技術会議
	OMB	Office of Management and Budget：行政管理予算局
	PCAST	President's Council of Advisors on Science and Technology：大統領科学技術諮問会議
	SCI	Sensitive Compartmented Information：機密区画情報[5]
	SEAD[4]	Security Executive Agent directive：安全保障エグゼクティブ・エージェント指令
	UARC	University Affiliated Research Center：大学付属研究センター
カナダ	CSA	Canadian Space Agency：カナダ宇宙庁

[4] https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

[5] https://www.commerce.gov/osy/programs/information-security/sci-program

区分	用語	定義
	DFO	Department of Fisheries and Oceans：水産海洋省
	DND	Department of National Defence：国防総省
	ECCC	Environment and Climate Change Canada：環境・気候変動省
	ISED	Innovation, Science and Economic Development Canada ：イノベーション・科学経済開発省
	PHAC	Public Health Agency of Canada：カナダ公衆衛生局
	PSC	Public Service Commission：公安省
	SSC	Shared Services Canada：シェアードサービスカナダ
英国	BBB	British Business Bank：英国ビジネスバンク
	BBSRC	Biotechnology and Biological Sciences Research Council：生物科学研究会議
	BPSS	Baseline Personnel Security Standard：政府ベースライン人員セキュリティ基準[6]
	CST	Council for Science and Technology：総合科学技術会議
	DASA	Defence and Security Accelerator：国防・セキュリティ促進機構
	DEFCON	Defense Condition：防衛契約条件[7]
	DEFRA	Department for Environment, Food and Rural Affairs：環境・食糧・農村地域省
	DERA	Defence Evaluation and Research Agency：国防評価研究庁
	DfT	Department for Transport：運輸省
	DSIT	Department for Science, Innovation and Technology：科学技術省
	Dstl	Defence Science and Technology Laboratory：国防科学技術研究所
	EPSRC	Engineering and Physical Sciences Research Council：工学・物理科学研究会議
	FCDO	Foreign, Commonwealth and Development Office：外務・英連邦・開発省
	GCHQ	Government Communications Headquarters：英国政府通信本部
	Go Science	UK Government Office for Science：政府科学局
	GSCP	Government Security Classifications Policy：政府セキュリティ分類ポリシー
	MoD	Ministry of Defence：国防省

[6] https://assets.publishing.service.gov.uk/media/5a7b257940f0b66eab99f4b1/baseline-personnel-security.pdf

[7] https://www.gov.uk/guidance/defence-procurement-useful-information

区分	用語	定義
	MoST	Ministry of Science and Technology：中華人民共和国科学技術部
	MRC	Medical Research Council ：医学研究会議
	NCSC	National Cyber Security Centre：国家サイバーセキュリティセンター
	NSIA	National Security and Investment Act：国家安全保障投資法
	NSMS	National Strategy for Maritime Security：海洋安全保障のための国家戦略
	NSS	National Space Strategy：国家宇宙戦略
	NSSIF	National Security Strategic Investment Fund：国家安全保障戦略投資基金
	NSV	National Security Vetting：国家安全保障審査
	RVC	Research Venture Catalyst：リサーチ・ベンチャーズ・カタリスト基金
	SPF	Security Policy Framework：セキュリティポリシーフレームワーク
	TRI	Trusted Research and Innovation：信頼できる研究とイノベーション
	UKRI	UK Research and Innovation：英国研究・イノベーション機構
	UKSA	United Kingdom Space Agency：英国宇宙庁
	UNCLOS	United Nations Convention on the Law of the Sea：国際海洋法条約
ドイツ	BMBF	Bundesministerium für Bildung und Forschung：連邦教育研究省
	BMI	Bundesministerium des Innern und für Heimat：連邦内務・国土省
	BMVg	Bundesministerium der Verteidigung：連邦国防省
	BMWK	Bundesministerium für Wirtschaft und Klimaschutz：連邦経済・気候保護省
	DLR	Deutsches Zentrum für Luft- und Raumfahrt：ドイツ航空宇宙センター
	GBER	General Block Exemption Regulation：包括的適用除外規則
フランス	AID	Agence de l'innovation de défense：防衛イノベーション庁
	ANR	Agence nationale de la recherche：国立研究機構
	CNES	Centre national d'études spatiales：フランス国立宇宙研究センター
	CNRS	Centre national de la recherche scientifique：フラン

区分	用語	定義
		ス国立科学研究センター
	EUMSS	European Union Maritime Security Strategy : EU 海洋安全保障戦略
	GDPR	General Data Protection Regulation : EU 一般データ保護規則
	Ifremer	Institut Français de Recherche pour l'Exploitation de la Mer : フランス海洋開発研究所
	MAA	Ministère de l'Agriculture et de la Souveraineté alimentaire : 農業・食品省
	MEAE	Ministère de l'Europe et des Affaires étrangères : 欧州外務省
	MESRI	Le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation : 高等教育・研究・イノベーション省
	MTES	Ministère de la Transition écologique : 環境連帯移行省
	SGDSN	Secrétariat général de la défense et de la sécurité nationale : 国防安全保障事務総局
	SGMer	Secrétariat général de la Mer : 海洋総局
	SGPI	Secrétariat général pour l'investissement : 投資総局
オーストラリア	ACSC	Australian Cyber Security Centre : オーストラリアサイバーセキュリティセンター
	ASA	Australian Space Agency : オーストラリア宇宙庁
	ASIO	Australian Security Intelligence Organisation : オーストラリア保安情報機構
	DAFF	Department of Agriculture, Fisheries and Forestry : 農林水産省
	DAWE	Department of Agriculture, Water and the Environment : 農水環境省
	DCCEEW	Department of Climate Change, Energy, the Environment and Water : 気候変動・エネルギー・環境・水資源省
	DISR	Department of Industry, Science and Resources : 産業科学資源省
	DoD	Department of Defence : 国防省
	DoE	Department of Education : 教育省
	DoHAC	Department of Health and Aged Care : 保健・高齢者ケア省
	DSGL	Defence and Strategic Goods List : 防衛戦略物資リスト
	NHMRC	National Health and Medical Research Council : オーストラリア保健医学倫理委員会
	ONI	Office of National Intelligence : 国家情報局

区分	用語	定義
インド	DBT	Department of Biotechnology：バイオテクノロジー省
	DoS	Department of Space：宇宙省
	DRDO	Defence Research and Development Organisation：国防研究開発機構
	DST	Department of Science and Technology：科学技術庁
	DPIIT	Department for Promotion of Industry and Internal Trade：商工省産業国内取引促進局
	ISRO	Indian Space Research Organisation：インド宇宙研究機関
	MoD	Ministry of Defence：国防省
	MoES	Ministry of Earth Sciences：地球科学省
	MoST	Ministry of Science and Technology：科学技術省
	NIOT	National Institute of Ocean Technology：国立海洋研究開発機構
	VSSC	Vikram Sarabhai Space Centre：ヴィクラム・サラバイ宇宙センター
韓国	ADD	Agency for Defense Development：国防科学研究所
	ETRI	Electronics and Telecommunications Research Institute：韓国電子通信研究院
	KARI	Korea Aerospace Research Institute：韓国航空宇宙研究院
	KFRI	Korea Food Research Institute：韓国食品研究院
	KIMST	Korea Institute of Marine Science & Technology：海洋水産科学技術振興院
	KRIBB	Korea Research Institute of Bioscience and Biotechnology：韓国生命工学研究院
	KRICT	Korea Research Institute of Chemical Technology：韓国化学研究院
	ICMTC	Institute of Civil-Military Technology Cooperation：民軍協力振興院

3.2 調査方法

3.2.1 国内及び主要国の企業・国立研究所・会議等における秘密情報等の取扱い及びこれに従事する主な機関の調査及び整理

3.2.1.1 国内外の秘密情報の取り扱いに係る法令・ガイドライン等の調査・整理

（1）実施方針

本項においては、国内外で実施する研究開発を対象として、**秘密情報の取扱いに係る法令等**の調査・整理を行う。

国外の調査対象国については、日本と経済安全保障の領域で研究開発の観点で連携する可能性のある同志国の法令等について明らかにする観点から、仕様書にも記載のある**米国**、**英国**、**フランス**、**ドイツ**、**オーストラリア**とし、加えて隣国である**韓国**や米国と協定を締結している**カナダ**、**インド**、各国を横断する法令等も調査対象とする。

実施手順としては、まず法令等をリストアップする前に、対象国の研究開発や秘密情報保護関連政策の動向についてマクロ調査を行い、研究開発に関連する戦略や主要な研究開発機関（資金配分機関、国研、民間企業、大学等の研究開発実施主体）・研究開発プログラム、及び秘密情報の取り扱いに係る法体系・各法令の位置づけなどを明らかにする。なお、研究開発のマクロ調査にあたっては、最終的に日本における特定重要技術の効率的な開発支援に向けた課題等を分析することを念頭に、K プログラム事業の中で支援対象技術領域となっている宇宙・海洋・バイオ・サイバー領域や多義的な活用が期待される技術（以下、多義的技術）の動向については、必須調査事項とする。

その後、マクロ調査結果を踏まえて研究開発プログラムや法令等のリストアップによって、調査対象とする法令等の絞り込みを行い、その規定内容について調査する。なお、リストアップする法令等に関しては、マクロ調査で明らかとなった研究開発プログラムで準拠が求められているものの他、当該研究開発のみならず幅広い研究開発に影響のある分野横断的な法令等（例えば不正競争防止法や外為法、大学・研究機関全般向けの情報保全ガイドライン等）についても、政策動向のマクロ調査結果を踏まえて抽出を行う。

また、調査結果を踏まえて各国横断で比較・整理することによって、国・地域ごとの傾向や日本との違いについて明らかにする。

（2）実施項目・方法

1）マクロ調査

調査対象となる法令等のリストアップに向けて、調査対象国の研究開発動向及び秘密情報等の取り扱いに関する政策動向についてマクロ調査を実施する。

具体的には、まず調査対象国の**政治体制**、**人口**、**GDP**、**研究開発予算**といった基礎的事項を各国政府の統計資料等から整理するとともに、**政治（Politics）**、**経済（Economy）**、**社会（Society）**、**技術（Technology）**の観点から各国の最近の取組内容を調査（PEST 分析）し、

各国の動向をマクロに把握する。その後、特に秘密情報の取り扱いに係る政策動向および研究開発動向について、より範囲を絞ってマクロ調査を行う。

秘密情報の取り扱いに係る政策動向に関しては、研究開発に関連する秘密情報保護法令及びガイドライン等を抽出することを念頭に、**①安全保障の観点から国家機密に該当する情報等の保全政策**、**②技術移転の側面で研究開発に関連があると考えらえる安全保障貿易（輸出規制や外資規制等）関連政策**の動向及びその中で策定されている法令・ガイドラインについて主に調査を行う。

研究開発動向としては、各国の研究開発に関連する戦略や主要な研究開発機関（資金配分機関、研究開発実施主体）・研究開発プログラム等を把握する。**科学技術・イノベーション**や**安全保障関連技術の開発**といった全般的な動向のほか、**宇宙・海洋・バイオ・サイバー領域**及び**多義的技術**ごとに取り纏め、動向の調査を行うこととする。

調査方法は、公開情報、研究レポート、学術論文など対象とした机上調査を中心に行うとともに、適宜、関連機関に対するヒアリング（メール等での問い合わせを含む）を試みることで情報を補完する。

2）法令・ガイドライン等のリストアップ、調査対象の選定

マクロ調査の結果明らかとなった各国の研究開発や秘密情報の取り扱いに関する動向を踏まえ、詳細調査の対象とする法令等に抜け漏れがないよう、秘密情報の取り扱いに係る法令等のロングリストを作成する。ロングリストの作成では、国内 15 件、主要国 5 件程度を目安に、法令等の**①名称**、**②種別**（法令か、ガイドラインか）、**③策定機関**、**④策定年**、**⑤対象としている産業領域・技術分野**（※宇宙、海洋、バイオ、サイバー、多義的技術、その他、から整理）、**⑥規定の概要**等について公開情報等から整理する。

その後、ロングリストでリストアップした法令等を以下の観点から評価し、制度の詳細について調査を行う法令等をショートリストとして絞り込む。

（法令等の絞り込み観点）
- **整理可能な情報量の多寡（情報の取り扱いに関する十分な情報量があること）**
- **研究開発に対する影響の大きさ（多くの研究開発プログラムで参照されている、規程の中で研究開発について言及されているなど）**
- **国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも 1 つずつ選定すること**

3）法令・ガイドライン等の詳細調査

ショートリストとして絞り込んだ法令等については、情報保全の全容を把握することを念頭に、**①策定の背景・目的**、**②適用範囲（適用される機関の範囲、情報資産の範囲など）**、**③情報の分類（機密性・完全性・可用性など）**、**④情報管理策（組織的・人的・物理的・技術的管理策）**、**⑤罰則（主に法令の場合を想定）**について調査・整理する。

④の情報管理策として調査を行う内容としては、ISO/IEC 27001:2022 で規定されている**組織的・人的・物理的・技術的管理策**を参考にし、これに該当する具体的な内容について、

絞り込んだ法令等において調査・整理を行う。

3.2.1.2 研究開発の実施主体、推進会議等事務局における秘密情報等の取扱いに関する実態調査

（1）実施方針

3.2.1.1 で調査した各国の研究開発動向を踏まえて、**資金配分機関や研究開発実施主体における秘密情報等の取り扱いの実態**について調査する。特に資金配分機関の調査においては、同機関が資金提供を行う研究開発プログラムの推進に係る会議事務局における情報の取り扱いについて調査・整理を行う。また調査対象先としては、研究開発機関に加えて、特定重要技術の調査研究を担うシンクタンクの設立検討に資する情報を得ることを念頭に、民間・政府系シンクタンクについても調査対象とする。

（2）実施項目・方法

1）研究開発機関等及び研究開発プログラムのリストアップ、調査対象の選定

3.1.1.1 で実施した各国の研究開発動向で明らかとなった研究開発プログラムに対して資金提供している資金配分機関と、同機関が主催している研究開発プログラムをリストアップ（ロングリストを作成）する。リストアップする研究開発プログラムとしては国内 15 件、主要国 5 件程度を目安とし、**産業領域・技術分野**（宇宙、海洋、バイオ、サイバー、多義的技術）ごとに整理を行う。なお、基本的に研究開発プログラムは産業領域・技術分野ごとのマクロ調査結果に基づいて抽出を試みるが、所管課とも協議のうえ、以下のような理由から、米国の **SBIR 制度（中小企業技術革新研究プログラム）**及びそれを模倣した日本の SBIR 制度、英国の SBRI 制度に基づく研究開発プログラムについてはリストに含めることとする。

（SBIR プログラムを調査対象とした理由）
- **技術成熟度やプログラムの進捗に応じた段階的な情報保全に関する調査を充実させるため（SBIR 制度におけるステージゲート方式の存在）**
- **スタートアップ企業等の中小企業が、大企業に比して十分でない資金力や研究開発体制の中でどのように参加するプログラムにおける情報保全を図っているのかを調査するため**

資金配分機関及び研究開発プログラムのロングリストにおいては**①機関・プログラムの名称、②機関・プログラムの概要、③機関の研究開発予算規模、④プログラムの目標 TRL、⑤研究開発実施主体（国研、大学、民間企業等）**について公開情報等から整理する。

その後、ロングリストでリストアップした資金配分機関及び研究開発プログラムを以下の観点から評価し、詳細調査を行う対象をショートリストとして絞り込む。

この際、シンクタンクについてはその特性上、特定の技術・製品等の研究開発には取り組

んでいないことが想定されるため、特定重要技術の調査研究機関の新設に資する示唆を得る観点から、外部機関への調査委託等に関する情報が得られるものを抽出する。

（資金配分機関及び研究開発プログラムの絞り込み観点）

- **各国の戦略において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること**
- **国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるもの**

研究開発実施主体（国研、大学、民間企業等）については、基本的には上記のショートリストで絞り込んだ研究開発プログラムに参加している機関をロングリストとしてリストアップする。その際、民間企業は基本的に情報取り扱いに係る内部規則を社外秘としていることから、基本的に**政府系機関**を対象とする。中でも政府系機関は資金配分機関としての役割を兼ねている機関が存在することから、調査の効率性を鑑みて資金配分機関としてリストアップした機関を優先して調査対象として絞り込む。その他の絞り込みの観点については、資金配分機関及び研究開発プログラムと同様とする。

民間企業については、コンタクトの容易性や本事業への協力を得られる可能性の高いことから、**日本国内の企業**を中心に**ヒアリング**によって情報収集を行うこととする（民間企業を含むヒアリング調査の方法については以下の 4)で示す)。

なおプログラムに採択された研究機関が多数に及ぶ場合は、第三者機関の研究開発能力に関する格付けなどを踏まえて絞り込みを行う。なお、調査対象は原則個別の研究開発実施主体とするが、当該研究開発実施主体が特定の研究開発プロジェクトに参画し、複数の機関が一体となって研究開発に従事しているケースが確認された場合においては、該当するプロジェクト単位での調査も検討する。

2）資金配分機関及び研究開発プログラムにおける情報取り扱い実態の調査

資金配分機関及び研究開発プログラムは 3.2.1.2　1)で絞り込んだ資金配分機関および研究開発プログラムとし、資金配分機関の内部規則（情報保全ポリシーや研究助成規則）や研究開発プログラムの募集要項、契約約款等を確認することで調査を行う。

情報の取り扱いに関する調査項目としては、3.2.1.1 と同様に**情報管理策等**について調査する他、プログラムへの**参加資格**、**参加制限等**についても調査を行う。

3）研究開発実施主体における情報取り扱い実態の調査

研究開発実施主体については、政府系機関は公開されている内部規則（情報保全ポリシー等）を確認することによって調査を行い、民間企業についてはヒアリングによる調査を行う。

情報の取り扱いに関する調査項目は、政府系機関に対する机上調査項目としては 3.2.1.1 と同様に**情報管理策等**について調査する。ヒアリングを試みる民間企業については、研究開発プログラムに参加するために組成している**情報保全体制**、遵守している**情報保全措置**に関する事項（平素から組成・遵守しているものに加え、プログラムに参加するために特別に

組成・遵守しているものを含む）について調査するとともに、情報保全体制や情報保全措置を運用する上での**負担感**や**改善要望**についても調査する。

4）ヒアリング調査

3.2.1.1 に示すマクロ調査を踏まえてリストアップ、絞り込んだ研究開発機関等のうち、国内 8 機関以上、主要国のうち米国・英国の機関から以下のような観点を踏まえてヒアリング対象をリストアップする。

（ヒアリング対象機関のリストアップ観点）
- ヒアリングによる情報入手が困難でないもの（ロングリストのリストアップ時の基礎調査の結果を踏まえて判断）
- 政府の定める制度、研究開発の取り組み単位で定める規則、実施主体独自の規則等に複数準拠しており、複数の法令等の運用実態についてヒアリングすることができるもの
- 複数機関の参加する研究開発の取り組みに参加しており、複数機関間での情報の利用・受け渡し等の実態についてヒアリングすることができるもの

なお、日本については研究開発実施主体である民間企業をヒアリング先として、ヒアリングの企画・調整を進める。他の主要国に関しては、米国・英国の資金配分機関を対象として候補を選定、調整することとした。以下にヒアリング先の選定要領及びヒアリング項目の検討について記載する。

a）日本

日本のヒアリング先としては、所管課と協議のうえ、多義的技術の研究開発プログラムである防衛装備庁が所管する安全保障技術研究推進制度での受託実績を有する大企業（表 3.2-1）の他、当該大企業と比較して、情報保全やコンプライアンスに関する規程やリソース（システムや人材等）面で差異が見込まれるスタートアップ企業から選定することとする。

表 3.2-1　ヒアリング候補とする民間企業（大企業）

企業名	安全保障技術研究推進制度における研究課題名	採択年度
川崎重工	積層造形による AI 合金の熱物性と機械的特性の制御に関する研究	令和 5 年度
	海洋状況把握（MDA）等に適用可能な革新的画像処理技術の研究	令和 4 年度
	溶融池における合金化による新規機能材料の開発	令和 3 年度
	昆虫の偏光知覚を模倣した空の偏光航法に関する研究	令和 3 年度
ソフトバンク	水中航走用レーザー通信に向けた光トラッキング技術の研究開発	令和 4 年度
	有機正極二次電池の充放電機構の解明と高エネルギー密度化の研究	令和 4 年度
日本電気	海中通信・センシング向けの高性能配向圧電セラミックの基礎研究	令和 4 年度
	ナノチューブネットワーク制御による新規赤外線検出	令和 3 年度

企業名	安全保障技術研究推進制度における研究課題名	採択年度
	阻止の研究	
日立製作所	環境制御観察における超高感度３D 電磁場顕微鏡法の開発	令和３年度

スタートアップ企業に関しては、今年度から、SBIR（Small Business Innovation Research）制度に基づき設定された補助金を活用し、経産省、文科省等の各省が管理主体となって、スタートアップ企業を中心とした研究開発（大規模技術実証、フェーズ３）が実施されている。情報の鮮度を踏まえて、同制度で採択されたスタートアップ企業を候補として、ヒアリング先を絞り込むこととする（表 3.2-2）。

そして表 3.2-3 に整理した SBIR フェーズ 3 の採択企業のうち、本調査事業との関連性で◎とした企業をスタートアップ企業のヒアリング対象候補として絞り込み、企業規模（従業員数、資本金）や事業内容を踏まえて優先順位付けを行い、優先順位高の企業に対して順にコンタクトを行う方針とする（表 3.2-3、表 3.2-4）。

表 3.2-2　主な SBIR フェーズ 3 採択企業（2023 年 12 月 15 日時点）

所管省庁	分野	企業名	テーマ	本調査事業との関連性
文科省[8]	宇宙	インターステラテクノロジズ株式会社	民間ロケットの開発・実証	◎ （宇宙領域で関連性あり）
		株式会社 SPACE WALKER		
		将来宇宙輸送システム株式会社		
		スペースワン株式会社		
		株式会社アストロスケール	スペースデブリ低減に必要な技術開発・実証	
		株式会社 Pale Blue		
		株式会社 BULL		
	核融合	株式会社 MiRESSO	核融合原型炉等に向けた核融合技術群の実証	○ （核関係のテーマのため情報保全を徹底している可能性あり）
		株式会社 Helical Fusion		
		LiSTie 株式会社		
		京都フュージョニアリング株式会社		
	防災	株式会社バカン	災害対応を担う行政ニーズ等に応える地震・防災技術の実証	△
厚労省[9]	－	サナメディ株式会社	AI ホスピタル	△
		リージョナルデータコア株式会社	健康長寿社会	
経産省[10]	－	株式会社 ispace	月面ランダーの開発・運用実証	◎ （宇宙領域で関連性あり）
		株式会社 Synspective	衛星リモートセンシングビジネス高度化実証	◎ （同上）
		株式会社アークエッジ・スペース		
		株式会社 QPS 研究所		
		株式会社 New Space Intelligence		
		株式会社 sustainacraf		

[8] https://www.teitanso.or.jp/sbir-monka-hojo/download/

[9] https://www.teitanso.or.jp/cms/wp-content/uploads/2023/10/%E6%8E%A1%E6%8A%9E%E7%B5%90%E6%9E%9C.pdf

[10] https://www.teitanso.or.jp/sbir-keisan-hojo/download/

所管省庁	分野	企業名	テーマ	本調査事業との関連性
		株式会社天地人		
		LocationMind 株式会社		
		サグリ株式会社		
		株式会社 SkyDrive	空飛ぶクルマの機体開発及び型式証明取得等に向けた飛行試験等	△
		テトラ・アビエーション株式会社		
		株式会社 ACSL	行政ニーズ等に対応したドローンの開発・実証	△
		イームズロボティクス株式会社		
		VFR 株式会社		
		Terra Drone 株式会社		
		Intent Exchange 株式会社		
		WOTA 株式会社	小規模分散型水循環インフラの量産化・社会実装事業	△
		ダイナミックマッププラットフォーム株式会社	プローブカーデータを活用したグローバルでの高精度 3 次元地図データの更新技術の大規模実証	△
国交省[11]	災害に屈しない国土づくり、広域的・戦略的なインフラマネジメントに向けた技術の開発・実証	株式会社 リアルグローブ	都市デジタルツインの技術開発・実証	△
		株式会社 スペースデータ		
		株式会社 ユーカリヤ		
	国際競争力強化に資する交通基盤づくりに向けた技術の開発・実証	Universal Hands 株式会社	AUV（自律型無人潜水機）・ROV（遠隔操作型無人潜水機）を活用した港湾鋼構造物の点検効率化・高度化に関する技術開発・実証	○ 海洋領域で関連する可能性あり
		株式会社 FullDepth		
		ダイナミックマッププラットフォーム株式会社	空港業務の生産性向上に関する技術開発・実証	△
		avatarin 株式会社		

[11] https://www.teitanso.or.jp/sbir-kokkou-hojo/download/

表 3.2-3　ヒアリング対象候補としたスタートアップ企業と概要

企業名	創業年	従業員	資本金	事業概要	SBIR での研究開発テーマ
インターステラテクノロジズ株式会社	2013	144 名	1,000 万円	ロケットの開発・製造・打上げサービス 工場・研究所を保有	民間ロケットの開発・実証
株式会社 SPACE WALKER	2017	24 名	約 4.4 億円	有翼再使用ロケットの開発 東京理科大キャンパス内に R&D センター有	民間ロケットの開発・実証
将来宇宙輸送システム株式会社	2022	—	8.6 億円	宇宙輸送システムの事業化に向けた企画検討	民間ロケットの開発・実証
スペースワン株式会社	2018	—	71 億円	小型衛星用の宇宙輸送システムの開発	民間ロケットの開発・実証
株式会社アストロスケール	2013	450 名以上	—	宇宙デブリの除去技術を開発。英国、米国、フランス、イスラエルに子会社を保有	軌道上の衛星等除去技術・システムの開発・実証
株式会社 Pale Blue	2020	—	—	東大発宇宙スタートアップ 宇宙船用推進機を開発	衛星等の軌道離脱促進のための技術・コンポーネント開発・実証
株式会社 BULL	2022	—	—	スペースデブリ発生防止装置を開発	衛星等の軌道離脱促進のための技術・コンポーネント開発・実証
株式会社 ispace	2010	216 名	約 33 億円	月面探査ロボットを開発、Google Lunar XPRIZE に参加、米国拠点あり	月面ランダーの開発・運用実証
株式会社 Synspective	2018	150 名以上	1 億円	SAR 衛星開発を実施 シンガポールに子会社あり	衛星リモートセンシングビジネス高度化実証
株式会社アークエッジ・スペース	2003	—	1 億円	超小型衛星の設計・製作	衛星リモートセンシングビジネス高度化実証

企業名	創業年	従業員	資本金	事業概要	SBIR での研究開発テーマ
株式会社 QPS 研究所	2005	—	1 億円	九州大初ベンチャー 第５回宇宙開発利用大賞	衛星リモートセンシングビジネス高度化実証
株式会社 New Space Intelligence	—	—	—	衛星データの選択・統合・解析・提供を実施	衛星リモートセンシングビジネス高度化実証
株式会社 sustainacraf	—	—	—	自然保全プロジェクトの効果を評価	衛星リモートセンシングビジネス高度化実証
株式会社天地人	2019	—	—	衛星データを使ったサービス開発	衛星リモートセンシングビジネス高度化実証
LocationMind 株式会社	2019	52 名	24 億円	位置情報解析の東大発ベンチャー	衛星リモートセンシングビジネス高度化実証

表 3.2-4　ヒアリング対象候補のコンタクト優先順位

企業名	優先順位	順位付けの理由
株式会社 SPACE WALKER	1 位	ロケット開発をメインで実施。小人数のメンバーで（公表数値で 24 名）事業を実施しており、情報保全に関するリソースや機能をどのように確保しているのか、知見が得られる可能性有。R&D センターを有し、研究開発にも積極的に取り組んでいると想定
株式会社アストロスケール	2 位	宇宙デブリの除去技術を開発メインで実施。1 位の企業と比較して従業員数が多く（450 名以上）、英国、米国、フランス、イスラエルに子会社を保有しており、現在は比較的情報保全体制も充実していると想定。情報保全へのこれまでの取組や各国規制への対応面等で知見が得られる可能性を考慮し優先順位を設定
株式会社 QPS 研究所	3 位	情報セキュリティ基本方針が公表されており、情報保全に対して意識していることが確認できる。 歴史は比較的ある（2005 年創業）ため、どのような経緯で情報保全体制を構築してきたのか等確認できると想定
株式会社 Synspective	4 位	衛星データのソリューションプロバイダーであるとともに自ら SAR 衛星開発も実施しており、他の衛星リモートセンシング関連のスタートアップと比較して、研究開発に関する情報も得られる可能性があると想定
株式会社 Pale Blue	5 位	東大発宇宙スタートアップ、宇宙船用推進機を開発。2020 年に創業で他の優先順位が高い企業と比較して歴史が新しいため、情報保全要件への対応への工夫や課題等で新鮮な情報が聞くことができると想定
株式会社アークエッジ・スペース	6 位	事業内容に研究開発は含まれていないものの、SBIR 事業の他にも、NEDO 研究開発型ベンチャー支援事業や経済産業省「超小型衛星コンステレーション技術実証事業」に採択されており、国プロの中での情報保全要件への対応方法等を確認できる可能性
株式会社 ispace	7 位	月面ランダーの開発・運用実証に従事。2 位の企業と理由としてはほぼ同様で、従業員数や資本金ではやや劣るものの、比較的規模が大きい（従業員数：216 名、資本金約 36 億円）
インターステラテクノロジズ株式会社	8 位	ベンチャーとして創業されているが、事業規模・認知度も大きく、別途調整中の大手企業から得られる情報との差別化が出来ない可能性を考慮して優先順位を低めに設定

企業名	優先順位	順位付けの理由
スペースワン株式会社	9 位	情報が少ないため優先順位は低い。資本金は 71 億円と比較的大きいので、情報保全に投資するリソース等はある可能性
株式会社 BULL	10 位	情報が少ないため優先順位は低い
将来宇宙輸送システム株式会社	対象外	事業内容を事業企画としており、研究開発に関連した情報が期待できないと想定したため
株式会社 New Space Intelligence	対象外	事業内容がデータ解析サービス中心であることから、研究開発情報保全に関する情報は他と比較して期待できないと想定したため
株式会社 sustainacraf	対象外	
株式会社天地人	対象外	
LocationMind 株式会社	対象外	

以上を踏まえて、研究開発実施機関の情報取扱について調査するためのヒアリング対象機関としてコンタクトする国立研究所、民間企業（大企業、スタートアップ企業）をリストアップする（表 3.2-5　コンタクト先となるヒアリング対象機関）。

表 3.2-5　コンタクト先となるヒアリング対象機関

機関名	区分	選定理由
川崎重工	民間企業（大企業）	安全保障技術研究推進制度（多義的技術）採択実績から、同制度での情報保全に向けた対応状況について聴取することを期待
ソフトバンク	民間企業（大企業）	同上
日本電気	民間企業（大企業）	同上
日立製作所	民間企業（大企業）	同上
表 3.2-2 示すスタートアップ企業	民間企業（スタートアップ）	※表 3.2-2 に示す通り
宇宙航空研究開発機構（JAXA）	国研	宇宙領域の研究開発への取組について情報収集することを期待
海洋研究開発機構（JAMSTEC）	国研	海洋領域の研究開発への取組について情報収集することを期待
日本医療研究開発機構（AMED）	国研	バイオ領域の研究開発への取組について情報収集することを期待
情報通信研究機構（NICT）	国研	サイバー領域の研究開発への取組について情報収集することを期待

ヒアリング項目については、安全保障技術研究推進制度に参加している民間企業（大企業）と SBIR 事業に参加している民間企業（スタートアップ企業）に分け、以下の通り設定する。

（安全保障技術研究推進制度に参加している民間企業（大企業）に対するヒアリング項目）

■　情報保全体制について

・ 安全保障技術研究推進制度を履行する上で組成している本プロジェクト固有の情報保全体制等がある場合、その構成と役割
・ 上記で回答したプロジェクト内での情報保全体制とは別に、社内で定常的に組成し

ている情報保全体制を構築している場合、その構成と上記で回答したプロジェクト内（個社内）で構築している体制との情報共有の方法（特に情報保全上留意している内容）

■　情報保全措置について

・ 安全保障技術研究推進制度の中で遵守が求められている情報保全規則（人的・物理的・技術的事項）

・ 安全保障技術研究推進制度とは別に内部で定めている情報保全規則がある場合、その規則について（人的・物理的・技術的事項）

■　情報保全体制・措置の運用について

・ 上記で回答した情報保全体制や情報保全措置を運用する上で、特に負担に感じている体制の運用、規則等（あれば）

・ 上記で回答した負担感に対しての改善策・要望等（あれば）

（SBIR 事業に参加している民間企業（スタートアップ企業）に対するヒアリング項目）

■　社内で定めている情報保全規程について

・ 社内で定常的に定めている情報保全規程はあるか（あるとした場合は以下について回答）

・ どのような保全規程（組織的、人的、物理的、技術的規程）を定めているか

・ 政府が所管する研究開発プログラム（SBIR 事業等）で遵守が求められている規程と比較した場合、社内規程の網羅性（条項の過不足や基準の充足度等）はいかがか

■　研究開発における情報保全の運用について

・ 研究開発プログラムにおける情報保全措置の実現に向けた体制について

・ 情報保全規程を遵守・運用する上での負担感・課題の有無とその内容、改善に向けた施策など（あれば）

・ 効率的に保全措置を運用する上での工夫（社内教育やマニュアルなどの有無等）など（あれば）

※（研究開発プログラムにコンソーシアムで応募した経験がある場合は以下について回答）

・ コンソーシアム内の他企業とのデータのやり取りにおける情報保全措置を講じていたか

・ 上記のデータのやり取りを行っていた企業から、情報保全に係る支援等（リソースの提供や情報保全規程の共有など）を受けたことはあるか

b）米国

米国のヒアリング先としては、宇宙、海洋、サイバー、多義的技術領域等、日本のＫプログラムに関連した情報を収集することが期待できる機関を中心に選定を行う(表 3.2-6)。

表 3.2-6　米国のヒアリング対象候補機関

機関名	区分	選定理由
DARPA	政府機関	デュアルユース技術開発促進のためのコンテストの開催やＰＭに責任と権限が付与され、ハイリスク・ハイペイオフの研究開発に対しての資金援助やプロジェクト管理等を実施しており、ＰＪにおける情報保全の取組・事例に関しての情報を得られる可能性が高いため
DIU	政府機関	Ｋプログラムの研究領域である宇宙領域等の研究開発、デュアルユース技術開発を行う企業のスタートアップを支援し、軍全体へのそれらの商業技術の導入を促進していることから、各支援ＰＪ等における情報保全の取組・事例に関しての情報を得られる可能性が高いため
カリフォルニア大学共同バイオテクノロジー研究所	政府系研究機関(UARC)	Ｋプログラムと類似分野である領域をコアコンピテンシーとして研究開発を実施しており、会議体・PJ における情報保全に関する取組事例・情報を収集できるものと期待できるため
ジョンスホプキンス大学　応用物理学研究所	政府系研究機関(UARC)	同上
ペンシルベニア州立大学　応用物理学研究所	政府系研究機関(UARC)	同上
ハワイ大学　応用物理学研究所	政府系研究機関(UARC)	同上
テキサス大学　応用物理学研究所	政府系研究機関(UARC)	同上
ワシントン大学　応用物理学研究所	政府系研究機関(UARC)	同上
宇宙ダイナミクス研究室	政府系研究機関(UARC)	同上
Los Alamos National Laboratory	政府系研究機関(FFRDC)	Ｋ プログラムと関連した領域を研究分野として、研究開発を実施しており、会議体・PJ における情報保全に関する取組事例・情報を収集できるものと期待できるため

機関名	区分	選定理由
Sandia National Laboratories	政府系研究機関(FFRDC)	同上
Aerospace Federally Funded Research and Development Center	政府系研究機関(FFRDC)	同上
Brookhaven National Laboratory	政府系研究機関(FFRDC)	同上
National Renewable Energy Laboratory	政府系研究機関(FFRDC)	同上
Jet Propulsion Laboratory	政府系研究機関(FFRDC)	同上
Lawrence Berkeley National Laboratory	政府系研究機関(FFRDC)	同上
Lincoln Laboratory	政府系研究機関(FFRDC)	同上
NSF's National Optical-Infrared Astronomy Research Laboratory	政府系研究機関(FFRDC)	同上
Software Engineering Institute	政府系研究機関(FFRDC)	同上
Institute for Defense Analyses（IDA）	政府系研究機関(FFRDC)	同上
MITRE Corporation	政府系研究機関(FFRDC)	同上
RAND Corporation	政府系研究機関(FFRDC)	同上
CSIS	非営利組織	政策系シンクタンクであり、K プログラムに関連した領域も取り扱っていることから、情報保全に関する取組事例・情報を収集できるものと期待できるため

これらの機関から所管課と協議の上、情報保全に関する具体的な情報等を得られる可能性が高いものとして、以下の機関に絞り込みを実施する。(表 3.2-8)

表 3.2-8　米国のヒアリング対象候補機関（絞り込み後）

機関名	区分	選定理由
DARPA	政府機関	デュアルユース技術開発促進のためのコンテストの開催やＰＭに責任と権限が付与され、ハイリスク・ハイペイオフの研究開発に対しての資金援助やプロジェクト管理等を実施しており、ＰＪにおける情報保全の取組・事例に関しての情報を得られる可能性が高いため
ジョンスホプキンス大学　応用物理学研究所	政府機関	K プログラムと類似分野である宇宙、海洋、サイバー領域等をコンピテンシーとして研究開発を推進している。また独自研究開発プログラム（IRAD プログラム）といったスポンサーから資金提供を受けずに独自に国家戦略的技術開発を進める取組を実施しており、主体的な情報保全に関する取組事例を聴取することができると考えたため
MITRE Corporation	政府系研究機関(UARC)	K プログラムの研究領域である宇宙、サイバー領域等の研究を実施している他、National Security Engineering Center、National Cybersecurity Center of Excellence 等の FFRDC を 6 つ運営しており、会議体、PJ における情報保全に関する取組・事例についての情報を得られる期待が高い 複数の FFRDC を運営するとともに、独立した研究プログラムも実施しており、体系的な情報保全措置を構築していると想定され、有益な情報を得られるものと想定されるため
Sandia National Laboratories	政府系研究機関(UARC)	2021 年度において全 FFRDC の中で最も研究費の支出が多く、盛んに研究開発が行われていると推察される。また実用化研究への投資割合が多いため、社会実装フェーズに近しい研究開発関連情報に対する保全措置の取組について聴取できると想定される。国家安全保障やグローバルセキュリティに関する研究プログラムを推進しており、K プログラムに関連した情報も収集できるものと期待できるため
RAND Corporation	政府系研究機関(UARC)	シンクタンクであり、また National Defense Research Institute 等の FFRDC を 4 つ運営しており、会議体、PJ におけ

機関名	区分	選定理由
		る情報保全に関する取組・事例についての情報を得られる期待が高いため
CSIS	非営利組織	政策系シンクタンクであり、K プログラムに関連した領域も取り扱っていることから、情報保全に関する取組事例・情報を収集できるものと期待できるため

調整の結果、ヒアリングの実施が可能となった２つの機関(DARPA、CSIS)に対してヒアリングを実施する。ヒアリング項目については以下に示す。

(DARPA に対するヒアリング項目)

■ 研究開発推進会議体の内容

・ 会議体の構成等
  - DARPA のプログラム・プロジェクトでは PM を中心にテーマ選定やマイルストーンによる評価管理、研究者の調整等、会議体の取り纏めを行っているという理解であるが、具体的に組成する会議体の有無・構成。研究開発を管理する側の体制として、PM 以外の体制と各人員の役割
  - 社会実装に向けてプログラム・プロジェクトとして工夫している点。特に進捗確認の観点から、Ｒ＆Ｄの対象の絞り込みやステージゲートを設ける際の考え方、方法論（プログラムの継続・中止の判断も含む。）

・ 参加する機関・人員の制限
  - 会議体に参加する PM 以外のメンバー・機関の選定方法や参加要件、特にセキュリティ・クリアランス要件、各プログラムで共通して設定している事項等
  - プログラムによって、外国人、外国の企業・機関の参画が制限される事例。制限を設けるケース、制限の内容（例：FOCI）
  - DARPA の一般職員と PM に求められるクリアランスの差異。PM ごとに参画するプログラムに応じて求められるクリアランスの差異。および背景調査（バックグラウンドチェック））の有無。可能であれば、背景調査の調査項目やその調査内容の確認要領（オープンソースによる確認や関係機関等への確認を想定）について

・ 成果の帰属・段階的保全
  - DARPA では軍事技術を扱うプログラムを多く管理していると認識しているが、特に機密性の高い、もしくは経済安全保障上のリスクとなり得る研究開発成果を扱う場合の成果の帰属先に関する規定、同成果に対する公開制限の有無、ある場合それを規定する規則
  - DARPA が所管している SBIR プログラムでは中小企業による成果の商業利用を加速することがミッションの一つと認識しているが、軍事的即応性を維持することを念頭においたプログラムでもあり、経済安全保障上のリスクも懸念されると想定している。SBIR で審査する中小企業・スタートアップ企業に対して求める情報保全措置、審査の際に重視する、CI を扱うためのセキュリティ・クリアランス等の要件

- DARPA が所管する SBIR プログラムでは技術成熟度に応じてフェーズが 3 段階設定されていると認識している。フェーズが進むにつれて成果の周囲への影響度が上がり、経済安全保障リスクも増大するものと思われるが、フェーズごとの異なる情報保全規程の有無（また定めていない場合、）研究開発段階や成果の成熟度ごとに、異なる情報保全規程を設定することについての是非

■ 情報の取り扱い

・ 情報取り扱いに係る法令・ガイドラインの参照・規程の整備状況
  - DoD Cyber Security Requirements に基づき、DFARS § 252.204-7012 と NIST SP800-171 への準拠を原則としていることの正否
・ 情報取り扱いに係る人的事項
  - 研究プログラムの性質やプログラムへの関与度合い・役職に応じたパーソナル・セキュリティ・クリアランスの設定有無（例：SBIR プログラムに応募する事業者に対して求めているクアランス）
  - DARPA で実施している Bringing Classified Innovation to Defense and Government Systems（BRIDGES）プログラムでは、これまで政府と機密研究開発業務を実施した実績のない企業に対してセキュリティ・クリアランス取得支援や機密作業を行えるように促す取組を実施している。情報保全ノウハウのない企業に対して行っている具体的な支援策や感じている課題感
・ 情報取り扱いに係る物理的事項
  - DARPA として独自に、研究開発プログラムが対象とする技術の特性に応じて、または、情報の機密レベルに応じて施設ごとに設けているセキュリティ要件（施設へのアクセス制限や情報機器の持ち込み・使用制限等）
・ 情報取り扱いに係る技術的事項
  - 機密性の高い IT 環境の構築が求められる認識している。実験データ、ソフトウェア、プロトタイプ（試作品）、ノウハウなど、様々な種類の成果や中間生成物についての管理方法の実態

■ 情報取り扱いに係る規則の運用実態

・ 負担感
  - 情報取り扱いに係る規則で、実態として情報共有や手続き面での負担の有無及びその原因。特に DARPA では多様なプログラムを多数管理されている認識だが、特に情報保全で負担が大きなプログラムの特徴。また、これに係る研究室や研究者のような現場からの意見の有無・内容
・ 改善提案・要望
  - 上記に付随した改善提案、要望事項

（CSIS に対するヒアリング項目）

■ 情報保全体制について

・ CSIS が調査研究を実施する上で、政府（米国または外国）、国内外の 事業者・大学等と共同で調査研究を行う際に組成している/組成を求めるプロジェクト固有の情報保全体制等がある場合、その構成と役割

・ 上記で回答いただいたプロジェクト内での情報保全体制とは別に、CSIS 様内部で定常的に組成している情報保全体制を構築している場合、その構成と上記で回答いただいたプロジェクト内（委託先事業者等との間）で構築している体制との情報共有の方法（特に情報保全上留意している内容）

■ 情報保全措置について

・ CSIS 様の調査研究の中で委託先事業者や、政府（米国または外国）、国内外の事業者・大学等と共同で調査研究を行う際に相手に遵守を求められるまたは遵守を求める情報保全規則に関して、以下の事項及びそれが準拠している政府等の規則・ガイドライン等
・ 情報取扱に係る人的事項（外国籍の研究従事者又は共同研究機関として参画している大学等における留学生などに対する研究参加制限やパーソナル・セキュリティ・クリアランスの実施など、本プロジェクトへの従事者に対して設けている参加制限等）
・ 情報取扱に係る物理的事項（情報が保管されているスペースへのアクセス制限等）
・ 情報取扱に係る技術的事項（データ暗号化処理やネットワークの保護等）
・ 委託先事業者や、政府（米国または外国）、国内外の事業者・大学等と共同での調査研究とは別に、CSIS 様内部で定めている情報保全規則がある場合、その規則に関して以下の事項及びそれが準拠している政府の規則・ガイドライン等

■ 情報保全体制・措置の運用について

・ 情報保全体制や情報保全措置を運用する上で、特に負担に感じている体制の運用、規則等
・ 負担感に対しての改善策・（政府等への）要望等

c）英国

英国のヒアリング先としては、米国と同様に宇宙、海洋、サイバー、多義的技術領域等、日本のKプログラムに関連した情報を収集することが期待できる機関を中心に選定する(表3.2-9)。

表 3.2-9　英国のヒアリング対象候補機関

機関名	区分	選定理由
国防・セキュリティ促進機構（DASA）	政府機関	軍用技術の研究開発への主要な資金配分機関であることから、デュアルユース技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
英国宇宙庁（UK Space Agency）	政府機関	宇宙産業の研究開発への主要な資金配分機関であることから、Kプログラムの対象である宇宙分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
国立物理学研究所（National Physical Laboratory）	政府機関	計量学の観点からのバイオ、量子、航空宇宙等の研究開発への資金提供プログラムを持ち、Kプログラムの対象であるバイオ、量子、航空宇宙等の分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
高等研究発明局（Advanced Research & Invention Agency,ARIA）	政府機関	米国ARPAに倣った革新的な科学技術に対する資金配分機関であり、Kプログラムの対象となる領域、技術も資金提供対象となりうるため、これらの領域、技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため また、日本の指定基金協議会と同じく立ち上げて間もない機関であり、同じ立ち上げ段階の機関が情報の取扱等をどのように考えているのか情報を得られる可能性が高いため
工学・物理科学研究会議（EPSRC）	政府機関	工学・物理化学を中心とした幅広い領域の研究開発への資金提供プログラムを持ち、Kプログラムの対象である先端エネルギー、バイオ、先端材料等の分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
医学研究会議（MRC）	政府機関	医療領域の研究開発への資金提供プログラムを持ち、Kプログラムの対象であるバイオ分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
バイオテクノロジー・生物科学研究会議（BBSRC）	政府機関	バイオ領域の研究開発への資金提供プログラムを持ち、Kプログラムの対象であるバイオ分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
自然環境研究会議（NERC）	政府機関	環境に関連する研究開発への資金提供プログラムを持ち、Kプログラムの対象である先端エネル

機関名	区分	選定理由
		ギー技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
Innovate UK	政府機関	産業界や企業における研究開発への資金提供プログラムを持ち、K プログラムの対象である AI、センサーバイオ、量子等の領域、技術の研究開発も資金提供対象となりうるため、これらの領域、技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
国立ヘルスケアエクセレンス研究所（National Institute for Health and Care Excellence :NICE)	政府機関	医療領域の研究開発への資金提供プログラムを持ち、K プログラムの対象であるバイオ分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
英国ビジネスバンク（BBB）	政府系金融機関	デュアルユース技術を対象とした資金提供プログラムを持ち、デュアルユース技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため

これらの機関から所管課と協議の上、情報保全に関する具体的な情報等を得られる可能性が高いものとして、以下の機関に絞り込みを実施する。（表 3.2-10）

表 3.2-10　英国のヒアリング対象候補機関（絞り込み後）

機関名	区分	選定理由
国防・セキュリティ促進機構（DASA）	政府機関	軍用技術の研究開発への主要な資金配分機関であることから、デュアルユース技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
英国宇宙庁（UK Space Agency）	政府機関	宇宙産業の研究開発への主要な資金配分機関であることから、K プログラムの対象である宇宙分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
Innovate UK	政府機関	産業界や企業における研究開発への資金提供プログラムを持ち、K プログラムの対象である AI、センサーバイオ、量子等の領域、技術の研究開発も資金提供対象となりうるため、これらの領域、技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため
英国ビジネスバンク（BBB）	政府系金融機関	デュアルユース技術を対象とした資金提供プログラムを持ち、デュアルユース技術の研究開発に関する情報の取扱等の情報を得られる可能性が高いため

機関名	区分	選定理由
工学・物理科学研究会議（EPSRC）	政府機関	工学・物理化学を中心とした幅広い領域の研究開発への資金提供プログラムを持ち、K プログラムの対象である先端エネルギー、バイオ、先端材料等の分野の研究開発に関する情報の取扱等の情報を得られる可能性が高いため

調整の結果、ヒアリングの実施が可能となった機関(Innovate UK)及び上位組織の UKRI に対してヒアリングを実施する。ヒアリング項目については、以下のとおり。

（UKRI、Innovate UK に対するヒアリング項目）

■ 研究開発推進会議体の内容

・ 会議体の構成等
  - UKRI、Innovate UK が研究開発を支援するにあたり、研究開発推進のための会議体を組成するか。する場合、会議体の構成や構成員の役割について
  - UKRI の ISCF（産業戦略チャレンジ基金）では DARPA モデルを採用し、テーマごとにチャレンジ・ディレクターを選定、同ディレクターの裁量の下プロジェクトを推進していると認識だが、Innovate UK のプログラム・プロジェクトは基本的に DARPA モデルを採用しているのか
  - Innovate UK のプライバシー通知及び情報管理ポリシーのページ 1 にあるデータ保護責任者：Data Protection Officer、情報ガバナンス責任者：Head of Information Governance の役割及び研究開発プログラム・プロジェクトへ与える影響について
  - プロジェクトごとに割り当てられる Monitoring officer の役割は及び就任時・就任後に求められる要件

・ 参加する機関・人員の制限
  - UKRI、Innovate UK のホストするプログラム・プロジェクトによって、応募企業の所属国の要件が異なるが（英国に限る、特に問わない等）、どのような基準で所属国の要件を設定しているか
  - UKRI、Innovate UK のプログラムで採択する企業に対して人的・施設クリアランスを求めているか。求めている場合どのようなクリアランス制度に準拠しているか

・ 成果の帰属・段階的保全
  - UKRI、Innovate UK で基本的にプロジェクトの成果に関する所有権は受託者に帰属するものと理解しているが、成果物に Top Secret、Secret 等の機密情報などが含まれている場合の保全措置や機密情報が含まれているかの確認方法について
  - 成果に対する規制としては輸出管理法等が想定されるが、遵守すべき法令、ガイドラインの名称、それに関する UKRI、Innovate UK における内部規則の有無・内容について
  - UKRI、Innovate UK の所管プログラム・プロジェクトで設定されている技術成熟度（TRL など）の有無・概要、プロジェクトの進捗評価段階（中間評価や最終評価など）の有無・概要
  - 技術成熟度やプロジェクトの進捗評価段階ごとに異なる情報保全措置の有無・そ

の是非

- Innovate UK は主に実装フェーズの支援を実施している認識だが、実装フェーズと基礎研究段階にあるプログラム・プロジェクト及びその成果で、求める情報保全措置は異なるのか

■ 情報の取扱い

・ 情報取り扱いに係る法令・ガイドラインの参照・規定の整備状況
  - UKRI、Innovate UK は多様な分野の研究開発プログラム・プロジェクトを扱っているが、準拠すべき法令・ガイドラインをどのように選定し、応募資料に反映させているのか。円滑に準拠すべき法令・ガイドラインを特定し、応募資料に反映させるための工夫等はあるか。
  - 経済安全保障上の関係から準拠が求められる法令・ガイドラインの有無（例えば DSPCR）、Innovate UK の内部で定めている規則の有無・内容
・ 情報取り扱いに係る人的事項
  - 英国政府の持つ機密情報を扱う場合には HMG 人員セキュリティ管理等の政府共通のクリアランス制度に準拠するという認識だが、人的クリアランスを求めるプログラム・プロジェクトの基準はあるか
  - SBRI プロジェクトなどではスタートアップ企業の参画が想定されるが、スタートアップ企業に対しても大企業と同様の人的クリアランスを求めるのか。スタートアップ企業に対して何か人的クリアランスの取得支援を実施しているか。
・ 情報取り扱いに係る物理的事項
  - Innovate UK の情報管理ポリシーにおいて、制限区域へのアクセス制限や機密情報を保管する机の施錠等が定められているが、研究開発プログラム・プロジェクトに応じた、又は含まれるセキュリティ分類ポリシーの Top Secret、Secret、Official、Official-Sensitive 等の情報の機密性に応じた物理的な情報保全措置の有無・内容
・ 情報取り扱いに係る技術的事項
  - プログラムの参加者に対して、ネットワークや情報を保管するストレージやクラウド等セキュリティ要件を求める事の有無・内容
  - 様々なプログラム・プロジェクトで Innovate UK が収集、蓄積した情報を保管、内部・外部連携する上でのセキュリティ要件の有無・内容

■ 情報取り扱いに係る規則の運用実態

・ 負担感
  - Innovate UK は多種多様なプログラム・プロジェクト、情報を扱っていると認識しているが、情報の機密性を検討・判断する上での負担感、同情報を保全する上での負担感の有無・内容
・ 改善提案・要望
  - 上記の質問に付随した改善提案、要望事項

■ 研究開発プログラムの運営要領に関する質問

・ Innovate UK が、英国にとって重要な技術の研究開発・実用化や社会実装を進めるにあたって、民間企業等に研究開発を委託するプログラムの運営で工夫している事項

- どのように Innovate UK の支援する研究開発プログラムの研究テーマを選定しているのか
- どのようにプログラムの公募・採択を実施しているのか
- プロジェクト開始後は、どのように評価・進捗管理を行っているのか
- プログラムの成果の技術移転・実用化の手法
- 上記の工夫を可能にする Innovate UK の組織構造や体制

3.2.2 指定基金協議会の効果的な運営に資する事例調査

（1）実施方針

指定基金協議会による特定重要技術の研究開発とその成果の活用促進を効果的に行うことを念頭に、各国の研究開発推進に係る会議等の運営事例を調査する。指定基金協議会は、複数機関が研究開発テーマごとに複数の機関・団体が参加するプログラムの形態であることから、3.2.1.2 でショートリストとして抽出した研究開発プログラムを主な調査単位とする。他方、資金配分機関が特徴的なプログラムの運営モデルを有している場合などは機関を単位とした調査についても行う。

調査対象として抽出したプログラムの運営要領及び成功（失敗）の評価に関する事実を調査したのち、成功（失敗）の要因に関する分析を行い、その結果を各国・会議等横並びで比較する。成功（失敗）の定義としては、商業的な実用化、国際標準規格等の獲得の有無等とし、比較分析を行うことで、成功の要因、方法論、課題等（会議の規模、構成員の種別、開催形式・頻度、協議内容など）を明らかにする。

（2）実施項目・方法

3.2.1.2 で絞り込み抽出した資金配分機関または研究開発プログラムの中から、公開情報等が比較的充実しており運営実態を把握することが可能であること、及び特徴的なプログラムの運営モデルを有している等の観点から調査対象を絞り込む。当該研究開発プログラムの実施規程及びその評価・管理を実施する研究開発推進会議体の運営要領等を対象として下記の項目について調査を実施する。

調査件数については、政府機関の公開情報等が比較的充実・整理されており運営実態を把握することが可能であること、及び同盟国・同志国・日本との環境の親和性等の理由から国内 3 件以上のほか、米国、英国、韓国の各国 1 件以上を目途とする。

1）研究テーマの選定プロセス

調査対象となる機関・プログラムは研究開発テーマを選定するにあたって、どのような地位・役職に当たる責任者が裁量を持って検討を実施しているのか、テーマの決定に至るまで踏んでいるプロセスやそれに要する期間、検討にあたって実施している特徴的な取り組み（外部有識者との意見交換やニーズのヒアリングなど）について整理する。

2）公募・採択プロセス

研究テーマを選定した後、プロジェクトの公募を行い採択に至るまでのプロセスについて、プロセスの段階的実施事項や、どのような地位・役職に当たる責任者が決定権を持っているのか、具体的な指標・評価決定要領等について整理する。

3）プロジェクトの評価・管理方法

プロジェクトが開始した後、プロジェクトの進行状況の把握・管理を行っている責任者の裁量や、管理のためのステージゲート等マイルストーンの設定、プロジェクト継続の可否を判断する評価基準等について整理する。

4）知的財産権の扱い

プロジェクトの成果を商業的な実用化、社会実装に繋げるために実施している取り組み（ニーズを持つ主体とのマッチング等）や、成果がより活用されるための知的財産権の管理、成果の帰属に関する規定内容等について整理する。

5）海外企業の参画に係る制約

プログラムに海外の企業等が参加するにあたり課せられる、参加制限や研究場所の指定、研究員の受け入れ、輸出管理等の制約について整理する。

6）他のプログラム・機関との差別化要素

上記のプログラムの運営要領における、当該プログラム・機関の持っている特徴的な事項について整理し、特に当該プログラム・機関の成功（失敗）に関する原因等と紐づく理由のある場合、記載する。

3.2.3 意見交換の開催

(1) 実施方針

国内及び主要国の企業・国立研究所・会議等における秘密情報等の取扱い及びこれに従事する主な機関の調査及び整理及び指定基金協議会の効果的な運営に資する事例調査に関する調査・分析の状況について、隔月１回程度を目安に、政府関係者等を交えた意見交換会を実施する。

(2) 実施項目・方法

意見交換に関しては、全4回オンラインで、議題についての調査結果を報告後、調査結果に基づいて、政府関係者等と意見交換を実施することとした。(第2回意見交換会以降については前回の意見交換で得られたコメントに対する反映結果についても報告に含まれている)意見交換会の日程及び主な議題については以下の通りである。(表 3.2-11)

表 3.2-11　意見交換会の日程及び主な議題

回	日程	主な議題
第1回	令和5年8月31日	・ 調査進捗(多目的技術開発に係る日・英・米・韓の動向) ・ ヒアリング対象機関の候補、ヒアリング項目案 ・ 意見交換 ➢ ヒアリング候補機関について ➢ ヒアリング項目について
第2回	令和5年10月27日	・ 前回の意見交換会でいただいたコメントに対する調査結果 ・ 研究開発成果の段階的保全に関する調査結果 ・ 現地ヒアリングの調整状況 ・ 意見交換 ➢ 段階的保全に関する調査結果を踏まえて、段階的な成果の情報保全を図っていくべきか・否か ➢ リストアップした質問事項以外に聞いた方が良い内容について
第3回	令和5年12月26日	・ 前回の意見交換会の振り返り ・ 領域別研究開発における情報保全措置の調査結果 ・ 意見交換 ➢ 領域（宇宙・海洋）別に情報保全上留意が必要と思われる事項について ➢ 本調査事業で得られた調査結果の整理・分析の取り纏め方針について
第4回	令和6年3月1日	・ 前回の意見交換会の振り返り ・ ヒアリング結果の共有 ・ 研究開発プログラムにおける情報保全措置・運営要領に関する比較・整理及び総括

回	日程	主な議題
		・　意見交換 ➢　比較・整理結果を踏まえた、総括の観点や導き出せる示唆・課題について

4. 調査結果

4.1 国内及び主要国の企業・国立研究所・会議等における秘密情報等の取扱い及びこれに従事する主な機関の調査及び整理

4.1.1 国内外の秘密情報の取り扱いに係る法令・ガイドライン等の調査・整理

(1) 日本

1) 基本情報

- 政治体制：議員内閣制
- 人口：約 1 億 2,452 万人（2023 年 6 月現在）
- 名目 GDP：約 591.5 兆円　実質：約 558.7 兆円（2023 年度）
- 研究開発予算：約 20 兆 7,040 億円（2022 年度科学技術研究費）

■　政治動向

日本は歴史的経緯から米国との深い同盟関係を有している一方、周辺環境ではロシア、中国、北朝鮮等の力による現状変更行為に懸念のある国々と近接していることから、安全保障上の懸念を多く有しており、近年は国際関係における均衡を特にインド太平洋地域に求め、「自由で開かれたインド太平洋（FOIP)」のビジョンのもと、米国をはじめとして英国、ドイツ、フランス、オーストラリア、インド、韓国等の同志国と経済・安全保障面で協力を強化している[12]。

■　経済動向

日本は天然資源に乏しいことからエネルギー資源を中心に輸入への依存度が高く、紛争に起因する原油等エネルギー価格の上昇から 2022 年度に過去最大の貿易赤字を記録した。産業構造としては、電子・電気機器、輸送機器（自動車、船舶)、化学製品、鉄鋼などの製造輸出に強みを持っている。

世界第 3 位の GDP を有しているが、1990 年代初頭のバブル経済崩壊以降、内需の減少や生産年齢人口の減少といった供給力の低下を背景として実質 GDP 成長率は 20 年間で平均 0.8%程度となっており、低成長が続いている[13]。

現政権の主要政策では「新しい資本主義」を掲げ、リスキリングによる能力向上支援、個々の企業の実態に応じた職務給の導入、成長分野への労働移動の円滑化によって労働市場改革を進める他、金融資産所得の拡大などにより家計所得の増大を図るとともに多様な働き方の推進等を通じ企業の生産性を向上させることで構造的な賃上げの実現を図っている[14]。

---

[12] https://www.cas.go.jp/jp/siryou/221216anzenhoshou/hosyousennryaku_gaiyou.pdf

[13] https://www5.cao.go.jp/j-j/wp/wp-je15/h03-01.html

[14] https://www.kantei.go.jp/jp/headline/seisaku_kishida/newcapitalism.html

■　　社会動向

日本は長期の人口減少過程に入っており、約 40 年後には総人口が一億人を割り込むと推計されている。高齢化率についても年々上昇傾向にあり、65 歳以上人口は総人口の約 3 割を構成していることから少子高齢化社会に直面している。それにより社会保障費の増大による財政の圧迫、労働人口の減少による生産力の低下等が社会問題となっている[15]。

現政権の主要政策では、児童手当の拡充、出産・高等教育費の負担軽減等の経済的支援の強化等のこども・子育て政策の推進によって少子化傾向の反転を図っている。

■　　技術動向

日本の科学技術研究開発予算は米国・中国に続き世界第 3 位となっているが、4 位以降の韓国・ドイツとの差は緩やかに縮まりつつある[16]。

日本における科学技術政策は科学技術基本法を根拠とする科学技術基本計画を国の方針として推進されてきたが、2021 年に人文科学を含む科学技術の振興とイノベーション創出を図るため、科学技術基本法は「科学技術・イノベーション基本法」に改正され、現在は第 6 期科学技術・イノベーション基本計画（2021 年）に沿った政策が実行されている。

科学技術・イノベーション政策の推進体制としては、上記の科学技術・イノベーション基本計画に則り、司令塔的機能を持つ内閣府の総合科学技術・イノベーション会議（CSTI）、科学技術・イノベーション推進事務局等を通じて、各領域を担当する省庁及び省庁の所管する独立行政法人、国立研究開発法人等のうち資金配分機能を持つ機関・部署から民間企業、大学等への資金提供が行われ研究開発プログラムが実行される体制となっている（図 4. 1-1）。

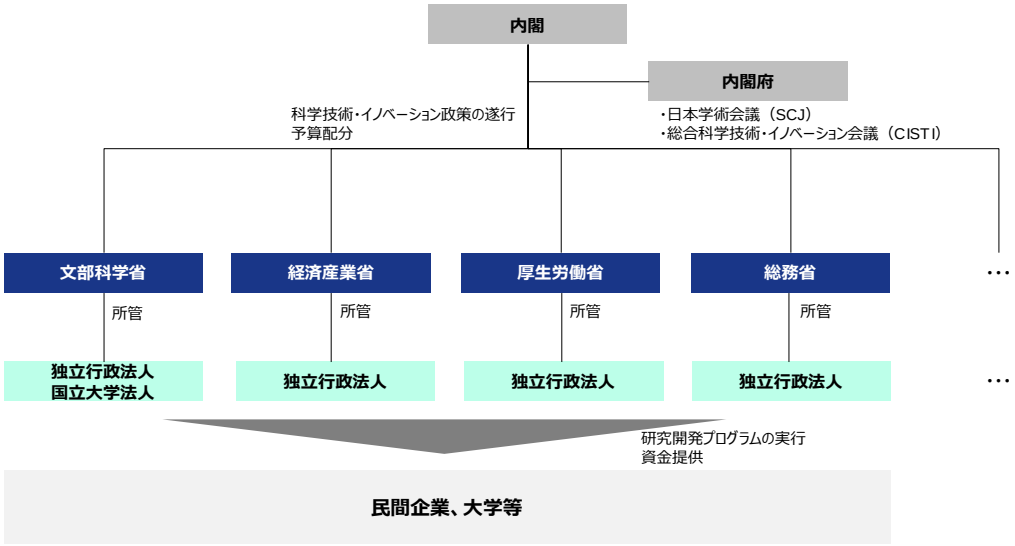


図 4. 1-1　日本の科学技術・イノベーション政策の推進体制

[15] https://www8.cao.go.jp/kourei/whitepaper/w-2022/html/zenbun/s1_1_1.html

[16] https://www8.cao.go.jp/cstp/kihonkeikaku/6gaiyo.pdf

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

日本では、政府機関の扱う秘密情報については 1947 年に制定された国家公務員法に基づき、国家公務員に「職務上知ることのできた秘密」の守秘義務が課されてきた。ここでの秘密とは「非公知の事実であって、実質的にもそれを秘密として保護するに値すると認められるもの」が該当するとされる[17]。

そして 2006 年から 2007 年にかけて、国家公務員法の守秘義務に加えて政府統一的な秘密保全制度の必要性について議論がなされ、「カウンターインテリジェンス推進会議」が組織され「カウンターインテリジェンス機能の強化に関する基本方針」が決定された。同方針によって「国の行政機関が保有する国の安全、外交上の秘密その他の国の 重大な利益に関する事項であって、公になっていないもののうち、特に秘匿することが必要なものとして当該機関の長が指定したもの」を「特別管理秘密」として指定し、適格性を確認した者にのみ取り扱わせる「特別管理秘密に係る基準」が 2009 年に施行された[18]。

その後、2010 年の尖閣諸島中国漁船衝突映像流出事件や、ファイル共有ソフト「Winny」を通じた警視庁国際テロ捜査情報流出事件などを経て、機密性の高い情報を取り扱う政府機関における情報保全措置の必要性が求められたことから、2013 年に特定秘密保護法が成立し、安全保障（国の存立に関わる外部からの侵略等に対して国家及び国民の安全を保障すること）に関する情報のうち防衛・外交・特定有害活動・テロリズムに関する事項など特に秘匿することが必要であるものを「特定秘密」として指定してその漏洩に罰則を設ける等して保護することとなった[19]。特定秘密には「武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの製作、検査、修理又は試験の方法」など研究開発に関係する情報についても類型が規定されている。

軍事・防衛に関する秘密については、1954 年に制定された自衛隊法によって国家公務員法と同様の守秘義務が自衛隊員にも規定されており、それによって職務上知ることのできた秘密（いわゆる省秘等）の保全が図られている[20]。また同年には「日米相互防衛援助協定等に伴う秘密保護法」の制定によって米国政府から供与された装備品等についての構造又は性能その他の事項及びそれに係る文書、図画又は物件で公になっていないものは「特別防衛秘密」として指定され、保全が図られることとなった。

2001 年に自衛隊法改正によって「防衛秘密」制度が創設され、一般に公開されていない情報で防衛上特に秘匿する必要があり、防衛大臣が指定した情報を「防衛秘密」として保全措置を講じることとなったが、前記の 2013 年の特定秘密保護法成立に伴い、自衛隊法の防衛秘密に関する規程は削除され特定秘密に統合された[21,22]。

---

17 https://elaws.e-gov.go.jp/document?lawid=322AC0000000120（第 100 条）

18 https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2013pdf/20131202015.pdf

19 https://www.cas.go.jp/jp/tokuteihimitsu/index.html

20 https://elaws.e-gov.go.jp/document?lawid=329AC0000000165（第 59 条）

21 https://www.nikkei.com/article/DGXNASFS0103Z_R01C13A1PP8000/

22 https://www.kantei.go.jp/jp/topics/2013/headline/houritu_gaiyou.pdf

近年では国家安全保障上のリスクが経済活動の領域にも拡大したことから、現政権において経済安全保障は重要施策として位置付けられており、2021 年に成立した「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（以降、経済安全保障推進法)」では安全保障を確保するための経済施策として①重要物資の安定的な供給の確保②基幹インフラ役務の安定的な提供の確保③先端的な重要技術の開発支援④特許出願の非公開に関する制度が創設された[23]。各種制度の中では電気、ガス、水道等基幹インフラの重要設備導入・維持管理等の委託に係る事前審査や、安全保障上機微な発明の特許出願について公開や流出を防止するなど、経済活動において安全保障上公にすべきでない情報の保全に関する取組みが進められている。

また経済安全保障推進法の成立に付随して、民間企業等が先進的技術開発に係る同盟国の政府調達に参加する際、国際的に通用する統一的な情報保全措置が必要となることや、安全保障の概念が経済・技術の分野へと拡大していることを踏まえて、政府が機密情報の取り扱い資格者を認定することによって情報保全を図るセキュリティ・クリアランス制度の検討が内閣官房の「経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議」において 2023 年 2 月から進められていた。2024 年 1 月に報告された最終とりまとめでは、セキュリティ・クリアランス制度の必要性に触れるとともに、政府が保有する経済安全保障上重要な情報として指定された情報（CI(Classified Information))にアクセスする必要がある者の信頼性を確認した上でアクセスを認める制度の整備が求められている[24,25]。

産業分野における経済安全保障的観点からの情報保全推進の一例として、F-35 等の米国 FMS 調達装備品の国内企業による製造・維持整備、SM-3 等の日米共同開発・生産、日英伊による次期戦闘機共同開発（GCAP）といった防衛産業の国際化の進展に伴い、米国をはじめとする同盟国との間で秘密情報を適切に保護するための産業保全制度の実質的同等性が必要となったことから、米国の「国家産業保全プログラム運用マニュアル（NISPOM)」のような他国の例に倣い、防衛産業に関係する秘密情報の保全に関する法令、防衛省内規則を一元的に取り纏めた「防衛産業保全マニュアル」が 2023 年 7 月に防衛装備庁によって整備されている[26]。

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

日本では 1949 年以降外国為替、外国貿易その他の対外取引を総合的に対象とする「外国為替及び外国貿易法（外為法)」を根拠として、安全保障の観点から国の安全に関わる対内投資の規制強化、国際的な輸出管理レジームへの批准に伴う貿易管理の強化など、時代に即して更新が図られてきた。同法は輸出規制や外資規制等に係る法令として、武器や軍事転用可能な貨物や技術の輸出について規制する安全保障貿易管理制度や、外国からの対内直接投資について制限を設ける対内直接投資管理制度などの根拠法となっている。

安全保障貿易管理制度については、2021 年に日本国内における居住者から非居住者への

---

[23] https://www.cao.go.jp/keizai_anzen_hosho/

[24] https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/index.html

[25] https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/4index.html

[26] https://www.mod.go.jp/atla/dism.html

技術提供について管理する「みなし輸出」について、人を介した機微技術流出のリスクに対応するため管理強化を行うことが閣議決定され、2022 年に施行・適用された。

これにより、これまで入国後 6 ヶ月経過もしくは日本国内に勤務する外国人（居住者）への技術提供は、みなし輸出管理の対象外とされていたが、居住者への技術提供であっても雇用契約や経済的利益等に基づき外国政府もしくは外国法人（非居住者）の強い影響を受けている状態に該当する者への技術提供は、みなし輸出として管理されることが明確化された[27]。

研究開発においても、安全保障貿易管理は大学や研究機関の国際的な人的交流や外国との共同研究などの機会で遵守する必要があるため、経済産業省は 2008 年に「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）」を策定し、以降外為法上の規制強化に伴うその内容を更新してきた。現在は上記のみなし輸出管理の強化を反映した第四版が最新となっている[28]。

[27] https://www.meti.go.jp/policy/anpo/anpo07.html

[28] https://imo.chiba-u.jp/risk/security/files/an_gui4.pdf

3）研究開発プログラムにおける法令・ガイドライン等

a）宇宙領域

■　国家戦略等

日本では 1967 年の宇宙条約への加盟以降、宇宙救助返還条約、宇宙損害責任条約、宇宙物体登録条約といった国際的な宇宙諸条約に加盟してきたものの、民間企業等非政府組織の宇宙活動に対する国内法は整備されてこなかった。その後民間の宇宙活動の進展に伴い[29]、宇宙諸条約を担保するために 2008 年に国内の宇宙開発の基本的な方針を定めた「宇宙基本法」を制定し、次いで 2016 年には「人工衛星等の打上げ及び人工衛星の管理に関する法律（宇宙活動法）[30]」「衛星リモートセンシング記録の適正な取扱いの確保に関する法律（衛星リモートセンシング法）[31]」（宇宙 2 法）が制定された。

そして宇宙基本法を根拠として、政府が宇宙開発利用に関する施策の総合的かつ計画的な推進を図るため、宇宙開発利用に関する基本的な計画として「宇宙基本計画」を定めている。宇宙基本計画は毎年更新され、最新の令和 5 年度宇宙基本計画では、(1)宇宙安全保障の確保　(2)国土強靭化・地球規模課題への対応とイノベーションの実現　(3)宇宙科学・探査における新たな知と産業の創造　(4)宇宙活動を支える総合的基盤の強化を目標に掲げており、宇宙安全保障の確保面では、情報収集衛星や衛星コンステレーションによる情報収集、宇宙領域把握（SDA）体制の構築、宇宙安全保障と宇宙産業の発展の好循環を目指すとしている[32]。

経済安全保障の側面では、外為法上の安全保障貿易管理の規制品目リストや、対内直接投資審査制度の事前届出対象業種には宇宙領域に関連した技術・貨物・業種の指定が確認できることから、宇宙領域は日本の経済安全保障的観点において規制対象となっていることが伺える。例えば、安全保障貿易管理制度のリスト規制貨物の武器、ミサイル、センサー等、航法装置、機微品目に軍用人工衛星又はその部分品、宇宙用光学部品、衛星航法システムといった宇宙領域に関連した貨物・技術が見られる[33]ほか、対内直接投資審査制度では事前届出対象業種のうち国の安全等を損なうおそれの大きい業種（コア業種）に武器・航空機・宇宙・原子力関連業種が指定されている[34]。

■　研究開発機関

宇宙領域の研究開発推進体制としては、内閣の宇宙開発戦略本部及びその事務局たる内閣府宇宙開発戦略推進事務局が宇宙基本計画の策定と関係省庁との総合調整を行っている。宇宙領域に関係する機関は多岐に渡るが、主に内閣府、総務省、文部科学省、経済産業省の共同所管する宇宙航空研究開発機構（JAXA）が衛星利用、宇宙環境利用、有人宇宙活動、宇宙科学探査、ロケット・輸送システムといった分野で基礎研究から実用化まで一貫した研究開発を実施しているほか、静止気象衛星の運用を中心とした研究開発を所管する気象庁や、

[29] https://www8.cao.go.jp/space/comittee/dai65/siryou1-3-1.pdf

[30] https://elaws.e-gov.go.jp/document?lawid=428AC0000000076

[31] https://elaws.e-gov.go.jp/document?lawid=428AC0000000077

[32] https://www8.cao.go.jp/space/plan/keikaku.html

[33] https://www.meti.go.jp/policy/anpo/guidance/guidance.pdf

[34] https://www.meti.go.jp/policy/anpo/shiryo-toushikanri.pdf

安全保障分野における宇宙空間の利用について任務遂行能力の構築を実施する防衛省などが宇宙領域の研究開発を実施している（図 4.1-2）。

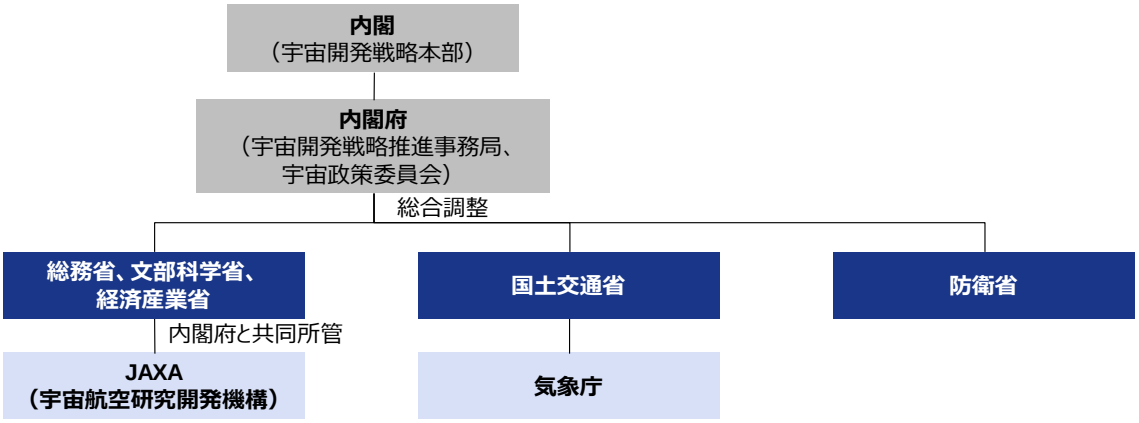


図 4.1-2　日本における宇宙領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン等

・　革新的衛星技術実証プログラム

JAXA が所管するプログラムであり、大学や研究機関、民間企業等が開発した部品や機器、超小型衛星、キューブサットに宇宙実証の機会を公募によって提供するプログラム。現在は第 5 号機に搭載する実証テーマの公募を行っている[35]。

研究開発にあたり遵守すべき法令等としては、委託研究開発の契約書において外為法の遵守が求められている他、前記の宇宙 2 法（宇宙活動法及び衛星リモートセンシング法）に係る政府の許可を取得することが公募要領に示されている。

宇宙活動法ではロケットや人工衛星の打上げについて政府による許可制度を設けているほか、衛星リモートセンシング法では人工衛星に搭載された装置により得られたデータ（リモートセンシングデータ）の適正な取扱いを確保するため衛星リモートセンシング装置の使用に係る許可制度や衛星リモートセンシング記録保有者の義務、取り扱い者の認定などについて定められている。

・　課題解決に向けた先進的衛星リモートセンシングデータ利用モデル実証プロジェクト

内閣府宇宙開発戦略推進事務局が所管する研究開発プロジェクトであり、新事業・新サービスの創出、既存産業の価値・生産性向上、地方創生、制度改革やマニュアル化等による行政利用の促進等に貢献する、実用化を目指した衛星データ利用モデルの実証提案を募集している[36]。

[35] https://www.kenkai.jaxa.jp/kakushin/index.html

[36] http://www.uchuriyo.space/model/document/fy2023_outline.pdf

b）海洋領域

■　国家戦略等

日本の海洋領域に関する政策の総合的な計画は、海洋基本法を根拠とした「海洋基本計画」　によって定められている。海洋基本計画は 5 年に 1 回見直しが行われ、現在は 2023 年 4 月に成立した海洋基本計画（第 4 期）が最新となっている [37]。

海洋基本計画（第 4 期）は政策的支柱として「Ⅰ　総合的な海洋の安全保障」と「Ⅱ　持続可能な海洋の構築」の２つを定めており、「Ⅰ　総合的な海洋の安全保障」は領海における国益の確保、国際的な海洋秩序の維持・発展、自然災害の防災・減災、経済安全保障に資する取り組みの推進、海上状況把握（MDA）能力の強化などに重点を置いている。「Ⅱ　持続可能な海洋の構築」はカーボンニュートラル、海洋環境の保全・維持、水産資源の管理など、脱炭素社会の実現と海洋産業の成長に重点を置いている。

経済安全保障の側面では、外為法上の規制において安全保障貿易管理制度のリスト規制品目にセンサーや航法装置等の海洋領域との関連が見られるほか、「海洋関連」という項で海洋領域に関連した貨物全般の規制がなされている。対内直接投資審査制度においても海運分野は規制対象業種となっている [38]。

■　研究開発機関

海洋領域の研究開発推進体制としては、内閣の総合海洋政策本部及びその事務局たる内閣府総合海洋政策推進事務局によって海洋基本計画に基づいた施策の実行に係る総合調整が行われている。

海洋領域に関係する機関は多岐に渡るが、主に文部科学省、経済産業省（資源エネルギー庁）、農林水産省、環境省、国土交通省、防衛省及び各省庁の所管する研究開発法人等によって海洋科学・地球科学・海洋技術（JAMSTEC）、海底資源・エネルギーの探査開発（JOGMEC）、水産・漁業資源の利用（FRA）、環境問題・生態系保護（NIES）、海上輸送、港湾開発、周辺海域における安全保障の確保（国土交通省、防衛省）など様々な面から研究開発が実施されている（図 4.1-3）。

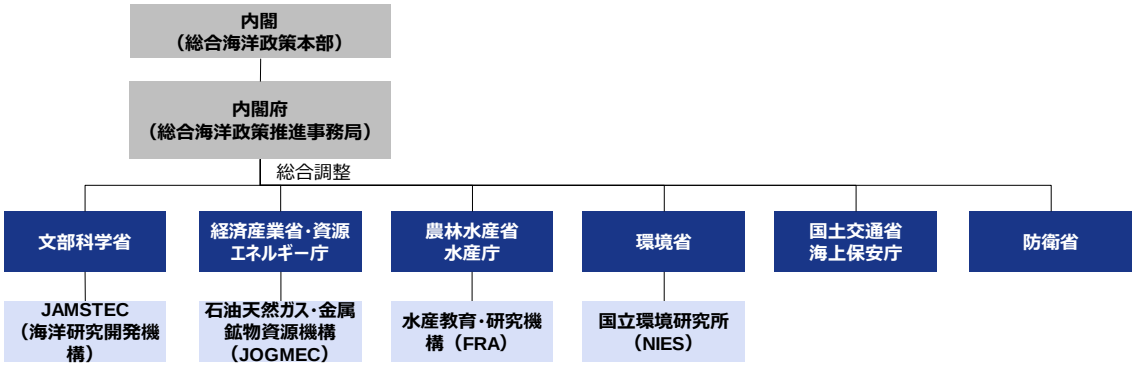


図 4.1-3　日本における海洋領域研究開発の主要機関

[37] https://www8.cao.go.jp/ocean/policies/plan/plan04/plan04.html

[38] https://www.meti.go.jp/policy/anpo/guidance/guidance.pdf

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン等

・ SIP 第 3 期課題「海洋安全保障プラットフォームの構築」

2023 年から開始された内閣府の所管する戦略的イノベーション創造プログラムの第 3 期における研究課題の一つであり、第 2 期までの成果を活用してレアアースの生産技術の確立、海洋環境広域モニタリングシステムの構築などを行うとしている[39]。

研究開発にあたり遵守すべき法令等としては、研究推進法人である JAMSTEC が JOGMEC との間に「南鳥島周辺海域における海洋調査活動で取得した探査・調査データ及びサンプルの取り扱いに関する合意書」を締結しており、JOGMEC から JAMSTEC へ提供された探査・調査データ及びサンプルのうち、研究開発のために JAMSTEC から参加研究機関へ提供される探査・調査データ及びサンプル（JOGMEC データ）の取り扱いについて、特約条項を規定している[40]。

[39] https://www2.njss.info/offers/view/25011850

[40] https://www.jamstec.go.jp/sip3/j/structure/index.html

c）バイオ領域

■　国家戦略等

日本では「2030 年に世界最先端のバイオエコノミー社会を実現」することを目標とした国家戦略として、2019 年に「バイオ戦略 2019」が策定された。そしてバイオ戦略 2019 に沿って政府予算約 62 億円を投じてバイオ製造実証に向けた技術開発などを推進していたものの、新型コロナウイルス感染症の流行に伴う経済減速・サプライチェーンの寸断などの影響を受け、感染症に対応するワクチン開発やエネルギー資源の自立分散化のためのバイオマス利活用の重要性が認識された。

上記のような情勢変化を踏まえて、（当時）直ちに取り組むべき感染症対策に係る研究開発や経済回復を見据えた「バイオ戦略 2020」が策定され、バイオ戦略 2020 では、以下のような基本施策が規定されている[41]。

（バイオ戦略 2020 における基本方針）

1. **新型コロナウイルス感染症対策に係る研究開発等の推進**
   - **診断法、治療法、ワクチン開発、機器・システムの開発等研究開発の推進**
   - **研究開発等環境の整備、国際連携等**
   - **ワクチンの早期実用化のための体制整備**
2. **市場獲得を実現するデータ連携促進**
   - **バイオデータ連携・利活用に関するガイドライン（仮称）の策定**
3. **グローバルバイオコミュニティ・地域バイオコミュニティの形成**
   - **グローバルバイオコミュニティ・地域バイオコミュニティの認定、連携促進、市場領域の推進、 国内外への情報発信**

■　**研究開発機関**

バイオ領域の研究開発推進体制としては、内閣府に設置されたバイオ戦略会議、健康・医療戦略推進事務局等が中心となってバイオ領域を含む研究開発に関する基本的な指針の策定を所管しており、その下で厚生労働省、文部科学省、農林水産省及びその所管の研究開発法人等が中心となって、医療・健康、感染症対策、遺伝学、農業技術・生物産業などの観点からバイオ領域に係る研究開発が進められている。

厚生労働省の所管では日本医療研究開発機構（AMED）が医療分野の基礎から実用化までの一貫した研究開発を実施している他、国立感染症研究所（NIID）が感染症の病原、病因及びその予防・治療に関する研究を実施している。NIID は日本で初めて BSL-4（バイオセーフティレベル[42]）の対応施設に指定された実績を持つ。

また文部科学省の所管する国立遺伝学研究所（NIG）では菌などの分子レベルから生物集団に至るまでの遺伝学に関する幅広い基礎的研究を実施している他、農林水産省所管の農業・食品産業技術総合研究機構（NARO）では農業技術の発達、新たな生物産業の創出を目的とした農業分野のバイオテクノロジー研究開発を実施している（図 4.1-4）。

41 https://www8.cao.go.jp/cstp/bio/index.html

42 世界保健機関（WHO）の定める Laboratory biosafety manual に基づき分類される、細菌・ウイルス等微生物・病原体を扱う施設のセキュリティ格付け

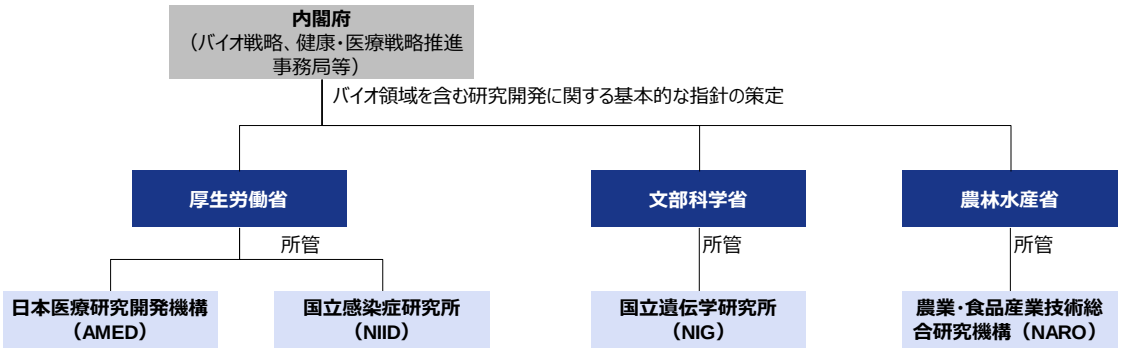


図 4.1-4　日本におけるバイオ領域研究開発の主要な機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　新興・再興感染症に対する革新的医薬品等開発推進研究事業

AMED の所管する研究開発プログラムであり、国内外で対策が必要な感染症について、患者及び病原体に関わる疫学調査、病原体のゲノム及び性状・特性等の解析、病態解明等、総合的な感染症対策の強化を目指した基盤的研究を継続して推進することで、得られた知見をもとに新たな診断法・治療法・予防法の開発を目指すとしている[43]。

令和 6 年度事業では公募対象課題として、「重点感染症対策（薬剤耐性感染症以外）に資する研究」「重点感染症対策（薬剤耐性感染症）に資する研究」「その他の感染症対策に資する研究」「横断的な感染症対策に資する研究」の 4 区分に分類される 13 の公募研究開発課題を設定している[44]。

参加にあたり遵守すべき法令等としては、公募要領において医療研究に関する法令・倫理指針の他に、外為法（安全保障貿易管理制度）や国際連合安全保障理事会決議第 2321 号（北朝鮮に対する制裁措置）の科学技術協力に関する規程等、以下の法令等への対応等が示されている。

（新興・再興感染症に対する革新的医薬品等開発推進研究事業で遵守が必要な法令等）
- 外国為替及び外国貿易法
- 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）
- 大学・研究機関のためのモデル安全保障貿易輸出規程マニュアル
- 安全保障貿易ガイダンス（入門編）
- 国際連合安全保障理事会決議第 2321 号の厳格な実施について（依頼）
- AMED における研究開発データの取扱いに関する基本方針
- AMED 研究データ利活用に係るガイドライン
- 公文書管理制度（内閣府）
- 個人情報保護法等
- 情報公開制度（総務省）
- その他、医療研究、倫理等に関する法令等多数

[43] https://www.amed.go.jp/koubo/11/02/1102B_00083.html

[44] https://www.amed.go.jp/content/000119305.pdf

・　ウイルス等感染症対策技術開発事業

AMED の所管する研究開発プログラムであり、感染症の課題解決につながる研究開発や、新型コロナウイルス感染症対策の現場のニーズに対応した機器・システムの基礎研究・実証・改良研究を支援するために主として、①感染症の早期・大量診断に必要とされる機器・設備・システム、②感染拡大防止や早期対応に向けた機器・システム、③感染症の重症患者のための治療機器に関する機器・システム等の社会実装のための基礎研究・実証・改良研究の課題を公募課題としている。

参加にあたり遵守すべき法令等としては、公募要領において医療研究に関する法令・倫理指針の他に、外為法（安全保障貿易管理制度）に関する規程等、以下の法令等への対応等が示されている。

（ウイルス等感染症対策技術開発事業で遵守が必要な法令等）

- **外国為替及び外国貿易法**
- **安全保障貿易ハンドブック**
- **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）**
- **AMED における研究開発データの取扱いに関する基本方針**
- **AMED 研究データ利活用に係るガイドライン**
- **その他、医療研究、倫理等に関する法令等多数**

d）サイバー領域

■　国家戦略等

日本のサイバー領域に係る国家戦略としては、セキュリティの面では内閣サイバーセキュリティセンターが中心となって「サイバーセキュリティ戦略」が策定されており、政府から産業界に向けた働きかけや政府機関、重要インフラ事業者、大学・研究機関によるセキュリティ確保の取り組み、国家安全保障におけるサイバー分野の取り組み強化といった面から方針が示されている[45]。

研究開発及び産業戦略としては、「第６期科学技術・イノベーション基本計画」において Beyond 5G、スパコン、宇宙システム、量子技術、半導体等の次世代インフラ・技術の整備・開発等が重点施策として示されている他[46]、量子技術に対して国際的な注目が高まっている背景から、量子技術に関する戦略的な取り組みを示すために、社会変革に向けたビジョンを示した「量子未来社会ビジョン」、研究開発戦略である「量子技術イノベーション戦略」、実用化・産業化戦略の「量子未来産業創出戦略」がそれぞれ内閣府量子技術イノベーション会議によって策定されている[47]。

■　研究開発機関

日本では内閣サイバーセキュリティ戦略本部が主導してサイバーセキュリティに係る連携・協力が行われ、総務省、文部科学省及び所管の研究機関等を中心にサイバー領域の研究開発を実施し、また厚生労働省や国道交通省等の重要インフラ所管省庁は重要インフラのサイバーセキュリティに係る取り組みを実施する他国立研究開発法人・独立行政法人等を所管している（図 4.1-5）。

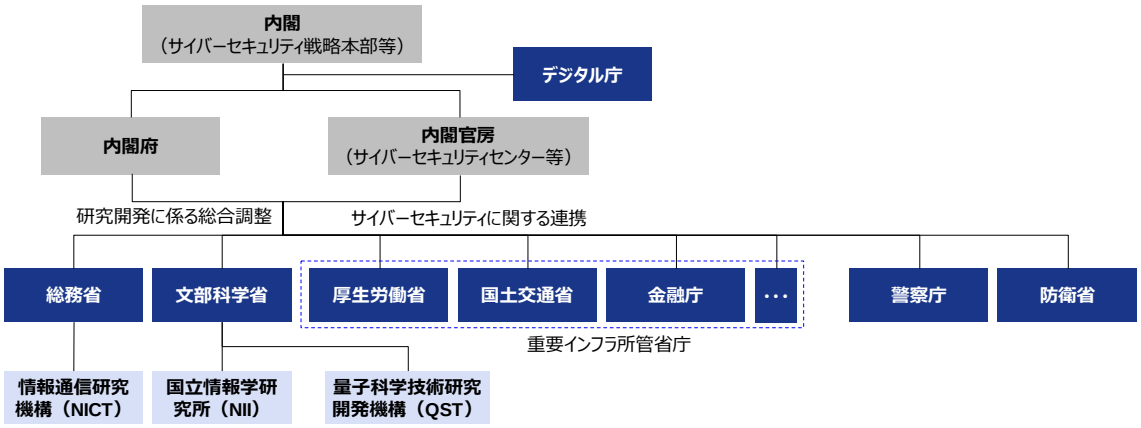


図 4.1-5　日本におけるサイバー領域研究開発の主要な機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　令和３年度 情報通信技術の研究開発に係る提案の公募：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発

45 https://www8.cao.go.jp/cstp/kihonkeikaku/6gaiyo.pdf

46 https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf

47 https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshigijutsu.html

総務省が所管している研究開発プログラムであり、総務省が研究開発課題を指定して、その研究開発の実施機関を公募し、これを選定の上、民間等の研究開発機関に委託することにより研究開発を行うものである。令和 3 年度は 3 つの研究開発課題について公募を実施しており、その中で「グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発」を公募している。

公募要領で準拠している法令等としては、サイバー領域特有ではないものの、安全保障貿易管理について外為法及び関連するガイドラインについて遵守を求めているほか、研究インテグリティや成果の帰属等の観点から以下のような法令等の遵守を求めている[48]。

（令和 3 年度 情報通信技術の研究開発：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発で遵守が必要な法令等）

- **外国為替及び外国貿易法**
- **安全保障貿易ハンドブック**
- **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）**
- **研究機関における公的研究費の管理・監査のガイドライン**
- **研究活動における不正への対応等に関するガイドライン**
- **産業技術力強化法**

- 2019 年度新規委託研究の公募（第三弾）：サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発

NICT が所管するプログラムであり、2019 年～2020 年にかけて実施された。NICT が開発中のマルウェア活動の活性化を自動的に検知する技術と連携し、その検知したイベントに関連するマルウェア・脆弱性・脅威情報などを実時間で精緻に提供することで、より有用性の高いセキュリティ情報自動分析基盤技術の確立を目指す研究開発を支援するものである[49]。

公募要領では、基本的に公募・提案に係る事務は NICT の事務マニュアルによって行うとしており、遵守を求める法令等については産業競争力強化法について成果の帰属の観点から触れている程度である。

[48] https://www.soumu.go.jp/menu_news/s-news/01tsushin03_02000323.html

[49] https://www.nict.go.jp/press/2019/08/28-1.html

e）多義的技術

■　国家戦略等

日本では、国内の科学者の代表機関である日本学術会議から 1950 年に「戦争を目的とする科学の研究は絶対にこれを行わない」旨の声明を、また 1967 年には「軍事目的のための科学研究を行わない声明」を発し、2017 年にも同様の立場を継承する声明を発するなど、多義的技術の研究開発には学術研究の自主性・自律性、研究成果の公開性の担保といった観点から慎重な姿勢が求められてきた[50]。しかし 2022 年に日本学術会議の発出した科学技術相に対する回答文書では、多義的技術について「新興科学技術には、用途の多様性ないし両義性の問題が常に内在している」「単純に二分することはもはや困難」「研究対象となる科学技術をその潜在的な転用可能性をもって峻別し、その扱いを一律に判断することは現実的ではない」との見解を示し、研究の進展に応じて研究成果の公開と安全保障面の配慮のバランスを慎重に考慮するなど、研究者や大学などの研究機関が研究の進め方を適切に管理することを求めている[51]。

他方、日本の防衛政策において多義的技術の重要性は高まっており、2021 年には防衛装備庁に同庁の研究者（研究職技官）を中心に、最先端技術に知見を有する民間の第一線の研究者（特別研究官）で構成する技術シンクタンク機能が創設され、研究職技官が、将来の戦い方とそれを実現するための技術をマッチングし、特別研究官が当該技術の調査や助言を行うという官民コラボレーションによる新たな取組が進められている。2022 年度版防衛白書では、「民生技術の進展が著しく、それらの先端技術が将来の戦闘様相を一変させ得る」「米国や中国をはじめとする各国が競って様々な民生技術の育成に多額の投資を行っていることは、経済的競争力のみならず、安全保障上の優位性をもたらす」と示された[52]。

日本における多義的技術分野に相当する研究開発プログラムとしては、2015 年から防衛装備庁において開始された安全保障技術研究推進制度があり、将来的に防衛分野に資することが期待できる先進的な基礎研究の公募・委託が実施されている他[53]、2022 年から経済安全保障推進法の下、日本にとって不可欠な先端的な重要技術について、科学技術の多義性を踏まえ、民生利用のみならず公的利用につながる研究開発及びその成果の活用を目指す研究開発プログラムである K プログラムが運用されている[54]。

■　研究開発機関

日本における多義的技術の研究開発は国の安全保障を所掌する防衛省を中心として実施されており、民間に研究開発を委託する研究開発プログラムとしては上記の安全保障技術研究推進制度が該当するため、当該制度の関係機関について記載する。

安全保障技術研究推進制度では、研究実施機関が応募された研究課題に対し、防衛装備庁及びその内部に設置された外部有識者委員会によって資金配分・委託、採択及び研究成

50 https://www.scj.go.jp/ja/member/iinkai/gunjianzen/index.html

51 https://www.scj.go.jp/ja/member/iinkai/kanji/pdf25/siryo328-integrity-kaitou25-1.pdf

52 https://www.mod.go.jp/j/publication/wp/wp2022/html/n440203000.html

53 https://www.mod.go.jp/atla/funding.html

54 https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html

果の評価等に係る審査・評価・審議が行われる体制となっている[55]。研究実施機関には、大学等教育機関、独立行政法人、特殊法人又は地方独立行政法人、民間企業や研究を目的とする交易社団法人、公益財団法人、一般財団法人等が含まれるが、原則として全ての機関・研究実施場所は日本国内に所在することが必要となる（図 4.1-6）。

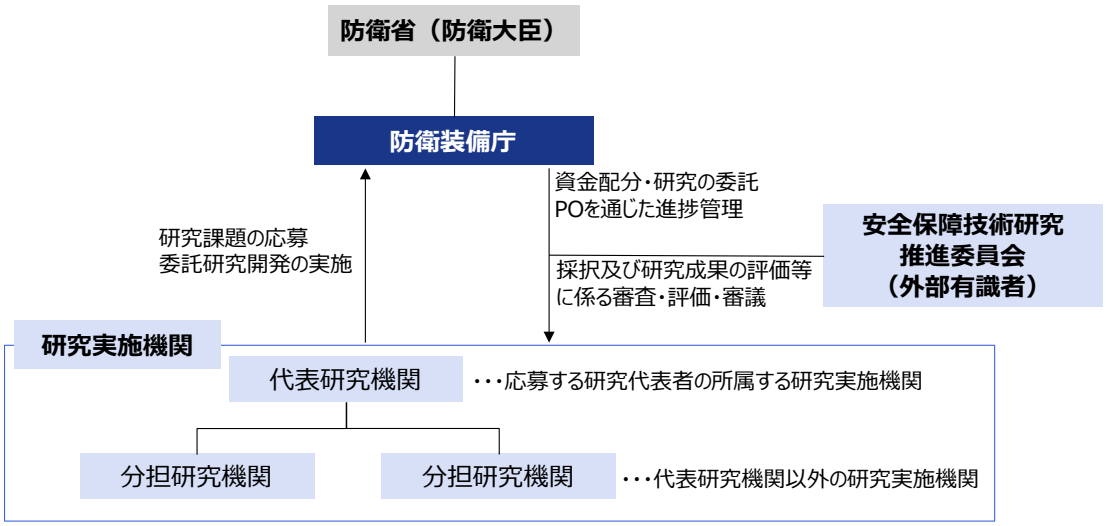


図 4.1-6　安全保障技術研究推進制度の関係機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　安全保障技術研究推進制度

防衛省　防衛装備庁が所管する研究開発プログラムであり、防衛分野での将来における研究開発に資することを期待して、先進的な民生技術についての基礎研究を公募している。

防衛装備庁から対象とする研究テーマを提示した上で研究課題を公募し、外部有識者による審査のうえ採択する課題を決定する。その後代表者の所属する機関と委託契約を締結する。特に革新性を有するアイデアに基づき科学技術領域の限界を広げるような基礎研究が求められ、いわゆるハイリスク研究も推奨している[56]。

参加にあたり遵守すべき法令等としては、防衛省における「保護すべき情報」を取り扱う可能性のある場合、「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」が契約事業者に適用されることとなっている。

[55] https://www.mod.go.jp/atla/funding/koubo/r05/r05koubo_full.pdf

[56] https://www.mod.go.jp/atla/funding.html

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして 46 件リストアップした（詳細は Appendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも 1 つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして 5 件抽出した（表 4.1-1)。

表 4.1-1　詳細調査を行う法令等のショートリスト

法令等の名称	理由
特定秘密保護法	日本における安全保障上機密として保護すべき情報の取り扱いについて規定している法律であり、機微情報を取り扱う研究開発の前提となる可能性のあるため
外為法	輸出管理や外国投資規制の根拠となる法律であり、研究開発における機微情報・技術の取扱いに関係する可能性のあるため
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）　第四版	上記外為法に係る具体的な大学・研究機関における情報管理策を確認できる可能性のあるため
研究データリポジトリ整備・運用ガイドライン	研究開発で取り扱うデータ全般の管理方法について確認できる可能性のあるため
大学における秘密情報の保護ハンドブック	大学の研究開発で取り扱う情報の管理方法について確認できる可能性のあるため

以下に表　4.1-1 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）特定秘密保護法 [57]

■　　策定機関・策定時期

2013 年

■　　策定の背景・目的

日本の安全保障（国の存立に関わる外部からの侵略等に対して国家及び国民の安全を保障することをいう。以下同じ。）に関する情報のうち特に秘匿することが必要であるものについて、これを適確に保護する体制を確立した上で収集し、整理し、及び活用するため、当該情報の保護に関し、特定秘密の指定及び取扱者の制限その他の必要な事項を定めたもの。

[57] https://elaws.e-gov.go.jp/document?lawid=425AC0000000108

■　適用範囲

主として行政機関の職員等を対象としているが、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等の基準に適合した、特定秘密に係る「物件の製造又は役務の提供を業とする者（適合事業者）」についても特定秘密を取り扱うことがある。

■　情報の分類

行政機関の長は、①法律の別表に該当する事項に関する情報であって、②公になっていないもののうち、③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を「特定秘密」として指定することができる。別表では「防衛に関する事項」「外交に関する事項」「特定有害活動の防止に関する事項」「テロリズムの防止に関する事項」の４項とその詳細が規定されている。

行政機関の長は、特定秘密の有効期間（上限５年で更新可能）を定め、有効期間満了前においても、指定の要件を欠くに至ったときは速やかに指定を解除する。指定の有効期間は通算３０年を超えることができず、やむを得ない理由を示して内閣の承認を得た場合に限り、通算３０年を超えて延長できる。ただし、この場合であっても、暗号や人的情報源等を除き通算６０年を超えて延長することはできない。

行政機関の長は、特定秘密を取扱う職員の範囲を定め、文書に特定秘密の表示をするなど、保護のために必要な措置を講じることとなっている。

■　情報管理策

主に本法律では特定秘密の指定、提供に係る組織的管理策と特定秘密取り扱い者の制限といった人的管理策について規定しており、物理的・技術的な管理策は「各行政機関の長が保護の為に必要な措置を講じること」とされている。

・　組織的管理策

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。

その他、特定秘密の取扱いの業務を行わせる従業者の範囲その他特定秘密の保護に関し必要な事項を契約に定めることによって安全保障上の特段の必要による事業者への特定秘密の提供を行う事や、外国の政府又は国際機関、刑事事件の捜査その他公益上特に必要があると認められる業務などに対して特定秘密を提供することができる

・　人的管理策

特定秘密の取扱いの業務を行うことができる者は、適性評価により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行政機関の職員若しくは事業者の従業者又は都道府県警察の職員に限る（行政機関の長、国務大臣等はその限りではない）。

適正評価では、①特定有害活動及びテロリズムとの関係に関する事項、②犯罪及び懲戒の経歴に関する事項、③情報の取扱いに係る非違の経歴に関する事項、④薬物の濫用及び影

響に関する事項、⑤精神疾患に関する事項、⑥飲酒についての節度に関する事項、⑦信用状態その他の経済的な状況に関する事項について調査を受ける。

■　　罰則

次に掲げるものによる故意又は過失による漏えいの処罰を規定している。

（特定秘密保護法で規定される故意又は過失による漏えいの罰則） **・　特定秘密を取り扱うことを業務とする者** **（故意：１０年以下の懲役、過失：２年以下の禁錮・５０万円以下の罰金）** **・　公益上の必要により行政機関から特定秘密の提供を受け、これを知得した者** **（故意：５年以下の懲役、過失：１年以下の禁錮・３０万円以下の罰金）**

また、外国の利益等を図る目的で行われる次に掲げる特定秘密の取得行為（未遂、共謀、教唆又は煽動を含む）の処罰を規定している。

（特定秘密保護法で規定される特定秘密の取得行為に係る罰則） **・　人を欺き、人に暴行を加え、又は人を脅迫する行為** **・　財物の窃取** **・　施設への侵入** **・　有線電気通信の傍受** **・　不正アクセス行為** **・　上記以外の特定秘密の保有者の管理を侵害する行為**

b）外国為替及び外国貿易法

■　　策定機関・策定時期

1949 年

■　　策定の背景・目的

外国為替、外国貿易その他の対外取引を総合的に対象とする法律であり、日本における対外取引の基本法となっている。1949 年の設立当初は対外取引原則禁止を定めるものであったが、1980 年の対外取引の原則自由化による規制の緩和や、安全保障の観点から国の安全に関わる対内投資の規制強化、国際的な輸出管理レジームへの批准に伴う貿易管理の強化など、時代に即して更新が図られてきた。研究開発及び情報保全に関わる主な規制としては、武器や軍事転用可能な貨物や技術の輸出について規制する安全保障貿易管理制度や、外国からの対内直接投資について制限を設ける対内直接投資審査制度などの根拠法となっている。

■　　適用範囲

・　安全保障貿易管理制度

安全保障貿易管理の対象となるのは貨物の輸出と技術の提供であり、貨物の輸出とは「船舶、航空機等を利用した一般的な輸送、ハンドキャリー、国際郵便（EMS）や国際宅配

便（クーリエ）等を利用した送付など貨物を本邦から外国に向けて送付すること」、技術の提供とは「技術データや技術支援（技術指導や技能訓練、コンサルティングサービス等）といった貨物の設計、製造又は使用に必要な特定の情報を、外国においてもしくは、居住者から非居住者又は特定類型に該当する居住者へ輸出、通信、人的交流等によって提供すること」が類型として該当する。

・　対内直接投資審査制度

対内直接投資審査の対象となるのは外国投資家（非居住者である個人、外国の会社、これらの者から 50%以上出資を受けている本邦の会社等）が、②国の安全等の観点から指定される事前届出の必要な業種を営む企業に対して、③投資等を行う場合である。

■　　情報の分類

記載なし

■　　情報管理策

安全保障貿易管理制度、対内直接投資審査制度では、輸出管理、対内投資に係る組織的な情報管理策を規定しているほか、取引に関係する個人・法人の居住性を判断するための人的管理策を規定している。物理的・技術的管理策は規定していない。

・　組織的管理策

安全保障貿易管理制度では国際的な合意を踏まえ、武器並びに大量破壊兵器等及び通常兵器の開発等に用いられるおそれの高い貨物・技術を法令等でリスト化して、そのリストに該当する貨物や技術を輸出や提供する場合には、経済産業大臣の許可を必要としている（リスト規制）。また、リスト規制に該当しない貨物や技術であっても、大量破壊兵器等や通常兵器の開発等に用いられるおそれがある場合は経済産業大臣の許可が必要となる（キャッチオール規制）。

規制対象となる貨物・技術は政省令で定められており、例えば貨物は輸出令・別表第１において武器、原子力、化学兵器、生物兵器、ミサイル、先端技術、材料加工、エレクトロニクス、電子計算機、通信、センサー等、航法装置、海洋関連、推進装置、その他、機微品目の 15 項に分けられている。規制対象の貨物・技術の詳細な機能や仕様は「貨物等省令」に規定されている。

対内直接投資審査制度では、外国投資家（非居住者である個人、外国の会社、これらの者から 50%以上出資を受けている本邦の会社等）が、国の安全等の観点から指定される事前届出の必要な業種を営む企業に対して、投資等を行う場合に外国投資家は財務大臣及び事業所管大臣あてに事前届出を行う必要がある。

「投資等」には上場会社の 1%以上の株式取得や、非上場会社の 1 株以上の株式取得、外国投資家やその関係者の取締役・監査役への就任、事業の譲渡や廃止に関する提案・同意などが含まれる。

事前届出の必要な業種としては以下のような業種が対象となる。事前届出の必要な業種のうち１つでも営んでいる場合は事前届出の対象であり、事業規模には関係がなく、子会社が以下の業種を営んでいる場合も事前届出の対象となる。

（対内直接投資審査制度に基づき事前届出の対象となる業種）

- 武器・航空機（無人航空機を含む）・宇宙開発・原子力関連の製造業、及び、これらの業種に係る修理業、ソフトウェア業
- 軍事転用可能な汎用品の製造業
- 感染症に対する医薬品に係る製造業、高度管理医療機器に係る製造業
- 重要鉱物資源に係る金属鉱業・製錬業等、特定離島港湾施設等の整備を行う建設業
- 肥料（塩化カリウム等）輸入業
- 永久磁石製造業・素材製造業
- 工作機械・産業用ロボット製造業等
- 半導体製造装置等の製造業
- 蓄電池製造業・素材製造業
- 船舶の部品（エンジン等）製造業
- 金属３D プリンター製造業・金属粉末の製造業
- サイバーセキュリティ関連業種（情報処理関連の機器・部品・ソフトウェア製造
- 業種、情報サービス関連業種）
- インフラ関連業種（電力業、ガス業、通信業、上水道、鉄道業、石油業、熱供
- 給業、放送業、旅客運送）
- その他（警備業、農林水産業、皮革製品製造業、航空運輸業、海運業）

・ 人的管理策

外為法では取引に関係する個人・法人の居住性を規定しており、財務省通達「外国為替法令の解釈及び運用について」を参照すると居住者・非居住者は以下のように判定される（表 4.1-2）。

表 4.1-2　外為法上の居住者の判定基準

	居住者	非居住者
日本人（個人）の場合	①我が国に居住する者 ②日本の在外公館に勤務する者	①外国にある事務所に勤務する目的で出国し外国に 滞在する者 ②２年以上外国に滞在する目的で出国し外国に滞在する者 ③出国後外国に２年以上滞在している者 ④上記①～③に掲げる者で、一時帰国し、その滞在 期間が６月未満の者
外国人（個人）の場合	①我が国にある事務所に勤務する者 ②我が国に入国後６月以上経過している者	①外国に居住する者 ②外国政府又は国際機関の公務を帯びる者 ③外交官又は領事官及びこれらの随員又は使用人（ただし、外国において任命又は雇用された者に限る。）
法人等の場合	①我が国にある日本法人等 ②外国の法人等の我が国にある支店、出張所その他の	①外国にある外国法人等 ②日本法人等の外国にある支店、出張所その他の事務所

	居住者	非居住者
	事務所 ③日本の在外公館	③我が国にある外国政府の公館及び国際機関
その他	—	合衆国軍隊等及び国際連合の軍隊等

■　　罰則

安全保障貿易管理制度では、必要な許可を取得しないで規制対象である貨物の輸出や技術の提供を行った場合など、法令の規定に違反した場合に、以下のような刑事罰、行政制裁や行政指導として警告がなされる他、経緯書・報告書を提出する必要がある。違反について自主的に経済産業省へ報告を行った場合には、処分等において考慮されることがある。

（安全保障貿易管理制度に基づく主な罰則）

■　刑事罰：

・　10 年以下の懲役

・　10 億円以下の罰金（法人の場合）

・　3 千万円以下の罰金（個人の場合）

■　行政制裁：

・　3 年以内の、貨物の輸出や技術の提供の禁止

・　別会社の担当役員等への就任禁止

c）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）第四版[58]

■　　策定機関・策定時期

経済産業省　2022 年（第四版）

■　　策定の背景・目的

安全保障に関連する機微技術の流出の懸念が拡大する中、大学や研究機関においても、国際的な人的交流や外国との共同研究等の国際化を一層進展するためにも、法律で遵守が義務づけられている輸出者等遵守基準を遵守する必要があることから、外為法に基づく技術の提供等の管理について、大学・研究機関が実施すべきことを取り纏め、法令遵守のための効果的な体制整備と機微な技術情報の管理水準の向上を促進する目的で経済産業省が策定したもの。

■　　適用範囲

大学・研究機関によって活用されることを想定している。

■　　情報の分類

本ガイダンスは外為法上の安全保障貿易管理制度に関係する内容であるため、保全の対象については外為法における武器並びに大量破壊兵器等及び通常兵器の開発等に用いられるおそれの高い貨物の輸出と技術の提供である。

[58] https://www.meti.go.jp/policy/anpo/law_document/tutatu/t07sonota/t07sonota_jishukanri03.pdf

■　情報管理策

・　組織的管理策

遵守基準に基づきリスト規制技術・貨物を扱う場合は、提供に関する文書、図面又は電磁的記録を適切な期間保存するよう努めなければならないとしている。

なお、リスト規制技術・貨物を扱っていない場合でも、少なくとも懸念が払拭されず審査票を起票し、取引実施の最終判断を経て行った技術提供に関しては、文書や電磁的記録を保存しておくと、万が一違反を疑われた際に法令に則って適切な対応をしていたことを示すため、役に立つとして保存を推奨している。

具体的な保存期間については、安全保障貿易管理を確実に行うことが重要と考えられる武器及び大量破壊兵器等関連（輸出令別表第１及び外為令別表の１の項から４の項中欄[59]）の貨物の輸出又は技術の提供に係るものについては少なくとも７年間、それ以外でも通常兵器関連等（輸出令別表第１及び外為令別表の５の項から１６の項中欄[59]）の貨物の輸出又は技術の提供に係るものについては少なくとも５年間と設定することが望ましいとしている。

・　人的管理策

留学生の受け入れや教育指導にあたって、みなし輸出として管理する対象となるもの、そうでないケースの類型を示している。

・　物理的管理策

大学・研究機関に推奨する情報セキュリティに関する事項において、パソコン等の盗難防止対策として、パソコンにワイヤーロックを付けるなどの盗難対策を行うことで、パソコン等の中にある技術情報も保護することができると推奨している。

・　技術的管理策

窃盗や不正アクセス等、予期せぬところで規制技術が流出してしまわないよう、普段からの情報管理を推奨している。大学・研究機関で既にＩＤ・パスワード管理や情報機器の取扱い等が規定された情報セキュリティに関する諸規程がある場合、それを準用し技術情報へのアクセス管理を行うこととしている。

また、情報セキュリティ規定の無い場合について、以下のような事項を参考として示している。

（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）第四版で示される情報セキュリティ規程が存在しない場合の管理策の例）

■　規制技術が入っているパソコン等の情報機器の管理

・　個人認証

・　パソコン管理、ＵＳＢメモリ等接続制限

・　パソコン等の盗難防止対策

[59] https://www.meti.go.jp/policy/anpo/matrix_intro.html

■　サーバ等の共用データベースの管理
・　アクセス管理
・　アクセスログ等の保存
・　外部からのアクセスの制限

■　技術情報の暗号化

■　組織的な対応（ハード面等での工夫）
・　シンクライアントシステムの利用
・　不正アクセスの防止対策
　　スパイウェア（マルウェア）対策
・　情報機器の廃棄の際の注意

■　　罰則
記載なし

d）研究データリポジトリ整備・運用ガイドライン[60]

■　　策定機関・策定時期
内閣府　国際的動向を踏まえたオープンサイエンスの推進に関する検討会　2019 年

■　　策定の背景・目的
研究環境の ICT 化により研究データの電子化が促進され、研究データを収集・蓄積して公開することにより各学問領域の研究活動の迅速化や学際的な研究活動の進展、データ科学による新たな研究領域の創成が期待されている国際的な潮流に対応するため、日本においても 2018 年６月に閣議決定された「統合イノベーション戦略」において、今日の「知の源泉」の鍵はデータ・情報であるとの認識の下、オープンサイエンスのためのデータ基盤の整備を行う方針を打ち出している。
本ガイドラインは、上記方針の具体的施策として 2019 年に内閣府における「国際的動向を踏まえたオープンサイエンスの推進に関する検討会」で策定された物であり、データリポジトリの整備・運用を行う国研及び大学等が国際的にも信頼され、研究データの保存・公開を適切に進めることができるよう、その整備・運用の指針を示すことを目的としている。

■　　適用範囲
データリポジトリの整備・運用を行う国研及び大学等を対象としている。

■　　情報の分類
本ガイドラインでいうデータリポジトリは電子的データの保存・共有等を行うための広い意味の情報基盤であり、計算機基盤（狭義の情報基盤）のみならず、運営体制及び人的基

[60] https://www8.cao.go.jp/cstp/tyousakai/kokusaiopen/guideline.pdf

盤を含む（ガイドライン２章より）。

ガイドラインの対象とするデータリポジトリとしては、国研・大学等により整備されるものであって、とくに公的資金により得られた研究データを再利用できる形で保存・管理し、当該機関内または機関外へのデータ利用サービスに供するものを対象としている。

■　情報管理策

本ガイドラインでは、データリポジトリの運用・整備について組織に求められる体制（組織的管理策）、運用・整備に従事する人材に求められる事項（人的管理策）、データリポジトリの備えるべき機能等（技術的管理策）を示しており、物理的管理策については規定されていない。

・　組織的管理策

データリポジトリは中長期的に安定して運営されることが求められることから、永続的な組織によって運営すること、人的・IT リソース、資金を十分に用意すること、運用スタッフが検収や能力開発を受けられることが必要としている。その他、データリポジトリの整備・運用に関する運営計画や基本的なデータポリシーを策定することの必要性について示している。

・　人的管理策

ガイドラインでは、データリポジトリの整備・運用に携わる人材に求められる業務や技能・経験のほか人材の配置・育成に関する指針を示している。データリモジトリの整備・運用における業務と必要な技能・経験については以下の通り（表 4.1-3）。

表 4.1-3　データリポジトリの整備・運用に携わる人材に必要な業務と技能・経験

業務	業務の内容	必要な技能・経験
管理的業務	リポジトリのミッションに則した企画・運営、ポリシーの作成、広報・コミュニケーション活動など	リポジトリ運営全般（経営、財務、法律、ポリシー、各種契約、データ受入審査、データライセンス、コンプライアンス等）の知識・経験、リポジトリに関するコンサルタントや広報の技能・経験
コンテンツ運用業務	データ・メタデータの受入・管理、データ提供やキュレーション（受入データの前処理、クリーニング、整形、管理）など	データキュレーション、データ品質管理、メタデータ管理、永続識別子の付与、データ公開やデータカタログへの登録、個人情報管理、データ・メタデータに関するコンサルタントの技能・経験に加えデータ提供者や利用者とのコミュニケーション力・経験
計算機システム運用業務	サーバやストレージなど、計算機基盤の構築や運用・保守や障害復旧、セキュリティ対策、設備の管理など	ハードウェア・ソフトウェア・ネットワーク管理や障害対応、セキュリティ対策に関する技能・経験

・　技術的管理策

データリポジトリがその目的を達成するために必要な機能として、提供されたデータの受入・保管、メタデータの管理・保管及びデータの変更を含むデータキュレーションを実施するとともに、その管理等を行うためのデータ管理システムや、保管するデータの破損や紛失に備えて、研究データのバックアップの取得・保管、及びデータのリストアを実施するためのデータバックアップシステム、保管するデータまたはそのメタデータに対してアクセス可能なデータ検索システムを備えておかなければならないとしている。

■　　罰則

記載なし

e）大学における秘密情報の保護ハンドブック [61]

■　　策定機関・策定時期

経済産業省　2016 年（全部改訂）

■　　策定の背景・目的

イノベーション創出を目的として、大学、高等専門学校、大学共同利用機関等の教育研究機関と企業の間の産学連携活動が盛んになったことにより、共同研究等を通じて企業から秘密として保持すべき情報が大学に持ち込まれるなど、大学が企業等の秘密情報を保有し、これを取り扱う可能性が従前よりも増大していることを背景に、大学における適切な秘密情報管理の参考となるよう経済産業省が策定したもの。

■　　適用範囲

大学によって使用されることを想定している。

■　　情報の分類

本ハンドブックは、大学においては既に公開された研究成果など秘密とする必要のない情報のある一方、試験問題や特許出願前（未公開）の研究成果等の秘密情報が多数存在しており、その保全を図るために秘密情報を区別して管理する方法について紹介している。その中で、秘密情報の分類の類型について3分類型、4分類型の例を示している(表 4.1-4)。

表 4.1-4　ハンドブックにおける秘密情報の分類例

3 分類型		4 分類型		情報の例
レベル 2	機密として保護すべきもの	レベル 3	漏えい等の事象が自学の業務等に深刻かつ重大な影響を及ぼすもの	機微情報、入試情報
		レベル 2	漏えい等の事象が自学の業務等に重大な影響を及ぼすもの	成績情報、進路情報

[61] https://www.meti.go.jp/policy/innovation_corp/himitsujoho/161012_himitsujoho.pdf

3 分類型		4 分類型		情報の例
レベル 1	機密としての保護は要しないが、その漏えい等の事象が自学の業務等に影響を及ぼすおそれがあるもの	レベル 1	漏えい等の事象が自学の業務等に軽微な影響を及ぼすもの	教職員出勤簿、出納記録
レベル 0	保護不要	レベル 0	保護不要	公開情報

■　　情報管理策

本ハンドブックでは、主に大学が秘密情報を把握・分類し、その管理をルール化する組織的対策と、一部で大学生の研究参加等に関する人的対策、情報漏洩対策の例として物理的な対策について示している。

・　組織的管理策

これまでに秘密情報を区別して管理するための規程等や体制を整備してこなかった大学を念頭に、自学が保有する情報から秘密情報を決定するまでのステップとして①大学が保有する情報（紙媒体、電子データ、ノウハウ等）の全体像の把握、②保有情報の評価、③評価の高低に基づく秘密情報の決定の 3 ステップを示している他、秘密情報の管理に係る学内体制の参考として、秘密情報管理委員会の設置等を挙げている。

・　人的管理策

大学の研究には学生等の参加を想定されることから、研究活動への学生等の参加の是非を検討するとともに、学生等を対象とした通則等での指示、秘密保持に関する誓約書の提出などを求めることを推奨している。

・　物理的管理策

分類に応じた情報漏洩対策の例として、施錠管理・入退室制限等といった区域制限等を行うことにより、アクセス権限を有しない者を対象情報に近づけない「接近の制御」や、秘密情報が記載された資料等の回収、学内のノートＰＣの固定、記録媒体の複製制限、教職員の私物ＵＳＢメモリ等の携帯メモリの持込み・利用を制限すること等によって、当該秘密情報を無断で複製・持ち出すことを阻止する「持ち出し困難化」、職場のレイアウトの工夫、資料・ファイルの通し番号管理、録画機能付き防犯カメラの設置、入退室の記録、ＰＣのログ確認等により、秘密情報に正当に又は不当に接触する者の行動が記録されたり、他人に目撃されたり、事後的に検知されたりしやすい環境を整える「視認性の確保」を挙げている。

■　　罰則

記載なし

（2）米国

1）基本情報

- 政治体制：大統領制
- 人口：約 3 億 5,000 万人(2023 年 10 月現在)[62]
- 名目 GDP：25 兆 4,627 億ドル(2022 年)、実質 GDP：20 兆 5,290 億ドル(2022 年)[63]
- 研究開発予算：1,720 億ドル（2022 年）[64]

■ 政治動向

2021 年からバイデン政権が継続をしているが、2023 年 5 月現在連邦上院では民主党が多数、連邦下院では共和党が多数を占めるねじれ議会となっている

バイデン政権は優先課題として米国の国際的地位の回復を掲げ、対中関係を 21 世紀最大の地政学的試練と位置づけ、国家安全保障戦略においても中国の台頭を警戒しており、その一環として、外交面では国家安全保障戦略で示したデュアルトラックアプローチに基づき、あらゆる国と共通の課題に取り組みつつ、民主主義の同盟、友好国とはさらなる協力関係を深める方針を採っている[65,66]。

■ 経済動向

新型コロナ等の影響を受けつつも、以前として GDP は世界 1 位である。しかし、近年は中国に追いつかれつつあり、危機感を抱いている。

台頭した中国に対抗するため、バイデン政権は、2021 年 11 月には米国内のインフラの現代化によるインフレ圧力の緩和、サプライチェーンの強化、雇用促進等を目的とした「IIJA（Infrastructure Investment and Jobs Act：インフラ投資雇用法)」、2022 年 8 月に、気候変動対策への投資を目的とする「IRA（Inflation Reduction Act：インフレ削減法)」と、半導体製造等を支援するための「CHIPS Plus ACT（CHIPS and Science Act：半導体科学法)」等を成立させ、国内投資促進やサプライチェーン強靭化へ重点を置く政策を展開するとともに、政権は同年 10 月に国家安全保障戦略を公表し、インド太平洋地域を始めとする民主的な同盟国やパートナーとの間で、技術、貿易、安全保障に関する連携を拡大することを強調した[67]。

■ 社会動向

人口は世界第 3 位の約 3 億 5000 万人[62]であり、多様な人種がいる多民族国家であるが、

---

62 https://www.mofa.go.jp/mofaj/area/usa/data.html

63 https://www.worldeconomics.com/GrossDomesticProduct/Real-GDP/United%20States.aspx#:~:text=Real%20GDP%20in%20United%20States,in%20Americas%2C%20ahead%20of%20Brazil.

64 https://www.aaas.org/news/some-facts-about-biden-rd-budget

65 https://www.jetro.go.jp/ext_images/world/n_america/us/biden_administration/administration202307_v2.pdf

66 https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

67 https://www.whitehouse.gov/build/guidebook/

黒人に対する暴行等に端を発したデモ運動(BLM 運動等)があるように、特定の人種に対する差別問題が存在している。

また、米国は銃社会であり、銃を比較的容易に入手することができることから、それに伴い、学校等で銃乱射により多数の死傷者出るような事件がたびたび発生している。バイデン政権において 28 年ぶりに銃規制法案が成立はしたが、その後も依然として同様の銃乱射事件が発生している[68],[69]。

■　技術動向

米国は世界トップの科学技術力を有してきたが、最近では中国等の国で科学技術に関する競争力が増してきており、米国の優位性が失われてきている状況である。

このような状況に対応するため、米国はトランプ政権の 2020 年に「重要・新興技術のための国家戦略」を策定、重要・新興技術を特定し、特定した分野における米国のリーダーシップを維持するための取り組み方針をまとめた。バイデン政権おいても科学技術政策の基本的な方向性はトランプ政権から変化していない。(なお特定した分野についてはバイデン政権の 2022 年に更新され、先進コンピューティング、人工知能、量子情報技術、半導体とマイクロエレクトロニクス、宇宙技術とシステム等の 19 分野となっている)

特に半導体分野においては、2022 年には「CHIPS Plus ACT」が制定され半導体技術の国内における製造開発に大規模な資金援助・投資を実施する一方で、中国やロシア等の国(懸念国と呼称)への投資等の制限を行うガードレール条項を設ける等の技術情報の国外流出防止に関する措置を行っている。

米国における研究開発は、まず大統領府内に、大統領に対して専門的助言を実施する APST (Assistant to the President for Science and Technology：科学技術担当大統領補佐官) や PCAST (President's Council of Advisors on Science and Technology：大統領科学技術諮問会議)、研究開発予算を含む予算案を作成する OMB(Office of Management and Budget：行政管理予算局) や連邦政府内での科学技術政策の推進・調整を行う OSTP (Office of Science and Technology Policy：科学技術政策局)等があり、その OSTP が事務局となる NSTC (National Science and Technology Council：国家科学技術会議)において、大統領府と各省庁の間の、科学技術政策に関する調整が行われる。これらの予算、政策等調整の下、各省庁は自らが所管する分野の研究開発や政策立案を省庁、機関およびその傘下の研究所で実施する (図 4.1-7)。[70],[71],[72]

---

[68] https://www.anzen.mofa.go.jp/od/ryojiMailDetail.html?keyCd=143180

[69] https://www.congress.gov/bill/117th-congress/senate-bill/2938?q=%7B%22search%22%3A%5B%22s2938%22%2C%22s2938%22%5D%7D&s=6&r=1

[70] https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

[71] https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

[72] https://www.jst.go.jp/crds/pdf/2021/FR/CRDS-FY2021-FR-02.pdf

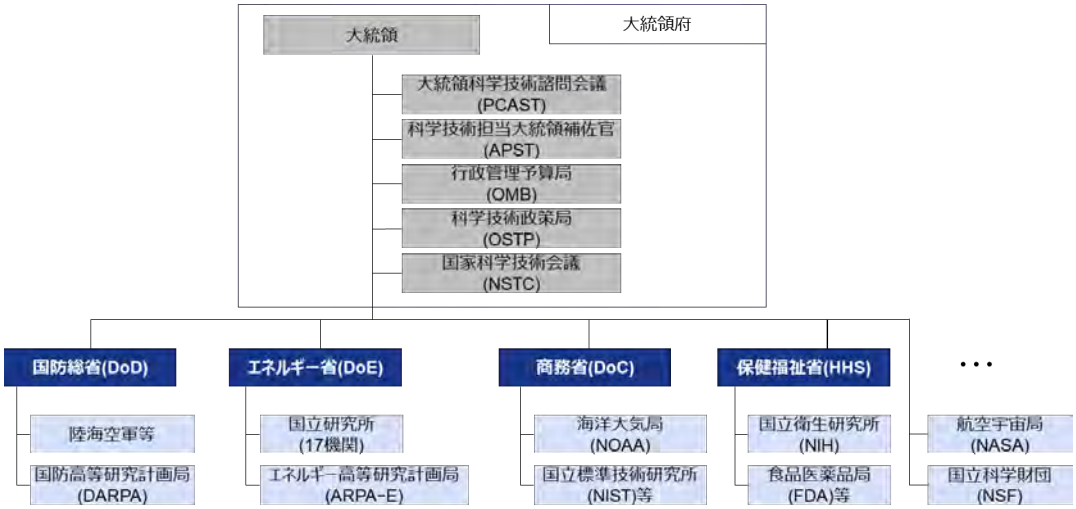


図 4.1-7 米国の研究開発に係る主な政府関連機関

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

米国では1940年に出された「E.O.8381（Executive Order 8381：大統領令8381号)」によって、それまで軍部が基本的に持っていた機密情報の取扱いを大統領が持つということとなった。機密情報の取り扱いに関する大統領令はその後、E.O.10104、10290、10501、12356、12958、13292と修正等が加えられ、現在は2009年に出された「E.O.13526」が米国の機密情報管理の根拠となっている。E.O.13526では、前のE.O.13292から、分類情報の管理、アクセス、取り扱いに関するガイドラインを更新し、これまで多さが問題視されてきた秘密指定に関して、機密として分類される情報の種類を明確にし、情報が公開されるタイミングの基準を設定した。

同令では、①軍事計画・兵器システムまたは軍の運用、②外国政府情報、③インテリジェンス活動・情報源・方法または暗号、④機密情報源を含む連邦政府の外交関係または対外活動、⑤国家安全保障に関連する科学的・技術的・経済的事項、⑥核物質または核施設の防護策のための政府プログラム、⑦国家安全保障に関連するシステム・設備・インフラ・プロジェクト・計画・防護サービスの脆弱性または能力、⑧大量破壊兵器の開発等の情報、を機密情報として定義し、情報の重要性に応じて3つのレベル(Top secret、Secret、Confidential)に分けている(表 4.1-5)[73]。

表 4.1-5 米国における情報の機密性レベルの定義

レベル	定義
Top Secret	その情報が不正に開示されることにより、国家安全保障に極めて重大な損害が生じることが合理的に予想され、かつ、当初の分類機関がそれを特定または説明できる場合に適用する。
Secret	その情報が不正に開示された場合、国家安全保障に重大な損害を与えることが合理的に予想される情報であって、元の分類機関が特定または説明できるものに適用される。
Confidential	その情報が不正に開示された場合、国家安全保障に損害を与えることが合理的に予想される情報であって、元の分類機関が特定または説明できるものに適用される。

機密情報を取り扱う民間企業については、機密情報を保護するための連邦政府と民間企業との間のパートナーシップであり、民間企業に対する機密文書の公開の必要性を審議し監督するために2002年の「E.O.12829」で「NISP（National Industrial Security Program：国家安全保障産業プログラム)」が定められた。そのNISPの具体的な運用マニュアルとして「32CFR(Code of Federal Regulations：連邦規則集) part117 NISPOM（National Industrial Security Program Operating Manual:国家安全保障産業プログラム運用マニュアル)」が制定された。この規定の中で、民間企業に対する機密情報の取扱い、保管方法、セキュリティ・クリアランス等に関する枠組みが規定されている[74]。

[73] https://www.archives.gov/isoo/policy-documents/cnsi-eo.html

[74] https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-pro

また、機密情報には該当しないが、安全保障に影響を及ぼす可能性があり、特定の管理基準や保護措置が必要な情報として、一般市民への情報公開が原則的に制限されるCUI(Controlled Unclassified Information：管理された非機密情報)という情報管理区分がある。この情報の分類についても当初は連邦政府各機関で独自の規則のもと管理されており、共有等の面で混乱が生じていた。この CUI という情報分類について、2010 年に発令されたE.O.13556で乱立していたCUIの分類に統一的な分類の枠組みが定められ[75]、また、これに基づいて具体的な管理方法等を「32CFR part2002 (Controlled Unclassified Information)」、CUI のシステム上での管理方法等を「NIST SP800-171」、「NIST SP800-172」、国防総省内全ての CUI の管理方法について「DoDI(DoD Instruction) 5200.48 (Controlled Unclassified Information)」等の法令等が規定された。

その他、増加するサイバーセキュリティの脅威に対して、業種、業態、事業規模等問わず、組織がサイバーセキュリティを管理し、強化するための手段等を定めたガイドラインとして、NIST が 2014 年に作成した「Framework for Improving Critical Infrastructure Cybersecurity(重要インフラのサイバーセキュリティを改善するためのフレームワーク)」がある他、成果物・知的財産については「35 U.S.C. (United States Code：連邦規則集) Chapter18 (バイ・ドール法)」や「FAR(Federal Acquisition Regulations：連邦調達規則) Part27 (特許、データ及び著作権)」、「DFARS(Defense Federal Acquisition Regulation Supplement：国防連邦調達規則補足)252.227.7038 (特許権-請負業者(大企業)による所有権)」等で請負業者の成果物・知的財産に関する所有権に関する規程等が定められている[76,77,78,79]。

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

米国では増大する中国の脅威に対抗するために、輸出管理や外資規制について 2018 年の「NDAA2019 (National Defense Authorization Act of 2019：国防権限法 2019)」によって大きく改正が行われた[80]。

まず輸出規制については、「ECRA(Export Control Reform Act：輸出管理改革法)」が制定され、2001 年に失効していた「EAA(Export Administrative Act：輸出管理法)」に代わって、米国の多義的技術用品の規制のための根拠として機能していた行政規則である「EAR (Export Administration Regulations：輸出管理規則)」に上位法である連邦法という、より確固とした根拠を与えた。ECRA では、新たに EAR に新興・基盤的技術としてバイオテクノロジーや量子等の 13 分野を指定し、禁輸対象国へのまたは禁輸対象国の国内における輸

gram-operating-manual-nispom

75 https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

76 https://www.nist.gov/cyberframework

77 https://www.acquisition.gov/far/part-27

78 https://www.law.cornell.edu/uscode/text/35/part-II/chapter-18

79 https://www.acquisition.gov/dfars/252.227-7038-patent-rights%E2%80%94ownership-contractor-large-business.

80 https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf

出、再輸出、または国内における移転に対して輸出許可受が義務付けられた[81]。

輸出管理については、他に武器関連品目・技術の取引について規定した「ITAR (International Traffic in Arms Regulations：国際武器取引規則)」がある[82]。

外資規制については、同じく国防権限法2019で「FIRRMA(Foreign Investment Risk Review Modernization Act：外国投資リスク審査近代化法)」が制定された。

同法では、従来のCFIUS (The Committee on Foreign Investments in the United States：対米外国投資委員会)で定められた審査対象である外国人による米国事業の支配（control）をもたらす合併、取得、買収に加えて、基本的には引き続き外国からの対米投資の歓迎方針を掲げつつも、重要技術の流出や重要インフラへの悪影響などの防止の観点からセンシティブな米国政府施設に近接する不動産取引や、重要技術を扱う米国事業の外国人による「支配」を伴わない投資を審査対象取引に加え、また一部の取引の際にはCFIUSへの事前届け出が義務付けられている。[83]

[81] https://www009.web.fc2.com/EAR_J/ECRA.pdf

[82] https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

[83] https://www.congress.gov/bill/115th-congress/house-bill/5841/text

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　国家戦略等

米国では2020年の「National Space Policy（国家宇宙政策）」で、責任ある建設的な宇宙利用の主導、強固な商業宇宙産業の促進、米国人の月への帰還と火星への準備、探査の主導、宇宙における米国と同盟国の利益の擁護に対する国家のコミットメント等、米国の宇宙活動全般の方向性を示している[84]。

宇宙領域の防衛分野においては2020年の「DEFENSE SPACE STRATEGY（防衛宇宙戦略）」において今後10年間で宇宙を望ましい状態にするための4つの努力目標（(1)宇宙における包括的な軍事的優位の構築、(2)宇宙を国家、合同、統合作戦に統合、(3)戦略的環境の形成、(4)同盟国、パートナー、産業界および他の米国政府省庁との協力）と、それを達成するための段階別アプローチが設定されている[85]。

外交分野においては2022年の「Strategic Framework for Space Diplomacy（宇宙外交の戦略的枠組み）」で、アルテミス協定や破壊的な対衛星ミサイル実験に反対するコミットメントを含め、相互に有益な宇宙活動に関する国際協力を拡大するための枠組みが定められた。同枠組みは大きく3つの柱（(1)宇宙のための外交、(2)外交のための宇宙、(3)宇宙外交に関する労働力の強化）から成り立っている[86]。

■　研究開発機関

米国における宇宙関連の研究開発を主導している主な政府機関として、NASA（National Aeronautics and Space Administration：航空宇宙局）および国防総省の傘下にあるDARPA（Defense Advanced Research Projects Agency：国防高等研究計画局）が挙げられる。

宇宙領域全般については、NASAが担当しており、NASAは国内20カ所にあるセンターと施設、そして宇宙にある唯一の国立研究所で、気候を含む地球、太陽、太陽系、そしてその先の世界を研究している。最近ではアルテミス計画と呼ばれるSLS（Space Launch System：宇宙発射システム）、オリオン宇宙船、ゲートウェイ月面基地を使用し、月面に最初の女性と次の男性を送り込むことを目標とした研究開発等を実施している[87]。

DARPAは、宇宙領域だけでなく、あらゆる領域の研究開発を行っている機関であり、通常では資金提供されないようなテーマ等を設定して、それに対して資金を提供し、将来的に軍で使用されることを目的としたハイリスクハイリターンの新技術の研究開発の支援を実施している[88]。

---

[84] https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf

[85] https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF

[86] https://www.state.gov/wp-content/uploads/2023/05/Space-Framework-Clean-2-May-2023-Final-Updated-Accessible-5.25.2023.pdf

[87] https://www.nasa.gov/

[88] https://www.darpa.mil/

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ NextSTEP-2(Next Space Technologies for Exploration Partnerships-2)

NASA が所管するプログラムであり、地球低軌道を超え、最終的には火星の表面に有人ミッションを送り込むという NASA の戦略的目標を追求するために ISS、キスルナー宇宙、火星で重要な能力を実証するためのコンセプトや技術の募集を目的としている。

同プログラムの公募要領には、プログラム参加にあたり遵守すべき情報保全に関する法令等として、細かい規定は確認できなかったが、いずれも NASA の内部規則等に準拠しているものと思われる、また輸出管理については以下のような法令等が記載されている[89]。

（NextSTEP-2 で遵守が必要な輸出管理関係の法令等）
- EAR
- ITAR

その他、具体的な規則ではないが、NASA は、NASA に研究提案書または研究プロジェクト計画書を提出する全ての研究者に対して、最終的な研究データを管理し、アクセスできるようにするための計画(データ管理計画(DMP))を含めるか、データを一般に公開できない、または公開する必要がない理由を述べることを義務付けている。

・ Ouija Technical・Area 2

DARPA が所管するプログラムであり、低軌道にある人口衛星のデータを活用して、宇宙の一部であるイオノスフィアと呼ばれる層において、軍事で使用されるような高周波無線がどのような動きをするのかについて理解し、予測することを目的としている。

同プログラムの公募要領には、プログラム参加にあたり遵守すべき情報保全に関する法令等として、いずれも宇宙特有のものは確認できないものの、以下のような法令等が記載されている[90,91]。

（Ouija Technical・Area 2 で遵守が必要な機密情報・CUI 関連の法令等）
- 機密情報関連
  - DoDM 5200.01（DoD 情報セキュリティプログラム）（第 1 巻～第 4 巻）
  - DoD 5220.22-M（国家産業安全保障プログラム）
  - DoD 5200.22-M Sup.1（国家産業安全保障プログラム）
- CUI 関連
  - 32CFR part 2002（管理された非機密情報(CUI)）
  - DoDI 5200.48（管理された非機密情報(CUI)）
  - NIST SP800-171
  - DoDI 8582.01

89 https://www3.nasa.gov/sites/default/files/atoms/files/nextstep-2_omnibus_baa_amendment_22_2022-12-06.pdf

90 https://www.darpa.mil/program/ouija

91 https://sam.gov/opp/bb6c10279c794a07b1d0696e5e2ec6bd/view

- DARPA CUI Guide

・ その他
- DFARS 252.204-7000（情報の開示）
- DFARS 252.204-7008（対象となる防衛情報の保護管理への準拠）
- DFARS 252.204-7012（対象となる防衛情報の保護とサイバーインシデントの報告）

b）海洋領域

■ 国家戦略等

米国では2004年の「NSPD-41 (NATIONAL SECURITY PRESIDENTIAL DIRECTIVE-41：国家安全保障大統領令41号)」により、米国の海洋権益保護を通じて、米国の国家安全保障と国土安全保障を強化するための米国の政策、指針、実施行動が定められ、それをもとに8つの計画(①海洋領域認識達成のための国家計画、②グローバル海洋情報統合計画、③海上作戦脅威対応計画、④国際的な支援と調整戦略、⑤海上インフラ復旧計画、⑥海上輸送システムセキュリティ計画、⑦海上貿易の安全保障計画、⑧国内支援計画)から成る「National Strategy for Maritime Security (海洋安全保障国家戦略)」が策定された[92],[93]。

防衛分野においては、2020年に「NAVAL RESEARCH&DEVELOPMENT FRAMEWORK (海軍研究開発フレームワーク)」が定められており、海洋領域において決定的な能力をいち早く実用化することを目標に、海軍技術の「発見から配備」までの連続的な会話と努力の指針となるフレームワークの3つの構成要素 (Align、Allocate、Accelerate) とともに、取り組むべき重要な問題を提示している[94]。

■ 研究開発機関

国における海洋関連の研究開発を主導している主な政府機関として、商務省の傘下であるNOAA (National Oceanic and Atmospheric Administration：海洋大気庁)および国防総省の傘下にあるDARPAが挙げられる。

NOAAは、天気の予報の他、研究開発では気候変動、海洋、大気等幅広く行っており、海洋領域については、海洋学、海洋生態系、海洋資源管理等、海洋領域の全般に関する研究開発を担当している[95]。

DARPAは海洋領域だけでなく、あらゆる領域の研究開発を行っている機関であり、通常では資金提供されないようなテーマ等を設定して、それに対して資金を提供し、将来的に軍で使用されることを目的としたハイリスクハイリターンの新技術の研究開発の支援を実施している。

92 https://irp.fas.org/offdocs/nspd/nspd41.pdf

93 https://www.dhs.gov/national-plan-achieve-maritime-domain-awareness

94 https://media.defense.gov/2020/May/18/2002302044/-1/-1/1/NRE-ADDENDUM-TO-THE-R-AND-D-FRAMEWORK_070617.PDF

95 https://www.noaa.gov/

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Ocean of Things

DARPA が所管するプログラムであり、分散型センサーネットワークとして漂流する、低コストで環境に優しいインテリジェント・フロート数千台を配備することで、広い海域での持続的な海上状況認識を可能にすることを目的としている。

同プログラムの公募要領には、プログラム参加にあたり遵守すべき情報保全に関する法令等として、いずれも海洋特有のものは確認できないものの、以下のような法令等が記載されている[96,97,98]。

(Ocean of Thing で遵守が必要な法令等)
・ DFARS 252.204-7000（情報の開示）
・ DFARS 252.204-7008（対象となる防衛情報の保護管理への準拠）
・ DFARS 252.204-7012（対象となる防衛情報の保護とサイバーインシデントの報告）
・ NIST SP 800-171

c）バイオ領域

■　国家戦略等

米国では、外国に過度に依存していたバイオ関連産業の国内回帰を図るため、2022 年に持続可能な安全でセキュアな米国のバイオエコノミーのために進化するバイオ技術・製造に関する大統領令が発せられた。同大統領令では、外国に過度に依存しているとされるバイオテクノロジー関連産業の国内回帰を促し、国内サプライチェーンの強化などを目的としており、具体的な取り組みとして①国内バイオ製造能力の拡大、②バイオ製品の市場機会拡大、③研究開発の推進、④専門人材育成、⑤バイオ産業製品に対する規制合理化等が掲げられた[99]。

また、2023 年にはそれを基にバイオテクノロジーとバイオ製造を推進するための新たな目標が設定された。これは国のバイオテクノロジーおよびバイオ製造を推進するため、政府内外の行動を喚起する３つの新たな目標(①社会的目標達成に向けたバイオテクノロジー・バイオ製造の研究開発の活用、②国防総省のバイオ製造における優先順位の確立、③国のバイオエコノミーの経済価値の評価)を設定したものである[100]。

防衛分野においては 2022 年に「National Biodefense Strategy and Imple-mentation Plan（国家バイオディフェンス戦略と実施計画)」が策定された。同計画は、生物学的脅威から米国民とその世界的利益を守るために、米国政府全体で実施されるあらゆる活動を組

96 https://oceanofthings.darpa.mil/

97 https://www.darpa.mil/attachments/HR001120S0020.pdf

98 https://www.darpa.mil/attachments/HR001120S0042.pdf

99 https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/12/executive-order-on-advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american-bioeconomy/

100 https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf

織化するための、単一の調整された取り組みをまとめたものであり、①リスク認識と検知を可能にし、生物防衛事業全体の意思決定に反映、②バイオインシデントを防止のためのバイオディフェンス企業の能力を確保、③バイオインシデントの影響を軽減するためのバイオディフェンス事業準備態勢の確保、④バイオ事故の影響を抑えるための迅速な対応、⑤バイオインシデント後の地域社会、経済、環境の回復促進の５つの目標が設定されている[101]。

バイオ領域については、2004 年に米国国立科学アカデミーによって発行されたバイオテクノロジーと生物兵器の潜在的な脅威に関する重要な報告書である「Biotechnology Research in an Age of Terrorism(テロリズムの時代における生命工学研究(通称 Fink Report))」において、生物科学の進歩が公衆衛生、農業、医療などで多大な利益をもたらす一方で、生物兵器としての悪用の可能性も高めると警告している等、その多義的技術への利用について、潜在的なリスクがあることから慎重な姿勢を採るべきであるとの提言もされている。

■　研究開発機関

国におけるバイオ関連の研究開発を主導している主な政府機関として、保健福祉省の傘下である NIH（National Institutes of Health：国立衛生研究所）および国防総省の傘下にある DARPA が挙げられる。

NIH は、医学研究の推進、健康の向上、疾病の予防と治療方法の発見等、医療・バイオ全般の研究開発を担当している。

DARPA はバイオ領域だけでなく、あらゆる領域の研究開発を行っている機関であり、通常では資金提供されないようなテーマ等を設定して、それに対して資金を提供し、将来的に軍で使用されることを目的としたハイリスクハイリターンの新技術の研究開発の支援を実施している[102]。

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ FSHARP（Fieldable Solutions for Hemorrhage with bio-Artificial Resuscitation Products）

DARPA が所管するプログラムであり、負傷した戦闘員を維持するための出血対策として、展開可能で常温保存可能な普遍的な全血代替品を開発するとしている、

同プログラムの公募要領には、プログラム参加にあたり遵守すべき情報保全に関する法令等として、いずれもバイオ特有のものは確認できないものの、以下のような法令等が記載されている[103]。

（FSHARP で遵守が必要な法令等）
・ CUI 関係
  ➢ 32CFR part 2002（管理された非機密情報(CUI)）

[101] https://www.whitehouse.gov/ostp/news-updates/2023/03/22/fact-sheet-biden-harris-administration-announces-new-bold-goals-and-priorities-to-advance-american-biotechnology-and-biomanufacturing/

[102] https://www.nih.gov/

[103] https://sam.gov/opp/36db79ac97b0496399f472d5f2d5dd5a/view

- DoDI 5200.48（管理された非機密情報(CUI)）
- NIST SP800-171
- DoDI 8582.01
- DARPA CUI Guide

・ その他

- DFARS 252.204-7000（情報の開示）
- DFARS 252.204-7008（対象となる防衛情報の保護管理への準拠）
- DFARS 252.204-7012（対象となる防衛情報の保護とサイバーインシデントの報告）

d）サイバー領域

■ 国家戦略等

米国は、サイバー領域において、量子情報科学研究開発に関する中国やEU等の各国の動向を受け、量子情報科学分野において米国の持続的なリーダーシップを確実にすることを目的に2018年に、「NATIONAL QUANTUM INITIATIVE ACT（国家量子イニシアティブ法)」を制定している。同法では米国の持続的なリーダーシップを確実にするため、①人材パイプラインの構築、②連邦政府における計画策定の改善、省庁間の連携強化、③連邦政府による研究開発や実証の効果の最大化、④連邦政府、国立研究機関、産業界、大学の連携推進、⑤国際標準の開発の推進の5つの行動を挙げている[104]。

2023年に脅威を増し続けているサイバー攻撃から、国家の安全保障、公共の安全、経済的繁栄を守るための戦略として「NATIONAL CYBER SECURITY STRATEGY（国家サイバー安全保障戦略)」が定められた。同戦略ではサイバー攻撃に対抗するための5つの柱として①重要インフラの防衛、②脅威ある行動者への対抗、③安全と強靭性を促進させるための市場形成④強靭な未来への投資、⑤共通する目標を追求する国際パートナーシップの構築が掲げられている[105]。

また、2023年、国家安全保障戦略や「NATIONAL CYBER SECURITY STRATEGYを踏まえてDepartment of Defense Cyber Strategy（国防総省サイバー戦略)」が作成された。同戦略では、国防総省のサイバー防衛と作戦に対する取組みについて説明し、省庁間パートナーとの協力による脅威からの防衛、国防総省ネットワーク内のサイバーセキュリティの確立等の重要性が挙げられている[106]。

■ 研究開発機関

米国におけるサイバー関連の研究開発を主導している主な政府機関として、商務省の傘下であるNIST（National Institute of Standards and Technology：国立標準技術研究所)および国防総省の傘下にあるDARPAが挙げられる。

NISTは、科学技術分野における計測、標準に関する研究を実施しており、サイバー領域

104 https://www.congress.gov/bill/115th-congress/house-bill/6227/text

105 https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

106 https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

については、多くの場所でサイバー攻撃対処のための指標となっている「Framework for Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティを改善するためのフレームワーク)」の策定をしている[107]。
DARPA はサイバー領域だけでなく、あらゆる領域の研究開発を行っている機関であり、通常では資金提供されないようなテーマ等を設定して、それに対して資金を提供し、将来的に軍で使用されることを目的としたハイリスクハイリターンの新技術の研究開発の支援を実施している。

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Cyber-Hunting at Scale

DARPA が所管するプログラムであり、新しい攻撃ベクトルを検出して特徴付け、適切なコンテキストデータを収集し、企業内および企業間で保護対策を広めるための自動化ツールを開発するとしている。

同プログラムについては、提案書提出時に、TA1、TA2、TA4 のすべての提案者は、最高機密（Top Secret）のクリアランスを有し、SCI（Sensitive Compartmented Information ：機密区画情報）へのアクセス資格を有するチームメンバーを少なくとも 1 名擁していなければならない等の規定があり、プログラム参加にあたり遵守すべき情報保全に関する法令等として、いずれもサイバー特有のものは確認できないものの、以下のような法令等が記載されている[108]。

（Cyber-Hunting at Scale で遵守が必要な法令等）
- 機密情報関係
  - DoDM 5200.01 Sup.1（DoD 情報セキュリティプログラム）（第 1 巻～第 4 巻）
  - DoD 5220.22-M（国家産業安全保障プログラム）
- CUI 関係
  - NIST SP800-171
- その他
  - DFARS 252.204-7000（情報の開示）
  - DFARS 252.204-7008（対象となる防衛情報の保護管理への準拠）
  - DFARS 252.204-7012（対象となる防衛情報の保護とサイバーインシデントの報告）

e）多義的技術

■　国家戦略等

米国では、それまでは軍事分野で行われた研究開発の成果を民生分野へと移行するスピンオフが主流であったが、1950 年代末に民生分野で集積回路が発明されて以降、多義的技術の研究開発についてはスピンオンが主流となった。政府としては、発展する民生技術を軍需へ技術移転させる政策の作成が急務となり、連邦政府によって得られた技術を、州・地方政府および民間セクタへ移転することを促進するため、1980 年スティーブンソン・ワイド

107 https://www.nist.gov/

108 http://www.fbodaily.com/archive/2017/06-June/02-Jun-2017/FBO-04527128.htm.

ラー技術革新法等の技術移転を促進する政策が打ち出された。また、また 1980 年には軍需企業と民生半導体企業とのペアで研究開発を行なわせることで、軍の求めるハイテク兵器へ民生技術を組み入れることを目的とした VHSIC（Very High Speed Integrated Circuit：超高速集積回路）開発計画が実施された。

DARPA においては、2004 年から DARPA チャレンジと呼ばれる懸賞金によるイベント形式での研究支援プログラムを開始、大学や民間企業に特定の目標を短時間でクリアするためのアイデアを競わせ、低コストで多義的技術等の特定の課題に対するアイデアを発掘するという手法が採られている[109]。

2010 年代から民間の AI・量子技術といった新興技術の急速な発展や、米中の技術覇権争い、2014 年に提唱されたサードオフセット戦略による先端技術における民生技術の比重増大等の背景もあり、多義的技術開発については DARPA 等の政府機関の他に UARC（University Affiliated Research Center：大学付属研究センター）や FFRDC（Federally Funded Research and Development Centers：連邦政府出資研究開発センター）といった大学、民間企業が運営する機関において多く実施されている他、法令についても 2018 年に国家量子イニシアティブ法、2022 年に CHIPS Plus ACT 等、多義的技術に係る研究開発に対して積極的に資金援助を行う等の動きが見られる。

■　研究開発機関

米国における多義的技術の研究開発は国防総省を中心として実施されており、あらゆる領域の研究開発で通常では資金提供されないようなテーマ等を設定して、それに対して資金を提供し、将来的に軍で使用されることを目的としたハイリスクハイリターンの新技術の研究開発の支援を実施している DARPA、政府やその他の民間機関では効果的に満たすことができない研究開発ニーズを充足するため設立され、連邦政府機関のスポンサーから資金提供を受ける独立した非営利組織である FFRDC や国防総省と大学法人が提携する非営利組織であり、軍事・防衛に関する長期的ニーズを踏まえた専門分野（コア・コンピテンシー）について研究開発を行うため、大学内に設置される UARC 等が挙げられる。（図 4.1-8）[110,111]

[109] https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles

[110] https://www.nsf.gov/statistics/ffrdclist/

[111] https://defenseinnovationmarketplace.dtic.mil/ffrdcs-uarcs/

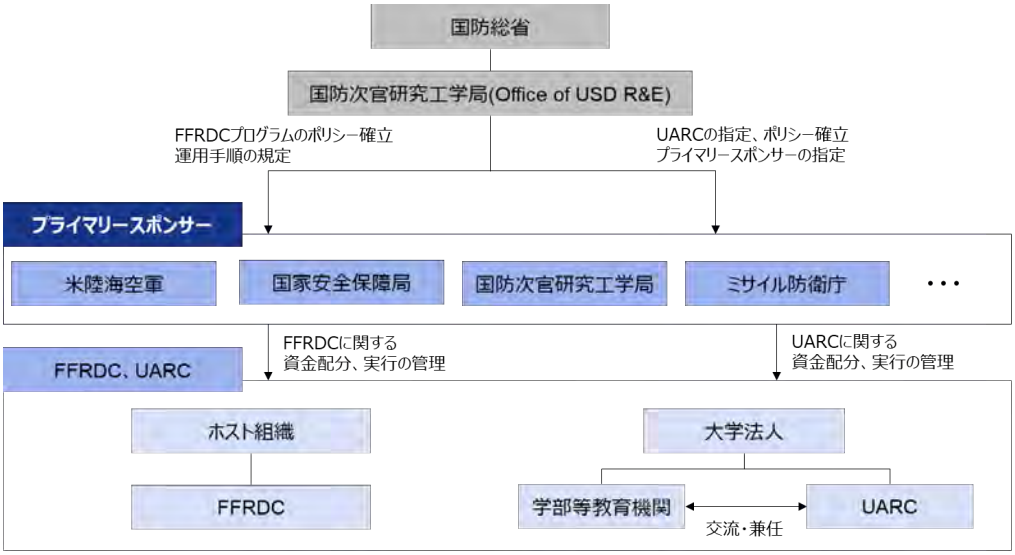


図 4.1-8　FFRDC、UARC の推進体制

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　DARPA のプログラム

多義的技術に関する研究開発プロジェクトは主に DARPA のような組織で実施されている。DARPA では各領域で記載をしたプログラムをはじめ、多くの多義的技術に関するプログラムを実施している。

DARPA による多義的技術に関するプログラムで共通して遵守が求められる法令等として共通するものには以下のようなものがある。

（DARPA の主なプログラムで遵守が必要な法令等）

・　プログラム内容に機密に関連するものがある場合
  - E.O.13526
  - DoDM 5200.01（DoD 情報セキュリティプログラム）（第 1 巻～第 4 巻）
  - DoD 5220.22-M（国家産業安全保障プログラム）
  - DoD 5220.22-M Sup.1（国家産業安全保障プログラム）

・　プログラム内容に CUI に関連するものがある場合
  - E.O.13556
  - 32CFR part 2002（管理された非機密情報(CUI)）
  - DoDI 5200.48（管理された非機密情報(CUI)）
  - NIST SP800-171
  - DoDI 8582.01
  - DARPA CUI Guide

・　その他
  - DFARS 252.204-7000（情報の開示）
  - DFARS 252.204-7008（対象となる防衛情報の保護管理への準拠）
  - DFARS 252.204-7012（対象となる防衛情報の保護とサイバーインシデントの報告）

・ DoD SBIR

SBIR(Small Business Innovation Research)は、米国国内で研究開発を行う中小企業を対象とした中小企業の研究開発の事業化を目的とした資金支援プログラムであり、中小企業技術革新法(Small Business Innovation Development Act)を根拠に、1982 年から実施している。

プログラムについては、全体を中小企業庁(Small Business Administration:SBA)が管轄しいるが、各プログラムについては連邦機関の各省庁が実施する。

DoD の SBIR プログラムについても DoD に属する各機関(米軍、DARPA 等)で実施されており、契約要件として情報保全に関連する以下のような法令等の準拠が求められている[112]。

(DoD SBIR で遵守が必要な法令等)
・ DFARS 252.204-7000 (情報の開示)
・ DFARS225.7901-4 (輸出管理契約条項)
・ DFARS252.225-7048 (輸出管理品目)
・ DFARS 252.204-7008 (対象となる防衛情報の保護管理への準拠)
・ DFARS 252.204-7012 (対象となる防衛情報の保護とサイバーインシデントの報告)
・ NIST SP800-171

[112] https://www.defensesbirsttr.mil/

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして47件リストアップした（詳細はAppendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、および国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも1つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして4件抽出した。（表 4.1-6）

表 4.1-6　詳細調査を行う法令等のショートリスト

法令等の名称	理由
E.O.13526 32CFR part117(NISPOM)	国家機密情報の保護の根拠となる大統領令であり、これに基づいて規定された機密情報に関してどのように保護するのかについて32CFR part117(NISPOM)のような規則で規定されており、多くの情報を得られるため。
E.O.13556 32CFR part2002 NIST SP800-171	CUIの管理の根拠となる大統領令であり、これに基づいて32CFR part2002(CUI)やNIST SP800-171等の規則も規定されており、多くの情報を得られるため。
ECRA EAR	米国の安全保障貿易の根本となる法令であり、これに基づいて輸出管理規則(EAR)についても定められているため。
FIRRMA	安全保障貿易に関連する外国投資の規制についての法令であるため。

以下に表 4.1-6に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）E.O.13526／32CFR part117(NISPOM)[113],[114]

■　策定機関・策定時期

E.O.13526（2009年）/32CFR part117(NISPOM)（2021年）

■　策定の背景・目的

これまで米国では、秘密情報の分類が明確でなく、過剰な機密指定により、多くの情報が機密情報として指定され、様々な情報が機密指定のまま公開されないことが問題視されており、その制度を改善する必要があった。

E.O.13526の目的は、安全保障に不可欠な情報を保護し、機密基準の正確かつ責任ある適用と日常的、安全かつ効果的な機密解除を通じて開かれた政府へのコミットメントを示す

[113] https://www.archives.gov/isoo/policy-documents/cnsi-eo.html

[114] https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117

ことである。

E.O.13526 で定められた機密情報に関して、民間企業の具体的な管理方法等については 32CFR part117 の中で具体的に規定している。

■ 適用範囲

E.O.13526、32CFR part117 で、機密情報について以下のように定義されている。

(E.O.13526、32CFR part117 における機密情報に関する記述)

■ E.O.13526

・ 情報は以下の条件が満たされている場合にのみ機密情報として分類することができる
  - ➢ 当初の分類機関がその情報を分類していること
  - ➢ その情報が合衆国政府によって所有され、合衆国政府のために作成され、または合衆国政府の管理下にあること
  - ➢ その情報が、この命令の第 1.4 節に列挙されている情報のカテゴリーの 1 つ以上に該当すること
  - ➢ 当該情報が不正に開示されることにより、国家安全保障(国際テロリズムに対する防衛を含む)に損害が及ぶことが合理的に予想され、かつ、当該損害について特定または説明することができると、当初の分類機関が判断する場合

・ 第 1.4 節に挙げられている情報のカテゴリーについては以下の８つ
  - ① 軍事計画・兵器システムまたは軍の運用
  - ② 外国政府情報
  - ③ インテリジェンス活動・情報源・方法または暗号
  - ④ 機密情報源を含む連邦政府の外交関係または対外活動
  - ⑤ 国家安全保障に関連する科学的・技術的・経済的事項
  - ⑥ 核物質または核施設の防護策のための政府プログラム
  - ⑦ 国家安全保障に関連するシステム・設備・インフラ・プロジェクト・計画・防護サービスの脆弱性または能力
  - ⑧ 大量破壊兵器の開発等の情報

■ 32CFR part117

・ E.O.13526、またはその前任もしくは後任の命令、および改正原子力法に従い、国家安全保障のために不正な開示から保護する必要があると決定され、そのように指定された情報をいう。

■ 情報の分類

E.O.13526 では機密情報に該当する情報を、それらが不正に開示された場合に予想される損害等の影響度に応じて、Top Secret、Secret、Confidential の 3 つのレベルに分類している(表 4.1-7)

表 4.1-7 米国における情報の機密性レベルの定義

レベル	定義
Top Secret	その情報が不正に開示されることにより、国家安全保障に極めて重大な

レベル	定義
	損害が生じることが合理的に予想され、かつ、当初の分類機関がそれを特定または説明できる場合に適用する。
Secret	その情報が不正に開示された場合、国家安全保障に重大な損害を与えることが合理的に予想される情報であって、元の分類機関が特定または説明できるものに適用される。
Confidential	その情報が不正に開示された場合、国家安全保障に損害を与えることが合理的に予想される情報であって、元の分類機関が特定または説明できるものに適用される。

■　情報管理策

32CFR part117 において、E.O.13526 で示される情報の機密性レベルごとに請負事業者に対して組織的管理策が示されている。

・　組織的管理策

情報分類	請負業者に求めていること
共通	・　機密扱いを受けたすべての職員が、機密情報を安全でない電話や安全が確保されていない電話、公共の交通機関や場所、その他無許可の人物による傍受を許容するような方法で機密情報を話し合うことの禁止を、すべての許可された職員に周知せること ・　緊急事態における機密文書の保護手順を策定すること ・　機密情報および資料を送受信するための手順を確立すること ・　機密情報が許可された者にのみ開示されるプロセスを確立すること ・　保有する機密情報が、現在の契約を支援するものであること、または契約期間終了後も保持する権限が与えられていることを確認するため、定期的に保有する機密情報を見直す手順を確立する
Top Secret	・　Top Secret にアクセスし、説明責任の記録を保持するコントロール担当者を指定すること ・　Top Secret の年次棚卸しを行うこと ・　２人の承認された人物による Top Secret の廃棄手順を確立すること ・　契約者が分類された材料のコピーを 2 年以上保持したい場合、原則として、特定の文書リストで識別すること
Secret	・　契約者が分類された材料のコピーを 2 年以上保持したい場合、一般的な件名と文書のおおよその数で識別すること
Confidential	Secret と同じ

・　人的管理策

32CFR part117 において、E.O.13526 で示される情報の機密性レベルごとに請負事業者に対して人的管理策が示されている。

情報分類	請負業者に求めていること
共通	・ 契約上の機密分類仕様書または同等の文書に記載された処分指示に基づき、保有する機密資料を破棄すること
Top Secret	・ Top Secret を請負業者の所在地の外に送信するには、政府から書面による許可を得ること ・ 外国政府の Top Secret または同等の情報の複製には、発信元の政府の書面による承認を得ること ・ Top Secret の各項目にシリーズ番号を付けること。メディア形式に関わらず、すべての Top Secret および関連する取引文書にコピー番号を付けること ・ Top Secret の破棄に立ち会い、破棄証明書を作成し、その破棄証明書を 2 年間保持すること
Secret	・ アメリカ合衆国およびその領土域内に転送する場合には、GSA（米国一般調達局）との契約者である商業配送業者を通じて行うこと ・ Secret が手持ち搬送できる分類資料の最高レベルであり、その資料は大きさと重さが、搬送者が常時その資料を所持し続けることができる程度であること
Confidential	Secret と同じ

・ 物理的管理策

32CFR part117 において、E.O.13526 で示される情報の機密性レベルごとに請負事業者に対して物理的管理策が示されている。

情報分類	請負業者に求めていること
共通	・ 施設に出入りする者は、機密文書にアクセスする可能性が低い場合を除き、その身辺を検査される可能性があることを、該当するすべての出入り口に目立つように掲示すること
Top Secret	・ 機密情報および資料を、GSA 公認のセキュリティ・コンテナ、連邦規格 832 に準拠した保管庫、または 32CFR 2001.53 に従って建設されたオープンストレージエリアに保管すること。さらに、以下の追加のコントロールが必要。 i） GSA 公認のコンテナの場合、以下のいずれかの追加措置が必要： A） シークレットレベル以上でクリアランスを持つ従業員が 2 時間ごとにコンテナの検査を行うこと B） 侵入検知システム（IDS）を設置し、警報が発生してから 15 分以内に対応する担当者が到着すること C） コンテナが連邦仕様 FF-L-2740 に準拠するロックを装備している場合、コンテナが位置するエリアのセキュリティ・イン・デプスで保護すること

情報分類	請負業者に求めていること
	ii) セキュリティ・イン・デプスでカバーされるオープンストレージエリアの場合、侵入検知システム（IDS）を設置し、警報が発生してから 15 分以内に対応する担当者が到着すること iii) セキュリティ・イン・デプスでカバーされないオープンストレージエリアの場合、警報が発生してから 5 分以内に対応する担当者が到着すること。
Secret	・ Top Secret と同様の方法で保管するか、または 2012 年 10 月 1 日までは、GSA 認可外のコンテナで保管することができる。これには、組み合わせ錠がついた非 GSA 認可のコンテナ、または剛性金属製のロックバーと機関長が承認した南京錠で固定された非 GSA 認可のコンテナが含まれる。GSA 認可外のコンテナまたはオープンストレージエリアが位置するエリアでは、セキュリティ・イン・デプスが必要。GSA 認可のコンテナや連邦基準 832 に準拠した金庫での保管を除き、以下のいずれかの追加コントロールが必要： i) シークレットレベル以上でクリアランスを持つ従業員によるコンテナまたはオープンストレージエリアの 4 時間ごとの検査 ii) 侵入検知システム（IDS）を設置し、警報が発生してから 30 分以内に対応する担当者が到着すること。
Confidential	Secret と同じ

・ 技術的管理策

32CFR part117 において、E.O.13526 で示される情報の機密性レベルごとに請負事業者に対して技術的管理策が示されている。

情報分類	請負業者に求めていること
共通	・ 各業務日の終了時に、すべての機密資料とセキュリティ保管庫が保管されたことを確認するために、セキュリティチェックのシステムを確立すること ・ 機密取扱品の保管を許可された請負業者は、その施設からの機密取扱品の無許可の持込みまたは持ち出しを阻止し、発見するためのシステムを確立し、維持すること。技術的手段（侵入検知システムなど）により合理的に防止できる場合は、それ以上の管理は必要ない。
Top Secret	・ 契約者の場所内外での Top Secret の転送用の連続受領システムの確立すること
Secret	―
Confidential	―

■　罰則

「18 U.S.C.§793、794、798」で以下情報の漏えいに関連した以下のような行為に対して罰則が定められている。

（18 U.S.C.§793 で規定される主な罰則）[115]

・　以下のような行為をした場合、罰則として、罰金、10 年以下の懲役、またはその両方が科される。
  - 国防に関連する場所や情報への不正アクセス、取得、または提供を意図した行為
  - 国防に関連する資料の不正な複製、撮影、作成、取得
  - 国防に関連する資料を不正に受領、保持する行為
  - 国防に不利な方法で国防に関連する資料を他者に伝達する行為
  - 無許可で国防に関連する資料を保持、アクセス、管理する行為
  - 国防に関連する資料の適切な保管場所からの不正な持ち出し、紛失、盗難、破壊を報告しない行為

（18 U.S.C.§794 で規定される主な罰則）[116]

・　戦時中という状況下において、以下のような行為をした場合、罰則として死刑もしくは終身刑に処せられる。
  - 外国政府等に国防に関連する情報を伝達しようとする行為
  - 戦時における敵への情報提供を意図した行為

（18 U.S.C.§798 で規定される主な罰則）[117]

・　以下のような行為をした場合、罰則として、罰金、10 年以下の懲役、またはその両方が科される
  - 米国の安全または利益に対する損害、または外国の利益のために機密情報を不正に伝達、公開、利用する行為
  - 米国または外国政府の暗号、通信諜報に関連する情報の不正な取り扱い

b）E.O.13556／32CFR part2002／NIST SP800-171[118, 119, 120]

■　策定機関・策定時期

E.O.13556(2010 年)／32CFR part2002(2016 年)／NIST SP800-171(NIST　2015 年)

■　策定の背景・目的

115 https://www.law.cornell.edu/uscode/text/18/793

116 https://www.law.cornell.edu/uscode/text/18/794

117 https://www.law.cornell.edu/uscode/text/18/798

118 https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

119 https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002

120 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

制定以前、米国では機密情報ではないが、公開等に制限のある情報ということで、連邦政府機関で管理のための独自の分類規則が制定されて各機関での連携や管理等に混乱が生じていいた。

E.O.13556 は、これらの情報の分類について統一的な枠組みを定めることを目的として制定されたものであり、その情報指定、取扱、管理解除当に関する方針を定めたものとして 32CFR part2002、システムにおける CUI の規定について NIST SP800-171 で定められている。

■　適用範囲

E.O.13556 では CUI の明確な定義については確認できないが、本大統領令の目的の中で管理するための対象情報としては、以下のような記載がある

（E.O.13556 の目的）
本命令は、法律、規則、および政府全体のポリシーに従って保護または拡散を制御する必要のある情報を管理するための、オープンで統一的なプログラムを策定する。但し、2009 年 12 月 29 日の E.O.13526 または改正原子力法に基づき機密とされた情報を除く。

また、E.O.13556 に基づいて策定された 32CFR part2002 では CUI について以下のように定義されている。

（32CFR part2002 における CUI の定義）
- 管理対象非機密情報（CUI）とは、政府が作成もしくは保有する情報、またはある機関が政府のためにもしくは政府のために作成もしくは保有する情報であり、法律、規則、または政府全体の方針が、保護管理もしくは配布管理を使用して取り扱うことを機関に要求または許可するものである。
- ただし、CUI には、機密情報、または、行政府機関もしくは行政府機関のために行動する団体に由来しない、もしくは、行政府機関もしくは行政府機関のために作成または所有していない、非行政府機関が所有し、自己のシステムに保持する情報は含まれない。

■　情報の分類

CUI の分類について、32CFR part2002 で以下のような２つのレベルに分類されている（表 4.1-8）。

表 4.1-8　CUI のレベル・定義

レベル	定義
CUI Basic	・　認可する法律、規則、または政府全体の方針が、具体的な取扱いまたは普及管理を定めていない CUI のサブセット
CUI Specified	・　権限を与える法律、規則、または政府全体の方針が、CUI Basic のものとは異なる、各省庁が使用することを要求または許可する特定の取扱管理を含む CUI のサブセット

■　情報管理策

・　組織的管理策

組織的管理策については、以下のような事項が定められている。

（32CFR part2002 で規定される主な組織的情報管理策）

- CUI EA[121]は、必要に応じて CUI レジストリに保護基準を発行し、必要に応じて更新する。これらの基準は、認可された保有者によるタイムリーなアクセスを可能にする一方で、不正開示のリスクを最小化する方法で、常に CUI を保護することを機関に要求する
- 外国機関と協定または取決めを締結する場合、機関は、可能な限り、命令、本編、および CUI 登録簿に従って CUI を保護するよう当該機関に促すべきであるが、CUI を保護するという最終目標を念頭に置き、何をどの程度伝達するかについては、機関の判断を用いることができる
- CUI SAO は、機関の訓練方針を策定し、実施しなければならない。少なくとも、訓練方針は、機関の CUI 訓練の手段、方法、および頻度について述べなければならない
- 省庁の訓練方針は、CUI にアクセスできる要員が、CUI の指定、関連する CUI カテゴ リーおよびサブカテゴリー、CUI 登録、関連するマーキング、および適用される保護、配布、および管理解除の方針および手順に関する訓練を受けることを保証しなければならない
- 機関は、職員が初めて機関に勤務する時、およびその後少なくとも 2 年に 1 回は CUI の指定、関連する CUI カテゴリーおよびサブカテゴリー、CUI 登録、関連するマーキング、および適用される保護、配布、および管理解除の方針および手順に関する訓練を受けさせなければならない

・　人的管理策

人的管理策については、以下のような事項が定められている。

（32CFR part2002 で規定される主な人的情報管理策）

- 権限を付与された保有者は、CUI レジストリに示された基本的な当局の要件に従って、指定された CUI を保護する
- 権限のある保有者の管理下にある CUI の保護。権限のある保有者は、CUI の不正な開示を防ぐために以下のような合理的な予防措置を講じなければならない
  - ➢　不正なアクセスや開示から CUI を保護するための管理環境を確立し、その管理環境を活用すること
  - ➢　権限のない個人が CUI にアクセスしたり、CUI を観察したり、CUI に関する会話を立ち聞きしたりできないことを合理的に確保すること
  - ➢　CUI を権限保持者の直接管理下に置くか、少なくとも 1 つの物理的バリアで保護し、管理された環境の外では、権限保持者または物理的バリアが不正アクセスまたは観察から CUI を保護することを合理的に確保すること

[121] CUI EA（CUI Exective Agent）：国立公文書記録管理局（NARA）のことを指す。同局は行政府全体の CUI プログラムを実施し、命令を遵守するための連邦機関の行動を監督する。NARA はこの権限を情報セキュリティ監督局（ISOO）局長に委任している。

（NIST SP800-171 で規定される主な人的情報管理策）

- システム媒体上の CUI へのアクセスを、認可されたユーザに限定する
- システムへのアクセスは、認可されたユーザ、認可されたユーザに代わって動作するプロセスおよび（その他のシステムを含む）デバイスに限定する
- 共謀が関与しない場合の有害行為のリスクを減らすため、個人の職務を分離する
- ユーザがインストールしたソフトウェアを管理し監視する
- 必要なアクセス認可のないメンテナンス職員のメンテナンス行為を監督する
- CUI を含む組織のシステムへのアクセス認可に先立って、個人を審査する
- 退職や異動などの人事措置中、およびその後において、CUI を含む組織のシステムが保護されていることを確実にする

・ 物理的管理策

物理的管理策については、以下のような事項が定められている。

（32CFR part2002 で規定される主な物理的情報管理策）

- 権限のある CUI の保有者は、CUI を権限保持者の直接管理下に置くか、少なくとも 1 つの物理的バリアで保護し、管理された環境の外では、権限保持者または物理的バリアが不正アクセスまたは観察から CUI を保護することを合理的に確保しなければならない。
- 機関は、CUI 用のカバーシートを使用することができる。カバーシートの使用を選択した場合、CUI EA が承認したカバーシートを使用しなければならない。

・ 技術的管理策

技術的管理策については、以下のような事項が定められている。

（32CFR part2002 で規定される主な技術的情報管理策）

- CUI を処理、保管または転送する情報システム：FIPS PUB 199 に従い、CUI Basic は、中程度の機密性影響レベル以上に分類される。省庁はまた、FIPS PUB 200 および NIST SP 800-53 の適切なセキュリティ要件および管理を、リスク・ベースの調整決定に従い、CUI に適用しなければならない
- 省庁は、非連邦情報システム上で、CUI の機密性を保護するためのセキュリティ要件を確立する場合、NIST SP800-171 を使用しなければならない（関係する情報の CUI カテゴリーまたはサブカテゴリーに関する CUI レジストリに記載されている認可法、規則、または政府全体のポリシーが、情報の機密性を保護するための特定の保護要件を規定している場合、または CUI Basic を中程度以上の機密性で保護するための要件が協定で定められている場合を除く）
- CUI Basic：権限のある保有者は、アクセスが以下に規定される要件を満たす場合、いかなる受領者に対しても CUIBasic へのアクセスを普及させ、奨励すべきである。
  - CUI カテゴリーまたはサブカテゴリーを定めた法律、規制、または政府全体の方針を遵守すること
  - 政府の合法的な目的を促進すること

- CUI EA によって確立された、許可された限定的な普及コントロールによって制限されていないこと
- その他法律で禁止されていないこと

（NIST SP800-171 で規定される主な技術的情報管理策）

- CUI を含むシステムの媒体を廃棄または再利用する前に、サニタイズまたは破壊する
- 代替的な物理的保全措置によって保護されている場合を除き、デジタル媒体上に保存された CUI の秘匿性を輸送時に保護するため、暗号メカニズムを実装する
- システムコンポーネント上のリムーバブルメディアの使用を管理する
- ポータブルストレージデバイスのオーナーを識別できない時には、ストレージデバイスの使用を禁止する
- システムへのアクセスは、認可されたユーザが実行を許可されているタイプのトランザションおよび機能に限定する
- 非アクティブ状態が一定時間経過後のデータのアクセスおよび閲覧を防止するために、隠蔽用パターンの表示によるセッションロックを使用する
- 規定された条件が成立した場合には、ユーザセッションを終了させる
- リモートアクセスセッションを監視し、管理する
- リモートアクセスセッションの秘匿性を保護するために暗号メカニズムを採用する
- 管理されたアクセス制御ポイント経由でリモートアクセスをルーティングする
- 認証および暗号を使用してワイヤレスアクセスを保護する
- モバイルデバイスの接続を管理する
- モバイルデバイスおよびモバイルコンピューティングプラットフォーム上の CUI を暗号化する
- 外部システムへの接続および使用を検証し、管理・限定する
- 外部システム上でのポータブルストレージデバイスの使用を限定する
- 公衆アクセス可能なシステム上に掲載または処理される CUI を管理する
- オンデマンドでの分析および報告をサポートするための監査記録の集約および報告書生成機能を提供する
- 必須でないプログラム、機能、ポート、プロトコルおよびサービスの使用を制限、無効化または防止する
- システムのユーザ、ユーザに代わって動作するプロセス、およびデバイスを識別する
- 組織のシステムへのアクセスを許可する前提条件として、ユーザ、プロセス、またはデバイスのアイデンティティを認証または検証する
- 多要素認証を特権アカウントによるローカルおよびネットワークアクセスならびに非特権アカウントによるネットワークアクセスに使用する
- 特権および非特権アカウントによるネットワークアクセスに、リプレイ耐性のある認証メカニズムを採用する
- 規定された期間、ID の再利用を防止する
- 規定された非アクティブな期間が過ぎた後、ID を無効化する
- 新しいパスワードが作成される際には、パスワードの最小限の複雑性と文字の変更を強制する
- 指定された生成回数の間、パスワードの再利用を禁止する
- システムログオン時、常用パスワードに即時変更することを条件として一時的パスワ

ードの使用を許可する
- 暗号技術で保護されたパスワードのみを保存および伝送する
- 認証情報のフィードバックを隠す
- オフサイトで行われるメンテナンスのために取り外される装置からすべての CUI がサニタイズされていることを確実にする
- 外部ネットワーク接続を介して非ローカルメンテナンスセッションを確立する際には多要素認証を要求し、非ローカルメンテナンスの完了時にはその接続を切断する
- システムおよびアプリケーションの脆弱性スキャンを定期的に、かつ、それらのシステムおよびアプリケーションに影響する新たな脆弱性が特定された場合に実施する
- 組織のシステムの欠陥を修正し、脆弱性を軽減または排除することを意図した実施計画書を作成し、実施する
- システムのセキュリティ管理策が継続的に有効であることを確実にするため、その管理策を継続的に監視する
- システムの境界、運用環境、セキュリティ要件の実装方法、および他のシステムとの関係または他のシステムへの接続について記述したシステムセキュリティ計画書を作成し、文書化し、定期的に更新する
- 通信（組織のシステムによって送受信される情報）を、組織のシステムの外部境界および主要な内部境界において監視、管理、および保護する
- 組織のシステム内で効果的な情報セキュリティを促進するような、アーキテクチャ設計、ソフトウェア開発技法、およびシステムエンジニアリングの原則を採用する
- システム管理機能からユーザ機能を分離する
- 共有システム資源を経由した、認可されてない情報転送や意図しない情報転送を防止する
- 内部ネットワークから物理的または論理的に分離された、公開アクセス可能なシステムコンポーネント用のサブネットワークを実装する
- デフォルト設定によりネットワーク通信トラフィックを拒否、また例外によりネットワーク通信トラフィックを許可する
- リモートデバイスが、組織のシステムとの非リモート接続を確立すると同時に、外部ネットワーク内にある資源へその他何らかの接続を介して通信することを防止する
- 代替的な物理的保全措置によって保護されている場合を除き、伝送中の CUI の認可されてない開示を防止するために、暗号メカニズムを実装する
- 通信セッション終了時、または規定された非アクティブ時間経過後、そのセッションに関連するネットワーク接続を切断する
- 組織のシステムで採用される暗号技術のための暗号鍵を設定し、管理する
- CUI の秘匿性保護には、FIPS 認証された暗号技術を採用する
- 共同コンピューティングデバイスのリモートからの活性化を禁止し、そのデバイスに存在するユーザに対して使用中のデバイスを表示する
- モバイルコードの使用を管理および監視する
- インターネットプロトコルによる音声通信（VoIP）技術の使用を管理および監視する
- 組織のシステム内の指定された場所で、悪意のあるコードからの保護機能を提供する
- システムのセキュリティアラートおよび勧告を監視し、対応措置を講ずる
- 悪意のあるコードからの保護メカニズムが新たにリリースされた場合、更新する
- 組織のシステムの定期的スキャンを実行すると共に、外部ソースからのファイルのリ

アルタイムスキャンを、ファイルのダウンロード、開封、実行される都度実行する ・ 攻撃および潜在的攻撃の兆候を検知するために、出入する通信トラフィックを含めて組織のシステムを監視する

■ 罰則

32CFR part2002 の中で罰金等具体的な罰則が定められているわけではないが、CUI の不正使用の項目の中で、以下の２点が規定されている。

(32CFR part2002 で規定される罰則に関する事項) ・ CUI を誤用した職員に対して行政処分を行う権限が、省庁の長に与えられている場合、誤用を管理する CUI ポリシーは、その権限を反映したものでなければならない。 ・ CUI の特定のカテゴリーまたはサブカテゴリーを管理する法律、規制、または政府全体の方針が、制裁を特に定めている場合、各機関はかかる制裁を遵守しなければならない。

c) ECRA／EAR／ITAR[122, 123, 124]

■ 策定機関・策定時期

ECRA(2018 年)/EAR (1979 年)/ITAR(1976 年)

■ 策定の背景・目的

ECRA は EAA が失効し、以降は緊急経済権限法に基づいて暫定的な運用となっていた米国の輸出管理体制に関して、輸出管理に関する EAA に代わる法律が必要とされており、また多義的技術の発展等により、それらの技術情報等に関する輸出管理についても対応する必要があったため、それ以前まで米国の多義的技術品の規制のための根拠として機能していた行政規則である EAR に対する、より確固とした連邦法という根拠を与えるために制定された。

ITAR は、米国の国防に関連する技術や製品が、不正な手段で敵対国やテロリスト、その他の米国の利益に反する勢力の手に渡ることを防ぐために制定された。

■ 適用範囲

ECRA では、現行の輸出管理規制において規制対象となっている技術の中から多義的技術の発展等を背景に新たに新興・基盤的技術として 14 の技術を EAR の CCL (Commerce Control List：規制品目リスト) に追加をした。下位規則の EAR では、CCL のカテゴリーとして 10 の技術分野に区分をして、それら製品の輸出については許可を取得しなければならない等の規定を定めている。

122 https://www009.web.fc2.com/EAR_J/ECRA.pdf

123 https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

124 https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

（EAR の CCL にリストアップされる 14 の新興・基盤的技術）

①バイオテクノロジー

i.ナノバイオテクノロジー、ii.合成生物学、iii.遺伝子工学 iv.神経工学

②AI・機械学習

i.ニューラルネットワーク・ディープラーニング、ii.進化的・遺伝的コンピューティング、iii.強化学習、iv.コンピュータビジョン、v.エキスパートシステム、vi.音声・音響処理、vii.自然言語処理、viii.プランニング、ix.オーディオ・ビデオ操作技術、x.AI クラウド技術、xi.AI チップセット

③測位技術

④マイクロプロセッサー

i.SoC（Systems-on-Chip（SoC））、ii.チップ上スタックメモリ

⑤先進コンピューティング

メモリ集約型論理

⑥データ分析

i.視覚化、ii.自動分析アルゴリズム、iii.文脈把握コンピューティング

⑦量子情報・量子センシング

i.量子コンピューティング、ii.量子暗号、iii.量子センシング

⑧補給関連技術

i.携帯電力、ii.モデリング・シミュレーション、iii.総資産可視化、iv.DBLS（Distribution-based Logistics Systems：流通型物流システム）

⑨付加製造技術

⑩ロボティクス

i.マイクロドローン・ロボティクスシステム、ii.群制御技術、iii.自己集合ロボット、iv.分子ロボット、v.ロボットコンパイラ装置、vi.スマートダスト（Smart Dust）

⑪ブレインコンピュータインターフェース

i.ニューラルコントロールインターフェース、ii.マインドマシンインターフェース、iii.DNI（Direct neural interfaces）、iv.ブレイン・マシン・インターフェース

⑫極超音速

i.飛行制御アルゴリズム、ii.推進技術、iii.熱防御システム、iv.　　特殊素材

⑬先端材料

i.適応迷彩、ii.機能性繊維、iii.バイオ素材

⑭先進セキュリティ技術

顔認証、声紋認証技術

（EAR の CCL カテゴリー）

0　核物質、核施設、核装置、その他の品目
1　材料、化学物質、微生物、有毒物質
2　材料加工
3　エレクトロニクス
4　コンピュータ
5　通信・暗号
6　レーザー・センサー
7　航法装置・航空電子

8　海洋技術
9　推進システム・宇宙機器・関連装置

ITARでは、以下のようなUSML（United States Munitions List：米国軍需品リスト）が策定されており、リストに記載された製品、技術などの輸出、再輸出、再移転について、許可が必要になる等の規定を定めている。

（ITARにおける米国軍需品リスト(カテゴリー)）
カテゴリーⅠ　火器および関連物品
カテゴリーⅡ　火砲および兵器
カテゴリーⅢ　銃砲弾および兵器
カテゴリーⅣ　打上げ用の飛翔体、誘導・弾道ミサイル、ロケット、魚雷、爆弾および地雷
カテゴリーⅤ　爆発物および高エネルギー物質、推進薬、焼夷剤並びにこれらの成分
カテゴリーⅥ　軍用水上艦艇および海軍関連特別装備品
カテゴリーⅦ　陸上車両
カテゴリーⅧ　航空機および関連物品
カテゴリーⅨ　軍事訓練関連装置および軍事訓練
カテゴリーⅩ　個人用の防御装備品
カテゴリーⅪ　軍事用電子装置
カテゴリーⅫ　火器管制装置、レーザー、撮像装置、および誘導装置
カテゴリーⅩⅢ　材料およびその他の物品
カテゴリーⅩⅣ　毒素物質（化学剤、生物剤および関連装置を含む）
カテゴリーⅩⅤ　宇宙航空システムおよび関連装置
カテゴリーⅩⅥ　核兵器関連物品
カテゴリーⅩⅦ　機密扱いの物品、技術資料および防衛役務で他の項目で列挙されていないもの
カテゴリーⅩⅧ　指向性エネルギー兵器
カテゴリーⅩⅨ　ガスタービンエンジンおよび関連装置
カテゴリーⅩⅩ　潜水艦および関連物品
カテゴリーⅩⅩⅠ　他のカテゴリーで列挙されていない物品、技術資料、および防衛役務

■　情報の分類
記載なし

■　情報管理策
・　組織的管理策
CCLに掲載されている品目については原則として、商務省の輸出許可が必要となる。
CCLに掲載の無い品目はEAR99として規制対象品に入ってはいるものの、そのほとんどは輸出や再輸出の許可は不要となっている。しかし、EARには10個の一般禁止事項が定められており、その中の4～10に該当する場合は原則CCLの規制品目かどうか問わずに、商務省の輸出許可が必要となる。

（EAR における一般禁止事項）

1. 規制品目のリスト（Entity List(米国の安全保障・外交政策上の利益に反する、または大量破壊兵器の開発等に関与した企業等のリスト)）の対象国への輸出および再輸出（輸出および再輸出）
2. 外国製物品の再輸出および外国からの輸出
3. 外国直接製品（FDP）規則
4. 拒否命令によって禁止されている行為に関与すること
5. 輸出、再輸出、または禁止されている最終用途もしくは最終使用者（エンドユーズ・エンドユーザ）への移転（国内）
6. 禁輸措置が取られた目的地への輸出、再輸出、および移転（国内）
7. 拡散活動および特定の軍事情報エンドユースとエンドユーザの支援
8. 輸送中の貨物および船舶または航空機から積み下ろされる物品
9. 命令、条項、条件の違反
10. 違反が発生した、または発生しようとしていることを知りながら取引を進めること

ITAR では USML による規制の他、以下のような対象国については防衛物品・役務の輸出について拒否を原則している

（ITAR において防衛物品・役務の輸出を禁止している国）

- ベラルーシ
- ビルマ
- 中国
- キューバ
- イラン
- 北朝鮮
- シリア
- ベネズエラ

■ 罰則

ECRA では、不法行為として以下のような行為を規定し、それらの不法行為を意図的に犯したり、意図的に犯すことを試みたりまたは意図的に犯すことを共謀したり、加担して手伝って幇助した者は 100 万ドル以下の罰金および個人の場合には 20 年以下の拘禁に処せられるか、またはこれを併科されるもの規定されている。

また民事的には本法令に違反をした場合、商務長官は、ECRA または ECRA のもとに発行された規則、命令若しくは輸出許可の当該者による各違反者については、当該者に対して 30 万ドル以下または罰則が課せられる違反の根拠となっている取引額の 2 倍以下のいずれか高額の罰金、本パートに基づいて当該者に発行される輸出許可の取り消し、当該者が本パートで規制される品目を輸出、再輸出、または国内において移転できることを禁じることができる。

（ECRA で規定される主な不法行為）

(1) 通則 ある者が、本パートまたは本パートのもとに発行された規則、命令、輸出許可、若しくはその他の認可に違反すること、違反を試みること、違反を共謀すること、違反を引き起こすことは違法であるものとする（(2)項で規定されるいずれかの不法行為を含む）。

(2) 特別な不法行為本項で規定される不法行為は、以下のものである

(A) 何人も、本パート、EAR、またはこれらのもとに発行された規則、命令、輸出許可、若しくは認可によって禁止された行為またはそれらに反する行為に従事してはならない、或いはそれらによって義務づけられている行為に従事することをやめてはならない

(B) 何人も、本パート、輸出管理規則、またはこれらのもとに発行された規則、命令、輸出許可、若しくは認可によって禁止された行為を行うこと若しくはそれらによって義務付けられている行為を怠ることを、引き起こしたり、手助けをしたり、教唆したり、助言したり、命じたり、誘導したり、周旋したり、承認したりしてはならない

(C) 何人も、本法律、輸出管理規則、またはこれらのもとに発行された規則、命令、輸出許可若しくは認可に対する違反を教唆したり、企ててはならない

(D) 何人も、いかなる方法または目的においても、本パート、輸出管理規則、またはこれらのもとに発行された規則、命令、輸出許可若しくは認可に対して違反となる行為を、引き起こしたり、行なうことを一人以上の他の者と協力して共謀したり、実行してはならない

(E) 何人も、米国から輸出される品目若しくは米国から輸出される予定の品目または別途輸出管理規則の規制を受ける品目に関連して、本パート、輸出管理規則、またはこれらのもとに発行された規則、命令、輸出許可若しくは認可に対する違反が発生したこと、今にも発生しようとしていること、或いは発生する意図があることを知りながら、これらの品目の一部または全部について、発注、購入、移動、隠匿、貯蔵、使用、販売、貸与、処分、譲渡、輸送、融資、発送、またはその他の役務を行なったり、それらの行為の手助けをするために交渉を行ってはならない（ただし、それらに対して正当な認可が取得されている場合を除く）

(F) 何人も、下記の場合において、商務省若しくはその他の米国機関（国土安全保障省および司法省を含む）の担当官に直接的に、または他の者を通して間接的に、虚偽若しくは誤解をまねく説明、申告または証明をしたり、重要な事実を偽ったり、隠蔽してはならない

- 輸出管理規則の対象となる調査またはその他の活動の過程において
- 輸出管理書類または輸出管理規則に基づいて提出される報告書または提出されることが義務付けられている報告書の作成、提出、発行、使用または維持に関連して
- 輸出管理規則の対象品目の輸出、再輸出、若しくは国内における移転または第 1754 節で記載される米国人の役務若しくはその他の行為を成就する目的でまたはこれに関連して

(G) 何人も、輸出管理規則又はこれらのもとに発行された命令、輸出許可、若しくは認可の条項を回避することを意図して、取引に従事したり、その他の行為をとってはならない

(H) 何人も、輸出管理規則又はこれらのもとに発行された命令、輸出許可、若しくは

認可の報告又は記録保管要求事項に従うことを怠ったり、拒否してはならない
(I) 輸出管理規則において又は商務省による書面において明確に認可されている場合を除いて、何人も、輸出管理規則のもとに発行された輸出許可証、認可証、輸出管理文書又は命令書を変造してはならない
(J) 何人も、本パート、輸出管理規則、又はこれらのもとに発行された命令、輸出許可若しくは認可の差し迫った違反を防ぐために、商務省により発行される剥奪命令又は一時的剥奪命令により禁止されている行為をとってはならない

ITAR については以下のような違法行為に該当した場合、100 万ドル以下の罰金、もしくは 20 年以下の懲役、またはその両方を科されるものとされている。

(ITAR で規定される主な違法行為)
- 以下の行為は違法行為である
  - 本副章により輸出許可若しくは書面による認可を必要とする防衛物品若しくは技術資料を米国から輸出すること若しくは輸出を企てること、又は本副章により輸出許可若しくは書面による認可を必要とする防衛役務を提供すること若しくは提供することを企てること
  - 一つの外国の最終需要者、最終用途、又は仕向先から、他の外国の最終需要者、最終用途、又は仕向先に本副章により輸出許可若しくは書面による認可を必要とする防衛物品、技術資料、又は防衛役務で指定されるところにより、本副章のいずれかの除外条項に基づいて輸出許可なしに米国から輸出された防衛物品、技術資料、又は防衛役務を含む）を再輸出若しくは再移転すること又は再輸出若しくは再移転を企てること
  - 本副章により輸出許可を必要とするいかなる場合においても、防衛物品を輸入すること又は輸入を企てること
  - 本副章により輸出許可若しくは書面による認可を必要とする防衛物品、技術資料、又は防衛役務を共謀して輸出、輸入、再輸出、再移転若しくは提供すること、又は人に輸出、輸入、再輸出、再移転若しくは提供させること
  - 22 U.S.C. 2778 および 2779、又はそれらに基づいて発行された規則、輸出許可、認可、若しくは命令に違反して、何らかの防衛物品を、その防衛物品を輸出又は移転する目的で、所有する、若しくは所有することを企てること
  - 本副章に基づいて与えられた輸出許可若しくは認可、本副章に記載される除外条項、又は本副章に記載されるルール若しくは規則の条件に違反すること
  - 最初に防衛取引管理部から登録されることなく又は必要な輸出許可若しくは書面による認可を取得することなく、登録および輸出許可又は書面による認可が本副章により必要とされる仲介行為の事業に従事すること
  - 登録要求事項に従わずに、米国内で、防衛物品の製造事業若しくは輸出事業又は防衛役務を提供する事業に従事すること

d) FIRRMA(Foreign Investment Risk Review Modernization Act)[125]

■ 策定機関・策定時期

[125] https://www.congress.gov/bill/115th-congress/house-bill/5841/text

2018 年

■　策定の背景・目的

米国の外国直接投資に関しては従来、米国事業の「支配（control)」をもたらす合併、取得、買収を「審査対象取引」と定めて、それらが安全保障に与える脅威を審査してきたが、中国をはじめとした外国企業の米国企業への買収や投資が増加し、これが技術や知的財産の流出に繋がる懸念があり、米国の外国直接投資に対する審査体制を拡大・強化する必要があった。

■　適用範囲

FIRRMA では、基本的には引き続き外国からの対米投資の歓迎する方針を掲げつつも、従来の CFIUS で定められた審査対象である外国人による米国事業の支配をもたらす合併、取得、買収に加えて、審査対象範囲を拡大して重要技術の流出や重要インフラへの悪影響などの防止の観点からセンシティブな米国政府施設に近接する不動産取引や、重要技術を扱う米国事業の外国人による「支配」を伴わない投資も審査対象としている。

■　情報の分類

記載なし

■　情報管理策

・　組織的管理策

FIRRMA では以下のような行為について規制対象とし、該当する投資行為等に関しては、CFIUS の審査を受けなければならない。

（FIRRMA の規制対象行為）

1. 支配を及ぼす投資
2. 支配を及ぼさない一定の投資
3. 追加投資により、支配を及ぼす投資、支配を及ぼさない一定の投資行為にあたるようになった場合
4. 上記以外の取引、移転、合意等であって、FIRRMA の規制を潜脱する目的のものである場合

（支配を及ぼさない一定の投資の定義）

外国人による以下のような米国事業関与者への支配を及ぼさない投資（株式・持分等の取得行為）であって、かつ、以下のいずれかにあたるもの。

1. 米国事業関与者の実質的な非公知情報へのアクセスが可能になる場合
2. 米国事業関与者の役員又は役員に準じる職位若しくはその選任が可能になる場合、又は
3. 株主としての議決権行使以外の方法で、以下のいずれかについての決定に関わることが出来る場合。
   - 米国事業関与者が保有又は収集している米国人の機微な個人データの利用、取得、保持、若しくは開示

- 重大な技術（critical technologies）の利用、開発、獲得、若しくは開示、又は
- 重大なインフラ（critical infrastructure）の管理、運用、製造、若しくは供給

（規制対象行為の対象となる米国事業関与者）

1. 重大な技術を生産、設計、テスト、製造、変改、若しくは開発している米国事業関与者
2. 重大なインフラを保有、運用、製造、供給、若しくはサービスしている米国事業関与者
3. 米国人の機微な個人データを保有若しくは収集している米国事業関与者

（重要な技術、重要なインフラ、機微な個人データの定義）

1. 重要な技術
   - ITAR に定める米国軍需品リストに含まれる防衛品または防衛サービス
   - CCL に含まれ、かつ、管理される品目
   - 国家安全保障に関連する理由を含む多国間レジームに従って管理される、もしくは国家安全保障、化学兵器および生物兵器の拡散、核不拡散、またはミサイル技術に関連する理由を含む、多国間体制に従って管理されるもの
   - 地域の安定または盗聴に関する理由
   - 連邦規則集第 10 編第 810 部（外国の原子力活動への支援に関するもの）に含まれる、特別に設計・準備された原子力機器、部品・構成要素、材料、ソフトウェア、技術
   - 連邦規則集第 10 編第 110 部（核装備品および核物質の輸出入に関するもの）の対象となる核施設、核装備品および核物質
   - 連邦規則集第 7 編第 331 部、同第 9 編第 121 部、または同第 42 編第 73 部の対象となる選択薬剤および毒素
   - ECRA 従って管理される新興技術および基盤技術

2. 重要なインフラ [126]

委員会が定める規制に従い、物理的であるか仮想的であるかにかかわらず、米国にとって極めて重要なシステムおよび資産を意味し、そのシステムまたは資産の機能停止または破壊は、国家安全保障に衰弱的な影響を与えるものとして 28 のインフラ(インターネット・プロトコル・ネットワーク、情報通信サービス、海底ケーブル、衛星(衛星システムを含む)等)を規定

3. 機微な個人データ

(a) 機密個人データとは、本条(b)項に定める場合を除き、以下のものをいう：

(1) 識別可能なデータ：

(i) 以下の米国企業によって保持または収集されるデータ

A) 情報、国家安全保障、または国土安全保障を担当する米国の行政府機関または軍部、あるいはその職員および請負業者を対象とする製品またはサービス

B) §800.104(b)(2)から(4)に記載されたいずれかの事象が発生した日（該当する場合）、または書面による通知の提出日もしくは申告書の提出日のうち最も早い日に先立つ 12 ヶ月のいずれかの時点において、100 万人を超える個人につ

[126] https://www.ecfr.gov/current/title-31/subtitle-B/chapter-VIII/part-800/appendix-Appendix%20A%20to%20Part%20800

いて、本項(a)(1)(ii)に記載されたー つ以上のカテゴリーに含まれる識別可能なデータを維持または収集していたこと。ただし、米国事業者が、当該取引の完了日の時点で、100 万人を超える個人について、本項(a)(1)(ii)に記載される1つ以上のカテゴリーに含まれる識別可能なデータを維持する能力も、収集する能力も有していないか、又は有する予定であることを証明できる場合を除く

C) 100 万人を超える個人について、本項(a)(1)(ii)に記載される 1 つ以上のカテゴリーに含まれる個人を特定できるデータを維持または収集する事業目的が実証されており、かつ、当該データが米国事業の主要な製品またはサービスの統合された一部であること

(ii) 以下のカテゴリーのいずれかに含まれるもの

A) 個人の経済的困窮または苦難を分析または判断するために使用され得る財務データ

B) 15 U.S.C.1681a に基づき定義される消費者報告書のデーター式。ただし、かかるデータが 15 U.S.C.1681b(a)に特定される 1 つ以上の目的のために消費者報告機関から取得され、かかるデータが 15 U.S.C.1681a に基づき定義される消費者ファイルの全内容と実質的に類似していない場合を除く

C) 健康保険、介護保険、専門職業賠償責任保険、住宅ローン保険、または生命保険の申請書のデーター式

D) 個人の身体的、精神的、または心理的な健康状態に関するデータ

E) 米国企業の製品またはサービスの利用者間または利用者間の電子メール、メッセージング、チャット通信を含む非公開の電子通信（当該製品またはサービスの主な目的が第三者の利用者との通信を容易にすることである場合）

F) モバイル・アプリケーション、車両 GPS、その他の車載マッピング・ツール、またはウェアラブル電子デバイスを介するなど、測位システム、携帯電話タワー、または WiFi アクセス・ポイントを使用して収集されたジオロケーション・データ

G) 顔、音声、網膜／虹彩、手のひら／指紋テンプレートを含む、バイオメトリクス登録データ

H) 州政府または連邦政府の身分証明書を作成するために保存および処理されるデータ

I) 米国政府職員のセキュリティ・クリアランスの状態に関するデータ

J) 米国政府職員のセキュリティ・クリアランスの申請書、または公の信頼に値する地位での雇用の申請書に含まれる一連のデータ

(2) 個人の遺伝子検査の結果（関連する遺伝子配列データを含む。このような結果には、米国政府によって維持され、研究目的のために民間団体に定常的に提供されるデータベースから得られるデータは含まれない。本項において、「遺伝子検査」は、合衆国法律集第 42 編第 300g-91 条(d)(17)に規定される意味を有するものとする

(b)機微な個人データという用語には、本項(a)に記載された基準の適用可否にかかわらず、以下を含めてはならない

(1) 米国企業によって保持または収集される、当該米国企業の従業員に関するデータ。

ただし、当該データが、米国政府の要員セキュリティ・クリアランスを保持する米国政府請負業者の従業員に関するものである場合を除く
(2) 裁判所記録や一般に公開されているその他の政府記録など、公文書となっているデータ

■ 罰則

FIRRMA では、虚偽申告を行った者に対して、25 万ドル以下の罰金が科され、事前申告が必要なものに関して、その義務を怠った者には 25 万ドルまたは、取引額のいずれか大きい額の罰金が科される。

(FIRRMA において事前申告が必要な主な取引)

1. 単一の外国（例外外国を除く）の国または準国家政府が実質的な利害を有する外国人による米国事業の技術、インフラ、データの実質的な利害の取得をもたらす対象取引

2. 1 つ以上の重要な技術の輸出、再輸出、移転(国内)又は再譲渡のために米国の規制当局の許可が必要とされる、当該重要な技術を生産、設計、試験、製造、加工又は開発する技術、インフラ、データの米国事業が関係する対象取引

(3) カナダ

1) 基本情報

- 政治体制：議院内閣制
- 人口：4,009 万 7,761 人（2023 年 7 月現在）[127]
- 名目 GDP：1.9 兆米ドル（2021）、実質 GDP：1.6 兆米ドル（2021）[128]
- 研究開発予算：345 億米ドル（2022） OECD 購買力平価 換算

■ 政治動向

2021 年 9 月に第三次トルドー政権樹立。首相を除く閣僚 38 名のうち女性が 19 名と半数を占めており、女性の社会進出を支援する現政権の姿勢が色濃く反映されている。

現政権の優先事項は、①気候変動、②中間層支援の強化、③先住民との和解、④国民の安全と健康、⑤不安定な国際社会におけるカナダの成功 の 5 課題

カナダは伝統的に米国を最も緊密な同盟国と位置付け、対米関係を最重要視。更に国連、NATO、G7、WTO、米州機構（OAS）等の多国間の枠組みを活用した多国間外交を展開している。

■ 経済動向

カナダは世界第 9 位の GDP を有し、主要産業は金融・保険・不動産などのサービス業、製造業、建設業、鉱業、農林業などであり、第 3 次産業が盛んである。また、石油・天然ガスや鉱物を豊富に有する資源輸出国である。

世界的な原油及び食料価格の高騰や足許のサプライチェーンの断絶の影響等により恒常的な超過需要が起こっており、2021 年には 1%～4%台後半で推移していた消費者物価指数（CPI）は、2022 年に入り 5%台～8%台にまで上昇している。この状況を踏まえて、カナダ中央銀行は、2022 年 3 月から 10 月の間に 6 回の政策金利の引き上げを行っている。

■ 社会動向

世界 24 位の人口を有する。移民の受入に積極的であり、国民の 4 人に 1 人が移民、2025 年まで年間 50 万人の移民を受け入れる計画となっている。

先住民の所得は全体的に低く、アルコール中毒や犯罪に関わる者も目立つが、その背景である先住民に対する同化政策の歴史を踏まえ、先住民の権利回復に関する取組みを重視している。

■ 技術動向

カナダにおけるベンチャー投資は年々拡大を続け、分野別では情報通信技術（ICT）への投資が約 7 割を占める。特に人工知能（AI）分野では、世界的に著名な教授や研究者が集積して最先端の研究開発が行われており、カナダ企業への活発な投資とともに、グローバル IT 企業のカナダ進出が増えている。カナダ政府は、ベンチャーやイノベーションを積極的に推

[127] https://www150.statcan.gc.ca/n1/pub/91-215-x/91-215-x2023001-eng.htm

[128] https://www.mofa.go.jp/mofaj/area/canada/data.html

進しており、競争力強化により、良質な雇用の創出や対内投資拡大を目指している。

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

カナダでは、「Security of Information Act（情報セキュリティ法)」が策定され、情報の漏洩、スパイ行為、テロリズムへの関与などの国家安全保障に影響を及ぼす可能性のある行為に対して法的な措置を講じるための枠組みを定めた。また、同年には「Access to Information Act（情報アクセス法)」についても制定され、その中では基本的に要求された記録の内、企業秘密、またはカナダ政府もしくは政府機関に属し、実質的価値を有するか、もしくは実質的価値を有する可能性が合理的に高い財務、商業、科学もしくは技術情報や、政府機関の役員又は職員が研究を通じて得た科学的又は技術的な情報であって、その開示により当該役員又は職員が公表の優先権を奪われることが合理的に予想される情報について、政府はその要求を拒否できると規定されている。[129],[130]

また2019年には政府のセキュリティ管理を効果的にし、カナダ政府の安全管理に関してカナダ人、パートナー、監督機関、その他の関係者に保証を提供することを目的とした「Policy on Government Security（政府のセキュリティポリシー)」が策定され、ここで示された目的を達成するため、同年には、各部門等で分けられていた情報セキュリティ基準等が統合され、「Directive on Security Management（セキュリティマネジメント指令)」が策定された。

この規定の中で、一般的な情報については、機密性の喪失（不正な開示の結果）、完全性の喪失（不正な改ざん又は破壊の結果）、又は可用性の喪失（不正な除去又はその他の破壊の結果）の結果として合理的に予想される損害の程度を反映するために、「非常に高い（Very high)」、「高い（High)」、「中程度（Medium)」、又は「低い（Low)」影響度に分類され、機密情報については、その不正な開示が影響する度合いによって「最高機密（Top secret)」、「極秘（Secret)」、「機密（Confidential)」の3つのレベルに分けられている[131],[132]。

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

カナダでは1985年に策定された、「Export and Import Permits Act（輸出入許可法)」の規定に則り品目を管理しており、輸出入の管理リストに記載のある品目をあつかう事業者等は、ライセンスの発行を受ける必要がある他、ライセンスを受けた者は、本法の遵守状況を当局が判断するために必要な情報を保存することが義務付けられている。管理品目の中には「Dual-use Goods and Technology to Certain Destinations」と多義的技術に関連する品目も含まれており、それらの技術が不法に海外等に流出しないようにしている。[133]

また、海外からの投資については、2021年に「Investment Canada Act（カナダ投資法)」が改正されており、国家の経済成長、雇用機会の奨励および国家安全保障の保護を目的と

[129] https://laws-lois.justice.gc.ca/eng/acts/o-5/

[130] https://laws-lois.justice.gc.ca/eng/acts/a-1/

[131] https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578

[132] https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611

[133] https://laws-lois.justice.gc.ca/eng/acts/e-19/

して、非カナダ市民（個人、政府、機関）による投資の、イノベーション・科学・経済開発省に通知および審査申請の義務化や、当局が必要と認める場合、海外投資がもたらす国家安全保障への影響を審査する等、海外資本によるカナダ国内への直接投資（新規事業および既存事業の買収）等の規制を定められている。[134]

その他、研究機関を対象として、研究保護の必要性や研究に関するセキュリティリスクを示し、それに対処するためのトレーニングを提供することを目的としたガイドラインである「Safeguarding Your Research」や、カナダ政府（競争局）の競争法における知的財産法の取扱い方針に関する専門家向けのガイドラインである「Intellectual Property Enforcement Guidelines（知的財産行使ガイドライン）」等が策定されている。

[134] https://laws-lois.justice.gc.ca/eng/acts/i-21.8/

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　国家戦略等

2019 年に ISED （Innovation, Science and Economic Development Canada ：イノベーション・科学経済開発省） によって A New Space Strategy for Canada が制定された。これは宇宙産業の発展に関する戦略で、5 本柱として、①LUNAR GATEWAY MISSION への参加、②次世代の教育、③衛星による社会経済的利益の向上（通信・防衛能力の向上）、④宇宙分野の雇用創出および⑤宇宙データの活用、が掲げられている [135]。経済安全保障との関連性として、本戦略の中で、「宇宙分野はカナダの主権、安全保障、経済成長にとって不可欠な国家戦略資産」と位置付けられている。

2022 年に ISED によって Canada’s Strategy for Satellite Earth が制定された。これは衛星を用いた地球観測に関する戦略で、目標として、①地球観測データのオープンアクセス化、②気候変動問題への対応、③データサービス提供の強化、④次世代のための能力開発、を掲げている [136]。経済安全保障との関連性として、衛星への投資は防衛戦略を補完・強化するために活用可能であると述べている。また、衛星情報をもとに作物の収量予測を行うことで、食料の安全保障の支援の可能性についても取り上げている。

■　研究開発機関

宇宙領域の研究開発関係機関としては、民生分野における研究では CSA(Canadian Space Agency：カナダ宇宙庁)、防衛分野では DND(Department of National Defence：国防総省)が主要な役割を担っている。CSA は ISED が所管している国立研究所の一つで、カナダにおける宇宙関連の研究開発をリードする目的で設立された。DND はカナダの国防政策に従って国家主権を守るための活動を行っており、国防に関係する研究開発も所管している（図 4.1-9）。

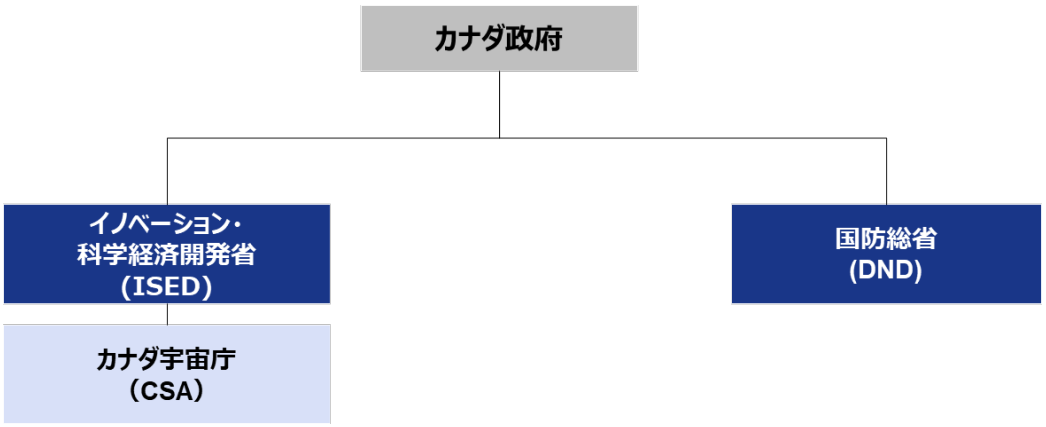


図 4.1-9 カナダにおける宇宙領域研究開発の主要機関

[135] https://www.asc-csa.gc.ca/pdf/eng/publications/space-strategy-for-canada.pdf

[136] https://www.asc-csa.gc.ca/pdf/eng/publications/canada-strategy-for-satellite-earth-observation-v2.pdf

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Terrestrial Snow Mass Mission - Phase 0[137]

CSA が所管するプログラムであり、地上積雪水量の高分解能測定を実現するための開発計画を更新・改善することを目標としている。CoReH20 フェーズ 0 及びフェーズ A により装置開発、積雪についての特性評価・モデリングについて成果が得られたため、本プロジェクトにおいて高性能化を図ることが求められる。得られた成果は ECCC（Environment and Climate Change Canada：環境・気候変動省）の気象研究部門で活用される予定である。

本プログラムの提案から生じるフォアグラウンド知的財産の所有権はカナダ政府が保持するとあるが根拠となる法令等の記載はなく、本プログラムにおける契約は基本的にはケベック州で施行されている法令に従って解釈・管理されると規定されている。

b）海洋領域

■　国家戦略等

2004 年に Privy Council Office によって Securing an Open Society: Canada’s National Security Policy が策定された。これはカナダの国家安全政策で、海洋領域については、①責任の明確化と取り組み調整の強化、②ネットワーク化された Marine Security Operations Centres (MSOC)の設立、③カナダ軍、王立カナダ騎馬警察、カナダ沿岸警備隊の水上駐留と DFO（Department of Fisheries and Oceans：水産海洋省)の航空監視の強化④安全なフリート通信の強化、⑤米国との海洋安全保障協力の拡大および⑥海洋施設のセキュリティ強化、の 6 項目が掲げられている [138]。経済安全保障との関連性としては、輸送セキュリティの観点から、海洋の安全保障が重視されていることが挙げられる。

2010 年に DFO によって Maritime Security Framework が策定された。これは Canada’s National Security Policy に基づく海洋セキュリティの枠組みで、①Marine Security Operations Centres（MSOC）への参加、②艦隊の水上駐留、③Marine Communications and Traffic Services（MCTS）システムのネットワーク化が連邦執行機関と諜報機関の利益のための重点ポイントとして掲げられている [139]。経済安全保障との関連性として、輸送セキュリティの観点から、海洋の安全保障が重視されていることが挙げられる。

■　研究開発機関

カナダの海洋領域の研究開発関係機関としては、民生分野における研究では DFO、防衛分野では DND が主要な役割を担っている。DFO はカナダ政府が所管している政府機関の一つで、カナダ政府が所掌している水域の管理と保安を行っており、海洋領域における研究開発への資金提供も行っている。DND はカナダの国防政策に従って国家主権を守るための活動を行っており、国防に関係する研究開発も所管している（図 4.1-10）。

137 https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-18-00855778

138 https://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf

139 https://waves-vagues.dfo-mpo.gc.ca/library-bibliotheque/342662.pdf

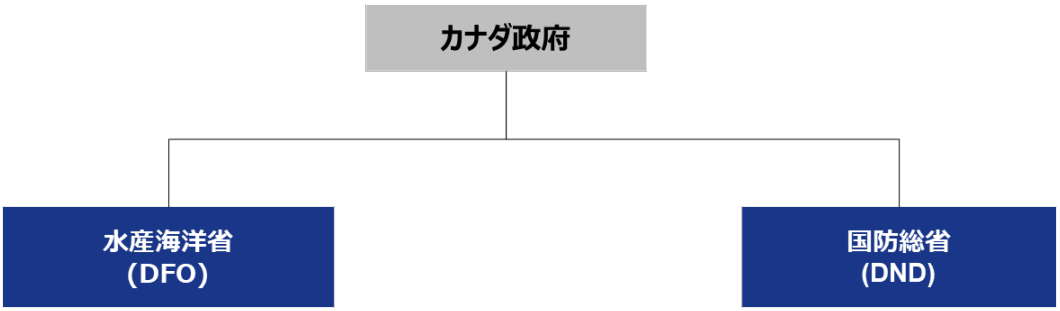


図 4.1-10　カナダにおける海洋領域研究開発の主要機関

■　　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　Oceans Management Contribution Program による船舶交通データシステムの開発支援 [140, 141]

DFO が所管するプログラムであり、カナダの海洋保護目標の取り組みに助成金を提供する Oceans Management Contribution Program のひとつとして、ダルハウジー大学の船舶追跡データと地図の公開システム（AISviz）構築を支援するものである。

情報保全については、情報アクセス法（Access to Information Act）に準拠するように求められている。

c）バイオ領域

■　　国家戦略等

2018 年に PHAC（Public Health Agency of Canada：カナダ公衆衛生局）によって Canadian Biosafety Guideline: Conducting a Biosecurity Risk Assessment が策定された。これはヒトおよび動物の病原体および毒素を取り扱い、保管する施設のバイオセキュリティリスクを評価するための方法論を示すガイドラインであり、事前準備、対象物、バイオセキュリティにおける脅威、評価、リスクレベルの決定、リスク許容度、改善、調査報告の各段階に方法論が示されている。経済安全保障との関連性としては、バイオセキュリティにおける脅威（盗難、誤用、転用、意図的な流出、偶発的な損失など）を防ぐためには適切な戦略を示すことが必要と述べられている。

■　　研究開発機関

カナダのバイオ領域の研究開発関係機関としては、民生分野における研究では PHAC、防衛分野では DND が主要な役割を担っている。PHAC はカナダ保健省が所管している機関の一つで、公衆衛生におけるリーダーシップ、パートナーシップ、イノベーションを通じて国民の健康を促進・保護することをミッションとし、感染症の予防や制御、公衆衛生上の緊急事態の対応、公衆衛生に関する政府間協力の強化や公衆衛生政策と計画への各国のア

140 https://www.dfo-mpo.gc.ca/oceans/funding-financement/management-gestion/terms-conditions-modalites-programme/index-eng.html

141 https://www.canada.ca/en/fisheries-oceans/news/2023/06/funded-projects-for-the-oceans-management-contribution-program.html

プローチの促進を行っている。DND はカナダの国防政策に従って国家主権を守るための活動を行っており、国防に関係する研究開発も所管している（図 4.1-11）。

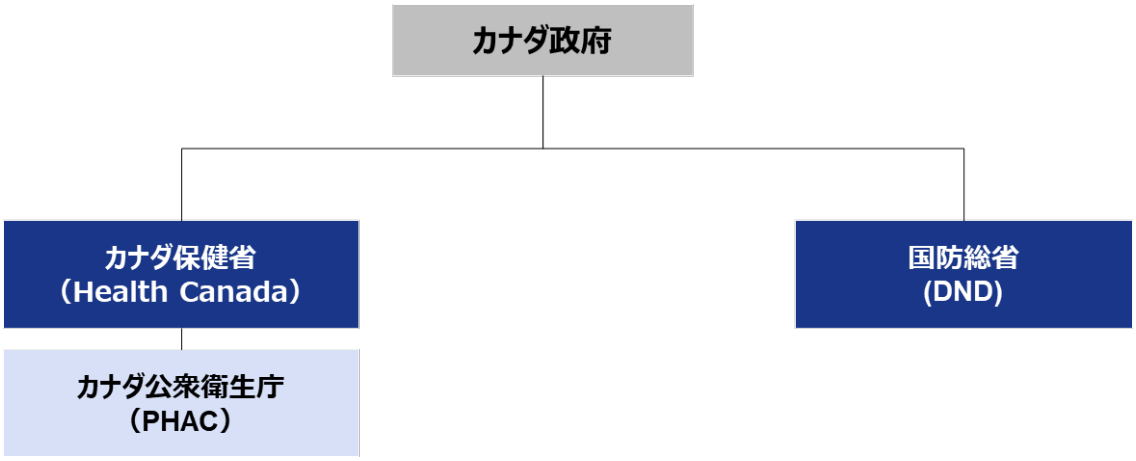


図 4.1-11　カナダにおけるバイオ領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Stabilized Whole Blood Product[142]

PHAC が所管するプロジェクトであり、HIV/AIDS に関連するカナダ公衆衛生庁の免疫学的品質評価および標準化 (QASI) 対策の一環として、保存培地中に安定化されたヒト赤血球および白血球を含む、分析済みの全血品質管理製品の調達を行っている。

受託者は、情報アクセス法(Access to Information Act)第 67.1 条、または州/準州レベルでの同等の条項に準拠することが求められる。

d）サイバー領域

■　国家戦略等

2018 年に PSC (Public Service Commission：公安省)よって National Cyber Security Strategy が策定された。これはサイバーセキュリティに関する国家戦略で、①政府機関におけるセキュリティの強化、②政府機関以外の重要サイバーシステムの保護のための連携、③サイバーセキュリティ確保のための支援、について述べられている [143]。経済安全保障との関連性としては、「サイバーセキュリティの強化はカナダのイノベーション及び繁栄のためには不可欠な要素である」と述べられている。

2022 年に ISED によって Canada’s National Quantum Strategy が策定された。これは量子分野における国家戦略で、3 本柱として、①基礎研究と応用研究の支援、②人材育成、③研究成果の商業化の支援、を掲げている。また、3 つの重要ミッションとして、①量子コンピューティングのハードウェアとソフトウェアの継続的な開発、展開、使用においてリーダーシップをとること、②安全な量子通信ネットワークと量子計算機暗号構想を構築

142 https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-edm-002-10005

143 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

すること、③量子センシング技術の開発・採用の実施、を掲げている[144]。経済安全保障との関連性としては、「量子科学と関連技術の成熟は、カナダの産業の競争力、技術的優位性において重要である」と述べられている。

■　研究開発機関

カナダのサイバー領域の研究開発関係機関としては、民生分野における研究では SSC（Shared Services Canada：シェアードサービスカナダ）、防衛分野では DND が主要な役割を担っている。SSC はカナダ政府が所管している政府機関の一つで、カナダ政府全体の情報技術サービスを統合・管理することを目的として 2011 年に設立され、ネットワークセキュリティの確保・エンタープライズツールの実装・アプリケーションプラットフォームの最新化等を実現することで、テクノロジーの強化を行うことを重要目標としている。DND はカナダの国防政策に従って国家主権を守るための活動を行っており、国防に関係する研究開発も所管している（図 4.1-12）。

図 4.1-12　カナダにおけるサイバー領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ TBIPS-SA: C.1 Strategic IT Security Planning and Protection Consultant, Level 3 [145]

SSC が所管するプログラムであり、SSC にて行われる SSC 変革プログラム・プロジェクトにおける非機密、機密、およびすべての指定領域における IT セキュリティ・サポートおよびサービス（サイバーセキュリティサブプログラム機能、IT セキュリティサービスサブプログラム、カナダ政府セキュリティインフラストラクチャサブプログラム機能、エンタープライズセキュリティ要件の定義と統合サービス機能）を提供することを求めている。

受託者は、セキュリティリスクへの対応として、DOS（Designated Organization Screening：指定組織審査）を受けている必要がある。

[144] https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy#s4

[145] https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-18-00844238

e）多義的技術

■　国家戦略等

カナダの多義的技術に関する研究開発について、DND では、DSST プログラム(Defence and Security Science and Technology (DSST) program：防衛・安全保障科学技術プログラム)を発表し、国防総省とカナダ軍メンバーの支援、仮想環境と物理環境での戦闘、先進的なプラットフォームと武器、指揮・制御・インテリジェンスの加速、北米の防衛、安全性とセキュリティの実現、組織の効率化、科学技術の進化という 8 つの戦略的重点分野を定めている[146]。

DND 傘下の DRDC (Defence Research and Development Canada：カナダ国防研究開発省)では、DSST プログラムで定められた研究開発分野の管理を実施する他、2017 年に DND が発表した SSE (Strong, Secure, Engaged) と呼ばれるカナダ軍強化政策に基づいて、2018 年に IDEaS (Innovation for Defence Excellence and Security：卓越した防衛と安全保障のためのイノベーション) を開始している。本プログラムでは、カナダ軍が直面している課題の解決を目的として、無人航空機、量子技術、エネルギー、情報通信、医療、海洋等の分野に、20 年間で防衛と安全保障のイノベーションに 16 億ドルを投資するものであり、国内および要件を満たせば民間企業や大学等の多くの研究開発機関が傘下することができる[147]。

■　研究開発機関

カナダの多義的技術に関する研究開発機関としては、DRDC が挙げられる。DRDC は 1947 年に設立された DND 傘下の機関であり、カナダの国防能力を向上させ、カナダ国民を保護し、国際平和と安全保障に貢献するため、国防に関連する幅広い科学技術の研究開発を主導し、実施する責任を負っている。DRDC は DSST プログラムや IDEaS の他にも科学技術 (S&T) と政策、作戦、情報との融合を通じて、自然災害、重大事故、犯罪、テロリズムを予測、予防、緩和、準備、対応、回復するカナダの能力を強化することを目的とした CSSP (Canadian Safety and Security Program：カナダ安全保障プログラム) 等の資金提供プログラムについても所管している[148,149]。

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Blood Biomarkers for Crush Injury/Crush Syndrome[150]

DND が所管するプログラムであり、挫滅損傷・クラッシュシンドロームの適切かつ迅速な診断につながる血液のバイオマーカー分析を行うことを求めている。

本プログラムでは、データ侵害については the Standard Acquisition Clauses and Conditions Manual に従い、受託者が全責任を負うこととなっている。

---

146 https://www.canada.ca/en/defence-research-development/corporate/publications/defence-st-strategy.html

147 https://www.canada.ca/en/department-national-defence/programs/defence-ideas.html

148 https://www.canada.ca/en/defence-research-development.html

149 https://science.gc.ca/site/science/en/canadian-safety-and-security-program

150 https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-edm-002-10005

・ Innovation for Defence Excellence and Security (IDEaS) - Innovation Networks: Micro-nets[151]

DND が所管するプログラム。持続可能な研究ネットワークの構築には時間がかかることを踏まえ、イノベーション・ネットワークは、科学技術に関する課題の 1 つまたは複数の側面について研究を行う小規模なネットワーク（マイクロネット）の創設を支援するための提案募集を行っている。マイクロネットとは、少なくとも 3 つの適格な組織・機関からなる学際的なチームであり、共通の関心を持つ科学技術課題の側面について学際的な研究を行う取組である。

プロジェクトにおける情報保全は、情報セキュリティ法やプライバシー法に従うように規定されている。

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして 17 件リストアップした（詳細は Appendix 1）参照）。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも 1 つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして 6 件抽出した（表 4.1-9）。

表 4.1-9 詳細調査を行う法令等のショートリスト

法令・ガイドライン等の名称	理由
Security of Information Act (SOIA)	機密情報のセキュリティ保護を目的とした法律のため
Policy on Government Security	安全保障方針として主要機関のセキュリティ管理について規定されているため
Export and Import Permits Act	安全保障上の懸念に対応する法令のため
Investment Canada Act	安全保障貿易に関する法律のため
Safeguarding Your Research	研究開発におけるセキュリティ保護が規定されたガイドラインのため
Intellectual Property Enforcement Guidelines	知的財産権の取扱に関するガイドラインのため

以下に表 4.1-9 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

[151] https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/innovation-networks/challenge/defence-applications-of-quantum-technologies/defence-applications-of-quantum-technologies-guide2023.html

a）Security of Information Act (SOIA)[152,153]

■　策定機関・策定時期

2021 年

■　策定の背景・目的

2021 年 12 月に the Official Secrets Act を修正し、情報セキュリティへの対応を新たに規定するもので、「特別運用情報 (Special Operational Information)」や「永久に守秘義務を負う者 (persons permanently bound to secrecy)」などの規定を導入することで、諜報活動に関する規定を更新し、機密情報のセキュリティ保護を目的としている。

■　適用範囲

カナダにおける機密情報を対象としており、対象となる情報やその情報にアクセスできる人物、違反した場合の罰則について「目的や範囲などの一般条項」「犯罪区分」などに区分して記載されている。

■　情報の分類

不正に開示されると政府に明確な損害を及ぼす機密情報を「特別運用情報」として規定している。

■　情報管理策

機密情報の保護方法を規定する組織的管理策と守秘義務を負う対象者を規定する人的管理策のみ記載されているため、物理的・技術的管理策は規定していない。

・　組織的管理策

不正に開示されると政府に明確な損害を及ぼす機密情報を「特別運用情報」として規定して保護する。「特別運用情報」には、カナダ政府に機密情報を提供する情報源の身元、軍事情報、情報収集方法および収集者の身元、これらの情報の保護方法などが含まれている。

・　人的管理策

カナダ安全情報局、王立カナダ騎馬警察などのセキュリティに関わる連邦政府機関を指定し、その職員および、必要に応じて、同機関での業務に従事する契約者を「永久に守秘義務を負う者」として規定する。対象者は退職後、契約終了後も守秘義務を負うものとされている。対象者による不正な情報開示は制裁の対象とされている。

■　罰則

同法に違反した場合、正式起訴による 14 年以下の懲役、または略式起訴による 12 か月

152 https://laws-lois.justice.gc.ca/eng/acts/o-5/

153 https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12323

以内の懲役または 2,000 カナダドル以下の罰金、あるいはその両方を科せられる可能性がある。

b) Policy on Government Security[154]

■ 策定機関・策定時期

2019 年

■ 策定の背景・目的

2009 年 1 月に発行された安全保障方針に代わる方針として発行され、金融行政法第 7 条に基づいて作成された。カナダ政府が信頼できるサービスを提供することや、情報、個人及び資産の保護を支援するために、政府のセキュリティ管理を効果的に行えるようにすることを目的としており、カナダ政府におけるセキュリティ管理について、各機関の役割について明記している。

■ 適用範囲

情報技術セキュリティの要件、慣行、および制御は、情報システムのライフサイクルのすべての段階を通じて定義、文書化、実装、評価、監視、および保守され、情報システムが情報を適切に保護し、許容可能な方法で使用され、政府のプログラム、サービス、および活動をサポートするために信頼できることを合理的に保証している。さらに、物理的セキュリティの要件、慣行、および管理は、個人、情報、および資産が適切に保護されていることを合理的に保証し、それによって政府のプログラム、サービス、および活動の提供をサポートするために、不動産および資材管理ライフサイクルのすべての段階を通じて定義、文書化、実装、評価、監視、および維持されることが規定されている。

■ 情報の分類

Policy on Government Security の目的を達成するための具体策として策定された Directive on Security Management[155]において、以下のように規定されている。

(Policy on Government Security で規定される保全対象情報の分類)
- Top Secret：不正な開示が国益に著しく重大な損害を与えることが合理的に予想される場合、非常に限られた量の情報に適用される。
- Secret：不正な開示が国益に重大な損害を与えることが合理的に予想される場合に適用される
- Confidential：不正な開示が国益に限定的または中程度の損害を与えることが合理的に予想される場合に適用される

■ 情報管理策

セキュリティ管理において求められる役割を示す組織的管理策のみ記載されているため、

154 https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578

155 https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611

人的・物理的・技術的管理策は規定していない。

・　組織的管理策

各政府機関でのセキュリティ管理において求められる主な役割について述べられている。

セキュリティ機関の副長官においては、セキュリティガバナンスの確立やセキュリティ・クリアランスの拒否・取り消し・一時停止、内外の利害関係者への潜在的な影響を考慮したセキュリティ要件の特定、毎年見直しがなされる部門別セキュリティ計画の承認とセキュリティ要件を満たすための戦略の設定が求められる。カナダ保安情報局においては、保安検査サービスの提供、安全保障に対する脅威を調査・分析し、関連する報告や助言を政府に提供することが求められる。通信セキュリティ施設においては、通信セキュリティ（COMSEC）及び国家信号諜報機関（SIGINT）としての機能、IT セキュリティに関連する技術的事項におけるリーダーシップ、政府にとって重要な電子情報及び情報インフラの保護が求められる。国防省においては、科学技術安全保障研究、防衛情報、軍事システムに対する安全保障上の脅威の調査、立憲政治の継続性と国内のテロ対策に関連した公安への支援提供が求められる。枢密院事務局においては、内閣信任の安全保障のための政策の方向性の確立、個人のセキュリティ・クリアランスに関するセキュリティインテリジェンス審査委員会の勧告に関するアドバイスの提供が求められる。カナダ公安局においては、国家安全保障および国家安全保障問題に関する調整と戦略的政策立案の主導、政府全体、政府間、重要インフラ、または国家に影響を与える可能性のある複数の連邦省庁が関与するセキュリティイベントに関連する調整、情報共有、および状況認識のための運用上のリーダーシップの提供が求められる。財務省事務局においては、政府の安全保障に関連するすべての事項についての政策のリーダーシップ、助言、ガイダンスの提供、政府全体に影響を与える可能性のあるセキュリティイベントを管理するための戦略的な政策監視と調整が求められる。

■　罰則

記載なし

c）Export and Import Permits Act[156]

■　策定機関・策定時期

1985 年（輸出入許可法）

■　策定の背景・目的

外国勢力やテロリストグループによるスパイ行為や国家への脅迫などの国家安全保障上の懸念に対応するために制定された法律である。

■　適用範囲

情報の通信又は受信についての定義が以下のように規定されている。

（Export and Import Permits Act における情報通信・受信の定義）
・　伝達または受領の定義には、全部または一部を問わず、スケッチ、計画、モデル、記

[156] https://laws.justice.gc.ca/eng/acts/O-5/index.html

事、メモ、文書または情報自体、またはそれらの内容、効果、または説明のみが伝達または受信されているかどうかにかかわらず、通信または受信が含まれる
- スケッチ、計画、模型、記事、メモ、または文書の取得または保持の定義には、スケッチ、計画、モデル、記事、メモ、または文書の全部または一部をコピーすること、またはコピーさせることが含まれる
- スケッチ、計画、モデル、記事、メモ、または文書の通信の定義には、スケッチ、計画、モデル、記事、メモ、または文書の転送または送信が含まれる

■　情報の分類

情報の通信・受信の定義については規定されているが、情報の部類については規定していない。

■　情報管理策

不正な情報伝達を防ぐための組織的管理策と秘密保持を科される対象者を規定する人的管理策のみ記載されているため、物理的・技術的管理策は規定していない。

・　組織的管理策

情報の不正な伝達として以下の行為を禁じている。

（Export and Import Permits Act で規定される情報の不正伝達行為）
- 暗号語、パスワード、スケッチ、計画、モデル、記事、メモ、文書または情報を、通信する権限を与えられた者、または国家の利益のためにそれを伝達する義務がある者以外の者に伝達すること
- 外国勢力の利益のために、又は国家の安全若しくは利益を害するその他の方法により、自己の所有する情報を使用すること
- スケッチ、計画、模型、記事、メモ、または文書を保持する権利がない場合、または保持する義務に反する場合、または返還または廃棄に関して合法的な当局によって発行されたすべての指示に従わない場合に、スケッチ、計画、モデル、記事、メモ、または文書を所有または管理して保持すること
- 秘密の公式コードワード、パスワード、スケッチ、計画、モデル、記事、メモ、文書、または情報に合理的な注意を払わないこと、安全を危険にさらすような行為をすること

・　人的管理策

永久に秘密保持を求められる対象者として以下が挙げられている。

（Export and Import Permits Act で規定される永続的に秘密保持が求められている対象者）
- 国家安全保障情報審査局の新旧メンバー
- 国会議員の国家安全保障情報委員会の新旧メンバー
- 第 10 条（1）（特別な情報へのアクセスを許可されている者）または第 11 条（2）（第 10 条（1）で指名されていないが同項に基づく規則で指名された者）でセキュ

リティ・クリアランスを付与された者

■　罰則

国家の利益を損なう恐れのあるテロリストグループと情報の通信を行った場合、終身刑に処される可能性がある。また、国家の経済的利益や国際関係、国家安全保障に損害を与える恐れのある外国勢力に営業秘密を伝達した場合、10 年以下の懲役に処される可能性がある。

d）Investment Canada Act[157, 158]

■　策定機関・策定時期

2021 年

■　策定の背景・目的

海外資本によるカナダ国内への直接投資（新規事業および既存事業の買収）を規制する法令である。国家の経済成長、雇用機会の奨励および国家安全保障の保護を目的としている。非カナダ市民（個人、政府、機関）による投資は、イノベーション・科学・経済開発省に通知または審査申請を行う必要があり、当局が必要と認める場合、海外投資がもたらす国家安全保障への影響を審査する。

■　適用範囲

海外資本によるカナダ国内への直接投資（新規事業および既存事業の買収）を対象としており、「目的や範囲などの一般条項」「組織と義務」「免除」「通知」「レビュー」「国家安全保障に有害な投資」「規則と推定」「一般」「救済策、犯罪および罰則」「移行、修正および開始」に項目分けされて説明がなされている。

■　情報の分類

海外資本による直接投資を規制する方法については規定されているが、情報の部類については規定していない。

■　情報管理策

海外資本による投資の際に必要な情報提供を規定する組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

海外資本による新規事業および既存事業に対する投資の際には、イノベーション・科学・経済開発省への通知が必要である。海外資本による国内の既存事業の買収（議決権またはアセットの取得）については、同省が審査を行う。また、同省大臣が国家安全保障に

157 https://www.jetro.go.jp/world/n_america/ca/invest_02.html

158 https://laws-lois.justice.gc.ca/eng/acts/I-21.8/index.html

有害な投資であると合理的に判断した場合、非カナダ市民（個人、政府、機関）に対する審査命令が可能である。その場合、対象者は必要情報の提供が必要である。

・

■　　罰則

非カナダ市民が同法を順守せず、大臣からの是正指示を受けた後にも改善されなかった場合、上級裁判所の裁定に基づき、1 日当たり 10,000 カナダドルを超えない罰金を科せられる可能性がある。

e）Safeguarding Your Research[159]

■　　策定機関・策定時期

ISED[160]　2024 年

■　　策定の背景・目的

カナダ政府による研究セキュリティに関するガイドラインの全般的な概説である。研究機関を対象として、研究保護の必要性や研究に関するセキュリティリスクを示し、それに対処するためのトレーニングを提供している。加えて、研究パートナーシップの開発、評価、資金提供における国家安全保障の考慮事項ガイドラインも提供している。

■　　適用範囲

カナダにおける研究セキュリティのあり方を対象としており、「研究セキュリティの一般情報」「研究セキュリティ導入のためのガイドラインとツール」について説明がなされている。

■　　情報の分類

研究セキュリティの取り組みについては記載されているが、情報の部類については規定していない。

■　　情報管理策

セキュリティを担保するための手法を示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

研究セキュリティの一般情報では、セキュリティ保護の必要性、リスクを負うのは誰か、リスクとは何か、トレーニングコース、研究セキュリティ、研究保護、カナダ政府と大学作業部会、国際研究セキュリティリソース、バイオセキュリティ等を提供している。研究セキュリティ導入のためのガイドラインとツールでは、研究パートナーシップの国家セキ

159 https://science.gc.ca/site/science/en/safeguarding-your-research

160 https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships

ュリティガイドライン、リスクプロファイルの評価、オープンソースデューデリジェンス実施ガイダンス、セキュリティリスクの軽減、研究機関と基金提供者へのガイダンス、ケーススタディ、サイバーセキュリティを提供している。

また、指針となる「研究パートナーシップの国家セキュリティガイドライン」では、以下を提供している。

（研究パートナーシップの国家セキュリティガイドラインの概要）

- 原則：政府は、学問の自由、組織の自律性、表現の自由、公平性、多様性、包括性、公益のための研究、透明性、完全性および協力の原則を研究機関と共有する
- 研究パートナーシップにおける国家セキュリティリスク：カナダ国家・経済に混乱もたらす恐れがある国家や集団の軍事、安全保障、諜報能力の進歩に寄与する可能性、諜報活動、不正な知識の移転が、リスクとして挙げられている
- リスク要素：研究分野（二重用途、軍事、諜報、監視機能の研究、悪用されるとカナダの経済、社会、重要インフラに悪影響を及ぼす可能性がある研究や成果、重要データおよびインフラへの不正アクセス）、パートナーのステータス（外国政府、軍、その代理人等への情報流出の可能性の有無）が挙げられている
- リスクの特定と軽減：リスク評価フォーム等を使用した検証を推奨する。リスク軽減のため、パートナーの動機の検証、サイバーセキュリティ、データ管理の確保、研究成果の権利契約を結ぶ等を実施する
- 導入：カナダ自然科学・工学研究会議(NSERC)への申請を通じて研究助成金の提供を管理することで、国家安全保障を確保する
- Annex A - 機密性の高い研究分野：輸出管理による規制を受ける、二重用途分野、研究での重要インフラや大型データの取扱い等が挙げられている
- Annex B - パートナーリスク：カナダ安全情報局やサイバーセキュリティセンターからの情報や、パートナーのステータス（国有機関である等）を検討する

■ 罰則

記載なし

f) Intellectual Property Enforcement Guidelines[161]

■ 策定機関・策定時期

Competition Bureau 2023 年

■ 策定の背景・目的

カナダ政府の競争法における知的財産法（IP 法）の取扱い方針に関する専門家向けのガイドラインで、効率的な経済の推進を目的とする IP 法と競争法のバランスについて、政府の立場の明確化を行うものである。

[161] https://ised-isde.canada.ca/site/competition-bureau-canada/en/how-we-foster-competition/education-and-outreach/intellectual-property-enforcement-guidelines#sec02

■　適用範囲

カナダにおける IP 法のあり方を対象としており、「イントロダクション」「IP 法と競争法の概要」「IP 法と競争法の仲立ち」「IP が関わる法の適用」「IP の文脈における分析のフレームワーク」「競争ポリシーの擁護」「IP への競争法の適用」に項目を分けて説明がなされている。

■　情報の分類

IP 法の取り扱い方針については記載されているが、情報の部類については規定していない。

■　情報管理策

IP 法の取り扱い方針を示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

本ガイドラインでは IP 法について以下が示されている。

（IP 法における主な組織的情報管理策）

- IP 法と競争法の概要：保護の対象となる IP 権（特許、商標、著作権、工業意匠、集積回路のレイアウト設計、植物育種者の権利、営業秘密や未登録商標）および競争法の概説を行う
- IP 法と競争法の仲立ち：私有財産権は市場経済の基礎であるという立場から、IP 法による権利の保護と競争法による競争市場促進の双方の重要性を挙げている
- IP が関わる法の適用：IP が関わる（市場）競争の妨害に関する分析に必要な要素として、関連市場の定義、市場支配力、競争制限効果、効率および事業の正当性を挙げている
- IP の文脈における分析のフレームワーク：関連市場の定義、市場支配力、競争制限効果、効率および事業の正当性について競争局の検討方法を示す
- 競争ポリシーの擁護：競争を促すために当局の介入が可能であることおよび事例を示している
- IP への競争法の適用：IP が関わる仮説例（IP 権の侵害、価格協定、独占的ライセンス、買い手よる差し押さえ、独占契約、生産ロイヤリティ、特許プール契約等）を示す

■　罰則

記載なし

（4）英国

1）基本情報

- 政治体制：議員内閣制
- 人口：約 6,703 万人[162]（2021 年）
- 名目 GDP：約 3.1 兆米ドル[163]（2022 年）、 実質：約 3.0 兆米ドル[164]（2021 年）
- 研究開発予算：140 億ポンド[165]（2021 年）

■ 政治動向

英国はイギリス君主を元首とする立憲君主制であり、内閣が議会の信任に基づいて政治を行う議員内閣制を採用している。また、G8 や NATO に所属しており、国連でも安全保障理事会の常任理事国を務めていることなどから国際的な発言力を有している一方で、2020 年 1 月に EU から離脱したことにより貿易や出入国管理に影響が及んでいる。

2022 年 10 月、与党・保守党の新党首に選出されたリシ・スナク氏が首相に就任し、新内閣が発足した。国営医療サービスの強化や教育の改善、治安の向上、国境の管理、環境の保護、英国軍の支援、地域活性化、英国の EU 離脱の機会活用などの実現を通じて、経済の安定性と信頼性を目指すとしている。

■ 経済動向

2022 年の名目 GDP で世界 6 位に位置しており、2022 年の実質 GDP 成長率は 4.1%となっている[166]。自動車、航空機、電気機器、エレクトロニクス、化学、石油、ガス、金融を主要産業としており、自動車、医薬品及び医療用品、発動機などを主な貿易品目としてドイツ、米国、オランダ、中国、フランスなどと取引している[167]。

新型コロナウイルス禍からの復興やロシアによるウクライナ侵攻を背景にしたエネルギー価格の高騰を要因としてインフレ率は上昇しており、国家統計局（ONS）によると、2022 年の消費者物価指数（CPI）は 9.1％と高い水準となっている。英国政府は 2022 年 10 月から家計のエネルギー価格の負担軽減に向けた支援措置を導入するとともに、イングランド銀行も 2021 年 12 月以降利上げを継続している。

---

162 https://www.jetro.go.jp/world/europe/uk/basic_01.html
163 https://www.globalnote.jp/post-1409.html
164 https://www.globalnote.jp/post-1332.html
165 https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgovernmentexpenditureonscienceengineeringandtechnology/2021#:~:text=1.-,Main%20points,%C2%A314.5%20billion%20in%202021.
166 https://www.jetro.go.jp/world/europe/uk/basic_01.html
167 https://www.mofa.go.jp/mofaj/area/uk/data.html

■　社会動向 [168, 169, 170]

英国の人口は約 6,703 万人（2021 年時点で世界 22 位）で、2011 年比で 1.1%増加している。国家統計局（ONS）によると、2020 年半ば時点で 85 歳以上の人口は 170 万人（英国人口の約 2.5%）で、2045 年半ばまでにほぼ 2 倍の 310 万人に増加し、高齢化が進むと予測されている。また、英国では 2018 年に世界ではじめて孤独担当大臣を設置し、国レベルで高齢者をはじめとする孤独問題への対応を進めている。

■　技術動向 [171, 172]

2023 年 3 月、英国政府は 2030 年までに英国を世界の科学技術大国として確固たる地位を築くための政府計画（The UK Science and Technology Framework）を公表し、5 つの重要技術（人工知能、工学生物学、次世代通信技術、半導体、量子技術）を特定している。

また、英国政府は 2023 年 7 月、最先端の科学技術の開発を支援すべく、「リサーチ・ベンチャーズ・カタリスト基金（Research Venture Catalyst、RVC）」を設立した。RVC は、最大 5,000 万ポンドの政府投資により、英国の科学、研究、イノベーションに対する民間および慈善活動の支援がさらに促進するとしている。

英国における研究開発は、英国政府内の科学に関連する政策と助言を提供する総合科学技術会議（Council for Science and Technology：CST）と政府科学局（UK Government Office for Science：Go Science）が掲げる全体方針の下、各政府省庁及び関連する公共機関が予算を民間の研究実施主体等に配分して実施される（図 4.1-13）。

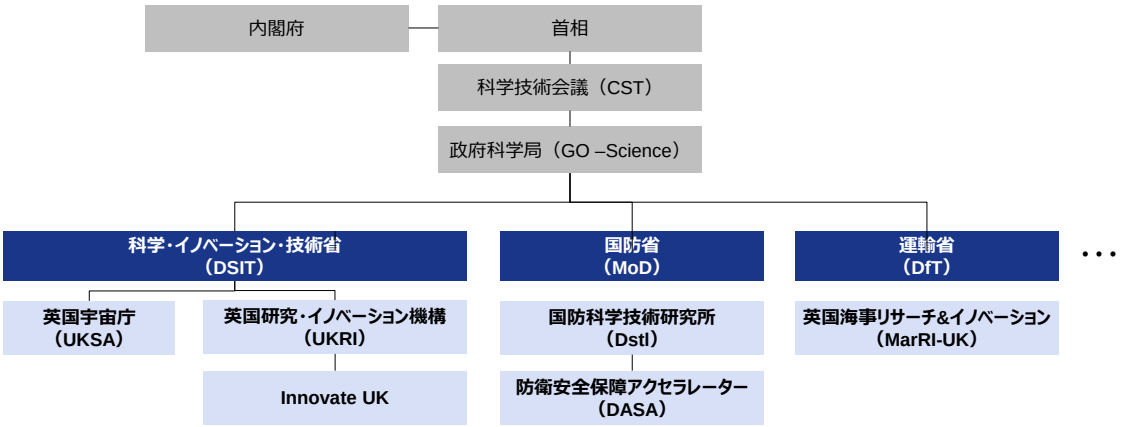


図 4.1-13　英国の研究開発に係る主な政府関連機関

168 https://www.globalnote.jp/p-cotime/?dno=9230&c_code=826&post_no=13021

169 https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/bulletins/annualmidyearpopulationestimates/latest#population-estimates-data

170 https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationprojections/bulletins/nationalpopulationprojections/2020basedinterim

171 https://www.gov.uk/government/publications/uk-science-and-technology-framework/the-uk-science-and-technology-framework#identifying-critical-technologies

172 https://www.gov.uk/government/news/game-changing-fund-opens-in-uk-to-boost-science-and-tech-research

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

英国では公務秘密法（Officials Secret Act 1911, 1920, 1939 and 1989）[173]により、政府の有する秘密漏えい行為等に対する刑事制裁を科しており、同法に基づき国内のスパイ活動の防止が図られてきた。その後、2023 年国家安全保障法(National Security Act 2023)[174]が策定、1911 年、1920 年および 1939 年公務秘密法が廃止され、スパイ行為、政治制度への干渉、妨害行為に対する国家安全保障の強化が図られている。なお、同法ではスパイ活動を保護された情報の取得・開示及び外国の諜報機関の支援と定義している。

英国では、2000 年以前は積極的に政府が管理する情報の公開は行っていなかったが、2000 年に情報自由法（Freedom of Information Act 2000）[175]が策定され、政府、議会、地方公共団体等の公的部門が保有する情報へのアクセスする手段が規定された。

2013 年には、セキュリティポリシーのフレームワーク（Security policy framework）[176]を策定し、英国政府の資産（人材、情報、インフラストラクチャ）を保護するために必要な標準、ベスト プラクティスのガイドライン、アプローチを示している。同フレームワークでは、機密性に従って情報を識別および評価し、適切な保護を推進するために、政府セキュリティ分類ポリシー （Government Security Classifications Policy：GSCP）[177]で定義される３つの機密性レベル（OFFICIAL、SECRET、TOP SECRET）及びそれぞれに紐づく個別のセキュリティの取り決めに基づいて運用されることが示されている。

上記の他、デジタル技術の進展に伴うサイバー空間上でのリスク増大への対応として、いくつかのサイバーセキュリティ関連法規制が規定されている。例えば、ネットワークおよび情報システム規則（2018 年 NIS 規則）[178]では、クラウドサービスプロバイダーや公共サービスプロバイダーにセキュリティ義務を課すとともに、重大なサイバーセキュリティインシデントが発生した場合には遅滞なく Ofcom(Office of Communications:英国情報通信庁)に報告することを義務付けている。また、英国のすべての携帯通信会社のサイバー攻撃に対するネットワークセキュリティを規制する目的で 2021 年電気通信（セキュリティ法）[179]が策定されている。

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

英国では 2021 年に、国家安全保障を脅かす可能性がある、外国企業や投資家による英国企業に対する合併・買収などについて、一定の条件を超える場合、事前に政府への届け出を義務付け、政府が調査・介入できることを強化する 2021 年国家安全保障・投資法（National

173 https://www.legislation.gov.uk/ukpga/1989/6/contents
174 https://www.legislation.gov.uk/id/ukpga/2023/32
175 https://www.legislation.gov.uk/ukpga/2000/36/contents
176 https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework
177 https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html#definitions-for-official-secret-and-top-secret
178 https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
179 https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted

Security and Investment（NS&I）Act 2021）を策定している。

また、国家安全保障・投資法の制定に先立ち、2020 年 6 月に安全保障やメディア寡占、金融、公衆衛生、特定技術（軍民両用技術、コンピュータハードウエア、量子技術、AI、先端材料、暗号化認証）において重要な公益が損なわれると判断される合併・買収について、政府に介入権限を与える「2002 年企業法（Enterprise Act 2002）[180]」改正規則が施行されている。

貿易規制の側面では、2008 年輸出管理指令（Export Control Order 2008）[181]や 2018 年制裁・資金洗浄防止法（Sanctions and Anti-Money Laundering Act 2018）[182]において、貿易統制対象品目や軍事品の輸出、供給・配送、使用を可能とすること、技術移転の禁止、軍事品と軍事技術に関連する技術的支援や金融サービス、他国同士の間の仲介サービスを提供することの禁止が規定されている。

[180] https://www.legislation.gov.uk/id/ukpga/2002/40

[181] https://www.legislation.gov.uk/uksi/2008/3231/contents/made

[182] https://www.legislation.gov.uk/ukpga/2018/13/contents

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　　国家戦略等

2021 年 9 月、英国政府は科学技術省（DSIT）と国防省（MoD）が共同で宇宙領域における民間防衛戦略を組み合わせた、国家宇宙戦略（National Space Strategy：NSS）[183]を発表した。同戦略には今後 10 年間の宇宙戦略ビジョンと政策フレームワークが定められており、合わせて 100 億ポンド以上の資金提供計画が示されている（図 4.1-14）。

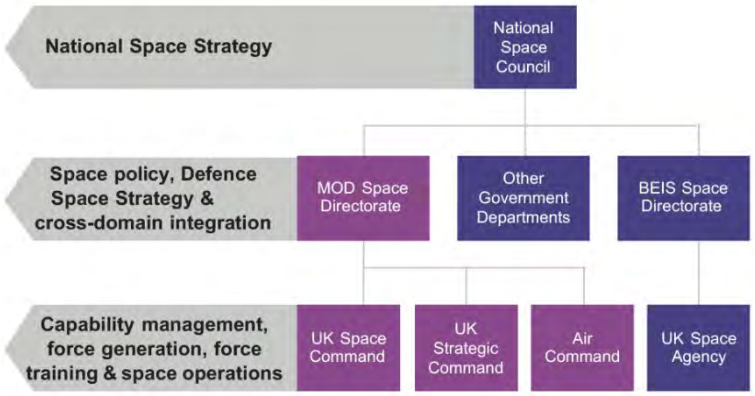


図 4.1-14　英国国家宇宙戦略と関連政策・機関の関係

NSS では、宇宙領域および技術は英国の安全保障と回復力にとって不可欠であるとともに、戦略的優位性と軍事作戦の成功の基礎であり、重要な国家インフラ（CNI:Critical National Infrastructure）の一部として定義されている。また、2021 年国家安全保障および投資法（NSI 法）においても、国家安全保障上の懸念が生じやすい 17 分野の一つとして衛星・宇宙技術を定めており、英国の重要領域・技術の一つとして認識されていると考えられる。

また宇宙領域に関する法制度としては、宇宙物体の打上げ・運用及び宇宙空間における活用について規定した 1986 年宇宙活動法の内容を拡充し、宇宙での商業活動の拡大及び宇宙港事業に関する規制の枠組みを定める 2018 年宇宙産業法が 2018 年に制定された。同法は、イギリスにおける宇宙飛行活動及び宇宙港事業に関して、免許制度を設けるもので、宇宙飛行活動を行うには「事業者免許」、宇宙港事業を行うには「宇宙港免許」が必要となる [184]。

■　　研究開発機関

英国における宇宙関連の研究開発を主導している政府機関としては、DSIT 及びその所管機関の一つである英国宇宙庁（UKSA）[185]が挙げられる。DSIT は英国の科学、研究、技術成果の奨励・開発・管理責任を負っており、2023 年 11 月には、DSIT が中心となり、韓国と科学技術協定を締結されているが、その中で宇宙開発においても 2 国間で連携していくことが示されている。UKSA は国家宇宙戦略の実現に向けて宇宙分野への投資を行う中心的な機関

183 https://www.gov.uk/government/publications/national-space-strategy
184 https://dl.ndl.go.jp/view/download/digidepo_11117156_po_02760104.pdf?contentNo=1
185 https://www.gov.uk/guidance/uk-space-programmes-and-missions

として位置付けられており、以下をはじめとする様々な宇宙関連のプログラムを所管している。

（UKSA が所管する主なプログラム）
- LaunchUK：
  英国宇宙分野の小型衛星および準軌道飛行市場をサポートする衛星打ち上げプログラム
- Innovation プログラム：
  高リスクのプロジェクト開発に共同で資金を提供する国家宇宙イノベーションプログラム（NSIP）、革新的な宇宙技術の研究開発をサポートする Enabling Technologies プログラム、新しい宇宙技術の設計と飛行を目的とした General Support Technology プログラム、測位、ナビゲーション、タイミング技術の研究を支援する Navigation Innovation Support プログラム（NavISP）が含まれる
- Discovery プログラム：
  宇宙ミッションのための科学ペイロードとデータ処理施設の設計、開発、運用に資金を提供する宇宙科学プログラムと、微小重力やその他の宇宙環境研究プラットフォームを使用した実験をサポートする宇宙探査プログラムが含まれる
- その他のプログラム：
  多岐にわたり、環境モニタリングのための地球観測、国際協力促進のための ESA 技術調和、重要な衛星ナビゲーションおよびタイミングサービスを提供するための宇宙ベースの測位、ナビゲーションおよびタイミングプログラム、および電気通信システムの先端研究（ARTES）プログラムなどがある

宇宙領域では科学技術の他、安全保障・防衛の側面からも研究開発が行われており、MoD および MoD が所管する国防科学技術研究所（Defence Science and Technology Laboratory：Dstl）や国防・セキュリティ促進機構（Defence and Security Accelerator：DASA）が主導している。

Dstl は MoD の執行機関として MoD および政府全体に機密性の高い専門的な科学技術サービスを提供しており、そのスコープには先駆的な宇宙技術開発を含んでいる。また、DASA は英国の繁栄を支援するために活用可能なイノベーションを見つけ資金を提供することを目的とした MoD の管轄機関であり、Dstl とも連携し、宇宙領域における軍事と民生の両方の可能性を強化し保護する将来の宇宙技術の開発を目的とした Space to Innovate キャンペーンなどを実施している。

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

- National Space Innovation Programme（NSIP）[186]

UKSA が所管するプログラムで、英国の宇宙セクターに、気候変動と戦うための衛星データの使用や軌道上のアプリケーションをより持続可能にするためのサービス提供などの課題に取り組む、斬新で価値のある商業的イノベーションを開発する機会を提供することを目的としている。2020 年の試験打ち上げ以来、NSIP は英国の組織に 2,500 万ポンドを超え

[186] https://www.gov.uk/government/publications/national-space-innovation-programme-kick-starter-open-call-call-1

る資金を提供しており、その中には 2023 年 6 月に打ち上げられた初の中波長赤外線(MWIR)衛星の開発も含まれる。

本プログラムの補助金交付契約書によると、情報保全や安全保障に関連して準拠が求められる法令等としては、いずれも宇宙領域に特有のものは確認できないものの、以下のような規程が定められている。

（NSIP における情報取扱に関連する法令等）
- UK GDPR
- 2018 年データ保護法（DPA）
- 2000 年情報自由法（FOIA）
- 2014 年環境情報規則（EIR）

b）海洋領域

■ 国家戦略等

英国では 2022 年、運輸省（DfT）、環境・食糧・農村地域省（DEFRA）、外務・英連邦・開発省（FCDO）、内閣府及び MoD が共同で、今後 5 年間の海洋安全保障に対する英国のアプローチを定めた、海洋安全保障のための国家戦略（National Strategy for Maritime Security：NSMS）[187]を発表しており、同戦略の中で現在の海洋安全保障上の課題を特定するとともに、現在および将来における課題に対処するための取組方針について示している。

（NSMS で定めている５つの戦略的目標）
1. 国家の保護（Protecting our homeland）：国境、港湾、インフラストラクチャのために、世界で最も効果的な海上安全保障のフレームワークを提供する DEF
2. 脅威への対処（Responding to threats）：世界をリードする能力と専門知識を駆使し、新たな脅威に対応するため、システム全体で対応する
3. 繁栄の確保（Ensuring prosperity）：国際海運の安全を確保し、物資、情報、エネルギーの円滑な輸送を実現することで、継続的な世界的発展と経済的繁栄を支える
4. 価値観の尊重（Championing values）：国連海洋法条約(UNCLOS)を、海洋におけるあらゆる活動の法的フレームワークとして支持する
5. 安全で強靭な海洋の支援（Supporting a secure, resilient ocean）：効果的に管理され、清潔で、健康的で、安全で、生産的で、生物学的に多様な海洋を目指す

■ 研究開発機関

英国の海洋領域で研究開発を実施している政府機関としては、革新技術の開発に取り組んでいる Innovate UK、国家安全保障の側面から技術開発を担っている Dstl や DASA、主に海事分野の脱炭素化などのグリーン技術の開発を推進している運輸省（DfT）や同傘下の英国海事リサーチ&イノベーション（MarRI-UK）などが挙げられる。

[187] https://www.gov.uk/government/publications/national-maritime-security-strategy

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

全般的には、NSMS において国際海洋法条約（UNCLOS）の遵守を明言していることから、指定される海域区分で実施する研究開発活動においては、同条約の順守が前提となると考えられる。また、UNCLOS を補完するガイドラインとして Marine Science Research（MSR）Guidance が公表されており、英国およびその王室属領／海外領土内で海洋科学調査（MSR）を希望する英国以外の船舶と、海外での調査を希望する英国船舶両方を対象として必要な手続きを解説している。

・ marine and maritime in the Great South West - R1 CR&D[188]

Innovate UK が所管する英国でも著名な海洋・海事セクターが存在するグレート・サウス・ウエストを対象としたイノベーションクラスターへの資金提供プログラムで、海の安全性を向上させる破壊的テクノロジーや最先端のセンサー・通信技術の開発に焦点を当てている。

公募要領には主に個人情報に関する取扱いに関する法令等や補助金助成に係る準拠法が示されている他、提案の適格性の検討資料としてオーシャン・フューチャーズ・イノベーションの目論見書[189]や運輸省の政策文書である Maritime 2050：navigating the future[190]などが示されている。

（marine and maritime in the Great South West - R1 CR&D で遵守が求められる法令等）
・ UK GDPR
・ 2018 年データ保護法（DPA）

c）バイオ領域

■　国家戦略等

2023 年 6 月に、英国政府はバイオセキュリティ戦略 2023 [191]を公表し、2030 年までに責任あるバイオイノベーションの実践を促進し、多義的な側面を持つバイオテクノロジーの輸出規制を評価・更新を行うことで国際的懸念に対処するとともに、バイオテクノロジーの悪用を防止することが示されている。

（英国バイオセキュリティ戦略で示された主な取組）
・ 脅威やリスクをリアルタイムで監視する「生物脅威レーダー」を立ち上げること
・ バイオセキュリティ戦略担当の専任大臣を設置し、国会に定期的に報告すること
・ 国内および国際的な演習を定期的に実施すること
・ 英国バイオセキュリティ・リーダーシップ協議会（UK Biosecurity Leadership

188 https://apply-for-innovation-funding.service.gov.uk/competition/1755/overview/ae818f18-b18f-48bc-a9a1-a5de6c7bb5c7

189 https://oceanfutures.co.uk/wp-content/uploads/2022/01/Ocean-Futures-Prospectus.pdf

190 https://www.gov.uk/government/publications/maritime-2050-navigating-the-future?_ga=2.133390542.1969874031.1704851518-717689553.1688814473

191 https://www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html

Council）を設立し、現場の企業や組織と連携すること

他方、英国イノベーション戦略[192]において技術戦略上の重要技術として「バイオインフォマティクスとゲノミクス」や「工学生物学（Engineering Biology)」が示されており、今後、バイオセキュリティに留意しつつも、同領域の研究開発に対しては積極的政府投資が行われるものと想定される。

■　研究開発機関

英国のバイオ領域の政府系研究開発機関としては、UKRI 傘下の生物科学研究会議（Biotechnology and Biological Sciences Research Council：BBSRC）[193]や医学研究会議（Medical Research Council ：MRC）[194]が挙げられる。前者は英国におけるバイオサイエンス領域の主要な政府資金提供者であり、持続可能な食料生産、気候変動、健康的な高齢化などの地球規模の課題への取り組みに貢献する画期的な発見を提供し、バイオベースのソリューションを開発することをミッションとしている。後者は、疾患領域における生物医学の領域にわたる研究をサポートしており、NHS（英国保険サービス）などと緊密に連携して英国国民の健康改善に取り組みことをミッションとしている。

その他、MOD 系列の Dstl や DASA においてもバイオ領域の研究開発等に取り組んでいる。特に Dstl は、国際生物安全保障プログラム（IBSP）を所管しており、生物兵器能力の開発を模索している国家やテロリストが生物兵器を脅かす可能性のある物質や専門知識を取得し、使用するリスクを最小限に抑えることを目的に取組を進めている[195]。

（IBSP のミッション）
- パートナー国における効果的な病原体セキュリティ、バイオセーフティ、診断および疾病監視能力の開発支援
- 科学の「悪用」と科学の「デュアルユース」に関する国際的な懸念への対処
- 不拡散の意識を強化
- 協力的な生物学的セキュリティ活動を通じて、技術協力、援助、持続可能な能力構築の機会改善

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ China UK One Health research for epidemic preparedness and AMR[196]

MRC、BBSRC 等が主導する英中共同の AMR（薬剤耐性）と蔓延可能性のある感染性病原体に関する研究プログラム。両国の研究者の交流を支援することでパートナーシップ強化を図ることもミッションの一つとなっている。中国サイドの共同出資者としては中華人民共和

192 https://www.gov.uk/government/publications/uk-innovation-strategy-leading-the-future-by-creating-it/uk-innovation-strategy-leading-the-future-by-creating-it-accessible-webpage
193 https://www.ukri.org/councils/bbsrc/
194 https://www.ukri.org/councils/mrc/
195 https://www.gov.uk/government/publications/uk-biological-security-strategy/uk-biological-security-strategy-html
196 https://www.ukri.org/opportunity/china-uk-one-health-research-for-epidemic-preparedness-and-amr/

国科学技術部（MoST)が参画している。

国際共同研究の位置づけであることからUKRI Trusted Research and Innovation（TRI）[197]原則や国家安全保障投資法（NSI法）[198]への準拠が求められる。

原則、参加者は学術研究者を想定しているが、民間の研究機関と連携する場合はMRC産業連携フレームワーク（MRC ICF）[199]への準拠が求められる。また、ヒトを参加者として含む研究（臨床試験、臨床介入研究、公衆衛生または行動介入研究など）については、MRCの「研究データの公開に関する方針：臨床試験と公衆衛生介入」（Open research data: clinical trial and public health interventions)[200]の要件の遵守が求められる。

基本的には上位機関であるUKRIの助成規程の遵守が必要となるが、医学研究を実施するための運営上、立法上、倫理上の要件を定めたMRCの利用規約[201]の遵守も必要となる。

（China UK One Health research for epidemic preparedness and AMR）
- **2018年データ保護法（DPA）**
- **国家安全保障・投資法**
- **国家安全保障および投資法：高等教育および研究集約型セクター向けのガイダンス**

d）サイバー領域

■　国家戦略等

2022年、英国政府は急速に変化するデジタル世界で英国が自信、能力、回復力を維持できるようにするための戦略として国家サイバー戦略（National Cyber Strategy）2022[202]を公表した。同戦略の主な目的として、１：サイバーに不可欠な技術分野で英国の能力を強化すること、２：個々のサプライヤーや、英国の価値観とは相容れない体制下で開発された技術への依存を減らしていくということ、の２つが提示されている。

また、同戦略を支える5つの柱が示されており、そのうち第3の柱では、サイバーパワーに死活的重要性をもつ技術を先導するために、産業の能力を増強し、将来のテクノ ロジーを確保するフレームワークを構築すること、第5の柱では、サイバー空間の内部およびサイバー空間を通じた英国の安全保障の強化のために敵対者を検知し、攪乱し、抑止することが示されている（図 4.1-15）。

197 https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf

198 https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors

199 https://www.ukri.org/councils/mrc/guidance-for-applicants/types-of-funding-we-offer/mrc-industry-collaboration-framework-icf/

200 https://beta.ukri.org/who-we-are/mrc/our-policies-and-standards/research/open-research-data-clinical-trials-and-public-health-interventions/

201 https://www.ukri.org/publications/mrc-funding-additional-terms-and-conditions/

202 https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

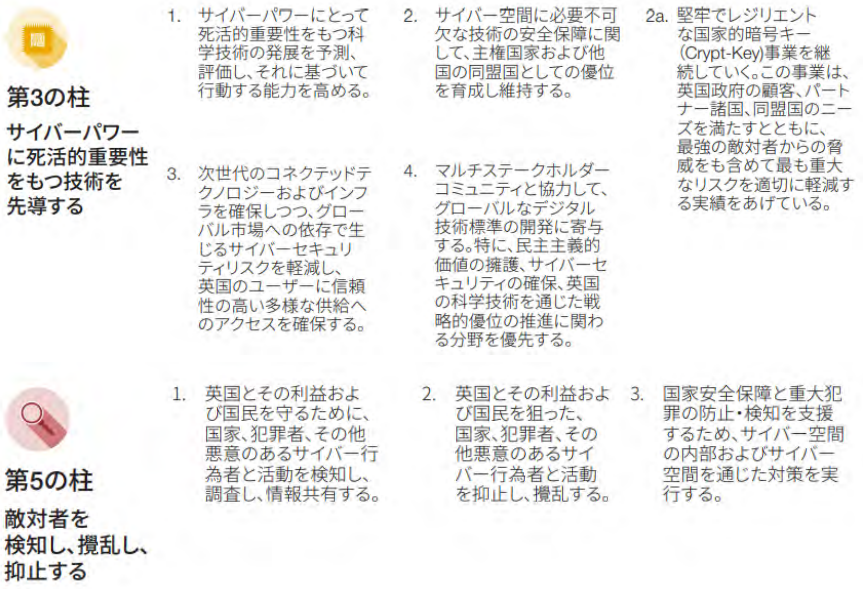


図 4.1-15　国家サイバー戦略 2022 における 5 つの柱（第 3、第 5 の柱）

■　研究開発機関

英国のサイバー領域の政府系研究機関としては、UKRI 傘下の工学・物理科学研究会議（Engineering and Physical Sciences Research Council：EPSRC）が挙げられる。EPSRC は、英国における工学および物理科学研究への主要な資金配分機関であり、デジタル技術からクリーンエネルギー、製造から数学、先端材料から化学まで多岐にわたる。

他領域と同様、MoD 傘下の Dstl、DASA もサイバー領域の研究開発を主導しており、主に国家安全保障を揺るがすサイバーリスクの定量化・低減技術に対して投資をしている。

サイバー領域における国家安全保障を確保するという観点では、英国政府通信本部（GCHQ）の傘下の国家サイバーセキュリティセンター （NCSC）やサイバー空間の内部およびサイバー空間を通じた効果的作戦のための 国家的研究センターである国家サイバー部隊（NCF）がその主要な役割を担っている。

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Quantum Technology Research Hubs[203]

EPSRC が所管する、より広範な技術とイノベーションのエコシステムを構築することを目的とした、最先端の量子技術研究の英国の拠点（ハブ）を設立するための資金提供プログラム。1 ハブあたり 1500 万～1950 万ポンドの資金が最長 60 カ月間提供され、これによりハブは、量子技術の開発と商業化を加速させるための、学界、産業界、その他のパートナーを巻き込んだ共同イニシアティブとして機能する。

プログラムの原則として、EPRC の責任あるイノベーションのためのフレームワーク [204]に

[203] https://www.ukri.org/opportunity/epsrc-quantum-technology-research-hubs/

[204] https://www.ukri.org/who-we-are/epsrc/our-policies-and-standards/framework-for-responsible-innovation/

基づいて取り進めることが推奨されている。また、提案に国際協力者を含める場合は UKRI の Trusted Research ガイダンスの参照が推奨されている。

（Quantum Technology Research Hubs で遵守が求められる法令等） ・　準拠が必要な法令等の情報は公募ページには掲載されていない

e）多義的技術

■　国家戦略等

英国における多義的技術に関連する取組として、1999 年に主に防衛系の政府機関と民間の研究機関が取り組んでいる技術の相互交流を目的に英国国防省（MoD）の傘下である国防評価研究庁（DERA）の内部に防衛多角化庁（DDA）が設立され、DDA を中心に相互技術移転の調整が図られたこと一つの契機になったと考えられる。2001 年に DERA は、民営化として設立された QinetiQ と Dstl（国防科学技術研究所）に分割されたが、QinetiQ は DERA に蓄積された技術を民間領域で利用を促進することを期待されていた。

2016 年に Dstl 傘下に安全保障上の課題に対する革新的な解決策の開発を支援する目的で国防・セキュリティ促進機構(DASA)が設立され、幅広く安全保障にかかわる技術開発を民間部門に呼びかける（資金提供する）構造が築かれた。また、2018 年には英国政府と英国ビジネスバンク(British Business Bank：：BBB)による多義的技術を対象にした共同イニシアティブである国家安全保障戦略投資基金（National Security Strategic Investment Fund ：NSSIF）が開始され、先端技術企業に対する長期的な株式投資が行われている。

上記の通り、英国では 2000 年前後から多義的技術の開発を積極的に取り進めているが、他方で 2021 年に公表された MoD のレポート「競争的時代における防衛：Defence in a Competitive Age」[205]では、機密技術、防衛技術、多義的技術に対する国家安全保障を脅かす敵対的な投資に対する保護の強化が述べられており、他国からの干渉も考慮しながら推進していくことが示されている。

■　研究開発機関

上述した MoD 及び傘下の Dstl 及び DASA が多義的技術の研究開発プログラムの主催を担っている。また投資中心であるが、BBB における国家安全保障戦略投資基金経由でも政府資金が多義的技術の開発に利用されている。

Dstl や DASA が取り組んでいる多義的技術の内容としては、宇宙、サイバー（AI、データサイエンス、通信ネットワークなど含む)、海洋・水上・水中、戦隊材料などの領域やセンシング、ロボット、自律システムなどの技術分野など多岐にわたっている。

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　The Defence Technology Exploitation Programme[206]

防衛技術活用プログラム（DTEP)は、企業が新たなビジネスを獲得し、産業能力を開発、国内外の防衛問題に対する新たな最先端の答えを提供するよう促すことを目的とした

[205] https://www.gov.uk/government/publications/defence-in-a-competitive-age

[206] https://www.gov.uk/government/publications/the-defence-technology-exploitation-programme

Innovate UK が後援する DASA のプログラム。

応募者は英国で登録された企業に限定されるが、特に外資系企業の場合は国家安全保障・投資法の遵守が求められる。

その他、基本的には Innovate UK の利用規約[207]への遵守が義務付けられるが、その中で規定されている法令等としては、内閣府の「政府一般補助金受領者の行動規範」[208]、UKRI の TRI 原則、国家インフラ保護センター（CPNI）[209] のガイダンスや UK GDPR、2018 年データ保護法等が挙げられる。また、DTEP の一環として開発された技術および製品の将来の輸出の可能性に関して、輸出管理およびライセンスに関する 内閣府のガイダンス [210]や輸出管理に関する MOD のガイダンス [211]に注意する必要が示されている。

・ Space to Innovate Campaign – Bravo Drop[212]

DASA が Dstl および UKSA と協力して立ち上げたキャンペーン。軍事および民間宇宙能力の両方を強化する技術を開発することによって、英国の宇宙における行動の自由を維持するための提案を求めており、宇宙から地上および宇宙から宇宙への軍事および諜報アプリケーション向けの新しいセンシングテクノロジーおよび ISR（インテリジェンス、監視、偵察） テクノロジーの開発などに焦点を当てている。

本プログラムの契約条件書によると準拠が求められる法令等としては基本的には NSIP と同様であるが、一部の規程に関しては DEFCON への準拠が義務付けられている。本プログラムで規定されている法令等及び DEFCON は下記の通りである。

（Space to Innovate Campaign – Bravo Drop で遵守が求められる法令等）

■ 法令
- UK GDPR
- 2018 年データ保護法（DPA）
- 2000 年情報自由法（FOIA）
- 2014 年環境情報規則（EIR）

■ DEFCON

（準拠が求められる DEFCON）
- DEFCON 126（国際的なコラボレーション）
- DEFCON 514（重大な違反/契約不履行）
- DEFCON 531（情報開示）
- DEFCON 532（個人情報保護）
- DEFCON 608（契約者が提供するアクセスと設備）
- DEFCON 632（第三者の知的財産-権利と制限）

[207] https://www.ukri.org/wp-content/uploads/2023/02/IUK-15022023-Terms-and-conditions-of-an-Innovate-UK-Grant-Award-Jan-2023-FINAL-with-Header.pdf?_ga=2.103058761.896306053.1704851276-717689553.1688814473

[208] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771152/2019-01-15_Code_of_Conduct_for_Grant_Recipients_v._1.01.pdf

[209] https://www.npsa.gov.uk/

[210] https://www.gov.uk/business-and-industry/export-controls

[211] https://www.gov.uk/guidance/uk-strategic-export-controls

[212] https://www.gov.uk/government/publications/competition-space-to-innovate-campaign-bravo-drop

- DEFCON 646（法律と裁判管轄（外国のサプライヤー））
- DEFCON 658（サイバー（フロー・ダウン））
- DEFCON 705（知的財産権-研究および技術）

・ Look Out! Maritime Early Warning Innovations[213]

DASA が所管する、海上作戦のための新しい早期警戒（EW：Early Warning）方法を提供する革新的技術の開発提案を求めたプログラム。監視範囲や目標検出能力の向上による空母および沿岸打撃群の状況認識に焦点を当てている。

契約条件[214]に示される情報保全に関する法令等及び DEFCON は下記の通りである。

（Look Out! Maritime Early Warning Innovations で遵守が求められる法令等）

■ 法令
- UK GDPR
- 2018 年データ保護法（DPA）
- 2000 年情報自由法（FOIA）
- 2014 年環境情報規則（EIR）

■ DEFCON
- DEFCON 126（国際的なコラボレーション）
- DEFCON 514A（重大な違反/契約不履行）
- DEFCON 524（拒絶）
- DEFCON 532A（個人情報保護）
- DEFCON 607（無線通信）
- DEFCON 608（契約者が提供するアクセスと設備）
- DEFCON 630（フレームワーク協定）
- DEFCON 658（サイバー）
- DEFCON 659A（セキュリティ対策）
- DEFCON 705（知的財産権-研究および技術）

・ Biosensing across wide areas [215]

MoD、Dstl、DASA が主導するプログラムで、防衛および安全保障活動の利益のために、現場で危険な生物剤を迅速に検出および位置特定するための改善された方法を提供する革新的な技術を求めている。

同プログラムの利用規約 [216]に基づく情報保全に係る法令等及び DEFCON は以下の通りである。

---

213 https://www.gov.uk/government/publications/competition-look-out-maritime-early-warning-innovations

214 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/984924/LOOK_OUT_-_MARITIME_EARLY_WARNING_INNOVATIONS_FRAMEWORK__SC2_CONTRACT_DOC.pdf

215 https://www.gov.uk/government/publications/competition-biosensing-across-wide-areas

216 https://assets.publishing.service.gov.uk/media/5e870824d3bf7f1fba0d7083/ISC_Terms_Biosensing_PDF.pdf

（Biosensing across wide areas で遵守が求められる法令等）

■ 法令

- 2000 年情報自由法（FOIA）
- 2014 年環境情報規則（EIR）

■ DEFCON

（準拠が求められる DEFCON）

- DEFCON 126（国際的なコラボレーション）
- DEFCON 514A（重大な違反/契約不履行）
- DEFCON 531（情報開示）
- DEFCON 532B（個人情報保護）
- DEFCON 601（余剰物資）
- DEFCON 608（契約者が提供するアクセスと設備）
- DEFCON 609（契約者の記録）
- DEFCON 611（取得財産）
- DEFCON 694（第三者の知的財産 - 権利と制限）
- DEFCON 705（知的財産権-研究および技術）

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして 44 件リストアップした（詳細は Appendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも 1 つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして 2 件抽出した（表 4.1-10)。

表 4.1-10　詳細調査を行う法令等（英国）

法令・ガイドライン等の名称	理由
・ セキュリティポリシーフレームワーク（Security Policy Framework：SPF） ・ 政府セキュリティ分類ポリシー（Government Security Classifications Policy：GSPC） ・ 政府ベースライン人員セキュリティ基準（Baseline Personnel Security Standard：BPSS）	政府職員や政府から業務を請け負事業者等、政府資産にアクセスする可能性のあるものを対象にした基本的なセキュリティ規則であり、政府資金を原資として実施されている研究開発プロジェクトにおいても、推進会議体（資金配分機関）に属する政府関係者及び研究実施主体となる民間事業者を対象に、情報保全上の前提となっていると考えられるため
・ 国家安全保障・投資法（National Security and Investment：NSI） ・ 国家安全保障・投資法：高等教育および研究集約型セクター向けのガイダンス（National Security and Investment Act: guidance for the higher education and research-intensive sectors）	投資規制の側面から保全を行っている法令の一つであり、セキュリティポリシーとは異なる視点からの情報保全措置に関する情報を俯瞰できると考えられる。一部の研究開発プロジェクトの応募要領でも言及されており、また、研究開発向けのガイドラインも公表されていることから、研究開発領域とも親和性が高いと考えられるため

以下に表 4.1-10 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）セキュリティポリシーフレームワーク [217]（政府セキュリティ分類ポリシー：GSPC[218]、政府ベースライン人員セキュリティ基準：BPSS[219])

■　策定機関・策定時期

2014 年

[217] https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework#preparing-for-and-responding-to-security-incidents

[218] https://www.gov.uk/government/publications/government-security-classifications

[219] https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

■　策定の背景・目的

セキュリティポリシーフレームワークは、英国政府の資産（人材、情報、インフラストラクチャ)）を保護するために必要な標準、ベスト プラクティスのガイドライン、アプローチを示したもので、英国政府から 2013 年に公表された。

同セキュリティポリシーフレームワークには、GSPC やベースライン人員セキュリティ基準（BPSS）に基づく情報の識別・評価及び人材確保上のセキュリティ施策の必要性が明記されており、以下の項目については GSPC、BPSS の内容も踏まえて整理する。

■　適用範囲

・　英国政府資産（人材、情報、インフラストラクチャ)を対象とした保全指針

■　情報の分類

政府が保有する情報資産の機密性（侵害、損失、または悪用によって生じる可能性のある影響）に関しては、政府セキュリティ分類ポリシー（GSCP）により、OFFICIAL、SECRET、TOP SECRET の３階層に分類され、機密性区分ごとに適切なベース動作が示されている。

ベースライン動作は機密性レベルごと及び情報の種類（口頭情報、ハードコピー情報、電子情報）ごとに示されている。なお、OFFICIAL レベルに関しては、通常の OFFICIAL 分類に加えて OFFICIAL- SENSITIVE マークが付記される分類が用いられる場合があり、その場合はより機密性を求めた追加の規制を受ける可能性がある。

表 4.1-11　英国における情報の機密性レベルの定義

情報分類	定義
OFFICIAL （-SENSITIVE）	・　公共部門及びパートナー組織で作成、処理、送受信される情報の大部分を占める、侵害された場合に中程度の 被害しかもたらさない情報資産。微妙な防護策を使用して、能力の異なる広範な脅威主体から防御する必要がある ・　GSCP の対象となる組織によって作成または処理されるすべての情報は、より高いレベルで分類されていない限り、デフォルトで「OFFICIAL」となる ・　通常の「OFFICIAL」レベルの情報資産にはは脅威アクターにとって関心が持たれる可能性が低い日常的な運用、ポリシー、サービス情報も含まれるが、-SENSITIVE とマークされた OFFICIAL 情報は脅威アクターや活動家、またはメディアにとってある程度関心のある情報が指定され、機密性の高い OFFICIAL 情報を限定的に配布するためにマークされるものである
SECRET	・　保護された専用物理インフラ上の安全なネットワークの使用、適切に定義され実施された境界セキュリティ管理など、高度な能力と決意を持った脅威行為者から防御するのに適した、強化された保護管理が必要とされる非常に機微な情報 ・　漏洩により（個人または集団の）生命が脅かされたり、英国の安全保障、国際関係、財政安全保障／安定性に深刻な損害を与えたり、重大な組織犯罪を捜査する能力に支障をきたす恐れがある

情報分類	定義
TOP SECRET	・ 英国またはその同盟国の国家安全保障を直接的に支援または通知する極めて機密性の高い情報資産 ・ 高度に保護された専用物理インフラ上の安全なネットワークを使用し、強固に定義・実施された境界セキュリティ管理により、あらゆる脅威から極めて確実に保護される必要がある ・ TOP SECRET 情報が侵害されると広範な人命の損失を引き起こしたり、英国や友好国の安全や経済的幸福を脅かしたりする可能性が生じる

■ 情報管理策

・ 組織的管理策

GSCP で示される情報の機密性レベルごと、及び情報の種類（口頭情報、ハードコピー情報、電子情報）ごとに組織・企業に対してベースラインとなる動作が示されている。（表 4.1-12）

表 4.1-12 GSCP に基づく主な組織的ベースライン動作

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
OFFICIAL	—	—	—
-SENSITIVE	—	—	—
SECRET	・ SECRET 情報が扱われる会議が頻繁に開催されるオフィスエリアについて、定期的な技術的監視対策（盗聴対策）を検討すること	・ 文書を認識しやすくするために、SECRET 文書をピンクの紙に印刷することを検討すること ・	—
TOP SECRET	・ 会議スペースの完全性を確保するために、技術的な監視対策（盗聴対策）の掃討を定期的に実施する ・ 家具などの TOP SECRET エリアに入る物品を適切に調達し、必要に応じて改ざんの兆候がないか検査を行うこと	・ 文書を認識しやすくするために、SECRET 文書を黄色の紙に印刷することを検討すること	—

・ 人的管理策

セキュリティポリシーフレームワークでは、人材確保上のセキュリティ施策としてンBPSS を参照している。BPSS は政府資産にアクセスできる個人の雇用前審査の標準として英国政府内で認識されており、BPSS の他、国家安全保障審査(NSV:National Security Vetting)のプロセスなどが規定されている。BPSS は英国政府が利用可能な人的保証基準の一つで、

政府資産にアクセスする可能性のある全スタッフは原則 BPSS の適用を受ける必要がある。

BPSS 以外の利用可能な人的保証基準としてはセキュリティチェック（SC）、発展型審査（Developed Vetting：DV）、テロ対策チェック（Counter-Terrorist Check：CTC）があり、BPSS を除くこれらの基準はいずれも国家安全保障審査（NSV）プロセスを通じて取得される正式なセキュリティ・クリアランスとして位置付けられている。なお NSV は、当該審査を実施する前段階で必ず BPSS に基づく資格確認を受けることが必要とされている。

（BPSS に基づく主な人的管理基準）

- BPSS は「知る必要性」の原則に基づき「OFFICIAL」レベルの英国資産へのアクセスについて許可を与えるものであり、「OFFICIAL」レベル以外の情報資産へのアクセスについては以下の許可が与えられる
  - 通常の業務において、または会議、講座、ブリーフィングの際に、「SECRET」レベルの英国資産に時折アクセスすること
  - 少量の「SECRET」レベルの英国資産の保管
  - 「SECRET」レベルの英国資産が保管されている区域への立ち入り
  - SECRET および TOP SECRET レベルの情報が立ち機器される可能性のある区域への立ち入り
  - アクセス管理が行われていることを条件として、SECRET レベルの情報を取り扱うことができる機器を使用すること
  - 公共サービスネットワーク（PSN）へのユーザクセス

- BPSS では以下の内容が許可されていない
  - 他国または国際機関（NATO など）に属する、機密情報以上に分類された資産へのアクセス、またはその知識、保管
  - 海外代理人請負業者が SECRET またはそれ以上に分類される資産にアクセスする、またはその資産に関する情報を保管すること（この場合、セキュリティ・チェック（SC）が必要となる）
  - 海外訪問中の制限区域への立ち入り
  - SECRET レベルのコードワード資料または TOP SECRET レベルの資料へのアクセス
  - 公共サービスネットワーク（PSN）への論理的なアクセス（システムを攻撃する能力と機会を持つ管理者など）

- 政府施設内で働く請負業者、コンサルタント、代理店スタッフについては、BPSS をはじめとする政府職員と同様のチェックを受けることを推奨する。また、派遣会社を通じてスタッフが提供される場合については、BPSS が適用されていることを契約書に明記する必要がある。請負業者に対して各省庁は以下を行う必要がある
  - 請負業者の契約遵守状況を定期的に監視する
  - 請負業者は、すべての法的要件を満たすスタッフを提供するようにする。例えば、セキュリティスタッフは、必要に応じて適切な SIA（Security Industry Authority：警備業協会）ライセンスを保持する
  - 請負業者が、その業界の基準を認定する公認の専門スキーム（例えば、セキュリティ請負業者のための SIA（Security Industry Authority）の Approved Contractors Scheme）に参加していることを確認する

- 請負業者とパス、写真付き身分証明書、スタッフリストを含む共同システムについて合意し、請負業務に従事する個人が本当に出勤した本人であることを確認する
- 通常の契約スタッフが不在または不在の場合、臨時の代役を立てるための手 順に合意する
- 個人が特権情報や多額の現金にアクセスする際には、段階的アプローチを検討する
- 可能であれば、契約スタッフが施設内にいるとき、または特に敏感なエリアに アクセスできるときは常に、契約スタッフを監督する

（BPSS の手順）

・ BPSS は①アイデンティティ（身元確認）、②国籍および入国ステータス（当該業務に従事する資格を含む）、③職歴（過去 3 年間）、④犯罪歴の検証による行われる。また、従業員候補者は、海外で過ごした重要な期間（過去 3 年間に 6 ヶ月以上）に ついて、合理的な説明をすることが求められる。
・ ①身元（アイデンティティ）確認：採用プロセスにおいて、また採用内定に先立ち、個人は最低限、以下の情報を提供するよう求められなければならない
  - 氏名、生年月日、住所の確認
  - （必要に応じて）国民保険番号またはその他の固有の個人識別番号
  - 過去 3 年間の雇用者の詳細（氏名、住所、日付）
  - 必要な資格／免許の確認
  - 学歴の詳細（推薦状は、新入社員が必要と思われる場合に提出する）
  - 英国での就労許可の確認
・ ②国籍および入国ステータスの確認：適切な書類を物理的にチェックするか、例外的な状況には、英国ビザ・移民局（UKVI）の記録を独自にチェックすることで確認する
・ ③職歴の確認：前職の雇用主への確認、および/または推薦者のフォローアップ、あるいは市販の履歴書チェックサービス、または Civil Service Resourcing の電子職歴チ ェックによって行う。また、BPSS が国家安全保障上の審査の下準備として実施される場合、職歴は最低限、過去 1 年分を確認する必要がある
・ ④犯罪歴の確認（未決囚のみ）：ディスクロージャー・アンド・バーリング・サービス（DBS）とディスクロージャー・スコットランドは、ベーシック・ディスクロージャー・サービスを通じて「未経歴」の犯罪歴のチェックを提供している。2018 年 2 月 1 日以降、イン グランドおよびウェールズでの求人については、DBS を使用してチェックを行う必要がある。なお、BPSS が国家安全保障のための審査の一環として実施される場合は、「未決」の前科 を確認する義務は適用されない

（その他の主な規定）

・ 一部の情報は真実でなかったり、文脈から外れていたりする可能性があるが 現行の手続きを強化するためにその場限りでインターネットによるチェックを行うことができる
・ 英国に居住していないため、英国内で意味のある調査を行うことができない 場合、BPSS の一環として、従業員候補者は、相当期間（過去 3 年間に 6 ヶ月以上）海 外に居住していたことを合理的に説明することが求められる（英国に居住していないこと自体が、自動的に雇用の障害となるべきではない）
・ 個人がある組織から別の組織へ異動する場合、異動を受 け入れる部署、機関、請負業者は、BPSS が満たされ ていることを自ら確認しなければならない

表 4.1-13　英国の国家安全保障審査に関連して取得可能な主なクリアランス

クリアランスの種類	与えられる主な許可	主な確認事項
ベースライン要員セキュリティ基準(BPSS)	・英国の OFFICIAL 資産へのアクセスと、英国の SECRET 資産への時折のアクセス ・SECRET 情報および TOP SECRET 情報が聞かれる可能性のある領域で作業 ・Public Services Network (PSN)へのアクセス	・身元 ・職歴（過去 3 年） ・国籍及び移民のステータス ・犯罪歴
認定チェック（AC）	・英国空港のセキュリティ制限区域に伴走なしの立入 ・英国の航空保安訓練 ・英国への貨物輸送	・身元 ・学歴、職歴（過去 5 年間） ・犯罪歴 ・英国政府及び関連機関が保持する記録との照会
テロ対策チェック（CTC）/レベル 1B	・テロ攻撃の特別な危険にさらされていると評価される著名人への接近 ・テロリストにとって価値があると評価された情報または資料へのアクセス ・テロ攻撃の特別な危険にさらされていると評価される特定の軍事、民間、工業、商業施設への付き添いなしの立ち入り	・BPSS の完了 ・個人によるセキュリティ質問書への記入 ・部門/会社の記録（個人ファイル、スタッフ報告書、病気休暇申告書、セキュリティ記録など）のチェック ・犯罪歴 ・保安局記録のチェック ・（セキュリティ上の懸念がある場合）個人による面接
セキュリティチェック（SC）	・SECRET 資産への長期的かつ頻繁かつ制御されないアクセス、および/または TOP SECRET 資産への時折の制御されたアクセス	・BPSS の完了 ・個人によるセキュリティ質問書への記入 ・部門/会社の記録（個人ファイル、スタッフ報告書、病気休暇申告書、セキュリティ記録など）のチェック ・犯罪歴 ・信用調査機関による信用及び財務履歴の調査 ・保安局記録のチェック ・（セキュリティ上の懸念がある場合）個人による面接 ・（経済的な懸念がある場合）人の財務状況を完全に

クリアランスの種類	与えられる主な許可	主な確認事項
		調査できるように、個別の財務アンケートへの回答 ※各チェックはセキュリティ質問書に含まれる第三者にも及ぶ場合がある
発展型審査（Developed Vetting：DV）	・TOP SECRET 資産への頻繁勝つ無制限のアクセス ・TOP SECRET のコードワード資料へのアクセス	・BPSS の完了 ・個人による DV セキュリティアンケートへの記入 ・部門/会社の記録（個人ファイル、スタッフ報告書、病気休暇申告書、セキュリティ記録など）のチェック ・犯罪歴 ・信用調査機関による信用及び財務履歴の調査 ・保安局記録のチェック ・個人の財務状況のチェック ・訓練を受けた捜査官による詳細な聞き取り ・訓練を受けた捜査官が行う審判員との面談を含む更なる取り調べ ※各チェックはセキュリティ質問書に含まれる第三者にも及ぶ場合がある ※個人財務の完全なレビューには、個人ベースの評価と、配偶者またはパートナーとの共同の立場を考慮した個人の資産、負債、収入および支出の評価が含まれる

また、GSCP で示される情報の機密性レベルごと、及び情報の種類（口頭情報、ハードコピー情報、電子情報）ごとに組織・企業に属する個人に対して人的なベースライン動作が示されている。（表 4.1-14）

表 4.1-14　GSCP に基づく主な人的ベースライン動作

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
OFFICIAL	・公共の場で自由にディスカッション可能であるが、組織のメンバーなどに聞かれる可能性があることに注意すること ・リモート作業時、共有スペースで話し合うことは可能であるが、スマートリスニングデバイスによって盗聴される可能性があることに注意すること	・オフィスで使用していない情報のハードコピーを机の上に置かないこと ・公共の場で情報にアクセスすることは可能であるが、周囲に見られないように注意すること ・明確なビジネス上の必要性がない限り、オフィスの外へ持ち出すことは避けること ・輸送する場合は信頼できる民間宅配業者を使用すること ・自宅や公共のごみ箱に捨てないこと ・廃棄のためにオフィスに持ち込む前に、自宅で安全に保管する必要がある ・オフィス内の情報は、機密ゴミ箱やシュレッダーの使用など、組織によって義務付けられた正しい廃棄方法を使用すること	・企業システムの共有領域に保存することが可能 ・資産を共有ドライブに保存する場合は、部門の情報管理原則に従うこと ・公共の場、リモート作業中に情報にアクセス可能であるが、周囲に見られないように注意すること ・情報作成者の許可がなくとも情報を共有することが可能 ・
-SENSITIVE	・公共の場で周囲に聞かれる可能性がある場合はディスカッションを避けること ・リモート作業時の議論はプライベート空間でのみ行うこと	・公衆の場で情報にアクセスすることは避けること ・見られる可能性のある場所でリモート作業しないこと ・輸送する場合は記録郵便サービスまたは信頼できる民間宅配業者を使用すること	・ローカルシステム上の複数のコピーをできる限り最小限に抑えること ・フォルダーにアクセスできるすべての人がその情報を知る必要があると確信できる場合にのみ、そのフォルダーに保存すること

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
			・ 情報は知る必要のある場合と共有する必要がある場合に基づいて、組織外の個人と情報共有可能 ・
SECRET	・ 会議を行う場合、議長は、会議が始まる前に、SECRET 情報が議論されることを明確にすること ・ 人前で議論しないこと ・ 個別の組織や組織によって明示的にリスク評価および許可されている場合を除き、すべての個人用通信デバイスおよびウェアラブルテクノロジー（スマートウォッチなど）を部屋から取り外すこと	・ 自宅またはその他のリモート作業現場で機密情報のハードコピーを扱う必要がある場合、現地組織に沿って他の職員に委任されている場合を除き、上級管理職（SCS1）および SSA/SA の承認を常に事前に取得する必要がある ・ SECRET 情報を含む手書きのメモは避けること。取得する必要がある場合は、他の SECRET 文書と同様に扱う必要がある ・ 極力情報の輸送は避け、目的地で安全に印刷を行うこと ・ 可能であれば、情報の輸送は避け、目的地で安全に印刷を行うこと ・ 物理的資産を手で輸送する場合は少なくとも SC のセキュリティ・クリアランスが必要 ・ 資産を運ぶ上で 2 人の護衛を設ける必要があるかリスク評価を行う ・ 海外に情報を輸送す	・ 組織が許可されたエリアでのみ処理作業を行うこと ・ 公共の場または権限のない職員がいる場所では、SECRET 資料にアクセスしたり読んだりしないこと ・ 短時間であっても、ワークスペースから離れるときは、デバイスをロックすること ・ 権限のない同居者、訪問者、または通行人が情報を見落とす可能性がある場所ではリモート作業しないこと ・ SECRET ノートパソコンを自宅や職場以外の場所に持ち歩かないようにすること ・ 公衆 Wi-Fi 経由で SECRET IT システムにアクセスしない ・

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
		る場合、海外に資産を郵送する前に、情報作成者、SSA/SA の承認を求めること ・ 情報を破壊する際は CSE（Catalog of Security Equipment）の製品を使用すること	
TOP SECRET	・ 個人または企業の通信デバイス、ウェアラブル テクノロジー（スマートウォッチなど)、およびスマート リスニング デバイス（音声起動スピーカーなど）は、組織によって特別に承認されていない限り、TOP SECRET エリアに持ち込まないこと	・ TOP SECRET 情報はリモートワークで扱うことはできない ・ 物理的資産を手で輸送する場合は少なくとも DV のセキュリティ・クリアランスが必要 ・ 指定された政府の安全なゾーン内以外で持ち運ぶ場合、少なくとも 2 名の DV のクリアランスを保有する護衛を設けること ・ 海外に情報を輸送する場合、海外に資産を郵送する前に、情報作成者、SSA/SA、および上級管理者(SCS1)の承認を求めること ・ 情報作成者からの書面による承認なしに資産を破壊しないこと ・ DV のセキュリティ・クリアランスを有する証人の立会いのもと破壊すること	・ 情報作成者の許可なしに、また知る必要のない限り、組織外の人と共有しない ・ 情報を破壊する際は CSE（Catalog of Security Equipment）の製品を使用すること

・ 物理的管理策

セキュリティポリシーフレームワークには、より良い政策と公共サービスの提供及び、スタッフと訪問者に安全な作業環境を提供するために、第三者が保有・管理する政府資産も含めて物理的セキュリティ管理の必要性を示している。

（セキュリティポリシーフレームワークにおける物理的セキュリティの指針）
- 物理的なセキュリティの範囲は状況や業務要件、脅威の種類（自然災害、その他の破壊的課題、犯罪、テロリズム、スパイ活動など）によって異なるが、セキュリティの例としては、境界の管理と警備、建物の設計上の特徴、出入りの制限、遮蔽、その他の方法による管理、適切な備品やオフィス家具、特に機密性の高い業務用の建物内の別エリアの使用などが挙げられる
- 管理は過度に厳格なものではなく、適切なものでなくてはならない
- 特にテロリズムによる脅威が増大した場合に、セキュリティ対策を適応させ、強化するための体制を整えておくべきであり、必要でない人の出入りを制限、職員や訪問者のチェックや手荷物検査の頻度を高める、追加の周辺規制やその他の警備活動を設けることが必要になる場合がある

また、GSCP で示される情報の機密性レベルごと、及び情報の種類（口頭情報、ハードコピー情報、電子情報）ごとに組織・企業に対して物理的なベースライン動作が示されている（表 4.1-15）。

表 4.1-15　GSCP に基づく物理的ベースライン動作

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
OFFICIAL	－	・オフィスで使用していないときは、不透明なフォルダーまたは容器に保管すること ・公共の場で作業する際は、偶発的な紛失を防ぐために安全に保護できる不透明なフォルダー、袋、または容器に保管すること ・リモートで作業する場合は目立たない不透明な容器に保管すること ・輸送する場合、書類は１つの密閉された不透明カバーを使用すること	－

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
-SENSITIVE	―	・オフィスで使用していないときは、不透明なフォルダーまたは容器に保管し、無人のときは施錠して鍵をかけて保管すること ・確実に施錠できるオフィス家具・物理的セキュリティ機器を使用すること ・海外に輸送する場合、書類は不透明な二重封筒/梱包を使用すること	―
SECRET	―	・国家保護安全局(NPSA)が承認したSECRET用の物理セキュリティ機器に保管すること ・輸送する場合、丈夫で不透明な二重封筒またはその他の適切な包装に入れ、承認された不正開封防止パッケージを使用すること ・政府の建物の外に手で持ち運ぶ場合は、目立たない、不透明で施錠されたセキュリティ コンテナ内に配置すること	―
TOP SECRET	・会話が盗聴されないように、TOP SECRET認定の会議室を使用してディスカッションを行うこと ・	・使用しないときは、TOP SECRETとして承認されたNPSA (National Protective Security Authority) 認定の	―

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
		物理セキュリティ機器に保管すること ・ 輸送する場合、書類は丈夫で不透明な二重封筒またはその他の適切な包装に入れること ・ セキュリティ機器カタログ(CSE)で NPSA によって承認された不正開封防止パッケージのみを使用すること	

・ 技術的管理策

GSCP で示される情報の機密性レベルごと、及び情報の種類（口頭情報、ハードコピー情報、電子情報）ごとに組織・企業に対して技術的なベースライン動作が示されている(表 4.1-16)。

表 4.1-16 GSCP に基づく技術的ベースライン動作

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
OFFICIAL	・ 組織によって承認されたデバイスのみを使用してディスカッションを行うこと	・ 組織によって承認された企業システムまたはデバイスでのみ印刷すること	・ 情報を電子的に共有する際は、件名に取扱い指示を含めるか電子ラベルを使用すること
-SENSITIVE	同上	同上	同上
SECRET	・ 組織によって承認された IT システムまたは電話システムのみ使用してディスカッションを行うこと ・ 可能な限り組織によって承認されているヘッドフォンを使用してディスカッションを行うこと	・ 組織によって承認された企業システムまたはデバイスでのみ印刷すること	・ 組織によって承認された IT システム上でのみ、電子情報の作成、保存、または共有を行うこと ・ 安全な隔離ネットワークの外に情報を送信しないこと（たとえば、公式電子メールアカウントやオープンインターネット

情報分類	ベースライン動作		
	口頭情報	ハードコピー情報	電子情報
			経由で送信しないこと）
TOP SECRET	同上	同上	同上

■　罰則

GSCP は英国政府によって設定され、以下の英国内の法令の枠内で運用されるため、同法に基づく罰則規定が適用され得ると考えられる。

（GSCP に関連する法令と主な罰則規定）

- 1989 年公務機密法（OSA）
  - 情報の種類ごとに、不正な開示によって発生した、または発生する可能性がある損害の種類の補足する
  - OSA での罰則規定は以下の通り
    - 第 8 条の(1)(4)及び(5)に基づく違反（合法的な権限なしに開示することが違反となる文書その他の物品の所持または管理に基づく違反）の場合、略式有罪で「3 ヶ月以下の懲役もしくは標準尺度の 5 レベルを超えない罰金、またはその両方」が科される
    - 第 8 条の(1)(4)及び(5)以外の規程に基づく違反の場合、起訴により有罪判決を受けた場合、「2 年以下の懲役もしくは罰金、またはその両方」、略式有罪の場合、「6 ヶ月以下の懲役、法定刑の上限を超えない罰金、またはその両方」が科せられる
- 2018 年公務機密法（DPA）
  - 個人データの取り扱いは、データ保護法に準拠する必要がある一方、国家安全保障を守るために、英国一般データ保護規則（UK GDPR ）の要件の多くからの免除を規定していることから、各省庁は国家安全保障上の懸念に対処し、データ保護法を遵守することが可能かどうかを評価する必要がある
  - 本法に違反した場合、最高で 2,000 万ユーロまたは当該事業の前会計年度における年会総売上の 4%の罰金が科せられる
- 2000 年情報公開法（FOIA）
  - 機密性分類に応じて、FOIA の免除が適用されるか検討することに役立てることが可能
  - データ保護法に基づく個人の権利を侵害した情報公開が行われた場合などについて違法行為として規定しており、例えば、データ管理者の違法行為によって損害・苦痛を被った場合、個人はデータ管理者に対して損害補償を要求することができることが示されている [220]
- 公記録法
  - 政府機関や公共団体が生成した記録物の保管、管理、公開に関する規則を規程

[220] https://www.clair.or.jp/j/forum/c_report/pdf/283.pdf

b）2021 年国家安全保障・投資法（国家安全保障・投資法:高等教育および研究集約型セクター向けのガイダンス）[221]

■　策定機関・策定時期

2021 年

■　策定の背景・目的[222]

英国政府は外国企業や投資家による英国企業に対する合併・買収に対する監視を強めており、2020 年 6 月の「2002 年企業法改正」により、政府が合併・買収案件を調査・介入できるようになった。さらに政府の調査・介入を強化する目的で、2021 年国家安全保障・投資法が策定され、国家安全保障を脅かす可能性がある、外国企業や投資家による英国企業に対する合併・買収などについて、一定の条件を超える場合、事前に政府への届け出を義務付け、特定の種類の事業体および資産に対する支配権の取得から生じる国家安全保障上のリスクへの対応を行っている。

また国家安全保障・投資法の施行に合わせて、高等教育および研究集約型セクター向けのガイダンスが公表され、高等教育機関およびその他の研究機関の国家安全保障・投資法に対する理解醸成や同法に基づく通知要否などを整理している。

■　適用範囲

国家安全保障上の懸念が生じやすい 17 分野での特定の取引（合併・買収）及び買収側企業から通知される情報に対して、国家安全保障上のリスクの有無が審査される。

（国家安全保障・投資法上の通知義務がある 17 分野）
先端素材、先進ロボット工学、人工知能、民生用原子力、通信、コンピュータハードウエア、政府への重要なサプライヤー、危機管理に関する重要なサプライヤー、暗号認証、データ・インフラストラクチャー、防衛、エネルギー、生物工学、軍民併用技術、量子技術、衛星・宇宙技術、輸送

通知対象となる取引は Trigger event と呼ばれ以下の場合が該当する。

（NSI 法で通知義務が生じるケース）[223]
- **発行済株式数もしくは議決権の保有割合が 25%以下の状態から、25%超取得することになる場合**
- **同 50%以下の状態から 50%超となる場 合**
- **同 75%未満の状態から 75%以上となる場合**
- **対象企業の経営方針に重大な影響力を行使することができる場合**

[221] https://www.gov.uk/government/collections/national-security-and-investment-act

[222] https://www.jetro.go.jp/world/europe/uk/invest_02.html

[223] https://www.grantthornton.jp/globalassets/1.-member-firms/japan/pdfs/newsletter/advisory/advisory__202111.pdf

・　対象企業の事業統治に関連する決議を通過させる、もしくは阻止することができる議決権を有している場合

研究開発機関が適格事業体（買収対象企業）となる場合に想定される機関の種類や適格資産（買収対象資産）の種類については、高等教育および研究集約型セクター向けのガイダンスに言及されている。

（研究開発領域における NSI 法に基づく適格事業体及び適格資産の例）[224]

・　適格事業体となる研究開発機関の例
- 大学（大学からのスピンアウト企業、子会社含む）
- 研究機関
- 高等教育機関または研究機関と契約業務を行う民間企業または法人

・　研究開発領域で想定される適格資産の例
- デザイン
- 計画、図面、仕様書
- ソフトウェア
- 企業秘密
- データベース
- ソースコード
- アルゴリズム
- 数式
- 土地
- 実験器具などの有形の動産

■　情報の分類

NSI 法を通じて保全対象となる事業体及び資産に関して、政府セキュリティ分類ポリシーに基づく分類（OFFICIAL、SECRET、TOP SECRET）に該当するかについての詳細を通知することが規定されている。また、NSI 法に基づいて必要な情報を政府に通知する際、OFFICIAL 以上に分類されている情報を送信する場合は安全に提出する方法について政府に問い合わせを行う必要が述べられており、基本的に政府セキュリティ分類ポリシーに準拠した運用が行われていることが読み取れる。

■　情報管理策

・　組織的管理策

国家安全舗装・投資法は、買収を行おうとする外国企業に対して、同法に基づいて買収の詳細を政府に対する通知する義務を科すとともに、政府の審査結果に応じた買収の実行及び通知義務を怠った場合の罰金や懲役刑を科すことで、国家安全保障へのリスクを対処

[224] https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors

するものである。そのため、同法を通じて研究機関が有する情報資産等を外国の脅威を保全するという意味で、組織的管理策とした。

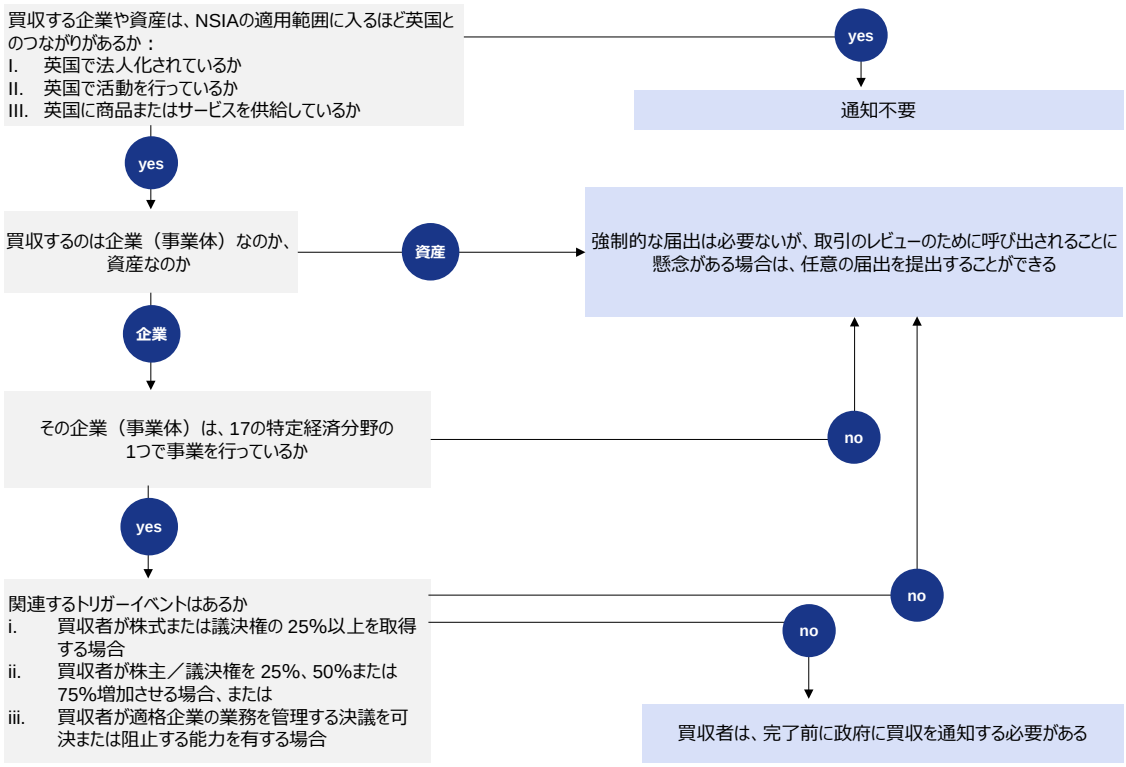


図 4.1-16　NSI 法に基づく通知判定フロー

買収を行おうとする企業に対して通知を求める情報は以下の通り。

（NSI 法に基づいて通知する義務のある情報）

- 連絡先の詳細と関連する通知
  - 通知フォームを送信する当事者の連絡先情報
  - 同時に支配権を獲得し、この買収に参加している追加の買収者全員の連絡先
  - 海外の投資審査制度の届出情報（投資審査制度の名称、届出国、提出日、指定された参照番号、結果）
- 買収の詳細
  - 対象分野
  - Trigger event のタイプ（議決権の保有割合やこの保有により生ずる権利等）
  - 買収が行われる日付
- 適格事業体（買収対象企業）の詳細
  - 適格事業体が提供・実行する活動・サービスの詳細及び同活動・サービスを支えるテクノロジーに関する情報
  - 政府セキュリティ分類や原子力規制当局（ONR）が定める分類ポリシーで該当する情報を受信・保持する権利を有しているか否かの情報
  - 英国で当該事業活動を行う上で保有しているライセンスの情報（Ofgem（Office of Gas and Electricity Markets：ガス・電力市場局）からの電力の生成・送電・配

電・供給ライセンス、Ofcom からの通信ライセンス等）
- 保有するデュアルユース品目の情報
- 英国政府との供給関係
- 過去 5 年間で英国政府からの資金提供に基づいて実施した防衛、国家安全保障、法執行、国家インフラ分野の研究開発に関する概要
- 国家安全保障審査(NSV)のクリアランスの保有状況
- 買収前後の所有権構造図（株主氏名、株式保有権又は議決権割合、株主の国籍、関連情報）
- 適格事業体の運営・意思決定に係る英国以外の政府の情報

・ 適格資産（買収対象資産）の詳細

※資産の所有者に関して要求される情報は、適格事業体で求められている情報と同様
- 取得される資産の使途/用途
- 当該資産が物的資産（機械や設備など）か非物的資産（知的財産権など）かどうか
- 対象資産の開発または管理において、当該資産に関連する活発な共同開発契約または学術提携があったかどうか
- 当該資産が、軍事利用やエネルギー利用に関連し得る独自の能力を提供しているかどうか
- 当該資産が、現在の英国市場にはない独自の能力を提供しているかどうか
- 当該資産に関するデュアルユース品目の情報
- 当該資産が英国国民に関するデータを収集するために使用されているかどうか

・ 取得者（買収を行うもの）の詳細
- 取得する組織/個人のフルネーム
- 設立国
- 取得当事者が法人である場合は定款

※法人が英国以外で設立された場合は、設立国、会社番号などの固有のビジネス参照情報（利用可能な場合）、および設立国内での完全な登録詳細（英国に関連するその他の情報）を提供する必要がある
- 取得当事者が個人の場合は国籍
- 英国政府以外の政府による取得者の株式所有権または議決権
- 取得者の運営・意思決定に係る英国以外の政府の情報
- 買収完了後の取得者とその他の当事者との間の株式所有権または議決権にアｋんする契約取り決めの情報
- 取得者の所有構造（株式の所有割合または議決権の 5%以上を有する株主の内容に関する情報、氏名と所有割合、議決権の詳細、記載されている株主の国籍 （個人の場合）または設立国（法人の場合）、関連情報）
- 取得者の取締役またはそれと同等のものに関する情報（氏名、生年月日、情報）

研究開発機関の場合に対象となる取引については高等教育および研究集約型セクター向けのガイダンスの中で事例が示されており、例えば、大学の研究開発に対して民間企業がスポンサーとして資金提供を行い、その結果、大学によってライセンス供与されている適格資産の管理権を取得した場合、これは有形の動産及び知的財産の取得として、NSI 法に基づく適格買収に相当する場合がある。

（研究開発領域で NSI 法の規程に関連する主な事例）[225]

- 外国企業が英国の大学に資金を提供し、外国企業に代わって大学が研究プロジェクトを実施するが、実質的な意思決定を外国企業が担い、研究から生じたすべての知的財産および有形の動産に対する権利を有する場合
  - 資金提供によって外国企業がこのプロジェクトを通じて生成された知的財産または有形の動産財産を管理できるようになり、計画された適格資産の取得に相当するため、買収が国家安全保障にリスクをもたらす可能性があると合理的に疑われる場合、計画中の買収の評価のために政府から取得者の召喚を要請する可能性がある
  - 他方、研究プロジェクトは適格事業体ではなく、義務的な通知は適格な事業体の特定の買収にのみ適用されるため、NSI 法に基づいて政府に通知する義務はない

- 民間企業が、17 の重要分野の 1 つで研究活動を行っており、適格事業体に指定されている大学子会社の株式の 30%を取得する場合
  - 投資計画を政府に通知し、事前に承認を得ることが法的に義務付けられる。これを行った場合、買収は無効となり、事前の承認なしに買収が完了した場合には、刑事罰または民事罰が課される可能性がある

- 学術機関 A が、連携協定を通じて学術機関 B の知的財産を使用する権利を取得する場合
  - 政府は、この買収が国家安全保障上のリスクを生じさせた、または生じさせる可能性があると合理的に疑われる場合、評価のために取得者に召喚を要請する可能性がある
  - 他方、知的財産の取得には通知義務が適用されないため、政府に通知する法的義務はない

- 学術機関 A が、連携協定を通じて学術機関 B の知的財産を使用する権利を取得する場合
  - 政府は、この買収が国家安全保障上のリスクを生じさせた、または生じさせる可能性があると合理的に疑われる場合、評価のために取得者に召喚を要請する可能性がある
  - 他方、知的財産の取得には通知義務が適用されないため、政府に通知する法的義務はない

- 外国企業が英国の学術機関と共同研究プロジェクトに参加し、提携契約の中で外国企業が学術機関によって生成され、さらなる研究を実施するために使用されている知的財産を使用するための非独占的ライセンス契約を締結する場合
  - ライセンスの付与が対象となる資産に対するコントロール権の取得に該当する

[225] https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors

ため、政府は、この買収が国家安全保障上のリスクを生じさせた、または生じさせる可能性があると合理的に疑われる場合、評価のために取得者に召喚を要請する可能性がある

- 他方、知的財産の取得には通知義務が適用されないため、政府に通知する法的義務はない

■ 罰則

届け出の結果、国家安全保障上のリスクがあると判断された場合、所管大臣は当該リスクを軽減するための改善措置を命令することができる。また、クリアランスを取得せずに完了した取引は無効とされるとともに、全世界売上高の 5%もしくは 1,000 万ユーロのいずれか大きい額の罰金が課される [226]。

[226] https://www.grantthornton.jp/globalassets/1.-member-firms/japan/pdfs/newsletter/advisory/advisory__202111.pdf

(5) ドイツ

1) 基本情報

- 政治体制：議院内閣制
- 人口：8340 万 8 千人（2021 年 7 月現在）
- 名目 GDP：名目 GDP：4.2 兆米ドル、実質 GDP：3.5 兆米ドル
- 研究開発予算：1532 億米ドル（2021 年） OECD 購買力平価 換算

■ 政治動向

2021 年 11 月にショルツ政権樹立。G8 や NATO に所属しており、EU においても主要国であることなどから、国際的な発言力を有している。

2023 年に国家安全保障戦略を策定し、ロシアの脅威への言及や、中国についてパートナー・競争相手・体制上のライバルとした上で今後、同戦略に続き、中国戦略も策定する予定となっている。

■ 経済動向

イギリスの主要産業は自動車、機械、化学・製薬等であり、第 3 次産業も盛んである。世界有数の先進工業国であるとともに貿易大国。GDP の規模では欧州内で第 1 位。主な貿易相手を地域別に見ると、輸出入ともに欧州が全体の 3 分の 2 程度を占める。

GDP 成長率はコロナ以前の２０１９年までの過去５年間では、0.6%～2.6%の間で推移していた。

■ 社会動向

人口は世界 19 位であり、国内市場は大きい。シリア内戦を機に難民が欧州に殺到した 2015 年、ドイツは大規模な受け入れに踏みきったが、財政負担増や治安悪化への不安から、政府への批判が高まった。

■ 技術動向

伝統的に製造業に強みを持っている。ドイツは総研究開発費で米国・中国・日本に次ぎ世界第 4 位、研究者数でも世界第 4 位（2019 年）と、科学技術、研究開発が盛んである。ドイツの総研究開発費は、2017 年に GDP に占める割合が 3.05%となり、EU の掲げる研究開発費対 GDP 比 3%目標を達成した。現在は、2025 年に 3.5%を目標として投資を拡大しているものの、コロナ禍やウクライナ危機といった社会情勢の大幅な変化を受けて実現は難しいとの見方が大勢である。メルケル政権発足直後の 2006 年に始まった科学技術イノベーション基本政策「ハイテク戦略」および後継の「未来戦略」が現在のドイツの科学技術イノベーション政策の基盤となっている。

2）秘密情報の取扱いに係る政策動向

ドイツにおける安全保障上の国家機密については、1994 年に制定された「Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen（連邦保安審査に関する機密事項の保護に関する法律)」（通称：Sicherheitsüberprüfungsgesetz （セキュリティチェック法）- SÜG）によって規定されている[227]。

SÜG は国家安全保障上注意を要する活動に従事する人物のセキュリティチェックの要件と手順を規定するものであり、公的機関がそのような活動に個人を任命する場合や、民間企業に対して機密情報を提供する場合などに活用される。他の法律で特に示されている機関としては、「Gesetz über die Rechtsstellung der Soldaten（兵士の法的地位に関する法律)」において職業軍人または臨時軍人としての最初の任用を予定している者に対して SÜG に基づくセキュリティチェックを実施しなければならないことを規定しており[228]、連邦刑事警察局（Bundeskriminalamt）の勤務者についても同様の規定がなされている[229]。

SÜG において取り扱う機密情報は「公衆の利益のために秘密にしておく必要があるすべての事実、物体、または調査結果」であり、提供される媒体の種類を問わず、その内容によって規定される。機密レベルは、当該情報が漏えいした場合に生じうるリスクによって 4 区分に分類されている[227]（表 4.1-17)。

表 4.1-17　SÜG における機密情報の区分

分類	漏洩で生じうるリスク
STRENG GEHEIM （最高機密）	無許可のアクセスにより、ドイツ連邦共和国またはその一国の存立または重大な利益が脅かされる可能性がある
GEHEIM （機密）	無許可のアクセスにより、ドイツ連邦共和国またはその一国の安全が脅かされ、またはその利益に重大な損害がもたらされる可能性がある
VS-VERTRAULICH （VS 秘密）	無許可のアクセスにより、ドイツ連邦共和国またはその一国の利益が損なわれる可能性がある
VS-NUR FÜR DEN DIENSTGEBRAUCH （VS-業務利用のみ）	無許可のアクセスにより、ドイツ連邦共和国またはその一国の利益を害する可能性がある場合。

機密情報保護体制は SÜG とその下位規則から構成され、下位規則の一つである「重要秘密保護に関する一般管理規則」（機密情報指示-VSA)にはその具体的な保全措置が規定されている[230]。

[227] https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/staatlicher-geheimschutz/staatlicher-geheimschutz-node.html

[228] https://www.gesetze-im-internet.de/sg/__37.html

[229] https://www.gesetze-im-internet.de/bkag_2018/__68.html

[230] https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SII554001405.htm

① 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

ドイツでは安全保障貿易管理や外資規制については、EU の共通政策に準拠する形で規制の整備が進められてきた。国内法としては、「Außenwirtschaftsgesetz（外国貿易及び支払法：AWG)」が安全保障貿易管理、外資規制に係る根拠法令となっている[231]。

輸出規制の面では、AWG によって以下のような取引に対して制限が課されることとなる。

（AWG で規定される主な取引制限）

1. 武器、弾薬およびその他の軍事装備品、および武器、弾薬およびその他の軍事装備品の開発、製造、配備のための物品。特に、その制限が国際協力で合意された輸出規制の実施に役立つ場合

2. 軍事行動の実施を目的とした物品。

外資規制の面では、EU の共通政策に則り非 EU 居住者による国内企業等の株式の買収に関して、その買収がドイツまたは他の EU 加盟国の公序良俗や安全を損なう可能性がある場合に制限を課すこととなっており、居住性をドイツ国内と EU 域内で AWG によって規定している。また、ドイツの安全保障上の利益を保証するために、特に以下のような企業に対する外国投資についても規制の対象となる。

（AWG において外国投資規制と対象となる企業）

1. 戦争兵器またはその他の軍事装備品を製造、開発、改造するか、そのような物品を実際に管理している、または過去に戦争兵器またはその他の軍事装備品を製造、開発、改良するか、そのような物品を実際に管理していて、現在でも知識やその他の物品を処分している。そのような商品の基礎となっている技術へのアクセスが可能

2. 機密情報を処理するための IT セキュリティ機能を備えた製品、またはそのような製品の IT セキュリティ機能に不可欠なコンポーネントを製造するか、そのような製品を製造した後もその基礎となる技術を廃棄し、その製品が連邦情報セキュリティ局からライセンスを受けている

[231] https://www.gesetze-im-internet.de/englisch_awg/englisch_awg.html#p0232

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　国家戦略等

2023 年に BMWK（Bundesministerium für Wirtschaft und Klimaschutz：連邦経済・気候保護省）によって The German Federal Government’s Space Strategy が策定された。これは宇宙開発における欧州との協力に関する方針で、9 つの優先分野として、①欧州および国際協力、②成長産業としての宇宙産業、③気候変動、資源および環境保護、④デジタル化、データおよびダウンストリーム、⑤セキュリティ、戦略的行動能力、世界的な安定性、⑥持続可能な宇宙の利用、⑦宇宙の研究、⑧国際宇宙探査および⑨宇宙旅行、が挙げられている [232]。経済安全保障との関連性としては、本方針の中で、「本方針で定めている活動分野は、2030 年を目標とする連邦政府の宇宙政策の戦略的、政治的、社会経済的、科学的目標を特定し、定義するための基礎として使用される」と述べられている。

■　研究開発機関

ドイツの宇宙領域の研究開発関係機関としては、民生分野における研究では DLR(Deutsches Zentrum für Luft- und Raumfahrt：ドイツ航空宇宙センター)、防衛分野では BMVg(Bundesministerium der Verteidigung：連邦国防省）が主要な役割を担っている。DLR は BMWK が所管する機関の一つで、航空、宇宙、エネルギー、交通、セキュリティに関する研究開発を行っている。BMVg はドイツ政府が所管する政府機関の一つで、ドイツの国防政策に従って国家主権を守るための活動を行っており、民間の研究機関への研究開発支援も実施している（図 4.1-17）。

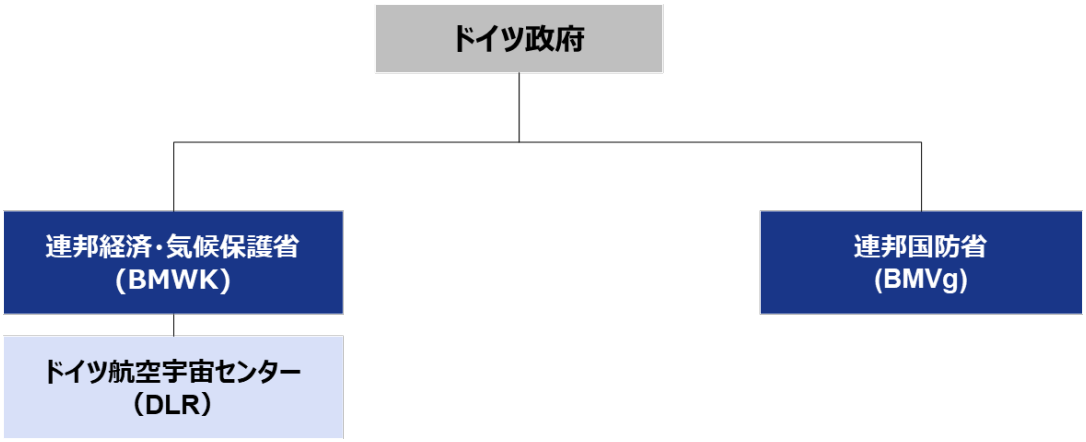


図 4.1-17　ドイツにおける宇宙領域研究開発の主要機関

[232] https://www.bmwk.de/Redaktion/EN/Publikationen/Technologie/the-german-federal-governments-space-strategy.pdf?__blob=publicationFile&v=1

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ The Environmental Mapping and Analysis Program (EnMAP)[233], [234], [235], [236], [237]

BMWK が所管するプログラムであり、ドイツで開発および製造された最初のハイパースペクトル衛星プロジェクトである。地表から反射された太陽放射を分析することで、地表の状態や変化を正確に表現することを目標としている。

本プログラムで得られたデータを使用するためには、ドイツの法律に基づいて作成された「EnMAP データ使用ライセンス契約」を締結する必要がある。本契約には、提供されたデータの販売、リース、レンタルまたはサブライセンスが禁じられ、許可なくデータを配布したり、操作可能な状態でインターネット上に公開したりすることはできない旨が記載されている。

b）海洋領域

■　国家戦略等

2016 年にドイツ政府によって National Masterplan for Maritime Technologies が策定された。これはドイツの海事部門の強化を目的として、海事産業を調整し、相互接続を行うための国家マスタープランで、将来的に重要となる技術的優先事項として民間海事セキュリティ技術（civil maritime security technologies）が挙げられている[238]。経済安全保障との関連性としては、本方針の中で、重要技術として民間開示セキュリティ技術が挙げられている。

2018 年に BMWK によって 2025 maritime research strategy が策定された。これは、海事分野の強化を目的とした研究開発戦略で、①海事全般に関わる研究（特に環境適合性とモビリティの移行、デジタル技術の使用、海上の安全とセキュリティ、海洋資源の開発の研究開発）、②海上安全とセキュリティのためのリアルタイム技術の開発、への資金提供が述べられている。経済安全保障との関連性として、海上の安全とセキュリティの研究開発、特に民間の安全とセキュリティを強化するためのリアルタイム技術が重視されている。

■　研究開発機関

ドイツの海洋領域の研究開発関係機関としては、民生分野における研究では DLR、防衛分野では BMVg が主要な役割を担っている DLR は BMWK が所管する機関の一つで、航空、宇宙、エネルギー、交通、セキュリティに関する研究開発を行っている。BMVg はドイツ政府が所管する政府機関の一つで、ドイツの国防政策に従って国家主権を守るための活動を行っており、民間の研究機関への研究開発支援も実施している（図 4.1-18）。

---

233 https://www.dlr.de/en/research-and-transfer/projects-and-missions/enmap

234 https://www.enmap.org/mission/

235 https://www.gfz-potsdam.de/en/section/remote-sensing-and-geoinformatics/projects/enmap

236 https://www.gfz-potsdam.de/en/press/news/details/ein-jahr-enmap-work-1-enmap-nutzer-workshop

237 https://www.gfz-potsdam.de/en/press/news/details/deutscher-umweltsatellit-enmap-start-in-den-regelbetrieb

238 ttps://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf

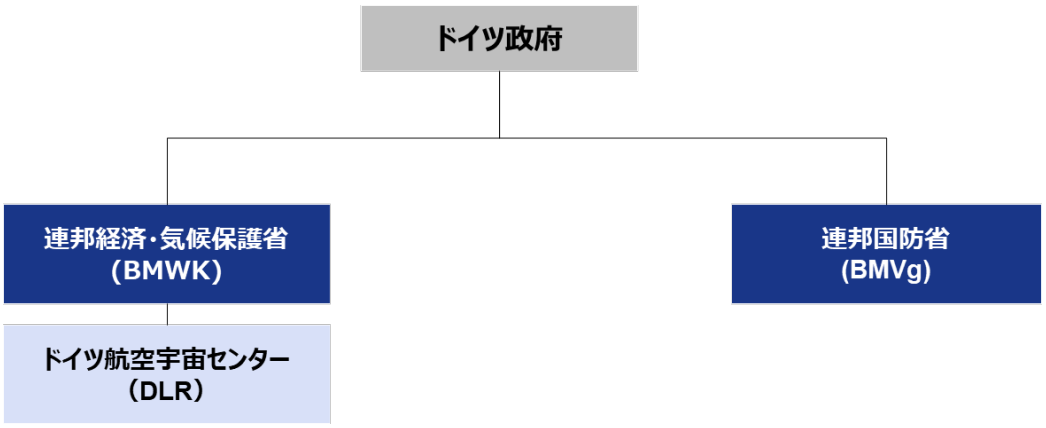


図 4.1-18　ドイツにおける海洋領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ MARITIME RESEARCH STRATEGY 2025[239, 240]

BMWK が所管するプログラムであり、国家研究コミュニティと造船および海洋技術産業を対象として資金提供を行っている。「海事セキュリティのためのリアルタイム技術」および「海事研究」を支援する。優先事項として、①海事環境保護、②海事分野のデジタル化、③海事セキュリティ、④海事資源および⑤環境ニュートラル船舶の 5 つの項目に分かれている。

本プログラムでは EU の GBER（General Block Exemption Regulation：包括的適用除外規則 [241]）が適用されており、知的財産権で保護されている研究成果については、欧州経済領域内の第三者が市場価格で使用できるようにする非独占的ライセンスを速やかに付与することが奨励されている。

c）バイオ領域

■　国家戦略等

2020 年にドイツ政府によって Global Health Strategy of the German Federal Government が策定された。これはドイツにおける健康戦略で SDGs 目標 3 も念頭に置いて策定されている。3 つの目標として、①ワンヘルスアプローチに沿った分野を超えた行動、②国内・国際・多国間レベルでの提携の強化、③様々なレベルで合意された行動の実施、が掲げられている [242]。経済安全保障との関連性としては、公衆衛生の担保は、人道及び社会経済などあらゆる分野に影響を与えるとされている。

239 https://www.ptj.de/projektfoerderung/maritime-forschungsstrategie-2025

240 https://trimis.ec.europa.eu/programme/real-time-technologies-maritime-security-mafo

241 https://eur-lex.europa.eu/EN/legal-content/summary/general-block-exemption-regulation.html

242 https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Broschueren/Global_Health_Strategy.pdf

■　研究開発機関

ドイツのバイオ領域の研究開発関係機関としては、民生分野における研究ではBMBF(Bundesministerium für Bildung und Forschung：連邦教育研究省)、防衛分野ではBMVgが主要な役割を担っている。BMBFはドイツ政府が所管している政府機関の一つで、連邦政府の研究開発資金のうち大部分を占めており、多数の資金提供プログラムを有している。その一環としてバイオ領域の研究開発への支援も行っている。BMVg はドイツ政府が所管する政府機関の一つで、ドイツの国防政策に従って国家主権を守るための活動を行っており、民間の研究機関への研究開発支援も実施している（図 4.1-19）。

図 4.1-19　ドイツにおけるバイオ領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　COMPUTATIONAL LIFE SCIENCES[243]

BMBF が所管するプログラムであり、生命科学におけるバイオインフォマティクス処理、モデリング、シミュレーションのための革新的な方法とソフトウェアツールの開発を行っている。

本プログラムにおいては、研究成果の利用範囲についてはドイツ連邦予算規則（Bundeshaushaltsordnung）に従うように求められている。

d）サイバー領域

■　国家戦略等

2021 年に BMI（Bundesministerium des Innern und für Heimat：連邦内務・国土省）によって Cyber Security Strategy for Germany 2021 が策定された。これは 2016 年に発出されたサイバーセキュリティ戦略に代わる戦略として打ち出されたもので、デジタル主権を強化し、デジタルトランスフォーメーションを促進する目的で策定された[244,245]。サイバーセキュリティ政策の長期的な方向性を定めており、指針・行動・戦略目標が記載されている。経済安全保障との関連性として、「サイバー空間における脅威は深刻であり、産業

[243] https://www.ptj.de/projektfoerderung/gesundheitsforschung/computational-life-sciences

[244] https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=BFCDD36F8AD4ECA01091D04DBAF7FC90.live872?__blob=publicationFile&v=4

[245] https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html

界と協力して重要インフラや企業を保護することが重要である」とされている。

■　研究開発機関

ドイツのサイバー領域の研究開発関係機関としては、民生分野における研究では BMBF、防衛分野では BMVg が主要な役割を担っている。BMBF はドイツ政府が所管している政府機関の一つで、連邦政府の研究開発資金のうち大部分を占めており、多数の資金提供プログラムを有している。その一環としてバイオ領域の研究開発への支援も行っている。BMVg はドイツ政府が所管する政府機関の一つで、ドイツの国防政策に従って国家主権を守るための活動を行っており、民間の研究機関への研究開発支援も実施している（図 4.1-20）。

図 4.1-20　ドイツにおけるバイオ領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　Anwendungsorientierte Quanteninformatik[246, 247]

BMBF が所管するプログラム。量子コンピューティングの潜在的な利用とその社会的、経済的影響に焦点を当てており、量子コンピューティングの実用的な利用を実証すること、またはその基礎を築くことを目的としている。

本プログラムにおいては、研究成果の利用範囲についてはドイツ連邦予算規則（Bundeshaushaltsordnung）に従うように求められている。

e）多義的技術

■　国家戦略等

ドイツの多義的技術領域における研究開発については、ドイツ連邦国防省（Bundesministerium der Verteidigung：BMVg）の文書等において言及が見られる。ドイツ連邦軍の軍事に関係する研究開発の報告書である「Military Scientific Research Annual Report 2021 Defence Research for the German Armed Forces」によると、ドイツでは軍事・防衛に関する研究開発は主に以下の 3 つの形態によって実施されるとしている[248]。

[246]https://www.foerderdatenbank.de/FDB/Content/DE/Foerderprogramm/Bund/BMBF/anwendungsorientierte-quanteninformatik.html

[247] https://www.quantentechnologien.de/forschung/foerderung/anwendungsorientierte-quanteninformatik.html

[248] https://www.bmvg.de/resource/blob/5536306/2b3d58bd18d845abe6b2e31d8caea4b6/military-scientific-research-annual-report-2021-data.pdf

（ドイツにおける軍事・防衛研究開発の形態）
1. ドイツ連邦軍の研究機関及び技術センターで行うもの
2. フラウンホーファー応用研究振興協会、ドイツ航空宇宙センター、および独仏サン・ルイ研究所と共同で行うもの
3. 産業界、大学その他の高等教育機関、大学以外の研究機関など、第三者に研究・技術契約や助成金を授与するもの

このうち、3 つ目の研究開発形態が民間企業等の研究開発実施主体に対して政府から資金提供を行い、委託研究開発を実施しているものと想定されるが、同報告書では「ほとんどのドイツ連邦軍が所管する研究開発プロジェクトはデュアルユースの原則に従い、民間の研究手法・成果を軍に取り入れている」としているため、ドイツにおいては民間の技術を軍事・防衛に対して活用するスピンオンが積極的に行われているものと考えられる。

■ 研究開発機関

前記のとおり、ドイツにおいて多義的技術領域の研究開発には、BMVg が中心となって取り組んでいる。BMVg の基に、ドイツ連邦軍の防衛装備の調達、開発、支援、および維持管理を行う Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr（連邦軍装備・情報技術・現業支援局（BAAINBw））[249]や各軍隷下の研究機関が存在している。例として Wehrtechnische Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung（船舶・海軍兵器技術局、海上技術・研究部：WTD 71）[250]が海軍には設置されており、これらの研究機関が前述の研究開発形態に基づき、多義的技術の取入れを含めた研究開発に取り組んでいると想定される。

■ 主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Analyse und Gestaltung des programmatischen Umfelds für den Schutz von Weltraumsystemen[251]

BMVg が所管するプログラムであり、「宇宙システムの保護」の分野における既存の国内および国際的なイニシアティブとプロジェクトを分析し、ドイツの参加の可能性に関してそれらの付加価値を評価することを目的としている。本プロジェクトによって得られた成果をもとに、ドイツの宇宙システムを保護するために必要な活動のための国家行動の枠組みの提案を行う想定をしている。

本プログラムにおいては、VS-ONLY FOR SERVICE USE (VS-NfD) - BAAINBw-B 096a の機密情報 (VS) の取り扱いに関する規定に準拠する必要がある。また、本プログラム期間中および終了後においても関連する法規制（具体的記載はなし）に従って本プログラムから得られた全ての秘密情報の保護を行う必要がある。

249 https://www.bundeswehr.de/de/organisation/ausruestung-baainbw/organisation/baainbw
250 https://www.bundeswehr.de/de/organisation/ausruestung-baainbw/organisation/wtd-71
251 https://www.evergabe-online.de/tenderdetails.html?12&id=588994

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして 11 件リストアップした（詳細は Appendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも 1 つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして 3 件抽出した（表 4.1-18)。

表 4.1-18　詳細調査を行う法令等のショートリスト

法令等の名称	理由
Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen（連邦保安審査に関する機密事項の保護に関する法律）	機密情報の保護のためのセキュリティチェックが規定されている法律のため
Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz(資料の秘密保護のための一般管理規則（機密事項指定規則）)	機密情報の取扱いや手順について規定されている法律のため
Außenwirtschaftsgesetz（外国貿易及び支払法）	安全保障上、脅威と思われる取引についての規制が規定されている法律のため

以下に表 4.1-18 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen（連邦保安審査に関する機密事項の保護に関する法律）[252]

■　策定機関・策定時期

1994 年

■　策定の背景・目的

公共及び非公共分野の機密情報の保護、機密情報を取扱う人物に対するセキュリティチェック（再審査を含む）の要件および手順に関する規定である。保護対象となるのは、機密情報と重要施設で、セキュリティチェック対象者は、機密情報を取扱う者、外国から機密情報にアクセスできる者である。セキュリティチェックの責任機関が、セキュリティ管理を効果的に行えるようにすることを目的としている。

[252] https://www.gesetze-im-internet.de/s_g/BJNR086700994.html

■　適用範囲

所管官庁からセキュリティ上重要な活動を委託される者、またはすでに委託されている者における機密情報の保護と、保護に関する手順を対象としている。

本法令では、「目的や範囲などの一般条項」「検証・実施手段の種類」「手続き」「セキュリティ・クリアランスとデータ処理」「非公共部門に対する特別規制」「渡航制限、外国からの要請によるセキュリティ・クリアランス」に項目を分けて説明がなされている。

■　情報の分類

公的機関による保護の必要性に応じて、以下のように分類されている。

（ドイツにおける保護対象情報の分類）

- **STRENG GEHEIM（最高機密）：無許可のアクセスにより、ドイツ連邦共和国の存続または重大な利益が脅かされる可能性がある情報**
- **GEHEIM（機密）：無許可のアクセスにより、ドイツ連邦共和国の安全が脅かされ、またはその利益に重大な損害がもたらされる可能性がある情報**
- **VS-VERTRAULICH（VS 秘密）：無許可のアクセスにより、ドイツ連邦共和国の利益が損なわれる可能性がある秘密**
- **VS-NUR FÜR DEN DIENSTGEBRAUCH（VS 業務利用のみ）：無許可のアクセスにより、ドイツ連邦共和国の利益を害する可能性がある情報**

■　情報管理策

機密情報を取扱う人へのセキュリティチェック方法を示す組織的管理策のみ記載されているため、組織的・物理的・技術的管理策は規定していない。

・　人的管理策

機密情報を取扱う人物に対するセキュリティチェックの実施を規定している。情報の分類に応じてセキュリティチェックを実施し、調査当局には、必要と認められる調査対象者のデータの収集が許可されている。セキュリティチェックの再審査は、基本的に 10 年ごとに実施するが、必要に応じて別途実施することができる。

・

■　罰則

この法律で保護されている公開されていない個人情報を不正に使用した場合、1 年以下の懲役または罰金が科せられる可能性がある。また、加害者および他人が報酬を得ることを目的とする、あるいは他人に危害を与える目的であった場合は、 2 年以下の懲役または罰金が科せられる可能性がある。

b）Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz（資料の秘密保護のための一般管理規則（機密事項指定規則））[253]

■　策定機関・策定時期

2023 年

■　策定の背景・目的

機密情報の取扱い要件および手順に関する規定である。技術的および組織的対策を組み合わせることで、攻撃によるリスクや悪影響の軽減を目的としている。政府間組織（EU や NATO 等）を含む海外機関との機密情報の開示についても規定している。

■　適用範囲

機密情報の取扱い要件や手順を対象としており、「目的や範囲などの一般条項」「機密情報保護機関と機密保護の文書化」「分類と制限」「海外の公的および民間機関との協力」「マテリアルと技術対策」「情報技術の使用」「情報の暗号化担当者および暗号化された資産の取扱い」に項目を分けて説明がなされている。

（各機関における機密情報の管理方針）

- 機密情報に関する指示は、機密情報を扱う連邦当局及び連邦政府直轄の公的機関（部門）、及び機密情報にアクセスできる、または機密情報にアクセスできる活動を実行する場で働く人を対象としている。連邦議会及び連邦参議院と協力して、各省庁はこの機密情報の指示を独占的に適用する
- 連邦諜報機関における機密保護に関する一般行政規則は、連邦内務省の同意を得て所轄の最高連邦当局が発布をする
- 連邦経済・気候行動省は、連邦内務省と合意の上非公共部門における機密保護に関 s るう一般行政規則を発布する
- 連邦国防省は、軍事治安当局として連邦内務省と合意をとり連邦国防省の責任領域における機密保護に関する一般行政規則を発布する

■　情報の分類

機密情報の概念と分類レベルは以下のように規定されている。

（Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz で示される機密情報の概念）

- 機密情報とは、公共の利益のために特に連邦政府または連邦国家の福祉を守るために、その表現形式を問わず、秘匿を必要とする事実、対象物、調査結果を指す（文書、図面、地図、コピー、写真資料、電子ファイル及びデータキャリア、電気信号、装置、技術設備、話し言葉等）。ビジネス、企業、発明、税務、その他の個人的な秘密や個人的な事情も、公共の利益のために守秘を必要とする場合がある
- 機密情報は、安全保障審査法第 4 条(2)に従い、部門による保護の必要性に応じて、また

[253] https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SII554001405.htm

は部門の発意により、以下の分類レベルに分類される
  - 最高機密（STRENG GEHEIM）：無許可のアクセスがドイツの存立または重大な利益を危険にさらす可能性がある場合
  - 極秘（GEHEIM）：権限のない者がアクセスすることにより、ドイツの安全が脅かされる、またはその英駅に重大な損害が生じる可能性がある場合
  - 機密（VS-VERTRAULICH）：権限のない者によるアクセスがドイツの利益を損なう可能性がある場合
  - 公用限定（VS-NUR FÜR DEN DIENSTGEBRAUCH）：権限のない者によるアクセスがドイツまたはその連邦州の利益を害する可能性がある場合
- 機密文書は、それが不法に知られた場合であっても、機密のままでなければならない

■　情報管理策

機密情報への責任の所在を示す人的管理策と、機密情報の管理方法を示す物理的管理策、機密情報の具体的な管理方法を示す技術的管理策、機密情報の保護を行う組織について規定されている組織的管理策がある。

・　組織的管理策

以下の取り組みにより機密情報の取り扱いに関する責任の明確化を行っている。

（Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz で示される機密情報の保護を行う組織体制）
- 部門長：部門の長は、その責任の範囲内で、この機密情報の指示の実施に責任がある。機密情報保護を確保するための条件を作成する必要がある。この業務のすべてまたは一部を部署のメンバーへ委任することが可能
- 機密情報保護官
  - 機密（VS-VERTRAULICH）以上に分類される機密情報を扱う部門は、機密情報保護官とそれを代表する権限のある人物を任命する必要がある。それ以外の場合にはおいては、部門長が機密情報保護官の職務を遂行する
  - 公用限定（VS-NUR FÜR DEN DIENSTGEBRAUCH）に分類された機密情報を独占的に扱う部門は、機密情報保護官及びそれを代表する権限のある人物を任命することが出来る。それ以外の場合は、部門長が機密情報保護官の職務を遂行する
  - 機密情報保護官は、この機密情報に関する指示を確実に実施し、機密情報の保護に関連する全ての事項について部門長に助言を行う。機密情報保護官は、各部門長に直接提言する権利を有する。機密情報保護官は、機密情報保護に関連する全ての措置に関与する必要がある。部門内において、機密情報保護官を支援するために特別職員（シークレットサービスオフィサー等）を任命することが可能
  - 機密情報保護官又は特別職員は、機密情報の取り扱い責任者に対して、このAllgemeine Verwaltungsvorschrift zum materiellen Geheimschutz（資料の秘密保護のための一般管理規則（機密事項指定規則））その他の機密情報保護に関する規定を周知させるために適切な措置を講じる必要がある

・　人的管理策

以下の取り組みにより機密情報に対する責任の明確化を行っている。

- 機密情報の責任者を任命する。情報保護管理者、IT セキュリティ管理者、機密情報登録官については、必要な専門知識を有する者を任命する
- 責任者は、適用される法令を考慮した機密情報の取扱い方法の文書化を行い、少なくとも 3 年ごとに見直しを行う
- 責任者は、かかる文書を従業員に公開することで、機密情報の適切な取り扱いを確保する

また、機密情報の取り扱いについて、以下のような人的管理策を実施している。

（Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz で示される機密情報の人的管理策）

- 機密情報は、職務を遂行するために知る必要のある者にのみ開示することができる。いかなる者に対しても、職務の遂行に必要な範囲を超えて、または必要な時期よりも早く、機密情報を知らせてはならない。必要な場合にのみ知るという原則が適用される
- 機密（VS-VERTRAULICH）またはそれ以上の機密情報へのアクセス権を付与される者、またはアクセス権を取得できる者は、機密情報アクセス法第 2 条第 3 項第 1 文第 1 号または第 2 号に基づき、その職責により機密情報にアクセスできる場合を除き、まず機密情報アクセス法に従って機密情報アクセス許可を受けなければならない
- 機密情報が委託され、またはアクセスできるようにされた者は、その機密情報をどのようにして知り、また所有するようになったかに関わらず、その適切な取り扱いについて個人的責任を負わなければならない

・ 物理的管理策

CONFIDENTIAL 以上の機密情報の作成は、決められた場所で、決められた手順によってのみ実施し、機密情報であることを既定の方法で表示することで、機密情報に対する責任の明確化を行っている。また、入館時の ID カードによる認証などにより、機密情報を取扱う場所へのアクセス権限を持たない者の侵入を防ぐことで機密情報の物理的保護を行っている。

・ 技術的管理策

IT 技術（アクセス制御、認証、情報の暗号化、情報フロー制御等）を用いることで機密情報のライフサイクルを通じて保護を行っている。

■ 罰則

記載なし

c）Außenwirtschaftsgesetz（外国貿易及び支払法）[254]

■　策定機関・策定時期

2013 年

■　策定の背景・目的

ドイツや他の EU 加盟国の公安および安全保障に対する脅威となる可能性がある海外との取引について規制を行うことを目的としている。規制対象として、物品取引（兵器）および外資によるドイツ企業（軍事および IT セキュリティ関連企業）への出資を含む金銭取引が想定されている。

■　適用範囲

ドイツや他の EU 加盟国の公安および安全保障に対する脅威となる可能性がある海外との取引を対象としており、「目的や範囲などの一般条項」「附則」「罰則」「最終条項」に項目を分けて説明がなされている。

■　情報の分類

海外とのやり取りにて規制される取引については規定されているが、情報の部類については規定していない。

■　情報管理策

海外とのやり取りで規制される事柄を示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

ドイツや他の EU 加盟国の公安や安全保障の保護を目的として以下が規定されている。

（Außenwirtschaftsgesetz で示される情報の組織的管理策）
- 連邦政府の条例による海外貿易や決済の規制が可能である
- 特定の分野（軍事および IT セキュリティ機能を有する製品）の取引についてライセンス制が可能である。必要なライセンスを得ていない法的契約は無効となる
- 管轄当局は、欧州共同体または欧州連合の直接適用法に基づき、特定の個人またはパートナーシップの金銭や経済資産の追跡および凍結が可能である
- 税関、ドイツ連邦銀行、連邦経済・輸出管理庁（BAFA）および連邦農業・食料庁は、本法律や関連条例の遵守の監視に必要な情報提出を求めることができる
- BAFA、ドイツ連邦銀行、連邦デジタル・交通省（BMDV）など第 13 条で規定されている連邦機関は、必要に応じて、個人データを含む情報を他の連邦機関に送信できる
- 情報の送受信について、送信の許容性に関する責任は所管官庁が負う。送信が受信機関の要求によって行われる場合には、責任は受信機関が負う

[254] https://www.gesetze-im-internet.de/awg_2013/

・　税関犯罪事務局は、個人情報検索の許容性について責任を負う。税関犯罪事務局のリーダーシップによって許可された職員のみが個人情報検索可能

■　罰則

ドイツや他の EU 加盟国の公安や安全保障の保護を目的とする条例に違反した場合、1-10 年の懲役や罰金が科せられる可能性がある。また、経済制裁を目的とする EU 法令またはライセンス要件への違反、デュアルユース用途の製品に関わる規制等に違反した場合、3 か月-5 年の懲役や罰金が科せられる可能性がある。加えて、当局に正しい情報を適切なタイミングで提供しなかった場合、罰金が科せられる可能性がある。

(6) フランス

1) 基本情報

- 政治体制：共和制
- 人口：約 6,804 万人(2023 年)[255]
- 名目 GDP：2 兆 9230 億ドル (2023 年)、実質 GDP：2 兆 3720 億ドル(2023 年)[256]
- 研究開発予算：76,952（100 万米ドル）（2021 年度） OECD

■ 政治動向

現在のマクロン政権は、多国間主義、気候変動、経済分野での国益追求といった目的を掲げる。仏独の連携を軸とした欧州における協力を積極的に推進し、自主性に基づく国防・外交を展開する意向。2018 年には仏のインド太平洋戦略更新版を策定した。2022 年 1 月から 6 月まで、EU 議長国を務める等国際的にも重要な立場にいた。

フランスは伝統的に国連を中心とした「国際協調」の重要性を主張しており、欧州統合を積極的に推進し、EU を通じたフランスの影響力拡大を目指す方針としている。

■ 経済動向

フランスは、西欧最大規模の農業を誇るとともに、工業に関しても自動車産業、宇宙・航空産業、原子力産業等の先端産業が発達している。GDP は世界 7 位であり、2015 年以降については緩やかな成長をしていた。コロナで 2020 年は－8%まで落ちたが、2021 年には 7%を記録している。

2 任期目に入ったマクロン大統領は、労働市場の柔軟化や SNCF 改革、エコロジー転換の加速や、能力向上・雇用等への 570 億ユーロ規模の投資、法人税率引下げを通じて、高失業率の改善や経済の活性化を図った。また、フランス政府は 2020 年 9 月に総額 1,000 億ユーロ規模の経済対策「France Relane（フランス再興プラン)」を発表。経済・生産構造のエコロジー転換、デジタル化等を進めるための施策も打ち出している。

■ 社会動向

フランスの GDP は世界 7 位であり経済規模は大きいが、一方で 2022 年の第 1 四半期の失業率は 7.3%で先進国の中でも高い失業率であり、慢性的な雇用問題を抱えている。

■ 技術動向

フランスは 2021 年に「複数年研究計画法」を発表した。この法律により、公的研究予算を段階的に増額、研究者のポスト増加、条件の改善、起業する研究者への支援、研究資金面での改善を行うとしている。

2021 年にはフランス政府が重視する領域に対して重点投資を行う「France2030」を発表した。2023 年 4 月には「France2030」の目標のテーマに沿った起業の支援を行う

[255] https://www.mofa.go.jp/mofaj/area/france/data.html

[256] https://www.imf.org/external/datamapper/profile/FRA

「FrenchTech2030」の開始を発表した。採択された企業は、規制、サイバーセキュリティ、投資等に関する専用の支援を受けることが可能になる。

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

フランスでは、1992 年に策定された「フランス刑法」の罰則において、国防上の利益を有するプロセス、物件、文書、情報、コンピュータネットワーク、コンピュータ化されたデータ又はファイルであって、その普及又はアクセスを制限することを意図した分類措置の対象となったものを国防上の秘密として分類し、その情報を職業等で任意に保持するものが、破壊、横領、複製等した場合には禁錮および罰金刑が科されると規定されている。[257]

また、2011 年には「Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale（2011 年 11 月 30 日、国防秘密保全に関する省庁間一般通達第 1300 号)」が策定され、その中で、秘密情報の保護に関する一般原則として、防衛、治安、金融・経済産業の保護、科学・文化遺産の保護等の活動全般等に関する情報等を国防秘密として定義し、「Code de la défense（国防法典)」の分類に従い、それらの情報を「最高機密(Très Secret)」、「極秘(Secret)」、「機密(Confidential Defense)」の 3 つのレベルに区分している[258, 259]。

2015 年には、1978 年に規定された「La loi n° 78-753 du 17 juillet 1978 a instauré un droit d'accès des citoyens aux documents administratifs（行政および公衆間の関係改善のための諸措置ならびに行政・経済・社会制度改善にかかわる諸措置に関する 1978 年 7 月 17 日法律)」に代わり「Code des relations entre le public et l'administration（公衆と行政の関係に関する法典)」が制定され、情報公開を要求される情報の内、政府および執行権にかかわる責任ある機関における審議の秘密、防衛上の秘密、フランスの対外政策の実施、国家の安全、治安、人々の安全又は行政機関の情報システムの安全、通貨と公債、裁判所の手続又は予審手続の実施（但し、権限ある機関による承認がある場合は除く)、捜査機関によるあらゆる犯罪の捜査および予防、環境法典等の情報については不開示情報として規定されている。

また、2021 年には、デジタル化の発展や安全保障政策における民間事業者や外国のパートナーとの交流の発展等の状況の変化に対応すること等を目的に、「より良い保護のためのより良い分類」を原則として 2011 年 11 月 30 日、国防秘密保全に関する省庁間一般通達第 1300 号の見直しが行われた。国防法典と同様に、３つあったレベル分けの内「機密(Confidential Defense)」を分類から削除し、秘密として保護される情報を、厳密に必要なものに限定するとともに、分類レベル別の保護措置を同盟国等の国際的な基準に合わせている[260, 261]。また、本見直しにおいては、国防秘密の使用を厳格に管理するという原則に基づき、特に、機密情報の分類と管理に関する規則の明確化が行われている[262]。

---

257 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000020933029

258 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039445194/2024-02-18/

259 https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000033293465

260 https://www.sgdsn.gouv.fr/files/files/Nos_missions/igi-1300-20210809.pdf

261 https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-secret-de-la-defense-nationale/reforme-de-la-protection-du-secret

262 https://www.vie-publique.fr/eclairage/281595-reforme-de-la-politique-de-protection-du-secret-de-la-defense-nationale

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

フランスでは、安全保障貿易関連等の内、輸出管理については2009年に制定された、EU規則の「Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items（二重用途物品の輸出、移送、仲介および輸送の管理に関する EU 域内体制を確立する2009年5月5日付理事会規則428/2009)」に準拠している。この法令では、多義的技術品目（ソフトウェアや技術を含む）の輸出、移送、仲介および輸送の管理制度の確立を目的とし、多義的技術品目リストに掲載されている物品の輸出は、管理当局の認可を必要とする他、リストに不記載であっても、輸出先国や流用等の懸念がある場合は、許可が必要となる等、多義的技術の流出防止のための規程が定められている[263]。

また、その他の第三国向けの輸出に関する共通規則として 2015 年に制定された、「Regulation (EU) 2015/479 of the European Parliament and of the Council of 11 March 2015 on common rules for exports（共通輸出規則に関する2015年3月11日付欧州議会・理事会規則2015/479)」に準拠しており、全ての工業製品および農産物に適用で公序良俗、公共政策または公安、または人間、動物、植物の健康と生命の保護、国宝、または産業的および商業的財産の保護を目的とする措置が必要な物に対して規制をかけている。

外国投資規制については、2019 年に「Décret n° 2019-1590 du 31 décembre 2019 relatif aux investissements étrangers en France（フランスへの対内投資に関する命令2019年12月31日第2019-1590号)」が制定されており、投資規制について、既存の審査対象事業だった防衛事業やエネルギー等公共の安全又は国家防衛にとって重要な事業に加え、新たに AI、半導体等の重要な技術に係る研究開発分野への投資についても財務省の事前認可が義務付けられた他、EU/EEA（European Economic Area）の域外の投資家に限っては、支配権の獲得のみならず一定の閾値（2019 年に 33%から 25%に引き下げ（上場企業の議決権については2023年12月31日まで10%））を超える議決権の取得についても対内直接投資に係る規制の対象とされた[264]。

263 https://eur-lex.europa.eu/eli/reg/2009/428/oj

264 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039727443

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　国家戦略等

2019 年に“Space” working group（軍事省を中心とする作業部会）によって SPACE DEFENCE STRATEGY が策定された。これは 2030 年までの宇宙防衛開発に関する指針で、宇宙防衛の強化、宇宙に関するガバナンスの整理、宇宙における研究開発の強化、専門知識の開発などについて述べられている [265]。経済安全保障との関連性としては、本指針の中で、「防衛において宇宙領域は基礎であり、欧州のパートナーと協力強化しつつ産業界とも関係構築することが必要」と述べられている。

■　研究開発機関

フランスの宇宙領域の研究開発関係機関としては、民生分野における研究では CNES (Centre national d'études spatiales：フランス国立宇宙研究センター)、防衛分野では AID(Agence de l'innovation de défense：防衛イノベーション庁）が主要な役割を担っている。CNES はフランス政府が所管する研究機関の一つで、フランスの宇宙政策を立案・管理・実施している。フランスの宇宙戦略「宇宙へのアクセル」「地球観測」「宇宙利用」「宇宙科学」「安全保障」に包括的に取り組んでいる。AID は軍事省が所管する政府機関の一つで、軍事省内におけるイノベーション関連業務の調整や、民間部門でのイノベーションの動向把握、有望な技術の取得、技術革新プロジェクトへの資金提供を行っている（図 4.1-21）。

図 4.1-21　フランスにおける宇宙領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　SPACE SURVEILLANCE AND TRACKING (SST)[266]

フランス政府が所管するプログラムであり、CNES を含む EU-SST コンソーシアムが参画している。法的枠組みとして 2030 年まで EU の重要宇宙インフラ保護を目的とするプロジ

[265] https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2020/08/france_-_space_defence_strategy_2019.pdf

[266] https://sst.cnes.fr/en/sst-space-surveillance-and-tracking-0

ェクトであり、衛星や軌道上のデブリの記録とカタログ化を行う。CNES は、衝突警報を処理する運用軌道決定センターの運用活動や、欧州レベルでのこのシステムの将来のアーキテクチャの定義への貢献を通じて、EU-SST コンソーシアムの活動を支援している。また宇宙監視と追跡は国家安全保障の問題であり、CNES はフランス軍事省とも緊密に連携している。

本プログラムにおいては、REGULATION (EU) 2021/696 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL に従って情報管理を行っており、EU に本部を置いていない機関が非公開情報にアクセスする場合は第 218 条に従って契約締結を結ぶ必要がある。

b) 海洋領域

■ 国家戦略等

2014 年に SGMer (Secrétariat général de la Mer:海洋総局)によって Action de l'État en mer (AEM)が策定された。防衛任務以外において、自らの資源を使用して公共の利益のために実行するすべての海上作戦について規定しており、海上の安全確保、海洋警備、海洋汚染の防止等が述べられている [267]。経済安全保障との関連性として、安全保障の観点から、「SGMer と SGDSN (Secrétariat général de la défense et de la sécurité nationale : 国防安全保障事務総局) は関係省庁と協力して、テロや海賊行為に対抗すべき予防、保護、対応システムの恒久的な改善に取り組む」とされている。

2015 年に the inter-ministerial sea committee にて National strategy for the security of maritime areas が策定された。EUMSS (European Union Maritime Security Strategy : EU 海洋安全保障戦略) の補完を目的としたフランスの海洋安全保障に関する国家戦略で、海洋での安全保障に対して包括的かつ分野横断的に取り組むことを述べている [268]。経済安全保障との関連性として、海洋安全保障は、「経済的及び環境的利益の保護と、フランスの国内・国際海域における領土保全及び国民の安全確保に関係する」と述べられている。

■ 研究開発機関

フランスの海洋領域の研究開発関係機関としては、民生分野における研究では Ifremer (Institut Français de Recherche pour l'Exploitation de la Mer : フランス海洋開発研究所)、防衛分野では AID が主要な役割を担っている。Ifremer は MESRI (Le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation : 高等教育・研究・イノベーション省) 、MTES (Ministère de la Transition écologique : 環境連帯移行省)、MAA (Ministère de l'Agriculture et de la Souveraineté alimentaire : 農業・食品省) が所管する国立研究所の一つで、持続可能な海洋資源開発、海洋保護、海自部門の社会経済的発展のための基礎研究と応用研究、専門家による評価、技術開発および産業開発の実施や促進を行っている。AID は軍事省が所管する政府機関の一つで、軍事省内におけるイ

[267] https://www.gouvernement.fr/action-de-l-etat-en-mer-sgmer

[268] https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2016/01/strategie_nationale_de_surete_des_espaces_maritimes_en_national_strategy_for_the_security_of_maritime_areas.pdf

ノベーション関連業務の調整や、民間部門でのイノベーションの動向把握、有望な技術の取得、技術革新プロジェクトへの資金提供を行っている（図 4.1-22）。

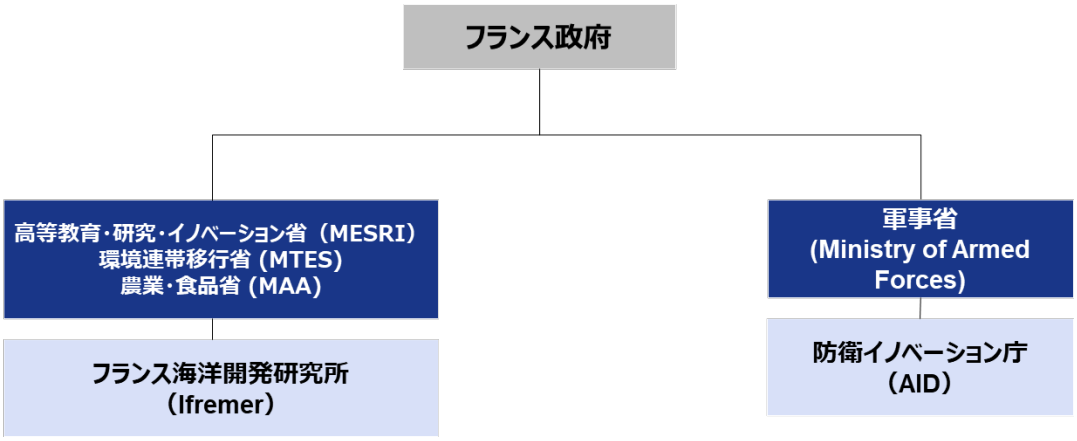


図 4.1-22　フランスにおける海洋領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Ocean & Climate: an ocean of solutions プロジェクト [269, 270, 271, 272]

CNRS（Centre national de la recherche scientifique：フランス国立科学研究センター）および Ifremer が所管するプログラムであり、大統領が設立した優先研究プログラムとして、主な科学的課題 に関する研究の支援を行う。対象は①海外県における気候変動に関わる極端な現象からの保護政策、②極海研究の強化、③海洋生態系の保護を目的とする海洋の「exposome（人間の健康に影響を与える環境暴露）」の特性把握、④海洋のより適正な理解に向けて革新的な観測・モデル化・プログラムの開発、⑤新しい統合管理方式の開発を通じた海洋環境の保護と回復力の向上、⑥持続可能性の科学に基づく海洋資源の活用、⑦参加型科学とオープンサイエンスアプローチを通じた科学的発見と海洋問題の公開に関する研究である。予算（4,000 万ユーロ）は MESRI と SGPI（Secrétariat général pour l'investissement：投資総局）から配分を受ける。

本プログラムにおいては、Deuxième Plan national pour la science ouverte（Second National Plan for Open Science：第 2 次オープンサイエンス国家計画 [273]）に従って成果物を公開するように求められている。

c）バイオ領域

■　国家戦略等

2022 年に MEAE（ Ministère de l'Europe et des Affaires étrangères：欧州外務省）に

[269] https://sdgs.un.org/partnerships/france-priority-research-program-ocean-and-climate-ocean-solutions

[270] https://www.ocean-climat.fr/

[271] https://www.ocean-climat.fr/content/download/156161/file/PPR20210609_VF.pdf

[272] https://crds.jst.go.jp/dw/20210624/2021062429119/

[273] https://www.ouvrirlascience.fr/second-national-plan-for-open-science-2021-2024/

よってFrance global health strategy 2023-2027が策定された。これはフランスにおける健康戦略で、5つの目標として、①持続可能な発展への貢献（SDGs目標3）、②健康における不平等の軽減、③パンデミックへの予防、④気候変動による健康への影響への対処、⑤研究開発の促進、が掲げられている[274,275]。経済安全保障との関連性として、リスクを予防し、検出し、対応できる強靭な保健システムを構築することが、健康安全保障において重要とされている。

■　研究開発機関

フランスのバイオ領域の研究開発関係機関としては、民生分野における研究ではANR（Agence nationale de la recherche：国立研究機構）、防衛分野ではAID　が主要な役割を担っている。ANRはMESRが所管する政府機関の一つで、研究プロジェクトに対する研究資金の融資やプログラムの管理を実施している。学際的な共同プロジェクトの出現を促進し、官民協力を奨励することによってイノベーションを刺激することを目的としている。AIDは軍事省が所管する政府機関の一つで、軍事省内におけるイノベーション関連業務の調整や、民間部門でのイノベーションの動向把握、有望な技術の取得、技術革新プロジェクトへの資金提供を行っている（図 4.1-23）。

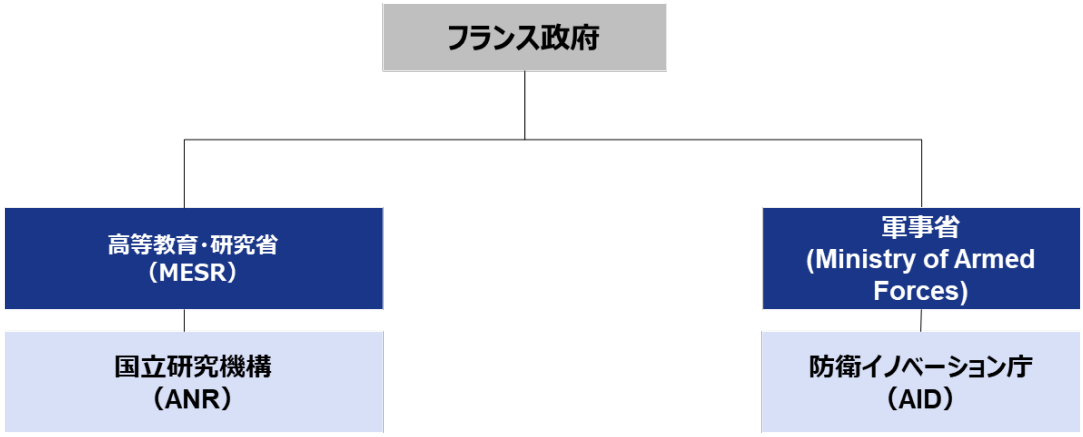


図 4.1-23　フランスにおけるバイオ領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Accompagnement spécifique des travaux d’intérêt Défense (ASTRID)Edition 2023[276]

ANR と AID が共同で所管するプログラムであり、防衛、民間研究、産業の各分野にとって有益な技術革新の源となる、潜在的なブレークスルーを特定することを目指している。ASTRID プログラムの下で実施されるプロジェクトは、将来の防衛・安全保障システムに必要かつ有用な技術の進化を予測し、制御することを目的とした AID 活動の一般的枠組みの一部である。また、本プログラムにより大規模な科学・産業コミュニティを創造し、民間

[274] https://www.diplomatie.gouv.fr/IMG/pdf/a5_strategy_global_health_v2_bd_cle49712b.pdf

[275] https://www.diplomatie.gouv.fr/en/french-foreign-policy/development-assistance/priority-sectors/health/france-and-international-health-security

[276] https://anr.fr/fileadmin/aap/2023/aap-astrid-2023-v4.pdf

研究との相乗効果を維持・発展させることも目指している。

本プログラムにおいては、国家科学技術保護令に従って科学技術的潜在力を保護するシステム（PPST：the system for protecting the scientific and technical potential of the nation）の対策を実施することが求められる。

d）サイバー領域

■　国家戦略等

2017 年に MEAE によって Stratégie internationale de la France pour le numérique が策定された。これはフランスの国際デジタル戦略で、基本的権利の尊重、公正な競争などを基本的な考え方としており、①オープンな国際デジタル環境の維持、②自由・成長・安全と基本としたデジタル環境の促進、③フランスにおけるデジタル市場の活性化、について述べられている [277]。経済安全保障との関連性として、外交政策の観点においても、「フランス経済の発展や世界規模での安全・安心・優位性の確保において、デジタル技術は重要な問題である」とされている。

■　研究開発機関

フランスのサイバー領域の研究開発関係機関としては、民生分野における研究では ANR、防衛分野では AID が主要な役割を担っている。ANR は MESR が所管する政府機関の一つで、研究プロジェクトに対する研究資金の融資やプログラムの管理を実施している。学際的な共同プロジェクトの出現を促進し、官民協力を奨励することによってイノベーションを刺激することを目的としている。AID は軍事省が所管する政府機関の一つで、軍事省内におけるイノベーション関連業務の調整や、民間部門でのイノベーションの動向把握、有望な技術の取得、技術革新プロジェクトへの資金提供を行っている（図 4.1-24）。

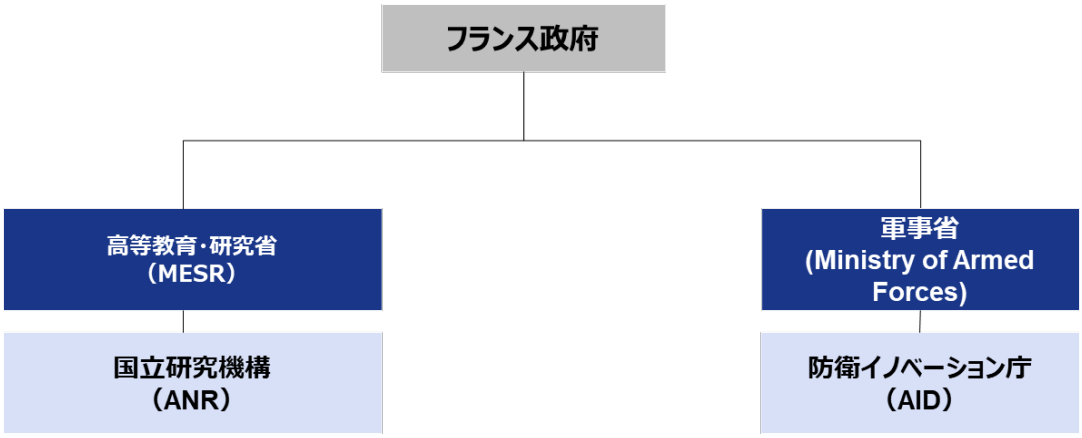


図 4.1-24　フランスにおけるサイバー領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　Accompagnement spécifique des travaux d’intérêt Défense (ASTRID)Edition

[277] https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf

2023[278]

ANR と AID が共同で所管するプログラムであり、防衛、民間研究、産業の各分野にとって有益な技術革新の源となる、潜在的なブレークスルーを特定することを目指している。ASTRID プログラムの下で実施されるプロジェクトは、将来の防衛・安全保障システムに必要かつ有用な技術の進化を予測し、制御することを目的とした AID 活動の一般的枠組みの一部である。また、本プログラムにより大規模な科学・産業コミュニティを創造し、民間研究との相乗効果を維持・発展させることも目指している。

本プログラムにおいては、国家科学技術保護令に従って科学技術的潜在力を保護するシステム（PPST：the system for protecting the scientific and technical potential of the nation）の対策を実施することが求められる。

e）多義的技術

■　国家戦略等

フランスでは、2006 年に ANR（Agence nationale de la recherche：国立研究機構）と軍事省参加の DGA（Direction générale de l'armement：軍事装備総局）が多義的技術研究に資する目的でパートナーシップを結んで以降、多義的技術に関する研究開発が推進されるようになり、2019 年には、ANR と DGA 傘下の AID（Agence de l'innovation de defense：国防イノベーション庁）についてもその協力関係を拡張する形でパートナーシップを結んでいる[279]。

また、2018 年には 2019～25 年の間、軍事・防衛関係の一般会計予算を毎年増やしていく具体的な目標を示した国の中期計画である「複数年軍事計画法」が制定されており、この法令の中で多義的技術に関する研究開発を含む防衛分野の研究開発についても重要視されている[280]。

プログラム関係においては、2011 年に AID 所管の ASTRID というプログラムが実施されている。ASTRID は、多義的技術に関する研究支援を行うプログラムであり、国防、民間研究、産業への潜在的な応用を伴う科学的・技術的進歩の促進を目的として、技術的成熟度レベル（TRL）1～4 のプロジェクトを支援する。傘下の国防イノベーション庁（AID）が資金を提供し、国立研究機構（ANR）が実施する。提出されたプロジェクトは 40 人以上の一流の科学者からなる評価委員会によって評価等が行われ、2011 年の創設以来、327 件のプロジェクトが選定されている。2022 年の ASTRID プログラムにおいては、情報工学、サイバー防衛、ナノテクノロジー--センサーとコンポーネント、フォトニクス、人工知能等の分野において募集が行われていた[281,282]。

---

278 https://anr.fr/fileadmin/aap/2023/aap-astrid-2023-v4.pdf

279 https://anr.fr/fr/actualites-de-lanr/details/news/signature-dun-accord-de-cooperation-entre-lagence-nationale-de-la-recherche-et-lagence-de-linno/

280 https://www.defense.gouv.fr/sites/default/files/ministere-armees/JOE_20180714_0161_0001_LPM2019-2025.pdf

281 https://anr.fr/en/call-for-proposals-details/call/specific-support-for-defence-research-projects-and-innovation-astrid-2022/

282 https://anr.fr/en/call-for-proposals-details/call/the-2023-call-for-proposals-astrid-maturation-specifi

ASTRID で成果を出したプロジェクトについては、2013 年に創設された TRL 5 以上のプロジェクトの支援を行うプログラムである ASTRID Maturation プログラムや、連結従業員数 2,000 人未満の企業が単独またはコンソーシアムで実施する多義的技術に関する研究開発に対する補助金制度であり、産業研究（TRL 3～5）または実験開発（TRL 6～7)を対象とした RAPID プログラムに応募することが可能である。(ASTRID（TRL 1～4）の 2011 年から 15 年までのプロジェクトの約 20%が（後継プロジェクトとして）ASTRID Maturation の資金提供を受けている[283]。

■ 研究開発機関

フランスの多義的技術に関する研究開発を行っている主な組織には ANR と AID が挙げられる。ANR は MESRI(Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation：フランス高等教育・研究・イノベーション省)の傘下にある 2005 年に設立された研究資金配分機関であり、科学・学術のあらゆる分野で公的事業者が相互に、または民間企業と協力して実施するプロジェクトベースの研究を募り、採択したものに対して資金提供を実施している[284]。

また、AID は、軍事省の DGA 傘下の部局であり、技術革新と科学技術研究に関する閣僚政策の実施に責任を負い、この分野で職員、部局、部局が策定する戦略を指導する他、ASTRID プログラム、ASTRID Maturation プログラムをはじめとした多義的技術に関する研究開発プログラムを所管している[285]。

■ 主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

- Accompagnement Spécifique des Travaux de Recherches et d'Innovation Défense : appel thématique sur l'extension des zones conflictuelles - fonds marins et espace[286],[287]

AID が所管するプログラムであり、学術研究の企業への技術移転促進を目的とする防衛イノベーションとして、海底領域において、5 つの軸（環境に関する知識、環境の熟知、監視、回復力および物体と変化の検出）のいずれかに該当する研究プロジェクトを「ASTRID（基礎研究)」および「MATHILDE（産業研究)」としてサポートしている。

本プログラムにおいては、GDPR（General Data Protection Regulation：EU 一般データ保護規則）や the 2019-2025 military programming law に従って、データ管理及び迅速な意思決定を行うことが求められている。

---

c-support-for-defence-projects-and-innovation/

283 https://www.defense.gouv.fr/aid/deposez-votre-projet/rapid-regime-dappui-linnovation-duale

284 https://anr.fr/fr/

285 https://www.defense.gouv.fr/aid

286 https://www.defense.gouv.fr/aid/appels-projets/cours/accompagnement-specifique-travaux-recherches-dinnovation-defense-appel-thematique

287 https://anr.fr/fr/detail/call/maturation-thematique-innovation-pour-la-defense-mathilde-appel-thematique-sur-lextension-des/

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして 13 件リストアップした（詳細は Appendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも 1 つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして 2 件抽出した（表 4.1-19)。

表 4.1-19　詳細調査を行う法令等のショートリスト

法令等の名称	理由
INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE N° 1300 SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE（国防秘密保全に関する省庁間一般通達第 1300 号）	国防のために機密情報保護を強化として出された通達であるため
Décret n° 2019-1590 du 31 décembre 2019 relatif aux investissements étrangers en France（フランスにおける外国投資に関する 2019 年 12 月 31 日付政令 2019-1590 号）	外国投資に関する政令であるため

以下に表 4.1-19 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE N° 1300 SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE(国防秘密保全に関する省庁間一般通達第 1300 号)[288]

■　策定機関・策定時期

2011 年

■　策定の背景・目的

国家や社会を不安定化させることを目的として、政治・軍事・外交・科学・経済・産業のあらゆる分野を対象として国防の秘密は標的となり得る。そのため、国防機密情報保護の強化を目的とする通達として発出された。

■　適用範囲

保護対象は、政治、軍事、外交、科学、経済、産業などの分野で、国防法典（Code de la défense）に基づく 2 つレベルの国防機密に分類される情報である。中央行政、すべての分散型国家サービスおよび大臣の権限下に置かれる国家公共施設、国防の秘密に関わる官民団体および個人すべてに適用される。国際機関や外国と交換される情報も保護する。

本法令では、「保護原則」「人に関するセキュリティ対策」「機密情報や媒体に関するセキュリティ対策」「機密情報または媒体の配布および転送」「配布制限に対する追加事項」に項

[288] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000033293465

目を分けて説明がなされている。

■　情報の分類

国防法典に基づき以下の 2 つのレベルで分類されている。

（国防法典に基づく機密性レベル）
- Très Secret Défense（国防最高機密）：国防および国家安全保障上の優先事項に関する情報および資料で、その開示が国防に重大な損害を与える可能性のあるものに限定される
- Secret Défense（国防機密）：国防に重大な損害を与える可能性のある情報および資料

■　情報管理策

機密情報へのアクセス等を規定する組織的管理策、アクセス者の明確化を行う人的管理策、機密情報を収容する施設へのアクセスを規定する物理的管理策についてのみ記載されているため、技術的管理策は規定していない。

・　組織的管理策

以下の方法で機密情報の分類と明確化を行い、情報へのアクセスや複製の制限、伝送方法の指定を行っている。

（国防秘密保全に関する省庁間一般通達第 1300 号における組織的管理策）
- 機密分類は、情報や媒体の性質、情報源を考慮し決定される
- 機密情報であることを既定の方法で表示する
- 情報の作成から伝送、廃棄、またはアーカイブ化に至るライフサイクルを通じて、その取扱い方法が規定されている

・　人的管理策

以下の方法で防衛機密情報にアクセスできる者を明確化している。

（国防秘密保全に関する省庁間一般通達第 1300 号における人的管理策）
- 防衛公安高等官（HFDS）は、各国家機関および官民機関で、分類レベルごとに、機密情報へのアクセスが必要な職務（ジョブカタログ）や指示リストを作成する
- ジョブカタログに基づく権限を有する者で、かつ必要な場合に限り、必要な範囲のアクセスに対する承認を行う

・　物理的管理策

機密情報を収容する施設へのアクセスは、労働法、サービス契約、刑法、刑事訴訟法に関する規定、または国際条約に基づく規定によって規制されている。

■　罰則

適用される規定に違反して機密性を侵害した者は、懲戒処分および刑事的処罰の対象となる可能性がある。

b) Décret n° 2019-1590 du 31 décembre 2019 relatif aux investissements étrangers en France（フランスにおける外国投資に関する 2019 年 12 月 31 日付政令 2019-1590 号）[289, 290, 291]

■ 策定機関・策定時期

2019 年

■ 策定の背景・目的

首相によるフランスにおける外国投資に関する政令である。企業の成長・変革のための行動計画(PACTE)の一環として、海外投資手続きの簡略化、明確化、迅速化を図ることを目的としている。海外投資により、国防や公安が侵害される可能性がある「産業分野」、「インフラ」および「重要機関技術研究」については、経済・財務・産業およびデジタル主権省の事前認可を必要とする。

■ 適用範囲

原則として、すべての外国企業は 、事前認可や届出なしで、フランスに直接投資が可能であるが、一部の分野については事前認可が必要であり、以下のように規定されている。

（フランスにおける外国投資の事前認可が必要な業種）

外国企業がフランス企業の経営権掌握をはかる場合、あるいはEU域外企業がフランス企業の議決権の 25%（上場企業の議決権は 2023 年 12 月 31 日まで 10%）超を取得する場合、国益に直接関係する次の分野への外国企業による投資については、事前認可が必要

- 公権力の行使に関与することで、国防上の利益を侵害する可能性または公共の秩序および公共の安全を侵害する可能性がある以下の事業
  - A) 軍事、戦争用などの武器、弾薬、火薬、爆発物に関わる事業
  - B) デュアル・テクノロジー関連品および技術
  - C) 国防上の機密を保有する企業が行う事業
  - D) 国防に関わる情報システムを管理している公共・民間事業者への情報システムのセキュリティ関連分野の事業（下請け業も含む）
  - E) A.～C.、F.の分野で、直接あるいは下請けを通して、国防省と契約を締結した企業が行う事業
  - F) 暗号の手段およびサービス
  - G) 傍受・盗聴、情報データ傍受関連技術および関連機器
  - H) IT 製品およびシステムのセキュリティ評価サービス
  - I) カジノを除く賭博事業
  - J) 病原物質、毒物の不正使用対策および不正使用による健康面の影響防止対策に関

[289] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039727443

[290] https://www.tresor.economie.gouv.fr/Articles/2020/01/02/publication-du-decret-et-de-l-arrete-relatifs-aux-investissements-etrangers-en-france-une-procedure-plus-simple-claire-et-rapide

[291] https://www.jetro.go.jp/world/europe/fr/invest_02.html

する事業
K) 所持、提供、漏洩などが 1.の a.～j.または 2.の事業に損害を与える可能性があるデータの処理、転送、保管事業

・ 公権力の行使に関与することで国防上の利益を侵害する、または公共の秩序および公共の安全を侵害する可能性がある以下の不可欠なインフラ、財、サービスに関する事業
A) エネルギー源の保全、安全性、調達の保障
B) 水源の保全、安全性、調達の保障
C) 運輸サービス・ネットワークの保全、安全性、運営の保障
D) 宇宙活動の保全、安全、活動の保障
E) 電子通信サービス・ネットワークの保全、安全性、運営の保障
F) 警察、憲兵隊、市民保護、税関の安全確保、民間警備企業の職務遂行
G) 国防の観点から、極めて重要な施設、設備、作業の保全、安全性、運営の保障
H) 公衆衛生の保護
I) 食料安全保障に関わる農産品の生産、加工、流通
J) 政治・一般情報の報道出版物の編集、印刷、配布、オンライン・サービス

・ 以下の事業で、公権力の行使に関与することで国防上の利益を侵害する可能性がある場合、または公共の秩序および公共の安全を侵害する可能性がある場合
A) 国家重要基幹技術（サイバーセキュリティ、AI、ロボット工学、付加製造技術、半導体、量子技術、エネルギー貯蔵、バイオテクノロジー、再生可能エネルギー生産に関する技術）に関する研究・開発事業
B) 2009 年 5 月 5 日付の EU 規則の附則Ⅰのリストに記載されているデュアル・テクノロジーに関する研究・開発事業

■ 情報の分類

投資情報を把握するための組織的管理策規定はされているが、情報の部類については規定していない。

■ 情報管理策

投資情報を提出するための規則を示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・ 組織的管理策

投資対象となるフランス企業は、以下の方針に従って経済・財務・産業およびデジタル主権省に外国からの投資情報を提出する必要がある。

（外国投資を受けるフランス企業が提出を義務付けられている情報）
・ 海外投資により国防や公安を侵害される可能性がある「産業分野」、「重要インフラ」および「研究開発事業」については、同省の事前認可が必要である
➢ 「産業分野」の対象は、国防省との契約（下請け業を含む）を締結する事業（軍事、二重用途製品・技術、国防機密を有する企業、暗号手段・サービス）および国防情報システムを管理する官民事業者に対する情報システムのセキュリティ関連分野（下請け業も含む）である
➢ 「重要インフラ」の対象は、国防に関わる施設のほか、電子通信サービス・ネット

ワークの保全、安全性、運営の保障等を含む
  - 「研究開発事業」の対象は、国家重要基幹技術（サイバーセキュリティ、AI 等）および 2009 年 5 月 5 日付の EU 規則の附則 I のリストに記載されている二重用途に関するものである
- 事業事前認可を受けた投資案件について、実施日、その実施結果による企業の資本の分配、投資額またはその見積もり額、投資の認可公布後の直接的および間接的な支配の変更事項について届出を行う
- 事前許可申請にあたっては、投資家に関する情報、投資の理由、投資計画の概要等に関する情報を明記する必要がある。以下の情報を経済・財務・産業およびデジタル主権省に提出する必要がある
  - 投資家側情報（企業の登記証明書、上場企業の場合には、5%以上の株を保有する株主、および代表取締役会のメンバーリスト、組織図、事業概要、過去 5 年間の EU 域外の国または公的機関との資本関係または財政的な支援等）
  - 投資対象企業情報（会社形態、SIREN 番号、組織図、最近の業績等）
  - 投資オペレーションの内容（金額、投資形態等）
  - 投資オペレーションの実施日程の予定
- 経済・財務・産業およびデジタル主権省は投資申請書類の受理後、30 営業日以内に、[1] 投資のオペレーションが事前認可の対象ではない、[2] 投資の申請を認可、[3] 投資を条件付きで認可するかどうか決定するために補足的な審査が必要、のいずれかを回答する。30 営業日以内に回答がない場合、申請は却下されたものとみなされる。[3] の場合、申請者が回答を受理してから 45 営業日以内に、経済・財務・産業およびデジタル主権省は補足的審査の結果を回答する。45 営業日以内に回答がない場合、申請は却下されたものとみなされる。フランス企業が事前認可の要否の判断を仰ぐことも可能で、この場合、経済・財務・産業およびデジタル主権省は 2 カ月以内に回答する

■　罰則

記載なし

（7）EU における関係法令

前記英国、ドイツ、フランスに関する調査結果を整理したが、EU では法体系として、EU 加盟国全てに対して直接適用される規則（Rugulation）、間接的に加盟国に対して特定の目標を達成するよう要求する指令（Directive）等として加盟国に対して適用される法令が存在することや、EU を離脱した英国においても EU 規則と同等性をもつ法令の施行（UK GDPR 等）が見られることから、EU の安全保障の観点から国家機密に該当する技術情報等の保全政策、及び技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策に関連した以下の法令の規定内容を調査した（表 4.1-20）。

表 4.1-20　EU の調査対象法令

法令等の名称	理由
COUNCIL REGULATION (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items（二重用途物品の輸出、移送、仲介および輸送の管理に関する EU 域内体制を確立する 2009 年 5 月 5 日付理事会規則 428/2009）　※EU の規則	デュアルユース品目の輸出について規定した規則のため
REGULATION (EU) 2015/479 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2015 on common rules for exports（共通輸出規則に関する 2015 年 3 月 11 日付欧州議会・理事会規則 2015/479）　※EU の規則	機密情報についての第三国への輸出に関する規則のため

a) COUNCIL REGULATION (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items（二重用途物品の輸出、移送、仲介および輸送の管理に関する EU 域内体制を確立する 2009 年 5 月 5 日付理事会規則 428/2009）[292]

■　策定機関・策定時期

2009 年

■　策定の背景・目的

EU における二重用途（デュアルユース）品目（ソフトウェアや技術を含む）の輸出、移送、仲介および輸送の管理制度の確立を目的としている。

■　適用範囲

二重用途品目リストに掲載されている物品の輸出を対象としており、管理当局の認可が必要となる。また、リストに不記載であっても、輸出先国や流用等の懸念がある場合は、許可が必要となる。物品の輸出には、電子媒体によるソフトウェアや技術の EU 圏外の宛先への送信も含んでいる。

[292] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02009R0428-20211007

本規則では、「目的や範囲などの一般条項」「輸出認可を行う機関」「二重用途品目リストの更新」「通関手順」「管理協力体制」「管理対策」に項目を分けて説明がなされている。

■　情報の分類

輸出管理を行う品目及びそのために加盟国間で共有される情報の規定はされているが、機密性に応じた情報の分類については規定していない。

（EU における輸出管理の為加盟国間で共有を行う情報）
対象となる情報
加盟国は、共同体の輸出管理体制の効率性を高めるため、権限のある当局間の直接的な協力及び情報交換を確立するためのあらゆる適切な措置を取る。対象となる情報には、以下のものが含まれる

- 国家制裁により、国内一般輸出許可を使用する権利を剥奪された輸出業者の詳細
- 機密性の高いエンドユーザ、疑わしい調達活動に関与する者、及び利用可能な場合はそのルートに関するデータ

（EU における輸出管理の対象となる品目）
COUNCIL REGULATION (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items（二重用途物品の輸出、移送、仲介および輸送の管理に関する EU 域内体制を確立する 2009 年 5 月 5 日付理事会規則 428/2009）は、輸出者が設立する加盟国の所轄官庁から、または(製造業者から受け取った情報などから)当該品目が、管轄当局によって、CONFIDENTIEL UE/EU CONFIDENTIAL と同等以上の保護的な国家安全保障分類マークを有するものとして分類されていることを知らされている場合にはその品目の輸出を許可しない

■　情報管理策

輸出管理許可が必要な品目の明確化を行う組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

- 組織的管理策

以下の方法で管理当局の輸出許可が必要な二重用途品目の明確化が行われている。

（EU において輸出許可が必要な二重用途品目）

- 二重用途品目のリストは、オーストラリア・グループ、ミサイル技術管理レジーム（MTCR）、原子力供給国グループ（NSG）、ワッセナー・アレンジメント、化学兵器禁止条約（CWC）等に基づくものである。当リストは、EU 加盟国が国際不拡散体制および輸出管理協定の加盟国として受け入れた関連する義務または国際条約の批准に従って更新される
- リストに不記載の品目であっても、 EU 加盟国の管轄当局から通知があった場合、購入国または仕向国が武器禁輸措置対象国の場合、輸出許可が必要になる
- 輸出者が、物品の目的は二重用途であることを認識している場合も、当局に通知し、許可を得る必要がある

- EU 加盟国は、輸出の許可要件に関する国内法の制定が可能である。必要に応じて他の加盟国および欧州委員会にその旨を通知する
  - 加盟国は、所管当局間の直接協力と情報交換を確立するためのあらゆる適切な措置を講じる二重用途品目の輸出者は、それぞれの加盟国で施行されている国内法または慣行に従って、輸出の詳細な登録または記録を保持する。当該登録簿又は記録には、特に、請求書、目録及び運送状等の商業文書並びに次の事項を識別できる十分な情報を含むその他の発送書類を含むこと
  - (A) 二重用途品目の説明
  - (B) 二重用途品目の数量
  - (C)輸出者及び荷受人の氏名及び住所
  - (D)判明している場合は、二重用途品目の最終用途とエンドユーザ
  - 仲介業者は、各加盟国において施行されている国内法又は慣行に従い、第五条の範囲に属する仲介業務の登録又は記録を保管し、要求に応じ仲介業務の対象となった二重用途品目の説明、当該商品が当該業務の対象であった期間及びその仕向地を証明できるようにしなければならない
  - 登録簿又は記録並びに書類は、輸出が行われた暦年又は仲介役務が提供された暦年の末日から少なくとも 3 年間保管しなければならない。それらは、要求に応じて、輸出者が設立された、または仲介業者が設立または居住している加盟国の管轄当局に提出すること

■ 罰則

各 EU 加盟国は、本規則の規定、またはその実施のために採用された規定の違反に適用される罰則を定めるものとする、とされている。

b) REGULATION (EU) 2015/479 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2015 on common rules for exports（共通輸出規則に関する 2015 年 3 月 11 日付欧州議会・理事会規則 2015/479）[293]

■ 策定機関・策定時期

2015 年

■ 策定の背景・目的

EU から第三国向けの輸出に関する共通規則として、加盟国が保護策を導入する場合の手続きを確立することを目的としている。

■ 適用範囲

公序良俗、公共政策または公安、または人間、動物、植物の健康と生命の保護、国宝、または産業的および商業的財産の保護を目的とする措置が必要な場合を対象としており、すべての工業製品および農産物に適用される。なお、農産物市場の共通組織を確立する文書、または加工農産物について条約第 352 条に基づき採択された特別文書の運用を損なうもの

[293] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0479

ではなく、本規則はこれらの文書を補完する形で運用されるものである。

■　情報の分類

輸出に関する保護策を導入する手続きは規定されているが、情報の部類については規定していない。

■　情報管理策

保護策を導入する際の手続きを示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

以下の方法で加盟国が保護策を導入する場合の手続きを確立している。

（EU 加盟国の輸出に関する保護策導入手続き）
- 加盟国が保護策の必要性を認識した場合、欧州委員会に報告する
- 欧州委員会は、セーフガード委員会に諮り、保護策の導入可否を決定する
- 採用された措置は、欧州議会および欧州理事会、加盟国に通知され、直ちに実行される
- 保護策は、公序良俗、公共政策または公安、または人間、動物、植物の健康と生命の保護、国宝、または産業的および商業的財産の保護を目的とする
- 欧州委員会は、理事会規則(EC)No 1225/2009(7)の第 22a 条に従って欧州議会および理事会に提出される貿易防衛措置の適用および実施に関する年次報告書に、本規則の実施に関する情報を含める

■　罰則

記載なし

(8) オーストラリア

1) 基本情報

- 政治体制：議院内閣制
- 人口：約 2600 万人(22 年度)
- 名目 GDP：1701(10 億米ドル) (22 年度)、実質 GDP：1466 (10 億米ドル) (2022 年)
- 研究開発予算：24,057 (100 万米ドル) (21 年度) OECD

■ 政治動向

2022 年 5 月の連邦議会総選挙で労働党が保守連合に勝利、約 9 年ぶりに政権交代が起こった。首相にはアルバニージー労働党党首が就任した。

オーストラリアは基本的には対米同盟を基軸にするとともに、アジア・太平洋を外交・貿易政策上の優先地域に位置づけ外交に取り組んでおり、日米豪印の 4 か国の QUAD による協議等が行われている。

中国とも 1972 年の国交樹立以降、順調に経済関係を構築していたものの、2017 年頃からの中国の対内投資や内政干渉を皮切りに、豪州内で中国に対する経済安全保障上の懸念が高まり関係は悪化している。

■ 経済動向

豪州経済は、1991／92 年度から 28 年連続して経済成長を実現し、2018 年度の GDP は 1991 年度に比べ 2 倍以上成長をしていたが、新型ウイルスの影響により 2019 年度第 3 及び第 4 四半期にマイナス成長を記録し、経済成長が途絶えリセッションに突入した。

その後急速に回復し、2020 年度の実質成長率は 1.4%、2021 年度の実質成長率は 4.9%とマイナス成長から大きく持ち直している。

■ 社会動向

オーストラリアは総人口約 2600 万人で、多くの移民がいる多民族国家であり、2011 年の段階で 30%だった移民の割合が 2022 年には 50%を越える等総人口における移民の割合は年々増加している。

国内問題としては地球温暖化による干ばつや大規模な森林火災 (それに伴う大気・水質汚染) 等がある。

■ 技術動向

オーストラリアは 2021 年に発表した「重要技術に関する行動計画」の中で、国益に影響を与える可能性のあるテクノロジーとして 7 つのカテゴリー(①先端材料及び製造、②AI、コンピューティング及び通信、③バイオ技術、遺伝子工学及びワクチン、④エネルギー及び環境、⑤量子、⑥センシング、タイミング及びナビゲーション、⑦輸送、ロボット工学及び宇宙)を特定し、国益に適う重要技術リストを作成した。

特に量子分野に最初に着手し、企業が新たな市場や投資家にアクセスするのを支援するため「量子商業化ハブ」を設置した。

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

オーストラリアにおける安全保障上の機密情報の保護については、現在は2018年に定められた「The Protective Security Policy Framework（保護セキュリティポリシーフレームワーク：PSPF)」によって規定されている。

PSPFは、オーストラリア政府機関が国内外で人員、情報、資産を保護するためのセキュリティ的な枠組みであり、①セキュリティガバナンス、②情報セキュリティ、③人員セキュリティ、④物理的セキュリティの４つの望ましい成果（outcome）を達成するためのセキュリティ施策を各主体が実施できるように支援することを目的としている。

PSPFは４つの成果の下に16のポリシーが定められており、それぞれのポリシーには各主体がどのような行動をとらなければならないのかという「コア要件(core requirements)」とその実装をサポートする「サポート要件（supporting requirements)」「ガイダンス」によって構成される[294]。

このうち、情報の機密性に応じた分類を規定しているのは「②情報セキュリティ」の成果（outcome）を達成するための「ポリシー8：分類システム」であり、漏洩により生じるリスクを基準に以下の４つの機密区分及び2つの非機密情報区分を定めている[295](表 4.1-21)。

表 4.1-21　PSPFの情報機密区分

	機密区分	漏洩時のリスク
Security Classified information	TOP SECRET	国家主体、組織もしくは個人に対して非常に重大な損害を与える
	SECRET	国家主体、組織もしくは個人に対して深刻な損害を与える
	PROTECTED	国家主体、組織もしくは個人に対して損害を与える
	OFFICIAL:Sensitive	一般に侵害された場合、個人、組織、政府に対する限定的な損害を与える
―	OFFICIAL	損害なし、もしくは軽微。この情報は日常的に扱う情報の大半である
	UNOFFICIAL	損害はない。この情報は公務の一部ではない

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

オーストラリアにおける安全保障貿易管理については、1958年に制定された「Customs (Prohibited Export) Regulations 1958（関税規則（輸出規制）1958)」によって規制が図られている。輸出規制を所管しているのはオーストラリア国防総省の傘下にある国防輸出管理局（DEC）であり、防衛戦略物資リスト（DSGL)に記載されている規制品目もしくは技術についての規制、及び特定の軍事および軍民両用途の物品および技術に関するオ

294 https://www.protectivesecurity.gov.au/policies

295 https://www.protectivesecurity.gov.au/system/files/2023-11/policy-8-classification-system-pspf_0.pdf

ールキャッチ規制・最終用途（end-use）規制が規定されている。

DGSL は「軍事用途のために特別に設計または改造された品目」であるパート１カテゴリーと、「一般に商業目的で使用されるが、化学兵器、生物兵器、または核兵器計画に役立つ可能性のある品目（二重用途品目）」であるパート２カテゴリーに大きく分けられる。

研究開発へ関係する規定としては、DGSL には特定の技術に対する免除規定が存在している。例えば「技術が出版物、製品パンフレット、公開ブログ、Web サイト、ポッドキャスト、データベースなどですでに一般に公開されている場合（パブリックドメイン）」や、「『現象の基本原理または観察可能な事実』にのみ拡張され、『主に特定の実際的な目的または目的を指向していない』技術」については基礎研究に該当するとして DSGL の規制を免除される。

その他、最終用途が医療用途となるように設計された一部の品目（核磁気共鳴装置の一部である極低温冷却器など）についても、管理対象品目が含まれている場合でも輸出に際して DGSL の規制が免除されるとしている[296]。

[296] https://www.defence.gov.au/business-industry/export/controls/export-controls/defence-strategic-goods-list

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　国家戦略等

2019 年に ASA（Australian Space Agency：オーストラリア宇宙庁）によって Australian Civil Space Strategy 2019-2028 が策定された。これは 2019 年から 2028 年までの民間宇宙開発に関する指針で、4 本柱として、①国際パートナーシップの確立、②宇宙分野事業を民間に開放することによる競争力の向上、③安全と国益の確保および④国民生活の向上、が掲げられている。経済安全保障との関連性として、本指針の中で、「宇宙領域は多くの分野に影響を与えており、オーストラリアの経済の発展や、安全・国益の確保において重要である」と述べられている。

■　研究開発機関

オーストラリアの宇宙領域の研究開発関係機関としては、民生分野における研究では ASA、防衛分野では DoD（Department of Defence：国防省）が主要な役割を担っている。ASA は DISR（Department of Industry, Science and Resources：産業科学資源省）が所管する国立研究所の一つで、オーストラリアにおける宇宙に関する研究開発をリードしている。DoD はオーストラリア政府が所管する政府機関の一つで、国防のために科学技術を応用する責任を負っている。次世代技術基金、 防衛科学パートナーシップ プログラム、および防衛 STAR Shots プログラムなどの資金提供プログラムを実施している（図 4.1-25）。

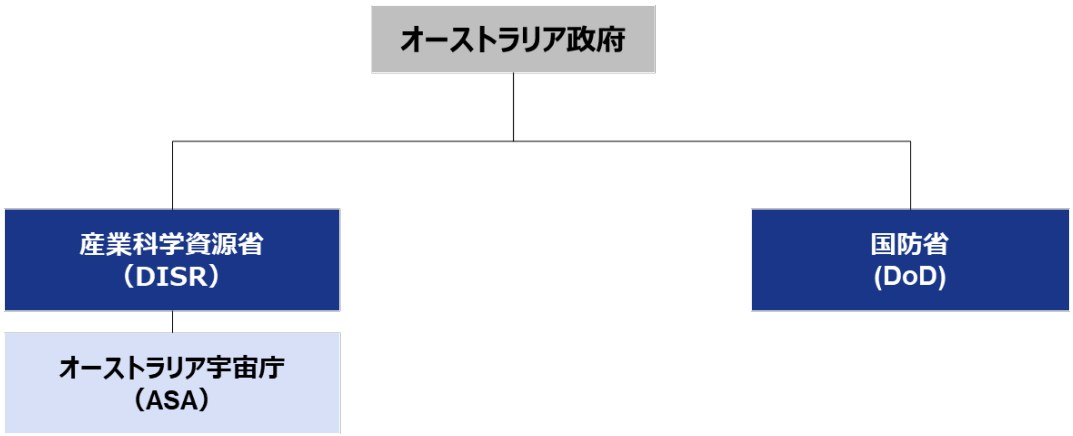


図 4.1-25　オーストラリアにおける宇宙領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ ACSER upgrades satellite receiver for new applications[297]

ASA が所管するプログラムであり、オーストラリア宇宙庁の国際宇宙投資イニシアチブからの資金提供を受けてニューサウスウェールズ大学は GPS とガリレオの 2 つの衛星システムからの信号を複数の周波数で受信する高度な GPS 受信機の開発することを目的としている。正確な測位、タイミング、速度情報を提供することが可能になる。これにより衛星

[297] https://www.space.gov.au/acser-upgrades-satellite-receiver-new-applications

から高品質な画像を生成することができる。

本プログラムにおいては、DoE（Department of Education：教育省）が提供する the University Foreign Interference Taskforce（UFIT）Guidelines 2021[298]をベースとする大学独自のガイドライン Framework to counter foreign interference[299]に準拠し、外国からの干渉（外国からの研究への件線的支援、外国の大学等での役職・職務の有無等）に関する情報の開示を実施している。

b）海洋領域

■　国家戦略等

2022 年に Department of Home Affairs によって Australian Government Civil Maritime Security が策定された。これは民間海上安全保障政策の方向性を定めた戦略で、①主権、航行および海上貿易の自由の保護、②海洋インフラの保護、③天然海洋資源の保護、④海事分野ユーザの保護、⑤国際法に則る秩序の支持、⑥地域内の関係強化および⑦民間海洋安全保障に対する政府全体のアプローチ管理が重点ポイントとして掲げられている。経済安全保障との関連性として、天然海洋資源保護という観点から、海洋科学研究の支援と活用の重視が挙げられる。

■　研究開発機関

オーストラリアの海洋領域の研究開発関係機関としては、民生分野における研究では DoE、防衛分野では DoD が主要な役割を担っている。DoE はオーストラリア政府が所管している政府機関の一つで、オーストラリアの教育システム戦略においてリーダーシップを執っている。その他にも、研究開発への資金提供も行っており、その一環として海洋領域の研究支援を行っている。DoD はオーストラリア政府が所管する政府機関の一つで、国防のために科学技術を応用する責任を負っている。次世代技術基金、防衛科学パートナーシッププログラムなどの資金提供プログラムを実施している（図 4.1-26）。

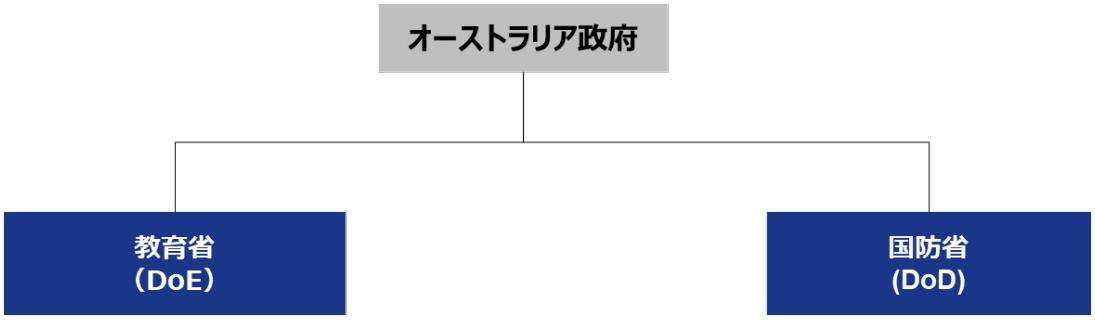


図 4.1-26　オーストラリアにおける海洋領域研究開発の主要機関

298 https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector

299 https://www.unsw.edu.au/content/dam/pdfs/unsw-adobe-websites/2022-05-planning-assurance/UNSW%20Framework%20to%20Counter%20Foreign%20Interference.pdf

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ National Collaborative Research Infrastructure Strategy (NCRIS) 2023[300],[301]

DoE が所管するプログラムであり、オーストラリアの研究インフラに対する投資戦略である。国の研究インフラの重要部分をサポートし、オーストラリアの研究者が確実にアクセスできるようにするために 2018 年から 2029 年までの 12 年間で 40 億豪ドルを投資することとしている。海洋領域システムでは、Integrated Marine Observing System (IMOS)、Marine National Facility (MNF)および National Sea Simulator (SeaSim)を支援している。

情報保全については、Freedom of Information Act 1982 (FOI Act)に基づく情報開示が求められる。

c）バイオ領域

■　国家戦略等

2022 年に DoHAC (Department of Health and Aged Care：保健・高齢者ケア省) によって Biotechnology in Australia – Strategic Plan for Health and Medicine が策定された。これはオーストラリアのバイオテクノロジー(健康及び医療)に関する戦略計画で、長期計画として、①産官学のパートナーシップを強化し世界クラスの研究開発を支援すること、②研究能力、プロセス、インフラストラクチャを継続的に改善することで、世界的な関心を集める高品質で安全な臨床開発を促進すること、③学術、科学組織、産業界間のパートナーシップや政府の協力を通じて商業化を加速すること、が重要ポイントとして掲げられている。経済安全保障との関連性として、バイオテクノロジー分野は現代社会において最も有望な分野の一つであり、今後も研究開発を引き続き支援するべきであるとされている。

■　研究開発機関

オーストラリアのバイオ領域の研究開発関係機関としては、民生分野における研究では DAWE (Department of Agriculture, Water and the Environment：農水環境省)、防衛分野では DoD が主要な役割を担っている。DAWE は 2022 年 1 月 1 日から農業・水部門は DAFF (Department of Agriculture, Fisheries and Forestry：農林水産省) に、環境部門は DCCEEW (Department of Climate Change, Energy, the Environment and Water：気候変動・エネルギー・環境・水資源省) として省が新設された。DAFF は農業、漁業、林業を強化するための活動を行っており、DCCEEW はオーストラリアの自然環境と遺産保護の活動を行っている。DoD はオーストラリア政府が所管する政府機関の一つで、国防のために科学技術を応用する責任を負っている。次世代技術基金、 防衛科学パートナーシップ プログラムなどの資金提供プログラムを実施している（図 4.1-27）。

[300] https://www.education.gov.au/national-research-infrastructure/resources/national-collaborative-research-infrastructure-strategy-2023-guidelines

[301] https://www.education.gov.au/national-research-infrastructure

図 4.1-27　オーストラリアにおけるバイオ領域研究開発の主要機関

■　　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　Biosecurity Business Grant Program 2020-21 to 2022-23[302], [303]

DAWE が所管するプロジェクトであり、オーストラリア北部およびトレス海峡におけるバイオセキュリティに関連した事業機会を開発するための、先住民企業および非営利団体を支援する資金提供することを目的としている。本プロジェクトを通じて、オーストラリア北部における認識、監視、対応を含むバイオセキュリティ能力の向上、先住民コミュニティの経済的機会を増やすことを目指している。

情報保全については、1988 年プライバシー法に準拠することが求められる。

d）サイバー領域

■　　国家戦略等

2023 年にオーストラリア政府によって 2023-2030 Australian Cyber Security Strategy が策定された。2030 年までにサイバーセキュリティ分野において世界的リーダーになることを目標としたオーストラリア政府のビジョンを実現するためのロードマップで、本戦略を通じて、サイバーセキュリティの改善、サイバーリスクの管理、市民および企業のサイバー環境整備の支援、を行うとしている[304], [305]。経済安全保障との関連性として、「サイバーセキュリティを強化することにより、企業の繁栄を支援することができ、サイバー攻撃からも迅速に立ち直ることができる」としている。

■　　研究開発機関

オーストラリアのサイバー領域の研究開発関係機関としては、民生分野における研究では ONI（Office of National Intelligence：国家情報局）、防衛分野では DoD が主要な役割を担っている。ONI はオーストラリアの法定情報機関であり、政府と国家安全保障委員

302 https://www.communitygrants.gov.au/grants/biosecurity-business

303 https://www.communitygrants.gov.au/sites/default/files/documents/2022-06/4214-biosecurity-business-grants.pdf

304 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

305 https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

会への助言及び国家情報コミュニティの戦略開発を行っている。DoD はオーストラリア政府が所管する政府機関の一つで、国防のために科学技術を応用する責任を負っている。次世代技術基金、防衛科学パートナーシップ プログラムなどの資金提供プログラムを実施している（図 4.1-28）。

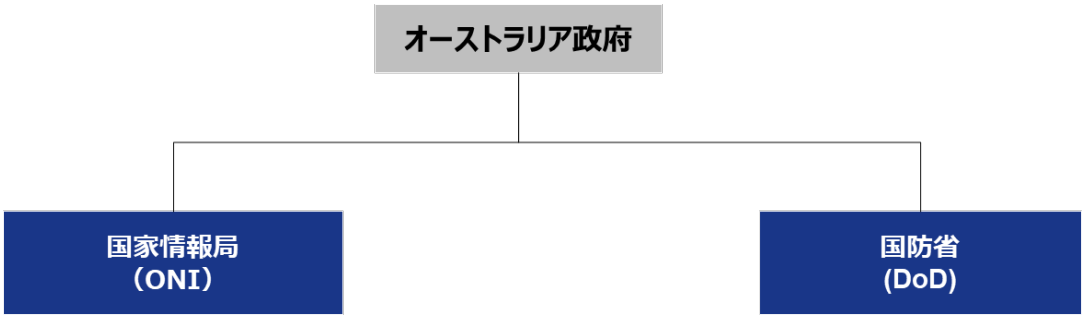


図 4.1-28　オーストラリアにおけるサイバー領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ National Intelligence and Security Discovery Research Grants(NISDRG)[306]

ONI と DoD が所管するプログラム。イノベーションを促進し、国家安全保障及び情報能力を開発し、オーストラリアの国家情報・安全保障コミュニティと研究・技術コミュニティの体系的な連携を実現することを目的とし、新興科学技術に対する理解を深め、情報及び国家安全保障上の関心事項に対処する研究活動を支援している。

本プログラムにおいては、プライバシー法に基づく個人情報の管理や、情報公開法に基づく情報の公開を行うことが求められている。

e）多義的技術

■　国家戦略等

オーストラリアにおいては、国防総省関連機関が多義的技術の研究開発・活用に関する政策の調整、実行を行っている。国防総省内で国家安全保障に資する科学技術政策に関する調整を DSTG（Defence Sience and Technology Group：防衛科学技術グループ）と、その傘下にある NSSTC（National Security Science Technology Centre：国家安全保障科学技術センター）が所管している。

NSTTC は以下のような、多義的技術を含む安全保障関連の科学技術政策に責任範囲を持っている[307]。

（NSTTC の責任（responsibilities））

1. 政府の国家安全保障科学技術全体を調整し、要件に優先順位を付け、ガバナンスを提供し、重複を削減し、科学技術保証を提供し、効果を向上させる。
2. 国家科学技術能力を構築し、オーストラリア国家安全保障機関への的を絞った提供

306 https://www.grants.gov.au/Fo/Show?FoUuid=765424e6-8767-41e7-a175-ce571c14ced9

307 https://www.dst.defence.gov.au/nsstc

を強化するために、学術と産業界の科学技術パートナーシップを促進することにより、科学技術価値の提供を確実にする。
3. 国際的な研究協力を主導してオーストラリアの最先端の能力を活用し、地域の科学外交を提供する。
4. DSTG の国家安全保障科学技術プログラムを管理し、DSTG の固有能力であるデュアルユースの適用を最大限に活用する。

NSTTC は学術界と産業界のパートナーシップの促進しており、2018 年にオーストラリアの 2 社の企業が、NSSTC の資金提供を受けて、爆発物痕跡検出および即席爆発装置のスタンドオフ検出装置を開発するなど成果を上げている。

■ 研究開発機関

前述のとおりオーストラリアにおいて多義的技術領域の研究開発を行う機関としては、DSTG、NSTTC が挙げられる。DSTG は自身も科学者やエンジニア、技術者等のスタッフを雇用する研究機関でありライセンス契約を通じた民間への技術移転（スピンオフ）を行うとともに、産業界やアカデミアと連携するための基金や資金提供プログラムを有しており、産業界・大学・科学コミュニティと緊密に連携し、オーストラリアの防衛および国家安全保障能力をサポートすることをミッションとしている[308]。

■ 主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ National Intelligence and Security Discovery Research Grants(NISDRG)[309]

DoD と ONI が所管するプログラム。イノベーションを促進し、国家安全保障及び情報能力を開発し、オーストラリアの国家情報・安全保障コミュニティと研究・技術コミュニティの体系的な連携を実現することを目的とし、新興科学技術に対する理解を深め、情報及び国家安全保障上の関心事項に対処する研究活動を支援している。

本プログラムにおいては、プライバシー法に基づく個人情報の管理や、情報公開法に基づく情報の公開を行うことが求められている。

[308] https://www.dst.defence.gov.au/partner-with-us/access-our-technology

[309] https://www.grants.gov.au/Fo/Show?FoUuid=765424e6-8767-41e7-a175-ce571c14ced9

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして19件リストアップした（詳細はAppendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも1つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして7件抽出した（表 4.1-22)。

表 4.1-22　詳細調査を行う法令等のショートリスト

法令等の名称	理由
Protective Security Policy Framework (PSPF)	連邦政府省庁にて適用される情報セキュリティを示す枠組みのため
Defence Trade Controls Act 2012	防衛に関係する品目の取引を規制するための法令のため
Defence Export Controls (DEC)	防衛及びデュアルユースに関係する品目の輸出を規制する法律の適正運用を監視するための枠組みのため
Applicable laws and obligations (NHMRC)	バイオ分野の研究開発における法規制の概要を示しているため
Management of Data and Information in Research	バイオ分野の研究開発におけるデータの取り扱い方針を示すガイドラインのため
Guidelines to counter foreign interference in the Australian university sector	大学における研究活動に対する外国からの干渉への対処方針を示すガイドラインのため
Australian Government intellectual property manual	知的財産権の保護効率的に行うための方法を示すガイドラインのため

以下に表 4.1-22 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）Protective Security Policy Framework (PSPF)[310, 311, 312]

■　策定機関・策定時期

Attorney-General’s Department　2018年（2023年8月から本フレームワークの責任をDepartment of Home Affairsに移管）

[310] https://www.defence.gov.au/security/clearances/about/overview

[311] https://www.protectivesecurity.gov.au/

[312] https://www.protectivesecurity.gov.au/system/files/2022-11/protective-security-guidance-for-executives.pdf

■　策定の背景・目的

PSPF は、Public Governance, Performance and Accountability Act 2013 の対象となる連邦政府省庁に適用される情報セキュリティの枠組みである。

■　適用範囲

PSPF の下で、機密扱いのセキュリティリソースにアクセスする担当者は、適切なセキュリティ・クリアランスが必要である。3 段階の機密情報を設定し、段階に応じた実践（物理的保護、アクセス制限）を求めている。

本ポリシーでは「原則」「望まれる要件（ガバナンス、情報、人員および物理的要件)」に項目を分けて説明がなされている。

■　情報の分類

機密情報の格付け区分として、情報流出による国益、組織、個人に与えうる損害の深刻度に基づくもので、「損害(保護情報)(PROTECTED)」、「深刻な損害(機密情報)(SECRET)」および「極めて重大な損害（最高機密情報）(TOP SECRET)」の 3 種類に分けている。

■　情報管理策

機密情報を保護するための管理体制を示す組織的・人的・物理的管理策のみ記載されているため、技術的管理策は規定していない。

・　組織的管理策

最高責任者責任者（Senior Executive Service レベル)を任命し、管理体制の整備や人員のセキュリティ意識を高めることで、責任の明確化を行っている。

以下の方法で機密情報であることの明確化を行っている。

(PSPF における組織的管理策)

- **機密情報の格付け区分は、情報流出による国益、組織、個人に与えうる損害の深刻度に基づくもので、「損害（保護情報）(PROTECTED)」、「深刻な損害（機密情報）(SECRET)」および「極めて重大な損害（最高機密情報）(TOP SECRET)」の 3 種類である**
- **これらの情報にアクセスする人員は、中央審査機関（AGSVA）の評価、または、それに準じたクリアランス評価が必要である。 同機関は連邦、州および準州の機関に対するクリアランス評価を行う連邦政府機関である**
- **各組織は、従業員、情報、アセットに安全かつセキュアな物理的保護（施設の設計、物理的アクセス制限等）を提供する**

・　人的管理策

各組織は、その従業員および請負業者がオーストラリア政府の資源にアクセスするのに適しており、誠実さと正直さの適切な基準を満たしているかを確認している。

(PSPF における人的管理策)

- **セキュリティアドバイザー（CSO）は、事業体の人、情報（ICT を含む）及び資産を保護するために、セキュリティの全分野を指揮する責任を負わなければならない。これ**

には、日常的な保護セキュリティの実施や、専門的な業務の遂行を支援するセキュリティアドバイザーを任命することも含まれる
・ 職員の適格性及び適性：各事業体は、オーストラリア政府の資源（人、情報及び資産）にアクセスする職員の適格性及び適性を確保しなければならない。事業体は、オーストラリア政府セキュリティ審査機関（AGSVA）を利用して審査 を行うか、権限を与えられている場合は、「人事セキュリティ審査基準」に沿った方法でセキュリティ審査を行う必要がある
・ 要員の継続的な評価：各事業体は、要員の継続的な適性を評価・管理し、適切な場合には、セキュリティ上の懸念がある関連情報を共有する必要がある
・ 離職者：各事業体は、離職する職員に対して以下のことを確実に行う必要がある
A) オーストラリア政府のリソースへのアクセスを停止する
B) 継続的なセキュリティ義務についての通知を行う

・ 物理的管理策

各事業体は、人、情報、および資産のために、安全でセキュアな物理的環境を提供する必要がある。

（PSPF における物理的管理策）
・ 事業体は、ガバナンス、人事、情報（ICT を含む）、物理的セキュリティにわたるすべてのセキュリティ関連事項の中心的な窓口として、監視された電子メールアドレスを維持しなければならない
・ 事業体資源の物理的セキュリティ：各事業体は、以下のリスクを最小化または排除する物理的なセキュリティ対策を実施する必要がある
A) 人への危害
B) 情報及び物理的資産資源が、操作不能またはアクセス不能にされる、または適切な権限なしにアクセス、使用、除去される
・ 事業体施設：各事業体は、次のことを実施する必要がある
A) 人、情報及び物理的資産を保護するための施設の計画、選択、設計及び変更のプロセスにおいて保護セキュリティが完全に統合されていること
B) 機密またはセキュリティ機密情報及び資産が使用、伝送、保管または議論される区域において、適用される ASIO テクニカルノートに従って施設の物理的セキュリティゾーンを認定する
C) セキュリティゾーンの認定
➢ 要件 1：施設の設計及び変更
a. 施設を設計又は変更する場合、事業体は次のことを行う必要がある事業体資源に対する最高リスクレベルに適合するように、アクセス制限区域を定義する
b. 以下に詳述するように、アクセス制限区域を定義する
ZONE1：一般の立ち入り
ZONE2：一般の立ち入り制限。許可された担当者のみ無制限アクセスが可能。アクセス制御に単一要素認証を使用可能
ZONE3：一般の立ち入りは禁止。許可された者のみアクセス可能。単一要素認証によるアクセス制御
ZONE4：一般の立ち入り禁止。訪問者の立ち入りについては、情報を知る必要のある訪問者のみに限定される。適切なセキュリティ・クリアランスを持つ関係者のみがアクセス可能。アクセス制御のために、単一要素認証を使用可能

ZONE5：一般の立ち入り禁止。訪問者の立ち入りは、情報を知る必要のある訪問者のみに限定される。適切なセキュリティ・クリアランスを持つ関係者のみアクセスが許可される。アクセス制御のためには、二要素認証が必要

- 要件 2：建物

事業者は以下の対応を確実に行う必要がある

a. 機密情報またはセキュリティ機密情報及び資産を保管する ZONE2~5 の施設は以下の該当セクションに従って建設する必要がある
   i. ASIO テクニカルノート 1/15 - 物理的セキュリティゾーン
   ii. ASIO テクニカルノート 5/12 - 物理的セキュリティゾーン（TOP SECRET）
b. セキュリティゾーンは、事業体のセキュリティリスク評価に従って、最も高いリスクレベルから保護するために構築される
   i. 一般市民及び権限を与えられた職員がアクセスできる場所
   ii. 機密及びセキュリティ機密資産以外の物的資産が保管されている場所

■ 罰則

記載なし

b）Defence Trade Controls Act 2012[313, 314]

■ 策定機関・策定時期

2018 年

■ 策定の背景・目的

オーストラリアの国益保護を目的として、DSGL（Defence and Strategic Goods List：防衛戦略物資リスト）記載品目、および米豪防衛貿易協力条約の対象品目の国外との取引を規制する法令である。

■ 適用範囲

軍事および二重用途の技術、ソフトウェアおよび物品を規制対象としている。これらの品目の取引には、国防大臣の許可が必要で、取引を許可された者は、記録を保持する義務がある。また、大臣は、法の執行に関わる情報収集を行うことができる。

本法令では、「目的や範囲などの一般条項」「DSGL 記載品目の取扱い」「米豪防衛貿易協力条約」「監視権限」「情報収集権限」「記録」「決定の見直し」に項目を分けて説明がなされている。

■ 情報の分類

外国との取引を規制する品目や方法については規定されているが、情報の部類については規定していない。

313 https://www.legislation.gov.au/Details/C2018C00318

314 https://services.anu.edu.au/research-support/ethics-integrity/defence-export-controls-and-your-research

■　情報管理策

取引の責任の所在を規定する組織的管理策及び職員の権限を規定する人的管理策のみ記載されており、物理的・技術的管理策は規定していない。

・　組織的管理策

以下の方針に従って責任の明確化を行っている。

（Defence Trade Controls Act 2012 における責任区分）

- 国防大臣は、取引規制対象のリスト（DSGL および米豪防衛貿易協力条約の対象品目を含む）を作成する。許可なくこれらの提供、技術提供のほう助、技術の公開を不正に行った場合、犯罪となる
- 取引には、大臣の許可が必要である。許可を受けた者は、許可要件に則り、記録を 5 年間保持する義務がある
- 同法遵守の監視は、大臣から任命された国防軍（warrant officer 以上）の者が実施する
- 大臣は、法の執行に関わる情報収集を行うことができる

・　人的管理策

以下の規定に従って職員へ権限を与えることにより情報管理を行っている。

（Defence Trade Controls Act 2012 における職員の権限）

- 権限を与えられた職員は、条件を遵守しているかどうかを確認する目的で、合理的な時間であればいつでも特定の施設に立ち入ることが可能
- 権限を与えられた職員は、少なくとも 24 時間前までに、当該職員が施設に立ち入る旨を当該者に通知しなければならない
- 施設に立ち入る権限を有する職員は、監視権限を行使することが可能。権限を与えられた職員は、必要かつ合理的である場合、他の者の支援を受けることができる
- 立ち入ることの可能な施設は以下の通り。以下の施設において、権限を与えられた職員は、監視権限を行使することが可能

  i. 承認の申請において第 3 条(1)米国防衛用品又は第 3 条(3)米国防衛用品を保管すること ができる施設として指定した施設

  ii. 書面で大臣に、第 3 条(1)項に規定する米国防衛用品又は第 3 条(3)項に規定する米国防衛用品が保管されている又は保管される可能性のある施設である旨を通知した施設

  iii. 居住地として使用される建物を除き、その者の事業運営の目的のためにその者が全体的または部分的に使用する、オーストラリア国内のあらゆる敷地

■　罰則

国外に不正に規制技術を提供した場合、10 年の懲役または 2500 単位の罰金あるいはその両方を科せられる可能性がある。

c）Defence Export Controls[315]

■　策定機関・策定時期

DEC　2012 年に策定された Defence Trade Controls Act をはじめとする様々な法律に基づいて管理されている枠組み

■　策定の背景・目的

オーストラリアの国益保護を目的として、軍用・二重用途品の輸出を規制する法律（米豪防衛貿易協力条約、税関法等）の遵守の推進と監視を行う枠組みである。

■　適用範囲

Defence Export Controls が適用される商品や技術が以下のように規定されている。

（Defence Export Controls の適用される技術・商品）

- 軍事目的のために設計または適合された、あるいは本質的に致死的、無力化的、破壊的な軍事物資および技術
- 商業的なニーズを満たすために開発されたが、軍事用部品として、または軍事システムもしくは大量破壊兵器の開発もしくは製造のために使用される可能性のある二重使用の商品および技術

■　情報の分類

外国との取引を規制する品目や方法については規定されているが、情報の部類については規定していない。

■　情報管理策

取引の責任の所在を規定する組織的・人的管理策のみ記載されているため、物理的・技術的管理策は規定していない。

・　組織的管理策

以下の方針に従って責任の明確化を行っている。

（Defence Export Controls における DSGL の責任）

- Defence Export Controls は、DSGL で指定された商品または技術の輸出、供給、仲介、公開を承認する。商品等が規制対象であるか、承認の必要性の確認については、オンラインツール（DSGL ツール）や助言を提供する
- 承認申請には、DECS Client Registration Number (DCRN)登録が必要だが、この登録には、税務局が発行した有効な事業者番号（ABN）または税関顧客 ID (CCID)が必要である。DEC は DCRN を使用して、追加情報の要請や申請の許可を行う
- 申請を定期的に行う組織に対して、ポリシー設定や従業員トレーニング実施等による責任の明確化を含む規制順守プログラム 「Export Control Compliance Program

[315] https://www.defence.gov.au/business-industry/export/controls

(ECCP)」の実施を推奨する
・ 輸出の際に誤りや違反があった場合は、自発的な報告と是正措置を促している

・ 人的管理策

人的管理策として、以下の意識向上トレーニングが提供されている。

(Defence Export Controls におけるトレーニングの提供)
・ オーストリアの輸出管理法、規制、コンプライアンスをユーザに提供するために以下のモジュールが提供されている
  ➢ モジュール 1：オーストリアの輸出管理の概要
・ (なぜ輸出規制があるのか、管理された財・技術の輸出、管理された財・技術の有形輸出、技術の供給、輸出管理の 4 つの W、国際的な規制と条約、主要政府機関)
  ➢ モジュール 2：オーストリアの輸出管理システムの概要
・ (オーストラリアの輸出管理制度、1901 年関税法 (The Customs Act 1901)、1958 年税関 (輸出禁止) 規則 - 規則 13E (The Customs (Prohibited Exports) Regulations 1958 – Regulation 13E)、2012 年国防貿易管理法 (The Defence Trade Controls Act 2012)、オーストラリアと米国の輸出規制、キャッチオール法規、制裁関税法、その他の法令に関する考慮事項)
  ➢ モジュール 3：規制とコンプライアンス
・ (オーストラリアのコンプライアンス哲学、コンプライアンス違反に対する罰則、横流しのリスク、サイバーセキュリティ、レッドフラッグ)
  ➢ モジュール 4：防衛・戦略物資リスト
・ (顧客登録、原則審査、申請と審査の流れ、発行可能な許可、オーストラリア一般輸出許可証 (AUSGELs)、不許可と手続き上の公正と条件、報告と記録管理)

■ 罰則

税関法では以下の罰則が規定されている。

(Defence Export Controls における罰則)
・ 許可なく DSGL 規制技術を提供した場合、10 年以下の懲役または 2500 単位の罰金あるいはその両方を科せられる可能性がある
・ 許可条件に違反して DSGL 製品を輸出した場合、100 単位以下の罰金を科せられる可能性がある
・ 軍事最終使用禁止通知の対象となる商品を意図的に輸出した場合、10 年以下の懲役または 2500 単位の罰金あるいはその両方を科せられる可能性がある

また、Defence Trade Controls Act 2012 では、許可条件に違反して DSGL 製品を輸出した場合、60 単位以下の罰金を科せられる可能性がある。また、大量破壊兵器拡散防止法、国連による制裁、刑法に基づく罰則が科せられる可能性がある。

d）Applicable laws and obligations（NHMRC）[316,317]

■　策定機関・策定時期

NHMRC　NHMRC が資金提供する研究において適用される法律・要件・義務等が記載されているが策定時期については明記されていない。

■　策定の背景・目的

NHMRC（National Health and Medical Research Council：オーストラリア保健医学倫理委員会）が資金提供を行う研究に関わる法規制を周知することを目的として、その概要やオーストラリア政府が資金提供を行う研究における政府機関の役割が述べられている。

■　適用範囲

本ガイドラインでは、NHMRC が資金提供を行う研究に関する法規制を対象として解説を行っており、「オーストラリアの研究に対する外国の介入」「子ども保護組織に関する国家原則」「国家救済制度補助金関連政策臨床試験の登録」「人間を対象とした研究」「同意なく個人情報を研究に利用すること」「ヒト胚に関する研究動物を使った研究」「動物を用いた研究」「遺伝子組み換え生物に関する研究」「発がん性または毒性の高い化学物質の使用」「研究目的でのデータセットの使用」「1989 年治療用品法（Therapeutic Goods Act 1989）」「アクセスと利益配分に関する名古屋議定書　(Nagoya Protocol on accesss and benefits-sharing)」「2012 年国防貿易管理法　(Defence Trade Contrils Act 2012)」「知的財産権」「外国アレンジメントスキーム」に項目を分けて説明がなされている。

■　情報の分類

研究開発における各機関の役割・責任については規定されているが、情報の部類については規定していない。

■　情報管理策

各機関の責任の所在を規定する組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

以下の方針に従って研究機関の責任の明確化を行っている。

（Applicable laws and obligations における研究機関の責任）
・　大学研究向けのガイドライン「Counter Foreign Interference in the Australian University Sector」に基づき、外国の干渉リスクや評価を実施する ・　軍用・二重用途品の輸出を規制する法律のひとつである Defence Trade Controls Act 2012（DTC）の遵守が必要である

316 https://www.nhmrc.gov.au/research-policy/applicable-laws-and-obligations

317 https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/templates-and-tools/australian-government-contacts

- 知的財産権の取扱いは、National Principles of Intellectual Property Management for Publicly Funded Research に基づく必要がある
- 1988 年プライバシー法(プライバシー法)は、プライバシー法第 95 条(s95 ガイドライン)またはプライバシー法第 95A 条(s95A ガイドライン)に基づいて承認されたガイドラインに従って調査が行われる場合、研究目的でオーストラリアのプライバシー原則(APP)の 1 つ以上に違反する個人情報の収集、使用、開示を許可している
  - プライバシー法第 95 条(s95 ガイドライン)は、提案された研究が、連邦機関が保有する個人情報（機密情報を含む）の使用を含む医学研究であり、同意を求めることが現実的でない場合に適用される
  - プライバシー法第 95A 条(s95A ガイドライン)は、提案された研究が、研究、公衆衛生、または公共の安全に関連する統計の編集または分析、または医療サービスの管理、資金提供、またはモニタリングのための健康情報の収集を目的として、民間部門の組織によるまたは、民間部門の組織によって保持されている健康情報の収集、使用、または開示を含む場合に適用される。同意を求めることは、現実的でない場合適用される。また、匿名化された情報は、統計活動の調査、または編集または分析の目的を達成しない場合に適用される

また、政府機関については、国際教育、高等教育、国家安全保障、保護安全保障、規制分野における各機関の責任を明確化している。防衛研究のセキュリティ義務の遵守については、国防省が企業や大学向けに Defence Industry Security Program (DISP)を通じて助言や支援を行っている。

■ 罰則

記載なし

e) Management of Data and Information in Research[318]

■ 策定機関・策定時期

NHMRC 2019 年

■ 策定の背景・目的

NHMRC が作成した、研究実施規範 (Australian Code for the Responsible Conduct of Research) 導入ガイドラインで、オーストラリアの機関が支援する研究に関わるデータおよび情報の取扱いの明確化を目的としている。研究の責任ある実施には、その範囲内に、データおよび情報の適切な生成、収集、アクセス、使用、分析、開示、保存、保持、廃棄、共有、再利用が含まれます。研究の実施を管理するために策定される制度的方針は、倫理指針、プライバシーに関する法律やガイドライン、その他の関連する法律や規制、ガイドライン、さらにはベストプラクティスのための研究分野特有の実践や基準、モデルに適切に注意を払う必要がある。

[318] https://www.nhmrc.gov.au/sites/default/files/documents/attachments/Management-of-Data-and-Information-in-Research.pdf

■　適用範囲

オーストラリア政府が支援する研究において取り扱われる情報を対象としており、その取扱い方法について、「イントロダクション」「研究機関の責任」「研究者の責任」「規約違反」に項目を分けて説明がなされている。

■　情報の分類

研究開発に関するデータの管理方法については規定されているが、ガイドライン特有の情報の分類は規定されておらず、一般的な情報分類が以下のように記載されている。

（Management of Data and Information in Research に記載された一般的な情報分類）
機密情報およびその他の機微情報の管理 研究者は、研究プロジェクトで使用される、または研究プロジェクトから生じる機密情 報またはその他の機微情報の取り扱いに注意を払わなければならない。守秘義務またはその他の機微性が適用される可能性のある研究データおよび情報は、一般的に以下のカテゴリーのいずれかに分類される

- 商業的な秘密情報、または本質的に秘密であり、秘密裏に提供されたデータまたは情報
  （例：秘密かつ神聖な宗教的・文化的慣習、または脆弱な種の生息場所に関する情報）
- プライバシー法の対象となる機密データまたは情報
  （例：特定可能な人間の医療／健康および個人データまたは情報）
- 分類規制およびその他の規制の対象となるデータまたは情報
  （例：国家安全保障情報、警察記録または情報、輸出規制の対象となる一次資料など）

■　情報管理策

各機関の責任の所在を規定する組織的・人的管理策のみ記載されているため、物理的・技術的管理策は規定していない。

・　組織的管理策

以下の方針に従って研究機関の責任の明確化を行っている。

（Management of Data and Information in Research における研究機関の責任）

- 研究機関は、データ管理ポリシーを作成し、データの生成から収集、アクセス、使用、分析、開示、保管、保持、廃棄、共有および再利用に至るまで、適切な取り扱いを確保する
- 研究実施規範の調査ガイドに基づき、規範の遵守について管理および調査を行う
  - 研究者の責任については以下の方針に従って責任の明確化を行っている。
- 研究者は、ポリシーを順守してデータ管理を行う。研究プロジェクトで使用、またはそこから派生した機密情報のほか、国家安全保障情報や輸出規制の対象となる情報の保護を確保する必要がある
- 研究データや一次資料の長期保存、および開示対象の決定を行う責任を負う
- 機微な研究データは、仲介によるアクセスの取り決めやリスク評価の枠組みを適用することにより、適切に共有することができる

- データ管理計画を研究プロセスの早い段階において、作成する必要がある。データ管理計画には以下のような詳細な内容を含めるべきである
  - 物理、ネットワーク、システムセキュリティ、その他のあらゆる技術的セキュリティ対策の方針と手順
  - 契約上およびライセンス上の取決めと機密保持契約
  - プロジェクトメンバーのためにトレーニングを適切な方法で実施すること
  - データまたは情報が格納される形式
  - データまたは、情報の利用目的または開示する権利を有しているか否か
  - データまたは、情報へのアクセスが他者に付与される場合の条件、およびデータ管理計画から得られる情報がある場合、その情報を潜在的な利害関係者に伝える必要がある

・　人的管理策

以下の方針に従って研究者の責任の明確化を行っている。

（Management of Data and Information in Research における研究者の責任）
- 研究者は、研究データおよび一次資料に使用されるセキュリティおよびプライバシー対策が、これらのデータおよび資料の機密性や機微性に関連するリスクに比例したものであることを保証しなければならない。これらの対策は、データおよび情報の保管、アクセス、共有に関連するものであり、データ管理計画に記録されるべきである
- 研究者を対象として、組織の管理ポリシーへの準拠トレーニングを実施する

■　　罰則

記載なし

f) Guidelines to counter foreign interference in the Australian university sector[319]

■　　策定機関・策定時期

DoE　2019 年

■　　策定の背景・目的

オーストラリア政府と同国大学が共同開発した、大学研究活動への外国の干渉に対処するためのガイドラインである。外国からの干渉により主権や国益が損なわれるリスクを評価し、軽減することを目的としている。

■　　適用範囲

大学の研究活動に対する外国からの干渉リスクを対象としており、「ガイドラインについて」「ガバナンスとリスクの枠組み」「通信、教育、ナレッジ共有」「デューデリジェンス、

[319] https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector

リスク評価と管理」「サイバーセキュリティ」「ケーススタディ」「テンプレートとツール」に項目を分けて説明がなされている。

■　情報の分類

外国からの干渉に備えた対応方法については規定されているが、情報の部類については規定していない。

■　情報管理策

各機関の役割・責任を規定する組織的・人的管理策のみ記載されているため、物理的・技術的管理策は規定していない。

・　組織的管理策

以下の方針に従って政府機関の責任の明確化を行っている。

（Guidelines to counter foreign interference in the Australian university sector における政府機関の責任）

- 大学にリスク評価や軽減のためのツール、フレームワークおよびリソースの開発や検討に役立つガイドラインを提供する
- 政府のサイバーセキュリティ機関である ACSC（Australian Cyber Security Centre：オーストラリアサイバーセキュリティセンター）を通じてインシデント対応戦略に関するガイダンスを提供する
- ASIO（Australian Security Intelligence Organisation：オーストラリア保安情報機構）主導の外国干渉対策タスクフォースを設立し、調査の実施と執行を行う
- サイバーセキュリティ戦略の実施を行う。サイバーセキュリティ戦略には以下の項目が含まれるが、これらに限定されない
  - セキュリティポリシー、標準、ガイドライン、手順
  - セキュリティの役割と責任
  - デジタル ID 管理コンポーネント
  - 資産、脆弱性、脅威管理をサポートするための対策
  - サイバーセキュリティの主な目的と管理方法
  - トレーニングと意識向上プログラム
  - 事業継続計画と災害復旧
  - サイバー脅威から生じるビジネスリスクの明確化
- セキュリティ戦略のフレームワークとして以下の実践例が提示されている。どのフレームワークを選択するのかは各大学の責任であるが、十分に考慮すべき主要な実践例である
  - 連邦情報セキュリティマニュアル（The Commonwealth Information Security Manual（ISM））

    エッセンシャル・インシデントサイバー・セキュリティ・インシデントを軽減するための戦略が引用されている。これらはオーストラリア信号総局（ASD）のオーストラリア・サイバーセキュリティ・センター（ACSC）が作成・発行しており、様々なガイダンス文書が付属している

- 米国国立標準技術研究所サイバーセキュリティ・フレームワーク（The US National Institute for Standards and Technology (NIST) Cyber security Framework）
  組織を保護するために必要な広範なコントロールに関する詳細な情報と裏付け調査を含む包括的なフレームワーク
- ISO 127001
  情報セキュリティマネジメントシステム（ISMS）を導入するためのフレームワークを提供している。ISMS は、システムやデータの機密性、完全性、可用性を維持するために必要なポリシーとプロセスの集合体

・ サイバーセキュリティ戦略では、具体的に以下の項目を達成する必要がある
- 大学が直面している脅威モデルとビジネスリスクを理解し、それに見合ったものであること
- 大学の関連する事業継続性及び情報セキュリティの目標に従って、全体戦略の有効性と比例性を測定する
- 戦略内の特定のセキュリティ目標に対する進捗状況を評価し、投資ギャップを判断するための指標を組込むこと
- 企業、教育、研究機能を含む大学運営に関する分野全般をカバーすること
- ポリシーや手順などの補足文書とともに、可能な限り多くの読者に公開し、セクター全体で共有すること
- 技術的負債やセキュリティ上の問題を引き起こす時代遅れのビジネス慣行の影響を考慮すること
- セキュリティ文化、ガバナンス、サプライチェーン、技術管理、セキュリティリスク、データ保護を網羅すること

・ 説明責任のある権限保持者、権限保持機関：外国の干渉に対抗するための人、情報、および資産のセキュリティに責任と説明責任を負う上級管理職または執行機関のこと。説明責任を持つ権限保持者、権限保持機関には以下のようなものがある
- 副学長
- 最高情報セキュリティ責任者
- 大学職員の上級職にふさわしい者
- 適切な大学レベルの上級委員会

大学については、以下の方針に従って責任の明確化を行っている。

（Guidelines to counter foreign interference in the Australian university sector における大学の責任）

・ 大学の人員、情報、アセットに対する脅威を特定して軽減し、回復力を促進、支援、強化するための枠組みとポリシーを設置する。責任者（上級職員や執行機関）の設置や、インシデント発生時の上申手順の設定を行う

・ 国際パートナーシップ活動や協力に従事するスタッフに対して、外国との提携、関係、経済的利益の特定を含む利益の開示を求める（デューデリジェンス）

・ 情報システムを不正なアクセス、改ざん、中断、損傷から保護し、その機密性、完全性、可用性を確保する

・ 人的管理策

以下の方針に従って研究機関の責任の明確化を行っている。

（Guidelines to counter foreign interference in the Australian university sector における研究機関の責任） コミュニケーション、教育、知識の共有として、意識を高めるためのコミュニケーション計画と教育プログラム、外国からの干渉を受ける危険性がある者への研修、大学間および政府との知識共有に関するプログラムの提供が奨励されている ・ 意識を高めるためのコミュニケーション計画と教育プログラム 大学は、コースの一部として議論されたトピックによる個人への嫌がらせや脅迫など、外国の干渉に関連する問題を含むさまざまなシナリオを使用して、教室での機密性の高い会話を管理するための教員向けの専門能力開発トレーニングを検討することが奨励されている ・ 外国からの干渉を受ける危険性がある者への研修 研究者は、自分の研究や外国との共同研究が、どのように外国の干渉の対象になるかを考慮する必要がある。大学のガイドラインとアドバイスを通して、変化する脅威環境に照らして必要に応じ、または政府の助言に従い、既存のセキュリティと個人の安全保護を適応させる必要がある ・ 大学間および政府との知識共有 大学と政府は、機関やセクター間およびセクター間で情報共有をする。これには、外国の干渉、不当な影響力の行使、またはその他の方法で学問の自由と価値を損なう試みの例を共有することが含まれる。セクリティ機関は、オンラインリソースなどを通じて、大学がリスクを特定し、それに見合った対応を行うのを同様に支援をする

■ 罰則

記載なし

g）Australian Government intellectual property manual[320]

■ 策定機関・策定時期

Department of Communications and the Arts 2018 年

■ 策定の背景・目的

オーストラリア政府職員を対象とする政府の知的財産（IP）保護のガイドラインである。Public Governance, Performance and Accountability Act 2013（PGPA）に基づき、効率的かつ効果的な方法で IP を識別、記録、使用、評価、保護、活用するためのシステムの実装を含む IP 管理を目的としている。

■ 適用範囲

オーストラリア政府の職員を対象とした IP 保護の手法を示しており、「IP について」「IP フレームワークの作成」「IP 管理」「IP 保護」「IP の評価」「IP を含む調達と助成金の

[320] https://www.infrastructure.gov.au/sites/default/files/consultation/pdf/ip-manual.pdf

取扱い」「第三者の IP の使用」「IP の共有と一般公開」「政府 IP の商用化」「IP 権に対する執行」に項目を分けて説明がなされている。

■　情報の分類

IP を保護するための管理方法については規定されているが、情報の部類については規定していない。

■　情報管理策

IP を保護するために必要な取組を示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

以下の方針に従って各政府機関のニーズに沿った IP 保護の取り組みを実施するためのガイドラインを提供している。

（Australian Government intellectual property manual における組織的管理策）

- 各機関は、IP のライフサイクルを通じて意思決定を行うために、IP ポリシー、ポリシー導入計画を含む枠組みを作成し、定期的な見直しを行う。適切なトレーニングやポリシーの文書化と提示を通じて職員の意識向上を促す
- IP 管理は、生成から廃棄に至るライフサイクルを通じて識別、記録、監査を行う。研究開発機関の場合は、新技術に関わる実験ノートの取扱いも定める。第三者とプロジェクトを締結する場合、請負業者により生成された新たな IP を特定する措置を講じる
- IP 保護については、発明の場合、特許の取得、機密情報としての保護、あるいは国家安全保障上の理由から保護するのかを考慮する。職員以外で機密情報にアクセスする者と適切な機密保持契約を締結する
- IP を含む調達の際には、調達ライフサイクル全体を通じて管理を行う。ICT ソフトウェア契約については、IP 所有権を持つサプライヤーに有利な立場を採用する
- 政府機関間の IP 共有および一般公開を行う際は、IP の所有権を確認し、プライバシーや国家安全保障等についても考慮する

■　罰則

職員により、IP に対する重大な侵害が行われた場合、在職・退職の状態に応じて、Public Service Act, the Parliamentary Service Act 1999, Defence Force Discipline Act 1982, Australian Federal Police Act 1979 等の関連法に基づく行政措置または懲戒処分を受ける可能性がある。

(9) インド

1) 基本情報

- 政治体制：議院内閣制
- 人口：14 億 1,717 万人（2022 年）[321]
- 名目 GDP：3 兆 3,851 億ドル（2022 年）、実質 GDP：約 2 兆ドル(2022 年)[322]
- 研究開発予算：587.2 億米ドル　（18 年度）

■　政治動向

東アジア諸国の中で民主主義国家として内政運営は比較的安定している。国境を接する中国・パキスタンと領土問題を抱えており、対中抑止の利害が一致しているため日米と QUAD、IPEF などで共同している。外交面では米国、日本、豪州等西側諸国と共同し、G20、BRICS のメンバーである他、インド洋に面しアジアーアフリカ間のシーレーンの中央に位置し国際社会での影響力を有している。

■　経済動向

1991 年の経済自由化以降、製造業を中心に発展した東アジア諸国と異なり、IT 産業などサービス業を中心とした経済発展を遂げた。経済重視の姿勢を掲げるモディ政権成立以降、GDP 成長率は 7～8%と高い水準を維持している。一時期コロナ禍の影響を受け GDP 成長率は 3%に低減したものの、2021 年以降コロナ前の水準に回復しつつある。

コロナ禍ではロックダウンによる内需停滞、輸入減少、輸送コストの上昇などによって国内産業が打撃を受け、サプライチェーンの脆弱性が浮き彫りとなったため対処方針として Self Reliant India を打ち出している。

■　社会動向

2023 年内に中国を抜いて世界最大の人口（14 億 3 千万人）に達すると見られており、巨大な中間所得層を有している。かつてのカースト制度は廃止されたものの、身分制度に基づく抑圧、経済的格差、宗教的対立などの問題が多く、不平等是正や弱者層救済といった課題に直面している。

■　技術動向

インドは地理的、歴史的経緯から IT 産業に強みを持ち、政府による支援もあいまって大規模な IT スタートアップ・エコシステムが形成され、インド国内のユニコーン企業の数は米国、中国に続いて世界第 3 位となっている。

他方、未だ労働人口の半数以上は農業で生計を立てている事実があり、農村部の開発や農村部住民の所得問題は現在も重要な政策課題である。

---

321 https://www.mofa.go.jp/mofaj/area/india/data.html

322 https://pib.gov.in/PressReleseDetailm.aspx?PRID=1928682

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

インドでは、国家機密に関する情報等の保全に関連するものとして、2005 年に「Right to Information Act（情報公開法)」が制定された。この法律の中で、情報を要求されたものの内、国家の安全、主権、統一に関わる情報や、国際関係に重大な影響を及ぼす情報、捜査・訴訟に関する情報、営業秘密、個人情報等については公開の例外として規定されている[323]。

また 2013 年には「National Information Security Policy and Guidelines（国家情報セキュリティ方針とガイドライン)」が策定された。本ポリシーおよびガイドラインは、政府および公共部門の組織等の管理下または所有権下にある情報を、そのライフサイクル全体を通じて保護することを目的としており、行政組織で利用可能なすべての情報については全て Top secret、Secret、Confidential、Restricted に分類すべきであると規定されている[324]。

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

インドでは輸出管理の法令として、1992 年に「The Foreign Trade (Development & Regulations) Amendment Act（外国貿易（開発・規制）法)」が策定された。本法令に基づいて輸出品目リストにより、軍事関連品目、通信、航空宇宙、ライフサイエンス、石油・ガス、原子力、化学、製造業、ソフトウェア、技術品目等の物品を分類してその輸出入を Prohibited、Restricted、STE(State Trading Enterprises)で規制していた。

2010 年には強化版として「The Foreign Trade (Development & Regulations) Amendment Act, 2010（2010 年外国貿易（開発・規制）法)」が策定され、罰則等の強化の他、輸出入の定義を商品だけでなく「技術」、「役務」にも拡大し、原子力や大量破壊兵器などの国家安全保障に関わる分野を「特定物品、役務および技術」として輸出の禁止・制限することで、多義的技術を含む重要な情報の流出防止を図っている[325]。

また、技術移転に関するガイドラインとして、2015 年には MoD（Ministry of Defence：インド国防省）傘下の DRDO（Defence Research and Development Organisation：防衛開発研究機構）によって、官民産業への技術移転制度確立を目的とするガイドラインである「Guidelines for transfer of technology」が出されている他、2019 年には学術期間の知的財産管理のためのガイドラインである「Draft Model Guidelines on Implementation of IPR Policy for Academic Institutions」、バイオ分野においては、2021 年にバイオサイエンス関連データの交換・共有促進プログラムのガイドラインである「Promotion of Research and Innovation though Data Exchange」が策定される等、あらゆる分野において情報の管理に関する法令等が策定されている。

---

323 https://cic.gov.in/sites/default/files/RTI-Act_English.pdf

324 http://164.100.58.63/files/NATIONAL%20INFORMATION%20SECURITY%20POLICY%20AND%20GUIDELINES.pdf

325 https://www.dgft.gov.in/CP/?opt=itchs-import-export

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　国家戦略等

2023 年に ISRO（Indian Space Research Organisation：インド宇宙研究機関）によって Indian Space Policy - 2023 が策定された。これはインド政府の今後の宇宙開発に関する指針を示すものであり、宇宙および地上資産の創出を含む、宇宙経済のバリューチェーン全体への民間部門の参加をさらに奨励・推進することにより、総合的なアプローチを追求することが掲げられている[326,327]。経済安全保障との関連性として、本指針の中でも「国家の社会経済的発展と安全保障、環境と生命の保護、宇宙の平和的探査の追求、国民の意識と科学的探求の刺激のため」などと触れられている。

■　研究開発機関

インドの宇宙領域の研究開発関係機関としては、民生分野における研究では ISRO、防衛分野では DRDO(Defence Research and Development Organisation：国防研究開発機構）が主要な役割を担っている。ISRO は DoS（Department of Space：宇宙省）が所管する国立研究所の一つで、インドの宇宙関連の研究開発をリードするために 1969 年に設立された。DRDO は MoD（Ministry of Defence：国防省）が所管する国立研究所の一つで、航空学、兵器、エレクトロニクス、戦闘車両、工学システム、計装、ミサイル、先端コンピューティング等の多岐にわたる分野をカバーする防衛技術の開発を行っている（図 4.1-29）。

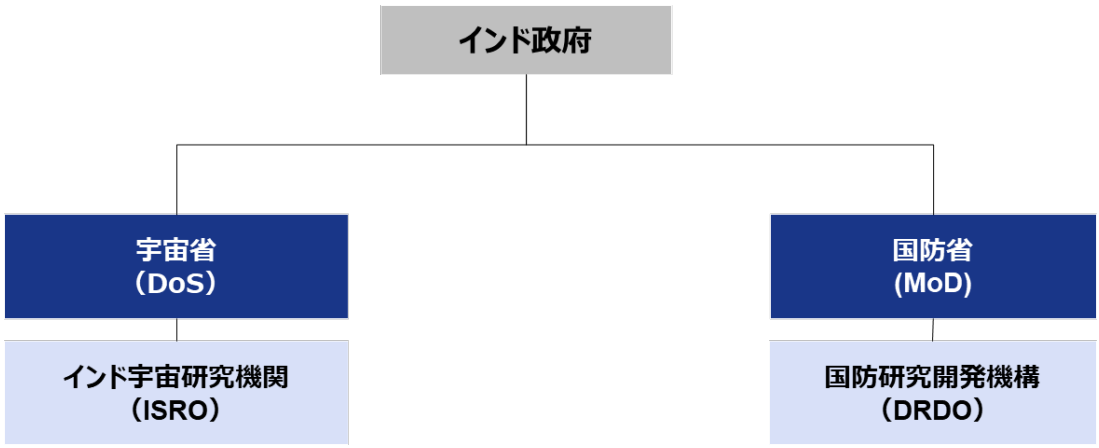


図 4.1-29　インドにおける宇宙領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　Respond BASKET - 2022[328,329,330]

ISRO が所管するプログラムであり、本プログラムの枠組みの下で、ISRO/DOS センター/

326 https://www.isro.gov.in/IndiaSpacePolicy.html

327 https://www.isro.gov.in/media_isro/pdf/IndianSpacePolicy2023.pdf

328 https://www.isro.gov.in/media_isro/pdf/programme/respond_basket_2022.pdf

329 https://www.isro.gov.in/RESPONDFormsandFormats.html

330 https://www.isro.gov.in/SupportedAreasofResearch.html

ユニット 14 機関が特定した最緊急の研究トピック（約 200 件）を ISRO が取りまとめて、学術界からの詳細な提案を募集し、支援するプロジェクトである。ISRO/DOS センターの専門家が、新規性、方法論、アプローチ、対象分野における PI の経験、プロジェクトの期間、予算などに基づいて評価を行う。

本プログラムにおける成果物の帰属についてはインドの法律・規則に従うことが記載されているが、具体的な記載はない。

b）海洋領域

■ 国家戦略等

2015 年に MoD によって Ensuring Secure Seas: Indian Maritime Security が策定された。これはインドの海洋におけるセキュリティ戦略で、The Science and Technology Roadmap (2015-2035) および Indian Naval Indigenisation Plan (2015-2027)に従い、海洋領域における研究開発の取り組みが活発化することを目指している [331]。経済安全保障との関連性として、インド海軍は、「ニッチ分野への投資と長期的視点における研究開発にも注力することで、他の政府機関や民間部門の取り組みを補完する」と述べられている。

■ 研究開発機関

インドの宇宙領域の研究開発関係機関としては、民生分野における研究では MoES (Ministry of Earth Sciences：地球科学省)、防衛分野では DRDO が主要な役割を担っている。MoES はインド政府が所管する政府機関の一つで、気象、海洋、自然災害等についての情報提供サービスを行っており、これらについての研究開発も実施している。DRDO は MoD が所管する国立研究所の一つで、航空学、兵器、エレクトロニクス、戦闘車両、工学システム、計装、ミサイル、先端コンピューティング等の多岐にわたる分野をカバーする防衛技術の開発を行っている（図 4.1-30）。

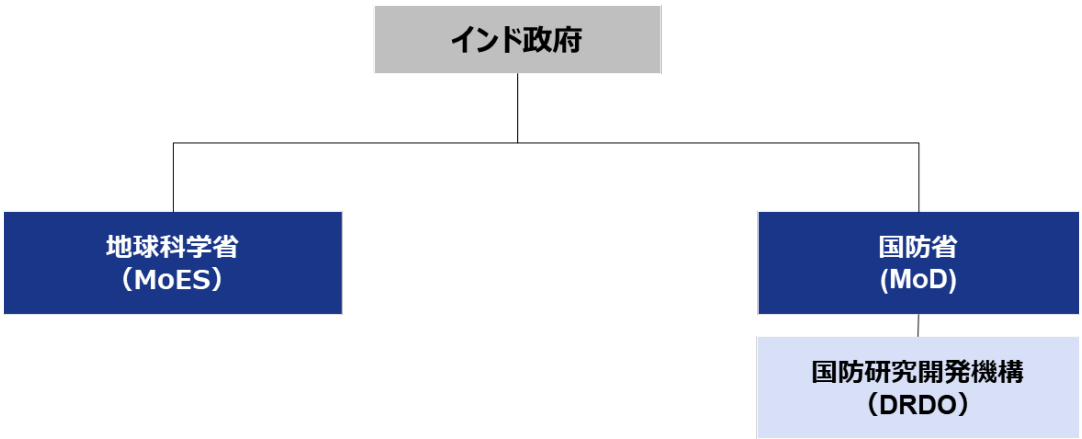


図 4.1-30 インドにおける海洋領域研究開発の主要機関

331 https://www.indiannavy.nic.in/sites/default/files/Indian_Maritime_Security_Strategy_Document_25Jan16.pdf

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Deep Ocean Mission (DOM)[332,333,334]

MoES が所管するプログラムであり、深海資源とその持続可能な利用のために深海を探索し、国の海洋および海事経済を成長させ、気候変動と汚染に取り組むための技術開発を目指すプロジェクト。プロジェクトの内容は i) 深海採掘および有人潜水船技術の開発、ii) 海洋気候変動アドバイザリーサービスの開発、iii) 深海の生物多様性の探査と保全のための技術革新、iv) 深海調査・探査、v) エネルギー・ 海洋からの淡水、vi) 海洋生物学のための先進海洋ステーションの 6 項目に分かれている。その一環として、MoES 傘下の NIOT (National Institute of Ocean Technology：国立海洋研究開発機構) と ISRO 傘下の VSSC (Vikram Sarabhai Space Centre：ヴィクラム・サラバイ宇宙センター) が協力して深海資源の探査を行う。

本プログラムにおける成果物の帰属についてはインドの法律・規則に従うことが記載されているが、具体的な記載はない。

c) バイオ領域

■　国家戦略等

2021 年に DBT (Department of Biotechnology：バイオテクノロジー省) によって NATIONAL BIOTECHNOLOGY DEVELOPMENT STRATEGY[335]が策定された。これは国の発展と社会の幸福のためのツールとしてバイオテクノロジーの可能性を活用することをビジョンと掲げているバイオテクノロジー戦略で、目標として、①教育・研究におけるエコシステムの構築と強化、②開発・展開において世界的なプレイヤーとなること、③産学連携による新興企業・起業家精神・産業基盤を構築・育成すること、④インドを強力なバイオ製造拠点とすること、の 4 つが掲げられている。経済安全保障との関連性として、バイオテクノロジー技術は暮らしやすさ、医療の改善、農業生産高の向上を実現することができ、経済的繁栄に大きな影響を与える重要な技術とされている。

■　研究開発機関

インドのバイオ領域の研究開発関係機関としては、民生分野における研究では DST (Department of Science and Technology：科学技術庁)、防衛分野では DRDO が主要な役割を担っている。DST は MoST (Ministry of Science and Technology：科学技術省) が所管する政府機関の一つで、科学技術の新領域を促進し、インドの科学技術活動を組織化し、調整・促進する役割を担っている。インドにおける主要な研究資金配分機関であり、基礎研究及び応用研究に係る主要な資金配分も担っている。DRDO は MoD が所管する国立研究所の

332 https://www.moes.gov.in/sites/default/files/PIB1806541.pdf

333 https://www.moes.gov.in/sites/default/files/2022-09/Advertisement-for-call-for-proposals-under-DOM2.pdf

334 https://www.indiascienceandtechnology.gov.in/announcementsopportunity/ministry-earth-sciences-moes-announces-call-proposals-collaborative-research-under-deep-ocean

335 https://www.europabio.org/wp-content/uploads/2023/09/India_NATIONAL-BIOTECHNOLOGY-DEVELOPMENT-STRATEGY_01.04.pdf

一つで、航空学、兵器、エレクトロニクス、戦闘車両、工学システム、計装、ミサイル、先端コンピューティング等の多岐にわたる分野をカバーする防衛技術の開発を行っている（図 4.1-31）。

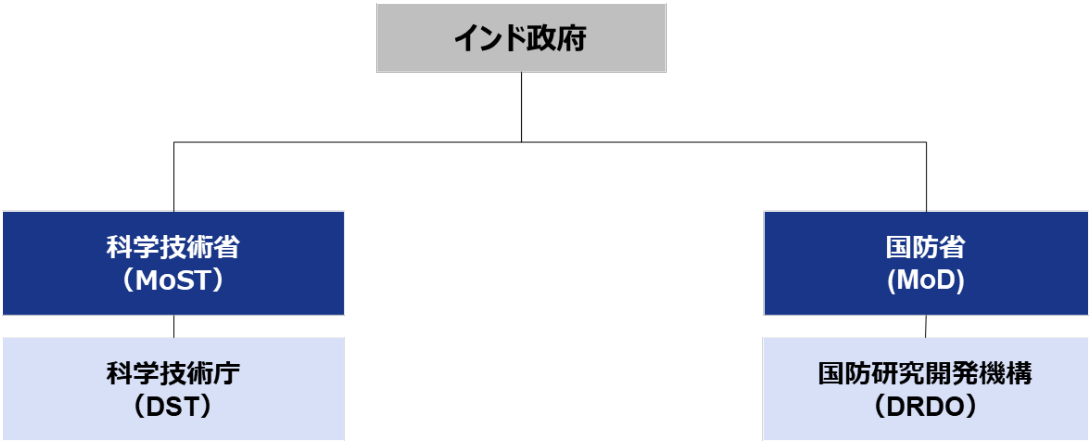


図 4.1-31　インドにおけるバイオ領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・ Intensification of Research in High Priority Areas（IRHPA）[336]

DST が所管するプロジェクトであり、高優先領域での研究を強化することを目的としている。複数の学問分野や機関の専門知識が必要な高優先領域の提案を支援し、特定の分野での国際的な科学マップにインドを位置づけることを目指しており、直近では BSL（生物安全レベル）3 および ABSL（動物生物安全レベル）3 施設の設立を目的とし、感染症原因体の取り扱い、薬剤発見、診断、新しいワクチンの研究に焦点を当てるプログラムが募集されていた。

本プログラムにおける成果物の帰属についてはインドの法律・規則に従うことが記載されているが、具体的な記載はない。

d）サイバー領域

■　国家戦略等

2013 年にインド政府によって National Cyber Security Policy -2013 が策定された。これは安全なサイバーエコシステム構築することを目的として策定されたサイバーセキュリティポリシー。①安全なサイバーエコシステムの構築、②安全なフレームワークの構築、③オープンスタンダードの奨励、④規制枠組みの強化、⑤電子ガバナンスの保護、⑥情報インフラの保護、⑦サイバーセキュリティに関する研究開発の推進、⑧サプライチェーンリスクの軽減、⑨人材育成、⑩サイバーセキュリティ意識の醸成、⑪官民連携、⑫情報共有、⑬実装に向けたアプローチ、⑭ポリシーの運用、について述べられている [337]。経済安全保障との関連性として、サイバー空間は国民、企業、軍事機関が使用する共通空間であ

[336] https://serbonline.in/SERB/Irhpa_Instruction?HomePage=New

[337] https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf

り、サイバーセキュリティフレームワークを作成して、セキュリティ強化を図ることは重要であるとされている。

■　研究開発機関

インドのサイバー領域の研究開発関係機関としては、民生分野における研究では DST、防衛分野では DRDO が主要な役割を担っている。DST は MoST が所管する政府機関の一つで、科学技術の新領域を促進し、インドの科学技術活動を組織化し、調整・促進する役割を担っている。インドにおける主要な研究資金配分機関であり、基礎研究及び応用研究に係る主要な資金配分も担っている。DRDO は MoD が所管する国立研究所の一つで、航空学、兵器、エレクトロニクス、戦闘車両、工学システム、計装、ミサイル、先端コンピューティング等の多岐にわたる分野をカバーする防衛技術の開発を行っている（図 4.1-32）。

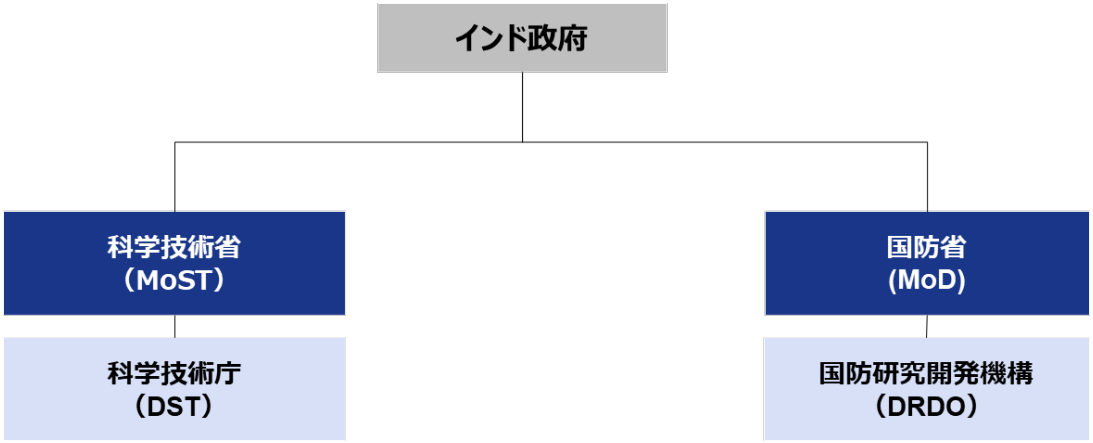


図 4.1-32　インドにおけるサイバー領域研究開発の主要機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　Intensification of Research in High Priority Areas (IRHPA)[338]

DST が所管するプログラムであり、高優先領域での研究を強化することを目的としている。複数の学問分野や機関の専門知識が必要な高優先領域の提案を支援し、特定の分野での国際的な科学マップにインドを位置づけることを目指しており、直近では地球環境をモデリングするための AI 技術の開発に関する募集がなされていた。

本プログラムにおける成果物の帰属についてはインドの法律・規則に従うことが記載されているが、具体的な記載はない。

e）多義的技術

■　国家戦略等

インドにおいては、2021 年にインド・イスラエル二国間イノベーション協定が結ばれ、ドローン、ロボット工学、人工知能、量子技術、フォトニクス、バイオセンシング、ブレイン・マシン・インターフェース、エネルギー貯蔵、ウェアラブルデバイス、自然言語処理等

[338] https://serbonline.in/SERB/Irhpa_Instruction?HomePage=New

の多義的技術分野における研究開発に関する協定が結ばれた他、2023 年には退役軍人のイニシアティブである STRIVE シンクタンクとメディア組織が主催した「アートマニルバール・バーラト（自立したインド）」に関する防衛対話の中で防衛部門と民間部門の両方に利益をもたらす多義的技術の開発を呼びかけられる等、多義的技術に対する取り組みが行われている[339,340]。

また、2023 年にはインドと米国の防衛エコシステムの促進・強化のための二国間パートナーシップであり、産学および官民主導で、主にスタートアップ企業を対象とする一連の支援体制の構築を目指す「INDUS-X（India-United States Defence Acceleration Ecosystem）」が結ばれる等、多義的技術の研究開発における他国との連携を強めている。

■　研究開発機関

インドにおける多義的技術の研究開発については、MoD や、その傘下の DRDO が主導して実施している。特に 2023 年に結ばれた INDUS-X においては、MoD および米国の DoD の主導のもと、スタートアップ企業を対象に、課題セット、指導、防衛の商業化、事業開発、製品の改良、技術の進歩、資金調達の機会等を提供する Accelerator Program for Defense Start-ups（防衛スタートアップを対象とするアクセラレータープログラム）、インドと米国の大学や研究所、技術ハブ（T-HUB）等を対象に、防衛イノベーション、守備、商業化のベストプラクティスに関するワークショップを提供する Academic & Start-up Programming Partnerships with Universities and Accelerators（大学およびアクセラレーターとのアカデミックおよびスタートアッププログラミング パートナーシップ）や、米国とインドの新興企業を対象に、国防省と DoD は外部関係者と協力し、両国に共通する多義的技術のユースケースを活用した共同課題を検討する Joint Challenges（ジョイント チャレンジ）等の多くのプログラムが実施されている[341]。

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　Torpedo/Underwater Vehicle Speed Measurement Device[342]

DRDO が所管するプログラムであり、新しい魚雷/水中車両の速度測定装置を開発することを目的とし、50 から 60 ノットの速度レベルまでの車両の絶対速度を測定する能力を有する装置を開発することが求められている。

本プログラムにおける成果物の帰属についてはインドの法律・規則に従うことが記載されているが、具体的な記載はない。

・　Artificial Intelligence Based Futuristic System For Autonomous Object Detection And Tracking[343]

DRDO が所管するプログラムであり、独立して展開可能なソリューションであり、(a)武器

339 https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1770299

340 https://pib.gov.in/PressReleasePage.aspx?PRID=1933019

341 https://media.defense.gov/2023/Jun/21/2003244837/-1/-1/0/FACTSHEET-INDUS-X-FINAL.PDF

342 https://tdf.drdo.gov.in/project/torpedounderwater-vehicle-speed-measurement-device-1

343 https://tdf.drdo.gov.in/project/artificial-intelligence-based-futuristic-system-autonomous-object-detection-and-tracking

としてのUAV、(b)搬送機としてのUAVの2の用途で使用できる自律的なUAV（無人航空機）システムの開発を目指している。

本プログラムにおける成果物の帰属についてはインドの法律・規則に従うことが記載されているが、具体的な記載はない。

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に以下の通り調査対象国の秘密情報の取扱いに係る法令等をロングリストとして10件リストアップした（詳細はAppendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも1つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして5件抽出した（表 4.1-23)。

表 4.1-23　詳細調査を行う法令等のショートリスト

法令等の名称	理由
National Information Security Policy and Guidelines	官民機関における情報セキュリティポリシーに関するガイドラインのため
The Foreign Trade (Development & Regulations) Amendment Act, 2010	輸出入管理を規定している法令のため
Guidelines for transfer of technology	国家機関が有する防衛関係の技術を官民産業へ移転する方法を示したガイドラインのため
BIOTECH-PRIDE (Promotion of Research and Innovation though Data Exchange) GUIDELINES	バイオ分野の研究開発におけるデータの交換・共有を行うための方針を示したガイドラインのため
Draft Model Guidelines on Implementation of IPR Policy for Academic Institutions	IP所有権の管理等についての管理方法を示したガイドラインのため

以下に表 4.1-23 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）National Information Security Policy and Guidelines[344]

■　策定機関・策定時期

Ministry of Home Affairs　2014年

■　策定の背景・目的

電子形式で様々な情報が作成・保存・処理・アクセス・送信されているが、これらの電子情報は不正アクセスに対して脆弱であり、サイバー攻撃により情報の機密性、可用性、完全性が損なわれる可能性がある。情報セキュリティを担保することは国家安全保障において

[344] https://barnala.punjabpolice.gov.in/wp-content/uploads/2022/03/06-National-Information-Security-Policy-and-Guidelines-v5.0.pdf

重要な事項であるため、インド政府（内務省）によって情報の取扱手順を規定するためのガイドラインとして策定された。

■　適用範囲

省庁やその下部組織において情報セキュリティを担保するためのガイダンスを示しており、省庁及びその下部組織において取り扱われる情報が対象となる。

本ガイドラインでは、「イントロダクション」「アプローチ」「情報セキュリティの中核となるドメインとその管理」「ICT セキュリティ」「セキュリティ慣行」に項目を分けて説明がなされている。

■　情報の分類

省庁やその下部組織において取り扱われる情報は、以下の 5 つに分類されている。

（National Information Security Policy and Guidelines における機密性レベルの区分）

- Top Secret：不正に開示された場合、国家安全保障や国益に極めて重大な損害を与えることが想定される情報。最高機密に分類されるため、細心の注意をもって取り扱われる必要がある
- Secret：不正に開示された場合、国家安全保障や国益に重大な損害を与えたり、大きな混乱を招いたりすることが想定される情報。通常使用される分類の中で最も高い分類である
- Confidential：不正に開示された場合、組織のセキュリティや利益に損害を与えたり、組織の機能に影響を与えたりする可能性がある情報。ほとんどの情報が Confidential に該当する
- Restricted：公的な目的のみに使用され、公的な目的以外には公開や伝達されない情報
- Unclassified：開示に対して保護を必要としない情報

■　情報管理策

・　組織的管理策

最高情報セキュリティ責任者を設置することが規定されており、組織全体の情報セキュリティ体制の設計・実装・管理を行うことが求められる。

・　人的管理策

従業員の採用プロセスの一環として身元調査又はセキュリティ・クリアランスを実施すること、従業員を対象とした情報セキュリティトレーニングを行うこと、情報へのアクセスが許可されている従業員のリスト化等を行うことが記載されている。

・　物理的管理策

ユーザ ID によるアクセス管理を行うことが記載されており、ユーザのアクセスを承認・付与・管理するための手順を文書化することが求められている。また、情報を管理している施設については、監視カメラや警報機、侵入検知器等により監視することも記載されている。

・　技術的管理策

暗号化技術を使用してデータを保護するように記載されており、Top Secret や Secret については SAG（Scientific Analysis Group）が承認した暗号化アルゴリズムを使用するよ

うに規定されている。

■　　罰則

記載なし

b）The Foreign Trade (Development & Regulations) Amendment Act, 2010[345, 346, 347]

■　　策定機関・策定時期

2010 年

■　　策定の背景・目的

インドの輸出入を管理する「1992 年外国貿易（開発・規制）法」を改正し、規則及び罰則を強化することを目的とした法令。

■　　適用範囲

輸出入の定義を商品だけでなく「技術」、「役務」にも拡大し、原子力や大量破壊兵器などの国家安全保障に関わる分野を「特定物品、役務および技術」として輸出の禁止・制限を行う対象としている。

本法令では、「目的や範囲などの一般条項」「中央政府による外国貿易ポリシー発令の権限」「輸出入業者コード番号とライセンス」「量的制限」「捜索、押収、罰則および没収」「特定の物品、役務および技術の輸出規制」「異議申し立てとレビュー」「雑則」に項目を分けて説明がなされている。

■　　情報の分類

貿易管理を行う特定商品又は役務・技術の定義として以下が規定されている。

（The Foreign Trade (Development & Regulations) Amendment Act, 2010 における貿易管理の対象となる商品・役務・技術の定義）

- **以下の理由により輸出、輸入、譲渡、再譲渡、経由及び積み替えが禁止または制限されている商品又は役務又は技術**
  - **インドの国家安全保障あるいは武器に関する二国間、多国間又は国際条約、規約、取り決めに基づく外交政策又は国際義務の推進に関連するものであること**
  - **大量破壊もしくはその運搬手段であること**

■　　情報管理策

輸出入を管理するための方法を示す人的・組織的管理策のみ記載されているため、物理的・技術的管理策は規定していない。

345 https://content.dgft.gov.in/Website/Foreign_Trade_(Development_&_Regulations)_Amendment_Act,_2010.pdf

346 https://www.indiacode.nic.in/bitstream/123456789/1947/3/A1992-22.pdf

347 https://commerce.gov.in/wp-content/uploads/2021/06/Foreign_Trade_Development__Regulation_Act_1992.pdf

・　人的管理策

事務局長または同等の権限を与えられた役人は、特定の商品又は役務・技術の輸出入に関する違反が認められた場合は、輸出入の許可証の保有者から輸出入許可を一時停止または取り消すことが可能とされている。

・　組織的管理策

輸出入管理を強化する目的として以下が規定されている。

(The Foreign Trade (Development & Regulations) Amendment Act, 2010 における輸出入管理強化の目的) ・　輸出入の定義を物品だけではなく「技術」、「役務」にも拡大する。「技術」には、パブリックドメインを除く、情報（商品またはソフトウェアの開発、生産または使用、産業活動または商業活動の開発または実行またはあらゆる種類のサービス提供に使用できる情報）が含まれる ・　中央政府は、本法および the Weapons of Mass Destruction and their Delivery Systems(Prohibition of Unlawful Activities) Act, 2005 (21 of 2005)などの関連法に基づき、原子力や大量破壊兵器などの国家安全保障や国際条約の遵守に関わる分野を「特定品目、役務および技術」として輸出の禁止・制限を行うことで貿易管理を行う ・　輸出入規定の違反として「当局に故意に虚偽文書を提出すること」を追加することで、罰則を強化する

■　罰則

本法令に違反した場合、以下の罰則が下される可能性がある。

(The Foreign Trade (Development & Regulations) Amendment Act, 2010 における罰則) ・　本法、関連規制または外国貿易ポリシーに違反する行為が行われた、または違反が試みられた場合、少なくとも 10,000 ルピーの罰金、または違反に関わる物品、役務、または技術の価値の 5 倍を超えない価格のうち、いずれか多い方の金額の罰金を科せられる可能性がある ・　記載事項が虚偽であることを知りながら、当局への提出文書に署名をした場合、少なくとも 10,000 ルピーの罰金、または虚偽の文書が提出された物品、役務、技術の価値の 5 倍以上の価格のうち、いずれか多い方の金額の罰金を科せられる可能性がある ・　「特定商品、役務および技術」に関わる違反行為については、the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 が適用される

c) Guidelines for transfer of technology[348]

■　策定機関・策定時期

[348] https://www.indiascienceandtechnology.gov.in/sites/default/files/file-uploads/guidelineregulations/1

DRDO　2015 年

■　　策定の背景・目的

MoD 傘下の DRDO から官民産業への ToT（Transfer of Technology：技術移転）制度確立を目的とするガイドラインである。

■　　適用範囲

DRDO が知的財産権（IP 権）を所有する技術について、同機構とのライセンスに基づく製造を通じたインド軍、内務省、政府機関への供給、および適切な国内外市場での販売を対象としている。

本ガイドラインでは、「DRDO ToT ガイドライン」「カテゴリーA 技術の移転ガイドライン」「カテゴリーB 技術の移転ガイドライン」に項目を分けて説明がなされている。

■　　情報の分類

機密度に応じて移転する技術の分類がなされており、MoD、内務省、その他の中央・地方政府機関のみをエンドユーザとする技術（MILTECH）をカテゴリーA、二重用途技術をカテゴリーB として分類している。

■　　情報管理策

ToT を行う際の方法を示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

DRDO が開発し、IP 権を持つすべての技術（爆発物を除く）の移転制度ガイドラインとして、技術分類・技術移転方法・契約締結の 3 項目について記載されている。

技術分類は、技術の機密度に基づき、MoD、内務省、その他の中央・地方政府機関のみをエンドユーザとする技術（MILTECH）をカテゴリーA、二重用途技術をカテゴリーB として分類されている。

技術移転方法としては、カテゴリーA のライセンスは、MoD、内務省およびその他の中央・地方政府機関に限定している。カテゴリーB のライセンスは、インド商工会議所による市場の適切性を検討し、ライセンス付与の可否を判断する。海外メーカーへの付与には、MoD および外務省の承認が必要であることが記載されている。

契約締結としては、IP 権保護のために、「機密保持および秘密保持契約（CNDA）」および「技術移転ライセンス契約（LATOT）」に加えて、メーカーへのサンプル提供時には「マテリアル移転契約（MTA）」を締結することが記載されている。

■　　罰則

記載なし

527507521_DRDO-guidelines-for-ToT.pdf

d）BIOTECH-PRIDE（Promotion of Research and Innovation though Data Exchange）GUIDELINES[349]

■　策定機関・策定時期

DBT　2021 年

■　策定の背景・目的

National Data Sharing and Accessibility Policy（NDSAP）に基づく、DBT によるバイオサイエンス関連データの交換・共有促進プログラムのガイドラインである。

■　適用範囲

国内の研究で生成されたすべてのバイオデータに適用され、データ生成後、合理的な期間内にデータを交換・共有を行うためのフレームワークと原則を提供している。

本ガイドラインでは、「イントロダクション」「定義」「データソースと種類」「データデポジット戦略とタイミング」「データ共有とアクセスの枠組み」「データ利用契約」「監査と法律問題」に項目を分けて説明がなされている。

■　情報の分類

生成されたデータをデータレベル 1（ローデータ）、データレベル 2（処理済みデータおよびメタデータ）に区別している。

また、データ管理においては、データの機密性に応じて「オープンアクセス」、「管理されたアクセス」、「アクセス不可」の 3 つに分類される。オープンアクセスの場合は誰でも利用可能であるが、管理されたアクセスの場合は特定の制限付きで共有されるデータのため、データのダウンロードには事前に Indian Biological Data Centre の許可が必要である。機密データについてはアクセス不可に分類される。

■　情報管理策

バイオデータを交換・共有するための基本原則を示す組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

国内の研究で生成されたすべてのバイオデータについて、データ生成後、合理的な期間内にデータを交換・共有を行うためのフレームワークと原則として以下の項目が記載されている。

（BIOTECH-PRIDE GUIDELINES におけるデータ公開・共有のための原則）

・　**生成されたデータは、特に公的資金を使用している場合、データレベル（1. ローデータ、2. 処理済データおよびメタデータ）に応じた既定の期間内に、適切な国家レポジトリに保存する必要がある。ただし、データが個人のプライバシー、絶滅危惧種等の保全、国家安全保障の観点から「機密データ」であるとして、公開免除の要求があった**

[349] https://dbtindia.gov.in/sites/default/files/Biotech%20Pride%20Guidelines%20July%202021_0.pdf

場合は、検討の上、免除される
- データの管理は、Indian Biological Data Centre が行う。Indian Biological Data Centre は、データの機密性に応じて 3 段階（オープンアクセス、管理されたアクセスおよびアクセス不可）の管理を行う。「機密データ」は、公的資金を使用して生成された場合でも、「アクセス不可」とする
- 当ガイドラインの実施は、省庁間国家運営委員会が監督・管理を行う。内務省は、国家安全保障の観点からデータセットを分析するため、同委員会のオブザーバーとなる
- データを使用するには、管理者である Indian Biological Data Centre とデータ利用契約を締結する必要がある
- データの所有権は、データを収集する政府機関/部門/省/団体に帰属する。データのアクセスや使用における違反は、National Data Sharing and Accessibility Policy (NDSAP)の枠組みで対処されるものとする

■ 罰則

記載なし

e) Draft Model Guidelines on Implementation of IPR Policy for Academic Institutions[350]

■ 策定機関・策定時期

DPIIT (Department for Promotion of Industry and Internal Trade：商工省産業国内取引促進局) 2019 年

■ 策定の背景・目的

学生主導のスタートアップ企業やベンチャー企業等が効率的に知的財産権を保護できるように支援することを目的としたガイドラインであり、知的財産権（IP 権）の実施に関するポリシーが規定されている。なお、本ガイドラインは既存の知的財産法を補完するためのものであり、学術機関がすでに採用しているガイドライン等を無効化するものではない。

■ 適用範囲

学術機関における IP 所有権の管理や譲渡、IP から生み出される収益分配を行うための効率的で公正かつ透明な管理プロセスを示しており、学術機関が保有している全ての知的財産に適用される。

本ガイドラインでは、「目的や範囲などの一般条項」「IP の所有権」「商用化と利益の共有」「起業スタートアップの推進」「ライセンス契約と利益共有」「責任制限」「IP 保護のためのコスト共有」「学術機関による知的財産権の放棄」「学術機関の知的財産リソースの使用」「第三者が所有する知的財産権の取り扱い」「Free and Open-Source Software(FOSS)使用の推奨」「機密性」「公開」「紛争解決」に項目を分けて説明がなされている。

■ 情報の分類

学術機関が保有する全ての知的財産が適用範囲であり、分野等による分類はなされてい

[350] https://dpiit.gov.in/draft-model-guidelines-implementation-ipr-policy-academic-institutions

ない。

■　　情報管理策

IPやIPから得られる収益の管理プロセスとして組織的管理策のみ記載されているため、人的・物理的・技術的管理策は規定していない。

・　組織的管理策

学術機関の IP 所有権の管理や譲渡、IP から生み出される収益分配を行うための効率的で公正かつ透明な管理プロセスとして、以下の基本方針が示されている。

（Draft Model Guidelines on Implementation of IPR Policy for Academic Institutions における IP 管理の基本方針） ・　本ガイドラインは、学術機関と法的関係を確立したすべての研究者に適用される。ただし研究者が本ガイドラインの発効日前に学術機関と明示的にこれに反する協定を締結した場合、または学術機関があらかじめ定められた権利義務に関して第三者と契約を締結していた場合は適用されない ・　IP 所有権（特許、著作権、商標、工業意匠、半導体集積回路および植物の新品種）は、基本的に学術機関に帰属する。ただし、研究者が学術機関のリソースを使用せずに考案または実施したと学術機関が判断した場合、所有権は研究者に帰属する。外部パートナーと研究協力を行う際には、関係者間の契約で帰属を決める ・　大学発の起業を推奨するため、学術機関の関与を最小限に抑えて独自に IP の商用化、保護、ライセンス供与を望むスタッフに対して、学術機関は契約に基づき IP 所有権を再譲渡することができる。IP 商用化の際に収益分配契約を締結しない場合は、ロイヤルティ/技術移転額の分配を研究者と学術機関で 60:40 の比率で行うことを提案する ・　学術機関内の機密データおよび個人情報を不正アクセス、紛失、破壊または侵害から保護することを目的として、学術機関は、情報ユーザと適切な機密保持契約を締結することが推奨される ・　研究活動から生じた出版物、文書および/または論文は、学術機関と研究者が共同所有するものとする。特許申請を行う場合は、出願前に公開されないように特に注意する。また学術機関は、公開される情報から特定部分の除外を要求する権利を有する

■　　罰則

記載なし

（10）韓国

1）基本情報

- 政治体制：大統領制、立憲共和制[351]
- 人口：約 5,163 万人[351]
- 名目 GDP：1 兆 6,643 億ドル（2022 年、韓国銀行）[351]
- 研究開発予算：約 23 兆 5 千億ウォン（2022 年度）[352]

■ 政治動向

韓国は朝鮮戦争の歴史的経緯から北朝鮮との間で準戦時体制を継続しており、援助を受けてきた米国と友好関係にある。日本とも経済協力・貿易等で関係は緊密であるが、歴史認識に係る問題等により、外交関係は厳しい状況が継続されてきた。

「南北関係の正常化」を掲げる現在の尹政権の発足により、対北朝鮮政策は融和に転換している。現政権は北朝鮮の実質的な非核化を条件に様々な経済支援を行うとする構想を提案したが、北朝鮮は同提案を拒否し軍事的挑発を継続している[353]。

■ 経済動向

天然資源に乏しいことから韓国経済は貿易への依存度が高く GDP の約 8 割を占めており、中国は最大の輸出入相手国である。

主要な産業構造は日本に似通っており、電子・電気機器、自動車、鉄鋼、船舶などに強みを持っている。特にサムスン電子を始めとした半導体関連産業品目は輸出全体の 20%を占め、韓国の国際競争力に大きな影響力がある。GDP 成長率は近年低迷し２～４％を推移しており、新型コロナウイルス感染症拡大の影響により 2020 年からはマイナスに転じた。現在は輸出と民間消費の好調等によりコロナ前と同水準に戻っている 353。

■ 社会動向

朝鮮戦争が未だ休戦状態にあることから準戦時体制を維持しており、徴兵制度が存在する。また、国内での北朝鮮・共産主義を賛美する行為を規制する国家保安法を制定しており、国民の自由に対する侵害にあたる等の議論が存在する。

2018 年に 65 歳以上人口の割合が全体の 14%を越え高齢社会に突入したことにより、年金や医療、福祉関連を中心に財政支出圧力が強まっており、政策の見直しや財源確保が大きな課題になっている 353。

■ 技術動向

韓国の科学技術研究開発投資は年々増加傾向にあり、2020 年時点で世界第 5 位に位置し

351 https://www.mofa.go.jp/mofaj/area/korea/data.html
352 https://spap.jst.go.jp/korea/experience/2021/topic_ek_05.html
353 https://www.mofa.go.jp/mofaj/area/korea/data.html

ている。

2022 年までの第 4 次科学技術基本計画では、大分類 11、中分類 43 から 120 の重点科学技術を導出している。第 3 次計画から特に人工知能、スマートホーム、スマートシティ、3D プリンター、大気汚染への対応など 12 の技術が追加された [354]。

科学技術政策の推進体制としては、大統領府直属で大統領を議長とする国家科学技術諮問会議（PACST）が科学技術政策の最高意思決定、諮問機関として設置されており、その方針の下、科学技術・研究開発を所管する科学技術情報通信部が中心となって、各部（省に相当）及びその傘下の専門機関を通じて民間企業、大学等研究機関への資金提供が行われることが一般的となっている（図 4.1-33）[355]。

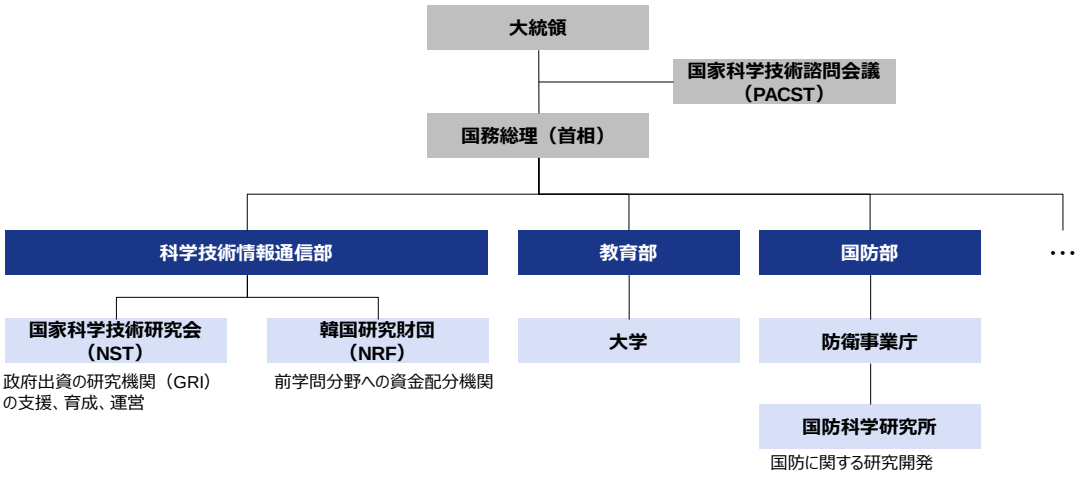


図 4.1-33　韓国の科学技術政策の推進体制

354 https://spap.jst.go.jp/resource/pdf/aprc-fy2022-pd-kor01.pdf

355 https://www.jst.go.jp/crds/pdf/2018/FR/CRDS-FY2018-FR-05/CRDS-FY2018-FR-05_10.pdf

2）秘密情報の取扱いに係る政策動向

① 安全保障の観点から国家機密に該当する技術情報等の保全政策

韓国では、1964 年に制定された保安業務規定が国家機密の保護に関する各種措置を規定している。国家機密は保安業務規定の根拠法である国家情報院法第 4 条第 1 項第 2 号において「国家の安全に対する重大な不利益を避けるために、限られた人員のみが知ることが許され、他の国家又は集団に対して秘密にする事実・物件又は知識として国家機密に分類された事項」として定義されており、その重要性からⅠ級秘密、Ⅱ級秘密、Ⅲ級秘密の等級に区分される[356]。

保安業務規定では秘密の分類、表示、受け渡し、保管、閲覧、開示、移管、破棄等の取扱いに関する要領のほか、秘密を取り扱う者の忠誠心や信頼性を確認するために、韓国の情報機関である国家情報院による身元調査を実施すること等が規定されている。

また、軍事上の機密については 1972 年から 1973 年に制定された軍事機密保護法及び同法施行令によって、その重要性から軍事Ⅰ級秘密、軍事Ⅱ級秘密、軍事Ⅲ級秘密の等級に区分されている。軍事機密については、軍事機密保護法及び同法施行令によって、機密の指定権者や保護措置の一部、機密指定の解除、公開等について保安業務規定とは別の規定が成されているが、軍事機密保護法施行令で示した事項以外については保安業務規定の定めによることとなっている[357]（表 4.1-24）。

表 4.1-24 韓国における情報の機密性レベルの定義

根拠	情報分類	定義
保安業務規定	Ⅰ級秘密	漏洩する場合、大韓民国と外交関係が断絶され、戦争を起こし、国家の防衛計画・情報活動及び国家防衛に必ず必要な科学と技術の開発を危うくするなどの懸念がある秘密
	Ⅱ級秘密	漏洩する場合、国家安全保障に莫大な支障を及ぼす恐れのある秘密
	Ⅲ級秘密	漏洩する場合、国家安全保障に害を及ぼす恐れのある秘密
軍事機密保護法施行令	軍事Ⅰ級秘密	軍事機密中で漏洩した場合、国家安全保障に致命的な危険を及ぼすと明らかに認められる価値を持つもの
	軍事Ⅱ級秘密	軍事機密中で漏洩した場合、国家安全保障に著しい危険を及ぼすと明らかに認められる価値を持つもの
	軍事Ⅲ級秘密	軍事機密中で漏洩した場合、国家安全保障に相当な危険を及ぼすと明らかに認められる価値を有するもの

356 https://www.law.go.kr/법령/보안업무규정

357 https://www.law.go.kr/법령/군사기밀보호법

② 技術移転の側面で研究開発に関連があると考えらえる安全保障貿易関連政策

韓国の安全保障貿易関連政策は、1987 年に対外貿易法へ「戦略物資輸出入告示」を導入したことに端を発し、以後ミサイル関連資機材・技術輸出規制（MTCR)、オーストラリア・グループ（AG)、ワッセナー・アレンジメント（WA)、化学兵器禁止条約（CWC）など国際的な輸出規制レジームに加盟して武器や軍事転用可能な貨物や技術の輸出について規制を図ってきた[358]。

また重要技術の管理に関する政策として、2007 年に「産業技術の流出防止および保護に関する法律（産業技術保護法)」が制定されており、国内外市場で占める技術的・経済的価値が高い、もしくは関連産業の成長潜在力が高く海外に流出する場合に国家の安全保障及び国民経済の発展に重大な悪影響を与える恐れがある技術を「国家核心技術」として指定し、輸出規制、安全保障・経済に影響を与える場合の情報の非公開、外国からの買収・合併の事前承認などの保護措置を講ずることが可能となっている。

近年では、2022 年に「国家先端戦略産業競争力強化および保護に関する特別措置法（国家先端戦略産業法)」が制定され、経済安全保障の確保および先端産業競争力の強化のため、「国家先端戦略技術」を指定し、関連産業（国家先端戦略産業）を育成・保護することとなった。「国家先端戦略技術」は産業通商資源部長官官の指定するものであり、先端戦略技術を外国企業などに輸出しようとする場合、または先端技術の保有者が海外 M&A・合弁投資を進めようとする場合、事前承認が必要となる。また、同技術を有する専門人材を指定し、離職・情報漏洩を防止する措置を講ずることになっている[359]。

[358] https://www.jstage.jst.go.jp/article/jafame/15/0/15_53/_pdf/-char/ja

[359] https://www.jetro.go.jp/biz/areareports/2022/53acfc046a91be41.html

3）研究開発プログラムにおける法令・ガイドライン

a）宇宙領域

■　国家戦略等

韓国では宇宙開発振興法を根拠とした「宇宙開発振興基本計画」が宇宙領域に関する最上位の法定計画であり、宇宙開発の中長期的な政策目標と方向性を定めている。宇宙開発振興基本計画は5年おきに更新されることとなっており、現在は2023年に策定された第4次基本計画が最新となっている。

第4次基本計画では、2045年の宇宙経済強国の実現を目指し、「宇宙探査の拡大」、「宇宙輸送の完成」、「宇宙産業の創出」、「宇宙安全保障の確立」、「宇宙科学の拡張」の5つを長期的なミッションとして定めているほか、2031年には月面着陸を成功させ、2045年には火星に着陸することで独自の宇宙探査計画を進めるとしている[360]。

経済安全保障の側面では、対外貿易法を根拠として宇宙関連技術・物資に輸出規制が課されており、宇宙関連技術・物資の輸出にあたっては産業通商資源部や原子力安全委員会、防衛事業庁をはじめとする輸出承認機関の許可を得ることが必要となっている[361]他、「産業技術の流出防止および保護に関する法律」によって指定される「国家核心技術」には、高性能・超低温ターボポンプ技術、極低温／高圧ダイヤフラム方式の開閉バルブ技術、超高解像度光学衛星の高速軌道の精密姿勢制御設計技術等４つの技術が宇宙分野として指定されており、国として規制・保護の対象となっていることが伺える[362]。

■　研究開発機関

韓国では、大統領直属の国家宇宙委員会が宇宙開発振興基本計画の策定等、宇宙開発に関する事項の審議を行っており、その下で科学技術情報通信部を中心として宇宙開発振興施行計画の策定・調整が行われ、宇宙関連政策が実行される。

関連機関としては、科学技術情報通信部の所管する韓国航空宇宙研究院（KARI）が韓国における航空宇宙分野の研究開発を主導するとともに、それに伴う産学研（産業、大学、KARI）の連携を推進しているほか、国防部所管の国防科学研究所（ADD）が国防宇宙領域の研究開発を実施しており、監視偵察システム、超小型衛星、軍の衛星通信システム等の研究を行っている。また、情報機関である国家情報院が情報活動の面で宇宙領域の関連機関として宇宙開発振興法に挙げられている（図 4.1-34）[363]。

360 https://www.msit.go.kr/bbs/view.do?sCode=user&bbsSeqNo=65&nttSeqNo=3017397

361 https://www.jetro.go.jp/biz/areareports/2022/53acfc046a91be41.html

362 https://unipass.customs.go.kr/clip/ctensrch/openULS0402007Q.do

363 https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%9A%B0%EC%A3%BC#undefined

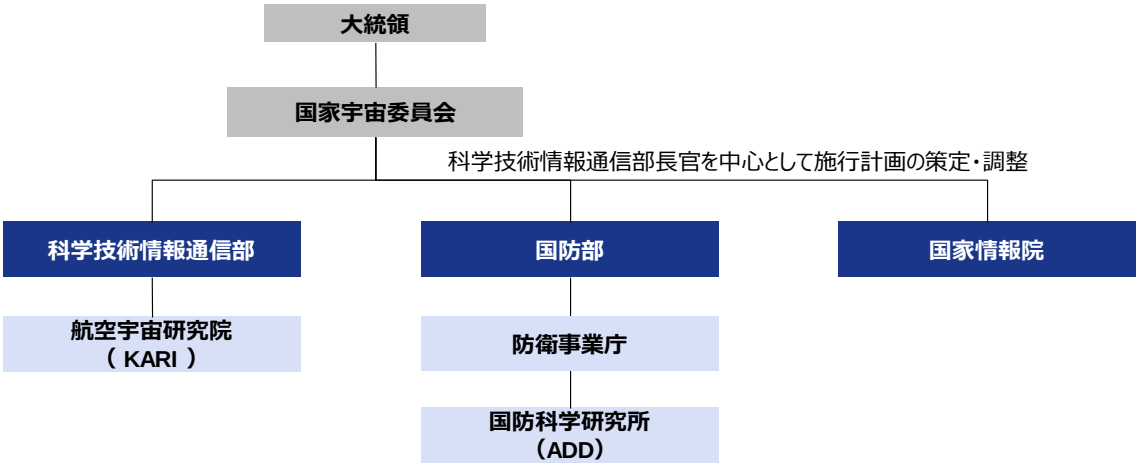


図 4.1-34　韓国における宇宙開発の主要な機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　多目的実用衛星 7A 号システム及び本体開発事業委託研究課題

航空宇宙研究院が所管する研究開発プログラムであり、2022 年に公募が実施されている。多目的実用衛星 7A 号のランダム方向撮影に最適なプロファイルの開発、機動区間の最適化方策、映像補正のための最適な機動について研究を実施するとされている。

公募要領等で準拠が示されている法令等には宇宙領域独自のものや、情報の取扱いに関するものは見受けられない。しかし本プロジェクトは宇宙開発振興施行計画にも記載があることから、宇宙開発振興法を根拠とした「宇宙開発事業」であると思料される。そのため、宇宙開発振興法及び施行令の罰則は適用されるものと思われる。

また衛星情報を取り扱う場合は、韓国では衛星情報を生産・構築・管理・流通及び活用する科学技術情報通信部及びその所属機関等を対象に、衛星情報の取扱いに関する事項を定めている「衛星情報セキュリティ管理規則」が存在しているため、適用される可能性はあるものの、公募要領等からは確認できなかった。

公募要領では以下のような法令等への準拠が示されている[364]。

（多目的実用衛星 7A 号システム及び本体開発事業委託研究課題の公募要領における準拠を求める法令等）

- **基礎研究振興及び技術開発支援に関する法律（参加機関の制限）**
- **国家研究開発事業の管理等に関する規定（公募要領で特に定めていない事項について準用するとしているが、2020 年に廃止されている）**
- **科学技術情報通信部所管科学技術分野研究開発事業処理規定（公募要領で特に定めていない事項について準用）**

・　有事の運用を考慮した地球同期軌道航法衛星のリアルタイム軌道

国防科学研究所が所管する研究開発プログラムであり、2023 年に公募が実施されている。

[364] https://www.kari.re.kr/cop/bbs/BBSMSTR_000000000261/selectBoardArticle.do?nttId=8166&kind=&mno=sitemap_02&pageIndex=2&searchCnd=&searchWrd

有事に限られた国内の一部の監視局だけが稼働しているような状況下で、衛星航法システムの精度を補正するための研究を実施するとされている。

公募要領等準拠が示されている法令等では、参加機関の資格要件として、「基礎研究振興および技術開発支援に関する法律」第 6 条第 1 項各号の機関を対象としている他、「国家を当事者とする契約に関する法律及び施行令」、「国家研究開発事業の管理等に関する規定」、「国家研究開発革新法」等を準用して入札（契約）及び国家研究開発参加制限措置を受けた業者、研究所等の参加を制限するとしている。

その他、本プログラムに提案を提出する場合は、国防部及び警察庁から、「保安業務規定」等の関係法令に基づき、身元調査を受けるため、その同意書及び身上事項を記載して提出しなければならないとしている。また外国人・外国機関・団体と共同で研究を実施している場合セキュリティ事故予防・対応方案などを提案に含める必要があるとしている [365]。

b）海洋領域

■　国家戦略等

韓国では、海洋水産発展基本法及び海洋水産科学技術育成法を根拠として、海洋・水産資源の開発・利用に係る基本方針である「海洋水産発展基本計画」[366]と、海洋領域にかかる重点技術開発戦略や、研究投資・人材育成の方向性を定める「海洋水産科学技術育成基本計画」[367]が策定されている。

海洋水産発展基本計画は 2021 年～2030 年の方針を定めた第 3 次基本計画が最新となっており、6 大推進戦略として①海洋水産安全強化②滞在したい漁村・沿岸造成③海洋水産業のデジタル転換④海洋水産業の質的跳躍⑤環境に優しい・合理的海洋利用⑥国際協力をリードする海洋強国　が掲げられており、海洋水産科学技術育成基本計画にも反映されていることが読み取れる。第 2 期海洋水産科学技術育成基本計画では、2023 年～2027 年の方針を定める第 2 期基本計画が最新となっており、4 大戦略として「Ⅰオーシャンデジタル・炭素中立の大転換」「Ⅱ 波を超える危機対応未来 R&D」「Ⅲ 民間成長動力の強化」「Ⅳ 海洋強国研究開発エコシステムの構築」が掲げられている。

経済安全保障の側面では、「産業技術の流出防止および保護に関する法律」によって指定される「国家核心技術」に造船分野が該当しており、８つの技術が指定されている [368]他、「外国人投資促進法」において外国人投資対象制限業種（30 種）が定められており、当該業種では一定の許容基準を満たす場合のみ投資が所管省庁から許可されている中、海洋関連（海洋水産部所管）では、「内航旅客運送業」「内航貨物運送業」などの海運業務が制限対象となっている [369]。

---

365 https://www.add.re.kr/kps/publicNtis/ntisView?pageNum=1&rowCnt=10&titleId=1535&menuId=MENU02201&titleId=0

366 https://www.aurum.re.kr/Legal/LegalSub.aspx?pcode=H09

367 https://polararchive.kr/board_view.php?key_type=b_sub_con&key_word=&pg=4&sn=1&pg4=22&pg3=52&pg2=25&pg1=1&mainCate=1&subCate=3&bo_table=nationalPolicy&idx=60&pn=2&sn=1&returnUrl=./_search_result.php

368 https://www.jetro.go.jp/biz/areareports/2022/53acfc046a91be41.html

369 https://www.jetro.go.jp/ext_images/jfile/country/kr/invest_02/pdfs/kr7A020_foreigner_inv_seigen.p

■　研究開発機関

韓国では海洋水産部長官とその所属である海洋水産発展委員会、海洋水産科学技術委員会が海洋領域の開発・管理、科学技術育成の基本計画を定めている。海洋領域の政府施策を遂行する主要な機関は海洋水産部の所管する海洋水産科学技術振興院（KIMST）が海洋水産科学技術育成のための専門機関として、研究開発事業等の企画・管理・評価等で海洋水産部を支援している他、同じく海洋水産部の下に位置する海洋警察庁が海上犯罪、密輸・密入国の監視と取締まり、海難救助、領海警備などを所管、環境部が自然環境及び生活環境の保全と、環境汚染防止などを所管している[370]。

軍事及びエネルギー関連は海洋領域とは別の枠組みで定めるため含まれないと海洋水産発展基本法第 6 条において規定されている（図 4.1-35）。

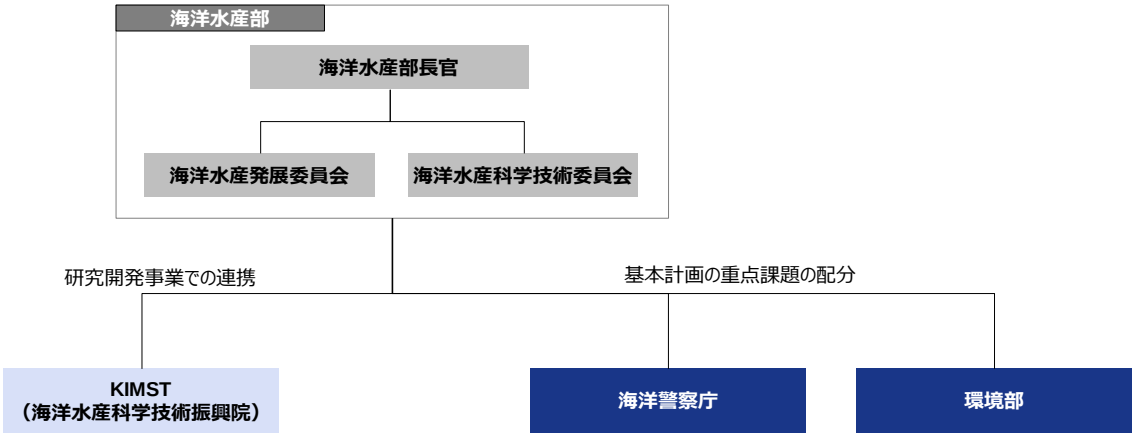


図 4.1-35　韓国における海洋領域研究開発の主要な機関

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　2023 年度海洋無人システム実証試験・評価技術開発事業新規課題

海洋水産科学技術振興院（KIMST）が所管するプログラムであり、2023 年に公募が実施された。ROV、AUV、USV などの海洋無人システムの試験評価体系を構築するとともに、運用技術に関する研究開発を実施するとしている。

公募要領等で準拠するとしている法令等としては、海洋領域特有のものではないが、参加機関の制限や選定基準・手順、研究開発成果の活用、セキュリティ等の面で「国家研究開発革新法」を参照しているほか、公募要領で示さない詳細は「海洋水産研究開発事業運営規定」「海洋水産研究開発事業管理指針」によるとしている[371]。

（2023 年度海洋無人システム実証試験・評価技術開発事業新規課題の公募要領で準拠を求める法令等）

・　国家研究開発革新法第 2 条第 3 号又は同法施行令第 2 条第 1 項のいずれかに該当する機

df

[370] https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%95%B4%EC%96%91%EC%88%98%EC%82%B0%EB%B0%9C%EC%A0%84%EA%B8%B0%EB%B3%B8%EB%B2%95

[371] https://www.iris.go.kr/contents/retrieveBsnsAncmView.do

関（参加制限） ・ 国家研究開発革新法第 10 条、14 条、同法施行令第 12 条、27 条（選定基準の根拠） ・ 国家研究開発革新法第 17 条、18 条、同法施行令第 34 条、38 条（研究開発成果の活用及び技術料納付の根拠） ・ 国家研究開発革新法第 21 条、同法施行令第 45 条（申請課題のセキュリティ等級の分類） ・ 海洋水産研究開発事業運営規定 ・ 海洋水産研究開発事業管理指針

c）バイオ領域

■ 国家戦略等

韓国では、バイオテクノロジーを効率的に育成・発展させ、その開発技術の産業化を促進し、経済発展を促すための法律として、バイオテクノロジー育成法が 1995 年から制定されている。同法では、バイオテクノロジーを「各種生物体の生物学的システム、生体、誘電体またはそれらに由来する物質・情報を研究・活用する学問と技術」として定義しており、その中には基礎医科学（生理学・病理学・薬理学）も含まれる [372]。

そして同法では科学技術情報通信部を中心として、バイオテクノロジーの育成に関する計画を策定することとなっており、現在は 2023 年～32 年の方針を定めた第 4 次バイオテクノロジー育成基本計画が最新となっている [373]。第 4 次基本計画では、「デジタル融合によるバイオイノベーション」「グローバル課題解決のためのバイオ融合 R&D 強化」「バイオ経済成果創出のためのスケールアップ促進」「バイオ融合エコシステムの組成」の 4 つの戦略目標が定められている。

経済安全保障の側面では、国家先端戦略産業競争力強化および保護に関する特別措置法において、現在「先端戦略産業」として指定されている 4 つの産業の中にバイオ産業が該当しているほか、産業技術の流出防止および保護に関する法律において「国家核心技術」にも生命工学 4 技術が含まれていることから、バイオ領域の技術については保護・育成が図られていることが伺える [374]。

■ 研究開発機関

韓国では、科学技術情報通信部長の下に、関係中央行政機関の次官級職員や、委嘱を受けたアカデミア、産業界の生命工学・生命倫理専門家等から構成される生命工学総合政策審議会が設置されている。同委員会では科学技術情報通信部長が委員長を務め、バイオテクノロジー育成基本計画を策定するために関係中央行政機関との総合的な調整を行うこととなっている [372]。

バイオ領域に関係する中央行政機関としては、科学技術情報通信部、保健福祉部、農林畜産食品部、産業通商資源部、環境部、海洋水産部など 15 省庁がバイオテクノロジー基本法では示されており、それらが所管する政府系研究所として韓国生命工学研究院（KRIBB）、国

372 https://www.law.go.kr/법령/생명공학육성법

373 https://doc.msit.go.kr/SynapDocViewServer/viewer/doc.html?key=baf87606eed846538f97b86efc439529&convType=html&convLocale=ko_KR&contextPath=/SynapDocViewServer/

374 https://www.jetro.go.jp/biz/areareports/2022/53acfc046a91be41.html

立感染症研究所、韓国食品研究院（KFRI）、韓国化学研究院（KRICT）等が存在している（図 4.1-36）。

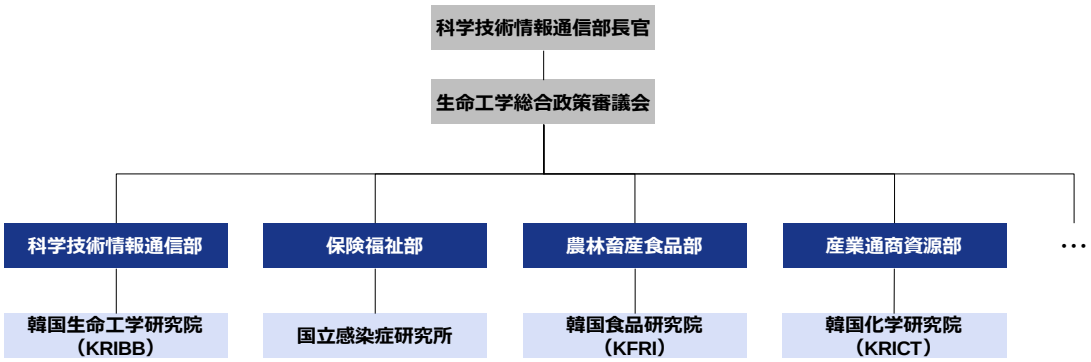


図 4.1-36　韓国のバイオ領域の研究開発に関係する主要機関

■　　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　2022 年度バイオ･医療技術開発事業（社会密着型感染病院泉技術開発）　1 次新規課題

韓国生命工学研究院が所管する研究開発プログラムであり、関係する海外機関との連携を通じた感染病対応国際共同研究を遂行するために、「コロナ 19 対応韓米研究協力及び共同研究推進のための基盤構築」に参加を募るもの。実施期間は 2022.3 月上旬～2022.12.31 であり、選定された機関には最大 2 億ウォンの資金提供が実施される。

研究開発プログラムが準拠する法令等としては、参加機関の資格として国家研究開発革新法や基礎研究振興及び技術開発支援に関する法律を参照しているほか、公告で定めない事項は以下の法令等や施行計画等を参照するように求めている[375]。

（2022 年度バイオ･医療技術開発事業（社会密着型感染病院泉技術開発）　1 次新規課題の公募要領で準拠を求める法令等）

- **科学技術基本法**
- **基礎研究振興及び技術開発支援に関する法律**
- **国家研究開発革新法**
- **国家研究開発革新法施行令**
- **国家研究開発事業研究開発費使用基準**
- **科学技術情報通信部所管の科学技術分野研究開発事業処理規定**
- **科学技術情報通信部研究開発事業総合施行計画**
- **2022 年度バイオ・医療技術開発事業施行計画**

d）サイバー領域

■　　国家戦略等

韓国では、国全体の科学技術政策の基本的な方針にあたる科学技術基本計画を、科学技

[375] https://www.kribb.re.kr/kor/sub03/sub03_01_03_view.jsp?b_idx=27887

術情報通信部が中心となって関係省庁との総合的な調整を行いつつ作成しているが、2022年12月に公表された現在の第5次科学技術基本計画では、今後5年間の重点育成分野として、「12大国家戦略技術」を提示し、任務中心研究開発（R&D）革新体系を導入し、官民の努力を結集するとしている。その中では半導体・ディスプレイ、サイバーセキュリティ、人工知能、次世代通信といったサイバー領域の技術についても提示されている[376]。

その他、2022年2月には「情報保護産業の戦略的育成策」を発表した。人工知能（AI）セキュリティや、非対面セキュリティ、融合セキュリティなど新しいセキュリティ市場の製品や技術の開発を通じ、情報保護産業の次世代戦略を推進することを打ち出した[377]。

2023年には科学技術情報通信部は、韓国初の量子科学技術についての国家戦略として「量子科学技術基本戦略」を発表し、「量子専門研究者」を現在384名から2035年までに2,500名に増加させることや、国防・安全保障への量子技術の導入を図り、暗号体系の崩壊に備えて、次世代暗号（量子耐性暗号）への転換計画を策定する等の7大方針を打ち出し、2035年までに韓国が量子技術分野で世界を主導することを目指すとされた[378]。

■　研究開発機関

韓国では、サイバー領域や情報通信技術に関する研究開発を主に所管しているのは、サイバー領域のみならず国の科学技術・イノベーション政策を所管している科学技術情報通信部である。主要な研究機関として、科学技術情報通信部の下に政府出資研究機関の韓国電子通信研究院（ETRI）があり、通信技術、情報技術、サイバーセキュリティを含む国のICT研究開発を統括している。

その他、国防部の下国防科学研究所についても軍事・安全保障の観点から指揮統制・情報戦技術に関する研究開発を実施しているほか、情報機関である国家情報院はサイバーセキュリティ関連情報の収集・作成・配布およびサイバー攻撃・脅威に対する予防・対応業務を実施している（図 4.1-37）。

376 https://www.medric.or.kr/Controls/Sub.aspx?d=06&s=01&g=NOTICE&m=VIEW&i=1669#:~:text=%EC%A0%9C5%EC%B0%A8%20%EA%B8%B0%EB%B3%B8%EA%B3%84%ED%9A%8D%EC%9D%80%20%EA%B3%BC%ED%95%99%EA%B8%B0%EC%88%A0%EA%B8%B0%EB%B3%B8%EB%B2%95%20%EC%A0%9C,%EC%99%80%20%ED%95%A8%EA%BB%98%20%EC%9D%B4%ED%96%89%ED%95%98%EA%B2%8C%20%EB%90%9C%EB%8B%A4.

377 https://www.jetro.go.jp/biznews/2022/02/36b64a99db32c664.html

378 https://crds.jst.go.jp/dw/20230807/2023080736241/

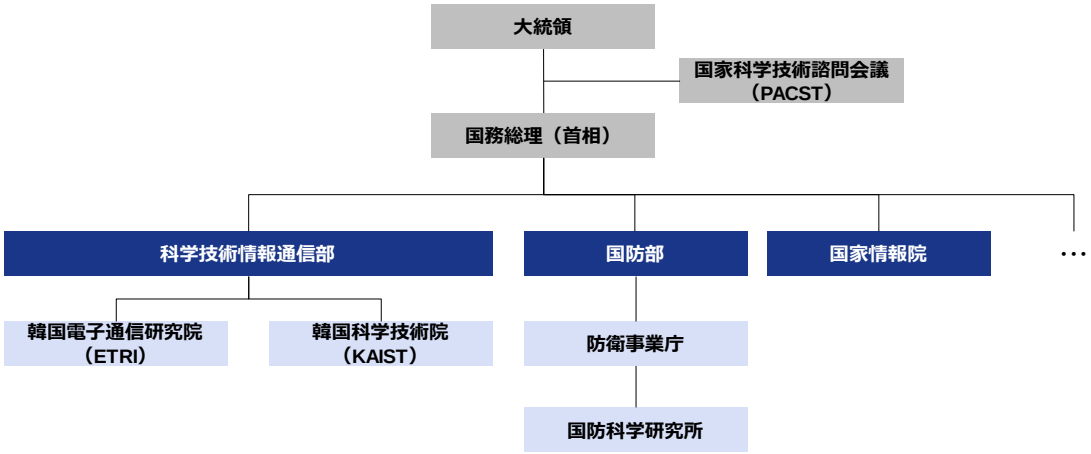


図 4.1-37　韓国のサイバー領域の研究開発に関係する主要機関

■　　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　2022 年 量子暗号通信デモインフラ構築・運営公募

科学技術情報通信部が、その傘下の専門機関である韓国知能情報社会振興院から公募・企画・審査等の支援をうけつつ実施する研究開発プログラムである[379]。

セキュリティ性の強化及び個人情報・産業機密の保護が必要な公共・民間の需要ある機関に量子暗号通信などの実証インフラ構築・運営を行うための提案を公募している。

プログラムに参加する研究開発実施主体には、以下のような事業管理に関する諸規則とその中で参照される法令等に準拠することが公募要領に記載されている[380]。

（2022 年 量子暗号通信デモインフラ構築・運営公募で準拠を求める法令等）
- （科学技術情報通信部）放送通信発展基金の運用・管理規定
  - 基金事業協約締結及び事業費管理などに関する指針
  - ICT 予算政策協議体の運営などに関する指針
  - 基金事業費の算定及び精算などに関する指針
  - 基金事業結果評価などに関する指針
  - 基金事業の成果管理及び活用などに関する指針
  - 基金事業の遂行状況及び精算報告などに関する指針
  - 基金事業点検計画などに関する指針
- （韓国知能情報社会振興院）ICT 基金事業及び研究開発事業の管理指針
  - 事業管理基本運営規則
  - -参加機関選定評価詳細運営指針

e）多義的技術

■　　国家戦略等

韓国では、デュアルユース技術の研究開発を行う政府主導の取り組みとして、1994 年に

379 https://www.msit.go.kr/bbs/view.do?sCode=user&mId=129&mPid=128&pageIndex=&bbsSeqNo=100&nttSeqNo=3177805

380 https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=78336&bcIdx=24404&parentSeq=24404

民・軍兼用技術活性化案が大統領報告され、1999 年に民・軍兼用技術事業促進法が成立、第 1 次基本計画が樹立した。そして 2014 年にそれまでのデュアルユース技術開発関係機関を統合し、民軍協力振興院を新設した。そして 2014 年に法改正により民・軍技術協力促進法が成立、参加省庁と事業のタイプが拡大し現在の民・軍技術協力事業に至っている [381]。

民・軍技術協力事業促進法では、非軍事部門と軍の技術協力の強化・研究開発の推進等を目的として民・軍技術開発事業、民・軍技術移転事業、民軍規格標準化事業、民軍技術情報交流事業といった政府事業の推進が規定されており、このうち狭義のデュアルユース技術の研究開発を行うものとしては、「民軍技術開発事業」の中でも民と軍で共通に活用できる素材、部品、工程およびソフトウェアなどの技術開発事業を行う「民軍兼用技術開発事業」が該当する [382]。

■　研究開発機関

多義的技術に関連する研究開発機関としては前記の民・軍技術協力事業の推進体制について記載する。

民・軍技術協力事業では、産業通商資源部がイニシアティブをとる形で民・軍技術開発事業基本計画が策定されており、それに基づいて関係中央行政機関が必要に応じ専門機関（関係中央行政機関の長から民・軍技術協力事業に対する予算及び事業管理を委託されて遂行する機関）を介する形で、国立研究機関、民間企業、大学等の研究機関と契約を結び研究を委託する体制となっている（図 4. 1-38）。

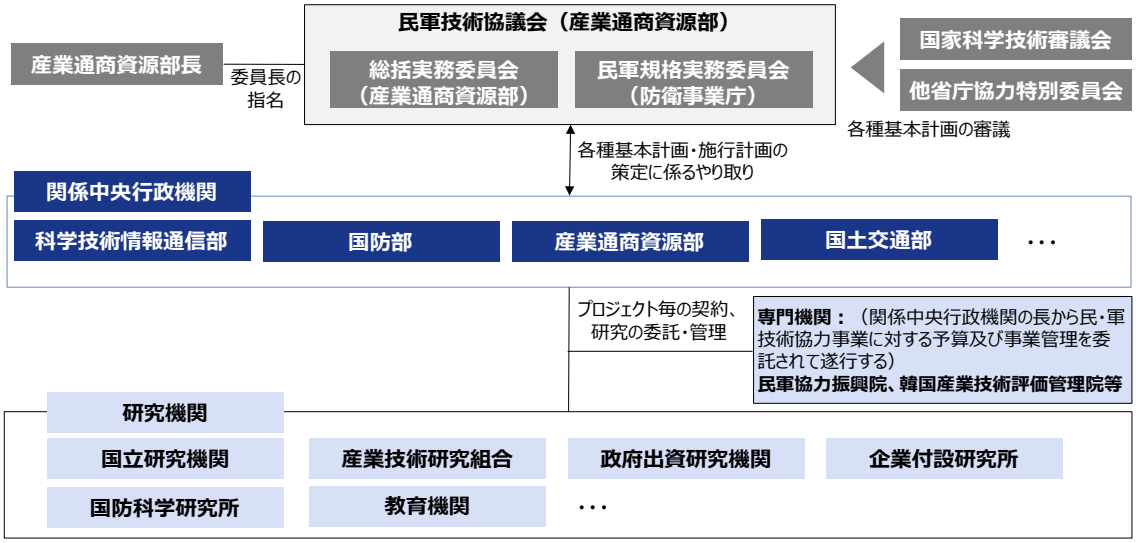


図 4. 1-38　民・軍技術協力事業の関係機関

381 https://www.icmtc.re.kr/board?menuId=MENU00308&siteId=null

382 https://www.law.go.kr/lsInfoP.do?lsiSeq=214211&lsId=000759&chrClsCd=010202&urlMode=lsInfoP&viewCls=lsInfoP&efYd=20200812&vSct=%EB%AF%BC%C2%B7%EA%B5%B0%EA%B2%B8%EC%9A%A9%EA%B8%B0%EC%88%A0%EC%82%AC%EC%97%85%EC%B4%89%EC%A7%84%EB%B2%95&ancYnChk=0#0000

■　主な研究開発プログラムにおいて遵守が求められる法令・ガイドライン

・　2023 年着手民軍技術協力事業主管研究機関選定公募[383]

民軍技術協力事業の専門機関である民軍協力振興院（ICMTC）が、民軍兼用技術開発事業の 2023 年度着手対象課題に対する主管研究開発機関選定を行うもの。「バッテリパックセル単位の EIS 推定のための BMS 搭載型 AI SoC およびバッテリ診断技術の研究」「完全半導体固定式光位相配列 LiDAR 3D イメージセンサモジュールの開発」の 2 課題について公募している。

研究開発プログラムで準拠している法令等については、申請資格について民・軍技術協力事業促進法や高等教育法を参照しているほか、以下の法令等を適用する旨述べられている。

（2023 年着手民軍技術協力事業主管研究機関選定公募で準拠を求める法令等）
・　国家研究開発革新法、同法施行令及び同法施行規則
・　科学技術基本法及び同法施行令
・　民・軍技術協力事業促進法及び同法施行令
・　民・軍技術協力事業共同施行規定
・　産業技術革新促進法および同法施行令

383 https://www.icmtc.re.kr/board/view?pageNum=1&rowCnt=10&menuId=MENU00333&schType=0&schText=&categoryId=&continent=&country=&boardStyle=&linkId=952

4）法令・ガイドライン等の詳細調査

マクロ調査の結果を基に調査対象国の秘密情報の取扱いに係る法令等をロングリストとして 41 件リストアップした（詳細は Appendix 1）参照)。

そしてリストアップした法令等のうち、整理可能な情報量の多寡、研究開発に対する影響の大きさ、及び国家機密情報の保護に関するもの、安全保障貿易に関するもの、少なくとも 1 つずつ選定することを考慮して詳細調査を行う法令等をショートリストとして 6 件抽出した（表 4.1-25）

表 4.1-25　詳細調査を行う法令等のショートリスト

法令等の名称	理由
保安業務規定	韓国における安全保障上機密として保護すべき情報の取り扱いについて規定している法律であり、機微情報を取り扱う研究開発の前提となる可能性のあるため
軍事機密保護法	同上
対外貿易法（戦略物資輸出入告示）	輸出管理の根拠となる法律であり、研究開発における機微情報・技術の取扱いに関係する可能性のあるため
外国人投資促進法	外国投資規制の根拠となる法律であり、研究開発における機微情報・技術の取扱いに関係する可能性のあるため
産業技術の流出防止および保護に関する法律	韓国において国益上保護すべき重要技術の保全を図る法律であり、研究開発における情報保全に関係する可能性のあるため
国家先端戦略産業競争力強化および保護に関する特別措置法	同上

以下に表 4.1-25 に掲載した法令等における秘密情報の取り扱い規程についての詳細調査結果を示す。

a）保安業務規程 [384]

■　策定機関・策定時期

1964 年

■　策定の背景・目的

韓国では、政府の情報機関である国家情報院が国家機密（秘密）に関係するセキュリティ業務を実施している。

[384] https://www.law.go.kr/법령/보안업무규정

国家情報院の設置根拠法である国家情報院法には、秘密について「国家の安全に対する重大な不利益を避けるために、限られた人員のみが知ることが許され、他の国家又は集団に対して秘密にする事実・物件又は知識として国家機密に分類された事項」として定義されており、本規程はその秘密に属する文書・資材・施設を管理する関係機関や秘密を扱う人員が遵守すべき事項を規定するものである。

■　適用範囲

本規程では、主として政府機関の職員を対象とした秘密の取り扱いについて記載されている。第8条（秘密・暗号資材の取扱い）には「秘密は、当該等級の秘密取扱認可を受けた者のみ取り扱うことができる」と記載されていることから、民間人についても対象となるかは明確には確認できない。

しかし、第46条（固有識別情報の処理）には、秘密を取り扱うための身元調査に関する事務を遂行する際に避けられない場合、「住民登録番号又は外国人登録番号を含む資料を処理することができる」と記載されており、国防部が行う一部の研究開発プログラムの公募要領では参加者に本規程第46条を根拠にした身元調査を要求する例も見られることから、民間人も一部秘密の取り扱いの対象となることが考えられる。

■　情報の分類

本規程で取り扱いや保護を規定しているのは、秘密、暗号資材、国家保安施設及び国家保護装備である。

秘密とは「国家の安全に対する重大な不利益を避けるために、限られた人員のみが知ることが許され、他の国家又は集団に対して秘密にする事実・物件又は知識として、本規程で国家機密に分類された事項」であり、その重要性からⅠ級秘密、Ⅱ級秘密、Ⅲ級秘密の等級に区分される（表 4.1-26）。

表 4.1-26　秘密の機密性レベルの定義

根拠	情報分類	定義
保安業務規定	Ⅰ級秘密	漏洩する場合、大韓民国と外交関係が断絶され、戦争を起こし、国家の防衛計画・情報活動及び国家防衛に必ず必要な科学と技術の開発を危うくするなどの懸念がある秘密
	Ⅱ級秘密	漏洩する場合、国家安全保障に莫大な支障を及ぼす恐れのある秘密
	Ⅲ級秘密	漏洩する場合、国家安全保障に害を及ぼす恐れのある秘密

暗号資材とは「秘密の保護及び情報通信セキュリティのために暗号技術が適用された装置又は手段であって、I 級、II 級及び III 級秘密通信用暗号資材に区分される装置又は手段」と定義されており、秘密を扱うための暗号を含む情報端末等を指すと考えられる。

国家保安施設及び国家保護装備とは、「破壊又は機能が侵害されたり秘密が漏洩した場合、戦略的・軍事的に莫大な損害が発生したり、国家安全保障に連鎖的混乱を起こすおそ

れがある施設及び航空機・船舶など重要装備」と定義されている。

■　情報管理策

・　組織的管理策

前記の定義によって情報を分類する際、秘密の過度又は過小な分類、他の秘密との関連性からの等級分類は禁止されている。また、外国政府や国際機関から受領した秘密は、その秘密を作成した機関が必要とする程度に保護できる等級に分類するとしている。

秘密や暗号資材となった情報・資材については、「秘密は、当該等級の秘密取扱認可を受けた者のみ取り扱うことができ、暗号資材は、当該等級の秘密疎通用暗号資材取扱認可を受けた者のみ取り扱うことができる」とされている。

そして各級機関の長は、秘密の作成・分類・受付・発送及び取扱い等に必要なすべての管理事項を記録するために秘密管理記録簿を整備しなければならない。Ⅰ級秘密管理記録簿のみは別に作成して整備しておく必要があり、暗号資材は暗号資材管理記録部で管理することとなっている。

秘密及び暗号資材は原則として複製することはできないが、Ⅰ級秘密はその生産者の許可を受けた場合、Ⅱ級秘密及びⅢ級秘密はその作成者が特定の制限をせず、当該等級の秘密取扱認可を受けた者が共用で使用する場合に複製することができる。また、電子的方法秘密を管理する場合、当該秘密を保管するために複製することが許される。

上記のように分類・管理された秘密は、当該等級の秘密取扱認可を受けた者のうち、その秘密と業務上直接関係のある者のみ閲覧することができる。秘密取扱認可を受けていない者に秘密を閲覧又は取り扱わせるときは、国家情報院長が定めるところにより所属機関の長（秘密が軍事に関する事項である場合には国防部長官）があらかじめ閲覧者の人的事項と閲覧しようとする秘密の内容等を確認し、閲覧時に秘密保護に必要な自己セキュリティ対策を設けるなどのセキュリティ措置をしなければならない。

取り扱いが適切に行われているかを確認するため、中央行政機関等の長は、本規程で定めた人員・文書・資材・施設・地域及び装備等の保安管理状態及びその適正可否を調査するために保安監査をすることとなっている。

・　人的管理策

国家情報院長は、国家機密を扱う人員の忠誠心・信頼性等を確認するために身元調査をすることができると第 36 条で定められている。関係機関の長は国家機密を扱う職位に任用される予定の公務員任用予定者や、秘密取扱認可予定者等の身元調査を国家情報院長に要請しなければならないとされており、身元調査の結果、国家安全保障に害を及ぼす情報があることが確認された者については、関係機関の長にその事実を通知され必要なセキュリティ対策が実施されることになっている。

・　物理的管理策

以下のような物理的対策が規定されている。

（保安業務規程における物理的管理策）
・　秘密は、その取扱者又は管理者に警告し、秘密取扱認可を受けていない者の接近を

防止するために分類（再分類を含む）と同時に等級によって区分された表示をしなければならない。
- 秘密は、盗難・流出・火災又は破壊から保護し、秘密取扱認可を受けない人の接近を防止できる適切な施設に保管しなければならない。
- 国家安全保障に係る人員・文書・資材・施設の保護のために必要な場所に一定の範囲の保護地域を設定することができる。保護地域は、その重要度に応じて制限地域、制限区域及び統制区域に分ける。保護地域に接近し又は出入しようとする者は、各級機関の長又は管理機関等の長の承認を受けなければならない
- 秘密を携帯して出張中の者は、秘密を安全に保護するために国内警察機関又は在外公館に保管を委託することができ、委託された機関はその秘密を保管しなければならない。
- 秘密は保管している施設外に搬出してはならない。ただし、公務上の搬出が必要なときは、所属機関の長の承認を受けなければならない。
- 関係機関の長は、緊急時に備えて秘密を安全に搬出又は破棄できる計画を樹立し、所属職員に周知させなければならない。
- 秘密は、一般文書保管所に移管してはならない。ただし、「公共記録物管理に関する法律」第 33 条第 2 項及び同法施行令第 68 条により記録物管理機関に移管する場合には、この限りでない。

・ 技術的管理策

詳細な技術的管理策は示されていないが、秘密は暗号化されていない状態で情報通信手段を利用して受領・発送してはならないとされている。

また、電子的方法を用いて秘密を管理する管理する場合は、国家情報院長が安全性を確認した暗号資材を使用して、秘密の偽造・変造・毀損及び流出等を防止するためのセキュリティ対策を設けて施行しなければならない。

■ 罰則

本規程自体には罰則は規定されていないが、国家機密の漏洩には刑法 98 条で罰則が規定されている。

（保安業務規程における罰則）
刑法 98 条：
・敵国のためにスパイをするもしくは敵国のスパイを幇助した者は、死刑、無期又は 7 年以上の懲役に処する。
・軍事上の機密を敵国に漏らした者も前項の刑と同じとする。

b）軍事機密保護法 [385]

■ 策定機関・策定時期

1972 年

[385] https://www.law.go.kr/법령/군사기밀보호법시행령

■　策定の背景・目的

軍事機密を保護し、国家安全保障に資することを目的としてその指定、解除、保護措置等に係る事項を定めた法律であり、詳細は軍事機密保護法施行令によって定められる。

■　適用範囲

主として軍事機密に関係する国防部関係者を対象としているが、保安業務規定に規定される秘密取扱認可権者も軍事機密指定権者となっているため、国防部関係者以外の政府職員を含む可能性がある。

また、法第 8 条、9 条には「技術開発、学問研究等を目的に研究機関等が要請するとき大統領令で定めるところにより軍事機密を提供又は説明することができる」「すべての国民は、軍事機密の公開を国防部長官又は防衛事業庁長に文書として要請することができる」と規定されているため、民間人も軍事機密の取り扱い対象になると考えられる。

■　情報の分類

本法で保護する軍事機密とは、一般人に知られていないもので、その内容が漏洩すると国家安全保障に明らかな危険を招く恐れのある軍関連文書、図画、電子記録など特殊媒体記録または物品として軍事機密という意味が表示または告知されたり、保護に必要な措置がなされたものとその内容をいう。軍事機密は、その内容が漏洩する場合、国家安全保障に及ぼす影響の程度に応じてⅠ級秘密、II 級秘密、III 級秘密で等級を区分している（表 4.1-27）。

表 4.1-27　韓国における軍事機密の機密性レベルの定義

根拠	情報分類	定義
軍事機密保護法施行令	軍事Ⅰ級秘密	軍事機密中で漏洩した場合、国家安全保障に致命的な危険を及ぼすと明らかに認められる価値を持つもの
	軍事Ⅱ級秘密	軍事機密中で漏洩した場合、国家安全保障に著しい危険を及ぼすと明らかに認められる価値を持つもの
	軍事Ⅲ級秘密	軍事機密中で漏洩した場合、国家安全保障に相当な危険を及ぼすと明らかに認められる価値を有するもの

■　情報管理策

情報管理策としては施行令 5 条に以下の組織的・人的・物理的管理策が規定されており、その他の事項については施行令第 10 条で「軍事機密保護に関してこの令で規定した事項を除いては、保安業務規定で定めるところによる」とされている。

・　組織的管理策

軍事機密は①法律により軍事機密の提出又は説明を求められたとき、②軍事外交上必要なとき、③軍事に関する条約又はその他の国際協定により、外国又は国際機関の要請を受

けたとき、④技術開発、学問研究等を目的に研究機関等が要請するとき　の 4 類型で提供又は説明することができるとされている。その際、以下の方法に従わなければならない。

（軍事機密保護法における軍事機密の提出・説明の際の遵守事項）
1. 秘密保護誓約などセキュリティ措置を設けること
2. 軍事機密を提供又は説明する前に、次の各首の事項を告知すること
- 軍事機密の機密等級
- 軍事機密に対する録音・メモ・撮影・抜粋及びコピー等の禁止
- 第三者に対する軍事機密の提供または説明の禁止
- 軍事機密を第三者に漏洩する場合、法 第 12 条から第 15 条まで及び第 18 条により処罰されるという事実
- 提供された軍事機密に対する盗難・紛失・火災又は破壊等からの保護義務

3. 軍事機密を説明する場合、第三者の出入制限等のセキュリティ措置がなされた場所で行うこと

また、軍事機密を扱う部隊の長は、現職者及び退職者が軍事機密を漏洩しないように、現職又は退職前にセキュリティチェック及びセキュリティ教育の実施、情報体系アカウントの削除、秘密引き継ぎ・引継ぎ実態確認、秘密保護誓約の執行を実施しなければならない。

・　人的管理策

軍事機密は、該当等級の秘密取扱認可を受けた者であり、業務上関連のある者にのみ扱わせることができる。

・　物理的管理策

軍事機密として指定されたものに対しては、軍事機密であるという旨を表示又は告知しなければならない。また軍事機密は盗難・紛失・火災又は破壊等から保護され、その生産過程と伝播経路を確認できるように対策を設けることが規定されている。

その他、軍事機密を管理又は取扱う部隊又は機関の長は、軍事機密の保護のために「軍事保護区域」を設定することができる。軍事保護区域は、軍事機密の表示又は告知が不可能又は不適切な軍事機密に対して接近を防止し、又は機密のある所を隠蔽するために一定の範囲を定めて設定しなければならない。軍事保護区域の区分、設定対象は表 4.1-28 の通り。その他表示の具体的な表記方法についても施行令別表で定めている。

表 4.1-28　軍事保護区域の区分・設定対象

区分	軍事制限区域：軍事機密及び軍事機密資材への非認可者の接近を防止するための出入りの制限及び案内が要求される区域 軍事統制区域：軍事保安上重要な軍事機密が保管されており、非認可者の出入りが禁止される区域
設定対象	・機密合同保管所または機密資料保管所 ・暗号処理室 ・秘密状況室

	・情報工作室 ・軍事機密装備の保管及び整備室

また、軍事保護区域には、以下の保護措置を行うことが示されている。

（軍事保護区域で実施すべき保護措置）
- 軍事機密保護のための警備
- 入退許可者の管理設定と非認可入退室の制御
- 保管容器または保管施設のロック装置の設置

■ 罰則

本法では、主に軍事機密の保護措置の不履行、損壊・隠蔽、検知・収集、漏洩、届出・提出の不履行、軍事保護区域に侵入することには以下のような罰則が規定されている。また、本法とは別に刑法 98 条で軍事上の機密を漏洩した者には、死刑、無期又は 7 年以上の懲役に処すると定められている。

（軍事機密保護法における罰則）

・ 軍事機密保護措置の不履行等

①軍事機密を取り扱う者が正当な事由なく表示、告知やその他軍事機密保護に必要な措置をしない場合には、2 年以下の懲役に処する。

②軍事機密を扱う者が正当な事由なく軍事機密を損壊・隠匿したりその他の方法でその効用を害した場合には、1 年以上の有期懲役に処する。

（探知・収集）

軍事機密を適法な手続によらない方法で検知し、又は収集した者は、10 年以下の懲役に処する。

・ 非認可者の軍事機密占有

業務上軍事機密を取り扱った者がその取扱認可が解除された後も軍事機密を占有している場合には、2 年以下の懲役又は 2 千万ウォン以下の罰金に処する。

・ 漏洩

①軍事機密を検知し、又は収集した者がこれを他人に漏洩した場合には、1 年以上の有期懲役に処する。

②偶然に軍事機密を知った、もしくは占有した者が軍事機密であることを知りながらもこれを他人に漏洩した場合には、5 年以下の懲役又は 5 千万ウォン以下の罰金に処する。

（業務上軍事機密漏洩）

①業務上軍事機密を取り扱う者又は取り扱った者がその業務上知った、もしくは占有した軍事機密を他人に漏洩した場合には、3 年以上の有期懲役に処する。

②第 1 項の規定による者以外の者が業務上知った、もしくは占有した軍事機密を他人に漏洩した場合には、7 年以下の懲役に処する。

・ 申告・提出・削除の不履行

①軍事機密を保管する者がこれを紛失又は盗難された場合に遅滞なくその事実を所属機関又は監督機関の長に申告しなかった場合には、3 年以下の懲役または 3 千万ウォン以下の罰金に処する。
②軍事機密を取得する、もしくは他人から提供を受けて占有した者が捜査機関又は軍部隊から提出要求を受けて直ちにこれを提出しなかった場合、2 年以下の懲役又は 2 千万ウォン以下の罰金に処する。
③押収の目的物である軍事機密が「刑事訴訟法」 第 106 条第 3 項又は同法 第 219 条により出力又は複製の方法で提出された場合、その占有者が検査(軍検査を含む)又はその指揮を受け取った司法警察官（軍事法警察官を含む）からコンピュータ用ディスク、その他これと同様の情報保存媒体に残っている軍事機密の削除要求を受けて直ちにこれを削除しなかったときは、2 年以下の懲役または 2 千万ウォン以下の罰金に処される。

・　軍事保護区域侵入等
①軍事保護区域を侵入した者は、2 年以下の懲役又は 2 千万ウォン以下の罰金に処する。
②軍事保護区域を侵入して軍事機密を盗んだ者又は軍事機密を損壊・隠匿したり、その他の方法でその効用を害した者は、1 年以上の有期懲役に処する。

c）対外貿易法

■　策定機関・策定時期

1987 年

■　策定の背景・目的

対外貿易法は韓国における輸出入取引、原産地の表示、輸入数量制限措置、輸出入の秩序維持などを扱っている法律であり、輸出入の管理制度としては 1987 年の「戦略物資輸出入告示」の導入以後、ミサイル関連資機材・技術輸出規制（MTCR）、オーストラリア・グループ（AG）、ワッセナー・アレンジメント（WA）、化学兵器禁止条約（CWC）など国際的な輸出規制レジームに加盟して武器や軍事転用可能な貨物や技術の輸出について規制を図ってきた。

本項においては主として研究開発・情報保全に関係する安全保障貿易管理関連の条項について記載する。

■　適用範囲

本法で輸出規制の対象となるのは、「国際的レジームに則って国際平和及び安全維持と国家安全のために輸出許可等の制限が必要な物品等（技術を含む)」であり、対象については「戦略物資輸出入告示」で示される品目のほか、「大量破壊兵器等の製造・開発・使用又は保管等の用途に転用される可能性が高い物品等」が、輸入者又は最終使用者がその物品等を大量破壊兵器等の製造・開発・使用又は保管等の用途に転用する可能性が高い場合等に輸出規制の対象となる。

輸出については「売買、交換、賃貸借、使用貸借、贈与などによって韓国国内から外国に物品が移動すること」を指し、居住者が非居住者に情報通信網を通じた伝送によってデータを伝送することや、サービス・役務の提供についても対象となる。

■　　情報の分類

記載なし

■　　情報管理策

・　組織的管理策

前記の戦略物資及び大量破壊兵器等の製造に転用される可能性の高い物品等を輸出するときは、産業通商資源部長官や関係行政機関の長の許可を得なければならない。本許可については「状況許可」と呼称されており、技術全般は産業通商資源部貿易安全保障課、原子力プラント関連は原子力安全委員会原子力統制課、軍用物資は防衛事業庁輸出協力課といったように輸出を承認し状況許可を発出する関係行政機関が指定されている。

・　人的管理策

輸出管理の対象となる居住者と非居住者については本法とは別に外国為替取引法第 3 条によって規定されている。居住者は「大韓民国に住所または居所を置いた個人と大韓民国に主な事務所を置いた法人」であり、非居住者は「居住者以外の個人および法人をいう。ただし、非居住者の大韓民国にある支店、出張所、その他の事務所は、法律上代理権の有無にかかわらず、居住者とみなす。」と規定されている。

■　　罰則

戦略物資等の拡散を図る目的で、輸出許可を受けず戦略物資を輸出する等の違反行為をした者は、7 年以下の懲役又は輸出・経由・為替・仲介する物品等の価格の 5 倍に該当する金額以下の罰金に処される等規制への違反行為に罰則が規定されている。未遂、過失による違反にも罰則が適用される。

d）外国人投資促進法 [386]

■　　策定機関・策定時期

1998 年

■　　策定の背景・目的

外国人投資促進法は、韓国における外国人投資を支援し、外国人投資に便宜を提供して外国人投資の誘致を促進することによって、韓国経済の発展に資することを目的として制定された法律である。

その目的上、法律に特別な定めのない限り外国人投資家に韓国人と同様の待遇を適用することや租税の減免、地方自治団体の外国人投資誘致活動に対する支援など、外国人投資に対する保護措置を規定しているが、国家の安全および公共秩序の維持に支障をもたらす場合など特定の条件における外国人投資に対する制限を規定している。

本項では、研究開発や情報保全に関係する、外国人投資に対する制限に関する規程について主に記載する。

386 https://www.law.go.kr/법령/외국인투자촉진법

■　適用範囲

本法の対象となる外国人投資について、外国人、外国人投資家、外国人投資について定義が定められている。

外国人とは「外国の国籍を持っている個人、外国の法律により設立された法人（以下「外国法人」という。）及び大統領令で定める国際経済協力機構（国際復興開発銀行・国際金融公社・アジア開発銀行など)」を指し、外国人投資家とは「本法により株式等を所有しているか出資をした外国人」を指す。

外国人投資については、以下の 5 類型が定められている。

（外国人投資促進法における外国人投資の類型）

1. 外国人がこの法律に従って大韓民国法人または企業の経営活動に参加するなど、その法人または企業と持続的な経済関係を樹立する目的で大統領令で定めるところにより、法人や企業の株式または持分（株式等）を次のいずれかの方法で所有するもの
   1）大韓民国法人又は企業が新たに発行する株式等を取得すること
   2）大韓民国法人又は企業が既に発行した株式又は持分(既存株式等)を取得すること
2. 次のいずれかに該当する者が当該外国人投資企業に貸付する 5 年以上の借款（最初の貸付契約時に定められた貸付期間を基準とする）
   1）外国人投資企業の海外親企業
   2）1)の企業と大統領令で定める資本出資関係がある企業
   3）外国投資家
   4）3)の投資家と大統領令で定める資本出資関係がある企業
3. 外国人がこの法に基づき科学技術分野の大韓民国法人又は企業として研究人材・施設等について大統領令で定める基準に該当する非営利法人と持続的な協力関係を樹立する目的でその法人に出捐すること
4. 外国人投資企業が未処分利益剰余金をその企業の工場施設の新設又は増設など大統領令で定める用途に使用するもの第 3 項による外国人投資比率を掛けた金額とする）
5. その他、外国人の非営利法人に対する出資として、非営利法人の事業内容等について大統領令で定める基準により、第 27 条による外国人投資委員会が外国人投資として認めるもの

■　情報の分類

記載なし

■　情報管理策

本法第 4 条では、以下のケースに該当する場合を除いて、外国人投資には制限を設けないことを規定しており、それに基づき外国人投資促進法施行令及び施行規則で詳細な制限対象業種等を定めている。

（外国人投資促進法における制限対象となる投資）

1. 国家の安全および公共秩序の維持に支障をもたらす場合
2. 国民の保健衛生または環境保全に影響を及ぼすか、公序良俗に著しく反する場合

3. 韓国の法令に違反する場合

・ 組織的管理策

外国人投資を行う場合、外国人は産業通商資源部令で定めるところにより、あらかじめ産業資源部長に対して申告を行わなければならない。

外国人投資の制限の対象となる業種（産業通商資源部長官が告示する「制限業種」）を営む企業へ投資を行う際、制限業種の売上高比率が 100 分の 1 以下である場合は投資に制限はない。しかし、外国人が当該企業の株式などを取得後、当該企業の総売上高のうち制限業種の売上高比率が 100 分の 1 を超えることになった場合は、その事業年度の決算確定日から 6 カ月以内に当該外国人の投資許容比率を超えて取得した株式などを韓国国民または韓国内の法人に譲渡しなければならない。さらに、外国人は外国人による投資が禁止される業種および部分的に許容される業種をともに営む企業に対しては投資することができず、制限業種を二つ以上営む企業の株式などを取得する場合には、外国人の投資許容比率が一番低い業種の外国人投資比率がその取得限度とされる。

投資が禁止される業種については、中央銀行や郵便業、行政関連などが該当する。制限業種は内航旅客運送業、有線放送業、無線および衛星通信業、国内銀行などの 30 業種が該当している。

また制限業種の他にも、以下に該当する外国人投資が国家安全保障に支障をきたすか否かについて所管省庁の長官や情報機関の長が検討要請を出し、産業通商資源部長官が外国人投資委員会の審議により「国家安全保障に該当する」と決定した場合は制限の対象となる。

（外国人投資促進法における国家安全保障に係る検討を要する外国人投資）

1. 外国人が既に設立された国内企業の株式等の取得を通じて当該企業の経営上支配権を実質的に取得しようとする場合

2. 次のいずれかに該当する場合

1)「防衛事業法」第３条第７号による防衛産業物資（以下「防衛産業物資」という）の生産に支障をきたすおそれがある場合

2)「対外貿易法」第 19 条による輸出許可又は承認対象物品等や技術として軍事目的で専用（轉用）される可能性が高い場合

3)「国家情報院法」第４条第１項第２号により国家機密（以下「国家機密」という）と扱われる契約等の内容が公開されるおそれがある場合

4) 国際平和及び安全維持のための国際連合等の国際的努力に深刻で重大な支障を招く恐れがある場合

5)「産業技術の流出防止及び保護に関する法律」第 2 条第 2 号による国家核心技術の流出の可能性が高い場合

・ 人的管理策

前記の通り、本法に則り株式等を所有しているか出資をした外国人（外国の国籍を持っている個人、外国の法律により設立された法人）による投資は規制の対象となることが定められている。

■ 罰則

本法に基づく対外送金、外国人投資によって外貨を逃避させた場合、1 年以上の有期懲役又は逃避額の 2 倍以上 10 倍以下に相当する罰金に処することとなっているほか、外国人投資企業の変更登録をしなかった者場合（5 年以下の懲役又は 5 千万ウォン以下の罰金）や、本法による許可又は申告に関連して偽書類を提出した場合（3 年以下の懲役又は 3 千万ウォン以下の罰金）などに罰則が適用される。

e）産業技術の流出防止および保護に関する法律 [387]

■　策定機関・策定時期

2006 年

■　策定の背景・目的

産業技術の流出防止および保護に関する法律（通称：産業技術保護法）は、国家安全保障に直接的な影響を及ぼす「国家核心技術」の海外流出を規制して産業技術の不正な流出を防止するためのセキュリティ意識の醸成や制度的基盤の構築を通じて韓国国内の核心技術を保護し、科学・産業技術者および研究者を保護・支援して国内産業の競争力を強化し、国家の安全と国民経済の安定を保障することを目的として制定された。

■　適用範囲

本法で保護される産業技術とは、製品又はサービスの開発・生産・普及及び使用に必要な諸方法又は技術上の情報のうち、行政機関の長（当該業務が委任又は委託された場合には、その委任又は委託を受けた機関又は法人・団体の長をいう）が産業競争力の向上や流出防止などのために、本法または他の法律や本法または他の法律で委任した命令によって、指定・告示・公告・認証する技術が対象となる。このうち、本法によって示された技術とは「国家核心技術」を指すため、本項では主に国家核心技術の保護に関する内容を記載する。

■　情報の分類

本法では、第 2 条第 3 号で「国内外市場で占める技術的・経済的価値が高いか、関連産業の成長潜在力が高く海外に流出する場合に国家の安全保障及び国民経済の発展に重大な悪影響を与える恐れがある技術として指定されたもの」を「国家核心技術」として定義している。

国家核心技術については、産業通商資源部長官の下に設置される産業通商資源部長官を委員長とした産業技術保護委員会によって、その総合計画、国家核心技術の指定変更及び解除に関する事項、国家核心技術の輸出等に関する事項、国家核心技術を保有する対象機関の海外引受・合併などに関する事項、総合計画の重要内容変更に関する事項を審議するとされている。

国家核心技術は 2023 年現在で半導体（11）、ディスプレイ（2）、電気電子（4）、自動車・鉄道（9）、鉄鋼（9）、造船（8）、原子力（5）、情報通信（7）、バイオテクノロジー（4）、機械（7）、ロボット（3）、水素（2）の計 12 分野 71 技術が指定されている [388]。

387 https://www.law.go.kr/법령/산업기술의유출방지및보호에관한법률

388 https://nct.or.kr/institution/institution01

■　　情報管理策

本法では、国家核心技術の輸出または当該技術保有者の合弁を進めるにあたっての事前承認等の組織的管理策を主に規定しており、物理的・技術的管理策は本法及び施行令、施行規則では規定していない。

・　組織的管理策

国家から研究開発費の支援を受けて開発した国家核心技術を保有した対象機関が該当国家核心技術を輸出しようとする場合には、産業通商資源部長官の承認を得なければならず、その他国家核心技術を保有・管理している対象機関が国家核心技術を輸出しようとする場合には、産業通商資源部長官に事前申告しなければならない。

産業通商資源部長官は、申告対象国家核心技術の輸出が国家安全保障に深刻な影響を及ぼし得ると判断される場合には、関係中央行政機関長との協議及び委員会審議を経て輸出中止・禁止・原状回復などの措置を命じることができるようにし、申告対象国家核心技術を輸出しようとする者は、該当国家核心技術が国家安保に関連するか否かに対して産業通商資源部長官に事前検討を申請することができる。

国家核心技術の海外流出を目的にした外国人投資を前もって防止・遮断することができるように、国家から研究開発費の支援を受けて開発した国家核心技術を保有する対象機関が、海外引受・合併等をしようとする場合、産業通商資源部長官に事前申告することになっている。

・　人的管理策

本法第 34 条で、産業技術を保有した企業・研究機関・専門機関・大学の職員（教授・研究員・学生含む）や、国家核心技術の指定・変更及び解除業務を遂行する者または国家核心技術の保護・管理等に関する支援業務を遂行する者、国家核心技術の輸出及び海外引受・合併等に関する事項を検討したり、事前検討、調査業務を遂行する者、海外引受・合併等を進行しようとする外国人及び外国機関職員等には、職務上知った秘密を漏洩又は盗用してはならない秘密保持義務が規定されている。

■　　罰則

主に産業技術の流出及び侵害行為禁止（本法第 14 条で規定）について、以下のような罰則が規定されている。

（産業技術保護法における罰則）

- **国家核心技術を外国で使用又は使用させる目的で第 14 条第 1 号から第 3 号までのいずれかに該当する行為をした者は、3 年以上の有期懲役に処する。この場合、15 億ウォン以下の罰金を併科する。**
- **産業技術を外国で使用又は使用させる目的で第 14 条各号（第 4 号を除く）のいずれかに該当する行為をした者（第 1 項に該当する行為をした者は除く）は 15 年以下の懲役または 15 億ウォン以下の罰金に処する。**
- **第 14 条各号（第 4 号・第 6 号・第 6 号の 2 及び第 8 号は除く）のいずれかに該当する行**

為をした者は、10 年以下の懲役又は 10 億ウォン以下の罰金に処する。

・ 第 14 条第 4 号及び第 8 号のいずれかに該当する行為をした者は、3 年以下の懲役又は 3 億ウォン以下の罰金に処する。

第 14 条の第 1～7 号において規定される産業技術の流出及び侵害行為禁止の類型は以下の通りである。

（産業技術保護法における産業技術の流出及び侵害行為禁止の類型）

第 14 条（産業技術の流出及び侵害行為禁止）

1. 切取・期待・脅迫その他の不正な方法で対象機関の産業技術を取得する行為又はその取得した産業技術を使用したり、公開（秘密を維持しながら特定人に知らせることを含む。以下同じ）する行為
2. 第 34 条（秘密保持義務）の規定又は対象機関との契約等により産業技術に対する秘密保持義務のある者が不正な利益を得たり、その対象機関に損害が発生することを知りながらも流出したり、その流出した産業技術を使用又は公開または第三者に使用させる行為
3. 第 1 号又は第 2 号の規定に該当する行為が介入された事実を知り、その産業技術を取得・使用及び公開したり、産業技術を取得した後にその産業技術について第 1 号又は第 2 号の規定に該当する行為が介入された事実を知り、その産業技術を使用または公開する行為
4. 第 1 号又は第 2 号の規定に該当する行為が介入された事実を重大な過失で知らず、その産業技術を取得・使用及び公開したり、産業技術を取得した後にその産業技術について第 1 号又は第 2 号の規定に該当する行為が介入された事実を重大な過失として知らず、その産業技術を使用または開示する行為
5. 第 11 条（国家核心技術の輸出等）第 1 項の規定による承認を得ないか又は不正な方法で承認を得て国家核心技術を輸出する行為
6. 国家核心技術を外国で使用し、又は外国で使用されることを知りながらも、第 11 条の 2 第 1 項による承認を受けない、又は偽り又はその他の不正な方法で承認を受けて海外引受・合併等をする行為

6-2. 国家核心技術を外国で使用するか、外国で使用することを知りながらも、第 11 条の 2 第 5 項及び第 6 項による申告をしない、又は偽り又はその他の不正な方法で申告をして海外引受・合併等をする行為

6-3. 第 34 条又は対象機関との契約等により産業技術に対する秘密保持義務のある自己産業技術に対する保有又は使用権限が消滅することにより、対象機関から産業技術に関する文書、圖畫、電子記録など特殊媒体記録の返還や産業技術の削除を要求されても不正な利益を得たり、その対象機関に損害を加える目的でこれを拒否または忌避したり、そのコピーを保有する行為

7. 第 11 条第 5 項・第 7 項及び第 11 条の 2 第 7 項・第 9 項による産業通商資源部長官の命令を履行しない行為
8. 産業技術関連訴訟など大統領令で定める適法な経路を通じて産業技術を含む情報を提供された者が情報を提供された目的以外の他の用途でその情報を使用又は開示する行為

f）国家先端戦略産業競争力強化および保護に関する特別措置法 [389]

■　策定機関・策定時期

2022 年

■　策定の背景・目的

国家先端戦略産業（定義は後述）の革新エコシステムの造成と技術力の強化を通じて産業の持続可能な成長基盤を構築することにより、国家・経済安全保障と国民経済発展に資することを目的として制定された。

■　適用範囲

本法の保護・支援対象となるのは、国家先端戦略技術とそれを研究開発・事業化する国家先端戦略産業である。

それぞれ国家先端戦略技術は「サプライチェーンの安定化など国家・経済安全保障に及ぼす影響および輸出・雇用など国民経済的効果が大きく、関連産業に及ぼす波及効果が顕著な技術であり、法第 11 条で指定された技術」、国家先端戦略産業は「戦略技術を研究・開発または事業化する等、これに必要な製品およびサービスを提供する産業として産業通商資源部長官が告示する産業」として定義されている。

■　情報の分類

前記の通り、「サプライチェーンの安定化など国家・経済安全保障に及ぼす影響および輸出・雇用など国民経済的効果が大きく、関連産業に及ぼす波及効果が顕著な技術であり、法第 11 条で指定された技術」を国家先端戦略技術として定義しているが、その指定や分類については、本法第 11 条で「産業通商資源部長官は、調整委員会の審議及び委員会の審議・議決を経て戦略技術を指定することができる。」とされているのみであり、具体的な区分は示されていない。

国家先端戦略産業技術を指定するにあたっては、以下のような要件を総合的に考慮するとしている。

（国家先端戦略産業技術の指定に係る検討要素）

- **当該技術が産業サプライチェーン及び国家・経済安全保障に及ぼす影響**
- **当該技術の成長潜在力と技術難易度**
- **当該技術が他の産業に及ぼす波及効果**
- **当該技術が持つ産業的重要性**
- **当該技術が輸出・雇用など国民経済に及ぼす影響**
- **その他大統領令で定める事項**

また、第 11 条で「自分が保有している技術が戦略技術に該当するか否かの判定を受けようとする者は、大統領令で定めるところにより産業通商資源部長官に申請することができる。」とされている通り、企業自らが国家先端技術への指定を希望することができるほか、

[389] https://www.law.go.kr/법령/국가첨단전략산업경쟁력강화및보호에관한특별조치법

「国家先端戦略技術を指定・変更又は解除した場合『産業技術の流出防止及び保護に関する法律』第 9 条により国家核心技術を指定・変更又は解除したものとみなす。」されていることから、国家核心技術と国家先端戦略技術は重複する可能性があると思われる。

■　情報管理策

本法では、主に国家先端戦略技術の輸出や国家先端戦略技術保有者の海外引受・合併等に係る規制といった組織的・人的管理策に加え、一部物理的な管理策についても規定している。

・　組織的管理策

国家先端戦略技術保有者が当該技術を外国企業等に売却又は移転等の方法で輸出する場合には、産業通商資源部長官の承認を受けなければならない。産業通商資源部長官は、その承認申請について、当該技術の輸出による国家・経済安全保障及び国民経済的波及効果等を検討し、関係中央行政機関の長と協議した後、「産業技術の流出防止及び保護に関する法律」第 7 条に規定される産業技術保護委員会の審議を経て承認することができる。

もし承認を受けていないか否定した方法で承認を受けて国家先端戦略技術の輸出をした場合、情報捜査機関の長に調査を依頼し、調査結果を産業技術保護委員会に報告した後、産業技術保護委員会の審議を経て当該戦略技術の輸出中止・輸出禁止・原状回復などの措置を命ずることができる。

また、国家先端戦略技術保有者が大統領令で定める海外引受・合併、合弁投資等外国人投資を進行しようとする場合についても輸出と同様の承認が必要となる。

・　人的管理策

国家先端戦略技術保有者は、技術を取り扱う人材（専門人材）の離職管理及び秘密保持等に関する契約締結をしなければならないとされている。

専門人材との契約には、「①海外同種業種への離職制限及びその期間②戦略技術関連の秘密流出防止」を含めることができるほか、以下のいずれかに該当する場合、国家先端戦略技術保有者は産業通商資源部長官に当該専門人材の出入国情報提供を申請することができる。

（国家先端戦略技術保有者が専門人材の出入国情報を提供できる場合）
- **戦略技術専門人材の同意がある場合**
- **戦略技術の海外流出が深刻に懸念される場合**
- **その他に戦略技術の海外流出を防止するために大統領令で定めた場合**

・　物理的管理策

国家先端戦略技術保有者は、国家先端戦略技術の流出を防止するために、「保護区域の設定・出入許可または出入時の携帯品検査」を実施しなければならないことが法第 14 条において規定されている。

■　罰則

「産業技術の流出防止および保護に関する法律」と同様に、国家先端戦略技術の流出及び

侵害行為禁止（本法第 15 条で規定）について、以下のような罰則が規定されている。

（国家先端戦略産業競争力強化および保護に関する特別措置法における罰則）

① 戦略技術を外国で使用又は使用することを目的として、第 15 条第 1 号から第 3 号までのいずれかに該当する行為をした者は、5 年以上の有期懲役に処する。この場合、20 億ウォン以下の罰金を併科する。

② 戦略技術を外国で使用又は使用することを目的として第 15 条第 5 号から第 8 号までのいずれかに該当する行為をした者は、20 年以下の懲役又は 20 億ウォン以下の罰金に処する。

③ 第 15 条各号（第 4 号・第 6 号及び第 8 号は除く）のいずれかに該当する行為をした者は、15 年以下の懲役又は 15 億ウォン以下の罰金に処する。

④ 第 15 条第 4 号又は第 8 号に該当する行為をした者は、5 年以下の懲役又は 5 億ウォン以下の罰金に処する。

⑤ 第 10 条第 5 項各号のいずれかに該当する行為をした者は、1 年以下の懲役又は 1 千万ウォン以下の罰金に処する。

第 15 条に規定される流出及び侵害禁止行為は以下の通り。

（国家先端戦略産業競争力強化および保護に関する特別措置法における侵害禁止行為）

1. 切取・期待・脅迫又はその他の不正な方法で対象機関の戦略技術を取得する行為又はその取得した戦略技術を使用又は開示する行為
2. 第 14 条による戦略技術保有者との契約又は「産業技術の流出防止及び保護に関する法律」第 34 条等により、戦略技術に対する秘密保持義務のある者が不正な利益を得たり、その対象機関に損害を与える目的で戦略技術を流出したり、その流出した戦略技術を使用または公開したり、第三者に使用させる行為
3. 第 1 号又は第 2 号に該当する行為が介入された事実を知り、その戦略技術を取得・使用及び公開したり、戦略技術を取得した後にその戦略技術に対して第 1 号又は第 2 号に該当する行為が介入された事実を知ってその戦略技術を使用または公開する行為
4. 第 1 号又は第 2 号に該当する行為が介入された事実を重大な過失で知らず、その戦略技術を取得・使用及び公開したり、戦略技術を取得した後にその戦略技術について第 1 号又は第 2 号に該当する行為が介入された事実を重大な過失で知らず、その戦略技術を使用または公開する行為
5. 第 12 条第 1 項の規定による承認を受けない又は不正な方法で承認を受けて戦略技術を輸出する行為
6. 戦略技術を外国で使用又は使用させる目的で第 13 条第 1 項の規定による承認を受けない、又は偽り又はその他の不正な方法で承認を受けて海外引受・合併等をする行為
7. 第 14 条による戦略技術保有者との契約又は「産業技術の流出防止及び保護に関する法律」第 34 条等により、戦略技術に対する秘密保持義務のある者が戦略技術に対する保有又は使用権が消滅するにつれ、当該戦略技術保有者から戦略技術に関する文書、圖畫、電子記録など特殊媒体記録の返還や戦略技術の削除を求められても不正な利益を得たり、その保有者に損害を加える目的でこれを行う拒否、回避、またはそのコピーを保持する行為

8. 戦略技術関連訴訟など大統領令で定める適法な経路を通じて戦略技術を含む情報を提供された者が情報を提供された目的以外の用途でその情報を使用または開示する行為

4.1.2 研究開発実施主体、推進会議等事務局における秘密情報等の取扱いに関する実態調査

（1）日本

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計 12 機関、13 件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細は Appendix 2）参照）。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして 6 件抽出した。また、3 章にて記載の通り日本においては中小企業技術革新研究プログラム（SBIR 制度）についても対象とすることとした（表 4.1-29）。

表 4.1-29 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連領域	主催している研究開発プログラム
宇宙航空研究開発機構（JAXA）	宇宙	革新的衛星技術実証プログラム
海洋研究開発機構（JAMSTEC）	海洋	SIP 第 3 期課題「海洋安全保障プラットフォームの構築」
日本医療研究開発機構（AMED）	バイオ	新興・再興感染症に対する革新的医薬品等開発推進研究事業
総務省	サイバー	令和 3 年度　情報通信技術の研究開発に係る提案の公募：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発
防衛装備庁	多義的技術	安全保障技術研究推進制度
SBIR 制度	宇宙、海洋、サイバー、バイオ、多義的技術	中小企業技術革新研究プログラム（SBIR 制度）

研究開発実施主体については、表 4.1-29 で絞り込んだ研究開発プログラムに参加している機関（資金配分機関のうち自ら研究開発を実施している機関も含む）をロングリストとして 33 件リストアップした（詳細は Appendix 2）参照）。

1）資金配分機関における情報取扱に係る詳細調査結果

a）宇宙航空研究開発機構（JAXA）

■　研究開発領域

宇宙

■　適用範囲

公開されている JAXA の規程類を確認したところ、JAXA において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[390]。

しかし、機構による情報公開の主な対象となる法人文書について、JAXA の文書管理規程は、「機構の役員又は職員が職務上作成し、又は取得した文書、図画、電磁的記録」を文書として定義し、「文書であって、機構の役職員が組織的に用いるものとして機構が保有しているもの」である法人文書の管理を対象としていることが示されている[391]。

■　情報の分類

公開されている JAXA の規程類からは、機密性・完全性・可用性などの観点から JAXA において取り扱われる情報を分類している規程等は確認できなかった。

しかし、JAXA の組織規程では、事業共通組織におけるセキュリティ・情報化推進部が「セキュリティ管理の統括、情報化に係る計画の企画、立案、調整及び推進、業務系情報システム、共通的な情報システム、スーパーコンピュータシステム、プロジェクト系に共通な情報共有システム及び情報基盤の整備、情報システムセキュリティに係る共通対策、技術情報・図書の蓄積及び利用促進並びに安全保障貿易管理に関する業務」を遂行するとされており、同部署の定める対策に従って情報の取り扱いが成されているものと思料される[392]。

■　情報管理策

公開されている JAXA の規程類からは、JAXA において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった。

しかし、国立研究開発法人宇宙航空研究開発機構法では第 16 条において機構の役員及び職が職務上知ることのできた秘密について、秘密保持義務が規定されており、違反した場合一年以下の懲役又は五十万円以下の罰金が科される[393]。

■　所管する主なプログラムと情報取扱規程

・　革新的衛星技術実証プログラム

【研究領域】宇宙

【概要】4.1.1　(1) 1) c)参照

【参加資格】

390 https://www.jaxa.jp/about/disclosure/regulations_j.html

391 https://www.jaxa.jp/about/disclosure/data/k15_21_18.pdf

392 https://www.jaxa.jp/about/disclosure/data/k15_3_152.pdf

393 https://elaws.e-gov.go.jp/document?lawid=414AC0000000161

革新的衛星技術実証プログラムでは、公募要領、契約書雛形において事業への参加資格が以下の通り規定されている。また、宇宙活動法に基づく人工衛星の管理に係る許可を取得することや、衛星リモセン法に基づくリモートセンシング装置の使用に係る許可の取得、外為法の遵守等が参加にあたって求められている。

（革新的衛星技術実証プログラムの参加資格）
- 日本国法に基づき設立された法人であること
- 財務状況が著しく悪い状況、反社会的勢力ではないこと
- 必要な技術・経済的能力を有すること
- 安全保障貿易管理上の禁輸国・地域の者、JAXA が技術情報を提供できない者ではないこと
- 第三者の知的財産を侵害しないこと
- 競争参加資格がある者、その他不適切な事情が無い者
- 秘密保持契約、技術実証契約を締結可能な者（応募前から締結が必要）

【情報取扱規程】

また、研究開発実施主体に求める情報取り扱いの規程としては、契約で規定される秘密情報の保全を求めている他、JAXA が取扱い条件を明示した情報を取り扱う場合、セキュリティ確保のため以下の措置を講じなければならないとしており、組織的・人的・物理的・技術的な情報管理策が確認できる。

（JAXA が革新的衛星技術実証プログラムで研究開発実施主体に求める情報取扱規程）
- 機構の情報を防護し、機密性、完全性を確保するために、機構の情報にアクセスできる者を本契約の履行に必要な範囲となるよう適切な管理を行うこと。
- 外部からの意図的な不正行為やその他の脅威から機構の情報を守るため、当該情報を扱う作業の実施施設に不正な入退場が行われないよう対策を講ずること。
- 情報システムの破壊、侵入、不正アクセス、コンピュータウイルスその他の脅威から機構の情報を扱う情報システムを防護するための措置を講ずるとともに、当該情報を扱う端末等では情報漏えいの危険性のあるソフトウェアの使用を禁ずること。
- 機構の情報を漏えい、破壊、改ざん、滅失又は毀損等（以下「漏えい等」という。）の事故が生じた場合には、直ちに機構に対しこれを報告し、適切な措置を講じること。
- 前号に定める措置を講じたときは、速やかに機構に対し漏えい等の範囲、拡大防止策、原因究明及び対策等の措置内容を報告すること。
- 前各号までの措置を周知徹底すること。
- ユーザ（研究開発実施主体）は、機構の情報を関係者に取扱わせる場合、前各号に定める措置を関係者にも遵守させること。ただし、第４号及び第５号の機構への報告については、ユーザから行うこと

成果の取り扱いについては、事業者に対しては「提案者が得た成果（プロジェクトの全過程で実施した発明等に係る知的財産権、取得した情報等一切の成果を言い、機構に帰属する知的財産権及び提案者との共有の知的財産権を除く。）に関する権利は提案者に帰属する」とされ、それに対し JAXA は研究開発目的で、提案者が得た成果を無償で自由に利用す

る（機構の研究開発目的で自己以外の者をして利用させる場合も含む。）ことができるものとし、提案者は予めこれに同意しなければならない[394]。

b）海洋研究開発機構（JAMSTEC）

■　研究開発領域

海洋

■　適用範囲

JAMSTEC では、機構内で取り扱われるデータやサンプルの取り扱いについていくつかの規程を纏めた「JAMSTEC データ・サンプル関連諸規程」で定めている[395]。

規程の中では、調査・研究等もしくは調査・研究を行う過程において、またはその成果として得られる以下に掲げるものを「研究成果物等」として「研究成果物等取扱規程」の対象としている（表 4.1-30）。その中でも、研究試料有体物のうちサンプル及びデータは、別に「サンプル取扱規則」「データ取扱規則」で詳細な定義が定められている。

表 4.1-30　JAMSTEC における研究成果物等の定義

研究成果物等	定義
研究試料有体物	サンプル、実験装置等 ・ サンプル：試薬、生物、堆積物、岩石、海水等をいい、「サンプル取扱規則」において掘削コア、ピストンコア等の柱状の岩石試料及び堆積物試料である「コアサンプル」、固形非定形の岩石試料である「岩石サンプル」、生死を問わない生物試料及び生物試料からの分離・抽出物である「生物サンプル」が定義されている ・ 実験装置：培養装置、解析装置、データ保存装置
データ	調査観測データ・シミュレーションデータ・数値データ、映像・画像等をいい、「データ取扱規則」によって「調査・研究活動を通じて生成され、又は取得された（以下「生成・ 取得」という。）あらゆる情報をいう。データには、研究の過程で新規に産出される 観測機器、計測機器、計算機器等の研究機器から生成され収集されたメタデータを 含むデータ、役職員自身が計測し、又は考案して作成したデータ等に加え、これら のデータを加工したデータも含まれる。」と定義される
ラボノート	ラボノートの詳細な定義はないが、JAMSTEC の法人文書管理規則規程第２条に定める法人文書は除くとしている。

データ、サンプルについては、さらに「共同利用研究課題航海により得られた調査観測データ・サンプル取扱い及び公開規則」において、共同利用研究課題を実施するための航海に

394 https://www.kenkai.jaxa.jp/kakushin/news/data/kakushin4_guide.pdf

395 https://www.jamstec.go.jp/ceist/j/datasample/files/JAMSTEC_DS_Regulations_jp.pdf

より得られた調査観測データ及びサンプルの取扱い、公開及び利用についても規定されている。

■　情報の分類

公開されている JAMSTEC の規程類からは、機密性・完全性・可用性などの観点から JAMSTEC において取り扱われる情報や前記取り扱い規程の対象となる研究成果物等の分類を行っていることは確認できなかった。

しかし、JAMSTEC は国立研究開発法人であり、「情報セキュリティ基本方針」において「『政府機関のサイバーセキュリティ対策のための統一規範』等を踏まえ、情報セキュリティ関連規程類を整備、運用する」旨記載されていることから、「政府機関等のサイバーセキュリティ対策のための統一基準」に則った情報の分類が成されているものと思料される[396]。

■　情報管理策

公開されている JAMSTEC の規程類（「JAMSTEC データ・サンプル関連諸規程」等）からは、研究成果物等の具体的な取り扱いについては「容易に他人に知られ、又は持ち出されないように適切かつ厳重に管理しなければならない」「当該外部機関及び機構の定めるところにより、その研究成果物等の取扱いに関し適切に対応しなければならない。」と定められているのみであり、必要な組織的・人的・物理的・技術的な管理策は公開されていない下位規則で定められているものと思われる。

その他、前記のとおり「政府機関等のサイバーセキュリティ対策のための統一基準」に則った情報の取り扱いが規定されている可能性は高いと思料される。

また、設置根拠である国立研究開発法人海洋研究開発機構法では第 15 条において機構の役員及び職が職務上知ることのできた秘密について、秘密保持義務が規定されており、違反した場合一年以下の懲役又は五十万円以下の罰金が科される[397]。

■　所管する主なプログラムと情報取扱規程

・　SIP 第 3 期　課題「海洋安全保障プラットフォームの構築」

【研究領域】海洋

【概要】4.1.1　(1) 1) c)参照

【参加資格】

現在公開されている情報では、NJSS、発注機関の JAMSTEC のページともに 404 エラーとなっており、公募要領、参加制限等は確認できなかった。

【情報取扱規程】

研究開発実施主体と JAMSTEC の締結する委託契約書雛形では、研究開発実施主体は秘密保持に違反しない限りは研究成果を公表することができ、また JAMSTEC が保有する船舶、探査機、曳航体等の設備・観測機器を用いて取得した全てのデータ及びサンプル（海底地形調査情報、海底下地層構造情報、船舶等に搭載された計測・観測機器等による位置情報、画像、

396 https://www.jamstec.go.jp/j/about/security/

397 https://elaws.e-gov.go.jp/document?lawid=415AC0000000095

重力情報及び磁力情報等の観測データ、並びに生物、堆積物、岩石・鉱石、海水及び採泥試料等のサンプルを含むがこれらに限らない）は JAMSTEC に帰属するとされる。

また、主管機関である JAMSTEC は、本プログラムの推進委員会の一員である JOGMEC（エネルギー・金属鉱物資源機構）との間に「南鳥島周辺海域における海洋調査活動で取得した探査・調査データ及びサンプルの取り扱いに関する合意書」を締結しており、JOGMEC から JAMSTEC へ提供された探査・調査データ及びサンプルのうち、研究開発のために JAMSTEC から研究機関へ提供される探査・調査データ及びサンプル（JOGMEC データ）の取り扱いについて、特約条項を課している。特約条項では以下のような具体的な JOGMEC データの取り扱いを研究開発実施主体へ求めている[398]。

（独立行政法人石油天然ガス・金属鉱物資源機構から提供される探査・調査データ及びサンプルの取り扱いに関する特約条項において研究開発実施主体に求めるデータ取扱要領）

- **目的外利用の禁止、適切な取り扱いの要求**
- **JOGMEC データを、バックアップの目的以外に複製してはならない**
- **JOGMEC データを使用、又は参照することにより得られた調査研究の成果を開示、又は公表する場合は、その内容について事前に JAMSTEC 及び JOGMEC の書面による承諾を得なければならない**
- **JOGMEC データのうち、具体的な位置を特定できる情報（緯度・経度情報が記載された詳細地図等）を公表する場合は、事前に機構及び JOGMEC の承諾を得なければならない**
- **JOGMEC データの一切については、国立研究開発法人産業技術総合研究所法第１０条の２にいう秘密に該当する**

c）日本医療研究開発機構（AMED）

AMED は、医療分野の研究開発とその環境整備の中核的な役割を担うため、それまで文部科学省・厚生労働省・経済産業省が独自に実施していた医療分野の研究開発を一元的に実施する国立研究開発法人たる資金配分機関（ファンディングエージェンシー）として、2015 年に設立された。

■　研究開発領域

バイオ

■　適用範囲

公開されている AMED の規程類を確認したところ、AMED において取扱要領を規則で定める情報の範囲や、情報取り扱いに係る規則の適用範囲について網羅的に言及している規程は確認できなかった。

他方、AMED では、AMED との委託研究開発契約等に基づき実施される委託研究開発、補助事業その他 AMED が支援を行う事業によって創出、取得又は収集されたデータやそのデータを加工等することによって生み出されたデータを「研究開発データ」としてその取扱いや利活用に係る以下のようなガイドライン等を定めている。また、AMED が委託者となる委託研

[398] https://www2.njss.info/8b8ae50c-d43f-44dc-a91e-0a3320b9f74a

究開発契約等において、どのようなデータが創出、取得又は収集され、誰がどこに保有しているのかを把握するためのデータマネジメントプラン（DMP）の作成・提出を研究開発実施主体に求めている[399]。

（研究開発実施主体に準拠を求める法令等）
・　AMED における研究開発データの取扱いに関する基本方針
・　AMED 研究データ利活用に係るガイドライン
・　データマネジメントプラン記載要領

■　情報の分類

公開されている AMED の規程類からは、機密性・完全性・可用性などの観点から AMED において取り扱われる情報や前記研究開発データの分類を行っていることは確認できなかった。

しかし、AMED は国立研究開発法人であることから、「政府機関等のサイバーセキュリティ対策のための統一基準」に則った情報の分類が成されている可能性は高いと思料される。

■　情報管理策

公開されている AMED の規程類からは、AMED と委託研究開発契約等を締結した研究開発実施主体の取り扱う情報全般に対して求める組織的・人的・物理的・技術的な管理策は確認できなかった。

しかし、前記の研究開発データについては、AMED の支援する研究は公的資金によって支援されているため、その結果得られた研究開発データについても第三者に公開される必要のあるとする一方で、研究開発実施主体による研究開発（製品開発、論文発表、特許出願を含む。）のインセンティブを損なわないことや、検体や臨床情報等を提供した研究参加者の権利や法律上の利益の保護並びに個人情報の保護の観点から、①個別研究開発課題ごとのデータマネジメントプランで設定する公開方法に従って公開する場合、②別途 AMED の承諾を得て第三者とデータシェアリングをする場合に限り、研究開発実施主体が研究開発データを第三者に対して開示又は提供することを許容している[400]。

その他、前記のとおり「政府機関等のサイバーセキュリティ対策のための統一基準」に則った情報の取り扱いが規定されている可能性は高いと思料される。

■　所管する主なプログラムと情報取扱規程

・　新興・再興感染症に対する革新的医薬品等開発推進研究事業

【研究領域】バイオ

【概要】4.1.1（1）1）c)参照

【参加資格】

本プログラムでは、応募者を特定の要件を満たす研究開発実施計画の策定や成果の取りまとめなどの責任を担う研究者（研究開発代表者）としている。研究開発代表者は、要件を

399 https://www.amed.go.jp/koubo/datamanagement.html

400 https://www.amed.go.jp/content/000117366.pdf

満たす国内の研究機関に所属する必要があるものの、日本国外の研究機関等に所属している研究者であっても、研究開発代表者として採択された場合、契約締結日又は令和６年４月１日までに、日本国内の研究機関に所属して研究を実施する体制を取ることが可能であれば応募が認められる。

また、委託研究開発契約の履行能力を確認するため、審査時に、代表研究機関及び分担研究機関の営む主な事業内容、資産及び負債等財務に関する資料等の提出を求めることがあるとしている。応募者の満たす必要のある要件は以下の通り。

（新興・再興感染症に対する革新的医薬品等開発推進研究事業の参加要件）

1. **以下の（A）から（G）までに掲げる研究機関等に所属していること。**
   - **(A) 国の施設等機関（研究開発代表者が教育職、研究職、医療職、福祉職、指定職又は任期付研究員である場合に限る。）**
   - **(B) 公設試験研究機関**
   - **(C) 学校教育法（昭和 22 年法律第 26 号）に基づく大学及び同附属試験研究機関等（大学共同利用機関法人も含む。）民間企業の研究開発部門、研究所等**
   - **(D) 研究を主な事業目的としている一般社団法人、一般財団法人、公益社団法人及び公益財団法人**
   - **(E) 研究を主な事業目的とする独立行政法人通則法（平成 11 年法律第 103 号）第 2 条に規定する独立行政法人及び地方独立行政法人法（平成 15 年法律第 118 号）第 2 条に規定する地方独立行政法人**
   - **(F) 非営利共益法人技術研究組合**
   - **(G) その他 AMED 理事長が適当と認めるもの**
2. **課題が採択された場合に、課題の遂行に際し、機関の施設及び設備が使用できること。**
3. **課題が採択された場合に、契約手続等の事務を行うことができること。**
4. **課題が採択された場合に、本事業実施により発生する知的財産権（特許、著作権等を含む。）及び研究開発データの取扱いに対して、責任ある対処を行うことができること。**
5. **本事業終了後も、引き続き研究開発を推進するとともに、追跡調査等 AMED の求めに応じて協力すること。**

【情報取扱規程】

研究開発実施主体に求める情報管理策については、公募要領では具体的に示されてはいないものの、外為法に基づき、リスト規制貨物の輸出又はリスト規制技術の外国への提供を業として行う場合には、安全保障貿易管理の体制構築を行うことを求めており、経済産業省のウェブサイトや「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）」などを参照している。

また、外為法上の規制対象となる貨物・技術の他に北朝鮮による核実験の実施及び累次の弾道ミサイル発射を受け平成 28 年 11 月 30 日、国連安全保障理事会によって採択された安保理決議第 2321 号に基づき、決議の厳格な実施（北朝鮮により公式に後援され又は北朝鮮を代表する個人又は団体が関係する科学技術協力の停止）に留意することを示している。

その他、前記のとおり研究開発データについては、研究開発実施主体が AMED からの支援（委託又は補助）を受けて行う研究開発に関連して創出、取得又は収集するあらゆる研究開発データを第三者に開示又は提供することを原則として禁止した上で、AMED のガイドライ

ン上で許容されている場合又はあらかじめ AMED の承諾を得た場合に限り、第三者に開示又は提供することを可能としている。

成果の取り扱いについては、知的財産権の研究開発実施主体への帰属を通じて研究開発活動を活性化し、その成果を事業活動において効率的に活用することを目的として産業技術力強化法（平成 12 年法律第 44 号）第 17 条に規定される要件を満たすことを前提に、研究機関に帰属させることとしている。しかし研究開発成果や当該研究開発成果に係る知的財産権を、国内の子会社から国外の親会社に承継する場合は、事前に AMED への相談が必要となる。

d）総務省

■ 研究開発領域

サイバー

総務省における情報保全の適用範囲や、情報の分類、情報管理策については公開情報からは確認できなかった。しかし内閣サイバーセキュリティセンターの策定する「政府機関等のサイバーセキュリティ対策のための統一基準」においては、全ての機関等において共通的に必要とされる情報セキュリティ対策の基準を示し、それに則って各府省庁において情報セキュリティ関係規程を策定することが示されているため、総務省についても統一基準に従っているものと考えられる [401]。以降「政府機関等のサイバーセキュリティ対策のための統一基準（以下、「統一基準」）」[402]の記載内容について整理する。

■ 適用範囲

統一基準の適用対象となる者は政府機関の全ての職員とされ、また対象となる情報については、以下の情報と定義されている。また情報システムは、統一基準の適用対象となる情報を取り扱う全ての情報システムを対象としている。

（政府機関等のサイバーセキュリティ対策のための統一基準の適用範囲）
（ア）職員等が職務上使用することを目的として機関等が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）
（イ）その他のシステム又は外部電磁的記録媒体に記録された情報（当該システムから出力された書面に記載された情報及び当該システムに入力された書面に記載された情報を含む。）であって、職員等が職務上取り扱う情報
（ウ）（ア）及び（イ）のほか、機関等が調達し、又は開発したシステムの設計又は運用管理に関する情報

■ 情報の分類

401 https://www.nisc.go.jp/policy/group/general/kijun.html

402 https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf

統一基準の適用対象となる情報については、機密性、完全性及び可用性の３つの観点を区別し、統一基準の遵守事項で用いる格付の区分の定義を示している（表 4.1-31）。

表 4.1-31　統一基準における情報の分類

観点	格付けの区分	分類基準
機密性	機密性 3 情報	国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成 23 年 4 月 1 日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報
	機密性 2 情報	・　国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 ・　独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報 ・　また、指定法人のうち、独法等情報公開法の別表第一に掲げられる法人（以下「別表指定法人」という。）についても同様とする ・　別表指定法人以外の指定法人における業務で取り扱う情 ・　報のうち、上記に準ずる情報
	機密性 1 情報	・　国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報独立行政法人又は別表指定法人における業務で取り扱う情報のうち、独法等情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 ・　別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報
完全性	完全性 2 情報	業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
	完全性 1 情報	完全性２情報以外の情報（書面を除く。）
可用性	可用性 2 情報	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
	可用性 1 情報	可用性２情報以外の情報（書面を除く。）

機密性 2 情報及び機密性 3 情報は「要機密情報」、完全性 2 情報は「要保全情報」、可用性 2 情報は「要安定情報」と呼称し、情報が要機密情報、要保全情報及び要安定情報に一つでも該当する場合は「要保護情報」と呼称される。

職員等は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。統括情報セキュリティ責任者は、以下を全て含む情報の取扱いに関する運用規程を整備し、職員等へ周知しなければならない。

（統括情報セキュリティ責任者が整備すべき情報の格付けと取り扱い制限に関する規程）
（ア）情報の格付及び取扱制限についての定義
（イ）情報の格付及び取扱制限の明示等についての手続
（ウ）情報の格付及び取扱制限の継承、見直しに関する手続

■　情報管理策

【組織的管理策】

基本的な組織、体制の整備として、以下の事項を遵守しなければならない。

（政府機関等のサイバーセキュリティ対策のための統一基準が求める組織・体制の整備）
- **最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置**
- **情報セキュリティ委員会の設置**
- **情報セキュリティ監査責任者の設置**
- **統括情報セキュリティ責任者・情報セキュリティ責任者等の設置**
- **最高情報セキュリティアドバイザーの設置**
- **情報セキュリティ対策推進体制の整備**
- **情報セキュリティインシデントに備えた体制の整備**
- **申請・承認及び監査・被監査の役割の兼務の禁止**

そして統括情報セキュリティ責任者は、自組織の情報資産の全容を把握するため、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

その他、組織として遵守すべき対策を計画的に実施するため、情報セキュリティ関係規程を整備・運用するとともに、情報セキュリティインシデントへの事前準備・対処・情報共有・再発防止・教育を行い、情報セキュリティ対策の自己点検、情報セキュリティ監査を実施し、その結果等を踏まえて情報セキュリティ対策の見直しを継続的に実施しなければならない。

【人的管理策】

職員等は、統括情報セキュリティ責任者が示す情報の格付け及び取り扱い制限に関する運用規定に従い、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用等しなければならない。

また統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、職員等に対して、情報セキュリティ関係規程に

係る教育を適切に受講させなければならない。

【物理的管理策】

執務室、会議室、サーバ室等の情報を取り扱う区域を「要管理対策区域」として、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保することが定められている。

「要管理対策区域」とは、機関等の管理下にある区域（機関等が外部の組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域と定義されている。そして要管理対策区域の範囲と特性に応じて、以下の観点を全て含む対策の基準を運用規程として定めなければならない。

（**要管理対策区域**における物理的管理策）

- **許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策**
- **許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策**

また、情報の利用・保存にあたって機密性３情報を機器等に保存・利用する際には、機密要管理対策区域外で情報処理を行う場合は、課室情報セキュリティ責任者の許可を得ることや、当該情報を保存した機器等について、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずることなどが示されている。

【技術的管理策】

技術的管理策については、情報システムのセキュリティ要件及びその利用に係る遵守事項が規定されている。

（**政府機関等のサイバーセキュリティ対策のための統一基準が求める技術的管理策**）

【情報システムのセキュリティ機能に係る遵守事項】

- **主体認証機能の導入、識別コード及び主体認証情報の管理**
- **アクセス制御機能の導入**
- **主体から対象に対するアクセスの権限の管理**
- **ログの取得・管理**
- **暗号化機能・電子署名機能の導入、暗号化・電子署名に係る管理**
- **監視機能の導入・運用**

【情報セキュリティの脅威への対策に係る遵守事項】

- **ソフトウェアに関する脆弱性対策の実施**
- **不正プログラム対策の実施**
- **サービス不能攻撃対策の実施**
- **標的型攻撃対策の実施**

【ゼロトラストアーキテクチャに係る遵守事項】

- **動的なアクセス制御における責任者の設置**

・　動的なアクセス制御の導入方針の検討
・　動的なアクセス制御の実装時の対策
【情報システムの利用に係る遵守事項】
・　情報システムの利用に係る規定の整備
・　情報システム利用者の規定の遵守を支援するための対策
・　情報システムの利用時の基本的対策
・　端末（支給外端末を含む）の利用時の対策
・　電子メール・ウェブの利用時の対策
・　識別コード・主体認証情報の取扱い
・　暗号・電子署名の利用時の対策
・　不正プログラム感染防止
・　Web 会議サービスの利用時の対策
・　クラウドサービスを利用した機関等外の者との情報の共有時の対策
【ソーシャルメディアによる情報発信に係る遵守事項】
・　ソーシャルメディアによる情報発信時の対策
【テレワークに係る遵守事項】
・　運用規程の整備
・　実施環境における対策
・　実施時における対策

■　所管する主なプログラムと情報取扱規程

・　令和 3 年度　情報通信技術の研究開発に係る提案の公募：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発

【研究領域】サイバー

【概要】4.1.1（1）1）c)参照

【参加資格】

本研究開発プログラムにおいては、以下の要件を満たす、単独ないし複数の企業、大学、国立研究開発法人等が応募可能であるとしている。

（令和 3 年度　情報通信技術の研究開発に係る提案の公募：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発の参加要件）

・　当該研究開発課題に係る技術又は関連技術についての研究開発の実績を有し、かつ、当該委託研究を実施するために必要な組織、人員等を有していること。
・　研究開発の実施の効率性や機動性向上の観点から、原則、日本国内に研究拠点を持つ研究開発機関等であること。海外研究拠点での研究開発は、研究項目の中で国内研究拠点において実施し得ないテーマ、海外の特殊な設備等を使用せざるを得ないテーマ等に限られていること。
・　当該委託研究を円滑に執行するために必要な経営基盤を有し、かつ資金等について十分な管理能力を有していること。
・　当該委託研究の全部又は一部を複数の企業等が共同して実施する場合（「共同研究」）、各研究開発機関等の役割と責任が明確に示されていること。また、各研究開発機関等の

とりまとめを行う代表的な研究開発機関等（「代表研究開発機関」）が定められていること。 ・ 府省共通研究開発管理システム（e-Rad）に対して、「所属研究開発機関の登録」及び「研究者の登録」がなされていること。 ・ 研究責任者（共同研究の場合は代表研究責任者）は、全ての研究開発期間を通じて、研究開発の遂行に関する全ての責務を負えること。 ・ 全ての研究責任者（共同研究の場合は代表研究責任者）及び研究者は、所属する研究開発機関等に対して、あらかじめ本研究開発へ提案することへの了解を得ていること。（研究開発の実施にあたって、研究資金は所属する研究開発機関等が管理するとともに、資金の経理処理も研究開発機関等が実施する必要がある。）

本研究開発プログラムで、総務省から研究開発実施主体に対して遵守を求める具体的な情報取扱規程等は公募要領等では確認できなかった。

しかし、海外への技術漏えいへの対処として、安全保障貿易管理制度の遵守を求めていることから、経済産業省のウェブサイトやガイドラインにおいて規定されている、安全保障貿易管理上の情報管理策については遵守する必要があるものと考えられる[403]。

その他、成果の取り扱いについては、研究開発実施中に知的財産権が発生した場合、「産業技術力強化法」に基づき、以下の条件の下、受託者側に帰属させることが可能となっている。

（令和 3 年度　情報通信技術の研究開発に係る提案の公募：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発における成果・知財の扱い） ・ 委託研究に係る成果（研究開発の実施により新たに発見ないし生み出されたものすべてを言い、知的財産権に関するもの、ノウハウに関するもの等すべてを含む。）が得られた場合には、遅滞なく、総務省にその旨を報告すること。 ・ 総務省が公共の利益のために特に必要があるとしてその理由を明らかにして求める場合には、無償で当該知的財産権を利用する権利を国に許諾するものとする。 ・ 当該知的財産権を相当期間活用していないと認められ、かつ、当該知的財産権を相当期間活用していないことについて正当な理由が認められない場合において、総務省が当該知的財産権の活用を促進するため特に必要があるとしてその理由を明らかにして求めるときは、当該知的財産権を利用する権利を第三者に許諾するものとする。 ・ 第三者に当該知的財産権の移転又は当該知的財産権についての専用実施権若しくは専用利用権の設定その他日本国内において排他的に実施する権利の設定若しくは移転の承諾をするときは、一部の場合を除き、あらかじめ総務省の承認を受けること。 ・ 上記のほか、必要と認められる事項がある場合には、契約書等において別途定める。

e）防衛装備庁

■　研究開発領域

多義的技術

403 https://www.soumu.go.jp/main_content/000740707.pdf

■　適用範囲

防衛装備庁については防衛省の下部組織であるため、情報の取扱いについても自衛隊法及び防衛省規則が適用される。防衛省職員に課される最も一般的な情報保全義務については自衛隊法第 59 条に規定される、職務上知り得た秘密を守る義務であり、いわゆる省秘は「防衛省の所掌する事務に関する知識及びそれらの知識に係る文書若しくは図画 （電磁的記録含む）又は物件であって～」と定義されているため、有形・無形のあらゆる形式の情報を対象としていると考えられる [404]。

■　情報の分類

防衛装備庁含む防衛省における秘密情報は、特定秘密保護法に基づく「特定秘密」、MDA 秘密保護法に基づく「特定秘密」、そして自衛隊法等により保護されている「秘」の３つの秘密により構成される。その他、や CUI (Controlled Unclassified Information)等に相当する非秘密情報 (Unclassified Information) であるものの管理を要する情報区分として「注意」及び「部内限り」がある。これらを防衛産業に関わる事業者等が取り扱う場合は、契約書に特約条項を付して「保護すべき情報」として、保護措置が講じられる [405](表 4.1-32)。

表 4.1-32　防衛省における情報の分類

区分	種別		概要
秘密情報	特定秘密		特定秘密の保護に関する法律（平成 25 年法律第 108 号）第３条の規定に基づき、行政機関の所掌事務に係る同法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として、行政機関の長が指定したもの。
	特別防衛秘密	機密 極秘 秘	日米相互防衛援助協定等に伴う秘密保護法（昭和 29 年法律第 166 号）第１条各号に揚げる事項（日米相互防衛援助協定等に基づき米国政府から供与された装備品等についての構造又は性能その他の事項等）及びこれらの事項に係る文書、図画又は物件で、公になっていないもの。
	秘（省秘）		防衛省の所掌する事務に関する知識及びそれらの知識に係る文書若しくは図画（電磁的記録含む）又は物件であって、秘密保全に関する訓令（平成 19 年防衛省訓令第 36 号）の規定に基づいて秘と指定したもの。

[404] https://www.mod.go.jp/igo/compliance/guidance/pdf/kanri04-himituhozen.pdf

[405] https://www.mod.go.jp/atla/img/dism/dism2023_jp.pdf

区分	種別	概要
保護すべき情報（管理対象非機密情報）	注意	当該事務に関与しない隊員にみだりに知られることが業務の遂行に支障を与えるおそれのあるもの。
	部内限り	防衛省の隊員以外の者にみだりに知られることが業務の遂行に支障を与えるおそ れのあるもの。

■　情報管理策

防衛装備庁が研究開発実施主体に求める情報管理策については、前記の特定秘密、特別防衛秘密に関する法律や自衛隊法を根拠にして対応する規則が制定されており、複雑な規則体系となっている。これら規則体系について一元的に整理し、標準的な防衛産業保全に関する措置を示しているマニュアルとして、防衛産業保全マニュアルがある[406]。

本項においては、防衛産業保全マニュアルに記載の情報管理策を組織的・人的・物理的・技術的管理策に分けて概要を整理する。

【組織的管理策】

秘密情報及び保護すべき情報の取扱いが求められる契約について、入札手続に参加を希望する事業者は、入札に参加する前の段階において、外国の所有、支配、影響（Foreign Ownership Control or Influence：FOCI）の有無を含めて秘密情報を取り扱うのにふさわしい履行体制を確保すること及び履行に必要な情報を取り扱うのにふさわしい契約を履行する業務に従事する従業者を確保することに関し、防衛装備庁の確認を受ける必要がある。

そのために防衛装備庁は、契約に関わる者の一覧、資格の無い従業員が秘密情報にアクセスすることを禁ずる社内規則、事業者に対し潜在的影響力を持つ外国を含む親会社又は他の事業者との契約関係及び資本関係といった資料の提出を事前に要求し、事業者側の体制が要求基準を満たしていない場合は、入札参加を認めない、もしくは必要な改善措置を講じさせる。

そして事業者が秘密情報を取り扱うためには、事業者秘密取扱適格性(Facility Security Clearance：FSC)の認定を受ける事が必要となる。事業者秘密取扱適格性を認められた事業者は「秘密取扱適格事業者」と呼ばれる。事業者秘密取扱適格性の申請においては、総括者の指定、秘密保全規則等の制定、保全教育の実施及び後述の秘密保全施設に係る申請が必要となる。

事業者秘密取扱適格性の認定を受けた後、事業者は秘密情報の接受、閲覧、作成、保管、提出、廃棄等を確実に実施し、それを証明するため、関係簿冊を整備しなければならない。また少なくとも月に一回は関係簿冊のほか、全ての秘密保全措置について社内検査を行わなければならない。社内検査の終了後には、月に１回管轄する地方防衛局の職員による保全検査を受検しなければならない。

また、秘密文書等を紛失した場合、秘密情報が漏えい若しくは破壊された場合又はそれらの疑い若しくはおそれがある場合等事故発生時の措置のため、防衛装備庁窓口への緊急連

406 https://www.mod.go.jp/atla/img/dism/dism2023_jp.pdf

絡体制、非常時の廃棄措置等を実施しなければならない。

その他、秘密情報の取り扱いを含む下請負契約についても規定されている。下請負契約は、原則として認められないが、当該下請負事業者が事業者秘密取扱適格性を認定されていることや、防衛装備庁と元請事業者と下請負事業者との三者間で、秘密保護契約が締結されていることなどを条件に許可される場合がある。下請負事業者は、秘密取扱適格事業者であるほか、元請事業者に課されている義務と同様の義務を課されることになる。

【人的管理策】

事業者が秘密情報を取り扱うにあたっては、従業員の個人単位で取り扱う秘密区分に応じた秘密取扱適格性（Personnel Security Clearance: PSC）を保有していることが必要である。秘密取扱適格性は、秘密情報を取り扱う契約の締結後に付与手続がとられる。

秘密取り扱い適格性の付与は、秘密情報を取り扱う必要がある従業者を記載する関係社員の名簿を作成する過程で行われる。総括者は、当該契約に係る秘密情報を取り扱う必要がある従業者を関係社員の候補として選抜し、秘密取扱適格性を取得する手続をとらせる。

そして事業者は、年に１回の保全教育を全関係社員に受講させなければならない。また、関係社員以外の全ての従業者に対して、定期的に必要な範囲の教育を行うこととされており、その教育内容に基づいた訓練を事業所単位で実施しなければならない。

教育内容には、秘密情報に関する法律、政令、訓令、通達その他関係規則の条文及びその解説、秘密保全の必要性、保全教育の意義・重要性、関係社員の役割及び責任、非常事態発生時の対処要領など 11 項目が示されており、防衛装備庁は、カウンターインテリジェンスを含む教育資料の提供等により事業者における教育の支援を実施するとしている。

【物理的管理策】

事業者は、秘密情報を取り扱う際には、「秘密保全施設」で取り扱わなければならない。秘密保全施設とは、秘密文書等を保管容器に格納する秘密保全施設のほか、機能試験等で秘密情報を取り扱うため期間を定めて設定する閉鎖区域、秘密物件が保管容器に保管できない場合に設置する保管庫又は金庫室を総称するものである。

秘密物件を保護するための秘密保全施設の構造基準として、天井、壁、床、間仕切り、出入口、扉及び錠、窓、開口部、警報装置、外柵、保管容器「保全外部区域」の設置といった具体的な備えるべき構造の要件が定められている。さらに秘密保全施設の管理の為、営業日毎の点検、鍵の管理、暗唱番号の管理、保守管理のための立ち入り手続きなどを履行しなければならない。

その他秘密情報の作成又は取扱いに使用する事業者の情報システムについても、原則として秘密保全施設に常設し、持ち出しを禁止するとともに、不正な持ち出しを防止するためにワイヤによる固定や修理の際の監視、所持品検査など必要な措置を講じなければならない。情報システムの修理や処分するためにやむを得ず秘密保全施設から持ち出すときは、記憶媒体を物理的に破壊する等秘密情報の漏えいを防止するための措置が必要となる。また秘密保全施設には、常設している情報システム以外の携帯型通信機器等の持込みを原則として禁止しなければならない。

また、作成等した秘密文書等に、秘密区分に応じた物理的な表示を行わなければならない。表示は、「特定秘密」、「特別防衛秘密（機密）」、「特別防衛秘密（極秘）」、「特別防衛秘密（秘）」、

「秘」のいずれかになる。秘密を記載しているページに加え、表紙及び裏表紙のそれぞれ右上及び左下に赤色で表示する必要がある。また、何が秘密情報なのかを明示した表示を行う必要がある。例えば、文書の一部分であれば下線部を引く又は○や□で囲うなど、挿絵、写真、図又は表などの場合は外周を赤枠で囲うなど、表内が秘密であることを明記する等の記載が必要となる。

さらに秘密文書等の作成等のために一時的に作成した反古紙等で、実質的に当該秘密の内容を含むものは、これらが探知され、又は収集されることのないよう廃棄及び保管について、秘密に準じた取扱いをしなければならない。廃棄に当たっては、秘密文書等を廃棄する方法と同様に秘密情報の内容を推測されないように実施しなければならない。

秘密文書等を廃棄する際は、防衛装備庁の指示に従い、総括者により指定された関係社員を最低１名以上立会させ、焼却、粉砕、細断、溶解、破壊等の方法により、秘密として探知されないように確実に廃棄し、それを記録して防衛装備庁に報告する必要がある。

【技術的管理策】

秘密情報の作成又は取扱いに使用する事業者の情報システムについては、以下のような技術的対策を行わなければならない。

（防衛産業保全マニュアルにおける秘密情報の作成又は取扱いに使用する事業者の情報システムに求められる対策）

- 通信：
  スタンドアローンとして使用するか、ネットワークに接続する場合は、秘密保全施設内において有線で配線接続する場合に限り構築でき、秘密保全施設外のいかなるものとも原則として接続してはならない。保全区画内においてワイヤレスネットワーク接続の使用は禁止しなければならない。
- 情報システムにインストールするソフトウェアについて：
  業務に必要なソフトウェアのみ使用し、悪意あるソフトウェアから秘密情報を保護するため、最新のウイルス対策ソフト等を用いて、悪意あるソフトウェアを検知するなどの対策を行わなければならない。
- 情報システムのメンテナンス等について：
  事業者は秘密情報を取り扱う情報システムのメンテナンス等（保守、点検、診断、修理、整備及びアップデートを含む。）を定期的及び必要に応じ実施するため、メンテナンス等計画を作成し、その計画に基づきメンテナンス等を実施する。メンテナンスの実施には立ち会い、監視を行うとともに、日時、人員、実施内容を記録する。
- 情報システムのメンテナンス等の外部委託について：
  メンテナンス等を秘密取扱適格事業者以外への外部委託は原則として禁止している。やむを得ず秘密取扱適格事業者以外への外部委託をしなければならない場合は、委託先への注意点及び要求事項の明示し、立ち入りには事前に地方防衛局の許可を受ける事、外部委託先が秘密情報に接触しないよう措置を講じることが必要となる。
- 可搬記憶媒体の取扱いについて：
  秘密情報を電子情報として取り扱う場合、原則として可搬記憶媒体へ保存しなければならない。可搬記憶媒体の取扱いに関する管理手順を作成し、事前の使用許可や貸し出し・返却の記録を残すとともに、可搬記憶媒体への情報の保存には電子政府推奨暗号等を使

用して秘匿し、その暗号鍵は厳格に管理すること、及び可搬記憶媒体の内容の複製及び破棄手順を定めなければならない。

・ アクセス制御方針の作成：
情報システムのアカウント管理者（アカウントの設定、変更及び削除等を行う者）を指定すること、情報システムの利用者ごとに業務遂行上必要最小限度の機能及び権限となるようアカウントを管理すること、情報システムを構成する機器の識別及び情報システム利用者の認証に関することを定めたアクセス制御方針を作成しなければならない。

・ 利用者ＩＤの設定：
情報システムを取り扱う関係社員ごとに利用者ＩＤを保有させ、関係社員自身でパスワードを設定させる必要がある。またログオン試行回数の上限を設定し、それを超える回数を失敗した場合は自動的にロックし、一定時間再試行できないように設定するとともに、非アクティブ状態であり続ける上限時間を定め、それを超える場合にはユーザセッションをロックするように設定する必要がある。

・ 情報システムの使用状況の記録：
情報システムの不正使用や不適切な運用のチェックなど、問題が発生したときの調査及びアクセス制御の監視を補うため、情報システムの使用状況を記録し、保存する必要がある。この記録は、少なくとも利用者ＩＤ、ログオン及びログオフの日時、アクセス者の端末ＩＤ、アクセスされたファイル並びに使用されたプログラム、情報システム及びデータへのアクセスの成否を含み、定期的及び必要に応じて点検しなければならない。

■ 所管する主なプログラムと情報取扱規程

・ 安全保障技術研究推進制度

【研究領域】多義的技術

【概要】4.1.1（1）1）c)参照

【参加資格】

本プログラムでは研究開発実施主体について、研究を実施する研究者（研究実施者）のうち、研究実施の中心となる代表者「研究代表者」と定義している。「研究代表者」以外の研究実施者は「研究分担者」となる。全ての研究実施者は、研究を実施する能力のある以下のいずれかの機関に所属していることが必要となる。また、これらの機関及び研究実施場所は、原則として全て日本国内に所在していることが必要となる。

（安全保障技術研究推進制度における研究実施者の所属する機関の要件）

・ 大学、高等専門学校又は大学共同利用機関
・ 独立行政法人（国立研究開発法人を含みます）、特殊法人又は地方独立行政法人
・ 民間企業や研究を主な目的とする公益社団法人、公益財団法人、一般社団法人、一般財団法人等

以下の者は研究実施者となることはできない。

（安全保障技術研究推進制度に参加できない者）

・ 応募時又は研究実施時に国家公務員又は地方公務員の職にある者
・ 防衛装備庁において研究に関する職（非常勤職員は除く）に従事し、当該職を離れてか

ら５年を経過していない者 ・ 本制度の研究費の不正使用等又は研究活動における不正行為等により、本制度への応募が制限されている者 ・ 国又は独立行政法人が所管している他の競争的研究費制度において、研究費の不正使用等又は研究活動における不正行為等により応募が制限されている者

さらに、研究代表者については加えて以下の条件を満たす必要がある。

（安全保障技術研究推進制度において研究代表者が満たすべき要件） ・ 日本国籍を有すること。 ・ 日本語による面接審査や評価に対応できること。 ・ 研究期間中、応募時に所属していた代表研究機関に継続的に在籍できること

【情報管理規程】

本プログラムでは公募要領において、研究開発実施主体に対して「受託者による研究成果の公表を制限することはありません。」「特定秘密を始めとする秘密を受託者に提供することはありません。」「研究成果を特定秘密を始めとする秘密に指定することはありません。」と明示されている[407]ため、特定秘密や特定防衛秘密、秘（省秘）の取り扱い規程を研究開発実施主体に課すことはない。

また、「応募に当たって、防衛装備庁が保有する情報又は施設の利用を前提とするような研究課題は避けてください。審査の対象外となる場合があります。」とされているため、「保護すべき情報」についても取り扱われる可能性は低いが、「研究を実施する過程で、防衛装備庁が保有する情報又は施設の利用が研究目的達成の上で有効であると、受託者及び防衛装備庁の双方が認めた場合」は防衛装備庁の保有する情報等の利用を調整するとしている。

そのため、前記の防衛装備庁における情報管理策のうち、「保護すべき情報」に関する管理策については、本プログラムの研究開発実施主体に適用される可能性があると考えられる[408]。

成果の取り扱いについては、他の政府所管研究開発プログラムと同様、産業技術力強化法（平成１２年法律第４４号）第１７条（日本版バイ・ドール規定）を踏まえた一定の条件を付した上で受託した研究実施機関に帰属させることができるとして、防衛装備庁としては、「本制度により受託者には積極的に知的財産権を取得していただきたい」旨を述べている。

f）内閣府等（SBIR 制度）

SBIR 制度については、技術成熟度やプログラムの進捗に応じた段階的な情報保全に関する調査を充実させることを意図して調査対象としたため、以下に技術成熟度やプログラムの進捗に応じた研究開発成果の保全状況について記載する。なお、スタートアップ企業等の中小企業が、大企業に比して十分でない資金力や研究開発体制の中でどのように参加するプログラムにおける情報保全を図っているのかについては、ヒアリングによって調査を実

407 https://www.mod.go.jp/atla/funding/koubo/r05/r5koubo_setsumei_shiryo.pdf

408 https://www.mod.go.jp/atla/funding/koubo/r05/r05koubo_full.pdf

施することとした。

日本の SBIR プログラムでは、技術成熟度では TRL に対応した多段階選抜方式を採用しており、プロジェクト内の進捗についてはステージゲート審査を設けているが、段階ごとに異なる情報保全措置が規定されていることは確認できなかった[409]。

公募に際して事業者に求める情報保全措置も、所管の省庁や国立研究開発法人によって異なっている。一般的に研究結果に基づく成果物に対しては、輸出管理規則や日本版バイ・ドール制度が適用されることが示されている（図 4.1-39）[410]。

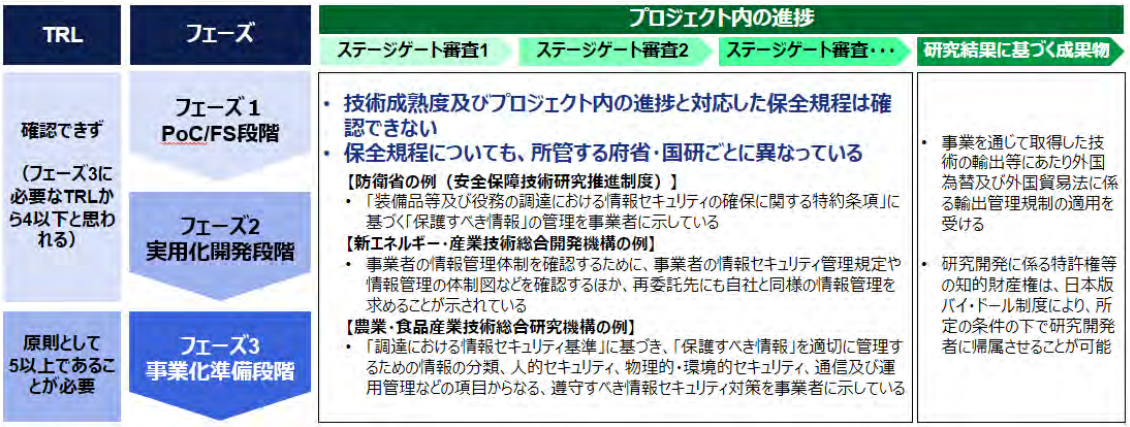


図 4.1-39　日本の SBIR プログラムにおける研究成果の保全イメージ

409 https://www.naro.go.jp/laboratory/brain/startup/koubo/R04.html

410 https://www.nedo.go.jp/content/100958311.pdf

2）研究開発実施主体における情報取り扱い実態の調査

a）東京大学

■　　選定理由

東京大学は日本の中で最高峰の大学であり、国内外の数多くのプロジェクトに参加をしていることから、調査で、情報保全に関連する有益な情報を多く獲得できることが期待できるため。

■　　参加している研究開発プログラム

・新興・再興感染症に対する革新的医薬品等開発推進研究事業
・ウイルス等感染症対策技術開発事業
・令和 3 年度　情報通信技術の研究開発に係る提案の公募：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発

■　　情報保全体制

東京大学セキュリティポリシーによると、大学全体に対する最高情報セキュリティ責任者(CISO:Chief Information Security Officer)を置き、情報セキュリティに関する施策の制定、それを全学に徹底させるために必要な措置の実施、必要な組織の設置等を行っている。

■　　情報保全措置

東京大学では、情報セキュリティポリシーの対象とする情報について、以下のように定義しており、DNA サンプル等を除いたあらゆる媒体の情報資産を管理の対象としていることが確認できる。

（情報セキュリティポリシーの適用範囲）

- **東京大学が保有する全ての情報資産**
- **情報資産は「情報」と「情報システム」を含む**
- **「情報」は、それを表現する媒体(磁気的媒体、光学的媒体、紙媒体など)の種類を問わない**
- **磁気ディスク、フラッシュメモリ、手書きメモは対象になる。ただし、当面の間、DNA サンプルのような試料は対象としない**
- **「情報システム」は、「情報」を扱うためのシステムであり、電子的システムだけでなく、紙媒体を扱うための学内便のようなシステムも含む**
- **なお、東京大学以外の情報システムに保管されるものであっても、東京大学保有の情報資産として認められるものは対象となる**

上記のような情報資産に対して、重要度による分類と相応の管理の徹底、侵害からの防衛、加害行為の防止、セキュリティ侵害等の早期検出と迅速な対応の実現といった観点から、対策基準および実施手順を定めている。

b）川崎重工業

川崎重工業は、東京、神戸に本社を置く総合エンジニアリングメーカーであり、船舶・鉄道車両・航空機・モーターサイクル・ガスタービン・ガスエンジン・産業プラント・油圧機器・ロボットなどの製造事業を展開している[411]。

なお、川崎重工業とはヒアリング調査を実施しており、具体的な情報保全措置や安全保障技術推進制度における取り組み等についても併せて記載する。

■　選定理由

ヒアリング対象企業であり安全保障技術研究推進制度（多義的技術）採択実績から、同制度での情報保全に向けた対応状況等について多くの情報を得られることが期待できるため。

川崎重工については、安全保障技術推進制度のプログラム参加者に対してヒアリングを実施した。

■　参加している研究開発プログラム

本調査の対象となった研究開発プログラムでは、川崎重工業は安全保障技術研究推進制度に参加している。

令和 4 年度公募において研究代表者所属機関として、分担研究機関である JAXA とともにタイプ C（小規模研究課題）に採択された。研究課題名は「海洋状況把握（MDA）等 に適用可能な革新的画像処理技術の研究」であり、夜間に人工衛星から撮像された光学画像から、人の目では判別できない程度の明るさの海上船舶等を自動的かつ確実に検出する新たな画像処理アルゴリズムを生成・開発し、昼夜を問わず海洋状況把握を可能とすることを目的とした研究開発を実施している[412]。

■　情報保全体制

川崎重工業は、本社 DX 戦略本部内に各カンパニーの情報システムを主管する組織を設置し、全社の方針に基づき安全対策の実施を行っている。

DX 戦略本部内のサイバーセキュリティ統括部が中心となって社内の情報セキュリティに係るルールの策定、教育・訓練を所管している。また標準・技術・制度に係る情報セキュリティ動向に関する情報収集や、自社がターゲットとなったサイバー攻撃・ネット犯罪への対応・改善処置を行い、情報セキュリティ業務への反映を行う体制となっている（図 4.1-40）[413]。

411 https://kawasakirobotics.com/jp/company/

412 https://www.mod.go.jp/atla/funding/kadai/r04kadai_2.pdf

413 https://www.khi.co.jp/sustainability/governance/security.html

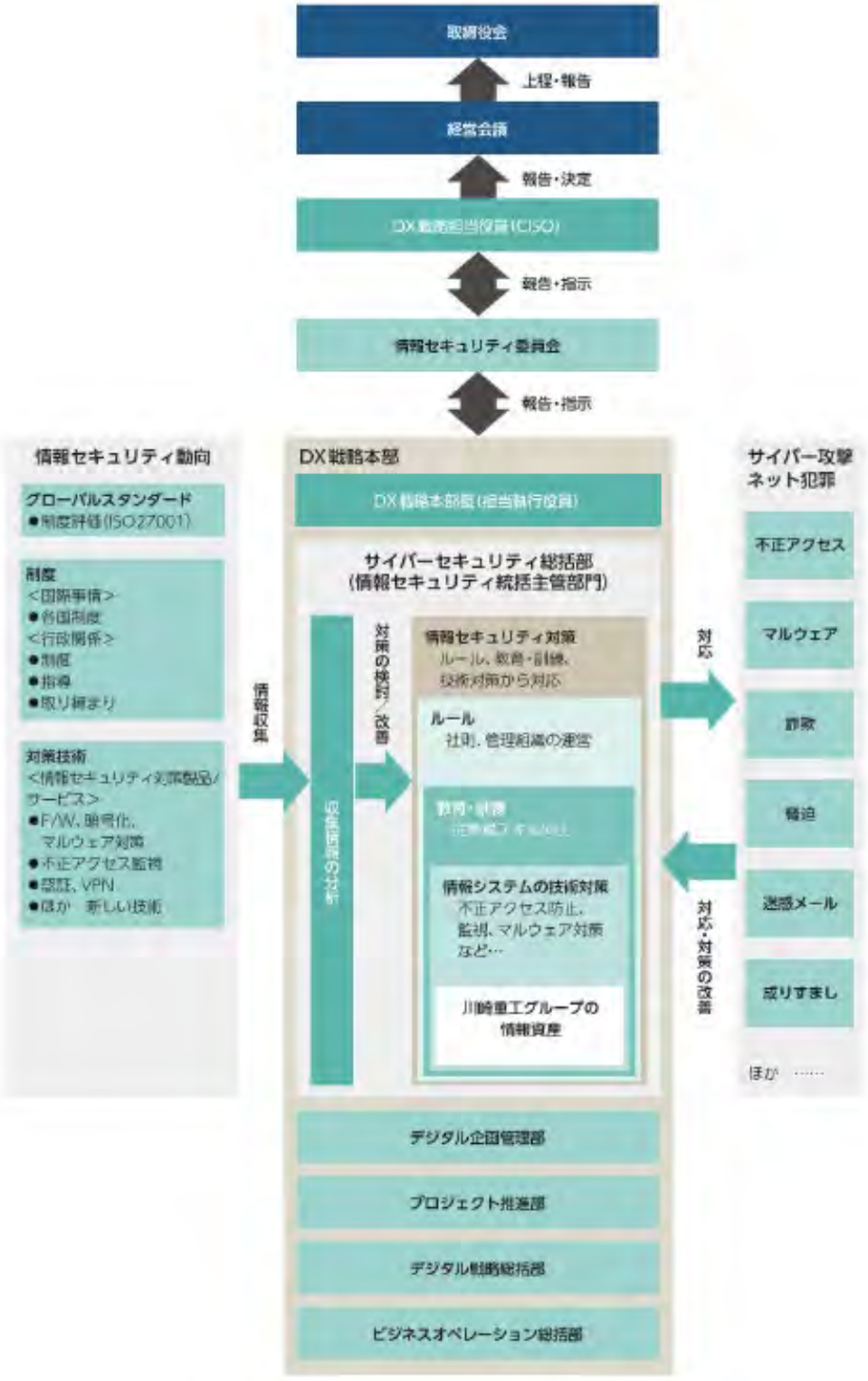


図 4.1-40　川崎重工業の情報セキュリティマネジメントシステム

■　　情報保全措置

川崎重工業の各カンパニーが平常業務において遵守している情報セキュリティ規則等は公開情報からは確認できなかったが、全社的に行っている対策の一部が公開されている。

技術的対策として、川崎重工業のデータセンターについては、外部ネットワークとの接点となる非武装地帯（DMZ）に設置・運用されるサーバの自社およびセキュリティベンダーによる脆弱性診断を実施し、また外部からの不正アクセス、社内からの情報漏洩、コンピュータウイルス感染を防止する仕組みの導入と不正行為のモニターなどを行う仕組みを導入している。

人的対策として、防衛分野の研究開発によっては外国籍の研究従事者等がメンバーに入らないことを念頭において、メンバー選定を実施している他、従業員に対して定期的に情報セキュリティの教育と訓練を実施している。教育内容は、法律やマナー、会社のルール、事故事例などについて、新入社員、一般従業員、幹部職員のそれぞれの立場にあった教育コースを実施している。訓練は、従業員が日常業務でサイバー攻撃やネット犯罪などの被害に遭わないよう、標的型疑似攻撃メールによる訓練演習を定期的に実施している。2022 年度においては、情報セキュリティ研修を 9,803 名が受講し、標的型疑似攻撃メールによる訓練を 2,308 名に対して実施している。

また、川崎重工業は個人情報の取り扱いについて、「個人情報の取扱いに関する方針」を公開しており、以下のような情報管理策を実施していることが確認できる。個人情報についてはEUおよび英国の一般データ保護規則（GDPR）についても遵守した社内規則を制定している [414]。組織的管理策として個人情報の取扱いに関する個人情報保護管理責任者を設置するとともに、個人情報を取り扱う従業者および当該従業者が取り扱う個人情報の範囲を明確化し、個人情報保護法に違反している事実又は兆候を把握した場合の個人情報保護管理責任者への報告連絡体制を整備しているほか、個人情報の取扱状況について、各部門では自己点検を実施するとともに、本社監査部門による監査を実施している。

人的管理策としては個人情報の取扱いに関する留意事項について、従業者に適切な方法で教育を実施するほか、個人情報についての秘密保持に関する事項を就業規則に記載している。

物理的管理策としては、個人情報を取り扱う区域において、従業者の入退室管理および持ち込む機器等の制限を行うとともに、権限を有しない者による個人情報の閲覧を防止する措置を実施している。また、個人情報を取り扱う機器、電子媒体および書類等の盗難又は紛失等を防止するための措置を講じるとともに、当該機器、電子媒体等を持ち運ぶ場合、容易に個人情報が判明しないよう措置を実施している。

技術的管理策としては、アクセス制御を実施して、担当者および取り扱う個人情報データベース等の範囲を限定しているほか、個人情報を取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入している。

c）日立製作所

日立製作所は同社を中心とした日立グループの中核企業であり、総合電機メーカーとして情報・通信システム、マルチメディア関連機器、家電品、電子デバイス、電力・エネルギーシステム、環境・公共システム、産業機器などの製品・サービスを取り扱っている [415]。

414 https://www.khi.co.jp/sustainability/governance/security.html

415 https://www.hitachi.co.jp/recruit/newgraduate/company/businessfield.html

なお、日立製作所とはヒアリング調査を実施しており、具体的な情報保全措置や安全保障技術推進制度における取り組み等についても併せて記載する。

■　選定理由

ヒアリング対象企業であり安全保障技術研究推進制度（多義的技術）採択実績から、同制度での情報保全に向けた対応状況等について多くの情報を得られることが期待できるため。

日立製作所については安全保障技術推進制度のプログラム参加者に対してヒアリングを実施した。

■　参加している研究開発プログラム

本調査の対象となった研究開発プログラムでは、日立製作所は安全保障技術研究推進制度に参加している。

令和 3 年度公募において研究代表者所属機関として、分担研究機関の公的機関 1 機関とともに、タイプ S（大規模研究課題）に採択された。研究課題名は「環境制御観察における超高感度 3D 電磁場顕微鏡法の開発」であり、電池などの項効率化・低コスト化の鍵となるガス中・液中環境下における反応メカニズム解明のため、電子顕微鏡による高感度電磁場計測技術を発展させる研究開発を実施している[416]。

■　情報保全体制

情報セキュリティおよび個人情報保護の実施・運用に関する責任・権限をもつ情報セキュリティ統括責任者である ChiefInformation Security Officer （CISO）は、日立製作所のすべての製品・サービスや社内設備を対象に情報セキュリティを推進する役割を担う。

情報セキュリティと個人情報保護に関する取り組み方針、各種施策は、CISO を委員長とする「情報セキュリティ委員会」が決定し、「情報セキュリティ推進委員会」などを通じて、各事業所およびグループ会社に伝達される体制となっている。

その下でビジネスユニット（BU）・事業所は、情報セキュリティ推進部署を設置し、原則 BU 長・事業所長を情報セキュリティ責任者として、各職場における情報セキュリティの徹底や従業員への教育などを行い、グループ会社でも同様の組織を設け、互いに連携している（図 4.1-41）[417]。

[416] https://www.mod.go.jp/atla/funding/kadai/r03kadai.pdf

[417] https://www.hitachi.co.jp/sustainability/download/pdf/ja_sustainability2023_31.pdf

図 4.1-41　日立製作所の情報セキュリティ推進体制

■　　情報保全措置

組織的管理策については、国際規格である ISO／IEC 27001 を元に、情報セキュリティマネジメントを構築している。また、昨今のサイバー攻撃の激化を鑑み、NIST SP800-171 に対応した「情報セキュリティ対策基準」により、情報セキュリティの強化を実施している。同基準を含めた、「情報セキュリティ・個人情報保護関連規則」を日立製作所および各グループ会社の本社からグローバルに展開している。

またサプライチェーンにおいて調達先からの情報漏えいを防止するために、機密情報を取り扱う業務を委託する際には、あらかじめ日立が定めた情報セキュリティ要求基準に基づき、調達パートナーの情報セキュリティ対策状況を確認・審査している。さらに、調達パートナーに対して、情報機器内の業務情報点検ツールとセキュリティ教材を提供し、個人所有の情報機器に対して業務情報の点検・削除を要請している。

人的管理策として、すべての役員および従業員を対象に、情報セキュリティおよび個人情報保護について、e ラーニングによる教育を毎年実施している。その他新入社員、新任管理職や情報システム管理者などを対象とした座学教育など、対象別・目的別に教育プログラムを用意し、情報セキュリティ教育を実施している。また、標的型攻撃メールなどのサイバー攻撃に対する教育として、実際に攻撃メールを装った模擬メールを従業員に送付し、受信体験を通してセキュリティ感度を高める「標的型攻撃メール模擬訓練」を実施している。

防衛分野等の研究開発においては、連携機関に海外のポストドクターが参加する場合、事前に防衛装備庁等へ報告をし、セキュリティ上問題がないかを確認しつつ研究開発を実施している。

情報漏洩防止に向けた技術的対策として、デバイス暗号化、セキュリティ PC、電子ドキュメントのアクセス制御／失効処理ソフト、認証基盤の構築による ID 管理とアクセス制御、メールや Web サイトのフィルタリングシステムなどを IT 共通施策として実施している。標

的型攻撃メールなどのサイバー攻撃に対しては、官民連携による情報共有に加え、多層防御などの IT 対策を実施している[418]。

d）日本電気

日本電気は住友グループに属する総合電機メーカーであり、システム・インテグレーション（システム構築、コンサルティング）、サポート（保守）、アウトソーシング・クラウドサービス、システム機器、ソフトウェア・サービス等の「IT サービス事業」とネットワークインフラ、通信事業者向けソフトウェア・サービスと航空宇宙防衛等の「社会インフラ事業」の 2 つの事業領域を主として、ヘルスケア・ライフサイエンス事業等を展開している[419]。

なお、日本電気とはヒアリング調査を実施しており、具体的な情報保全措置や安全保障技術推進制度における取り組み等についても併せて記載する。

■　選定理由

ヒアリング対象企業であり安全保障技術研究推進制度（多義的技術）採択実績から、同制度での情報保全に向けた対応状況等について多くの情報を得られることが期待できるため。

日本電気については安全保障技術推進制度のプログラム参加者に対してヒアリングを実施した。

■　参加している研究開発プログラム

本調査の対象となった研究開発プログラムでは、日立製作所は安全保障技術研究推進制度に参加している。

令和 3 年度公募において研究代表者所属機関として、分担研究機関の公的機関、企業 2 機関とともに、タイプ S（大規模研究課題）に採択された。研究課題名は「ナノチューブネットワーク制御による新規赤外線検出素子の研究」であり、半導体型カーボンナノチューブと負熱膨張剤を用いた新たな赤外線検出デバイスに向けた研究開発を実施した[420]。

■　情報保全体制

日本電気グループの情報セキュリティ推進体制は、情報セキュリティ戦略会議と下部組織、各関連組織で構成される。情報セキュリティ戦略会議は CISO が議長を務め、情報セキュリティ施策の審議・評価・改善、事故の原因究明と再発防止策の方向付け、情報セキュリティビジネスへの成果活用などを審議する。

CISO を補佐するコーポレート・エグゼティブ（Co.EX）は、サイバーセキュリティ対策を推進する CISO 統括オフィスと、サイバー攻撃を監視しインシデント時には迅速に収拾をはかる CSIRT を統括する。情報セキュリティ推進会議やワーキンググループは、セキュア開発・運用の推進計画、実行施策討議・調整、指示事項徹底、施策進捗管理などを行う。

各組織の情報セキュリティ管理責任者は、所管するグループ会社も含め情報セキュリテ

418 https://www.hitachi.co.jp/sustainability/download/pdf/ja_sustainability2023_31.pdf

419 https://jpn.nec.com/profile/corp/outline.html

420 https://www.mod.go.jp/atla/funding/kadai/r03kadai.pdf

ィの確保に責任を負い、組織内へルールの周知徹底、施策の導入・運用、実施状況の点検・見直し・改善などを継続的に実施している（図 4.1-42）[421]。

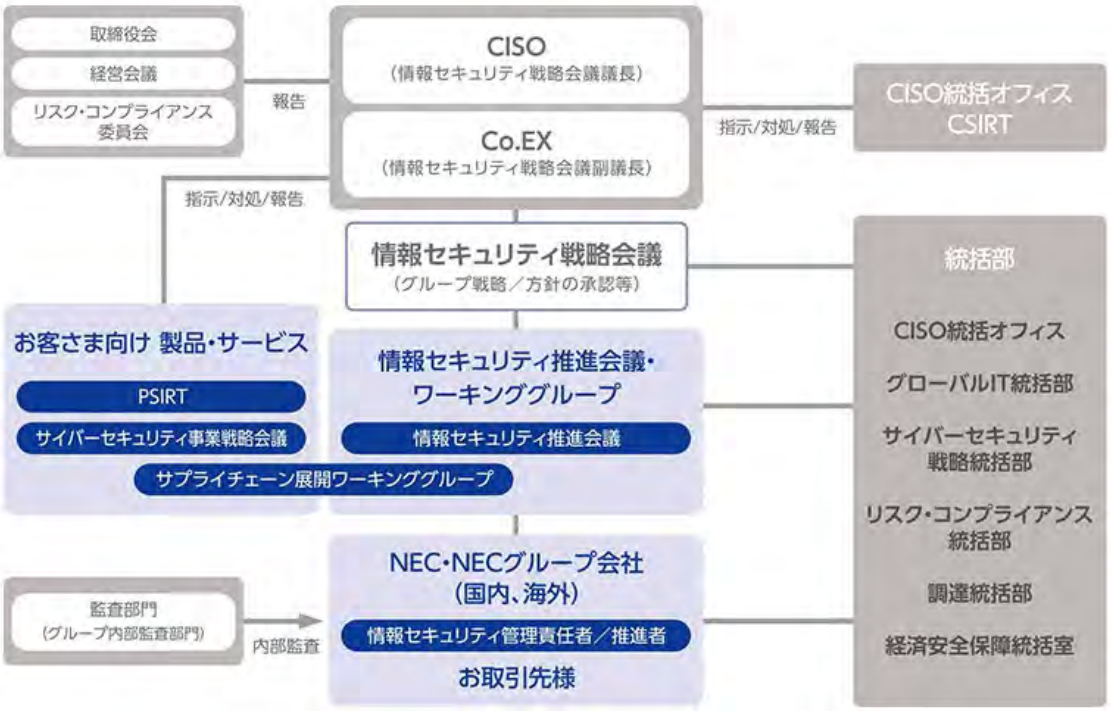


図 4.1-42　日本電気グループの情報セキュリティ体制

■　　情報保全措置

組織的管理策では、まず「NEC グループ情報セキュリティ基本方針」を公開し、情報セキュリティの基本規程、情報管理に関する規程、IT セキュリティに関する規程などを体系化している。取り扱う企業秘密を秘密区分によって分類して管理し、内部の各組織では、当該組織で取り扱う情報を細分化し、どのような情報がどの秘密区分に該当するのかを明確にして、重要な情報に対して、その重要度に応じた取り扱い・保管管理を定めており、情報漏えい対策を実施している。また、取引先と連携する際、その情報セキュリティ水準が、日本電気の定める水準に達していることを重視し、取引先の情報セキュリティ対策状況により情報セキュリティレベルを分類し、適切なレベルの取引先へ委託する仕組みを取り入れている。

人的管理策として、全社員を対象に、情報セキュリティと個人情報保護に関するウェブベースの教育を実施し、情報セキュリティの知識やスキルの向上を図っているほか、顧客情報や個人情報、企業秘密を扱う際に遵守すべき事項を定め、全社員に誓約させている。

技術的管理策として、ゼロトラスト成熟度モデル（CISA)をベンチマークとしてアイデンティティ、デバイス、ネットワーク、アプリケーション、データの 5 つの軸に沿って以下のようなセキュリティ対策を実施している [422]。

[421] https://jpn.nec.com/profile/governance/security.html

[422] https://jpn.nec.com/sustainability/ja/security/index.html

（日本電気で実施されている技術的管理策）

【アイデンティティ】

- ユーザ ID やパスワードに加え、組織情報、役職情報などのアクセス制御情報があり、業務システムなどへのアクセスを個人単位で認証・認可して制御
- 各社が管理する認証・認可に用いる情報が、どのシステムでどのような目的に利用されるのかを一元管理
- 重要情報を扱うシステムでは、ユーザ ID とパスワード（知識認証）に加え、電子証明書による個人認証（所有物認証）や顔認証（生体認証）を活用した多要素認証の導入を推進

【デバイス】

- 「暗号化」「デバイス制御」「ログの記録」を実施し、外部からの攻撃や内部不正による情報漏えいリスクへの対策を実施
- 暗号化：記憶装置とファイルを暗号化し、盗難・紛失による情報漏えいを防止。ファイル暗号化は、アクセス権や利用期限を設けた一定のセキュリティレベルを NEC グループ全体でデフォルト設定
- デバイス制御：USB メモリや SD カード、CD、DVD など外部記憶媒体や、スマートフォン、Bluetooth、赤外線など通信デバイスに対して、情報書き出しの禁止制限を実施。業務上デバイスの利用が必要な場合は、組織や利用者ごとにデバイスおよび機能制限を定義し、必要最小限の利用にとどめる
- ログの記録：社内 PC の操作ログをすべて記録。万が一、情報漏えい事故が発生した場合、ログの分析・解析により、事故による影響範囲の特定や状況把握、再発防止策の策定を実施。重要度の高いシステムには脆弱性情報の収集・対処、ログ管理、ネットワーク保護、認証、アクセス制御、特権管理、セキュア運用・保守手順、運用・保守作業チェック、セキュリティ設定、入退室管理、委託先管理などのセキュリティ対策を実施

【ネットワーク】

イントラネットワーク内のセグメンテーションとグローバルでの集中制御により、「未然防御」・「緊急遮断」・「ログ取得範囲の拡大」を実施し、セキュリティを強化

【アプリケーション】

- 社内で使用するクラウドサービス上のログを、監視・分析することで、重要なデータを取り扱うクラウドサービスに対する内部不正やサイバー攻撃への対策を実施
- 社内で使用されているクラウドサービスの利用状況を可視化し、未承認のリスクが高いクラウドサービスを監視

【データ】

- ファイル単位の自動分類・暗号化やトラッキング、アクセス権管理などを実施
- 極秘事項に該当する情報を安全に管理するインフラとして、セキュアストレージを導入

e）QPS 研究所

QPS 研究所は 2013 年に創業した九州大学発の宇宙工学ベンチャーで、人工衛星、人工衛星搭載機器、精密機器、電子機器、地上設備、ソフトウェア及び情報通信ネットワークの研

究開発、設計、製造、販売、運用、管理及び保守等に従事している[423]。

QPS 研究所は情報セキュリティ基本方針[424]を会社 HP で公表しており、QPS 研究所が管理する全ての業務活動に関わる情報資産を対象範囲とした情報セキュリティ方針を定めている。なお、QPS 研究所とはヒアリングを実施しており、具体的な情報保全体制や措置の実態についてはヒアリング結果に基づいて以下に記載する。

■　選定理由

ヒアリング対象企業であり情報セキュリティ基本方針が公表されており、情報保全に対して意識していることが確認できる他、宇宙関連の研究開発を行うベンチャー企業の中でも比較的歴史ある（2005 年創業）ため、どのような経緯で情報保全体制を構築してきたのか等が確認できるとの期待があるため。

また、安全保障技術研究推進制度（多義的技術）採択実績から、同制度での情報保全に向けた対応状況等について多くの情報を得られることが期待できるため、同プログラム参加者に対してヒアリングを実施した。

■　参加している主な研究開発プログラム

- 令和４年度小型 SAR 衛星コンステレーションの利用拡大に向けた実証（内閣府）
- 中小企業イノベーション創出推進事業　衛星リモートセンシングビジネス高度化実証（経済産業省）

■　**情報保全体制**

公開情報からは情報保全体制に関する情報は確認できなかった。

■　**情報保全措置**

公開情報からは情報保全措置に関する情報は確認できなかった。

423 https://i-qps.net/

424 https://i-qps.net/security-policy/

(2) 米国

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関および同機関の主催している研究開発プログラムをそれぞれ計5機関、8件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細はAppendix 2）参照)。

そしてリストアップした資金配分機関および研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、および国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、および独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして5件抽出した（表 4.1-33)。

表 4.1-33 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連領域	主催している研究開発プログラム
DARPA	海洋 サイバー バイオ 多義的技術	**海洋**：Ocean of Things **サイバー**：Cyber-Hunting at Scale(CHASE) **バイオ**：Fieldable Solutions for Hemorrhage with bio-Artificial Resuscitation Products (FSHARP) **多義的技術**：Joint University Microelectronics Program 2.0 (JUMP2.0)
NASA	宇宙	NextSTEP-2(Next Space Technologies for Exploration Partnerships)

1）資金配分機関における情報取扱に係る詳細調査結果

a）DARPA（DoD）

■　研究開発領域

宇宙、海洋、サイバー、バイオ、多義的技術

■　適用範囲

情報管理に関して、DoD では DoDI、DoDM（DoD Manuals）で主に以下のような内部規則が設定されている。

（DARPA、DoD の情報管理に関する内部規則）
- DoDM 5200.01（DoD 情報セキュリティプログラム）（1 巻-4 巻）[425, 426]
- DoDI 5220.31（国家産業安全保障プログラム）[427]
- DoDM 5220.32（国家産業安全保障プログラム）（1 巻-2 巻）[428, 429]

「DoDM 5200.01（DoD 情報セキュリティプログラム)」において、情報については以下のように定義されている。

（DoDM 5200.01 における情報の定義）

物理的な形態や特性にかかわらず、米国政府が所有し、米国政府のために作成され、または米国政府の管理下にある、伝達可能な知識または文書資料

（DoDM 5200.01 における適用範囲）
- OSD（Office of the Secretary of Defense：国防長官室）、軍部、統合参謀本部議長室および統合幕僚監部、戦闘司令部、国防総省監察総監部、国防省諸機関、国防総省現地活動部、および国防総省内のその他すべての組織体（以下、総称して「国防総省構成機関」という。）
- SCI は、DNI（Director of National Intelligence：国家情報長官）または DNI が発行した方針に従って情報コミュニティの各要素の責任者の既存の権限および責任を変更するものではない。SCI は、DoDM 5105.21 の第 1 巻から第 3 巻およびその他の適用可能なガイダンスにより実施される、DNI により発行された方針および手続に従って保護されるものとする。

■　情報の分類

「DoDM 5200.01（DoD 情報セキュリティプログラム)」において、情報の分類について以下のような方針が定められている。

425 https://www.esd.whs.mil/directives/issuances/dodm/

426 https://www.dodig.mil/Portals/48/Documents/Policy/520001_vol4.pdf

427 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/522031p.PDF?ver=mDTRtDQ3xsRpUKhwXp82Fg%3d%3d

428 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522032v1.PDF?ver=1BFNVqOKXaqdXcO618H-yg%3D%3D

429 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522032v2.PDF?ver=6r6Wq0aBhS44uQvw8Vne_w%3D%3D

(DoDM 5200.01 の情報分類に関する方針)

【分類方針】

- 情報は、国家安全保障を守るためにのみ機密扱いとする。情報を分類する必要性に重大な疑義がある場合、その情報は分類されないものとする。不必要または必要以上の分類は、禁止されている。情報は、分類する資格がなくなり次第、機密解除される。
- 分類は、米国政府によって所有され、米国政府のために作成され、又は米国政府の管理下にある情報にのみ適用することができる。情報は、その不正な開示が国家安全保障に識別可能または記述可能な損害を与えることが合理的に予想され、かつ、E.O.13526 の 1.4 節に規定されている以下のようなカテゴリーのいずれかに関係する場合に限り、分類の対象とみなすことができる
  - 軍事計画、兵器システム、または作戦
  - FGI(foreign government information：外国政府情報)
  - 諜報活動、諜報源または諜報方法、または暗号学
  - 機密情報源を含む、米国の外交関係または対外活動
  - 国家の安全保障に関わる科学的、技術的、経済的事項
  - 核物質または核施設を保護するための米国政府のプログラム
  - 国家安全保障に関連するシステム、施設、インフラ、プロジェクト、計画、または保護サービスの脆弱性または能力
  - 大量破壊兵器の開発、製造、使用)
- E.O.13526 または前任の命令に基づいて分類レベルを割り当てられた情報は、その他の必要な表示が省略されているにもかかわらず、その分類レベルで分類されたものとみなされる

【分類の禁止】

- 情報は、以下の目的で機密扱いされたり、機密扱いとして維持され続けたり、機密扱いを解除されなかったりしてはならない
  - 法律違反、非効率、または管理上の誤りを隠す
  - 個人、組織、または機関が恥をかくことを防ぐ
  - 競争を抑制する
  - 国家安全保障の利益のために保護を必要としない情報の公開を防止または遅延させる
- 基礎科学研究およびその結果は、明らかに国家安全保障に関連する場合を除き、機密扱いとすることはできない

【分類のレベル】

- 国家安全保障のために不正な開示から保護する必要があると特定された情報は、極秘、秘密、または機密に分類されるものとする。法令に別段の定めがある場合を除き、米国の機密情報を識別するために他の用語を使用してはならない
  - 最高機密(Top Secret)：OCA[430]が特定または説明できる、国家安全保障に例外的に重大な損害を与えることが合理的に予想される情報の不正開示に適用されるもの

[430] 大統領、副大統領、または大統領により指名された省庁の長もしくはその他の職員により、情報を最初に分類する権限を書面で付与された個人。

とする。

- 機密(Secret)：OCA が特定または説明できる、国家安全保障に重大な損害を与えることが合理的に予想される情報に適用される。
- 秘密(Confidential)：不正な開示により国家安全保障に損害を与えることが合理的に予想され、かつ OCA が特定または説明できる情報に適用される。

■ 情報管理策

DARPA の内部規則で情報の組織的・人的・技術的管理策について定めているのは確認できなかった。しかし、DARPA は DoD の部局であるため、国防総省の情報管理に関する規則・ガイドラインに従っていると考えられる。

「DoDI 5220.31（国家産業安全保障プログラム)」、「DoDM5220.32（国家産業安全保障プログラム)」は、「32CFR part117(NISPOM)」に基づいて作成された DoD の内部規則である。これらの規則の中で情報管理については主に以下のような規定がされている。

（DARPA、DoD の内部規則における情報管理策）

・ 組織的管理策

【DoDM 5200.01】

- 機密情報へのアクセス
  a. アクセス要件：以下の場合に限り、機密情報へのアクセスが許可されるものとする
     (1) 有効かつ適切なセキュリティ・クリアランスを保有していること
     (2) 適切な秘密保持契約を締結していること
     (3) 合法的かつ認可された政府機能を遂行するために、情報を知る正当な必要性がある場合
- 緊急時計画火災、自然災害、内乱、テロ活動、または敵対行為が発生した場合に、機密情報を保護、除去、または破壊し、漏洩のリスクを最小限に抑え、また、そのような事態が発生した後に、必要に応じて機密情報を回復するための計画を策定しなければならない。これらの計画の詳細レベル、テストおよびリハーサルの量は、情報を危険にさらす可能性のある敵対行為、外国情報による脅威、自然災害、またはテロ活動のリスクを評価することによって決定されるものとする
  a. COMSEC（communication security：機密通信セキュリティ）資料の緊急保護計画を策定する場合は、CNSS（Committee on National Security Systems：国家安全保障システム委員会）教令 4004 の要件を使用する
  b. 緊急時計画を作成する際には、次のことを考慮する
     (1) 手持ちの機密資料の量を減らす
     (2) 使用頻度の低い機密資料を他の安全な場所に保管する
     (3) オフサイト保管のため、電子形式で情報の定期的なバックアップコピーを作成する
     (4) 保持されている機密情報を可能な限りリムーバブルな電子メディアに移す
- 個人が機密情報および機密資料（IT 機器や関連する記憶媒体など）を自宅で持ち出し作業することがミッション・クリティカルである場合、特定のセキュリティ対策と承認が必要となる。適切な保護と徹底したセキュリティを提供し、無権限者によるアク

セスを防止するために、分類レベルに適したセキュリティ対策が実施されていなければならない

・ 人的管理策

【DoDM 5200.01】

- 国防総省の各部局の長は、その要員が以下のようなセキュリティ教育・訓練を受けることを確保しなければならない
  - a. セキュリティ機能の質の高い遂行を可能にするために必要な知識と情報を提供
  - b. 国防総省の情報セキュリティプログラムの方針と要件、および国家安全保障と国益にとってのその重要性の理解を促進する
  - c. セキュリティ要件に対する継続的な意識を植え付け、維持する
  - d. プログラム目標を支える高いモチベーションの促進を支援する
- セキュリティ教育とトレーニング・リソース
  - a. 安全保障教育と訓練は、国防総省内にプログラムを設けるか、国防安全保障サービス・アカデミーのような外部の資源を利用するか、あるいはその二つを組み合わせて行うことができる
  - b. 国防総省の各部門は、必要であれば、本マニュアルの第 4 巻に規定されている CUI に関する要件と、本書で規定されている教育・訓練要件を、1 つの全体的なプログラムに統合することができる
- 国防総省の文民、軍属、現場支援請負業者を含む組織の全職員は、国防総省情報セキュリティプログラムに関する初期オリエンテーションを受けるものとする
  - a. この初回オリエンテーションの目的は以下の通りである
    - (1) 機密情報と CUI を定義し、そのような情報を保護することの重要性を説明
    - (2) セキュリティポリシーと原則を基本的に理解する
    - (3) 職員に、セキュリティプログラムにおける各自の責任を通知し、適切な場合に適用される行政的、民事的、および／または刑事的制裁について知らせる
    - (4) 個人が所有する機密情報や CUI を適切に保護するための十分な情報を提供する。これには、そのような情報が保護されていないことが発見された場合、セキュリティの脆弱性が指摘された場合、またはそのような情報を求めている人物がいた場合に取るべき行動も含まれる
    - (5) 一般に公開される前に、国防総省のすべての非機密情報を確認する必要性を職員に知らせる
  - b. また、セキュリティ教育者は、初回オリエンテーションに、国防総省の上級機関職員および活動セキュリティ管理担当者の特定、その責任の説明および機密情報又は管理されている非分類の情報の保護に関与するか否かを含めることを検討しなければならない。初回オリエンテーションに含まれていない場合、当該情報は、本項.c.で要求される訓練に含まれなければならない
  - c. 本項 a および b の要件に加え、機密情報に最初にアクセスする際には、すべての要員は、セキュリティ方針および原則、並びに派生的な分類の慣行に関する研修を受けるものとする

【DoDM 5220.32】

- クリアランスの資格判定を受ける資格があるのは、米国市民のみである。非米国市民による特定の限定された機密情報へのアクセスを承認するやむを得ない理由が存在する場合がある。国防総省の CAF（Consolidated Adjudications Facility：統合裁定室）

は、その非米国市民が特定の USG の契約をサポートするために緊急に必要とされる、独特または異常な技能または専門知識を持ち、クリアまたはクリア可能な米国市民が存在せず、調査要件が満たされているような稀な状況において、契約社員に対して SECRET レベルまでの LAA(limited access authorization：限定アクセス許可)を許可することができる。LAA のための PSI は、DoDM 5200.02 に従って実施される。LAA に対するクリアされた請負業者の要請は、NISPOM に従って、担当の GCA を通じて国防総省の CAF に提出される

- LAA を付与された個人は、以下へのアクセスは許可されない
  (1) TOP SECRET 情報
  (2) RD(Restricted Data：制限データ)または FRD(Formerly Restricted Data：旧制限データ)
  (3) 米国政府指定の開示機関から、その個人が国籍を有する国への開示が承認されていない情報
  (4) COMSEC 情報
  (5) 諜報情報。ICD(Intelligence Community Directive:情報コミュニティ指令)704 に従い、SCI アクセス候補者は米国市民でなければならず、DNI または指名された者のみがこの要件を免除することができる
  (6) ただし、以下の場合を除く:NATO 加盟国の外国籍の者は、DSS (Defense Security Service：防衛警備局)がその者の本国から NATO のセキュリティ・クリアランス証明書を取得すれば、契約条件に従い NATO 情報へのアクセスを許可される。NATO へのアクセスは特定の NATO 契約の履行に限定される
  (7) 外国への開示の全部または一部が禁止されている情報
  (8) 第三者政府から米国政府に秘密扱いで提供された情報、および第三者政府から提供された機密情報
- 国防総省の CAF は、請負業者の従業員に対し、与えられた職務を遂行する上で機密情報へのアクセス資格の正当な要件があることを請負業者が国防総省に証明し、適切な人事安全調査が完了し、国防総省の CAF によって有利な裁定が下された後にのみ、資格を付与する。国防部審理・上訴局(Defense Office of Hearings and Appeals：DOHA)は、付随レベルで理由書を発行された請負業者従業員について、最終的に適格性の決定を行う。NISPOM に記載されているように、請負業者が従業員にアクセスできるようになる前に、DoD が付与した適格性が発生しなければならない
- GCA(Government Contracting Activities：政府契約活動)は、以下の場合を除き、請負業者従業員に機密情報へのアクセスを提供しない
  (1) 会社は、機密情報のレベルに応じた適切な FCL (Facility Security Clearance：施設クリアランス) を有している
  (2) 承認された国防総省の人事安全記録システムにおいて、その個人に適切なレベルの機密情報へのアクセス資格が米国政府から付与されている
  (3) 請負業者の従業員が与えられた職務を遂行する上で、機密情報にアクセスする正当な要件がある
  (4) 請負業者の従業員が SF(STANDARD FORM：標準書式)312「機密情報秘密保持契約」を実行した
- 請負業者要員は、雇用する請負業者の全体的な FCL よりも高いレベルの機密情報へのアクセスを許可されない

・　物理的管理策

【DoDM 5200.01】

- 保管庫から取り出された場合の保護権限を与えられた者は、保管場所から取り出された機密文書を常時監視下に置かなければならない。機密文書のカバーシート（SF703「最高機密（カバーシート）」、SF704「機密（カバーシート）」または SF705「機密（カバーシート）」）は、安全な保管場所にない機密文書に貼付されなければならない。カバーシートには、該当する分類レベルを、色やその他のすぐに認識できる書式や凡例で示す。
- 終業時のセキュリティチェック機密情報を処理又は保管する活動の責任者は、機密報が使用又は保管される区域が安全であることを確実にするため、各勤務および／または営業日の終了時に、セキュリティ・チェックのシステムを確立しなければならない。このようなチェックの記録には、SF701「活動セキュリティ・チェックリスト」を使用する。セキュリティ・チェック・システムの不可欠な部分は、機密情報の保管に使用されるすべての保管庫、安全な部屋、コンテナの安全確保である。SF702「セキュリティ・コンテナ・チェックシート」は、このような行為を記録するために使用されるものとする。SF701 および SF702 は、各部門の記録管理スケジュールに従って保管および廃棄されるものとする。

【DoDM 5220.32】

- 請負業者が機密情報を受領する前に、コンテナ保管能力を承認すること
- 機密情報の保管に使用する前に付随的な閉鎖区域又は保管庫を承認すること
- DSS は、DSS が定める所定の資格基準を満たす請負業者の職員に、追加の閉鎖区域または保管庫の承認権限を委任することができる。DSS は常に監督と最終承認の権限を保持する
- NISPOM に従い、閉鎖区域における機密文書のオープン棚またはビン保管の請負業者の要求を承認または不承認とする。請負業者による TOP SECRET 情報のオープン棚またはビン保管は許可されない

【DoDI 1035.01】

・　DoDI 1035.01（テレワーク・リモートワーク）は 5 U.S.C. chapter65（テレワーク）に基づいて DoD 内のリモートワークについて規定した規則であり、被雇用者または軍属が以下の不適格な非行により公式に懲戒処分を受けた場合、上司はテレワークを制限しなければならないと規定している。

・　年間 5 日以上の無断欠席

・　政府のコンピュータ上で、または連邦政府の職務遂行中に、ポルノを閲覧、ダウンロード、交換すること

■　所管する主なプログラムと情報取扱規程

・　プログラム名称「Cyber-Hunting at Scale(CHASE)」

【研究領域】サイバー

【概要】4.1.1（2）1）c）参照

【参加資格】

DARPA は、基本的に、学界（大学)、企業（大企業、中小企業、不利な立場にある小企業

など)、その他の組織（非営利団体を含む)、事業体（外国、国内、政府)、FFRDC、少数民族機関、その他を含む、政府のニーズを満たすことができる責任あるすべての情報源からの参加を歓迎する方針を採用しているが、以下のようなFFRDC、政府機関、海外からの参加については以下のような条件が付与される。

（Cyber-Hunting at Scale(CHASE)におけるFFRDC、政府機関、海外機関の参加制限）
【FFRDC】
- FFRDCは、適用される直接競争の制限の対象となり、以下の条件を満たさない限り、いかなる立場においても本プログラムに提案することはできない。FFRDCは、政府の募集に提案し、産業界と競争する資格を確立する具体的な権限、および関連するFFRDCスポンサー契約の条件を遵守していることを示す、スポンサー組織からの公式レターヘッドの書簡を提出しなければならない

【政府機関】
- 政府機関（政府／国立研究所、軍教育機関など）は、適用される直接競争の制限に従う。政府機関は、その業務が他の民間部門から入手できないことを明確に証明し、政府の募集に提案する能力を立証する特定の法令上の権限および契約上の権限（関連する場合）を引用する文書を提出しなければならない

【海外からの参加】
- 米国外の組織および／または個人は、その参加者が必要な秘密保持契約、セキュリティ規制、輸出管理法、および状況に応じて適用されるその他の管理法令を遵守する限りにおいて、参加することができる

また、本プログラムでは、基本的に取り扱うテーマは非機密とされているが、5つある分野で以下のような事項が求められている。

（Cyber-Hunting at Scale(CHASE)で参加にあたり求められる事項）
- 提案書提出時に、TA1、TA2、TA4の全ての提案者は、Top Secretのクリアランスを有し、SCIへのアクセス資格を有するチームメンバーを少なくとも1名擁していなければならない。
- 各TAに提案される研究責任者は、そのレベルのクリアランスを有していることが望ましい（必須ではない）。全てのTA5要員は、Top Secretのクリアランスを有し、SCIアクセス資格を有するべきである。
- CHASEは、非機密プログラムであり、学術と中小企業の参加が明確に奨励されているCHASEの技術開発は、非機密レベルで行われる。セキュリティ・クリアランスの要件は、すべてのTA1、TA2、TA4チームに適用されるが、チーム内の全ての人員に適用されるわけではない。

【情報の取扱い規定】

本プログラムでは、提案者が機密資格を提示するための資料が機密提出資料とされており、提案者は、その書類にE.O.13526に定義されている機密情報が含まれているの考え、資料を取り扱わなければならないと記載がある。

また、提案を提出する際には、以下のようなガイドラインが提供する機密情報の提出、分

類、取り扱いおよびマーキング等のガイダンスに従う必要があるとされている。

(Cyber-Hunting at Scale(CHASE)で準拠すべき法令等①) ・ DoDM 5200.01Sup.1（DoD 情報セキュリティプログラム）（第 1 巻～第 4 巻） ・ DoD 5220.22-M（国家産業安全保障プログラム） ・ DoD 5220.22-M Sup1（国家産業安全保障プログラム）

また提案者が厳密な基礎研究を行っている場合を除いて、以下を遵守しなければならないとしている。

(Cyber-Hunting at Scale(CHASE)で準拠すべき法令等②) ➢ DFARS 252.204-7000（情報の開示） ➢ DFARS 252.204-7008（対象となる防衛情報の保護管理の遵守） ➢ DFARS 252.204-7012（対象となる防衛情報の保護およびサイバーインシデントの報告） ・ これらの要件を遵守するためには NIST SP800-171 で指定されたセキュリティ要件を実施することが義務付けられている。

b）NASA

■ 研究開発領域

宇宙

■ 適用範囲

情報の取扱いに関する規定について、NASA では以下の NPD（NASA Policy Directive）や NPR（NASA Procedural Requirements）のような内部規則が定められている。

(NASA の情報取り扱いに関する内部規則) ・ NPD 2810.1F（NASA 情報セキュリティポリシー）[431] ・ NPD 1600.1（NASA セキュリティプログラム手続き要件）[432] ・ NPR 2810.1F（情報および情報システムのセキュリティ）[433] ・ NPR 2810.7（管理された未分類情報(CUI)）[434]

「NPD 2810.1F（NASA 情報セキュリティポリシー)」の中で、情報の取扱いについて機密・非機密を問わず、全ての NASA の情報と情報システムは、国家安全保障上の分類レベル、機密性、価値、重要性に見合った方法で保護するとしている。

また本ポリシーでは情報は以下のように定義され、また、情報セキュリティの適用範囲については以下のように規定されている。

[431] https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2810&s=1E

[432] https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_1600_001A_&page_name=main

[433] https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=2810&s=1A

[434] https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_2810_0007_&page_name=main

（NPD 2810.1F における情報の定義、情報セキュリティの適用範囲）

【情報の定義】

・ 物理的な形態や特性に関係なく伝達可能なあらゆる知識で、NASA が所有し、NASA が製作し、NASA のために製作され、または NASA の管理下にあるもの。

【情報セキュリティの適用範囲】

・ この NPD は、NASA 本部および NASA センター（コンポーネント施設、技術・サービス支援センターを含む）に適用される。この文言は、ジェット推進研究所（JPL）、連邦資金による研究開発センター、その他の請負業者、補助金受領者、または契約当事者に、契約、補助金、または契約で指定または参照されている範囲に限り適用される
・ 本 NPD は、NASA のプロジェクト、プログラム、およびミッションを支援する際の、情報システムのすべての NASA ユーザ（公務員および請負業者など）に適用される

■ 情報管理策

NASA の「NPR 2810.1F（情報および情報システムのセキュリティ）」、「NPR 2810.7（管理された未分類情報(CUI)）」で情報管理策については以下のように規定されている。

（NASA の内部規則における情報管理策）

・ 組織的管理策

【NPR 2810.1F】

- SAISO(Senior Agency Information Security Officer：上級情報セキュリティ責任者)は以下を行うものとする
  - a. NASA 全体のサイバーセキュリティ・プライバシープログラムを策定し、文書化する。このプログラムには、概要と成果の測定方法、企業情報セキュリティ・アーキテクチャ、重要インフラ、リスク管理戦略、情報セキュリティ評価と認可のプロセスが含まれる
  - b.情報セキュリティ文書のための NASA 全体のリポジトリを提供する
  - c.NASA Cybersecurity and Privacy Program を見直し、更新し、強化する
  - d. NASA サイバーセキュリティ・プライバシープログラムの計画、方針および要求事項が実施されるようにする
  - e.少なくとも年１回更新されるサイバーセキュリティ仕様書を通じて、組織として定義された価値を更新し、普及させる
  - f.行動計画とマイルストーンの策定、文書化、維持およびリスク受容のためのプロセスを定義する
  - g.非機密情報システムに関しては、NASA による NIST リスクマネジメントフレームワークの実施を確保する責任を負う
- 情報システム所有者(Information System Owner：ISO)は、b で要求される NASA 全体の情報セキュリティ文書リポジトリにおいて、情報セキュリティ文書を維持するものとする

【NPR 2810.7】

- NASA は、以下の場合に限り、CUI を普及させ、CUI へのアクセスを許可する

a. CUI のカテゴリを定めた法律、規制、または政府全体の方針に従うこと
b. 合法的な政府目的を促進すること
c. CUI エグゼクティブ・エージェンシーによって設定された、許可された限定的な配布コントロールによって制限されていないこと
d. その他法律で禁止されていないこと

- 特定の個人、機関、または組織への CUI の普及を制限するために使用できるのは、CUI レジストリに公開されている LDCM（limited dissemination controls：限定的普及コントロール）のみである。これらの普及コントロールは、合法的な政府目的を促進する場合、または法律、規制、あるいは政府全体の方針がその使用を要求または許可する場合にのみ使用することができる。
- LDCM の例には、以下が含まれる：
  a. 外国への配布禁止
  b. 連邦職員のみ、
  c. 連邦職員および請負業者のみ
  d. 請負業者への配布禁止
  e. 配布管理リスト
  f. 特定の国民にのみ公開が許可されている
  g. 表示のみ
- 組織は、個人、事務所または組織へのアクセスを制限する必要がある場合、配布リスト管理指定を使用することが要求される
- NASA は、CUI へのアクセスを違法または不当に制限する管理を課してはならない
- 外国人招聘研究者のような外国の組織と情報共有契約または取り決めを締結する場合、要員は、当該組織が E.O.13556、32CFR pt.2002 および CUI 登録簿に従って CUI を保護するよう促すべきである。
- CUI プログラムの確立前に締結された情報共有契約は、CUI プログラムの要件に抵触しないよう、可能な限り修正されなければならない
- 非執行部門との情報共有協定には、CUI プログラムに従った CUI の取扱いに関する条項を含める。非執行部門および権限を与えられた CUI 保有者は、CUI 基本情報および CUI 特定情報の区別、並びにそれぞれのマーキングおよび取扱い手順を熟知していなければならない。
- 非執行部門は、本規則の要求事項および今後の FAR 条項による CUI レジストリを遵守して CUI を取り扱う責任がある。この規則の非執行部組織への適用は、新たな潜在的責任を課すものである。非執行部門による CUI の誤用は、法律、規則、または政府全体の方針で定められた罰則の対象となり、取り扱い要件に対するあらゆる不適合は CUI PM(Program/Project Manager)に報告される。NASA が指定機関でない場合、要員はいかなる違反も指定機関に報告する

・ 人的管理策

【NPR 2810.1F】

- 全ての NASA 職員は、その職位に要求される役割に基づく訓練活動を完了するものとする
- SAISO は以下を行うものとする
  a. NASA 全体の情報セキュリティ意識と訓練を開発し、維持し、推進する

b. NASA 全体の情報セキュリティ意識およびトレーニングの要件を定義し、利用 可能にする。これには、NASA の全ユーザに関係する一般的な知識要件と、管理者、情報セキュリティ専門家、その他を対象とする役割ベースの要件が含まれる

c. 省庁の情報セキュリティ意識向上とトレーニングの要件を満たすために使用できる教育コースと教材を定義する

d. 機関全体および外部の利害関係者に対するトレーニング要件の履行を監督するこれには、機関の記録システムにおける情報セキュリティ意識向上およびトレーニング要件の完了の追跡と報告が含まれる

e. NASA ユーザ行動規範を維持し、ユーザの年次受諾を追跡する

- ISO は以下を行うものとする

  a. すべての情報セキュリティ意識およびトレーニング要件を遵守するユーザにのみ、情報システムへのアクセスを許可する

  b.重要な情報セキュリティ責任または昇格特権を役割に含む情報システムをサポートするすべての要員が、役割ベースの情報セキュリティ意識向上およびトレーニング要件 に準拠していることを確認する

- NASA ユーザは、以下を行うものとする

  役割ベースの情報セキュリティおよび意識向上のためのトレーニング要件に従う

- 人的資本最高責任者室の次長補佐は、研修の実施、研修結果および研修記録の管理のための NASA 全体のプラットフォームが利用可能であることを保証するものとする

【NPR 2810.7】

- 特定の CUI を扱う NASA 職員は、本ポリシーに記載されていることに加え、基本的な法律、規制、または政府全体のポリシーに概説されている保護基準を遵守するものとする

・ 物理的管理策

【NPR 2810.1F】

- CIO(Chief Information Officer：最高情報責任者)は、センターセキュリティ責任者およびセンター施設組織と協力し、各センターの情報システムに対して物理的および環境的な管理が満たされていることを確認するものとする
- ISO は以下を行うものとする

  a. セキュリティで保護された、または制限された物理的情報システム施設および場所への要員のアクセスを承認する

  b. セキュリティで保護された、または制限された物理的な情報システム施設および場所へのアクセスを許可されたすべての要員のリストを作成し、維持する

  c. 物理的・環境的セキュリティ管理および監視能力を検証する

【NPR 2810.7】

- CUI レジストリで異なる保護が指定されていない限り、CUI を含む物理的文書は、無人の場合、施錠されたオフィス、施錠された引き出し、または施錠されたファイルキャビネットに保管される。
- CUI を扱う NASA の職員は、CUI を所持、輸送、保管、使用、または処理する合法的な政府目的を持たない無許可の使用者または他者に CUI をさらさないように注意するものとする。カバーシートは、文書の上に置いてもよく、その内容を不用意に見られ

ないようにする。職員は、使用中はカバーシートを使用して CUI 文書を保護することができるが、使用しないときは、CUI 文書を机の引き出し、ファイルキャビネット、事務室などの施錠された場所に保管する。その他の予防措置には、以下のものが含まれる

a. NASA の職員は、権限のない個人が CUI にアクセスしたり、CUI を観察したり、CUI が話し合われている会話を立ち聞きしたりできないことを合理的に確保する

b. CUI は、管理された環境に保管されるべきである。管理された環境とは、権限のある保有者が、不正なアクセスや開示から CUI を保護するための適切な物理的または手続き上の管理があると判断した場所または空間と定義される

c. 作業場所の管理された環境から CUI を除去する必要がある場合（テレワーク、公用旅行など）、NASA の要員は、CUI を常に直接管理下に置くか、少なくとも 1 つの物理的バリア（カバーシートなど）で保護し、自分自身または物理的バリアが CUI を不正アクセスまたは観察から保護することを合理的に確保するものとする

- 旅行中は、あらゆる合理的な手段（例えば、安全な伝送、承認された電子 USB、またはリスクを軽減し、公式の出張中に CUI を携帯する必要性を制限するその他の承認された方法）が取られる。CUI が他人の目に触れる可能性のある公共交通機関内では、CUI を閲覧しない。ホテルの部屋では、CUI を使用しないときは、鍵付きのブリーフケースまたは部屋の金庫に保管する。CUI は、封筒、ブリーフケース、またはその他の方法で見えないように覆われている場合に限り、施錠された自動車内に保管することができる

・ 技術的管理策

【NPR 2810.1F】

- ISO は次のことを行うものとする

a. 接続先の情報システムへのリモートアクセスが許可され、承認されたデバイスのみに、組織の定義した価値観に合致した方法でリモートアクセスが許可されるようにする

b. すべてのリモートアクセスが、CIO により承認されたリモートアクセスポイントを経由することを保証する。

- プログラム管理者およびプロジェクト管理者は、その管理下にあるプログラム又はプロジェクトの情報システムに関して、すべてのリモートアクセスが NASA の認可されたアクセス制御ポイントを経由することを保証するものとする
- NASA ユーザは以下を行うものとする

a. NASA 非公開情報システムへのリモートアクセスには、NASA が認定し承認したデバイスのみを使用する

b. リモートで使用する情報および情報システムの機密性、完全性、可用性を確保し、誤った取り扱いの結果を理解するために、あらゆる合理的な努力を払う

- ISO は、その情報システムに保存され、送信され、または処理される情報が、NIST が承認した暗号化アルゴリズムに従って実行される暗号化によって保護されることを保証するものとする
- 暗号化を使用することが技術的に不可能であるか、またはシステムがそれぞれの使命、機能、または運用を遂行する能力に明らかに影響を及ぼす場合には、認可担当者が運用認可の付与を検討する前に、CIO から書面による承認を得るものとする

- NASA ユーザは、アクセス制限および／またはサニタイゼーションを用いて、自己の管理下にある媒体を安全に保護するものとする
- ISO は、その管理下にある情報が、輸送中に適切な暗号化により保護されることを保証しなければならない
- CIO は、NASA の共通システムおよび通信インフラストラクチャについて、NASA が適切なデータ漏えい防止策を策定し、実施し、維持することを確保するものとする
- SAISO は、共通のインフラまたはサービスを共有するシステムに対して、センタ・レベルのバウンダリ・プロテクションが提供されることを保証するものとする
- CIO は、自センターにおけるシステムおよび通信要件をサポートするために必要なソフトウェアおよびハードウェアの統合を確保するものとする
- ISO は、共有リソースポリシー、サービス拒否保護、境界保護および伝送の完全性および機密性が 実施されていることを保証するものとする

・ その他

【NPR8000.4C】

- 「NPR8000.4C（エージェンシーのリスク管理手続き要件）」は NASA におけるリスクマネジメントについて定めたものであり、プログラムやプロジェクトにおけるリスク管理要件を規定しているものであり、この規程に基づいて、「NASA Risk Management Handbook」が作成されている [435], [436]
- NASA では、リスク管理について RIDM(Risk Informed Disition Making：リスク情報に基づく意思決定)と CRM(Continuous Risk Management：継続的リスク管理)という 2 つのプロセスを 1 つ枠組みに統合しリスク管理を実施している
- RIDM はアーキテクチャや設計の決定、メークバイの決定、主要な調達における調達先の選定、予算の再配分（予備費の配分）といった重要な意思決定の際に発動されるもので、CRM は設計、計画、プロセスの実施に伴うリスクを管理するための具体的なプロセスである、RIDM の発動後、定義されたパフォーマンス要求の達成に向けて適用される

【NPR3600.2B】

- NPR3600.2B（NASA テレワークプログラム）は 5 U.S.C. Chapter65（テレワーク）に基づいて NASA 内のリモートワークについて規定した規則であり、参加要件について、職員は以下の例外を除きテレワークに参加資格があるとされている [437]
- 機密扱いの資料を定期的に取り扱う職務
- 従業員が、代替勤務地では実施できない現場での活動を日常的に行っている
- 暦年で 5 日を超える無断欠勤により、正式に懲戒処分を受けたことがある
- 連邦政府のコンピュータ上で、または連邦政府の公務遂行中に、児童ポルノを含むポルノグラフィを閲覧、ダウンロード、または交換したことで、「行政府職員の倫理的行動基準」のサブパート G に違反したとして正式に懲戒処分を受けたことがある

【NPD1600.1】

- NASA のセキュリティ要件に関連する規制または命令に故意に違反した、違反を試み

435 https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8000&s=4C

436 https://www.nasa.gov/wp-content/uploads/2023/08/nasa-risk-mgmt-handbook.pdf

437 https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=3600&s=2B

た、または違反を共謀した者は、18 U.S.C.§799 に基づく解雇および/または起訴の可能性を含む懲戒処分の対象となるとされている。

■　所管する主なプログラムと情報取扱規程

・ プログラム名称「NextSTEP-2(Next Space Technologies for Exploration Partnerships)」

【研究領域】宇宙

【概要】4.1.1 (2) 1) c) 参照

【参加資格】

NASA では外国機関との研究における基本的な方針は「資金を交換することなく米国以外の団体と研究を実施すること」であり、NextSTEP-2 においても、参加は、教育機関、産業界、非営利団体、NASA センター、その他の政府機関など、米国内外のあらゆるカテゴリーの組織に門戸が開かれている。研究責任者（PI）は、大学、連邦政府の研究所、民間企業、州および地方政府の研究所、 その他の国の研究者と共同研究を行うことができるとの記載があるが、以下の 3 つの場合は応募資格に制限が課されるとの記載がある。

（NextSTEP-2 における参加制限）

・ 米国内の機関等の提案に参加する国際チームメンバー
  - 明確な科学的利益またはコスト削減を示す国際共同研究は奨励されており、米国内に機関等の提案については海外チームメンバー、下請業者、または供給業者を含めることは可能
  - 米国外の機関等による研究開発活動の支援には使用することはできない(米国内の機関等による米国外からの研究とはならない供給品やサービスの直接購入は可能)
  - 米国市民ではないが、米国の機関に雇用されているか、米国の機関に留学している主任研究者や大学院生を含むその他のチームメンバーは、この BAA を通じて研究活動を支援するための資金を受け取ることが可能

・ 米国外の機関等からの提案
  - 米国外の機関等の提案には米国の機関等との共同研究を伴う必要あり
  - 米国外の機関等からの提案および米国外の機関等を含む米国内の機関等からの提案では、米国外の機関等は提案等する国の政府機関、または資金提供・スポンサー機関による承認が必要
  - 米国外の機関等からの提案については全て英語で記入されている必要がある

・ 中国に対する制限
  - 提案には資金が提供されるか、または資金交換のない取り決めの下で実行されるかに関わらず、中国または中国が所有する企業または団体との二国間参加、協力、または調整を含んではならない
  - 二国間関与が資金提供または資金交換なしの取り決めの下で行われるかに関わらず、主たる受領者レベルおよび全ての準受領者レベルにおいても中国または中国所有の企業と二国間で参加、協力、または調整するためのいかなる種類の助成金または協力協定を締結または資金提供することを制限されている

- 定義「中国または中国系企業」とは、中華人民共和国、中華人民共和国が所有する企業、または中華人民共和国の法律に基づいて設立された企業
- 制限は、補助金または協力契約の履行に必要な営利目的の供給品目には適用されない
- 提案書の提出により、申請者は中国または中国系企業ではないこと、また、二国間関与が資金提供または資金交換のない取り決めの下で行われるか否かにかかわらず、主たる受領者レベルまたは準受領者レベルにおいて、中国または中国系企業との二国間関与、協力、調整を行わないことを表明する必要がある

【情報の取扱い規定】

本プログラムにおける情報保全で具体的な遵守が求められる法令等の規定については、輸出管理で遵守すべき法令である EAR、ITAR 以外は確認することができなかったが、NASA のプログラムであるため、NASA の内部規定に従うものであると考えられる。

また、NASA は、NASA に研究提案書または研究プロジェクト計画書を提出する全ての研究者に対して、最終的な研究データを管理し、アクセスできるようにするための DMP(Data Management Plan：データ管理計画)を含めるか、データを一般に公開できない、または公開する必要がない理由を述べることを義務付けている。

2）研究開発実施主体における情報取り扱い実態の調査

情報保全ポリシーの公開されていない民間企業等については机上調査で情報取り扱い実態を把握することが困難であるため、ヒアリングによる調査結果を整理した。政府機関については公開されている内部規則や上位規則についての調査結果を整理した。

a）BAE Systems Inc.

BAE Systems Inc.は、英国に本社に置く国際的な防衛、航空宇宙、セキュリティ企業である「BAE Systems」の子会社で、米国の他、英国、スウェーデンにも拠点を持っている。BAE Systems, Inc.は、空軍、陸軍、海軍向けの幅広い製品とサービス、高度なエレクトロニクス、セキュリティ、情報技術ソリューション、カスタマーサポートサービスを提供している[438]。

■　参加している研究開発プログラム

BAE Systems Inc.は、2018年にDARPAのプログラムである「Cyber-Hunting at Scale (CHASE)」にPerspecta Labsとともに採択されている。このプロジェクトでは、新しい攻撃ベクトルを検出して特徴付け、適切なコンテキストデータを収集し、企業内および企業間で保護対策を広めるための自動化ツールの開発を行っている。上記プログラム以外にもDARPAのプログラムに参加している[439, 440, 441]。

■　情報保全体制

不明

■　情報保全措置

BAE Systemsは、情報セキュリティの標準規格であるISO27001等を取得している他、サプライヤーと共有する情報がサイバー攻撃等により漏えいすることを防ぐために DFARS やNIST SP800-171に準拠したセキュリティ対策に取り組んでいる[442, 443]。

BAE Systemsは、輸出管理についても厳格なコンプライアンス要件を設けており、サプライヤーに対してメディア検索、年次報告書、現地視察等を行い、当社が取引を禁止されている企業や個人を特定するためのデューデリジェンスを実施し、関係者にどのようなリスクがあるのかについて評価を行う。このデューデリジェンスはサプライヤーとの契約期間中、積極的に行われている。

---

438 https://www.baesystems.com/en-us/our-company

439 https://www.baesystems.com/en/article/bae-systems-to-develop-automated-cyber-defense-tools-for-darpa

440 https://militaryembedded.com/cyber/cybersecurity/darpa-signs-4-7-millin-cyberhunting-contract-with-perspecta-labs

441 https://www.baesystems.com/en/article/bae-systems-selected-by-darpa-to-progress-revolutionary-aircraft-design-and-testing

442 https://www.baesystems.com/en/digital/about-us/global-recognition/industry-standards-and-bodies

443 https://www.baesystems.com/en-us/our-company/sustainability/governance

BAE Systems はサプライヤーに対して責任ある取引原則に基づき、以下のような質問をしてそのリスク評価を行っている[444]。

（サプライヤーのリスク評価のための 6 つの重要な質問）

- **主要サプライヤーは、BAE システムズ社と同等の行動規範または責任ある取引方針を有しているか**
- **調達する製品またはサービスは、その製造、保管、配備、使用、廃棄において合理的に必要な以上の、持続的で重大な環境または健康への悪影響をもたらすか**
- **調達する製品またはサービスは、BAE システムズの製品安全ポリシーに適合しているか**
- **調達する製品やサービスにはどのような輸出規制が適用され、適切な通関手続きやライセンスが行われているか、または計画されているか**
- **この製品やサービスの生産が、市民の自由や人権を侵害する可能性はあるか**
- **調達する製品は、予見可能な将来に法規制や禁止される可能性があるか**

b）ジョージア工科大学

ジョージア工科大学は、米国ジョージア州アトランタに所在する州立大学であり、1885 年に設置された。米国内でもトップクラスの工科系大学として「航空宇宙工学」「応用物理学」「コンピュータ工学」等多くの研究を実施している[445]。

■　参加している研究開発プログラム

ジョージア工科大学は、米国政府の資金提供プログラムとしては、DARPA の JUMP2.0 プログラム（Joint University Microelectronics Program 2.0）に参加している。

JUMP2.0 は、情報通信技術における米国の進歩を加速させるために様々な電子システムの性能、効率、機能を大幅に向上させることを目指しているプログラムであり、ジョージア工科大学はそのプログラムの 7 つあるテーマ内、「認知：次世代 AI のシステムとアーキテクチャ」「行動のためのインテリジェント・センシング：センシング機能と組み込み知能による迅速かつ効率的な行動生成」の 2 つのテーマに取り組んでいる[446]。

■　情報保全体制

情報管理については、ジョージア工科大学の OIT（Office of Information Technology：情報技術局）で推進されており、CIO（Chief Information Officer：最高情報責任者）の下で統治されている。OIT は、情報技術のリーダーシップとサポートを提供し、学術部門やビジネスユニットと協力して、主要な研究大学固有のニーズを満たし、学生、教職員、および研究者をサポートするために、企業全体の情報技術および電気通信サービスの主要なソースとして機能している。

444 https://www.baesystems.com/en/sustainability/governance/oversight/policy-summaries/security-policy

445 https://www.gatech.edu/about

446 https://www.darpa.mil/news-events/2023-01-04

■　情報保全措置[447]

ジョージア工科大学では、情報の管理について、データガバナンスと管理方針、管理された未分類情報、サイバーセキュリティ方針、パスワードポリシー等で遵守すべき事項がまとめられている[448]。

ジョージア工科大学で取り扱うデータに関しては以下の事項が規定されている。

（ジョージア工科大学におけるデータ取り扱いの規程）

【データの分類】

- データガバナンスと管理方針に基づき、ジョージア工科大学で取り扱う全てのデータ（組織データ）については「公開」か「保護」のデータ保護カテゴリーに分類される

区分	内容
Public（公開）	一般利用を目的とした情報。例えば、一般閲覧用のウェブサイトコンテンツや、公表されたプレスリリースなど。
Protected（保護）	ジョージア工科大学コミュニティ以外の関係者が情報を一般的に入手することはできない。これは組織データのデフォルトの「データ保護分類」である。「保護」の分類は、そこに含まれるデータが常に機密または非開示であることを意味するものではなく、そのようなデータは、ジョージア州公開記録法またはその他の適用される法律および規制の下で開示の対象となる可能性がある。

【データガバナンスと管理方針】

- CISO(Chief Information Security Officer：最高情報セキュリティ責任者)によって任命されたジョージア工科大学のサイバーセキュリティ担当者は、情報の機密性、完全性、および可用性を保護するために、組織データの保存、使用、および配布のための安全な環境を促進するポリシー、ガイドライン、手順、およびリソースを作成する必要がある
- いかなるインターフェイス（ユーザセルフサービスを除く）を介した情報システムへのアクセスも、データユーザ、該当する各データドメインの関連データスチュワード、およびデータ管理者を通じて調整および検討されなければならない
- 情報システムへのアクセスは、追加的な承認（データ利用者の上司など）を必要とする場合もあれば、事前に承認された役割ベースの権限によってアクセスを許可する場合もある
- アクセスは「最小特権の原則」に基づいて付与され、本来意図された目的にのみ使用され、承認を受けた個々のデータ利用者のみが使用しなければならない
- アクセスが許可される前に、データ管理者および／又はシステム所有者による追加的なトレーニングが要求される場合がある
- 人事部は、従業員が解雇された場合、または従業員の地位が変更され、組織データおよび情報システムに対する当該従業員のアクセスを変更する必要が生じた場合には、データスチュワードおよびデータ管理者に通知しなければならない
- アクセスは、データガバナンス委員会により決定された頻度で、定期的にレビューされ、検証されなければならない

447 https://www.dorbit.space/downloads/security-policy.pdf

448 https://policylibrary.gatech.edu/information-technology

- ジョージア工科大学の全ユニットは、組織データの機密性、完全性、可用性が失われるリスクを低減するために、組織構造、職務、業務プロセスに適切な職務分掌システムが含まれていることを確認しなければならない

【サイバーセキュリティ方針】

- 利用者は、自分がアクセスする全てのデータおよびITリソースのセキュリティを保護する責任がある。これには、ジョージア工科大学のITリソースにアクセスするために使用される個人所有のデバイスに適切なセキュリティ対策を実施することも含まれる
- 全ての利用者は、ジョージア工科大学サイバーセキュリティが公表しているセキュリティ手順と基準に従わなければならない。これには、「ジョージア工科大学保護データ慣行」も含まれます
- 利用者は、インスティテュートパスワードポリシーに従って、自身のアカウントとパスワードを安全に管理しなければならない
- 研究者は、自己の行動に対して全責任を負い、研究活動がジョージア工科大学の他のITリソースやユーザに悪影響を及ぼさないように、適切な予防措置を講じなければならない

【パスワードポリシー】

- 単一要素認証(パスワード認証) または多要素認証(パスワードとトークン)を使用して、データアクセスポリシーおよびデータ保護標準で定義されている一意のログオンを必要とするシステムまたはアプリケーションに対する認証を行う必要がある
- ジョージア工科大学のアカウントユーザは、パスワードとアカウントを保護するためにあらゆる合理的な措置を講じる必要がある
- ジョージア工科大学のユーザは、サードパーティのサービスプロバイダー(Googleなど)を含む誰ともアカウントのパスワードを共有してはならない
- 各ユーザは、そのユーザのアカウントとパスワードを使用して実行されたすべてのアクションに対して責任を負う
- アカウントへのアクセスを共有するビジネスニーズがある場合、そのような共有はシステム権限の委任によって実現する必要がある
- 単一要素パスワード構成標準は、以下の条件を満たす必要がある

  - 11文字以上を含む
  - 次の4つの文字クラスのうち少なくとも3つの文字を含む
    - 大文字の英字(例: A-Z)
    - 小文字の英字(例: a-z)
    - 数値(例: 0-9)
    - 特殊文字(例: .,!@#$%~)
  - 120日ごとに期限切れ
  - 最後に選択した4つのパスワードと異なるパスワードである

- 多要素パスワード構成標準は、以下の条件を満たす必要がある。

  - 8文字以上を含む

- 次の 4 つの文字クラスのうち少なくとも 3 つの文字を含む。
  - 大文字の英字(例: A-Z)
  - 小文字の英字(例: a-z)
  - 数値(例: 0-9)
  - 特殊文字(例: .,!@#$%~)
- 365 日ごとに有効期限
- 最後に選択した 4 つのパスワードと異なるパスワードである

【管理された未分類情報】

- ジョージア工科大学は、CUI の使用に関連する連邦資金（政府から直接受け取るか、関連する契約や請負業者を通じて間接的に受け取るか）の受領を継続するために、CUI に関連するすべてのシステムとプロセスが NIST 800-171 に準拠していることを保証する義務がある
- CUI に関わるすべての活動は、NIST 800-171 基準に完全に準拠していなければならず、ジョージア工科大学システム・セキュリティ・プラン（GT SSP）に従う必要がある
- GT SSP からの逸脱には、CISO の承認が必要であり、CISO は、必要に応じて、研究または管理・財務に関連する上級副学長からの追加承認を求めます
- CUI を扱う環境は、サイバーセキュリティによる NIST 800-171 コンプライアンス評価を毎年受け、CISO または指名された者が署名した認証報告書を取得しなければならない
- 評価中に発見された不適合事項は、CUI との相互作用が許可される前に改善されなければならない
- CUI に関わる環境は、CUI に関わるサイバーインシデントを 72 時間以内に報告できるように運用されなければならない

c) CSIS

CSIS は、米国の外交政策及び国家安全保障に関連した問題に関する調査・研究を行うシンクタンクであり、1962 年にジョージタウン大学に設置された研究所を母体として、1982 年にワシントン D.C.を拠点に非営利組織として設立された。

世界の地域やトピックに焦点を当てたプログラムに沿って調査研究を実施しており、その範囲はアメリカ大陸、欧州、アジア、欧州、ロシア・ユーラシア、中東や、気候変動、サイバーセキュリティ、防衛・安全保障、食料安全保障、地政学、貿易、人道支援、人権、宇宙、核問題など多岐にわたる。

CSIS については、CSIS に出向している客員研究員に対してヒアリング調査を実施したことから、客員研究員から見た CSIS の情報保全体制及び措置について調査結果を踏まえて以下に記載する。

■ 情報保全体制

公開情報からは情報保全体制に関する情報は確認できなかった。

■　　情報保全措置

公開情報からは情報保全措置に関する情報は確認できなかった。

(3) カナダ

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計 6 機関、9 件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細は Appendix 2）参照)。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして 6 件抽出した（表 4.1-34)。

表 4.1-34 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連分野	主催している研究開発プログラム
国防省（Department of National Defence)	多義的技術	・ Innovation for Defence Excellence and Security (IDEaS) - Innovation Networks: Micro-nets
カナダ国防研究開発：(DRDC:Defense Research and Development Canada)	多義的技術	・ Blood Biomarkers for Crush Injury/Crush Syndrome
カナダ宇宙庁（Canadian Space Agency)	宇宙	・ Terrestrial Snow Mass Mission - Phase 0
水産海洋省（DFO、Department of Fisheries and Oceans)	海洋	・ Oceans Management Contribution Program による船舶交通データシステムの開発支援
カナダ公衆衛生庁（PHAC：Public Health Agency of Canada)	バイオ	・ Stabilized Whole Blood Product
Shared Services Canada（SSC)	サイバー	・ TBIPS-SA: C.1 Strategic IT Security Planning and Protection Consultant, Level 3

1）資金配分機関における情報取扱に係る詳細調査結果

a）国防総省（DND）

■　研究開発領域

多義的技術

■　適用範囲

・　DAOD 6001-0, Information Management[449]

国防省の従業員とカナダ軍の将校及び下士官（CAF メンバー）を対象として、情報資産（情報の本体を効果的に理解、共有、保護、活用できるように単一の単位として定義・管理される情報の本体）、図書館資料、情報アーキテクチャ（データコンポーネントの構造、相互関係などを規定する原則・ガイドライン）などの情報管理の方法を示している。

■　情報の分類

・　DAOD 6001-0, Information Management

管理の対象となる情報についての記載はあるが、それらの情報の分類については記載されていなかった。

■　情報管理策

・　DAOD 6001-0, Information Management

国防省の従業員と CAF メンバーに対して以下を実施することが求められている。

（DND における情報管理策）
- 国防省の従業員と CAF メンバー、請負業者、国防省と協力して業務を遂行している者は Information Management（以下 IM）のトレーニングを受ける
- IM スペシャリスト（常勤の情報管理責任者等）は IM トレーニングの支援を行う
- 国防省および CAF メンバーから常勤の情報管理責任者を選任する
- 関連性、信頼性、品質管理、費用対効果、運用上のニーズを考慮した情報の管理を行う
- 意思決定においては文書化を行い、評価・監査・レビューができるようにする

■　所管する主なプログラムと情報取扱規程

・　Innovation for Defence Excellence and Security (IDEaS) - Innovation Networks: Micro-nets[450]

【研究領域】サイバー、多義的技術

[449] https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/6000-series/6001/6001-0-information-management.html

[450] https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/innovation-networks/challenge/defence-applications-of-quantum-technologies/defence-applications-of-quantum-technologies-guide2023.html

【概要】

持続可能な研究ネットワークの構築には時間がかかることを踏まえ、イノベーション・ネットワークは、科学技術に関する課題の 1 つまたは複数の側面について研究を行う小規模なネットワーク（マイクロネット）の創設を支援するための提案募集を行っている。マイクロネットとは、少なくとも 3 つの適格な組織・機関からなる学際的なチームであり、共通の関心を持つ科学技術課題の側面について学際的な研究を行う取組である。

【参加資格】

- カナダの大学がプロジェクトへの申請者かつ助成金の最初の受領者になる必要がある
- 学際的な研究チームが支援の対象。研究者の主な所属は、少なくとも 3 つの別々の機関、組織である必要がある。対象となる機関、組織は以下の通り
  - カナダで設立された大学および教育機関
  - 営利目的の法人組織
  - 非営利法人
  - 州・準州・市町村政府機関
  - 海外大学及び教育機関
  - すべての組織・機関は、資金提供契約を締結するために必要な法的地位を有していること

【情報取扱規程】

情報公開法第 20 項（１）（ｂ）に準拠する必要がある。

（IDEaS - Innovation Networks: Micro-nets で準拠すべき情報公開法の規程）
・ 政府機関（DND など）は、第三者から政府機関に提供された機密情報であり、第三者によって一貫して機密として扱われている金融、商業、科学、技術情報を含む、同法に基づいて要求された記録の開示を拒否しなければならない
・ 第一に、DND に提供された申請者の文書には、財務、商業、科学または技術情報が含まれていなければならない。第二に、申請者はそのような情報を一貫して秘密扱いしなければならない。言い換えれば、DND は、申請者が自らの事業所において当該機密情報を保護するのと同様に、DND が保有する申請者の機密情報を保護する

個人情報保護法または情報公開法に基づいて行われた個人情報保護請求または情報公開請求が完了した場合、その請求に回答した日から 2 年間保管する。2 年間の保存期間終了後、プライバシーまたは情報公開請求ファイルは破棄される必要がある。また本プロジェクトから生じるすべての知的財産権は、採択者に帰属する。

b）カナダ国防研究開発：(DRDC)

■　研究開発領域

多義的技術

■　適用範囲

公開されている資料からは、DRDC において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[451]。

しかし、情報アクセス法やプライバシー法に基づく年次報告書を作成しており、これらの法令に従った管理をしていることが示されている[452]。

■　情報の分類

公開されている資料からは、機密性・完全性・可用性などの観点から DRDC において取り扱われる情報を分類している規程等は確認できなかった[453]。

しかし、情報アクセス法やプライバシー法に基づく年次報告書の中に、担当事務局にてこれら法令に準拠して活動を行っていることを管理監督している旨が示されている[454]。

■　情報管理策

公開されている資料からは、DRDC において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった 。

しかし、情報アクセス法やプライバシー法に基づく年次報告書の中に、担当事務局にて情報の管理と保護を行うためのポリシーや手順を従業員に公開する等の支援を実施している旨が示されており、一定の規定に従い情報の取扱がなされていると思料される 。

■　所管する主なプログラムと情報取扱規程

・　Blood Biomarkers for Crush Injury/Crush Syndrome[455]

【研究領域】バイオ、多義的技術

【概要】

挫滅損傷・クラッシュシンドロームの適切かつ迅速な診断につながる血液のバイオマーカー分析を行うプログラム。

【参加資格】

生化学、分子生物学、バイオテクノロジー、細胞生物学、または免疫学のいずれかの学士以上の学位、および検証された方法を使用して少量の生物学的サンプルの分析経験があること。

---

451 https://www.canada.ca/en/department-national-defence/corporate/transparency.html

452 https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/audit-privacy-protection-personal-information.html

453 https://www.canada.ca/en/department-national-defence/corporate/transparency.html

454 https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/audit-privacy-protection-personal-information.html

455 https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-edm-002-10005

【情報取扱規程】

本プログラム特有の情報取扱い規定はないが、the Standard Acquisition Clauses and Conditions Manual に従って請負業者はデータ侵害（第三者が所有する記録、データ、または情報への不正アクセスまたは不正開示につながるセキュリティまたは機密保持義務の違反に起因するカナダへのすべての損害）について全責任を負う旨が記載されている。加えて、知的財産権の侵害についても全責任を負うことも記載されている。

c）カナダ宇宙庁（Canadian Space Agency）

■　研究開発領域

宇宙

■　適用範囲

・　Scientific Integrity Policy（SIP）[456]

CSA の研究、科学、または関連活動を設計、実施、伝達、管理、レビューまたは利用する CSA 職員に適用される。またその活動を支援するサービスを提供する請負業者や協力者にも SIP は通知され、その規定と意図に従うことが奨励される。

■　情報の分類

・　Scientific Integrity Policy（SIP）

研究成果の開示が免除される情報としては、the Access to Information Act または the Security of Information Act に基づいて開示が免除されると考えられる、機密あるいは機微扱いの研究または科学情報（Classified or sensitive research or scientific information）と定義されているが、具体的な分類については記載されていなかった。

■　情報管理策

・　Scientific Integrity Policy（SIP）

組織的管理策として、科学的完全性の原則や責任の所在を規定し、宇宙科学技術情報の保護と政府情報の積極的かつ継続的な公開を促す情報管理方針が示されている。

（カナダ宇宙庁における SIP に基づいた情報管理策）

【科学的完全性の原則の規定】

- **CSA の研究と科学、研究または科学製品および関連するあらゆるコミュニケーションの実施が、該当する知的財産権（特許、著作権、商標、工業意匠など）を遵守し、政治的、商業的、顧客および利害関係者の干渉を受けないことを保証する（6.2）**
- **開示を制限する明確かつ正当な理由がない場合は、CSA が作成した研究および科学情報は、政府のオープンガバメント指令に従い、適宜公開される（6.3）**
- **CSA 職員は、科学的完全性の原則へのいかなる違反についても、管理者、マネージャーまたは指定された職員に報告する（6.8）**

[456] https://www.asc-csa.gc.ca/eng/publications/scientific-integrity-policy/2020-01-29-scientific-integrity-policy.asp

【責任の所在の規定】
- 副長官（Deputy Head）：CSA 職員へのポリシーの浸透、準拠の監視および必要に応じた是正措置の実施、ポリシーのパフォーマンス評価および政府全体の科学的完全性政策の実施のためのガバナンス委員会（the Governance Committee for Implementation of Government-Wide Scientific Integrity Policy）への年次報告など、CSA において科学的完全性のサポートおよび侵害に関する情報を開示できるオープンなコミュニケーションの文化を促進する責任を負う（8）。科学的完全性に対する違反への対応責任者である CSA Science Integrity Lead を任命する（7.2.2.2）
- バイスプレジデント、局長、ディレクター、マネージャーおよび管理者：ポリシーの導入責任を負う。具体的な責任は、このポリシーに基づく手順とガイドラインに明記される（8）
- 研究、科学または関連活動を行う CSA 職員： ポリシーに基づく活動を行う。科学的完全性に対する違反の疑いが生じた場合は速やかに報告し、調査に協力する（8）

【通報者の保護】
- CSA は個人情報の保護に努め、職員が科学的完全性の侵害の申し立てや調査に協力できるようにするための安全策の提供に努める（7.2.2.4）
- 公務員が the Values and Ethics Code for the Public または the Canadian Space Agency Organizational Values and Ethics Code への重大な違反を示す可能性がある情報を持つ場合、通報者の保護を目的とする the Public Servants Disclosure Protection Act[457]に基づく手順を利用できる（7.2.2.5）

■ 所管する主なプログラムと情報取扱規程

・ Terrestrial Snow Mass Mission - Phase 0[458]

【研究領域】宇宙

【概要】

地上積雪水量の高分解能測定を実現するための開発計画を更新・改善することを目標としている。CoReH20 フェーズ 0 及びフェーズ A により装置開発、積雪についての特性評価・モデリングについて成果が得られたため、本プロジェクトにおいて高性能化を図ることが求められる。得られた成果は環境・気候変動省（ECCC：Environment and Climate Change Canada）の気象研究部門で活用される予定である。

【参加資格】

記載なし

【情報取扱規程】

本プログラム特有の情報取扱い規定はないが、入札情報として、①プロジェクトを実施するチームの組織図、下請け業者等の協業を行うチームメンバーの役割、②主要メンバーの履歴書、を提出する必要がある。

457 https://laws-lois.justice.gc.ca/eng/acts/p-31.9/

458 https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-18-00855778

提案から生じるフォアグラウンド知的財産の所有権はカナダ政府が保持する。また、中間・最終・ミッション要件レビューでの議題として知的財産が挙げられており、実施事業者はフォアグラウンド知的財産及びバックグラウンド知的財産についての一覧表を提出する必要がある。

d）水産海洋省(DFO)

■　研究開発領域

海洋

■　適用範囲

公開されている資料からは、DFO において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[459]。

しかし、情報アクセス法やプライバシー法に基づく年次報告書を作成しており、これらの法令に従った管理をしていることが示されている[460,461]。

■　情報の分類

公開されている資料からは、機密性・完全性・可用性などの観点から DFO において取り扱われる情報を分類している規程等は確認できなかった 。

しかし、情報アクセス法やプライバシー法に基づく年次報告書の中に、担当事務局にてこれら法令に準拠して活動を行っていることを管理監督している旨が示されている ，。

■　情報管理策

公開されている資料からは、DFO において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[462]。

しかし、情報アクセス法やプライバシー法に基づく年次報告書の中に、担当事務局にて記録のスキャン・アップロード、ファイル管理等の管理サポートを実施している旨が示されており、一定の規定に従い情報の取扱がなされていると思料される[463,464]。

■　所管する主なプログラムと情報取扱規程

・ Oceans Management Contribution Program による船舶交通データシステムの開発支援[465,466]

【研究領域】海洋

---

459 https://www.dfo-mpo.gc.ca/about-notre-sujet/publications/index-eng.htm

460 https://www.dfo-mpo.gc.ca/transparency-transparence/aia-lai-22-23-eng.html

461 https://www.dfo-mpo.gc.ca/transparency-transparence/pa-lprp-22-23-eng.htm

462 https://www.dfo-mpo.gc.ca/about-notre-sujet/publications/index-eng.htm

463 https://www.dfo-mpo.gc.ca/transparency-transparence/aia-lai-22-23-eng.html

464 https://www.dfo-mpo.gc.ca/transparency-transparence/pa-lprp-22-23-eng.htm

465 https://www.dfo-mpo.gc.ca/oceans/funding-financement/management-gestion/terms-conditions-modalites-programme/index-eng.html

466 https://www.canada.ca/en/fisheries-oceans/news/2023/06/funded-projects-for-the-oceans-management-contribution-program.html

【概要】
カナダの海洋保護目標の取り組みに助成金を提供する Oceans Management Contribution Program のひとつとして、ダルハウジー大学の船舶追跡データと地図の公開システム（AISviz）構築を支援するものである。

【参加資格】
参加資格として、①非営利団体（NPO）、②先住民組織、③研究・教育機関、④カナダ国籍の個人、⑤従業員数 500 人未満の中小企業、⑥高齢者や若者のグループ等の地域グループおよび⑦州、準州、地方自治体およびその機関、が挙げられている。

【情報取扱規程】
情報保全については、情報アクセス法（Access to Information Act）に準拠するように記載されている。
プログラムから生じるすべての知的財産権は委託機関に帰属する。ただし、かかる知的財産権の対象となる著作物を制作、出版、翻訳、複製、配布、翻案、または使用するための取消不能で非独占的なロイヤリティフリーのライセンスを大臣に付与するものとされている。

e）カナダ公衆衛生庁（Public Health Agency of Canada）

■　研究開発領域
バイオ

■　適用範囲
公開されている資料からは、PHAC において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[467]。
しかし、情報アクセス法やプライバシー法に基づく年次報告書を作成しており、これらの法令に従った管理をしていることが示されている[468]。

■　情報の分類
公開されている資料からは、機密性・完全性・可用性などの観点から PHAC において取り扱われる情報を分類している規程等は確認できなかった[469]。
しかし、情報アクセス法やプライバシー法に基づく年次報告書の中に、ATIP オペレーション部門にてこれら法令に準拠して活動を行っていることを管理監督している旨が示されている[470]。

---

467 https://www.canada.ca/en/public-health/corporate/mandate/about-agency/access-information-privacy.html
468 https://www.canada.ca/en/public-health/corporate/mandate/about-agency/access-information-privacy/access-information-privacy-annual-reports/2022-2023-access-information-privacy-act.html
469 https://www.canada.ca/en/public-health/corporate/mandate/about-agency/access-information-privacy.html
470 https://www.canada.ca/en/public-health/corporate/mandate/about-agency/access-information-priva

■　情報管理策

公開されている資料からは、PHAC において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[471]。

しかし、情報アクセス法やプライバシー法に基づく年次報告書の中に、担当部門にてプライバシーポリシーとプログラムのガイダンスを提供している旨が記載されており、一定の規定に従い情報の取扱がなされていると思料される[472]。

■　所管する主なプログラムと情報取扱規程

・ Stabilized Whole Blood Product[473]

【研究領域】バイオ

【概要】

HIV/AIDS に関連するカナダ公衆衛生庁の免疫学的品質評価および標準化 (QASI) 対策の一環として、保存培地中に安定化されたヒト赤血球および白血球を含む、分析済みの全血品質管理製品の調達を行っている。

【参加資格】

RFSO(The Request for Standing Offers)を提出する必要がある。RFSO の内容としては、①一般情報（人権・労働基準等）、②提案者指示書（RFSO の条項および条件に適用される情報）、③提案書作成指示書（指定された評価基準に対応する提案書）、④評価手順および選考基準への情報、⑤証明書、⑥契約条項、の 6 項目がある。

【情報取扱規程】

情報アクセス法(Access to Information Act, R.S.C. 1985, c. A-1)第 67.1 条、または州/準州レベルでの同等の条項に準拠するように記載されており、情報アクセス法によって規定されているアクセス権を妨害する目的で、記録を破壊、変更、改ざん、隠蔽する者、または誰かにそうするように指示する者を規定している。

f) Shared Services Canada

■　研究開発領域

サイバー

---

cy.html

471 https://www.canada.ca/en/public-health/corporate/mandate/about-agency/access-information-privacy.html

472 https://www.canada.ca/en/public-health/corporate/mandate/about-agency/access-information-privacy/access-information-privacy-annual-reports/2022-2023-access-information-privacy-act.html

473 https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-edm-002-10005

■　適用範囲

公開されている資料からは、SSC において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[474]。

しかし、セキュリティ評価に関する監査報告書が発行されており、SSC の IT システムおよびサービスにおけるセキュリティについては規定のセキュリティ要件が満たされていることが示されている[475]。

■　情報の分類

公開されている資料からは、機密性・完全性・可用性などの観点から SSC において取り扱われる情報を分類している規程等は確認できなかった[476]。

しかし、セキュリティ評価に関する監査報告書の中で SSC のセキュリティ標準について言及されており、この標準の中で情報分類についても言及されている可能性が思料される[477]。

■　情報管理策

公開されている資料からは、SSC において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[478]。

しかし、セキュリティ評価に関する監査報告書の中で SSC のセキュリティ標準とガイダンスについて言及されており、これら文書の中で情報管理策が規定されていると思料[479]。

■　所管する主なプログラムと情報取扱規程

・ TBIPS-SA: C.1 Strategic IT Security Planning and Protection Consultant, Level 3 [480]

【研究領域】サイバー

【概要】

SSC にて行われる SSC 変革プログラム・プロジェクトにおける非機密、機密、およびすべての指定領域における IT セキュリティ・サポートおよびサービス（サイバーセキュリティサブプログラム機能、IT セキュリティサービスサブプログラム、カナダ政府セキュリティインフラストラクチャ（GCSI）サブプログラム機能、エンタープライズセキュリティ要件の定義と統合サービス機能）を提供することを求めている。

---

474 https://www.canada.ca/en/shared-services/corporate/publications.html

475 https://www.canada.ca/en/shared-services/corporate/publications/audit-security-assessment-authorization-march-2020.html

476 https://www.canada.ca/en/shared-services/corporate/publications.html

477 https://www.canada.ca/en/shared-services/corporate/publications/audit-security-assessment-authorization-march-2020.html

478 https://www.canada.ca/en/shared-services/corporate/publications.html

479 https://www.canada.ca/en/shared-services/corporate/publications/audit-security-assessment-authorization-march-2020.html

480 https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/pw-18-00844238

【参加資格】

TBIPS (Task-based informatics professional services) [481] EN578-170432[482] Supply Arrangement Holders に従う必要があり、セキュリティ要件として、受託者は供給契約(SA : supply arrangements) 発行時に最低でも指定組織審査 (DOS : Designated Organization Screening) を受けていなければならない。

【情報取扱規程】

内容は公開されていないが、企業セキュリティ指定組織審査 (DOS : Designated Organization Screening)及びリソースセキュリティを満たす必要があるとされている。

[481] https://www.tpsgc-pwgsc.gc.ca/app-acq/sptb-tbps/index-eng.html

[482] https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/cb-8513-20829715

2）研究開発実施主体における情報取り扱い実態の調査

情報保全ポリシーの公開されていない民間企業等については机上調査で情報取り扱い実態を把握することが困難であるため、ヒアリングによる調査結果を整理した。政府機関については公開されている内部規則や上位規則についての調査結果を整理した。

a）ダルハウジー大学[483]

■　参加している研究開発プログラム

Oceans Management Contribution Program による船舶交通データシステムの開発支援

■　情報保全体制

特定の情報管理システムに対する管理責任を持つ個人として、データスチュワードが存在する。データスチュワードは、データの品質、アクセス、使用に関するポリシーとガイドラインを設定し、維持している。加えて、データアクセス委員会は、機関データへのアクセスに関する方針、プロトコル、ガイドラインの開発と監督を担当しており、データスチュワードの活動をサポートし、機関全体のデータ管理の一貫性を保証する役割を担っている。

■　情報保全措置

データスチュワードは、管理する情報管理システム内に保管されている機関データへのアクセス要求を評価している。このプロセスでは要求がポリシーとガイドラインに適合しているかどうかを検討し、適切と判断された場合に限りアクセスを承認し、不適切な場合は拒否する。

また各会計年度の終了後 90 日以内に、データスチュワードは前会計年度に行われたすべてのアクセス決定の要約を含む年次報告書をデータアクセス委員会に提出する必要がある。

[483] https://www.dal.ca/dept/university_secretariat/policies/information-management-and-technology/institutional-data-access-policy.html

（4）英国

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計 6 機関、10 件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細は Appendix 2）参照)。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして 6 件抽出した（表 4.1-35)。

表 4.1-35 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連領域	主催している主な研究開発プログラム
UKRI（Innovate UK、MRC、EPSRC）	宇宙、海洋、バイオ、サイバー	・ marine and maritime in the Great South West - R1 CR&D ・ China UK One Health research for epidemic preparedness and AMR ・ Quantum Technology Research Hubs
MoD（Dstl、DASA）	宇宙、海洋、サイバー、バイオ、多義的技術	・ The Defence Technology Exploitation Programme[484] ・ Space to Innovate Campaign - Bravo Drop[485] ・ Look Out! Maritime Early Warning Innovations

[484] https://www.gov.uk/government/news/670k-shared-by-two-innovators-in-first-round-of-dtep-funding

[485] https://s3.amazonaws.com/thegovernmentsays-files/content/182/1825123.html

1）資金配分機関及び研究開発プログラムにおける情報取扱に係る詳細調査結果

a）UKRI（Innovate UK、MRC、EPSRC ほか）

英国研究・イノベーション機構（UK Research and Innovation：UKRI）は、2018 年に発足した科学・イノベーション・技術省（DSIT）が後援する政府機関で、研究開発・イノベーションに関する政府資金の MRC や EPSRC などの分野別に設置された 7 つの研究会議体と、主に産業界や企業におけるイノベーション活動を支援する Innovate UK、大学の研究評価、ブロック・グラントの配分、産学連携推進を担う ResearchEngland を含めた 9 つの組織を取り纏めている[486]。UKRI 傘下の各組織は UKRI の規程を基本としているものの、各組織や技術分野に固有の研究助成金利用規程やリスク管理規則などを定め、助成している研究開発プログラムにおける情報保全を実施している。

本項では主に下記の UKRI 及び 7 つの研究会議体、Innovate UK の規則中心に取り上げ、UKRI、UKRI 傘下の機関及び同機関から助成を受ける研究実施主体に求める情報保全規程について整理する。

（UKRI 系列の機関で取りまとめる主な規則）
- **UKRI 情報管理ポリシー**[487]
- **UKRI（及び 7 会議体）研究助成金利用規約** [488, 489]
- **Innovate UK プライバシー通知および情報管理ポリシー**[490]
- **Innovate UK 助成金授与規則** [491]

■ 研究開発領域

宇宙、海洋、バイオ、サイバーほか

■ 適用範囲

・ UKRI 情報管理ポリシー

UKRI は 1958 年および 1967 年に制定された公文書法の適用を受ける公文書機関であり、法規制環境に従って記録を管理することが法律で義務付けられており、UKRI 情報管理ポリシーでは、同法に従い、UKRI および UKRI 傘下の機関の企業情報（科学的情報、一次研究情報、関連資料には適用されない）の情報管理指針を規定している。同指針によると、UKRI の情報は、データ（または構造化情報）、記録、文書（非構造化情報）で構成される。

486 https://www.jst.go.jp/crds/pdf/2022/FR/CRDS-FY2022-FR-02/CRDS-FY2022-FR-02_20400.pdf
487 https://www.ukri.org/publications/ukri-information-management-policy/
488 https://www.ukri.org/wp-content/uploads/2021/04/UKRI-161123-FECGrantTermsAndConditions-Nov2023.pdf
489 https://www.ukri.org/wp-content/uploads/2021/04/UKRI-161123-FECGrantTermsAndConditionsGuidance-Nov2023.pdf
490 https://www.ukri.org/publications/innovate-uk-privacy-notice-and-information-management-policy/innovate-uk-privacy-notice-and-information-management-policy/
491 https://www.ukri.org/wp-content/uploads/2023/02/IUK-15022023-Terms-and-conditions-of-an-Innovate-UK-Grant-Award-Jan-2023-FINAL-with-Header.pdf

（UKRI 情報管理ポリシーに基づく情報資産の定義）

- データ（Data）：（データ戦略で定義され、利用可能になり次第定義が追加される）
- 記録（Records）：事業活動の証拠となるすべての情報であり、法的、規制的、事業的に保存要件 があるものと定義される。記録は廃棄規則の対象となるが、永続的な歴史的価値を持つ場合もある
- 文書（Document）：即時的または業務上の価値はあるが、企業的価値や事業活動の証拠となるものではない情報と定義される。文書は必要以上に長く保管すべきではなく、通常 3 年以内とする

・ Innovate UK プライバシー通知および情報管理ポリシー

UKRI の傘下機関である Innovate UK は、UKRI のプラバシー通知に加え、固有の情報管理ポリシーを定めており、個人データや機密情報、商業上の機密情報が含まれる可能性のあるユーザ（資金提供先の研究開発実施主体等）の情報を収集、保存、使用、共有するための Innovate UK の具体的な取り決めについて整理している。

本ポリシーに基づき、Innovate UK が収集する可能性のある情報としては、個人データ、特別なカテゴリのデータ、機密情報で区分しており、機密情報以外の情報については 2018 年データ保護法及び UK GDPR に準拠している。

（Innovate UK プライバシー通知および情報管理ポリシーに基づく情報資産の定義）

- 個人データ（Personal data）：名前、電子メール アドレス、住所、固定電話番号または携帯電話番号などの情報で構成される
- 特別なカテゴリのデータ（Special category data）：人種、民族的出身、政治、宗教、労働組合のメンバーシップ、遺伝学、生体認証、健康、性生活、または性的指向に関する情報が含まれる。特別なカテゴリのデータの収集はアンケートに限定され、ユーザの同意がある場合にのみ収集、使用される
- 機密情報（Confidential information）：助成金やその他の資金申請の場合、提出された提案から、潜在的に商業上の機密情報や機密情報を含む情報を収集する場合がある

■ 情報の分類

Innovate UK プライバシー通知および情報管理ポリシーによると、Innovate UK は収集した情報（個人データ、特別なカテゴリのデータ、機密情報）の「機密性」、「正確性」、「可用性」を保護することで、ユーザの情報セキュリティを維持すると示されている。

また、基本的に政府セキュリティ分類ポリシーに準拠しており、情報の機密性に応じた分類（OFFICIAL、SECRET、TOP SECRET）に基づき運用している。

■ 情報管理策

UKRI や Innovate UK で助成されるプロジェクト（およびプロジェクト従事者）に対しては、基本的に政府のセキュリティポリシーフレームワークやセキュリティ分類ポリシーで規定される情報の機密性分類（OFFICIAL、SECRET、TOP SECRET）に従い、適切な情報保全動作を求めているが、必ずしもすべてのプログラムにおいて高い機密性が求められるということではなく、リスクアセスメントに基づき、必要に応じて UKRI 全体で適切な措置や安全

保障に関する助言等を得る仕組みを設けて対応を行っている。 なお、プロジェクト従事者に対する情報保全要件（システムやネットワーク、情報の保管・共有などのセキュリティ要件）の詳細はプロジェクトの Tearms&Condition（契約条件）で規定されている。また、情報に対するアクセスの考え方としては、情報保全的な観点とともに、「知る必要性（Need to Know)」の観点に従って、職員に対して区分を設けている。

プログラムやプロジェクトに限らず、UKRI や Innovate UK が扱う情報に対する情報保全に関する措置については、以下の情報保全ポリシー等で整理されている。

・ UKRI 情報管理ポリシー

UKRI 及び傘下機関が保有する企業情報を対象として以下の組織的な情報管理施策が規定されている。

（組織的管理策）

・ 情報の作成、整理、保管方法

- UKRI の情報はすべて、適切かつ承認された企業情報管理システム（SharePoint、Teams、Objective など）に保存しなければならない。情報管理システム内の記録は、真正性と信頼性を確保するために登録され、バージョン管理されなければならない
- UKRI は、事業活動に関する適切かつ正確な記録を、電子形式と紙形式の両方で作成し、維持することを約束する。意思決定と活動を文書化するために、適切な情報とプロセスが整備されていなければならない。保存スケジュールは、事業活動の証拠として保存する必要のある記録を特定するための枠組みを提供する
- すべての UKRI 情報は識別可能でアクセス可能であり、情報の効果的な管理に必要な管理上の背景を提供するために、十分なメタデータを持たなければならない
- UKRI のすべての情報資産は、情報資産登録簿（IAR）に記載され、情報資産所有者によって管理される

・ 情報の利用、アクセス、共有方法

- UKRI の情報はすべて、職員がその役割の一部として必要な場合に公開されるべきである。機密または保護されている情報は、例外的に非公開とする
- UKRI は協調的でハイブリッドな職場環境の支援に取り組んでおり、情報はその機密性に応じて、UKRI のデータ保護およびセキュリティ分類ポリシーと関連する取り扱いガイダンスに沿って安全に共有することができる。職員は許可された企業コラボレーションツールのみを使用する
- 状況によっては、UKRI は情報の予定された破棄を防止し、「情報の権利に関する要請」、「苦情および内部告発」、「法務、人事、不正行為、研究の完全性に関する事例」、「2005 年照会法および 2006 年照会規則に基づく公的照会」、「情報委員会事務局などの規制当局による調査」のケースに該当する可能性のある情報に対して一時的な保全措置を適用する義務がある

・ 情報の廃棄方法と時期

- 情報は、UKRI の業務上の必要性および関連する法的・規制上の要件を満たすために必要な期間だけ保持しなければならない。UKRI の保存スケジュールでは、UKRI の機

能ごとに、これらの要件を満たすために必要な各記録の保存期間を定めている。文書は、作成後 3 年以上経過し、業務上の価値がなくなった時点で廃棄する。

- UKRI の保存スケジュールはすべての UKRI の記録に適用され、2018 年 4 月の UKRI 設立以前に評議会が作成した記録にも適用される。2018 年以前の記録にスケジュールを適用できないコンプライアンス上または重要な業務上の理由がある場合、審議会はこの規則の適用除外を申請することができる
- 情報保持に関しては、政府の戦略に沿って、UKRI の企業承認情報システムのポートフォリオにおいて「所定の位置」に管理される。UKRI のすべての情報システムには、関連する保持機能または保持管理のための承認されたプロセスがなければならない
- 保管期限を過ぎた情報の破棄は、資産所有者の負担を軽減し、効率を向上させるために、自動的に（すなわち、資産所有者の確認なしに）実行される。これは、ベストプラクティスと政府の期待に沿った願望であり、テクノロジーとリスク許容度が許す限り取り組まれるものである
- UKRI の機能と活動の重要性を示し、一般に関連する情報を提供する記録は、国立公文書館（The National Archives ：TNA）に移管され、20 年ルールの要件を満たす時期に永久保存される。企業記録の選定と移管は、TNA の鑑定方針および記録選定のための一般ガイドラインに沿って行われる
- TNA での永久保存のために選定された記録は、移管前に、英国一般データ保護規則（GDPR）および 2018 年データ保護法に基づく UKRI の義務に関して、機密性を審査される

・ UKRI 研究助成金利用規約

UKRI 及び傘下の 7 研究会議体が資金提供を行う研究開発実施主体を対象に、以下の組織的情報管理上の措置の実施が義務付けられている。

（組織的管理策）

- UKRI の助成金を受けている組織は、適切な保証レベルを提供するために、セキュリティ管理計画を策定し、関連する認証を取得する必要がある
- サイバーセキュリティのリスクアセスメントに基づき、強固な管理策を実施しなければならない
- 全スタッフと学生を対象としたサイバーセキュリティ研修プログラムを実施し、UKRI の「信頼される研究とイノベーションの原則」に沿って、積極的なサイバーセキュリティ文化を実現する必要がある
- デュアルユースのリスクが生じた場合、いついかなるときも当該リスクを検討、職員に助言と指導を提供し、潜在的なリスクが特定された研究の進捗を積極的に監視するための明確な方針とプロセスを持つべきである。対応例としては以下が挙げられる
  - 職員に助言と指導を提供し、潜在的なリスクが特定された研究の進捗を積極的に監視するための明確な方針とプロセスを持つ
  - デュアルユースの問題が生じる可能性のある分野で働く全スタッフに適切な研修と教育を提供し、合法的な懸念を安全に提起できるような方針を設ける

（信頼される研究とイノベーションの原則）[492]

- 「信頼できる研究」とは、英国の知的財産、機密性の高い研究、人材、インフラを、敵対的な行為者による干渉の結果などによる潜在的な盗難、操作、搾取から保護することを意味する研究およびイノベーション分野の用語であり、UKRI は国際共同研究のデューデリジェンスに関して、UKRI が資金提供する組織に対する UKRI の期待を定めた「UKRI 信頼される研究とイノベーションの原則」を策定している
- UKRI から資金提供を受けている組織は、これらの原則を採用し、これらの原則に合致した管理・対策を実施していることを証明できるようにする必要がある
- 関連する法令として NSI 法があり、同法で規定されている 17 分野に該当する研究開発プログラムについてはデューデリジェンスプロセスの対象となる
- また、先進通常軍事技術 （ACMT） や兵器の開発プログラムに知識が使用される可能性のある科目や研究分野を勉強または研究する留学生および研究者 （免除された国籍を除く）に要求される学術技術承認制度 （ATAS）証明書の取得も、研究の信頼性を担保する有効な取組として示されている
- 具体的な原則としては、①パートナーの適正評価、②情報と知識の共有の管理、③商業利用から成る

①**パートナーの適性評価**：協働パートナーとなりうる組織および／または個人について、適切なデューデリジェンス評価を実施する必要がある

- パートナー組織および／またはその組織が活動する国の法的枠組みや組織構成、その組織の所有者、他の企業、政府省庁、軍などとの正式な提携の有無について理解する必要がある
- パートナーが拠点を置く国の民主的・倫理的価値観を理解することが重要
- プロジェクトの成果物や潜在的な利用方法に対するリスクが特定された場合、共同研究が合意される前に、UKRI の資金提供を受けた組織のリスク許容度に沿って、合理的かつ適切な緩和策が実施されなければならない

②**情報と知識の共有の管理**：情報の透明性と保護の必要性のバランスを図るために、組織は、機密データや情報へのアクセスが適切に管理されるよう、強固な情報セキュリティ管理対策を講じることが必要

- 職員や学生に対するセキュリティ意識向上およびトレーニングプログラムの一環として導入されるサイバー管理策の開発を通じて達成される、強固なサイバーセキュリティ文化が必要
- 機密データは安全に保管されなければならず、情報交換のために共有プラットフォームが使用されている場合、データは論理的に異なる場所に分離され、権限を与えられた個人のみがアクセスできるようにしなければならない
- 機微データへのアクセスは、アクセスが必要な期間、アクセスが必要であることが明確な個人にのみ与えられるべき。また、データの取り扱いおよび使用の根拠は、情報が共有される前に明確に規定・理解され、すべての当事者によって合意されるべき

[492] https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/

- すべてのプロジェクト活動とプロジェクト成果の取り扱いは、適用される輸出管理法およびその他の法的要件に準拠していなければならない。加えて、デュアルユースや非倫理的な応用の可能性に関して、プロジェクト活動の性質と想定される成果物に対して十分な配慮がなされるべきである

③**商業利用**：英国を含む社会や経済に利益をもたらすような将来の商業的成果が実現する可能性がある場合には、プロジェクトから派生する機密データや知的財産権を含む知的資産が適切に管理されることを確保するために共同研究契約を締結すべき

- プロジェクトから生じる知的財産を含む知的資産は、専門的かつビジネスライクな方法で管理されるべき
- 共同研究に先立ち、全てのパートナーは、商業的に関連するデータや機密性の高いデータ、プロジェクトから得られた知見を公開する時期について正式に合意する必要がある
- 英国の輸出規制は、機密性の高い技術、知識、戦略物資の輸出や伝達を制限するために設けられており、学術界にも他の輸出者と同様に適用される

・ Innovate UK プライバシー通知および情報管理ポリシー

Innovate UK は、Innovate UK プライバシー通知および情報管理ポリシーに基づき、同機関が収集する個人データ、特別なカテゴリのデータ、機密情報の情報管理策を定めている。

（組織的管理策）
- データの収集から破棄まで、個人データの保管に関する英国情報コミッショナーのガイダンス[493]に従って運用する
- 情報への不正アクセスを防ぐため、厳格な手順とセキュリティ対策を講じる
- 保有するデータを、収集時点およびその後も定期的にチェックすることで正確かつ最新であることを保証する
- 非 EEA 諸国のパートナーとの共同作業が見込まれるプログラムにおいて、パートナー組織との情報交換は可能な限り非個人情報および非機密情報に限定される

（人的管理策）
- 訪問者にはスタッフの同伴を設ける
- ディスプレイモニターを通行人から保護する。また、放置されたときにパソコンをロックする

（物理的管理策）
- 従業員または認可された請負業者のみが情報を保管する建物にアクセスできるようにするための立ち入り制御を行う
- 個人情報を含む機密情報を保管する机や棚は常に施錠する
- 不要になった紙の文書はシュレッダーに、デジタル記憶装置は物理的に破壊する

（技術的管理策）
- 収集するすべての情報は Innovate UK が運営する安全なサーバに保管する

493 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

・ Innovate UK 助成金授与規則

UKRI の助成金利用規則と同様、資金提供先に対して NSI 法の準拠や「信頼される研究（Trusted Research)」に関する UKRI の原則及び国家保護セキュリティ局（CPNI）のガイドラインの考慮を求めている。また、助成を受けたプロジェクトの所有者が変更された際、それが英国の国家安全保障または国益一般に 対するリスクをもたらすと信じるに足る妥当な根拠を有する場合、Innovate UK は、追加通知なしにその助成金を一時停止または終了する権利を有することが示されている。

（CPNI の Trusted Research に関するガイダンス）[494]

・ Trusted Research は、民主主義や倫理的価値観が英国とは異なる国々と関係のある組織や研究パートナーと協力するときに発生する可能性のある、研究協力に対するリスクについての認識を高めるキャンペーンであり、本ガイドでは、上記リスクに対して研究を保護する方法等が説明されている

④戦略的アプローチ：適切な研究パートナーを選択し、安全で成功した長期的な研究関係を構築するために時間とリソースを投資することは、研究のセキュリティにとって非常に重要であり、組織に大規模な研究関係のポートフォリオがある場合は、研究戦略とパートナーを定期的に確認することが推奨される

⑤機密性の高い研究を特定：学術機関とどのような研究に取り組んでいるのかをよく理解し、その研究ポートフォリオの中で最も機密性の高い側面や重要な側面は何か検討することが重要である。機密性の評価を行う際は以下の問いを検討すること

- 研究の TRL は何か
- 仕事の一環としてどのようなデータまたはバックグラウンド IP を共有しているか。また、これはビジネスにとってどの程度機密性または重要性があるか
- 研究を成功させるには、会社と知的財産へのどのレベルのアクセスが必要か
- プロジェクトに資金のどのくらいの割合を提供しているか

⑥パートナーを知る：学術パートナーを選択する際には、あなたが取り組んでいる特定の研究分野における専門知識と実績、評判、設備、および過去の協力歴を考慮する必要がある

上記とは別に、医学・バイオ分野の研究開発及び研究開発プロジェクトに対する資金提供を行っている MRC、BBSRC は、英国のヘルスケア研究に従事する慈善団体である Welcome Trust（WT）と共同で、「研究不正利用のリスク管理」[495]の声明を公表しており、その中で医学・バイオ分野で重大なリスクを引き起こす恐れのある「デュアルユース研究」に対する管理方針を定めている。

（研究不正利用のリスク管理に関する共同声明）

・ 資金提供されるある種の研究成果が生物兵器の開発など大きな害をもたらすために

[494] https://www.npsa.gov.uk/trusted-research-industry

[495] https://www.ukri.org/wp-content/uploads/2021/08/MRC-0208212-MRC-BBSRC-and-WT-statement-on-managing-risks-of-research-misuse-July-2015.doc.odt

悪用されるリスクがあることに基づき、同リスクの管理として共通のアプローチを示し、研究コミュニティがどのように役割を果たすべきかを説明した MRC、BBSRC、WT の共同声明

・ この声明における重大なリスクをもたらす研究は「懸念されるデュアルユース研究」と呼ばれ、以下のように定義している
  ➢ 公衆衛生と安全、農作物やその他の植物、動物、環境、物質、国家安全保障に広範な潜在的結果をもたらす重大な脅威をもたらす可能性のある知識、情報、製品、技術を直接的に悪用する可能性が合理的に予想される生命科学研究
・ BBSRC、MRC、WT は、このような正当な懸念に対処するためには、危害をもたらすために悪用される可能性のある研究のレビューと監視のための適切なプロセスが、研究機関、国内、国際レベルで存在することが重要であると考えている
・ BBSRC、MRC、WT は、支援する研究が研究提案に関連する不正使用のリスクが、助成金提供プロセス中に特定・評価されるよう、助成金申請プロセスおよび資金提供要件に 5 つの重要な規定を設けた
  ⑦申請用紙に、提案に関連する短期的および中期的な悪用リスクを検討するよう申請者に求める質問を含める
  ⑧助成金申請書の査読を行う外部専門家へのガイダンスにおいて、検討すべき事項として、不正使用のリスクについて明確に言及する
  ⑨この問題に関する資金委員会向けの明確なガイダンスと、懸念が提起されたケースの評価プロセスの開発を行う
  ⑩不正使用のリスクに関する具体的な言及を含むよう、研究における適正実施に関するガイドラインを修正する
  ⑪デュアルユースリスクの状況に変化が生じた場合、あるいは資金提供された研究プロジェクトの過程で、当初の申請時には予想されていなかった新たなリスクが発生した場合には、資金提供者やその他の関連当局に通知することを義務付ける

■ 所管する主なプログラムと情報取扱規程

・ marine and maritime in the Great South West - R1 CR&D

【研究領域】海洋

【概要】4.1.1 (4) 3) b)参照

【参加資格】

➢ 規模を問わず英国に登録された企業であること

➢ 少なくとも一つ以上の中小企業（SME）が補助金を申請している、又は関与していること

➢ 英国に登録されている他の組織と協力すること

➢ グレート・サウス・ウェストの海洋および海事イノベーション・クラスターで積極的に活動する、または活動を拡大すること

➢ ビジネスの成長に対する明確な野心を持っていること

※学術機関は単独で主導・活動することはできない

【情報取扱規程】

➢ UKRI、Innovate UK の情報管理ポリシーに従う

・ China UK One Health research for epidemic preparedness and AMR

【研究領域】バイオ

【概要】4.1.1 (4) 3) c)参照

【参加資格】

研究者は、応募資格のある研究組織に雇用されていること必要がある。また、大学院の学位が必要。博士号または医学の学位を持っていることが望ましい

（応募資格のある機関）
- 高等教育機関
- 独立研究機関（IRO）及び NHS 機関
- 公的研究機関
- MRC 研究所(MRC Harwell, MRC Laboratory of Medical Sciences, MRC Laboratory of Molecular Biology)
- MRC ユニットとパートナー研究所
- 他の研究評議会から資金提供を受けている研究所やユニット
- 研究・技術機関

【情報取扱規程】

UKRI、Innovate UK および本プログラムの共同所感機関である MRC の規約やポリシーに準拠する。

（UKRI 助成条件）[496]
- ガバナンスと管理の視点から、以下のポリシーのコピーあるいは、リンクを提供すること
  - データ管理（サイバーセキュリティを含む）(Data Management (including cyber security))
  - 研究への誠実さ(Research Integrity)[497]
- UKRI の利用規約に基づき、研究機関はリスクに基づいた方法で資金提供が下請けされている第三者に対してデューデリジェンスを行うことが義務付けられている。また、下請け業者が海外に居住する場合に、どのようなデューデリジェンスチェックを実施しているのか詳細に情報提供すること。（デューデリジェンスチェックポリシーまたはアンケートのコピーを提示すること）
- 研究能力、実施能力
  - 研究戦略の主な目的と、上で指定した研究評議会（ただしこれに限定されない）を中心とした UKRI の任務と優先事項との関連性を説明する

[496] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.ukri.org%2Fwp-content%2Fuploads%2F2022%2F03%2FUKRI-250522-ApplicationForEligibiltyToApplyToUKRI.docx&wdOrigin=BROWSELINK

[497] https://www.ukri.org/what-we-do/supporting-healthy-research-and-innovation-culture/research-integrity/

こと

- 研究者のうち少なくとも 10 名について、研究主任または共同研究者を務めたプロジェクトの詳細と、過去 5 年間に学生を監督した経験を記載すること

（MRC の追加助成条件）

- 機密情報を取り扱っている全ての研究者は、所属する機関の規約または専門家としての行動規範に従って機密保持のため責任を確立すること [498]
- 応募の際に、候補者はデータ管理計画書（data management plan, DMP）を提出する必要がある [499]
  - DMP は、研究機関および研究データの方針、システム、手順に言及し、研究サイクル全体を通じて定期的に見直される必要がある。組織が ISO 27001 に準拠している場合は、登録番号も記載すること
  - DMP は、支援事例とともに査読者によるレビューを受ける。一貫性を確保し、査読を容易にするため、すべての DMP はデータ管理計画書テンプレート [500]を使用することが望ましい。DMP の質は、査読や申請の可否に影響する可能性がある
  - 集団および患者を対象とした研究の場合、DMP は、集団および患者を対象とした研究のデータ共有に関する MRC の詳細ガイダンスの要件、特に研究利用基準および独立した監視（研究とその変数が容易に発見可能であることを保証する手段）、特に正式なデータ標準の使用に関する要件をどのように満たすかを示すべきである
  - ヒトを参加者として含む介入研究（臨床試験、臨床介入研究、公衆衛生または行動介入研究など）については、DMP はその研究が MRC の「研究データの公開に関する方針：臨床試験と公衆衛生介入」(Open research data:clinical trial and public health interventions)[501]の要件をどのように満たしているかを示すべきである：
  - 研究データの共有または再利用に依存するパートナーシップ補助金には、既存のデータへのアクセスがどのように管理されるか、また新たに生成されたデータがどのようにアクセスされ、補助金の配給期間中どのように保存されるかについての簡単な概要を含めなければならない

[498] https://www.ukri.org/wp-content/uploads/2020/02/MRC-171123-AdditionalTermsConditionsGrantsNovember2023.pdf

[499] https://www.ukri.org/councils/mrc/guidance-for-applicants/what-to-include-in-your-application/2-2-attachments/#contents-list

[500] https://www.ukri.org/publications/data-management-plan-template/

[501] https://beta.ukri.org/who-we-are/mrc/our-policies-and-standards/research/open-research-data-clinical-trials-and-public-health-interventions/

b）MoD（Dstl、DASA）

英国国防省（MoD）は、英国の防衛・安全保障領域の研究開発資金を所管しており、参加の国防科学技術研究所（Dstl）や国防・セキュリティ促進機構（DASA）を通じて民間事業者に資金配分を行い、研究開発を実施している。

本項では主に下記の MoD 及び Dstl、DASA の規則を取り上げ、同機関及び同機関から助成を受ける研究実施主体に求める情報保全規程について整理する。

（MoD 系列の機関で取りまとめる主な規則）

- **防衛情報、知識、デジタルおよびデータ政策への取り組み**[502]**（MoD）**
- **防衛ネットワークのガバナンス（JSP 604）「規則 13：ICT は情報管理ポリシーに準拠しなければなりません」**[503]**、「規則 22：ICT は、暗号化製品の使用に関する HMG 情報保証ポリシーに準拠するものとします」**[504]**（MoD）**
- **DASA 標準利用規約**[505]**（DASA）**

■　研究開発領域

宇宙、海洋、サイバー、バイオ、多義的技術

■　適用範囲

MoD はガイダンス「防衛情報、知識、デジタルおよびデータ政策への取り組み」の中で、「情報」、「知識」、「データリソース」の 3 つの MoD における管理・活用方針を示している。

■　情報の分類

MoD のガイダンス「防衛ネットワークのガバナンス（604）」や DASA を通じて公募されている研究開発プログラムにおいて、政府セキュリティ分類ポリシーの情報分類に基づいた措置や運用が図られていることから、基本的には同分類ポリシーに準拠していると考えられる。

■　情報管理策

MoD 及び傘下の Dstl、DASA においては、MoD の情報管理ポリシーに従って、保有する情報の保全を行っている。MoD の情報管理ポリシーは、一部が MOD Joint Service Publication（JSP）として公表されている[506]ものの、すべての JSP が公表されていないため、アクセス可

[502] https://www.gov.uk/government/publications/jsp-441-defence-records-management-policy-and-procedures--2/defence-information-knowledge-digital-and-data-policy-commitments

[503] https://www.gov.uk/government/publications/joint-service-publication-jsp-604-network-rules/rule-13-ict-shall-be-compliant-with-information-management-policy

[504] https://www.gov.uk/government/publications/joint-service-publication-jsp-604-network-rules/rule-22-ict-shall-be-compliant-with-hmg-information-assurance-policy-for-the-employment-of-cryptographic-products

[505] https://www.gov.uk/guidance/defence-and-security-accelerator-terms-and-conditions-and-contract-guidance

[506] https://www.gov.uk/government/collections/joint-service-publication-jsp#information-management-and-technology

能な出版物の範囲内で、MoD が保有する情報、情報資産を対象とした管理策を整理する。

■　**ガイダンス「防衛情報、知識、デジタルおよびデータ政策への取り組み」**

（組織的管理策）

- 防衛における情報資産の管理、共有、使用方法について責任を負う適切な資格を持つ上級者を特定し、雇用する
- 情報要件を早期に特定する
- 共有と共通理解を支援するために、可能な限り承認された標準を採用する
- 法律および政府/国防規則に従って、個人のプライバシーを保護し、秘密保持を尊重する

■　**防衛ネットワークのガバナンス(JSP 604)「規則 13：ICT は情報管理ポリシーに準拠しなければなりません」**

（組織的管理策）

- データおよび情報を処理および保存するすべての ICT は、政府のセキュリティ分類に従ってそのデータおよび/または情報のセキュリティ分類を定義する属性を持ち、JSP440 Part 4（未公表）に従って適切なレベルの保護および制御を提供する必要がある
- プロジェクトによって処理または利用されるデータが作成/開始点から廃棄までどのように管理されるかを説明する詳細な計画を提供する必要がある

（技術的管理策）

- データおよび情報を処理および保管するすべての ICT は、データおよび/または情報が無許可の主体によって変更されていないことを検証するメカニズムを備え、その完全性に対する信頼を可能にする

■　**規則 22：「ICT は、暗号化製品の使用に関する HMG 情報保証ポリシーに準拠するものとします」**

（組織的管理策）

- OFFICIAL としてマークされたデータは、国家サイバーセキュリティセンター（NCSC）からのガイダンスに基づいて、業界で認められた暗号化のベスト プラクティスを採用する必要がある
- SECRET としてマークされたデータは、暗号鍵として知られる高保証暗号化システムを使用する必要がある。これらのシステムは NCSC によって独立して保証されている

主に DASA を経由して公募される研究開発については DASA のイノベーション標準契約規約[507]を通じて、資金提供を行う研究開発実施主体で遵守が必要な義務を規定している。

本規約の中で、情報の管理に関しては、主に情報の開示要件について述べられているものの情報の保全動作についての定めは特になく、情報資産に対する管理方針については同契約の中で参照される DEFCON の中で規定されている。DEFCON は MoD が発行する防衛契約条件で、付番される番号ごとにサイバーセキュリティや知的財産の管理方針等が規定されてい

[507] https://assets.publishing.service.gov.uk/media/62d18910e90e071e814807f2/DASA_Open_Call_Terms_and_Conditions_July_2022.pdf

る。このうち DEFCON 659 において、機密情報のセキュリティ対策について規定されている。なお、研究開発プログラムにどの DEFCON への準拠が求められるかについては、プログラムことの契約条件（T&C）で規定される。

（DEFCON 659 の概要）[508]

- 契約者及びその従業員は、当局から書面による別段の権限を与えられている場合を除き、契約の完了又は終了の前後を問わず、秘密事項が次の各号のいずれかに該当する者に開示され、又は取得されるおそれがあることを知り、又は合理的に知るべきであると思われる行為を行ってはならず、又は行うことを許可してはならない
  - 英国籍を持たないもの
  - 当局が、契約者に対し、秘密事項をその者に開示してはならない、またはその者が取得してはならないと書面で通知したもの
  - 契約者の従業員でないもの
  - 契約者の従業員であり、契約の適切な履行のために情報を知る必要のないもの

- 当局の書面による許可がある場合を除き、契約者及びその従業員は、契約の完了または終了の前後を問わず、以下のことを確保するためにあらゆる合理的な措置を講じるものとする
  - 契約の適切な履行に必要な範囲を除き、秘密事項の写真撮影および秘密事項のコピーの作成をしてはならず、秘密事項から抜粋してはならない
  - 秘密事項は常にセキュリティポリシーフレームワークに従って厳重に保護され、要求があれば、それを保持する権利を有する当局に引き渡されるものとする

- 請負事業者は当局の要請に応じて以下を提供すること、
  - 保管が義務付けられている秘密事項にアクセスした従業員の記録
  - 請負業者およびその従業員が本条件に基づく義務を遵守していることを確認するために、請負業者がその義務を遵守し、義務違反を防止するために講じた措置または提案した措置を含め、当局が随時要求する情報
  - 請負業者およびその従業員が、本条件に基づき発生する秘密事項に関する義務を遵守しなかった場合、そのような不履行が明らかになった時点で、その詳細のすべての情報

- 契約の完了または終了の前後を問わず、契約者またはその従業員が、権限を有しない者が秘密事項に関する情報を直接的または間接的に得ようとしている、または得ようとしていることを発見した場合、またはその疑いがある場合、契約者は、直ちに、その詳細を当局に通知するものとする

- 下請業者への秘密事項の開示を伴う下請契約の締結を請負業者が提案する場合、請負業者は以下を行うものとする
  - 下請け業者の名称、実施される作業の明細、および当局が合理的に要求する請負業

[508] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf

者が知っているその他の詳細について、当局の承認を得るために提出すること
➢ 本条件の付属書の条件および当局が指示する秘密保持義務およびセキュリティ義務を下請契約に組み込むこと
➢ 下請業者による秘密保持義務またはセキュリティ義務の違反に気づいた場合は、直ち に当局に報告し、当局から要請があった場合は、下請契約を解除すること

・ 当局は、以下の場合、直ちに契約を解除する権利を有する
➢ 契約者が本条件に基づく義務に違反した場合
➢ 請負業者が、王室との他の契約によって課された秘密保持義務またはセキュリティ義務に違反した場合
➢ 違反の状況が秘密事項の秘密性または安全性を危うくすると当局が判断した場合

■ 所管する主なプログラムと情報取扱規程

・ Space to Innovate Campaign – Bravo Drop

【研究領域】宇宙（多義的技術）

【概要】4.1.1 (4) 3) e)参照

【参加資格】

- 英国内外の学術機関、中小企業、大企業を含む、あらゆるイノベーターが参加可能。他方、提案が採択された場合、研究従事者のデューデリエンス・チェックを DASA が実施する場合があり、特に英国籍以外の従事者に対しては最大 6 週間程度要する可能性がある（契約者が提案する研究従事者が全員、SC レベルのセキュリティ・クリアランスを保持している場合はこのプロセスは除外される）
- 防衛・安全保障分野での実務経験は必須条件ではない
- 軍事的要件に対応した衛星の敏捷性とポインティング精度を向上させる技術を持っていること
- 研究開発に必要な物資等の原産国の輸出管理規制を遵守すること、提案に必要な輸出許可を取得できること。また、受託者が最終的に開発したソリューションを外国企業に販売する場合、関連するすべての輸出規制が適用される。なお、輸出許可が取得できないと DASA が判断した場合は、追加で検査が行われ、その結果、提案が拒否される場合がある
- 応募者はこのコンテストに参加するためにサプライヤー保証アンケート（Supplier Assurance Questionnaire：SAQ）[509]に回答する必要がある。SAQ は DCPP（Defense Cyber Protection Partnership）によって審査され、DASA のサイバーリスク評価（CRA：Cyber Risk Assessment）に準拠していないと評価された場合、契約締結前にサイバー実施計画（CIP）を作成し、サイバーレジリエンスを証明する必要がある。なお、本プログラムのサイバーリスクレベルは「非常に低い」と評価されている

（SAQ で回答が求められる主な項目）
・ 正式に認められた情報セキュリティポリシー（情報リスク管理体

[509] https://forms.office.com/Pages/ResponsePage.aspx?id=7WB3vlNZS0iuldChbfoJ5Tv4OR9pb0BHial1Ag-WKXVUOFk3Sk9SS0JDQ0FRWjhYNDhTVldHUDJaNy4u

制、ネットワーク セキュリティ、ユーザ教育と意識向上、マルウェア防止、リムーバブル メディア制御、安全な構成、ユーザ権限の管理、インシデント管理、モニタリングの分野を最低限考慮した文書化および維持されたポリシー）が導入されているか
- 組織内で情報セキュリティ関連の役割が特定され、責任が割り当てられているか
- サプライヤーとの関係における情報セキュリティのリスクに対処するポリシーを定義し、実装しているか
- 機密情報が明確に識別されるようにするためのポリシーがあるか
- 情報および情報処理施設へのアクセスを制御するポリシーがあるか
- リムーバブルメディアを介した情報交換を制御するポリシー（適切な暗号化を施しかつ最小限の使用に留めるなど）があるか
- ユーザカウントのアクセス権を管理するポリシー（機密情報にアクセスできるアカウントに多要素認証を設ける、情報資産へのアクセス記録を維持する等）があるか
- 契約のあらゆる側面に必要な範囲をカバーする Cyber Essentials Plus 認定を取得しているか　など

（Cyber Essentials Plus 認定について）[510]
- Cyber Essentials は、あらゆる規模の企業がさまざまなサイバー攻撃から身を守り、サイバーセキュリティへの取り組みを実装できるよう支援する政府支援の制度
- 2014 年以来、政府は、特定の種類の公的契約に入札するサプライヤーに対し、適切なサイバーセキュリティ管理が確実に実施され、サプライチェーンにおけるサイバーセキュリティリスクを軽減するために、Cyber Essentials または Cyber Essentials Plus 認定を取得すること（または同等の管理が実施されていることを証明すること）を義務付けている
- Cyber Essentials、Cyber Essentials Plus、または同等のコントロールが必要とされる契約としては以下の例が示されている
  - データが英国以外で保持・アクセスされる場合
  - データが EU-US データ・プライバシー・フレームワーク[511]の対象となる場合
  - データが定常的に独立した災害復旧拠点に保管されている場合　など
- Cyber Essentials では、一般的なインターネットベースのサイバー攻撃の大部分を防御する 5 つの技術的制御（ファイアウォールとインターネットゲートウェイ、安全な構成、アクセス制御、マルウェアからの保護、セキュリティアップデートの管理）を組織がどのように実装しているかを評価している
- Cyber Essentials は、組織がアンケートに回答する自己評価オプションで

[510] https://www.gov.uk/government/publications/ppn-0923-updates-to-the-cyber-essentials-scheme

[511] 2022 年に合意されたヨーロッパ連合（EU）とアメリカ合衆国（US）のデータ転送フレームワーク（https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf）

あり、その後、アンケートは独立した認証機関によって検証され、適切な基準が達成されているかどうかが評価され、認定される
- 認定されると組織は政府や業界が来ている技術的なサイバーセキュリティ基準/管理の最低限のベースラインを満たしていることを証明できる
- Cyber Essentials Plus ではリモート及びオンサイトでの脆弱性テストも含まれる

【情報取扱規程】

- 本プログラムの公募はセキュリティ分類ポリシーの「OFFICIAL」レベルで運用されており、該当するベースライン動作に準拠が求められる
- 受託者は 2000 年情報公開法や 2004 年環境情報規則に基づき、透明性情報（Transparency Information：契約内容および契約に基づいて DASA が受託者に支払った支払情報）が一般に公開される可能性があることを理解する必要がある
- 契約に関連して受領した情報は防衛契約条件(DEFCON)に従って管理される。本プログラムで適用される情報の取り扱いに関連する DEFCON は以下の通り

（本プロジェクトで適用される情報取扱に関する DEFCON）
- DEFCON 531（情報開示）
- DEFCON 532（個人情報保護）
- DEFCON 632（第三者の知的財産-権利と制限）
- DEFCON 658（サイバー（フロー・ダウン））
- DEFCON 705（知的財産権-研究および技術）

- Look Out! Maritime Early Warning Innovations

※上記のプログラムと重複する条件は割愛する

【研究領域】海洋、多義的技術

【概要】4.1.1 (4) 3) b)参照参照

【参加資格】

外国（英国外）の企業/団体と協力することは可能であるが、将来的な成果の活用ルートと輸出規制への影響（ITAR、EAR など）に考慮すること

【情報保全規程】

- 本プログラムで使用するデータセットの機密レベルは「OFFICIAL」で設定されており、これよりも高い機密資料を使用する提案を行う提案をし、落札された場合、契約内容を更新する必要がある
- 通り扱うデータセットが「OFFICIAL」であることも踏まえ、MoD が保有するデータセットの提供は想定しておらず、提案者独自のデータセットに基づきプロジェクトを進めること
- 成果物についても「OFFICIAL」の水準を想定しており、成果物の機密性が高くなる場合は上記と同様に契約内容の改訂する可能性が示唆されている

- The Defence Technology Exploitation Programme

【研究領域】多義的技術

【概要】4.1.1 (4) 3) e)参照参照

【参加資格】

- 下位層のサプライヤー（イノベーター）と上位層のサプライヤーの間で連携が確立されている必要があり、両方のサプライヤーが英国に登録されている必要がある
- 下位層のサプライヤー
  - ✓ 英国で登録された中小企業（または小規模）企業である必要がある
  - ✓ 外資事業を実施している場合はNSI法を遵守する必要がある
  - ✓ 現行のInnovate UK 助成金の資金制限に基づき、ロシア起源の商品またはサービスを含む、ロシアの事業体に資金を提供は行わない
  - ✓ 英国に拠点を置き、英国でプロジェクト開発活動を実行する必要がある
  - ✓ 英国でプロジェクトの成果を商業的に利用する意図があること
- 上位層のサプライヤー（下位層のサプライヤーと同様の条件は割愛）
  - ✓ 既存の防衛サプライチェーンの一部であるか、新規または既存の防衛省の技術分野向けに新しいサプライチェーンを開発または参加する予定であること
  - ✓ 防衛サプライチェーンに利益をもたらす、プロジェクトの明確な使用と商業化の道筋を示すこと

【情報保全規程】

- 共同で本プログラムを所管するInnovate UKの情報管理ポリシーが適用されている

2）研究開発実施主体における情報取り扱い実態の調査

調査した政府系の研究開発プログラムで採択された研究開発実施主体のうち、情報保全ポリシーが公開されているD-Orbit UK Ltd及びエディンバラ大学を対象として情報取扱実態について調査を行った。

a）D-Orbit UK Ltd[512]

D-Orbit UK Ltdは、イタリアに本社に置く民間航空宇宙会社「D-Orbit S.p.A」の子会社で。英国の他、ポルトガル、米国にも拠点を持っている。D-Orbitは複数の小型衛星を搭載可能な衛星軌道投入機「ION」の自社開発・製造を行っており、2023年には丸紅が出資を行っている[513]。

■　参加している研究開発プログラム

D-Orbit UK Ltdは2021年にUKSAが主催するプログラムである「National Space Innovation Programme (NSIP)」にHR Wallingford、Sayers and Partners、オックスフォード大学とともに採択されている。このプロジェクトでは、地球観測（EO）データを使用して気象関連の危険による建物や農業へのリスクの推定を行っている。上記の他にもUKSAの主催するプログラムに多数参加している[514,515]。

■　情報保全体制

不明

■　情報保全措置[516]

D-Orbitは、法令、ISO/IEC 27001:2022および独自の倫理規定に準拠し、情報セキュリティに関するポリシーを定義しており、情報セキュリティ対策は、持続可能な発展、社内プロセスおよびクライアントに提供するサービスの有効性、効率性、品質という原則に従って実施している。

D-Orbitでは、クライアントの情報と個人データの機密性と保護を保証するためには倫理規定の一貫した適用が不可欠であり、その目標を達成するために情報セキュリティマネジメントシステム（ISMS）を構築している。また、情報の機密性、完全性、可用性を保護するために必要な人材、情報、システム、インフラなどのリソースを確保するとともに、取締役会は、情報セキュリティ管理の継続的な改善と、施行中の法律および自社の倫理規定の遵守の徹底を図っている。

512 https://www.dorbit.space/

513 https://www.nikkei.com/article/DGXZRSP664294_Z01C23A1000000/

514 https://www.gov.uk/government/news/new-funding-to-support-sustainable-future-of-space

515 https://www.gov.uk/government/news/government-funds-uk-companies-at-the-forefront-of-space-innovation

516 https://www.dorbit.space/downloads/security-policy.pdf

（D-Orbit における ISMS 構築の目的）
D-Orbit は、以下の目的のために ISO/IEC 27001:2022 に準拠した ISMS を定め、維持している。

- 実施するプロジェクトやサービスを通じて取得、処理、作成される自社および顧客の情報である当社のノウハウを保護し、情報の機密性、完全性、可用性を保護すること
- 必要に応じて、適切な情報への適切なアクセスを確保し、D-Orbit の従業員およびスタッフ、または D-Orbit と提携して業務を行う人々への不正アクセスを回避すること
- 違反、誤用、不正行為から情報を保護するための ISMS セキュリティ対策を定め、実施すること
- 情報セキュリティに関する社内外の役割と責任を明確にすること
- セキュリティ意識向上とリスク最小化のために、情報セキュリティに関する適切なトレーニングを提供し、コースを実施することで、職員を支援すること
- 不利なシナリオや脅威が発生した場合に備え、情報セキュリティの継続性を確保すること
- 情報セキュリティに関する契約、法律、規制の遵守を維持すること

b）エディンバラ大学[517]

エディンバラ大学は、英国、スコットランドのエディンバラに所在する国立大学で人文社会科学部、医学・獣医学部、理工学部を有している。「医療とケアの未来の形成」、「「気候・環境危機への取り組み」、「益のためのデータ・デジタル・AI の活用」を研究ミッションとしており、このミッションに基づき、喫緊のグローバルな課題に取り組むために、大学全体の活動を活性化させる。

図 4.1-43　エディンバラ大学の研究課題及びミッション

[517] https://www.ed.ac.uk/

■　参加している研究開発プログラム

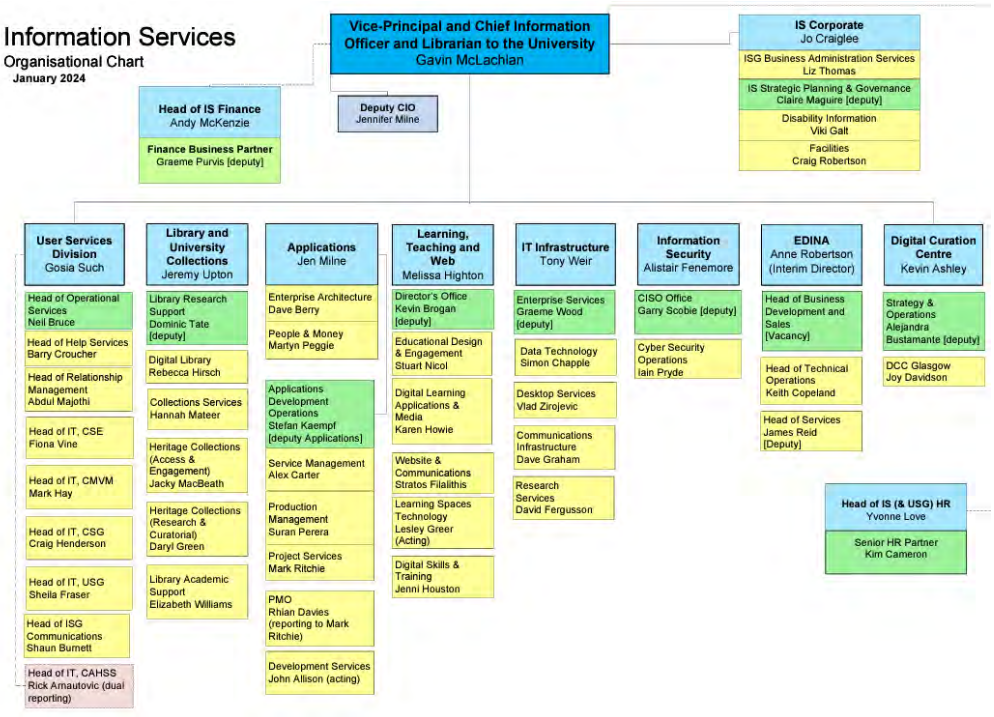
エディンバラ大学は、英国政府の資金提供プログラムとしては、UKSA の NSIP や DASA の「Look Out! Maritime Early Warning Innovations」プログラム等に参加している。

NSIP では、エディンバラ大学地球科学科（理工学部）が Global Satellite V u Ltd と共同で、衛星を使用した地球規模の災害を予測するのに役立つ先駆的な技術開発に取り組んでいる[518]。また DASA のプログラムではマルチスタティックレーダーネットワーク空中早期警戒システムの開発に取り組んでいる[519]。

■　情報保全体制

情報管理については、エディンバラ大学の情報サービスグループ（ISG）で推進されており、ISG の情報セキュリティ部門において、最高情報セキュリティ責任者（Chief Information Security Officer：CISO）の下で統治されている。

情報セキュリティ部門は、大学の情報セキュリティリスク管理戦略を主導、管理する責任を負い、情報セキュリティのリスクに対して総合的な対応を提供する。また同部門は、大学全体の情報セキュリティの取り組みも主導し、既存および新たな情報セキュリティの脅威に関する戦略的アドバイス、大学のあらゆる分野に指導を提供するとともに、これをサポートするセキュリティ意識向上トレーニングを提供する[520]。



[518] https://www.ed.ac.uk/bayes/bayes-media-centre/news/current-news/uni-edinburgh-space-project-funding

[519] https://www.gov.uk/government/publications/accelerator-funded-contracts/defence-and-security-accelerator-funded-contracts-1-april-2021-to-31-march-2022

[520] https://www.ed.ac.uk/information-services/about/organisation/is-org-infosec/infosec-what-we-do

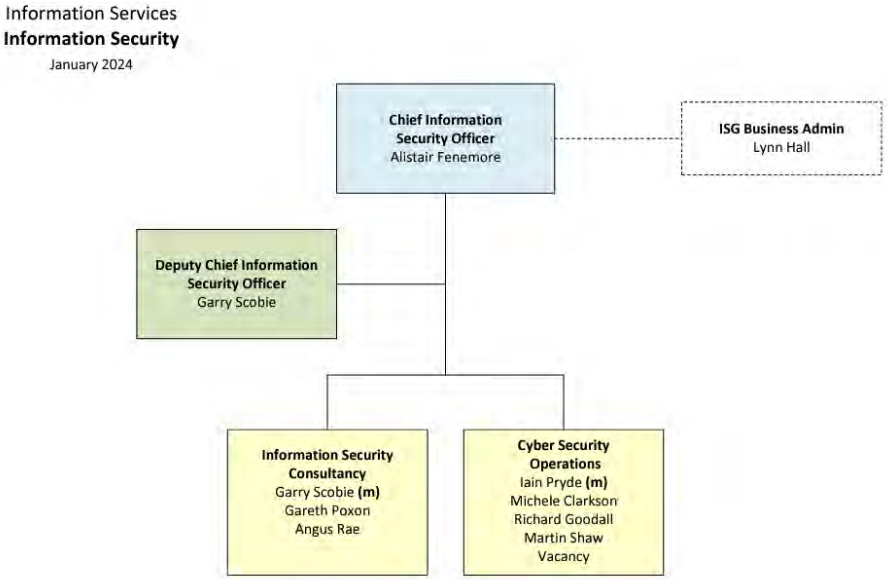


図 4.1-44　エディンバラ大学 ISG の組織図と情報セキュリティ部門 の体制

■　　情報保全措置 [521]

エディンバラ大学では、大学関係者全員が遵守しなければならない基本的なルールを定めた情報セキュリティポリシーを頂点に、情報セキュリティポリシーの達成のために遵守することが求められる基準（standard）と基準を実現するための具体的な手順で構成される情報セキュリティフレームワークを定めている。

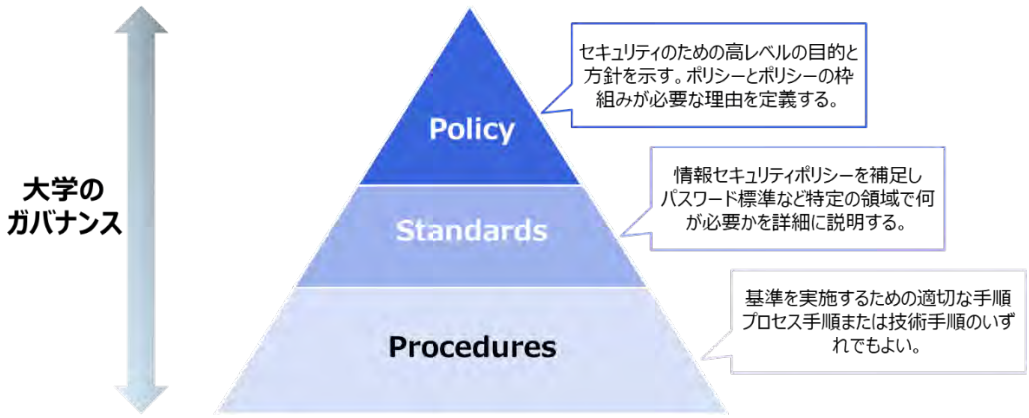


図 4.1-45　エディンバラ大学における情報セキュリティフレームワーク

また、データをすべての研究の中心であるとし、研究プロジェクトの一環としてデジタルデータを管理する人を対象に、安全に研究データを保つ方法を整理している [522]。

（データの分類） ・　データ分類スキームを使用することで、データの紛失、漏洩、悪用によるリスクと

[521] https://www.dorbit.space/downloads/security-policy.pdf
[522] https://infosec.ed.ac.uk/training

影響のレベルに応じて、さまざまな種類のデータをどのように管理するかを決定することができる

- エディンバラ大学では、以下の 3 レベルの分類スキームでデータを管理している

分類レベルと定義	データの例	セキュリティ管理の例
1：無制限 - 安全に公開できるデータ	匿名データ。オープンまたは公開されたデータ。	データが公開される場所と更新時期の登録
2：制限付き – 特定の視聴者向けのデータ・広範囲に公開すると損害が生じる可能性がある	個人を特定できる情報。商業上の機密情報。	暗号化してアクセス制御を適用する。紙文書を使用しないときは安全に保管する
3：機密 – 公開すると重大な損害を引き起こす可能性がある非常に機密性の高いデータ	特別なカテゴリのデータ (健康データなど)。機密保持契約の対象となる事項。法的に特権のある文書。	暗号化して厳格なアクセス制御を適用する。二要素認証を使用する。

（データのストレージ）

- さまざまなストレージオプション（ファイルサーバ、クラウドストレージなど） を利用できるため、それぞれのリスクと利点を評価してデータを保護し、データを最小限に抑えるための最も適切な方法を決定する必要がある
- 研究データを保護するには、研究データを集中管理されたネットワークドライブに保存することが強く推奨される。これにより、データが次の状態になることが保証される
- 1 か所に保存され、定期的にバックアップされます
- オフサイトで作業する場合など、必要に応じて VPN 経由で利用可能
- 紛失、盗難、不正使用のリスクを最小限に抑えて安全に保管

ストレージの種類	考慮事項	考慮事項 （データの機密性が高い場合）
クラウドストレージ	• データの損失や損傷を防ぐにはどのような対策があるか • クラウドサービスからデータを簡単に抽出することができるか	• クラウドサービスからデータを検証可能な形で削除できるか • データは不正アクセスから保護され、すべてのアクセスが監査されているか • クラウドサービスは、ISO 27001や27002など、公認のデータ管理／セキュリティ基準に準拠しているか • クラウドサービスプロバイダーには誰の法律が適用されるか • クラウドサービスプロバイダー間の契約には、誰の法律が適用されるか？
ポータブルストレージ （HDD/SSDドライブ、USBメモリなど）	• 信頼できるメーカーの高品質な製品を選ぶこと • 環境条件を含め、手入れや取り扱いについては、メーカーが提供する指示に従うこと • メディアが故障していないか定期的にチェックし、定期的にデータを「リフレッシュ」すること • 個人データや機密データが暗号化されていることを確認すること	

（データのバックアップ）

- データのバックアップにより、次のような原因による偶発的または悪意のあるデータ損失を防ぐことができる
  - ➢ ヒューマンエラー
  - ➢ ハードウェア障害
  - ➢ ソフトウェアまたはメディアの障害

- ウイルス感染や悪意のあるハッキング
- 停電

・ データを一元管理されたドライブに保存できない場合は、少なくとも 2 つの異なるメディアに少なくとも 3 つのデータのコピーを保管し、少なくとも 1 つのコピーをオフサイトに保管し、それらが正しく動作することを定期的にチェックすることが求められる
・ この方法により、ハードドライブが故障したり、ノートパソコンが盗まれたり、研究室が全焼したりといった災害シナリオが発生した場合でも、比較的新しいバックアップがあれば、最も重要なデータやファイルを復旧することができる

（強力なパスワード）

・ 不正なアクセスを防ぎ、研究データを確実に保護するためには、適切に強力なパスワードを選択する必要がある
・ パスワードマネージャー（LastPass、Keepass、1Password、Dashlane など。エディンバラ大学は、すべての職員と学生に LastPass への無料アクセスを提供している）は、パスワードの作成、保存、管理のプロセスを簡素化するために特別に設計されたツールで、選択できるオプションは多数あり、管理不能になることなく強力で安全なパスワードを生成するためのさまざまな機能が提供されている。一般的にパスワードマネージャーが提供する利点は以下の通り。
  - 覚えておく必要があるのはパスワードを 1 つだけ
  - アプリまたはブラウザ拡張機能を介してアクセスされるツール
  - デバイス間の同期
  - 安全なパスワードの自動生成
  - 保存されたパスワードの暗号化
  - 安全ではない、侵害された可能性のあるパスワードの特定
・ パスワードマネージャーを選択するときは、サービスが必要なセキュリティ機能を提供していることを確認するために、基本機能と提供されている追加機能を確認することが推奨される

（機密データの暗号化）

・ データがローカルストレージ、ネットワークストレージ、クラウドのいずれに保存されているかに関係なく、機密データは常に暗号化することが推奨される
・ 暗号化により、ラップトップやその他のストレージデバイスが紛失または盗難された場合など、誰かがあなたのファイルにアクセスしようとした場合に、他人があなたのデータにアクセスできないようにすることができる
・ 暗号化には様々な方法があり、暗号化の対象（コンピュータ・ラップトップ、スマートフォン・タブレット端末、ファイル・フォルダ・コンテナなど）によって採用する方法のニーズは異なる

（アクセス制御）

・ チームの一員として作業する場合、または他の機関と協力する場合、データファイルへのアクセスを共有する必要がある
・ アクセス制御やファイル許可などの物理的および技術的保護手段を実装し、暗号化

や強力なパスワードと組み合わせて使用することで、必要な特定の個人のみが必要なファイルにアクセスすることが可能となる

（ファイルを安全に転送する）

- データの転送に使用する方法に関係なく、データを不正アクセスから保護するには、転送前、転送中、転送後に機密データとファイルを確実に暗号化することが重要
- 暗号化キーを他の人と共有する場合は、安全に行うための手順を確実に講じる必要があり、暗号化キーやパスワードなどの機密情報を電子メールで送信しないこと。代わりに、面と向かって伝えるか電話で伝えるのが最も簡単で安全な方法である。相手に直接話すことで、キーが間違った受信者に誤って送信されることを防ぎ、直接制御できないサーバに機密情報が保存されることを防止できる

（安全な破壊）

- データを安全に破棄する必要がある場合（たとえば、データ共有契約でプロジェクトの終了時にデータを安全に削除することが求められている場合）、いかなる手段でもデータを復元できないような手順を実行する必要がある
  - ハードディスクからファイルを消去するのに役立つソフトウェア（Windows プラットフォームでは BCWipe、WipeFile、DeleteOnClick、Eraser、MacOS プラットフォームでは Permanent Eraser など）の利用
  - 暗号化キーの削除
  - 磁気消去
  - 分解、破砕、粉砕、焼却による物理的破壊

（リモートワーク）

- 大学管理のコンピュータがない場合は、共用コンピュータの使用を避け、自分専用のコンピュータを使用すること
- アクセスする大学のデータが大学のシステムとストレージに残っていることを確認すること
- 自分のコンピュータに、最新のオペレーティング システムがインストールされていること、パッチが完全に適用されて最新であることを確認し、適切なウイルス対策ソフトウェアがインストールされていることを確認すること
- 機密データを扱っている場合、または信頼できないネットワークから作業している場合は、教育機関の VPN（仮想プライベートネットワーク）を使用して、教育機関のファイルサーバに保持されているデータにアクセスすることを検討すること
- 公共ネットワーク、ホットスポット、会議、ホテルの Wi-Fi を使用して機密データにアクセスすることは避けること

(5) ドイツ

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計 5 機関、8 件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした

（詳細は Appendix 2）参照)。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして 5 件抽出した（表 4.1-36)。

表 4.1-36 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連分野	主催している研究開発プログラム
連邦国防省（BMVg）	多義的技術、宇宙	・ Analyse und Gestaltung des programmatischen Umfelds für den Schutz von Weltraumsystemen
連邦経済エネルギー省（BMWK）	宇宙、海洋	・ The Environmental Mapping and Analysis Program (EnMAP) ・ MARITIME RESEARCH STRATEGY 2025
連邦教育研究省（BMBF）	バイオ、サイバー	・ COMPUTATIONAL LIFE SCIENCES ・ Anwendungsorientierte Quanteninformatik

1）資金配分機関及び研究開発プログラムにおける情報取扱に係る詳細調査結果

a）連邦国防省（BMVg）

■　研究開発領域

多義的技術、宇宙

■　適用範囲

HP 上にて公開されている資料からは BMVg において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[523]。

しかし、ドイツは 2021 年 5 月に IT セキュリティ法改正法（IT セキュリティー法 2.0）が施行されており、改正法に準拠した対応を行っていると思料される[524]。

■　情報の分類

HP 上にて公開されている資料からは BMVg において機密性・完全性・可用性などの観点から BMVg において取り扱われる情報を分類している規程等は確認できなかった[525]。

しかし、ドイツは 2021 年 5 月に IT セキュリティ法改正法（IT セキュリティー法 2.0）が施行されており、改正法に準拠した対応を行っていると思料される[526]。

■　情報管理策

HP 上にて公開されている資料からは BMVg において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[527]。

しかし、ドイツは 2021 年 5 月に IT セキュリティ法改正法（IT セキュリティー法 2.0）が施行されており、改正法に準拠した対応を行っていると思料される[528]。

■　所管する主なプログラムと情報取扱規程

・ Analyse und Gestaltung des programmatischen Umfelds für den Schutz von Weltraumsystemen[529]

【研究領域】宇宙、多義的技術

【概要】

「宇宙システムの保護」の分野における既存の国内および国際的なイニシアティブとプロジェクトを分析し、ドイツの参加の可能性に関してそれらの付加価値を評価することを目的としている。本プロジェクトによって得られた成果をもとに、ドイツの宇宙システムを保

523 https://www.bmvg.de/de

524https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1706854756883

525 https://www.bmvg.de/de

526https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1706854756883

527 https://www.bmvg.de/de

528https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1706854756883

529 https://www.evergabe-online.de/tenderdetails.html?12&id=588994

護するために必要な活動のための国家行動の枠組みの提案を行う想定である。

【参加資格】

ドイツ競争法（GWB）セクション 123、124 及びサブスレッショルド調達規則（UVgO）セクション 31 に準拠しており、犯罪組織等と関係していないことを示す必要がある。

【情報取扱規程】

VS-ONLY FOR SERVICE USE（VS-NfD）- BAAINBw-B 096a の機密情報（VS）の取り扱いに関する規定に準拠する必要がある。また、本プログラム期間中および終了後においても関連する法規制（具体的記載はなし）に従って本プログラムから得られた全ての秘密情報の保護を行う必要がある。

b）連邦経済エネルギー省（BMWK）

■　研究開発領域

宇宙、海洋

■　適用範囲

HP 上にて公開されている資料からは BMWK において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[530]。

しかし、ドイツは 2021 年 5 月に IT セキュリティ法改正法（IT セキュリティ法 2.0）が施行されており、改正法に準拠した対応を行っていると思料される[531]。

■　情報の分類

HP 上にて公開されている資料からは BMWK において機密性・完全性・可用性などの観点から SSC において取り扱われる情報を分類している規程等は確認できなかった[532]。

しかし、ドイツは 2021 年 5 月に IT セキュリティ法改正法（IT セキュリティ法 2.0）が施行されており、改正法に準拠した対応を行っていると思料される[533]。

■　情報管理策

HP 上にて公開されている資料からは BMWK において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[534]。

しかし、ドイツは 2021 年 5 月に IT セキュリティ法改正法（IT セキュリティ法 2.0）が施行されており、改正法に準拠した対応を行っていると思料される[535]。

---

[530] https://www.bmwk.de/Navigation/DE/Home/home.html

[531]https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1706854756883

[532] https://www.bmwk.de/Navigation/DE/Home/home.html

[533]https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1706854756883

[534] https://www.bmwk.de/Navigation/DE/Home/home.html

[535]https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1706854756883

■　所管する主なプログラムと情報取扱規程

・ The Environmental Mapping and Analysis Program (EnMAP)[536,537,538,539,540]

【研究領域】宇宙

【概要】

ドイツで開発および製造された最初のハイパースペクトル衛星プロジェクトである。地表から反射された太陽放射を分析することで、地表の状態や変化を正確に表現することを目標としている。

【参加資格】

記載なし

【情報取扱規程】

EnMAP データの使用は、EnMAP 衛星の所有者である国の委託を受けた DLR が管理するライセンス制であり、個人・法人の使用者は「EnMAP データ使用ライセンス契約」に準拠する必要があり、この契約はドイツの法律に準拠・解釈されている。ライセンス契約では、DLR は EnMAP データの元のピクセル値をリバースエンジニアリングできる範囲で、EnMAP データの独占的所有権および知的財産権を保持している。EnMAP データを使用した付加価値製品については、個人・法人の使用者が生成した付加価値製品に対して、個人・法人の使用者に所有権が認められる。

・ MARITIME RESEARCH STRATEGY 2025[541,542]

【研究領域】

海洋

【概要】

国家研究コミュニティと造船および海洋技術産業を対象として資金提供を行っている。「海事セキュリティのためのリアルタイム技術」および「海事研究」を支援する。優先事項として、①海事環境保護、②海事分野のデジタル化、③海事セキュリティ、④海事資源および⑤環境ニュートラル船舶の 5 つの項目に分かれている。

---

536 https://www.dlr.de/en/research-and-transfer/projects-and-missions/enmap

537 https://www.enmap.org/mission/

538 https://www.gfz-potsdam.de/en/section/remote-sensing-and-geoinformatics/projects/enmap

539 https://www.gfz-potsdam.de/en/press/news/details/ein-jahr-enmap-work-1-enmap-nutzer-workshop

540 https://www.gfz-potsdam.de/en/press/news/details/deutscher-umweltsatellit-enmap-start-in-den-regelbetrieb

541 https://www.ptj.de/projektfoerderung/maritime-forschungsstrategie-2025

542 https://trimis.ec.europa.eu/programme/real-time-technologies-maritime-security-mafo

【参加資格】

①ドイツに恒久的施設または支店を持つ営利企業、②スタートアップ、SMEs、③地方および州の機関、連邦機関、大学、研究機関、非営利団体、が参加可能とされている。

【情報取扱規程】

本プログラムではEUの包括的適用除外規則（GBER[543]）が適用されており、知的財産権で保護されている研究成果については、欧州経済領域（EEA） 内の第三者が市場価格で使用できるようにする非独占的ライセンスを速やかに付与することが奨励されている。

c）連邦教育研究省（BMBF）

■　研究開発領域

サイバー、バイオ

■　適用範囲

HP 上にて公開されている資料からは BMBF において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[544]。

しかし、ドイツは2021年5月にITセキュリティー法改正法（ITセキュリティー法2.0）が施行されており、改正法に準拠した対応を行っていると思料される[545]。

■　情報の分類

HP上にて公開されている資料からはBMBFにおいて機密性・完全性・可用性などの観点からSSCにおいて取り扱われる情報を分類している規程等は確認できなかった 。

しかし、ドイツは2021年5月にITセキュリティー法改正法（ITセキュリティー法2.0）が施行されており、改正法に準拠した対応を行っていると思料される 。

■　情報管理策

HP上にて公開されている資料からはBMBFにおいて取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった 。

しかし、ドイツは2021年5月にITセキュリティー法改正法（ITセキュリティー法2.0）が施行されており、改正法に準拠した対応を行っていると思料される 。

■　所管する主なプログラムと情報取扱規程

・　COMPUTATIONAL LIFE SCIENCES[546]

【研究領域】バイオ

543 https://eur-lex.europa.eu/EN/legal-content/summary/general-block-exemption-regulation.html

544 https://www.bmbf.de/bmbf/en/home/home_node.html

545 https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1706854756883

546 https://www.ptj.de/projektfoerderung/gesundheitsforschung/computational-life-sciences

【概要】
生命科学におけるバイオインフォマティクス処理、モデリング、シミュレーションのための革新的な方法とソフトウェアツールの開発を行っている。

【参加資格】
ドイツに拠点を置く大学、研究機関、企業である必要があり、さらに企業の場合は、補助金の支給時にドイツ国内に事業者又は支店が存在することが求められる。

【情報取扱規程】
ドイツ連邦予算規則(Bundeshaushaltsordnung)等に基づき、研究成果の利用は、ドイツ、欧州経済領域、スイス内でのみ許可されている。また、研究データは、FAIR 原則（発見可能、アクセス可能、相互運用可能、再利用可能なデータ）に従って、再利用可能な形式で提供されるべきとされている。加えて、研究成果はオープンアクセスで公開され、研究データはデジタル形式で提供されることが求められている。

・ Anwendungsorientierte Quanteninformatik[547, 548]

【研究領域】
サイバー

【概要】
量子コンピューティングの潜在的な利用とその社会的、経済的影響に焦点を当てており、量子コンピューティングの実用的な利用を実証すること、またはその基礎を築くことを目的としている。

【参加資格】
ドイツに拠点を置く大学、研究機関、企業である必要があり、さらに企業の場合は、補助金の支給時にドイツ国内に事業者又は支店が存在することが求められる。

【情報取扱規程】
ドイツ連邦予算規則(Bundeshaushaltsordnung)等に基づき、研究成果の利用は、ドイツ、欧州経済領域、スイス内でのみ許可されている。

[547] https://www.foerderdatenbank.de/FDB/Content/DE/Foerderprogramm/Bund/BMBF/anwendungsorientierte-quanteninformatik.html
[548] https://www.quantentechnologien.de/forschung/foerderung/anwendungsorientierte-quanteninformatik.html

2）研究開発実施主体における情報取り扱い実態の調査

情報保全ポリシーの公開されていない民間企業等については机上調査で情報取り扱い実態を把握することが困難であるため、ヒアリングによる調査結果を整理した。政府機関については公開されている内部規則や上位規則についての調査結果を整理した。

a）GFZ[549]

■　参加している研究開発プログラム

The Environmental Mapping and Analysis Program (EnMAP)

■　情報保全体制

GFZ は、一般データ保護規則（GDPR)、その他の EU 加盟国の国家データ保護法、およびその他のデータ保護規制に定義されるデータ管理責任者である。GFZ には、データ保護責任者が指名されており、個人データの保護に関する全般的な責任を負っている。

■　情報保全措置

GFZ は、ウェブサイトの機能提供と関連コンテンツ・サービスの提供に必要な範囲でのみ、ユーザから収集した個人データを処理している。原則として、ユーザの同意を得て個人データを処理するが、事実上の理由で事前の同意が得られない場合や、法令が個人データの処理を許可している場合には例外が適用される。

また、保存された目的がなくなった時点で、個人データは削除またはブロックされる。加えて、EU または国家の立法者によって指定された保管期間が満了した場合、または契約の締結または履行のためにより長く保持する必要がある場合を除き、データは削除またはブロックされることとされている。

549 https://www.gfz-potsdam.de/en/data-protection

（6）フランス

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計5機関、7件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細はAppendix 2）参照)。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして5件抽出した（表 4.1-37)。

表 4.1-37 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連分野	主催している研究開発プログラム
防衛イノベーション庁（AID）	多義的技術、バイオ、サイバー	・ Accompagnement Spécifique des Travaux de Recherches et d’Innovation Défense : appel thématique sur l’extension des zones conflictuelles - fonds marins et espace ・ Accompagnement spécifique des travaux d’intérêt Défense (ASTRID)Edition 2023
フランス国立宇宙研究センター（Centre National d’Études Spatiales : CNES）	宇宙	・ 宇宙監視と追跡（EU-SST）
フランス海洋開発研究所（Ifremer）	海洋	・ Ocean & Climate: an ocean of solutions プロジェクト
国立研究機構（ANR）	バイオ、サイバー、多義的技術	・ Accompagnement spécifique des travaux d’intérêt Défense (ASTRID)Edition 2023

1）資金配分機関及び研究開発プログラムにおける情報取扱に係る詳細調査結果

a）防衛イノベーション庁（AID）

■　研究開発領域

多義的技術

Agence de l'innovation de défense の上位組織である軍事省ではポリシー[550]に従って以下のように機密情報の保護を行っており、下位組織の AID においても本ポリシーが適用されている可能性が考えられる。

■　適用範囲

刑法典で規定される国防秘密に適用さる。刑法典第 413 条 9 において国防秘密とは、国防にとって重要なプロセス、物品、文書、情報、コンピュータネットワーク、コンピュータ化されたデータまたはファイルの配布またはアクセスを制限することを目的とした分類措置として定義されている。

■　情報の分類

情報は、その重要性と領域（防衛、国内安全保障、国家の金融、経済、産業活動などの国家の基本的利益、または国の科学的および文化的財産の保護）に応じて、「機密」と「最高機密」に大別される。これらの分類レベルの違いは、必要とされるセキュリティ対策（物理的、論理的または組織的）の強度によるものであり、以下のように規定されている。

（AID における情報の分類）
- 機密：開示やアクセスが防衛および国家安全保障に害を及ぼす可能性がある情報および媒体
- 最高機密：開示やアクセスが防衛および国家安全保障に極めて重大な影響を与える可能性がある情報および媒体（防衛および国家安全保障に関する政府の優先事項に関わる場合は、首相が定義する特別分類の対象となる）

■　情報管理策

機密情報にアクセスする者を対象として、以下の組織的な情報管理施策が規定されている。実務レベルでは、分類レベルに応じて有効期限と種別が押印された文書や媒体は安全に保管され、権限のある者のみがアクセスできるようにする。また年次調査の対象とすることで、トレーサビリティが確保されている。

（AID における情報分類基準の設定）
- 首相：国防の責任者として、分類基準を含む国防機密の保護に必要な措置を定義する。対象となる要素が収容されている場所のリストを作成し、安全にアクセスするための条件を定義する
- 各大臣：委任により、各省庁で国防秘密として機密扱いにする文書を決定する

（組織の責任）
- 国防安全保障事務局（SGDSN）：国防支援組織として、国防機密の保護に関する安全

[550] https://www.defense.gouv.fr/sga/au-service-armees/droit-defense/informations-classifiees

保障ポリシーを省庁間レベルで設定し調整を行う。そのために必要な措置の提案、普及、施行、監視する責任を負う。EU および NATO からの機密情報のセキュリティの保証や一般安全保障協定の交渉における外国との対話を行う

- 各省庁：直属の大臣の下に属する自然人および法人に対する秘密の保護に関する規定を適用するために国防安全保障高官を設置する
- 官民組織：機密情報にアクセスする組織は、セキュリティ担当官を設置する

（アクセス制限の設定）

- 個人：行政手続きによる許可およびアクセスの必要性の 2 つの要素が必要である。ただし、許可を受けてもすべての機密文書に完全かつ無制限にアクセスすることはできない
- 法人：機密情報および資料にアクセス、管理、または保持する必要性および施設の物理的および人的保護能力の両方の要素を証明できる場合にのみ、機密情報へのアクセスを主張できる

（罰則の規定）

- 情報漏洩を行った場合、5 年の懲役および 7 万 5,000 ユーロの罰金を科せられる可能性がある。権限者が行った場合は、懲役 7 年および 10 万ユーロとより厳しいものになる

■ 所管する主なプログラムと情報取扱規程

- Accompagnement Spécifique des Travaux de Recherches et d'Innovation Défense : appel thématique sur l'extension des zones conflictuelles - fonds marins et espace[551,552]

【研究領域】宇宙、海洋、多義的技術

【概要】

学術研究の企業への技術移転促進を目的とする防衛イノベーションとして、海底領域においては 5 つの軸（環境に関する知識、環境の熟知、監視、回復力および物体と変化の検出）のいずれかに該当する研究プロジェクトを、宇宙領域においては 4 つの軸（環境に関する知識、環境の熟知、監視、回復力）のいずれかに該当する研究プロジェクトを「ASTRID（基礎研究）」および「MATHILDE（産業研究）」としてサポートしている。

【参加資格】

少なくとも 1 つの公的またはそれに類するフランスの研究パートナー（国立研究機構（ANR）基金の対象となる組織または研究および知識普及施設の研究室）と少なくとも 1 つの企業パートナーが含まれるコンソーシアムである必要がある。さらに、EU 加盟国、EEA またはスイス連邦の国民ではない非正規職員がプロジェクトに関与する場合は、応募前に AID による個別の承認が必要である。

551 https://www.defense.gouv.fr/aid/appels-projets/cours/accompagnement-specifique-travaux-recherches-dinnovation-defense-appel-thematique

552 https://anr.fr/fr/detail/call/maturation-thematique-innovation-pour-la-defense-mathilde-appel-thematique-sur-lextension-des/

【情報取扱規程】

「EU 一般データ保護規則（GDPR)」に準拠している必要がある。加えて、募集要項にて、プロジェクトに EU 加盟国以外の国の企業またはフランスに設立された子会社がパートナーとして含まれる場合、軍事省と対象国の署名者との間の拘束力のある規程を含む覚書（MoU）および技術協定（TA）を締結する必要があり、加えて、ANR はプロジェクト実施中にかかる企業が特に EU 圏外の別の組織に支配される可能性を考慮して必要とされる調査をすべて実施できると規定されている。また、the 2019-2025 military programming law（LPM）に従って、データ管理及び迅速な意思決定を行うことも求められている。

b）フランス国立宇宙研究センター（Centre National d’Études Spatiales ： CNES）

■　研究開発領域

宇宙

■　適用範囲

CNES 設置法第 331－1 条～第 331－8 条に基づいて設置され、宇宙活動法に従って研究開発活動を実施しているが、公開されている資料からは、CNES において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[553,554,555]。

■　情報の分類

CNES 設置法第 331－1 条～第 331－8 条に基づいて設置され、宇宙活動法に従って研究開発活動を実施しているが、公開されている資料からは、機密性・完全性・可用性などの観点から CNES において取り扱われる情報を分類している規程等は確認できなかった[556,557,558]。

■　情報管理策

CNES 設置法第 331－1 条～第 331－8 条に基づいて設置され、宇宙活動法に従って研究開発活動を実施しているが、公開されている資料からは、CNES において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[559,560,561]。

■　所管する主なプログラムと情報取扱規程

・　SPACE SURVEILLANCE AND TRACKING (SST)[562]

553 https://cnes.fr/fr/web/CNES-fr/11505-ambition-2020-l-espace-une-ambition-pour-la-france.php

554 https://cnes.fr/sites/default/files/drupal/201512/default/delegation_interne_cnes.pdf

555 https://stage.tksc.jaxa.jp/spacelaw/country/eu/16A-1.J.pdf

556 https://cnes.fr/fr/web/CNES-fr/11505-ambition-2020-l-espace-une-ambition-pour-la-france.php

557 https://cnes.fr/sites/default/files/drupal/201512/default/delegation_interne_cnes.pdf

558 https://stage.tksc.jaxa.jp/spacelaw/country/eu/16A-1.J.pdf

559 https://cnes.fr/fr/web/CNES-fr/11505-ambition-2020-l-espace-une-ambition-pour-la-france.php

560 https://cnes.fr/sites/default/files/drupal/201512/default/delegation_interne_cnes.pdf

561 https://stage.tksc.jaxa.jp/spacelaw/country/eu/16A-1.J.pdf

562 https://sst.cnes.fr/en/sst-space-surveillance-and-tracking-0

【研究領域】
宇宙

【概要】
2030 年まで EU の重要宇宙インフラ（特に Galileo、Copernicus）保護を目的とするプロジェクトであり、衛星や軌道上のデブリの記録とカタログ化を行う。CNES は、衝突警報を処理する運用軌道決定センター (COO) の運用活動や、欧州レベルでのこのシステムの将来のアーキテクチャの定義への貢献を通じて、EU-SST コンソーシアムの活動を支援している。また宇宙監視と追跡は国家安全保障の問題であり、CNES はフランス軍事省とも緊密に連携している。

【参加資格】
記載なし

【情報取扱規程】
REGULATION (EU) 2021/696 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL に準拠する必要があり、EU に本部を置いていない機関が非公開情報にアクセスを希望する場合は、第 218 条に従って契約締結しなければならない。また、本プログラムによって得られた EU 機密情報(EUCI)は Council Decision 2013/488/EU 及び Commission Decision (EU, Euratom) 2015/444 のセキュリティ規則に従って管理される必要がある。

c）フランス海洋開発研究所（Ifremer）

■ 研究開発領域
海洋

■ 適用範囲
公開されている資料からは、Ifremer において取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[563]。

■ 情報の分類
公開されている資料からは、機密性・完全性・可用性などの観点から Ifremer において取り扱われる情報を分類している規程等は確認できなかった[564]。

■ 情報管理策
公開されている資料からは、Ifremer において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[565]。

■ 所管する主なプログラムと情報取扱規程

563 https://en.ifremer.fr/The-Institute
564 https://en.ifremer.fr/The-Institute
565 https://en.ifremer.fr/The-Institute

・ Ocean & Climate: an ocean of solutions プロジェクト[566,567,568,569]

【研究領域】

海洋

【概要】

大統領が設立した優先研究プログラム（PPR）として、主な科学的課題に関する研究の支援を行う。対象は①海外県における気候変動に関わる極端な現象からの保護政策②極海研究の強化③海洋生態系の保護を目的とする海洋の「exposome（人間の健康に影響を与える環境暴露）」の特性把握④海洋のより適正な理解に向けて革新的な観測・モデル化・プログラムの開発⑤新しい統合管理方式の開発を通じた海洋環境の保護と回復力の向上⑥持続可能性の科学に基づく海洋資源の活用⑦参加型科学とオープンサイエンスアプローチを通じた科学的発見と海洋問題の公開に関する研究である。

【参加資格】

フランスの研究機関および大学（少なくとも 2 つの高等教育および研究機関が関与するコンソーシアム）であること。

【情報取扱規程】

機密保持、知的財産などを管理するコンソーシアム契約への署名が必要であり、プロジェクト選考時には ANR が、機密保持規則の厳格な遵守、陪審員または外部専門家とプロジェクトリーダーとの間につながりがないこと、および陪審員と外部専門家との利益相反がないことを保証する必要がある。違反が発生した場合は、ANR はその是正に必要な措置を講じる権利を有する。

本プログラムにおいては、資金調達契約の連絡後 12 か月以内に確立するコンソーシアム契約に基づき研究結果を評価し、その知的財産および産業財産を共有する。また、Open Sience（国家計画）に従って成果物を公開するように求められている。

d）国立研究機構（ANR）

■ 研究開発領域

バイオ、サイバー、多義的技術

■ 適用範囲

・ CONTRAT D’OBJECTIFS ET DE PERFORMANCE ÉTAT/ANR 2021-2025[570]

ANR が資金提供を行ったプロジェクトについて、研究提案の推移の分析と支援資金がもた

566 https://sdgs.un.org/partnerships/france-priority-research-program-ocean-and-climate-ocean-solutions

567 https://www.ocean-climat.fr/

568 https://www.ocean-climat.fr/content/download/156161/file/PPR20210609_VF.pdf

569 https://crds.jst.go.jp/dw/20210624/2021062429119/

570 https://anr.fr/fileadmin/documents/2022/ANR-COP-2021-2025.pdf

らす影響を測定するための、支援対象とするプロジェクトの選択、合意、監視に必要なデータを対象として規定している。

■　情報の分類

・　CONTRAT D’OBJECTIFS ET DE PERFORMANCE ÉTAT/ANR 2021-2025[571]

本資料においては、情報の分類についての規定はなされていなかった。

■　情報管理策

・　CONTRAT D’OBJECTIFS ET DE PERFORMANCE ÉTAT/ANR 2021-2025[572]

ISO 9001 認証の取得、情報システムセキュリティの強化、情報の公開と保護のバランス、情報収集方法の合理化、を行うことで情報管理を行っている。各対策の内容は以下の通り。

（CONTRAT D’OBJECTIFS ET DE PERFORMANCE ÉTAT/ANR 2021-2025 における情報管理策）
【ISO 9001 認証の取得】
ISO 9001 認証の取得により、選択プロセスにおけるユーザの平等な扱い、完全性、公平性、完全な透明性を備えた評価が保証される（目標 4.1）
（情報システムセキュリティの強化）
国家デジタルセキュリティガバナンスフレームワーク(PSSI-E)の 183 規則と ISO/IEC 27002 のベストプラクティスガイドに基づき、情報システムセキュリティポリシー(PSSI)を策定する（目標 6.1.5）
【情報の公開と保護のバランスを保つ】
科学的完全性の保護：科学的完全性の侵害に対処する手順が明確であり、周知され、透明であること、またそれらの手順が、秘密保持および関係者または内部告発者を保護することを保証する（目標 4.2）
管理：機密保持規則の範囲内で、自由に使用できるデータおよび分析と出版物に関して、適切な管理と公開性の原則を適用する（5. プロジェクトの監視と事後評価の強化）
【情報収集方法の合理化】
公開データの使用：プロジェクトの分析と監視を実行するために信頼できる十分なデータを保有することと研究者の利便性を目的として、新たな情報の提出要請よりも研究アーカイブの HAL や研究・高等教育評価高等審議会（Hceres）からの既存データの使用を優先する（目標 5.1）

■　所管する主なプログラムと情報取扱規程

・　Accompagnement spécifique des travaux d’intérêt Défense (ASTRID)Edition 2023[573]

【研究領域】
バイオ、サイバー、多義的技術

【概要】
防衛、民間研究、産業の各分野にとって有益な技術革新の源となる、潜在的なブレーク

571 https://anr.fr/fileadmin/documents/2022/ANR-COP-2021-2025.pdf
572 https://anr.fr/fileadmin/documents/2022/ANR-COP-2021-2025.pdf
573 https://anr.fr/fileadmin/aap/2023/aap-astrid-2023-v4.pdf

スルーを特定することを目指している。ASTRID プログラムの下で実施されるプロジェクトは、将来の防衛・安全保障システムに必要かつ有用な技術の進化を予測し、制御することを目的とした AID 活動の一般的枠組みの一部である。また、本プログラムにより大規模な科学・産業コミュニティを創造し、民間研究との相乗効果を維持・発展させることも目指している。

【参加資格】

フランスの研究に関与する少なくとも一つの公的又は類似の機関（ANR 資金の対象となる研究・知識普及組織または独立機関のラボ）を含んでいる必要がある。企業については、欧州連合加盟国内に実質的な本社を有し、フランス国内に事業所または支店を有する、自律的かつ独立した企業である必要がある。

【情報取扱規程】

本プログラムにおいて得られた個人データは、GDPR6.1 条に従って、収集・処理される。得られたデータは、公共の利益通級や法的義務の遵守のために必要なコンピュータ処理の対象となる。さらに、国家科学技術保護令に従って科学技術的潜在力を保護するシステム（PPST、the system for protecting the scientific and technical potential of the nation）の対策を実施することが求められる。

本プログラムに海外パートナーが含まれている場合には、プロジェクト提案書に記載されている知的財産の共有の原則（防衛のための安全性の観点から合理的な条件下で、その後の産業及び商業権を視野に入れる）必要がある。

2）研究開発実施主体における情報取り扱い実態の調査

情報保全ポリシーの公開されていない民間企業等については机上調査で情報取り扱い実態を把握することが困難であるため、ヒアリングによる調査結果を整理した。政府機関については公開されている内部規則や上位規則についての調査結果を整理した。

a）Airbus[574]

■　参加している研究開発プログラム

SYRACUSE IV

■　情報保全体制

エアバスは、EU の一般データ保護規則（GDPR）および各国の適用される個人データ保護法規に準拠し、個人の権利を保護することにコミットしている。特に、プライバシーと個人データの保護は、プロセス全体を通じて特に注意を払っている。

■　情報保全措置

個人データの収集・使用・共有とデータ転送、データセキュリティについて、以下の定義及び規定を設けている。

（エアバスにおける個人データの収集・使用・共有とデータ転送、データセキュリティについてに関する規程）

【個人データの収集】

・　ウェブサイト、ポータル、アプリケーション、マーケティングコミュニケーションの購読を通じて、直接または間接的に個人を特定できる情報（個人データ）を収集する。これには、名前、メールアドレス、職業データ、位置データ、IT/デジタル活動データ、アカウント情報などが含まれる

【個人データの使用目的】

・　製品/サービスのプロモーション、ブランドプロモーション、消費者プロファイリング、見込み客生成、ビジネスインテリジェンス、IT サービス、顧客サポート、製品/サービスの提供、法的コンプライアンス、会社資産の保護/管理、研究開発などの目的で個人データを使用する

【個人データの共有】

・　必要な範囲内で、エアバスの従業員、パートナー、代理店、サービスプロバイダー、ビジネスパートナー、法執行機関や政府機関などの承認された第三者と個人データを共有する

（国際データ転送）

・　個人データをサーバがある米国に転送し、保存する。この転送は、ユーザの同意に基づいて行われる

【データセキュリティ】

・　技術的および組織的なセキュリティ対策を使用して、個人データを偶発的または意図的な操作、損失、破壊、および不正アクセスから保護する

[574] https://intelligence.airbus.com/legal/privacy-policy/

（7）オーストラリア

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計5機関、6件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細はAppendix 2）参照)。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして5件抽出した（表 4.1-38)。

表 4.1-38 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連分野	主催している研究開発プログラム
国防省（Department of Defence）	多義的技術、サイバー	・ National Intelligence and Security Discovery Research Grants(NISDRG)
オーストラリア宇宙庁（Australian Space Agency: ASA）	宇宙	・ ACSER upgrades satellite receiver for new applications
教育省（DoE）	海洋	・ National Collaborative Research Infrastructure Strategy （NCRIS）2023
オーストラリア農水環境省（DAWE：Department of Agriculture, Water and the Environment）[575]	バイオ	・ Biosecurity Business Grant Program 2020-21 to 2022-23
国家情報局（ONI）	サイバー、多義的技術	・ National Intelligence and Security Discovery Research Grants(NISDRG)

[575] 2022年1月1日から農業・水部門はDepartment of Agriculture, Fisheries and Forestry（DAFF）に、環境部門はDepartment of Climate Change, Energy, the Environment and Water（DCCEEW）として省が新設された

1）資金配分機関及び研究開発プログラムにおける情報取扱に係る詳細調査結果

a）国防省（Department of Defence）

■　研究開発領域

サイバー、多義的技術

■　適用範囲

公開されている資料からは、DoDにおいて取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[576]。

しかし、Australian Parliament Senate Order 12によって、商業上の機密情報・個人を特定できる個人情報・セキュリティ機密情報に該当しない、オーストラリアの公文書館に転送されたファイル、事件関連ファイル、内部機密にあたるファイル以外のファイルのタイトルリストを公開することが義務付けられている[577]ため、何らかの規定に従って情報の範囲を規定していると思料される。

■　情報の分類

公開されている資料からは、DoDにおいて機密性・完全性・可用性などの観点からDoDにおいて取り扱われる情報を分類している規程等は確認できなかった[578]。

しかし、Australian Parliament Senate Order 12によって公開する情報の区分がなされているため、これらに準拠する規定に従って情報の分類を行っていると思料される。

■　情報管理策

公開されている資料からはDoDにおいて取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[579]。

しかし、DoDはAustralian Parliament Senate Order 12に従って情報公開を行っているため、少なくともAustralian Parliament Senate Order 12に準拠した情報管理は実施している。

■　所管する主なプログラムと情報取扱規程

・ National Intelligence and Security Discovery Research Grants(NISDRG)[580]

【研究領域】バイオ、サイバー、多義的技術

【概要】

イノベーションを促進し、国家安全保障及び情報能力を開発し、オーストラリアの国家情報・安全保障コミュニティと研究・技術コミュニティの体系的な連携を実現することを目的とし、新興科学技術に対する理解を深め、情報及び国家安全保障上の関心事項に対処する研究活動を支援している。

---

576 https://www.defence.gov.au/about/accessing-information

577 https://www.defence.gov.au/about/accessing-information/senate-order-12-agency-files

578 https://www.defence.gov.au/about/accessing-information

579 https://www.defence.gov.au/about/accessing-information

580 https://www.grants.gov.au/Fo/Show?FoUuid=765424e6-8767-41e7-a175-ce571c14ced9

【参加資格】
プログラムの助成ガイドラインに掲載されている組織（大学、研究機関）のみが応募できるように規制されている。掲載組織の選考理由については明記されていない。

【情報取扱規程】
受託事業者及びその下請事業者も含めてプライバシー法及びプライバシー原則を順守する必要があり、機密情報を開示する前には、オーストラリア政府の書面による同意が必要である。
本プログラム及び申請書類から生じるいかなる研究成果からの知的財産もオーストラリア政府は所有しない。オーストラリア政府が保有するすべての文書（NISDRG に関するものも含む）は情報の自由法（FOI 法）の対象となり、一般の人々はオーストラリア政府が保有する文書へのアクセスを求めることができる。

b）国家情報局（ONI）

■　研究開発領域
バイオ、サイバー

■　適用範囲
・　Office of National Intelligence Rules to protect the privacy of Australians[581]
国の政治的、戦略的または経済的に重要な問題に関わる公開されているオーストラリア人の個人情報と規定されている。

■　情報の分類
・　Office of National Intelligence Rules to protect the privacy of Australians[582]
ONI が収集する情報は、国の政治的、戦略的または経済的に重要な問題に関わる公開されているオーストラリア人の個人情報であり、情報の分類方法としては、オーストラリア人（市民および永住者）とそれ以外の個人情報となる。

■　情報管理策
・　Office of National Intelligence Rules to protect the privacy of Australians[583]
情報の収集及び管理を目的として、「オーストラリア人であることの推定」、「個人情報の収集」、「諜報情報の保持と取扱い」、「諜報情報の連絡」、「情報の正確性」、「情報安全検察官（IGIS：Inspector General of Intelligence and Security）による監査」の 6 項目が規定されている。諜報情報の保持と取扱いにおいては、情報の紛失、不正アクセス、不正利用、

581 https://www.oni.gov.au/sites/default/files/documents/2022-10/ONI%20Privacy%20Rules%20-%20As%20from%201%20October%202022.pdf
582 https://www.oni.gov.au/sites/default/files/documents/2022-10/ONI%20Privacy%20Rules%20-%20As%20from%201%20October%202022.pdf
583 https://www.oni.gov.au/sites/default/files/documents/2022-10/ONI%20Privacy%20Rules%20-%20As%20from%201%20October%202022.pdf

改ざんまたは開示などの悪用や干渉が行われないように適切な保護を行い、業務に必要な者のみがアクセスできるように管理する旨が記載されている。

■　所管する主なプログラムと情報取扱規程

・ National Intelligence and Security Discovery Research Grants(NISDRG)[584]

【研究領域】

バイオ、サイバー、多義的技術

【概要】

イノベーションを促進し、国家安全保障及び情報能力を開発し、オーストラリアの国家情報・安全保障コミュニティと研究・技術コミュニティの体系的な連携を実現することを目的とし、新興科学技術に対する理解を深め、情報及び国家安全保障上の関心事項に対処する研究活動を支援している。

【参加資格】

プログラムの助成ガイドラインに掲載されている組織（大学、研究機関）のみが応募できるように規制されている。掲載組織の選考理由については明記されていない。

【情報取扱規程】

受託事業者及びその下請事業者も含めてプライバシー法及びプライバシー原則を順守する必要があり、機密情報を開示する前には、オーストラリア政府の書面による同意が必要である。

本プログラム及び申請書類から生じるいかなる研究成果からの知的財産もオーストラリア政府は所有しない。オーストラリア政府が保有するすべての文書（NISDRG に関するものも含む）は情報の自由法（FOI 法）の対象となり、一般の人々はオーストラリア政府が保有する文書へのアクセスを求めることができる。

c）オーストラリア宇宙庁（Australian Space Agency: ASA）

■　研究開発領域

宇宙

■　適用範囲

・ Space（Launches and Returns）Act 2018[585]

ロケット等の打ち上げ施設の設立、打ち上げや帰還等の認可に関する法律であり、これらの宇宙活動に必要な情報を対象としている。

■　情報の分類

584 https://www.grants.gov.au/Fo/Show?FoUuid=765424e6-8767-41e7-a175-ce571c14ced9

585 https://www.legislation.gov.au/C2004A00391/latest/text

・ Space (Launches and Returns) Act 2018[586]
本法律においては、対象となる情報の具体的な分類については記載されていなかった。

■ 情報管理策

・ Space (Launches and Returns) Act 2018[587]
本法律においては、具体的な情報管理策については記載されていなかった。
一方で、情報公開については、宇宙活動の許可、変更、取り消し、一時停止、または移転の認可の際には、大臣が適切だと考える情報を記載した結果通知を DISR のウェブサイトで公開できるとされている。ただし、個人に関する通知の場合は、個人名以外の個人情報（the Privacy Act 1988 の範囲内）を含めてはならないことが規定されており、一定の基準に基づき情報管理がなされていると思料される。

■ 所管する主なプログラムと情報取扱規程

・ ACSER upgrades satellite receiver for new applications[588]
【研究領域】
宇宙

【概要】
オーストラリア宇宙庁の国際宇宙投資イニシアティブからの資金提供を受けてニューサウスウェールズ大学は GPS とガリレオの 2 つの衛星システムからの信号を複数の周波数で受信する高度な GPS 受信機の開発することを目的としている。正確な測位、タイミング、速度情報を提供することが可能になる。これにより衛星から高品質な画像を生成することができる。

【参加資格】
基となるシステム（リクエストに応じて無料で公開）はニューサウスウェールズ大学が開発したシステムであり、それを改良できることが要件として求められる。

【情報取扱規程】
記載なし

d）教育省（DoE）

■ 研究開発領域
海洋

■ 適用範囲
公開されている資料からは、取扱要領を規則で定める情報の範囲や、内部規則の適用範囲

586 https://www.legislation.gov.au/C2004A00391/latest/text
587 https://www.legislation.gov.au/C2004A00391/latest/text
588 https://www.space.gov.au/acser-upgrades-satellite-receiver-new-applications

について網羅的に言及している規程は確認できなかった[589]。
しかし、Freedom of Information Act 1982 (FOI Act)に基づいた情報公開は求められるため、所定の規定に従って情報の範囲を規定していると思料される[590]。

■ 情報の分類

公開されている資料からは、機密性・完全性・可用性などの観点からDoDにおいて取り扱われる情報を分類している規程等は確認できなかった[591]。
しかし、Freedom of Information Act 1982 (FOI Act)に基づいた情報公開は求められるため、所定の規定に従って情報の分類を実施していると思料される[592]。

■ 情報管理策

公開されている資料からはDoEにおいて取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[593]。
しかし、Freedom of Information Act 1982 (FOI Act)に基づいた情報公開は求められるため、所定の規定に従って情報管理策を実施していると思料される[594]。

■ 所管する主なプログラムと情報取扱規程

・ National Collaborative Research Infrastructure Strategy (NCRIS) 2023[595],[596]

【研究領域】

海洋

【概要】

オーストラリアの研究インフラに対する投資戦略である。国の研究インフラの重要部分をサポートし、オーストラリアの研究者が確実にアクセスできるようにするために2018年から2029年までの12年間で40億豪ドルを投資することとしている。海洋領域システムでは、Integrated Marine Observing System (IMOS)、Marine National Facility (MNF)およびNational Sea Simulator (SeaSim)を支援している。

【参加資格】

NCRIS 2018 ガイドライン、NCRIS 2021 ガイドライン、NCRIS 2022 ガイドラインを通じて資金提供を受けた組織、または既存のプロジェクトではカバーされないニーズを満たす

589 https://www.education.gov.au/about-us
590 https://www.education.gov.au/about-department/corporate-reporting/information-publication-scheme-ips
591 https://www.education.gov.au/about-us
592 https://www.education.gov.au/about-department/corporate-reporting/information-publication-scheme-ips
593 https://www.education.gov.au/about-us
594 https://www.education.gov.au/about-department/corporate-reporting/information-publication-scheme-ips
595 https://www.education.gov.au/national-research-infrastructure/resources/national-collaborative-research-infrastructure-strategy-2023-guidelines
596 https://www.education.gov.au/national-research-infrastructure

立場にある組織のみが応募することができる。

【情報取扱規程】

ガイドラインに秘密情報の取扱い条項（13.4 Confidential Information）があり、補助金申請及び契約に関する機密情報について、申請者は事前の書面による教育省の承認がない限り、外部に公開しないことに同意する必要がある。また教育省は、①機密情報であることおよびその理由が示されている、②営業秘密である、③情報を公開すると申請者その他に不当な損害を与える、という条件をすべて満たす場合、当該情報は公開しないとしている。さらに、Freedom of Information Act 1982 (FOI Act)に基づき、公益および情報に関わる個人およびビジネスの保護に必要な場合を除き、the Freedom of Information Coordinatorへの書面申請があれば情報開示が行われる。

e）オーストラリア農水環境省（DAWE：Department of Agriculture, Water and the Environment）[597]

■　研究開発領域

バイオ

■　適用範囲

公開されている資料からは、取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[598]。

しかし、Freedom of Information Act 1982 (FOI Act)に基づいた情報公開は求められるため、所定の規定に従って情報の範囲を規定していると思料される[599]。

■　情報の分類

公開されている資料からは、機密性・完全性・可用性などの観点からDAFFにおいて取り扱われる情報を分類している規程等は確認できなかった[600]。

しかし、Freedom of Information Act 1982 (FOI Act)に基づいた情報公開は求められるため、所定の規定に従って情報の分類を実施していると思料される[601]。

■　情報管理策

公開されている資料からはDAFFにおいて取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[602]。

---

[597] DAWEは2022年1月1日から農業・水部門はDepartment of Agriculture, Fisheries and Forestry (DAFF)に、環境部門はDepartment of Climate Change, Energy, the Environment and Water（DCCEEW）として省が新設された。DAFFは農業、漁業、林業を強化するための活動を行っており、DCCEEW はオーストラリアの自然環境と遺産保護の活動を行っている。

[598] https://www.agriculture.gov.au/about

[599] https://www.agriculture.gov.au/about/reporting

[600] https://www.agriculture.gov.au/about

[601] https://www.agriculture.gov.au/about/reporting

[602] https://www.agriculture.gov.au/about

しかし、Freedom of Information Act 1982 (FOI Act)に基づいた情報公開は求められるため、所定の規定に従って情報管理策を実施していると思料される[603]。

■　所管する主なプログラムと情報取扱規程

・ Biosecurity Business Grant Program 2020-21 to 2022-23[604, 605]

【研究領域】

バイオ

【概要】

オーストラリア北部およびトレス海峡におけるバイオセキュリティに関連した事業機会を開発するための、先住民企業および非営利団体を支援する資金提供することを目的としている。本プロジェクトを通じて、オーストラリア北部における認識、監視、対応を含むバイオセキュリティ能力の向上、先住民コミュニティの経済的機会を増やすことを目指している。

【参加資格】

法人であり、かつ連邦と補助金契約を締結する法的能力を有している必要がある。加えて、「アボリジニおよび／またはトレス海峡諸島民、または先住民組織」または「過去に先住民族と活動した経験や先住民族への支援を行っている非営利団体、登録慈善団体、公的資金を受けた研究組織等」である必要がある。

【情報取扱規程】

プライバシー法及びプライバシー原則に準拠している必要がある。さらに、Freedom of Information Act 1982 (FOI Act)に基づき、公益および情報に関わる個人およびビジネスの保護に必要な場合を除き、the Freedom of Information Coordinator への書面申請があれば情報開示が行われる。

603 https://www.agriculture.gov.au/about/reporting

604 https://www.communitygrants.gov.au/grants/biosecurity-business

605 https://www.communitygrants.gov.au/sites/default/files/documents/2022-06/4214-biosecurity-business-grants.pdf

2）研究開発実施主体における情報取り扱い実態の調査

情報保全ポリシーの公開されていない民間企業等については机上調査で情報取り扱い実態を把握することが困難であるため、ヒアリングによる調査結果を整理した。政府機関については公開されている内部規則や上位規則についての調査結果を整理した。

a）Australian Institute of Marine Science[606]

■　参加している研究開発プログラム

National Collaborative Research Infrastructure Strategy （NCRIS）2023
Reef Restoration and Adaptation Program

■　情報保全体制

AIMS では、プライバシー責任者（General Counsel）が、プライバシーに関する方針の策定と実施を担当している。

■　情報保全措置

IT システムは適用可能なセキュリティ基準とプロセスに準拠しており、以下のような措置を実施している。

（Australian Institute of Marine Science における情報保全措置）
- キーシステムへのアクセス制御とパスワードの設定
- リモートアクセスとデータセンターおよびそのデバイスへの物理的アクセスは、認証されたスタッフのみに制限
- 第三者サービスプロバイダーが AIMS のデータセンターやデバイスへ物理的にアクセスする場合、適切な規定を含む正式な契約アレンジメントが必要
- すべての重要な IT デバイスには特定のセキュリティソフトウェアをインストール
- IT 活動のリアルタイム監視を行い、誤った活動や悪意のある活動を検出・防止
- 政府規制により、特定の個人情報を他の公的機関に提供する必要がある場合は、電子ファイルを暗号化する

606 https://www.aims.gov.au/sites/default/files/2020-12/AIMS-IC-03%20AIMS%20Privacy%20Policy.pdf

(8) インド

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計5機関、8件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細はAppendix 2）参照)。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして5件抽出した（表 4.1-39)。

表 4.1-39 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連分野	主催している研究開発プログラム
国防研究開発機構（Defence Research & Development Organisation)	多義的技術	・ Torpedo/Underwater Vehicle Speed Measurement Device ・ Artificial Intelligence Based Futuristic System For Autonomous Object Detection And Tracking
インド宇宙研究機関（Indian Space Research Organization)	宇宙、海洋	・ Respond BASKET - 2022
地球科学省（MoES)	海洋、宇宙	・ Respond BASKET - 2022
科学技術庁（DST)	バイオ、サイバー、	・ Intensification of Research in High Priority Areas（IRHPA)

1）資金配分機関及び研究開発プログラムにおける情報取扱に係る詳細調査結果

a）国防研究開発機構（DRDO：Defence Research &Development Organisation）

■　研究開発領域

海洋、サイバー、多義的技術

DRDOの上位組織である国防省ではCyber Security Policy 2019[607]に従って以下のように情報の管理を行っており、下位組織のDRDOにおいても本ポリシーが適用されている可能性が考えられる。

■　適用範囲

情報資源の利用者、および情報システムや資源の管理を行うことを任務とする人員に適用され、国防省のすべての部署はこのポリシーに示されているガイドラインを遵守する必要がある。

■　情報の分類

電子的形式での情報は、『文書中の情報コンテンツ(the Nature of Information Cntent in the Documents)』の性質に従って分類され、以下のように規定されている。

（『文書中の情報コンテンツ(the Nature of Information Cntent in the Documents)』における電子的形式の情報の分類）
分類されたシステム分離：セキュリティを伴う木睦情報の取り扱い/処理を行うシステムにおいて、CONFIDENTIAL 以上の分類は、専用で分離されたコンピューティング環境である。このようなシステムはすべて、厳しい物理的アクセス制御機構を備えた安全な場所に保管される。
機密情報の安全な転送：情報所有者はネットワーク上で転送されるために必要な情報のセキュリティ分類が、ネットワーク/メディアのセキュリティ分類と相応になるように行われていることを保証する。

また、サイバーセキュリティの導入は、事業所長が事業所の情報資産の所有者となるという指針に基づいて行われ、情報資産を保護するために、所有者はすべての情報資産のセキュリティ分類と、その試算にアクセスするスタッフの適切なクリアランスレベルを割り当てる責任を負っている。

■　情報管理策

セキュリティポリシーと規格の実施が監視されており、人的及び物理・機器的管理策について以下のように規定されている。

（DRDOの情報管理策）
【人的管理】
・　安全なサイバー環境を確保するために人的管理として、適切なトレーニングとチェックを実施すること
【物理・機器的管理】
・　安全なエリア：情報の処理施設は、最新の物理セキュリティシステムを導入すること。安全なエリアは、許可された人員のみがアクセスできるように管理、規制、監視され

607 https://ddpdos.gov.in/sites/default/files/2019-12/Cyber%20Security%20Policy%20Template.pdf

る必要がある
- 物理・機器的管理：セキュリティ境界線（電気フェンス、監視システム、アクセスカード制御エントリーポイント、有人受付等）は、情報および情報処理施設を含む地域を保護するために使用される
- ネットワークキャブリング：ネットワークキャブリングとテストポイントは、不正な傍受と損害から保護されなければならない。改ざんを検出するための物理的なチェックはセキュリティチェックの一部として実施する必要がある

■ 所管する主なプログラムと情報取扱規程

・ Torpedo/Underwater Vehicle Speed Measurement Device[608]

【研究領域】

海洋、多義的技術

【概要】

新しい魚雷/水中車両の速度測定装置を開発することを目的とし、50 から 60 ノットの速度レベルまでの車両の絶対速度を測定する能力を有する装置を開発することが求められている。

【参加資格】

応募企業は、公開会社、私企業、パートナーシップ企業、有限責任パートナーシップ、一人会社、独資企業として、Companies Act, 1956/2013（会社法）に基づいて登録されている必要がある。企業の場合はインド居住者の市民によって所有および管理されている必要があり、49%を超える外国投資がある企業は資格がない。また、コンソーシアムを形成する際には、「個人の集合体（AOP）協定」に従って行われる必要があり、最大 3 つのメンバーに限定される。

【情報取扱規程】

DRDO と受託者はプロジェクト中に生成される Foreground Information に関する知的財産権の申請（特許申請を含む）を準備、提出、追求、維持するために相互に協議する必要がある。さらに、プロジェクト中に生成される Foreground Information を、互いの事前の書面による許可なしに第三者に開示することは禁じられている。

本プログラムにおいて開発された技術や知的財産権は DRDO と受託者が共有する。

・ Artificial Intelligence Based Futuristic System For Autonomous Object Detection And Tracking[609]

【研究領域】

サイバー

608 https://tdf.drdo.gov.in/project/torpedounderwater-vehicle-speed-measurement-device-1

609 https://tdf.drdo.gov.in/project/artificial-intelligence-based-futuristic-system-autonomous-object-detection-and-tracking

【概要】
独立して展開可能なソリューションであり、(a) 武器としての UAV、(b) 搬送機としての UAV の用途で使用できる自律的な UAV（無人航空機）システムの開発を目指している。

【参加資格】
応募企業は、公開会社、私企業、パートナーシップ企業、有限責任パートナーシップ、一人会社、独資企業として、Companies Act, 1956/2013（会社法）に基づいて登録されている必要がある。企業の場合はインド居住者の市民によって所有および管理されている必要があり、49%を超える外国投資がある企業は資格がない。また、コンソーシアムを形成する際には、「個人の集合体（AOP）協定」に従って行われる必要があり、最大 3 つのメンバーに限定される。加えて、国防省によって禁止/ブラックリストに登録されたり、取引が「一時停止」/「保留」された企業/組織は対象外となる。

【情報取扱規程】
DRDO と受託者はプロジェクト中に生成される Foreground Information に関する知的財産権の申請（特許申請を含む）を準備、提出、追求、維持するために相互に協議する必要がある。さらに、プロジェクト中に生成される Foreground Information を、互いの事前の書面による許可なしに第三者に開示することは禁じられている。
本プログラムにおいて開発された技術や知的財産権は DRDO と受託者が共有する。

b）インド宇宙研究機関（Indian Space Research Organization）

■ 研究開発領域
宇宙

■ 適用範囲
・ Indian Space Policy 2023[610]
インドにおける宇宙政策に関するポリシーで、衛星を活用したデータ取得などの宇宙活動における情報を対象としている。

■ 情報の分類
・ Indian Space Policy 2023
本ポリシーにおいては対象となる情報の具体的な分類については記載されていなかった。

■ 情報管理策
・ Indian Space Policy 2023
本法律においては、具体的な情報管理策については記載されていなかった。
一方で、情報公開については、衛星を利用したリモートセンシングデータを活用としたアプリケーションの公開を行うことや、スペースデブリ軽減について、安全で持続可能な宇宙運用を確保するための枠組みを確立して観察データを関連する利害関係者と共有を図るこ

610 https://www.isro.gov.in/media_isro/pdf/IndianSpacePolicy2023.pdf

と、と記載されており、一定の基準に基づき情報管理がなされていると思料される。

■　　所管する主なプログラムと情報取扱規程

・　Respond BASKET - 2022[611, 612, 613]

【研究領域】

宇宙

【概要】

RESPOND の枠組みの下で、ISRO/DOS センター/ユニット 14 機関が特定した最緊急の研究トピック（約 200 件）を CBPO が取りまとめて、学術界からの詳細な提案を募集し、支援するプロジェクトである。ISRO/DOS センターの専門家が、新規性、方法論、アプローチ、対象分野における PI の経験、プロジェクトの期間、予算等に基づいて評価を行う。

【参加資格】

学術機関/自主研究開発機関に所属する 65 歳未満の研究者・研究者グループと規定されている。

【情報取扱規程】

提案申請の際に、知的財産権の取扱いを含む Terms and Conditions of ISRO Research Grants に対する Declaration Form の提出が求められており、本プログラムにおいて開発された技術や知的財産権は DRDO と受託者が共有する。

c）地球科学省（MoES）

■　　研究開発領域

海洋

■　　適用範囲

・　Right to Information[614]

公開されている資料からは、取扱要領を規則で定める情報の範囲や、内部規則の適用範囲について網羅的に言及している規程は確認できなかった[615]。

しかし、Right to Information に基づいた情報公開は求められるため、所定の規定に従って情報の範囲を規定していると思料される。Right to Information にて情報公開が求められる情報の範囲は以下の通り

（情報に対する権利（Right to Information）に基づく情報の定義） ・　情報（Information）：記録、文書、メモ、電子メール、意見、助言、プレスリリ

611 https://www.isro.gov.in/media_isro/pdf/programme/respond_basket_2022.pdf

612 https://www.isro.gov.in/RESPONDFormsandFormats.html

613 https://www.isro.gov.in/SupportedAreasofResearch.html

614 https://www.moes.gov.in/right-to-information

615 https://www.moes.gov.in/right-to-information

ース、回覧、命令、日誌、契約書、報告書、書類、サンプル、モデル、あらゆる電子形式で保有されるデータ資料など、あらゆる形式の資料のことを指す。また、これには有効な法律に基づき公的機関がアクセスできる、民間団体に関連する情報も含まれる

■　情報の分類

・ Right to Information

公開されている資料からは、機密性・完全性・可用性などの観点から MoES において取り扱われる情報を分類している規程等は確認できなかった[616]。

しかし、Right to Information に基づいた情報公開は求められるため、所定の規定に従って情報の分類を実施していると思料される。

■　情報管理策

・ Right to Information

公開されている資料からは MoES において取り扱われる情報の組織的・人的・物理的・技術的な情報管理策を確認することはできなかった[617]。

ただし、Right to Information のサイトにおいて、情報管理責任者の名前とコンタクト先が公開されており、さらに、MoES の従業員を対象として Right to Information のトレーニングプログラムも開催されている。そのため、一定の基準に基づいた情報管理が行われていると思料される。

■　所管する主なプログラムと情報取扱規程

・ Deep Ocean Mission (DOM)[618,619,620]

【研究領域】

海洋

【概要】

深海資源とその持続可能な利用のために深海を探索し、国の海洋および海事経済を成長させ、気候変動と汚染に取り組むための技術開発を目指すプロジェクト。プロジェクトの内容は i) 深海採掘および有人潜水船技術の開発、ii) 海洋気候変動アドバイザリーサービスの開発、iii) 深海の生物多様性の探査と保全のための技術革新、iv) 深海調査・探査、v) エネルギー・ 海洋からの淡水、vi) 海洋生物学のための先進海洋ステーションの 6 項目に分かれている。その一環として、MoES 傘下の NIOT とインド宇宙研究機関(ISRO)傘下の VSSC が協力して深海資源の探査を行う。

616 https://www.moes.gov.in/right-to-information

617 https://www.moes.gov.in/right-to-information

618 https://www.moes.gov.in/sites/default/files/PIB1806541.pdf

619 https://www.moes.gov.in/sites/default/files/2022-09/Advertisement-for-call-for-proposals-under-DOM2.pdf

620 https://www.indiascienceandtechnology.gov.in/announcementsopportunity/ministry-earth-sciences-moes-announces-call-proposals-collaborative-research-under-deep-ocean

【参加資格】

参加要件として、①All India Council for Technical Education (AICTE)登録番号または University Grants Commission(UGC)通知番号持つ機関・大学、②Scientific and Industrial Research Organizations (SIRO)認定を持つ民間/登録団体および NGO、③National Institution for Transforming India (NITI Aayog)の Unique ID を持つ NGO 等、の条件が課されている。

【情報取扱規程】

本プログラムにおける研究成果を出版又は論文発表する際は、MoES の資金提供によって行われた研究であることを明示する必要がある。

d) 科学技術庁 (DST)

■ 研究開発領域

バイオ、サイバー

■ 適用範囲

・ National Data Sharing and Accessibility Policy (NDSAP)[621]

インド政府が直接または認可された機関を通じて、各省庁／部局／組織／機関および自治体から提供された公的資金を使用して作成、生成、収集、保存されたすべてのデータおよび情報に適用される。対象となる情報の定義は以下の通り。

(官報：National Data Sharing and Accessibility Policy (NDSAP)による情報管理の定義)

- データ(Data)： デジタルおよび/またはアナログ形式の情報、数値集計、観察、文書、事実、地図、画像、図表、概念の表現を意味する
- データアーカイブ(Data Archive)： 機械が読み取り可能なデータを取得、操作、文書化をした上で、分析・消費を目的として他者に配布する場所のこと
- データ生成(Data Generation)： データの初期生成／収集、または同一仕様へのデータ追加のこと
- データセット(Data set)： 加工されたデータまたは情報を含む、論理的に関連する機能の集合体のこと
- 地理空間データ(Geospatial Data):地理的に参照されるすべてのデータのこと
- 情報(Information):加工データのこと
- メタデータ(Metadata)： データソースと、そのデータが作成された時間、場所、条件を記述する情報のこと
- ネガティブリスト(Negative list)： 部門/組織が共有不可能と宣言しているデータのこと
- 制限データ(Resticted Data)： 各部門/組織による登録と承認という所定のプロセスを通じてのみアクセス可能なデータのこと
- 機密データ(Sensitive data)： インド政府の各種法律および規則で定義された個人情報のこと

621 https://dst.gov.in/national-data-sharing-and-accessibility-policy-0

- 共有可能なデータ(Sharable data): ネガティブリストの範囲に含まれず、本質的に機微でないデータのこと
- 標準(Standards): データ処理機能（データ収集、管理、転送、統合、公開など）を組み込み、オープンな標準化団体によって作成・維持されているデータ形式やデータ構文の仕様に準拠した方法でデータを操作するアプリケーションのこと

■ 情報の分類

・ National Data Sharing and Accessibility Policy (NDSAP)

データは公開可能なデータと公開不可のデータに分類されるとの記載はあるが、具体的な分類方法については記載されていなかった。

■ 情報管理策

・ National Data Sharing and Accessibility Policy (NDSAP)

情報管理策については記載されていなかったが、情報公開の方針については以下のように示されている。

(National Data Sharing and Accessibility Policy (NDSAP)の実施方法)
- 科学技術省は、National Infomatics Centre (NIC) を通じて data.gov.in を作成することにより、すべての中央省庁と情報技術省との緊密な連携を通じて、政策の調整と監視の結節点としての機能を果たす
- 共有可能なデータはすべて「現状、有姿 (as-is, where-as)」で提供される
- データとメタデータの技術や標準を含む詳細な実施ガイドラインは、情報技術省が作成する
- データにアクセスする／データを利用するすべてのデータ利用者は、あらゆる形式の出版物において、当該省庁に謝意を表するものとする
- すべての省庁は、政策通知後 3 ヶ月以内に、少なくとも 5 つの価値の高いデータセットを data.gov.in にアップロードする
- 残りのすべてのデータセットのアップロードは 1 年以内に完了する必要がある
- その後、すべてのデータセットを四半期ごとに定期的にアップロードすること
- data.gov.in にはメタデータとデータそのものが掲載され、各省庁のポータルサイトからアクセスできる
- 政府は、共有可能なデータへのオープンアクセスを増やすために、データ所有者に対する適切な予算インセンティブ・システムを設計し、付与する
- 政策とその規定の実施を促進するために、監視委員会を設置する
- 情報技術部門は、情報公開実施のための調整委員会を設置する

■ 所管する主なプログラムと情報取扱規程

・ Intensification of Research in High Priority Areas (IRHPA)[622]

【研究領域】

バイオ、サイバー

[622] https://serbonline.in/SERB/Irhpa_Instruction?HomePage=New

【概要】

高優先領域での研究を強化することを目的としている。複数の学問分野や機関の専門知識が必要な高優先領域の提案を支援し、特定の分野での国際的な科学マップにインドを位置づけることを目指しており、直近ではBSL（生物安全レベル） 3およびABSL（動物生物安全レベル） 3施設の設立を目的とし、感染症原因体の取り扱い、薬剤発見、診断、新しいワクチンの研究に焦点を当てるプログラムや、地球環境をモデリングするためのAI技術の開発に関する募集がなされていた。

【参加資格】

国家研究機関、大学、国家重要機関、またはthe Act of Parliament（議会法）によって設立された機関で、公共部門および民間部門の少なくとも 5 つの機関を含む地域クラスターを設立している必要がある。

【情報取扱規程】

記載なし

2）研究開発実施主体における情報取り扱い実態の調査

情報保全ポリシーの公開されていない民間企業等については机上調査で情報取り扱い実態を把握することが困難であるため、ヒアリングによる調査結果を整理した。政府機関については公開されている内部規則や上位規則についての調査結果を整理した。

a）National Institute of Ocean Technology (NIOT)[623]

■　参加している研究開発プログラム

Deep Ocean Mission (DOM)

■　情報保全体制

NIOT はポータルのコンテンツを管理しており、コンテンツの正確性と現行性を確保するための取り組みを実施している。

■　情報保全措置

NIOT が管理しているポータル内の著作権、プライバシー、ハイパーリンクについて、以下のポリシーに従って管理を実施している。

（NIOT のポータル内の著作権、プライバシー、ハイパーリンクに関する管理）
【著作権ポリシー】
ポータル内に掲載されている素材は、適切な許可を得た後、無料で再生産することができる。ただし、素材は正確に再生産されるべきであり、誤解を招く文脈や軽蔑的な方法で使用されるべきではない。素材を公開または他者に発行する場合は、出典を明確に示す必要がある。
【プライバシーポリシー】
個人を特定できる特定の個人情報（名前、電話番号、メールアドレスなど）を自動的に収集することはない。個人情報の提供を求める場合は、収集目的が明示され、個人情報の保護に適切なセキュリティ対策が講じられる。提供された個人情報は第三者に販売または共有されることはなく、紛失、濫用、不正アクセス、開示、改変、破壊から保護される。
【ハイパーリンクポリシー】
利便性のために他のポータルへのリンクが含まれているが、リンクされたポータルの内容や信頼性に対して NIOT は責任を負わない。リンクされたページの可用性については保証できない。

623 https://www.niot.res.in/websitepolicies.php

(9) 韓国

4.1.1.1 において実施した各国の研究開発動向で明らかとなった資金配分機関及び同機関の主催している研究開発プログラムをそれぞれ計 6 機関、6 件ロングリストとして産業領域・技術分野（宇宙、海洋、バイオ、サイバー、多義的技術）に区分してリストアップした（詳細は Appendix 2）参照)。

そしてリストアップした資金配分機関及び研究開発プログラムのうち、国の政策動向において重要な位置を占める産業分野・技術領域に取り組んでおり、その成果の社会実装に注力していること、及び国の秘密情報取り扱いに係る法令や、複数機関で構成される研究開発推進会議体の規定、及び独自の情報管理規定等に準拠しており、保全措置を講じている研究開発における情報取り扱いの参考となると思われるものであることを考慮して詳細調査を行う機関・研究開発プログラムをショートリストとして 5 件抽出した（表 4.1-40)。

表 4.1-40 詳細調査の対象となる資金配分機関・研究開発プログラムのショートリスト

機関名	関連領域	主催している研究開発プログラム
航空宇宙研究院（KARI）	宇宙	多目的実用衛星 7A 号システム及び本体開発事業委託研究課題
海洋水産科学技術振興院（KIMST）	海洋	2023 年度海洋無人システム実証試験・評価技術開発事業新規課題
韓国生命工学研究院（KRIBB）	バイオ	2022 年度バイオ･医療技術開発事業（社会密着型感染病院泉技術開発）1 次新規課題
韓国知能情報社会振興院（NIA）	サイバー	2022 年量子暗号通信デモインフラ構築・運営公募
民軍協力振興院（ICMTC）	多義的技術	2023 年着手民軍技術協力事業主管研究機関選定公募

1）資金配分機関及び研究開発プログラムにおける情報取扱に係る詳細調査結果

a）航空宇宙研究院（KARI）

■　研究開発領域

宇宙

■　適用範囲

公開されている KARI の規程類からは、KARI の保有する情報や所管する研究開発プログラムにおける情報管理の適用範囲は確認できなかった。

「宇宙開発事業セキュリティ管理規程」は存在するものの、これについては「国家の安全保障に関連して宇宙開発振興法を根拠として未来創造科学部長官（現在の科学技術情報通信部長官だが、現行法令でも古い記載となっている）が関係中央行政機関の長と協議して遂行する宇宙開発事業」を対象としているため、一般的ではないと思料される。

■　情報の分類

公開されている KARI の規程類からは、KARI の保有する情報や KARI の所管する研究開発プログラムにおける情報の分類は確認できなかった。

■　情報管理策

公開されている KARI の規程類からは、KARI や KARI の所管する研究開発プログラムにおける組織的・人的・物理的・技術的な情報管理策は確認できなかった。

■　所管する主なプログラムと情報取扱規程

・　多目的実用衛星 7A 号システム及び本体開発事業委託研究課題

【研究領域】宇宙

【概要】4.1.1(9) 1) c)参照

【参加資格】

本研究開発プログラムに参加を申請する研究開発実施主体については、以下のように「基礎研究振興及び技術開発支援に関する法律」及び同法施行令の基準で参加制限が課されている。

また、過去に履行不良によって研究開発課題が中断された経験のある場合や、不正行為を行ったなど政府が施行する研究開発事業に参加制限を受けている機関及び研究責任者は対象外となる。

（多目的実用衛星 7A 号システム及び本体開発事業委託研究課題の参加要件）

- **「政府出資研究機関等の設立・運営及び育成に関する法律」又は「科学技術分野 政府出資研究機関等の設立・運営及び育成に関する法律」により設立された政府出資研究機関**
- **「特定研究機関育成法」の適用を受ける研究機関**
- **「高等教育法」による大学・産業大学・専門大学及び技術大学**
- **国公立研究機関**
- **「産業技術革新促進法」第 42 条による専門生産技術研究所**

【情報取扱規程】

本研究開発プログラムの公募要領等では研究開発実施主体に対してどのような情報取扱規程の遵守を求めるかについては明言されていない。しかし、公募要領においては「本課題遂行に関連して特に定められていない事項は、『国家研究開発事業の管理等に関する規定』（中略）などを準用する。」と記載されている[624]。

「国家研究開発事業の管理等に関する規定」は、本研究開発プログラムの公募時点（2022年12月）で廃止されており、現在は「国家研究開発革新法施行令」がその位置を占めている。「国家研究開発革新法施行令」及びその上位法令たる「国家研究開発革新法」では、実施される研究開発課題（プロジェクト）のセキュリティ等級を分類して、「セキュリティ課題」に分類された課題に対するセキュリティ対策を研究開発実施主体に求める旨が規定されており、本プログラムで研究開発実施主体に提出を求める計画書にもセキュリティ等級の記載が求められている。

国家研究開発革新法施行令第45条に規定されるセキュリティ課題の分類基準については以下のとおり。

（セキュリティ課題の分類基準）
- 「防衛事業法」第3条第1号による防衛力改善事業に関する研究開発課題
- 次の各首のいずれかに該当する技術に関する研究開発課題
  - 外国で技術移転を拒否して国産化を推進している技術
  - 中央行政機関の長が保護の必要性があると認める未来核心技術
  - 産業技術の流出防止及び保護に関する法律」第2条第2号による国家核心技術
- 「対外貿易法」第19条第1項による輸出許可等制限が必要な技術

そしてセキュリティ課題に分類された課題の遂行にあたっては、「国家研究開発事業セキュリティ対策」において、研究開発実施主体が実施すべき事項や、セキュリティ対策を樹立するにあたって含めるべき事項などが示されているため、表 4.1-41 に措置を組織的・人的・物理的・技術的管理策に整理した[625]。

表 4.1-41　国家研究開発事業セキュリティ対策における情報管理策

区分	措置事項
組織的管理策	セキュリティ課題遂行過程で算出される文書と様々な形式の資料及びデータに対して追加的なセキュリティが必要かどうかを判断し、追加的なセキュリティが必要な場合、セキュリティ等級を区分して表記しなければならない
	上記の場合区分を自律的に定めることができる。ただし、セキュリティ等級を定めることが困難な場合、次の各号のような区分を準用することができる。 ・　Ⅰ級：流出する場合、大韓民国と外交関係が断絶され、戦争を起こし、

624 https://www.kari.re.kr/download/viewer/1643363066340/index.html

625 https://www.law.go.kr/행정규칙/국가연구개발사업보안대책/(2023-39,20231120)

区分	措置事項
	国家の防衛計画・情報活動及び国家防衛に必ず必要な科学と技術の開発を危うくするなどの懸念のあるセキュリティ課題の核心的な情報 ・ Ⅱ級：流出する場合 国家安全保障及び国家競争力確保に莫大な支障を及ぼす恐れのあるセキュリティ課題の核心的な情報で文書や電子媒体流出が課題重要事項の直接的な流出につながる場合 ・ Ⅲ級：流出する場合 国家安全保障及び国家競争力確保に害を及ぼす恐れのあるセキュリティ課題の核心的な情報で文書又は電子媒体流出が課題重要事項の直接的又は間接的な流出につながる場合
	研究開発機関の長は、セキュリティ事故が発生した場合には、その事故を知った直ちに必要な措置を行い、中央行政機関の長に報告しなければならない
	研究開発結果によってセキュリティ課題の有無が変わることがある場合、当該課題の最終評価をする際に、研究開発課題評価団が研究開発結果を考慮したセキュリティ課題の解除・分類ができる
人的管理策	研究開発機関の長は、セキュリティ課題に関して外国政府・機関・団体等と共同研究を遂行しようとする場合や、これらに研究の一部を遂行させようとする場合、中央行政機関の長の事前承認を得なければならない
	セキュリティ課題を遂行しているか遂行してから 3 年が経過しない研究者が外国に所在する政府・機関・団体又は外国人等とセキュリティ課題と関連して接触する場合には、当該接触日から 10 日以内に接触日時・場所・方法・内容等に関する事項を現在所属している研究開発機関の長に報告しなければならない。
	セキュリティ課題を遂行しているか遂行してから 3 年が経過しない研究者が外国政府・機関・団体等の支援を受けて研究開発を行う場合、事前に研究セキュリティ審議会の審議を経て現在の研究者が所属する研究開発機関の長の事前承認を受けなければならない。
物理的管理策	外郭、主要施設物に閉回路テレビ、侵入検知センサーなどの装備を設置・適用する事
	外部入居機関（ベンチャー企業含む）の研究施設内部出入管理措置を設ける事
	研究施設出入者に個人別のアクセス権を区別した付与及び統制、出入り状況管理を行うこと
技術的管理策	セキュリティ課題の実行に使用されたノートパソコン、外付けハードディスクドライブなどの情報通信媒体へのアクセス手順を定める事
	内部ネットワーク接続時のユーザ認証によるアクセス制限措置
	情報システムの使用記録を最低 6 ヶ月保管
	以下のような事項を含む、強化された情報通信ネットワークを使用すること ・ メッセンジャー、インターネットリポジトリ、外部メールなどの資料流出可能経路の接続を遮断 ・ 内部ネットワークの物理的又は論理的（ファイアウォールなど）な分離 ・ 情報通信媒体またはインターネットを通じた外部への資料伝送時は事前届け出等の措置を行う事

区分	措置事項
	・ 非認可の情報通信媒体の使用禁止を定める事 ・ 情報通信媒体の廃棄および外部移送時のセキュリティ措置を定める事 ・ 役職や業務に応じた各種電子資料に対する差別的なアクセス権を付与

b）海洋水産科学技術振興院（KIMST）

■ 研究開発領域

海洋

「海洋漁業研究開発事業セキュリティ管理指針」においては、海洋水産部の所管する研究開発事業（KIMST はその企画・運営を支援する専門機関の位置づけ）、KIMST 及びその研究開発課題を遂行する研究開発実施主体を同指針によるセキュリティ管理の対象とすることが述べられているため、同指針に沿った内容を KIMST については整理する[626]。

■ 適用範囲

「海洋漁業研究開発事業セキュリティ管理指針」の中では「研究開発事業関連情報」「研究開発成果」を保護するためのセキュリティ対策等について述べられている。詳細な用語の定義・範囲は規定されていないものの、研究開発で取り扱う情報全般と成果を管理の対象としている可能性が高いと思われる。

■ 情報の分類

「海洋漁業研究開発事業セキュリティ管理指針」では、他の国家研究開発事業と同様に実施される研究開発課題（プロジェクト）のセキュリティ等級を分類して、セキュリティ課題と一般課題に分けたセキュリティ対策を研究開発実施主体に求める旨が規定されている。そして研究開発課題の遂行過程において作られる全ての文書には、セキュリティ等級を表記しなければならないとされている。セキュリティ課題と一般課題の分類方法は表 4.1-42 のとおり。

表 4.1-42 海洋漁業研究開発事業セキュリティ管理指針でのセキュリティ等級の分類

セキュリティ等級	分類基準
セキュリティ課題	・ 世界初一流技術製品の開発に関連する研究開発課題 ・ 外国で技術移転を拒否して国産化を進めている技術または未来核心技術として保護の必要性が認められる研究開発課題 ・ 「産業技術の流出防止及び保護に関する法律」第 2 条第 2 号の国家核心技術に関する研究開発課題 ・ 「対外貿易法」 第 19 条第 1 項及び同法施行令第 32 条の 2 による輸出許可等の制限が必要な技術に関する研究開発課題 ・ その他、大臣がセキュリティ課題に分類すべき事由があると認める課題

626 https://www.law.go.kr/admRulLsInfoP.do?chrClsCd=010202&admRulSeq=2100000182850

一般課題	セキュリティ課題として指定されない課題

また、研究開発課題が「保安業務規定」によるⅠ級秘密、Ⅱ級秘密、Ⅲ級秘密またはこれに準ずる対外秘に分類された課題と「軍事機密保護法施行令」による軍事Ⅰ級秘密、軍事Ⅱ級秘密、軍事Ⅲ級又はこれに準ずる対外秘に分類された課題については、関係法令による管理を行うとしている。

■　情報管理策

「海洋漁業研究開発事業セキュリティ管理指針」では、他の国家研究開発事業と同様に研究開発課題（プロジェクト）に参加する研究開発実施主体に対して求めるセキュリティ措置が、すべての課題を対象としたものとセキュリティ課題のみを対象としたものに区分されて示されている。表　4.1-43 に措置を組織的・人的・物理的・技術的管理策に整理した。

表 4.1-43　海洋漁業研究開発事業セキュリティ管理指針における情報管理策

区分	措置事項	全ての課題が対象	セキュリティ課題のみ
組織的管理策	本要領又は関係法令により遂行機関のセキュリティ管理の実情を反映した自己セキュリティ管理既定の制定・改訂	●	
	実施課題のセキュリティ管理に関する各種案件を審議するための研究報告審議会の運営	●	
	実施課題のセキュリティ管理業務の総合計画・管理を担当するセキュリティ管理担当者及びセキュリティ業務担当職員の指定・配置	●	
	産業技術革新事業セキュリティ管理部門及び研究人材に対するセキュリティ管理規定教育・広報の実施	●	
	自己セキュリティ管理規定にセキュリティ優秀者及び規定違反者に対する相反措置を明示	●	
	セキュリティ事故予防措置・対応等再発防止策の策定	●	
	実施機関及び研究員に対する定期・随時セキュリティチェック及びセキュリティ教育の実施	●	
	火災、洪水、災害など緊急時対応計画の樹立	●	
	外国企業及び国外研究機関との共同研究、委託研究時大臣の事前承認手続きの履行	●	
	事業遂行結果活用時、国内にいる者を契約締結対象として優先検討	●	
	外部機関とセキュリティ課題の共同（参加機関含む）研究協約時の成果物の帰属、資料提供及び装備返却等に関する事前セキュリティ対策の策定及び適用		●

区分	措置事項	全ての課題が対象	セキュリティ課題のみ
	事業遂行成果物技術実施（使用）契約時「第三者技術実施（使用）権禁止条約」締結		●
人的管理策	参加研究員（外国人含む）の採用・更新・退職時に雇用契約書及び保安誓約書を受け、この場合研究課題のセキュリティ管理義務及びその上半期制裁等を明示	●	
	実施課題の実施研究者のセキュリティ意識を高めるためのセキュリティ関連教育の履修	●	
	退職（予定）者の搬出（予想）資料に対するセキュリティ性の検討、研究成果物の回収、電算網の接続遮断などを随時措置	●	
	参加研究員の国外出張時、事前セキュリティ教育及び帰国報告（出張期間に接触した者及び協議内容等を含む）	●	
	外国人研究員の別途セキュリティ措置（英文セキュリティ誓約書作成、出入地域制限、搬出・搬入物品制限、特異動向管理など）		●
	セキュリティ課題参加研究員が課題と関連して接触する外国人の現状管理		●
	外国人研究員のセキュリティ課題参加時、所属機関の長の承認手続きの履行		●
物理的管理策	実施課題実施過程中に作成される全ての文書にセキュリティ等級を表記	●	
	外郭、主要施設物に閉回路テレビ、侵入検知センサーなどの装備を設置・適用	●	
	外部入居機関（ベンチャー企業含む）の研究施設内部出入管理措置	●	
	研究施設出入者に個人別のアクセス権を区別した付与及び統制		●
	外部訪問者の出入時、セキュリティ管理担当者の事前許可後に担当職員が訪問者とともに訪問地域に同行		●
技術的管理策	ノートパソコン、外付け型ハードディスクドライブなど情報通信媒体の搬入・搬出手続きの準備及び履行	●	
	遂行課題のセキュリティを目的に、コンピュータネットワーク保護の為のファイアウォールシステム､侵入検知システムなど各種機器の設置･運営	●	
	外部から内部ネットワーク接続時のユーザ認証	●	

区分	措置事項	全ての課題が対象	セキュリティ課題のみ
	による情報システムアクセス制限措置		
	コンピュータに各種機器やソフトウェアをインストールする場合、セキュリティ管理担当者の事前承認	●	
	無線通信構築時の非認可ユーザの遮断の為のユーザ認証、暗号通信、暗号鍵の周期的変更などセキュリティ措置	●	
	事前に所属機関から認可されたセキュリティ移動型ストレージ媒体の使用	●	
	セキュリティシステム安全事故に備えたデータバックアップシステムの構築・運営及び遠距離地域のセキュリティ施設に重要データを別途コピー保管	●	
	非認可個人用情報通信媒体の搬入・出入制限及び内部ネットワーク接続制限	●	
	業務用コンピュータ対象セキュリティソフトウェア、セキュリティパッチなどのインストール及びアップデート	●	
	セキュリティ事故に備えて、情報システム使用記録（最低 6 ヶ月以上）保管	●	
	役職・業務に応じて各種計算資料への差別的アクセス権の付与	●	
	ネットワーク資料（システム構成、JP 現況など）の対外セキュリティ管理	●	
	電算装置の廃棄及び外部移管時、ハードディスクドライブ等に提示された主要資料が違法に復旧しないように措置	●	
	内部ネットワークの研究室別の物理的または論理的（ファイアウォール等）分離		●
	業務用コンピュータ資料を携帯電話、携帯型保存媒体など個人用の普通の新媒体にコピー、保存、送信する場合はセキュリティ管理担当者の事前承認		●
	インターネットを利用して外部へ資料転送時、承認手続きなどセキュリティ対策の策定及び履行		●
	メッセンジャー、インターネットリポジトリ、外部メールなどの資料流出可能経路（の特定）		●

■　所管する主なプログラムと情報取扱規程

・　2023 年度海洋無人システム実証試験・評価技術開発事業新規課題

【研究領域】海洋

【概要】4.1.1(9) 1) c)参照

【参加資格】

本プログラムでは、参加資格として国家研究開発革新法及び同法施行令に規定される機関であることを規定しているほか、債務不履行など財務上のリスクが認められる場合は参加を制限される場合があるとしている。

（2023 年度海洋無人システム実証試験・評価技術開発事業新規課題の参加資格のある機関）
・　国または地方自治体が直接設置して運営する研究機関
・　「高等教育法」第 2 条による学校（以下「大学」という。）
・　「政府出資研究機関等の設立・運営及び育成に関する法律」第 2 条による政府出資研究機関
・　「科学技術分野政府出資研究機関等の設立・運営及び育成に関する法律」第 2 条による科学技術分野政府出資研究機関
・　「地方自治体出資研究員の設立及び運営に関する法律」 第 2 条による地方自治体出資研究員
・　「特定研究機関育成法」第 2 条による特定研究機関
・　「商法」第 169 条による会社
・　その他大統領令で定める機関・団体

【情報取扱規程】

情報管理策については、本プログラムに参加する研究開発実施主体は、申請を実施するにあたり、自身の申請課題がセキュリティ課題に当てはまるか否かについて分類したうえで申請を行うこととなっている。また、公募要領で定めない事項については国家研究開発革新法及び同法施行令・施行規則、海洋水産研究開発事業運営規程（「海洋漁業研究開発事業セキュリティ管理指針」の上位規則）に従うとされているため、前記「海洋漁業研究開発事業セキュリティ管理指針」に規定されているセキュリティ措置に従う必要があるものと考えられる。

c）韓国生命工学研究院（KRIBB）

■　研究開発領域

バイオ

■　適用範囲

公開されている KRIBB の規程類からは、KRIBB の保有する情報や所管する研究開発プログラムにおける情報管理の適用範囲は確認できなかった。

■　情報の分類

公開されている KRIBB の規程類からは、KRIBB の保有する情報や所管する研究開発プログラムにおける情報の分類は確認できなかった。

■　情報管理策

公開されている KRIBB の規程類からは、KRIBB の保有する情報や所管する研究開発プログラムにおける情報管理の適用範囲は確認できなかった。

■　所管する主なプログラムと情報取扱規程

・ 2022 年度バイオ･医療技術開発事業（社会密着型感染病院泉技術開発） 1 次新規課題

【研究領域】

バイオ

【概要】

4.1.1(9) 1) c)参照

【参加資格】

本プログラムは、以下のような「国家研究開発革新法」に定める機関や、「基礎研究振興及び技術開発支援に関する法律」に定める企業等のうち、国家研究開発事業の同時遂行課題数などの条件を満たした者に参加資格が認められる。

（2022 年度バイオ･医療技術開発事業（社会密着型感染病院泉技術開発） 1 次新規課題参加資格のある機関）

・ 「国家研究開発革新法」第 2 条第 3 号で定める機関、団体及び当該機関所属研究者
  - 国または地方自治体が直接設置して運営する研究機関
  - 「高等教育法」第 2 条による学校（大学）
  - 「政府出演研究機関等の設立・運営及び育成に関する法律」第 2 条による政府出演研究機関
  - 「科学技術分野政府出演研究機関等の設立・運営及び育成に関する法律」第 2 条による科学技術分野政府出演研究機関
  - 「地方自治体出演研究員の設立及び運営に関する法律」第 2 条による地方自治体出演研究員
  - 「特定研究機関育成法」第 2 条による特定研究機関
  - 「商法」第 169 条による会社
  - その他大統領令で定める機関・団体
・ 「基礎研究振興及び技術開発支援に関する法律」第 14 条の 2 第 1 項により認められた企業付設研究所又は研究開発専属部署を保有する機関、団体及び当該機関所属研究者（次の区分にしたがって、当該研究機関で勤務する研究専門要員を常時確保し、科学技術情報通信部令で定める基準に適合した研究施設を備えた機関）
  - 「中小企業基本法施行令」 第 8 条第 1 項による小企業が設立した企業付設研究機関：3 人以上。ただし、小企業の創業日から 3 年までは 2 人以上とする。
  - 「中小企業基本法施行令」 第 8 条第 2 項による中企業が設立した企業付設研究機関：5 人以上。ただし、小企業で中企業となった企業は、中企業となった日から 1 年までは 3 人以上とする。

- 国外にある企業付設研究機関：5 人以上
- 科学技術情報通信部令で定める科学技術分野 研究機関の研究員及び大学の教員が創業した研究開発型中小企業又は「ベンチャー企業育成に関する特別措置法 」条によるベンチャー企業が設立した企業付設研究機関：2 名以上
- 「中堅企業成長促進及び競争力強化に関する特別法」第 2 条第 1 号による中堅企業が設立した企業付設研究機関：7 人以上
- その他の企業付設研究機関：10 名以上

【情報取扱規程】

本プログラムの公募要領では、研究開発実施主体に求める情報取扱規程等は確認できなかった。しかし、公募要領に定める以外の事項について、国家研究開発革新法及び施行令を参照していることから、施行令におけるセキュリティ関連事項の遵守が求められていると考えられる[627]。

国家研究開発革新法及び同法施行令、国家研究開発事業セキュリティ対策における情報取扱規程については、①航空宇宙研究院（KARI）の「多目的実用衛星 7A 号システム及び本体開発事業委託研究課題」における記載を参照。

d）韓国知能情報社会振興院（NIA）

■ 研究開発領域

サイバー

■ 適用範囲

公開されている NIA の規程類からは、NIA の保有する情報や所管する研究開発プログラムにおける情報管理の適用範囲は確認できなかった。

■ 情報の分類

公開されている NIA の規程類からは、NIA の保有する情報や所管する研究開発プログラムにおける情報の分類は確認できなかった。

■ 情報管理策

公開されている NIA の規程類からは、NIA の保有する情報や所管する研究開発プログラムにおける情報管理の適用範囲は確認できなかった。

■ 所管する主なプログラムと情報取扱規程

・ 2022 年 量子暗号通信デモインフラ構築・運営公募

【研究領域】

サイバー

627 https://www.kribb.re.kr/kor/sub03/sub03_01_03_view.jsp?b_idx=27887

【概要】

4.1.1(9) 1) c)参照

【参加資格】

本プログラムにおける研究開発実施主体は、以下のような機関が自由にコンソーシアムを組成して参加を申請できることとなっている[628]。

（2022 年 量子暗号通信デモインフラ構築・運営公募の参加資格のある事業者）
①通信・放送事業者
②ネットワーク機器・端末メーカー
③サービス・ソリューション会社
④ポータル/CP
⑤研究機関/大学/協会
⑥国家機関/自治体/公共機関

【情報取扱規程】

本プログラムの公募案内書では、提案・プログラムの実行に際し、以下の事項について遵守することを研究開発実施主体には求めている[629]。

（2022 年 量子暗号通信デモインフラ構築・運営公募において遵守を求める情報取扱事項）
・ 公募案内書以外のすべての事項については、提案参加企業の関係者以外の人に公開してはならず、公開した場合、これによるすべての法的責任を負わなければならない。
・ 投入人員は、事業関連で取得した全ての資料を対外秘扱いしなければならない。 ➢ 承認なしに外部流出または他の用途の使用を禁止する。 ➢ 事業に投入される投入人員に対してセキュリティ覚書を締結する。
・ 構築される装備・ソリューションなどのアクセス制御管理を遂行しなければならない。

公募案内の他に、プログラムの運営に関して放送通信発電基金運用・管理規定等の法令等を参照しているが、研究開発実施主体に対する組織的・人的・物理的・技術的な情報管理策の遵守を規定しているものは確認できなかった。

e）民軍協力振興院（ICMTC）

■ 研究開発領域

多義的技術

■ 適用範囲

628 https://doc.msit.go.kr/SynapDocViewServer/viewer/doc.html?key=866c157b39ad4d8299713ce45c1b753c&convType=html&convLocale=ko_KR&contextPath=/SynapDocViewServer/

629 https://doc.msit.go.kr/SynapDocViewServer/viewer/doc.html?key=260e256e1b0b477ea2769233f9c41813&convType=html&convLocale=ko_KR&contextPath=/SynapDocViewServer/

公開されている ICMTC の規程類からは、ICMTC の保有する情報や所管する研究開発プログラムにおける情報管理の適用範囲は確認できなかった。

■　情報の分類

公開されている ICMTC の規程類からは、ICMTC の保有する情報や所管する研究開発プログラムにおける情報の分類は確認できなかった。

■　情報管理策

公開されている ICMTC の規程類からは、ICMTC の保有する情報や所管する研究開発プログラムにおける情報管理の適用範囲は確認できなかった。

■　所管する主なプログラムと情報取扱規程

・　2023 年着手民軍技術協力事業選定公募

【研究領域】

多義的技術

【概要】

4.1.1(9) 1) c)参照

【参加資格】

本プログラムへの参加資格を持つ研究開発実施主体は、以下の「民・軍技術協力事業促進法」第 7 条第 2 項及び同法施行令第 14 条第 2 項に定める機関及び団体と、「高等教育法」第 2 条各号に定める学校であるが、不渡り、法定管理中の企業や直近 2 年決算標準財務諸表負債比率が連続 500%以上または流動比率が連続 50%以下の企業、完全資本浸食状態の企業など財務状況の悪い企業は参加することはできない[630]。

（2023 年着手民軍技術協力事業選定公募における参加資格のある機関）

- **国公立研究機関**
- **「特定研究機関育成法」の適用を受ける特定研究機関**
- **「産業技術研究組合育成法」による産業技術研究組合**
- **「科学技術分野政府出演研究機関等の設立・運営及び育成に関する法律」により設立された政府出演研究機関及び「産業技術革新促進法」第 42 条による専門生産技術研究所**
- **「基礎研究振興及び技術開発支援に関する法律」第 14 条の 2 第 1 項により認められた企業付設研究所**
- **「国防科学研究所法」による国防科学研究所**
- **「民法」や他の法律により設立された科学技術分野の非営利法人である研究機関**
- **「防衛事業法」第 3 条第 10 号による専門研究機関**
- **「高等教育法」第 2 条各号による学校**

630 https://www.icmtc.re.kr/board/view?pageNum=1&rowCnt=10&menuId=MENU00333&schType=0&schText=&categoryId=&continent=&country=&boardStyle=&linkId=952

・ 国内外の研究機関又は団体重民・軍技術開発事業に参加する資格があると産業通商資源部長官が関係中央行政機関の長と協議して認める機関

【情報取扱規程】

本プログラムの公募要領では、研究開発実施主体に求める情報取扱規程等は確認できなかった。しかし、公募要領に定める以外の事項について、国家研究開発革新法及び施行令を参照していることから、施行令におけるセキュリティ関連事項の遵守が求められていると考えられる[631]。

国家研究開発革新法及び同法施行令、国家研究開発事業セキュリティ対策における情報取扱規程については、①航空宇宙研究院（KARI）の「多目的実用衛星 7A 号システム及び本体開発事業委託研究課題」における記載を参照。

その他、民・軍技術協力事業促進法及び同法施行令、民・軍技術協力事業共同施行規定、産業技術革新促進法および同法施行令についても本プログラムにおいては参照されている。

2）研究開発実施主体における情報取り扱い実態の調査

情報保全ポリシーの公開されていない民間企業等については机上調査で情報取り扱い実態を把握することが困難であるため、ヒアリングによる調査結果を整理した。政府機関については公開されている内部規則や上位規則についての調査結果を整理した。

a）LG ユープラス

LG ユープラスは韓国の多国籍財閥企業グループの LG グループに属する大手電気通信事業者である。モバイルデータ通信、コンテンツ配信、5G サービスを用いたスマート工場・モビリティ・セキュリティ等、多岐にわたる電気通信事業を行っている[632]。

■ 参加している研究開発プログラム

本調査においては、韓国知能情報社会振興院（NIA）の所管する「2022 年 量子暗号通信デモインフラ構築・運営公募」において採択されている。

■ 情報保全体制

LG ユープラスでは、IT 運営経歴と情報技術関連の専門能力を保有した情報保護担当者を情報保護最高責任者（CISO）に選任し、CISO、セキュリティオフィサー、主要な下部組織の実務責任者によるセキュリティ委員会を設置している[633]。

631 https://www.kribb.re.kr/kor/sub03/sub03_01_03_view.jsp?b_idx=27887

632 https://www.lguplus.com/biz

633 https://www.lguplus.com/about/ko/sustainability/management-report

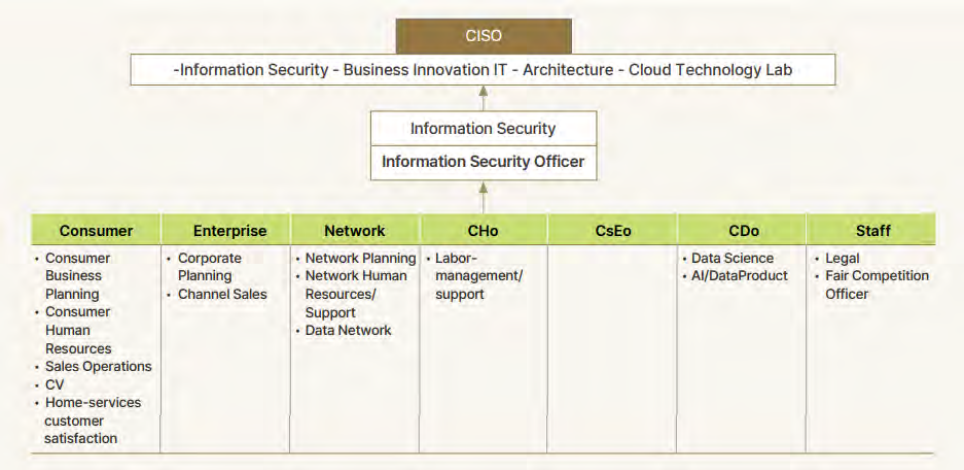


図 4.1-46　LG ユープラスの情報セキュリティマネジメント体制

■　情報保全措置

組織的な管理策として、セキュリティ基準を定めるため全社的なセキュリティ規定、13 のガイドライン、内部管理計画、32 のガイドを制定している。規程類は全社セキュリティポータルに掲載し、従業員がアクセスできるようになっている。規程類は年 1 回以上の定期的な改訂と、問題発生時の追加管理による継続的な更新を行うとしている（図 4.1-47)。また、別途情報保護危機管理マニュアルを制定し、平常時および緊急時の対応・管理活動に関する詳細なガイドラインを制定している。

	Guidelines (13) + Internal Control Plan (1)	Guides (32)
Enterprise security guidelines	• S01 Privacy Statement • S02 IT Security Guidelines • S03 Guidelines for Protecting Trade Secrets • S04 Guidelines for Organizing and Operating an Information Security Organization • S05 Human Security Guidelines • S06 Information Asset Management Guidelines • S07 Guidelines for Establishing and Revising Practice Guidelines • S08 Security Check Guidelines • S09 Geolocation Guidelines • S10 Internal Management Plan for Personal Information Protection • S11 Physical Security Guidelines • S12 Video Privacy Guidelines • S13 Guidelines for the Protection of Integrated Information and Communication Facilities • S15 Credit Information Management Protection Guidelines	• G01 Development Security • G02 Encryption • G03 Outsider IT Security • G04 PC and smart device security • G05 Network Operations Security • G06 Intrusion Detection and Prevention System Security • G07 Intrusion Prevention System Security • G08 VPN Operational Security • G09 Wireless LAN Security • G10 DBMS Security • G11 Web Server Security • G12 Securing UNIX Servers • G13 Securing Windows Servers • G14 Building a Security Server • G15 Security of Personal Information Processing Systems • G16 IT Security Incident Response • G17 Enforcing network isolation • G18 Vaccine Operations • G19 Commercial Device Security • G21 Big Data Security • G23 Building a Public Cloud Service • G24 Smartphone App Privacy • G25 Subcontracting and Third-Party Provision of Personal Information • G26 Guide to creating a privacy agreement and privacy policy • G27 External platform security review and inspection • G28 Pseudonymized (Anonymous) Information Processing Procedures • G29 Pseudonymization • G30 Privacy Attributes Definition Table • G31 Pseudonym (Anonymous) Information Check Site • G32 GHAS Performance Guide • G33 DX Tool Security • G34 Delegation of MyData Services

図 4.1-47　LG ユープラスの定めている情報セキュリティ規程類の構成

また、LG ユープラスは、セキュリティインシデントに対して迅速に対応するために、想定されるリスクに対しクラス A～D のレベル設定を行い、それぞれに応じたインシデント連絡体制を構築している。例えば、クラス D の個人情報漏洩リスクとは「個人情報漏洩・管理違反の兆候が発見された場合」とされている（図 4.1-48）。

Crisis Rating	Information leakage	Service compromise		
	Personal information leakage (Including location information)	Customer service breach (B2B/B2C/Terminal)	Internal service compromise	Network Service compromise
Class A	If leakage of personal information results in criminal penalties or fines (e.g., gross negligence or intentional leakage of the company)	When a failure occurs in the core service of a customer due to a security incident and the entire service is not possible		- If a national service for each network is not possible due to a security incident - In the event of a total failure on an individual unit of IDC
Class B	If a penalty is expected due to leakage/insufficient management of personal information (e.g., poor management/ oversight, etc.)	When a failure occurs in the core service of a customer due to a security incident and some services are not possible, or when a failure of a general service makes it impossible to provide a full service		- In the event of a failure of some services by network or region due to a security incident - In the event of a total failure on an individual unit of IDC
Class C	When a regulatory investigation is conducted/expected due to leakage/ insufficient management of personal information	If a security incident occurs and a service failure is suspected		If it is suspected that service is not possible for each network due to a security incident
Class D	When signs of personal information leakage/management violation are detected	When a security incident occurs, and a service failure occurs in the same industry and requires attention		- When a security incident causes a failure in the same industry by network and requires attention.

図 4.1-48　LG ユープラスのセキュリティインシデント・リスク評価

人的管理策として、新規雇用者や新たな取引先に対して、業務システムのアカウントを新規に作成する場合、初めてシステムを利用する場合は、情報セキュリティ教育を義務付けている。教育を修了しなければ業務ができない仕組みを取ることで全社的な情報セキュリティ意識の向上を図っている他、悪意あるメールの受信・攻撃に係る模擬訓練等を行っている。

技術的管理策として、全社的に U+クラウドという仮想環境で業務を実施させることによってセキュリティを強化していることや、同社の保有する情報通信インフラへの DDoS 攻撃を常時監視し、通信ネットワークを保護していることなどが 2022 年の経営報告書において記載されている。

b）SK ブロードバンド

SK ブロードバンドは、韓国の大手電機通信企業であり、モバイル通信事業や、総合エンターテイメント配信サービスに加え、電気自動車事業についても運営している[634]。

■　参加している研究開発プログラム

本調査においては、韓国知能情報社会振興院（NIA）の所管する「2022 年 量子暗号通信デモインフラ構築・運営公募」において採択されている。

■　情報保全体制

SK ブロードバンドの 2023 年度経営報告書によると、最高経営責任者（CEO）直轄の組織として、最高情報セキュリティ責任者（CISO）、最高個人情報保護責任者（CPO）を設置し、

634 https://www.skbroadband.com/kor/page.do?menu_id=K01020000

各部門が専門的に組織化され情報セキュリティの役割を機能別に 24 時間 365 日専門的に遂行できるように各部門を組織しているとされる。

また「情報通信ネットワーク法」「個人情報保護法」などの関連法改正を定期的に定期的に確認し、社内規程やガイドラインに反映させ、情報通信ネットワーク法や個人情報保護法などの関連法令の改正については、定期的にチェックし、社内規程やガイドラインに反映させ運用している。

上記の対策を SK ブロードバンド情報セキュリティフレームワークとして概念化・整理しており、ISMS 認証基準に基づいた組織的・物理的・技術的なセキュリティ体制を確立しているとしている（図 4.1-49）[635]。

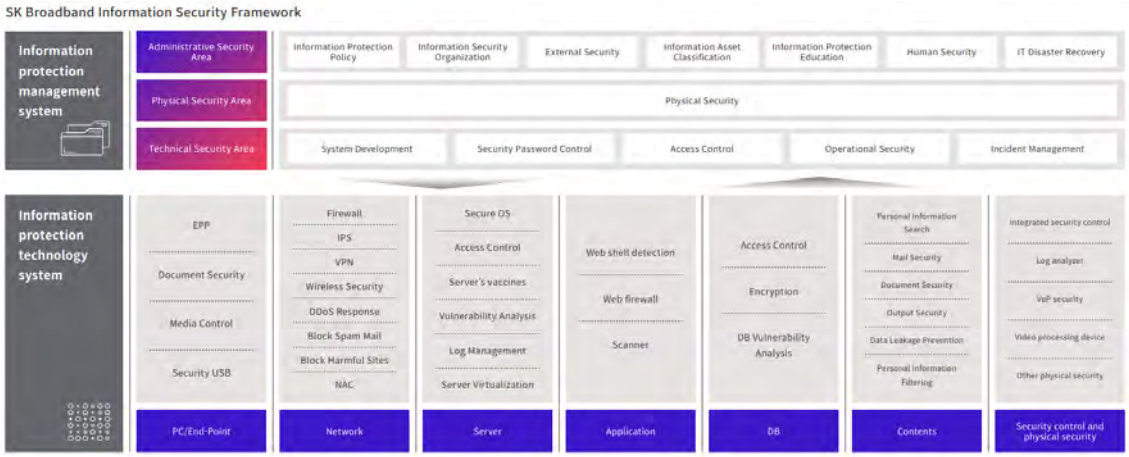


図 4.1-49　SK ブロードバンド情報セキュリティフレームワーク

■　情報保全措置

SK ブロードバンドは、定期的なセキュリティ点検、リスクアセスメント、臨時点検（模擬ハッキング）を実施し、問題点を洗い出し、問題が発見された場合には、速やかに改善計画を作成し、実施するリスクアセスメントプロセスを定めている（図 4.1-50）。

635 https://www.skbroadband.com/data/download/corp/invest/2022%EB%85%84_SK%EB%B8%8C%EB%A1%9C%EB%93%9C%EB%B0%B4%EB%93%9C_%EC%A7%80%EC%86%8D%EA%B0%80%EB%8A%A5%EA%B2%BD%EC%98%81%EB%B3%B4%EA%B3%A0%EC%84%9C_%EC%98%81%EB%AC%B8.pdf

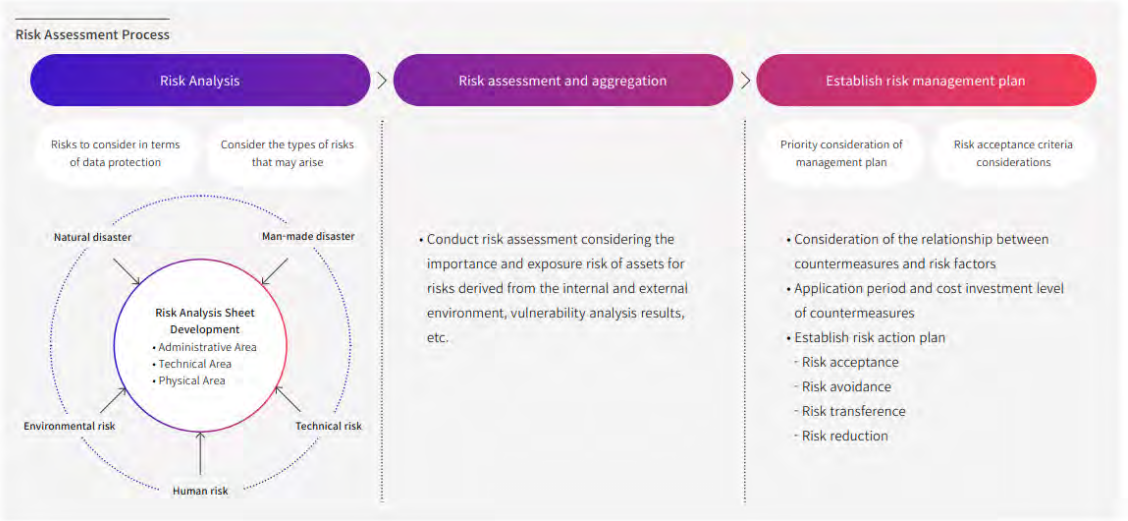


図 4.1-50　SK ブロードバンドのリスクアセスメントプロセス

また、顧客情報漏洩を重大なリスクとして認識し、情報漏洩に迅速に対応、被害を最小限に抑えるために、個人情報漏洩対応マニュアルを策定し、全社的なリスク管理体制をとっている。そして CEO、CISO、CPO を中心とした統合コントロールセンターを組織し、セキュリティインシデントの兆候を常時監視し、インシデントが発生した場合には関係機関や外部機関と連携した対応を実施するとしている（図 4.1-51）。

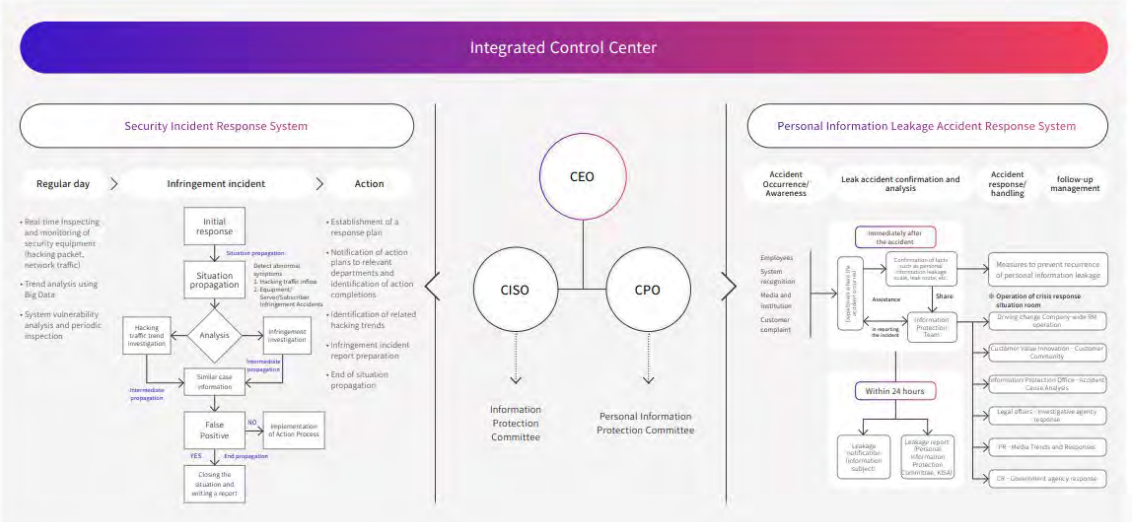


図 4.1-51　SK ブロードバンドのセキュリティインシデント対応システム

4.2 指定基金協議会の効果的な運営に資する事例調査

指定基金協議会の効果的な運営に資する事例調査にあたっては、4.1.1.2 でショートリストとして抽出した資金配分機関・研究開発プログラムの中から、公開情報等が比較的充実しており運営実態を把握することが可能であること、及び特徴的なプログラムの運営モデルを有している等の理由から、日本、米国、英国、韓国の４件を調査対象とすることとした（表 4.2-1）。

表 4.2-1　調査の対象となる研究開発プログラム・資金配分機関

国	名称	種別
日本	安全保障技術研究推進制度	プログラム
米国	SBIR プログラム／DARPA	プログラム 機関
英国	防衛技術活用プログラム(The Defence Technology Exploitation Programme：DTEP)	プログラム
韓国	民軍技術協力事業	プログラム

（1）安全保障技術研究推進制度

安全保障技術研究推進制度は、防衛装備庁によって運営されている、防衛分野での将来における研究開発に資することが期待できる先進的な基礎研究を公募する事業である。採択課題は大規模研究課題のタイプ S、小規模研究課題のタイプ A・C に分類され、タイプ S は最大 20 億円／5 年、タイプ A・C は最大 3 年間でそれぞれ 5200 万円／年、1300 万円／年の支援を受けることができる。

1）研究テーマの選定プロセス

防衛装備庁の公開している研究テーマに関する文書では、「防衛装備庁として、防衛分野での将来における研究開発に資することが期待できると考えて設定した研究テーマではありますが（中略）設定した研究テーマは、民生分野においても大いに発展が期待される研究分野であると認識しています」と記載されているため、ある程度省庁からのトップダウンでテーマを選定しているものと思料される。

そして防衛産業・技術に関する政府指針（防衛技術指針）には安全保障技術研究推進制度の研究テーマと類似性が見られるため、当該制度のテーマ選定にも関連していると思われる。参考として、防衛技術指針 2023 では、防衛省において国の防衛のために優勢を獲得すべき分野を特定した上で、その実現に必要な機能・能力から重要技術分野を導出したことが述べられている（図 4.2-1）。

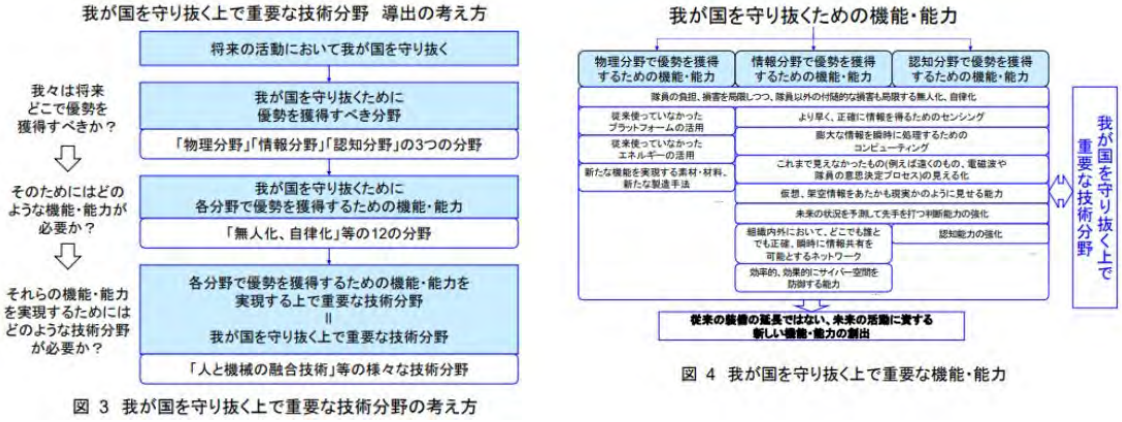


図 4.2-1　防衛技術指針 2023 における重要技術分野導出の考え方

2）公募・採択プロセス

安全保障技術研究推進制度における公募・採択は書類審査、面接審査、最終審査の３ステップで行われる。審査は、大学教授等の外部有識者からなる安全保障技術研究推進委員会が、科学的・技術的見地から実施される。

審査の観点は、タイプ S、A、C である程度共通しているが、タイプ C については小規模な研究を求めているという性格のものではなく、特にチャレンジングな応募を期待していることから、独創的なアイデアや研究能力を中心に審査するとしている（図 4.2-2）[636]。

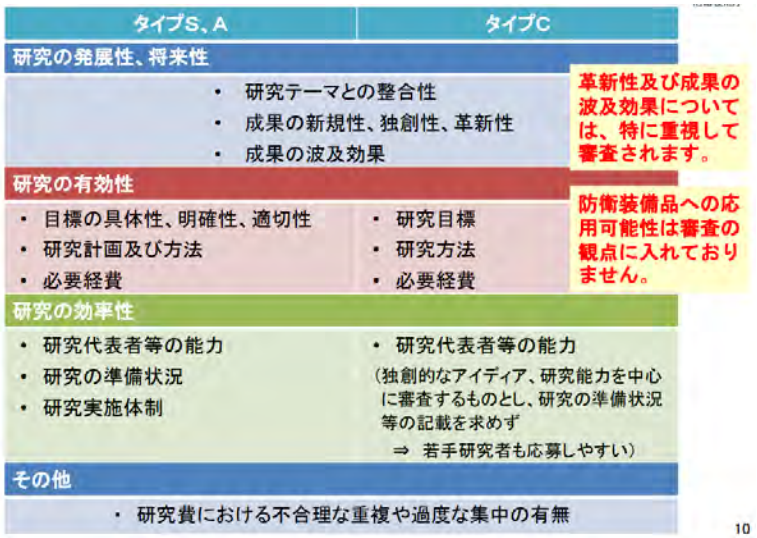


図 4.2-2　安全保障技術研究推進制度のタイプ別審査の観点

3）プロジェクトの評価・管理方法

進捗管理は、研究課題ごとに指名されるプログラムオフィサー（PO）が中心となって実施することとなっており、PO は防衛装備庁所属の研究者が担当する。PO は研究の円滑な実施の観点から、必要に応じ、研究計画や研究内容について調整、助言又は指導を行うが、PO が

636 https://www.mod.go.jp/atla/funding/koubo/r05/r5koubo_setsumei_shiryo.pdf

指導を行うのは、研究費の不正な使用及び不正な受給並びに研究活動における不正行為を未然に防止する必要がある場合のみであり、PO が、研究実施者の意思に反して研究計画を変更させることはないとしている。そのため研究は研究者自身の考えで自主的・自律的に行うものであると強調している。

評価については、全タイプ共通で研究期間終了後に終了評価を行うこととなっており、タイプＳのみ３年度目の１０月頃を目途に中間評価が行われる。それ以外にも、中間評価は、研究課題の進捗状況等から必要に応じて実施される可能性のある旨が示されている。

中間評価の結果によっては、必要に応じて、以後の研究計画の見直し又は中止、研究費の増額・減額、研究実施体制の見直し等の意見が付されることがある。

各評価段階の評価観点は以下の通り。

（安全保障技術研究推進制度における各評価段階の評価観点）
【中間評価の評価観点】
・　研究目標の達成可能性、進捗状況、今後の課題、研究計画、研究の効率性等
【終了評価の評価観点】
・　研究目標の達成度、発展性、計画時に想定していなかった副次的成果等、論文、特許、学会発表等の成果、研究の効率性等

4）知的財産権の扱い

安全保障技術研究推進制度では、受託者による研究成果の公表を制限することはなく、論文誌への投稿や学会発表等も推奨されている。

また研究を実施することにより取得した特許権等の知的財産権については、産業技術力強化法（平成１２年法律第４４号）第１７条（日本版バイ・ドール規定）を踏まえた一定の条件を付した上で受託した研究実施機関に帰属させることができる。なお、政府が公共の利益のために必要がある場合に、当該知的財産権を無償で国に実施許諾することがバイ・ドール制度適用の条件となる。

5）海外企業の参画に係る制約

安全保障技術研究推進制度では研究開発実施主体について、研究を実施する研究者（研究実施者）の所属する機関及び研究実施場所は、原則として全て日本国内に所在していることが必要となる。また、研究開発実施主体は国内に所在し、日本の法律に基づく法人格を有していることが求められており、研究代表者についても日本国籍を有すること、日本語による面接審査や評価に対応できること、研究期間中、応募時に所属していた代表研究機関に継続的に在籍できることが求められていることから、本プログラムに日本国外に所在する海外企業が参加することや、外国人が研究代表者となることはできない。

6）他のプログラム・機関との差別化要素

安全保障技術研究推進制度は、防衛省から研究開発実施主体に秘密情報を提供することや成果を秘密に指定することはないこと、研究開発内容の公表を制限しないこと、採択され

たことによって防衛省又は防衛装備庁が実施する研究開発事業への参加を強制されることはないこと、PO は研究内容について指示・指導をすることは無く研究は研究者自身の考えで自主的・自律的に行うものであること等が事業として強調されている。

上記のように制限を撤廃して、軍事・防衛に係る機関が公募する研究開発プログラムとしてはオープンな実施要領を規定することによって、新領域の開拓や新たな波及効果等が期待できる、革新的な基礎研究の支援を図っているものと考えられる。

(2) SBIR プログラム／DARPA

DARPA は米軍が今直面しているニーズに対応するのではなく、将来のニーズに対応するためのハイリスク・ハイペイオフ研究を支援し実用化を加速させる

リスクが高すぎたりミッションと一致しないなど、他の軍所属研究所では扱わない技術や、既存のシステム・概念を壊すような技術、軍司令部が現時点では必要とは認識していないが、将来的に必要になるであろう技術に投資する。

1) 研究テーマの選定プロセス [637]

研究テーマの設定・公募プロセスには、大きく以下の Step1～5 がある

Step1：解決すべき技術課題の特定

- 軍・DOD 部局のニーズを調査しながら、DARPA が自律的に課題を特定する

Step2：アイデアの生成

- PM が課題解決のための具体的アイデアを研究者・技術者コミュニティから見つけ出す

Step3：プログラムの立ち上げ

- PM がファンディング・プログラムを企画・立案。DARPA 内での承認プロセスを経て公募へ移行。

Step4：公募

- DARPA 局長の研究プロジェクト承認後、BAA（Broad Agency Announcement）による公募

Step5：審査・契約

- PM の裁量で採択案件を選定

[637] https://www.jst.go.jp/crds/pdf/2013/FU/US20130626.pdf

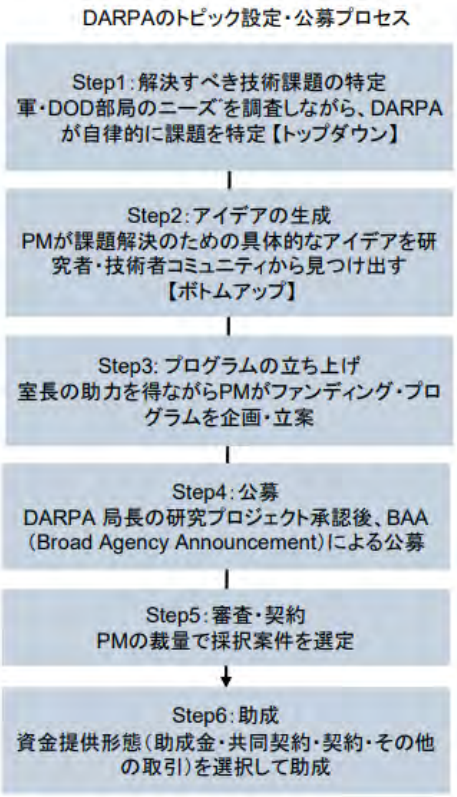


図 4.2-3　DARPA の設定・公募プロセス

選定プロセスは Step1～3 が該当する。各 Step の詳細は以下のとおり。

Step1：解決すべき技術課題の特定

- DARPA は、直近の軍部のニーズと、長期的な戦略の分析によって 2 年毎に戦略計画を策定。DARPA の主要課題は、DOD の 4 年ごとの国防計画見直し（QDR）や国防科学委員会（DSB）等で掲げられた優先事項に対応する。
- DARPA の上級マネジャーと PM は、各軍の次官や司令官など軍関係者と頻繁に意見交換等を重ねて DOD の技術ニーズの把握につとめる。

（DARPA の実施する意見交換の具体例）
・　国防長官、国防次官（技術担当）からの具体的な要請
・　陸・海・空軍、DOD の他の内部部局からの要請・意見交換
・　政府情報機関（CIA、NSA（アメリカ国家安全保障局））からの要請・意見交換
・　NASA、NSF（アメリカ国立科学財団）、FAA（連邦航空局）等や政府以外の機関（NAS（米国科学アカデミー）等）との意見交換

Step2：アイデアの生成

- PM は、全米各地を回って以下のようなルートから、革新的なアイデアとそれを持つ人を探し出す。

（DARPA がアイデアを探し出すルートの具体例）
- 産業界、学界からの提案
- プログラムマネージャー自身の研究者人脈
- 学会への参加、ワークショップの主催
- DSB 等、DOD の諮問機関からの提案
- DARPA がスポンサーをしている研究会からの提案
- 海外技術動向調査：諸外国において発生した技術ブレークスルーからのアイデア抽出

Step3：プログラムの立ち上げについて
- PM は新しいアイデアを見つけ出し、プログラムになるようそれらを統合して提案書を作成、直属の室長（Office Director）にそのアイデアでプログラムを立ち上げることを説得する。
- DARPA 局長に提案するだけの価値があるかどうかを室長が判断する。局長・室長の役割は以下のとおりである。
- 局長・室長の最重要業務は、新しいアイデアを持つ創造性の高いプログラムマネジャーを募集・雇用し、権限を与え、導くこと
- 局長・室長は様々な協力者を結集し、PM に連携を促す
- DARPA 局長、局次長、室長で構成される技術審議会（technology council）で研究プログラムが検討され、局長が最終決定する。

2）公募・採択プロセス[637]

上記のプロセスのうち、Step4～6 が該当する。詳細は以下の通り。

Step4：公募について
- DARPA 局長の研究プロジェクト承認後、BAA（Broad Agency Announcement）による公募

Step5：審査・契約について
- DARPA の PM は、専門家の意見を求めるが、最も魅力があると判断したプロジェクトを選択する権限を持っている。
- 提案内容は、以下の基準に沿った技術審査によって評価・選定される。

（DARPA における技術審査の評価・選定基準）
- 科学的・技術的なメリットがあるか（Overall Scientific and Technical Merit）
- 国防上の課題を解決し、DARPA のミッションに貢献するか（Potential Contribution and Relevance to the DARPA Mission）
- コストの見積もりは現実的か（Cost Realism）
- 提案されたスケジュールは現実的か（Realism of Proposed Schedule）
- 技術移転を実現する計画と能力があるか（Plans and Capability to Accomplish Technology Transition）

・ 提案者の能力と関連する経験は十分か（Proposer’s Capabilities and/or Related Experience）

SBIR を通じて支援する場合に、各フェーズで必要な提案書と評価基準は以下の通り。[638, 639]

フェーズ	内容
フェーズⅠ	● 次の内容からなる提案書を提出 ・ カバーシート 提案する研究開発プロジェクトについて期待される利益、商業的応用等を含む技術概要。 ・ 技術説明 提案する研究開発プロジェクトを直接的、簡潔、かつ十分な情報を提供するよう説明。 ・ コスト計算 費用見積もり。人件費、設備・機器、交通費等を説明。 ・ 商用化レポート 当該企業における過去の SBIR フェーズ II の商用化に関する定量的結果を報告。（売上、追加的投資、DoD による利用実績、特許数、従業員数の増加、株式上場等）（SBIR 利用実績がなくても提出必須。） ・ 外国との提携又は外国との関係の開示 海外拠点の有無や、懸念国（中国、北朝鮮、ロシア、イラン等）からの資金提供の有無、懸念国への知的財産の販売や移転の有無について回答。 ● 原則として次の基準で提案書を評価 ・ 提案された方法、課題解決に向けた進捗の妥当性、技術的メリット、及びイノベーション ・ 代表研究者、支援人員、コンサルタントの有する資格。研究開発の実施だ けでなく、成果を商用化する能力も含む。 ・ 商用利用（政府、または民間）の潜在性、当該商用化から発生が期待される利益（技術的評価で複数の提案者が同等とされた場合、政府へのコストを勘案して決定。）
フェーズⅡ	● 原則として、フェーズⅠ受託者のみが対象。（直接フェーズ II に申請できるパイロットプログラムを除く。） ● 提出書類は、フェーズ Ⅰ に同じ。さらに商用化戦略を述べる（技術を利用した初の製品、顧客・市場規模、上市に必要な費用・調達方法、マーケティングの専門知識の有無、競合他社・競合製品の価格・質、等）。 ● 評価基準は、フェーズⅠに同じ。

638 https://scirex.grips.ac.jp/resources/download/MRI_hokukokusyo_2.pdf

639 https://media.defense.gov/2023/Nov/14/2003339823/-1/-1/0/DoD_SBIR_24.4_Preface_111423.PDF

フェーズ	内容
	● フェーズII受託後は、商用化にかかる成果を定期的に報告する義務がある。

Step6：助成について

- DARPA による研究資金提供には、助成（Grants）、協力契約（Cooperative Agreements）、技術投資契約（Technology Investment Agreements:TIA）、連邦調達規則に基づく調達契約（Federal Acquisition Regulation-based procurement contracts）等がある。

3）プロジェクトの評価・管理方法[640]

フェーズⅡの提案時には、プロジェクトの開始後１年後、完了時、完了後の定量的な事業成果を示すスケジュールを含める必要がある。フェーズⅡの承認後、受託した企業は年に一度、実際の売上と投資のデータを報告する必要がある。

また、各フェーズで最終レポートの提出が求められている。レポートには、プロジェクトの目的、実施した作業、得られた結果、及び技術的な実現可能性の見積もりを含める必要がある。さらに、月次のステータス及び進捗レポートが要求される場合がある。

4）知的財産権の扱い[640]

SBIR の場合、提案に基づいて締結された契約の下で開発された技術データやソフトウェアに関する権利は、一般的に契約業者に残る。しかし、政府は契約の授与からプロジェクト完了後 20 年間、政府目的でこれらのデータを使用するための無償ライセンスを取得する。20 年の制限ライセンス期間が終了すると、政府は SBIR データに関して政府目的権利を持つ。ライセンス期間中、政府は（1）評価目的、（2）契約業者による明示的な許可、または（3）政府が運用するアイテムの緊急修理やオーバーホールに必要な使用、公開、または開示を除き、SBIR データを第三者に公開または開示してはならない。

5）海外企業の参画に係る制約

提案時に外国との提携又は外国との関係の開示をしなければならないので、懸念国との関係性が疑われる企業については、応募の段階で排除するものと思われる。

DARPA の局長と副局長が、各機関全体の優先事項を設定し、バランスの取れた投資ポートフォリオを確保しながら、新しいプログラムを承認し、進行中のプログラムをレビューする。

6）他のプログラム・機関との差別化要素

他方で、SBIR プログラムから資金を受けた小規模ビジネス事業者向けの商業化戦略策定

640 https://media.defense.gov/2023/Nov/14/2003339823/-1/-1/0/DoD_SBIR_24.4_Preface_111423.PDF

ガイドライン [641]には、革新的な研究を実施し、開発マイルストーンを達成するだけでは、成功には十分ではなく、ビジネスの現実的な問題に対処する必要性が強調されている。また、技術移行と商業化を成功させるためには、技術ニーズの評価、市場分析、ビジネス準備計画の要素が盛り込んだ戦略が必要だとされている。このことから、DARPA の SBIR プログラムにおいては、開発マイルストーンの達成はもちろんであるが、技術移行と商業化をより重要視していることがうかがえる。

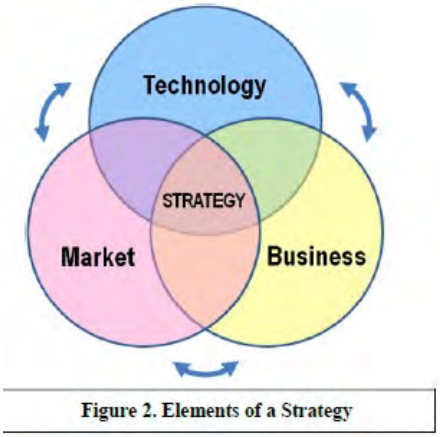


図 4.2-4　DARPA・SBIR の戦略

641 https://www.darpa.mil/attachments/Transition-and-Commercialization-Guide-041922.pdf

(3) DASA（MoD、Dstl）

1）研究テーマの選定プロセス

DASA は市場調査により既存のソリューション、開発中の新しいソリューション、および潜在的にさらなる投資が必要な分野を特定しており、その結果を踏まえて一部が正式な DASA コンテストとして公開されている[642]。

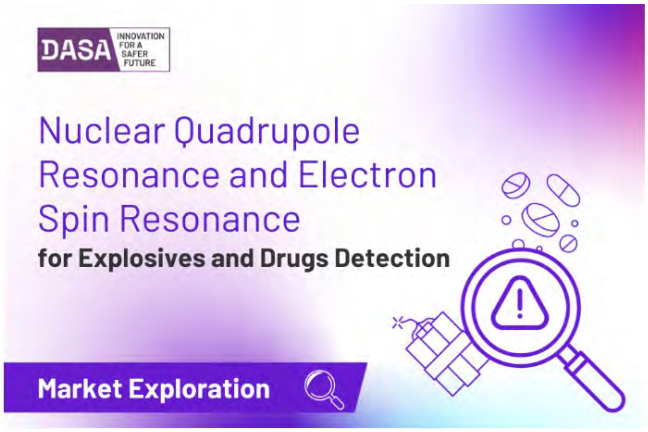


図 4.2-5　DASA での市場調査の例[643]

市場調査に対する回答は DASA submission service[644]を通じて提出が求められ、回答するイノベーションのタイトル、概要、組織、アイデア、テクノロジーの成熟度などの質問項目が主に設定されている。また、質問回答に伴い、いかなる機密情報も提出することは認められず、政府セキュリティ分類ポリシーへの準拠が求められる。なお、DASA が資金提供するイノベーションに関しては、MoD のテクノロジー準備レベル（TRL）を使用して指標が示されている。

表 4.2-2　DASA で適用している TRL の定義

TRL	MoD の定義
1	基本原則の観測・報告
2	技術コンセプトおよび/またはアプリケーションの策定・構築
3	分析的・実験的な重要機能および/または特性の概念実証
4	実験室環境における技術の基本的検証
5	周辺環境における技術の基本的検証
6	周辺環境における技術モデルまたはプロトタイプの実証
7	実用環境における技術プロトタイプの実証
8	試験・実証を通じた実技術の完成・認定
9	ミッションの成功による実技術の認定

642 https://www.gov.uk/government/collections/market-exploration

643 https://www.gov.uk/government/publications/market-exploration-nuclear-quadrupole-resonance-and-electron-spin-resonance-for-explosives-and-drugs-detection

644 https://accelerator-community.force.com/s/

2）公募・採択プロセス

DASA の一般的な公募（コンテスト）は、以下の 10 プロセスで構成されている。

（DASA での公募プロセス）

① コンテストの開始
- 資金申請ページ[645]でコンテストの公募が行われる
- コンテストに関心がある場合は DASA が設置しているイノベーションパートナー[646]に問い合わせを行うことができる

② 提案書の提出
- DASA submission service を通じてオンラインで提案書を提出する
- 提案書提出するに当たっては、プログラムごとに設定される利用規約を熟読すること、及び提案書の評価者が 1 時間 30 分以内に読み・理解し・評価できるように作成することが求められている

③ コンテストの終了

④ プレシフト（事前審査）
- 提案書に対する事前審査プロセスで、「防衛・安全保障への影響について検証されていない」、「競争範囲をどのように満たすか説明されていない」、「技術的評価を行うための技術情報が不足している」、「適切なテクノロジー準備レベル(TRL)に達していない」などに該当する場合、この段階で提案が拒否される可能性がある

⑤ 評価
- プレシフト後、英国政府全体の専門家が提案書を評価するためにアサインされる
- 英国政府以外の人物が評価に使用される場合、機密保持契約が締結される
- 評価フェーズでは、「戦略的適合性」、「エンドユーザのサポートの有無」、「技術的信頼性」、「革新性」、「リスク」、「専門的知識」、「コスト（コストパフォーマンス）」、「プエロジェクトの実施計画」などが基準として設定される

⑥ モデレーション
- 評価後、モデレータが提案概要や評価コメントをまとめ、当該提案に対する「助成（資金提供）」、「助成（資金提供）なし」を推薦する形式で、総合的な結果を提供する

⑦ チャレンジ
- 利害関係者／モデレータは、各提案に対して出された「助成」または「助成なし」の勧告に異議を唱えるよう求められる
- 異議申立人は、書面を配布し、また決定会議において自分の主張を発表する

⑧ 決定会議
- 主要な利害関係者が一堂に会して勧告について議論する
- モデレータは決定会議に出席し、提案に対する「助成」または「助成なし」の勧告を提示し、提出された異議に対して提案を弁護する
- 異議申立人は、「助成」または「助成なし」の決定を下す前に、しっかりとした議論を行うために、決定会議に出席して異議申立を行う

645 https://www.gov.uk/government/collections/apply-for-funding

646 https://www.gov.uk/guidance/contact-a-dasa-innovation-partner

- 決定会議の最後に、各提案に対して出資するかどうかの決定が下される
- イノベーターは決定会議に出席することはできない

⑨ 採択結果のリリース

- 採択された場合、決定後すぐにコマーシャル・チームから契約開始の連絡を行う
- 提案の詳細は、DASA の透明性データの一部として DASA のウェブサイトで公開される

⑩ フォードバックのリリース

- 落選した場合、該当する決定日から数週間以内に書面による簡単なフィードバックが送られる
- フィードバックは全審査員のコメントと決定会議での議論に基づき、モデレータによって作成される

3）プロジェクトの評価・管理方法

契約後は、DASA のスタッフとテクニカルパートナーの両方が、プロジェクトの期間中、サポートとアドバイスを行う。

期間中、随時の進捗報告、中間報告書及び最終報告書の作成・提出が契約条件に基づき求められる。契約に基づくすべての報告書は、MoD のために作成される科学技術報告書の体裁、書式、作成に関する要件を定義した国防研究報告書仕様書（DRRS）[647]に準拠しなければならない。

（各種報告書に対する要件）

- 中間報告書および進捗報告書
  - 対象期間中に行われた作業の結果を詳細に、文書化し、要約したものでなければならず、達成された結果、実質的な実績、現在の実質的な実績の説明、遭遇した問題点および／または存在する可能性のある問題点を、提案された是正措置とともに包括的に説明するのに十分な詳細さでなければならない
  - 計画された進捗と実際の進捗との間に差異がある場合、なぜ差異が生じたのか、また、計画された進捗より遅れている場合、どのような是正措置が計画されているのかについての説明を行う必要がある
- 最終報告書
  - 契約に基づいて実施された作業全体について、実施された作業と達成された結果を包括 的に説明するのに十分な詳細さで記載するものとし、その中で開発されたハードウェア、ソフトウェア 、プロセス、またはシステムのすべての関連する技術的詳細を含むものとする。技術的な詳細は、当該 プロセスまたはシステムの独立した複製を可能にするのに十分なものでなければならない

4）知的財産権の扱い

DASA では、DEFCON 705 に準拠した知的財産権に関する扱いを定めており、すべてのフォ

647 https://www.gov.uk/guidance/submit-a-report-to-athena

アグランド知的財産権（当該契約に基づく業務の遂行において発生する技術情報に含まれる知的財産権）は契約者（プログラムの採択者）に帰属することを基本としている。

一方でDASAは、提供された技術情報および関連する知的財産を特定の目的で使用するための一連の権利を取得する。

（DASAで技術情報、知的財産に対して取得可能な権利の例

- **英国政府省庁、英国警察および民間防衛機関に開示すること**
- **研究技術協定に基づき政府機関または政府間機関に開示すること**
- **契約期間中またはその後5年間などの機関において契約者に対して防衛市場及びその他の市場におけるフォアグランド技術情報・知的財産の活用計画について報告するよう要求すること　など**

また、契約者はフォアグランド技術情報またはその一部を公表することができるが、公共機関が国益に反すると判断した場合は契約者に異議を申し立てることができる。そのために契約者は公表を意図していることを事前に公共機関に書面で通知し、公共機関が異議を申し立てるために45営業日の猶予を与えることとしている。

なお、MoD系列の機関における知的財産に関する規則としては、DEFCON 705の他にDEFCON 703が存在する。DEFCON 703が適用される場合、MoDが契約に伴う知的財産権をすべて所有し、契約者に利用する権利は付与されない。DEFCON 703はMoDが全額出資する業務に適用され、結果の開示および利用を管理するためにMoDによる所有が必要とされる、または他国政府に対して負う義務を遵守するために必要とされる、極めて機微な性質を有する業務などが該当する。

5）海外企業の参画に係る制約

DASAのプログラムでは、民間企業、学術機関、個人（個人事業主）、および公共研究機関の参加を歓迎しており、ほとんどの場合、その国籍に対して制限を設けていない（契約を締結する前に組織の法的地位を調査は実施する）。他方、個々のプログラムの応募要領には必要な制限が詳細に記載されるとしており、プログラムによっては制限を設定する場合もあると想定される[648]。

6）他のプログラム・機関との差別化要素

市場調査を行い広範な民間企業や学術団体からニーズを収集し、それを参考に研究テーマを選定しており、企画段階から実用化に繋がる可能性の高いテーマを意識していると想定される。

また、Ideas Marketplace（アイデアマーケットプレイス）というプラットフォームを設けており、英国のイノベーターが防衛とセキュリティの分野で優秀な人材と簡単に連携できるように設計されている。

[648] https://www.gov.uk/guidance/defence-and-security-accelerator-terms-and-conditions-and-contract-guidance

（4）防衛技術活用プログラム（DTEP）[649]

DTEP は、英国全土の中小企業(SME)が革新的な材料、技術、プロセスを開発し、防衛サプライチェーンの強化を目的とした最高 1,600 万ポンドで 3 年間の助成金ベースの技術開発プログラムで、2021 年 3 月の国防・安全保障戦略（DSIS）[650]の中で、英国全土で取組まれることが発表された。DTEP は、2022 年 7 月から、Innovate UK と提携して MoD 傘下の DASA によって提供され、英国に登録された下位層サプライヤー（SME）と上位層サプライヤーの間のコラボレーションに最大 50%の助成金を提供する（図 4.2-6）。

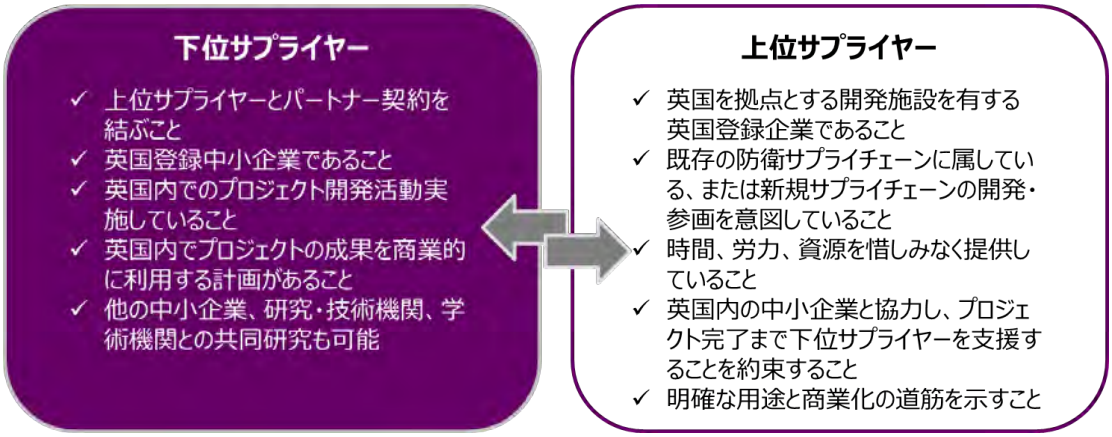


図 4.2-6　DTEP が求められるサプライヤー間のパートナーシップ [651]

1）研究テーマの選定プロセス

DTEP で扱う研究テーマは、国務長官が承認した MoD の永続的能力(Enduring Capability)課題に合致していることが求められる。MoD の永続的能力課題は、DSIS や長期的な軍事能力の優先順位と課題を明確にした国防能力フレームワーク [652]と一致していることから、MoD の防衛ニーズに基づいてテーマが選定されていると考えられる。

表 4.2-3　MoD の永続的能力課題とそれに対応する DTEP で求める研究テーマ

能力課題	DTEP の研究テーマ（技術領域）
1. 広範なフルスペクトル・マルチドメイン諜報・監視・偵察（ISR）	1.1 処理、評価、配布（PED）
	1.2 処理、評価、配布（PED）

649 https://www.gov.uk/government/publications/the-defence-technology-exploitation-programme/guidance-document-the-defence-technology-exploitation-programme-dtep#section-3

650 https://www.gov.uk/government/publications/defence-and-security-industrial-strategy/defence-and-security-industrial-strategy-accessible-version

651 （https://assets.publishing.service.gov.uk/media/63738b978fa8f5596451d5eb/DASA_DTEP_Webinar_Presentation.pdf）を参考にＮＴＴデータ経営研究所で作成

652 https://assets.publishing.service.gov.uk/media/62d7d1668fa8f50c0a8a4029/MOD_Defence_Capability_Framework_Accessible_Jul22.pdf

能力課題	DTEP の研究テーマ（技術領域）
	1.3 センサーと検出器
2. マルチドメインのコマンド、制御、通信およびコンピューティング（C4）	2.1 ヒューマンマシンのチーミング
	2.2 将来の軍事衛星通信を実現する技術（MilSatCom）
3. サブスレッショルドにおける優位性の確保と維持	3.1 ソーシャルメディアの「影響力」キャンペーンの最適化と評価
	3.2 通信のセキュリティと復元力
4. 非対称性とハードパワー	4.1 脅威の検出
	4.2 防御策
5. アクセスと作戦行動の自由	5.1 UXV のスウォーミングと高度な連携
	5.2 スペース・ドメイン・アウェアネス（SDA）強化のためのソリューション
	5.3 サポートチェーンの最適化技術

2）公募・採択プロセス

公募・採択は、STEP1：防衛サプライチェーンに利益をもたらすプロジェクトの特定（Identity）、STEP2：概略提案書の作成と専門家によるレビュー（Review）、STEP3：完全な提案書の完成とピッチ（Pitch）、STEP4：MoD による提案書の評価（Assesment）、STEP5：採択（Grant）の 5 つのプロセスで構成される。

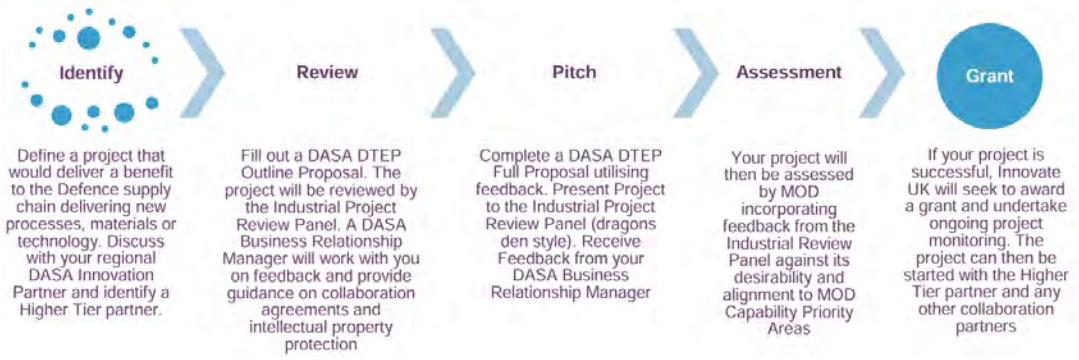


図 4.2-7　DTEP の公募・採択の流れ [653]

（DTEP の公募・採択プロセスの詳細）

① Identity

- 新たなプロセス、材料、技術をインプットすることで、防衛サプライチェーンに利益をもたらすプロジェクトを定義するプロセス
- このプロセスではコンソーシアムを形成する上位サプライヤーを特定することが求

[653] https://assets.publishing.service.gov.uk/media/63738b978fa8f5596451d5eb/DASA_DTEP_Webinar_Presentation.pdf

められるが、上位サプライヤーの特定に当たっては、DASA のビジネス・リレーションシップ・マネージャー（Business Relationship Managers）に相談することが推奨されている
- ビジネス・リレーションシップ・マネージャーは、効果的なコンソーシアムの形成やプログラムの仕組みに関するガイダンスを提供し、申請プロセス全体を通じて支援を提供する

②Review
- 概略提案書を作成するプロセス。概略提案書は産業界の専門家を含む産業プロジェクト審査委員会（Industry Project Review Panel）によって、革新性、MoD の永続的能力課題への適合性、商業化の可能性についてレビューされる。産業プロジェクト審査委員会には、さまざまな防衛組織や英国の幅広い地域を代表する産業界の専門家が含まれる
- その後、ビジネス・リレーションシップ・マネージャーを通じて産業プロジェクト審査委員会からのフィードバックを受け、提案をブラッシュアップする。なお、ビジネス・リレーションシップ・マネージャーは、共同研究契約や知的財産の保護に関するガイダンスも提供する

③Pitch
- 産業プロジェクト審査委員会のフィードバックを踏まえて提案書を完成させ、ピッチを行うプロセス。産業プロジェクト審査委員会が完成した提案書とピッチをレビューする（ドラゴンズ・デン スタイル）。ピッチの後、産業プロジェクト審査委員会からの質疑に回答を行う。

④Assesment
- 提案書と産業プロジェクト審査委員会からのフィードバックを MoD 評価者から評価を受けるプロセス。MoD の評価者は、提案が MoD の永続的能力課題に合致しているかについて評価を行う

⑤Grant
- 提案書が採択されるプロセス。プロジェクトが資金提供に推薦された場合、Innovate UK のイノベーション・ファンディング・サービスを通じてフォームに記入するよう求められる。Innovate UK は、信用調査に合格することを条件に助成金を交付する。その後、上位のサプライヤー及びその他のコンソーシアムパートナーとともにプロジェクトを開始することができる

3）プロジェクトの評価・管理方法

公募・採択プロセスで提案を支援した DASA のビジネス・リレーションシップ・マネージャーは、プロジェクトの実施中も採択された研究実施主体の支援を行う。

また、Innovate UK は、プロジェクト全体を通してプロジェクトの進捗を監視するモニタリング・オフィサーをアサインする。モニタリング・オフィサーは、プロジェクトのリスク、実績、資金がプロジェクトチームによって効果的に管理されていることを Innovate UK に保証する役割を果たす。定期的に面談（キックオフミーティング、四半期ごとのミーティング、最終的なクロージング）を行い、プロジェクトで問題が発生した場合の最初の窓口となるとともに、プロジェクトに関連する問題を観察、指導し、必要に応じてエスカレーション

を行う。なお、モニタリング・オフィサーはあくまでプロジェクトの資金管理をその役割とし、プロジェクトチームの代わりにプロジェクトや管理業務を引き受けることはできず、また、専門家としてアドバイザーを務めることもできない。他方、イノベーションのアイデアを進展させ、機会を活用するために役立つ可能性のある他の情報源を紹介することで、組織に貴重なサポートを提供することはできる[654]

4）知的財産権の扱い

DTEP では上位のサプライヤーと下位のサプライヤー間で連携が必須であるため、下位のサプライヤーが活用する、または開発する知的財産権については、標準的なビジネス慣行プロセスに従って、適切に保護を行う必要がある。下位のサプライヤーはプロジェクトの開発の過程および概略段階と完全な提案の両方において、登録済みと未登録の両方の適切な知的財産保護メカニズムと、強力な知的財産保護ポートフォリオの形成について、ビジネス・リレーションシップ・マネージャーによりサポート・指導される。

本プロジェクトで関連する知的財産に対して MoD は権利を主張せず、プロジェクト成果の実用化を積極的に推進している。実用化の視点はプロジェクトの採択基準にも反映されており、プロジェクトの明確な防衛利用・事業化計画が産業プロジェクト審査委員会及び MoD 評価者によって評価される。

（事業化計画に含めるべき内容）

- **最終製品の想定ユーザと、コンソーシアムが過去にそのユーザと関与したことがあるかどうか**
- **既存のエンドユーザ調達プログラムに対する認識と整合性**
- **提案するソリューションが防衛サプライチェーンにもたらすと予想される利益（コスト、時間、能力向上など）**
- **独立した製品になるか、他の技術やプラットフォームと統合されるか**
- **運用配備可能な商用製品を開発するために、プロジェクト（補助金）終了後に必要と予想される追加作業（製造のための「スケールアップ」、サイバーセキュリティ、既存技術との統合、環境動作条件など）**

また、DTEP の一環として開発された技術および製品の将来の輸出の可能性に関して、輸出管理およびライセンスに関する内閣府や MoD の輸出管理のガイダンスに留意する必要がある。なお、該当する場合は、ビジネス・リレーションシップ・マネージャーから助言を貰うことができる。

5）海外企業の参画に係る制約

国家保護保安局（NPSA）の Trusted Research ガイドラインの考慮及び NSI 法の要件に準拠する必要が言及されている。

654 https://youtu.be/v5liAn39XBw?si=NzYIdgp_u9tLsIY9

6）他のプログラム・機関との差別化要素

2022 年 7 月以降、現在まで DTEP では 5 つのプロジェクトが資金提供を受けている。

図 4.2-8　DTEP の採択事業者

他の助成プログラムとの差別化要素としては、ビジネス・リレーション・マネージャーにより、産業界からのアドバイスも受けられる点が挙げられている。ビジネス・リレーション・マネージャーは中小企業が協力関係を築く際のガイドラインとして、例えば ISO 44003 のようなツールに基づく指示を応募者に行うことができる。

また、DTEP の実現に当たっては上位サプライヤーと下位サプライヤーのマッチングを含めた、下位サプライヤーの適切なフォローアップと考えられるが、DASA は DTEP の仕組みの中で下位サプライヤーをサポート可能な多様な後援者を配置している

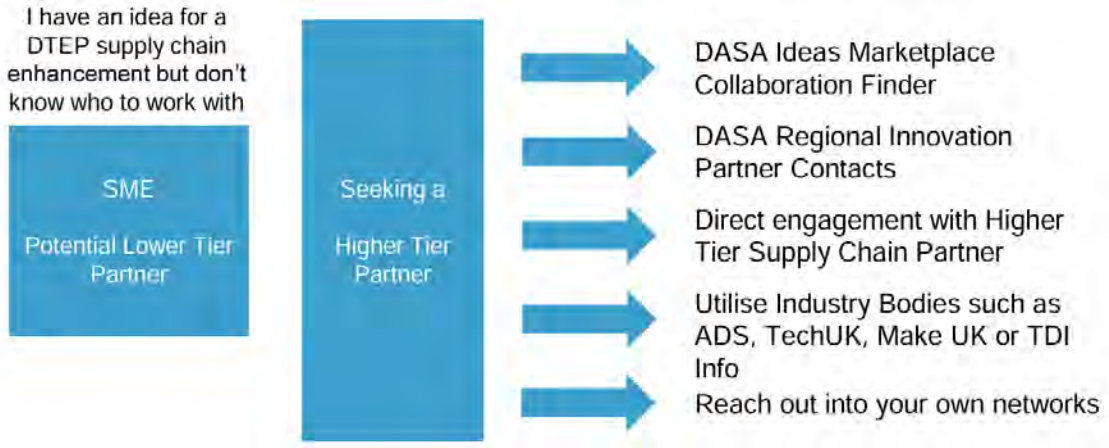


図 4.2-9　上位サプライヤーの探索する上で利用可能なサポート

（5）民軍技術協力事業

非軍事部門と軍の技術協力の強化・研究開発の推進等を目的として制定された、民・軍技術協力事業促進法を根拠とする政府の研究開発プログラムであり、同法やその周辺規則を根拠として民・軍技術開発事業、民・軍技術移転事業など、広義・狭義のデュアルユース研究開発にあたる事業が進められている。

1）研究テーマの選定プロセス

民軍技術協力事業においては、関係行政機関が産・学・軍に対する技術需要調査や妥当性評価などのプロセスを経て研究テーマを導出している。

まず関係行政機関は、輸出、市場規模の拡大、経済性、波及効果が期待され、民と軍の両部門に共通活用できる技術及び先端武器体系開発のための先端技術について、産・学・軍からの調査書の提出を受け付ける（基本計画の重点分野を対象）。

次いで提案された技術需要調査書を基に、重複した研究が無いか、民間での活用性・軍での活用性などについて妥当性評価を行い、導出された技術を基に研究開発課題を設定する。

最終的に企画された研究課題を含めた施行計画が作成され、総括実務委員会、民軍技術協議会での協議を経て決定されることとなっている（図 4.2-10）。

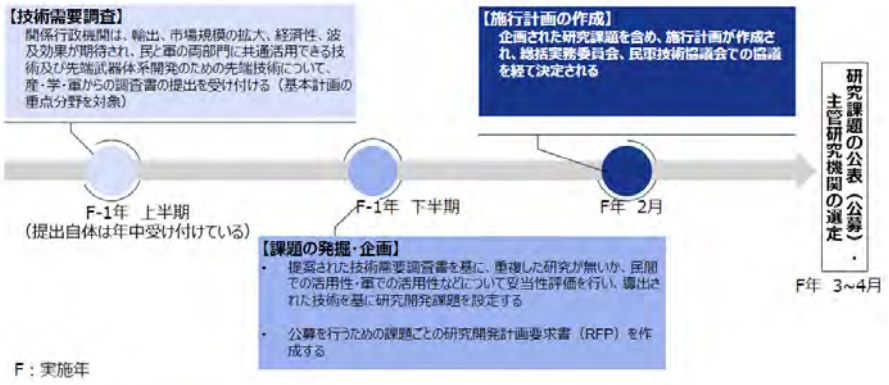


図 4.2-10　民軍技術協力事業における研究課題導出から公募までのプロセス

2）公募・採択プロセス

民軍技術協力事業の選定は、前記の技術需要調査や課題の発掘・企画のための審議を含めて、民軍協力振興院などの専門機関（関係中央行政機関の長から民・軍技術協力事業に対する予算及び事業管理を委託されて遂行する機関）の中に設置された技術別専門委員会によって実施されている。

専門委員会の委員は、民軍技術協力事業を遂行しない内部及び外部の専門家で構成する。この時、軍側専門家は各軍、国防部、放射庁及び国防研究開発専門機関（国防科学研究所、国防技術品質院など）に推薦を依頼して構成することができる。

研究開発実施主体の選定には、申請された提案に対して以下のような事項を重点的に評価される。

1. 研究開発計画書の RFP を満たすか
2. 開発要素技術の識別、要素技術の開発目標及び評価方法など研究方法の適切性
3. 研究責任者及び主管研究官の優秀性
4. 申請研究開発費及び研究開発期間の適切性
5. 委託研究課題及び／又は協同研究課題編成の適切性
6. 事業化・電力化計画の卓越性
7. 研究開発範囲の調整に関する意見
8. 研究開発費の規模と研究開発期間の調整に関する意見
9. 他の課題との冗長性など

3）プロジェクトの評価・管理方法

各プロジェクト（課題）の評価・管理については、民軍協力振興院などの専門機関の中に設置された技術別専門委員会によって実施されている。

各プロジェクトの研究開発段階は基礎・応用・試験開発の 3 段階に分かれており、また研究成果に対する評価（ステージゲート審査）が各研究段階の終了前にも行われることとなっている（表 4.2-4）。

表 4.2-4　民軍技術協力事業における研究開発段階・評価の区分

研究開発段階・評価の区分		概要
研究開発段階	基礎研究段階	特別な応用または事業を直接目標とせず、現象および観察可能な事実に関する新しい知識を得るために挑戦的・革新的に遂行する理論的または実験的研究段階
	応用研究段階	基礎研究段階で得られた知識を用いて主に実用的な目的で新しい科学的知識を得るために行う独創的な研究段階
	試験開発段階	一次開発された製品、工程またはソフトウェアに対して目標とする性能が出るように、試験、設計変更、製作または二次開発、再試験、試験評価を繰り返して推進される段階
研究開発結果の評価	進度評価	継続課題について毎年研究現場を確認し、課題の進捗状況を点検する。評価の等級は「継続」、「中断（誠実失敗、不誠実失敗）」、「補完」、「早期完了」（非常に優秀、優秀、普通）」で区分する
	段階評価	研究段階が終了する直前に研究現場確認と公開発表会などを通じて実績を点検する。評価の等級は「継続（非常に優秀、優秀、普通）」、「中断（誠実失敗、不誠実）」失敗）」、「補完」、「早期完了（非常に優秀、優秀、普通）」で区分する
	最終評価	全ての研究段階が終了する直前に性能・技術開発性と確認及び活用計画を点検する。評価等級は「成功（優秀、優秀、普通）」、「失敗（誠実失敗、不誠実失敗）」）」で区分する

4）知的財産権の扱い

民軍技術協力事業の進度・段階評価結果「早期完了」又は最終評価結果が「成功」と判定された課題の研究開発結果所有機関の長は、結果通知後 1 ヶ月以内にその成果の実施企業と技術料徴収を含む技術実施契約を締結して成果を活用しなければならないことが義務付けられている。

事業の遂行過程で得られる知的財産権、研究報告書の版権などの無形成果物は、主管研究機関の所有が原則とされているが、遂行機関の相互協約で定めるところに従うことができる。また、研究開発結果物を所有することになる機関が国外にある場合、事業を所管する中央行政機関の長は、当該機関と共に研究を遂行した国内所在の主管研究機関、協同研究機関または参加機関の所有とするか、またはこれらの機関が優先的に無償で実施権を獲得できるように努力しなければならないとして、国内の活用を図っている。

他方、事業を所管する中央行政機関は、以下のいずれかに該当する場合は研究成果を国の所有にすることができるとされている。

（民軍技術協力事業において成果を国の所有とできる場合）
1. 国家安全保障上必要な場合
2. 研究開発結果物を公共の利益を目的に活用するために必要な場合
3. 研究機関等が国外に所在する場合
4. 遂行機関のうち営利機関が直接実施しようとする研究開発結果物に対して正当な事由なくこれを実施しない場合
5. その他、研究機関等が所有するには不適当と認められる場合

5）海外企業の参画に係る制約

民軍技術協力事業の参加資格については、公募情報を確認すると以下の「民・軍技術協力事業促進法」第 7 条第 2 項及び同法施行令第 14 条第 2 項に定める機関及び団体と、「高等教育法」第 2 条各号に定める学校であるが、参加機関に求めるセキュリティ対策（国家研究開発革新法及び同法施行令、国家研究開発事業セキュリティ対策における情報取扱規程）の中で「研究者の管理（外国人含む）」とあることから、参加人員の制限を国籍などでは設けていないと考えられる。

また、「セキュリティ課題を外国政府・機関・団体等と共同研究を遂行しようとする場合や、これらに研究の一部を遂行させようとする場合、中央行政機関の長の事前承認を得なければならない」等の人的管理策を国家研究開発事業セキュリティ対策において規定していることから、外国機関の参加については行政機関の確認の下承認されていることが確認できる。

6）他のプログラム・機関との差別化要素

民軍協力振興院の発表では、民軍技術協力事業は 2012～2017 年の間、合計 4028.9 億ウォンの政府投資に対する 12.7 倍の経済効果の創出に成功し、2012～2016 年の間、開発された

技術の実用化率は約 71.4%とされている[655]。

高い実用化率の背景としては、民軍技術協力事業では各課題が成功裏に終了したならば、終了後 1 ヶ月以内にその成果の実施企業と技術料徴収を含む技術実施契約を締結して成果を活用しなければならないことを規定していることから、最終的な実用化を見通した研究開発の推進が図られていると考えられる。

[655] https://www.icmtc.re.kr/board?menuId=MENU00324&siteId=null

4.3 意見交換の開催

4.3.1 第 1 回意見交換会

■　　実施日時

令和 5 年 8 月 31 日　13:00～14:30

■　　実施方式

オンライン(WebEX)

■　　議題

第 1 回意見交換会の議題については、以下の通りである。

（第 1 回意見交換会の議題）

1. **全体の調査方針**
2. **調査進捗（多目的技術開発に係る日・英・米・韓の動向）**
3. **ヒアリング対象機関の候補、ヒアリング項目案**
4. **意見交換（ヒアリング対象機関・項目について）**
5. **意見交換結果の総括**
6. **今後の予定**

■　　コメント及び調査への反映方針

・　ヒアリング候補機関について

ヒアリング候補機関として、米国のジョンスホプキンス大学応用物理研究所、サンディア国立研究所、英国の DASA、韓国の民軍協力振興院に加えて、米国の RAND、MITRE や英国版 DARPA(ARIA)等の機関がヒアリング候補機関として挙げられるのではないかとのコメントがあったことからヒアリング候補機関として挙げられた機関が妥当であるかについての検討を行うために机上調査を実施することとした。

また、ヒアリング候補機関の対象として、宇宙、サイバー、量子、海洋等の分野について研究開発を実施している機関を選定するのが良いのではないかとのコメントがあったことから分野別の機関についても机上調査を実施することとした。

対象となる国については、多義的技術の研究開発が進んでいる米国、英国や日本の隣国で、技術的先進性や日本との環境の親和性等がある韓国に加えて、近年多義的技術に注力している国(ドイツ等)の機関についても挙げてはどうかとのコメントがあったことから、各国の多義的技術の研究開発状況についても机上調査を実施することとした。

・　ヒアリング項目について

ヒアリング項目として、挙げていた会議体の構成、成果の帰属、参加制限、情報の取り扱いに関する事項等に加えて、各国のファンディング候補機関の選定プロセスや観点、委託先に求める情報保全事項、研究機関の採用時における、米国の EAR や ITAR のナショナリティ規制等がヒアリング項目として挙げられたため、ヒアリングのスコープとして追加するとともに、選定プロセス・要件等について机上調査を実施することとした。

4.3.2 第 2 回意見交換会

■　実施日時

令和 5 年 10 月 27 日　15:00～16:15

■　実施方式

オンライン(WebEX)

■　議題

第 2 回意見交換会の議題については、以下の通りである。

（第 2 回意見交換会の議題）
1. 前回の意見交換会の振り返り、本意見交換会の趣旨
2. 前回の意見交換会でいただいたコメントに対する調査結果
   2.1 研究開発テーマの選定に関する考え方（日米韓）
   2.2 研究開発プログラム・プロジェクト、機関への参加制限（日米韓）
   2.3 要注目機関の個別調査（RAND、MITRE、ARIA）
3. 研究開発成果の段階的保全に関する調査結果
   3.1 調査アプローチ
   3.2 調査結果（日米英韓）
   3.3 総括
4. 現地ヒアリングの調整状況
   4.1 前回からの進捗
   4.2 今後の調整方針
   4.3 ヒアリング項目の詳細
5. 意見交換
   5.1 意見交換の論点
   5.2 意見交換結果の総括
6. 今後の予定

■　コメント及び調査への反映方針

・　段階的保全に関する調査結果を踏まえた、段階的情報保全実施の可否について

段階的保全制度の構造、運用の明確化を図るため、米国 DARPA のケース等を中心に研究段階区分に基づく身元調査、ファシリティ等の参加制限、日々の研究情報・研究ノート・データの管理に関するガイダンスの有無や技術流出に係る営業秘密管理の在り方、ガイダンスの有無、営業秘密管理と成果発表管理における組織内部の対応方法について、エンフォースメント面で契約上、制度上、刑事罰上の対応（CI 以外の CUI の扱いも含める）という観点から明らかにしてはどうかとのコメントがあったことからヒアリング項目として反映することとした。

・　リストアップした質問事項以外に聞いた方が良い内容について

リストアップした事項以外に質問事項に加えた方が良い事項として、機密解除された情報の照会、プロジェクト内容が当初の想定以上に安全保障等に関係するようになった場合の対応、プロジェクトの参加で共同研究者や提携先に求められる要件、情報保全措置に係る経費の支援制度や選定プロセスにかかる時間等が項目として挙げられたため、ヒアリン

グ項目に反映することとした。

4.3.3 第 3 回意見交換会

■　　日時

令和 5 年 12 月 26 日　11:00～12:00

■　　実施方式

オンライン(WebEX)

■　　議題

第 3 回意見交換会の議題については、以下の通りである。

（第 3 回意見交換会の議題）
1.　前回の意見交換会の振り返り
2.　本意見交換会の趣旨
3.　領域別研究開発における情報保全措置の調査結果
3.1　調査アプローチ
3.2　調査結果（日米英韓）
3.3　総括
4.　意見交換
4.1　意見交換の論点
4.2　意見交換結果の総括
5.　今後の予定

■　　コメント及び調査への反映方針

・　領域（宇宙・海洋）別に情報保全上留意が必要と思われる事項について

調査結果の中で情報保全上留意が必要な事項としてデューデリジェンス、研究インテグリティや研究セキュリティの観点のものについては、可能な限り強調するような表示にすることとのコメントがあったことから、報告書の中で反映をすることとした。

また、米国の宇宙領域で調査した NASA のプログラムにおける「中国または中国企業の参加制限」について、この規定は米側の中国に対する脅威認識が高さに由来するのか、NASA の他のプログラムでも同様の参加制限があるのか、また、宇宙以外の他の領域における、セキュリティ・クリアランスを要さないプログラムにおいても同趣旨の制限は設定されているのかについて確認してほしいとのコメントがあったことから、机上調査を実施することとした。

・　本調査事業で得られた調査結果の整理・分析の取り纏め方針について

整理内容について、組織内部のみならず、外部委託先に求める情報保全措置についても可能な限りピックアップして整理してほしいとのコメントがあったことから、報告書の整理に反映することとした。

また、法令等を取り纏める際、産業技術保護法等の経済安全保障との関わりがあると思われる法令等は、留意して整理してほしいとのコメントがあったことから、報告書の整理に反映することとした。

4.3.4 第 4 回意見交換会

■　日時

令和 6 年 3 月 1 日　15:00～16:00

■　実施方式

オンライン(WebEX)

■　主な議題

第 4 回意見交換会の議題については、以下の通りである。

（第 4 回意見交換会の議題）
1. 前回の意見交換会の振り返り
2. 本意見交換会の趣旨
3. ヒアリング結果・予定の共有
3.1 ヒアリング結果
3.2 今後のヒアリング予定機関
4. 研究開発プログラムにおける情報保全措置・運営要領に関する比較・整理及び総括
4.1 比較・整理
4.2 総括
5. 意見交換
5.1 意見交換の論点
5.2 意見交換結果の総括

■　コメント及び調査への反映方針

・　ヒアリング結果、及び今後ヒアリング予定の内容について

背景調査、デューデリジェンスの机上調査では不明であった調査項目及びそれら調査結果の確認要領（オープンソースまたは関係機関等との連携を想定）について、ヒアリングの場を通じての確認していただきたい旨コメントがあったことから、ヒアリング事項として追加で確認することとした。

また、米国シンクタンクでは採用時・採用後のジョブディスクリプションでセキュリティ・クリアランスを求められることがあると聞いている。ヒアリングを実施する上で参考としていただきたい旨コメントがあったことからヒアリング事項として追加で確認することとした。

・　調査結果の比較・整理、総括の観点について

引き続き調査結果の取り纏めにあたり、ファクトベースでの整理を実施いただきたい旨コメントがあったことから、継続して報告書取り纏めの際の留意事項とした。

CUI の扱い、デューデリジェンス・背景調査で確認する具体の項目や評価方法など CI 情報だけでなく CUI 情報の場合も上記の内容について意識してヒアリングを実施していただくとともに、結果を整理いただきたいとのコメントがあったことから、それらの結果等も踏まえて報告書に反映することとした。

また、シンクタンク的な機能に関する観点があるとありがたいとのコメント及び情報漏

洩があった場合の罰則、不正があった際の法的・内規的な制裁などの調査観点があるとありがたい旨コメントがあったことから、罰則、制裁等についてヒアリング等で確認するとともに、報告書に反映することとした。

・　比較・整理、総括結果について

表の「―」部分については、調査情報から確認できなかったものであることを明記するとよい旨コメントがあったことから、報告書に反映することとした。

4.4 比較・分析の対象とする調査結果

5 章、6 章において実施する研究開発における情報保全措置、運営要領、及び指定基金協議会の設置・運営に係る比較・分析は、4 章調査結果のうち、日米英韓で調査を行った法令・ガイドライン、資金配分機関の関係規則、研究開発プログラムの公募要領・契約約款、研究開発実施主体の関係規則から得られた情報をもって行う事とした（表 4.4-1）。

表 4.4-1　比較・分析に用いる情報

国	区分		参照した情報
日本	法令		特定秘密保護法
			外為法
	ガイドライン		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）　第四版
			研究データリポジトリ整備・運用ガイドライン
			大学における秘密情報の保護ハンドブック
	資金配分機関の関係規則等	JAXA	法人文書管理規程
		JAMSTEC	JAMSTEC データ・サンプル関連諸規程
			研究成果物等取扱規程
			サンプル取扱規則
			データ取扱規則
			法人文書管理規則
		AMED	AMED における研究開発データの取扱いに関する基本方針
			AMED 研究データ利活用に係るガイドライン
			データマネジメントプラン記載要領
		総務省	政府機関等のサイバーセキュリティ対策のための統一基準
		防衛装備庁	防衛産業保全マニュアル
	プログラム公募要領・契約約款等	革新的衛星技術実証プログラム（JAXA）	公募要領、契約書雛形
		SIP 第 3 期　課題「海洋安全保障プラットフォームの構築」（JAMSTEC）	契約書雛形
		新興・再興感染症に対する革新的医薬品等開発推進研究事業（AMED）	公募要領
		令和 3 年度　情報通信技術の研究開発に係る提案の公募：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発（総務省）	公募要領
		安全保障技術研究推進制度（防衛装備庁）	公募要領
	研究開発実施主体の関係規則等	川崎重工業	公式 HP、情報セキュリティ方針、ヒアリング
		日立製作所	公式 HP、日立サステナビリティレポート、ヒアリング

国	区分		参照した情報
		日本電気	公式 HP、情報セキュリティ報告書 2023、ヒアリング
		QPS 研究所	公式 HP、情報セキュリティ基本方針、ヒアリング
米国	法令		E.O.13526、32CFR part117(NISPOM)
			E.O.13556、32CFR part2002
			ECRA、EAR、ITAR（輸出管理改革法、輸出管理規則、武器取引国際規制）
			FIRRMA（外国投資リスク調査現代化法）
			DFARS 252.204-7000（情報の開示）
			DFARS 252.204-7008（対象となる防衛情報の保護管理の遵守）
			DFARS 252.204-7012（対象となる防衛情報の保護およびサイバーインシデントの報告）
	ガイドライン		NIST SP800-171
	資金配分機関の関係規則等	DARPA	DoDM 5200.01（DoD 情報セキュリティプログラム）(1 巻-4 巻)
			DoDI 5220.31（国家産業安全保障プログラム）
			DoDM 5220.32（国家産業安全保障プログラム）(1 巻-2 巻)
			DoD 5220.22-M(国家産業安全保障プログラム）
			DoD 5220.22-M Sup1（国家産業安全保障プログラム）
			DoDI 1035.01（テレワーク・リモートワーク）
		NASA	NPD 2810.1F（NASA 情報セキュリティポリシー）
			NPR 2810.1F（情報および情報システムのセキュリティ）
			NPR 2810.7（管理された未分類情報(CUI)）
			NPR8000.4C（エージェンシーのリスク管理手続き要件）
			NPR3600.2B(NASA テレワークプログラム）
	プログラム公募要領・契約約款等	Cyber-Hunting at Scale(CHASE)（DARPA）	公募要領
		SBIR プログラム（DARPA）	公募要領
		NextSTEP-2（NASA）	公募要領
	研究開発実施	BAE Systems Inc.	公式 HP

国	区分		参照した情報
	主体の関係規則等	ジョージア工科大学	公式 HP、ポリシーライブラリ
英国	法令		公務秘密法（Officials Secret Act 1911, 1920, 1939 and 1989）
			情報自由法（Freedom of Information Act 2000）
			セキュリティポリシーフレームワーク（Security policy framework）
			政府セキュリティ分類ポリシー（Government Security Classifications Policy：GSCP）
			政府ベースライン人員セキュリティ基準（Baseline Personnel Security Standard：BPSS）
			2018 年 NIS 規則
			2021 年国家安全保障・投資法（National Security and Investment（NS&I）Act 2021）
			2008 年輸出管理指令（Export Control Order 2008）
			2018 年制裁・資金洗浄防止法（Sanctions and Anti-Money Laundering Act 2018）
	ガイドライン		国家安全保障・投資法: 高等教育および研究集約型セクター向けのガイダンス（National Security and Investment Act: guidance for the higher education and research-intensive sectors）
	資金配分機関の関係規則等	UKRI（Innovate UK、MRC、EPSRC ほか）	UKRI 情報管理ポリシー
			UKRI 研究助成金利用規約
			Innovate UK プライバシー通知および情報管理ポリシー
			Innovate UK 助成金授与規則
			UKRI の Trusted Research の原則
			CPNI の Trusted Research に関するガイダンス
			研究不正利用のリスク管理に関する共同声明
		MoD（Dstl、DASA）	防衛情報、知識、デジタルおよびデータ政策への取り組み
			防衛ネットワークのガバナンス（JSP 604）
			DASA 標準利用規約

国	区分		参照した情報
			DEFCON 659（セキュリティ対策）
			DEFCON 531（情報開示）
			DEFCON 532（個人情報保護）
			DEFCON 632（第三者の知的財産-権利と制限）
			DEFCON 658（サイバー（フロー・ダウン））
			DEFCON 703（当局への知的財産権の帰属）
			DEFCON 705（知的財産権-研究および技術）
	プログラム公募要領・契約約款等	marine and maritime in the Great South West - R1 CR&D（UKRI）	公募要領、MRC の追加助成条件
		Space to Innovate Campaign - Bravo Drop（MoD）	公募要領
		Look Out! Maritime Early Warning Innovations（MoD）	公募要領
		防衛技術活用プログラム（DTEP）（MoD）	公募要領
	研究開発実施主体の関係規則等	D-Orbit UK Ltd	公式 HP
		エディンバラ大学	公式 HP、情報セキュリティフレームワーク
韓国	法令		保安業務規定
			軍事機密保護法
			対外貿易法（戦略物資輸出入告示）
			外国人投資促進法
			産業技術の流出防止および保護に関する法律
			国家先端戦略産業競争力強化および保護に関する特別措置法
			国家研究開発革新法、施行令
	資金配分機関の関係規則等	航空宇宙研究院（KARI）	公式 HP
		海洋水産科学技術振興院（KIMST）	海洋漁業研究開発事業セキュリティ管理指針
		韓国生命工学研究院（KRIBB）	公式 HP
		韓国知能情報社会振興院（NIA）	公式 HP
		民軍協力振興院（ICMTC）	公式 HP
	プログラム公募要領・契約約款等	多目的実用衛星 7A 号システム及び本体開発事業委託研究課題（KARI）	公募要領

国	区分		参照した情報
			国家研究開発事業セキュリティ対策
		2023 年度海洋無人システム実証試験・評価技術開発事業新規課題（KIMST）	公募要領
		2022 年度バイオ･医療技術開発事業（社会密着型感染病院泉技術開発） 1 次新規課題（KRIBB）	公募要領
		2022 年 量子暗号通信デモインフラ構築・運営公募（NIA）	公募要領
		2023 年着手民軍技術協力事業選定公募（ICMTC）	公募要領
			民・軍技術協力事業促進法、施行令、共同施行規定
			産業技術革新促進法、施行令
	研究開発実施主体の関係規則	LG ユープラス	公式 HP、サステナビリティ経営レポート
		SK ブロードバンド	公式 HP、投資家向けレポートレポート

5. 調査結果の比較整理・分析

5.1 研究開発の情報保全措置に関する比較・分析

日・米・英・韓の情報保全措置に関する比較・分析にあたっては、本事業で調査対象とした研究開発プログラムの一般的な構成を踏まえ、研究開発実施主体の公募・採択から研究開発の実施、成果の活用に至るまでの中で情報保全上留意すべき観点を設定して比較することとした（図 5.1-1）。なお、比較に際しては、各研究開発プログラムで取り扱われる情報の機微度に差異がある点に注意が必要である。

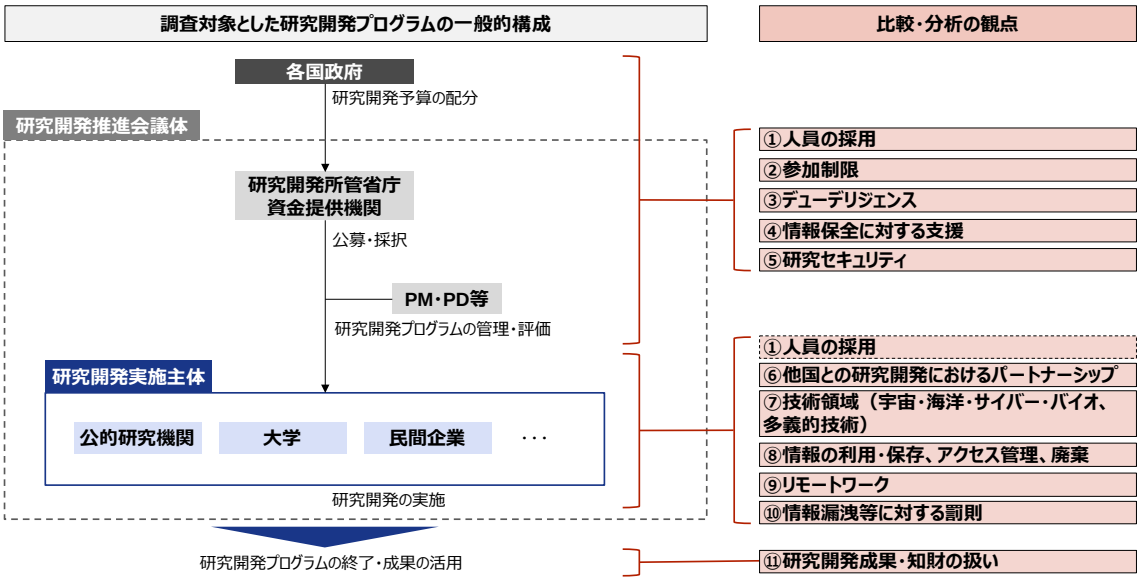


図 5.1-1　調査対象とした研究開発プログラムの構成を踏まえた比較・分析観点の設定

(1) 人員の採用

日本以外では、機密情報へのアクセス制限を意識した採用制限や身元調査（セキュリティ・クリアランス）が資金配分機関・研究開発実施主体において規定されていることが確認できた（表 5.1-1）。

表 5.1-1　人員の採用制限に関する比較

国	人員の採用制限	
	資金配分機関	研究開発実施主体
日本	・　国家公務員法、自衛隊法等の規定（禁固以上の刑に処されている者、懲戒免職から 2 年以上経過しない者	—[656]

656 表の「—」部分については、調査情報から確認できなかった

国	人員の採用制限	
	資金配分機関	研究開発実施主体
	等）によって制限が課されている者は採用されない（防衛装備庁、総務省等）	
米国	・ 一般的に米国市民もしくは合法的な永住権保持者でない限り、連邦政府機関に採用されない ・ 特定の連邦政府機関の職種には市民権・居住地及びセキュリティ・クリアランスの取得等に関する要件がある	・ 32CFR Part117 において政府と契約する請負業者は、非米国市民が機密情報へのアクセスを必要とする可能性のある職務に雇用されないよう、あらゆる努力を払わなければならないと規定している ・ UARC、FFRDC 等の採用ポジションによってはセキュリティ・クリアランスが必要となる
英国	・ 政府資産にアクセスできる個人を対象とした雇用前審査の位置づけで BPSS（ベースライン人員セキュリティ基準）が定められており、BPSS では、身元（氏名・生年月日・住所、学歴など）、国籍および入国ステータス、職歴、犯罪歴などが審査される。政府と契約する請負事業者についても対象となる ・ BPSS の他にも、特定の職務・作業に従事する人員を対象に、追加のセキュリティ・クリアランスとして SC（セキュリティチェック）、DV（Developed Vetting）、CTC（Counter-Terrorist Check）などが定められている	
韓国	・ 中央行政機関の公務員任用予定者のうち、国家安全保障に限られた国家機密を扱う職位に任用される予定の人員に関しては、国家情報院長に身元調査を要請しなければならないと保安業務規程で定められている ・ 身元調査の結果、国家安全保障に害を及ぼす情報があることが確認された者については、関係機関の長にその事実を通知され必要なセキュリティ対策が実施される	―

(2) 参加制限

プログラムの実施に必要な研究開発能力・体制、財務基盤を有している事や、研究インテグリティ、輸出規制等に関する法令の遵守等については共通して制限が見られた（表 5.1-2）。

表 5.1-2　各国に共通的な参加制限措置

国	規程内容
日本	・ 研究開発に必要な実績、組織、人員、経営基盤、資金管理能力を有する

国	規程内容
	ことが求められる（JAXA、総務省等） ・ 宇宙活動法に基づく人工衛星の管理に係る許可、衛星リモセン法に基づくリモートセンシング装置の使用に係る許可の取得が求められる（JAXA） ・ 外為法（安全保障貿易管理制度）の遵守が求められる（JAXA、総務省、AMED等） ・ 研究費の不正使用等又は研究活動における不正行為等により応募が制限されている者は参加できない（防衛装備庁）
米国	米国外の組織および／または個人は、その参加者が必要な秘密保持契約、セキュリティ規制、輸出管理法、および状況に応じて適用されるその他の管理法令を遵守する限りにおいて、参加することができる（DARPA）
英国	・ 研究開発に必要な物資等の原産国の輸出管理規制を遵守すること、提案に必要な輸出許可を取得できることが求められる（DASA） ・ 外国（英国外）の企業/団体と協力することは可能であるが、将来的な成果の活用ルートと輸出規制への影響（ITAR、EAR など）に考慮することが求められる（DASA）
韓国	過去に履行不良によって研究開発課題が中断された経験のある場合や、不正行為を行ったなど政府が施行する研究開発事業に参加制限を受けている機関及び研究責任者は対象外となる（KARI、KIMST 等）

日本との差異として、安全保障上の要件から外国機関・研究従事者の参加制限や、セキュリティ・クリアランスの取得を参加の要件とすることが挙げられる。

日本においても国内法に基づく法人格の保有や、研究開発実施場所を原則国内に制限する場合があるが、安全保障上の要件であるかについては確認できなかった。他方、米国 NASA の NextSTEP-2 における中国の参加制限は、安全保障に係る技術やデータが中国へ流出しないことを目的とした連結歳出法のウォルフ条項を根拠としていることから、安全保障上の要件であることが伺える（表 5.1-3）。

表 5.1-3　日本との差異のある規程

国	規程内容
米国	提案に際して中国または中国が所有する企業または団体との二国間参加、協力、または調整を含んではならない（NASA：NextSTEP-2） 最高機密（Top Secret）のクリアランスを有し機密情報（SCI）へのアクセス資格を有するチームメンバーを少なくとも 1 名擁していなければならない（DARPA：CHASE）
英国	プログラムで取り扱う情報の機密性レベルを「OFFICIAL」として規定（「OFFICIAL」レベルの英国資産へのアクセスには BPSS の取得が必要）（DASA）
韓国	セキュリティ課題については外国政府・機関・団体等と共同研究を遂行しようとする場合や、これらに研究の一部を遂行させようとする場合、中央行政機関の長の事前承認を得なければならない（KARI、KIMST 等）

(3) デューデリジェンス

デューデリジェンスとは一般的に資金提供先の財務健全性、履行能力（事業継続性）を確認するための審査を指すが、共通して当該研究開発プログラムを履行する為に必要な能力・体制を有しているか確認することを目的として、研究開発実施主体（組織）に対するデューデリジェンスが実施されていることが確認できた（表 5.1-4）。

表 5.1-4　一般的なデューデリジェンスの実施

国	規程内容
日本	提案審査時に、履行能力を確認するために代表研究機関及び分担研究機関の営む主な事業内容、資産及び負債等財務に関する資料の提出を求めることがある（AMED）
米国	提案者が募集の条件を満たしているかどうかを確認するために、NASA は提案者と情報交換(デューデリジェンス交換)を行う権利がある（NASA）
英国	NSI 法（国家安全保障投資法）で規定される 17 分野に該当する研究開発プログラムについてはデューデリジェンスプロセスの対象となり、UKRI から資金提供を受けている機関は同法を遵守した管理・対策を実施していることを証明できなければならない（UKRI）
韓国	調査情報からは確認できなかった

日本との差異としては、研究開発に従事する個人に対するデューデリジェンス（背景・身上調査）が実施されていることが挙げられる。英国 DASA では SC のクリアランスを取得していない従事者が FORM388 という人的詳細事項を記入する様式の提出を求められ、また韓国の国防科学研究所でも機密情報保護に係る保安業務規則を根拠とした身上調査が実施されることから、財務健全性、履行能力の確認とは別にセキュリティリスクの低減を目的とした「デューデリジェンス」が存在すると考えられる（表 5.1-5）。

表 5.1-5　セキュリティリスクの低減を目的としたデューデリジェンスの実施

国	規程内容
米国	・ DARPA 等の一部の研究開発プログラムの参加に求められるセキュリティ・クリアランスの取得にあたっては、身上・背景に関する申告・調査が実施される
英国	・ 提案が採択された場合研究従事者のデューデリエンス・チェックを DASA が実施する場合があり、特に英国籍以外の従事者に対しては最大 6 週間程度要する可能性がある（契約者が提案する研究従事者が全員、SC レベルのセキュリティ・クリアランスを保持している場合はこのプロセスは除外される）（DASA） ・ DASA のデューデリジェンス実施のため、研究に従事する者は FORM388（Researcher’s Personal Particulars form：研究者の人的詳細様式）という様式を記入し、提出する必要がある ・ FORM388 については、DASA の研究開発プログラムに関する説明会で寄せられた QA において「すべての DASA コンペティションは OFFICIAL

国	規程内容
	（OFFICALSENSITIVE ではない）クラスで実施されます。サプライヤーが SC クリアである必要はありません。もし入札者／落札者が SC クリアでない場合、FORM388 の記入が必要となります。FORM388 の記入自体が SC のクリアランスを付与するわけではありません。」と DASA から回答されているため、セキュリティリスクを低減するための考慮であることが伺える
韓国	・ 国防科学研究所の所管するプログラムにおいて、参加者は保安業務規則に基づく軍・警察による身上調査に同意しなければならないことが公募要領で規定されている（国防科学研究所）

(4) 情報保全に対する支援

共通して情報保全に関する教育について政府が研究開発実施主体へ支援を実施していることが確認できた。日本との差異として、米英韓では教育以外の面からも機密情報へのアクセス、環境の整備、金銭的な支援が実施されていることが挙げられる（表 5.1-6）。

表 5.1-6　人員の教育・支援の実施状況

国	教育に対する支援	教育以外の支援
日本	・ 防衛装備庁は秘密を取り扱う事業者に対して、カウンターインテリジェンスを含む教育資料の提供等により事業者による教育の支援を実施することが防衛産業保全マニュアルにおいて示されている ・ 川崎重工、日立、NEC 等の研究開発実施主体が情報セキュリティ教育を自組織の職員に対して実施している	・ 調査情報からは確認できなかった
米国	・ DARPA、NASA では DoDM 5200.01 や NPR 2810.1F に基づき職員に対してセキュリティ教育・訓練を実施している	・ DARPA はこれまで DoD と機密扱いの研究開発を実施してこなかった企業等からも革新的なアイデアを募集するために、セキュリティ・クリアランスの取得支援や機密作業区域とネットワークへのアクセスを支援する BRIDGES プログラムを実施している
英国	・ エディンバラ大学等の研究開発実施主体が情報セキュリティ教育を自組織の職員に対して実施している	・ 調査情報からは確認できなかった
韓国	・ 調査情報からは確認できなかった	・ KARI 等の研究開発プログラムに適用される国家研究開発事業セキュリティ対策において、「研究開発機関の長は、セキュリティ課題を遂行する研究者に対してセキュリティ手当支給など優遇措置を行うことができる。」

国	教育に対する支援	教育以外の支援
		と定めており、より機密性の高い研究開発に取り組む研究者に対してインセンティブを設定できることを政府が定めている

(5) 研究セキュリティ

日本においては、研究開発プログラム実施にあたって情報保全に関するリスクアセスメントや、その結果に基づくプロジェクトの機密性レベルの設定、プロジェクトの進捗に応じた成果の段階的保全といった研究セキュリティ措置の実施は確認できなかった。

英国、韓国においては情報保全に関するリスクアセスメントの実施やプロジェクト及び取り扱う情報に対する機密性レベルの設定/再設定に関する規程が確認できた。

差異の生じた理由として、諸外国においては統一的なセキュリティ・クリアランス制度が確立されていることや、日本においては学術研究の自主性・自律性の担保といった観点から研究開発成果の公表・活用制限に対しては慎重な姿勢が求められてきたことが考えられる(表 5.1-7)。

表 5.1-7　研究セキュリティに関する規程内容

国	研究セキュリティに関する規程	
	リスクアセスメントの実施	プロジェクトに対する機密性レベルの設定
米国	・ NASA ではリスクマネジメントについて、NPR 8000.4C「エージェンシーのリスク管理手続き要件」とそれに基づいて「NASA リスク管理ハンドブック」が策定されている	・ DARPA のプロジェクトで扱う情報については大統領令 13526 号、13556 号に準拠して機密性レベル（TOP SECRET、SECRET、Confidential、Contrilled Unclassified Inoformation）が設定されている
英国	・ DASA の Space to Innovate Campaign – Bravo Drop の公募に参加するために研究開発実施主体はサプライヤー保証アンケート（SAQ）に回答する必要がある。SAQ によって DASA のサイバーリスク評価(CRA)に準拠していないと評価された場合、研究開発実施主体は契約締結前にサイバー実施計画(CIP)を作成し、サイバーレジリエンスを証明する必要がある ・ UKRI、Innovate UK では、国家安全保障投資法や機密保全上のリスクアセスメントの結果をもってプロ	・ DASA の公募で扱う情報についてはセキュリティ分類ポリシーに準拠して機密性レベル（OFFICIAL、SECRET、TOP SECRET）が設定されており、そのレベルに基づき契約条件が設定されている ・ プロジェクトで使用するデータセットやプロジェクト成果物が当初の設定レベルよりも上位にあることが判明した場合、DASA は契約条件をアップグレードすることがある

国	研究セキュリティに関する規程	
	リスクアセスメントの実施	プロジェクトに対する機密性レベルの設定
	グラムで取り扱う情報の機密性レベルを定めている	
韓国	・ 国家研究開発事業へ参加する研究開発実施主体は、応募するにあたって自らの提案がセキュリティ課題に該当するか否か、及びその理由についての報告を求められることがある	・ 国家研究開発事業では、実施される研究開発課題（プロジェクト）のセキュリティ等級を分類して、セキュリティ課題と一般課題に分けた管理が成されている ・ セキュリティ課題とは輸出規制に該当する技術や、産業技術保護法等で保護されている技術を含む研究開発プロジェクトであり、その他の課題（一般課題）よりも厳しいセキュリティ要件が研究開発実施主体に課されることとなる ・ 研究開発の結果によってセキュリティ課題の有無が変わることがある場合、当該課題の最終評価をする際に、結果を考慮したセキュリティ課題の解除・再分類ができることとなっている

(6) 他国との研究開発におけるパートナーシップ

共通して輸出規制や国際的な制裁措置といった規程が確認できた。輸出規制の面では外国機関とのパートナーシップや共同研究を実施するにあたり輸出規制関係法令（外為法、ITAR、EAR 等）の考慮を求められており、国際的な制裁措置の面では、北朝鮮、ロシア等の特定の国家主体に対する研究協力・資金提供の禁止が規定されている（表 5.1-8）。

表 5.1-8　共通したパートナーシップに対する制限

国	規程内容
日本	・ 国際的な人的交流や外国との共同研究等においては輸出者等遵守基準を守る必要があるため、「安全保障貿易に係る機微技術管理ガイドライン」が経済産業省によって策定されており、JAXA や AMED、総務省の所管する研究開発プログラムにおいて研究開発実施主体に参照を求めている ・ 国連安保理決議第 2321 号に基づき北朝鮮に後援される又は北朝鮮を代表する個人又は団体に関係する科学技術協力の停止を求めている（AMED）
米国	・ 米国外の組織および／または個人は、その参加者が必要な秘密保持契約、セキュリティ規制、輸出管理法、および状況に応じて適用されるその他の管理法令を遵守する限りにおいて参加することができる（DARPA）

国	規程内容
英国	・ 外国の企業/団体と協力することは可能であるが、将来的な成果の活用ルートや輸出規制への影響（ITAR、EAR など）に考慮することが研究開発実施主体に求められる（DASA） ・ 2022 年のウクライナ侵攻の影響により、現行の Innovate UK 助成金の資金制限ではロシア起源の商品またはサービスを含むロシアの事業体に資金提供は行わないとしている（Innovate UK）
韓国	・ セキュリティ課題（セキュリティ上の懸念がある国の研究開発課題）の要件には輸出規制や産業技術保護法等が関係するため、パートナーシップに当たって考慮を求められる可能性はあるが、公募要領等では明言されていない

日本との差異としては、セキュリティ上の要件から外国機関とのパートナーシップを禁止、もしくは事前確認を実施することや、パートナーシップの締結にあたり潜在的なリスクを認識するための資金配分機関によるガイダンスの提供などが見られた（表 5.1-9）。

表 5.1-9　日本と差異のあったパートナーシップに対する制限

国	規程内容
米国	・ NASA は 2012 年連結歳出法で追加されたウォルフ条項（中国の参加制限条項）を根拠に、一部の研究開発プログラムでは研究開発実施主体に対して中国とのパートナーシップの締結を禁止している
英国	・ UKRI では、英国と異なる価値観を持つ国々と関係のある組織や研究パートナーと協力するときに発生する可能性のあるリスクについての認識を高めるため、Trusted Research に関するガイダンス（パートナーの適正評価、情報セキュリティ管理対策の実施、共同研究契約の締結の必要性など）を定めている
韓国	・ 国家研究開発事業に関して、研究開発実施主体がセキュリティ課題を実施するにあたり外国政府・機関・団体等と共同研究を遂行しようとする場合や、これらに研究の一部を遂行させようとする場合、中央行政機関の長の事前承認を得なければならない

（7）技術領域（宇宙・海洋・サイバー・バイオ）

特定の技術領域に対して共通して領域固有・特徴的な情報保全措置を図っていることは確認できなかったが、国際条約に則った国内法の整備、デュアルユースのリスクを考慮した研究評価など領域ごとの状況が共通して確認できた

全体として、一部で産業規制等として研究開発プログラムに関係することはあるものの、情報保全については技術領域毎の特性は大きく影響せず、取り扱う情報の機密性・安全保障上の観点から保全措置が講じられているもの考えられる（表 5.1-10）。

表 5.1-10　技術領域毎の研究開発に関係する規程

技術領域	国	規程内容
宇宙	日本	・ 国際的な宇宙諸条約に則った、宇宙 2 法によるロケットの打ち上げ・リモートセンシング情報の取扱いに関する規程への準拠が求められている
	米国	・ U.S.Code Title 51 によって研究開発等の活動、商業利用、資金助成、リモートセンシングに係るライセンス規程等、米国が実施する宇宙領域の活動に関する規程が定められている
	韓国	・ 衛星情報セキュリティ管理規則によって、衛星情報の取扱いに際して規程への準拠が求められる
海洋	英国	・ 国際海洋法条約 (UNCLOS)に則ったガイドラインとして Marine Science Research (MSR) Guidance が公表されており、英国およびその王室属領／海外領土内で海洋科学調査（MSR）を希望する英国以外の船舶と、海外での調査を希望する英国船舶両方を対象として必要な手続きを定めている
バイオ・医療	米国	・ 米国国立科学アカデミーによって発行されたバイオテクノロジーと生物兵器の潜在的な脅威に関する報告書である Fink Report において、生物科学の進歩が生物兵器としての悪用の可能性を高める警告を実施しており、その多義的技術への利用について、研究の誤用・悪用を防止するための 7 つの禁止項目を提言している ・ 米国保健福祉省は鳥インフルエンザ研究課題に対するデュアルユースリスク審査基準を 2013 年に提案している
	英国	・ デュアルユース研究に基づくリスクの特定と評価に関するプロセスやデュアルユースリスクを引き起こす可能性のある研究分野としてバイオ・医療領域（ワクチン効果を無効にする方法の実証や治療上有用な抗生物質または抗ウイルス剤に対する耐性を与える実験など）を示している(MRC、BBSRC、ウェルカムトラストの共同声明より) ・ 上記の声明に基づき、助成金の申請者へ提案に関連する悪用リスクについて質問する、助成金の外部評価機関の検討すべき事項として不正使用のリスクを含める、悪用の懸念があるケースの評価プロセスの開発及びガイダンスの検討等を行っている

(8) 情報の利用・保存、アクセス管理、廃棄

主として情報の区分ごとに取扱要領が把握することを念頭に、機密情報・管理対象非機密上の取り扱いに関する規程の比較を行った。共通して以下のような規程が確認できた。

- 情報の利用・保存：国の指定する機密情報や管理対象非機密情報について物理的・電子的な手段で保存・利用するにあたっての具体的な保管要領が法令・ガイドライン等によって規定されている
- 情報のアクセス管理：機密性レベルに応じたクリアランスを保持する者以外に対して当該機密情報を扱わせることの無いよう、物理的な施設への入退室管理や、電子的システムにおけるユーザー認証等によって制限を図っている

- 情報の廃棄：国の指定する機密情報や管理対象非機密情報については当該情報を廃棄する場合の要領として、使用する機材、手段、人員の立ち合いといった事項が法令・ガイドライン等に規定されている

日本との差異としては、米英において情報の保管や廃棄に用いる具体的な手段・要領について標準規格や具体的製品を参照していること、特に英国では情報について口頭、ハードコピー、電子といった形態に分けた取扱要領を定めていることが確認できた(表 5.1-11)。

表 5.1-11　情報の利用・保存、アクセス管理、廃棄に係る規程の比較

国	対象	機密区分	参照規則	利用・保存	アクセス管理	廃棄
日本	防衛省における秘密情報	秘密情報（特定秘密、特別防衛秘密、省秘） 保護すべき情報	防衛産業保全マニュアル	・ 秘密情報を取り扱う際には、秘密保全施設で取り扱わなければならない ・ 秘密情報を電子情報として取り扱う場合、原則として可搬記憶媒体へ保存 ・ 可搬記憶媒体への情報の保存には電子政府推奨暗号等を使用して秘匿し、その暗号鍵は厳格に管理	・ 秘密保全施設の構造基準として、天井、壁、床、間仕切り、出入口、扉及び錠、窓、開口部、警報装置、外柵、保管容器「保全外部区域」の設置といった具体的な備えるべき構造の要件を規定 ・ 情報システムのアカウント管理者を指定し、情報システムの利用者ごとに業務遂行上必要最小限度の機能及び権限となるようアカウントを管理	・ 秘密文書等を廃棄する際は、防衛装備庁の指示に従い関係社員を最低１名以上立会させ、焼却、粉砕、細断、溶解、破壊等の方法により廃棄、記録して防衛装備庁に報告
米国	機密情報	TOP SECRET SECRET Confidential	大統領令 13526 号 /32CFR part117(NISPOM)	・ GSA 認可のセキュリティ・コンテナ、連邦規格（FED STD）832 に従って構築された保管庫、または§2001.53 に従って構築された開放保管場所に保管	・ 機密情報にアクセスできる人員は、DoDM 5200.02、ICD 704、E.O. 13467、E.O. 12968、E.O. 13764 に従った継続的評価の対象	・ 32 CFR 2001.47 に従った機密文書破棄のガイダンスおよび 32 CFR 2001.42(b) に従った破棄設備基準に従う
	管理対象非機密情報	CUI Basic CUI Specified	大統領令第 13556 号 /32CFR part2002/NIST SP800-171	【電子】 ・ CUI へのアクセスを、認可されたユーザに限定 ・ FIPS PUB 200 および NIST SP 800-53 の適切なセキュリティ要件および管理を、リスク・ベースの調整決定に従い、CUI に適用 【物理】	【電子】 ・ CUI へのアクセスを、認可されたユーザに限定 ・ システムへのアクセスは、認可されたユーザ、認可されたユーザに代わって動作するプロセスおよび（その他のシステムを含む）デバイスに限定	・ CUI を含むシステムの媒体を廃棄または再利用する前に、サニタイズまたは破壊する ・ 32 CFR Part 2002「CUI」に基づき、読み取り、判読、復元不可能な方法で廃棄 ・ 当該機関で廃棄方法が

国	対象	機密区分	参照規則	利用・保存	アクセス管理	廃棄
				・ CUI を権限保持者の直接管理下に置くか、少なくとも 1 つの物理的バリアで保護し、管理された環境の外では、権限保持者または物理的バリアが不正アクセスまたは観察から CUI を保護することを合理的に確保 ・ CUI 用のカバーシートを使用することができる。カバーシートの使用を選択した場合、CUI EA が承認したカバーシートを使用		定められていない場合、NIST SP800-88「メディア・サニタイゼーションのガイドライン」における破棄のガイダンスや、32 CFR 2001.47「破棄」等に従った廃棄を実施
英国	英国政府資産	TOP SECRET	GSPC BPSS	【ハードコピー】 ・ TOP SECRET として承認された NPSA 認定の物理セキュリティ機器に保管 ・ セキュリティ機器カタログ（CSE）で NPSA によって承認された不正開封防止パッケージのみを使用 【電子】 ・ 組織によって承認された IT システム上でのみ、電子情報の作成、保存、または共有を行う	【口頭】 ・ 会話が盗聴されないように、TOP SECRET 認定の会議室を使用	【電子】 ・ 情報を破壊する際は CSE（Catalog of Security Equipment）の製品を使用
		SECRET		【ハードコピー】 ・ NPSA が承認した物理セキュリティ機器に保管	【電子】 ・ 組織が許可されたエリアでの	【ハードコピー】 ・ CSE の製品を使用して破棄

国	対象	機密区分	参照規則	利用・保存	アクセス管理	廃棄
				【電子】 ・ TOPSECRET に同じ	み処理作業を行うこと	・ 情報作成者からの書面による承認なしに資産を破壊しない ・ DV のセキュリティ・クリアランスを有する証人の立会いのもと破壊
		Official(-Sensitive)		【ハードコピー】 ・ 不透明なフォルダーまたは容器に保管 【電子情報】 ・ フォルダーにアクセスできるすべての人がその情報を知る必要があると確信できる場合にのみ、そのフォルダーに保存	【ハードコピー】 ・ オフィスで使用していないときは、不透明なフォルダーまたは容器に保管し、無人のときは施錠して鍵をかけて保管	【ハードコピー】 ・ 組織によって義務付けられた正しい廃棄方法を使用
韓国	秘密	Ⅰ級秘密 Ⅱ級秘密 Ⅲ級秘密	保安業務規程	・ 電子的方法を用いて秘密を管理する場合、国家情報院長が安全性を確認した暗号資材を使用 ・ 盗難・流出・火災又は破壊から保護し、秘密取扱認可を受けない人の接近を防止できる適切な施設に保管 ・ 一定の範囲の保護地域を設定	・ 秘密は、当該等級の秘密取扱認可を受けた者のうち、その秘密と業務上直接関係のある者のみ閲覧することができる ・ 秘密取扱認可を受けていない者の接近を防止するために分類（再分類を含む）と同時に等級によって区分された表示 ・ 保護地域に接近し又は出入しようとする者は、各級機関の長又は管理機関等の長の承認を受けなければならない	・ 緊急時に備えて秘密を安全に搬出又は破棄できる計画を樹立
	軍事機密	軍事Ⅰ級秘密 軍事Ⅱ級秘密	軍事機密保護法	・ 軍事保護区域には入退室の制御、保管容器または保管施設の	・ 軍事機密の表示又は告知が不可能又は不適切な軍事機密に	・ ―（法で定めない事項は保安業務規程に準拠）

国	対象	機密区分	参照規則	利用・保存	アクセス管理	廃棄
		軍事Ⅲ級秘密		ロック装置の設置	対して接近を防止し、又は機密のある所を隠蔽するために軍事保護区域を設定	

(9) リモートワーク

共通してリモートワークについてはアクセスポイントの制限や多要素認証の導入、使用するデバイスの指定といった規程を定めていることが確認できた（表 5.1-12)。

表 5.1-12　共通したリモートワークに関する規程内容

国	規程内容
日本	・　サイバーセキュリティ統一基準において、政府機関職員の行うリモートワークについて、リモートアクセスに多要素認証を求めることや、許可された端末に限定すること等の規程整備、実施環境の対策、実施時の対策が規程されている
米国	・　NASA では NPR 2810.1F リモートアクセスにおいて、承認されたデバイスのみで組織に合致した方法でリモートアクセスを許可すること、CIO により承認されたリモートアクセスポイントを経由すること等が定められている
英国	・　セキュリティ分類ポリシーにおけるベースライン動作の中にリモート作業時の留意事項が含まれる
韓国	・　調査情報からは確認できなかった

日本との差異としては、米英においてリモートワークを実施することのできる人員に対して背景・身上に係る制限を加えている事や、機密情報を扱うためのリモートワークに関する規程が確認できた（表 5.1-13)

表 5.1-13　日本と差異のあるリモートワークに関する規程内容

国	規程内容
米国	・　5 USC chapter65「テレワーク」において、行政機関職員は「5 日を超える無断欠勤により公式に懲戒処分を受けた場合」や「連邦政府のコンピュータ上で、または連邦政府の公務遂行中に、児童ポルノを含むポルノグラフィを閲覧、ダウンロード、または交換したことで懲戒処分を受けたことがある場合」にリモートワークを行うことができないとしており、それに従い、NASA、DoD、DoE 等が各省・機関の規則を定めている ・　NASA では機密扱いの資料を定期的に取り扱う職務はリモートワークへの参加資格がないとされているが、DoDI 1035.01 ではリモートワークで機密情報が扱われる場合、「DoD CIO および USD(I&S)が定めた手続きに従い、極秘テレワーク機器が GFE （政府支給機器）として提供されるか、または職責の遂行に必要な機密情報の取り扱い、協議、処理について認定を受けた施設に適時に出頭する必要がある。」としている
英国	・　SECRET の電子情報を扱うベースライン動作として、「同居者、訪問者、通行人等が見る可能性がある場所ではリモート作業しないこと」が規程されている
韓国	・　調査情報からは確認できなかった

（10）情報漏洩等に対する罰則

共通して、国家安全保障上の機密の漏洩、輸出規制に抵触する貨物・技術情報の提供や、特定の産業分野に対する外国投資に事前申告を怠った場合等に法令による罰則が規定されている他、機関の内部職員による情報漏洩に対する罰則、研究開発プログラムにおける情報漏洩では研究開発実施主体に対する金銭面・参加制限等の罰則等が規定されていることが確認できた。

前述のとおり各国の研究開発プログラムでは機密情報の取り扱いや輸出管理に関係する法令の参照を行っていることから研究開発実施主体がそれらの法令に違反した場合法令を根拠とした罰則が適用される他、予算の返還や資金配分機関による今後の研究開発への参加制限が実施されるものと考えられる。

日本以外では、米国・韓国において国家安全保障上の機密漏洩に対しては死刑・終身刑等の厳罰を規定していることが差異として挙げられる（表 5.1-14）。

表 5.1-14　各国の機密情報、産業技術保護、輸出規制、研究開発等に係る情報漏洩に対する罰則

国	区分	法令等	罰則の内容
日本	法令	特定秘密保護法	特定秘密を取り扱うことを業務とする者、公益上の必要により行政機関から特定秘密の提供を受け、これを知得した者の故意又は過失による漏えいの処罰（最大 10 年以下の懲役）を規定しているほか、外国の利益等を図る目的で行われる特定秘密の取得行為（未遂、共謀、教唆又は煽動を含む）の処罰を規定している
		外為法	必要な許可を取得しないで規制対象である貨物の輸出や技術の提供を行った場合など、法令の規定に違反した場合に、刑事罰（最大 10 年以下の懲役）、行政制裁（3 年以内の輸出・技術提供の禁止等）や行政指導として警告がなされる他、経緯書・報告書を提出する必要がある。
	機関内規	国立研究開発法人宇宙航空研究開発機構法	第 16 条において機構の役員及び職が職務上知ることのできた秘密について、秘密保持義務が規定されており、違反した場合一年以下の懲役又は五十万円以下の罰金が科される
		国立研究開発法人海洋研究開発機構法	第 15 条において機構の役員及び職が職務上知ることのできた秘密について、秘密保持義務が規定されており、違反した場合一年以下の懲役又は五十万円以下の罰金が科される
	公募要領・契約	令和 3 年度　情報通信技術の研究開発に係る提案の公募要領	委託研究を通じて取得した技術等について外為法に係る規制違反が判明した場合には、契約の全部又は一部を解除する場合がある
		安全保障技術研究推進制度　公募要領	研究費の不正な使用及び不正な受給並びに研究活動における不正行為や関連法令・指針への違反に対し、防衛装備庁では委託契約の解除・変更、研究費の全部又は一部の返還、本制度への応募又は参加の制限、厳重注意、他府省を含む他の競争的資金制度への応募又は参加の制限、当該不正事案等の概要の原則公表といった措置をとるとしている
米国	法令	U.S. Code: Title18(U.S.C18) §793、794、798	国防に関連する場所、情報、資料等の不正なアクセス、取得、複製等の行為、それらの情報の伝達及び情報の不正な持ち出し、紛失、盗難等を報告しない行為等について罰則として、罰金、10 年以下の懲役、またはその両方が科される（§793） 戦時中という状況下において、外国政府等に国防に関連する情報を伝達しようとする行為及び戦時における敵への情報提供を意図した行為について、罰則として、死刑もしくは終身刑に処せられる（§794） 米国の安全または利益に対する損害、または外国の利益のために機密情報を不正に伝達、公開、利用する行為及び米国または外国政府の暗号、通信諜報に関連する情報の不正な取り扱い行為について、罰則として、罰金、10 年以下の懲役、またはその両方が科される（§798）

国	区分	法令等	罰則の内容
		ECRA (Export Control Reform Act：輸出管理改革法)	EARA やそれを元に発行された規則、命令、輸出許可、もしくはその他の認可に違反する行為、それらの違反を教唆、共謀する行為、規則への違反が発生もしくは発生しようとしていることを隠匿等の行為、商務省等の担当官に虚偽の報告、説明をする行為、許可省、命令等を偽造・変造する行為等について罰則として、100 万ドル以下の罰金及び 20 年以下の懲役、またはその両方が科される また民事的には本法令に違反をした場合、商務長官は、ECRA または ECRA のもとに発行された規則、命令若しくは輸出許可の当該者による各違反者については、当該者に対して 30 万ドル以下または罰則が課せられる違反の根拠となっている取引額の 2 倍以下のいずれか高額の罰金、本パートに基づいて当該者に発行される輸出許可の取り消し、当該者が本パートで規制される品目を輸出、再輸出、または国内において移転できることを禁じることができる
		ITAR (International Traffic in Arms Regulations：国際武器取引規則)	輸出許可等が必要な防衛物品もしくは技術資料を輸出する行為、米国から輸出された防衛物品、技術資料等を許可なしに再輸出、再移転する行為、それらの行為を教唆、共謀する行為、許可が必要な防衛物品、技術資料等を不正に輸出、移転する目的で所有する、もしくは所有することを企てる行為等について、罰則として、100 万ドル以下の罰金及び 20 年以下の懲役、またはその両方が規定されている。
		FIRRMA (Foreign Investment Risk Review Modernization Act:外国投資リスク審査近代化法)	虚偽申告を行った者に対して、25 万ドル以下の罰金が科され、事前申告が必要なものに関して、その義務を怠った者は 25 万ドルまたは、取引額のいずれか大きい額の罰金が科される。 ※事前申告が必要なもの：単一の外国（例外外国を除く）の国または準国家政府が実質的な利害を有する外国人による米国事業の技術、インフラ、データの実質的な利害の取得をもたらす対象取引及び 1 つ以上の重要な技術の輸出、再輸出、移転(国内)又は再譲渡のために米国の規制当局の許可が必要とされる、当該重要な技術を生産、設計、試験、製造、加工又は開発する技術、インフラ、データの米国事業が関係する対象取引
	機関内規	DoDM 5200.01 （ DoD Information Security Program:DoD 情報セキュリティプログラム）	国防総省の機密情報、CUI を権限のないものへ開示する行為等について罰則として、警告、停職、給与の没収、解任、懲戒免職、機密情報および/または CUI へのアクセス権の喪失または拒否、および分類権限の剥奪が含まれる。また刑事上の制裁が行われる場合もある。
		NPD 1600.1 （NASA Security Program Procedural Requirements:NASA セキュリティプロ	NASA のセキュリティ要件に関連する規制または命令に故意に違反した、違反を試みた、または違反を共謀した者は、18 U.S.C. § 799 に基づく解雇および/または起訴の可能性を含む懲戒処分の対象となる。

国	区分	法令等	罰則の内容
		グラム手続き要件）	
	公募要領・契約	NextSTEP-2 （Next Space Technologies for Exploration Partnerships-2）	ECRA、EAR、ITAR 等の規制に違反した場合、刑事罰または民事罰が科される可能性がある。
英国	法令	National Security Act 2023 （2023 年国家安全保障法）	スパイ行為として、保護された情報を取得または開示する犯罪に関する最高刑は終身刑、また、営業秘密の取得または開示に関する新たな犯罪は、と規定されている最高刑は 14 年以下の懲役および/または罰金
		Official Secret Act 1989 （1989 年公務秘密法）	①傍聴とインテリジェンスについての情報、②防衛情報、③国際関係、外国や国際機関から入手した情報、④犯罪についての情報、⑤通信傍受に関する情報、⑥上記についての情報で、他国に内密に伝達されたもの、を保全対象情報として規定されており、公務員が①から⑥のいずれかに該当する情報を流した場合、最長で２年の禁固刑及び（あるいは）無期限の罰金の可能性」と規定されている ※スパイ行為については National Security Act 2023 にて規程
		National Security and Investment Act 2021 （2021 年国家安全保障・投資法）	株式・議決権や資産（※アイデア、情報又は技術という無形資産を含む）の取引に関して、国家安全保障上の懸念が生じやすい 17 分野に該当し、その資産が、①英国における事業活動に関して使用される場合、若しくは②英国に対して供給する商品・役務に関して使用する場合には、当局の審査権限の対象となる 上記に基づき、取引を実行する前に、当局に届出を行い、クリアランスを取得することが必要となるが、クリアランスを得ずに実行された取引は無効となり、また、届出義務に違反した場合、ペナルティとして、全世界売上高の 5%又は 1,000 万ポンドのいずれか高い金額を上限とする罰金を課される可能性がある
	機関内規	UKRI （Managing Performance and Conduct Policy ）	UKRI の従業員に対して、規律違反が発生し、そのインシデントの重大性に応じて口頭警告、書面による警告、最終警告、通知による解雇、略式解雇（予告なし解雇）などの段階的な処分手続きが示されている また、警告文書の中には給与支給の保留などの罰則が示されているとされる 重大な不正行為の中には、守秘義務違反や UKRI の信用を失墜させる行為、などが例示されている
	公募要領・契約	DASA Open Call Terms and Conditions	請負業者の債務不履行によって生じた損失に関する請負業者の責任総額は 500 万ポンドが上限と示されている

国	区分	法令等	罰則の内容
韓国	法令	保安業務規程	本規程自体には罰則は規定されていないが、国家機密の漏洩には刑法 98 条で罰則が規定されている。 刑法 98 条： 敵国のためにスパイをするもしくは敵国のスパイを幇助した者は、死刑、無期又は 7 年以上の懲役に処する。 軍事上の機密を敵国に漏らした者も前項の刑と同じとする。
		軍事機密保護法	主に軍事機密の保護措置の不履行、損壊・隠蔽、検知・収集、漏洩、届出・提出の不履行、軍事保護区域に侵入することに罰則（最高で 7 年以下の懲役）が規定されている。また、本法とは別に刑法 98 条で軍事上の機密を敵国に漏洩した者には、死刑、無期又は 7 年以上の懲役に処すると定められている。
		対外貿易法	戦略物資等の拡散を図る目的で、輸出許可を受けず戦略物資を輸出する等の違反行為をした者は、7 年以下の懲役又は輸出・経由・為替・仲介する物品等の価格の 5 倍に該当する金額以下の罰金に処される等規制への違反行為に罰則が規定されている。
		外国人投資促進法	本法に基づく対外送金、外国人投資によって外貨を逃避させた場合、1 年以上の有期懲役又は逃避額の 2 倍以上 10 倍以下に相当する罰金に処することとなっているほか、外国人投資企業の変更登録をしなかった者場合（5 年以下の懲役又は 5 千万ウォン以下の罰金）や、本法による許可又は申告に関連して偽書類を提出した場合（3 年以下の懲役又は 3 千万ウォン以下の罰金）などに罰則が適用される
		産業技術の流出防止および保護に関する法律	主に産業技術の流出及び侵害行為禁止について、最高で 15 年以下の懲役または 15 億ウォン以下の罰金といった罰則が規定されている。
		国家先端戦略産業競争力強化および保護に関する特別措置法	「産業技術の流出防止および保護に関する法律」と同様に、国家先端戦略技術の流出及び侵害行為禁止について、最高で 20 年以下の懲役または 20 億ウォン以下の罰金といった罰則が規定されている
		国家研究開発革新法	国家研究開発事業に関わる公務員とみなされる者は、業務遂行過程で知った秘密を他の人に漏洩したり、職務上目的以外の用途で利用した者は、2 年以下の懲役又は 2 千万ウォン以下の罰金に処される
		民・軍技術協力事業促進法	民・軍技術協力事業に参加した者は、参加過程で知った秘密を漏洩してはならず、違反した者は、3 年以下の懲役又は 3 千万ウォン以下の罰金に処される

（11）研究開発成果・知財の扱い

一定の条件の下研究開発実施主体に対して知的財産権を帰属させること、及び公共の利益のため政府にも一定の権利を帰属させる規程が共通して確認できた（表 5.1-15）。

表 5.1-15 共通した研究開発実施主体／政府への成果の帰属・知財の扱いに関する規程

国	研究開発実施主体への帰属	政府への帰属
日本	・ 日本版バイ・ドール制度を踏まえ一定の条件を付した上で受託した研究開発実施主体に帰属させることを各研究開発プログラムで確認	・ 国が公共の利益のために必要がある場合に、当該知的財産権を無償で国に実施許諾することがバイ・ドール制度適用の条件となる
米国	・ 35 U.S. Code Chapter 18（バイ・ドール法）や連邦政府機関の調達規則であるFAR Part27「特許、データ及び著作権」、DFARS252.227.7038「特許権-請負業者(大企業)による所有権」において請負業者が発明の所有権を保持することができる旨規定されている	・ 35 U.S. Code Chapter 18、FAR Part27、DFARS252.227.7038等において、合理的な理由なく研究開発実施主体が権利の保持を選択・報告しない場合に政府に所有権が譲渡される規程が存在する
英国	・ DEFCON705、UKRI、Innovate UK の標準助成規程において原則として知的財産権は研究開発実施主体に帰属するが、政府は内密に他の政府機関に開示・共有する権利を有する	・ MoD 関係機関の知的財産規程として DEFCON703 があり、適用される場合 MoD が知的財産権を所有し契約者には付与されない。保全が必要な機微な性質を有する業務などが該当する
韓国	・ 民軍協力事業促進法共同施行規定においては原則として知的財産権は研究開発実施主体に帰属する	・ 正当な理由なく研究開発実施主体が民軍技術強力事業の成果を活用しない場合、**政府の所有**とすることができる

日本との差異として、安全保障的側面から政府が成果の公表・帰属を制限することができる規程が個別に設定されていること等が挙げられる。差異が生じた理由としては、日本では学術研究の自主性・自律性の担保といった観点から研究開発成果の公表・活用制限に対しては慎重な姿勢が求められてきたことが考えられる（表 5.1-16）。

表 5.1-16　日本と差異のある研究開発実施主体／政府への成果の帰属・知財の扱いに関する規程

国	規程内容
米国	・ FAR Part27 において「対外諜報活動または防諜活動を行う権限を与えられている政府当局が、対象発明の所有権を保持する権利の制限または排除が、当該活動の安全を保護するために必要であると判断した場合」に発明の所有権を政府に譲渡することを研究開発実施主体に要求できると規定されている
英国	・ DEFCON705 において研究開発実施主体による成果の公表が国益に反する場合それを制限することができることが規定されている
韓国	・ 民軍協力事業促進法共同施行規定では国家安全保障上必要な場合、民軍技術協力事業によって生み出された研究成果を国家の所有とすることができる旨規定されている

5.2 研究開発の運営要領に関する比較・分析

(1) 研究テーマの選定プロセスに関する比較

政府の安全保障上のニーズに基づいたテーマ選定が共通して行われていることが確認できた。日本との差異としては、米国では PM が中心となって自律的なテーマ選定を行っている事や、英国・韓国では市場調査、需要調査などでより広範な成果の活用可能性について模索していることが挙げられる（表 5.2-1）

産業界・アカデミアからのニーズ調査等は、研究テーマ選定に際して政府のニーズ以外に市場規模の拡大・経済性や波及効果についての観点を加えることができ、より幅広い研究開発実施主体の参加を促すものと考えられる。

表 5.2-1　テーマ選定プロセスの共通・差異部分

国	共通したプロセス	日本と差異のあるプロセス
日本	安全保障技術研究推進制度では、防衛装備庁として、防衛分野での将来における研究開発に資することが期待できると考えて設定した研究テーマを公募している	―
米国	PM による軍・DOD 部局のニーズ調査がプロセスに含まれる	PM が自律的に行動し、軍・DoD の課題解決のための具体的なアイデアを研究者・技術者コミュニティから見つけ出す

国	共通したプロセス	日本と差異のあるプロセス
英国	DTEP で扱う研究テーマは、国務長官が承認した MoD の永続的能力（Enduring Capability）課題に合致していることが求められる	DASA は市場調査により既存のソリューション、開発中の新しいソリューション、および潜在的にさらなる投資が必要な分野を特定している
韓国	右の需要調査には、軍からの安全保障上のニーズが含まれる	関係行政機関は、輸出、市場規模の拡大、経済性、波及効果が期待され、民と軍の両部門に共通活用できる技術及び先端武器体系開発のための先端技術について、産・学・軍からの調査書の提出を

(2) 公募・採択プロセスに関する比較

資金配分機関が外部からアドバイザーを招き、提案とテーマとの合致、研究内容の革新性・計画性、コストパフォーマンスなどの観点から評価を行っていることが共通して確認できた（表 5.2-2)。

表 5.2-2　共通した公募・採択プロセス

国	共通したプロセス
日本	・　安全保障技術研究推進制度では、研究の発展性、将来性、有効性、効率性等について大学教授等の外部有識者からなる安全保障技術研究推進委員会が、科学的・技術的見地から評価
米国	・　PM 及び専門家によって、科学的・技術的メリット、国防上の課題解決・DARPA ミッションへの貢献、コスト・スケジュール・技術移転の計画及び能力等を評価
英国	・　戦略的適合性、エンドユーザのサポートの有無、技術的信頼性、革新性、リスク、専門的知識、コスト（コストパフォーマンス）、プロジェクトの実施計画といった観点から評価
韓国	・　民軍協力振興院などの専門機関の中に設置された技術別専門委員会によって RFP の充足、研究者の能力、費用・期間の適切性等を評価

日本との差異としては、提案事項の中に外国・懸念国との関係についての申告が含まれる点（米国）や、提案にあたり研究開発実施主体に支援を行うアドバイザーの存在（英国)、評価観点に安全保障上の課題解決可能性、商用化・実用化の可能性等が含まれている（米国、英国、韓国）ことが挙げられる。差異の生じた要因としては、安全保障技術研究推進制度が基礎研究を対象としたプログラムであり、かつ成果を直ちに防衛用途に活用することを目的としてないことが考えられる。

英国のように提案段階から研究開発実施主体に支援を行うアドバイザーが存在することは、研究開発実施主体の不安を低減し、効率的な提案・評価・採択に寄与するものと考えられる（表 5.2-3)。

表 5.2-3　日本と差異のある公募・採択プロセス

国	日本と差異のあるプロセス
米国	・　DARPA の PM は、専門家の意見を求めるが、最も魅力があると判断したプロジェクトを選択する権限を持っている ・　提案事項の中に外国・懸念国との関係についての申告が含まれる
英国	・　コンテストに関心がある場合は DASA が設置しているイノベーションパートナー に問い合わせを行うことができる ・　提案の段階からビジネスリレーションシップマネージャーが研究開発実施主体を支援
韓国	・　調査情報からは確認できなかった

(3) プロジェクトの評価・管理方法に関する比較

共通して資金配分機関のアドバイザー（PM、PO 等）が研究開発実施主体に対する助言や進捗状況の把握を行っていることが確認できたが、アドバイザーの関与度や進捗の把握頻度等については各国に差異が見られた。プログラムの目的にもよるが米英ではより積極的にアドバイザーが研究開発の実行に関与していることが確認できた（表 5.2-4）。

表 5.2-4　評価・管理方法に関する比較

国	アドバイザーの関与度	進捗状況の把握
日本	安全保障技術研究推進制度では、防衛装備庁所属の PO が担当する。PO は研究の円滑な実施の観点から必要に応じて研究計画や研究内容について調整、助言又は指導を行うが、PO が指導を行うのは、研究費の不正な使用及び不正な受給並びに研究活動における不正行為を未然に防止する必要がある場合のみ	・　全タイプ共通で研究期間終了後に終了評価を行うこととなっており、タイプ S のみ３年度目の１０月頃を目途に中間評価が行われる ・　中間評価は、研究課題の進捗状況等から必要に応じて実施される可能性がある
米国	プログラム・マネージャーは、DARPA の室長とその代理人に対して報告し、プログラムの進捗管理を担当する	・　SBIR フェーズⅡの採択後、受託した企業は年に一度、実際の売上と投資のデータを報告する必要がある。 ・　また、各フェーズで最終レポートの提出が求められている。 ・　月次のステータス及び進捗レポートが要求される場合がある
英国	【DASA】 DASA のスタッフとテクニカルパートナーの両方が、プロジェクトの期間中、サポートとアドバイスを行う 【DTEP】 ・　公募・採択プロセスで提案を支援	【DASA】 期間中、随時の進捗報告、中間報告書及び最終報告書の作成・提出が契約条件に基づき求められる 【DTEP】 モニタリング・オフィサーは定期的に

国	アドバイザーの関与度	進捗状況の把握
	した DASA のビジネス・リレーションシップ・マネージャーは、プロジェクトの実施中も採択された研究実施主体の支援を行う ・ プロジェクト全体を通してプロジェクトの進捗を監視するモニタリング・オフィサーがアサインされる。モニタリング・オフィサーは、プロジェクトのリスク、実績、資金がプロジェクトチームによって効果的に管理されていることを Innovate UK に保証する役割を果たす	面談（キックオフミーティング、四半期ごとのミーティング、最終的なクロージング）を行い、プロジェクトに関連する問題を観察、指導し、必要に応じてエスカレーションを行う
韓国	評価・管理については、民軍協力振興院などの専門機関の中に設置された技術別専門委員会によって実施されているが、関与度は不明	各プロジェクトの研究開発段階は基礎・応用・試験開発の 3 段階に分かれており、また研究成果に対する評価（ステージゲート審査）が毎年及び各研究段階の終了前にも行われることとなっている

(4) 知的財産権の扱い

研究開発実施主体に一定の条件下で知的財産権を帰属させるとともに、政府に一部権利を帰属させる規程が共通して確認できた。

知的財産権の活用に向けた取り組みには差異が確認できた。英国では知的財産ポートフォリオの形成や成果の輸出の可能性に関して助言を行うアドバイザーが存在し、また韓国ではプロジェクトが成功裏に終了した場合、成果を活用する企業と技術実施契約を結ぶことを義務付けていることなどが特徴的であり、成果の社会実装を促進するものと考えられる（表 5.2-5）。

表 5.2-5　知的財産権の帰属、活用に関する規程

国	知的財産権の帰属		知的財産権の活用に向けた規程
	研究開発実施主体への知的財産権の帰属	政府への知的財産権の帰属	
日本	知的財産権については、産業技術力強化法（日本版バイ・ドール規定）を踏まえた一定の条件を付した上で受託した研究実施機関に帰属	政府が公共の利益のために必要がある場合に、当該知的財産権を無償で国に実施許諾することがバイ・ドール制度適用の条件となる	調査情報からは確認できなかった
米国	提案に基づいて締結され	政府は契約の授与からプ	調査情報からは確認でき

国	知的財産権の帰属		知的財産権の活用に向けた規程
	研究開発実施主体への知的財産権の帰属	政府への知的財産権の帰属	
	た契約の下で開発された技術データやソフトウェアに関する権利は、一般的に契約業者に残る	ロジェクト完了後 20 年間、政府目的でこれらのデータを使用するための無償ライセンスを取得する	なかった
英国	DASA ではすべてのフォアグランド知的財産権は契約者（プログラムの採択者）に帰属する	DASA は、提供された技術情報および関連する知的財産を特定の目的で使用するための一連の権利を取得する DTEP の成果は MoD には帰属しない	DTEP ではビジネス・リレーションシップ・マネージャーが知的財産権ポートフォリオの形成や輸出について支援する
韓国	事業の遂行過程で得られる知的財産権、研究報告書の版権などの無形成果物は主管研究機関を原則とした研究開発実施主体に帰属する	事業を所管する中央行政機関は、安全保障上の必要性や公共の利益のため、成果が不当に活用されない場合は研究成果を国の所有にすることができる	最終評価結果が「成功」と判定された課題の研究開発結果所有機関の長は、結果通知後１ヶ月以内にその成果の実施企業と技術料徴収を含む技術実施契約を締結して成果を活用しなければならない

(5) 海外企業の参画に係る制約

研究開発代表者の本国への居住性や、懸念国との関係、外国投資規制など様々な観点で制限を加えていることが共通して確認できた。

日本との差異として、米国・英国・韓国では経済含む安全保障上の要件から海外企業の参画に制限を加えていることが確認でき、より明確なセキュリティ意識をもって規制を設けていることが伺える（表 5.2-6）。

表 5.2-6　海外企業の参画に係る制約

国	規程内容
日本	・　研究を実施する研究者（研究実施者）の所属する機関及び研究実施場所は、原則として全て日本国内に所在していることが必要となる ・　研究開発実施主体は国内に所在し、日本の法律に基づく法人格を有していることが必要 ・　研究代表者についても日本国籍を有すること、日本語による面接審査や評価に対応できることが求められる
米国	・　提案時に外国との提携又は外国との関係の開示をしなければならないので、懸念国との関係性が疑われる企業については、応募の段階で排除するものと思わ

国	規程内容
	れる
英国	・ プログラムによっては制限を設定する場合もあると想定される（DASA） ・ 国家保護保安局（NPSA）の Trusted Research ガイドラインの考慮及び NSI 法の要件に準拠する必要が言及されている（DTEP）
韓国	・ セキュリティ課題を外国政府・機関・団体等と共同研究を遂行しようとする場合は、中央行政機関の長の事前承認を得なければならない

(6) 他のプログラム・機関との差別化要素

日本では軍事・防衛に係る機関が公募する研究開発プログラムとしてはオープンな実施要領を規定することによって革新的な基礎研究を募集していることが挙げられる一方、米国、英国、韓国では成果の実用化や商業化、優秀な人材とのマッチングや産業界アドバイザーの設置などが差別化要素として挙げられた。安全保障技術研究推進制度については基礎研究のみを対象としている特性上、他国との差異が生じると予測できるが、米国、英国、韓国ではより成果の社会実装を意識した取り組みが実施されていると考えられる（表 5.2-7）。

表 5.2-7　各国機関の差別化要素

国	規程内容
日本	・ 安全保障技術研究推進制度では、研究者自身の考えで自主的・自律的に研究開発を行うように制限を撤廃し、軍事・防衛に係る機関が公募する研究開発プログラムとしてはオープンな実施要領を規定することによって、新領域の開拓や新たな波及効果等が期待できる、革新的な基礎研究の支援を図っている
米国	・ 革新的な研究を実施し、開発マイルストーンを達成するだけにとどまらず、技術ニーズの評価、市場分析、ビジネス準備計画の要素が盛り込んだ戦略による技術移行と商業化を研究開発実施主体向けのガイドラインで促している
英国	・ Ideas Marketplace（アイデアマーケットプレイス）というプラットフォームを設けており、英国のイノベーターが防衛とセキュリティの分野で優秀な人材と簡単に連携できる（DASA） ・ ビジネス・リレーション・マネージャーにより、産業界からのアドバイスを受けられる（DTEP）
韓国	・ 各課題が成功裏に終了したならば、終了後 1 ヶ月以内にその成果の実施企業と技術料徴収を含む技術実施契約を締結して成果を活用しなければならないことを規定している

6. 指定基金協議会の設置・運営に係る分析

分析にあたっては、特定重要技術の開発支援に向けた課題・方向性を検討するため、指定基金協議会の設置・運営に係る全体像を意識して、「研究開発の情報保全措置」に関する観点と、「研究開発の運営要領」の観点から分析を行うこととした（図 5.2-1、図 5.2-2）。

なお、課題・方向性の検討にあたり現在の特定重要技術の開発支援及び指定基金協議会の状況については関係法令の他、「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）[657]」（以下、基本指針）、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律第 62 条第 1 項に規定する協議会に関する協議会モデル規約 [658]」（以下、モデル規約）及び経済安全保障重要技術育成プログラム（K プログラム）の各種公表資料を参考とした。なお、比較に際しては、各研究開発プログラムで取り扱われる情報の機微度に差異がある点に注意が必要である。

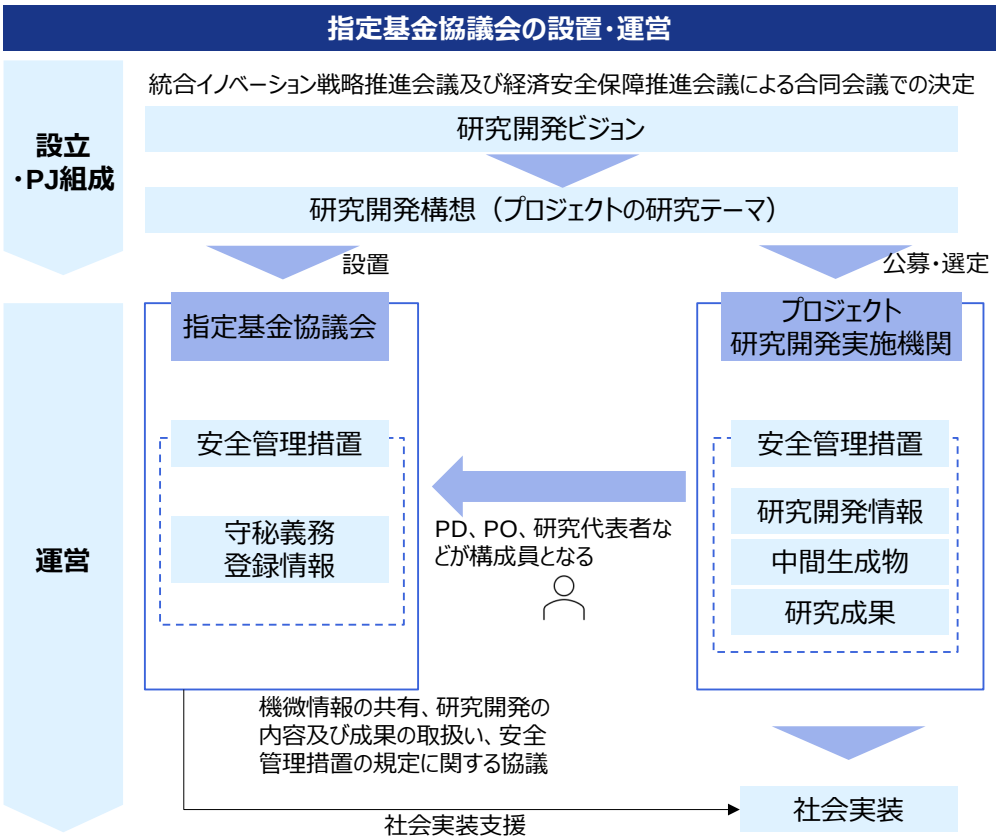


図 5.2-1　指定基金協議会の設置・運営の全体像 [659]

657 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin3.pdf

658 https://www.cao.go.jp/keizai_anzen_hosho/doc/3_kyogikai_mkiyaku.pdf

659 指定基金協議会モデル規約等公開情報を参考に NTT データ経営研究所作成

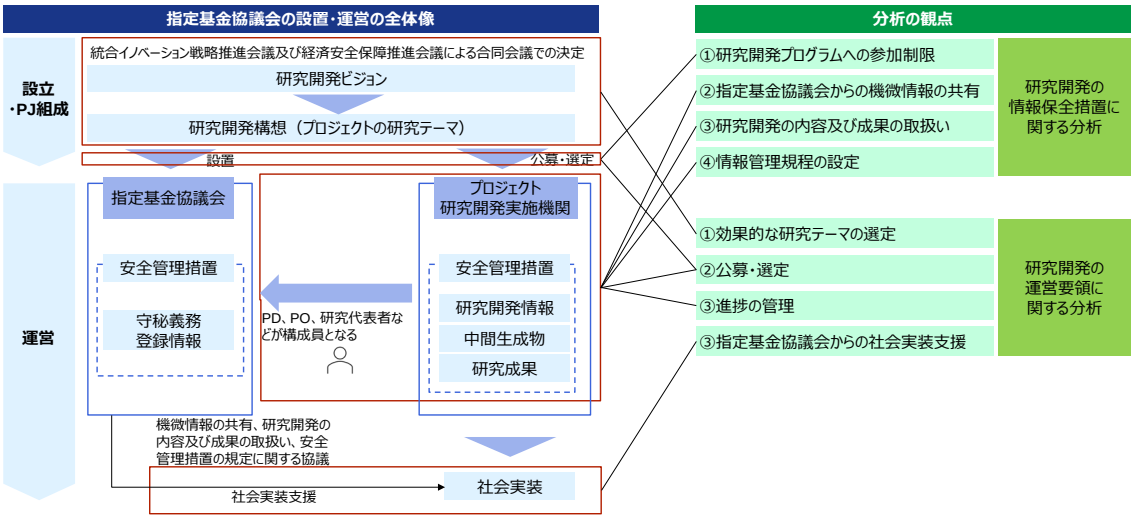


図 5.2-2　指定基金協議会の設置・運営の全体像と分析観点

6.1 情報保全措置に関する分析

（1）研究開発プログラムへの参加制限

米国・英国・韓国ではセキュリティ・クリアランスの取得や、外国主体との関係・研究開発実施主体の組織や運営に影響を及ぼす可能性の申告、研究開発実施主体及び所属する個人に対する背景・身上に係るデューデリジェンス等の参加制限措置が見られた（表 6.1-1）。

表 6.1-1　日本（Kプログラム）と各国の研究開発プログラムへの参加制限

項目	日本（Kプログラム）	米国	英国	韓国
審査対象	・ 研究提案者 ・ 研究代表機関 ・ 主たる研究分担者	・ 米国の大学、企業、非営利団体等 ・ 米国外の組織・個人	・ 英国に登録された企業、研究組織 ・ 英国外の企業・団体	・ 国内法に規定される大学、企業、非営利団体等 ・ 国外の組織・個人
主な基準	・ 研究開発拠点の所在 ・ 法人格 ・ 居住性 ・ 履行能力	・ セキュリティ・クリアランスの取得 ・ 懸念国との関係申告、特定の国家に対する制限 ・ 財務健全性・履行能力	・ セキュリティ・クリアランスの取得 ・ 身上に係るデューデリジェンスの実施 ・ 特定の国家に対する制限 ・ 財務健全性・履行能力	・ 軍・警察による身元調査の同意 ・ 財務健全性・履行能力
内容	・ 国内に研究開発拠点を有し、日本の法律に基づく法人格を有している機関に所属する日本の居住者＊であること（研究提案者） ・ 国内に研究開発拠点を有し、日本の法律に基づく法人格を有している機関であること（研究代表機関） ・ 日本の居住者であること（主たる研究分担者） ＊:外為法の居住者（特定類型該当者を除く）	・ 提案者はTop Secretのクリアランスを有し、SCIへアクセスできるメンバーを少なくとも1名確保（DARPA） ・ 海外拠点の有無や、懸念国（中国、北朝鮮、ロシア、イラン等）との関係を申告（DARPA） ・ 中国または中国が所有する企業または団体との二国間参加、協力、または調整を含んではならない（NASA）	・ 研究従事者へのデューデリジェンス実施のため、FORM388（人的詳細様式）を提出。SCレベルのクリアランスを保有する場合除外（DASA） ・ 外資事業を実施している企業の場合、NSI法を遵守（DASA） ・ 国外の企業・団体と協力する場合は輸出規制の影響に考慮（DASA） ・ ロシア起源の商品またはサービスを含む、ロシアの事業体に資金提供はされない（DASA）	・ 研究参加者は保安業務規定に基づく身元調査に同意（国防科学研究所） ・ 外国の機関と共同で研究を行う場合、関係行政機関の事前承認が必要（国家研究開発事業：セキュリティ課題）

(2) 指定基金協議会からの機微情報の共有

米国・韓国では機微情報の共有にあたり、情報の機密性レベルに応じた情報の取り扱いが統一的に規定されているため、当該要領に基づいた共有が成されているものと想定される。また機密情報を取り扱うための作業区域とネットワークへのアクセスの提供や金銭的な支援の規程によって支援を行っており、機密情報の共有を円滑化していると考えられる（表6.1-2)。

表 6.1-2　日本（Kプログラム）と各国の機微情報の共有

項目	日本（Kプログラム）	米国	英国	韓国
プログラムにおける機微情報の共有・保全の方法	・ 指定基金協議会を通じた機微情報の共有・保全方法は、協議会での議論を経て全会一致で決定されることとなる ・ 研究開発の進捗状況によっては、当初想定していた安全管理措置のレベルを超えた機微性の高い情報の取り扱いが発生した場合、安全管理措置の更新とそれに伴う施設の増改築、技術的アセットの導入等コストが必要となる可能性がある（弊社理解）	・ 大統領令 13526 号/32CFR part117(NISPOM)や大統領令第 13556 号/NIST SP800-171 などによって機密レベルに応じた情報の取り扱いが統一的に規定されているため、資金配分機関等政府機関から提供される機密情報についても、当該要領に基づくと想定される ・ DARPA ではこれまで機密を扱うことの無かった事業者に対して機密情報を取り扱うための作業区域とネットワークへのアクセスを支援する BRIDGES プログラムを実施している	・ 政府セキュリティ分類ポリシーなどによって機密レベルに応じた情報の取り扱いが統一的に規定されているため、資金配分機関等政府機関から提供される機密情報についても、当該要領に基づくと想定される	・ 保安業務規定、軍事機密保護法などによって機密レベルに応じた情報の取り扱いが統一的に規定されているため、資金配分機関等政府機関から提供される機密情報についても、当該要領に基づくと想定される ・ 機密性の高い研究開発を行う研究開発実施主体へのセキュリティ手当の支給に関する規程を設定している

(3) 研究開発の内容及び成果の扱い

米国・英国・韓国ではプログラムで取り扱う情報の機密性レベルや研究開発課題自体のセキュリティ等級の設定による研究開発の内容・成果の一律の保全レベルの基準や、安全保障上の必要性から成果の帰属・公表に対する制限が規定されている（表 6.1-3)。

表 6.1-3　日本（Kプログラム）と各国の研究開発の内容及び成果の扱い

項目	日本（Kプログラム）	米国	英国	韓国
事業者への成果の帰属	産業技術力強化法(日本版バイ・ドール制度)の適用を基本として、研究開発実施主体に帰属	35 U.S. Code Chapter 18 や FAR Part27、DFARS252.227.7038 等において請負業者が発明の所有権を保持することができる旨規定	DEFCON705、UKRI、Innovate UK の標準助成規程において原則として知的財産権は研究開発実施主体に帰属するが、政府は内密に他の政府機関に開示・共有する権利を有する	民軍協力事業促進法共同施行規定においては原則として知的財産権は研究開発実施主体に帰属する
成果の帰属・公表に係る制限	成果から守秘義務登録情報が直接的ないし実質的に了知されない限りにおいて守秘義務の対象とならず、その公表にあたっても一律の事前確認を研究開発実施主体へ求めることはない 成果は公開を基本とし、公開制限の一律の基準は設定されておらず、また協議会での議論の結果、参加者全員の合意を得なければ制限を課すことはない	DARPA のプロジェクトで扱う情報については大統領令 13526 号、13556 号に準拠して機密性レベルを設定 合理的な理由なく研究開発実施主体が権利の保持を選択・報告しない場合に政府に所有権が譲渡 対外諜報活動・防諜活動を行う政府当局が、発明の所有権を保持する権利の制限または排除が、当該活動の安全を保護するために必要と判断した場合に発明の所有権を政府に譲渡することを研究開発実施主体に要求する	DASA の公募で扱う情報についてはセキュリティ分類ポリシーに準拠して機密性レベルを設定し、契約条件を設定 保全が必要な機微な性質を有する業務には DEFCON703 が適用され、MoD に全ての権利が帰属する DEFCON705 において研究開発実施主体による成果の公表が国益に反する場合それを制限することができることが規定	実施される研究開発課題（プロジェクト）のセキュリティ等級を分類して、セキュリティ課題と一般課題に分けた管理を設定 正当な理由なく研究開発実施主体が民軍技術強力事業の成果を活用しない場合、政府の所有とすることができる 民軍協力事業促進法共同施行規定では国家安全保障上必要な場合、研究成果を国家の所有とすることができる旨規定

（4）情報管理規程の設定

米国・英国・韓国では、情報管理策の設定にあたっては開発推進会議体やプロジェクトに依らず情報の機密性に応じた統一的な情報管理策を各機関が参照する形をとっているほか、物理的・技術的な情報の保存・利用、管理、廃棄等の要領について技術標準や政府の認定規格等を参照することや、口頭情報、ハードコピー情報、電子情報といった情報の形態に沿った取扱要領を規定している（表 6.1-4）。

表 6.1-4　日本（Kプログラム）と各国の情報管理規程の設定

項目	日本（Kプログラム）	米国	英国	韓国
情報管理策の規程方法	・ 指定基金協議会の情報保全措置（情報管理規程）については、その具体的内容は、情報の性質や技術の進展状況等を踏まえ、協議会ごとに参加者全員の合意をもって決定	・ 資金配分機関の内規・助成規程に加え、研究開発実施主体の遵守すべき法令・ガイドラインとして、DoD 5220.22-M（国家産業安全保障プログラム）などが示され、そのプログラムで扱う機密情報のレベルに応じた取扱要領を一律に規定	・ 資金配分機関の内規・助成規程に加え、プログラムで取り扱う情報にはセキュリティ分類ポリシーに応じた機密性レベルが規定されており、該当するベースライン動作の準拠が求められる	・ 基本的に当該研究開発事業の根拠法の下位規則に則ったセキュリティ基準が適用される ・ 特定の要件に該当する場合、セキュリティ課題に分類されセキュリティ要件が高度になる ・ 国家機密を扱う場合は、当該機密の取り扱いを規定する法律（保安業務規定等）に準拠する
情報管理策の内容の特徴	・ 「特定重要技術研究開発協議会情報管理規程（モデル）」ではIC カード等による入退出管理を始めとした、機微な情報を取り扱う区域の管理、電子媒体・資料等を持ち出す際の漏えい・盗難の防止、データ等へのアクセスログの記録化といった組織的・人的・物理的・技術的な対策が図られていることが確認できる	・ 情報の利用・保管にあたり、GSA 認可のセキュリティ・コンテナ、連邦規格（FED STD）832 に従って構築された保管庫の使用を規定 ・ 情報の廃棄にあたり、NIST SP800-88、32 CFR 2001.47 などを参照して具体的基準を規定	・ 情報の利用・保管にあたりセキュリティ機器カタログ（CSE）で NPSA によって承認された物理セキュリティ機器、不正開封防止パッケージを指定 ・ 情報の破棄にあたり、CSE の製品を使用しての破壊を指定 ・ 口頭情報、ハードコピー情報、電子情報の形態ごとのベースライン動作を規定	・ 機密情報については情報の提供・共有に係る組織的管理策、取り扱い許可に係る人的管理策、保管場所・入退制限等の物理的管理策を主に規定 ・ 研究開発プログラムで参照される規則類では、情報端末へのアクセス手順や認証、ネットワークの閉域化等の技術的管理策についても規定

6.2 指定基金協議会の運営要領に関する分析

(1) 効果的な研究テーマの選定

米国・英国・韓国においては、政府の課題解決に繋がる具体的なアイデアを見つけるための広範な産官学コミュニティへのヒアリング、市場調査による潜在的な投資価値の把握、専門家であるPMによる自律的な企画立案といったプロセスが規定されている（表 6.2-1)。

表 6.2-1　日本（Kプログラム）と各国の研究テーマの選定

項目	日本（Kプログラム）	米国	英国	韓国
研究テーマの主な選定主体	・ 政府会議体 例:統合イノベーション戦略推進会議、経済安全保障推進会議、プログラム会議	・ 有識者 例：PM（プログラム・マネージャー） ・ 政府機関 例：DARPA	・ 政府機関 例：DASA（MoD）	・ 政府機関 例:民軍技術協力事業の関係行政機関 ・ 政府会議体 例：総括実務委員会、民軍技術協議会
主な選定プロセス・手法	・ プログラム会議において、各府省のシーズ・ニーズや大学･企業等における研究開発動向等を踏まえ研究開発ビジョン案を策定する ・ 研究開発ビジョン案は統合イノベーション戦略推進会議及び経済安全保障推進会議による合同会議での審議を経て決定され、それに基づき研究開発構想･公募要領として示される	・ DARPA による自律的な政府課題の特定、PM による主体的な課題解決のアイデアに関する研究者･技術者コミュニティからの情報収集、PM によるファンディング･プログラムの企画立案を経て、DARPA 局長等が承認する	・ DTEP で扱う研究テーマは、国務長官が承認した MoD の永続的能力（Enduring Capability)課題に合致していることが求められる ・ DASA ポータルサイト（DASA submission service）を通じた潜在的にさらなる投資が必要な分野の特定	・ 関係行政機関は、産・学・軍からの輸出、市場規模の拡大、経済性、波及効果が期待される技術に関する調査書の収集による、民間での活用性･軍での活用性の把握を行う ・ 調査結果に基づき、総括実務委員会、民軍技術協議会の審議を経て決定される

(2) 公募・選定

米国・英国では、意思決定機構/非意思決定機構を分けた評価体制の構築や、最終的な決定権を PM に委ねた公募・採択が実施されている（表 6.2-2)。

表 6.2-2　日本（Kプログラム）と各国の公募・採択

項目	日本（Kプログラム）	米国	英国	韓国
採択における評価の主な関係主体	・　資金配分機関 ・　PD・PO ・　関係府省（評価基準の提示）	（DARPA） ・　PM ・　外部専門家	（UKRI、Innovate UK） ・　プログラムボード（UKRI、政府省庁等） ・　アドバイザリーグループ（産学界） ・　チャレンジ・ディレクター	（民軍技術協力事業） ・　技術別専門委員会（内部及び外部の専門家、関係行政機関、軍関係者等）
主な評価基準	・　達成目標の妥当性、研究成果活用の実現可能性 ・　研究開発項目・内容、実施体制、資金計画、安全管理措置の妥当性　等	（DARPA：SBIR） ・　科学・技術的メリット ・　国防上の課題解決 ・　コスト、スケジュール ・　技術移転の計画・能力　等	（DASA：DTEP） ・　戦略的適合性 ・　エンドユーザのサポート ・　技術的信頼性、革新性　等	（民軍技術協力事業） ・　RFP（提案依頼書）の充足性 ・　研究方法の適切性 ・　研究者の能力 ・　事業化計画の卓越性　等
主な評価・採択の要領	・　資金配分機関は、専門的知見のあるPD・POを任命し、公募・採択における評価を実施 ・　資金配分機関は、PD・PO、資金配分機関の所管府省及び関係府省と連携して、公募・採択における評価基準を定めている	・　PMが評価に当たって外部の専門家と連携するが、最も実施価値の高いプロジェクトの選択権限はPMに委ねられている	・　UKRIのシニア・リーダーや政府省庁のシニア外部ステークホルダーで構成される意思決定機関たるプログラムボードと、産学界のステークホルダーで構成される非意思決定機関であるアドバイザリーグループがプロジェクトの選定に携わる ・　アドバイザリーグループのメンバー構成は、課題をよく理解するチャレンジ・ディレクターが構成案を作る	・　技術別専門委員会がRFPの充足性、計画性、研究者の能力などを考慮した評価を行う

(3) 進捗の管理

米国・英国では、PM による研究実施体制の変更も含めた進捗管理や、アドバイザーの設置による産業界からのアドバイスの提供、提案段階から継続した研究開発実施主体の支援、プロジェクトの難易度・リスクに応じた進捗管理責任者の業務範囲の設定等を行っている（表 6.2-3)。

表 6.2-3　日本（Kプログラム）と各国の進捗の管理

項目	日本（Kプログラム）	米国	英国	韓国
進捗管理・支援の主な実施主体	・　PD・PO ・　資金配分機関 ・　同所管省庁 ・　指定基金協議会参加府省（支援）	（DARPA） ・　PM	（UKRI、Innovate UK） ・　モニタリング・サービスプロバイダー （DASA） ・　ビジネス・リレーション・マネージャー	（民軍技術協力事業） ・　技術別専門委員会
主な責任範囲・支援内容の特徴	指定基金協議会では社会実装のイメージや研究開発の進め方についての議論・共有を行う 各プログラムでは PD・PO が進捗管理・評価を行う。PD・PO は担当する研究開発課題の進捗状況を常に把握し、プログラム会議の求めに応じて進捗状況報告を行うとともに、意見交換会への参加、他課題との連携等で支援する	DARPA では、PM が進捗管理を担当し、必要に応じ研究実行者を入れ替えや、プログラムの再構築までも行う SBIR プログラムでは、年に一度、定量的な事業成果を示すために実際の売上と投資のデータを報告する	・　UKRI、Innovate UK では、プロジェクト毎に割り当てられたモニタリングサービスプロバイダー（MSP）がプロジェクトの進捗状況の定期的なレビューや、研究開発実施主体側の責任者と連絡を取り、納品管理、財務管理等を行っている。 ・　DASA ではビジネス・リレーション・マネージャーの設置によって産業界からのアドバイスの提供や、提案段階から継続して研究開発プロジェクトの実施中にも研究開発実施主体を支援している	・　各プロジェクト（課題）の評価・管理については、民軍協力振興院などの専門機関の中に設置された技術別専門委員会によって実施される ・　各プロジェクトの研究開発段階は基礎・応用・試験開発の 3 段階に分かれており、また研究成果に対する評価（ステージゲート審査）が各研究段階の終了前にも行われる

(4) 社会実装の支援

米国・英国・韓国においては、商業化戦略策定のためのガイドラインの策定や、アドバイザーによる知的財産権ポートフォリオの形成や輸出規制への対応等についての支援、一定期間以内に成果活用先との技術実施契約の締結を行うことを研究開発実施主体の義務として規定する等実施している（表 6.2-4)。

表 6.2-4　日本（Kプログラム）と各国の社会実装の支援

項目	日本（Kプログラム）	米国	英国	韓国
社会実装支援の主な実施主体	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（指定基金協議会への参加省庁）	DARPA	(UKRI、Innovate UK) モニタリング・サービスプロバイダー (DASA) ビジネス・リレーション・マネージャー	民軍技術強力事業の所管関係行政機関
社会実装の主な支援内容・支援内容の特徴	指定基金協議会では社会実装のイメージや研究開発の進め方を議論・共有し、必要に応じ規制緩和の検討や国際標準化の支援など、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、組織の枠を超えた伴走支援を行う	DARPA の SBIR プログラムで、はSBIR プログラムから資金を受けた小規模ビジネス事業者に向けた商業化戦略策定ガイドラインを策定している	UKRI、Innovate UK ではチャレンジ・ディレクターが資金調達や産業界との連携に係る支援を行う DASA ではビジネス・リレーションシップ・マネージャーが研究開発実施主体に対して、知的財産権ポートフォリオの形成や輸出規制への対応等についても支援している	一定期間の間に成果の活用先との技術実施契約の締結を行うことを研究開発実施主体の義務としている 正当な理由なく研究開発実施主体が成果を活用しない場合は政府に成果が帰属される

7. Appendix

1）法令・ガイドライン等のロングリスト

2）研究機関等のロングリスト

3）研究開発実施主体に関する外部格付け機関の評価